Algebra ir geometrija informatikams. Paskaitų konspektas. Rimantas Grigutis

1 paskaita *Įvadas. Kurso struktūra. Teiginys ir įrodymas. Matematinės indukcijos metodas.*

Įvadas.

Algebros kaip matematinės disciplinos pavadinimas žinomas iš mokyklos laikų. Lygiai taip pat kaip ir geometrijos.

Sofi Žermen: Algebra - tai ne kas kita, kaip simboliais užrašyta geometrija, o geometrija - tai paprasčiausiai figūromis išreikšta algebra.

Algebra - tai mokslas apie algebrines operacijas, atliekamas su įvairių aibių elementais. Visa ko pradžia : elementarioji aritmetika.

Žymus 20-ojo šimtmečio fizikas *P.Dirakas(P.Dirac,1902-1984,anglų fizikas)* minėjo, kad neeuklidinė geometrija ir nekomutatyvioji algebra yra būtinos bendram fizikiniam pasaulio aprašymui.

Paminėsime svarbias algebros gaires mokslo istorijoje:

1) XIX a. *N.Abelis(N.H.Abel,1802-1829,norvegų matematikas)* ir *E.Galua (E.Galois,1811-1832,prancūzų matematikas)* algebriniais metodais išsprendė lygties $x^n+a_{n-1}x^{n-1}+\cdots+a_0=0$ išsprendžiamumo "radikalais" problemą. Įrodyta, kad kai $n\geq 5$ neįmanoma rasti lygties sprendinių formulės išreikštos aritmetiniais veiksmais ir šaknimis.

2) Struktūrinė molekulių teorija aprašoma grupėmis - tam tikromis algebrinėmis struktūromis. O viskas prasidėjo tuo, kad dar 1891 metais buvo rastos visos 230 taip vadinamos kristalografinės grupės, aprašančios visas fizikinių kūnų kristalų simetrijas.

3) Baigtinių kūnų teorijos taikymas kodavimo teorijoje. Taip vadinama tiesinių kodų teorija, o ji kaip tik ir taikomi praktikoje, susiveda galų gale prie specialių matricų konstravimo ir tiesinių lygčių sprendimo virš baigtinių kūnų.

Paminėsime pagrindinius žymenis, kuriais naudosimės.

$\mathbf{N}$ - natūraliųjų skaičių aibė; $n, m, k, l, ...$ - natūralieji skaičiai; $p, q, ...$ - pirminiai skaičiai; $\mathbf{Z}$ - sveikųjų skaičių aibė; $a, b, c, d, ...$ - sveikieji skaičiai; $\mathbf{Q}$ - racionaliųjų skaičių aibė; $\mathbf{R}$ - realiųjų skaičių aibė.

Kvantoriai (lot. quantum - "kiek", kiekybinė charakteristika):

$\exists c$ - egzistuoja c; $\forall a$ - bet kuris a; $\exists! b$ - egzistuoja vienintėlis toks b.

Kurso struktūra

Šis algebros ir geometrijos (o vėliau ir algebros) kursas, kaip ir bet kuris kitas matematikos kursas, - tai teiginių, išvadų, teoremų, lemų seka, kurią sieja teisingas samprotavimas .

Trumpai aptarkime teisingo samprotavimo būdą - logiką.

Apibrėžimas 1.1. *Teiginys - tai sakinys, kuris gali būti teisingas arba klaidingas, bet negali būti ir teisingas ir klaidingas tuo pačiu metu.*

Teiginius priimta žymėti didžiosiomis raidėmis: P, Q, T, ... Teisingą teiginį žymi simboliu 1, o klaidingą teiginį - simboliu 0.

Formuluodami sudėtinius teiginius naudosime šiuos žodžius,veiksmus

P yra Q	$P = Q$	tapatybė
P arba Q	$P \vee Q$	sudėtis
P ir Q	$P \wedge Q$	daugyba
jei P, tai Q	$P \Longrightarrow Q$	implikacija
P tada ir tik tada, kai Q	$P \Longleftrightarrow Q$	ekvivalentumas
netiesa, kad P	$\bar{P}$	neiginys

Tik paprasčiausių teiginių teisingumas apsprendžiamas iš konteksto. Sudėtinių teiginių teisingumas nustatomas įrodymais. Ne visus samprotavimus galime vadinti įrodymais. Įrodymai turėtų tenkinti tam tikrus reikalavimus, vadinamus loginio įrodymo dėsniais.

Loginio įrodymo dėsniai:

D1. Nepriešstaravimo dėsnis : $P \wedge \bar{P} = 0$.

D2. Trečiojo negalimumo dėsnis : $P \vee \bar{P} = 1$.

D3. Teisingos išvados dėsnis: iš teisingo teiginio išplaukia tik teisingas teiginys: jei $(1 \Rightarrow Q) = 1$, tai $Q = 1$.

D4. Klaidingos išvados dėsnis: klaidingas teiginys išplaukia tik iš klaidingo teiginio: jei $(P \Rightarrow 0) = 1$, tai $P = 0$.

Loginio įrodymo dėsnius apibendrina lentelė:

$0 \Longrightarrow 0 = 1$	$0 \Longleftrightarrow 0 = 1$
$0 \Longrightarrow 1 = 1$	$0 \Longleftrightarrow 1 = 0$
$1 \Longrightarrow 0 = 0$	$1 \Longleftrightarrow 0 = 0$
$1 \Longrightarrow 1 = 1$	$1 \Longleftrightarrow 1 = 1$

Pavyzdžiai 1.2. 1 Teiginys " *Jei lygtis* $x^2 + 1 = 0$ *turi realią šaknį, tai* 121 *dalijasi iš* 13" yra teisingas.

2. Teiginys "*Jei lygtis* $x^2 + 1 = 0$ *turi realią šaknį, tai* 121 *dalijasi iš* 11" yra teisingas.

3. Teiginys "*Jei lygtis* $x^2 - 1 = 0$ *turi realią šaknį, tai* 121 *dalijasi iš* 13" yra klaidingas.

4. Teiginys "*Jei lygtis* $x^2 - 1 = 0$ *turi realią šaknį, tai* 121 *dalijasi iš* 11" yra teisingas.

Sudėtingesni teiginiai vadinami teoremomis.

Apibrėžimas 1.3. *Teorema yra teiginys, kurio teisingumas patvirtinamas arba paneigiamas įrodymu.*

Teoremą dažniausiai užrašo implikacijos būdu: $P \Longrightarrow Q$, čia $P-$ *teoremos prielaida* (hipotezė), o $Q-$ *teoremos išvada*.

Apibrėžimas 1.4. Jei teoremą $P \Longrightarrow Q$ vadina *tiesiogine*, tai teorema
$Q \Longrightarrow P$ vadinama *atvirkštinė* teorema,
$\bar{P} \Longrightarrow \bar{Q}$ vadinama *priešinga* teorema,
$\bar{Q} \Longrightarrow \bar{P}$ vadinama *priešingoji atvirkštinei* teorema.

Pavyzdžiai 1.5. 1. Pitagoro*(*$\Pi\iota\theta\alpha\gamma o\rho\alpha\xi$*, apie 570 p.K.-apie 500 p.K., graikų mąstytojas)* teorema: Jeigu trikampis yra status (teiginys P), tai $a^2 + b^2 = c^2$ (teiginys Q). Tai tiesioginės teoremos pavyzdys.

Atvirkštinės teoremos pavyzdys yra Atvirkštinė Pitagoro teorema: $Q \Rightarrow P$, t.y. jeigu $a^2 + b^2 = c^2$, tai trikampis yra status.

Priešinga teorema skamba taip: jeigu trikampis yra nestatus, tai $a^2 + b^2 \neq c^2$.

Ir priešingoji atvirkštinei teorema: Jeigu $a^2 + b^2 \neq c^2$, tai trikampis yra nestatus.

Pastebėsime, kad visi čia suformuluoti teiginiai yra teisingi.

2. Tiesioginė teorema: $\boxed{\text{Skaičius } n \text{ yra lyginis}} \Rightarrow \boxed{\text{Skaičius } n \text{ dalus iš } 4}$.
Atvirkštinė teorema: $\boxed{\text{Skaičius } n \text{ dalus iš } 4} \Rightarrow \boxed{\text{Skaičius } n \text{ yra lyginis}}$.
Priešinga teorema: $\boxed{\text{Skaičius } n \text{ yra nelyginis}} \Rightarrow \boxed{\text{Skaičius } n \text{ nedalus iš } 4}$.
Priešingoji atvirkštinei teorema: $\boxed{\text{Skaičius } n \text{ nedalus iš } 4} \Rightarrow \boxed{\text{Skaičius } n \text{ yra nelyginis}}$.

Be didesnių komentarų pateiksime šiuos teiginius:

Teiginys1.6(kontrapozicija). Tiesioginė teorema yra ekvivalenti priešingai atvirkštinei teoremai, t.y.

$$(P \Longrightarrow Q) \Longleftrightarrow \left(\bar{Q} \Longrightarrow \bar{P}\right).$$

Teiginys 1.7. Atvirkštinė teorema yra ekvivalenti priešingai teoremai, t.y.

$$(Q \Longrightarrow P) \Longleftrightarrow \left(\bar{P} \Longrightarrow \bar{Q}\right) .$$

Teiginio 1.6 pagrindu formuluojamas *prieštarų metodas*(kontrapozicijos principas).Ši loginė schema praktiškai realizuojama šitaip:

norime įrodyti tiesioginę teoremą $(P \Longrightarrow Q) = 1$, *kai sąlyga* P *teisinga(*$P = 1$*). Tariame, kad teisingas ne teiginys* Q*, o jam priešingas teiginys* $\bar{Q}\left(\bar{Q} = 1\right)$ *ir įrodome, kad tuomet teisingas teiginys* $\bar{P}$ *(t.y.* $\left(\bar{Q} \Longrightarrow \bar{P}\right) = 1$*). Tai ir įrodo tiesioginę teoremą,*

nes gauname vienu metu du prieštaringus teiginius $P = 1$ ir $\bar{P} = 1$. Bet pagal neprieštaravimo dėsnį D.1 to negali būti. Vadinasi, prielaida, kad teisingas teiginys $\bar{Q} = 1$, buvo klaidinga. O jeigu $\bar{Q}$ $\left(\bar{Q} = 0\right)$klaidingas, tai pagal trečiojo negalimumo dėsnį D.2 teisingas $Q\,(Q = 1)$.

Pavyzdys 1.8. *Teorema. Jeigu studento sesijos pažymiai 7,8,ir 9, tai studentas yra pažangus.(Pažangiu vadiname studentą, neturinčio skolų).*

Įrodymas. Šiuo atveju teoremos prielaida P yra "studento sesijos pažymiai 7,8,ir 9" , o teoremos išvada Q yra "studentas yra pažangus". Įrodysime prieštaros metodu.

Sakykime, studentas yra nepažangus. Tada jis turi nors vieną skolą, t.y. bent vienas jo sesijos pažymis < 5 . Bet tai prieštarauja teoremos prielaidai $P = 1$ ir įrodo teoremą.

Pavyzdys 1.9. *Teorema. Jeigu n^2 yra nelyginis sveikas skaičius, tai ir n yra nelyginis skaičius.*

Įrodymas prieštaros metodu. Atvirkštinė priešingai teorema formuluojama taip: *Jei n yra lyginis skaičius, tai ir n^2 yra lyginis skaičius.* Ši teorema įrodoma tiesiogiai: jei n yra lyginis, tai $n = 2k$ su sveiku k. Tada $n^2 = 4k^2 = 2(2k^2)$ yra lyginis skaičius, nes $2k^2-$ sveikas.

Prieštaros metodas rodo, kaip loginio įrodymo dėsniai formuoja patį įrodymą. Sutikime, kad prieštaros metodas yra ne pats paprasčiausas įrodymas. Yra ir paprastesnių. Išvardinkime juos.

1. *Tiesioginis įrodymas(įrodymas konstruojant* = Proof by Construction).

Šis įrodymo būdas remiasi tiesioginiu konstruktyviu samprotavimu teoremos išvados link, naudojantis teoremos hipoteze.

Pavyzdys 1.10. *Teorema. Jeigu n yra nelyginis sveikas skaičius, tai ir n^2 yra nelyginis sveikas skaičius.*

Įrodymas. Įrodysime tiesioginiu būdu. Teoremos hipotezė - tai teiginys: " *n yra nelyginis sveikas skaičius".* Sakykime ši hipotezė yra teisinga. Tada turime, kad $n = 2k + 1$ su sveiku k. Pakėlę paskutinę lygybę kvadratu turėsime $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Bet skaičius $2k^2 + 2k$ irgi sveikas, todėl n^2 yra nelyginis sveikas skaičius.

2. *Įrodymas, nagrinėjant atvejus*(Case Analysis).

Ne visada lengva įrodynėti teiginius tiesiogiai. Ypač taip bendrai suformuluotas teoremas:

" Teorema. Jeigu n yra sveikas skaičius, tai teiginys S teisingas."

Žinodami, kad skaičius n gali būti arba lyginis, arba nelyginis skaičius pakanka įrodyti duotos teoremos du atskirus atvejus:

ATVEJIS I: Tegu n yra lyginis skaičius. Tada ... . Todėl teiginys S yra teisingas.

ATVEJIS II: Tegu n yra nelyginis skaičius. Tada ... . Todėl teiginys S yra teisingas.

Pastebėsime, kad išraiška " Tada ..." yra įrodymo pagrindas ir priklauso nuo nagrinėjamos situacijos.

Pavyzdys 1.11. *Teorema. Su visais sveikais skaičiais n skaičiaus* n^2 *dalybos iš* 4 *liekana yra arba* 0, *arba* 1.

Įrodymas. Nagrinėsime du atvejus.

ATVEJIS I: n yra lyginis. Tada $n = 2k$ su sveiku k. Tada $n^2 = (2k)^2 = 4k^2$ ir n^2 dalybos iš 4 liekana yra 0.

ATVEJIS II: n yra nelyginis. Tada $n = 2k + 1$ su sveiku k. Tada $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$ ir n^2 dalybos iš 4 liekana yra 1.

Išnagrinėti atvejai išsemia visas skaičiaus n galimybes ir abiem atvejais teiginys " *skaičiaus* n^2 *dalybos iš* 4 *liekana yra arba* 0, *arba* 1" yra teisingas. Tuo pačiu teisinga ir pati teorema.

3. *Įrodymas, ieškant kontrpavyzdžio(*Proof by Counterexample).

Šis įrodymo būdas yra skirtas įrodyti tam, kad teorema yra neteisinga(t.y. patikrinti, kad galioja $(P \Rightarrow Q) = 0$).

Pavyzdys 1.12. Įrodykite arba paneikite: Skaičius $6k + 1$ yra pirminis su visais teigiamais sveikais skaičiais k.

Įrodymas. Teiginys teisingas, kai $k = 1, 2$ ir 3, nes skaičiaus $6k + 1$ reikšmės atitinkamai lygios $7, 13$ ir 19 (pirminiai skaičiai). Tačiau, kai $k = 4$ turime $6 \cdot 4 + 1 = 25-$ sudėtinis skaičius. Taigi, teiginys yra neteisingas. Pastebėsime, kad pakanka *vieno* pavyzdžio, paneigiančio teoremą.

Formuluodami teoremas(teiginius, lemas) dažnai naudosimės išsireiškimu " būtina ir pakankama sąlyga". Paaiškinsime šio išsireiškimo prasmę.

Nagrinėkime teoremą $(P \Longrightarrow Q) = 1$. Teoremos prielaidą P vadiname pakankama sąlyga teiginiui Q , o teoremos išvadą Q vadiname būtina sąlyga teiginiui P.

Pavyzdžiai 1.13.1. *Teorema.* Jei $\dfrac{\pi}{2} < \alpha < \pi$, tai $\cos\alpha < 0$.

Sakome , kad $\dfrac{\pi}{2} < \alpha < \pi$ yra pakankama sąlyga nelygybei $\cos\alpha < 0$, o pati nelygybė $\cos\alpha < 0$ yra būtina sąlyga dvigubai nelygybei $\dfrac{\pi}{2} < \alpha < \pi$.

2. Suformuluokime dvi vieną kitai atvirkštines teoremas.

Teorema A. Jei $0 < a < 1$, tai $\log_a 3 < 0$.

Teorema B. Jei $\log_a 3 < 0$, tai $0 < a < 1$.

Abi šios teoremos yra teisingos. Šiuo atveju sakoma, kad teoremos sąlyga $0 < a < 1$ yra būtina ir pakankama sąlygai $\log_a 3 < 0$. Teoremas galima sujungti

į vieną:

Teorema C. Tam, kad $\log_a 3 < 0$ būtina ir pakankama $0 < a < 1$.

Teoremą B vadinsime "teorema iš kairės į dešinę", o teoremą A vadinsime "teorema iš dešinės į kairę".

Matematinės indukcijos metodas.

Tai dar vienas, dažnai naudojamas būdas teiginiams įrodinėti.

Nagrinėkime sveikųjų skaičių aibę $\mathbf{Z}$ ir tvarkos sąryšį $\leq$ šioje aibėje. .

Sakysime, kad $a \leq b$, jei $b-a \geq 0$. Šis dviejų sveikųjų skaičių sąryšis pasižymi savybėmis:

i) $a \leq a$ (refleksyvumas) ;

ii) ($a \leq b) \wedge (b \leq a) \Longrightarrow a = b$ (nesimetriškumas) ;

iii) $(a \leq b) \wedge (b \leq c) \Longrightarrow (a \leq c)$ (tranzytivumas) .

Tuo atveju, kai $a \leq b$ ir $a \neq b$ rašome $a < b$.

Aišku, kad bet kuriai sveikųjų skaičių porai a ir b teisinga arba $(a \leq b)$, arba $(b \leq c)$. Todėl aibę Z vadina tiesiškai sutvarkyta aibe. Su šia tvarka surišti tam tikri principai. Išvardinkime kai kuriuos iš jų.

Visiško sutvarkymo principas(well-ordering Principle) *sveikiesiems skaičiams.* Tegu a - sveikasis skaičius. Bet kuris netuščias sveikųjų skaičių $\geq a$ $(\leq a)$ poaibis turi mažiausią(didžiausią) elementą.

Visiško sutvarkymo principas(well-ordering Principle) *natūraliesiems skaičiams.* Bet kuris netuščias natūraliųjų skaičių poaibis turi mažiausią elementą.

Natūraliuosius skaičius apibrėžia *Dž.Peano(G.Peano,1858-1932,italų matematikas)* aksiomų sistema. Iš šios sistemos išplaukia taip pat ir

Matematinės indukcijos principas: *tegu su kiekvienu* $n \in \mathbf{N}$ *turime teiginį* $T(n)$*. Sakykime, kad žinome būdą teiginio* $T(l)$, $\forall l$*, teisingumui nustatyti, jeigu teisingi teiginiai* $T(k)$ *su visais* $k<l$ *(tame tarpe teisingas T(1) teiginys).Tada teisingas ir teiginys* $T(n)$*su visais* $n \in \mathbf{N}$*.*

Įrodymas. Nagrinėkime aibę

$S = \{s | s \in N,$ teiginys $T(s)$ neteisingas$\} \subseteq N$.

Tegu $S \neq \emptyset$. Tada egzituoja mažiausias aibės S elementas s_0., t.y. teiginys

$T(s_0)$ neteisingas. Jeigu $s_0 = 1$, tai prieštarauja indukcijos bazei, o jeigu $s_0 > 1$, tai visi teiginiai $T(s), s < s_0$, yra teisingi ir todėl žinome būdą teiginio $T(s_0)$ teisingumui nustatyti.

Prieštaravimas įrodo matematinės indukcijos metodą.