

VILNIAUS PEDAGOGINIS UNIVERSITETAS

Rimantas Skrabutėnas

ALGEBRA IR SKAIČIŲ TEORIJA

(Paskaitų konspektas I)

I . Logikos ir aibių teorijos elementai.
Algebrinės struktūros ir skaičių sistemos

II . Tiesinės algebros pagrindai

Vilnius, 2004

Leidinyi apsarstyti ir rekomenduoti spaudai VPU Matematikos ir informatikos fakulteto algebros ir statistikos katedros posėdyje 2003 gegužės 23 d., protokolo Nr. 5.

Katedros nutarimas patvirtintas VPU Matematikos ir informatikos fakulteto tarybos posėdyje 2003 birželio 21., protokolo Nr. 29.

Recenzavo: *doc. dr. Liucija Griniuvienė,*
doc. dr. Gintautas Bareikis

Ž O D I S S K A I T Y T O J U I

Algebros ir skaičių teorijos kursas būsimesiems matematikos ir informatikos mokytojams skaitomas jau kelis dešimtmečius. Ši disciplina yra vienas iš bazinių aukštosios matematikos dalykų, suteikiančių Matematikos ir informatikos fakulteto studentams profesinio išsilavinimo pagrindus. Metams bėgant, kurso programa keitėsi: tai siaurėjo, tai vėl plėtėsi, tačiau ją dėstę katedros dėstytojai visada stengdavosi išryškinti itin tamprių algebros bei skaičių teorijos dalyko ryšį su mokykliniu matematikos kursu.

Šio leidinio autorius algebros ir skaičių teorijos paskaitas studentams - matematikams skaito bemaž tris dešimtis metų. Atsižvelgdamas į mūsų Universiteto tikslus ir čia stojančiųjų realias galimybes, stengiausi nesusižavėti dabar madingu moderniuoju dėstymo stiliumi, kai aukštas abstrakcijos laipsnis, savokų ir terminų gausa jaunam žmogui (dažnai, mūsų požiūriu, turinčiam nepakankamą pasiruošimą studijoms aukštojoje mokykloje) užgožia dalyko esmę, jau nekalbant apie minėtas sąsajas su mokykline matematika.

Pateikiamas paskaitų konspektas negali pakeisti vadovėlių ir uždavinynų, skirtų išsamioms algebros ir skaičių teorijos studijoms. Šis konspektas laikytinas pagalbine, studijų darbą sisteminančia priemone. Tačiau tikiuosi, kad leidinys bus naudingas ne tik studentams, bet ir matematikos - informatikos mokytojams. Konspektai, pagal atskiruose semestruose dėstomą tematiką, sąlyginai padalyti į keturias dalis, kurių kiekviena sudaryta iš atskirų, atitinkamai sunumeruotų paskaitų. Jose, savo ruožtu, išskirti potemiai.

Pagal atnaujintą studijų programą, *algebrą* numatoma dėstyti II ir IV semestruose, *skaičių teoriją* - III semest্রে, pirmajame semest্রে pateikiant įžanginį *diskrečiosios matematikos* (matematinės logikos elementai, aibių teorijos ir kombinatorikos pagrindai) modulį.

Be to, pirmuosiuose semestruose dar supažindiname su svarbiausiomis *algebrinėmis struktūromis* bei jų bendrosiomis savybėmis. Tuo pagrindu vėliau aksiomatiškai aptariamos *skaičių sistemos*, ypatingą dėmesį skiriant realiųjų skaičių lauko plėtimui, - kompleksiniams skaičiams.

Antrame semest্রে studijuojami *tiesinės algebros* pagrindai (tiesinių lygčių sistemos, matricos ir determinantai, vektorinės erdvės ir tiesiniai operatoriai), supažindinama su paprasčiausiais optimizavimo uždaviniais.

Trečiame semest্রে studijuojame *skaičių teoriją*.

ALGEBRA IR SKAIČIŲ TEORIJA

Ketvirtas semestras skiriamas *polinomų teorijai*. Įrodoma pagrindinė algebros teorema, vėl grįžtant prie pirmame semestre pradėtos algebrinių lygčių tematikos.

Visą, per keturis semestrus dėstomą medžiagą, apjungiame bendru pavadinimu „*algebra ir skaičių teorija*“.

Nuoširdžiai dėkoju recenzentams docentams *Liucijai Griniuvienei* ir *Gintautui Bareikiui*, kurių geranoriškos kritinės pastabos man buvo labai naudingos.

Autorius

Paskaita 1 – 01

Pirmoji užduotis: pakartoti *mokyklinės matematikos* kursą. Nemanykite, kad mokyklinės matematikos žinios toliau bus nereikalingos. Kaip tik atvirkščiai: tie, kas dar mokykloje gerai įsisavino matematikos pagrindus, žymiai tvirčiau jausis ir studijuodami matematiką - informatiką Universitete. Maža to, būsimasis mokytojas turi neblogai išmanyti ir daugelį kitų dalykų, o ypač – savo gimtąją kalbą.

Jei gerai išlaikėte *valstybinį matematikos egzaminą*, tai labai tikėtina, jog matematikos studijoms pasiruošta normaliai. Bet pakartoti mokyklines matematikos žinias patarčiau visiems.

Santrumpos. Taupant laiką ir vietą, konspekte dažnai naudojamos santrumpos. Nors tekste dauguma iš jų paaiškinamos, bet svarbiausias išvardijame jau dabar:

Ap	– apibrėžimas;
Įr	– įrodymas;
LF	– loginė formulė (forma);
KNF	– konjunkcinė normalioji forma;
DNF	– disjunkcinė normalioji forma;
PF	– predikatinė formulė (forma);
BS	– binaris sąryšis;
ES	– ekvivalentumo binaris sąryšis;
FS	– funkcinis binaris sąryšis (funkcija);
AO	– algebrinė operacija;
AS	– algebrinė struktūra;
KAD	– komutatyvumas, asociatyvumas ir distributyvumas;
MIP	– matematinės indukcijos principai;
AA	– Archimedo aksioma;
MSP	– mažiausiojo skaičiaus principas;
DSP	– didžiausiojo skaičiaus principas;
DP	– Dedekindio pjūvis;
KS	– kompleksinis skaičius;
TF	– kompleksinio skaičiaus trigonometrinė forma;
PŠ	– primityvioji (vieneto) šaknis;
TLS	– tiesinių lygčių sistema;
THLS	– tiesinių homogeninių lygčių sistema;
EP	– elementarieji pertvarkiai;
TN	– tiesiškai nepriklausomas (vektorių rinkinys);
TP	– tiesiškai priklausomas (vektorių rinkinys);
VE	– vektorinė erdvė;
EE	– Euklido erdvė;
TO	– tiesinis operatorius.

Matematinės kalbos pagrindai

Matematinės logikos elementai. Paprasti ir sudėtiniai teiginiai

Matematikoje plačiai naudojama tam tikra žymenų sistema bei formaliosios logikos samprotavimo taisyklės. Tai sutrumpina užrašus, sistemina matematinių faktų (teoremų) įrodymus. Matematikoje samprotaujama *teiginiais*.

Ap. **Teiginiu** vadinamas teigiamojo pobūdžio sakiny, kuris išreiškia tiesą arba netiesą.

Teiginius žymėsime raidėmis $p, q, r, \dots$. Kartais naudosime ir indeksus.

Jei teiginys p yra teisingas, sutrumpintai rašysime $\tau(p) = 1$, jei klaidingas, - $\tau(p) = 0$. (Dažnai rašoma dar trumpiau: $p = 1$ ir, atitinkamai, $p = 0$).

Yra *paprasti* ir *sudėtiniai* teiginiai. *Paprastais* (elementariaisiais) vadinami teiginiai, kurių negalima suskaidyti į sudėtinę dalį, kurios vėl būtų teiginiai. Pavyzdžiui, teiginys “*lauke dabar sniega*” yra paprastas (vasarą, – klaidingas) teiginys. Tuo tarpu teiginys “*Lietuva yra nepriklausoma valstybė ir Paryžius yra jos sostinė*” yra jau sudėtinis, nes jį sudaro paprasti teiginiai “*Lietuva yra nepriklausoma valstybė*” ir “*Paryžius yra jos sostinė*” sujungti žodeliu “ir”. Tokių sudėtinių teiginių teisingumą tiria matematinė logika. Gi paprastų teiginių teisingumo reikšmę nustatome remdamiesi mokslo žiniomis, savo patirtimi ar stebėjimo būdu. Pastarajame pavyzdyje pirmasis iš sudėtinį teiginį sudarančių teiginių yra teisingas, antrasis, – klaidingas, o viso sudėtinio teiginio teisingumo reikšmė kol kas neaiški.

Matematinėje logikoje atsiribojama nuo teiginių turinio ir domimasi tik jų teisingumu. Tad sudėtinis teiginys gali skambėti ir neįprastai. Pavyzdžiui, “*du kart du yra penki arba Paryžius nėra Lietuvos sostinė*”.

Loginės jungtys ir operacijos

Sudėtiniai teiginiai gaunami iš paprastųjų, panaudojant *logines jungtis*. Yra penkios *loginės jungtys* išreiškiamos žodžiais: “*arba*”, “*ir*”, “*jei, tai*”, “*tada ir tik tada*”, “*netiesa, kad*”. Jas atitinka penkios pagrindinės *loginės operacijos*: *disjunkcija*, *konjunkcija*, *implikacija*, *ekvivalencija*, *neiginy*. Tam, kad samprotavimuose galėtume nustatyti sudėtinių teiginių teisingumo reikšmes, įrodyti įvairius neakivaizdžius faktus, naudojame *loginių operacijų apibrėžimus*, *logikos dėsnius* ir *išvedimo taisykles*.

Ap. Jei p, q - bet kokie teiginiai, tai jų **disjunkcija** yra vadinamas naujas teiginys “ p arba q ”, kuris laikomas klaidingu tik kai abu disjunkcijos nariai p, q yra klaidingi.

Žymima $p \vee q$. Panašiai apibrėžiamos ir kitos keturios loginės operacijos. Jų apibrėžimus suformuluokite patys. Naudojami loginių operacijų žymėjimai ir (atitinkamu apibrėžimu nustatomos) jų teisingumo reikšmės, pateikiamos šioje lentelėje:

		Disjunkcija	Konjunkcija	Implikacija	Ekvivalencija	Neiginys
		p arba q	p ir q	jei p , tai q	p tada ir tik tada, kai q	netiesa, kad p
p	q	$p \vee q$	$p \wedge q$	$p \Rightarrow q$	$p \Leftrightarrow q$	$\bar{p}$
1	1	1	1	1	1	0
1	0	1	0	0	0	0
0	1	1	0	1	0	1
0	0	0	0	1	1	1

Dabar jau aišku, kad mūsų sudarytas sudėtinis teiginys “*Lietuva yra nepriklausoma valstybė ir Paryžius yra jos sostinė*”, pagal teiginių konjunkcijos apibrėžimą, yra klaidingas, o teiginys “*dukart du yra penki arba Paryžius nėra Lietuvos sostinė*”, pagal teiginių disjunkcijos apibrėžimą, yra teisingas, nors abiem atvejais tik vienas iš sudėtinį teiginį sudarančių paprastų teiginių yra teisingas.

Loginės formulės. Iš lentelėje išvardintų *pagrindinių formulių*, panaudojant, kaip ir paprastose algebroje, skliaustus, galima sudaryti kitas, sudėtinges *logines formules* (sutrumpintai: LF), kurių teisingumas nustatomas remiantis pateiktais lentelėje apibrėžimais. LF sudarymas grindžiamas tam tikrais reikalavimais, kurių visuma gali būti laikoma formaliu LF apibrėžimu.

Ap. Baigtinė simbolių seka iš aibės $\{p, q, r, \dots, \vee, \wedge, \Rightarrow, \Leftrightarrow, \bar{}, (,)\}$ sudaryta laikantis reikalavimų:

- $p, q, r, \dots$ laikomi LF (paprasčiausiomis);
- kai P ir Q yra LF, tai $(P \vee Q), (P \wedge Q), (P \Rightarrow Q), (P \Leftrightarrow Q), \bar{P}$ irgi yra LF;
- kitokių LF nėra,

vadinama LF.

Be to, susitarsime nerašyti išorinių skliaustų.

Pavyzdžiui, išraiška $\bar{q} \Leftrightarrow (p \Rightarrow (\bar{w} \vee r))$ yra LF, o seka $\bar{q} \Leftrightarrow (p \Rightarrow \wedge(\bar{w} \vee r))$ nėra LF, nes, pagal apibrėžimą, ženklai $\Rightarrow$ ir $\wedge$ negali stovėti greta.

Teiginius žyminčios raidės $p, q, r, \dots$ vadinamos *propozicinėmis raidėmis*. Kai formulėje yra k tokių raidžių, tai, sudarant jos *teisingumo lentelę*, iš viso reikia išnagrinėti 2^k atvejų. Pavyzdžiui, kadangi formulėje $q \Leftrightarrow (p \Rightarrow (w \vee r))$ yra keturios propozicinės raidės p, q, r ir w , tai jos teisingumo lentelėje, – 16 atvejų. Vienu iš jų, kai $p = q = r = w = 1$, ši LF yra teisinga.

LF, kuri visais galimais atvejais yra teisinga, vadinama *tautologija* ir žymima **1**, o LF, kuri visais galimais atvejais yra klaidinga, vadinama *prieštara* ir žymima **0**. Pavyzdžiui, formulė $(\bar{p} \vee q) \Leftrightarrow (p \Rightarrow q)$ yra tautologija, nes jos teisingumo lentelėje visose keturiose eilutėse yra vienetai:

p	q	$(\bar{p} \vee q) \Leftrightarrow (p \Rightarrow q)$
1	1	1
1	0	1
0	1	1
0	0	1

Ap. Dvi loginės formulės P ir Q vadinamos **ekvivalenčiomis**, jei jų teisingumo reikšmės visais galimais atvejais sutampa.

Žymėsime: $P \equiv Q$. Pavyzdžiui, $p \vee \bar{q} \equiv q \Rightarrow p$.

Ap. Sakome, kad formulė Q yra formulės P **loginė išvada**, jei Q yra teisinga visais tais atvejais, kai teisinga P .

Žymėsime: $P \rightarrow Q$. Pavyzdžiui, $p \wedge q \rightarrow p \vee q$.

Nesunku parodyti, kad :

- dvi loginės formulės P ir Q yra ekvivalenčios tada ir tikrai tada, kai jų ekvivalencija $P \Leftrightarrow Q$ yra tautologija,
- formulė Q yra formulės P loginė išvada tada ir tikrai tada, kai implikacija $P \Rightarrow Q$ yra tautologija.

Teiginių logikos dėsniai. Dvi ekvivalenčios LF nusako *matematinės logikos dėsni*. Logikos dėsniais ir grindžiami matematiniai samprotavimai įrodymuose. Štai keletas dažniausiai vartojamų dėsnių:

$p \vee q \equiv q \vee p$	– disjunkcijos komutatyvumo dėsnis,
$p \wedge q \equiv q \wedge p$	– konjunkcijos komutatyvumo dėsnis,
$p \vee (q \vee r) \equiv (p \vee q) \vee r$	– disjunkcijos asociatyvumo dėsnis,
$p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$	– konjunkcijos asociatyvumo dėsnis,
$p \vee p \equiv p \wedge p \equiv p$	– idempotencijos dėsniai,
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	– pirmasis distributyvumo dėsnis,
$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	– antrasis distributyvumo dėsnis,
$((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r) \equiv 1$	– silogizmo dėsnis,
$\bar{p} \vee q \equiv p \Rightarrow q$	– implikacijos keitimo disjunkcija dėsnis,
$p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$	– ekvivalencijos keitimo implikacija dėsnis,
$\overline{p \vee q} \equiv \bar{p} \wedge \bar{q}$	– pirmasis <i>de Morgano</i> dėsnis,
$\overline{p \wedge q} \equiv \bar{p} \vee \bar{q}$	– antrasis <i>de Morgano</i> dėsnis,
$p \Rightarrow q \equiv (p \wedge \bar{q}) \Rightarrow (r \wedge \bar{r})$	– suvedimo į prieštarą dėsnis,
$p \Rightarrow q \equiv \bar{q} \Rightarrow \bar{p}$	– kontrapozicijos dėsnis,
$p \vee \bar{p} \equiv 1$	– negalimo trečiojo dėsnis,

$$\underline{p} \wedge \overline{p} \equiv 0$$

– prieštaravimo dėsnis,

$$\underline{p} \equiv p$$

– dvigubo neigimo dėsnis ir t.t.

Čia **1** ir **0**, kaip minėjome, reiškia, atitinkamai, *visais atvejais teisingą* ir *visais atvejais klaidingą* loginę formulę. Visi šie dėsniai lengvai įrodomi sudarant atitinkamų LF teisingumo lenteles.

Tad teiginių logikoje tautologijos sąvoka yra labai svarbi. Norėdami patikrinti, ar formulė yra tautologija, galime sudaryti jos teisingumo lentelę, tačiau kai propozicinių raidžių yra daug, tai sudarinėti teisingumo lentelę yra neracionalu (pavyzdžiui, kai jų yra 10, – reiktų ištirti net $2^{10} = 1024$ atvejus). Tokiais atvejais dažnai naudojamos kitais metodais. Trumpai paminėsime vieną iš jų.

Normaliosios formos. Norėdami nustatyti, ar LF yra tautologija ar priešara, užrašome jai ekvivalenčias *konjunkcinę normaliąją formą* (KNF) arba, atitinkamai, *disjunkcinę normaliąją formą* (DNF).

Ap. Propozicinių raidžių arba jų neiginių disjunkcija vadinama elementariąja disjunkcija. Propozicinių raidžių arba jų neiginių konjunkcija vadinama elementariąja konjunkcija.

Ap. Formulė sudaryta iš elementariųjų konjunkcijų disjunkcijos ir ekvivalenti duotajai LF, vadinama pastarosios DNF. Formulė sudaryta iš elementariųjų disjunkcijų konjunkcijos ir ekvivalenti duotajai LF, vadinama jos KNF.

Pavyzdžiai. Formulė $\overline{p} \vee \overline{q} \vee r$ yra elementarioji disjunkcija, formulė $\overline{p} \wedge q \wedge r$ - elementarioji konjunkcija. Formulė $(p \wedge \overline{q}) \vee (\overline{p} \wedge q) \vee (\overline{p} \wedge \overline{q})$ yra formulės $p \Rightarrow \overline{q}$ DNF, o formulės $(p \vee q) \Rightarrow (r \wedge \overline{q})$ KNF yra $(\overline{p} \vee r) \wedge (\overline{q} \vee \overline{q})$.

Pasirodo, kad kiekviena LF turi (dažnai net ne vienintele) ir KNF, ir DNF. Be to, nesunku įsitikinti, kad:

- LF yra tautologija tada ir tik tada, kai į kiekvieną jos KNF elementariąją disjunkciją įeina nors viena propozicinė raidė kartu su savo neiginiu,

- LF yra priešara tada ir tik tada, kai į kiekvieną jos DNF elementariąją konjunkciją įeina nors viena propozicinė raidė kartu su savo neiginiu.

Pavyzdžiui, norėdami užrašyti jau minėtos LF $(\overline{p} \vee q) \Leftrightarrow (p \Rightarrow q)$ konjunkcinę normaliąją formą, nuosekliai pasinaudosime dėsniais:

$$P \Leftrightarrow Q \equiv (P \Rightarrow Q) \wedge (Q \Rightarrow P),$$

$$P \Rightarrow Q \equiv \overline{P} \vee Q,$$

$$P \wedge P \equiv P,$$

$$P \Rightarrow Q \equiv \overline{P} \vee Q,$$

$$\overline{P \vee Q} \equiv \overline{P} \wedge \overline{Q},$$

$$(P \wedge Q) \vee R \equiv (P \vee R) \wedge (Q \vee R)$$

ir turėsime:

$$\begin{aligned} (\bar{p} \vee q) &\Leftrightarrow (p \Rightarrow q) \equiv ((\bar{p} \vee q) \Rightarrow (p \Rightarrow q)) \wedge ((p \Rightarrow q) \Rightarrow (\bar{p} \vee q)) \equiv \\ &\equiv ((\bar{p} \vee q) \Rightarrow (\bar{p} \vee q)) \wedge ((\bar{p} \vee q) \Rightarrow (\bar{p} \vee q)) \equiv (\bar{p} \vee q) \Rightarrow (\bar{p} \vee q) \equiv \\ &\equiv ((\bar{p} \vee q) \vee (\bar{p} \vee q)) \vee (\bar{p} \vee q) \equiv (p \wedge \bar{q}) \vee (\bar{p} \vee q) \equiv (p \vee \bar{p} \vee q) \wedge (\bar{q} \vee \bar{p} \vee q). \end{aligned}$$

Tai ir yra ieškomoji KNF. Kadangi kiekvienoje jos elementariojoje disjunkcijoje yra propozicinė raidė kartu su savo neiginiu, tai LF yra tautologija.

Pastebėsime, kad tai nėra vienintelis KNF radimo kelias. Šiuo atveju galėjome elgtis kiek racionaliau, t.y. iš karto pakeisti implikaciją disjunkcija ir pasinaudoti dėsnio $P \Leftrightarrow P \equiv P \vee \bar{P}$.

Predikatai

*Ap. Teigiamojo pobūdžio sakiny su n kintamųjų, kuris virsta teiginiu kai vietoje visų kintamųjų įstatomos konkrečios reikšmės, vadinamas **n -viečiu predikatu**.*

Pavyzdžiui, sakiny “miestas x didesnis už miestą y ” yra dvivietis predikatas. Šis sakiny yra teigiamojo pobūdžio, bet nėra teiginys, nes nežinoma jo teisingumo reikšmė. Jeigu vietoje x įrašysime žodį “Ignalina”, o vietoje y – žodį “Briuselis”, tai gausime klaidingą teiginį: “miestas Ignalina didesnis už miestą Briuselį”.

Aišku, kad ne su visomis kintamųjų reikšmėmis predikatas virsta prasmingu teigiamojo pobūdžio sakiniu, kurio teisingumo reikšmę vienaip ar kitaip galima nustatyti. Pavyzdžiui, predikatas $x^2 \leq y^3 + z^3$, x – sui suteikus reikšmę “Vilnius”, y – kui reikšmę “matematika”, o z – tui – reikšmę “Nemunas” virsta beprasmiu sakiniu “Vilniaus kvadratas neviršija matematikos ir Nemuno kubų sumos”, o ne teiginiu.

Taigi kiekvienas predikatas turi tam tikrą *apibrėžimo* (prasmingumo) *sritį*. Mūsų pavyzdyje apie miestus tokia sritimi galėtų būti visos galimos miestų poros. Antrajame pavyzdyje tai galėtų būti sveikųjų skaičių trejetų aibė. Kiekvienu konkrečiu atveju tokia aibė arba nurodoma, arba yra aiški iš konteksto.

Predikatus žymėsime taip: $P(x)$, $Q(x, y)$, $T(x, y, z)$ ir t.t. Bet kuri lygtis ar nelygybė su n kintamųjų yra n -vietis predikatas. Pavyzdžiui, nelygybė $x^2 - 3y^3 < y + 2 \sin x$ yra dvivietis predikatas, kurį galime pažymėti $Q(x, y)$.

*Ap. Aibė $A_p := \{(x_1, x_2, \dots, x_n) \mid P(x_1, x_2, \dots, x_n) = 1\}$ yra vadinama **predikato $P(x_1, x_2, \dots, x_n)$ teisingumo aibe**.*

Kartais ta pati aibė A_p vadinama *predikatu $P(x_1, x_2, \dots, x_n)$ apibrėžiama aibe*.

Pavyzdžiui, predikato $P(x) := x^2 - 3x + 2 = 0$ teisingumo aibė yra $A_p = \{1, 2\}$. Tad iš mokyklos pažįstamas kvadratinės lygties $x^2 - 3x + 2 = 0$ sprendimo uždavinys šioje terminologijoje yra predikato $P(x)$ teisingumo aibės A_p nustatymo uždavinys.

Kvantoriai. Predikatas virsta (teisingu arba klaidingu) teiginiu, jei :

- visus kintamuosius pakeičiame konkrečiomis (galimomis, predikato apibrėžimo sričiai priklausančiomis) reikšmėmis arba
- panaudojame visuotinio bei egzistencijos **kvantorius**, kurie atitinkamai reiškia žodžius “su kiekvienu” bei “egzistuoja” ir žymimi simboliais $\forall, \exists$.

Pavyzdžiai. Sakinys “ $x \neq 3,14$ ” yra predikatas, o sakinys “ $(\forall x \in R) x \neq 3,14$ ” yra klaidingas teiginys. Sakinys “ $\sin x \leq 0,5$ ” yra vienvietis predikatas, kurį, sujungus su egzistencijos kvantoriumi $\exists$ gauname teisingą teiginį: “ $(\exists x \in R) \sin x \leq 0,5$ ”.

Nesunku suvokti tokio tipo teiginių *neigimo taisyklės*. Tereikia atidžiai perskaityti matematiniais simboliais užrašytą sakinį ir suprasti, ką jis tvirtina.

Pavyzdžiui, teiginys $(\forall x \in R) x^2 \neq 2$ tvirtina, kad “ne su visais realiaisiais x teisinga $x^2 \neq 2$ ”. Perfrazavus išplaukia, kad “yra realiųjų x – są, su kuriais $x^2 \neq 2$ yra klaidinga”, t.y. “yra realiųjų x – są, su kuriais $x^2 = 2$ ”. Simboliais:

$$(\forall x \in R) x^2 \neq 2 \equiv (\exists x \in R) x^2 \neq 2 \equiv (\exists x \in R) x^2 = 2.$$

Tad bendru atveju vienviečiam predikatui $P(x)$ yra teisingos taisyklės:

$$\overline{(\forall x)P(x)} \equiv (\exists x)\overline{P(x)} ; (\exists x)\overline{P(x)} \equiv (\forall x)\overline{P(x)}.$$

Pastebėsime, kad vienas kvantorius “suriša” tik vieną kintamąjį. Todėl, kai $P(x)$, $Q(x, y)$, $T(x_1, x_2, \dots, x_n)$ yra predikatai, tai sakiny $(\forall x)P(x)$ yra jau teiginys, o sakiniai $P_1(x) := (\forall y)Q(x, y)$, $T_1(x_1, x_3, x_4, \dots, x_n) := (\forall x_2)T(x_1, x_2, \dots, x_n)$ yra predikatai. Be to, $P_1(x)$ yra vienvietis, o $T_1(x_1, x_3, x_4, \dots, x_n)$ – $n-1$ – vietis predikatas. Pavyzdžiui, trivietis predikatas $x^2 \leq y^2 + 2z^2$, “surišus” kintamąjį x visuotinio kvantoriumi $\forall$, virsta dviviečiu predikatu $Q_1(y, z) := (\forall x)x^2 \leq y^2 + 2z^2$, pridėjus dar vieną visuotinio kvantorių, – vienviečiu predikatu $P_2(z) := (\forall x)(\forall y)x^2 \leq y^2 + 2z^2$. Pagaliau, jeigu predikato $x^2 \leq y^2 + 2z^2$ apibrėžimo sritimi laikysime aibę $R \times R \times R$, tai sakiny $(\forall x)(\forall y)(\exists z)x^2 \leq y^2 + 2z^2$ jau yra teisingas teiginys.

Predikatinės formos. Predikatai gali būti jungiami minėtų loginių jungčių pagalba taip gaunant sudėtinius predikatus, *predikatinės formos* (sutrumpintai: PF).

Jei $P(x)$ ir $Q(x)$ yra du vienviečiai predikatai, tai panašiai, kaip teiginių algebroje, loginių jungčių pagalba, gauname *pagrindines* PF: $\overline{P(x)}$, $P(x) \vee Q(x)$, $P(x) \wedge Q(x)$, $P(x) \Rightarrow Q(x)$, $P(x) \Leftrightarrow Q(x)$.

Kitas PF gauname iš šių pagrindinių formų, pagal taisyklės analogiškas LF sudarymui, t.y.: baigtinį skaičių kartų pavartoję predikatus žyminčias raides, logines jungtis bei skliaustus. Pavyzdžiui, išraiškos $(\overline{P(x)} \wedge Q(x)) \Rightarrow (Q(x) \vee P(x))$ bei $(Q(x) \wedge \overline{T(x)}) \Leftrightarrow (P(x) \Rightarrow T(x))$ yra PF.

Lygiai taip pat apibrėžiame ir daugiavietes predikatinės formas.

Atskiru atveju, kai n – viečiai predikatai $P(x_1, x_2, \dots, x_n)$ ir $Q(x_1, x_2, \dots, x_n)$ yra lygtys ar nelygybės, tai PF $P(x_1, x_2, \dots, x_n) \wedge Q(x_1, x_2, \dots, x_n)$ vadinama lygčių ar nelygybių (ar mišria) sistema ir žymima:

$$\begin{cases} P(x_1, x_2, \dots, x_n), \\ Q(x_1, x_2, \dots, x_n), \end{cases}$$

o predikatinė forma $P(x_1, x_2, \dots, x_n) \vee Q(x_1, x_2, \dots, x_n)$ vadinama lygčių, nelygybių (ar mišria) visuma ir žymima:

$$\left[P(x_1, x_2, \dots, x_n), Q(x_1, x_2, \dots, x_n) \right].$$

Ap. Dvi n – vietės PF $P(x_1, x_2, \dots, x_n)$ ir $Q(x_1, x_2, \dots, x_n)$ vadinamos **ekvivalenčiomis**, jei jų teisingumo aibės sutampa.

Rašome: $P(x_1, x_2, \dots, x_n) \equiv Q(x_1, x_2, \dots, x_n)$.

Pavyzdžiui, iš dviviečių predikatų $P(x, y) := 2x - 3y = 1$, $Q(x, y) := -x + 2y = 3$ ir $T(x, y) := (x + 1)^2 + (y - 1)^2 = 0$ sudarytos predikatinės formos $P(x, y) \wedge Q(x, y)$ ir $T(x, y)$ yra ekvivalenčios, nes $A_{P \wedge Q} = A_T = \{(-1, 1)\}$.

Apie aksiomas, teoremas ir įrodymus. Kiekviena matematinė teorija prasideda nuo pagrindinių (dažnai suprantamų intuityviai) sąvokų išskyrimo ir apibūdinimo. Jos kartais vadinamos *pirminėmis*. Pvz., tokios sąvokos geometrijoje yra: “taškas”, “tiesė”, “plokštuma”.

Kitos reikalingos sąvokos (pvz., geometrijoje: “atkarpa”, “laužtė”, “trikampis”) jau griežtai apibrėžiamos. Teiginiai, kurie nusako esminius pagrindinėmis sąvokomis apibrėžiamų objektų bruožus ir, kurie yra priimami be įrodymo, vadinami *aksiomomis*.

Atskiros matematikos srities aksiomų visuma vadinama tos srities *aksiomų sistema*. Tad galime kalbėti apie planimetrijos aksiomų sistemą, stereometrijos aksiomų sistemą, tikimybių teorijos aksiomų sistemą ir t.t.

Aksiomų sistemos suformulavimas konkrečiai matematinei teorijai nėra paprastas uždavinys. Kartais ilgai ir nesėkmingai bandoma kokios nors aksiomos atsisakyti, ją įrodant kaip teoremą. Pavyzdžiui, kelis šimtmečius buvo bandyta įrodyti, kad plokštumoje, per tašką, esantį šalia tiesės, tegalima nubrėžti vienintelę tai tiesei lygiagrečią tiesę. To įrodyti nepavyko. Dar daugiau, paaiškėjo, kad geometrijai priimtina ir kitokia aksioma: *tokių lygiagrečių yra daugiau nei viena*. Skirtumas tas, kad tada gauname kitokią, mums neįprastą (taip vadinamąją *neeuklidinę*) geometriją, kurioje trikampio vidaus kampų suma jau nėra lygi 180° ...

Pagrindiniai aksiomų sistemai keliami reikalavimai yra: sistemos *minimalumas*, *neprieštaringumas*, *pilnumas* ir *nepriklausomumas*.

Jei pavyksta sukonstruoti aibę, kurios elementams yra teisinga konkreti aksiomų sistema, tai ta aibė vadinama tos aksiomų sistemos *interpretacija*. Vėliau šiame semestre, aksiominiu būdu konstruosime įvairias skaičių sistemas: natūraliųjų skaičių sistemą, sveikųjų, racionaliųjų, realiųjų skaičių sistemas ir čia aptartas sąvokas dar kartą prisiminsime.

Teiginys, kurio teisingumas nėra akivaizdus, o reikalauja tam tikro loginio pagrindimo (įrodymo) dažnai vadinamas *teorema*. Pagalbinės teoremos dar vadinamos *lemomis*.

Teoremos paprastai formuluojamos loginės formulės $p \Rightarrow q$ pavidalu. Tokio pavidalo teorema vadinama *tiesiogine*. Teiginys p vadinamas *prielaida (sąlyga)*, teiginys q – *išvada*. Tada teorema $q \Rightarrow p$ vadinama *atvirkštine*. Atitinkamai, teoremos pavidalo $\bar{p} \Rightarrow \bar{q}$ bei $\bar{q} \Rightarrow \bar{p}$ vadinamos *priešingąja ir priešingąja atvirkštinei*. Pavyzdžiui, teoremą “*Jei trikampis yra statusis, tai jo statinių kvadratų suma lygi įžambinės kvadratu*” laikant tiesiogine, jai priešingoji teorema skambės taip: “*Jei trikampis nėra statusis, tai jokių jo dviejų kraštinių kvadratų suma nebus lygi trečiosios kraštinės kvadratu*”. Pasirodo, šios keturios teoremos sudaro dvi ekvivalenčių LF poras. Tiksliau, yra teisinga tokia teorema.

Teorema apie teoremas. *Tiesioginė teorema yra ekvivalenti priešingajai atvirkštinei, o atvirkštinė, - priešingajai.*

Trumpiau: $p \Rightarrow q \equiv \bar{q} \Rightarrow \bar{p}$, $q \Rightarrow p \equiv \bar{p} \Rightarrow \bar{q}$.

Įrodymui pakanka palyginti atitinkamas teisingumo lenteles.

Dažnai atsitinka, kad teoremą $\bar{q} \Rightarrow \bar{p}$ galima įrodyti paprasčiau negu tiesioginę teoremą $p \Rightarrow q$. Remiantis teorema apie teoremas, šitoks sukeitimas yra logiškai teisėtas ir kai kada vadinamas *netiesioginiu įrodymu*.

Kai teoremą $p \Rightarrow q$ pakeičiame viena iš jai ekvivalenčių loginių formų: $(p \wedge \bar{q}) \Rightarrow (r \wedge \bar{r})$, $(p \wedge \bar{q}) \Rightarrow \bar{p}$, $(p \wedge \bar{q}) \Rightarrow \bar{q}$, tai sakome, kad įrodinėjame “suvedant į prieštarą” (lot. *reductio ad absurdum*).

Pvz., teoremą “*jei sveikųjų skaičių a ir b suma yra nelyginis skaičius, tai vienas iš skaičių a , b yra nelyginis, o kitas - lyginis*”, įrodysime suvedimo į prieštarą metodu.

Tarkime, kad p : *sveikųjų skaičių a ir b suma yra nelyginis skaičius*, bet $\bar{q}$: *netiesa, kad vienas iš skaičių a , b yra nelyginis, o kitas, - lyginis*. Pastarasis teiginys ekvivalentus teiginiui: arba a , b abu lyginiai (t.y. $a = 2a'$, $b = 2b'$) arba a, b abu nelyginiai ($a = 2a'+1$, $b = 2b'+1$). Tačiau ir pirmuoju atveju $a + b = 2(a'+b') \rightarrow \bar{p}$, ir antruoju atveju $a + b = 2(a'+b'+1) \rightarrow \bar{p}$. Belieka pasinaudoti dėsniu $p \Rightarrow q \equiv (p \wedge \bar{q}) \Rightarrow \bar{p}$. Teorema įrodyta.

Teoremą pavidalo $p \Leftrightarrow q$ vadiname *teorema su būtina ir pakankama sąlyga*. Kadangi $p \Leftrightarrow q \equiv (p \Rightarrow q) \wedge (q \Rightarrow p)$, tai tokių teoremų įrodymas paprastai susideda iš dviejų dalių: *pakankamumo* $p \Rightarrow q$ ir *būtinumo* $q \Rightarrow p$.

Teoremos įrodymas, - tai mąstymo procesas, kurio metu, naudojantis aksiomomis, logikos dėsniais ir išvedimo taisyklėmis, iš duotų prielaidų baigtinio žingsnių skaičiaus pagalba išvedame teoremoje suformuluotus teiginius.

Paminėsime paprasčiausias tokio mąstymo schemas.

Teisingos išvados dėsnis (lot. *modus ponens*): jei teiginiai p ir $p \Rightarrow q$ teisingi, tai ir q yra teisingas.

Klaidingos išvados dėsnis (lot. *modus tollens*): jei teiginys $p \Rightarrow q$ yra teisingas, o q – neteisingas, tai ir p yra neteisingas.

Vienas svarbiausių matematiniuose įrodymuose yra *silogizmo dėsnis*: jei teiginiai $p \Rightarrow q$ ir $q \Rightarrow r$ yra teisingi, tai ir teiginys $p \Rightarrow r$ yra teisingas. Arba: *implikacija* $((p \Rightarrow q) \wedge (q \Rightarrow r)) \Rightarrow (p \Rightarrow r)$ yra tautologija.

Negalimo trečiojo dėsnis: iš dviejų teiginių p ir $\bar{p}$ vienas ir tik vienas yra teisingas.

Prieštaravimo dėsnis: teiginys $p \wedge \bar{p}$ yra prieštara.

Paskaita 1 – 02

Aibių teorijos elementai

Aibės. Teiginių algebrai analogiškas savybes turi ir *aibių algebra*. *Aibės* sąvoka matematikoje yra *pirminė*, neapibrėžiama, bet labai svarbi. Aibių *lygybė*, aibės *poaibis* bei *aibių veiksmas* jau griežtai apibrėžiami, o tų veiksmų savybės ir įrodomos, remiantis jau aptartais matematinės logikos dėsniais. Aibes įprasta žymėti didžiosiomis raidėmis: $A, B, C, \dots$

Ap. Aibė A yra vadinama aibės B poaibiu, kai kiekvienas A elementas yra tuo pat metu ir B elementas. Žymima $A \subset B$.

Simboliais tas pats apibrėžimas užrašomas taip:

$$\text{Ap. } A \subset B \equiv (a \in A) \rightarrow (a \in B).$$

Pastebėsime, kad ženklas $\rightarrow$ čia reiškia ne implikaciją, o *loginės išvados* sąryšį.

Pavyzdžiui, VPU Matematikos ir informatikos fakulteto studentų aibė M yra visų VPU studentų aibės V poaibis, t.y. $M \subset V$. Kartais naudojamas terminas “*viršaišis*”. Rašoma $V \supset M$.

Apibrėšime *aibių lygybę* (žymima $A = B$).

$$\text{Ap. } A = B \equiv ((a \in A) \equiv (a \in B)). \text{ Arba kitaip: } A = B \equiv (A \subset B \wedge B \subset A).$$

Aibę galima nusakyti išvardijant jos elementus, arba predikatu nurodant jos elementams būdingą požymį, dėsningumą. Pvz., $A = \{a \mid a \leq 1\}$, $B = \{\pi, 0, \sqrt{2}\}$, $C = \{5, 10, 15, 20, \dots\}$. Beje, užrašas $C = \{n \mid n = 5k, k \in N\}$ yra tikslesnis, nei elementų vardinimas, kuris, ypač begalinės aibės atveju, visada palieka nevienareikšmiškumo galimybę.

Raide $\emptyset$ žymime tuščią (neturinčią nė vieno elemento) aibę, o raide U žymime *universalią aibę*, t.y. aibę, kuriai teisinga savybė: $(\forall A) A \subset U$. Kartais universali aibė žymima raide I ar dar kitaip. Universalioji aibė nėra nusakoma vienareikšmiškai. Tai priklauso nuo to, kokiomis aibėmis operuojame. Mokiny, mokydamasis temą “sveikųjų skaičių daugyba”, nagrinėja tik sveikųjų skaičių aibės poaibius, todėl jis gali laikyti, kad $U = Z$. Sociologas tiria tam tikras žmonių grupes, todėl jam universali aibė yra tos vietovės gyventojų aibė.

Aibių veiksmas. Apibrėžiami šie veiksmas: *aibių sudėtis*, *aibių daugyba*, *aibių atimtis*, *aibių Dekarto daugyba*. Atkreipiame dėmesį, kad loginių operacijų ir jų rezultatų pavadinimai buvo vienodi, o aibėms, – jau skirtingi. Pvz., aibių A ir B sudėties rezultatas vadinamas *aibių suma* (*sąjunga*). Žymima $A \cup B$.

$$\text{Ap. } A \cup B := \{a \mid a \in A \vee a \in B\}.$$

Žodžiais šį apibrėžimą galima suformuluoti šitaip: “**aibių A ir B suma** yra nauja aibė sudaryta iš visų elementų, priklausančių bent vienai iš aibių A, B ”.

$$\text{Pavyzdžiui, kai } A_0 = \{0, 2, 5\}, \text{ o } B_0 = \{a, -2, 0, 5\}, \text{ tai } A_0 \cup B_0 = \{a, -2, 0, 2, 5\}.$$

Atkreipkite dėmesį, kad, vardindami aibės elementus, pasikartojančius pažymime *tik vieną kartą*.

Aibių *daugybės*, *atimties*, *Dekarto daugybės* rezultatai vadinami, atitinkamai: **aibių sankirta** (*pjūviu*) ir žymima $A \cap B$, **aibių skirtumu**, kuris žymimas $A \setminus B$ ir **aibių Dekarto sandauga**, kuri žymima $A \times B$. Tai – *naujos aibės* kurios apibrėžiamos taip:

$$\text{Ap. } A \cap B = \{a \mid a \in A \wedge a \in B\}.$$

$$\text{Ap. } A \setminus B = \{a \mid a \in A \wedge a \notin B\}.$$

$$\text{Ap. } A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

(Uždutis: šiuos apibrėžimus suformuluokite žodžiais.)

Skirtumas $U \setminus A$ vadinamas aibės A **papildiniu** ir žymimas $\overline{A}$.

$$\text{Ap. } \overline{A} := U \setminus A := \{a \mid a \in U \wedge a \notin A\} = \{a \mid a \notin A\}.$$

Pavyzdžiai. Aibėms A_0, B_0 gausime: $A_0 \cap B_0 = \{0, 5\}$, $A_0 \setminus B_0 = \{2\}$, $A_0 \times B_0 = \{(0, a), (0, -2), (0, 0), (0, 5), (2, a), (2, -2), (2, 0), (2, 5), (5, a), (5, -2), (5, 0), (5, 5)\}$.

Norėdami užrašyti aibes $\overline{A_0}$ ir $\overline{B_0}$, turime apsispręsti, kokia (mūsų situacijoje) yra universalioji aibė U . Jei, tarkime, $U = \{a, b, c, -2, -1, 0, 1, 2, 3, 4, 5\}$, tai:

$$\overline{A_0} = U \setminus A_0 = \{a, b, c, -2, -1, 1, 3, 4\}, \quad \overline{B_0} = \{b, c, -1, 1, 2, 3, 4\}.$$

Aibių veiksmų savybės. Pateiksime keletą įprastų aibių veiksmų savybių. Pabrėžiame, kad visos savybės yra *įrodomos*, remiantis jau aptartais matematinės logikos faktais. Atkreipkite dėmesį ir į tai, kad žemiau išvardintos savybės yra analogiškos *logikos dėsniams*.

$$A \cup A = A \cap A = A, \quad \text{- idempotencijos savybės,}$$

$$A \cup B = B \cup A, \quad A \cap B = B \cap A, \quad \text{- komutatyvumo savybės,}$$

$$A \cup (B \cap C) = (A \cup B) \cap C, \quad \text{- asociatyvumo savybės,}$$

$$A \cap (B \cup C) = (A \cap B) \cup C.$$

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C), \quad \text{- distributyvumo savybės,}$$

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C),$$

$$(A \setminus B) \cap C = (A \cap C) \setminus (B \cap C),$$

$$(A \cup B) \times C = (A \times C) \cup (B \times C).$$

$$A \cup \emptyset = A \cap U = A, \quad A \cap \emptyset = \emptyset,$$

$$(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D),$$

$$\overline{A \cup B} = \overline{A} \cap \overline{B}, \quad \overline{A \cap B} = \overline{A} \cup \overline{B} \quad \text{- de Morgano dėsniai.}$$

$$\text{Bet: } A \times B \neq B \times A, \quad (A \times B) \times C \neq A \times (B \times C).$$

Pavyzdžiui, įrodysime, kad su bet kokiomis aibėmis A, B, C yra teisinga lygybė

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C).$$

Tarkime a yra bet koks aibės $(A \cap B) \cup C$ elementas. Tada, pasinaudoję aibių sąjungos ir sankirtos apibrėžimais, galėsime užrašyti, kad:

$$a \in (A \cap B) \cup C \equiv (a \in A \cap B) \vee (a \in C) \equiv (a \in A \wedge a \in B) \vee (a \in C).$$

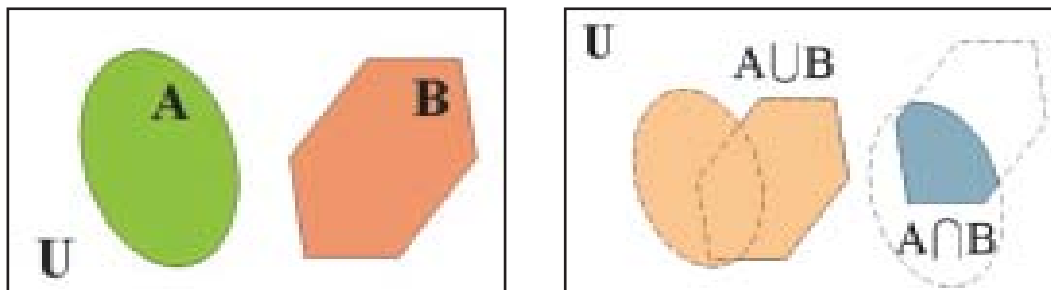
Dabar pasinaudosime dėsniais: $(p \wedge q) \vee r \equiv (p \vee r) \wedge (q \vee r)$ ir, dar sykių - aibių sąjungos ir sankirtos apibrėžimais:

$$\begin{aligned} (a \in A \wedge a \in B) \vee (a \in C) &\equiv (a \in A \vee a \in C) \wedge (a \in B \vee a \in C) \equiv \\ &\equiv (a \in A \cup C) \wedge (a \in B \cup C) \equiv a \in (A \cup C) \cap (B \cup C). \end{aligned}$$

Tad gavome, kad $a \in (A \cap B) \cup C \equiv a \in (A \cup C) \cap (B \cup C)$, su visais a . O tai, pagal aibių lygybės apibrėžimą, ir reiškia, kad $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.

Tiesa, dar reiktų aptarti situaciją, kai aibė $(A \cap B) \cup C$ yra tuščia. Bet tada, vėl remdamiesi sąjungos ir sankirtos apibrėžimais, lengvai išvedame, kad turi būti tuščia ir aibė $(A \cup C) \cap (B \cup C)$. Įrodymas baigtas.

Veiksmus su aibėmis ir tų veiksmų savybes dažnai iliustruoja brėžiniais, kuriuose universalioji aibė U vaizduojama kokia nors plokštumos figūra (kvadratu, stačiakampiu ar skrituliu), o visos aibės, – tos figūros dalimis. Pavyzdžiui:



Tokie piešiniai vadinami *Oilerio – Veno diagramomis*.

(Užduotis: dar keletą iš pateiktų savybių įrodykite remdamiesi matematinės logikos dėsniais; nubraižykite atitinkamas Oilerio – Veno diagramas.)

Aibė $A \times A$ vadinama aibės A Dekarto kvadratu ir žymima: $A \times A = A^2$. Aibių sąjungos (sumos), sankirtos, Dekarto sandaugos sąvokas nesunku apibendrinti ir daugiau nei dviejų aibių atveju. Pavyzdžiui, kai $A_1, A_2, \dots, A_n$ yra bet kokios aibės, tai jų suma yra nauja aibė, kuri apibrėžiama taip:

$$\bigcup_{k=1}^n A_k := A_1 \cup A_2 \cup \dots \cup A_n = \{a \mid a \in A_1 \vee a \in A_2 \vee \dots \vee a \in A_n\}.$$

Pamėginkite savarankiškai apibrėžti kelių aibių sankirtą ir Dekarto sandaugą.

Kai iš konteksto aišku, kad raidės A, B, C, D, F, H reiškia būtent aibes, – vietoje simbolių $A \cup B, D \cap F, C \setminus H$ vartojami įprasti žymenys: $A + B, DF, C - H$.

Binariai sąryšiai

Sąryšio tarp kokių nors objektų (aibių elementų) sąvoka ir realiame gyvenime, ir matematikoje nesunkiai suprantama intuityviai. Jei turime kokias nors aibes A, B , tai jų elementus (kiekvieną atskirai, ar elementų poras, ar trejetus...) gali sieti kokie nors *sąryšiai* (t.y. bendros savybės, požymiai). Jei sąryšis sieja aibių A ir B elementus, tai jis vadinamas sąryšiu *tarp aibių* A ir B . Jei sąryšis sieja aibės A elementus, tai jis vadinamas *sąryšiu aibėje* A . Atskirus elementus siejantis sąryšis vadinamas *unariniu*, elementų poras siejantį sąryšį vadinsime **binariu sąryšiu** (BS), trejetus – *ternariniu* ir t.t. BS žymėsime viena raide σ, τ, ω, f ir pan. Pavyzdžiui, jei aibėje N apibrėšime binarį sąryšį σ žodžiais: “du natūralieji skaičiai m ir n susieti sąryšiu σ , jei $m = n^2$ ”, tai galėsime užrašyti: $4 \sigma 2, 25 \sigma 5$, bet: $5 \overline{\sigma} 25, 6 \overline{\sigma} 7$.

Panaudojant aibių Dekarto sandaugos sąvoką, BS galima apibrėžti griežčiau.

Ap. Binariu sąryšiu tarp aibių A ir B vadiname bet kokią aibės $A \times B$ poaibį σ .

Ap. Binariu sąryšiu aibėje A vadiname bet kokią aibės A^2 poaibį τ .

Aukščiau aprašytas binaris sąryšis $\sigma \subset N^2$ apibrėžiamas taip: $\sigma := \{ (n^2, n) \mid n \in N \}$.

Svarbesnieji BS tipai. Savybės

Ap. BS $\sigma \subset A \times A$ vadinamas refleksyviu, jei

$$(\forall a \in A) a \sigma a.$$

Pvz., tiesių lygiagretumas yra refleksyvus BS, nes kiekviena tiesė yra lygiagreti pati sau. Gi tiesių statmenumo BS, akivaizdu, nėra refleksyvus.

BS vadinamas *antirefleksyviu*, kai nė vienas aibės A elementas nėra tuo sąryšiu susietas pats su savimi. Pavyzdžiui, studentų aibėje įvedę sąryšį “mažesnis” (ūgio prasme), turėsime antirefleksyvaus BS pavyzdį.

Ap. BS $\sigma \subset A \times A$ vadinamas simetrišku, jei teisinga

$$(\forall a, b \in A) (a \sigma b) \Rightarrow (b \sigma a).$$

Pvz., tiesių statmenumo BS yra simetriškas.

Naudojamas ir terminas *antisimetriškas* BS: tai toks BS, kuriam teisinga:

$$(\forall a, b \in A) (a \sigma b) \Rightarrow (b \overline{\sigma} a).$$

Pvz., žmonių aibėje BS “vyresnis” (amžiaus prasme) yra antisimetriškas.

Ap. BS $\sigma \subset A \times A$ vadinamas tranzityviu, jei teisinga

$$(\forall a, b, c \in A) ((a \sigma b) \wedge (b \sigma c)) \Rightarrow (a \sigma c).$$

Pvz., dalumo sąryšis sveikųjų skaičių aibėje yra tranzityvus. Tuo tarpu draugystės sąryšis žmonių aibėje nėra tranzityvus ☹.

Ap. Sakome, kad BS $\sigma \subset A \times A$ turi trichotomijos savybę, jei bet kuriems $a, b \in A$ teisingas vienas ir tiksliai vienas iš teiginių:

$$1) a \sigma b; \quad 2) b \sigma a; \quad 3) a = b.$$

Pvz., dalumo sąryšis sveikųjų skaičių aibėje trichotomijos savybės neturi. Tuo tarpu sąryšis “mažiau” realiųjų skaičių aibėje turi trichotomijos savybę.

Ekvivalentumo sąryšiai ir aibės faktorizavimas

Ap. BS $\sigma \subset A \times A$ vadinamas **ekvivalentumo sąryšiu** (ES), jei jis yra refleksyvus, simetrinis ir tranzityvus vienu metu.

Pvz., tiesių lygiagretumas yra ES.

Toliau mes dažnai naudosimės šia svarbia teorema.

Faktorizavimo teorema. Jei aibėje A yra apibrėžtas ES σ , tai jo pagalba aibę A galima suskaidyti į poaibius (ekvivalentumo klases), neturinčius bendrų elementų.

Įr. 1. Suskaidymo galimumas. Kai $a \in A$, pažymėkime:

$$K_a = \{b \mid b \in A \wedge b \sigma a\}.$$

Tuokart akivaizdu, kad

$$A = \bigcup_{a \in A} K_a,$$

t.y. aibės K_a , $a \in A$ ir yra teoremoje įvardinti poaibiai – *ekvivalentumo klasės*.

2. Belieka pasiekti, kad visos ekvivalentumo klasės kas dvi neturėtų bendrų elementų, t.y. skirtingoms klasėms K_a, K_b galiotų sąlyga: $K_a \cap K_b = \emptyset$. Pasirodo, tam pakanka tik pareikalauti, kad klases generuojantys elementai a, b būtų nesusieti ES σ . Iš tikrųjų, jeigu paimtume $a \bar{\sigma} b$, bet tartume, kad:

$$(\exists c \in A) c \in K_a \wedge c \in K_b,$$

tai, pasinaudoję sąryšio σ tranzityvumu, gautume:

$$(a \sigma c) \wedge (c \sigma b) \rightarrow (a \sigma b),$$

o tai prieštarauja pradinei prielaidai $a \bar{\sigma} b$. QED.

Ap. Iš visų ekvivalentumo klasių sudaryta aibė $A/\sigma := \{K_a, K_b, K_c, \dots\}$ vadinama *faktoraibe*.

Pastaba. Raidės QED, užbaigiančios teoremos įrodymą, yra sakinio lotynų kalba “quod erat demonstrandum” (tai ir reikėjo įrodyti), santrumpa.

Funkciniai sąryšiai

Ap. BS $f \subset A \times B$ vadinamas **funkciniu sąryšiu** (sutrumpintai: FS), arba atvaizdžiu, arba tiesiog – funkcija, jei teisinga:

$$((x, y_1) \in f \wedge (x, y_2) \in f) \Rightarrow y_1 = y_2.$$

Terminai ir žymenys: jei $f \subset A \times B$ yra FS ir $(x, y) \in f$, tai sakome, kad y yra x – *so vaizdas*, o x yra y – *ko pirmavaizdis* (originalas). Žymime: $A \xrightarrow{f} B$, $x \xrightarrow{f} y$ arba įprasčiau $y = f(x)$.

Funkciją galima apibrėžti labai įvairiai: formule, lentele, žodžiais, grafiku. Viena iš paprasčiausių yra *tiesinė* funkcija: $y = ax + b$. Jos *grafikas* yra tiesė.

Kartais sakoma, kad funkcija yra *apibrėžta aibėje* A , o *reikšmes* *igyja aibėje* B . Jei taisyklę f į aibę B atvaizduojame tik aibės A poaibį A_0 , tai sakome, kad funkcija *apibrėžta aibėje* $A_0 \subset A$, arba: funkcijos *apibrėžimo sritis* yra aibė A_0 . Funkcijos *apibrėžimo sritį* žymėsime simboliu D_f , t.y.:

$$D_f := \{x \mid x \in A \wedge (\exists y \in B)(x, y) \in f\} = A_0.$$

Tuo atveju, kai funkcinio sąryšio f apibrėžimo sritis D_f sutampa su aibe A , dažnai vartojami terminai, apibūdinantys specialius FS (atvaizdžius): *siurjekciją*, *injekciją* ir *bijekciją*.

Įveskime žymenį:

$$E_f = \{y \in B \mid (\exists x \in A)f(x) = y\}.$$

Aibę E_f vadinsime funkcinio sąryšio *reikšmių sritimi*. Tuo atveju, kai $D_f = A$, reikšmių sritį vadinsime (*pilnuoju*) *aibės* A *vaizdu* ir žymėsime $E_f = f(A)$.

Ap. Jei $f(A) = B$, tai FS f vadinamas **siurjekcija**.

Ap. Jei $f(A) \subset B$ ir kiekvienam vaizdui yra tiksliai vienas pirmavaizdis, tai FS f vadinamas **injekcija**.

Pasakykite tiksliau: kiekvienas aibės B elementas turi ne daugiau kaip vieną pirmavaizdį. Tuo norima pabrėžti: jei $y \in f(A)$ tai jo pirmavaizdis x yra tiksliai vienas. Jeigu gi $y \notin f(A)$, tai y nėra vaizdas, todėl *pirmavaizdžio* apskritai neturi.

Ap. FS f vadinamas **bijekcija** (arba: *abipus vienareikšmišku atvaizdžiu*), jei jis yra ir *siurjekcija*, ir *injekcija* tuo pat metu.

Pavyzdžiai. Jeigu $A = [0, \pi]$, $B = [-1, 1]$, o $f = \cos$, tai atvaizdis $A \xrightarrow{\cos} B$ yra bijekcija; imant $A = [-\pi, \pi]$, $B = [-1, 1]$, taisyklė $f = \cos$ yra siurjekcija, o kai $A = [0, \pi]$, $B = [-2, 2]$, tai ta pati taisyklė $f = \cos$ yra injekcija.

Dabar prisiminkime, “mokyklinį” funkcijos apibrėžimą:

Ap. Taisyklė arba dėsniš f , pagal kurį kiekvienam aibės X elementui x priskiriamas vienintelis aibės Y elementas y , vadinama *atvaizdžiu* arba *funkcija*.

Ar pastebite, kai šis apibrėžimas reikalauja to paties, kaip ir funkcinio BS apibrėžimas? Taigi, – abu apibėžimai yra *ekvivalentūs*.

Tvarkos sąryšiai

Ap. BS $\tau \subset A \times A$ vadinamas **tiesinės tvarkos sąryšiu**, jei jis yra *antirefleksyvus*, *tranzityvus* ir turi *trichotomijos savybę*.

Jeigu aibėje A yra apibrėžtas tiesinės tvarkos sąryšis, tai aibė vadinama *sutvarkyta*.

Pavyzdžiui, žodyno žodžių aibė sutvarkoma įvedant *leksikografinę* tvarkos sąryšį, kai pradžioje žodžiai grupuojami pagal pirmąją raidę, po to – pagal antrąją ir t.t.

Sutvarkytose aibėse įvedamos sąvokos: “elementas a eina prieš elementą b ”, “pirmasis ir paskutinis elementai”, “elementas c yra tarp elementų a ir b ”, “atviras ir uždaras intervalai”, “gretimi elementai”, “*tiršta aibė*”, “*diskrečioji aibė*” (plačiau žr. vadovėlio I d. 45 – 46 psl.).

Aibės galia. Norint palyginti dvi baigtines aibes pagal jų elementų gausumą, reikia suskaičiuoti, kiek kiekviena iš jų turi elementų. Ta aibė, kurios elementų skaičius *didesnis*, ir yra gausesnė. Sakoma: jos *galia* yra *didesnė*. Tad *baigtinės aibės galia* galima laikyti jos *elementų skaičių*. Begalinėms aibėms toks metodas netinka. Iš pirmo žvilgsnio natūraliųjų skaičių aibė N lyg ir gausesnė už aibę $N_5 := \{5k \mid k \in N\}$. Tačiau tokio teiginio niekuo pagrįsti negalime, nes nelygybė $\infty < 5 \cdot \infty$ yra beprasmė. Be to, pamatysime, kad tuodvi begalinės aibės yra *vienodai gausios*!

Begalinių aibių palyginimui panaudosime *aibių ekvivalentumo* sąvoką.

*Ap. Jei tarp aibių A ir B galime nustatyti nors vieną bijekciją, tai šitokias aibes vadiname **ekvivalenčiomis**, arba **vienodos galios aibėmis**. Žymima: $A \sim B$.*

Šitoks apibrėžimas apima ir baigtinių aibių atvejį, nes tarp baigtinių aibių tada ir tikrai tada galima nustatyti bijekciją, kai jos turi po tiek pat elementų.

Aibės A (baigtinės ar begalinės) galia žymima simboliu $\text{Card } A$.

Dabar, norėdami begalines aibes palyginti pagal elementų gausumą, turėsime susitarti dėl *etalono*, t.y. aibės, su kuria lyginsime kitas aibes. Panašiai, matuodami atstumą, tai darome sutartais (etaloniniais) vienetais: metrais, kilometrais, sieksniais, parsekais ar sprindžiais. Tokiu etalonu pasirenkama savo paprastumu išsiskirianti aibė N .

*Ap. Begalinės aibės, ekvivalenčios natūraliųjų skaičių aibei N , vadinamos **skaičiomis**.*

Pavyzdžiui, kadangi atvaizdis $\varphi : n \leftrightarrow 5n$ yra bijekcija, tai aibės N ir N_5 yra ekvivalenčios. Tuo įrodėme, kad aibė N_5 yra *skaiti*, t.y. tokios pat galios, kaip ir natūraliųjų skaičių aibė N .

Suformuluosime keletą teoremų apie skaičias aibes.

1 teorema. *Kiekviena begalinė aibė turi skaitų poaibį.*

2 teorema. *Kai $A_i, i = 1, 2, 3, \dots$ yra skaičių aibių seka, tai skaiti yra ir aibė*

$$\bigcup_{i=1}^{\infty} A_i$$

Išvada. Racionaliųjų skaičių aibė Q yra skaiti.

3 teorema. *Intervalo $[0, 1]$ realiųjų skaičių aibė nėra skaiti.*

*Ap. Begalinės aibės, ekvivalenčios intervalo $[0, 1]$ realiųjų skaičių aibei, vadinamos **kontinumo galios aibėmis**.*

Lengva įsitikinti, kad aibių ekvivalentumo sąryšis yra ES. Tad jo pagalba visos aibės (ir baigtinės, ir begalinės) suskirstomos į ekvivalentumo klases. Kiekvienai klasei priskiriame bet kurios jos aibės galią žymintį specialų simbolį, kurį vadinsime aibės **kardinaliniu skaičiumi**. Baigtinėms aibėms jis sutampa su aibės elementų skaičiumi.

Pasirodo, kardinalinius skaičius galima *palyginti*, o tai, savo ruožtu, įgalina *sutvarkyti* aibes pagal jų elementų gausą. Jei aibių A ir B kardinaliniai skaičiai yra atitinkamai α ir β , tai:

1) $\alpha = \beta$, jei $A \sim B$. Sakome: aibių A ir B kardinaliniai skaičiai yra lygūs (aibės yra vienodos galios.)

2) $\alpha < \beta$, jei $A \not\sim B$, bet $A \sim B_1$, $B_1 \subset B$. Sakome, α yra mažesnis už β , (arba β yra didesnis už α .)

4 teorema (Kantoro)(Georg Cantor, 1845 – 1918, žymus vokiečių matematikas). *Kiekvienos aibės A visų poaibių galia yra didesnė už aibės A galią.*

Išvada. Egzistuoja kiek norint dideli kardinaliniai skaičiai.

Algebrinės operacijos

Tarkime A ir B yra bet kokios aibės. Funkcija $A \times A \xrightarrow{f} B$ vadinama *operacija* (veiksmu), apibrėžta aibėje A . Kai f apibrėžimo sritis yra $A \times A$, o reikšmių sritis $f(A \times A)$ yra koks nors A poaibis (t.y. $f(A \times A) \subset A$), tai funkciją f vadiname **algebrine operacija** (sutrumpintai – AO), apibrėžta aibėje A .

Beje, kai $f(A \times A) \subset A$, tai sakoma, kad aibė A yra *uždara operacijos f atžvilgiu*. Todėl galimas ir toks algebrinės operacijos supratimas: *operacija aibėje vadinama algebrine, jeigu aibė jos atžvilgiu yra uždara*. Pastarasis apibūdinimas dažnai būna patogesnis, kai reikia praktiškai patikrinti operacijos algebriškumą.

Pavyzdžiui, jei $A = R$, tai sudėties veiksmas “+” irgi gali būti suprastas, kaip funkcija (operacija), kuri schematiškai nusakoma šitaip: $R \times R \xrightarrow{+} R$; pvz., $(2, -3) \xrightarrow{+} -1$. Intuityviai suprantame, kad tai – *algebrinės operacijos* pavyzdys.

Kita vertus, jei $A = N$, o operacija $\otimes$ nusakoma taisykle:

$$(\forall m, n \in N) m \otimes n = m - 2n,$$

tai $\otimes$ jau nėra algebrinė operacija. Žodžiais tai skambėtų taip: ne su visais natūraliaisiais m, n skaičius $m - 2n$ yra natūralusis. Tikrai, jei $m = n = 3$, tai $m - 2n = 3 - 2 \cdot 3 = -3 \notin N$.

Pakartokime: operacija f aibėje A tai funkcija: $A \times A \xrightarrow{f} B$. Iki šiol mes buvome įpratę, kad A, B – skaičių aibės, o f dažniausiai reiškė sudėtį, atimtį, daugybą, dalybą. Dabar Jums norima paaiškinti, kad operacijos sąvoka žymiai platesnė: aibės A ir B gali būti bet kokios, funkcija f , – irgi. Pavyzdžiui, A gali būti visų lietuvių kalbos žodžių aibė. Bet kuriuos du žodžius žymėkime raidėmis x, y , o taisyklę f nusakykime taip: kiekvieną porą

$(x, y) \in A \times A$, f atvaizduoja į natūralųjį skaičių m , kuris yra lygus sumariniam balsių abiejuose žodžiuose skaičiui. Simboliškai:

$$A \times A \xrightarrow{f} N \text{ arba } (x, y) \xrightarrow{f} m, \text{ arba } f(x, y) = m.$$

Aišku, kad, taip apibrėžus, turime: $f(\text{oras}, \text{mokslas}) = 4$, $f(\text{ir}, \text{universitetas}) = 7$, $f(\text{Europa}, \text{Lietuva}) = 8$ ir t.t.

Svarbu: aibėje A apibrėžta operacija vadinama *algebrine*, jeigu, ją atlikus, operacijos rezultatas vėl priklauso aibei A . Tik ką mūsų apibrėžta operacija nėra algebrinė, nes natūralieji skaičiai formaliai nėra lietuvių kalbos žodžiai. Jeigu operaciją h apibrėšime taisykle:

$$(\forall (x, y) \in A) h(x, y) = \text{Lietuva},$$

tai turėsime jau algebrinės operacijos pavyzdį.

Paskaita 1 – 03

Kombinatorikos pagrindai

Praktinėje veikloje dažnai tenka sudarinėti įvairių objektų rinkinius pagal kokius nors požymius. Pavyzdžiui, tai gali būti: gėlių puokštės komponavimo uždavinys, Seimo delegacijos (sakykime, vizitui į užsienio valstybę) sudarymas, automašinos, telefono numerio parinkimas ir t.t. Tokie (kokios nors) aibės elementų rinkiniai vadinami **junginiais**. *Dažniausiai domimasi ne pačiais junginiais, o jų skaiiniumi.*

Junginius sudarantys elementai vienos situacijos gali kartotis, kitose, - ne. Taigi, sudarinėjami *kartotiniai* ir, atitinkamai, *nekartotiniai (paprasti)* junginiai. Pavyzdžiui, parlamentari Seimo delegacijoje kartotis negali, o automobilio numerio – raidės ir skaitmenys, – gali.

Sudarant junginius, priklausomai nuo konkrečios situacijos, kartais svarbūs tik juos *sudarantys elementai*, kartais – tų elementų išsidėstymo *tvarka*, o kai kada, - ir viena, ir kita. Pvz., automobilio numeryje svarbūs ir jį sudarantys elementai (raidės ir skaitmenys), ir jų išdėstymo tvarka. Numeriai ARS 224, ARS 242, RSA 074 ir LRS 224 priklauso skirtingiems automobiliams.

Pradžioje suformuluosime dvi kombinatorikoje dažnai naudojamas akivaizdžias taisykles.

Kombinatorinė sudėties taisyklė paprasčiausiu dviejų aibių atveju formuluojama taip:

Jei iš dviejų baigtinių aibių A ir B , neturinčių bendrų elementų, reikia išrinkti vieną elementą, tai šitai galima padaryti $m + n$ būdų. Jia $\text{Card } A = m$, o $\text{Card } B = n$.

Kombinatorinė daugybos taisyklė skamba taip:

Jei iš dviejų baigtinių aibių A ir B reikia išrinkti elementų porą (x, y) taip, kad būtų $x \in A$ ir $y \in B$, tai šitai galima padaryti $m \cdot n$ būdų.

Abi šios taisyklės apibendrinamos kelių aibių atvejui. Pvz., kai turime r baigtinių aibių A_k , $k = 1 \div r$ ir $\text{Card } A_k = m_k$, tai rinkinį iš r elementų $(a_1, a_2, \dots, a_r)$, kuriame $a_k \in A_k$, $k = 1 \div r$, galima sudaryti $m_1 m_2 \dots m_r$ būdų.

Dabar junginių sudarymo situacijas aprašysime detaliau. Pradžioje aptarsime paprastus (nekartotinius) junginius.

Paprasti junginiai. Tarkime, turime aibę $A = \{a_1, a_2, \dots, a_n\}$ sudarytą iš n elementų, kurių prigimtis mums nėra svarbi.

*Ap. Junginius, sudarytus iš n aibės A elementų po k elementų (aišku, $k \leq n$), kurie skiriasi vienas nuo kito arba pačiais elementais, arba jų išdėstymo tvarka, vadiname **gretiniais**.*

Gretinių iš n elementų po k elementų skaičius žymimas simboliu A_n^k ir apskaičiuojamas pagal formulę

$$A_n^k = \frac{n!}{(n-k)!} = n(n-1)(n-2)\dots(n-k+1). \quad (1)$$

Formulės (1) įrodymas lengvai išplaukia iš kombinatorinės daugybos taisyklės.

Pvz., jei, sudarant Seimo narių delegaciją, susitarsime, kad ją sudarys trys nariai, be to, vienas iš jų bus vadovas, kitas, - jo pavaduotojas, o trečias, - tiesiog paprastas narys, tai (laikant, kad Seime yra 141 narys) delegacijos sudarymo variantų kiekis bus aprašomas (1) formule. Taigi, galėsime sudaryti

$$A_{141}^3 = 141 \cdot 140 \cdot 139 = 2743860$$

skirtingų delegacijų.

*Ap. Junginius, sudarytus iš n elementų po k elementų, kurie skiriasi vienas nuo kito tik pačiais elementais, o jų išdėstymo tvarka yra nesvarbi, vadiname **deriniais**.*

Derinių iš n elementų po k elementų skaičius žymimas simboliu C_n^k ir apskaičiuojamas pagal formulę

$$C_n^k = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots 3 \cdot 2 \cdot 1}. \quad (2)$$

Pvz., jei iš 33 VPU pirmakursių (kurie gerai moka anglų kalbą) tarpo pažintinei kelionei į Roterdamo universitetą sudarome keturių studentų delegaciją, tai svarbūs tik patys asmenys, o ne jų parinkimo tvarka. Todėl, tokiomis sąlygomis, galima sudaryti

$$C_{33}^4 = \frac{33!}{4! \cdot 29!} = \frac{33 \cdot 32 \cdot 31 \cdot 30}{4 \cdot 3 \cdot 2 \cdot 1} = 11 \cdot 4 \cdot 31 \cdot 30 = 40920$$

skirtingų delegacijų.

Kartais objektai junginyje, sudarytame iš n elementų nekeičiami, o keičiama tik jų išdėstymo tvarka, t.y. nagrinėjame gretinius iš n elementų po n elementų. Tokie nekartotiniai junginiai turi savo atskirą pavadinimą.

*Ap. Junginius, sudarytus iš n elementų po n elementų, kurie vienas nuo kito skiriasi tik elementų išdėstymo tvarka, vadiname **kėliniais**.*

Kitaip sakant, kėliniai yra gretiniai iš n elementų po n .

Kėlinių iš n elementų skaičius žymimas P_n ir apskaičiuojamas pagal formulę

$$P_n = A_n^n = n! \quad (3)$$

Pvz., jei penkis gerus draugus norite kasmet per savo gimtadienį vis kitaip susodinti prie stalo, tai visiems variantams išbandyti prireiks $P_5 = 5! = 120$ metų.

Kartotiniai junginiai. Kai nagrinėjame kartotinius junginius, tai situacija skiriasi tuo, kad aibės A elementai juose gali kartotis. Todėl gauname dar tris junginių rūšis: kartotinius gretinius, kartotinius derinius ir kartotinius kėlinius.

Ap. Kartotinius junginius, sudarytus iš n aibės A elementų po k elementų, kurie skiriasi vienas nuo kito arba pačiais elementais, arba jų išsidėstymo tvarka, vadiname kartotiniais **gretiniais**.

Kartotinių gretinių iš n elementų po k elementų skaičius žymimas $\overline{A}_n^k$ ir apskaičiuojamas pagal formulę:

$$\overline{A}_n^k = n^k. \quad (4)$$

Tikrai, kadangi mums reikia parinkti k elementų, bet jie gali kartotis, tai kiekvieną iš jų galime parinkti n būdų. Tada, pagal *kombinatorinę daugybos taisyklę*, visą k elementų rinkinį galėsime parinkti $n \cdot n \cdot \dots \cdot n = n^k$ būdų.

Pvz., iš skaitmenų 2,5,7,9 sudarysime visus galimus penkiaženklis skaičius. Nesunku suprasti, kad šiuo atveju svarbu ir patys skaitmenys, ir jų užrašymo tvarka. Be to, skaitmenys gali kartotis. Tad turėsime kartotinius gretinius iš 4 elementų po penkis elementus. Pagal (4) formulę, tokių skaičių kiekis yra lygus

$$\overline{A}_4^5 = 4^5 = 1024.$$

Kai kartotiniuose junginiuose elementų tvarka nesvarbi, tai sakome, kad turime *kartotinius derinius*.

Kartotinių derinių iš n elementų po k elementų skaičius žymimas $\overline{C}_n^k$ ir apskaičiuojamas pagal formulę:

$$\overline{C}_n^k = C_{n+k-1}^k = \frac{(n+k-1)!}{k!(n-1)!}. \quad (5)$$

Pagaliam, kai m rūšių ($m \leq n$) elementai iš aibės $A = \{a_1, a_2, \dots, a_n\}$ kartotiniame junginyje nesikeičia (turi pastovius *kartotinumus* $k_1, k_2, \dots, k_m$), o keičiasi tik jų išsidėstymo tvarka, tai kalbame, apie *kartotinius kėlinius* iš $k_1 + k_2 + \dots + k_m$ elementų. Jų skaičius žymimas simboliu $P(k_1, k_2, \dots, k_m)$ ir apskaičiuojamas pagal formulę:

$$P(k_1, k_2, \dots, k_m) = \frac{(k_1 + k_2 + \dots + k_m)!}{k_1! k_2! \dots k_m!}. \quad (6)$$

Pavyzdžiui, kai turime aštuonis trijų rūšių skaitmenis 2, 2, 2, 5, 5, 7, 7, 7, tai, pagal (6) formulę, iš jų galima sudaryti $P(3, 2, 3) = \frac{(3+2+3)!}{3! 2! 3!} = \frac{8!}{36 \cdot 2} = 560$ skirtingų aštuoniaženklų skaičių.

Kombinatorinės tapatybės. Yra daug junginius siejančių sąryšių, kuriuos įprasta vadinti *kombinatorinėmis tapatybėmis*. Štai kelios iš jų:

$$A_n^k = P_k \cdot C_n^k;$$

$$C_n^k = C_n^{n-k};$$

$$C_n^k + C_n^{k-1} = C_{n+1}^k;$$

$$C_k^k + C_{k+1}^k + \dots + C_{k+m-1}^k = C_{n+m}^{k+1}.$$

Formulė $A_n^k = P_k \cdot C_n^k$ išplaukia iš kombinatorinės daugybos taisyklės suvokus, kad kiekvienas derinys iš n po k elementų, jį *sutvarkius*, virst kaskart nauju gretiniu iš n elementų po k elementų. Bet k elementų sutvarkymų (kėlinių) yra $P_k = k!$ Tuo įrodėme ir (2) formulę.

Vėliau mes naudosime tapatybę $C_n^k + C_n^{k-1} = C_{n+1}^k$. Įrodysime ją.

Pagal derinių skaičiaus formulę, panaudodami faktorialo savybę, turėsime:

$$\begin{aligned} C_n^k + C_n^{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} = \frac{n!}{(k-1)!(n-k)!} \left(\frac{1}{k} + \frac{1}{n-k+1} \right) = \\ &= \frac{n!}{(k-1)!(n-k)!} \left(\frac{n+1}{k(n-k+1)} \right) = \frac{(n+1)!}{k!(n+1-k)!} = C_{n+1}^k. \end{aligned}$$

Naudojant pirmosiose paskaitose įvestus terminus, junginius galima apibrėžti tiksliau.

Ap. Deriniu (nekartotiniu) iš n elementų turinčios aibės A , po k elementų vadiname bet kokią aibės A poaibį, turintį k elementų.

Tad C_n^k išreiškia aibės A poaibių skaičių.

Ap. Gretiniu (nekartotiniu) iš n elementų turinčios aibės A , po k elementų vadiname bet kokią sutvarkytą aibės A poaibį, turintį k elementų.

Tuo būdu, A_n^k reiškia sutvarkytų aibės A poaibių skaičių.

Ap. Kėliniu (nekartotiniu) iš k aibės A elementų, vadiname bet kokią aibės A poaibio, turinčio k elementų, sutvarkymą.

Tad P_k išreiškia bet kurio aibės A poaibio, turinio k elementų, skirtingų sutvarkymų skaičių.

Paskaita 1 – 04

Algebrinės struktūros

Prisiminkime terminus: funkcija (atvaizdis), funkcijos apibrėžimo sritis, pilnas vaizdas, reikšmių sritis, pirmavaizdis, vaizdas, operacija, algebrinė operacija.

Algebrinė operacija, algebrinė struktūra

Pakartokime: funkcija $A \times A \xrightarrow{f} A$ vadinama **algebrine operacija** (sutrumpintai – AO), apibrėžta aibėje A .

Tolesniems žingsniams *algebrinės operacijos* sąvoka yra labai svarbi, todėl pasistenkite ją įsisavinti!

Pavyzdžiui, aibėje $A = \{0, 1, 2, 3, 4, 5\}$ *lentelių pagalba* apibrėžkime dvi operacijas, kurias susitarkime žymėti ženklais ♣ ir ♠:

♣	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	6
2	2	3	4	5	6	7
3	3	4	5	6	7	8
4	4	5	6	7	8	9
5	5	6	7	8	9	10

♠	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Nesunku pastebėti, kad operacija ♣ nėra algebrinė, nes $f(A \times A) \not\subset A$. Pavyzdžiui, $5 \clubsuit 3 = 8 \notin A$, tuo tarpu ♠ yra AO, nes $(\forall a, b \in A) a \spadesuit b \in A$.

Tarkime A yra bet kokia aibė, o $f_1, f_2, \dots$ – joje apibrėžtos algebrinės operacijos.

Ap. Aibę A kartu su joje apibrėžtomis AO $f_1, f_2, \dots$ vadinsime **algebrine struktūra** (arba *algebra*; sutrumpintai – AS) ir žymėsime $A := (A, f_1, f_2, \dots)$. Aibė A dažnai vadinama algebrinės struktūros A *bazine aibe*.

Pavyzdžiui, tik ką išnagrinėtame pavyzdyje turėtume algebrinę struktūrą $A := (A, \spadesuit)$, o $Z = (Z, +, \cdot)$ žymėtų sveikųjų skaičių struktūrą.

Algebrinių operacijų savybės

Dažnai mums bus svarbu, ar tiriamosios AO yra :

- komutatyvios,
- asociatyvios,
- tarpusavyje distributyvios.

Suformuluosime atitinkamus apibrėžimus.

Ap. Tarkime $A:=(A, *)$ yra bet kokia algebrinė struktūra, o $*$ yra jos AO. Jei

$$(\forall a, b \in A) a * b = b * a,$$

tai sakome, kad operacija $*$ yra komutatyvi.

Pvz., natūraliųjų skaičių sudėtis yra komutatyvi, o atimtis, – ne.

Ap. Jei

$$(\forall a, b, c \in A) a * (b * c) = (a * b) * c,$$

tai sakome, kad AO $*$ yra asociatyvi.

Pvz., sveikųjų skaičių daugyba yra asociatyvi, o atimtis šios savybės neturi.

Ap. Tarkime $A:=(A, \oplus, \otimes)$ yra algebrinė struktūra su dviem AO $\oplus$ ir $\otimes$. Jei

$$(\forall a, b, c \in A) a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c),$$

tai sakome, kad operacija $\otimes$ yra distributyvi iš kairės operacijos $\oplus$ atžvilgiu.

Pvz., racionaliųjų skaičių daugyba yra distributyvi iš kairės atimties atžvilgiu.

AO gali būti komutatyvi, bet neasociatyvi, ir atvirkščiai: nekomutatyvi, bet asociatyvi.

(Užduotis. Suformuluokite distributyvumo iš dešinės apibrėžimą).

Kai operacija $\otimes$ yra komutatyvi, tai distributyvumo iš kairės ir dešinės sąvokos sutampa.

Tuokart sakome: “operacija $\otimes$ yra distributyvi operacijos $\oplus$ atžvilgiu”.

Pavyzdžiai. Sveikųjų skaičių aibėje Z taisyklėmis:

$$a \oplus b = a + 2b, \quad a \otimes b = 3ab \tag{1}$$

apibrėžkime kiek neįprastas “sudėti” ir “daugyti.” Akivaizdu, kad tai, – algebrinės operacijos, nes jų rezultatai visada yra sveikieji skaičiai. Kadangi:

$$a \oplus b = a + 2b \neq b + 2a = b \oplus a, \quad \text{o} \quad a \otimes b = 3ab = 3ba = b \otimes a,$$

tai tokia “daugyba” yra komutatyvi, o tokia “sudėtis”, – nėra komutatyvi.

Taisykle $a * b = a^2 + b^2$ sveikųjų skaičių aibėje apibrėžta operacija $*$ akivaizdžiai yra komutatyvi. Įsitikinti tuo, kad ji nėra asociatyvi galima ir pavyzdžio (kontrapavyzdžio) pagalba:

$$3 * ((-2) * 4) = 3 * ((-2)^2 + 4^2) = 3 * 20 = 9 + 400 = 409,$$

$$(3 * (-2)) * 4 = (9 + 4) * 4 = 13 * 4 = 169 + 16 = 185.$$

Bet $409 \neq 185$. Darome išvadą, – operacija $*$ nėra asociatyvi.

Ap. Kai $A: = (A, *)$ yra AS su $AO *$ ir egzistuoja toks bazinės aibės A elementas e , kad

$$(\forall a \in A) a * e = e * a = a,$$

tai sakome, kad e yra neutralusis aibės A elementas operacijos $*$ atžvilgiu.

Galima sakyti ir taip: e yra operacijos $*$ neutralusis elementas.

1 teorema. Jei aibė A turi neutralųjį ($*$ atžvilgiu) elementą, tai tikrai vienas.

Įr. Tare, priešingai, kad tokių elementų yra bent du, t.y. e_1 ir e_2 , turėtume:

$$e_1 * e_2 = e_1 \text{ ir } e_1 * e_2 = e_2, \text{ t.y. } e_1 = e_2. \text{ Prieštara. QED.}$$

Dabar tarkime $A: = (A, *)$ yra tokia AS, kurios bazinė aibė A turi neutralųjį operacijos $*$ atžvilgiu elementą e .

Ap. Jei a yra bet kuris bazinės aibės A elementas ir egzistuoja toks elementas $x \in A$, kad

$$a * x = x * a = e,$$

tai sakome, kad x yra elementas simetriškas elementui a (operacijos $*$ atžvilgiu).

Arba: elementas a turi sau simetrišką elementą. Žymime: $x = a'$.

Pvz., struktūros $(Z, +)$ bazinėje aibėje yra neutralusis elementas 0, o kiekvienas bazinės aibės elementas turi sau simetrišką: $3' = -3$, $-117' = 117$.

Laikykime, kad algebrinės struktūros $A: = (A, *)$ operacija $*$ yra asociatyvi. Tada galima įrodyti keletą svarbių faktų.

2 teorema. Jei asociatyvios algebrinės operacijos $*$ atžvilgiu elementas $a \in A$ turi sau simetrinį elementą a' , tai tikrai vienas.

Įrodymo idėja ta pati kaip ir pračioje teoremoje. Tare, kad tokių elementų yra bent du, (t.y. a_1 ir a_2) turėtume:

$$a_1 * a * a_2 = a_1 * (a * a_2) = a_1 * e = a_1 \text{ ir } a_1 * a * a_2 = (a_1 * a) * a_2 = e * a_2 = a_2.$$

Iš čia: $a_1 = a_2$. Prieštara. QED.

Ap. Kai su kiekviena aibės A ($e \in A!$) elementų pora a ir b išsprendžiamos lygtys

$$a * x = b, \quad y * a = b, \quad (2)$$

tai sakome, kad: aibėje A įvykdoma operacijai $*$ atvirkštinė operacija.

Pastebėkime, kad bendruoju atveju $x \neq y$ ir kad x, y surandami vienareikšmiškai.

3 teorema. Jei aibėje A yra neutralusis asociatyvios algebrinės operacijos $*$ atžvilgiu elementas e ir kiekvienas A elementas a turi sau simetrišką a' , tai aibėje A įvykdoma operacijai $*$ atvirkštinė operacija.

Įrodymas. Išspręskime, pavyzdžiui, lygtį $a * x = b$. Paėmę $x = a' * b \in A$, turime:

$$a * x = a * (a' * b) \stackrel{\text{asoc}}{=} (a * a') * b = e * b = b.$$

Įsitikinkite, kad elementas $y = b * a' \in A$ yra lygties $y * a = b$ sprendinys. QED.

Išvada. Kai operacija $*$ yra komutatyvi, tai (2) lyginių sprendiniai x ir y – sutampa.

Aptarsime svarbesnius algebrinių struktūrų tipus *klasifikuodami* jas pagal jose apibrėžtų algebrinių operacijų savybes.

Pusgrupis, grupė

Ap. Algebrinė struktūra $A: = (H, *)$ su viena asociatyvia AO vadinama pusgrapiu.

Jei, be to, operacija $*$ yra ir komutatyvi, tai pusgrupis A vadinamas *komutatyviuoju*.

Jei bazinėje aibėje yra neutralusis elementas, tai pusgrupis vadinamas *monoidu*.

Pvz., $ASA: = (Z, +)$ yra komutatyvusis pusgrupis, o struktūra $B: = (Z, \oplus)$ - nėra pusgrupis, nes (žr. (1) formule nusakytą apibrėžimą):

$$(\forall a, b, c \in Z) a \oplus (b \oplus c) = a \oplus (b + 2c) = a + 2(b + 2c) = a + 2b + 4c,$$

kai tuo tarpu

$$(\forall a, b, c \in Z) (a \oplus b) \oplus c = (a + 2b) \oplus c = a + 2b + 2c.$$

Taigi, struktūros B operacija $\oplus$ nėra asociatyvi.

Ap. AS $G: = (A, *)$ su viena asociatyvia algebrine operacija $*$, kuriai įvykdoma atvirkštinė operacija, vadinama **grupe** (vok. - Gruppe, angl.- group, rus. – группа). Jei, be to, operacija $*$ yra ir komutatyvi, tai grupė vadinamas *komutatyviąja arba Abelio grupe*.

4 teorema. Jei $G: = (A, *)$ yra grupė, tai bazinėje aibėje A yra vienintelis neutralusis (operacijos $*$ atžvilgiu) elementas e ir bet kuriam $a \in A$ vienintelis simetriškas elementas $a' \in A$.

Irodymas. Kadangi, pagal apibrėžimą, grupėje įvykdoma atvirkštinė operacija, tai lygtys (2) yra išsprendžiamos su visais $a, b \in A$. Todėl $(\exists y \in A) y * a = b$. Be to, atskiru atveju, kai $a = b$: $(\exists x \in A) a * x = a$. Pažymėkime $x = e_a$. Tačiau:

$$b * e_a \stackrel{b=y*a}{=} (y * a) * e_a = y * (a * e_a) = y * a = b.$$

Tad darome išvadą, kad $e_a = e_b := e''$ ir elementą e'' vadiname aibės A neutraliuoju elementu iš dešinės.

Analogiškai samprotaudami parodytume, kad egzistuoja neutralusis aibės A elementas iš kairės; žymėkime jį e' .

Bet tada: $e' * e'' = e'$ ir $e' * e'' = e''$, t.y. $e' = e'' := e$ ir e tenkina neutralaus elemento apibrėžimą. Neutralaus elemento e vienatis išplaukia iš 1 teoremos.

Panašiai įrodomas ir teoremos tvirtinimas apie simetrinio elemento $a' \in A$ egzistenciją. Vienatis išplaukia iš 2 teoremos. QED.

Pastabos

1. Apie du grupės apibrėžimus. Jei grupę apibrėžiame taip kaip šiame konspekte, tai elementų e ir $a' \in A$ egzistencija ir vienatis yra *įrodoma* (4 teorema). Jeigu apibrėžimą pateikiame pagal vadovėlį (79 psl.) tai tada įrodomas lygčių (2) *išsprendžiamumas* (konspekte: 3 teorema; vadovėlyje: 4 savybė, 80 psl.). Galima elgtis kaip mums aiškiau, patogiau.

2. Apie terminus: adicinė, multiplikacinė grupė. Kai grupės operacija yra *sudėtis* (ar kažkuo panaši į sudėtį), tai pačią grupę vadiname *adicine*, jos neutralųjį elementą, – *nuliniu*, o simetriškąjį, – *priešinguoju* (žymima: $-a$). Kai operacija vadinama *daugyba*, tai grupę vadinama *multiplikacine*, jos neutralusis elementas vadinamas *vienetiniu*, o simetriškasis – *atvirkštiniu* (žymima: a^{-1}).

3. Apie kalbos “laisvę”. Kartais, lakoniškumo dėlei, grupė (lauku, žiedu) pavadinama grupės (lauko, žiedo) bazinė aibė; žodį “išplaukia” matematinėje literatūroje įprasta žymėti implikacijos simboliu “ $\Rightarrow$ ”, nors, mano nuomone, korektiškiau būtų naudoti loginės išvados simbolį “ $\rightarrow$ ”. Operacijų ženklai, paprastumo dėlei, irgi dažnai nedetalizuojami. Pavyzdžiui, sudėties veiksmas skaičių, funkcijų, vektorių aibėse apibrėžiamas skirtingai, bet jam pažymėti naudojame tą patį ženklą “+”.

4. Apie operacijos konkretumo svarbą. Grupės sąvoka bazinę aibę neatsiejamai suriša su joje apibrėžta algebrine operacija. Pvz., struktūra $(Q, +)$ yra adicinė Abelio grupė, o struktūra $(Q, \cdot)$ grupės aksiomų jau netenkina.

5. Algebrinės operacijos sąvoką, naudinga kiek išplėsti. AO $A \times A \xrightarrow{f} A$ vadinama *vidine*, o operacija $B \times A \xrightarrow{f} A$ vadinama *išorine binare (algebrine) operacija*. Pvz., vektorių sudėtis plokštumoje yra vidinė algebrinė binarė operacija, o vektoriaus daugyba iš skaičiaus – išorinė.

Paskaita 1 – 05

Algebrinės struktūros (tęsinys)*Primename:*

Ap. Algebrinė struktūra $G:=(A, *)$ su viena asociatyvia algebrine operacija $*$, kuriai įvykdoma atvirkštinė operacija, vadinama *grupe*. Jei, be to, operacija yra dar ir komutatyvi, tai grupė vadinamas *komutatyviaja* arba *Abelio* grupe.

Ap. (*Alternatyvus*). Algebrinė struktūra $G:=(A, *)$ su asociatyvia algebrine operacija $*$, turinti neutralųjį ir kiekvienam elementui simetrišką elementus vadinama *grupe*. Jei, operacija yra komutatyvi, tai grupė vadinama *Abelio* grupe.

Pastebėjime: abu apibrėžimai yra ekvivalentūs.

Žiedai

Susipažinome su algebrinėmis struktūromis, kurios vadinamos *grupėmis*. Tai yra svarbus tipas struktūrų su viena AO. Kitas mus dominantis AS tipas yra taip vadinamieji *žiedai* (vok. – *Ring*, angl. – *ring*, rus. – *кольцо*).

Ap. AS $\mathbf{Z}:=(A, \oplus, \otimes)$ (su dviem algebrinėmis operacijomis, kurias kalbos sklandumui susitarkime vadinti: $\oplus$ - sudėtimi, $\otimes$ - daugyba) vadinama *žiedu*, jei yra išpildytos tokios sąlygos:

- struktūra $(A, \oplus)$ yra adicinė Abelio grupė,
- abiems operacijoms galioja komutatyvumo bei asociatyvumo savybės; be to, operacija $\otimes$ yra distributyvi operacijos $\oplus$ atžvilgiu (sutrumpintai: KAD).

Pavyzdžiai. Jei nagrinėsime AS, kurios bazinė aibė yra lyginių sveikųjų skaičių aibė Z_2 , o operacijos, – įprastinės skaičių sudėtis ir daugyba, tai $(Z_2, +, \cdot)$ yra žiedas.

Aibėje $L_6 = \{0, 1, 2, 3, 4, 5\}$ apibrėžkime sudėtį ir daugybą įprastai, tik susitarkime, kad, atlikdami sudėties, atimties ir daugybos veiksmus, rezultatą padidinsime ar sumažinsime skaičiaus 6 kartotiniu taip, kad jis vėl priklausytų aibei L_6 : $2 + 3 = 5$, $4 \cdot 3 = 12 - 2 \cdot 6 = 0$, $5 + 3 = 8 - 6 = 2$, $2 - 5 = -2 + 6 = 4$, $5 \cdot 4 = 20 - 3 \cdot 6 = 2$ ir t.t. Lengva patikrinti, kad struktūra $(L_6, +, \cdot)$ yra komutatyvus žiedas su nuliniu elementu 0.

Kartais nagrinėjami žiedai, kuriuose daugybos veiksmas nėra komutatyvus. Tokie žiedai vadinami *nekomutatyviaisiais*. Žiedai su neasociatyvia daugyba vadinami *neasociatyviaisiais žiedais*. Nekomutatyvių žiedų pavyzdžių pateiksime antrame semestre, o neasociatyvių žiedų nenagrinėsime.

Paprasčiausios žiedų savybės

Patogumo dėlei, savybių formulavimuose operacijas $\oplus$ ir $\otimes$ žymėkime įprastai: $+$ ir $\cdot$.

1. Kadangi žiedas yra kartu ir adicinė grupė, tai jame yra vienintelis *nulinis* (neutralusis “sudėties” atžvilgiu) elementas. Jį žymėsime O_A .

2. Kiekvienas žiedo bazinės aibės A elementas a turi vienintelį sau *priešingą* elementą, kurį žymėsime $-a \in A$.

3. Galioja “prastinimo” taisyklė, t.y. $a + b = a + c \rightarrow b = c$.

4. Egzistuoja vienintelis lygties $b + x = a$ sprendinys, kuris vadinamas elementų a ir b *skirtumu* ir žymimas $a - b$.

5. $(\forall a \in A) -(-a) = a$.

6. $(-a) + (-b) = -(a + b)$.

Naudojamos ir įprastos santrumpos na , $-na$. Detaliau: žr. vadovėlio 87 psl.

7. $O_A \cdot a = O_A$.

8. $(-a)b = -(ab)$.

9. $(-a)(-b) = ab$.

10. $(\forall a, b, c \in A) a(b - c) = ab - ac$. D dėsnis atimties operacijai.

Visos savybės yra įrodomos.

6 sav. įrodymas. Pirmiausia, savybę suformuluokime žodžiais, tada ir įrodymo eiga bus aiškesnė.

Turime parodyti, kad: *elementų a ir b priešingųjų elementų suma yra sumos $a + b$ priešingasis*.

Prisiminę, kad elemento s priešinguoju vadinamas toks elementas x , su kuriuo galioja $s + x = x + s = O_A$, tikriname:

$$(a + b) + ((-a) + (-b)) \stackrel{K, A}{=} a + (b + (-b)) + (-a) = a + O_A + (-a) = O_A. \text{ QED.}$$

8 sav. įrodymas. Dabar turime parodyti, kad: *elementų $-a$ ir b sandauga yra sandaugos ab priešingasis elementas*. Iš tikrųjų,

$$ab + (-a)b \stackrel{\text{distrib}}{=} (a + (-a))b \stackrel{7 \text{ sav}}{=} O_A \cdot b = O_A. \text{ QED.}$$

Pabrėžtina, kad žiedas gali ir neturėti vienetinio elemento. Pvz., $(Z_2, +, \cdot)$.

Laukai

Apibrėšime dar vieną svarbų AS tipą: *laukus* (angl. – *field*, rus. – *поле*). Beje, kituose literatūros šaltiniuose vartojamas žiedui adekvatus terminas: *kūnas* (angl. – *solid*, vok. – *Körper*, rus. – *тело*).

Ap. AS $L := (A, \oplus, \otimes)$ (su dviem AO, kurias vėlgi susitarkime vadinti: $\oplus$ – sudėtimi, $\otimes$ – daugyba) vadinama **lauku**, jei yra išpildytos tokios sąlygos:

- bazinė aibė A turi bent du skirtingus elementus,
- struktūra $(A, \oplus)$ yra adicinė Abelio grupė,
- struktūra $(A \setminus \{O_A\}, \otimes)$ yra multiplikacinė Abelio grupė,
- daugyba sudėties atžvilgiu yra distributyvi.

Pavyzdžiui: racionaliųjų skaičių struktūra $(Q, +, \cdot)$ yra laukas.

Laukų savybės didele dalimi išplaukia iš to, kad struktūros $(A, \oplus), (A \setminus \{O_A\}, \otimes)$ yra komutatyvios grupės. Tad lauke yra: vieninteliai *nulinis* ir *vienetinis* bei kiekvienam elementui *priešingasis* ir (ne nuliui) *atvirkštinis*, galioja *distributyvumo* dėsnis atimčiai, bei visos kitos jau aptartos grupių ir žiedų savybės.

Tačiau laukai turi ir specifinių savybių. Viena iš svarbiausių yra ta, kad laukas *neturi nulinio daliklio*. T.y. nenulinių lauko elementų sandauga visada nelygi O_A .

Teorema. Dviejų lauko elementų a ir b sandauga tada ir tik tada lygi nuliniam lauko elementui O_A , kai bent vienas iš dauginamųjų lygus O_A .

Įr. Metodas, – suvedimas į prieštarą. Tariame, kad yra du tokie nenuliniai lauko elementai a ir b , kad $a \cdot b = O_A$. Tačiau tada lauko bazinėje aibėje yra ir elemento b atvirkštinis b^{-1} . Padauginę abi lygybės $a \cdot b = O_A$ puses iš to b^{-1} , turime:

$$(a \cdot b) \cdot b^{-1} = O_A \cdot b^{-1} \xrightarrow{\text{asoc; 7 sav.}} a \cdot (b \cdot b^{-1}) = O_A \cdot b^{-1} = O_A \rightarrow a \cdot 1_A = O_A \rightarrow a = O_A.$$

Tai prieštarauja prielaidai, kad a – nenulinis lauko elementas. QED.

Žieduose bendruoju atveju ši teorema nėra teisinga.

Ap. Komutatyvusis žiedas be nulinio daliklio vadinamas **integralumo sritimi**.

Pavyzdžiui, struktūra $(L_6, +, \cdot)$ nėra integralumo sritis, nes $2 \cdot 3 = 4 \cdot 3 = 0$, o struktūra $(Z_2, +, \cdot)$ yra integralumo sritis.

Lauko charakteristika. Lauko bazinės aibės elementai gali būti ir ne skaičiai. Tokių laukų savitumas nusakomas naujos sąvokos, **lauko charakteristikos**, pagalba.

Ap. Mažiausią natūralųjį skaičių m , su kuriuo galioja lygybė $m \cdot e_L = O_L$, vadiname lauko L charakteristika ir žymime $m = \text{char}L$. Jei tokio m nurodyti negalima, tai sakome, kad laukas yra nulinės charakteristikos ir rašome $\text{char}L = 0$.

Pavyzdys. Aibėje $A = \{a, b, c\}$ lentelių pagalba įveskime “sudėtį” $\oplus$ ir “daugybą” $\otimes$.

$\oplus$	a	b	c	$\otimes$	a	b	c
a	a	b	c	a	a	a	a
b	b	c	a	b	a	b	c
c	c	a	b	c	a	c	b

Nesunku pastebėti, kad struktūra $L: = (A, \oplus, \otimes)$ tenkina lauko aksiomas, be to: $O_A = a, e_A = b$. Bet $3b = b \oplus b \oplus b = (b \oplus b) \oplus b = c \oplus b = a = O_A \rightarrow \text{char } L = 3$.

Galima parodyti, kad: $\text{char } L \neq 0 \rightarrow \text{char } L \in P$. Čia P , – sveikųjų pirminių skaičių aibė.

Nenulinės charakteristikos laukai turi nemažai neįprastų savybių. Pvz., jei $\text{char } L = p$, tai $(\forall a, b \in L)(a + b)^p = a^p + b^p$.

Algebrinių struktūrų homomorfizmai ir izomorfizmai

Kartais dvi AS, turinčios skirtingos prigimties bazines aibes ir savitas algebrines operacijas, visgi (būtent, tų operacijų *savybių prasme*) yra labai panašios ir skiriasi nebent tik “matmenimis”, t.y. bazinės aibės galia, arba yra ir visai identiškos.

Tarkime (A_1, Ω_1) ir (A_2, Ω_2) yra dvi AS, su baigtinėmis operacijų σ_{kj} aibėmis Ω_k . Čia $\sigma_{kj} \in \Omega_k$; $j = 1, 2, \dots, n$; $k = 1, 2$.

Ap. AS (A_1, Ω_1) ir (A_2, Ω_2) vadinamos **homomorfiškomis** (atitinkamai: **izomorfiškomis**), jeigu tarp jų bazinių aibių galima nustatyti tokią surjekciją (atitinkamai: bijekciją) φ , kad galiojūt sąlygos:

$$(\forall a, b \in A_1)(\forall j) \varphi(a \sigma_{1j} b) = \varphi(a) \sigma_{2j} \varphi(b). \quad (1)$$

Pavyzdžiui, jei viena iš operacijų abiejose bazinėse aibėse yra sudėtis, tai (1) sąlyga atrodo taip:

$$(\forall a, b \in A_1) \varphi(a + b) = \varphi(a) + \varphi(b),$$

t.y. sumos vaizdas turi būti lygus vaizdų sumai.

Homomorfiškos (ar izomorfiškos) grupės, žiedai ar laukai turi panašias savybes, todėl vienos tyrinėjimą galima pakeisti kitos (pvz., su paprastesne bazine aibe) tyrinėjimu.

Ap. Dvi grupės $(A_1, \otimes_1)$ ir $(A_2, \otimes_2)$ vadinamos **homomorfiškomis** (atitinkamai: **izomorfiškomis**), jeigu tarp jų bazinių aibių galima nustatyti tokią surjekciją (atitinkamai: bijekciją) φ , kad galiojūt sąlygos:

$$(\forall a, b \in A_1) \varphi(a \otimes_1 b) = \varphi(a) \otimes_2 \varphi(b).$$

(Užduotis: suformuluokite homomorfiškų bei izomorfiškų žiedų ir laukų apibrėžimus).

Minėta surjekcija (atitinkamai: bijekcija) φ dažnai vadinama tiesiog **homomorfizmu** (**izomorfizmu**). Teisinga tokia teorema (tiesą sakant, - net šešios teoremos) apie pagrindinių mūsų apibrėžtų ir aptartų AS homomorfiškus vaizdus.

Teorema. *Homomorfiškas (izomorfiškas) grupės (žiedo; lauko) vaizdas yra grupė (žiedas; laukas).*

Įr. Pakomentuokime formuluotę, kai kalbame apie *grupių izomorfizmą*. Tada teoremos duomenys (prielaidos, sąlygos) yra tokie: turime grupę $G = (A_1, *)$ ir kitą AS $(A_2, \circ)$; tarp bazinių aibių nustatyta tokia bijekcija $\varphi: A_1 \leftrightarrow A_2$, kad

$$(\forall a, b \in A_1) \varphi(a * b) = \varphi(a) \circ \varphi(b).$$

Reikia įrodyti, kad $AS(A_2, \circ)$ yra grupė.

Irodymui verta prisiminti grupės apibrėžimą (vienokį ar kitokį) ir patikrinti, ar struktūra $(A_2, \circ)$ tenkina grupės aksiomas.

1. Patikrinsime operacijos $\circ$ algebriskumą (tai daryti nebūtina; tuo tik parodome, jog struktūros $(A_2, \circ)$ operacijos $\circ$ algebriskumas gali būti ir nepostuluotas).

$(\forall a', b' \in A_2)(\exists a, b \in A_1) a' = \varphi(a) \wedge b' = \varphi(b) \rightarrow a' \circ b' = \varphi(a) \circ \varphi(b) \stackrel{\text{izomorf}}{=} \varphi(a * b) \in A_2$, nes φ yra bijektyvus atvaizdis.

2. Aptarsime operacijos $\circ$ asociatyvumą.

$$\begin{aligned} & (\forall a', b', c' \in A_2)(\exists a, b, c \in A_1) a' = \varphi(a) \wedge b' = \varphi(b) \wedge c' = \varphi(c) \rightarrow (a' \circ b') \circ c' \stackrel{\text{izomorf}}{=} \\ & = (\varphi(a) \circ \varphi(b)) \circ \varphi(c) \stackrel{\text{izomorf}}{=} \varphi(a * b) \circ \varphi(c) \stackrel{\text{izomorf}}{=} \varphi((a * b) * c) \stackrel{\text{asoc}}{=} \varphi(a * (b * c)) \stackrel{\text{izomorf}}{=} \\ & \stackrel{\text{izomorf}}{=} \varphi(a) \circ \varphi(b * c) \stackrel{\text{izomorf}}{=} \varphi(a) \circ (\varphi(b) \circ \varphi(c)) = a' \circ (b' \circ c'). \end{aligned}$$

3. Lieka parodyti, kad aibėje A_2 įvykdoma operacijai $\circ$ atvirkštinė operacija. Tai galima padaryti dvejopai: arba įrodant, kad su bet kokiais aibės A_2 elementais a', b' , yra išsprendžiamos lygtys $a' \circ x' = b'$, $y' \circ a' = b'$, arba, – įrodant, kad aibėje A_2 yra neutralusis ir kiekvienam priešingas (operacijos $\circ$ atžvilgiu) elementai. Patariu išbandyti abu būdus. Čia mes parodysime lygčių išsprendžiamumą. Pavyzdžiui, nagrinėkime lygtį $a' \circ x' = b'$ (kita situacija aptariama analogiškai). Jos “vaizdas” (atitinkmuo) $a * x = b$ grupės G bazinėje aibėje A_1 turi sprendinį x (nes G – grupė). Kadangi tarp aibių A_1 ir A_2 yra nustatyta bijekcija φ , tai egzistuoja $x' \in A_2$ toks, kad $\varphi(x) = x'$. Todėl:

$$a' \circ x' = \varphi(a) \circ \varphi(x) \stackrel{\text{izomorf}}{=} \varphi(a * x) \stackrel{a * x = b}{=} \varphi(b) = b',$$

o tai ir reiškia, kad lygties sprendiniu yra elementas $x' \in A_2$. QED.

Pavyzdys. Prisiminkime lauko, kurio charakteristika lygi 3, pavyzdį: $L = (A, \oplus, \otimes)$. Jo bazinė aibė buvo $A = \{a, b, c\}$, o operacijas $\oplus$ ir $\otimes$ apibrėžėme lentelių pagalba.

Nagrinėkime struktūrą $L_3 = (B, +, \times)$, kurios bazinė aibė yra $B = \{1, 2, 3\}$, o veiksmams $+$ ir $\times$ irgi apibrėžti lentelėmis:

+	1	2	3	×	1	2	3
1	2	3	1	1	1	2	3
2	3	1	2	2	2	1	3
3	1	2	3	3	3	3	3

Vėlgi, lengvai įsitikiname, kad L_3 tenkina lauko aksiomas. Kadangi bijekcija $\varphi: a \leftrightarrow 3; b \leftrightarrow 1; c \leftrightarrow 2$; tenkina izomorfizmo reikalavimus (patikrinkite!), tai laukai L ir L_3 yra *izomorfiški*. Žymime: $L \cong L_3$.

AS poaibiai

Kartais tikrinis bazinės aibės poaibis yra, savo ruožtu, grupė (žiedas, laukas) tų pačių operacijų atžvilgiu.

Ap. Jei $G_1 = (A_1, *)$ ir $G_2 = (A_2, *)$ yra dvi grupės (tos pačios operacijos atžvilgiu), o $A_1 \subset A_2$, tai grupę $G_1 = (A_1, *)$ vadiname grupės $G_2 = (A_2, *)$ **pograpiu**.

Pvz., lyginių sveikųjų skaičių adicinė grupė $(Z_2, +)$ yra visų sveikųjų skaičių adicinės grupės $(Z, +)$ pograpius.

Savarankiškai suformuluokite **požiedžio** ir **polaukio** apibrėžimus.

Teorema. (Pograpių kriterijus). Tam kad poaibis būtų pograpiu būtina ir pakankama, kad jis būtų uždaras grupės tiesioginės ir atvirkštinės operacijų atžvilgiu.

Įr. **Būtinumas.** Duota grupė $(A, *)$ ir jos pograpius $(H, *)$. Reikia įrodyti, kad H uždara tiesioginės operacijos $*$ ir jai atvirkštinės operacijos atžvilgiu. Tačiau $(H, *)$ yra grupė, todėl ši sąlyga yra išpildyta.

Pakankamumas. Duota, kad struktūros $(H, *)$ bazinė aibė uždara operacijos $*$ ir jai atvirkštinės operacijos atžvilgiu, be to $H \subset A$. Reikia įrodyti, kad $(H, *)$ yra grupė. Iki įrodymo tetrūksta patikrinti operacijos $*$ aibėje H asociatyvumą. Bet

$$(\forall a, b, c \in H) \xrightarrow{H \subset A} a, b, c \in A \rightarrow a * (b * c) = (a * b) * c. \text{ QED.}$$

Teorema. Kelių pograpių (požiedžių, polaukių) sankirta yra pograpius (požiedis, polaukis).

Įr. Panaudojant pograpių kriterijų. Savarankiškai.

(Užduotis. Suformuluoti ir įrodyti požiedžio ir polaukio kriterijus).

Paskaita 1 – 06

Skaičių sistemos

Pabandysime įvestų sąvokų pagrindu susisteminti ir išplėsti mokyklinės matematikos žinias apie skaičius.

Natūraliųjų skaičių aibė N . Matematinė indukcija. Paprasčiausia skaičių aibė, atrodytų, yra natūraliųjų skaičių aibė. Tačiau, išmokus sudėti 2 ir 3, atsakyti į klausimą, kodėl suma yra 5 - labai nelengva. Dar sunkiau paaiškinti, kas tai yra tie, rodos, įprasti simboliai (skaičiai) 2, 3, 5,

Pirmoje paskaitoje jau minėjome, kad sisteminant, griežtinant matematines žinias elgiamasi vienodai: pradžioje išskiriamos pagrindinės, intuityviai suprantamos, *neapibrėžiamos sąvokos*. Jų pagalba formuluojami kitas reikalingas sąvokas apibūdinantys *apibrėžimai*. Tada aptariama, kokie pagrindiniai teiginiai – faktai yra savaime suprantami ir priimami be įrodymo. Juos vadiname *aksiomomis*. Nuspręsti, ką vadinti aksioma, kokie faktai įtrauktini į aksiomų sąrašą dažnai būna irgi nelengva problema. O, suformulavus *aksiomų sistemą*, iškyla nelengvesnė, aksiomų sistemos *interpretacijos*, t.y. aibės, kuriai galioja ta aksiomų sistema, konstrukcijos užduotis. Toliau vystoma pati matematinė teorija: įrodinėjamos *teoremos*, formuluojamos taisyklės. Ieškoma racionaliausių konkrečios matematinės teorijos išdėstymo kelių, todėl tie išdėstymai neretai skiriasi, jie tikslinami, tobulinami.

Norėdami griežtai apibrėžti natūraliuosius skaičius, daugelio kartų matematikai irgi svarstė, kas priimtina be įrodymo, o kas įrodytina. Šiuo metu visuotinai priimta italų matematiko *D. Peano* (Giuseppe Peano, 1859 – 1932) *aksiomų sistema*.

Aibės sąvoka, kaip minėjome, yra pagrindinė, neapibrėžiama. Tuo tarpu *sąryšius* jau galima apibrėžti aibių teorijos terminais. Natūraliųjų skaičių struktūrai apibrėžti iš esmės ir pakanka šių dviejų sąvokų.

Ap. Natūraliaisiais skaičiais vadiname elementus bet kurios netuščios aibės N , kurioje apibrėžtas elementų unarinis sąryšis “eina po”, tenkinantis keturias aksiomas.

1. Yra toks N elementas (vadinkime jį vienetu ir žymėkime 1), kuris neina po jokio elemento.
2. Po kiekvieno elemento a eina vienas ir tiksliai vienas elementas. Jį žymėsime a' .
3. Kiekvienas elementas eina ne daugiau kaip po vieno elemento.
4. (Indukcijos aksioma). Kiekvienam poaibiui $M \subset N$ tokiu, kad $1 \in M$ ir teisinga $a \in M \Rightarrow a' \in M$, galioja: $M = N$.

Aišku, tuoj pat kyla klausimas: ar yra konkreti aibė tenkinanti šią aksiomų sistemą?

Pasirodo, kad *taip*. Be to, tą aibę galima sukonstruoti *ne vieninteliu būdu*. Konstrukcijos keliams, visoms natūraliųjų skaičių savybėms aptarti ir įrodyti reiktų nemažai laiko. Tai daroma specialiuose matematikos kursuose, o mes apsiribosime tik konstatavimu, kad aibių, tenkinančių Peano aksiomų sistemą, tikrai yra ir aptarsime kelias svarbesnes aibės N savybes.

Kai iš atskirų faktų daromos apibendrintos išvados, tai sakoma, kad samprotaujama *induktyviai*. Induktyvus mąstymas (indukcija) būdingas žmogui: štai ryte ateiname į troleibuso stotelę ir po kelių minučių sulaukiame troleibuso, vežančio mus reikiama kryptimi. Taip elgiamės išeidami iš to, kad žinome atskirus faktus: troleibusų judėjimo grafiką, maršrutus, tai, kad mieste, kuriame esame, reikiamame maršrute nevyksta remonto darbai ir pan. Iš tų atskirų, kas rytą pasitvirtinančių faktų, darome bendrą (mums svarbią) išvadą: kas rytą tam tikroje vietoje, tuo pačiu laiku sustoja mums reikalingas troleibusas.

Kitoks yra *deduktyvusis* mąstymo būdas (*dedukcija*), kai atvirkščiai: iš bendros informacijos, nustatomas atskirų konkrečių teiginių teisingumas. Pvz., iš ilgametės patirties žinome: vidurdienį yra šviesu. Darome išvadą: vidurdienį bus šviesu ir šiandien, ir rytoj, ir poryt.

Abu mąstymo būdai naudojami realiame gyvenime: ekonomikoje, sporte, kriminalistikoje ir t.t. Deja, matematikai jų nepakanka, nes matematika – tikslusis mokslas ir, jei jau koks faktas įrodomas, tai jis teisingas *visada*: pvz., Pitagoro teorema yra teisinga *viesiems* statiesiems trikampiams. Jos teisingumas griežtai įrodytas, o ne patikrintas. Kad ir kiek stačiųjų trikampių išmatuotume, Pitagoro teorema tuo nebus įrodyta. Galėsime (induktyviai mąstydami) tik suformuluoti hipotezę: *greičiausiai* viesiems statiesiems trikampiams įžambinės kvadratas lygus statinių kvadratų sumai. Tuo tarpu matematinis įrodymas nepalieka jokių išlygų “*greičiausiai*”.

Be to, induktyvaus (ar deduktyvaus) mąstymo keliu suformuluota hipotezė gali pasirodyti neteisinga: troleibusas gali tiesiog sugesti, o vidurdienį toje vietovėje įvykti pilnas saulės užtemimas...

1640 m. prancūzų matematikas P.Ferma (Fermat) suformulavo hipotezę, kad skaičiai

$$F_n := 2^{2^{n-1}} + 1$$

su visais natūraliaisiais n yra pirminiai. Taip jis nusprendė betarpiškai patikrinęs pirmuosius penkis iš jų:

$F_1 = 3$, $F_2 = 5$, $F_3 = 17$, $F_4 = 257$, $F_5 = 65537$. Jie tikrai pasirodė besą pirminiai. Tačiau skaičius $F_6 = 2^{32} + 1$ patikrinti (tais laikais skaičiuoklių dar nebuvo...) Ferma nesugebėjo. Tik 1732 m. garsus šveicarų matematikas L.Oileris (Euler) paneigė Ferma hipotezę ir parodė, kad:

$$F_6 = 2^{32} + 1 = 641 \cdot 6700417.$$

Ketvirtoji iš aibę N nusakančių aksiomų pagrindžia svarbų *matematinės indukcijos principą* (MIP), plačiai vartojamą griežtam matematinių faktų įrodymui.

Tarkime $P(n)$ yra vienvietis predikatas, o jo apibrėžimo sritis yra N .

Paprasčiausias yra toks MIP variantas.

Teorema (MIP – 1). *Jei predikatas $P(n)$ yra teisingas kai $n = 1$ ir iš jo teisingumo kokiame nors natūraliajam skaičiui $n = k$ išplaukia, kad jis teisingas ir skaičiui $n = k' = k + 1$, tai tas predikatas yra teisingas su visais $n \in N$.*

Įr. Pažymėję $M = \{n \in N \mid P(n) = 1\}$ įsitikiname, kad M yra toks N poaibis, kuris tenkina 4–tosios Peano aksiomos reikalavimus. Pagal jį: $M = N$. Tiek ir tereikėjo ... ☺ . QED.

Yra ir bendriau formuluojamų MI principų: *apibendrintasis MIP - 2, sustiprintasis MIP - 3* ir, pagaliau, *sustiprintasis – apibendrintasis MIP - 4*.

Pvz., *apibendrintasis MI principas*, naudojant matematinius simbolius, formuluojamas taip:

Jei predikatui $P(n)$ yra teisinga:

- $(\exists n_0 \in N) P(n_0) = 1$,
- iš prielaidos $P(k) = 1$ su natūraliuoju $k > n_0$, išplaukia $P(k + 1) = 1$,

tai: $(\forall n \in N, n \geq n_0) P(n) = 1$.

Toks MIP variantas reikalingas tada, kai koks nors predikatas virsta teisingu teiginiu su visais n , išskyrus keletą pirmųjų. Pvz., nelygė $2^{n^2} > 5n^2 + 7$ yra teisinga su visais $n \geq 3$, todėl MIP – 1 jai nepritaikomas, tenka remtis MIP – 2.

Sustiprintas MIP – 3 skiriasi nuo MIP – 1 prielaidos formulavimu.

MIP – 3. Jei predikatui $P(n)$ yra teisinga:

- $P(1) = 1$,
- iš prielaidos $P(l) = 1$ su visais natūraliaisiais $l < k$, išplaukia $P(k) = 1$,

tai: $(\forall n \in N) P(n) = 1$.

Pastebėkime, kad MIP – 3 prielaida yra *sustiprinta*, - leidžiama naudoti daugiau, nei MIP – 1.

Pagaliau *sustiprintasis-apibendrintasis* principas MIP – 4, skiriasi nuo čia pateikiamo MIP – 3, tuo, kad pirmasis žingsnis (sakoma: *indukcijos bazė*) yra teiginio $P(n_0) = 1$, patikrinimas kai $n_0 \in N, n_0 > 1$, t.y. predikatas keliems pirmiesiems n virsta neteisingu teiginiu.

Natūraliųjų skaičių sudėtis ir daugyba. Savybės. Tarkime, vienaip ar kitaip jau sukonstravome aibę N . Tačiau kol kas be pačios aibės nieko daugiau neturime: “nemokame” nei dauginti, nei sudėti, “nežinome” (t.y. nesame įrodę) jokių veiksmų su natūraliaisiais skaičiais savybių. Pripraskime prie svarbiausio dalyko: *visi įprasti, iš mokyklos žinomi faktai apie natūraliuosius skaičius turi būti išvesti iš Peano aksiomų sistemos!*

Pradėkime nuo natūraliųjų skaičių *sudėties* operacijos aptarimo.

Ap. Natūraliųjų skaičių sudėtis apibrėžiama taisyklėmis:

- S1. $(\forall n \in N) n + 1 = n'$,
- S2. $(\forall m, n \in N) n + m' = (n + m)'$.

Šios dvi taisyklės įgalina *sudėti*, bet kokius du natūraliuosius skaičius. Pvz.,

$$2 + 3 \stackrel{3=2'}{=} 2 + 2' \stackrel{S2}{=} (2 + 2)' \stackrel{2=1'}{=} (2 + 1)' \stackrel{S2}{=} ((2 + 1)')' = (3')' \stackrel{3'=4}{=} 4' \stackrel{4'=5}{=} 5.$$

Maža to, įprastos šio veiksmo (algebrinės operacijos) savybės: *komutatyvumas* (K) ir *asociatyvumas* (A) yra įrodomos. Pvz., jei tarsime, kad A -savybė jau įrodyta (žr. vadovėlio I d. 71 psl.), tai, remiantis MIP - 1, galima įrodyti ir natūraliųjų skaičių sudėties K -savybę.

Teorema. *Natūraliųjų skaičių sudėtis yra komutatyvi.*

Įr. Turime parodyti, kad $(\forall m, n \in N) n + m = m + n$. Taikysime MIP - 1 m atžvilgiu ir darysime tai dviem etapais.

1. Pradžioje įrodysime, kad, kai $m = 1$, tai $(\forall n \in N) n + 1 = 1 + n$ yra teisingas teiginys. Pažymėję jį $(\forall n \in N) P(n)$, pastebime, kad dabar galime taikyti MIP - 1 pagal n .

Turime:

$$1.1. P(1) = 1, \text{ nes } 1 + 1 = 1 + 1 = 1' = 2.$$

$$1.2. \text{ Tarkime } P(k) = 1, \text{ t.y. teiginys } k + 1 = 1 + k \text{ yra teisingas, kai } k \in N.$$

$$1.3. \text{ Parodysime, kad ir } P(k') = 1. \text{ Tikrai:}$$

$$k' + 1 \stackrel{S1}{=} (k + 1) + 1 \stackrel{\text{prielaida}}{=} (1 + k) + 1 \stackrel{\text{asoc}}{=} 1 + (k + 1) \stackrel{S1}{=} 1 + k'.$$

Pagal MIP - 1, teiginys $(\forall n \in N) n + 1 = 1 + n$ yra teisingas.

2. Leiskime, kad teiginys $(\forall n \in N) n + s = s + n$ yra teisingas su koku tai $s \in N$.

3. Parodysime, kad jis teisingas ir su s' , t.y. $(\forall n \in N) n + s' = s' + n$:

$$\begin{aligned} n + s' &\stackrel{S1}{=} n + (s + 1) \stackrel{\text{asoc}}{=} (n + s) + 1 \stackrel{\text{prielaida}}{=} (s + n) + 1 \stackrel{\text{asoc}}{=} s + (n + 1) \stackrel{\text{punktas1}}{=} s + (1 + n) = \\ &\stackrel{\text{asoc}}{=} (s + 1) + n \stackrel{S1}{=} s' + n. \end{aligned}$$

Pagal MIP - 1, teiginys $(\forall m, n \in N) n + m = m + n$ yra teisingas. QED.

Panašiai apibrėžiamas ir natūraliųjų skaičių *daugybės* veiksmas.

Ap. Natūraliųjų skaičių daugyba apibrėžiama taisyklėmis:

$$D1. (\forall n \in N) n \cdot 1 = n,$$

$$D2. (\forall m, n \in N) n \cdot m' = nm + n.$$

Toliau reiktų įrodyti daugybės K ir A -savybes, bei daugybės *distributyvumo* (D) savybę sudėties atžvilgiu (žr. vadovėlio 72 psl). Šių savybių įrodymus mes praleidžiame.

Natūraliųjų skaičių aibėje nesunku apibrėžti ir tiesinės tvarkos sąryšį “mažiau”, t. y. aibę N *sutvarkyti*.

Ap. Jei m ir n yra bet kokie natūralieji skaičiai, tai sakome, kad m yra mažesnis už n (ir rašome $m < n$), jei egzistuoja toks natūralusis skaičius k , kad $m + k = n$.

Pvz., $17 < 29$, nes $17 + 12 = 29$.

Nesunkiai įrodoma, kad šitaip apibrėžtas BS “ $<$ ” yra *tiesinės tvarkos sąryšis* (t.y. antirefleksyvus, tranzityvus ir turi trichotomijos savybę). Taigi, jo pagalba, aibė N yra *sutvarkyta*.

Paminėsime dar keletą iš Peano aksiomų išplaukiančių faktų, kuriuos dažnai taikysime ateity: *Archimedo aksiomą* (AA), *mažiausiojo skaičiaus principą* (MSP), *didžiausiojo skaičiaus principą* (DSP).

Teorema. (AA). $(\forall m, n \in \mathbb{N}) (\exists k \in \mathbb{N}) k \cdot m > n$.

Teorema. (MSP). Kiekvienas netuščias N poaibis turi mažiausiąjį elementą.

Teorema. (DSP). Kiekvienas netuščias baigtinis N poaibis turi didžiausiąjį elementą. Jų įrodymus irgi praleidžiame.

MIP pagalba galima įrodyti ir *Niutono binomo formulę* (Isaac Newton, 1642 – 1727, garsus anglų matematikas ir fizikas).

Niutono binomo formulė.

$$(\forall n \in \mathbb{N}) (\forall a, b \in \mathbb{R}) (a + b)^n = \sum_{k=0}^n C_n^k a^k b^{n-k}.$$

Įrodymas. Naudosime MIP.

$$1. \text{ Kai } n = 1, \text{ tai } \sum_{k=0}^1 C_1^k a^k b^{1-k} = C_1^0 a^0 b^1 + C_1^1 a^1 b^0 = b + a = (a + b)^1.$$

2. Darome prielaidą, kad formulė yra teisinga su koku nors fiksuotu $n > 1$.

3. Naudodamiesi šia prielaida, parodysime, kad Niutono binomo formulė teisinga ir sekančiam natūraliajam skaičiui $n' = n + 1$. Iš tikrųjų, pirmiausia:

$$(a + b)^{n+1} \stackrel{\text{prielaida}}{=} (a + b) \cdot \sum_{k=0}^n C_n^k a^k b^{n-k} = \sum_{k=0}^n C_n^k a^{k+1} b^{n-k} + \sum_{k=0}^n C_n^k a^k b^{n+1-k}.$$

Dabar pirmoje sumoje atskirkime paskutinį dėmenį, o antroje, – pirmąjį:

$$(a + b)^{n+1} = C_n^n a^{n+1} + \sum_{k=0}^{n-1} C_n^k a^{k+1} b^{n-k} + \sum_{k=1}^n C_n^k a^k b^{n+1-k} + C_n^0 b^{n+1}.$$

Toliau, panaudosime kombinatorines tapatybes:

$$C_n^0 = C_{n+1}^0 = C_n^n = C_{n+1}^{n+1}; \quad C_n^k + C_n^{k-1} = C_{n+1}^k.$$

Tuo tikslu pakeiskime pirmosios sumos sumavimo indeksą į $i - 1$, po to, vietoje i vėl rašydami k , sujunkime visus keturis dėmenis:

$$\begin{aligned} (a + b)^{n+1} &= C_n^n a^{n+1} + \sum_{i=1}^n C_n^{i-1} a^i b^{n-i+1} + \sum_{k=1}^n C_n^k a^k b^{n+1-k} + C_n^0 b^{n+1} = \\ &= C_{n+1}^{n+1} a^{n+1} + \sum_{k=1}^n C_n^{k-1} a^k b^{n-k+1} + \sum_{k=1}^n C_n^k a^k b^{n+1-k} + C_{n+1}^0 b^{n+1} = \sum_{k=0}^{n+1} C_{n+1}^k a^k b^{n+1-k}. \text{ QED.} \end{aligned}$$

Pastebėkime, kad vietoje R galime imti bet kokią nulinės charakteristikos lauką L .

Išvada. $C_n^0 + C_n^1 + C_n^2 + \dots + C_n^n = 2^n$.

Šią kombinatorinę tapatybę gauname Niutono binomo formulėje paėmę $a = b = 1$. Ji reiškia, kad baigtinė aibė, kurioje yra n elementų, turi 2^n poaibių.

Niutono binomo bendriniai

1. *Polinominė formulė.* Kartais reikia natūraliuoju laipsniu n kelti ne dvinarį, o k narių sumą: $a_1 + a_2 + \dots + a_k$. Tada teisinga tokia formulė:

$$(a_1 + a_2 + \dots + a_k)^n = \sum_{i_1 + i_2 + \dots + i_k = n} P(i_1, i_2, \dots, i_k) a_1^{i_1} a_2^{i_2} \dots a_k^{i_k}.$$

2. Kai kada naudojamas ir toks Niutono formulės bendrinys:

$$(\forall n \in N) (\forall a, b, \mu \in R) (a + b)^\mu = \sum_{k=0}^{\infty} \binom{\mu}{k} a^{\mu-k} b^k.$$

Čia simboliu $\binom{\mu}{k}$ žymime taip vadinamuosius *apibendrintuosius derinius*. Jie bet kokiam realiajam μ apibrėžiami formule:

$$\binom{\mu}{k} = \frac{\mu(\mu-1)\dots(\mu-k+1)}{k!}.$$

Savaime suprantama, kad toks Niutono binomo bendrinys turi prasmę tiksliai tada, kai eilutė dešinėje formulės pusėje konverguoja.

Paskaita 1 – 07

Skaičių sistemos (tęsinys)

Sveikųjų skaičių žiedas. Aptarėme natūraliųjų skaičių aibę N . Operuojant algebrinių struktūrų terminais, $(N, +)$ yra adicinis pusgrupis, o $(N, \cdot)$ - multiplikacinis.

Labai greitai žmonės pastebėjo, kad natūraliųjų skaičių aibė N netenkina net paprasčiausių praktinių poreikių: jei žinotume tik natūraliuosius skaičius, tai negalėtume išspręsti net tokios elementarios lygties: $4 + x = 3$ arba, bendresniu atveju, lygties $m + x = n$ kai $m, n \in N$ ir $m > n$.

Iškyla uždavinys: taip išplėsti aibę N , kad naujoje aibėje (žymėkime ją Z) tokios lygtys jau būtų išsprendžiamos, o sudėties ir daugybos veiksmas būtų atliekami kaip ir anksčiau, bei turėtų įprastas savybes.

Kadangi lygties $m + x = n$ išsprendžiamumas ekvivalentus atvirkštinės operacijos sudėčiai (t.y. atimties) įvykdomumui, tai nesunku suvokti, kad Z turi tenkinti žiedo aksiomas. Taigi ieškomoji AS $(Z, +, \cdot)$ turėtų tenkinti tokius reikalavimus (aksiomas):

- | | |
|---|-----|
| <ul style="list-style-type: none"> - $Z \supset N$, - AS $(Z, +, \cdot)$ - komutatyvus žiedas, - Z yra <i>minimali</i> aibė, tenkinanti pirmuosius du reikalavimus. | (*) |
|---|-----|

Aibę Z vadinsime (jei ją rasime) *sveikųjų skaičių aibe*, o AS $Z := (Z, +, \cdot)$ - *sveikųjų skaičių žiedu*. Neretai pasitaiko, kad pasakome trumpiau: "sveikųjų skaičių žiedas Z ", o ne "sveikųjų skaičių žiedo $Z := (Z, +, \cdot)$ bazinė aibė Z ". T.y. sutapatiname aibę Z su algebrine struktūra Z . Griežtai sakant, šitaip elgtis yra nekorektiška; šitai toleruojama tik kalbos lakoniškumo dėlei ir tik tada, kai iš konteksto aišku, apie ką kalbama.

Apie bazinės aibės Z paieškas. Be abejo, ieškomoji aibė egzistuoja, juk apie sveikuosius skaičius, bent jau mokykloje, esame girdėję. Tai, – aibė sudaryta iš simbolių $0, -1, 1, -2, 2, -3, 3, \dots$, su kuriais mokykloje išmokome atlikti įprastus aritmetinius veiksmus.

Griežčiau kalbant, tuo tarpu mes žinome, kad: simboliai $1, 2, 3, \dots$ žymi bet kokios aibės, tenkinančios *Peano aksiomų sistemą*, elementus. Susitarėme juos vadinti *natūraliaisiais skaičiais*. Aptarėme jų sudėtį, daugybą ir pabrėžėme, kad visas įprastas šių veiksmų savybes (KAD) galima įrodyti. Natūraliųjų skaičių sudėties komutatyvumą ir įrodėme matematinės indukcijos metodu.

Tačiau, tiksliai apibūdinti, ką reiškia simboliai $0, -1, -2, -3, \dots$, - kol kas nemokame. Visos žinios apie juos paremtos argumentu "taip sakė matematikos mokytojas (-ja)".

Vadovėlyje (99–101psl.) trumpai aptarta, kaip pasiekti, kad minėta aibė $Z := \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$ tenkintų (*) reikalavimus. Tai, – tik vienas iš galimų sveikųjų skaičių žiedo konstrukcijos metodų (modelių). Jis vadinamas *mokykliniu sveikųjų skaičių žiedo modeliu*. Pabandykite eiti kitu aksiomų sistemos (*) interpretacijos paieškų keliu.

Pirmiausia apibrėžkite naują aibę $A := N \times N$. Jai, kaip žinia, priklauso visos *sutvarkytos natūraliųjų skaičių poros*. Šioje aibėje apibrėškime tokį binarią sąryšį σ :

$$(\forall (m, n), (k, l)) \quad (m, n) \sigma (k, l) \equiv m + l = n + k.$$

Kartais sąryšiu σ susietos poros vadinamos tiesiog *lygiomis*.

Pavyzdžiui, $(4, 7) \sigma (13, 16)$, nes $4 + 16 = 7 + 13$, tačiau $(4, 7) \overline{\sigma} (1, 6)$, nes $4 + 6 \neq 7 + 1$.

Lengva įsitikinti, kad σ - ES. Patikrinkite tai savarankiškai.

Tuokart, pagal faktorizacijos teoremą (žr. P 1 – 02), galima sukonstruoti *faktoraibę* $Z_0 := A / \sigma$, kurią, kaip minėjome, sudaro porų *ekvivalentumo klasės* pagal sąryšį σ . Pvz., viena iš klasių yra aibė $K_{(1,4)} = \{(1,4), (2,5), (3,6), (4,7), \dots, (13,16), \dots\}$, kita - $K_{(1,1)} = \{(1,1), (2,2), (3,3), \dots, (9,9), \dots\}$ ir t.t.

Toliau nagrinėjame būtent aibę Z_0 . Patogumo dėlei, susitarkime jos elementus (porų klases) žymėti taip: $K_{(m,n)} =: [m, n]$.

Aibėje Z_0 galima apibrėžti tokią “*sudėtį*” ir tokią “*daugybą*”, kad $AS (Z_0, +, \cdot)$ būtų *komutatyvus žiedas*. Be to, aibės Z_0 elementai yra (porų) aibės, o aibių lygybės sąvoka mums jau žinoma. Tad užrašą $[m, n] = [k, l]$ čia suprasime taip: šios klasės yra *lygios kaip aibės*. Beje, iš *faktorizacijos teoremos* žinome, kad: kai elementai (m, n) ir (k, l) nesusieti sąryšiu σ (t.y. nėra ekvivalentūs (lygūs)), tai klasės $[m, n]$ ir $[k, l]$ neturi nė vieno bendro elemento, o kai susieti, - jos sutampa.

$$Ap. \quad (\forall [m, n], [k, l] \in Z_0) \quad [m, n] + [k, l] = [m + k, n + l].$$

$$Ap. \quad (\forall [m, n], [k, l] \in Z_0) \quad [m, n] \cdot [k, l] = [mk + nl, ml + nk].$$

Teorema. $AS (Z_0, +, \cdot)$ yra komutatyvus žiedas su vienetu.

Įr. Detaliau, – savarankiškai ir per pratybas. Čia pateiksime kelis įrodymo žingsnius.

- taip apibrėžtos *sudėties komutatyvumas* išplaukia iš to, kad

$$[k, l] + [m, n] = [k + m, l + n] = [m + k, n + l] = [m, n] + [k, l],$$

kadangi klasės $[k + m, l + n]$, $[m + k, n + l]$ generuojančios atitinkamas poros $(k + m, l + n)$ ir $(m + k, n + l)$ yra *lygios* (ekvivalenčios, susietos sąryšiu ES σ).

Iš tikrųjų, pagal apibrėžimą turi būti: $k + m + n + l = l + n + m + k$, bet kadangi jau žinome, jog *natūraliųjų skaičių sudėtis yra komutatyvi ir asociatyvi*, tai pastaroji lygybė yra akivaizdi. Panašiai įrodomas ir sudėties *asociatyvumas* aibėje Z_0 .

- dabar jau nesunku parodyti, kad struktūra $(Z_0, +)$ yra *adicinė Abelio grupė*. Tikrai, elementas $[m, m] = [1, 1]$ yra neutralusis (nulinis) aibės Z_0 elementas, o elementui $[m, n] \in Z_0$ simetriškas (priešingas) yra $[n, m]$. Patikrinkite tai savarankiškai.

- įsitikinkime, kad klasė $K_{[m, m+1]} := e = [m+1, m]$ yra aibės Z_0 vienetinis elementas. Iš tikrųjų:

$$(\forall [k, l] \in Z_0) [k, l] \cdot [m+1, m] = [k(m+1) + lm, km + l(m+1)] = [k, l], \text{ nes} \\ k(m+1) + lm + l = km + l(m+1) + k.$$

Tiesą sakant, reiktų dar patikrinti, ar ir sudėties bei daugybos veiksmi aibėje Z_0 apibrėžti *korektiškai*.

Ką norima tuo pasakyti ?

Akcentavome: $[m, n] = [m', n']$, kai tik $(m, n) \sigma (m', n')$, t.y. $m + n' = n + m'$. Pvz., nulinis elementas $[m, m]$ gaunamas imant bet kurį natūralųjį skaičių m . T.y. $O_{Z_0} = [1, 1] = [2, 2]$ ir t.t. Korektiškumo klausimas formuluojamas taip: ar aibėje Z_0 apibrėžiant sudėtį (daugybą) rezultatas nepasikeis, jei klasių $[m, n]$, $[k, l]$ “generuojančias” poras (m, n) , (k, l) pakeisime kitomis:

$$(m, n) \longrightarrow (m', n') \text{ ir } (k, l) \longrightarrow (k', l')?$$

$$\text{T.y. ar } [m, n] + [k, l] = [m', n'] + [k', l']?$$

Įsitikinkite, kad atsakymas į šį klausimą yra: *nepasikeis*.

Izomorfizmo principo taikymas. Tačiau, struktūra $(Z_0, +, \cdot)$, deja, dar nėra ieškomoji, nes netenkinama pirmoji iš (*) sąlygų – bazinė aibė nėra bazinės aibės N viršais. Šis nesklandumas įveikiamas panaudojant AS izomorfizmo sąvoką. Kai $N_1 := \{[n+k, n] \mid n, k \in N\}$, tai struktūra $(N_1, +, \cdot)$ yra *izomorfiška* struktūrai $(N, +, \cdot)$. Bijekcija φ tarp bazinių aibių nustatoma taisykle $\varphi: [n+k, n] \leftrightarrow k$. T.y. $\varphi([n+k, n]) = k$. Jei $\varphi([m+l, m]) = l$, tai, tikrindami, ar *sumos vaizdas lygus dėmenų vaizdų sumai*, gautume: $\varphi([n+k, n] + [m+l, m]) = \varphi([n+m+k+l, n+m]) = k+l = \varphi([n+k, n]) + \varphi([m+l, m])$.

Panašiai patikrinama ir sąlyga sandaugos vaizdui.

Belieka tokie konstravimo žingsniai:

- imame aibę $(Z_0 \setminus N_1) \cup N =: Z$. Aibėje Z jau “atsiranda” visi natūralieji skaičiai, t.y. $Z \supset N$;

- likusius aibės Z elementus pažymime taip: $[n, n+k] := -k$, $[m, m] := 0$. Kadangi tiesinės tvarkos sąryšis “ $<$ ” aibėje N jau apibrėžtas, tai, pagal jam galiojančią *trichotomijos savybę*, kitokių variantų ir nėra;

- iš naujo aptariame (apibrėžiame) *sudėties* ir *daugybės* veiksmus aibėje Z . Pagrindinė idėja: apibrėžiant veiksmus tarp “naujų” ir “senų” elementų $n + [k, l]$, $n \cdot [k, l]$ su bet kokių $n \in N$, tereikia prisiminti, kad $n = \varphi([1 + n, 1])$, todėl, pavyzdžiui, sumą $n + [k, l]$ natūralu apibrėžti šitaip:

$$n + [k, l] = [1 + n, 1] + [k, l] = [n + k + 1, l + 1] = [n + k, l].$$

Veiksmų su “senais” elementais $[n, m]$ ir $[k, l]$ apibrėžimai išlieka nepakitę, o veiksmų su natūraliaisiais skaičiais apibrėžimai pažodžiui perkeliama iš temos “Natūralieji skaičiai”.

Nesunku įsitikinti, kad žiedas $(Z_0, +, \cdot)$ ir AS $(Z, +, \cdot)$ yra izomorfiški (tinka taip pat apibrėžiama bijekcija φ), todėl, *pagal izomorfizmų teoremą*, ir struktūra $(Z, +, \cdot)$ yra žiedas. Šis žiedas tenkina jau visus (*) reikalavimus, todėl jis vadinamas *sveikųjų skaičių žiedu*, o jo bazinės aibės Z elementai – *sveikaisiais skaičiais*.

Toliau galima aptarinėti ir įrodinėti visas žinomas sveikųjų skaičių savybes: pvz., aibėje Z apibrėžti sąryšį “mažiau”. Tiesinės tvarkos sąryšis “mažiau” sveikųjų skaičių aibėje, nusakomas panašiai kaip tai buvo padaryta aibėje N . Būtent:

Ap. Jei m ir n yra bet kokie sveikieji skaičiai, tai sakome, kad m yra mažesnis už n (ir rašome $m < n$), jei egzistuoja toks natūralusis skaičius k , kad $m + k = n$.

Pvz., $-7 < -5$, nes $-7 + 2 = -5$.

Vėlgi, lengvai parodoma, kad sąryšis “<” yra *tiesinės tvarkos sąryšis*. Galima apibrėžti ir absoliutinio didumo sąvoką, įrodyti “trikampio” nelygybę, aptarti dalumo sąryšį ir t.t.

Skyriuje “Skaičių teorija” sveikųjų skaičių žiedo savybes studijuosime nuodugniau.

Nesunkiai parodoma, kad sukonstruoti sveikųjų skaičių struktūra $(Z, +, \cdot)$ yra *minimali* ta prasme, kad nėra Z tiesioginio poaibio, tenkinančio (*) reikalavimus.

Racionaliųjų skaičių aibė Q . Prireikus išspręsti lygtį $5x = 12$ (bendru atveju: $m \cdot x = n$, $m, n \in Z$, $m \neq 0$), paaiškėja, kad ir aibė Z neišsprendžia visų praktinių problemų, nes yra paprasčiausiai *per siaura*: joje ne visada įmanomas atvirkštinis daugybai veiksmas, – *dalyba*. Skyrelyje “Algebrinės struktūros” jau minėjome, kad struktūrą, kurios bazinė aibė uždara *sudėties* ir *daugybės* bei *atimties* ir *dalybos* (iš ne nulio) operacijų atžvilgiu ir tenkinamas sąlygų kompleksas KAD, vadiname *lauku*.

Tad ieškodami naujos skaičių aibės Q , jai turėsime kelti tokius reikalavimus:

- | | |
|---|------|
| <ul style="list-style-type: none"> - $Q \supset Z$, - struktūra $(Q, +, \cdot)$ yra <i>laukas</i>, - Q yra minimalus žiedo Z plėtinys. | (**) |
|---|------|

Šiuos reikalavimus tenkina, pavyzdžiui, tokia aibė

$$Q_0 := \left\{ \frac{m}{n} \mid m \in Z, n \in N \right\}.$$

Čia simbolis $\frac{m}{n}$ tuo tarpu nereiškia dalybos, o yra *tik simbolis*. Kaip ir konstruojant sveikųjų skaičių žiedą, reiktų nagrinėti ne pačius simbolius, o *lygių* (ekvivalenčių) simbolių aibes – klases. Simbolių $\frac{m}{n}$ ir $\frac{k}{l}$ lygybės sąryšį (žymėkime jį “=”) apibrėžiame šitaip:

$$Ap. \frac{m}{n} = \frac{k}{l} \equiv ml = nk .$$

Išitikinkite, kad “=” yra ES aibėje Q_0 !

Dabar aibę Q_0 turėtume pakeisti faktoraibe $Q_0 / \equiv$, su elementais :

$$K_{\frac{m}{n}} := \left\{ \frac{k}{l} \mid \frac{k}{l} \in Q_0, \frac{k}{l} = \frac{m}{n} \right\}.$$

Pvz., $K_{\frac{2}{5}} := \left\{ \frac{k}{l} \mid \frac{k}{l} \in Q_0, \frac{k}{l} = \frac{2}{5} \right\} = \left\{ \frac{2}{5}, \frac{4}{10}, \frac{6}{15}, \dots \right\}$. Paprastumo dėlei, susitarkime

klasę $K_{\frac{m}{n}}$ kaip ir anksčiau žymėti simboliu $\frac{m}{n}$, suprasdami jį kaip aibę $\left\{ \frac{k}{l} \mid \frac{k}{l} \in Q_0, \frac{k}{l} = \frac{m}{n} \right\}$.

Tokių simbolių (trupmenų) sudėtį ir daugybą reikia formaliai apibrėžti, o veiksmų savybes, postuluojamas apibrėžime (**), – griežtai įrodyti. Apibrėžimai yra tokie:

$$Ap. \frac{m}{n} + \frac{k}{l} = \frac{ml + nk}{nl}.$$

$$Ap. \frac{m}{n} \cdot \frac{k}{l} = \frac{mk}{nl}.$$

Svarbu suvokti: kol kas tai nėra įprastos trupmenos, o tik specialūs simboliai. Veiksmų apibrėžimai, kaip matome, veda mus prie mokyklinio sąvokos “trupmena” supratimo, bet tai mes darome griežtai aksiomatiškai.

Pastebėsime dar, kad įprastas šitaip apibrėžtų veiksmų su aibės Q_0 elementais savybes KAD galima įrodyti. Be to, ir šiuo atveju prireikia aptarti operacijų apibrėžimo korektiškumą, bei pasinaudoti *izomorfizmo principu*, nes vėlgi formaliai $Q_0 \not\supset Z$. Panašiai kaip konstruojant sveikųjų skaičių aibę, elgiamasi taip: imame aibę

$$Q := \left(Q_0 \setminus \left\{ \frac{m}{1} \mid m \in Z \right\} \right) \cup Z,$$

ir parodome, jog struktūros $(Q_0, +, \cdot)$ ir $(Q, +, \cdot)$ yra izomorfiškos.

Aibę Q vadinsime *racionaliųjų skaičių aibe*, o algebrinę struktūrą $\mathcal{Q} := (Q, +, \cdot)$, – *racionaliųjų skaičių lauku*. Jos elementus vadinsime *racionaliaisiais skaičiais*.

Galimi ir kitokie racionaliųjų skaičių įvedimo būdai.

Racionaliųjų skaičių lauko savybės. Visos kitos įprastos sąvokos ir racionaliųjų skaičių (trupmenų) savybės išplaukia iš apibrėžimo ir anksčiau aptartų faktų. Pvz., lauką $\mathcal{Q}$ galima sutvarkyti įvedant jau įprastą sąryšį “mažiau”.

Ap. Racionalusis skaičius $r = \frac{m}{n}$ vadinamas teigiamu, jei $mn \in \mathbb{N}$. Rašome $r > 0$.

Ap. Sakome, kad skaičius $a \in \mathcal{Q}$ yra mažesnis už $b \in \mathcal{Q}$, jeigu egzistuoja toks teigiamas racionalusis skaičius c , kad $a + c = b$. Rašome $a < b$.

Pasirodo, kad sąryšis “ $<$ ” yra tiesinės tvarkos sąryšis, taigi, – laukas $(\mathcal{Q}, +, \cdot)$ yra sutvarkytas laukas.

Laukas $\mathcal{Q}$ turi ir keletą specifinių ypatybių.

Laukas $(\mathcal{Q}, +, \cdot)$ yra išsidėstęs. Terminu “išsidėstęs” nurodoma, kad racionaliųjų skaičiai skirstomi į teigiamus ir neigiamus ir kad bazinės aibės $\mathcal{Q}$ poaibis $\mathcal{Q}_+ := \{a \in \mathcal{Q} \mid a > 0\}$, yra uždaras sudėties ir daugybos operacijų atžvilgiu.

Dar viena svarbi lauko $(\mathcal{Q}, +, \cdot)$ savybė yra ta, kad jis yra pirminis laukas.

Ap. Laukas vadinamas pirminiu, jei jis neturi tiesioginių polaukių.

Teorema. Laukas $(\mathcal{Q}, +, \cdot)$ yra pirminis.

(Šią lauko $(\mathcal{Q}, +, \cdot)$ savybę galima suformuluoti taip: $\mathcal{Q}$ yra pats “siauriausias” iš skaičių laukų.)

Įr. Jei lauką $\mathcal{Q}$ sutapatinsime su visų nesuprastinamų trupmenų aibe $\left\{ \frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N} \right\}$,

tai tarus, kad egzistuoja jo tiesioginis polaukis $(\mathcal{Q}', +, \cdot)$, $\mathcal{Q}' \subset \mathcal{Q}$, turėtume:

$$1. \quad \mathcal{Q}' \supset \mathbb{Z} \rightarrow (m, n \in \mathbb{Z}) m, n \in \mathcal{Q}'.$$

$$2. \quad \text{Bet } (\mathcal{Q}', +, \cdot) \text{ yra laukas, todėl ir } \frac{m}{n} \in \mathcal{Q}'.$$

$$3. \quad \text{Kadangi } \left(\forall \frac{m}{n} \in \mathcal{Q} \right) \frac{m}{n} \in \mathcal{Q}', \text{ tai } \mathcal{Q} \subset \mathcal{Q}'. \text{ Tai prieštarauja tam, kad } (\mathcal{Q}', +, \cdot) \text{ yra}$$

tiesioginis $\mathcal{Q}$ polaukis. QED.

Ap. Sutvarkyta aibė A vadinama *tiršta*, jei

$$(\forall a, b \in A): a < b \rightarrow (\exists c) a < c < b.$$

Teorema. Racionaliųjų skaičių lauko $(\mathcal{Q}, +, \cdot)$ bazinė aibė $\mathcal{Q}$ yra tiršta.

Įrodymas išplaukia iš to, kad

$$a < \frac{a+b}{2} < b \quad \text{ir} \quad \frac{a+b}{2} \in \mathcal{Q}.$$

Realiųjų skaičių aibė R . Kad nepakanka ir aibės Q rodo paprasta algebrinė lygtis $x^2 = 2$. Nesunku įsitikinti, kad ši lygtis *racionaliųjų* sprendinių neturi. Ką daryti? Aišku, ką: plėsti aibę Q iki tokios aibės $R \supset Q$, kuri turėtų visas mums įprastas “geras” (tiksliau: *lauko*) savybes ir kurioje panašios lygtys jau būtų išsprendžiamos. Vėlgi (žinoma, ne taip paprastai kaip norėtusi...) pasirodo, kad tokią aibę R sukonstruoti *galima* ir dargi ne vieninteliu būdu. Pabrėžtina, kad išeities pozicija yra tokia: *apie racionaliuosius skaičius viskas yra žinoma ir griežtai pagrįsta*.

Čia paminėsime vieną iš realiųjų skaičių lauko konstravimo būdų, kuris grindžiamas taip vadinamąja *Dedekindio pjūvio* (DP) sąvoka (Richard Dedekind, 1831 - 1916, garsus vokiečių matematikas). DP galima apibrėžti bet kokiame sutvarkytame lauke L . Mes DP apibrėžimą suformuluosime atveju, kai $L = Q$. Kaip matėme, lauke Q galima apibrėžti tiesinės tvarkos sąryšį “ $<$ ”, kurio pagalba laukas Q yra sutvarkytas.

Ap. Racionaliųjų skaičių aibės Q suskaidymą į du tokius poaibius A ir V , kad galiotų trys sąlygos:

- 1) $A \cup V = Q$;
- 2) $A \cap V = \emptyset$;
- 3) $(\forall a \in A)(\forall v \in V) a < v$,

vadiname DP lauke Q ir žymima $A|V$.

Svarbu suprasti, ko trūksta aibei Q ir, konstruojant naują aibę R , į tai atsižvelgti. Paaiškėja, kad lauke Q yra dviejų tipų DP: *su režiu*, – kai aibė A turi didžiausią elementą (arba aibė V turi mažiausią elementą), ir *be režio* – kai A neturi didžiausio, o V – mažiausio.

1 pvz., kai $A = \{r \mid r \in Q, r < 2\}$, o $V = \{r \mid r \in Q, r \geq 2\}$, tai $A|V$ pjūvis *su režiu*: būtent, viršutinėje klasėje V yra mažiausias elementas 2.

2 pvz., kai $A = \{r \mid r \in Q, r \leq 2\}$, o $V = \{r \mid r \in Q, r > 2\}$, tai $A|V$ pjūvis *su režiu*: būtent, apatinėje klasėje A yra didžiausias elementas 2.

3 pvz., kai $A = \{r \mid r \in Q, r^2 < 2 \vee r < 0\}$, o $V = \{r \mid r \in Q, r^2 > 2 \wedge r > 0\}$, $A|V$ pjūvis *be režio*. Tare, kad a yra teigiamas A elementas, įsitikinkime, kad jis didžiausiu elementu klasėje A būti negali. Tikrai: galima parinkti tiek didelį n , kad galiotų:

$$\left(a + \frac{1}{n}\right)^2 < 2,$$

nes ši nelygybė ekvivalenti tokiai

$$a^2 + \frac{2}{n} + \frac{1}{n^2} < 2,$$

arba kitaip

$$\frac{2a}{n} + \frac{1}{n^2} < 2 - a^2.$$

Pastaroji nelygybė tuo labiau bus teisinga, jei dydį $\frac{1}{n^2}$ pakeisime didesniu $\frac{1}{n}$, t.y. pareikalausime, kad galiotų:

$$\frac{2a+1}{n} < 2 - a^2.$$

Tam užtenks parinkti n tokį, kad:

$$n > \frac{2a+1}{2-a^2},$$

o tai visada galima (pagal Archimedo aksiomą). Panašiai įrodytume, kad klasėje V negali būti mažiausio elemento.

Ap. Sutvarkytas laukas L vadinamas tolydžiuoju, jei jame kiekvienas DP turi rėžį.

Tad, DP terminais, laukas Q nėra tolydus, t.y. jame egzistuoja DP be rėžio. Pasirodo, - tai ir yra tas pagrindinis aibės Q trūkumas.

Detalus visų reikalingų (įvedant papildomus, *irracionaliuosius skaičius*) faktų pagrindimas yra gana plati ir abstrakti tema. Skirti tam pakankamai laiko mes, deja, negalime. Pasakysime tik, kad, einant šiuo keliu, DP su rėžiu (1,2 Pvz.) sutapatinami su jau žinomais racionaliaisiais skaičiais, o kai rėžio nėra (3 Pvz.), tai sakome, kad atitinkamas DP apibrėžia naują, *irracionalųjį* skaičių. Naujai gauta (racionaliųjų ir irracionaliųjų) skaičių aibė vadinama **realiųjų skaičių** aibe. Pasinaudojant DP sąvoka, apibrėžiama realiųjų skaičių lygybė, tiesinės tvarkos sąryšis “mažiau”, aritmetiniai veiksmi.

Tad nuo šiol įsidėmėkime, kad:

- *realiųjų skaičių laukas R* yra AS $(R, +, \cdot)$, su bazine aibe R , kurioje tinkamai apibrėžtos *sudėties* ir *daugybės* operacijos, tenkinančios *lauko* aksiomas. Bazinė aibė R yra minimalus struktūros $(Q, +, \cdot)$ bazinės aibės Q viršaišis. Be to, laukas $(R, +, \cdot)$ *tolydinis* (t.y., lauke R visi DP turi rėžį).

- laukas $R = (R, +, \cdot)$, kaip ir laukas $Q = (Q, +, \cdot)$, yra *išsidėstęs*; bazinė aibė R yra *tiršta*.

- nuolat formuluojamą *minimalumo* reikalavimą kiek išsamiau aptarsime paskaitoje 1 - 08.

Paskaita 1 – 08

Kompleksinių skaičių laukas

Primename: Lauko $\mathbf{Q}$ plėtinio $\mathbf{R}$ konstravimas, panaudojant DP sąvoką. DP pagalba pavyksta tiksliau apibūdinti tuos bruožus, kuriuos turėtų turėti laukas $(R, +, \cdot)$, o laukas $(Q, +, \cdot)$ dar neturi. Tai – *lauko tolydumas*. Tad pagrindinis lauko $(Q, +, \cdot)$ trūkumas yra tas, jog jis yra *netolydinis*. DP terminais: jame egzistuoja DP be rėžio. Buvome sukonstravę tokio DP pavyzdį:

$$A = \{r \in Q \mid r \leq 0 \vee r^2 < 2\}, \quad V = \{r \in Q \mid r > 0 \wedge r^2 > 2\}.$$

Bazine aibę pasirinkus visų DP racionalųjų skaičių lauke aibę $R_0 := \{A \mid V\}$, bei tinkamai apibrėžus *sudėtį* ir *daugybą*, aibė R_0 tampa *tolydiniu lauku*. Kadangi ji nėra aibės $\mathbf{Q}$ viršaišis, tai, kaip įprasta, padeda *izomorfizmo principas*.

Ar *realiųjų skaičių lauke* $\mathbf{R}$ jau yra pakankamai skaičių? Pabandžius išspręsti paprastą algebrinę lygtį $x^2 + 1 = 0$, konstatuojame – ne, nepakankamai. Realųjų skaičių lauko bazinė aibė $\mathbf{R}$ irgi yra *per siaura*, - ją reiktų praplėsti. Toliau elgiamės standartiškai: aptariame, *kokios skaičių aibės norėtume*, o tada stengiamės būtent tokią aibę *sukonstruoti*.

Reziumuokime, pirmiausia, ko norėtume. Norėtusi, pagaliau, turėti tokią skaičių aibę $K \supset \mathbf{R}$, kurioje skaičių būtų *pakankamai*, t.y. joje būtų galima atlikti ir keturis aritmetinius veiksmus, ir šaknies traukimo operaciją, ir išspręsti lygtį $x^2 + 1 = 0$ bei visas kitas algebrines lygtis. Be to, žinoma, reiktų, kad ir naujųjų skaičių sudėtis bei daugyba būtų *komutatyvios, asociatyvios* ir *tarpusavyje distributyvios*.

Tiksliau sakant, ieškome $AS (K, +, \cdot)$, tenkinančios reikalavimus:

- $K \supset \mathbf{R}$,
- $AS (K, +, \cdot)$ yra laukas, (***)
- aibėje K išsprendžiamos visos *algebrinės lygtys* (atskiru atveju, $x^2 + 1 = 0$),
- aibė K yra *minimalus* lauko $\mathbf{R}$ plėtinys, tenkinantis išvardintus reikalavimus.

Kyla klausimas, ar tokią AS galima sukonstruoti? Pasirodo, - tai p.

Bazinės aibės konstravimas

Pradžiai pastebėsime, kad, geometriškai vaizduojant realiuosius skaičius skaičių tiesėje, “nepanaudotų” taškų jau nelieta, nes laukas $\mathbf{R}$ yra tolydus, t.y. kiekvienas DP šiame lauke turi rėžį. Todėl intuityviai darosi aišku, jog nauji skaičiai tiesėje tiesiog *nebetelpa*, - t.y. jų ieškant tenka “išeiti” į plokštumą. O plokštumoje tašką atitinka jau skaičių *pora*, - to taško Dekarto koordinatės. Štai todėl naujos skaičių aibės paieškas pradedame sukonstruodami visų realiųjų skaičių *porų* aibę K' .

$$K' := \{(a, b) \mid a \in R \wedge b \in R\} = R \times R = R^2.$$

Šiai aibei priklauso, pavyzdžiui, poros $(1, 0)$, $(0, 1)$, $(0, 0)$, $(-3, \sqrt{2})$ ir t.t.

Tačiau aibė K' kol kas netenkina nė vieno iš mūsų aptartų reikalavimų (***) : ji nėra aibės R viršaišis, joje kol kas nemokame nei sudėti (atimti), nei sudauginti (padalinti), nei, tuo labiau, - traukti šaknį. Todėl ir lygties $x^2 + 1 = 0$ išspręsti kol kas nemokame.

Pradėkime mokytis. Kaip ir kiekvienoje matematinėje teorijoje, pirmiausia, - keletas svarbių apibrėžimų, nusakančių aibės K' elementų lygybės sąryšį, sudėties ir daugybos algebrines operacijas.

Tarkime, turime du *bet kokius* aibės K' elementus, t.y. poras (a, b) , (c, d) .

Tada postuluojuame:

$$Ap. \quad (a, b) = (c, d) \equiv (a = c) \wedge (b = d).$$

$$Ap. \quad (a, b) + (c, d) = (a + c, b + d).$$

$$Ap. \quad (a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

Keliais pavyzdžiais pailiustruosime šiuos apibrėžimus. Pagal juos išplaukia, kad:

$$(1, 12) \neq (12, 1); \quad (-2, 4) = (-2, 4); \quad (1, -3) + (-5, 7) = (-4, 4);$$

$$(3, 5) \cdot (2, -1) = (3 \cdot 2 - 5 \cdot (-1), 3 \cdot (-1) + 5 \cdot 2) = (11, 7).$$

Pastebime, kad, atlikdami veiksmus, neišeiname iš aibės K' . Taigi, - apibrėžtosios binarės operacijos yra *algebrinės*. Be to, gana lengvai įrodoma, kad abu apibrėžtieji veiksmai turi įprastas *komutatyvumo* ir *asociatyvumo* savybes, o apibrėžtoji daugyba yra ir *distributyvi* tokios sudėties atžvilgiu.

Pvz., pagal apibrėžimą, $(a, b) + (c, d) = (a + c, b + d)$, $(c, d) + (a, b) = (c + a, d + b)$. Bet lauke R sudėtis yra komutatyvi, todėl: $a + c = c + a$, $b + d = d + b$, o tai pagal porų lygybės apibrėžimą ir reiškia, kad $(a, b) + (c, d) = (c, d) + (a, b)$, t.y., kad šitaip apibrėžta sudėtis yra komutatyvi. (Kitas KAD savybes pabandykite įrodyti patys.)

Pastaba. Atidesnis klausytojas jau pastebėjo, kad mes sau leidžiame tam tikrą kalbos laisvę: pvz., neretai lauku (grupe, žiedu) vadiname lauko (grupės, žiedo) bazinę aibę. Tikslas: lakoniškesnė kalba. Štai ir dabar, apibrėždami sudėtį ir daugybą aibėje K' rašome: $(a, b) + (c, d) = (a + c, b + d)$. Bet toks užrašas, griežtai kalbant, yra ne visai korektiškas, nes ženklas “+” jame panaudotas dviem visai skirtingom prasmėm... Apibrėžiant porų sudėtį, reiktų rašyti, pvz., taip:

$$(a, b) \oplus (c, d) = (a + c, b + d).$$

Taip nedarome tik vengdami ženklų, pažymėjimų gausos.

Teorema. $AS(K', +, \cdot)$ yra laukas.

Įr. Lieka aptarti *atimties* ir *dalybos iš nenulinio elemento* veiksmus. Jie nusakomi kaip atitinkamai *atvirkštiniai* sudėčiai ir daugybai.

Pvz., atimties įvykdomumas yra ekvivalentus lygties $(c, d) + (x, y) = (a, b)$, išsprendžiamumui aibėje K' . Pasinaudoję porų lygybės ir sudėties apibrėžimais, gauname: $(c + x, d + y) = (a, b)$, todėl $c + x = a$, $d + y = b$. Tada (realiųjų skaičių atimtis jau žinoma!) išaiškėja, kad porų atimtis atliekama taip:

$$(x, y) := (a, b) - (c, d) = (a - c, b - d) \in K'.$$

Pora $(a - c, b - d) \in K'$ vadinama elementų (a, b) ir (c, d) skirtumu.

Atskiru atveju, aibės K' nulinis elementas yra pora $(0, 0)$.

Panašiai samprotaujant, parodoma, kad *dalyba* iš nenulinio elemento atliekama taip:

$$(a, b) : (c, d) = (x, y). \text{ Čia } x = \frac{ac + bd}{c^2 + d^2}, y = \frac{bc - ad}{c^2 + d^2}, \text{ o } (c, d) \neq (0, 0).$$

Be to, pora $(1, 0)$ yra aibės K' vienetinis elementas, t.y. $(a, b) \cdot (1, 0) = (a, b)$. QED.

Galima buvo elgtis ir kitaip (žiūrint, kaip jau Jums aiškiau): pvz., įrodant atimties įvykdomumą (egzistavimą), - parodyti, kad :

- aibėje K' egzistuoja neutralusis sudėties atžvilgiu (nulinis) elementas;
- kiekvienas K' elementas (a, b) turi aibėje K' sau simetrišką (priešingą).

Patikrinti, kad pora $(0, 0)$ yra aibės K' neutralusis elementas, o pora $(-a, -b)$ yra bet kokiai porai $(a, b) \in K'$ priešingas elementas, - tikrai nesunku. Tereikia prisiminti nulio ir priešingojo elementų apibrėžimus.

Dabar, jei lygtį $x^2 + 1 = 0$ perrašysime mūsų situacijai, tai ji atrodys taip:

$$(x, y)^2 + (1, 0) = (0, 0).$$

Pora $(0, 1)$ tenkina šią lygtį, nes $(0, 1)^2 = (-1, 0)$. Ši ypatinga pora žymima raide i . T.y. $i := (0, 1)$. Ji vadinama *menamu vienetu*.

Tad aibė K' jau įgavo nemažai mums reikalingų savybių: struktūra $(K', +, \cdot)$ yra laukas, jame išsprendžiamas lygties $x^2 + 1 = 0$ atitikmuo. Tačiau K' vis dar nėra aibės R (todėl ir aibių Q, Z, N) viršaišis kaip mes norėjome. Iš tikrųjų, aibėje K' nėra realiųjų skaičių: ją sudaro *realiųjų skaičių poros*. Šį nesklandumą lengvai įveikiame eilinį kartą panaudodami *izomorfizmo principą* ir pakeisdami visas poras $(a, 0)$ atitinkamai realiaisiais skaičiais a . Pažymėkime: $K_0 = \{(a, 0) | a \in R\}$.

Teorema. *Algebrinės struktūros $(R, +, \cdot)$ ir $(K_0, +, \cdot)$ yra izomorfiškos.*

Įr. Reikiama bijekcija yra apibrėžiama šitaip: $(\forall a \in R) \varphi : a \leftrightarrow (a, 0)$, arba kitaip: $\varphi(a) = (a, 0)$. Įrodymo detalės – savarankiškai.

Planas: patikriname, ar tikrai *sumos* (sandaugos) *vaizdas lygus vaizdų sumai* (sandaugai).

Išvada. $AS (K_0, +, \cdot)$ yra lauko $(K', +, \cdot)$ polaukis.

Dabar atliekame veiksmą su aibėmis:

$$(K' \setminus K_0) \cup R.$$

Naujai gautą aibę pažymėkime raide K . Apibrėžkime joje sudėtį ir daugybą taip pat, kaip ir aibėje K' , tačiau prisimindami, kad $a \leftrightarrow (a, 0)$. Pvz.,

$$a + (c, d) := (a, 0) + (c, d) = (a + c, d); \quad a \cdot (c, d) := (a, 0) \cdot (c, d) = (ac, ad).$$

Veiksmai tarp realiųjų skaičių: $a + b$, $a \cdot b$ ir veiksmai tarp porų: $(a, b) + (c, d)$, $(a, b) \cdot (c, d)$ apibrėžiami taip, kaip tai jau padaryta anksčiau aptariant laukus R ir $(K', +, \cdot)$.

Teorema. $AS K := (K, +, \cdot)$ yra laukas.

Įr. Patiems. Planas:

- iš naujo patikriname *sudėties* ir *daugybės* veiksmų aibėje K algebriskumą, komutatyvumą, asociatyvumą ir tarpusavio distributyvumą,
- įsitikiname, kad aibėje K įvykdoma atimtis ir dalyba iš nenulinio elemento.

Galimas ir kitas įrodymo kelias: parodyti, kad struktūros $(K', +, \cdot)$ ir $(K, +, \cdot)$ yra izomorfiškos. Tada teoremos įrodymas išplauks iš to, kad $(K', +, \cdot)$ jau yra laukas. Savarankiškai apmąstykite pasiūlytą įrodymo būdą.

Lauko K minimalumas. Dabar aibė K tenkina beveik visus jai iškeltus reikalavimus. Lieka tik aptarti gauto plėtinio K minimalumo reikalavimą.

Ap. Sakome, $AS (A, \Omega)$ yra minimalus $AS (A_1, \Omega)$ plėtinys tam tikrų savybių atžvilgiu, jei nėra tokios $AS (B, \Omega)$, kad būtų $A_1 \subset B \subset A$, $B \neq A$, kuri turėtų tas pačias savybes operacijų sąrašo Ω atžvilgiu.

Mūsų atveju, minimalumas komentuojamas taip: nėra tokio tikrinio bazinės aibės K poaibio $K_1 \supset R$, kad $AS (K_1, +, \cdot)$ būtų laukas, o lygtis $x^2 + 1 = 0$ aibėje K_1 irgi būtų išsprendžiama.

Teorema. $AS (K, +, \cdot)$ yra minimalus lauko $(R, +, \cdot)$ plėtinys.

Įrodymo schema: tarę, kad yra tokia $AS (K^*, +, \cdot)$, kuri tenkina apibrėžime (***) postuluojamus reikalavimus ir $K^* \subset K$, parodome, kad $K^* = K$.

$AS K = (K, +, \cdot)$ vadiname *kompleksinių skaičių lauku*, jos bazinę aibę K – *kompleksinių skaičių aibe*, o jos elementus – *kompleksiniais skaičiais* (KS).

Algebrinė ir trigonometrinė kompleksinio skaičiaus formos. Naudodami aptartus žymenis ir veiksmų apibrėžimus, kiekvieną kompleksinį skaičių (t.y. realiųjų skaičių porą) $z = (a, b)$ iš aibės K galima užrašyti taip:

$$z = (a, b) = (a, 0) + (0, b) = (a, 0) + (0, b)(0, 1) = a + bi.$$

Sakome, kad KS z užrašytas *algebrine forma*. Pvz. $z = (-3, 4) = -3 + 4i$.

Terminai: realusis skaičius a vadinamas KS $z = a + bi$ *realiąja dalimi*; realusis skaičius b vadinamas KS $z = a + bi$ *menamąja dalimi*; žymima $a = \operatorname{Re} z$; $b = \operatorname{Im} z$. Jei $a = 0$, tai KS vadinamas *grynai menamu*.

KS geometrinė interpretacija: KS $z = (a, b) = a + bi$ geometriškai vaizduojamas vektoriumi, jungiančiu taškus $(0, 0)$, (a, b) . Tada KS sudėtį ir atimtį galima iliustruoti *lygiagrečiojo taisyklės* pagalba.

KS dauginant, dalinant, o ypač, - traukiant šaknį, patogiau naudoti KS *trigonometrinę formą* (TF)

$$z = a + bi = r(\cos \varphi + i \sin \varphi).$$

Ap. Neneigiamą realųjį skaičių $r := \sqrt{a^2 + b^2}$ vadiname KS $z = a + bi$ **moduliu**.

Kartais žymima: $\sqrt{a^2 + b^2} = |z|$. Aišku, kad $r = 0 \equiv z = 0$.

Jei KS z nelygus nuliui, tai galime parašyti:

$$z = r \left(\frac{a}{r} + \frac{b}{r} i \right).$$

Kadangi, $\left| \frac{a}{r} \right| \leq 1$ ir $\left| \frac{b}{r} \right| \leq 1$, be to $\frac{a^2}{r^2} + \frac{b^2}{r^2} = 1$, tai iš trigonometrijos žinių išplaukia, jog yra kampas φ toks, kad:

$$\cos \varphi = \frac{a}{r} \quad \text{ir} \quad \sin \varphi = \frac{b}{r}. \quad (*)$$

Šis kampas vadinamas kompleksinio skaičiaus z **argumentu** ir žymimas: $\varphi = \operatorname{Arg} z$. Iš sinuso ir kosinuso periodiško išplaukia, kad KS *argumentas nustatomas nevienareikšmiškai*. Iš tikrųjų, jei φ yra koks nors sistemos (*) sprendinys, tai, su visais sveikaisiais k , skaičiai $\varphi + 2k\pi$ irgi tenkina (*). Ir atvirkščiai, jei:

$$\cos \varphi_1 = \frac{a}{r}, \sin \varphi_1 = \frac{b}{r} \quad \text{ir} \quad \cos \varphi_2 = \frac{a}{r}, \sin \varphi_2 = \frac{b}{r},$$

tai iš čia gauname:

$$\cos \varphi_1 \cos \varphi_2 = \frac{a^2}{r^2} \quad \text{bei} \quad \sin \varphi_1 \sin \varphi_2 = \frac{b^2}{r^2},$$

$$\cos \varphi_1 \cos \varphi_2 + \sin \varphi_1 \sin \varphi_2 = \frac{a^2 + b^2}{r^2} = 1 \rightarrow \varphi_1 - \varphi_2 = 2\pi k, \quad k \in \mathbb{Z},$$

t.y., du to paties kompleksinio skaičiaus argumentai gali skirtis tik skaičiumi $2k\pi$, $k \in \mathbb{Z}$.

Argumento reikšmė φ_0 , kuri tenkina sąlygą $0 \leq \varphi_0 < 2\pi$ (kartais, $-\pi < \varphi_0 \leq \pi$), vadinama *pagrindine argumento reikšme*. Susitarta, KS užrašant trigonometriniu forma, iš daugelio galimų imti būtent *pagrindinę* argumento reikšmę. Ją žymėsime: $\varphi_0 = \arg z$.

Pavyzdžiui,

$$z = 1 + i = \sqrt{2} \left(\cos \frac{\pi}{4} + i \sin \frac{\pi}{4} \right), \text{ nes } r = \sqrt{1^2 + 1^2} = \sqrt{2}, \text{ o iš lygybių } \cos \varphi = \frac{1}{\sqrt{2}},$$

$$\sin \varphi = \frac{1}{\sqrt{2}}, \text{ nesunku suvokti, kad } \varphi = \arg z = \pi/4 + 2k\pi, \quad k \in \mathbb{Z}. \text{ Todėl: } \arg z = \pi/4.$$

Geometriškai KS modulis reiškia vektoriaus, vaizduojančio tą KS, ilgį, o argumentas yra kampas, kurį tas vektorius sudaro su teigiama x – są ašies kryptimi (prieš laikrodžio rodyklę).

Bendru atveju, formalus KS užrašas trigonometriniu forma gali būti gaunamas įvairiais būdais. Galima elgtis, pavyzdžiui, taip (kai $a \neq 0$):

- pagal realiųjų skaičių $a := \operatorname{Re} z$ ir $b := \operatorname{Im} z$ ženklus nustatome, kuriame ketvirtyje yra kompleksinį skaičių $z = a + bi$ vaizduojantis vektorius;

$$\text{- kadangi } \operatorname{tg} \varphi = \frac{b}{a}, \text{ o } -\frac{\pi}{2} < \operatorname{arctg} \varphi < \frac{\pi}{2}, \text{ tai:}$$

$$\text{kai } z \in \text{I ketv.}, \text{ tai } \varphi = \operatorname{arctg} \frac{b}{a};$$

$$\text{kai } z \in \text{II ketv. arba III ketv.}, \text{ tai } \varphi = \pi + \operatorname{arctg} \frac{b}{a};$$

$$\text{pagaliau, kai } z \in \text{IV ketv.}, \text{ tai } \varphi = 2\pi + \operatorname{arctg} \frac{b}{a}.$$

Pavyzdžiui, jei TF ieškosime skaičiui $z = -1,1 + \sqrt{3}i$, tai $z \in \text{II ketvirčiui}$, tad:

$$\arg z = \pi + \operatorname{arctg} \left(\frac{\sqrt{3}}{-1,1} \right) = \pi - \operatorname{arctg} \frac{\sqrt{3}}{1,1}; \quad r = \sqrt{1,21 + 3} = \sqrt{4,21}.$$

$$\text{Ats. } z = \sqrt{4,21} \left(\cos \left(\pi - \operatorname{arctg} \frac{\sqrt{3}}{1,1} \right) + i \sin \left(\pi - \operatorname{arctg} \frac{\sqrt{3}}{1,1} \right) \right).$$

Jei norėtume šitokią rezultatą pavaizduoti geometriškai, tai tektų surastą pagrindinę argumento reikšmę (PC ar skaičiuoklio pagalba) apskaičiuoti apytikriai.

KS argumentui užrašyti galima naudoti ir funkcijas $\arcsin x$ ar $\arccos x$. Pvz., kai $z = \sqrt{3} - i$, tai akivaizdu, kad vektorius, vaizduojantis KS, yra IV ketvirtyje. Tad reikia laukti, jog pagrindinė argumento

reikšmė $\varphi_0 = \arg z$ patenka į intervalą $\left(\frac{3\pi}{2}, 2\pi\right)$ t.y. $\varphi_0 \in (270^\circ, 360^\circ)$. Šiuo atveju $r = 2$, o

$$\sin \varphi = \frac{b}{r} = -\frac{1}{2} \rightarrow \varphi_0 = \arcsin\left(-\frac{1}{2}\right) = -\frac{\pi}{6}.$$

Atsakymas $z = \sqrt{3} - i = 2\left(\cos\left(-\frac{\pi}{6}\right) + i \sin\left(-\frac{\pi}{6}\right)\right)$ yra formaliai teisingas, tik neatsižvelgta į

susitarimą, kad $\varphi_0 \in [0, 2\pi)$. Todėl korektiškiau būtų rašyti :

$$z = 2\left(\cos\left(2\pi - \frac{\pi}{6}\right) + i \sin\left(2\pi - \frac{\pi}{6}\right)\right) = 2\left(\cos\frac{11\pi}{6} + i \sin\frac{11\pi}{6}\right).$$

Teorema. *Dauginant du KS, užrašytus TF, jų moduliai sudauginami, o argumentai sudedami. Kompleksinius skaičius dalijant, jų moduliai atitinkamai dalijami vienas iš kito, o argumentai atimami.*

Įrodymas išplaukia iš trigonometrinių formulių:

$$\sin(\alpha \pm \beta) = \sin \alpha \cos \beta \pm \sin \beta \cos \alpha; \quad \cos(\alpha \pm \beta) = \cos \alpha \cos \beta \mp \sin \alpha \sin \beta.$$

1 išvada. (Muavro formulė). $(\forall n \in \mathbb{N}) z^n = r^n (\cos n\varphi + i \sin n\varphi)$.

Įr. Naudosimės MIP ir įrodyta teorema.

1. Kai $n = 1$ formulė teisinga.
2. Tarkime ji yra teisinga su vienu fiksuotu n .
3. Naudodamiesi prielaida, įrodysime, kad ji teisinga ir skaičiui $n + 1$. Turime:

$$\begin{aligned} z^{n+1} &= z^n \cdot z \stackrel{\text{pagal prielaidą}}{=} r^n (\cos n\varphi + i \sin n\varphi) \cdot r (\cos \varphi + i \sin \varphi) = \\ &\stackrel{\text{pagal teoremą}}{=} r^{n+1} (\cos(n\varphi + \varphi) + i \sin(n\varphi + \varphi)) = r^{n+1} (\cos(n+1)\varphi + i \sin(n+1)\varphi). \text{ QED.} \end{aligned}$$

2 išvada. (KS rodiklinė forma). Jei r – KS $z = a + bi$ modulis, o φ – jo argumentas, tai galima užrašyti: $z = re^{i\varphi}$.

Įr. Jei laikysime, kad i yra tiesiog konstanta, tai tada galima kalbėti apie funkcijos $f(\varphi) := e^{-i\varphi} (\cos \varphi + i \sin \varphi)$ išvestinę. Tiesa, šios funkcijos reikšmės yra kompleksiniai skaičiai. Kompleksinių skaičių lauke ribos ir funkcijos išvestinės sąvokas bei įprastas diferencijavimo taisyklės reiktų aptarti iš naujo. Čia mes tik pastebėsime, kad šitai galima

padaryti. Tada, nesunku įsitikinti, kad $(\forall \varphi \in \mathbb{R}) f(\varphi)'_{\varphi} = 0$. Taigi, $f(\varphi) = \text{const} = c$. Bet,

$$f(0) = 1 \rightarrow c = 1. \text{ Todėl: } (\forall \varphi \in \mathbb{R}) e^{-i\varphi} (\cos \varphi + i \sin \varphi) = 1 \rightarrow$$

$$\rightarrow e^{i\varphi} = \cos \varphi + i \sin \varphi \rightarrow z = r(\cos \varphi + i \sin \varphi) = re^{i\varphi}.$$

Pvz., *algebrinės* formos kompleksinį skaičių $z = -1 + \sqrt{3}i$ galime užrašyti *trigonometrinėje* :

$$z = \sqrt{1+3}(\cos(\pi - \arctg \sqrt{3}) + i \sin(\pi - \arctg \sqrt{3})) = 2\left(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}\right),$$

arba *rodiklinėje*: $z = 2e^{\frac{2\pi}{3}i}$ formoje.

Paskaita 1 – 09

Kompleksinių skaičių laukas (tęsinys)

Primename: KS modulis ir argumentas, trigonometrinė ir rodiklinė formos.

Teorema. *Dauginant du KS, užrašytus TF, jų moduliai sudauginami, o argumentai sudedami. Kompleksinius skaičius dalijant, moduliai atitinkamai dalijami vienas iš kito, o argumentai atimami.*

Muavro formulė. $(\forall n \in \mathbb{Z}) (\forall z \in K, z \neq 0) z^n = r^n (\cos n\varphi + i \sin n\varphi)$.

Pateiktas formulės variantas skiriasi nuo to, kurį įrodėme paskaitoje 1 – 08. Čia $n \in \mathbb{Z}$, todėl reiktų dar įsitikinti formulės teisingumu, kai $n \leq 0$.

Apibrėžus, kad $(\forall z \in K, z \neq 0) z^0 = 1$, o $(\forall z \in K, m \in \mathbb{N}, z \neq 0) z^{-m} = \frac{1}{z^m}$, Muavro formulė išplaukia iš lygybių: $(\forall \varphi \in \mathbb{R}) \cos(0 \cdot \varphi) + i \sin(0 \cdot \varphi) = 1 = z^0$,

$$\frac{1}{z^m} = \frac{\cos 0 + i \sin 0}{\cos(m\varphi) + i \sin(m\varphi)} = \cos(-m\varphi) + i \sin(-m\varphi) = \cos((-m)\varphi) + i \sin((-m)\varphi).$$

Pavyzdžiui, jei $z = 1 - i$ ir $w = 1 + \sqrt{3}i$, tai, užrašius z ir w trigonometrine forma, turėsime:

$$z = \sqrt{2} \left(\cos \frac{7\pi}{4} + i \sin \frac{7\pi}{4} \right), \quad w = 2 \left(\cos \frac{\pi}{3} + i \sin \frac{\pi}{3} \right). \text{ Todėl:}$$

$$z \cdot w = 2\sqrt{2} \left(\cos \left(\frac{7\pi}{4} + \frac{\pi}{3} \right) + i \sin \left(\frac{7\pi}{4} + \frac{\pi}{3} \right) \right) = 2\sqrt{2} \left(\cos \left(\frac{\pi}{12} \right) + i \sin \left(\frac{\pi}{12} \right) \right),$$

$$z : w = \frac{\sqrt{2}}{2} \left(\cos \left(\frac{7\pi}{4} - \frac{\pi}{3} \right) + i \sin \left(\frac{7\pi}{4} - \frac{\pi}{3} \right) \right) = \frac{\sqrt{2}}{2} \left(\cos \left(\frac{17\pi}{12} \right) + i \sin \left(\frac{17\pi}{12} \right) \right).$$

Šaknies traukimas. Su trigonometrinėje formoje užrašytais KS galima atlikti dar vieną realiųjų skaičių lauke įprastą veiksmą, - šaknies traukimą.

Ap. Jei $z \in K$, tai skaičius $w \in K$ vadinamas n -tojo laipsnio ($n \in \mathbb{N}$) šaknimi iš skaičiaus z , jei $w^n = z$. Rašome $w = \sqrt[n]{z}$.

Pavyzdžiui, $\sqrt[3]{-2-2i} = 1-i$, nes $(1-i)^3 = -2-2i$.

Teorema. *Jei $z = a + bi = r(\cos \varphi + i \sin \varphi)$, o $n \in \mathbb{N}$, tai visos n -tojo laipsnio šaknys iš z gaunamos iš tokios formulės:*

$$z_k := \sqrt[n]{z} = \sqrt[n]{r} \left(\cos \frac{\varphi + 2k\pi}{n} + i \sin \frac{\varphi + 2k\pi}{n} \right), \quad k = 0, 1, 2, \dots, n-1.$$

Įrodymas išplaukia iš Muavro formulės ir KS, užrašytų TF, lygybės.

Tad n -tojo laipsnio šaknų iš duotojo KS z yra lygiai n . Žinoma, kai kurios iš jų gali būti lygios tarpusavyje. Suvokus, kad visų n šaknų iš KS moduliai vienodi, darome išvadą, kad

visos n -tojo laipsnio šaknys iš KS z išsidėsčiusios ant apskritimo, kurio spindulys yra $\sqrt[n]{r}$. Iš čia, be to, išplaukia, kad realiųjų šaknų yra daugiausiai dvi (jas atitinka minėto apskritimo susikirtimo su realiaja ašimi taškai, t.y. realieji skaičiai $\pm \sqrt{r}$).

Nereikia pamiršti, kad $R \subset K$, todėl *realieji skaičiai yra tuo pat metu ir kompleksiniai*, bet ne atvirkščiai! Pvz. $-5 = (-5, 0) = -5 + 0 \cdot i \in K$, bet: $3 - 2i \notin R$. Ir dar: sąryšio “mažiau” lauke K neįvedėme, todėl įprasti ženklai “<” ir “>” tarp KS netaikomi.

Kvadratinės lygtys. Baigdami pokalbį apie kompleksinius skaičius pastebėsime, kad dabar jau *mokame* išspręsti ir kvadratinę lygtį $x^2 - 2x + 2 = 0$, nors jos diskriminantas ir neigiamas. Nesunku (pabandykite!) patikrinti, kad kompleksiniai skaičiai $x_1 = 1 - i$, $x_2 = 1 + i$ tenkina šią lygtį.

Beje, sprendimui tinka “mokyklinė” formulė! Taip yra todėl, kad traukiant kvadratinę šaknį iš KS $z = r(\cos \varphi + i \sin \varphi)$, gauname du tik ženklais besiskiriančius atsakymus:

$$z_k = \sqrt{z} = \sqrt{r} \left(\cos \frac{\varphi + 2k\pi}{2} + i \sin \frac{\varphi + 2k\pi}{2} \right), \quad k = 0, 1; \quad z_1 = -z_0.$$

Tad, pertvarkę kvadratinę lygtį ($a \neq 0$) $ax^2 + bx + c = 0$ taip:

$$a \left(x^2 + 2 \frac{b}{2a} x + \frac{b^2}{4a^2} \right) = -c + \frac{b^2}{4a},$$

arba taip:

$$\left(x + \frac{b}{2a} \right)^2 = \frac{b^2 - 4ac}{4a^2},$$

gauname, kad:

$$x + \frac{b}{2a} = \sqrt{\frac{b^2 - 4ac}{4a^2}} = \pm \frac{\sqrt{D}}{2a},$$

o tai - ta pati, mums žinoma formulė.

Be to, kvadratinę šaknį iš KS $z = a + bi$ galima rasti ir nesinaudojant skaičiaus z trigonometrine forma. Primenu, kad abi kvadratinės šaknys iš z skiriasi viena nuo kitos tik ženklu.

Jei $w = u + vi$ yra kvadratinė šaknis iš $z = a + bi$, tai:

$$u = \pm \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}}, \quad v = \pm \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}} \quad \text{ir} \quad \operatorname{sgn}(uv) = \operatorname{sgn} b.$$

Pvz., apskaičiuokime $\sqrt{5-12i} =: z_{1,2}$. Kadangi

$$u = \pm \sqrt{\frac{\sqrt{5^2+12^2}+5}{2}} = \pm\sqrt{9} = \pm 3, \text{ o } \pm\sqrt{4} = \pm 2 \text{ ir } \operatorname{sgn}(uv) = \operatorname{sgn}(-12), \text{ tai}$$

$$z_{1,2} = \sqrt{5-12i} = \pm(3-2i).$$

Čia $\operatorname{sgn} x$ žymi skaičiaus x ženklą. Detaliau, žr. vadovėlio 127 psl.

Šaknies iš KS traukimo formulė įgalina išspręsti ir *bet kokią* n - tojo laipsnio ($n \in \mathbb{N}$) *dvinarę lygtį* pavidalo:

$$(a+bi)z^n = c+di.$$

Pavyzdžiui, išspręskime lygtį: $i \cdot z^5 = -1+i$.

Turime: $z^5 = (-1+i):i = 1+i = \sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)$. Todėl

$$z_k = \sqrt[5]{1+i} = \sqrt[10]{2}\left(\cos\left(\frac{\pi}{20} + \frac{2}{5}k\pi\right) + i\sin\left(\frac{\pi}{20} + \frac{2}{5}k\pi\right)\right), k = 0, 1, 2, 3, 4.$$

Pastebėsime, kad gautųjų penkių sprendinių argumentai sudaro aritmetinę progresiją su $a_1 = \frac{\pi}{20}$ ir $d = \frac{2\pi}{5}$, todėl, atsakymus $z_i, i = 0, 1, 2, 3, 4$ vaizduojančių vektorių galai išsidėstę taisyklingojo penkiakampio (bendru atveju, - taisyklingojo n -kampio) viršūnėse.

Kai kurios KS savybės

Ap. $\bar{z} := a - bi$ yra vadinamas skaičiui $z = a + bi$ **jungtiniu** (sujungtiniu) KS.

Nesunku įrodyti, kad:

$$\begin{aligned} |z| &= |\bar{z}|; \quad z + \bar{z} = 2a \in \mathbb{R} \quad \text{ir} \quad z \cdot \bar{z} = r^2 \in \mathbb{R}; \quad \arg \bar{z} = 2\pi - \arg z; \\ |z_1 \cdot z_2| &= |z_1| \cdot |z_2|; \quad |z_1 : z_2| = |z_1| : |z_2|; \quad |z_1| - |z_2| \leq |z_1 \pm z_2| \leq |z_1| + |z_2|. \end{aligned}$$

Pvz., įrodysime “trikampio” nelygybę: $|z_1 + z_2| \leq |z_1| + |z_2|$.

[r. Jei $z_1 = a + bi$, o $z_2 = c + di$, tai:

$$|z_1 + z_2| = \sqrt{(a+c)^2 + (b+d)^2}; \quad |z_1| + |z_2| = \sqrt{a^2 + b^2} + \sqrt{c^2 + d^2}.$$

Toliau galima samprotauti šitaip: ($\forall a, b, c, d \in \mathbb{R}$)

$$(ad - bc)^2 \geq 0 \equiv 2abcd \leq a^2d^2 + b^2c^2 \equiv a^2c^2 + b^2d^2 + 2abcd \leq a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$$

arba

$$(ac + bd)^2 \leq (a^2 + b^2)(c^2 + d^2) \rightarrow 2ac + 2bd \leq 2\sqrt{(a^2 + b^2)(c^2 + d^2)}.$$

Tad

$$\begin{aligned} a^2 + b^2 + d^2 + c^2 + 2ac + 2bd &\leq a^2 + b^2 + d^2 + c^2 + 2\sqrt{(a^2 + b^2)(c^2 + d^2)} \rightarrow \\ &\rightarrow (a+c)^2 + (b+d)^2 \leq \left(\sqrt{a^2 + b^2} + \sqrt{c^2 + d^2}\right)^2. \quad \text{QED.} \end{aligned}$$

Paskaita 1 – 10

Vieneto šaknų grupė

Primenime: Dvinarių ir kvadratinų lygčių su kompleksiniais koeficientais sprendimo metodika.

Kvadratinei lygčiai tinka ta pati “mokyklinė” formulė. Be to, kvadratinę šaknį iš KS $z = a + bi$ galima rasti ir nesinaudojant skaičiaus z trigonometrine forma.

Vieneto šaknys. Atskiru atveju, lygtis

$$z^n = 1$$

irgi turi n sprendinių. Kadangi $1 = 1 + 0i = \cos 0 + i \sin 0$, tai

$$\varepsilon_k := \sqrt[n]{1} = 1 \cdot \left(\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \right), k = 0, 1, 2, \dots, n-1. \quad (*)$$

KS ε_k vadinami n -ojo laipsnio *vieneto šaknimis*, o jų aibė $\{\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}\} := V_n$ pasižymi įdomiomis savybėmis, apie kurias ir pakalbėsime šiame skyrelyje.

Teorema. $AS (V_n, \cdot)$ yra multiplikacinė Abelio grupė.

Įr. Iš (*) formulės ir veiksmų su KS taisyklių gauname paeiliui: $\varepsilon_k \cdot \varepsilon_l =$

$$= \left(\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \right) \cdot \left(\cos \frac{2l\pi}{n} + i \sin \frac{2l\pi}{n} \right) = \left(\cos \frac{2(k+l)\pi}{n} + i \sin \frac{2(k+l)\pi}{n} \right) = \varepsilon_{k+l},$$

t.y. aibė V_n yra uždara daugybos atžvilgiu. (Kai $k+l \geq n$, tai $k+l \longrightarrow k+l-n$).

$\varepsilon_k \cdot \varepsilon_0 = \varepsilon_0 \cdot \varepsilon_k = \varepsilon_k$, t.y. ε_0 yra neutralus aibės V_n elementas.

$\varepsilon_k \cdot \varepsilon_{n-k} = \varepsilon_0 = 1$. Todėl $\varepsilon_{n-k} = \varepsilon_k^{-1}$, t.y. aibėje V_n kiekvienas elementas turi sau atvirkštinį.

Pagaliau, kadangi $V_n \subset K$, tai daugyba aibėje V_n yra ir asociatyvi, ir komutatyvi. Taigi, visos grupės aksiomos išpildytos, teorema įrodyta.

Pavyzdžiui, grupėje V_{13} daugybos ir dalybos veiksmas atliekami taip:

$$\varepsilon_3 \cdot \varepsilon_{10} = \varepsilon_{13} = \varepsilon_0 = 1, \text{ todėl } \varepsilon_3^{-1} = \varepsilon_{10},$$

$$\varepsilon_6 \cdot \varepsilon_{11} = \varepsilon_{17} = \varepsilon_{13+4} = \varepsilon_4,$$

$$\varepsilon_8 : \varepsilon_3 = \varepsilon_8 \cdot \varepsilon_3^{-1} = \varepsilon_8 \cdot \varepsilon_{10} = \varepsilon_5.$$

Primityviosios vieneto šaknys. Kai kurios n -tojo laipsnio vieneto šaknys, keliant jas laipsniais $0, 1, 2, \dots, n-1$, duoda kaskart skirtingą rezultatą, t.y. *generuoja visas kitas* to paties laipsnio šaknis. Kitos gi, – tokios savybės neturi.

Pvz., nesunku įsitikinti, kad $V_4 = \{1, i, -1, -i\}$. Čia $\varepsilon_2 = -1$ ir: $\varepsilon_2^0 = 1, \varepsilon_2^1 = -1, \varepsilon_2^2 = 1, \varepsilon_2^3 = -1$. Tad, pvz., $\varepsilon_2^0 = \varepsilon_2^2 = 1$. Tuo tarpu, ε_1 generuoja visas kitas ketvirtąjo laipsnio vieneto šaknis: $\varepsilon_1^0 = 1 = \varepsilon_0, \varepsilon_1^1 = i = \varepsilon_1, \varepsilon_1^2 = -1 = \varepsilon_2, \varepsilon_1^3 = -i = \varepsilon_3$.

Ap. n -ojo laipsnio vieneto šaknį ε_k vadinsime **primityviaja vieneto šaknimi** (PŠ), jei visi jos laipsniai $\varepsilon_k^l, l = 0, 1, 2, \dots, n-1$ yra skirtingi.

Tad $\varepsilon_1 \in V_4$ yra primitivioji šaknis, o $\varepsilon_2 \in V_4$ - nėra PŠ.

Kadangi $(\forall l) \varepsilon_k^l \in V_n$, tai gauname, jog $V_n = \{\varepsilon_k^0, \varepsilon_k^1, \dots, \varepsilon_k^{n-1}\}$. T.y. aibę V_n sudaro visi skirtingi primitivios vieneto šaknies laipsniai.

Sakome, kad grupę $(V_n, \cdot)$ generuoja jos elementas ε_k . Vieno elemento generuojamos grupės vaidina svarbų vaidmenį algebroje. Joms pavadinti yra įvestas specialus terminas.

Ap. Grupę G , kurią generuoja vienas jos elementų g vadinama **cikline grupe** ir žymima $G = \langle g \rangle$.

Pvz., lyginių sveikųjų skaičių adicinė grupė $(Z_2, +)$ yra ciklinė grupė, generuojama elemento $g = 2$, t.y. $(Z_2, +) = \langle 2 \rangle$.

Kaip nustatyti, ar konkreti n -ojo laipsnio vieneto šaknis yra PŠ? Atsakymą randame tokioje teoremoje.

Teorema. n -tojo laipsnio vieneto šaknis ε_k tada ir tik tada yra primitivus, kai $D(k, n) = 1$.

I. Duota: ε_k - PŠ. Reikia įrodyti, kad: $D(k, n) = 1$.

Tarkime priešingai, - nors ε_k yra PŠ, bet $D(k, n) = d > 1$. Tada $\varepsilon_k^0 = 1$ ir

$$\varepsilon_k^{\frac{n}{d}} = \left(\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \right)^{\frac{n}{d}} = \cos \frac{2k\pi \cdot n}{n \cdot d} + i \sin \frac{2k\pi \cdot n}{n \cdot d} = \cos \frac{2k\pi}{d} + i \sin \frac{2k\pi}{d} = 1,$$

nes $k : d \in Z$. Tad $\varepsilon_k^0 = \varepsilon_k^{\frac{n}{d}}$, o tai prieštarauja tam, kad ε_k yra PŠ.

II. Duota $D(k, n) = 1$. Įrodyti: ε_k - PŠ.

Vėlgi, tarkime priešingai: nors $D(k, n) = 1$, tačiau ε_k nėra PŠ, t.y. egzistuoja bent du lygūs tarpusavyje šaknies ε_k laipsniai: ε_k^m ir ε_k^s ($0 \leq m < s \leq n-1$). Tada

$$\varepsilon_k^m = \varepsilon_k^s \rightarrow \cos \frac{2km\pi}{n} + i \sin \frac{2km\pi}{n} = \cos \frac{2ks\pi}{n} + i \sin \frac{2ks\pi}{n} \rightarrow \frac{2km\pi}{n} = \frac{2ks\pi}{n} + 2l\pi, l \in Z.$$

Iš čia: $km = ks + nl \rightarrow k(m-s) = nl$, t.y. $n \mid m-s$. Prieštara, nes $|m-s| < n$. QED.

1 išvada. n – ojo laipsnio vieneto šaknų grupė $(V_n, \cdot)$ yra ciklinė grupė.

Tikrai, juk $D(1, n) = 1$, todėl ε_1 visada yra PŠ ir $(V_n, \cdot) = (\varepsilon_1)$.

2 išvada. Visos n – ojo laipsnio šaknys z_k iš KS z gali būti gautos iš formulės:

$$z_k = z_0 \cdot \varepsilon_k, \quad k = 0, 1, \dots, n-1.$$

Tai išplaukia iš šaknies traukimo formulės.

Primityvių n -ojo laipsnio vieneto šaknų yra tiek, kiek yra natūraliųjų skaičių m , neviršijančių n ir tokių, kad $D(m, n) = 1$. Tokių $m \in N$ skaičius žymimas $\varphi(n)$ ir vadinamas *Oilerio funkcija* (L.Euler – žymus XVIII a. šveicarų matematikas).

Pavyzdžiui, $\varphi(10) = 4$, todėl iš 10 dešimtojo laipsnio vieneto šaknų primitiviosios yra keturios: $\varepsilon_1, \varepsilon_3, \varepsilon_7, \varepsilon_9$.

3 išvada. Jei ε_k yra n – ojo laipsnio PŠ, tai ε_k negali būti jokio mažesnio laipsnio primitiviaja vieneto šaknimi.

Įr. Tarkime ε_k yra n – ojo laipsnio PŠ, $l < n$ ir ε_k yra taip pat ir l – ojo laipsnio PŠ.

Bet tada $\varepsilon_k^0 = \varepsilon_k^l = 1$, t.y. ε_k nėra n – ojo laipsnio PŠ, - prieštara.

Paskaita 1 – 11

Kubinės ir ketvirtojo laipsnio lygtys

Išmokome spręsti visas kvadratinės bei dvinarės lygtis su kompleksiniais koeficientais.

Susipažinome su vieneto šaknų grupės savybėmis.

Kubinės lygtys

Aptarsime bendriausio pavidalo trečiojo laipsnio lygčių

$$ax^3 + bx^2 + cx + d = 0, \quad a, b, c, d \in K, \quad a \neq 0, \quad (1)$$

sprendimo metodą, kuris vadinamas *Kardano* (*Geronimo Cardano*, 1501–1576, italų matematikas) vardu. Pasakojama, kad iš tikrųjų tą metodą atrado Kardano mokinys *Tartalia* (*Niccolo Tartaglia*, 1500 – 1557).

Kardano teorema. *Kiekviena (1) pavidalo lygtis turi tris sprendinius (jų tarpe gali būti lygių tarpusavyje).*

Įr. Pirmiausia, pakeitimo $x = y - \frac{b}{3a}$ pagalba, (1) lygtį suvedame į pavidalą:

$$ay^3 + p'y + q' = 0, \quad p', q' \in K.$$

Padalinę abi lygties puses iš koeficiento a , gauname *redukuotą (standartinę)* kubinės lygties su kompleksiniais koeficientais pavidalą:

$$y^3 + py + q = 0, \quad p = \frac{3ac - b^2}{3a^2}; \quad q = \frac{2b^3 - 9abc + 27a^2d}{3a^2}. \quad (2)$$

Dabar, išskaidykime y į du nenulinius dėmenis: $y = u + v$. Tuokart vieną iš dėmenų galime pasirinkti laisvai (pvz., jei $y=207$, o $u=\pi$, tai $v=207 - \pi$). Pasirinkime u ir v taip, kad galiotų sąlyga $3uv + p = 0$. Tada, (2) lygtis virsta sistema:

$$\begin{cases} 3uv + p = 0, \\ u^3 + v^3 + q = 0. \end{cases}$$

Arba, pirmąją lygtį pakėlus kubu,

$$\begin{cases} u^3 v^3 = -\frac{p^3}{27}, \\ u^3 + v^3 = -q. \end{cases} \quad (3)$$

Iš (3) nesunku pastebėti, kad u^3, v^3 yra kvadratinės lygties

$$z^2 + qz - \frac{p^3}{27} = 0$$

(vadinamos pradinės lygties (2) *rezolvente*) sprendiniai. Iš čia:

$$u^3 = \frac{-q + \sqrt{q^2 + \frac{4p^3}{27}}}{2} = -\frac{q}{2} + \sqrt{D}, \quad v^3 = \frac{-q - \sqrt{q^2 + \frac{4p^3}{27}}}{2} = -\frac{q}{2} - \sqrt{D}.$$

Skaičius $D := \frac{q^2}{4} + \frac{p^3}{27}$ vadinamas kubinės lygties (2) *diskriminantu*. (Kai kada lygties

(2) diskriminantu vadina skaičių $-108D = -4p^3 - 27q^2$).

Dabar, panaudodami šaknies iš KS traukimo formulę, gauname:

$$u = u_k = \sqrt[3]{-\frac{q}{2} + \sqrt{D}}, \quad v = v_k = \sqrt[3]{-\frac{q}{2} - \sqrt{D}}, \quad k = 0, 1, 2. \quad (4)$$

Viso galima sudaryti devynias poras skaičių u ir v . Tačiau mums tinka tik trys iš jų, būtent tos, kurios tenkina suformuluotąją sąlygą $uv = -\frac{p}{3}$. Tada, jei u_0 ir v_0 yra būtent tokia pora, tai nesunku patikrinti, kad tinka ir poros $u_0\varepsilon_1, v_0\varepsilon_2$ bei $u_0\varepsilon_2, v_0\varepsilon_1$ (įsitikinkite, kad kitos 6 galimos poros – netinka). Todėl:

$$\begin{aligned} y_0 &= u_0 + v_0 & \text{ir} & \quad x_0 = u_0 + v_0 - \frac{b}{3a}, \\ y_1 &= u_0\varepsilon_1 + v_0\varepsilon_2 & \text{ir} & \quad x_1 = u_0\varepsilon_1 + v_0\varepsilon_2 - \frac{b}{3a}, \\ y_2 &= u_0\varepsilon_2 + v_0\varepsilon_1 & \text{ir} & \quad x_2 = u_0\varepsilon_2 + v_0\varepsilon_1 - \frac{b}{3a}. \end{aligned}$$

Čia $\varepsilon_1 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, $\varepsilon_2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$ yra atitinkamos *trečiojo laipsnio* vieneto šaknys. QED.

Kardano metodas svarbus daugiau teorine prasme: įrodoma kad kiekviena kubinė lygtis yra išsprendžiama formulių (4) pagalba. Praktiškai šios formulės nėra labai patogios: tenka operuoti su “negražiais” skaičiais, atlikti daug skaičiavimų. Tačiau atskirais atvejais sprendimas Kardano formulių pagalba yra gana vaizdus ir lakoniškas.

Pavyzdžiui, išspręskime lygtį: $x^3 - 3x^2 + 6x - 4 - 2i = 0$. Po pakeitimo $x = y + 1$ gauname lygtį: $y^3 + 3y - 2i = 0$. Iš čia gauname tokią *rezolventę*:

$$z^2 - 2iz - 1 = 0.$$

Todėl, šiuo atveju, $u^3 = v^3 = i = \cos \frac{\pi}{2} + i \sin \frac{\pi}{2}$. Ištraukus kubinę šaknį, gausime:

$$u_k = v_k = \cos \varphi_k + i \sin \varphi_k, \quad \varphi_k = \frac{\pi}{6} + \frac{2\pi k}{3}, \quad k = 0, 1, 2.$$

Nesunku pastebėti, kad sąlygą $uv = -1$ tenkina, pavyzdžiui, pora u_0, v_1 . Taigi, pagal Kardano teoremą:

$$\begin{aligned} y_0 &= u_0 + v_1; & x_0 &= u_0 + v_1 + 1 = 1 + i; \\ y_1 &= u_0 \varepsilon_1 + v_1 \varepsilon_2; & \rightarrow & x_1 = u_0 \varepsilon_1 + v_1 \varepsilon_2 + 1 = 1 + i; \\ y_2 &= u_0 \varepsilon_2 + v_1 \varepsilon_1; & x_2 &= u_0 \varepsilon_2 + v_1 \varepsilon_1 + 1 = 1 - 2i. \end{aligned}$$

Kardano ir Tartalijos amžininkams labai komplikuotai atrodė atvejis, kai $a, b, c, d \in R$, o

$$D = \frac{q^2}{4} + \frac{p^3}{27} < 0.$$

Mat tada apskaičiuojant lygties (2) sprendinius tenka traukti kvadratinę šaknį iš neigiamo skaičiaus, – atsakymai, kaip žinia, yra kompleksiniai skaičiai. Ilgus metus matematikai nemokėjo rasti realiojo kubinės lygties sprendinio, nors ir žinojo, kad jis egzistuoja. Šis atvejis buvo pavadintas *Casus irreducibilis* ir buvo daugelio 15-16a. matematikų nesėkmingų tyrinėjimų objektu, kol prancūzų matematikas F.Vieta (Vieta, 1540-1603), pasinaudodamas KS trigonometrine forma, pateikė išsamų šio atvejo aprašymą – sprendimą.

Teorema. *Redukuota kubinė lygtis (2) su realiaisiais koeficientais p, q visada turi bent vieną realų sprendinį. Kai $D > 0$, – kiti du sprendiniai yra tarpusavyje jungtiniai KS. Kai $D \leq 0$ – visi trys lygties (2) sprendiniai yra realieji skaičiai.*

Įr. Kai p, q – realieji, o $D > 0$, tai iš (4) formulių išplaukia, jog tinkamos poros yra: u_0, v_0 ; $u_0 \varepsilon_1, v_0 \varepsilon_2$; $u_0 \varepsilon_2, v_0 \varepsilon_1$.

$$\text{Čia } u_0, v_0 \in R, \text{ o } \varepsilon_1 = -\frac{1}{2} + \frac{\sqrt{3}}{2}i, \quad \varepsilon_2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

$$\text{Bet tada } y_0 = u_0 + v_0 \in R, \quad y_{1,2} = -\frac{u_0 + v_0}{2} \pm \frac{u_0 - v_0}{2} \cdot i\sqrt{3} \in K.$$

Kai $D < 0$, tai akivaizdu, kad $p < 0$. Pažymėję $p = -p'$, $p' > 0$ ir $D' = -\frac{q^2}{4} + \frac{p'^3}{27} > 0$ iš Kardano formulių (4) turėsime:

$$u = u_k = \sqrt[3]{-\frac{q}{2} + i\sqrt{D'}}, \quad v = v_k = \sqrt[3]{-\frac{q}{2} - i\sqrt{D'}}, \quad k = 0, 1, 2. \quad (5)$$

Kaip matome, (5) formulių pošakniuose yra tarpusavyje jungtiniai KS. Jei, tarkime, skaičiaus $-\frac{q}{2} + i\sqrt{D'}$ argumentas yra φ , tai, kaip žinome, jam jungtinio skaičiaus $-\frac{q}{2} - i\sqrt{D'}$ argumentas yra $-\varphi + 2\pi$. Tuo tarpu abiejų pošaknių *moduliai* yra lygūs skaičiui $\sqrt[3]{-\frac{p^3}{27}}$.

Tad ir skaičių u_k, v_k moduliai yra vienodi ir lygūs $\sqrt[6]{-\frac{p^3}{27}} = \sqrt{\frac{-p}{3}}$, o argumentus formaliai galima užrašyti taip:

$$u_k : \quad \frac{\varphi}{3}, \frac{\varphi + 2\pi}{3}, \frac{\varphi + 4\pi}{3};$$

$$v_k : \quad \frac{-\varphi + 2\pi}{3}, \frac{-\varphi + 4\pi}{3}, \frac{-\varphi + 6\pi}{3}.$$

Mums tinka tie u_k, v_k , kurių argumentų suma kartotinė 2π . Matome, kad tokios yra poros: $u_0, v_2; u_1, v_1; u_2, v_0$. Tačiau, tada:

$$y_0 = u_0 + v_2 = r \left(\cos \frac{\varphi}{3} + i \sin \frac{\varphi}{3} + \cos \frac{6\pi - \varphi}{3} + i \sin \frac{6\pi - \varphi}{3} \right) = 2r \cos \frac{\varphi}{3} \in R;$$

$$y_1 = u_1 + v_1 = r \left(\cos \frac{\varphi + 2\pi}{3} + i \sin \frac{\varphi + 2\pi}{3} + \cos \frac{4\pi - \varphi}{3} + i \sin \frac{4\pi - \varphi}{3} \right) = 2r \cos \frac{\varphi + 2\pi}{3} \in R;$$

$$y_2 = u_2 + v_0 = r \left(\cos \frac{\varphi + 4\pi}{3} + i \sin \frac{\varphi + 4\pi}{3} + \cos \frac{2\pi - \varphi}{3} + i \sin \frac{2\pi - \varphi}{3} \right) = 2r \cos \frac{\varphi + 4\pi}{3} \in R.$$

Atskiru atveju, kai $D = 0$, tai abiejuose požakniuose yra tas pats *realusis skaičius* $-q/2$, todėl abiem atvejais arba $\varphi = 0$ (kai $q < 0$), arba $\varphi = \pi$. T.y. skaičių $u_k = v_k$ argumentai yra:

$$0, \frac{2\pi}{3}, \frac{4\pi}{3},$$

arba (kai $\varphi = \pi$)

$$\frac{\pi}{3}, \pi, \frac{5\pi}{3}.$$

Nesunku pastebėti, kad atveju $\varphi = 0$ tinka poros: $u_0, v_0; u_1, v_2; u_2, v_1$. Tuokart:

$$y_0 = u_0 + v_0 = r(\cos 0 + i \sin 0 + \cos 0 + i \sin 0) = 2r \cos 0 = 2r \in R;$$

$$y_1 = u_1 + v_2 = r \left(\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} + \cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3} \right) = 2r \cos \frac{2\pi}{3} = -r \in R;$$

$$y_2 = u_2 + v_1 = r \left(\cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3} + \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} \right) = 2r \cos \frac{4\pi}{3} = -r = y_1 \in R.$$

Atveju $\varphi = \pi$ tinka: $u_0, v_2; u_1, v_1; u_2, v_0$. Tada:

$$y_0 = u_0 + v_2 = r \left(\cos \frac{\pi}{3} + i \sin \frac{\pi}{3} + \cos \frac{5\pi}{3} + i \sin \frac{5\pi}{3} \right) = 2r \cos \frac{\pi}{3} = r \in R;$$

$$y_1 = u_1 + v_1 = r(\cos \pi + i \sin \pi + \cos \pi + i \sin \pi) = 2r \cos \pi = -2r \in R;$$

$$y_2 = u_2 + v_0 = r \left(\cos \frac{5\pi}{3} + i \sin \frac{5\pi}{3} + \cos \frac{\pi}{3} + i \sin \frac{\pi}{3} \right) = 2r \cos \frac{\pi}{3} = r = y_0 \in R.$$

Išvada: tuo atveju, kai $D = 0$, du iš trijų realių sprendinių sutampa. Pagaliau, kai ir $q = 0$, sutampa visi trys sprendiniai, t.y. $y_i = 0$, $i = 1, 2, 3$.

Reikia dar nepamiršti, kad pradinė (1) lygtis yra x atžvilgiu. T.y., radius y , reikia prisiminti, kad

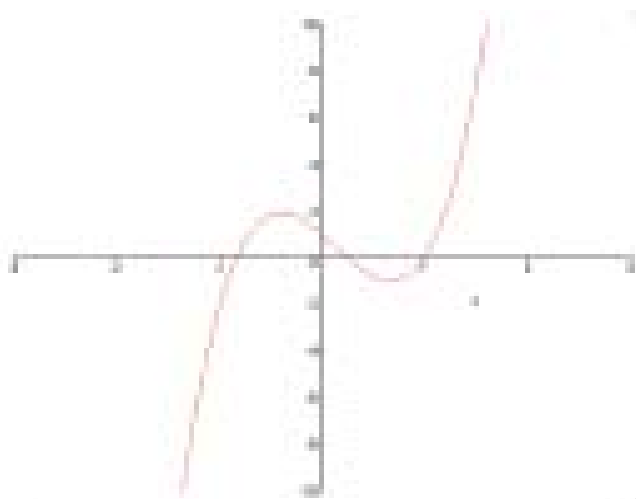
$$x_k = y_k - \frac{b}{3a}, \quad k = 0, 1, 2.$$

Teorema įrodyta.

Pvz., redukuota kubinė lygtis $x^3 - 6x + 2 = 0$ turi tris realiuosius sprendinius, nes

$$D = \frac{2^2}{4} - \frac{6^3}{27} = 1 - 8 = -7 < 0.$$

Grafinis sprendimas. Kai nereikia didelio tikslumo, kubinę lygtį galima spręsti ir grafiškai. Pavyzdžiui, kompiuteriu nubrėžtas funkcijos $y = 5x^3 - 2x^2 - 4x + 1$ grafiko eskizas



rodo, kad atitinkama lygtis $5x^3 - 2x^2 - 4x + 1 = 0$ turi **tris** realiuosius sprendinius. Be to, $x_3 \approx 1$, $x_2 \approx 0,2$, $x_1 \approx -0,8$. Jei tokio tikslumo nepakanka, kompiuteriu lengva patikslinti

brėžinį, arba – spręsti lygtį Kardano metodu. Patikslinus, gautume: $x_3 \approx 1,000000$, $x_2 \approx 0,23851648$, $x_1 \approx -0,83851648$. Ir jau visai tikslūs atsakymai yra:

$$1, -\frac{3}{10} + \frac{1}{10}\sqrt{29}, -\frac{3}{10} - \frac{1}{10}\sqrt{29}.$$

Ketvirtojo laipsnio lygtys

Toliau natūralu pasidomėti bendriausia ketvirtojo laipsnio lygtimi:

$$ax^4 + bx^3 + cx^2 + dx + e = 0, a, b, c, d, e \in K, a \neq 0. \quad (6)$$

Pristatysime italų matematiko *L.Ferrari* (1522 - 1565) išvestąjį sprendimo algoritmą.

Ferrari teorema. *Kiekviena (6) pavidalo lygtis turi keturis sprendinius (jų tarpe gali būti lygių tarpusavyje).*

Įr. Pakeitimas $x = y - \frac{b}{4a}$ ir dalyba iš a įgalina (6) lygtį suvesti į *redukuotą* pavidalą:

$$y^4 + 2py^2 + qy + r = 0, \quad p, q, r \in K. \quad (7)$$

(Koeficientus p, q, r apskaičiuokite patys.)

Metodo idėja: išskaidyti (7) lygties kairę pusę į dviejų kvadratinių trinarių sandaugą. Pasirodo, kad tai visada galima padaryti.

Pažymėkime raide t kol kas nežinomą parametą. Užrašykime (7) lygtį pavidalu:

$$(y^2 + p + t)^2 - (2y^2t - qy + t^2 + 2pt + p^2 - r) = 0.$$

Pareikalausime, kad antruoje skliaustuose užrašytas kvadratinis, y atžvilgiu, trinaris būtų pilnas kvadratas. Kaip žinia, tam reikia, kad jo diskriminantas būtų lygus nuliui, t.y.

$$q^2 - 4 \cdot 2t \cdot (t^2 + 2pt + p^2 - r) = 0.$$

Kitaip sakant, reikia, kad skaičius t būtų kubinės lygties (vadinamos (6) lygties *rezolvente*)

$$8t^3 + 16pt^2 + 8(p^2 - r)t - q^2 = 0$$

sprendinys. Iš *Kardano teoremos* žinome, kad tokių skaičių (bendriausiu atveju) yra trys. Jei t_0 - vienas iš jų, tai (7) lygtį galima užrašyti šitaip:

$$(y^2 + p + t_0)^2 - \left(\sqrt{2t_0} \left(y - \frac{q}{4t_0} \right) \right)^2 = 0.$$

Iš čia, suskaidę, gauname:

$$\left((y^2 + p + t_0) - \sqrt{2t_0} \left(y - \frac{q}{4t_0} \right) \right) \left((y^2 + p + t_0) + \sqrt{2t_0} \left(y - \frac{q}{4t_0} \right) \right) = 0.$$

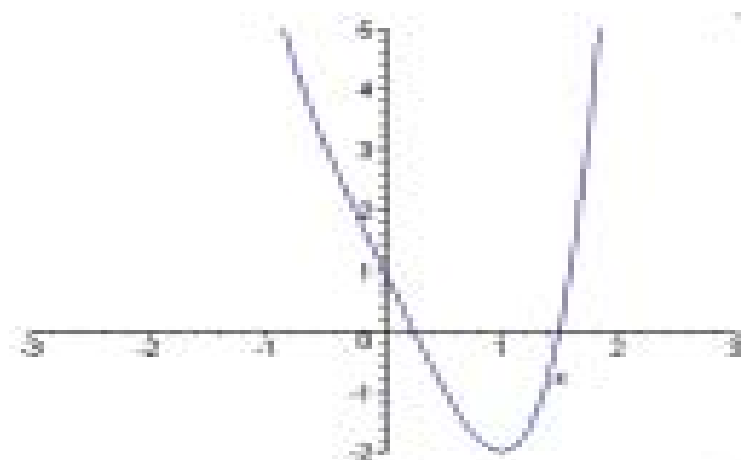
Tai - dviejų *kvadratinų* lygčių su kompleksiniais koeficientais sandauga. Išsprendę kiekvieną iš jų atskirai, gausime keturis (7) lygties, o iš jų – keturis (6) lygties sprendinius. Aišku, jų tarpe gali būti lygių. QED.

Ferrari metodas be pakeitimų tinka ir atvejui, kai lygties koeficientai yra realieji skaičiai. Tuokart galimi tokie atvejai:

- (6) lygtis turi 4 realiuosius sprendinius,
- (6) lygtis turi 2 realiuosius ir 2 kompleksinius sprendinius. Pastarieji yra tarpusavyje jungtiniai skaičiai,
- (6) lygtis turi 4 kompleksinius sprendinius, kurie yra dvi tarpusavyje jungtinių skaičių poros.

Su šiuolaikine skaičiavimo technika nesunku ir ketvirtojo, ir aukštesnio laipsnio lygtis spręsti *grafiškai*. Tačiau, sprendžiant grafiškai, sunku gauti didelį tikslumą. Be to, grafikas parodo tik realiuosius lygties sprendinius.

Pvz., išspręskime redukuotą lygtį: $x^4 + 4x - 1 = 0$. Čia $p = 0$, $q = 4$, $r = -1$. Nubrėžę grafiką



matome, kad lygtis turi du realiuosius sprendinius. Be to, $x_1 \approx 0,25$, $x_2 \approx 1,45$.

Ferrari metodu gautume, kad pradinės lygties rezolventė atrodo taip:

$$8t^3 + 8t - 16 = 0.$$

Pastebime, kad viena iš jos šaknų yra: $t_0 = 1$. Todėl pradinė lygtis užrašoma šitaip:

$$(x^2 + 1)^2 - 2(x - 1)^2 = 0.$$

Taigi, telieka išspręsti dvi kvadratinės lygtis:

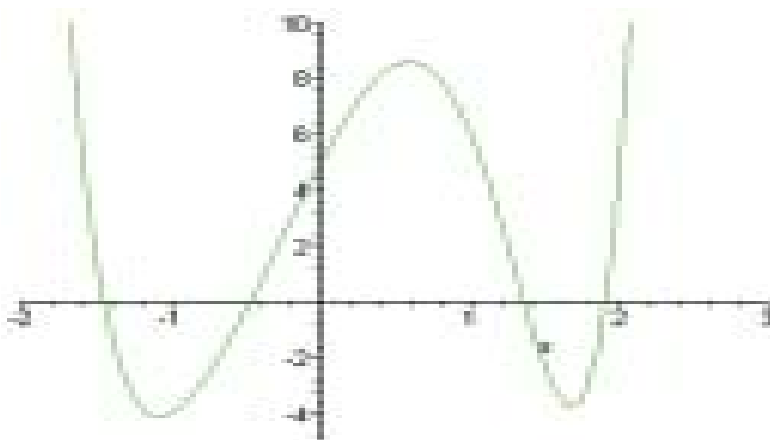
$$x^2 + 1 - \sqrt{2}(x - 1) = 0 \quad \text{ir} \quad x^2 + 1 + \sqrt{2}(x - 1) = 0$$

ir turime tikslų atsakymą:

$$x_{1,2} = \frac{\sqrt{2}}{2} \pm \frac{\sqrt{2+4\sqrt{2}}}{2} i; \quad x_{3,4} = -\frac{\sqrt{2}}{2} \pm \frac{\sqrt{-2+4\sqrt{2}}}{2}.$$

Spręsdami šeštojo laipsnio lygtį

$$x^6 - 2x^4 - 5x^3 - 3x^2 + 10x + 5 = 0,$$

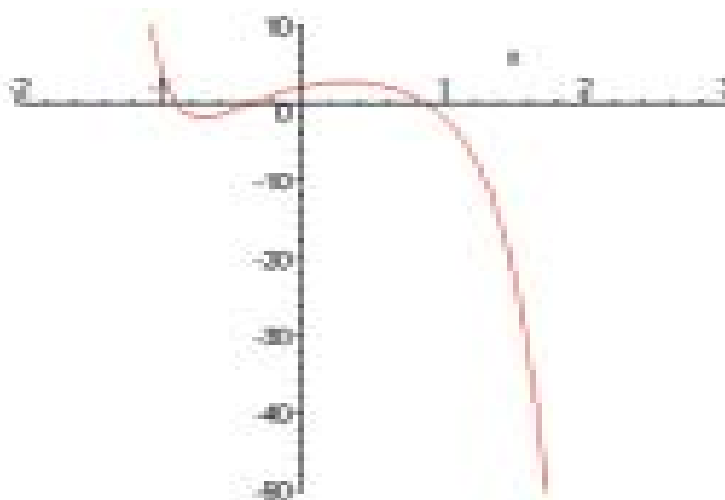


pastebime, kad lygtis tikrai turi 4 (realiuosius) sprendinius, tačiau negalime būti tikri, kad daugiau realiųjų sprendinių nėra. Be to, neaišku, ar lygtis turi dar ir kompleksinių sprendinių. Antrame kurse, susipažinę su bendrąja polinomų teorija, parodysime, kad n – tojo laipsnio lygtis KS lauke visada turi n sprendinių. Aptarsime ir būdus realiesiems sprendiniams (tiksliai arba apytikriai, bet norimu tikslumu) rasti.

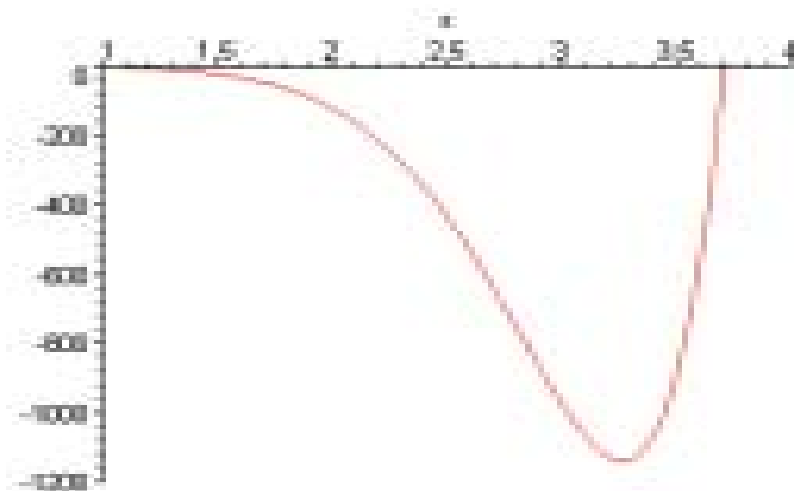
Pateiksime dar vieną pamokantį algebrinės lygties grafinio sprendimo pavyzdį.

$$x^8 - 5x^7 + 5x^6 - 2x^4 - 2x^3 + 4x + 2 = 0.$$

Atrodytų, grafikas gana vaizdžiai charakterizuoja situaciją: yra trys realieji sprendiniai; galima pateikti ir jų apytikres reikšmes: $x_1 \approx -0,9$; $x_2 \approx -0,4$; $x_3 \approx 0,8$.



Tačiau, tas pats grafikas, jį detalizavus, atrodo jau taip:



Tenka konstatuoti: yra ir ketvirtasis realusis pradinės lygties sprendinys, $x_4 \approx 3,7$. Taigi, grafiku perdėm pasikliauti negalima, prireikia išsamesnio tyrimo. Išsamiau apie tai ir kalbėsime II kurse, skyriuje “Polinomų algebra”.

Toliau, nuosekliai reiktų ieškoti penktojo ir aukštesnių laipsnių lygčių su kompleksiniais koeficientais sprendimo metodų. Istorškai taip ir buvo: įvairių šalių matematikai XVI - XVIII a. ieškojo Kardano ir Ferrari metodų analogų lygtims, kurių laipsnis $n \geq 5$. Tačiau visi bandymai buvo nesėkmingi. Po ilgų nesėkmių metų pradėta galvoti kitaip: ar apskritai yra formulės, tarkime, bendriausios penktojo laipsnio lygties sprendiniams rasti? Kartais sako: ar galima tokią lygtį *išspręsti radikalais*?

Sakoma, kad algebrinė lygtis yra *išsprendžiama radikalais*, kai formulėje, išreiškiančioje lygties sprendinius per koeficientus, naudojami tik keturi aritmetikos veiksmai ir šaknies traukimas.

1824 m. norvegų matematikas *N. Abelis* (*Niels Henrik Abel*, 1802-1829) parodė, kad atsakymas į šitaip formuluojamą klausimą yra neigiamas. Kita vertus, akivaizdu, kad atskiroms (pvz., dvinarėms) lygtims tokios formulės tikrai egzistuoja. Imta domėtis, kokių tipų lygtims tas formules galima rasti. Talentingas prancūzų matematikas *E. Galua* (*Evariste Galois*, 1811-1832) išvystė bendrą teoriją (*Galua teoriją*), kurioje *grupių* terminais atsakoma į klausimą: kada algebrinė lygtis yra *išsprendžiama radikalais*. Paminėtos problemos yra šiuolaikinės *moderniosios algebras* dėmesio centre. Labai tikėtina, kad po kurio laiko, ir AST’os programa bus peržiūrėta. Tai, ką mes dabar vadiname moderniaja algebra taps Universitete dėstoma klasika.

Paskaita 1 – 12

Grupės ir pogrupiai. Lagranžo teorema

Aptarėme algebrinių lygčių virš KS lauko $\mathbf{K}$ sprendimą. Pastebėjome, kad tais atvejais, kai lygtį mokame *išspręsti radikalais*, sprendinių skaičius (įskaitant ir pasikartojančius) yra lygus lygties laipsniui. Toks faktas yra teisingas ir bendru atveju, tačiau jo griežtam pagrindimui mums dar trūksta žinių.

Ciklinės grupės ir jų savybės

Jau esame aptarę *grupės, pogrupio* sąvokas. Prisiminkime dar sykį: *grupė*, tai AS su viena asociatyvia algebrine operacija, turinti neutralųjį elementą ir kiekvienam elementui – simetrinį. Naujausias grupės (baigtinės) pavyzdys - $(V_n, \cdot)$.

Grupės sąvoka algebroje yra labai svarbi. Minėjome, kad grupių ir baigtinių laukų teorijos kūrėju laikomas prancūzų matematikas *E. Galua*. Jo darbai paskatino audringą šios fundamentaliosios matematikos šakos vystymąsi.

Susipažinsime su keliomis svarbesnėmis grupių teorijos sąvokomis. Pabrėžtina, kad tai yra tik įžanginiai žingsniai. Grupių teorija šiuolaikinėje algebroje yra pažengusi labai toli ir bent kiek išsamesnės jos studijos pareikalautų daug laiko ir pastangų.

Pradžioje prisiminsime ir apibendrinsime *ciklinės grupės* sąvoką. Primenu, kad AS $(V_n, \cdot)$ yra ciklinės grupės pavyzdys. Aprašysime bendrąją grupės $G = (G, *)$ *ciklinio pogrupio* $H = (H, *)$ sudarymo metodą. Kad užrašai būtų paprastesni, grupės operaciją vadinkime *daugyba*.

Tarkime $a \in G$. Aibė $H = \{a^m \mid m \in \mathbb{Z}\}$ akivaizdžiai yra grupės G bazinės aibės G poaibis. Čia:

$$a^m := \underbrace{aa \dots a}_{m \text{ kartų}}; \quad a^0 = e; \quad a^{-m} := (a')^m, \text{ su visais } m \in \mathbb{N}.$$

Kadangi tenkinamos pogrupio kriterijaus sąlygos, tai AS $H = (H, \cdot)$ yra grupės G pogrupis. Jis vadinamas elemento a generuotu *cikliniu pogrupiu* ir žymima:

$$(H, \cdot) = (a).$$

Štai keletas konkrečių tokių pogrupių pavyzdžių.

1. Kai $G = (\mathbb{Z}, +)$, o $a = 5$, tai $a^m := \underbrace{a + a + \dots + a}_{m \text{ kartų}} = 5m$, o pogrupio $H = (H, +) = (5)$

bazinė aibė $H = \{5m \mid m \in \mathbb{Z}\}$ yra ne kas kita, kaip skaičiui 5 kartotinių sveikųjų skaičių aibė, dažnai žymima $\mathbb{Z}_5$. Taigi, $(\mathbb{Z}_5, +) = (5)$ yra grupės $G = (\mathbb{Z}, +)$ ciklinis pogrupis.

2. Baigtinės grupės $(V_{20}, \cdot)$ pogrupio (ε_4) bazinė aibė irgi baigtinė $\{\varepsilon_0, \varepsilon_4, \varepsilon_8, \varepsilon_{12}, \varepsilon_{16}\}$.

Ap. Baigtinės grupės G eile vadiname jos bazinės aibės elementų skaičių.

Žymima $E(G)$. Pvz., $E(V_{20}) = 20$, $E((\varepsilon_4)) = 5$.

Primenu, kad, lakoniškumo dėlei, grupę kartais pavadiname jos bazinę aibę.

3. Begalinės multiplikacinės grupės $(R_+, \cdot)$ elementas $a = -1$ generuoja baigtinį pogrupį $(-1) = \{-1, 1\}$, kurio eilė yra 2.

Baigtinės grupės atveju, visi vieno kokio nors elemento laipsniai (kartotiniai) negali būti skirtingi, kitaip grupė būtų begalinė.

Ap. Mažiausias natūralusis skaičius d , su kuriuo galioja lygybė $a^d = e$, vadinamas grupės elemento a eile ir žymima $E(a)$.

Pvz., grupės $(V_{20}, \cdot)$ elemento ε_4 eilė yra 5. Tikrai:

$$\varepsilon_4^5 = \left(\cos \frac{2\pi \cdot 4}{20} + i \sin \frac{2\pi \cdot 4}{20} \right)^5 = \left(\cos \frac{2\pi \cdot 4 \cdot 5}{20} + i \sin \frac{2\pi \cdot 4 \cdot 5}{20} \right) = \varepsilon_0 = 1.$$

Todėl $E(\varepsilon_4) = 5$.

Tas faktas, kad elemento eilė sutapo su jo generuoto pogrupio eile nėra atsitiktinumas, o bendroji visų baigtinių ciklinių pogrupių savybė.

Teorema. *Baigtinės ciklinės grupės generuojančio elemento eilė sutampa su jo generuotos grupės eile. T.y. $E(a) = E((a))$.*

Irodymas išplaukia iš to, kad aibėje $\{a^m \mid m \in \mathbb{Z}\}$ skirtingi yra tik tokie laipsniai: $a^0, a^1, \dots, a^{d-1}$. Iš tikrųjų, bet koks neigiamas laipsnis $-s$ gali būti išreikštas pavidalu:

$$-s = (-t)d + r \text{ su natūraliuoju } t \text{ ir neneigiamu } r \in \{0, 1, \dots, d-1\}.$$

Todėl:

$$a^{-s} = (a^{-1})^d \cdot a^r = ((a^{-1})^d) a^r = e \cdot a^r = a^r. \text{ Be to, iš } a^k = a^l \text{ su } k, l \in \{0, 1, \dots, d-1\}$$

tuoj pat gautume prieštarą (pvz., kai $k > l$): $a^{k-l} = e$ ir $k-l < d$. Taigi,

$$(a) = \{a^0, a^1, \dots, a^{d-1}\}. \quad \text{QED.}$$

1 išvada. Jei $a^m \in (a)$ ir $a^m = e$, tai $d \mid m$.

2 išvada. Ciklinė grupė yra Abelio grupė. Tai išplaukia iš laipsnio a^m apibrėžimo.

3 išvada. Ciklinės grupės pogrupiai yra cikliniai.

Tarp pogrupio H elementų yra natūraliųjų laipsnių a^m . Tada yra ir laipsnis su mažiausiu rodikliu k (MSP). Tuokart: $H = (b)$, $b = a^k$. Tarus, kad yra toks $a^m \in H$, kad $a^m \neq (a^k)^l$, turėtume, kad: $m = kl + r$ ir $r < k$. Bet išvada $a^m = a^r \in H$ prieštarauja mažiausiojo skaičiaus principui.

4 išvada. Visos tos pačios eilės baigtinės ciklinės grupės yra izomorfiškos. Izomorfiškos tarpusavyje ir visos begalinės ciklinės grupės.

Kai $G_1 = (a)$, o $G_2 = (b)$, tereikia apibrėžti tokią bijekciją: $(\forall m \in \mathbb{Z}) \varphi(a^m) = b^m$ ir įsitikinti, kad tenkinamos izomorfizmo sąlygos.

Gretimos klasės. Lagranžo teorema

Ap. Kai $G = (G, \cdot)$ yra baigtinė eilės n grupė, o $H = (H, \cdot)$ - jos pogrupis, kurio eilė yra m , tai aibę $Hg := \{h_1g, h_2g, \dots, h_mg\}$ vadinsime elemento $g \in G$ generuota **gretima klase** pagal pogrupį H (kurio bazinė aibė yra $H = \{h_1, h_2, \dots, h_m\}$).

Aišku, kai grupė G nėra Abelio grupė, tai reikia skirti *kairinę* $gH := \{gh_1, gh_2, \dots, gh_m\}$ ir *dešinę* $Hg := \{h_1g, h_2g, \dots, h_mg\}$ gretimas klases.

Gretimos klasės pasižymi įdomiomis savybėmis, kurios padeda išryškinti baigtinių grupių struktūrą.

1. $(\forall g \in G) \text{Card}(Hg) = m.$
2. $Hg = H \equiv g \in H.$
3. Dvi gretimos klasės Hg_1 ir Hg_2 arba neturi bendrų elementų, arba sutampa.
4. $(\forall g \in G) g \in Hg.$

Lagranžo teorema. (J.Lagrange, 1736 – 1813, žymus prancūzų matematikas).

Baigtinės grupės eilė dalijasi iš jos kiekvieno pogrupio eilės.

Įrodymas išplaukia iš akivaizdžios lygybės:

$$G = \bigcup_{g \in G} Hg.$$

Čia sąjunga imama pagal visus bazinės aibės G elementus. Kadangi skirtingų gretimų klasių skaičius j yra baigtinis, ir, pagal 1 savybę, kiekvienoje tokioje klasėje yra lygiai m aibės G elementų, tai $n = j \cdot m$. QED.

Išvada. Grupės eilė dalijasi iš jos kiekvieno elemento eilės.

Normalieji dalikliai. Faktorgrupė

Ap. Jei $(\forall g \in G) gH = Hg$, tai pogrupis H vadinamas grupės G **normaliuoju dalikliu** (sutrumpintai: ND).

Pavyzdžiui, bet koks grupės $(V_n, \cdot)$ pogrupis H yra jos normalusis daliklis, nes $(V_n, \cdot)$ - Abelio grupė.

Teorema. Grupės G pogrupis H yra jos ND tada ir tik tada, kai

$$(\forall h \in H)(\forall g \in G) ghg^{-1} \in H.$$

Įr. 1. Duota: H yra ND. Įrodyti: $(\forall h \in H)(\forall g \in G) ghg^{-1} \in H$.

Jei H – ND, tai, pagal apibrėžimą, $(\forall g \in G) gH = Hg$. Todėl, jei $gh \in gH$, tai yra toks $h' \in H$, kad $gh = h'g \in Hg$. Tačiau grupėje yra elemento g simetriškas g^{-1} . Padauginę pastarąją lygybę iš g^{-1} , gausime: $ghg^{-1} = h' \cdot e = h' \in H$.

2. Duota: $(\forall h \in H)(\forall g \in G) ghg^{-1} \in H$. Įrodyti: H yra ND, t.y. $(\forall g \in G) gH = Hg$.

Imame $g \in G$ ir sudarome gretimą klasę gH . Kadangi, $(g^{-1})^{-1} = g$, tai, pagal sąlygą, $(\forall h \in H) g^{-1}hg \in H$. Todėl $g(g^{-1}hg) \in gH$. Kita vertus, $g(g^{-1}hg) = (gg^{-1})hg = hg \in Hg$. Todėl $gH \subset Hg$. Panašiai įrodoma ir kad $gH \supset Hg$. QED.

Komentaras: ND tai toks (nebūtinai Abelio) grupės pogrupis pagal kurį kairiosios ir dešinėsios gretimos klasės sutampa.

Išvada. Kai H – ND, lieka galioti 1 – 4 gretimų klasių savybės. Įrodymai irgi iš esmės nesikeičia.

Tarkime G – grupė, o H – jos ND. Tada, kaip jau matėme, iš gretimų klasių savybių išplaukia:

$$G = \bigcup_{g \in G} Hg.$$

Be to, remiantis gretimų klasių savybėmis, lengva parodyti, kad:

$$Ha = Hb \equiv a \in Hb \vee b \in Ha.$$

Ap. Skirtingų gretimų klasių pagal ND aibę

$$G/H := \{Hg \mid g \in G\}$$

vadinsime aibės G **faktoraibe**, pagal normalųjį daliklį H .

Ap. Gretimų klasių Ha, Hb sandauga vadinsime gretimą klasę Hab .

Rašysime: $Ha * Hb = Hab$.

Suprantama, taip apibrėžta “daugyba” $*$ yra *algebrinė operacija* faktoraibėje G/H .

Teorema. *Algebrinė struktūra $(G/H, *)$ yra grupė.*

Įr. Patikrinsime grupės aksiomas.

1. Operacijos asociatyvumas:

$$Ha * (Hb * Hc) = Ha * Hbc = Ha(bc) = H(ab)c = Hab * Hc = (Ha * Hb) * Hc.$$

2. Neutraliuoju yra elementas $He = H$.

3. Klasei Ha simetriška (atvirkštinė) yra klasė Ha^{-1} , nes, pagal apibrėžimą:

$$Ha * Ha^{-1} = He = H. \quad \text{QED.}$$

1 išvada. Jei G – Abelio grupė, tai ir $(G/H, *)$ – Abelio grupė.

2 išvada. Jei G – ciklinė grupė, tai ir $(G/H, *)$ – ciklinė grupė.

Grupių homomorfizmai. Pagrindinė teorema (PHT)

Esame susipažinę su grupių izomorfizmo ir homomorfizmo sąvokomis, įrodėme teorema, kad izomorfiškas (homomorfiškas) grupės vaizdas yra grupė.

Tarkime $\varphi : G \longrightarrow G_1$ yra grupių G ir G_1 homomorfizmas. Grupės G neutralųjį elementą žymėkime e , grupės G_1 neutralųjį elementą, – e_1 , o abiejų grupių operacijas, paprastumo dėlei, vadinkime *daugyba*.

Ap. Homomorfizmo $\varphi : G \longrightarrow G_1$ branduoliu vadinama aibė:

$$\text{Ker}\varphi := \{a \mid a \in G, \varphi(a) = e_1\}.$$

Teorema. Kai $\text{Ker}\varphi$ yra homomorfizmo $\varphi : G \longrightarrow G_1$ branduolys, tai $(\text{Ker}\varphi, \cdot)$ yra grupės G normalusis daliklis.

Iš I. Pirmiausia įsitikinsime, kad $(\text{Ker}\varphi, \cdot)$ yra grupės G pogrupis. Tiesiog iš apibrėžimo išplaukia, kad $\text{Ker}\varphi \subset G$, todėl galime taikyti pogrupio kriterijų.

1. $\text{Ker}\varphi$ yra uždaras operacijos atžvilgiu, nes:

$$(\forall a, b \in \text{Ker}\varphi) \varphi(ab) = \varphi(a)\varphi(b) = e_1 e_1 = e_1 \rightarrow ab \in \text{Ker}\varphi.$$

2. $e \in \text{Ker}\varphi$, nes

$$(\forall a \in \text{Ker}\varphi) \varphi(ae) = \varphi(a)\varphi(e) = e_1 \varphi(e) = \varphi(e) \rightarrow \varphi(e) = e_1 \rightarrow e \in \text{Ker}\varphi.$$

3. Jei $a \in \text{Ker}\varphi$, tai $a^{-1} \in \text{Ker}\varphi$, nes

$$e_1 = \varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}) = e_1 \varphi(a^{-1}) \rightarrow \varphi(a^{-1}) = e_1 \rightarrow a^{-1} \in \text{Ker}\varphi.$$

II. Dabar pritaikome ND kriterijų: $(\forall g \in G)(\forall h \in \text{Ker}\varphi)$

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)e_1\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(e_1) = e_1 \rightarrow ghg^{-1} \in \text{Ker}\varphi.$$

QED.

Teorema. (PHT). Jei $\varphi : G \longrightarrow G_1$ yra homomorfizmas, tai $G / \text{Ker}\varphi \cong \varphi(G)$.

Teorema galima formuluoti ir taip: kiekvienas homomorfizmas $\varphi : G \longrightarrow G_1$ indukuoja izomorfizmą $\bar{\varphi} : G / \text{Ker}\varphi \leftrightarrow \varphi(G)$.

Įrodymo idėjas pailiustruosime pavyzdžiu. Tarkime:

$$G = V_{20}; G_1 = V_4; \varphi : V_{20} \longrightarrow V_4, \varphi(\varepsilon_k^{(20)}) = (\varepsilon_k^{(20)})^5 = \varepsilon_k^{(4)}.$$

$$\text{Tada: } e = \varepsilon_0^{(20)}; e_1 = (\varepsilon_0^{(20)})^5 = \varepsilon_0^{(4)}; H := \text{Ker}\varphi = \{\varepsilon_0^{(20)}, \varepsilon_4^{(20)}, \varepsilon_8^{(20)}, \varepsilon_{12}^{(20)}, \varepsilon_{16}^{(20)}\};$$

$$V_{20} / H = \{H\varepsilon_0^{(20)} = H, H\varepsilon_1^{(20)}, H\varepsilon_2^{(20)}, H\varepsilon_3^{(20)}\}.$$

PHT: $(V_{20} / H, *) \cong (V_4, \cdot)$. Postuluojamas izomorfizmas $\bar{\varphi}$ apibrėžiamas taisykle:

$$\bar{\varphi}(H\varepsilon_k^{(20)}) = \varepsilon_k^{(4)}.$$

Paskaita 2 – 01

Tiesinės algebros elementai

Kalbėjome apie **logikos** bei **aibių teorijos** pagrindines sąvokas ir dėsnius. Formuluodami veiksmų su aibėmis apibrėžimus ir įrodinėdami tų veiksmų savybes, naudojome *logines operacijas* ir *logikos dėsnius*. Susipažinę su **algebrinės struktūros** sąvoka, platesniu centru ir griežčiau nei mokykloje, aptarėme skaičių aibes: natūraliųjų skaičių *pusgrupę*, sveikųjų skaičių *žiedą*, racionaliųjų, realiųjų ir, pagaliau, – kompleksinių skaičių *laukus* (kūnus). Apskritai, galima pasakyti, kad mes susipažinome su **matematinės kalbos** abėcėle ir pagrindinėmis tos kalbos “gramatikos” taisyklėmis. Įgytas žinias taikėme mokyklinės matematikos faktams pagrįsti ir išplėsti.

Tiesinė lygtis, tiesinių lygčių sistema. Labai dažnai (ypač, ekonomikoje) gamybines situacijas pavyksta aprašyti (sumodeliuoti) *tiesinės algebros* terminais. Su svarbiausiomis šios matematikos srities sąvokomis, faktais bei paprasčiausių tiesinės algebros uždavinių sprendimo metodais ir susipažinsime šiame semestre.

Ap. Lygybė (kitaip: n – vietis predikatas)

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = b \quad (1)$$

vadinama n kintamųjų **tiesine lygtimi** (kartais sakoma: ... ir su n nežinomųjų).

Čia - a_i , $i = 1, 2, \dots, n$ ir b yra kokio nors konkretaus lauko L žinomi elementai. Atskiru atveju, tai gali būti realieji arba kompleksiniai skaičiai. a_i vadinami (1) lygties *koeficientais*, o b – *laisvuju nariu*.

Pavyzdžiui, $-13x_1 + (10 - \sqrt{5})x_2 - 14x_3 = 27$ yra *trijų kintamųjų tiesinė lygtis* (lygtis su trimis kintamaisiais, nežinomaisiais). Jos koeficientai ir laisvasis narys yra realieji skaičiai.

Ap. Sutvarkytą lauko L elementų rinkinį $(k_1, k_2, \dots, k_n)$ vadiname *tiesinės lygties* (1) **sprendiniu**, jei jis *tenkina* tą lygtį (arba kitaip: *rinkinys* $(k_1, k_2, \dots, k_n)$ *priklauso* (1) *predikato teisingumo aibei*).

Pvz., rinkinys $(1, 0, 2)$ *netenkina* lygties $-13x_1 + (10 - \sqrt{5})x_2 - 14x_3 = 27$, todėl nėra jos sprendinys. Tuo tarpu rinkinys $(-1, 0, -1)$ šią lygtį *tenkina* (įsitikinkite tuo), todėl jis yra jos sprendinys.

Kartais turime keletą (1) pavidalo lygčių ir reikia rasti jų *bendruosius sprendinius*. Tokiu atveju sakome, kad turime **tiesinių lygčių sistemą** (sutrumpintai žymėsime – TLS):

Daugeliu atvejų pakanka tik žinoti, ar TLS suderinta, o patys sprendiniai arba yra nesvarbūs iš principo, arba jų suradimas patikimas kompiuteriui ir tada svarbu tik, kad jų *būtų*; atsakymą randa skaičiavimo technika. Tad pirmasis klausimas, – irgi labai svarbus.

Kol kas mes domėsime tik atsakymu į trečiąjį klausimą: *kaip rasti TLS sprendinius?* Norint rasti atsakymus į du pirmuosius klausimus, teks aptarti keletą mums naujų algebros sąvokų ir faktų. Tai mes padarysime šiek tiek vėliau.

Jau dabar įvesime *matricos* sąvoką.

Ap. TLS koeficientų matrica (arba tiesiog – **matrica**) vadiname stačiakampę lauko elementų (atskiru atveju – skaičių) lentelę:

$$A := \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}. \quad (3)$$

Sakome: ši matrica turi m eilučių ir n stulpelių. Arba trumpiau: A yra $m \times n$ eilės matrica. Jei $m = n$, tai A vadinama **kvadratine** n -osios eilės matrica.

Matrica, gauta iš A , papildžius ją (iš dešinės) laisvųjų narių stulpeliu, vadinama **išplėstąja TLS matrica**. Žymima $\bar{A}$.

Matrica, gauta iš A , sukeitus jos eilutes su stulpeliais vietomis, vadinama **transponuotąja matrica**. Žymima A^T .

TLS sprendimo Gauso metodas

Aptarsime universalų (2) TLS sprendimo būdą, – **Gauso metodą** (K.- F. Gauss, 1777-1855, genialus vokiečių matematikas). Pradėsime nuo TLS elementariųjų pertvarkių apibrėžimo.

Ap. TLS elementariaisiais pertvarkiais (EP) vadiname tokius veiksmus:

- dviejų lygčių sukeitimą vietomis,
- lygties padauginimą iš nelygaus nuliui skaičiaus,
- vienos lygties pridėjimą „panariui“ prie kitos.

*Ap. Dvi TLS vadiname **ekvivalentėmis**, jei jų sprendinių aibės sutampa.*

Mums svarbiausia, kad yra teisinga tokia teorema apie EP.

Ekvivalentumo teorema. EP nekeičia TLS sprendinių aibės.

(Arba: sistamai pritaikius EP, ji lieka *ekvivalenti* pradinei.)

Įrodymo mini – konspektas: pažymėjus duotosios TLS sprendinių aibę S , o sistemos, kuri, EP pagalba, gauta iš duotosios, sprendinių aibę – S' , parodome, kad yra teisingi teiginiai

$S \subset S'$ ir tuo pat metu $S' \subset S$, o iš to, remdamiesi aibių lygybės apibrėžimu, darome išvadą, kad $S = S'$.

Šiuo faktu ir grindžiama Gauso metodo idėja: *nuoseklus kintamųjų eliminavimas*. Pirmiausia, Gauso metodą paaiškinsime išsprendami keletą konkrečių TLS. Be to, paprastumo dėlei, tolesniuose samprotavimuose dažniausiai laikysime, kad $L = R$.

Priminsime, kad, pagal apibrėžimą, *TLS sprendinys yra visų TLS lygčių bendrasis sprendinys*. Tada, pažymėjus visos TLS sprendinių aibę raide S , o atskiros, sakykime, i -osios lygties sprendinių aibę raide S_i , galėsime parašyti:

$$S = S_1 \cap S_2 \cap \dots \cap S_m. \quad (4)$$

Prisiminę veiksmų su aibėmis savybes, dabar aptarsime du atskirus, bet mums labai svarbius tiesinių lygčių atvejus, pasitaikančius sprendžiant TLS Gauso metodu. Jei, taikant EP, viena iš TLS lygčių (tarkime, tai - i -oji sistemos lygtis) įgyja pavidalą:

$$0 \cdot x_1 + 0 \cdot x_2 + \dots + 0 \cdot x_n = b_i, \quad (L_i)$$

tai galimi du atvejai:

o) $b_i = 0,$

oo) $b_i \neq 0.$

Atveju o) lygtį (L_i) tenkina bet kuris rinkinys $(k_1, k_2, \dots, k_n)$, t.y. jos sprendinių aibė yra: $S_i = R^n$. Aibę R^n šiuo atveju galime laikyti *universalioja aibe* U . Betgi žinome, kad $(\forall A) A \cap U = A$. Todėl, o) atveju, (4) lygybė virsta tokia:

$$S = S_1 \cap S_2 \cap \dots \cap S_{i-1} \cap R^n \cap S_{i+1} \cap \dots \cap S_m = S_1 \cap S_2 \cap \dots \cap S_{i-1} \cap S_{i+1} \cap \dots \cap S_m.$$

Taigi, šiuo atveju lygtį (L_i) galime tiesiog atmesti (išbraukti iš sistemos).

Atveju oo), lygties (L_i) netenkina joks rinkinys $(k_1, k_2, \dots, k_n)$, t.y. jos sprendinių aibė yra tuščia ($S_i = \emptyset$). Tada iš (4) lygybės ir aibių sankirtos savybių išplaukia, kad $S = S_1 \cap \dots \cap \emptyset \cap \dots \cap S_m = \emptyset$.

Todėl oo) atveju TLS yra nesuderinta (neturi sprendinių).

Pirmas pavyzdys. Išsprendkime TLS ($m = 3, n = 4$).

$$\begin{cases} x_1 + 2x_2 + x_3 + x_4 = 1, \\ 2x_1 + 3x_2 + 3x_3 - 2x_4 = 0, \\ -x_1 - x_2 - 2x_3 + 3x_4 = 2. \end{cases}$$

Paprastai visa TLS neperrašinėjama. Pertvarkoma tik TLS išplėstoji matrica. Turėsime (vėl atkreipkite dėmesį į siūlomas santrumpas):

$$\left(\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 1 \\ 2 & 3 & 3 & -2 & 0 \\ -1 & -1 & -2 & 3 & 2 \end{array} \right) \xrightarrow[\sim]{-2L_1+L_2, L_1+L_2} \left(\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 1 \\ 0 & -1 & 1 & -4 & -2 \\ 0 & 1 & -1 & 4 & 3 \end{array} \right) \xrightarrow{L_2+L_3} \left(\begin{array}{cccc|c} \dots & & & & 1 \\ \dots & & & & -2 \\ 0 & 0 & 0 & 0 & 1 \end{array} \right).$$

Tad paskutinė lygtis įgavo 00) pavidalą. Atsakymas: TLS – **nesuderinta**.

Antras pavyzdys. Spręsimė TLS ($m=4, n=3$).

$$\begin{cases} x_1 + 2x_2 + x_3 = 1, \\ 2x_1 + 3x_2 + 3x_3 = 0, \\ 2x_2 + 2x_3 = 1, \\ -x_1 + 2x_2 + 3x_3 = 1. \end{cases}$$

Taikydami nurodytus EP, gausime:

$$\left(\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 1 \\ 2 & 3 & 3 & 0 & 0 \\ 0 & 2 & 2 & 1 & 1 \\ -1 & 2 & 3 & 1 & 1 \end{array} \right) \xrightarrow[\sim]{-2L_1+L_2, L_1+L_4} \left(\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 1 \\ 0 & -1 & 1 & -2 & -2 \\ 0 & 2 & 2 & 1 & 1 \\ 0 & 4 & 4 & 2 & 2 \end{array} \right) \xrightarrow[\sim]{2L_2+L_3, 4L_2+L_4} \left(\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 1 \\ 0 & -1 & 1 & -2 & -2 \\ 0 & 0 & 4 & -3 & -3 \\ 0 & 0 & 8 & -6 & -6 \end{array} \right) \xrightarrow{-2L_3+L_4} \left(\begin{array}{cccc|c} 1 & 2 & 1 & 1 & 1 \\ 0 & -1 & 1 & -2 & -2 \\ 0 & 0 & 4 & -3 & -3 \\ 0 & 0 & 0 & 0 & 0 \end{array} \right)$$

Atmetę ketvirtąją sistemos lygtį (nes ji yra 0) pavidalo), remdamiesi *ekvivalentumo teorema*, darome išvadą, kad pradinė sistema *ekvivalenti* tokiai:

$$\begin{cases} x_1 + 2x_2 + x_3 = 1, \\ -x_2 + x_3 = -2, \\ 4x_3 = -3. \end{cases}$$

Pastaroji sistema jau turi tokią formą (sakoma: TLS suvesta į *trikampę formą*), iš kurios lengva gauti atsakymą, tereikia, kylant iš apačios į viršų, nuosekliai apskaičiuoti x_3, x_2, x_1 . Gauname:

$$x_3 = -\frac{3}{4}; \quad -x_2 = -x_3 - 2 = \frac{3}{4} - 2 = -\frac{5}{4}; \quad x_1 = -2x_2 - x_3 + 1 = -\frac{10}{4} + \frac{3}{4} + 1 = -\frac{3}{4}.$$

Atsakymas. TLS turi vienintelį sprendinį: $\left(-\frac{3}{4}, \frac{5}{4}, -\frac{3}{4}\right)$.

Trečias pavyzdys. Reikia išspręsti TLS ($m=4, n=5$).

$$\begin{cases} -2x_1 - 2x_2 + 2x_3 + x_4 - x_5 = 2, \\ 2x_1 + 3x_2 - 3x_3 - 2x_4 + 2x_5 = -3, \\ x_2 - x_3 - x_4 + x_5 = -1, \\ -x_1 + 2x_2 + 2x_3 - 3x_4 = 2. \end{cases}$$

Visada yra tam tikras pasirinkimas, kokius konkrečius EP taikyti, norint *nuosekliai eliminuoti* kintamuosius. Nėra esminiai svarbi nei eliminavimo tvarka, nei pavidalas, ta prasme, kad eliminavimo “laiptukus” galime pradėti iš bet kurios sistemos vietos. *Tereikia tik, kad atitinkamas (pradinis) koeficientas būtų nelygus nuliui.* Žinoma, skaičiuoti *mums* patogiau, kai tas koeficientas yra lygus plius ar minus vienetui, ar bent jau yra nedidelis sveikasis skaičius, bet *kompiuteriui* šitai visiškai nesvarbu. Turėkite tai omenyje ir nesibaiminkite “negražių” skaičių!

Šį kartą, po elementariųjų pertvarkių $2L_4 + L_2, -2L_4 + L_1, L_1 \longleftrightarrow L_4$, išplėstąjį TLS matricą toliau keisime taip:

$$\begin{pmatrix} -1 & 2 & 2 & -3 & 0 & 2 \\ 0 & 7 & 1 & -8 & 2 & 1 \\ 0 & 1 & -1 & -1 & 1 & -1 \\ 0 & -6 & -2 & 7 & -1 & -2 \end{pmatrix} \xrightarrow{\substack{6L_3+L_4, \\ -7L_3+L_2, \\ L_2 \leftrightarrow L_3}} \begin{pmatrix} -1 & 2 & 2 & -3 & 0 & 2 \\ 0 & 1 & -1 & -1 & 1 & -1 \\ 0 & 0 & 8 & -1 & -5 & 8 \\ 0 & 0 & -8 & 1 & 5 & -8 \end{pmatrix} \xrightarrow{\substack{L_3+L_4, \\ išbraukti L_4}} \sim \begin{pmatrix} -1 & 2 & 2 & -3 & 0 & 2 \\ 0 & 1 & -1 & -1 & 1 & -1 \\ 0 & 0 & 8 & -1 & -5 & 8 \end{pmatrix}.$$

Matome, kad TLS, pritaikius jai Gauso metodą, susivedė į sistemą, kurios paskutinėje lygtyje dar liko *daugiau nei vienas kintamasis*. Sakoma: TLS suvesta į *trapecijų formą*.

Galima būtų pasakyti ir taip: pabaigus taikyti nuoseklaus eliminavimo metodą, lygčių liko mažiau, negu yra kintamųjų.

Toliau, samprotaujame taip: TLS pertvarkome, kad kairėje lygčių pusėje liktų tik pasirinkti *trys* kintamieji, kuriuos toliau vadinsime *baziniais*. Likusius kintamuosius perkeliame į dešinę lygčių pusę ir toliau vadinsime *laisvaisiais*. Baziniais kintamaisiais pasirinkę x_1, x_2, x_4 , gauname, kad pradinė TLS *ekvivalenti* tokiai:

$$\begin{cases} -x_1 + 2x_2 - 3x_4 = -2x_3 + 2, \\ x_2 - x_4 = x_3 - x_5 - 1, \\ -x_4 = -8x_3 + 5x_5 + 8. \end{cases} \quad (5)$$

Taip pasirinkome tik todėl, kad atsakymas būtų “gražesnis”. Nėra esminio skirtumo, kuriuos kintamuosius padarysime baziniais. Kita vertus, pabrėžtina, kad, bendru atveju, baziniais gali būti *ne visi* kintamieji. Per pratybas tuo įsitikinsime.

Belieka pastebėti, kad suteikus *laisviesiems* kintamiesiems x_3, x_5 *bet kurias* reikšmes, *bazinių* kintamųjų reikšmės vienareikšmiškai randamos iš sistemos (5). Pvz., pasirinkę

$x_3 = x_5 = 0$, lengvai randame, kad $x_1 = 4$, $x_2 = -9$, $x_4 = -8$. Sakoma, kad rinkinys $(4, -9, 0, -8, 0)$ yra (5) sistemos, o kartu ir pradinės TLS, *atskirasis* sprendinys.

Jei norime užrašyti *bendrąją* pradinės TLS sprendinį, tai, pasinaudoję (5) sistema, bazinius kintamuosius x_1, x_2, x_4 išreiškiame laisvaisiais x_3, x_5 . Gauname:

$$x_4 = 8x_3 - 5x_5 - 8; x_2 = 9x_3 - 6x_5 - 9; x_1 = -4x_3 + 3x_5 + 4.$$

Atsakymas. TLS yra suderinta ir neapibrėžta, jos bendrasis sprendinys yra:

$$(-4x_3 + 3x_5 + 4, 9x_3 - 6x_5 - 9, x_3, 8x_3 - 5x_5 - 8, x_5). \text{ Čia: } x_3, x_5 \in \mathbb{R}.$$

Pasirodo, kad šiais pavyzdžiais aptartos visos galimos situacijos. Tiksliau, yra teisinga tokia teorema.

Teorema. TLS (2) su realiaisiais koeficientais arba neturi sprendinių, arba gali būti suvesta į vieną iš dviejų pavidalų: trikampį ar trapecinį. Pirmuoju atveju TLS turi vienintelį sprendinį (sakome: sistema yra suderinta ir apibrėžta), antruoju – be galo daug sprendinių (sakome: sistema yra suderinta ir neapibrėžta).

Pagrindinė įrodymo idėja *schematiškai* yra tokia: jeigu $a_{11} \neq 0$, tai po EP

$$\left(\begin{array}{cccccc|c} a_{11} & o & o & o & \dots & o & b_1 \\ a_{12} & o & o & o & \dots & o & b_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{m1} & o & o & o & o & o & b_m \end{array} \right) \xrightarrow{a_{11}^{-1}a_{12}L_1+L_2} \left(\begin{array}{cccccc|c} a_{11} & o & o & o & \dots & o & b_1 \\ 0 & a'_{22} & o' & o' & \dots & o' & b'_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ o & o & o & o & o & o & o \end{array} \right)$$

gautoji sistema *lieka ekvivalenti pradinei*. Tačiau šios pastarosios TLS antrojoje lygtyje neliko kintamojo x_1 ! Tai ir yra pirmasis eliminavimo žingsnis.

Čia koeficientus, kurie pertvarkymo eigoje nesikeitė, žymime simboliu “o”, vieną kart perskaičiuotus, – simboliu “o'”, dukart perskaičiuotus “o''” ir t.t.

Kas toliau? Toliau eliminavimo žingsnis taikomas *visoms kitoms lygtims, išskyrus pirmąją*. Jei pakeliui gauname o) pavidalo lygtį, - *ją išbraukiame*; jei, taip pertvarkant, viena iš TLS lygčių įgyja oo) pavidalą, tai darome išvadą, kad pradinė TLS *nesuderinta* ir *sprendimą nutraukiame*.

Pastaba. Jeigu $a_{11} = 0$, tai pakanka sukeisti lygtis, ar kintamuosius vietomis taip, kad kairiajame viršutiniame kampe atsirastų nelygus nuliui koeficientas.

Jeigu TLS turėjo m lygčių, tai visose lygtyse, išskyrus pirmąją, eliminavus x_1 , lygčių skaičius galėjo sumažėti, o pati sistema arba įgijo pavidalą

$$\left(\begin{array}{cccccc|c} a_{11} & o & o & o & \dots & o & b_1 \\ 0 & a'_{22} & o' & o' & \dots & o' & b'_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & a'_{r2} & o' & o' & o' & o' & b'_r \end{array} \right)$$

arba nustatėme jos nesuderintumą. Čia $r \leq m$.

Tarkime, toliau, kad $a'_{22} \neq 0$. (Jei ši sąlyga nėra išpildyta, keičiame lygtis ar kintamuosius vietomis.) Tada, panaudodami pastarojo TLS pavidalo *antrąją lygtį*, EP pagalba pasieksime, kad visose lygtyse, išskyrus pirmąją ir antrąją, neliks kintamojo x_2 ir TLS arba suvesime į pavidalą

$$\left(\begin{array}{cccccc|c} a_{11} & o & o & o & \dots & o & b_1 \\ 0 & a'_{22} & o' & o' & \dots & o' & b'_2 \\ 0 & 0 & a''_{33} & o'' & \dots & o'' & b''_2 \\ 0 & 0 & a''_{43} & o'' & \dots & o'' & b''_3 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & a''_{d3} & o'' & \dots & o'' & b''_d \end{array} \right),$$

arba pakeliui būsime gavę oo) pavidalo lygtį. Čia $d \leq r \leq m$, o kintamųjų numeracija gali būti pasikeitusi.

Šį procesą tęsiame ir toliau: laikydami, kad $a''_{33} \neq 0$, iš visų lygčių, pradedant ketvirtąją, eliminuosime kintamąjį x_3 , vėliau, panašiu būdu, - x_4 ir t.t., kol nesibaigs sistemos lygtys, arba, kol nesigaus oo) pavidalo lygtis. Pabaigoje gausime tokią, pradinei TLS ekvivalenčią, sistemą:

$$\left(\begin{array}{cccccc|c} a_{11} & o & \dots & o & o & \dots & o & b_1 \\ 0 & a'_{22} & \dots & o' & o' & \dots & o' & b'_2 \\ 0 & 0 & \dots & o'' & o'' & \dots & o'' & b''_3 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a^{(k-2)}_{k-1,k-1} & o^{(k-2)} & \dots & o^{(k-2)} & o^{(k-2)} \\ 0 & 0 & \dots & 0 & a^{(k-1)}_{kk} & \dots & o^{(k-1)} & o^{(k-1)} \end{array} \right).$$

Čia $(\forall i) a^{(i-1)}_{ii} \neq 0$ ir $k \leq m$. Be to, pastebėkime, kad EP taikymo eigoje, gal būt, teko sukeisti kintamųjų numeraciją. Tokiu atveju, užrašant atsakymą, sukeitimus reikia turėti omenyje.

Dabar galimi du atvejai:

- $k = n$, t.y. šitaip pertvarkytos sistemos paskutinėje lygtyje yra tik vienas (tarkime n – tasis) kintamasis, arba kitaip: sistemoje lygčių liko tiek, kiek ir kintamųjų. Tada sakoma, kad sistema suvesta į *trikampį* pavidalą. Nesunku suvokti, kad sąlygos $(\forall i) a^{(i-1)}_{ii} \neq 0$ įgalina vienareikšmiškai rasti *vienintelį* sistemos sprendinį.

b) $k < n$. Tada paskutinėje lygtyje yra likę daugiau nei vienas kintamasis. Arba: sistemoje lygčių liko *mažiau*, negu yra kintamųjų. Sakoma, kad sistema suvesta į *trapecinį* pavidalą. Pirmuosius k kintamųjų vadiname *baziniais* (pagrindiniais), likusius - *laisvais*. Laisviesiems kintamiesiems suteikus bet kokias reikšmes, sistema tampa *trikāmpe* TLS su kintamaisiais $x_1, x_2, \dots, x_k$. Tad kiekvienam laisvųjų kintamųjų parinkimui atitinka vienintelis pradinės TLS sprendinys. Darome išvadą: šiuo atveju TLS turi *be galo daug sprendinių*, t.y. ji yra suderinta ir neapibrėžta.

Kyla klausimas, ar tokiu metodu tikrai gaunami *visi* pradinės TLS sprendiniai? Lengva įsitikinti, kad *taip*. Tarus, kad $(k_1, k_2, \dots, k_n)$ yra bet koks pradinės sistemos sprendinys ir atlikus tuos pačius EP, nesunkiai parodoma, kad jis tegali būti gautas tik vienu iš $a-b$) būdų. QED.

Pastaba. Jei lauko L , kuriam priklauso TLS koeficientai, charakteristika yra m , $m \in N$, tai bazinė aibė turi tik m skirtingų elementų. Tada trapecinės sistemos atveju sprendinių yra *daugiau negu vienas*, bet *ne be galo daug*. Tiksliau: sprendinių yra m^{n-k} . Čia k – bazinių kintamųjų skaičius.

Išvada. THLS, kurioje $m < n$, yra suderinta ir neapibrėžta. Kitaip sakant, *trapecinės formos THLS turi ir nenulinių sprendinių*.

Paskaita 2 – 02

Kvadratinės matricos determinantas. Kramerio taisyklė

TLS, TLS sprendiniai, TLS matrica. EP, ekvivalentumo teorema. TLS sprendimas Gauso metodu. Trikampio ir trapecijos formos TLS. THLS, jų suderintumas.

Determinantai. Kai $n = 2, 3$, tai kvadratinei matricai A galima vienareikšmiškai priskirti *skaičių* (paprastai žymimą $|A|$), vadinamą jos *determinatu*.

Būtent: kai $n = 2$, tai:

$$A \longrightarrow |A| = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} := a_{11}a_{22} - a_{12}a_{21},$$

o kai $n = 3$, tai:

$$A \longrightarrow |A| = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} :=$$

$$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}.$$

Šiais abiem atvejais įrodoma tokia šveicarų matematiko *G. Cramer* (1704-1752) vardu pavadinta teorema. Kai $n = 3$, ji formuluojama taip:

Kramerio teorema. Jei TLS koeficientų matricos A determinantas $|A|$ nelygus nuliui, tai sistema turi vienintelį sprendinį (k_1, k_2, k_3) randamą iš formulių:

$$k_i = \frac{|A_i|}{|A|}; i = 1, 2, 3.$$

Čia A_i yra matrica, gauta pakeitus i -ąją matricos A stulpelį laisvųjų narių stulpeliu.

Įrodymą tuo tarpu praleidžiame. Teoremą įrodysime vėliau, bendresniu atveju.

Pasirodo, kad determinanto sąvoką bei Kramerio teoremą galima apibendrinti ir bet kokiam natūraliajam n .

Tarkime, turime n – osios eilės kvadratinę matricą

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

su elementais iš realiųjų skaičių lauko R (beje, vietoje R gal būti ir laukas K , ir apskritai, – bet koks laukas). Sudarykime jos elementų sandaugą

$$a_{1k_1} a_{2k_2} \dots a_{nk_n}, \quad (1)$$

vadovaudamiesi principu: iš kiekvienos eilutės ir kiekvienos stulpelio imame lygiai po vieną elementą. T.y. antrųjų indeksų junginys $k_1, k_2, \dots, k_n$ yra vienas iš kėlinių, sudarytų iš skaičių $1, 2, \dots, n-1, n$. Kadangi kėlinių iš n elementų yra $n!$, tai tiek galima sudaryti ir (1) pavidalo sandaugų iš duotosios kvadratinės matricos A elementų.

Inversijos ir transpozicijos. Dabar (1) sandaugai specialiu būdu priskirsime ženklą. Tam reikės *inversijos* (lietuviškai: *netvarkos*) kėlinyje iš elementų $1, 2, \dots, n-1, n$ sąvokos.

Ap. Sakysime, kad du indeksai k_i ir k_j kokiame nors kėlinyje $k_1, \dots, k_i, \dots, k_j, \dots, k_n$ sudaro inversiją (netvarką), jei $k_i > k_j$.

Pvz., kėlinyje $5, 1, 2, 3, 4$ indeksų poros $(5, 1); (5, 2); (5, 3)$ ir $(5, 4)$ sudaro netvarkas, o pora $(1, 4)$ netvarkos nesudaro.

Tarkime, kad kėlinyje $k_1, k_2, \dots, k_n$ iš viso yra s netvarkų.

Ap. Kai s , – lyginis skaičius tai (1) sandaugai priskirsime ženklą “+”, o kai nelyginis, – tai ženklą “-”. Patį kėlinį pirmuoju atveju vadinsime lyginiu, antruoju – nelyginiu.

Pvz., kėlinyje $5, 1, 2, 3, 4$ iš viso yra 4 netvarkos, todėl jis vadintinas lyginiu, o atitinkamam (1) pavidalo skaičiui $a_{15}a_{21}a_{32}a_{43}a_{54}$, sudarytam iš penktos eilės kvadratinės matricos elementų, yra priskirtinas ženklas “plius”.

Ap. Dviejų indeksų sukeitimą vietomis kėlinyje vadinsime transpozicija.

Pavyzdžiui, iš kėlinio $5, 1, 2, 3, 4$, indeksų 1 ir 3 transpozicijos pagalba gausime kėlinį $5, 3, 2, 1, 4$.

Patikrinkime, koks yra naujai gauto kėlinio lyginumas (lygiškumas): indeksas 5 sudaro 4 netvarkas, 3 sudaro dvi netvarkas, 2 – vieną, o indeksai 1 ir 4 naujų netvarkų nesudaro. Tad viso kėlinyje susidarė $4 + 2 + 1 = 7$ netvarkos. Taigi, lyginis kėlinys virto nelyginiu. Pasirodo, kad taip yra kas kartą, kai tik atliekama viena transpozicija.

1 Lema. Kiekviena transpozicija keičia kėlinio lyginumą į priešingą.

Įrodymo planas. 1. Kai sukeičiamieji indeksai k_i ir k_j yra greta – lemos tvirtinimas akivaizdus. 2. Kai tarp indeksų k_i, k_j yra s kitų indeksų, tai k_i ir k_j sukeisime vietomis $2s + 1$ kartą sukeisdami greta stovinčius indeksus, todėl, pagal pirmą įrodymo dalį, kėlinio lyginumas pasikeis.

2 Lema. Tarp visų $n!$ kėlinių lygiai pusė yra lyginių, kita pusė, – nelyginių.

Įrodymas. MIP pagalba, savarankiškai.

Dabar galime suformuluoti svarbų **kvadratinės matricos determinanto** apibrėžimą.

Ap. Algebrinę sumą visų $n!$ (1) pavidalo sandaugų, vadinsime kvadratinės matricos A determinantu, žymėsime $|A|$ ir rašysime:

$$A \longrightarrow |A|, \quad |A| = \sum (-1)^s a_{1k_1} a_{2k_2} \dots a_{nk_n}.$$

Sandauga $a_{1k_1} a_{2k_2} \dots a_{nk_n}$ toliau vadinama matricos A determinanto nariu.

Svarbu suprasti, kad matrica yra skaičių (lauko elementų) lentelė, o jos determinantas – konkretus skaičius (bendriau: lauko elementas), gaunamas apskaičiavus $n!$ (1) pavidalo narių, paimtų su atitinkamais ženklais, sumą.

Be to, atsiminkite, kad *determinantą turi tik kvadratinės matricos.*

Pagal šį apibrėžimą, trečios eilės kvadratinės matricos determinantas yra sudarytas iš $3! = 6$ narių. Pagal antrą lemą, trys iš jų yra turi ženklą “plius”, kiti trys, – “minus”. Pvz., narys $a_{13} a_{22} a_{31}$ imamas su minusu, nes jo antrųjų indeksų kėlinyje 3, 2, 1 yra nelyginis skaičius (t.y., 3) inversijų. Prisiminę paragrafo pradžioje pateiktą trečios eilės kvadratinės matricos determinanto apibrėžimą, matome, kad jis visiškai atitinka čia suformuluotąjį.

Keitiniai. Atkreipiu skaitytojų dėmesį į tai, kad (1) sandaugoje pirmuosius indeksus (paprastumo dėlei) surašėme didėjimo tvarka, todėl jų kėlinys inversijų visai neturi. Užtat mes jį lyg ir “pamirštame”. Apibrėžiant kvadratinės matricos determinantą, kartais elgiamasi kiek kitaip: imami domėn abu kėliniai, – ir pirmųjų indeksų, ir antrųjų. Tada su matricos determinanto nariu

$$a_{i_1 j_1} a_{i_2 j_2} \dots a_{i_n j_n}, \quad (2)$$

kuriame jau ir pirmieji indeksai eina nebūtinai eilės tvarka, siejama kėlinių pora

$$\begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix},$$

kuri vadinama **n -ojo laipsnio keitiniu**.

Keitinį patogiu suprasti, kaip atvaizdį $(i_k \longrightarrow j_k)$, kuris kėlinį $i_1, i_2, \dots, i_n$ keičia kėliniu $j_1, j_2, \dots, j_n$. Tarkime kėlinyje $i_1, i_2, \dots, i_n$ yra u netvarkų, o kėlinyje $j_1, j_2, \dots, j_n$ – v netvarkų. Tada nariui (2) priskiriamas ženklas $(-1)^{u+v}$, o matricos A determinantu vadinama suma

$$\sum (-1)^{u+v} a_{i_1 j_1} a_{i_2 j_2} \dots a_{i_n j_n},$$

kurioje, kaip ir anksčiau, yra $n!$ dėmenų (determinanto narių).

Keitiniai turi daug įdomių savybių. Visų n -ojo laipsnio keitinių aibėje K_n apibrėžus algebrinę keitinių *daugybės* operaciją, galima įrodyti, kad algebrinė struktūra $(K_n, \cdot)$ yra nekomutatyvi grupė. Plačiau su keitiniais ir jų savybėmis susipažinsime per pratimus.

Kaip matome, mūsų pasirinktas determinanto apibrėžimas nemažina bendrumo, o tik supaprastina situaciją, pakeičiant bendrą keitinio

$$\begin{pmatrix} i_1 & i_2 & \dots & i_n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$$

pavidalą jam ekvivalenčiu (atvaizdžio prasme) *kanoniniu* pavidalu,

$$\begin{pmatrix} 1 & 2 & \dots & n \\ k_1 & k_2 & \dots & k_n \end{pmatrix},$$

panaudojant keitinio stulpelių sukeitimą vietomis (transpoziciją). Akivaizdu, kad tokia transpozicija minėto atvaizdžio nekeičia. Svarbu dar ir tai, kad tokia transpozicija nekeičia ir keitinio kėlinių *sumarinio lyginumo*, nes pagal pirmąją lemą, viena keitinio stulpelių transpozicija abiejų keitinio kėlinių lyginumą pakeičia į priešingą. Atskiru atveju, kai kėlinys $i_1, i_2, \dots, i_n$ transpozicijų pagalba virsta kėliniu $1, 2, \dots, n$, atsiduriame jau aptartoje situacijoje, kai nario (2) ženklą lemia tik antrųjų indeksų (apatinio) kėlinio $k_1, k_2, \dots, k_n$ inversijų skaičiaus s lyginumas, nes $0 + s = s$. Tokio bendresnio determinanto sąvokos supratimo prireikia, kai norime įrodyti matricos *determinanto savybes* (DS).

Determinanto savybės. Kadangi n -osios eilės kvadratinės matricos determinantas, pagal apibrėžimą, yra suma iš $n!$ dėmenų (narių), tai, kai $n \geq 4$, tuos narius darosi painu išrašyti: kai $n = 4$, jų yra jau 24, o, kai $n = 5$, – net 120. Todėl skaičiuoti matricos determinantą (ypač, kai $n > 3$), betarpiškai pagal apibrėžimą, yra nepatogu. Skaičiuojant determinantus, labai praverčia lengvai įrodomos jų savybės, kurias dabar ir išvardinsime.

1. *Matricos ir transponuotos matricos determinantai yra lygūs.*
2. *Jei matricoje yra nulinė eilutė (ar stulpelis), tai matricos determinantas lygus nuliui.*
3. *Jei dvi matricos eilutės (stulpeliai) sukeisime vietomis, tai jos determinantas tik pakeis savo ženklą.*
4. *Jei matricoje yra dvi vienodos eilutės (stulpeliai), tai jos determinantas lygus nuliui.*
5. *Pastovų eilutės (stulpelio) daugiklį galima iškelti prieš determinanto ženklą.*
6. *Jei viena matricos eilutė sudaryta iš sumų $a_i + b_i$, $i = 1 \div n$, tai determinantas lygus dviejų determinantų sumai: pirmajame atitinkama eilutė yra $a_1, a_2, \dots, a_n$, antrajame, – $b_1, b_2, \dots, b_n$.*
7. *Matricos eilutę (stulpelį) padauginus iš skaičiaus ir panariui pridėjus prie kitos eilutės (stulpelio), – matricos determinantas nesikeičia.*

8. Jei matricos eilutė (stulpelis) yra kitų eilučių (stulpelių) tiesinis darinys, tai tokios matricos determinantas lygus nuliui.

Savybių neįrodinėsime. Kai kurios iš jų yra paprasta apibrėžimo išvada. Pvz., - antroji, penktoji, šeštoji. Pirmoji savybė išplaukia iš to, kad po transponavimo narys $a_{1k_1} a_{2k_2} \dots a_{nk_n}$ išlieka naujos matricos determinanto nariu, o jo ženklą apsprendžiantis suminis inversijų skaičius keitinyje

$$\begin{pmatrix} k_1 & k_2 & \dots & k_n \\ 1 & 2 & \dots & n \end{pmatrix},$$

yra lygus $s + 0$, t.y. lieka nepakitęs.

Minorai ir adjunktai. Laplaso teorema

Kad bendru atveju įrodytume Kramerio teoremą, turime susipažinti su dar viena – matricos k -osios eilės *minoru* sąvoka.

Ap. Jei $m \times n$ eilės matricoje $A = (a_{ij})$ laisvai pasirinkime k eilučių ir k stulpelių (aišku, $k \leq \min(m, n)$), tai jų susikirtime esančios kvadratinės k -osios eilės matricos determinantą vadinsime matricos A k -osios eilės **minoru**. Žymima: M_k .

Atskiru atveju, kai $k = 1$, (pirmosios eilės) minoras tiesiog sutampa su matricos elementu, esančiu pasirinktųjų eilutės ir stulpelio sankirtoje.

Pavyzdžiui, matricoje

$$A = \begin{pmatrix} 1 & -2 & 0 & 3 & 5 \\ 9 & 0 & -1 & 7 & 4 \\ 1 & 1 & 2 & 2 & 6 \\ 0 & -1 & 4 & 0 & 5 \end{pmatrix}$$

pasirinkę antrą, trečią ir ketvirtą eilutes, bei pirmą, ketvirtą ir penktą stulpelius, gausime tokį šios matricos 3 – osios eilės minorą:

$$M_3 =: M_{234,145} = \begin{vmatrix} 9 & 7 & 4 \\ 1 & 2 & 6 \\ 0 & 0 & 5 \end{vmatrix} = 55.$$

Kai matrica A yra kvadratinė, tai pasirinkus po k eilučių ir stulpelių, lieka nepasirinkta po $n - k$ eilučių ir stulpelių, iš kurių sudarytos $n - k$ -osios eilės matricos determinantas vadinamas minorui M_k *papildomu minoru* ir žymimas M'_k .

Tarkime pasirinktųjų eilučių numeriai yra $i_1, i_2, \dots, i_k$, o stulpelių – $j_1, j_2, \dots, j_k$. Pažymėkime: $s_M = i_1 + \dots + i_k + j_1 + \dots + j_k$.

Ap. Dydi $(-1)^{s_M} M'_k := A_k$ vadiname *minoru* M_k **adjunktu**.

Pvz., kai turime tokią *ketvirtosios eilės* kvadratinę matricą:

$$A = \begin{pmatrix} 1 & 2 & 1 & 1 \\ 2 & 3 & 3 & 2 \\ 0 & 0 & 5 & 1 \\ -1 & 2 & 2 & 7 \end{pmatrix},$$

tai vienas jos *antrosios eilės* minorų yra $M_{23,34} = \begin{vmatrix} 3 & 2 \\ 5 & 1 \end{vmatrix}$, jam *papildomas minoras* yra

$$M'_{23,34} = \begin{vmatrix} 1 & 2 \\ -1 & 2 \end{vmatrix} = 4, \quad s_M = 2 + 3 + 3 + 4 = 12, \text{ o dydis } A_{23,34} := (-1)^{12} M'_{23,34} = 4 \text{ ir yra}$$

minoru $M_{23,34}$ adjunktas. Tad: *minoru adjunktas irgi yra skaičius, gaunamas pagal apibrėžime nurodytą taisyklę.*

Lema. *Matricos minoru M_k ir jo adjunkto $A_k = (-1)^{s_M} M'_k$ sandauga yra lygi matricos A determinanto $k!(n-k)!$ narių, paimtų su tais ženklais, su kuriais jie įeina į determinantą, sumai.*

Įr. 1. Tarkime minoras M_k yra pirmosiose k eilučių ir stulpelių. Tada jo adjunktas $A_k = (-1)^{s_M} M'_k$ sutampa su papildomu minoru M'_k , sudarytu iš likusių $n-k$ eilučių ir stulpelių, nes $s_M = 2(1 + \dots + k)$. Jei bendrasis minoru M_k narys yra:

$$(-1)^{s_1} a_{1\alpha_1} a_{2\alpha_2} \dots a_{k\alpha_k},$$

o jo papildomo minoru, atitinkamai:

$$(-1)^{s_2} a_{k+1,\beta_{k+1}} a_{k+2,\beta_{k+2}} \dots a_{n,\beta_n},$$

tai jų sandauga

$$(-1)^{s_1+s_2} a_{1\alpha_1} a_{2\alpha_2} \dots a_{k\alpha_k} \cdot a_{k+1,\beta_{k+1}} a_{k+2,\beta_{k+2}} \dots a_{n,\beta_n}$$

akivaizdžiai turi lygiai po vieną atstovą iš kiekvienos matricos A eilutės ir stulpelio. Be to, kiekvienas iš indeksų α_i , $i = 1 \div k$ yra mažesnis už bet kurį iš β_j , $j = (k+1) \div n$, todėl inversijų skaičius kėlinyje $\alpha_1, \dots, \alpha_k, \beta_{k+1}, \dots, \beta_n$ irgi lygus $s_1 + s_2$. Kadangi minoras M_k turi $k!$ narių, o papildomas minoras M'_k - $(n-k)!$ narių, tai, pagal kombinatorinę daugybos taisyklę, sandauga $M_k M'_k$ iš viso duos $k!(n-k)!$ matricos A determinanto narių su atitinkamais ženklais.

2. Kai matricos A minoras M_k yra eilutėse ir stulpeliuose su numeriais $i_1, i_2, \dots, i_k$ ir $j_1, j_2, \dots, j_k$, tai, atlikę $i_1 - 1 + i_2 - 2 + \dots + i_k - k$ eilučių ir $j_1 - 1 + j_2 - 2 + \dots + j_k - k$ stulpelių sukeitimų vietomis, matricos A determinantą suvesime į jau aptartą atvejį. Šie sukeitimai tik

$i_1 + i_2 + \dots + i_k + j_1 + j_2 + \dots + j_k - 2(1 + 2 + \dots + k) = s_M - k(k+1)$ kartų pakeis matricos determinanto ženklą. Bet, $(-1)^{s_M - k(k+1)} M'_k = (-1)^{s_M} M'_k = A_k$. QED.

Laplaso teorema (P.S. de Laplace, 1749 – 1827, prancūzų matematikas). *Matricos determinantas yra lygus visų bet kuriose k eilučių esančių minorų ir jų adjunktų sandaugų sumai.*

Irodysime šią teoremą tik atskiru atveju, kai $k = 1$. Tada pasirinkus, pavyzdžiui, i – tąją eilutę, jos elementai a_{ij} , $j = 1 \div n$ ir bus teoremoje minimi minorai. Pažymėjus jų adjunktus A_{ij} , $j = 1 \div n$, teoremos tvirtinimą galėsime užrašyti taip:

$$|A| = a_{i1}A_{i1} + a_{i2}A_{i2} + \dots + a_{in}A_{in}. \quad (3)$$

Pagal lemą apie minoro ir adjunkto sandaugą, kiekvienas dėmuo $a_{ij}A_{ij}$, $j = 1 \div n$ yra lygus $1! \cdot (n-1)!$ determinanto $|A|$ narių. Tačiau atskirose sandaugose gauti nariai skiriasi atstovu iš i – tosios eilutės, todėl viso gauname $n \cdot (n-1)! = n!$ skirtingų determinanto narių, t.y. *visus narius*. QED.

Dvi svarbios išvados iš Laplaso teoremos

1. Teorema apie matricių sandaugos determinantą. *Kvadratinių matricių sandaugos determinantas yra lygus dauginamųjų matricių determinantų sandaugai.*

Irodymui sukonstruojame pagalbinį $2n$ – osios eilės determinantą:

$$\Delta = \begin{vmatrix} A & O_n \\ -E_n & B \end{vmatrix}.$$

Jo kairiajame viršutiniame kampe yra matricos $A = (a_{ij})$ elementai, dešiniajame apatiniame – matricos $B = (b_{ij})$ elementai, O_n simbolizuoja n – osios eilės kvadratinę nulinę *matricę*, $(-E)$ schematiškai reiškia vienetinei matriciai priešingąją matricę. Išskleidę determinantą Δ pagal pirmąsias n eilučių, gauname:

$$\Delta = |A| \cdot (-1)^{n(n+1)} |B| = |A| \cdot |B|.$$

Determinanto Δ stulpeliams taikydami atitinkamus EP, vietoje matricos B , galime parašyti matricę O_n . Tada pastarosios vietoje atsiras matricos $C := (c_{ij}) = A \cdot B$ elementai. T.y. gausime:

$$\Delta = \begin{vmatrix} A & C \\ -E_n & O_n \end{vmatrix}.$$

Dar kartą skleidami determinantą Δ , tik dabar jau pagal paskutinius n stulpelių, turėsime:

$$\Delta = |C| \cdot (-1)^{1+2+\dots+n+(n+1)+\dots+2n} |-E| = |C| \cdot (-1)^{2n^2+2n} = |C|.$$

$$|A| \cdot k_1 = |A_1|.$$

Kadangi, pagal teoremos sąlygą, $|A| \neq 0$, tai iš pastarosios lygybės skaičius k_1 randamas *vienareikšmiškai*:

$$k_1 = \frac{|A_1|}{|A|}.$$

Analogiškai įsitikiname kad ir kiti k_i , $i = 2, 3, \dots, n$ vienareikšmiškai randami formulių (4) pagalba. Taigi, jeigu sprendinys egzistuoja, tai jis yra *vienintelis* ir randamas iš formulių (4). Lieka patikrinti, ar duotoji TLS yra tikrai suderinta. Tuo tikslu skaičius k_i , $i = 1, 2, \dots, n$ įstatykime į bet kurią, pavyzdžiui, i -ąją sistemos lygtį. Naudodami sutrumpintus žymenis, galime parašyti:

$$\sum_{j=1}^n a_{ij} \frac{|A_j|}{|A|} = \frac{1}{|A|} \sum_{j=1}^n a_{ij} \sum_{l=1}^n b_l A_{lj} = \frac{1}{|A|} \sum_{j=1}^n \sum_{l=1}^n a_{ij} b_l A_{lj} = \frac{1}{|A|} \sum_{l=1}^n b_l \sum_{j=1}^n a_{ij} A_{lj} = \frac{1}{|A|} \cdot b_i \cdot |A| = b_i.$$

Kramerio teorema įrodyta.

Išvada. THLS, kurioje $m = n$, tada ir tik tada turi nenulinių sprendinių, kai $|A| = 0$.

Pavyzdžiui, išspręskime TLS (čia: $n = 4$):

$$\begin{cases} x_1 + 2x_2 + x_3 + x_4 = 1, \\ 2x_1 + 3x_2 + 3x_3 + 2x_4 = 0, \\ \qquad \qquad \qquad 5x_3 + x_4 = 0, \\ -x_1 + 2x_2 + 2x_3 + 7x_4 = 0. \end{cases}$$

Taikydami Laplaso teoremą, apskaičiuosime šios TLS matricos A determinantą ir stengsimės skaičiuoti kuo racionaliau. Skleidimui ne tik pasirinksimė *trečiąją* eilutę ($i = 3$, nes joje yra nulių!), bet prieš tai ją dar ir pertvarkysime, panaudodami DS. O, būtent: *ketvirtąją* stulpelį padauginsime iš skaičiaus (-5) ir *panariui pridėsime prie trečiojo*. Matrica A pasikeis į tokia:

$$B = \begin{pmatrix} 1 & 2 & -4 & 1 \\ 2 & 3 & -7 & 2 \\ 0 & 0 & 0 & 1 \\ -1 & 2 & -33 & 7 \end{pmatrix}.$$

Remiantis išvardintomis DS, konstatuojame, kad $|A| = |B|$. Bet, pagal, Laplaso teoremą:

$$|A| = |B| = 0 + 0 + 0 + 1 \cdot (-1)^{3+4} \cdot \begin{vmatrix} 1 & 2 & -4 \\ 2 & 3 & -7 \\ -1 & 2 & -33 \end{vmatrix}.$$

Šį determinantą jau nesunku apskaičiuoti tiesiogiai, pagal aukščiau pateiktą apibrėžimą. Tačiau mes dar pratęsimė DS taikymą toliau. Turime (čia veiksmus su eilutėmis aprašėme santrumpomis):

$$|A| = - \begin{vmatrix} 1 & 2 & -4 \\ 2 & 3 & -7 \\ -1 & 2 & -33 \end{vmatrix} \stackrel{-2L_1+L_2,}{L_1+L_3} = - \begin{vmatrix} 1 & 1 & -4 \\ 0 & -1 & 1 \\ 0 & 4 & -37 \end{vmatrix} = -1 \cdot (-1)^{1+1} \cdot \begin{vmatrix} -1 & 1 \\ 3 & -37 \end{vmatrix} = -(37 - 4) = -33.$$

Kadangi TLS matricos determinantas nelygus nuliui, tai TLS turi (*vienintelį*) sprendinį. Toliau, apskaičiuokime, pavyzdžiui, $|A_4|$:

$$|A_4| := \begin{vmatrix} 1 & 2 & 1 & 1 \\ 2 & 3 & 3 & 0 \\ 0 & 0 & 5 & 0 \\ -1 & 2 & 2 & 0 \end{vmatrix} = (-1)^{1+4} \begin{vmatrix} 2 & 3 & 3 \\ 0 & 0 & 5 \\ -1 & 2 & 2 \end{vmatrix} = -(-1)^{2+3} \cdot 5 \cdot \begin{vmatrix} 2 & 3 \\ -1 & 2 \end{vmatrix} = 5(4 + 3) = 35.$$

Panašiai: $|A_1| = 85$, $|A_2| = -73$, $|A_3| = -7$. Tad vienintelis duotosios TLS sprendinys yra skaičių rinkinys: $\left(-\frac{85}{33}, \frac{73}{33}, \frac{7}{33}, -\frac{35}{33}\right)$.

Paskaita 2 – 03

Matricų algebra

Determinantai, jų savybės, Laplaso, Kramerio teoremos.

Taikant tiesinės algebros metodus praktikoje, tenka operuoti didelėmis duomenų bazėmis, nuolat spręsti patogaus ir saugaus tų duomenų laikymo, koregavimo ir tvarkymo uždavinius. Duomenys (kompiuterių atmintyje) dažniausiai kaupiami *matricų* pavidalu.

Matricų veiksmai. Keli apibrėžimai:

Ap.1. Dvi vienodos eilės $m \times n$ matricas $A = (a_{ij})$ ir $B = (b_{ij})$ vadiname **lygiomis**, jeigu $(\forall i, j) a_{ij} = b_{ij}$. Rašome: $A = B$.

Ap.2. Dviejų eilės $m \times n$ matricų $A = (a_{ij})$ ir $B = (b_{ij})$ **suma** vadiname tokią eilės $m \times n$ matricą $C = (c_{ij})$, kurioje $(\forall i, j) c_{ij} := a_{ij} + b_{ij}$. Rašome: $C = A + B$.

Ap.3. Matricos $A = (a_{ij})$ ir lauko elemento (skaičiaus) k **sandauga** vadiname matricą $D = (d_{ij})$, kurioje $(\forall i, j) d_{ij} := k \cdot a_{ij}$. Rašome: $D = kA$.

Ap.4. Dviejų matricų: $A = (a_{ij})$, $m \times s$ ir $B = (b_{ij})$, $s \times n$ **sandauga** vadiname eilės $m \times n$ matricą $\tilde{C} = (\tilde{c}_{ij})$, kurioje $(\forall i, j) \tilde{c}_{ij} := a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{is}b_{sj}$. Rašome: $\tilde{C} = AB$.

Pavyzdžiai. Kai

$$A = \begin{pmatrix} 1 & -2 & 2 & 5 & 0 \\ 0 & -4 & 1 & 3 & 1 \\ -2 & 0 & 3 & -1 & 7 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -3 & 1 & 1 & 0 \\ 2 & -4 & 3 & 3 & 1 \\ -2 & 0 & 3 & -1 & 6 \end{pmatrix},$$

tai

$$A + B = \begin{pmatrix} 1 & -5 & 3 & 6 & 0 \\ 2 & -8 & 4 & 6 & 2 \\ -4 & 0 & 6 & -2 & 13 \end{pmatrix}, \quad -3A = \begin{pmatrix} -3 & 6 & -6 & -15 & 0 \\ 0 & 12 & -3 & -9 & -3 \\ 6 & 0 & -9 & 3 & -21 \end{pmatrix}.$$

$$\text{Kai } A = \begin{pmatrix} 1 & -2 & 1 & 0 & 0 \\ 0 & -1 & 1 & 3 & 1 \\ -1 & 0 & 3 & -1 & 0 \end{pmatrix}, \text{ o } B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ -1 & 1 \\ 0 & 2 \end{pmatrix}, \text{ tai } AB = \begin{pmatrix} 2 & -2 \\ -2 & 4 \\ 3 & -1 \end{pmatrix}.$$

Apibrėžtieji matricų veiksmai turi skaičių algebroje įprastas savybes:

$$A + B = B + A, \quad A + (B + C) = (A + B) + C, \quad (A + B)C = AC + BC, \quad A(BC) = (AB)C.$$

Tačiau: skaičių *daugybės komutatyvumo* savybė $ab = ba$, matricoms *negalioja*! Kad tuo įsitikintume, užtenka panagrinėti kad ir aukščiau pateiktą pavyzdį: matricų A ir B sandaugą AB mes suradome, o, pabandę apskaičiuoti BA , pastebime, kad to padaryti *negalima*, nes nesuderintos matricų B ir A eilės. Nesunku parinkti ir tokias dvi matricas A ir B , kurioms sandaugos AB ir BA egzistuos, bet būtų nelygios.

Būtent, kai

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}, \text{ o } B = \begin{pmatrix} 1 & -1 \\ 0 & 0 \end{pmatrix}, \text{ tai } AB = \begin{pmatrix} 1 & -1 \\ 3 & -3 \end{pmatrix}. \text{ Tuo tarpu } BA = \begin{pmatrix} -2 & -2 \\ 0 & 0 \end{pmatrix} \neq AB.$$

Matricų, kurių eilė yra $m \times n$, o elementai yra iš lauko R aibę žymėsime $M_{m \times n}(R)$.

Teorema. *Algebrinė struktūra $(M_{m \times n}(R), +)$ yra Abelio grupė.*

Įr. Svarbiausia yra įrodyti, kad matricų sudėčiai yra įvykdoma atvirkštinė operacija: matricų atimtis. Prisiminę bendrąją algebrinių struktūrų teoriją, konstatuojame, kad tam užtenka parodyti, jog matricų aibėje $M_{m \times n}(R)$ yra neutralusis sudėties atžvilgiu (nulinis) elementas, bei kiekvienai matricai simetriškas (priešingas) elementas. Tai išplaukia iš šitokių apibrėžimų.

Ap. Matricą $O = (o_{ij})$, kuri tenkina sąlygą $A + O = A$, su visomis eilės $m \times n$ matricomis A , vadiname **nuline matrica**. Akivaizdu, kad tokia matrica yra ir, kad $(\forall i, j) o_{ij} = 0$.

Ap. Kai $A \in M_{m \times n}(R)$, tai matricą $B = (b_{ij})$, kuri tenkina sąlygą $A + B = O$, vadiname matricai A **priešingą matrica**. Akivaizdu, kad tokia matrica yra ir, kad $(\forall i, j) b_{ij} = -a_{ij}$.

KAD savybes įrodykite savarankiškai.

Ap. Kvadratinę n -osios eilės matricą $E_n = (e_{ij})$, kurioje $\begin{cases} e_{ij} = 1, & \text{kai } i = j, \\ 0, & \text{kai } i \neq j \end{cases}$ vadiname

vienetinė matrica.

Nesunku įsitikinti, kad, jei tik daugyba galima, tai $AE = EA = A$.

Atvirkštinė matrica

Ap. Tarkime $A := (a_{ij})$ yra bet kokia n -osios eilės kvadratinė matrica. Matricą B vadinsime matricai A **atvirkštinė matrica**, jei $AB = BA = E$. Žymime $B = A^{-1}$.

Atvirkštinė matrica egzistuoja ne visoms kvadratinėms matricoms.

Teorema. *Kvadratinei matricai $A := (a_{ij})$ atvirkštinė matrica egzistuoja tada ir tik tada, kai matricos A determinantas $|A|$ nelygus nuliui.*

1. Tarkime priešingai: nors A^{-1} egzistuoja, bet $|A| = 0$. Tačiau tada, pasinaudoję teorema apie matricų sandaugos determinantą ir lygybe $AA^{-1} = E$, gauname prieštarą:

$$AA^{-1} = E \rightarrow |AA^{-1}| = |E| = 1 \text{ ir tuo pat metu } |AA^{-1}| = |A| \cdot |A^{-1}| = 0 \cdot |A^{-1}| = 0.$$

2. Jeigu $|A| \neq 0$, tai nesunku patikrinti, kad matrica

$$A^{-1} := \frac{1}{|A|} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots & \dots & \dots & \dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix} \quad (*)$$

tenkina atvirkštinės matricos apibrėžimą. QED.

*Ap. Kvadratinė matrica, kurios determinantas nelygus nuliui, vadinama **reguliaria** (kitaip: **neišsigimusia**).*

Duotajai matricai atvirkštinę matricą galima rasti *elementariųjų pertvarkių būdu*.

1 pavyzdys. Matricai

$$A = \begin{pmatrix} -1 & 0 & 0 \\ 3 & 1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$$

apskaičiuosime atvirkštinę matricą EP metodu. Tuo tikslu sudarome matricą $A|E$ ir, taikydami EP *tiktai eilutėms*, matricą A pertvarkome į vienetinę. Nesunku įrodyti, kad tada E vietoje atsiranda A^{-1} .

$$\begin{aligned} & \left(\begin{array}{ccc|ccc} -1 & 0 & 0 & 1 & 0 & 0 \\ 3 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & -1 & 0 & 0 & 1 \end{array} \right) \xrightarrow{3L_1+L_2} \left(\begin{array}{ccc|ccc} -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 3 & 1 & 0 \\ 0 & 1 & -1 & 0 & 0 & 1 \end{array} \right) \xrightarrow{-L_2+L_3} \\ & \rightarrow \left(\begin{array}{ccc|ccc} -1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 3 & 1 & 0 \\ 0 & 0 & -1 & -3 & -1 & 1 \end{array} \right) \xrightarrow{-L_1; -L_3} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 3 & 1 & 0 \\ 0 & 0 & 1 & 3 & 1 & -1 \end{array} \right). \end{aligned}$$

Tad (patikrinkite):

$$A^{-1} = \begin{pmatrix} -1 & 0 & 0 \\ 3 & 1 & 0 \\ 3 & 1 & -1 \end{pmatrix}.$$

Užduotis: savarankiškai patikrinkite, kad kai $n = 3$, formulė (*) apibrėžta matrica A^{-1} tenkina sąlygą: $AA^{-1} = A^{-1}A = E$.

2 pavyzdys. Kai $A = \begin{pmatrix} 1 & 0 & 0 \\ 2 & 3 & 0 \\ 0 & 1 & -1 \end{pmatrix}$, tai $|A| = -3 \neq 0$. Todėl A^{-1} egzistuoja. Ją rasime

formulės (*) pagalba. Radę adjunktus $A_{11} = (-1)^{1+1} \begin{vmatrix} 3 & 0 \\ 1 & -1 \end{vmatrix} = -3$, $A_{21} = (-1)^{2+1} \begin{vmatrix} 0 & 0 \\ 1 & -1 \end{vmatrix} = 0$,

$A_{31} = 0$, $A_{12} = 2$, $A_{22} = -1$, $A_{32} = 0$, $A_{13} = 2$, $A_{23} = -1$, $A_{33} = 3$, ir, pastebėję, kad adjunktų matrica formulėje (*) yra *transponuota*, gauname:

$$A^{-1} = -\frac{1}{3} \begin{pmatrix} -3 & 0 & 0 \\ 2 & -1 & 0 \\ 2 & -1 & 3 \end{pmatrix}.$$

Išvada. Jei kvadratinė matrica A turi atvirkštinę, tai tikrai viena.

Tikrai, tarus, kad matricai A yra bent dvi *skirtingos* atvirkštinės matricos A' ir A'' , iš matricų daugybos asociatyvumo ir atvirkštinės matricos apibrėžimo tuoj gauname:

$$1) A'AA'' = (A'A)A'' = EA'' = A'';$$

$$2) A'AA'' = A'(AA'') = A'E = A'. \text{ Bet tada } A' = A''. \text{ Prieštara.}$$

Reguliarių n – osios eilės kvadratinų matricų aibę žymėsime $M_n^0(R)$, t.y.:

$$M_n^0(R) = \{A \mid A \in M_{n \times n}(R), |A| \neq 0\}.$$

Teorema. *Algebrinė struktūra $(M_n^0(R), \cdot)$ yra nekomutatyvioji grupė.*

Irodymas išplaukia iš teoremos apie matricų sandaugos determinantą ir matricų daugybos asociatyvumo.

Ap. Kvadratinę n – osios eilės matricą $A = (a_{ij})$ vadinsime įstrižainine, jei

$$(\forall i, j, i \neq j) a_{ij} = 0.$$

Pavyzdžiui, vienetinė matrica yra įstrižaininė.

Išvada. Reguliarių įstrižaininių matricų aibė yra multiplikacinė Abelio grupė.

Paskaita 2 – 04

Vektorių – eilučių erdvė R^n

Matricų algebra. Įsitikinome, kad algebrinė struktūra $(M_{m \times n}(R), +)$ yra Abelio grupė, o struktūra $(M_n^0(R), \cdot)$ yra nekomutatyviosios grupės pavyzdys. Čia:

$$M_n^0(R) := \{A \mid A \in M_{n \times n}(R), |A| \neq 0\}.$$

Susipažiname su *atvirkštinės matricos* sąvoka, jos radimo algoritmais.

Vektoriai ir jų veiksmai

Ap. *Sutvarkytą realiųjų skaičių rinkinį $(k_1, k_2, \dots, k_n)$ vadinsime ***n*-mačiu vektoriumi** – ***eilute*** ir žymėsime $\alpha := (k_1, k_2, \dots, k_n)$.*

Visų tokių vektorių aibę žymima R^n . Prisiminę aibių Dekarto sandaugos apibrėžimą, galime užrašyti, kad $R^n = R \times R \times \dots \times R$.

Pavyzdžiui, $\alpha = (-1, 2, 3, 0)$ yra *keturmatis* vektorius - eilutė. T.y. $\alpha \in R^4$.

n-matį vektorių – eilutę dažnai vadinsime tiesiog *vektoriumi*.

n-matis vektorius gali būti suprantamas kaip eilės $1 \times n$ matrica. Tada *vektorių veiksmų* apibrėžimai bus jau matyti ir todėl lengviau suprantami bei įsimenami.

Ap. *Vektorių $\alpha := (k_1, k_2, \dots, k_n)$ ir $\beta := (l_1, l_2, \dots, l_n)$ suma vadiname naują *n*-matį vektorių $\alpha + \beta := (k_1 + l_1, k_2 + l_2, \dots, k_n + l_n)$.*

Ap. *Skaičiaus $c \in R$ ir vektoriaus $\alpha := (k_1, k_2, \dots, k_n)$ sandauga vadiname vektorių $c\alpha := (ck_1, ck_2, \dots, ck_n)$.*

Šie veiksmai turi visas *įprastas savybes*, kurias jau aptarėme kalbėdami apie matricų algebrą. Tad nesunku aptarti ir vektorių *skirtumą*, *nulinį* vektorių O ir vektoriui α *priešingą* vektorių $-\alpha := (-1)\alpha$. Galima konstatuoti, kad: *struktūra $(R^n, +)$ yra adicinė Abelio grupė*.

Dar pastebėsime, kad visiškai panašiai galima apibrėžti *n*-mačius vektorius – *stulpelius* (t.y. transponuotas eilutes) ir veiksmus su jais.

Ap. *Algebrinė struktūra $(R^n, +, \cdot)$ vadinama ***n*-mate aritmetine (vektorine) erdve**.*

Aibes R^2 ir R^3 geometriškai galima interpretuoti kaip plokštumą ir trimatę erdvę.

Vektorių rinkinio tiesinė nepriklausomybė

Ap. *Jei turime kelių *n*-mačių vektorių rinkinį (kartais sakoma: sistemą) $\alpha_1, \alpha_2, \dots, \alpha_m$ (sutrumpintai - $(\alpha)_m$) ir rinkinį bet kokių realiųjų skaičių $l_1, l_2, \dots, l_m$, tai naują *n*-matį vektorių $\alpha := l_1\alpha_1 + l_2\alpha_2 + \dots + l_m\alpha_m$ vadinsime rinkinio $(\alpha)_m$ ***tiesine kombinacija*** (kartais: *tiesiniu dariniu*).*

Pavyzdžiui, jei $\alpha_1 = (-1, 2, 3, 1)$, $\alpha_2 = (-1, 2, 3, 2)$, $\alpha_3 = (-1, 2, 3, 5)$, tai viena iš šios sistemos tiesinių kombinacijų yra vektorius $\alpha = 1 \cdot \alpha_1 + 1 \cdot \alpha_2 + 1 \cdot \alpha_3 = (-3, 6, 9, 8)$.

Tiesinėje algebroje viena svarbiausių yra vektorių rinkinio $(\alpha)_m$ tiesinės nepriklausomybės sąvoka.

*Ap. Jei n -mačių vektorių rinkinio $\alpha_1, \alpha_2, \dots, \alpha_m$ tiesinė kombinacija $\alpha := l_1 \alpha_1 + l_2 \alpha_2 + \dots + l_m \alpha_m$ lygi nuliniam vektoriui $O := (0, 0, \dots, 0)$ tiksliai tada, kai visi skaičiai $l_i, i = 1, 2, \dots, m$ yra lygūs nuliui, tai rinkinys $(\alpha)_m$ vadinamas **tiesiškai nepriklausomu** (sutrumpintai – TN).*

*Priešingu atveju, šis vektorių rinkinys vadinamas **tiesiškai priklausomu** (sutrumpintai – TP).*

Pavyzdžiui, rinkinys $\alpha_1 = (-1, 0, 3, 1)$, $\alpha_2 = (-1, 0, 1, 2)$, $\alpha_3 = (2, 0, -4, -3)$ yra tiesiškai priklausomas, nes $1 \cdot \alpha_1 + 1 \cdot \alpha_2 + 1 \cdot \alpha_3 = (0, 0, 0, 0) = O$. Tuo tarpu rinkinys $\beta_1 = (-1, 0, 0, 0)$, $\beta_2 = (0, 1, 0, 0)$, $\beta_3 = (0, 0, 2, 0)$ yra tiesiškai nepriklausomas, nes iš sąlygos $l_1 \cdot \alpha_1 + l_2 \cdot \alpha_2 + l_3 \cdot \alpha_3 = (-l_1, l_2, 2l_3, 0) = (0, 0, 0, 0)$ ir vektorių lygybės apibrėžimo, tuoj pat išplaukia, kad $l_1 = l_2 = l_3 = 0$.

Vektorių tiesinė priklausomybė plokštumoje R^2 reiškia vektorių *kolinearumą*, o trimatėje erdvėje R^3 , – vektorių *komplanarumą*. Tuo atveju, kai turime didesnio nei trečio matavimo vektorius, – vaizdžios geometrinės interpretacijos nėra.

Teisingi tokie teiginiai - teoremos:

- jei vektorių rinkiniui $(\alpha)_m$ priklauso nulinis vektorius O , tai rinkinys yra TP;
- vektorių rinkinys $(\alpha)_m$ yra TP tada ir tiksliai tada, kai bent vienas rinkinio vektorių yra kitų rinkinio vektorių tiesinė kombinacija;
- jei vektorių sistema (rinkinys) $(\alpha)_m$ yra TN, tai ir bet kokia jos posistemė $(\alpha_i)_r, r \leq m$ irgi yra TN;
- jei vektorių rinkinio dalis (posistemė) yra TP, tai ir visas rinkinys yra TP;
- jei turime TN vektorių rinkinį $(\alpha)_m$ ir kiekvienas jo vektorius yra kito vektorių rinkinio $(\beta)_k$ tiesinė kombinacija, tai $m \leq k$.

Šių teoremų įrodymai remiasi vektorių rinkinio tiesinės nepriklausomybės apibrėžimu. Pateiksime pirmųjų dviejų savybių įrodymus.

1. Jei $O \in (\alpha)_m$, tai lengva suvokti, kad tada rinkinio vektorių tiesinėje kombinacijoje konstantą prie vektoriaus O paėmę nelygią nuliui, o visas kitas – lygias nuliui, gausime nulinį vektorius. Tad, $(\alpha)_m$ - TP.

2. a) Tarkime, kad vektorių rinkinys $(\alpha)_m$ yra TP. Tada egzistuoja rinkinys skaičių $l_1, l_2, \dots, l_m$, iš kurių bent vienas (tarkim, pavyzdžiui, l_2) nelygus nuliui, bet $l_1 \alpha_1 + l_2 \alpha_2 + \dots + l_m \alpha_m = O$. Tačiau tai, kad $l_2 \neq 0$, leidžia pastarąją lygybę perrašyti taip:

$\alpha_2 = -\frac{l_1}{l_2}\alpha_1 - \frac{l_3}{l_2}\alpha_3 - \dots - \frac{l_m}{l_2}\alpha_m$, o tai ir reiškia, kad vienas rinkinio $(\alpha)_m$ vektorius (būtent, α_2) yra likusių vektorių tiesinė kombinacija.

b) Tarkime, atvirkščiai: vienas iš rinkinio vektorių (tegu, pvz., α_1) yra kitų rinkinio vektorių tiesinė kombinacija, t.y. $\alpha_1 = l_2\alpha_2 + l_3\alpha_3 + \dots + l_m\alpha_m$.

Bet ši lygybė gali būti perrašyta ir taip: $-\alpha_1 + l_2\alpha_2 + l_3\alpha_3 + \dots + l_m\alpha_m = O$ ir, kaip matome, koeficientas prie pirmojo vektoriaus yra $-1 \neq 0$. Tad 2 savybė pilnai įrodyta.

3. – 4. savybių įrodymai – savarankiškai.

Detaliau aptarsime dar paskutinės, 5 - osios savybės įrodymą.

5. Tarkime priešingai: nors rinkinys $(\alpha)_m$ yra TN ir kiekvienas jo vektorius yra kito vektorių rinkinio $(\beta)_k$ tiesinė kombinacija, t.y.

$$(\forall i)(\exists a_{ij})\alpha_i = a_{i1}\beta_1 + a_{i2}\beta_2 + \dots + a_{ik}\beta_k = \sum_{j=1}^k a_{ij}\beta_j$$

bet $m > k$. Tada, pažymėję k – mačius vektorius $\gamma_j = (a_{j1}, a_{j2}, \dots, a_{jk})$, konstatuojame, kad jų rinkinys $(\gamma)_m$ yra TP. Mat vektorinė lygtis

$$k_1\gamma_1 + k_2\gamma_2 + \dots + k_m\gamma_m = O$$

yra ekvivalenti THLS (užrašykite ją!), kurioje lygčių yra *mažiau* nei kintamųjų ($k < m$). Kaip žinia, tokia THLS turi ir nenulinių sprendinių, t.y. egzistuoja toks nenulinis rinkinys $(k_1, \dots, k_m)$, kad

$$\sum_{i=1}^m k_i a_{ij} = 0, \quad j = 1, 2, \dots, k.$$

Iš čia gauname:

$$\sum_{i=1}^m k_i \alpha_i = \sum_{i=1}^m k_i \sum_{j=1}^k a_{ij} \beta_j = \sum_{j=1}^k \sum_{i=1}^m k_i a_{ij} \beta_j = \sum_{j=1}^k \left(\sum_{i=1}^m k_i a_{ij} \beta_j \right) = \sum_{j=1}^k a_{ij} \left(\sum_{i=1}^m k_i a_{ij} \right) \beta_j = O,$$

t.y. rinkinys $(\alpha)_m$ yra TP. Prieštara. QED.

Vektorių rinkinio bazė ir rangas

Ap. Vektorių sistemos (rinkinio) $(\alpha)_m$ posistemę $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_r}$ vadiname **base**, jeigu ji tenkina du reikalavimus:

- posistemė $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_r}$ yra TN;
- kiekvienas sistemos $(\alpha)_m$ vektorius tiesiškai išsireiškia per posistemę $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_r}$.

Kitas tos pačios sąvokos apibrėžimo variantas yra toks.

Ap. Maksimalią tiesiškai nepriklausomą sistemos $\alpha_1, \alpha_2, \dots, \alpha_m$ posistemę $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_r}$ vadiname vektorių sistemos (rinkinio) $(\alpha)_m$ baze.

Lengva patikrinti, kad šie du apibrėžimai yra ekvivalentūs. Mes dažniau naudosime pirmąjį iš šių apibrėžimų. Būtų korektiška įrodyti teoremą apie apibrėžimų ekvivalentumą. Pabandykite tai padaryti savarankiškai.

Iš 5 – osios vektorių tiesinės nepriklausomybės savybės nesunku gauti tokią svarbią išvadą.

Teorema. *Visos vektorių rinkinio $(\alpha)_m$ bazės turi vienodą vektorių skaičių.*

Įr. Tarkime $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_r}$ ir $\alpha_{j_1}, \alpha_{j_2}, \dots, \alpha_{j_t}$ yra dvi kokios nors rinkinio $(\alpha)_m$ bazės. Sutrumpintai žymėkime jas atitinkamai $(\alpha_i)_r$ ir $(\alpha_j)_t$. Tačiau $(\alpha_i)_r$ kaip bazė yra TN ir tiesiškai išsireiškia per $(\alpha_j)_t$, kadangi $(\alpha_j)_t$ irgi yra bazė. Tada iš 5 – tosios TN savybės išplaukia: $r \leq t$. Analogiškai gauname ir $t \leq r$. Todėl, $t = r$. QED.

Taigi, bazės vektorių skaičius yra konkrečios sistemos $(\alpha)_m$ invariantas (nekeičiamas dydis). Jam suteikiamas specialus pavadinimas.

Ap. Bazės vektorių skaičių r vadiname vektorių rinkinio $(\alpha)_m$ rangu.

Žymime $r = \text{rang}(\alpha)_m$.

Pavyzdžiui, jau nagrinėto rinkinio $(\alpha)_3$: $\alpha_1 = (-1, 0, 3, 1)$, $\alpha_2 = (-1, 0, 1, 2)$, $\alpha_3 = (2, 0, -4, -3)$ bazę sudaro, vektoriai α_1 ir α_3 . Mat, kaip nesunku įsitikinti, jie sudaro tiesiškai nepriklausomą sistemos $(\alpha)_3$ posistemę. Be to, $\alpha_2 = -\alpha_1 - \alpha_3$. Todėl: $\text{rang}(\alpha)_3 = 2$.

Vektorių – stulpelių erdvė. Primenu: visos čia aptartos sąvokos ir savybės lieka galioti, jei kalbame ne apie vektorius – eilutes, o apie vektorius – stulpelius. Pvz., vektorių – stulpelių rinkinys

$$\alpha_1 = \begin{pmatrix} 2 \\ -1 \\ 0 \\ 4 \end{pmatrix}, \alpha_2 = \begin{pmatrix} 3 \\ -1 \\ 0 \\ 1 \end{pmatrix}, \alpha_3 = \begin{pmatrix} 0 \\ -1 \\ 7 \\ 2 \end{pmatrix}, \alpha_4 = \begin{pmatrix} 5 \\ -1 \\ -2 \\ 0 \end{pmatrix}, \alpha_5 = \begin{pmatrix} 3 \\ 0 \\ 3 \\ -4 \end{pmatrix}$$

yra tiesiškai priklausomas, nes vektorių yra daugiau nei keturi. Nesunku patikrinti, kad vektoriai $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ yra šio rinkinio bazė. Tad $\text{rang}(\alpha)_5 = 4$.

Paskaita 2 – 05

TLS suderintumo kriterijus

Vektorių – eilučių aritmetinė erdvė $\mathbf{R}^n := (R^n, +, \cdot)$. Svarbios sąvokos: TN vektorių rinkinys, vektorių rinkinio bazė ir rangas.

Vektorius koordinatės. Galima kalbėti ir apie visos vektorių – eilučių erdvės $\mathbf{R}^n$ bazę. Apibrėžimas lieka beveik pažodžiui toks pat:

Ap. Erdvės $\mathbf{R}^n$ **bazė** vadiname tokį jos vektorių rinkinį $(\alpha)_m$, kuriam yra išpildytos dvi sąlygos:

- $(\alpha)_m$ yra TN;
- $(\forall \beta \in R^n)(\exists l_1, l_2, \dots, l_m) \beta = l_1 \alpha_1 + l_2 \alpha_2 + \dots + l_m \alpha_m$.

Arba: Erdvės $\mathbf{R}^n$ bazė vadiname maksimalią TN vektorių sistemą $(\alpha)_m$.

Lieka teisinga ir teorema apie tai, kad: visos erdvės bazės turi vienodą vektorių skaičių. Jos įrodymas yra toks pat kaip ir baigtinio vektorių rinkinio atveju.

Išvada. Bet kuri erdvės $\mathbf{R}^n$ bazė turi lygiai n vektorių.

Įrodymui užtenka patikrinti, kad n -mačių vektorių rinkinys $(\epsilon)_n$:

$$\epsilon_1 = (1, 0, 0, \dots, 0),$$

$$\epsilon_2 = (0, 1, 0, \dots, 0),$$

$$\dots\dots\dots,$$

$$\epsilon_n = (0, 0, 0, \dots, 1)$$

tikrai sudaro $\mathbf{R}^n$ bazę. Juk rinkinyje $(\epsilon)_n$ yra n vektorių.

Bazė $(\epsilon)_n$ kartais vadinama *standartine* (paprasčiausia) baze.

Skaičiai l_i iš bet kurio vektoriaus $\beta \in R^n$ tiesinės išraiškos per bazės $(\alpha)_n$ vektorius:

$$\beta = l_1 \alpha_1 + l_2 \alpha_2 + \dots + l_n \alpha_n$$

vadinami to vektoriaus β koordinatėmis bazėje $(\alpha)_n$. Žymima: $\beta = (l_1, l_2, \dots, l_n)_{[\alpha]}$.

Teorema. Vektoriaus koordinatės duotoje (sistemos ar visos erdvės) bazėje nustatomos vienareikšmiškai.

Įr. Tare, pavyzdžiui, kad $(\alpha)_n$ yra visos erdvės bazė, ir yra vektorius $\beta \in R^n$, kuriam teisingos bent dvi skirtingos išraiškos:

$$\beta = l_1 \alpha_1 + l_2 \alpha_2 + \dots + l_n \alpha_n,$$

$$\beta = k_1 \alpha_1 + k_2 \alpha_2 + \dots + k_n \alpha_n,$$

atėmę jas vieną iš kitos gautume (turėdami omenyje, kad (!) *ne su visais* i , $l_i = k_i$):

$$0 = (l_1 - k_1) \alpha_1 + (l_2 - k_2) \alpha_2 + \dots + (l_n - k_n) \alpha_n.$$

Bet tai prieštarauja teiginiui, kad $(\alpha)_n$ yra bazė, taigi, – TN rinkinys. QED.

Pvz., rinkinys: $\varepsilon_1 = (1, 0, 0, 0)$, $\varepsilon_2 = (1, 1, 0, 0)$, $\varepsilon_3 = (1, 1, 1, 0)$, $\varepsilon_4 = (1, 1, 1, 1)$ yra erdvės $\mathbf{R}^4$ bazė, o vektoriaus $\beta = (-3, 2, 1, 2)$ koordinatės joje yra tokios:

$$l_1 = 1, \quad l_2 = 1, \quad l_3 = -1, \quad l_4 = 2.$$

Bendruoju atveju jos surandamos iš vektorinės lygties

$$\beta = l_1 \varepsilon_1 + l_2 \varepsilon_2 + \dots + l_n \varepsilon_n,$$

kuri, sulyginus atitinkamas koordinates, virsta TLS kintamųjų l_i , $i = 1 \div n$ atžvilgiu.

Matricos rangas

Ap. Matricos **rangu** vadiname jos stulpelių rinkinio rangą.

Žymime $r = \text{rang} A$.

Vėliau mums bus naudinga tokia sąvoka.

Ap. n -mačių vektorių rinkiniai $(\alpha)_m$ ir $(\beta)_k$ vadinami **ekvivalenčiais**, jei kiekvienas rinkinio $(\alpha)_m$ vektorius tiesiškai išsireiškia per rinkinio $(\beta)_k$ vektorius ir atvirkščiai: kiekvienas rinkinio $(\beta)_k$ vektorius tiesiškai išsireiškia per rinkinį $(\alpha)_m$.

Teorema. Ekvivalenčių vektorių rinkinių rangai yra vienodi.

Teoremos įrodymas išplaukia dukart pasinaudojus 5 – tąja vektorių TN savybe.

Yra keletas metodų matricos rangui rasti. Pirmasis iš jų remiasi tokiu vokiečių matematiko Frobenijaus (F.G.Frobenius, 1849-1917) įrodytu faktu.

Frobenijaus teorema. Jei matrica turi r – osios eilės nelygų nuliui minorą, o visi $r+1$ – osios eilės matricos minorai lygūs nuliui, tai skaičius r yra lygus matricos rangui.

Įr. Tarkime, kad tas r -osios eilės minoras M_r yra kairiajame viršutiniame matricos kampe:

$$A = \begin{pmatrix} a_{11} & \dots & a_{1r} & a_{1,r+1} & \dots & a_{1n} \\ a_{21} & \dots & a_{2r} & a_{2,r+1} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{r1} & \dots & a_{rr} & a_{r,r+1} & \dots & a_{rn} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{m1} & \dots & a_{mr} & a_{m,r+1} & \dots & a_{mn} \end{pmatrix}.$$

Pažymėję matricos stulpelius $\beta_1, \dots, \beta_r, \dots, \beta_n$, konstatuojame, kad:

1. Pirmieji r stulpelių $\beta_1, \dots, \beta_r$ yra TN. Kitaip determinantas M_r , priešingai teoremos sąlygai, būtų lygus nuliui.

2. Bet kuris kitas, pvz., l – tasis stulpelis β_l tiesiškai išsireiškia per $\beta_1, \dots, \beta_r$. Iš tikrųjų, paimkime pagalbinį $r+1$ – osios eilės determinantą:

$$\Delta = \begin{vmatrix} a_{11} & \dots & a_{1r} & a_{1l} \\ \dots & \dots & \dots & \dots \\ a_{r1} & \dots & a_{rr} & a_{rl} \\ a_{i1} & \dots & a_{ir} & a_{il} \end{vmatrix},$$

gautą prijungus vieną iš likusių $\beta_{r+1}, \dots, \beta_n$ stulpelių, ir *bet kurią*, pavyzdžiui, i -ąją eilutę. Tada gausime, kad $\Delta = 0$ arba kaip minorą M_r *apgaubiantis* $r+1$ – osios eilės minoras, arba kaip determinantas, kurio dvi eilutės yra vienodos. Išskleidę jį pagal paskutinę eilutę, gausime:

$$a_{i1}A_1 + a_{i2}A_2 + \dots + a_{ir}A_r + a_{il}M_r = 0.$$

Šitokia lygybė yra teisinga su visais $l = 1 \div m$, be to, skaičiai A_k , $k = 1 \div r$ nuo i nepriklauso. Tai ir reiškia, kad l -asis stulpelis yra stulpelių $\beta_1, \dots, \beta_r$ tiesinė kombinacija.

Jei minoras M_r būtų kitose matricos A eilutėse ir stulpeliuose, tai, reikiamą kiekį kartų sukeitę juos vietomis, perkeltume minorą į kairįjį viršutinį kampą. Eilučių (stulpelių) sukeitimas vietomis tiksliai keičia determinanto ženklą. Todėl teorema teisinga ir bendruoju atveju. QED.

Antrasis matricos rango radimo metodas pagrįstas tokia teorema.

Teorema. *Matricos eilučių ir matricos stulpelių rangai sutampa. Be to, tiek eilučių, tiek ir stulpelių EP nekeičia matricos rango.*

Irodymas išplaukia kaip išvada iš Frobenijaus teoremos ir teoremos apie ekvivalenčių vektorių rinkinių rangus.

Iš tikrųjų, paėmus, pvz., eilės $n \times m$ matricos stulpelių rinkinį $\beta_1, \beta_2, \dots, \beta_m$ ir atlikus visus tris EP (stulpelių sukeitimas vietomis, padauginimas iš $c \neq 0$, dviejų stulpelių sudėjimas) gautume (keisdami, paprastumo dėlei, tik β_1, β_2 ir β_3) rinkinį

$$\beta_2, \beta_1, \beta_3 + c\beta_2, \dots, \beta_m,$$

kuris yra *ekvivalentus pradiniam*. Vektorius β_3 iš sistemos $\beta_1, \beta_2, \dots, \beta_m$ taip išsireiškia per sistemą $\beta_2, \beta_1, \beta_3 + c\beta_2, \dots, \beta_m$:

$$\beta_3 = -c\beta_2 + 0 \cdot \beta_1 + 1 \cdot (\beta_3 + c\beta_2) + 0 \cdot \beta_4 + \dots + 0 \cdot \beta_m.$$

Atvirkščiai, vektorius $\beta_3 + c\beta_2$ per rinkinį $\beta_1, \beta_2, \dots, \beta_m$ išreiškiamas taip:

$$\beta_3 + c\beta_2 = 0 \cdot \beta_1 + c \cdot \beta_2 + 1 \cdot \beta_3 + 0 \cdot \beta_4 + \dots + 0 \cdot \beta_m.$$

Kitų vektorių išraiškos dar paprastesnės. QED.

Pavyzdžiui, abiem būdais rasime matricos

$$A = \begin{pmatrix} 2 & -1 & 0 & 1 \\ 1 & -2 & 1 & 3 \\ 3 & -3 & 1 & 4 \end{pmatrix}$$

rangą. Pradėsime nuo EP būdo. Naudodami įprastus žymenis, turėsime:

$$\begin{pmatrix} 2 & -1 & 0 & 1 \\ 1 & -2 & 1 & 3 \\ 3 & -3 & 1 & 4 \end{pmatrix} \xrightarrow{\substack{-3L_1+L_2 \\ -4L_1+L_3}} \begin{pmatrix} 2 & -1 & 0 & 1 \\ -5 & 1 & 1 & 0 \\ -5 & 1 & 1 & 0 \end{pmatrix} \xrightarrow{\substack{-L_2+L_3 \\ S_4+S_2, \\ -2S_4+S_1}} \begin{pmatrix} 0 & 0 & 0 & 1 \\ -5 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix} \xrightarrow{\substack{-S_3+S_2, \\ 5S_3+S_1}} \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

todėl $r = \text{rang} A = 2$. Iš tikrųjų, nesunku pastebėti, kad trečiasis ir ketvirtasis pastarosios matricos stulpeliai yra TN vektorių sistema. Jeigu bandysime prie jos prijungti dar vieną (t.y. pirmą ar antrą) stulpelį, tai į sistemą pateks *nulinis stulpelis*, todėl, pagal anksčiau minėtą savybę, toks rinkinys jau taps TP. Tad du minėti stulpeliai yra *maksimali TN stulpelių rinkinio posistemė*. Išvada: $r = \text{rang} A = 2$.

Verta įsidėmėti, kad EP metodo matricos rangui rasti esmė yra tokia: naudodami EP eilutės ir stulpelius, matricą keičiame taip, kad *vienoje iš jos įstrižainių stovėtų nenuliniai elementai, o visur kitur – nuliai. Nenulinių elementų skaičius ir yra matricos rangas.*

Dabar tos pačios matricos rangą apskaičiuosime panaudodami Frobenijaus teoremą. Pastebėję, kad matricoje yra nelygių nuliui pirmosios ir antrosios eilės minorų (pvz., $M_{1,2} = -1 \neq 0$, $M_{12,12} = -3 \neq 0$, ar $M_{12,13} = 2 \neq 0$), nesunkiai įsitikiname, kad visi galimi trečiosios eilės minorai lygūs nuliui (patikrinkite!). Todėl $\text{rang} A = 2$.

Be to, Frobenijaus teoremos įrodymo eigoje įsitikinome, kad, radus k -osios eilės nelygų nuliui minorą M_k , toliau reikia tikrinti ne visus $k+1$ -osios eilės minorus, o tiktai *apgaubiančius* M_k .

Suformuluosime dar vieną svarbią teoremą apie matricų sandaugos rangą.

Teorema. *Matricų sandaugos rangas neviršija dauginamųjų matricų rangų.*

Įr. Tarkime A, B yra atitinkamai eilių $m \times n$ ir $n \times s$ matricos; jų stulpelius pažymėkime atitinkamai $\alpha_1, \alpha_2, \dots, \alpha_n$ ir $\beta_1, \beta_2, \dots, \beta_s$, jų sandaugą $C = AB = (c_{ik})$, o sandaugos stulpelius $\gamma_1, \gamma_2, \dots, \gamma_s$. Remdamiesi matricų daugybos apibrėžimu, turėsime:

$$c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \dots + a_{in}b_{nk}, \quad i = 1 \div m,$$

bet šitai reiškia ne ką kitą, kaip vektorinę lygybę:

$$\gamma_k = b_{1k}\alpha_1 + b_{2k}\alpha_2 + \dots + b_{nk}\alpha_n,$$

t.y. rinkinys $(\gamma)_s$ tiesiškai išsireiškia per rinkinį $(\alpha)_n$. Tačiau tada ir rinkinio $(\gamma)_s$ bazė tiesiškai išsireiškia per rinkinio $(\alpha)_n$ bazę. Pagal 5 – ają vektorių tiesinė nepriklausomybės savybę $\text{rang} C = \text{rang}(\gamma)_s \leq \text{rang}(\alpha)_n = \text{rang} A$.

Panašiai, remdamiesi lygybe

$$c_{ik} = a_{i1}b_{1k} + a_{i2}b_{2k} + \dots + a_{in}b_{nk}, \quad k = 1 \div s,$$

įsitikintume, kad matricos C eilučių sistema tiesiškai išsireiškia per matricos B eilučių rinkinį.

Bet ir eilučių rangas sutampa su matricos rangui, todėl $\text{rang} C \leq \text{rang} B$. QED.

Dabar jau galime atsakyti ir į semestro pradžioje suformuluotą klausimą: *kada TLS yra suderinta* (turi sprendinių)?

TLS suderintumo kriterijus

Kronekerio – Kapelli teorema. *Tiesinių lygčių sistema*

$$\sum_{j=1}^n a_{ij}x_j = b_i, \quad i = 1, 2, \dots, m$$

yra suderinta tada ir tik tada, kai jos matricos ir išplėstinės matricos rangai sutampa, t.y. $\text{rang} A = \text{rang} \bar{A}$.

Įrodymo žingsniai: 1. Jei TLS suderinta, tai lygybė $\text{rang} A = \text{rang} \bar{A}$ išplaukia iš to, kad matricos A ir išplėtosios matricos $\bar{A}$ stulpelių rinkiniai $\beta_1, \beta_2, \dots, \beta_n$ ir $\beta_1, \beta_2, \dots, \beta_n, \beta$ yra *ekvivalentūs*. Tikrai, kadangi egzistuoja bent vienas TLS sprendinys $(k_1, k_2, \dots, k_n)$, tai iš m teisingų lygybių

$$\sum_{j=1}^n a_{ij}k_j = b_i, \quad i = 1, 2, \dots, m,$$

išplaukia vektorinė lygybė:

$$\beta = k_1\beta_1 + k_2\beta_2 + \dots + k_n\beta_n.$$

Kiti stulpelių rinkinių vektoriai vieni per kitus išreiškiami trivialiai.

2. Jeigu matricų A ir $\bar{A}$ rangai sutampa, tai ir baziniai (*ranginiai*) stulpeliai $\beta_{i_1}, \beta_{i_2}, \dots, \beta_{i_r}$ jose, – taip pat. Bet tada laisvųjų narių stulpelis β turi per bazinius tiesiškai išsireikšti, kitaip, priešingai prielaidai, matricos $\bar{A}$ rangas būtų bent $r + 1$. Taigi, egzistuoja toks rinkinys $k_{i_1}, k_{i_2}, \dots, k_{i_r}$, kad:

$$\beta = k_{i_1}\beta_{i_1} + k_{i_2}\beta_{i_2} + \dots + k_{i_r}\beta_{i_r}.$$

Akivaizdu, kad rinkinys $(0, \dots, 0, k_{i_1}, 0, \dots, 0, k_{i_2}, 0, \dots, 0, k_{i_r}, 0, \dots, 0)$ yra TLS sprendinys. QED.

TLS suderintumo kriterijų pailiustruosime pavyzdžiais. Sistema

$$\begin{cases} 2x_1 - 3x_2 - 5x_3 = -8, \\ -x_1 + 4x_2 + 11x_3 = 15 \end{cases}$$

yra suderinta, nes akivaizdu, kad $\text{rang} A = \text{rang } \bar{A} = 2$. Tuo tarpu sistema

$$\begin{cases} x_1 - 3x_2 - x_3 = -1, \\ -x_1 + 4x_2 + 2x_3 = 1, \\ x_2 + x_3 = -1 \end{cases}$$

sprendinių neturi, nes $\text{rang} A = 2$, o $\text{rang } \bar{A} = 3$.

Apibendrintasis Kramerio metodas

Panaudojant šį TLS suderintumo kriterijų, Kramerio metodu galima spręsti jau *bet kokias suderintas* TLS. Pavyzdžiui, TLS

$$\begin{cases} x_1 - 3x_2 - x_3 = -1, \\ -x_1 + 4x_2 + 2x_3 = 1, \\ x_2 + x_3 = 0 \end{cases}$$

yra suderinta, nes $\text{rang} A = \text{rang } \bar{A} = 2$. Taip yra todėl, kad TLS matricoje yra antrosios eilės minorų (pvz., $M_{12,13}$) nelygių nuliui, o vienintelis trečiosios eilės minoras

$$M_{123,123} = |A| = \begin{vmatrix} 1 & -3 & -1 \\ -1 & 4 & 2 \\ 0 & 1 & 1 \end{vmatrix} = 0.$$

Abu išplėtosios matricos $\bar{A}$ trečiosios eilės minorai irgi lygūs nuliui (įsitikinkite!). Formaliai Kramerio taisyklės taikyti negalima, nes, kaip matėme, $|A| = 0$. Tačiau iš to, kad $M_{12,13} \neq 0$, išplaukia, kad duotoji TLS ekvivalenti tokiai:

$$\begin{cases} x_1 - x_3 = 3x_2 - 1, \\ -x_1 + 2x_3 = -4x_2 + 1. \end{cases}$$

Šią TLS jau galime spręsti Kramerio taisyklės pagalba, nes jos matricos determinantas $M_{12,13} = 1 \neq 0$. Turime:

$$x_1 = \frac{\begin{vmatrix} 3x_2 - 1 & -1 \\ -4x_2 + 1 & 2 \end{vmatrix}}{1} = 2x_2 - 1, \quad x_3 = \frac{\begin{vmatrix} 1 & 3x_2 - 1 \\ -1 & -4x_2 + 1 \end{vmatrix}}{1} = -x_2.$$

Todėl **bendrasis** TLS sprendinys yra toks: $(2x_2 - 1, x_2, -x_2)$, $x_2 \in R$.

Imdami konkrečias $x_2 \in R$ reikšmes gausime *atskirusius* TLS sprendinius, kurių suprantama, yra *be galo daug*. Vienas iš jų (kai $x_2 = 1$) yra rinkinys $(1, 1, -1)$.

Paskaita 2 – 06

Vektorinės erdvės

Vektoriai, erdvė $\mathbf{R}^n$, vektorių – eilučių (stulpelių) rinkinio bazė, rangas, *matricos rangas*; Kronekerio – Kapelli teorema.

Erdvės $\mathbf{R}^n$ ir n -mačio vektoriaus - eilutės sąvokas galima natūraliu būdu apibendrinti.

Tarkime turime kokią nors aibę V ir skaliarų (nebūtinai skaičių) lauką L .

Tarkime, aibėje V yra apibrėžta vidinė algebrinė binarė operacija, kurią mes vadinsime *sudėjimu* ir žymėsime "+". Toliau, laikysime, kad aibė V yra uždara ir joje apibrėžtos išorinės operacijos *daugybės iš lauko L elemento*, kurią žymėsime " $\cdot$ ", atžvilgiu.

Ap. Struktūrą $V := (V, +, \cdot)$ vadinsime **vektorine erdve** (VE) virš lauko L , o jos elementus **vektoriais**, jei yra išpildomi tokie reikalavimai – aksiomos:

1. $(V, +)$ yra adicinė Abelio grupė.
2. Operacija " $\cdot$ " yra komutatyvi, asociatyvi ir dukart distributyvi, t.y.

$$(\alpha, \beta \in V) (\forall l, k \in L) \quad l\alpha = \alpha l, \quad (lk)\alpha = l(k\alpha),$$

$$(l+k)\alpha = l\alpha + k\alpha, \quad l(\alpha + \beta) = l\alpha + l\beta.$$

Pavyzdžiai.

1. Atskiru atveju, šitokią apibrėžimą tenkina aibė $\mathbf{R}^n$ ir laukas $\mathbf{R}$.
2. Galima imti $V = M_{m \times n}(K)$, o $L = Q$.
3. V gali būti tolydinių intervale $[a, b]$ realiųjų funkcijų aibė $C[a, b]$; $L = \mathbf{R}$.

Tad erdvė $(\mathbf{R}^n, +, \cdot)$ yra tik vienas iš daugelio vektorinės erdvės pavyzdžių. Beje, kartais vektorine erdve pavadiname jos bazinę aibę V .

Savybės. Iš apibrėžimo išplaukia, kad aibėje V yra vienintelis *nulinis vektorius* ir kiekvienam vektoriui α vienintelis *priešingas vektorius* (t.y. $-\alpha$). Be to, veiksmai su vektoriais turi įprastas savybes:

1. $(\forall \alpha \in V) (\forall l \in L) \quad 0_L \cdot \alpha = l \cdot O = O.$
2. $(\forall \alpha \in V) \quad (-1_L) \cdot \alpha = -\alpha.$
3. $(\forall \alpha_i \in V, i = 1 \div m) (\forall l_j \in L, j = 1 \div n) \left(\sum_{j=1}^n l_j \right) \cdot \left(\sum_{i=1}^m \alpha_i \right) = \sum_{j=1}^n \sum_{i=1}^m l_j \alpha_i.$

Kaip ir anksčiau, vektorių $\alpha := l_1 \alpha_1 + l_2 \alpha_2 + \dots + l_m \alpha_m$ vadinsime vektorių rinkinio $(\alpha)_m$ *tiesiniu dariniu (kombinacija)*. Čia $l_1, l_2, \dots, l_m$, - yra bet kokie lauko L elementai. Kartais,

norėdami pabrėžti, kad O yra konkrečios vektorinės erdvės $(V, +, \cdot)$ nulinis vektorius, vietoje O rašysime O_V .

Svarbus vektorių rinkinio $(\alpha)_m$ tiesinės nepriklausomybės apibrėžimas išlieka beveik nepakitęs. Pakartokime jį:

*Ap. Jei vektorių rinkinio $(\alpha)_m$ tiesinė kombinacija $\alpha := l_1\alpha_1 + l_2\alpha_2 + \dots + l_m\alpha_m$ lygi nuliniam vektoriui tiksliai tada, kai visi skaliariai $l_i, i = 1, 2, \dots, m$ yra lygūs 0_L , tai rinkinys $(\alpha)_m$ vadinamas **tiesiškai nepriklausomu**.*

Lieka teisingos ir teoremos - savybės:

- jei vektorių rinkiniui $(\alpha)_m$ priklauso nulinis vektorius O , tai rinkinys yra TP ;
- vektorių rinkinys $(\alpha)_m$ yra TP tada ir tiksliai tada, kai bent vienas rinkinio vektorius yra kitų rinkinio vektorių tiesinė kombinacija;
- jei vektorių sistema (rinkinys) $(\alpha)_m$ yra TN , tai ir bet kokia jos posistemė $(\alpha_i)_r, r \leq m$ irgi yra TN ;
- jei vektorių rinkinio dalis (posistemė) yra TP , tai ir visas rinkinys yra TP ;
- jei turime TN vektorių rinkinį $(\alpha)_m$ ir kiekvienas jo vektorius yra kito vektorių rinkinio $(\beta)_k$ tiesinė kombinacija, tai $m \leq k$.

Teoremų įrodymai beveik nesikeičia.

Ir vektorių rinkinio, ir visos erdvės bazės apibrėžimai skamba taip pat, kaip ir anksčiau:

*Ap. Vektorių sistemos $(\alpha)_m$ posistemę $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_r}$ vadiname **baze**, jeigu ji tenkina du reikalavimus:*

- posistemė $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_r}$ yra TN ;
- kiekvienas sistemos $(\alpha)_m$ vektorius tiesiškai išsireiškia per $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_r}$.

Vėlgi vektorių rinkinio bazę galima apibrėžti ir taip:

*Ap. Maksimalią vektorių tiesiškai nepriklausomą sistemos $\alpha_1, \alpha_2, \dots, \alpha_m$ posistemę $\alpha_{i_1}, \alpha_{i_2}, \dots, \alpha_{i_r}$ vadiname vektorių sistemos (rinkinio) $(\alpha)_m$ **baze**.*

Akivaizdu, kad lieka teisinga:

Teorema. Visos vektorių rinkinio $(\alpha)_m$ bazės turi vienodą vektorių skaičių.

*Ap. Bazės vektorių skaičių r vadiname vektorių rinkinio $(\alpha)_m$ **rangu**.*

Žymime $r = \text{rang}(\alpha)_m$.

*Ap. Visos erdvės V bazės vektorių skaičių d vadiname erdvės **dimensija**.*

Žymime $d = \dim V$.

Bazės keitimas. Kartais tenka vieną VE bazę keisti kita. Kyla klausimas, kaip susietos to paties vektoriaus koordinatės skirtingose bazėse?

Jei $(\alpha)_n$ ir $(\beta)_n$ yra dvi VE bazės, tai kiekvienas “naujosios” bazės $(\beta)_n$ vektorius tiesiškai išsireiškia per “senąją” bazę $(\alpha)_n$, t.y. (pvz. kai $L=R$):

$$(\forall i, i = 1 \div n) (\exists t_{ij} \in R, j = 1 \div n) \beta_i := \sum_{j=1}^n t_{ij} \alpha_j.$$

Ap. Kvadratinė n – osios eilės matrica $T := (t_{ij})$ vadinama **bazės keitimo matrica**.

Teorema. Jei vektoriaus $\alpha \in V$ koordinačių bazėje $(\alpha)_n$ eilutė yra $(l_1, l_2, \dots, l_n)$, o bazėje $(\beta)_n - (k_1, k_2, \dots, k_n)$, tai:

$$(l_1, l_2, \dots, l_n) = (k_1, k_2, \dots, k_n) \cdot T.$$

1 išvada. Bazės keitimo matrica T yra reguliari.

2 išvada. $(k_1, k_2, \dots, k_n) = (l_1, l_2, \dots, l_n) \cdot T^{-1}$.

Skirtingai nuo n -mačių vektorių – eilučių erdvės $(R^n, +, \cdot)$, kurios dimensija, kaip prisimename, yra n , bendrosios vektorinės erdvės gali būti ir *begaliniamatės*.

Pvz., vektorinė erdvė $(C[a, b], +, \cdot)$ yra begalinės dimensijos erdvės pavyzdys. Be įprastų, tokios erdvės turi ir įdomių specifinių savybių. Toliau mes domėsime tik *baigtinės dimensijos* vektorinėmis erdvėmis.

Poerdviai

Ap. Kai $(V, +, \cdot)$ yra VE virš lauko L , o $V_1 \subset V$ ir $(V_1, +, \cdot)$ irgi yra VE virš to paties lauko, tai $AS (V_1, +, \cdot)$ vadinama $VE (V, +, \cdot)$ **poerdviu**.

Kiekviena VE turi bent du poerdvius: $(\{0\}, +, \cdot)$ ir $(V, +, \cdot)$. Jie vadinami *trivialiaisiais* poerdviais. Kai norime patikrinti, ar poaibis yra ir poerdvis, naudojame tokia teorema.

Poerdvio kriterijus. Jei $V_1 \subset V$, tai $AS (V_1, +, \cdot)$ tada ir tik tada yra $VE (V, +, \cdot)$ poerdvis, kai aibė V_1 yra uždara vektorių sudėties ir daugybos iš lauko L elemento atžvilgiu.

Įrodymas - savarankiškai (žr. pogrupio kriterijaus įrodymą 1 – 05 paskaitoje).

Pvz., vektorinės erdvės $(M_{m \times n}(R), +, \cdot)$ poerdvis yra struktūra $(M_{m \times n}^i(R), +, \cdot)$. Čia $M_{m \times n}^i(R)$ – yra įstrižaininių matricų aibė.

Išvada. Kai $(V, +, \cdot)$ yra VE virš lauko L , o $(\alpha)_m$ yra vektorių iš V rinkinys, tai aibė

$$H(\alpha_1, \alpha_2, \dots, \alpha_m) := \left\{ \beta \in V \mid \beta = \sum_{i=1}^m l_i \alpha_i, l_i \in L \right\}$$

yra $(V, +, \cdot)$ poerdvis. Jis vadinamas vektorių rinkinio $(\alpha)_m$ *generuotu* poerdviu.

Poerdvių sankirta, suma, tiesioginė suma

Ap. Dviejų VE $(V, +, \cdot)$ poerdvių $(V_1, +, \cdot)$ ir $(V_2, +, \cdot)$ **sankirta** vadiname struktūrą $(V_1 \cap V_2, +, \cdot)$.

Ap. Dviejų VE $(V, +, \cdot)$ poerdvių $(V_1, +, \cdot)$ ir $(V_2, +, \cdot)$ **suma** vadiname struktūrą $(V_1 + V_2, +, \cdot)$, kurios bazinė aibė $V_1 + V_2$ yra sudaryta iš visų galimų sumų pavidalo $\alpha_1 + \alpha_2$, kai $\alpha_1 \in V_1$, o $\alpha_2 \in V_2$.

Ap. Poerdvių suma vadinama **tiesiogine suma**, jei kiekvienas jos bazinės aibės $V_1 + V_2$ vektorius α pavidalu $\alpha_1 + \alpha_2$ užrašomas vieninteliu būdu.

Teorema. Kelių VE poerdvių suma ir sankirta yra VE poerdviai.

Įrodymui (palyginimui žr. teoremą apie pogrupių sankirtą) tereikia pasinaudoti poerdvio kriterijumi.

Teorema. Būtina ir pakankama sąlyga, kad poerdvių $(V_1, +, \cdot)$ ir $(V_2, +, \cdot)$ suma $(V_1 + V_2, +, \cdot)$ būtų tiesioginė yra: $V_1 \cap V_2 = \{O\}$.

Įr. Būtinumas. Jei poerdvių suma yra tiesioginė, o $V_1 \cap V_2 \neq \{O\}$, tai iš to, kad yra nenulinis vektorius $\beta \in V_1 \cap V_2$, gauname prieštarą, kad nulinis vektorius išskaidomas dvejopai: $O = \beta + (-\beta) = (-\beta) + \beta$.

Pakankamumas. Jei $V_1 \cap V_2 = \{O\}$, bet egzistuoja bent dvejopai užrašomas vektorius $\beta \in V_1 + V_2$, tai iš lygybių $\beta = \alpha_1 + \alpha_2$, $\alpha_1 \in V_1$, $\alpha_2 \in V_2$ ir $\beta = \alpha'_1 + \alpha'_2$, $\alpha'_1 \in V_1$, $\alpha'_2 \in V_2$ išplaukia:

$$O = \alpha_1 - \alpha'_1 + \alpha_2 - \alpha'_2 =: \gamma_1 + \gamma_2, \quad \gamma_1 \in V_1, \gamma_2 \in V_2.$$

Jeigu dabar $\gamma_1 = \alpha_1 - \alpha'_1 \neq O$, tai iš $\gamma_1 = -\gamma_2$ gautume, kad $\gamma_1 \in V_1 \cap V_2$. Prieštara. QED.

THLS sprendinių poerdvis

Kaip žinome, THLS

$$\sum_{k=1}^n a_{ik} x_k = 0, \quad i = 1, 2, \dots, m, \quad a_{ij} \in R$$

yra visada suderinta. Nesunku patikrinti, kad jos sprendinių aibė S tenkina poerdvio kriterijaus sąlygas. Todėl struktūra $(S, +, \cdot)$ yra erdvės $(R^n, +, \cdot)$ poerdvis.

Teorema. $\dim S = n - r$. Čia $r = \text{rang} A$.

Įrodymą praleidžiame.

Ap. THLS sprendinių aibės S bazę vadiname **fundamentine sprendinių sistema**.

Vektorinių erdvių izomorfizmai

Ap. Dvi VE $(V_1, +, \cdot)$ ir $(V_2, +, \cdot)$ vadinsime **izomorfiškomis** (atitinkamai – homomorfiškomis), jei tarp bazinių aibių V_1 ir V_2 galima nustatyti bent vieną tokią bijekciją $\varphi : V_1 \longleftrightarrow V_2$ (atitinkamai – surjekciją), kad galiojūt sąlygos:

1. $(\forall a, b \in V_1) \varphi(a + b) = \varphi(a) + \varphi(b)$.
2. $(\forall a \in V_1)(\forall l \in L) \varphi(l \cdot a) = \varphi(a) \cdot \varphi(l)$.

Teorema. Dvi VE virš $\mathbf{R}$ yra izomorfiškos tada ir tik tada, kai jų dimensijos yra lygios.

Irodymo žingsniai.

1. Pakankamumas išplaukia iš tokios lemos:

Lema. Izomorfizmas $\varphi : V_1 \longleftrightarrow V_2$ bazę atvaizduoja į bazę.

2. Būtinumas. Kai erdvių $(V_1, +, \cdot)$ ir $(V_2, +, \cdot)$ dimensijos yra vienodos, o $(\alpha)_n$ ir $(\beta)_n$ yra jų kokios nors bazės, tai bijekciją φ tarp bazinių aibių V_1 ir V_2 apibrėžiame taip:

$$(\forall \alpha \in V_1) \alpha = \sum_{i=1}^n x_i \alpha_i \xrightarrow{\varphi} \alpha' \in V_2, \quad \alpha' := \sum_{i=1}^n x_i \beta_i.$$

Paskaita 2 – 07

Euklido erdvės

Vektorinės erdvės ir poerdviai. Poerdvių suma, sankirta, tiesioginė suma. THLS sprendinių aibės savybės.

Skaliarinė vektorių daugyba. Apibendrintose vektorinėse erdvėse neturime įprastų ir reikalingų *vektoriaus ilgio, normos, kampo tarp vektorių* sąvokų. Jas galima įvesti erdvėje $(V, +, \cdot)$ (paprastumo dėlei, laikykime, kad $L = R$) apibrėžus vektorių *skaliarinę daugybą* (SS).

Ap. Dviejų argumentų realią funkciją $V \times V \xrightarrow{f} R$ vadiname vektorių **skaliarinę daugybą**, jei ta funkcija tenkina tokias keturias aksiomas:

1. $(\forall \alpha, \beta \in V) f(\alpha, \beta) = f(\beta, \alpha)$.
2. $(\forall k \in L)(\forall \alpha, \beta \in V) f(k\alpha, \beta) = kf(\alpha, \beta)$.
3. $(\forall \alpha, \beta, \gamma \in V) f(\alpha + \beta, \gamma) = f(\alpha, \gamma) + f(\beta, \gamma)$.
4. $(\forall \alpha \in V, \alpha \neq O) f(\alpha, \alpha) > 0$.

Paprasčiausias tokios funkcijos erdvėje $(R^n, +, \cdot)$ pavyzdys: kai $\alpha = (a_1, a_2, \dots, a_n)$, o $\beta = (b_1, b_2, \dots, b_n)$ tai

$$f(\alpha, \beta) = \langle \alpha, \beta \rangle = \sum_{j=1}^n d_j a_j b_j. \quad (1)$$

Čia d_j - bet kokie teigiami realieji skaičiai. Dažniausiai imama $d_j = 1, j = 1, 2, \dots, n$.

Ap. n – matę vektorinę erdvę $(E, +, \cdot)$, kurioje yra apibrėžta skaliarinė daugyba, vadinama n – mate Euklido erdve (EE).

Skaliarinės daugybos savybės

1. $(\forall \alpha \in V) \langle \alpha, O \rangle = 0$.
2. $\langle l\alpha + t\beta, \gamma \rangle = l\langle \alpha, \gamma \rangle + t\langle \beta, \gamma \rangle, (\forall l, t \in R)$.
3. $\langle \alpha, \alpha \rangle = 0 \equiv (\alpha = O)$.
4. $(\forall \alpha_i, \beta_j \in V)(\forall l_i, k_j \in R) \left\langle \sum_{i=1}^m l_i \alpha_i, \sum_{j=1}^r k_j \beta_j \right\rangle = \sum_{i=1}^m \sum_{j=1}^r l_i k_j \langle \alpha_i, \beta_j \rangle$.

Vektoriaus ilgis, norma

Ap. Dydis $\|\alpha\| := \langle \alpha, \alpha \rangle$ vadinamas vektoriaus $\alpha \in V$ **norma**, $|\alpha| := \sqrt{\langle \alpha, \alpha \rangle}$ vektoriaus **ilgiu**.

Kai skaliarinė daugyba apibrėžta standartiniu būdu (1) formulės pagalba, tai:

$$|\alpha| := \sqrt{\sum_{i=1}^n d_i^2 a_i^2}.$$

Košy – Buniakovskio nelygybė

Kampas tarp vektorių apibrėžiamas įrodžius tokią teoremą.

Teorema. $(\forall \alpha, \beta \in V) |\langle \alpha, \beta \rangle| \leq |\alpha| \cdot |\beta|$.

Įrodymas. 1. Jei α, β yra tarpusavyje TN, tai su visais $l \in R$, $\alpha \neq l\beta$. Tada

$\alpha - l\beta \neq O$, o iš čia, pagal 4 SS aksiomą, išplaukia, kad kvadratinis trinaris l atžvilgiu

$$\langle \alpha - l\beta, \alpha - l\beta \rangle = l^2 \langle \beta, \beta \rangle - 2\langle \alpha, \beta \rangle \cdot l + \langle \alpha, \alpha \rangle$$

yra visada teigiamas. Taip yra kai jo diskriminantas yra neigiamas, t.y.

$$\langle \alpha, \beta \rangle^2 - \langle \beta, \beta \rangle \cdot \langle \alpha, \alpha \rangle < 0.$$

Tai ir reiškia teoremos tvirtinimą.

2. Kai $\alpha = l\beta$, tai gauname lygybę:

$$|\langle \alpha, \beta \rangle| = |l| \cdot |\alpha|^2 = |l\alpha| \cdot |\alpha| = |\beta| \cdot |\alpha|. \text{ QED.}$$

Kampas tarp vektorių. Ortogonalūs vektoriai

Dabar jau galime apibrėžti kampo φ tarp vektorių α ir β kosinusa.

$$\text{Ap. } \cos \varphi = \frac{\langle \alpha, \beta \rangle}{|\alpha| \cdot |\beta|}.$$

Ap. Du nenuliniai vektoriai α ir β vadinami **ortogonaliais**, jei jų skaliarinė sandauga lygi nuliui.

Pastebėkime, kad ortogonalumo sąvoka susijusi su tuo, kaip vektorinėje erdvėje apibrėžta skaliarinė daugyba. Pvz., vektorių - eilučių erdvėje $(R^3, +, \cdot)$ skaliarinę daugybą apibrėžus (1) formule, kurioje $d_1 = d_2 = d_3 = 1$ vektoriai $\alpha = (1, -2, 5)$, $\beta = (-1, 2, 1)$ yra ortogonalūs, nes:

$$\langle \alpha, \beta \rangle = 1 \cdot (-1) + (-2) \cdot 2 + 5 \cdot 1 = 0.$$

Jeigu $d_1 = 1$, $d_2 = 2$, $d_3 = 3$, tai tie patys vektoriai jau nėra ortogonalūs, nes:

$$\langle \alpha, \beta \rangle = 1 \cdot 1 \cdot (-1) + 2 \cdot (-2) \cdot 2 + 3 \cdot 5 \cdot 1 = 6 \neq 0.$$

Ortogonalizavimas. Ortogonalios ir ortonormuotos bazės

Ap. Vektorių rinkinys $(\alpha)_m$ vadinamas **ortogonalium**, jei $(\forall i \neq j) \langle \alpha_i, \alpha_j \rangle = 0$. Jei, be to, $(\forall i) \|\alpha_i\| = 1$, tai vektorių rinkinys $(\alpha)_m$ vadinamas **ortonormuotu**.

Taikymuose patogiu, kai VE bazė yra ortonormuota. Tada skaičiavimai labai supaprastėja. Pasirodo, VE bazę visada galima ortonormuoti. Pradžioje parodysime, kad rinkinio ortogonalumas ir tiesinė nepriklausomybė yra tarpiai susijusios sąvokos.

Teorema. *Ortogonalus nenulinių vektorių rinkinys yra TN.*

Įr. Tare, kad nenulinių vektorių rinkinys $(\alpha)_m$ yra ortogonalus, bet TP, išvedame:

$$(\exists (l_1, l_2, \dots, l_m) \neq (0, 0, \dots, 0)) \sum_{i=1}^m l_i \alpha_i = O. \quad (2)$$

Jei, pvz., $l_k \neq 0$, tai, dauginami vektorių $\sum_{i=1}^m l_i \alpha_i$ iš vektoriaus α_k ir pasinaudoję rinkinio

$(\alpha)_m$ ortogonalumu, iš (2) gauname:

$$\left\langle \sum_{i=1}^m l_i \alpha_i, \alpha_k \right\rangle = l_k \langle \alpha_k, \alpha_k \rangle = 0.$$

Prieštara. QED.

Teorema. *Kiekvieną TN rinkinį $(\alpha)_m$ galima ortonormuoti.*

Įrodymo žingsniai. Kai $(\alpha)_m$ yra TN vektorių rinkinys, tai jo ortogonalų atitikmenį $(\beta)_m$

gauname imdami: $\beta_k = \alpha_k + \sum_{j=1}^{k-1} c_{kj} \langle \alpha_k, \beta_j \rangle, k = 1 \div m.$

Čia konstantos c_{kj} vienareikšmiškai randamos iš formulių:

$$c_{kj} = -\frac{\langle \alpha_k, \beta_j \rangle}{\|\beta_j\|}, j = 1 \div k-1.$$

Dabar belieka vektorius β_j normuoti pakeičiant juos vektoriais $\varepsilon_j := \frac{1}{\|\beta_j\|} \beta_j$. Aišku,

kad vektorius dauginant iš konstantų jų tarpusavio ortogonalumas nesikeičia.

Ap. VE bazę $(\alpha)_n$ vadinsime ortonormuota, jei rinkinys $(\alpha)_n$ yra ortonormuotas.

Teorema. *Euklido erdvėje vektorių skalarinė sandauga tada ir tik tada yra lygi koordinačių sandaugų sumai, kai erdvės bazė yra ortonormuota.*

Įr. 1. Kai bazėje $(\alpha)_n$ bet kokiems vektoriams

$$\alpha = \sum_{i=1}^n x_i \alpha_i, \beta = \sum_{i=1}^n y_i \alpha_i$$

turime

$$\langle \alpha, \beta \rangle = \sum_{i=1}^n x_i y_i,$$

tai baziniams vektoriams iš tiesinės išraiškos

$$\alpha_k = 0 \cdot \alpha_1 + 0 \cdot \alpha_2 + \dots + 0 \cdot \alpha_{k-1} + 1 \cdot \alpha_k + 0 \cdot \alpha_{k+1} + \dots + 0 \cdot \alpha_n$$

gauname

$$(\forall k) \langle \alpha_k, \alpha_k \rangle = 1, (\forall k \neq j) \langle \alpha_k, \alpha_j \rangle = 0.$$

2. Kai bazė $(\alpha)_n$ yra ortonormuota, tai iš skaliarinės daugybos savybių išplaukia:

$$\langle \alpha, \beta \rangle = \sum_{i=1}^n \sum_{j=1}^n x_i y_j \langle \alpha_i, \alpha_j \rangle = \sum_{i=1}^n x_i y_i. \quad \text{QED.}$$

EE izomorfizmai

Ap. Dvi EE $(E_1, +, \cdot)$ ir $(E_2, +, \cdot)$ vadinsime **izomorfiškomis** (atitinkamai – homomorfiškomis), jei tarp aibių E_1 ir E_2 galima nustatyti bent vieną tokią bijekciją $\varphi: E_1 \longleftrightarrow E_2$ (atitinkamai – siurjekciją), kad galiotų sąlygos:

1. $(\forall \alpha, \beta \in E_1) \varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta).$
2. $(\forall \alpha \in E_1) (\forall l \in L) \varphi(l \cdot \alpha) = l \varphi(\alpha).$
3. $(\forall \alpha, \beta \in E_1) \langle \alpha, \beta \rangle = \langle \varphi(\alpha), \varphi(\beta) \rangle.$

Teorema. Bet kokios dvi n – matės EE virš $\mathbf{R}$ yra izomorfiškos.

Įr. Kai $(E_1, +, \cdot)$ ir $(E_2, +, \cdot)$ dvi n – matės EE, o $(\varepsilon)_n$ ir $(\eta)_n$ jų ortonormuotos bazės, tai bijekcija φ tarp bazinių aibių E_1 ir E_2 apibrėžiama šitaip:

$$(\forall \alpha \in E_1) \alpha = \sum_{i=1}^n x_i \varepsilon_i \xrightarrow{\varphi} \alpha' \in E_2, \quad \alpha' := \sum_{i=1}^n x_i \eta_i.$$

Belieka patikrinti 1 – 3 apibrėžimo reikalavimus.

QED.

Praktiniai poreikiai dažniau pateikia situacijas, kurios aprašomos (modeliuojamos) ne lygtimis, o *nelygybėmis* bei jų sistemomis. Panagrinėsime paprasčiausią, - *tiesinių* nelygybių atvejį. Aukštesnio laipsnio nelygybių sistemų ir su jomis susietų optimizavimo uždavinių sprendimui yra sukurti specialūs, sudėtingi metodai, kurių studijos reikalauja gilesnio matematinio pasiruošimo ir žymiai daugiau laiko, todėl į mūsų studijų programą ši tematika neįtraukta.

$$a_1x_1 + a_2x_2 + \dots + a_nx_n \leq b. \quad (1)$$

Kaip ir lygtyse, čia a_i , $i = 1, 2, \dots, n$ ir b yra bet kokie *žinomi* skaičiai (gali būti ir kompleksiniai, arba ir bet kokio lauko elementai). Skaičiai a_i vadinami (1) nelygybės *koeficientais*, o skaičius b – *laisvuju nariu*. Vietoje ženklo “ $\leq$ ” gali būti negriežtos nelygybės ženklas “ $<$ ”. Nelygybė su ženklu “ $\geq$ ” (ar “ $>$ ”) lengvai suvedama į (1) pavidalą padauginant ją iš minus vieneto. Pavyzdžiui, $-3x_1 + 10x_2 - x_3 - 4x_4 \geq -7$ (arba, atitinkamai, $3x_1 - 10x_2 + x_3 + 4x_4 \leq 7$) yra nelygybė su *keturiais* kintamaisiais.

*Ap. Sutvarkytą skaičių rinkinį $(k_1, k_2, \dots, k_n)$ vadiname tiesinės nelygybės (1) **sprendiniu**, jei jis tenkina šią nelygybę (arba kitaip: rinkinys $(k_1, k_2, \dots, k_n)$ *priklauso* (1) predikato teisingumo aibei).*

Pvz., rinkinys $(-1, 0, 1, -1)$ šią nelygybę *tenkina* (įsitikinkite tuo!), todėl jis yra jos sprendinys.

Kelių (1) pavidalo nelygybių konjunkcija vadinama *tiesinių nelygybių sistema*. Jos bendrasis pavidalas yra toks:

$$\left\{ \begin{array}{l} a_{11}x_1 + a_{12}x_2 + ... + a_{1n}x_n \leq b_1, \\ a_{21}x_1 + a_{22}x_2 + ... + a_{2n}x_n \leq b_2, \\ \\ a_{m1}x_1 + a_{m2}x_2 + ... + a_{mn}x_n \leq b_m . \end{array} \right. \quad (2)$$

(Taigi, TNS yra m predikatų (n -viečių) konjunkcija).

Ap. TNS sprendiniu vadiname sutvarkytą skaičių rinkinį $(k_1, k_2, \dots, k_n)$, kuris tenkina visas sistemos (2) nelygybes.

Ap. TNS neneigiamu sprendiniu vadiname tokį sprendinį $(k_1, k_2, \dots, k_n)$, kurio visos komponentės k_i yra neneigiami realieji skaičiai.

Neneigiamo sprendinio sąvokos prireikia todėl, kad komponentės k_i praktikoje dažniausiai reiškia arba prekių kiekius, arba jų kainas, ar kitokius panašius dydžius, kurie pagal prasmę turi būti neneigiami.

Kaip matome, terminai ir sąvokos - panašūs naudotiems TLS situacijoje. Deja, TNS sprendimo keliai gerokai sudėtingesni, nei TLS atveju. Todėl mes susipažinsime tik su paprasčiausiu TNS su *dviem kintamaisiais* sprendimo metodu, kuris, beje, iliustruos ir bendresnes idėjas.

TNS tenka spręsti taip vadinamuose *tiesinio programavimo* (arba bendriau – *optimizavimo*) uždaviniuose. Žemiau pateiksime jų bendrą formuluotę, o pradėsime nuo pavyzdžio.

Sakykime, Jūs esate atsakingas už parduotuvės (ar parduotuvių) aprūpinimą prekėmis. Rytą, atėję į darbą, pastebėjote (Jums pranešė), kad sandėlyje trūksta *dvių* rūšių prekių. Tad darbo dienos bėgyje Jūs spręsite uždavinį: *dviuose* mieste esančiose didmeninėse bazėse nupirkti savo parduotuvei trūkstamų prekių. Planuojamą pirkti i -tosios rūšies prekęs j – oje bazėje vienetų kiekį pažymėkime x_{ij} . Be to, Jūs žinote, kad i -tosios rūšies prekės vieneto kaina j -toje bazėje yra vidutiniškai a_{ij} litų. Tad, pirkdamas prekes j -toje bazėje, iš viso sumokėsite $a_{1j}x_{1j} + a_{2j}x_{2j}$ litų. Bet įvairios ekonominės ir asmeninės priežastys neleidžia Jums j – toje bazėje išleisti daugiau kaip b_j litų. Todėl prekių kiekiai (pagal prasmę – *neneigiami skaičiai*) x_{ij} , turi tenkinti nelygybių sistemą:

$$\begin{cases} a_{11}x_{11} + a_{21}x_{21} \leq b_1, \\ a_{12}x_{12} + a_{22}x_{22} \leq b_2. \end{cases}$$

Atsivežtosios prekės, uždėjus prekybos antkainį, turi būti parduotos. Susumavus visas išlaidas, kiekvienas nupirktosios prekės vienetas davė Jums, sakykime, c_{ij} litų pelno. Tada funkcija (dažnai vadinama *tikslo funkcija*)

$$f(x_{11}, x_{12}, x_{21}, x_{22}) := c_{11}x_{11} + c_{12}x_{12} + c_{21}x_{21} + c_{22}x_{22}$$

reiškia *visą Jūsų gautą pelną*.

Akivaizdu, kad Jūsų tikslas yra: taip suplanuoti prekių pirkimą, jų pristatymą bei pardavimą, kad tikslo funkcija $f(x_{11}, x_{12}, x_{21}, x_{22})$ įgytų *didžiausią* reikšmę.

Dar paprastesniu atveju, kai dėl kokių nors priežasčių (pvz., taip patogiau planuoti transportavimą) abiejose bazėse planuojame pirkti vienodus abiejų rūšių prekių kiekius, kintamųjų skaičius sumažėja iki dviejų: $x := x_{11} = x_{12}$ ir $y := x_{21} = x_{22}$.

Standartinis tiesinio programavimo uždavinys formuluojamas taip:

$$\left\{ \begin{array}{l} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n \leq b_1 , \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n \leq b_2 , \\ \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n \leq b_m \end{array} \right.$$
$$f(x_1, x_2, \dots, x_n) := c_1 x_1 + c_2 x_2 + \dots + c_n x_n.$$

Aptarsime standartinio tiesinio programavimo uždavinio *geometrinį* sprendimo būdą paprasčiausiu atveju, kai $n = 2$. Tada tikslo funkcija yra ypač paprasta $f(x_1, x_2) = c_1 x_1 + c_2 x_2$.

Naudinga pastebėti, kad $f(x_1, x_2)$ yra dviejų vektorių: žinomo $\vec{c} = (c_1, c_2)$ ir nežinomo $\vec{x} = (x_1, x_2)$ skaliarinė sandauga, t.y.

$$f(x_1, x_2) = \langle \vec{x}, \vec{c} \rangle.$$

Kita vertus, pažymėję kampą tarp vektorių $\vec{x} = (x_1, x_2)$ ir $\vec{c} = (c_1, c_2)$ raide α , turime:

$$f(x_1, x_2) = \langle \vec{x}, \vec{c} \rangle = |\vec{x}| \cdot |\vec{c}| \cdot \cos \alpha.$$

Dydis $\left| \vec{c} \right|$ yra pastovus, o sandauga $\left| \vec{x} \right| \cdot \cos \alpha$ geometriškai reiškia vektoriaus $\vec{x}$ *projekciją* į vektorių $\vec{c}$. Darome išvadą, kad uždavinio sprendiniu bus tas vektorius $\vec{x} = (x_1, x_2)$, *kurio projekcija į duotąjį vektorių $\vec{c}$ yra didžiausia.*

Lieka išsiaiškinti, kaip rasti *leistinų sprendinių* aibę, t.y. kaip išspręsti TNS.

Kai kintamųjų tėra du, tai TNS galima spręsti geometriškai, tuo pat metu įvedant bei paaiškinant ir bendram atvejui reikalingas savokas ir idėjas.

Tiesinė nelygybė su dviem kintamaisiais

$$a_1x_1 + a_2x_2 \leq b$$

geometriškai reiškia pusplokštumą, kurios skiriamoji linija yra tiesė

$$a_1x_1 + a_2x_2 = b.$$

Nesunku pastebėti, kad kelių tokių nelygybių bendri sprendiniai (t.y. kelių pusplokštumų sankirta) sudaro aibę, kuri gali būti:

- tuščia,
- *iškilas* daugiakampis,
- neapibrėžta *iškila* aibė.

Prisiminkime *iškilo daugiakampio* sąvoką, aptartą dar vidurinės mokyklos geometrijos pamokose. Tiesinio programavimo uždaviniuose iškilos aibės sąvoka yra viena iš svarbiausių.

Ap. Aibės R^n poaibis A ($A \subset R^n$) vadinamas **iškilu**, jei su kiekvienu realiuoju $t \in [0, 1]$ ir bet kuriais $\alpha, \beta \in A$ elementas $t\alpha + (1-t)\beta$ irgi priklauso A .

Šis formalus apibrėžimas tuo atveju, kai $n = 2, 3$, turi aiškia geometrinę prasmę: aibė A yra *iškila*, jei sujungus bet kuriuos du jos taškus α ir β tiesės atkarpa, visi tos atkarpos taškai irgi priklauso aibei A .

Nesunku įrodyti tokią teoremą.

Teorema. Suderintos TNS (ar TLS) neneigiamų sprendinių aibė yra *iškila*.

Kai $n = 2$, ta aibė yra, kaip minėjome, yra *iškilas* daugiakampis, o kai $n = 3$, - TNS sprendinių aibė yra *iškilas* erdvinis briaunainis. Be to, tiek šiais abiem atvejais, tiek bendru atveju (kai $n \geq 4$) sprendinių aibė gali būti ir *neapibrėžta*. Pavyzdžiui, TNS

$$\begin{cases} x - y \leq 2, \\ x - y \geq 1, \\ x, y \geq 0 \end{cases}$$

sprendinių aibė geometriškai yra begalinė juosta pirmojo ketvirčio taškų esančių tarp tiesių $x - y = 2$ ir $x - y = 1$. Pastebėsime, kad ir neapibrėžta sprendinių aibė formaliai išlaiko iškilumo savybę.

Labai svarbi yra iškilos aibės *ekstreminio taško* sąvoka.

Ap. Iškilos aibės A elementą (tašką) γ vadinsime **ekstreminiu tašku**, jei su jokiais $\alpha, \beta \in A$ ir $0 < t < 1$, jo negalima užrašyti pavidalu $t\alpha + (1-t)\beta$.

Kai $n = 2, 3$, šiai sąvokai irgi galima suteikti aiškia geometrinę prasmę. Iškilajame daugiakampyje *ekstreminiai taškai* yra ne kas kita, kaip jo *viršūnės*; atitinkamai, briaunainyje, - tai – *erdvinių kampų viršūnės*. Neapibrėžtos aibės atveju, ekstreminiai taškai yra be galo nutolę.

Suformuluosime svarbią teoremą.

Teorema. Jei sprendinių aibė yra aprėžta, tai bet kuri tikslo funkcija įgyja savo maksimalią reikšmę bent viename ekstreminiame taške.

Iš šios teoremos išplaukia, kad ieškant *optimalaus* sprendinio, nereikia tikrinti visų sprendinių, užtenka pasidomėti tik ekstreminiais sprendinių aibės taškais.

Be to, yra metodų (vienas iš jų vadinamas *simpleks*-metodu), įgalinančių ir ekstreminius taškus tyrinėti ne bet kaip, o tiksliai: kaskart ieškant tokio ekstreminio taško, kuriame *tikslo funkcijos* reikšmė būtų jau mažesnė, nei prieš tai.

Užduotis. Geometriškai pavaizduokite TNS sprendinių aibes.

$$a. \begin{cases} x - y \leq 2, \\ x - y \geq 1, \\ -3 \leq x \leq 5. \end{cases} \quad b. \begin{cases} 5x - 3y \leq 5, \\ x + y \leq 4 \\ y \leq 3, \\ x \geq 0. \end{cases}$$

Raskite tiesinių funkcijų $f_1(x, y) = -2x + y$ bei $f_2(x, y) = -x - 4y$ maksimalias ir minimalias reikšmes šių TNS sprendinių aibėse.

Paskaita 2 – 09

Tiesiniai operatoriai

TNS. Paprasčiausi optimizavimo uždaviniai.

Operatoriai

Šioje paskaitoje trumpai susipažinsime su funkcijomis, kurių argumentai ir reikšmės yra ne skaičiai, o vektoriai.

Ap. Jei turime dvi VE virš lauko $\mathbf{R}$ $(V_1, +, \cdot)$ ir $(V_2, +, \cdot)$, tai funkciją $V_1 \xrightarrow{f} V_2$ vadiname **operatoriumi**.

Operatorius žymėsime raidėmis $\mathcal{A}, \mathcal{B}, \mathcal{C} \dots$

Ap. Du operatorius $\mathcal{A}: V_1 \longrightarrow V_2$ ir $\mathcal{B}: V_1 \longrightarrow V_2$ vadinsime **lygiais**, jei

$$(\forall \alpha \in V_1) \mathcal{A}(\alpha) = \mathcal{B}(\alpha).$$

Ap. Operatorių $\mathcal{A}: V_1 \longrightarrow V_2$ vadinsime **tiesiniu operatoriumi** (TO), jei

- 1) $(\forall \alpha, \beta \in V_1) \mathcal{A}(\alpha + \beta) = \mathcal{A}(\alpha) + \mathcal{A}(\beta),$
- 2) $(\forall \alpha \in V_1)(\forall l \in R) \mathcal{A}(l\alpha) = l \mathcal{A}(\alpha).$

Pirmoji sąlyga dažnai vadinama operatoriaus *adityvumo* savybe, antroji – *tiesiškumo* savybe. TO kai kada vadinamas *tiesine transformacija*.

Iš apibrėžimo išplaukia, kad $\mathcal{A}(O_{V_1}) = O_{V_2}$.

Bet to, remiantis MIP, nesunkiai patikrinama, kad bet kokiam TO $\mathcal{A}: V_1 \longrightarrow V_2$ yra teisinga savybė:

$$(\forall l_i \in R, i = 1 \div r)(\forall \alpha_i \in V_1, i = 1 \div r) \mathcal{A}\left(\sum_{i=1}^r l_i \alpha_i\right) = \sum_{i=1}^r l_i \mathcal{A}(\alpha_i).$$

Pavyzdžiai. 1. Bet kokiam trimatės erdvės $(R^3, +, \cdot)$ vektoriui $\alpha = (x_1, x_2, x_3)$, priskirsime keturmatį vektorių $\alpha' = (2x_1, x_1 + x_2, x_3, 3) \in R^4$. Akivaizdu, kad šitokia taisyklė yra funkcija, taigi, *operatorius*. Pažymėkime jį $\mathcal{A}$. T.y. $\mathcal{A}: R^3 \longrightarrow R^4$ ir $\mathcal{A}(\alpha) = \alpha'$.

2. Operatorių, kuris kiekvienam $\alpha \in R^m$ priskiria vektorių $O_n = (0, 0, \dots, 0) \in R^n$, vadinsime *nuliniu operatoriumi* ir žymėsime $\mathcal{O}$. T.y. $\mathcal{O}: R^m \longrightarrow R^n$.

3. Operatorių, kuris kiekvienam $\alpha \in R^n$ priskiria tą patį vektorių $\alpha \in R^n$ vadinsime *vienetiniu operatoriumi* ir žymėsime $\mathcal{E}$. Simboliais: $\mathcal{E}: R^n \longrightarrow R^n$.

4. Operatorių, kuris kiekvienam $\alpha = (x_1, x_2, \dots, x_n) \in R^n$ priskiria vektorių $\alpha = (x_1, x_2, \dots, x_m, 0, \dots, 0) \in R^n$, $m < n$ vadinsime *projektoriumi* ir žymėsime $\mathcal{P}$.

5. Funkcija $\mathcal{B}: R^3 \longrightarrow R^3$, apibrėžiama taisykle:

$$(\forall \alpha = (x_1, x_2, x_3) \in R^3) \quad \mathcal{B}(\alpha) = (x_1, 2x_2, 3x_3),$$

irgi yra operatorius.

Nesunku patikrinti, kad operatoriai $\mathcal{Q}, \mathcal{E}, \mathcal{P}, \mathcal{B}$ yra TO. Operatorius $\mathcal{A}$ nėra tiesinis, nes netenkina adityvumo sąlygos: kai $\beta = (y_1, y_2, y_3)$, tai $\mathcal{A}(\alpha + \beta) =$

$$= \mathcal{A}((x_1 + y_1, x_2 + y_2, x_3 + y_3)) = (2(x_1 + y_1), x_1 + y_1 + x_2 + y_2, x_3 + y_3, 3).$$

Tačiau

$$\begin{aligned} \mathcal{A}(\alpha) + \mathcal{A}(\beta) &= (2x_1, x_1 + x_2, x_3, 3) + (2y_1, y_1 + y_2, y_3, 3) = \\ &= (2x_1 + 2y_1, x_1 + x_2 + y_1 + y_2, x_3 + y_3, 6) \neq (2(x_1 + y_1), x_1 + y_1 + x_2 + y_2, x_3 + y_3, 3). \end{aligned}$$

Tiesinio operatoriaus matrica

Tarkime TO $\mathcal{A}$ yra apibrėžtas erdvėje $(V_1, +, \cdot)$, kurios dimensija yra m , o reikšmės įgyja erdvėje $(V_2, +, \cdot)$, kurios dimensija yra n . Jei $(\alpha)_m$ yra kokia nors erdvės $(V_1, +, \cdot)$ bazė, tai bet koks vektorius $\alpha \in V_1$ tiesiškai išsireiškia per bazę $(\alpha)_m$, t.y. egzistuoja tokie realieji skaičiai $x_i, i = 1 \div m$, kad

$$\alpha = \sum_{i=1}^m x_i \alpha_i.$$

Kadangi $\mathcal{A}$ yra TO, tai iš čia išplaukia lygybė:

$$\mathcal{A}(\alpha) = \sum_{i=1}^m x_i \mathcal{A}(\alpha_i). \quad (1)$$

Bet $\mathcal{A}(\alpha_i) \in V_2$, todėl, jei $(\beta)_n$ yra erdvės $(V_2, +, \cdot)$ bazė, tai turi egzistuoti skaičiai $a_{ij}, j = 1 \div n$, kad:

$$\mathcal{A}(\alpha_i) = \sum_{j=1}^n a_{ij} \beta_j. \quad (2)$$

Taigi, fiksuotoms bazėms $(\alpha)_m$ ir $(\beta)_n$, TO $\mathcal{A}$ bus apibrėžtas tada ir tik tada, kai žinosime skaičius a_{ij} .

Ap. Eilės $m \times n$ matricą $A := (a_{ij})$ vadiname operatoriaus $\mathcal{A}$ matrica.

Pavyzdys. 5 pavyzdyje, imdami standartinę erdvės R^3 bazę $(\epsilon)_3$, turėsime:

$$\mathcal{B}(\epsilon_1) = \mathcal{B}((1, 0, 0)) = (1, 0, 0); \quad \mathcal{B}(\epsilon_2) = \mathcal{B}((0, 1, 0)) = (0, 2, 0);$$

$$\mathcal{B}(\epsilon_3) = \mathcal{B}((0, 0, 1)) = (0, 0, 3).$$

Todėl operatorių $\mathcal{B}$ vienareikšmiškai atitinka jo matrica B :

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Parodysime, kad TO poveikis *tolygus vektoriaus koordinačių eilutės daugybai iš operatoriaus matricos.*

1 teorema. Tiesinio operatoriaus $\mathcal{A}: V_1 \longrightarrow V_2$ reikšmės (vaizdo) $\mathcal{A}(\alpha) \in V_2$ koordinačių eilutė lygi pirmavaizdžio $\alpha \in V_1$ koordinačių eilutei, padaugintai iš dešinės iš operatoriaus $\mathcal{A}$ matricos A .

Įr. Tarkime $\alpha \in V_1$ yra bet koks vektorius, $(x_1, x_2, \dots, x_m)$ yra jo koordinačių erdvės V_1 bazėje $(\alpha)_m$ eilutė, $\mathcal{A}(\alpha) \in V_2$ yra jo vaizdas, o $(y_1, y_2, \dots, y_n)$ yra jo koordinačių erdvės V_2 bazėje $(\beta)_n$ eilutė. Iš (1-2) formulių gauname:

$$\sum_{j=1}^n y_j \beta_j = \mathcal{A}(\alpha) = \sum_{i=1}^m x_i \mathcal{A}(\alpha_i) = \sum_{i=1}^m x_i \sum_{j=1}^n a_{ij} \beta_j = \sum_{j=1}^n \left(\sum_{i=1}^m a_{ij} x_i \right) \beta_j.$$

Remdamiesi vektoriaus koordinačių duotoje bazėje vienareikšmiškumu, turime:

$$y_j = \sum_{i=1}^m x_i a_{ij}, \quad j = 1 \div n,$$

arba

$$(y_1, y_2, \dots, y_n) = (x_1, x_2, \dots, x_m) A.$$

QED.

TO veiksmas

Dabar parodysime, kad tarp TO $\mathcal{A}: V_1 \longrightarrow V_2$ aibės $\mathcal{T}(V_1, V_2)$ ir matricų aibės $M_{m \times n}(R)$ yra ne tik bijekcijos, bet ir izomorfizmo sąryšis.

Pirmiausia, pagal analogiją su matricomis, apibrėšime *TO sudėtį* ir *TO daugybą iš skaičiaus*.

Tarkime $\mathcal{A}, \mathcal{B} \in \mathcal{T}(V_1, V_2)$ yra bet kokie TO.

Ap. Sąlyga

$$(\forall \alpha \in V_1) \mathcal{C}(\alpha) = \mathcal{A}(\alpha) + \mathcal{B}(\alpha)$$

apibrėžiamas operatorius $\mathcal{C}$ vadinamas operatorių $\mathcal{A}$ ir $\mathcal{B}$ **suma**.

Rašome: $\mathcal{C} = \mathcal{A} + \mathcal{B}$.

Ap. Sąlyga

$$(\forall \alpha \in V_1)(\forall l \in R) \mathcal{D}(\alpha) = l \cdot \mathcal{A}(\alpha)$$

apibrėžiamas operatorius $\mathcal{D}$ vadinamas skaičiaus l ir operatoriaus $\mathcal{A}$ sandauga.

Rašome: $\mathcal{D} = l\mathcal{A}$.

2 teorema. Operatoriai $\mathcal{C}$ ir $\mathcal{D}$ yra tiesiniai. Tiksliau: $\mathcal{C}, \mathcal{D} \in \mathcal{T}(V_1, V_2)$.

Įr. Apibrėžimuose nurodytos sąlygos rodo, kad ir $\mathcal{C}$, ir $\mathcal{D}$ tikrai yra apibrėžti erdvėje V_1 ir įgyja reikšmes iš erdvės V_2 . Lieka patikrinti adityvumo ir tiesiškumo sąlygas, formuluojamas TO apibrėžime. Įrodysime tik adityvumo savybę operatorių $\mathcal{A}$ ir $\mathcal{B}$ sumai $\mathcal{C}$, bei tiesiškumo savybę operatoriaus $\mathcal{A}$ ir realaus skaičiaus l sandaugai $\mathcal{D}$. Kitas savybes nesunkiai įrodysite savarankiškai.

1. $(\forall \alpha, \beta \in V_1) \mathcal{C}(\alpha + \beta) = \mathcal{A}(\alpha + \beta) + \mathcal{B}(\alpha + \beta) \stackrel{TO\ ap.}{=} \mathcal{A}(\alpha) + \mathcal{A}(\beta) + \mathcal{B}(\alpha) + \mathcal{B}(\beta) \stackrel{K,A}{=} [\mathcal{A}(\alpha) + \mathcal{B}(\alpha)] + [\mathcal{A}(\beta) + \mathcal{B}(\beta)] \stackrel{TO\ ap.}{=} \mathcal{C}(\alpha) + \mathcal{C}(\beta)$.
 2. $(\forall \alpha \in V_1)(\forall k \in R) \mathcal{D}(k\alpha) = l \mathcal{A}(k\alpha) \stackrel{TO\ ap.}{=} l[k\mathcal{A}(\alpha)] = k[l\mathcal{A}(\alpha)] \stackrel{TO\ ap.}{=} k\mathcal{D}(\alpha)$.
- QED.

3 teorema. Algebrinė struktūra $(\mathcal{T}(V_1, V_2), +, \cdot)$ yra vektorinė erdvė.

Įrodymo schema. 2 teoremoje parodėme, kad TO suma bei operatoriaus ir skaičiaus sandauga yra TO. Tad TO sudėtis bei TO daugyba iš skaičiaus yra algebrinės operacijos.

Trumpai aptarsime kitas VE aksiomas. Aibėje $\mathcal{T}(V_1, V_2)$ lygybe

$$(\forall \alpha \in V_1) \mathcal{O}(\alpha) = O_{V_2}$$

galima apibrėžti (žr. 2 pavyzdį) nulinį operatorių $\mathcal{O}$. Savo ruožtu, operatorių $\mathcal{B}$, kuris apibrėžiamas lygybe:

$$(\forall \alpha \in V_1) \mathcal{B}(\alpha) = -\mathcal{A}(\alpha),$$

tenkina operatoriui TO $\mathcal{A}$ priešingo operatoriaus apibrėžimą. T.y. $\mathcal{B} = -\mathcal{A}$.

Be to, nesunkiai parodoma (kaip ir 2 teoremoje), kad operatoriai $\mathcal{O}$, $\mathcal{B}$ yra tiesiniai.

Kadangi su visais $\alpha \in V_1$

$$(\mathcal{A} + \mathcal{B})(\alpha) = \mathcal{A}(\alpha) + \mathcal{B}(\alpha) \stackrel{K}{=} \mathcal{B}(\alpha) + \mathcal{A}(\alpha) = (\mathcal{B} + \mathcal{A})(\alpha),$$

tai TO sudėtis yra komutatyvi. Panašiai patikrinamas ir operatorių sudėties asociatyvumas.

Todėl galima tvirtinti, kad struktūra $(\mathcal{T}(V_1, V_2), +)$ yra adicinė Abelio grupė.

Belieka įsitikinti, kad TO daugyba iš skaičiaus yra dukart distributyvi. T.y.:

1. $(\forall l, k \in R)(l + k)\mathcal{A} = l\mathcal{A} + k\mathcal{A}$,
2. $(\forall l \in R)(\forall \mathcal{A}, \mathcal{B} \in \mathcal{T}(V_1, V_2)) l(\mathcal{A} + \mathcal{B}) = l\mathcal{A} + l\mathcal{B}$.

Tikiuosi, kad skaitytojai jau įgudo ir šį patikrinimą be vargo atliks savarankiškai.

Tad tuo 3 teoremos įrodymo aptarimą ir baigiame.

4 teorema. *Vektorinės erdvės $(\mathcal{A}(V_1, V_2), +, \cdot)$ ir $(M_{m \times n}(R), +, \cdot)$ yra izomorfiškos.*

Įr. Bijekciją (žymėkime ją raide φ) tarp bazinių aibių jau esame nustatę: kai $\mathcal{A}$ ir $\mathcal{B}$ yra bet kokie TO iš aibės $\mathcal{A}(V_1, V_2)$, o A ir B atitinkamai yra jų matricos iš aibės $M_{m \times n}(R)$, tai

$$\varphi(\mathcal{A}) = A = (a_{ij}), \quad \varphi(\mathcal{B}) = B = (b_{ij}).$$

Patikrinsime, ar TO *sumos vaizdas lygus vaizdų sumai*, t.y. ar TO sumos $\mathcal{A} + \mathcal{B}$ matrica tikrai yra $A + B$.

Tarkime $(\alpha)_m$ yra kokia nors erdvės $(V_1, +, \cdot)$ bazė, o $(\beta)_n$ - erdvės $(V_2, +, \cdot)$ bazė.

Tada:

$$\mathcal{A}(\alpha_i) = \sum_{j=1}^n a_{ij} \beta_j, \quad \mathcal{B}(\alpha_i) = \sum_{j=1}^n b_{ij} \beta_j, \quad i = 1 \div m.$$

Kadangi

$$(\mathcal{A} + \mathcal{B})(\alpha_i) = \mathcal{A}(\alpha_i) + \mathcal{B}(\alpha_i) = \sum_{j=1}^n (a_{ij} + b_{ij}) \beta_j,$$

tai

$$\varphi(\mathcal{A} + \mathcal{B}) = (a_{ij} + b_{ij}) = A + B = \varphi(\mathcal{A}) + \varphi(\mathcal{B}).$$

Panašiai samprotaujant, gauname:

$$(l\mathcal{A})(\alpha_i) = l\mathcal{A}(\alpha_i) = l \sum_{j=1}^n a_{ij} \beta_j = \sum_{j=1}^n (la_{ij}) \beta_j,$$

t.y.

$$\varphi(l\mathcal{A}) = (la_{ij}) = lA = l\varphi(\mathcal{A}).$$

QED.

Išvada. $\dim \mathcal{A}(V_1, V_2) = mn$.

TO daugyba

Panaginėsime TO, kurie ir apibrėžti, ir reikšmes įgyja toje pačioje vektorinėje erdvėje V , $\dim V = n$. Tokie TO vadinami *erdvės V tiesiniais operatoriais*. Jų aibę žymėsime $\mathcal{A}(V)$. Aišku, kad erdvė $(\mathcal{A}(V), +, \cdot)$ yra izomorfiška n – osios eilės kvadratinių matricų erdvei $(M_n(R), +, \cdot)$.

Pasirodo, kad tokių TO erdvėje galima pamatyti dar vieną analogiją su matricomis, tuo parodant, kad atitiktis tarp bazinių aibių $\mathcal{T}(V)$ ir $M_n(R)$ yra gilesnė, nei paprastas izomorfizmas.

Ap. Erdvės $\mathcal{T}(V)$ tiesinių operatorių $\mathcal{A}, \mathcal{B}$ sandauga vadinamas operatorius $\mathcal{C}$ apibrėžiamas lygybe:

$$(\forall \alpha \in V) \mathcal{C}(\alpha) = \mathcal{B}(\mathcal{A}(\alpha)).$$

Kitaip sakant, operatorių $\mathcal{A}, \mathcal{B}$ sandauga yra “paeiliui” veikiantis operatorius: iš pradžių pirmavaizdį α operatoriumi $\mathcal{A}$ atvaizduojame į vektorių $\mathcal{A}(\alpha)$, po to, pastarąjį vektorių veikiamo operatoriumi $\mathcal{B}$ ir gauname galutinį rezultatą $\mathcal{B}(\mathcal{A}(\alpha))$.

Pavyzdys. Plokštumoje R^2 operatorių $\mathcal{A}$ apibrėžkime kaip projektorių į x – sų ašį, o operatorius $\mathcal{B}$ lai reiškia posūkį apie koordinatų pradžios tašką 90° kampų (prieš laikrodžio rodyklę). Abu šie operatoriai yra tiesiniai. Kai $\alpha = (1, 1)$, tai

$$\mathcal{A}(\alpha) =: \beta = (1, 0), \text{ o } (\mathcal{A}\mathcal{B})(\alpha) = \mathcal{B}(\mathcal{A}(\alpha)) = \mathcal{B}(\beta) = (0, 1).$$

$$\text{Kadangi } \mathcal{B}(\alpha) = (-1, 1), \text{ tai } (\mathcal{B}\mathcal{A})(\alpha) = \mathcal{A}(\mathcal{B}(\alpha)) = \mathcal{A}((-1, 1)) = (-1, 0).$$

Konstatuojame, kad $\mathcal{A}\mathcal{B} \neq \mathcal{B}\mathcal{A}$.

Išvada. Operatorių daugyba yra nekomutatyvi.

5 teorema. *TO sandauga yra TO.*

Įr. Iš tikrųjų, su kiekvienu $l \in R$ ir bet kokiais $\alpha, \beta \in V$, remdamiesi atitinkamais apibrėžimais, TO sandagai $\mathcal{A}\mathcal{B}$ gauname:

1. $(\mathcal{A}\mathcal{B})(l\alpha) = \mathcal{B}(\mathcal{A}(l\alpha)) = \mathcal{B}(l\mathcal{A}(\alpha)) = l\mathcal{B}(\mathcal{A}(\alpha)) = l(\mathcal{A}\mathcal{B})(\alpha),$
2. $(\mathcal{A}\mathcal{B})(\alpha + \beta) = \mathcal{B}(\mathcal{A}(\alpha + \beta)) = \mathcal{B}(\mathcal{A}(\alpha) + \mathcal{A}(\beta)) =$
 $= \mathcal{B}(\mathcal{A}(\alpha)) + \mathcal{B}(\mathcal{A}(\beta)) = (\mathcal{A}\mathcal{B})(\alpha) + (\mathcal{A}\mathcal{B})(\beta).$

QED.

6 teorema. *TO sandaugos matrica lygi dauginamųjų operatorių matricų sandagai.*

Įr. Tarkime $\mathcal{A}, \mathcal{B} \in \mathcal{T}(V)$ yra bet kokie TO, o A, B - jų matricos. Erdvės V bazėje $(\alpha)_n$ kiekvienas vektorius turi vienareikšmiškai nustatomą koordinatų eilutę. Jei $(x_1, x_2, \dots, x_m)$ yra vektoriaus α koordinatės, $(y_1, y_2, \dots, y_n)$ žymi vektoriaus $\mathcal{A}(\alpha)$ koordinatų eilutę, o $(z_1, z_2, \dots, z_n)$ yra vektoriaus $(\mathcal{A}\mathcal{B})(\alpha)$ koordinatų eilutė, tai, remdamiesi 1 teorema, su kiekvienu $\alpha \in V$, gauname:

$$(y_1, y_2, \dots, y_n) = (x_1, x_2, \dots, x_m)A,$$

$$(z_1, z_2, \dots, z_n) = (y_1, y_2, \dots, y_n)B.$$

Kadangi matricų daugyba asociatyvi, tai iš pastarųjų lygybių išvedame:

$$(z_1, z_2, \dots, z_n) = (x_1, x_2, \dots, x_m)(AB),$$

o tai ir reiškia, kad operatoriaus $\mathcal{AB}$ matrica yra AB . QED.

Išvada. AS $(\mathcal{T}(V), +, \cdot)$ yra nekomutatyvus žiedas. Čia “+” reiškia TO sudėtį, o “.” tokių operatorių daugybą.

Analogijas tarp TO ir matricų galima tęsti ir toliau. Lygybėmis

$$\mathcal{AA}^{-1} = \mathcal{A}^{-1}\mathcal{A} = \mathcal{E}$$

apibrėžus operatoriui $\mathcal{A}$ atvirkštinį operatorių (čia $\mathcal{E}$ žymi vienetinį operatorių, žr. 3 pvz.), galima parodyti, kad:

- TO atvirkštinis operatorius irgi yra TO;
- TO tada ir tik tada turi atvirkštinį operatorių, kai jo matrica yra reguliari;
- tokių TO aibė yra multiplikacinė nekomutatyvioji grupė; ji yra izomorfiška n -tosios eilės kvadratinų reguliariųjų matricų grupei.

Paskaita 2 – 10

Tiesiniai operatoriai (tęsinys)

Pakartokime: TO, jo matrica. Erdvių $(\mathcal{A}(V_1, V_2), +, \cdot)$ ir $(M_{m \times n}(R), +, \cdot)$ izomorfiškumas.

Bazės keitimas

Savaime suprantama, kad TO matrica priklauso nuo to, kokios bazės pasirinktos erdvėse V_1 ir V_2 . Atskiru atveju, kai kalbame apie TO $\mathcal{A}$ iš aibės $\mathcal{A}(V)$, jo matrica priklauso nuo bazės erdvėje $(V, +, \cdot)$ pasirinkimo. Bazėje $(\alpha)_n$ operatoriaus matrica yra $A = (a_{ij})$, o kitoje (“naujoje”) bazėje $(\beta)_n$ apskritai *kitokia* kvadratinė n – osios eilės matrica $B := (b_{ij})$. Kaip susietos šios dvi matricos?

Paskaitoje 2 – 06 esame įvedę bazės *keitimo matricos* T sąvoką. Primename, kad $T = (t_{ij})$ yra reguliari matrica, kurios elementai t_{ij} yra randami iš lygybių:

$$\beta_i = \sum_{j=1}^n t_{ij} \alpha_j, \quad i = 1 \div n, \quad (1)$$

o to paties vektoriaus $\alpha \in V$ koordinačių eilutes bazėse $(\alpha)_n$ ir $(\beta)_n$ sieja sąryšis:

$$(l_1, l_2, \dots, l_n)_{[\alpha]} = (k_1, k_2, \dots, k_n)_{[\beta]} \cdot T.$$

Teorema. $B = TAT^{-1}$.

Įr. Keitimo matricai T atvirkštinės matricos T^{-1} elementus pažymėkime h_{kl} , t.y.

$$\alpha_k = \sum_{l=1}^n h_{kl} \beta_l, \quad T^{-1} = (h_{kl}).$$

Dabar iš (1) lygybės gauname:

$$\mathcal{A}(\beta_i) = \sum_{j=1}^n t_{ij} \mathcal{A}(\alpha_j). \quad (2)$$

Kadangi

$$\mathcal{A}(\alpha_j) = \sum_{k=1}^n a_{jk} \alpha_k, \quad \mathcal{A}(\beta_i) = \sum_{l=1}^n b_{il} \beta_l, \quad i, j = 1 \div n, \quad (3)$$

tai iš čia ir iš (2) nuosekliai išvedame:

$$\mathcal{A}(\beta_i) = \sum_{j=1}^n t_{ij} \mathcal{A}(\alpha_j) = \sum_{j=1}^n t_{ij} \sum_{k=1}^n a_{jk} \alpha_k = \sum_{j=1}^n t_{ij} \sum_{k=1}^n a_{jk} \sum_{l=1}^n h_{kl} \beta_l = \sum_{l=1}^n \left(\sum_{k=1}^n \sum_{j=1}^n t_{ij} a_{jk} h_{kl} \right) \beta_l.$$

Palyginę (3) ir gautą formules, matome, kad

$$(\forall i, l = 1 \div n) b_{il} = \sum_{k=1}^n \sum_{j=1}^n t_{ij} a_{jk} h_{kl} \rightarrow B = TAT^{-1}.$$

QED.

Matricų panašumas

Ap. Dvi n -osios eilės matricas A ir B vadinsime **panašiomis**, jeigu egzistuoja tokia reguliari n -osios eilės matrica C , kad $B = CAC^{-1}$.

Tad įrodėme, kad to paties TO matricos skirtingose bazėse yra *panašios*.

Teorema. Matricų panašumo sąryšis yra ES.

Įr. 1. Matricinę lygybę $B = CAC^{-1}$, daugindami (iš dešinės) iš matricos C ir (iš kairės) iš matricos C^{-1} , gauname $A = C^{-1}BC = C^{-1}B(C^{-1})^{-1}$, todėl panašumo sąryšis yra *simetriškas*.

2. Kai A yra panaši B , tai $B = CAC^{-1}$. Jei B , savo ruožtu, panaši matricai D , tai $D = HBH^{-1}$ su reguliaria matrica H . Tačiau tada $D = HCAC^{-1}H^{-1} = (HC)A(HC)^{-1}$, todėl ir A su D yra panašios. Tad matricų panašumo sąryšis yra *tranzityvus*.

3. *Refleksyvumas* išplaukia iš lygybės $A = EAE^{-1}$. QED.

1 *išvada*. n – osios eilės kvadratinių matricų aibė panašumo sąryšio pagalba suskaidoma į (panašių tarpusavyje matricų) ekvivalentumo klases (faktorizavimo teorema).

2 *išvada*. Iš teoremos apie matricų sandaugos rangą (paskaita 2 – 05) išplaukia, kad *panašių matricų rangai yra lygūs*, todėl *visos tos pačios klasės matricos turi vienodą rangą*.

Kadangi visos TO matricos sudaro panašių matricų klasę, tai 2 *išvada* leidžia suformuluoti tokį apibūrinimą.

Ap. TO $\mathcal{A}$ matricos A rangą vadiname **TO rangą**. Žymėsime: $\text{rang } \mathcal{A}$.

Teorema. Jeigu $\text{rang } \mathcal{A} = r$, tai egzistuoja toks erdvės $(V, +, \cdot)$ $n - r$ – matis poerdvis H , kurį operatorius $\mathcal{A}$ atvaizduoja į nulinį vektorių.

Be įrodymo.

Ap. Erdvės $(V, +, \cdot)$ poerdvis, kurį TO $\mathcal{A}$ atvaizduoja į nulinį vektorių, vadinamas **TO branduoliu**. Žymima: $\text{Ker } \mathcal{A}$.

Ap. Erdvės dimensijos ir operatoriaus rango skirtumas vadinamas operatoriaus **defektu**.

TO tikrinės reikšmės ir tikriniai vektoriai

Taikymuose svarbu pasirinkti tokią erdvės $(V, +, \cdot)$ bazę, kad visi skaičiavimai būtų kuo paprastesni.

Ap. Skaičius $\lambda \in R$ vadinamas TO $\mathcal{A} \in \mathcal{T}(V)$ **tikrine reikšme**, o nenulinis vektorius $\alpha \in V$ vadinamas **TO tikriniu vektoriumi**, jei

$$\mathcal{A}(\alpha) = \lambda \alpha. \quad (4)$$

Teorema. Operatoriaus $\mathcal{A} \in \mathcal{T}(V)$ tikriniai vektoriai, atitinkantys skirtingas tikrines reikšmes yra TN.

Jr. Remsimės MIP. 1. Kai turime dvi skirtingas tikrines reikšmes l_1 ir l_2 , tai, tarus, kad jas atitinkantys tikriniai vektoriai α_1 ir α_2 yra TP, gautume prieštarą:

$$\alpha_2 = c\alpha_1 \rightarrow \mathcal{A}(\alpha_2) = c \mathcal{A}(\alpha_1) = c(l_1\alpha_1 = l_1(c\alpha_1)) = l_1\alpha_2 \rightarrow l_2 = l_1.$$

2. Tarkime, kad teoremos tvirtinimas teisingas atveju, kai yra $k-1$ skirtinga tikrinė reikšmė $l_1, l_2, \dots, l_{k-1}$, t.y. jas atitinkantys tikriniai vektoriai $\alpha_1, \alpha_2, \dots, \alpha_{k-1}$ yra TN.

3. Parodysime, kad iš prielaidos teoremos tvirtinimas išplaukia ir imant k skirtingų tikrinių reikšmių: $l_1, l_2, \dots, l_{k-1}, l_k$. Jei tartume, kad jas atitinkantys tikriniai vektoriai $\alpha_1, \alpha_2, \dots, \alpha_{k-1}, \alpha_k$ yra TP, tai gautume, kad vektorius α_k tiesiškai išsireiškia per vektorius $\alpha_1, \alpha_2, \dots, \alpha_{k-1}$, t.y.

$$\alpha_k = \sum_{j=1}^{k-1} c_j \alpha_j \quad (5)$$

ir bent viena iš konstantų c_j , $j = 1 \div (k-1)$ yra nelygi nuliui.

Paveikę šį vektorių operatoriumi $\mathcal{A}$, gausime:

$$l_k \alpha_k = \mathcal{A}(\alpha_k) = \sum_{j=1}^{k-1} c_j \mathcal{A}(\alpha_j) = \sum_{j=1}^{k-1} c_j l_j \alpha_j.$$

Iš čia, pasinaudojus (5) išraiška, išplaukia:

$$l_k \alpha_k = l_k \sum_{j=1}^{k-1} c_j \alpha_j = \sum_{j=1}^{k-1} c_j l_j \alpha_j,$$

t.y.

$$\sum_{j=1}^{k-1} c_j (l_k - l_j) \alpha_j = O.$$

Tačiau ši lygybė prieštarauja prielaidai, kad vektoriai $\alpha_1, \alpha_2, \dots, \alpha_{k-1}$ yra TN, nes $l_k \neq l_j$ ir bent vienam j , $c_j \neq 0$. QED.

Charakteristinė lygtis

Kaip rasti konkretaus TO $\mathcal{A} \in \mathcal{T}(V)$ tikrines reikšmes l ir jas atitinkančius tikrinius vektorius α ? Jei kokioje nors bazėje operatoriaus matrica yra A , tai, pažymėję tikrinio vektoriaus α koordinates toje bazėje $(x_1, x_2, \dots, x_n)$, (4) lygybę galėsime užrašyti tokiu matriciniu pavidalu:

$$(x_1, x_2, \dots, x_n) A = l (x_1, x_2, \dots, x_n),$$

arba

$$(x_1, x_2, \dots, x_n) A = I (x_1, x_2, \dots, x_n) E_n.$$

Pastaroji lygtis ekvivalenti tokiai:

$$(x_1, x_2, \dots, x_n)(A - lE_n) = O.$$

Kai tikrinė reikšmė l jau surasta, tai tikrinio operatoriaus koordinates randame sprenddami šią matricinę lygtį, arba ją atitinkančią THLS:

[illegible]

Bet tikriniai vektoriai pagal apibrėžimą yra nenuliniai, tad mus domina tik *nenuliniai* (6) *THLS sprendiniai*. Žinome (išvada iš Kramerio teoremos), kad THLS tada ir tik tada turi nenulinių sprendinių, kai jos matricos determinantas lygus nuliui. Kadangi matricos ir transponuotos matricos determinantai yra lygūs, darome išvadą: tikrinės TO reikšmės yra lygties (vadinamos *operatoriaus $\mathcal{A}$ charakteristine lygtimi*)

$$|A - \chi E_n| = 0$$

sprendiniai.

Pavyzdys. Kaip jau nustatėme, TO $\mathcal{B}: R^3 \longrightarrow R^3$, apibrėžiamo taisykle:

$$(\forall \alpha = (x_1, x_2, x_3) \in R^3) \mathcal{B}(\alpha) = (x_1, 2x_1, 3x_2),$$

matrica B standartinēje erdvēs R^3 bazēje yra tokia:

$$B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

Rasime šio TO tikrines reikšmes ir jas atitinkančius tikrinius vektorius.

Pirmiausia, spęsdami operatoriaus $\mathcal{B}$ charakteristinę lygtį:

$$\begin{vmatrix} 1-x & 0 & 0 \\ 0 & 2-x & 0 \\ 0 & 0 & 3-x \end{vmatrix} = 0 \equiv (x-1)(x-2)(x-3) = 0,$$

randame jo tikrines reikšmes: $l_1 = 1, l_2 = 2, l_3 = 3$.

Dabar surasime TO tikrinius vektorius, atitinkančius tikrinę reikšmę $l = 1$. Tuo tikslu sprendžiame (6) THLS atitikmeni:

$$\begin{cases} 0 \cdot x_1 + 0x_2 + 0 \cdot x_3 = 0, \\ 0 \cdot x_1 + 1 \cdot x_2 + 0 \cdot x_3 = 0, \\ 0 \cdot x_1 + 0 \cdot x_2 + 2 \cdot x_3 = 0. \end{cases}$$

Jos bendrasis sprendinys yra $(t, 0, 0)$, $t \in R$. Tad tikrinę reikšmę $l = 1$ atitinka tikriniai vektoriai $(t, 0, 0)$, $t \in R$, $t \neq 0$. Panašiai rastume ir kitas tikrines reikšmes atitinkančius tikrinius vektorius.

Invariantiniai poerdviai. Paprasto spektro TO

Tarkime $\mathcal{A} \in \mathcal{T}(V)$. Erdvės $(V, +, \cdot)$ kokio nors poerdvio $(V_1, +, \cdot)$ pilnąjį vaizdą pažymėkime $\mathcal{A}(V_1)$.

Teorema. $\mathcal{A}(V_1, +, \cdot)$ yra VE.

Įr. savarankiškai (žr. vadovėlio 119 t).

Tačiau bendruoju atveju erdvė $(\mathcal{A}(V_1), +, \cdot)$ nėra erdvės $(V_1, +, \cdot)$ poaibis.

Ap. Jeigu yra išpildyta sąlyga $\mathcal{A}(V_1) \subset V_1$, tai vektorinės erdvės $(V_1, +, \cdot)$ poerdvis $(\mathcal{A}(V_1), +, \cdot)$ vadinamas **invariantiniu poerdviu** operatoriaus $\mathcal{A}$ atžvilgiu.

Pavyzdžiui, TO branduolys yra invariantinis poerdvis.

Plačiau aptarsime, vienmačius invariantinius poerdvius TO atžvilgiu. Parodysime, kad, jų radimui, užtenka pasinaudoti informacija apie TO tikrines reikšmes ir tikrinius vektorius.

Aišku invariantinio poerdvio $(\mathcal{A}(V_1), +, \cdot)$ dimensija tenkina nelygybę $\dim \mathcal{A}(V_1) \leq \dim V_1$.

Jei $(V_1, +, \cdot)$ yra invariantinis poerdvis ir $\dim V_1 = 1$, tai:

$$1. (\forall \alpha, \beta \in V_1) (\exists c \in R) \beta = c\alpha.$$

Tikrai, jei α_1 yra poerdvio V_1 bazinis vektorius, tai

$$(\alpha = c_1\alpha_1) \wedge (\beta = c_2\alpha_1) \rightarrow \beta = c_2c_1^{-1}\alpha := c\alpha.$$

$$2. (\forall \alpha, \beta \in V_1; \alpha \neq 0) \quad \mathcal{A}(\alpha) = l\alpha \quad \text{ir} \quad \mathcal{A}(\beta) = \mathcal{A}(c\alpha) = c \mathcal{A}(\alpha) = cl\alpha = l\beta.$$

1 išvada. Vienmačio invariantinio poerdvio $(V_1, +, \cdot)$ visi nenuliniai vektoriai yra operatoriaus $\mathcal{A}$ tikriniai vektoriai, atitinkantys tą pačią tikrinę reikšmę l .

2 išvada. Jei $\alpha_1, \dots, \alpha_k$ yra tikriniai vektoriai, atitinkantys tikrinę reikšmę l , tai ir bet kokia jų tiesinė kombinacija (tiesinis darinys)

$$\alpha = \sum_{i=1}^k c_i \alpha_i$$

yra tikrinis vektorius, atitinkantis tą pačią tikrinę reikšmę l .

3 išvada. Jei $\alpha_1, \dots, \alpha_k$ yra tikriniai vektoriai, atitinkantys tikrinę reikšmę l , tai ir kiekvienas nenulinis jų generuoto invariantinio poerdvio $H(\alpha_1, \dots, \alpha_k)$ vektorius yra tikrinis vektorius, atitinkantis tikrinę reikšmę l .

Atskiru atveju, kai turime vieną tikrinį vektorių α , atitinkantį tikrinę reikšmę l , tai jo generuotas poerdvis $H(\alpha)$ ir bus ieškomasis vienmatis invariantinis poerdvis. Atžvilgiu.

Ap. TO **spektru** vadinama visų jo tikrinių reikšmių aibė.

Ap. TO $\mathcal{A}$ vadinamas **paprasto spektro operatoriumi**, jei jis turi lygiai n realių ir skirtingų tikrinių reikšmių.

Pavyzdžiui, praeitoje paskaitoje nagrinėto TO $\mathcal{B}: R^3 \longrightarrow R^3$, apibrėžiamo taisykle:

$$(\forall \alpha = (x_1, x_2, x_3) \in R^3) \quad \mathcal{B}(\alpha) = (x_1, 2x_2, 3x_3),$$

tikrinę reikšmę $l_1 = 1$ atitinkančio vienmačio invariantinio poerdvio bazinė aibė yra $\{t(1, 0, 0)\}$, $t \in R$, o pats operatorius $\mathcal{B}$ yra paprasto spektro operatorius, nes jis turi tris skirtingas realias tikrines reikšmes.

Paprasto spektro operatoriaus matrica visada yra panaši į įstrižaininę matricą. Tiksliau, teisinga tokia:

Išvada. Erdvės $(V, +, \cdot)$ tiesinis operatorius $\mathcal{A}$ tada ir tiksliai tada yra paprasto spektro TO, kai jo matrica panaši į įstrižaininę matricą, kurios pagrindinės įstrižainės elementai yra skirtingi realieji skaičiai.

LITERATŪRA

1. K.Bulota, P.Survila. Algebra ir skaičių teorija. I dalis, “Mokslas”, 1989.
2. K.Bulota, P.Survila. Algebra ir skaičių teorija. II dalis, “Mokslas”, 1990.
3. J.Kubilius. Realus kintamojo funkcijų teorija. “Mintis” , 1970.
4. L.Griniuvienė. Matematinė logika. Vilnius, 1997.
5. B.Kvedaras. Matricų teorija VDU leidykla, 1999.
6. A.Matuliauskas. Algebra. “Mokslas”, 1985.
7. R.Skrabutėnas, P.Survila. Algebros ir skaičių teorijos uždavinynas. “Mokslo ir enciklopedijų leidykla”, 1995.
8. В.А.Ильин, Э.Г.Позняк. Линейная алгебра. М., “Физматлит”, 2001.
9. А. Г. Курош. Курс высшей алгебры.М., “Физматгиз”, 1975.
10. Л. Я. Куликов. Алгебра и теория чисел. М., “Высшая школа ”, 1979.
11. С. В. Ларин. Числовые системы. М., Акад.ИЦ, 2001.
10. Б. Л. ван дер Варден. Алгебра. М., “Наука”, 1976.
11. А. И. Кострикин. Введение в алгебру 1 - 3. М., “Физматлит”, 2001.
12. Л. Б. Шнеперман. Сборник задач по алгебре и теории чисел. Минск, “Вышэйшая школа”, 1982.
13. Л. Б. Шнеперман. Курс алгебры и теории чисел в задачах и упражнениях . “Вышэйшая школа”, ч.І ,1986, ч.ІІ ,1987 .
14. Д. К. Фадеев, И. С. Соминский. Задачи по высшей алгебре. М., СПб.: Лань, 2001.
15. И. В. Проскуряков. Сборник задач по линейной алгебре. М., ЛАБЗ, 2001.
16. С. В. Яблонский. Введение в дискретную математику. М., „Высшая школа “.
17. G. Asser. Grundbegriffe der Mathematik. VEB Verlag, 1988.
18. J. Wisliceny. Aufgabensammlung I. VEB Verlag, 1989.

Turinys

ŽODIS SKAITYTOJUI	3
Paskaita 1 – 01	5
MATEMATINĖS KALBOS PAGRINDAI	
Paskaita 1 – 02	15
AIBIŲ TEORIJOS ELEMENTAI	
Paskaita 1 – 03	24
KOMBINATORIKOS PAGRINDAI	
Paskaita 1 – 04	28
ALGEBRINĖS STRUKTŪROS	
Paskaita 1 – 05	33
ALGEBRINĖS STRUKTŪROS (TĘSINYS)	
Paskaita 1 – 06	39
SKAIČIŲ SISTEMOS	
Paskaita 1 – 07	45
SKAIČIŲ SISTEMOS (TĘSINYS)	
Paskaita 1 – 08	53
KOMPLEKSINIŲ SKAIČIŲ LAUKAS	
Paskaita 1 – 09	61
KOMPLEKSINIŲ SKAIČIŲ LAUKAS (TĘSINYS)	
Paskaita 1 – 10	64
VIENTO ŠAKNŲ GRUPĖ	
Paskaita 1 – 11	67
KUBINĖS IR KETVIRTOJO LAIPSNIO LYGTYS	
Paskaita 1 – 12	76
GRUPĖS IR POGRUPIAI. LAGRANŽO TEOREMA	
Paskaita 2 – 01	81
TIESINĖS ALGEBROS ELEMENTAI	

ALGEBRA IR SKAIČIŲ TEORIJA

Paskaita 2 – 02	90
KVADRATINĖS MATRICOS DETERMINANTAS. KRAMERIO TAISYKLĖ	
Paskaita 2 – 03	100
MATRICŲ ALGEBRA	
Paskaita 2 – 04	104
VEKTORIŲ – EILUČIŲ ERDVĖ R^n	
Paskaita 2 – 05	108
TLS SUDERINTUMO KRITERIJUS	
Paskaita 2 – 06	114
VEKTORINĖS ERDVĖS	
Paskaita 2 – 07	119
EUKLIDO ERDVĖS	
Paskaita 2 – 08	123
TIESINĖS NELYGYBĖS. OPTIMIZAVIMO UŽDAVINYS	
Paskaita 2 – 09	128
TIESINIAI OPERATORIAI	
Paskaita 2 – 10	135
TIESINIAI OPERATORIAI (TĘSINYS)	
LITERATŪRA	141

Rimantas Skrabutėnas
ALGEBRAIRSKAČIŲ TEORIJA
(Paskaitų konspektas I)

Redagavo autorius
Maketavo Donaldas Petrauskas
Viršelio dailininkė Eglė Varankaitė

SL 605. Sp. l. 18. Tir. 350 egz. Užsak. Nr. 04-047

Išleido Vilniaus pedagoginis universitetas, Studentų g. 39, LT-08106 Vilnius

Spausdino VPU leidykla, T. Ševčenkos g. 31, LT-03111 Vilnius

Kaina sutartinė