VILNIAUS UNIVERSITETO VADOVĖLIS

Paulius Drungilas,
Hamletas Markšaitis

ALGEBRA

I dalis

ALGEBRA

I dalis

VILNIAUS UNIVERSITETO VADOVĖLIS

Paulius Drungilas, Hamletas Markšaitis

ALGEBRA

I dalis

Vilniaus universiteto leidykla
Vilnius, 2013

Vilniaus universiteto Senato posėdžio
2012 m. birželio 19 d. nutarimu
(protokolas Nr. S-2012-5) leidiniui suteiktas
Vilniaus universiteto vadovėlio statusas

Apsvarstė ir rekomendavo spaudai
Vilniaus universiteto Matematikos ir
informatikos fakulteto taryba (2012 m.
gegužės 15 d.; protokolas Nr. 10)

Recenzentai:
doc. dr. EDMUNDAS GAIGALAS
Vilniaus universitetas
prof. dr. ALEKSANDRAS KRYLOVAS
Vilniaus Gedimino technikos universitetas

ISBN 978-609-459-128-0

Turinys

Pratarmė **8**

1 Aibės ir atvaizdžiai **11**
1.1 Aibės sąvoka 11
1.2 Veiksmai su aibėmis 13
1.3 Sąryšis 17
1.3.1 Nesutvarkytosios poros (nesutvarkytieji dvejetai) 17
1.3.2 Funkcinis sąryšis (funkcija). Atvaizdis 20
1.4 Ekvivalentumo sąryšis. Faktoraibė 27
1.5 Tvarkos sąryšiai. Sutvarkytosios aibės 32
1.5.1 Tiesiškai ir visiškai sutvarkytosios aibės 33
1.5.2 Kryptinės aibės 36
1.5.3 Sutvarkytųjų aibių tipas 37
1.6 Cermelo-Frenkelio aibių teorijos aksiomatika 38
1.7 Trumpa aibių teorijos raidos apžvalga 41

2 Kompozicijos dėsniai **44**
2.1 Vidiniai kompozicijos dėsniai 44
2.2 Asociatyvūs kompozicijos dėsniai 47
2.3 Indukuotieji kompozicijos dėsniai 50
2.4 Faktorkompozicijos dėsniai 50
2.5 Neutralus elementas. Simetriniai elementai 51
2.5.1 Neutralus elementas 51
2.5.2 Simetrinis elementas 52
2.5.3 Komutatyvūs kompozicijos dėsniai 53
2.6 Išoriniai kompozicijos dėsniai 53
2.7 Algebrinės struktūros 55

3 Natūralieji ir sveikieji skaičiai **56**
3.1 Elementari dalumo teorija . . . 56
3.2 Euklido algoritmas . . . 59
3.3 Pagrindinė aritmetikos teorema . . . 62

4 Tiesinių lygčių sistemos **67**
4.1 Gauso metodas . . . 69
4.1.1 Gauso metodas. Algoritmas . . . 69
4.1.2 Gauso metodas. Trapecinė lygčių sistema . . . 71
4.2 Pavyzdžiai . . . 74
4.3 Tiesinių lygčių sistemos sprendinių aibės sandara . . . 77

5 Grupės **80**
5.1 Bendros sąvokos . . . 80
5.1.1 Taisyklingųjų kūnų simetrijų grupės . . . 88
5.1.2 Tiesės afiniųjų atvaizdžių grupė . . . 89
5.1.3 Afinioji plokštuma . . . 90
5.1.4 Projekcinė plokštuma . . . 91
5.2 Pogrupiai . . . 93
5.3 Cikliniai pogrupiai . . . 97
5.4 Grupės skaidinys . . . 99
5.5 Normalieji pogrupiai . . . 106
5.6 Grupės faktorgrupė . . . 108
5.7 Homomorfizmai . . . 109
5.8 Grupių tiesioginės sandaugos . . . 118
5.9 Grupės veikimas aibėje . . . 124
5.10 Baigtinių Abelio grupių struktūra . . . 129
5.11 Simetrinė grupė . . . 139
5.11.1 Keitinio lyginumas I . . . 143
5.11.2 Keitinio lyginumas II . . . 148
5.12 Sujungtinių elementų klasės . . . 152
5.13 Sylovo teoremos . . . 157

6 Žiedai ir žiedų homomorfizmai **167**
6.1 Žiedai . . . 167
6.2 Matricų algebra . . . 174
6.2.1 Matricų sudėtis . . . 175
6.2.2 Matricų daugyba iš kūno k elementų . . . 175
6.2.3 Matricų daugyba . . . 176
6.3 Žiedo idealai . . . 180
6.4 Žiedo faktoržiedas pagal idealą . . . 183
6.5 Žiedų homomorfizmai . . . 184

6.6 Dalumas žieduose 190
6.7 Kompleksinių skaičių kūnas 193
6.7.1 Kompleksinių skaičių geometrinė interpretacija 194
6.7.2 Kompleksinių skaičių trigonometrinė išraiška 195
6.7.3 Kompleksinių skaičių rodiklinė išraiška 198
6.7.4 Šaknies traukimas 199
6.7.5 Kompleksinės plokštumos vienetinis apskritimas 200
6.7.6 n-tojo laipsnio šaknys iš vieneto 202
6.8 Polinomų žiedai 203
6.8.1 Polinomų sudėtis ir daugyba 204
6.8.2 Dalybos su liekana formulė 206
6.8.3 Polinomų šaknys 209
6.8.4 Polinomo išvestinė 215
6.8.5 Pirminiai polinomai 219
6.8.6 Racionaliųjų trupmenų kūnas 222
6.8.7 Polinomai su kompleksiniais koeficientais 232
6.8.8 Polinomai su realiaisiais koeficientais 233
6.8.9 Polinomai su racionaliaisiais koeficientais 237
6.8.10 Polinomo šaknų lokalizavimas 240
6.9 Polinomų žiedo $k[x]$ idealų struktūra 249

7 Matricos ir determinantai 254
7.1 Antrosios eilės matricos determinantas 254
7.2 Trečiosios eilės matricos determinantas 255
7.3 Aritmetinė tiesinė erdvė k^n 257
7.4 Matricos 258
7.5 Kvadratinės matricos determinanto funkcija 262
7.6 Determinantų savybės 268
7.7 Determinanto skaičiavimas 270
7.8 Matricų sandaugos determinantas 276
7.9 Atvirkštinė matrica 280
7.10 Atvirkštinės matricos skaičiavimo pavyzdžiai 285
7.11 Kramerio taisyklė 287
7.12 Hamiltono-Keilio teorema 288

Literatūra 291

Pavardžių rodyklė 293

Dalykinė rodyklė 296

Pratarmė

Šis algebros vadovėlis (pirmoji dalis) parašytas Vilniaus universiteto Matematikos ir informatikos fakulteto matematikos specialybės studentams skaitomų algebros paskaitų pagrindu.

Šiuolaikinę matematiką galima palyginti su galinga pramone. Tuo tarpu šis vadovėlis – tai pradžių pradžia, be kurios neįmanoma išsiversti norint žengti į šią pramonę. Dabar aptarsime kai kuriuos algebros aspektus, nagrinėjamus šioje vadovėlio dalyje.

Pirmasis skyrius skirtas aibėms ir aibių atvaizdžiams. Nagrinėjami įvairūs aibės elementų kompozicijos dėsniai (operacijos), apibrėžiantys vienokią ar kitokią jose algebrinę struktūrą.

Antrajame skyriuje nagrinėjama bendra aibės elementų kompozicijos dėsnio (operacijos, veiksmo) sąvoka. Aibėje apibrėžta elementų operacijos, veiksmo arba kompozicijos dėsnio sąvoka yra pirmykštė. Ši sąvoka buvo išryškinta ir pradėta tirti XIX šimtmečio pirmojoje pusėje. Priklausomai nuo aibėje apibrėžtai elementų operacijai ar kelioms apibrėžtoms operacijoms formuluojamų aksiomų, aibėje gauname vienokias ar kitokias algebrines struktūras: grupes, žiedus, kūnus ir kitas. Apibrėžus išorinio kompozicijos dėsnio aibėje sąvoką, galima nagrinėti tiesines erdves, algebras, Li algebras virš kūnų, modulius virš žiedų ir t. t.

Trečiame skyriuje nagrinėjami natūralieji ir sveikieji skaičiai. Įrodoma pagrindinė aritmetikos teorema – pamatas, kuriuo pagrįsta visa sveikųjų skaičių aritmetika.

Tiesinių lygčių sistemos nagrinėjamos ketvirtame skyriuje. Jame išdėstytas Gauso metodas. Taip pat be įrodymų suformuluotos Kronekerio-Kapelio bei tiesinių homogeninių lygčių sistemos sprendinių aibės sandaros teoremos. Šių teoremų įrodymai bus pateikti antroje vadovėlio dalyje.

Penktas skyrius skirtas grupėms. Pavyzdžiui, jei aibėje apibrėžta viena operacija, tenkinanti tris natūraliai paprastas aksiomas, tai ši aibė operacijos atžvilgiu yra vadinama grupe. Grupių yra be galo daug – tiek baigtinių, tiek begalinių.

Grupės gana lengvai apibrėžiamos, bet, kaip rodo praktika, yra sudėtingas matematinis objektas. Grupė labai svarbus matematinis objektas, persmelkiantis ne tik visą matematiką, bet ir fiziką. Grupių kalba aprašomos simetrijos. Žodis „simetrija“kiekvienam žmogui kelia vienokias ar kitokias asociacijas ir kiekvienas ją supranta savaip. Iš pirmo žvilgsnio ir simetrijos sąvoka yra paprasta, nes ji matoma gamtoje (gėlyčių žiedų, daugelio augalų simetrijos), žmonės gėrisi bažnyčių statinių, kurie ir pasižymi įvairiomis simetrijomis, grožiu, net galima žavėtis paprastoje balutėje matoma žydra bedugne ir joje atsispindinčiais plaukiančiais debesėliais. Veidrodinės simetrijos lengviausiai įžvelgiamos. Yra kur kas sudėtingesnės sandaros simetrijų. Pavyzdžiui, analizuojant ornamentus prireikia smulkiai algebriškai apibūdinti 17 ornamentų simetrijų grupių. Įžymus matematikas Veilis simetrijai paskyrė savo nuostabią knygelę „Symmetry“, kurioje daug simetrijos iliustracijų įvairiausiose srityse, ypač mene. Be to, autorius atlieka nuodugnią simetrijų įvairovės matematinę analizę, kaip minėjome, pagrįstą grupių teorija. Ornamentų simetrijų pagrindu Ispanijoje, Granados mieste vienos Alhambra rūmų salės (Sala de Camas) lubos, sienos, grindys išpuoštos nuostabiomis XIV šimtmečio marokiečių (ist. maurų) menininkų mozaikomis. Kaip rašė Veilis, didžiausi ornamentų meistrai buvo arabai. Nepakartojami įžymaus olandų dailininko Ešero kūriniai taip pat persunkti simetrija. Marokiečių dailininkų mozaikos Ešerui padarė nemažą įtaką. Ešero kūrinių simetrijos gana sudėtingos. Sudėtingų simetrijų taip pat galima pamatyti kilimų, juostų raštuose. Iš tikrųjų, simetrijos tema neišsemiama. Fizikoje, kaip išsiaiškinta, simetrijos ir tvermės dėsniai yra neatsiejami. Energijos, impulso, impulso momento, elektros krūvio ir kiti tvermės dėsniai yra susiję su aptinkamomis sąveikų simetrijomis. Simetrijų pagrindu yra sukurti matematiniai modeliai, apimantys stipriąsias, elektromagnetines ir silpnąsias sąveikas. Fizikai, remdamiesi simetrijomis, kūrė elementariųjų dalelių matematinius modelius ir numatė naujų elementariųjų dalelių, kurios tik vėliau buvo aptiktos, egzistavimą. Dažnai simetrijos būna paslėptos, ir jas aptikus pasiseka išspręsti ypač sudėtingus uždavinius. Nuo 1964 metų aptikus daugelio evoliucinių netiesinių dalinių išvestinių diferencialinių lygčių (Kortevego de-Fryzo, sin-Gordono, Kademciavo-Petiašvilio ir kitų) slepiamas simetrijas, pasisekė šias lygtis išspręsti. Be to, buvo aptikti sprendiniai, vadinami solitonais (labai stabilios bangos, primenančios daleles), tai naujos, anksčiau visiškai nežinomos prigimties sprendiniai. Čia paminėtina ir Galua teorija, atsakanti į klausimą, kada polinomo šaknis galima užrašyti naudojant polinomo koeficientus, kurias nors konstantas, radikalus ir racionalius veiksmus (sudėtį, atimtį, daugybą, dalybą). Atsakymas: tada ir tik tada, kai šio polinomo šaknų simetrijos, kurias ir įžvelgė Galua, sudaro išsprendžiamą grupę.

Šeštame skyriuje nagrinėjami žiedai ir jų homorfizmai, t. y. vieno žiedo atvaizdis į kitą, išsaugantis žiedo elementų kompozicijos dėsnių savybes.

Septintas skyrius skirtas matricoms, veiksmams su matricomis, matricų determinantams ir atvirkštinėms matricoms. Matricų koeficientai gali būti tiek racionalieji, tiek realieji ar kompleksiniai skaičiai. Matricų kalba patogu nagrinėti tiesinių lygčių sistemas ir jų sprendinius. Šiame skyriuje rasite Gauso algoritmą, taikomą bendroms tiesinių lygčių sistemoms spręsti.

Baigiant būtina pasakyti keletą žodžių apie atskirą žiedų klasę – kūnus, nors jie bus nagrinėjami antrojoje vadovėlio dalyje. Tai svarbus matematikos objektas. Racionaliųjų skaičių aibėje apibrėžta sudėtis ir daugyba. Sudėtis pasižymi keturiomis savybėmis. Analogiškai daugyba racionaliųjų skaičių aibėje be nulio taip pat pasižymi tokiomis pat keturiomis savybėmis. Sudėtis ir daugyba yra susijusios distributyvumo dėsniu. Visa tai galima pakartoti ir kalbant apie realiuosius skaičius. Ir štai galima nagrinėti abstrakčią aibę, pareikalauti, kad joje būtų apibrėžtos dvi aibės elementų operacijos, kurios tenkintų analogiškas racionaliųjų skaičių aibės sudėties ir daugybos savybes. Tokia aibė joje apibrėžtų dviejų operacijų, tenkinančių devynias aksiomas, atžvilgiu vadinama kūnu. Ką galima pagalvoti ir ko tikėtis, taip apibrėžus naujus objektus? Pasirodo, tokių objektų yra be galo daug. Nuostabu, kad yra baigtinių tokių objektų. Visus baigtinius kūnus aprašė Galua. Matricas galima nagrinėti ne tik su racionaliųjų, realiųjų ar kompleksinių skaičių koeficientais, bet ir su koeficientais kuriame nors kūne k. Panašiai galima nagrinėti tiesinių lygčių sistemas su koeficientais kūne k. Tiesinės lygtys pačiu bendriausiu atveju su koeficientais kūne k gerai ištirtos. Antrojoje vadovėlio dalyje rasite pagrindinius rezultatus apie tiesines lygčių sistemas: Kronekerio-Kapelio teoremą, homogeninių tiesinių lygčių sistemos sprendinių aibės struktūrą ir pagaliau bendros tiesinių lygčių sistemos sprendinių aibės struktūrą.

Autoriai nuoširdžiai dėkoja Algirdui Ambrazevičiui, Aleksui Domarkui, Artūrui Dubickui, Edmundui Gaigalui, Jonui Jankauskui, Aleksandrui Krylovui, Vladui Skakauskui ir Gražvydui Šemetulskiui už vertingas pastabas.

Būtume labai dėkingi, jei pastebėtas klaidas, netikslumus ar pasiūlymus atsiųstumėte el. pašto adresu:
paulius.drungilas@mif.vu.lt

Pastebėtas klaidas ir pataisymus galite rasti tinklalapyje:
http://web.vu.lt/mif/p.drungilas/

Autoriai

2014 m. rugsėjo 1 d.

1 skyrius

Aibės ir atvaizdžiai

1.1 Aibės sąvoka

1.1.1. Šiuolaikinėje matematikoje aibių teorijos yra grindžiamos aksiomų sistemomis. Pagrindinėms algebros struktūroms išdėstyti tinkamiausia yra aibių teorija, pagrįsta Cermelo-Frenkelio (taip pat Bernaiso-Giodelio) aksiomų sistema. Bet aksiomatiškai aibių teorijos mes nedėstysime, nes mūsų tikslams visiškai pakaks pačių elementariausių šios teorijos sąvokų.

Aibių teorijoje, kurią sukūrė Kantoras, aibės ir elemento priklausomumo aibei sąryšio sąvokos buvo grindžiamos intuicija. Pavyzdžiui, Cermelo-Frenkelio aibių teorijoje aibės ir elemento priklausomumo aibei sąryšio sąvokos yra laikomos pirminėmis, o pagrindinės jų savybės nusakomos aksiomomis. Kantoras pateikė tokį aibės apibrėžimą: „Aibę suprasime kaip objektų, kuriuos vieną nuo kito gerai galime atskirti savo intuicija arba mintimis, sujungimą į vieną visumą.“

Nors, kaip rodo aibių teorijos raida, intuicija pasikliauti negalima, mes vis dėlto laikysimės Kantoro apibrėžimo. Tik pabrėšime, kad ne kiekviena kurių nors elementų ar objektų visuma sudaro aibę. Pavyzdžiui, tarę, kad visų aibių visuma yra aibė, neišvengtume paradoksų. Štai vienas paprasčiausių, Bertrano Raselo paradoksas. Pažymėkime raide C visų aibių, kurios nėra savo pačios aibės elementas, visumą. Pavyzdžiui, visų natūraliųjų skaičių aibė $\mathbb{N}$ nėra natūralusis skaičius, visų racionaliųjų skaičių aibė $\mathbb{Q}$ taip pat nėra racionalusis skaičius, t. y. šios aibės priklauso C. Tarę, kad C yra aibė, išsiaiškinkime, ar aibė C yra aibės C elementas, ar ne. Jei aibė C yra aibės C elementas, tai aibė C nepriklauso aibei C pagal C apibrėžimą. Jei aibė C nėra aibės C elementas, tai aibė C priklauso C pagal C apibrėžimą. Kaip matome, tikrai labai paprastas paradoksas.

Dėl aptiktų Kantoro aibių teorijoje paradoksų matematikams iškilo problema pagrįsti aibių teoriją taip, kad joje nebūtų paradoksų, o Kantoro aibių teorijos esminiai pasiekimai – kardinalų ir ordinalų teorija – būtų išsaugoti. Nebuvo sugalvota nieko geresnio, kaip kurti aibių teorijas aksiomatiškai. Vėliau apie tai kalbėsime kiek plačiau.

1.1.2. Aptarsime aibių teorijos elementariausias sąvokas ir žymėjimus. Užrašai „$a \in A$“ arba „$A \ni a$“ yra skaitomi „a yra aibės A elementas“ arba „a priklauso aibei A“. Užrašai „$a \notin A$“ arba „$A \not\ni a$“ yra skaitomi „a nėra aibės A elementas“ arba „a nepriklauso aibei A“. Aibė, neturinti nė vieno elemento, vadinama tuščiąja ir yra žymima $\emptyset$. Baigtinę aibę, sudarytą iš elementų $x_1, x_2, \ldots, x_n$, sutarkime užrašyti $\{x_1, x_2, \ldots, x_n\}$.

1.1.3 apibrėžimas (aibės poaibio apibrėžimas)**.** Sakoma, kad aibė A yra aibės B *poaibis* ir žymima $A \subset B$ arba $B \supset A$, jei aibės A kiekvienas elementas yra ir aibės B elementas. Aibės poaibio apibrėžimas matematiniais simboliais užrašomas taip:

$$A \subset B \Longleftrightarrow \forall a(a \in A \Rightarrow a \in B).$$

Užrašai „$A \not\subset B$“ arba „$B \not\supset A$“ yra skaitomi „aibė A nėra aibės B poaibis“. Aibė A nėra aibės B poaibis, jei egzistuoja toks aibės A elementas a, kuris nepriklauso aibei B. Apibrėžimą „aibė A nėra aibės B poaibis“ matematiniais simboliais galime užrašyti taip:

$$A \not\subset B \Longleftrightarrow \exists a(a \in A \wedge a \notin B).$$

Aibių įdėties sąryšis $\subset$ (arba $\supset$) turi tokias savybes:

1. Jei $A \subset B$ ir $B \subset C$, tai $A \subset C$. Matematinių simbolių žymėjimais ši savybė atrodo taip:
$$A \subset B \wedge B \subset C \implies A \subset C.$$
2. Kiekvienai aibei A, $\emptyset \subset A$. Matematinių simbolių žymėjimais ši savybė atrodo taip:
$$\forall A(\emptyset \subset A).$$

1.1.4 apibrėžimas (aibių lygybės apibrėžimas)**.** Aibės A ir B yra vadinamos *lygiomis* ir žymima $A = B$, jei $A \subset B$ ir $B \subset A$. Matematinių simbolių žymėjimais šis apibrėžimas atrodo taip:

$$A = B \iff A \subset B \wedge B \subset A.$$

Aibių lygybės sąryšis $=$ pasižymi tokiomis savybėmis:

1. Kiekvienai aibei A, $A = A$.

2. Jei $A = B$, tai $B = A$. Matematiniais simboliais ši savybė užrašoma taip:

$$A = B \implies B = A.$$

3. Jei $A = B$, $B = C$, tai $A = C$. Matematiniais simboliais ši savybė užrašoma taip:

$$A = B,\ B = C \implies A = C.$$

1.1.5 (aibės poaibiai)**.** Fiksuotos aibės A visų poaibių visuma sudaro aibę, kuri yra žymima $P(A)$ arba 2^A. Taigi $X \subset A \iff X \in P(A)$.

Aibės A poaibiai dažnai yra apibrėžiami kuria nors savybe S, kurią turintys aibės A elementai ir sudaro aibės A poaibį. Aibės A elementų, turinčių savybę S, visumą žymėsime $\{x \in A \mid S(x)\}$. Pavyzdžiui, $\{x \in \mathbb{R} \mid x > 2\}$ yra realiųjų skaičių aibės poaibis, sudarytas iš realiųjų skaičių, didesnių už 2. Aibių teorijoje, grindžiamoje aksiomų sistema, yra kruopščiai aptariamos savybių klasės, leistinos nagrinėjamoje teorijoje. Tos savybės, kurias vėliau nagrinėsime, norėdami apibrėžti kurios nors aibės tam tikrus poaibius, nesukels jokių loginių sunkumų.

1.2 Veiksmai su aibėmis

1.2.1 apibrėžimas (aibių sumos (junginio) apibrėžimas)**.** Aibių A ir B *suma* (*junginiu*, *sąjunga*), žymima $A \cup B$, yra vadinama aibė, sudaryta iš visų tų elementų, kurie priklauso bent vienai iš aibių – A arba B. Matematinių simbolių žymėjimais aibių suma apibrėžiama taip:

$$x \in A \cup B \iff x \in A \vee x \in B.$$

Aibių sumą galima apibrėžti ir taip:

$$A \cup B = \{x \mid x \in A \text{ arba } x \in B\}.$$

Panašiai galima apibrėžti ir užrašyti ir aibių šeimos sumą. Aibių *šeima* yra vadinama tokia aibių A_α visuma $\{A_\alpha\}_{\alpha \in I}$, kurios elementai „sunumeruoti“kurios nors aibės I elementais α. Aibių šeimos $\{A_\alpha\}_{\alpha \in I}$ aibės, kurių indeksai skirtingi, gali būti lygios.

1.2.2 apibrėžimas (aibių šeimos suma)**.** Aibių šeimos $\{A_\alpha\}_{\alpha \in I}$ *suma* (*junginiu*, *sąjunga*), žymima

$$\bigcup_{\alpha \in I} A_\alpha,$$

vadinama aibė, sudaryta iš visų tų elementų, kurie priklauso bent vienai iš aibių A_α, $\alpha \in I$. Matematinių simbolių žymėjimais aibių šeimos suma apibrėžiama taip:

$$\bigcup_{\alpha \in I} A_\alpha = \{x \mid \exists \alpha \in I (x \in A_\alpha)\}.$$

Pratimai.
Įrodykite, kad bet kurioms aibėms A, B, C teisingos tokios lygybės:

1. $A \cup (B \cup C) = (A \cup B) \cup C$. Ši savybė vadinama aibių sudėties *asociatyvumu.*

2. $A \cup B = B \cup A$. Ši savybė vadinama aibių sudėties *komutatyvumu.*

3. $A \cup A = A$. Ši savybė vadinama aibių sudėties *idempotentumo* dėsniu.

1.2.3 apibrėžimas (aibių sankirtos (sandaugos) apibrėžimas)**.** Aibių A ir B *sankirta* (*sandauga*), žymima $A \cap B$, vadinama aibė, sudaryta iš visų tų elementų, kurie priklauso ir aibei A ir aibei B. Matematinių simbolių žymėjimais šis apibrėžimas atrodo taip:

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

arba

$$x \in A \cap B \iff x \in A \wedge x \in B.$$

1.2.4 apibrėžimas (Aibių šeimos sankirta (sandauga))**.** Aibių šeimos $\{A_\alpha\}_{\alpha \in I}$ *sankirta* (*sandauga*), žymima

$$\bigcap_{\alpha \in I} A_\alpha,$$

vadinama aibė, sudaryta iš visų tų elementų, kurie priklauso kiekvienai aibei A_α, $\alpha \in I$. Matematinių simbolių žymėjimais aibių šeimos sankirta apibrėžiama taip:

$$\bigcap_{\alpha \in I} A_\alpha = \{x \mid \forall \alpha \in I (x \in A_\alpha)\}.$$

Pratimai.
Įrodykite, kad bet kurioms aibėms A, B, C teisingos tokios lygybės:

1. $(A \cap B) \cap C = A \cap (B \cap C)$ (aibių sankirtos asociatyvumo dėsnis).

2. $A \cap B = B \cap A$ (aibių sankirtos komutatyvumo dėsnis).

3. $A \cap A = A$ (aibių sankirtos idempotentumo dėsnis).

1.2.5 apibrėžimas (aibių skirtumo apibrėžimas)**.** Aibių A ir B *skirtumu*, žymimu $A \backslash B$, vadinama aibė, sudaryta iš visų tų aibės A elementų, kurie nepriklauso aibei B. Matematinių simbolių žymėjimais šis apibrėžimas atrodo taip:

$$A \setminus B = \{x \in A \mid x \notin B\}$$

arba

$$x \in A \setminus B \iff x \in A \wedge x \notin B.$$

Akivaizdu, kad $A \setminus B \subset A$ ir

$$A \setminus B = A \Longleftrightarrow A \cap B = \emptyset.$$

Be to, teisinga lygybė $A \cap B = A \setminus (A \setminus B)$.

1.2.6 apibrėžimas (aibių simetrinio skirtumo apibrėžimas)**.** Aibių A ir B *simetriniu skirtumu*, žymimu $A \ominus B$, vadinama aibė

$$(A \setminus B) \cup (B \setminus A).$$

1.2.7 (distributyvumo dėsniai)**.** Aibių sudėtis ir sankirta yra susijusios *distributyvumo* dėsniais. Bet kurioms aibėms A, B, C teisingos lygybės:

1. $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ (pirmasis distributyvumo dėsnis, siejantis aibių sudėtį ir sankirtą).
2. $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ (antrasis distributyvumo dėsnis, siejantis aibių sudėtį ir sankirtą).

Pratimai.

1. Įrodykite anksčiau užrašytus distributyvumo dėsnius, siejančius aibių sudėtį ir sankirtą.
2. Įrodykite, kad bet kurioms aibėms A, B, C teisingos lygybės:

   a) $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$;

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

   Šios lygybės vadinamos de Morgano dėsniais. De Morgano dėsnius galima užrašyti bendriausiu atveju:

   $$A \setminus (\bigcap_{\alpha \in I} B_\alpha) = \bigcup_{\alpha \in I} (A \setminus B_\alpha)$$

   ir

   $$A \setminus (\bigcup_{\alpha \in I} B_\alpha) = \bigcap_{\alpha \in I} (A \setminus B_\alpha).$$

3. Įrodykite, kad bet kurioms aibėms A, B, C teisingos lygybės:

   a) $(A \setminus B) \cap C = (A \cap C) \setminus (B \cap C)$. Kaip matome, aibių skirtumas ir sankirta susiję distributyvumo dėsniu.

   b) $(A \ominus B) \ominus C = A \ominus (B \ominus C)$. Kaip matome, simetrinis aibių skirtumas yra asociatyvus.

   c) $(A \ominus B) \cap C = (A \cap C) \ominus (B \cap C)$. Kaip matome, simetrinis aibių skirtumas ir aibių sankirta susiję distributyvumo dėsniu.

1.2.8 apibrėžimas (aibės papildinio apibrėžimas)**.** Aibės A poaibio X *papildiniu* iki aibės A, žymimu $C_A X$, vadinama aibė $A \ominus X = A \setminus X$.

1.2.9 pastaba. Paprastumo dėlei tais atvejais, kai iš konteksto aišku, iki kokios aibės yra imamas papildinys, apatinį indeksą A praleisime.

Pratimai.
Tarkime, kad $X \subset A$, $Y \subset A$. Įrodykite, jog teisingos tokios lygybės:

1. $C(CX) = X$.

2. $X \subset Y \Longrightarrow CX \supset CY$.

3. $C(X \cap Y) = CX \cup CY$.

4. $C(X \cup Y) = CX \cap CY$.

Aibės papildinio trečioji ir ketvirtoji savybės – tai de Morgano dėsniai. Remdamiesi aibės papildinio pirmąja ir antrąja savybėmis, gauname, kad

$$X = Y \Longleftrightarrow CX = CY.$$

Pavyzdžiai ir pratimai.
Bet kuriam natūraliajam skaičiui n ir bet kuriam sveikajam skaičiui r pažymėkime

$$n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \quad \text{ir}$$

$$r + n\mathbb{Z} = \{r + nk \mid k \in \mathbb{Z}\}.$$

1. Įrodykite, kad $n\mathbb{Z} \subset m\mathbb{Z}$ tada ir tik tada, kai skaičius m dalija skaičių n.

2. Įrodykite, kad $n\mathbb{Z} \cap m\mathbb{Z} = r\mathbb{Z}$, čia skaičius r yra skaičių m ir n mažiausias bendrasis kartotinis.

3. Tegu $r_1, r_2 \in \mathbb{Z}$. Įrodykite, kad $r_1 + n\mathbb{Z} = r_2 + n\mathbb{Z}$ tada ir tik tada, kai skaičius n dalija $r_1 - r_2$. Taip pat įrodykite, kad jei n nedalija $r_1 - r_2$, tai
$$(r_1 + n\mathbb{Z}) \cap (r_2 + n\mathbb{Z}) = \emptyset.$$

4. Įrodykite, kad $\bigcup_{j=0}^{n-1}(j + n\mathbb{Z}) = \mathbb{Z}$.

5. Bet kuriam $s \in \mathbb{Q}$ apibrėžkime aibę $s\mathbb{Z} = \{sk \mid k \in \mathbb{Z}\}$. Įrodykite, kad aibė
$$\bigcup_{j=0}^{\infty} \frac{1}{p^j}\mathbb{Z},$$
čia p – pirminis skaičius, sudaryta iš tų racionaliųjų skaičių, kurių vardiklis – pirminio skaičiaus p laipsnis, t. y.
$$\alpha \in \bigcup_{j=0}^{\infty} \frac{1}{p^j}\mathbb{Z} \iff (\exists m \in \mathbb{Z})(\exists s \in \mathbb{N}) \left(\alpha = \frac{m}{p^s}\right).$$

6. Įrodykite, kad bet kuriam natūraliajam skaičiui m teisinga lygybė:
$$\bigcup_{j=0}^{\infty} \frac{1}{p^j}\mathbb{Z} = \bigcup_{j=m}^{\infty} \frac{1}{p^j}\mathbb{Z}.$$

7. Įrodykite, kad
$$\mathbb{Q} = \bigcup_{\substack{0 \le r < 1 \\ r \in \mathbb{Q}}} (r + \mathbb{Z}),$$
čia $r + \mathbb{Z} = \{r + n \mid n \in \mathbb{Z}\}$.

1.3 Sąryšis

1.3.1 Nesutvarkytosios poros (nesutvarkytieji dvejetai)

Kad ir kokie būtų objektai x ir y, egzistuoja aibė A, kurios elementai yra x ir y. Šią aibę sutarkime užrašyti $\{x, y\}$ ir vadinti *nesutvarkytąja pora* (arba *nesutvarkytuoju dvejetu*). Matematinių simbolių žymėjimais aibė $A = \{x, y\}$ apibrėžiama taip:
$$\forall x \forall y \exists! A\, (z \in A \implies z = x \lor z = y).$$

Savaime aišku, kad $\{x, y\} = \{y, x\}$. Jei $x = y$, tai aibę $\{x, x\}$ žymėsime $\{x\}$. Panašiai galima apibrėžti nesutvarkytąjį trejetą, ketvertą ir t. t.

1.3.1 apibrėžimas (sutvarkytosios poros (sutvarkytieji dvejetai))**.** Apibrėšime sutvarkytosios poros Kuratovskio konstrukciją. Imkime bet kokius objektus x ir y ir sudarykime aibę $(x, y) = \{\{x\}, \{x, y\}\}$. Atkreipkite dėmesį, kad pirmiausia iš objektų x ir y yra sudaromos aibės $\{x\}$ ir $\{x, y\}$, o iš tų aibių yra sudaroma aibė $\{\{x\}, \{x, y\}\}$. Akivaizdu, kad $(x, y) \neq (y, x)$, jei tik $x \neq y$. Aibė (x, y) vadinama *sutvarkytąja pora* (arba *sutvarkytuoju dvejetu*), x – sutvarkytosios poros pirmuoju elementu, o y – sutvarkytosios poros antruoju elementu. Svarbiausia sutvarkytosios poros (sutvarkytojo dvejeto) savybė yra:

$$(x_1, y_1) = (x_2, y_2) \iff x_1 = x_2 \wedge y_1 = y_2.$$

Dėl šios savybės ir yra apibrėžiama sutvarkytoji pora. Teiginį „z yra sutvarkytoji pora“ar „z yra sutvarkytasis dvejetas“suprasime taip: egzistuoja tokie objektai x ir y, kad $z = (x, y)$.

Panašiai galima apibrėžti sutvarkytuosius trejetus, ketvertus ir t. t. Sutvarkytojo n objektų rinkinio $(x_1, x_2, \ldots, x_n)$ pagrindinė savybė yra tokia:

$$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \iff x_1 = y_1 \wedge x_2 = y_2 \wedge \ldots \wedge x_n = y_n.$$

1.3.2 apibrėžimas (sąryšio apibrėžimas)**.** Aibė R, kurios elementai yra sutvarkytosios poros (sutvarkytieji dvejetai), vadinama *binariuoju (dviviečiu) sąryšiu* arba binariąja (dviviete) atitiktimi. Šis apibrėžimas, užrašytas matematinių simbolių žymėjimais, atrodo taip:

$$R - \text{sąryšis} \iff \forall z (z \in R \Longrightarrow z - \text{sutvarkytoji pora}).$$

Sakoma, kad elementas x susijęs sąryšiu R su elementu y ir žymima xRy, jei sutvarkytoji pora $(x, y) \in R$. Kitaip tariant, $xRy \iff (x, y) \in R$.

1.3.3 apibrėžimas (sąryšio apibrėžimo ir kitimo sritys)**.** Visų sutvarkytųjų porų, priklausančių R, pirmųjų elementų aibė $D(R)$ vadinama sąryšio R *apibrėžimo sritimi*, o tų sutvarkytųjų porų antrųjų elementų aibė $E(R)$ – sąryšio R *kitimo sritimi* (arba sąryšio R *reikšmių aibe*). Matematinių simbolių žymėjimais šie apibrėžimai atrodo taip:

$$D(R) = \{x \mid \exists y((x, y) \in R)\},$$

$$E(R) = \{y \mid \exists x((x, y) \in R)\}.$$

Galime užrašyti ir taip:

$$D(R) = \{x \mid \exists y(xRy)\},$$

$$E(R) = \{y \mid \exists x(xRy)\}.$$

1.3.4 apibrėžimas (atvirkštinis sąryšis)**.** Sąryšis

$$R^{-1} = \{(x,y) \mid yRx\}$$

vadinamas atvirkštiniu sąryšiui R.

Galima užrašyti ir taip:

$$xR^{-1}y \Longleftrightarrow yRx \quad \text{arba} \quad (x,y) \in R^{-1} \Longleftrightarrow (y,x) \in R.$$

Akivaizdu, kad $D(R^{-1}) = E(R)$, $E(R^{-1}) = D(R)$.

1.3.5 apibrėžimas (sąryšių kompozicija (superpozicija))**.** Sąryšių R_1 ir R_2 kompozicija (superpozicija) vadinamas sąryšis

$$R_2 \circ R_1 = \{(x,y) \mid \exists z((x,z) \in R_1 \land (z,y) \in R_2)\}.$$

Akivaizdu, kad $D(R_2 \circ R_1) \subset D(R_1)$, $E(R_2 \circ R_1) \subset E(R_2)$.

Pratimai.
Įrodykite, kad bet kokiems sąryšiams R_1, R_2, R_3 teisingos lygybės:

1. $(R_3 \circ R_2) \circ R_1 = R_3 \circ (R_2 \circ R_1)$.
2. $(R_2 \circ R_1)^{-1} = R_1^{-1} \circ R_2^{-1}$.
3. $(R^{-1})^{-1} = R$.

1.3.6 (sąryšio siaurinys)**.** Tarkime, R – sąryšis, $D(R)$ – sąryšio R apibrėžimo sritis. Kiekvienam aibės $D(R)$ poaibiui X egzistuoja sąryšis

$$R\big|_X = \{(x,y) \in R \mid x \in X\}.$$

Panašiai kiekvienam sąryšio R reikšmių srities $E(R)$ poaibiui Y egzistuoja sąryšis

$${}_Y\big|R = \{(x,y) \in R \mid y \in Y\}.$$

Sąryšis $R\big|_X$ vadinamas sąryšio R *siauriniu*, gaunamu susiaurinant sąryšio R apibrėžimo sritį $D(R)$ iki poaibio X. Panašiai ${}_Y\big|R$ vadinamas sąryšio R siauriniu, gaunamu susiaurinant sąryšio R kitimo sritį $E(R)$ iki poaibio Y. Akivaizdu, kad

$$R\big|_X \subset R, \;\; D(R\big|_X) = X, \;\; E(R\big|_X) \subset E(R),$$

$${}_Y\big|R \subset R, \;\; D({}_Y\big|R) \subset D(R), \;\; E({}_Y\big|R) = Y.$$

Pratimai.
Remdamiesi sąryšio siaurinio apibrėžimu, įrodykite:

1. Jei $X_1 \subset X_2 \subset D(R)$, tai $(R\big|_{X_2})\big|_{X_1} = R\big|_{X_1}$.
2. Jei $Y_1 \subset Y_2 \subset E(R)$, tai ${}_{Y_1}\big|({}_{Y_2}\big|R) = {}_{Y_1}\big|R$.
3. Jei $X \subset D(R)$, $Y \subset E(R)$, tai ${}_{Y}\big|(R\big|_{X}) = ({}_{Y}\big|R)\big|_{X}$.

1.3.7 (sąryšio plėtinys)**.** Sąryšis S vadinamas sąryšio R *plėtiniu*, jei $D(R) \subset D(S)$, $E(R) \subset E(S)$, $R = S\big|_{D(R)}$. Sąryšio R plėtinį galima apibrėžti ir kita prasme: sąryšis S yra sąryšio R plėtinys, jei $R = {}_{E(R)}\big|S$.

1.3.8 (veiksmai su sąryšiais)**.** Kadangi sąryšiai yra aibės, tai veiksmai su sąryšiais tokie pat, kaip ir su aibėmis. Taigi galima apibrėžti sąryšių sumą, sankirtą, skirtumą ir t. t.

Pratimai.
Įrodykite, jog bet kuriems sąryšiams R_1, R_2, R_3 teisingos tokios lygybės:

1. $D(R_1 \cup R_2) = D(R_1) \cup D(R_2)$, $E(R_1 \cup R_2) = E(R_1) \cup E(R_2)$;
2. $D(R_1 \cap R_2) \subset D(R_1) \cap D(R_2)$, $E(R_1 \cap R_2) \subset E(R_1) \cap E(R_2)$.
3. $D(R_1 \setminus R_2) \supset D(R_1) \setminus D(R_2)$, $E(R_1 \setminus R_2) \supset E(R_1) \setminus E(R_2)$.
4. $(R_1 \cup R_2)^{-1} = R_1^{-1} \cup R_2^{-1}$, $(R_1 \cap R_2)^{-1} = R_1^{-1} \cap R_2^{-1}$, $(R_1 \setminus R_2)^{-1} = R_1^{-1} \setminus R_2^{-1}$.
5. $(R_1 \cup R_2) \circ R_3 = (R_1 \circ R_3) \cup (R_2 \circ R_3)$, $R_1 \circ (R_2 \cup R_3) = (R_1 \circ R_2) \cup (R_1 \circ R_3)$.
6. $(R_1 \cap R_2) \circ R_3 \subset (R_1 \circ R_3) \cap (R_2 \circ R_3)$, $R_1 \circ (R_2 \cap R_3) \subset (R_1 \circ R_2) \cap (R_1 \circ R_3)$.

1.3.2 Funkcinis sąryšis (funkcija). Atvaizdis

1.3.9 apibrėžimas. Sąryšis R vadinamas *funkciniu sąryšiu* arba *funkcija*, jei

$$(\forall x \forall y \forall z)\left((x, y) \in R \wedge (x, z) \in R \Longrightarrow y = z\right).$$

Galima pasakyti ir taip: R yra funkcija, jei aibei R nepriklauso du skirtingi sutvarkytieji dvejetai su tuo pačiu pirmuoju elementu, t. y., jei $(a, b) \in R$ ir $(a, c) \in R$, tai $b = c$.

Funkcijas žymėsime raidėmis f, g, h, ir t. t.

1.3.10 pastaba. Jei f yra funkcija, tai bendruoju atveju f^{-1} nėra funkcija. Pavyzdžiui, $f = \{(x, x^2) \mid x \in \mathbb{R}\}$ yra funkcija, bet $f^{-1} = \{(x^2, x) \mid x \in \mathbb{R}\}$ nėra funkcija, nes $(1, 1) \in f^{-1}$ ir $(1, -1) \in f^{-1}$, šių sutvarkytų dvejetų pirmieji elementai yra lygūs, o antrieji – nėra lygūs. Panašiai $g = \{(x, \sin x) \mid x \in \mathbb{R}\}$ yra funkcija, o g^{-1} nėra funkcija.

1.3.11 pastaba. Funkcijų f ir g sąjunga (suma) $f \cup g$ bendruoju atveju nėra funkcija. Pavyzdžiui, $f = \{(1,2)\}$, $g = \{(1,3)\}$ yra funkcijos, o

$$f \cup g = \{(1,2),(1,3)\}$$

nėra funkcija, nes sutvarkytųjų dvejetų $(1,2)$ ir $(1,3)$, priklausančių $f \cup g$, pirmieji elementai yra lygūs, o antrieji – nėra lygūs.

1.3.12 pastaba. Funkcijų f ir g sankirta $f \cap g$, jei tik netuščia, visuomet yra funkcija.

1.3.13 apibrėžimas (atvaizdžio apibrėžimas)**.** Funkcija f vadinama *atvaizdžiu* iš aibės A į aibę B, jei $D(f) = A$, $E(f) \subset B$. Šiuo atveju taip pat sakoma, kad f yra atvaizdis, apibrėžtas aibėje A ir įgyjantis reikšmes aibėje B. Atvaizdis f iš aibės A į aibę B žymimas $f : A \to B$ arba $A \xrightarrow{f} B$. Jei $(a,b) \in f$, tai elementas $b \in B$ vadinamas elemento $a \in A$ *vaizdu* ir yra žymimas $f(a)$.

Dažnai naudojami ir tokie atvaizdžio f iš aibės A į aibę B žymėjimai:

$$A \ni a \mapsto f(a) \in B, \quad \text{arba} \quad A \to B, a \mapsto f(a).$$

Šie žymėjimai dažniausiai naudojami tais atvejais, kai apibrėžiamas atvaizdis f, nurodant aibės A elemento a vaizdą $f(a) \in B$ formule ar kuria nors vienareikšmiškai nusakoma taisykle ir t. t. Pavyzdžiui, $f : \mathbb{R} \to \mathbb{R}$, $x \mapsto x^2$, $\sin : \mathbb{R} \to \mathbb{R}$, $x \mapsto \sin x$ ir t. t.

Tarkime, kad f yra atvaizdis iš aibės A į aibę B. Tuomet kiekvienam $a \in A$ egzistuoja toks vienintelis $b \in B$, kad $(a,b) \in f$ (arba afb). Todėl dažnai atvaizdis $f : A \to B$ literatūroje vadinamas taisykle f, kuria remiantis kiekvienam aibės A elementui a priskiriamas vienas ir tik vienas aibės B elementas b, kuris yra žymimas $f(a)$ ir vadinamas elemento a vaizdu.

1.3.14 apibrėžimas. Tarkime, kad $f : A \to B$ yra atvaizdis, $X \subset A$, $Y \subset B$. Aibė $f(X) = \{f(x) \mid x \in X\}$, sudaryta iš aibės A poaibio X elementų vaizdų, vadinama aibės A poaibio X *vaizdu.* Jei $X = \{a\}$, tai vietoje $f(\{a\})$ rašysime $f(a)$.

Aibės A poaibio X vaizdą $f(X)$ galime apibrėžti ir taip: $f(X) = E(f\,\big|_X)$ arba $f(X) = \{b \in B \mid (\exists x \in X)(f(x) = b)\}$.

1.3.15 apibrėžimas. Aibė $f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}$, sudaryta iš visų tokių aibės A elementų, kurių vaizdai priklauso Y, $Y \subset B$, vadinama aibės B poaibio Y *pilnuoju pirmavaizdžiu* (dažniausiai žodis „pilnasis“yra praleidžiamas). Jei $Y = \{b\}$, tai vietoje $f^{-1}(\{b\})$ rašysime $f^{-1}(b)$.

Aibės B poaibio Y pilnąjį pirmavaizdį $f^{-1}(Y)$ galime apibrėžti ir taip:

$$f^{-1}(Y) = D({}_Y\big|f) \text{ arba } f^{-1}(Y) = E(f^{-1}\big|_Y).$$

1.3.16 (atvaizdžių kompozicija)**.** Sakykime, kad $f : A \to B$ ir $g : B \to C$ yra atvaizdžiai. Tuomet, remdamiesi atvaizdžio apibrėžimu, gauname, kad funkcijų g ir f kompozicija $g \circ f$ yra atvaizdis $g \circ f : A \to C$, kuris vadinamas atvaizdžių f ir g *kompozicija.*

Jei $f : A \to B$ ir $g : B \to C$ – atvaizdžiai, tai kiekvienam $a \in A$, $(g \circ f)(a) = g(f(a))$.

Pratimas. Sakykime, kad $f : A \to B$, $g : B \to C$, $h : C \to D$ yra atvaizdžiai. Įrodykite, kad $h \circ (g \circ f) = (h \circ g) \circ f$. Remdamiesi šia lygybe, matome, kad atvaizdžių kompozicija yra asociatyvus dėsnis.

1.3.17 apibrėžimas. Visų atvaizdžių iš aibės A į aibę B visuma sudaro aibę, kuri yra žymima B^A. Pagal apibrėžimą

$$f \in B^A \iff f : A \to B - \text{ atvaizdis.}$$

Pratimai.
Tarkime, kad $f : A \to B$ yra atvaizdis, $X_1, X_2 \subset A$, $Y_1, Y_2 \subset B$. Įrodykite tokias lygybes:

1. $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$.
2. $f(X_1 \cap X_2) \subset f(X_1) \cap f(X_2)$.
3. $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$.
4. $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f^{-1}(Y_2)$.
5. $f^{-1}(Y_1 \setminus Y_2) = f^{-1}(Y_1) \setminus f^{-1}(Y_2)$.
6. $f^{-1}(Y_1 \ominus Y_2) = f^{-1}(Y_1) \ominus f^{-1}(Y_2)$.
7. $f(f^{-1}(Y_1)) = Y_1$.
8. $f^{-1}(f(X_1)) \supset X_1$.

1.3.18 pastaba. Jei f yra atvaizdis iš aibės A į aibę B, tai, remdamiesi aibės vaizdo pilnojo pirmavaizdžio apibrėžimais, matome, kad f generuoja atvaizdį iš aibės $P(A)$ į aibę $P(B)$, o f^{-1} (gal ir nebūdamas atvaizdis iš aibės $E(f)$ į aibę A) generuoja atvaizdį iš aibės $P(B)$ į aibę $P(A)$, kuriuos žymime f ir f^{-1}. Induktyviai būtų galima apibrėžti atvaizdžius

$$P^n(f) : P^n(A) \to P^n(B), n \in \mathbb{Z}, n \geq 1,$$

generuotus atvaizdžio $f : A \to B$ ir atvaidžius

$$P^n(f^{-1}) : P^n(B) \to P^n(A), n \in \mathbb{Z}, n \geq 1,$$

generuotus atvaizdžio $f^{-1} : P(B) \to P(A)$, čia $P^n(A) = \underbrace{P(P(\ldots(P}_{n}(A))\ldots))$.

1.3.19 apibrėžimas (aibių Dekarto sandauga)**.** Aibių A ir B *Dekarto sandauga*, žymima $A \times B$, vadinama aibė, sudaryta iš visų sutvarkytųjų dvejetų (a, b), $a \in A$, $b \in B$. Matematinių simbolių žymėjimais šis apibrėžimas atrodo taip:

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

Egzistuoja kanoniniai atvaizdžiai

$$pr_1 : A \times B \to A,\ pr_1((a, b)) = a$$

ir

$$pr_2 : A \times B \to A,\ pr_2((a, b)) = b,$$

kurie vadinami aibių A ir B Dekarto sandaugos $A \times B$ *projekcijomis* atitinkamai į pirmąjį ir antrąjį dauginamuosius A ir B.

Panašiai galima apibrėžti aibių A_1, A_2, ..., A_n Dekarto sandaugą

$$A_1 \times A_2 \times \cdots \times A_n$$

ir projekcijas

$$pr_j : A_1 \times A_2 \times \cdots \times A_n \to A_j,\ 1 \leq j \leq n.$$

Jei $A_1 = A_2 = \cdots = A_n$, tai vietoje

$$\underbrace{A \times A \times \cdots \times A}_{n}$$

rašoma A^n.

Kadangi

$$A^n = \{(a_1, a_2, \ldots, a_n) \mid a_j \in A,\ 1 \leq j \leq n\},$$

tai A^n galima sutapatinti su visų atvaizdžių iš $\{1, 2, \ldots, n\}$ į A aibe. Kaip matome, žymėjimas A^n yra suderintas su žymėjimu B^A (žr. 1.3.17 apibrėžimą).

1.3.20 apibrėžimas (aibių šeimos Dekarto sandauga)**.** Aibių šeimos $\{A_\alpha\}_{\alpha \in I}$ *Dekarto sandauga* vadinama aibė $\prod\limits_{\alpha \in I} A_\alpha$, sudaryta iš visų atvaizdžių f, apibrėžtų aibėje I, ir kiekvienam $\alpha \in I$ įgyjančių reikšmę $f(\alpha) \in A_\alpha$. Egzistuoja kanoninės projekcijos

$$pr_\alpha : \prod_{\beta \in I} A_\beta \to A_\alpha,\quad pr_\alpha(f) = f(\alpha),\quad f \in \prod_{\beta \in I} A_\beta,\quad \alpha \in I.$$

1.3.21 apibrėžimas (atvaizdžio grafikas)**.** Tarkime, kad $f : A \to B$ yra atvaizdis. Aibės $A \times B$ poaibis $\Gamma_f = \{(a, f(a)) \,|\, a \in A\}$ vadinamas atvaizdžio f *grafiku.*

1.3.22 pastaba. Remdamiesi atvaizdžio f apibrėžimu, matome, kad f ir Γ_f kaip aibės yra lygios. Kalbant apie atvaizdžio f grafiką $\Gamma_f = f$, svarbu tai, kad abi aibės Γ_f ir f nagrinėjamos kaip aibės $A \times B$ poaibiai. Savaime suprantama, kad atvaizdžio grafikas $\Gamma_f \subset A \times B$ vienareikšmiškai apibrėžia patį atvaizdį $f : A \to B$.

1.3.23 pavyzdys. Atvaizdžio $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$, $x \in \mathbb{R}$, grafikas $\Gamma_f = \{(x, x^2)|x \in \mathbb{R}\}$ yra plokštumos $\mathbb{R}^2$ kreivė, kuri vadinama parabole.

1.3.24 apibrėžimas (injekcinis atvaizdis (injekcija))**.** Atvaizdis $f : A \to B$ vadinamas *injekciniu atvaizdžiu* arba *injekcija*, jei bet kuriems $x, y \in A$,

$$f(x) = f(y) \Longrightarrow x = y.$$

Galima injekcinį atvaizdį apibrėžti ir taip: atvaizdis $f : A \to B$ yra vadinamas injekciniu atvaizdžiu arba injekcija, jei bet kuriems $x, y \in A$,

$$x \neq y \Longrightarrow f(x) \neq f(y).$$

Injekcinį atvaizdį galima apibūdinti dar ir taip: kiekvieno elemento $y \in f(A)$ pilnasis pirmavaizdis $f^{-1}(y)$ sudarytas tik iš vieno elemento.

Jei $f : A \to B$ yra injekcinis atvaizdis, tai apibrėžtas atvaizdis $f^{-1} : f(A) \to A$, $f^{-1}(f(a)) = a$, $a \in A$.

1.3.25 pavyzdys. Atvaizdis $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$, yra injekcija, nes $x^3 = y^3 \Leftrightarrow x = y$, $x, y \in \mathbb{R}$. Atvaizdis $g : \mathbb{R} \to [0, \infty]$, $g(x) = x^2$, nėra injekcija, nes $f(-1) = f(1)$.

1.3.26 apibrėžimas (siurjekcinis atvaizdis (siurjekcija))**.** Atvaizdis $f : A \to B$ vadinamas *siurjekciniu atvaizdžiu* arba *siurjekcija*, jei $f(A) = B$.

Kitaip tariant, atvaizdis $f : A \to B$ yra siurjekcinis, jei kiekvienam $b \in B$, egzistuoja toks $a \in A$, kad $f(a) = b$.

1.3.27 pavyzdys. Atvaizdis $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$, yra siurjekcija, nes $\mathbb{R} = E(f)$. Atvaizdis $g : \mathbb{R} \to [0, \infty]$, $g(x) = x^2$, yra siurjekcija, nes $[0, \infty] = E(g)$. Atvaizdis $h : \mathbb{R} \to \mathbb{R}$, $h(x) = 2\sin(x)$, nėra siurjekcija, nes, pavyzdžiui, funkcija $2\sin(x)$ neįgyja reikšmės $3 \in \mathbb{R}$, t. y. $3 \notin E(h) = [-2, 2]$. Atvaizdis $p : \mathbb{R} \to [-2, 2]$, $p(x) = 2\sin(x)$, yra siurjekcija, nes $[-2, 2] = E(p)$.

1.3.28 apibrėžimas (bijekcinis atvaizdis (bijekcija))**.** Atvaizdis $f : A \to B$ vadinamas *bijekciniu atvaizdžiu* arba *bijekcija*, jei f yra injekcinis ir siurjekcinis atvaizdis.

1.3.29 pavyzdys. Atvaizdis $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3$, yra bijekcija, nes jis yra injekcinis ir siurjekcinis. Atvaizdis $g : \mathbb{R} \to [0, \infty]$, $g(x) = x^2$, nėra bijekcija, nes jis nėra injekcija. Atvaizdis $h : \mathbb{R} \to \mathbb{R}$, $h(x) = 2\sin(x)$, nėra bijekcija, nes jis nėra siurjekcija.

Pratimai.
Sakykime, kad $f : A \to B$, $g : B \to C$ yra atvaizdžiai. Įrodykite šiuos teiginius:

1. Jei f ir g yra injekciniai atvaizdžiai, tai ir $g \circ f$ yra injekcinis atvaizdis.
2. Jei f ir g yra siurjekciniai atvaizdžiai, tai ir $g \circ f$ yra siurjekcinis atvaizdis.
3. Jei $g \circ f$ yra injekcinis atvaizdis, tai ir atvaizdis f yra injekcinis. Pateikite pavyzdį, kad $g \circ f$ būtų injekcinis atvaizdis, bet atvaizdis g nebūtų injekcinis.
4. Jei $g \circ f$ yra siurjekcinis atvaizdis, tai ir atvaizdis g yra siurjekcinis. Pateikite tokį pavyzdį, kad $g \circ f$ būtų siurjekcinis atvaizdis, bet atvaizdis f nebūtų siurjekcinis.
5. Jei $g \circ f$ yra injekcinis atvaizdis, f – siurjekcinis atvaizdis, tai atvaizdis f yra bijekcinis, o g – injekcinis atvaizdis.
6. Jei $g \circ f$ yra siurjekcinis atvaizdis, g – injekcinis atvaizdis, tai atvaizdis f yra siurjekcinis, o g – bijekcinis atvaizdis.

1.3.30 apibrėžimas (aibių ekvivalentumas)**.** Aibės A ir B yra vadinamos *ekvivalenčiomis*, jei egzistuoja bijekcija $f : A \to B$.

Pavyzdžiui, baigtinės aibės, turinčios tiek pat elemenų, yra ekvivalenčios. Baigtinės aibės A elementų skaičių žymėsime $|A|$.

Anksčiau sutarėme aibės A visų poaibių aibę žymėti $P(A)$ arba 2^A. Dabar pagrįsime žymėjimą 2^A.

1.3.31 teorema. *Aibės $P(A)$ ir $\{0,1\}^A$ yra ekvivalenčios (žr.* 1.3.17 *apibrėžimą).*

Įrodymas. Tarkime, kad $X \in P(A)$, t. y. $X \subset A$. Tuomet aibės A poaibiui X priskirkime atvaizdį $f_X : A \to \{0,1\}$,

$$f_X(a) = \begin{cases} 0 & \text{jei } a \in X, \\ 1 & \text{jei } a \notin X. \end{cases}$$

Taigi apibrėžėme atvaizdį:

$$F : P(A) \to \{0,1\}^A, \quad F(X) = f_X, \quad X \in P(A).$$

Įrodysime, kad F yra bijekcija.

Pirmiausia įsitikinsime, kad F yra injekcinis atvaizdis. Vadinasi, reikia įrodyti, kad, jei $X \neq Y$, tai ir $F(X) = f_X \neq f_Y = F(Y)$. Norint įrodyti, kad $f_X \neq f_Y$, reikia nurodyti bent vieną tokį aibės A elementą a, kad būtų $f_X(a) \neq f_Y(a)$. Tad sakykime, kad $X, Y \in P(A)$, $X \neq Y$. Kadangi $X \neq Y$, tai bent viena iš šių aibių yra netuščia. Tarkime, kad $X \neq \emptyset$. Jei $X \not\subset Y$, tai ezistuoja toks $a \in X$, kad $a \notin Y$. Šiuo atveju $F(X) = f_X \neq f_Y = F(Y)$, nes $f_X(a) = 0 \neq 1 = f_Y(a)$. Jei $X \subset Y$, tai egzistuoja toks $a \in Y$, kad $a \notin X$. Ir šiuo atveju $f_X(a) = 1 \neq 0 = f_Y(a)$, t. y. $F(X) = f_X \neq f_Y = F(Y)$. Taigi įrodėme, kad

$$F : P(A) \to \{0,1\}^A$$

yra injekcinis atvaizdis.

Dabar įsitikinsime, kad F yra siurjekcinis atvaizdis. Tam reikia įrodyti, jog bet kuriam $g \in \{0,1\}^A$ egzistuoja toks $X \in P(A)$, kad $F(X) = f_X = g$. Apibrėžkime X taip:

$$X = \{x \in A \mid g(x) = 0\}.$$

Akivaizdu, kad $f_X = g$. Taigi įrodėme, kad atvaizdis F yra siurjekcinis. □

Įrodysime dar vieną svarbią teoremą.

1.3.32 teorema. *Aibės A ir $P(A)$ nėra ekvivalenčios aibės.*

Įrodymas. Šią teoremą įrodysime vadinamuoju Kantoro įstrižainės metodu.

Tarkime, kad A ir $P(A)$ yra ekvivalenčios. Vadinasi, egzistuoja bijekcija $f : A \to P(A)$. Apibrėžkime aibę

$$X = \{x \in A \mid x \notin f(x)\}.$$

Taigi $X \subset A$, t. y. $X \in P(A)$, o $f^{-1}(X)$ yra aibės A elementas. Pažymėkime $a = f^{-1}(X)$. Išsiaiškinkime, ar $a \in X$, ar $a \notin X$. Jei $a \in X = f(a)$, tai, pagal aibės X apibrėžimą, gauname, kad $a \notin f(a) = X$. Jei $a \notin X$, tai vėl, remdamiesi aibės X apibrėžimu, gauname, kad $a \in X$. Vadinasi, prielaida, kad aibės A ir $P(A)$ yra ekvivalenčios, prieštaringa. □

Kantoro įstrižainės metodu įrodoma, kad natūraliųjų skaičių aibė $\mathbb{N}$ ir realiųjų skaičių intervalas (0, 1) nėra ekvivalenčios aibės. Kitaip tariant, realiųjų skaičių intervalas (0, 1) (vadinasi, ir visų realiųjų skaičių aibė) nėra skaiti aibė (aibė vadinama *skaičia*, jei ji ekvivalenti natūraliųjų skaičių aibei).

Pratimai.

Įrodykite šiuos teiginius:

1. Jei A ir B yra baigtinės aibės, tai $|A^B| = |A|^{|B|}$.

2. Jei A ir B yra baigtinės aibės, tai $|A \times B| = |A||B|$.

3. Aibės $(A^B)^C$ ir $A^{B\times C}$ yra ekvivalenčios.

Jei A, B, C yra baigtinės aibės, tai, remiantis pirmuoju ir antruoju pratimais, akivaizdu, kad $\left|(A^B)^C\right| = \left|A^{B\times C}\right|$. Šiuo atveju matome, kad aibės $(A^B)^C$ ir $A^{B\times C}$ yra ekvivalenčios. Bendruoju atveju pasinaudokite nurodymu: jei $f \in (A^B)^C$, tai kiekvienam $c \in C$, $f(c) \in A^B$, t. y. bet kuriems $c \in C$ ir $b \in B$, $(f(c))(b) \in A$. Tuomet atvaizdžiui f priskirkite atvaizdį $\tilde{f} \in A^{B\times C}$, apibrėžiamą lygybe: $\tilde{f}(b,c) = (f(c))(b)$. Įsitikinkite, kad atvaizdis

$$(A^B)^C \ni f \to \tilde{f} \in A^{B\times C}$$

yra bijekcija.

1.3.33 (aibė $\mathcal{A}utA$)**.** Visų bijekcijų $f : A \to A$ aibę žymėsime $\mathcal{A}utA$.

Pratimai.
Įrodykite tokius teiginius:

1. $f, g \in \mathcal{A}utA \Longrightarrow f \circ g \in \mathcal{A}utA$.

2. $\mathrm{id} \in \mathcal{A}utA$ (atvaizdis id apibrėžiamas taip: $\mathrm{id} : A \to A$, $\mathrm{id}(a) = a$, $a \in A$). Įsitikinkite, kad $f \circ \mathrm{id} = \mathrm{id} \circ f = f$, $f \in \mathcal{A}utA$.

3. $f \in \mathcal{A}utA \Longrightarrow f^{-1} \in \mathcal{A}utA$, $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}$.

1.4 Ekvivalentumo sąryšis. Faktoraibė

1.4.1 apibrėžimas (ekvivalentumo sąryšio apibrėžimas)**.** Aibės $A \times A$ poaibis R vadinamas *ekvivalentumo sąryšiu*, apibrėžtu aibėje A, jei

1. Kiekvienam $a \in A$, $(a, a) \in R$ (sąryšio R refleksyvumo savybė).

2. $(a, b) \in R \Longrightarrow (b, a) \in R$ (sąryšio R simetriškumo savybė).

3. $(a, b) \in R, (b, c) \in R \Longrightarrow (a, c) \in R$ (sąryšio R tranzityvumo savybė).

1.4.2 pastaba. Ekvivalentumo sąryšį R, apibrėžtą aibėje A, paprastumo dėlei vadinsime ekvivalentumo sąryšiu aibėje A.

Ekvivalentumo sąryšį $R \subset A \times A$ aibėje A galima apibrėžti ir taip:

1'. $\Delta(A) \subset R$, $\Delta(A) =: \{(a, a) \,|\, a \in A\}$ – aibės $A \times A$ poaibis, kuris yra vadinamas aibės $A \times A$ įstrižaine.

2'. $R = R^{-1}$ (žr. 1.3.4 apibrėžimą).

3'. $R \circ R \subset R$ (žr. 1.3.5 apibrėžimą).

Akivaizdu, kad $R \circ R = R$.

Aibės A elementai a ir b susiję ekvivalentumo sąryšiu R, jei $(a, b) \in R$. Elementai $a, b \in A$, susiję ekvivalentumo sąryšiu R, vadinami ekvivalenčiais ir vietoje žymėjimų aRb ar $(a, b) \in R$ yra naudojami tokie:

$$a \underset{R}{\sim} b \quad \text{arba} \quad a \equiv b \pmod{R}.$$

Šiais naujais žymėjimais ekvivalentumo sąryšio R aibėje A savybės užrašomos taip: bet kuriems $a, b, c \in A$

1''. $a \underset{R}{\sim} a$ arba $a \equiv a \pmod{R}$.

2''. $a \underset{R}{\sim} b \Longrightarrow b \underset{R}{\sim} a$ arba $a \equiv b \pmod{R} \Longrightarrow b \equiv a \pmod{R}$.

3''. $a \underset{R}{\sim} b, b \underset{R}{\sim} c \Longrightarrow a \underset{R}{\sim} c$ arba

$$a \equiv b \pmod{R},\ b \equiv c \pmod{R} \Longrightarrow a \equiv c \pmod{R}.$$

1.4.3 pastaba. Konkrečių ekvivalentumo sąryšių aibėse atvejais galimi ir kitokie žymėjimai.

Pavyzdžiai.

1. Tarkime, A – netuščia aibė, $R = \Delta(A)$ – aibės $A \times A$ įstrižainė. R yra ekvivalentumo sąryšis aibėje A ir

   $$a \underset{R}{\sim} b \Longleftrightarrow a = b.$$

   Tai vienas iš dviejų kraštutinių atvejų.

2. Tarkime, A – netuščia aibė, $R = A \times A$. R yra ekvivalentumo sąryšis aibėje A ir šiuo atveju bet kurie aibės A elementai yra ekvivalentūs. Tai kitas kraštutinis atvejis.

3. Tarkime, n – fiksuotas natūralusis skaičius, $n \geq 1$,

   $$R_n = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid n|(a - b)\}$$

   (jei sveikasis skaičius a dalija sveikąjį skaičių b, tai rašome $a|b$, jei a nedalija skaičiaus b, tai rašome $a \nmid b$). R_n yra ekvivalentumo sąryšis aibėje $\mathbb{Z}$, nes bet kuriems $a, b, c \in \mathbb{Z}$, R_n tenkina ekvivalentumo sąryšio apibrėžimo sąlygas:

1”. $a \underset{R_n}{\sim} a$, nes $n|(a-a)=0$.

2”. $a \underset{R_n}{\sim} b \Longrightarrow b \underset{R_n}{\sim} a$, nes, jei $n|(a-b)$, tai $n|(b-a)$.

3”. $a \underset{R_n}{\sim} b, b \underset{R_n}{\sim} c \Longrightarrow a \underset{R_n}{\sim} c$, nes, jei $n|(a-b)$ ir $n|(b-c)$, tai $n|(a-c)$ (kadangi $a-c=(a-b)+(b-c)$).

Ekvivalentumo sąryšio R_n aibėje $\mathbb{Z}$ atveju vietoje $a \underset{R_n}{\sim} b$ dažnai rašoma

$$a \equiv b \pmod{n}.$$

Šį žymėjimą naudojo Gausas.

4. Tarkime, A – plokštumos $\mathbb{R}^2$ visų tiesių aibė. Tegu

$$R=\{(a,b)\in A\times A \mid a||b\},$$

čia $a||b$ žymi, kad tiesės a ir b yra lygiagrečios. (Tiesės a ir b vadinamos lygiagrečiomis, jei $a=b$ arba a ir b neturi bendrų taškų.) Akivaizdu, kad R yra ekvivalentumo sąryšis aibėje A.

5. Tarkime, kad A – plokštumoje $\mathbb{R}^2$ visų trikampių aibė,

$$R=\{(a,b)\in A\times A \mid \text{ trikampių } a \text{ ir } b \text{ plotai lygūs}\}.$$

Tuomet R – ekvivalentumo sąryšis aibėje A.

6. Tarkime, kad A – plokštumoje $\mathbb{R}^2$ visų trikampių aibė,

$$R=\{(a,b)\in A\times A \mid a\sim b\},$$

čia $a\sim b$ žymi, kad trikampis a yra panašus į trikampį b. Akivaizdu, kad R yra ekvivalentumo sąryšis.

1.4.4 apibrėžimas (ekvivalentumo klasės apibrėžimas)**.** Tarkime, R yra ekvivalentumo sąryšis aibėje A. Elemento $a\in A$ *ekvivalentumo klase* R atžvilgiu vadinamas aibės A poaibis $\{x\in A \mid x \underset{R}{\sim} a\}$, sudarytas iš aibės A elementų, ekvivalenčių elementui a, ir žymimas $a \pmod{R}$.

Remdamiesi ekvivalentumo sąryšio apibrėžimu, gauname:

1. Jei $x,y\in a \pmod{R}$, tai x ir y yra ekvivalentūs. Matematinių simbolių žymėjimais šis teiginys yra užrašomas taip:

$$x,y\in a \pmod{R} \Longrightarrow x\equiv y \pmod{R}.$$

Iš tikrųjų, jei $x,y\in a \pmod{R}$, tai $x\equiv a \pmod{R}$, $y\equiv a \pmod{R}$, t. y. $x\equiv a \pmod{R}$, $a\equiv y \pmod{R}$. Taigi ir $x\equiv y \pmod{R}$.

2. Jei $x \equiv y \pmod R$ ir $y \in a \pmod R$, tai ir $x \in a \pmod R$. Matematinių simbolių žymėjimais šis teiginys užrašomas taip:

$$x \equiv y \pmod R, \;\; y \in a \pmod R \Longrightarrow x \in a \pmod R.$$

Dabar įrodysime vieną iš svarbiausių aibės A elementų ekvivalentuno klasių savybių.

1.4.5 teiginys. *Tarkime, R yra ekvivalentumo sąryšis aibėje A. Tuomet aibės A elementų a ir b ekvivalentumo klasės $a \pmod R$ ir $b \pmod R$ arba sutampa, arba neturi bendrų elementų.*

Įrodymas. Jei $a \pmod R \cap b \pmod R = \emptyset$, tai teiginys įrodytas. Tarkime, kad $c \in a \pmod R \cap b \pmod R$. Tuomet $c \in a \pmod R$, $c \in b \pmod R$. Remdamiesi 2-ąja ir 3-iąja ekvivalentumo sąryšio apibrėžimo savybėmis, gauname, kad $a \equiv b \pmod R$.

Jei $x \in a \pmod R$, tai $x \equiv a \pmod R$. Kadangi $a \equiv b \pmod R$, tai, remiantis 3-iąja ekvivalentumo sąryšio apibrėžimo savybe, galima parašyti $x \equiv b \pmod R$. Kaip matome, jei $x \in a \pmod R$, tai $x \in b \pmod R$. Taigi $a \pmod R \subset b \pmod R$. Panašiai įrodoma, kad $b \pmod R \subset a \pmod R$. Taigi, jei $a \pmod R \cap b \pmod R \neq \emptyset$, tai $a \pmod R = b \pmod R$. □

1.4.6 išvada. *Tarkime, R yra ekvivalentumo sąryšis aibėje A. Tuomet ekvivalentumo klasės $a \pmod R$ ir $b \pmod R$ sutampa tada ir tik tada, kai $a \equiv b \pmod R$.*

1.4.7 išvada. *Tarkime, R yra ekvivalentumo sąryšis aibėje A. Jei $x \in a \pmod R$, tai $x \pmod R = a \pmod R$.*

1.4.8. Jei R ekvivalentumo sąryšis aibėje A, tai skirtingos aibės A elementų ekvivalentumo klasės suskaido aibę A į netuščius, neturinčius bendrų elementų poaibius. Iš tikrųjų, kiekvienas aibės A elementas a patenka tik į vieną ekvivalentumo klasę $a \pmod R$, o skirtingos elementų ekvivalentumo klasės neturi bendrų elementų.

1.4.9 teiginys. *Kiekvienam netuščios aibės A skaidiniui netuščiais, neturinčiais bendrų elementų poaibiais egzistuoja toks ekvivalentumo sąryšis aibėje A, kad aibės A elementų ekvivalentumo klasės sutampa su aibės A skaidinio poaibiais.*

Įrodymas. Sakykime, kad $A = \bigcup\limits_{\alpha \in I} A_\alpha$ yra aibės A skaidinys netuščiais, neturinčiais bendrų elementų poaibiais A_α, $\alpha \in I$, t. y. kiekvienam $\alpha \in I$, $A_\alpha \neq \emptyset$ ir jei $\alpha \neq \beta$, $\alpha, \beta \in I$, tai $A_\alpha \cap A_\beta = \emptyset$. Apibrėžkime sąryšį R aibėje A taip: $a \underset{R}{\sim} b$ tada ir tik tada, kai egzistuoja toks $\alpha \in I$, kad $a, b \in A_\alpha$. Remdamiesi R apibrėžimu, matome:

1. Kiekvienam $a \in A$, $a \underset{R}{\sim} a$.

2. Jei $a \underset{R}{\sim} b$, tai $b \underset{R}{\sim} a$.

3. Jei $a \underset{R}{\sim} b$, $b \underset{R}{\sim} c$, tai $a \underset{R}{\sim} c$.

Taigi R yra ekvivalentumo sąryšis aibėje A. Be to, akivaizdu, kad aibės A elemento a ekvivalentumo klasė yra A_α, jei $a \in A_\alpha$. $\square$

1.4.10. Yra glaudus ryšys tarp ekvivalentumo sąryšių R aibėje A ir siurjekcijų $f : A \to B$.

Sakykime, kad $f : A \to B$ – siurjekcija. Tuomet $A = \bigcup\limits_{b \in B} f^{-1}(b)$ yra aibės A skaidinys netuščiais, neturinčiais bendrų elementų poaibiais. Toks skaidinys, kaip įrodėme (žr. 1.4.9), apibrėžia ekvivalentumo sąryšį aibėje A.

Sakykime, kad R – ekvivalentumo sąryšis aibėje A, $A = \bigcup\limits_{\alpha \in I} A_\alpha$ – aibės A skaidinys aibės A elementų ekvivalentumo klasėmis, t. y. kiekvienam $\alpha \in I$, $A_\alpha \neq \emptyset$ ir jei $\alpha \neq \beta$, $\alpha, \beta \in I$, tai $A_\alpha \cap A_\beta = \emptyset$, A_α, $\alpha \in I$ – aibės A elementų ekvivalentumo klasės. Tuomet atvaizdis $f : A \to B$, $B = \{A_\alpha \mid \alpha \in I\}$, $f(a) = A_\alpha$, jei $a \in A_\alpha$, yra siurjekcija.

1.4.11 apibrėžimas (faktoraibės apibrėžimas)**.** Tarkime, kad R – ekvivalentumo sąryšis aibėje A,

$$A = \bigcup_{\alpha \in I} A_\alpha$$

– aibės A skaidinys skirtingomis aibės A elementų ekvivalentumo klasėmis. Aibė $\{A_\alpha \mid \alpha \in I\}$, kurios elementai yra aibės A elementų ekvivalentumo klasės, vadinama aibės A *faktoraibe* pagal ekvivalentumo sąryšį R ir žymima A/R. Egzistuoja kanoninė siurjekcija $j : A \to A/R$, $j(a) = A_\alpha$, jei $a \in A_\alpha \subset A$, $\alpha \in I$, t. y. atvaizdis j kiekvienam aibės A elementui a priskiria jo ekvivalentumo klasę – faktoraibės A/R elementą A_α.

1.4.12 pavyzdys. Jei $A \neq \emptyset$, $R = \Delta(A) = \{(a, a) \mid a \in A\}$ – aibės $A \times A$ įstrižainė, tai $A/R = A$.

1.4.13 pavyzdys. Jei $A \neq \emptyset$, $R = A \times A$, tai $A/R = \{A\}$ – aibė, sudaryta iš vieno elemento A.

1.4.14 pavyzdys. Tegu $A = \mathbb{Z}$, $R_n = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid n|(a - b)\}$, n – sveikasis teigiamas skaičius, $n \geq 1$ (žr. 3 pratimą, p. 17). Tuomet aibės $\mathbb{Z}$ elemento i ekvivalentumo klasė yra

$$i + n\mathbb{Z} = \{i + nl \mid l \in \mathbb{Z}\}.$$

Gausas ekvivalentumo klasę $i+n\mathbb{Z}$ žymėjo $i \pmod n$. Priminsime, kad $i+n\mathbb{Z} = j+n\mathbb{Z}$ tada ir tik tada, kai $n|(i-j)$. Faktoraibė $\mathbb{Z}/R_n$ dar yra žymima $\mathbb{Z}_n$ arba $\mathbb{Z}/n\mathbb{Z}$. Taigi

$$\mathbb{Z}_n = \{n\mathbb{Z}, 1+n\mathbb{Z}, 2+n\mathbb{Z}, \ldots, n-1+n\mathbb{Z}\}.$$

1.4.15 pavyzdys. Apibrėžkime ekvivalentumo sąryšį R aibėje

$$\mathbb{R}^2 = \{(\alpha, \beta) \mid \alpha, \beta \in \mathbb{R}\}$$

taip:

$$(\alpha, \beta) \underset{R}{\sim} (\gamma, \delta) \text{ tada ir tik tada, kai } \alpha^2+\beta^2 = \gamma^2+\delta^2.$$

Aibės $\mathbb{R}^2$ elementų ekvivalentumo klasės yra plokštumos $\mathbb{R}^2$ apskritimai, kurių centrai koordinačių pradžioje $(0,0)$, ir taškas $(0,0)$. Faktoraibė A/R ekvivalenti aibei $\mathbb{R}_+ = \{\alpha \mid \alpha \geq 0\}$. Tai įrodoma taip: apibrėžiame siurjekciją $f : \mathbb{R}^2 \to \mathbb{R}_+$, $f((\alpha, \beta)) = \alpha^2 + \beta^2$. Tuomet $\mathbb{R}^2 = \bigcup\limits_{r \geq 0} f^{-1}(r)$, $f^{-1}(r)$ – spindulio $r \geq 0$ apskritimas, kurio centras yra taške $(0,0)$. Atvaizdis f generuoja bijekciją $\bar{f} : \mathbb{R}^2/R \to \mathbb{R}_+$, $\bar{f}(f^{-1}(r)) = r$, $r \geq 0$.

1.4.16. Tarkime, kad R – ekvivalentumo sąryšis aibėje A, $f : A \to B$ – toks atvaizdis, kad $f(a) = f(b)$, kai $a \pmod R = b \pmod R$. Tuomet egzistuoja toks atvaizdis $\bar{f} : A/R \to B$, kad diagrama

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "j"'] & & B \\ & A/R \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

yra komutatyvi, t. y. kiekvienam $a \in A$, $f(a) = (\bar{f} \circ j)(a)$. Iš tikrųjų, atvaizdį $\bar{f} : A/R \to B$ galima apibrėžti taip:

$$\bar{f}(a \pmod R) = f(a), \quad a \in A.$$

Įsitikinkite, kad atvaizdis $\bar{f}$ apibrėžtas korektiškai ir tenkina minėtą savybę.

1.5 Tvarkos sąryšiai. Sutvarkytosios aibės

1.5.1 apibrėžimas (tvarkos sąryšio apibrėžimas)**.** Sakykime, kad aibėje A apibrėžtas sąryšis R. Aibė A vadinama *sutvarkytąja*, jei

1. $(a,a) \in R$ (refleksyvumas).

2. (a,b), $(b,a) \in R \Longrightarrow a = b$ (antisimetriškumas).

3. $(a,b), (b,c) \in R \Longrightarrow (a,c) \in R$ (tranzityvumas).

Sąryšio R atžvilgiu sutvarkytoji aibė A žymima (A, R), o pats sąryšis R vadinamas *tvarka* aibėje A. Dažnai vietoje R rašoma $\leq$.

1.5.2 pavyzdys. Sakykime, A – netuščia aibė, $P(A)$ – aibės A visų poaibių aibė. Aibė $P(A)$ aibių įdėties sąryšio $\subset$ atžvilgiu yra sutvarkytoji aibė.

1.5.3 pavyzdys. Aibės $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sąryšio $\leq$ atžvilgiu yra sutvarkytosios aibės.

1.5.4 pavyzdys. Aibė $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ dalybos sąryšio $|$ ($a|b$ reiškia, kad b dalijasi iš a) atžvilgiu yra sutvarkytoji aibė.

1.5.5 pavyzdys. Aibė $\{a, b, c\}$ sąryšio $R = \{(a, a), (b, b), (c, c), (a, b), (a, c)\}$ atžvilgiu yra sutvarkytoji aibė.

1.5.6 pavyzdys. Aibė $\{a, b, c, d, e, f\}$ sąryšio

$$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (f, f), (a, c), (b, c), (c, d),$$

$$(c, e), (a, d), (a, e), (b, d), (b, e), (a, f), (b, f), (c, f), (d, f), (e, f)\}$$

atžvilgiu yra sutvarkytoji aibė. Pasitelkę ženklą „$\leq$“, tvarkos sąryšį R aibėje $\{a, b, c, d, e, f\}$ dar galime apibūdinti ir taip:

$$a \leq c \leq d \leq f, \quad b \leq c \leq e \leq f.$$

1.5.7 apibrėžimas. Sakykime, (A, R) – sutvarkytoji aibė. Aibės A elementai a ir b vadinami *palyginamais*, jei $(a, b) \in R$ arba $(b, a) \in R$.

Kaip žinome, jei $a \neq b$, tai tik vienas iš dviejų sutvarkytųjų dvejetų (a, b) ar (b, a) gali priklausyti R. Bendruoju atveju sutvarkytoje aibėje (A, R) gali būti nepalyginamų elementų. Pavyzdžiui, 1.5.4 pavyzdyje skaičiai 2 ir 3 nepalyginami, nes $2 \nmid 3$ (t. y. 2 nedalija 3) ir $3 \nmid 2$.

1.5.1 Tiesiškai ir visiškai sutvarkytosios aibės

1.5.8 apibrėžimas. Sutvarkytoji aibė (A, R) vadinama *tiesiškai sutvarkyta aibe*, jei bet kurie du aibės A elementai yra palyginami. Kitaip tariant, bet kuriems aibės A elementams a ir b, $(a, b) \in R$ arba $(b, a) \in R$.

1.5.9 pavyzdys. Sutvarkytosios aibės $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$ yra tiesiškai sutvarkytos aibės.

1.5.10 pavyzdys. Sutvarkytoji aibė $(P(A), \subset)$, čia A – netuščia aibė, nėra tiesiškai sutvarkyta aibė.

1.5.11 apibrėžimas. Sutvarkytosios aibės $(A, \leq)$ elementas a vadinamas *maksimaliuoju*, jei aibėje A nėra tokio elemento b, kad $b \neq a$ ir $a \leq b$. Panašiai apibrėžiamas sutvarkytosios aibės $(A, \leq)$ *minimalusis elementas*.

1.5.12 pavyzdys. Sutvarkytose aibėse $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$ nėra nė vieno maksimalaus ir nė vieno minimalaus elemento.

1.5.13 pavyzdys. Sutvarkytoje aibėje $(\mathbb{N}, \leq)$ yra minimalus elementas 0, bet nėra nė vieno maksimalaus elemento.

1.5.14 pavyzdys. Sutvarkytoje aibėje $(\{a, b, c\}, R)$,

$$R = \{(a, a), (b, b), (c, c), (a, b), (a, c)\},$$

egzistuoja du maksimalūs elementai b ir c ir vienas minimalus elementas a.

1.5.15 pavyzdys. Sutvarkytoje aibėje $(\{a, b, c, d, e\}, R)$,

$$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, c), (b, c),$$

$$(c, d), (c, e), (a, d), (a, e), (b, d), (b, e)\},$$

yra du maksimalūs elementai d ir e ir du minimalūs elementai a ir b.

1.5.16 pavyzdys. Sutvarkytoje aibėje $(\{a, b, c, d, e, f\}, R)$,

$$R = \{(a, a), (b, b), (c, c), (d, d), (e, e), (f, f), (a, c), (b, c), (c, d),$$

$$(c, e), (a, d), (a, e), (b, d), (b, e), (a, f), (b, f), (c, f), (d, f), (e, f)\},$$

yra vienas maksimalus elementas f ir du minimalūs elementai a ir b.

1.5.17 apibrėžimas. Sutvarkytosios aibės $(A, \leq)$ elementas a vadinamas *galiniu*, jei kiekvienam aibės elementui b, $b \leq a$.

Akivaizdu, kad sutvarkytosios aibės $(A, \leq)$ galinis elementas yra šios aibės vienintelis maksimalus elementas. Be to, jei tiesiškai sutvarkytoje aibėje egzistuoja maksimalus elementas, tai jis yra galinis šios aibės elementas.

1.5.18 apibrėžimas. Sutvarkytosios aibės $(A, \leq)$ elementas a vadinamas *pradiniu*, jei kiekvienam aibės elementui b, $a \leq b$.

Akivaizdu, kad sutvarkytosios aibės $(A, \leq)$ pradinis elementas yra šios aibės vienintelis minimalus elementas. Kita vertus, jei tiesiškai sutvarkytoje aibėje egzistuoja minimalus elementas, tai jis yra pradinis šios aibės elementas.

1.5.19 apibrėžimas. Sutvarkytosios aibės $(A, \leq)$ poaibis B vadinamas *aprėžtu iš viršaus*, jei egzistuoja toks aibės A elementas a, kad kiekvienam poaibio B elementui b, $b \leq a$. Panašiai galima suformuluoti *aprėžto iš apačios* poaibio apibrėžimą.

1.5.20 apibrėžimas. Tiesiškai sutvarkyta aibė $(A, \leq)$ vadinama *visiškai sutvarkyta*, jei kiekviename šios aibės netuščiame poaibyje indukuotos tvarkos atžvilgiu egzistuoja minimalusis elementas.

1.5.21 pavyzdys. Natūraliųjų skaičių aibė $(\mathbb{N}, \leq)$ įprastos tvarkos $\leq$ atžvilgiu yra visiškai sutvarkyta aibė. Kita vertus, sveikųjų skaičių aibė $(\mathbb{Z}, \leq)$ įprastos tvarkos $\leq$ atžvilgiu nėra visiškai sutvarkyta.

Suformuluosime aibių teorijoje svarbią aksiomą, vadinamą *ėmimo*, *parinkimo* arba *Cermelo aksioma*, taip pat *Cermelo teoremą* ir *Corno lemą*.

1.5.22 (Cermelo aksioma)**.** Sakykime, $\{X_\alpha\}_{\alpha \in I}$ – netuščių aibių šeima, kurios aibės su skirtingais indeksais neturi bendrų elementų. Tuomet egzistuoja tokia aibė A, kuri su kiekviena aibe X_α turi vieną ir tik vieną bendrą elementą.

Ši Cermelo aksioma ekvivalenti ir kitaip formuluojamam teiginiui.

1.5.23 teorema. *Tegu $\{X_\alpha\}_{\alpha \in I}$ – netuščių aibių šeima. Tuomet šios aibių šeimos sandauga $\prod\limits_{\alpha \in I} X_\alpha$ – netuščia aibė.*

Cermelo aksioma taip pat ekvivalenti vadinamajai „visiškos tvarkos“ teoremai.

1.5.24 teorema (visiškos tvarkos teorema (Cermelo teorema))**.** *Kiekvienoje netuščioje aibėje A galima apibrėžti tvarką R, kurios atžvilgiu A yra visiškai sutvarkyta aibė.*

Pratimas. Racionaliųjų skaičių aibėje $\mathbb{Q}$ apibrėžkite tvarką, kurios atžvilgiu ši aibė būtų visiškai sutvarkyta.

1.5.25 teorema (Corno lema)**.** *Tarkime, $(A, \leq)$ – sutvarkytoji aibė. Jei kiekvienas aibės A indukuotos tvarkos atžvilgiu tiesiškai sutvarkytas poaibis yra aprėžtas iš viršaus, tai aibėje A egzistuoja bent vienas maksimalus elementas.*

Analogiškai Corno lemoje sąlygą galima performuluoti taip, kad sutvarkytoje aibėje $(A, \leq)$ egzistuoja bent vienas minimalus elementas.

Cermelo aksioma sukėlė daug diskusijų ir konstruktyviosios matematikos atstovams yra nepriimtina. Bet be Cermelo aksiomos nebūtų galima įrodyti daug svarbių matematinės analizės faktų.

Cermelo aksioma, Cermelo teorema, suformuluotoji teorema apie netuščių aibių šeimos sankirtą (1.5.23 teorema) ir Corno lema Cermelo-Frenkelio aibių teorijos sistemoje yra ekvivalentūs teiginiai. Vieną šių teiginių pasirinkę kaip aksiomą, kitus tris teiginius galėtume įrodyti kaip teoremas. Algebroje egzistencijos teoremoms įrodyti patogiausia remtis Corno lema. Nagrinėdami žiedus pasitelkę Corno lemą įrodysime, kad kiekviename komutatyviame žiede su vienetu egzistuoja maksimalus idealas (o kiekvienas maksimalus idealas yra pirminis).

Taip pat, remdamiesi Corno lema, įrodysime, kad kiekvienoje tiesinėje erdvėje virš kūno k egzistuoja bazė ir kiekvienam tiesinės erdvės tiesiniam poerdviui egzistuoja bent vienas papildomas tiesinis poerdvis. Remiantis Corno lema, funkcinėje analizėje įrodoma svarbi Hano-Banacho teorema apie pusnormės, apibrėžtos normuotos erdvės tiesiniame poerdvyje, pratęsimą į visą erdvę. Labai sunku būtų išvardyti visus svarbius faktus, kurie įrodomi remiantis Corno lema.

1.5.2 Kryptinės aibės

1.5.26 apibrėžimas. Sutvarkytoji aibė $(A, \leq)$ yra vadinama *kryptine, kurios kryptis į dešinę*, jei bet kuriems aibės A elementams a ir b egzistuoja toks aibės A elementas c, kad $a \leq c$, $b \leq c$.

Analogiškai galima apibrėžti *kryptinės aibės, kurių kryptis į kairę*, sąvoką.

1.5.27 pavyzdys. Sutvarkytoji aibė $(A, \leq)$, kurioje egzistuoja galinis elementas, yra kryptinė aibė, kurios kryptis į dešinę.

1.5.28 pavyzdys. Sutvarkytosios aibės $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$ yra kryptinės aibės, kurių kryptis – tiek į dešinę, tiek į kairę.

1.5.29 pavyzdys. Sutvarkytoji aibė $(P(A), \subset)$ yra kryptinė aibė, kurios kryptis – tiek į dešinę, tiek į kairę.

1.5.30 pavyzdys. $I = [0, 1]$ – uždaras intervalas. Parinkę šio intervalo taškus

$$0 = x_0 < x_1 < x_2 < \cdots < x_n = 1,$$

gauname intervalo $[0, 1]$ baigtinį skaidinį

$$[0, 1] = \bigcup_{j=1}^{n} [x_{j-1} x_j],$$

kurį sutarkime žymėti $a = (I, \{x_0, x_1, \ldots, x_n\})$. Nagrinėkime intervalo I visų baigtinių skaidinių aibę A ir joje apibrėžkime tvarkos sąryšį taip: jei

$$a = (I, \{x_0, x_1, \ldots, x_r\}),\ b = (I, \{y_0, y_1, \ldots, y_s\}),\ r, s \in \mathbb{N},$$

tai

$$a \leq b \Longleftrightarrow \{x_0, x_1, \ldots, x_r\} \subset \{y_0, y_1, \ldots, y_s\}.$$

Nesunku įsitikinti, kad $(A, \leq)$ kryptinė aibė, kurios kryptis į dešinę. Ši skaidinių aibė svarbi apibrėžiant Rymano integralą.

Kryptinės aibės svarbios apibrėžiant grupių, žiedų, modulių virš žiedų šeimų injekcines ir projekcines ribas.

1.5.3 Sutvarkytųjų aibių tipas

1.5.31 apibrėžimas. Sakykime, $(A, \leq)$ ir $(B, \leq)$ – sutvarkytosios aibės. Atvaizdis $f : A \to B$ yra vadinamas *monotoniniu*, jei bet kuriems $a_1, a_2 \in A$, $a_1 \leq a_2$, $f(a_1) \leq f(a_2)$.

1.5.32 teiginys. *Jei $(A, \leq)$, $(B, \leq)$ ir $(C, \leq)$ – sutvarkytosios aibės, $f : A \to B$ ir $g : B \to C$ – monotoniniai atvaizdžiai, tai $g \circ f : A \to C$ yra monotoninis atvaizdis.*

Įrodymas. Šį teiginį įrodyti paliekame skaitytojui. □

1.5.33 apibrėžimas. Sutvarkytosios aibės $(A, \leq)$ ir $(B, \leq)$ vadinamos *to paties tipo*, jei egzistuoja monotoninė bijekcija $f : A \to B$, kurios atvirkštinis atvaizdis f^{-1} taip pat monotoninis.

1.5.34 pavyzdys. Sutvarkytosios aibės $(\mathbb{R}_+^*, \leq)$ ir $(\mathbb{R}, \leq)$ yra to paties tipo. Iš tikrųjų, $\ln : \mathbb{R}_+^* \to \mathbb{R}$ – bijekcija ir bet kuriems $a, b \in \mathbb{R}_+^*$, $a \leq b$ tada ir tik tada, kai $\ln a \leq \ln b$.

1.5.35 pavyzdys. Sutvarkytosios aibės $(\mathbb{Q}_+^*, \leq)$ ir $(\mathbb{Q}, \leq)$ yra to paties tipo. Iš tikrųjų, apibrėžkime atvaizdį $f : \mathbb{Q}_+^* \to \mathbb{Q}$ taip:

$$f(x) = \begin{cases} x - 1, & \text{jei } x \geq 1, \\ -\frac{1}{x} + 1, & \text{jei } 0 < x \leq 1 \end{cases}.$$

Tuomet f – bijekcija. Be to, atvaizdžiai f ir f^{-1} yra monotoniniai.

1.5.36 pavyzdys. Sutvarkytosios aibės $((-\frac{\pi}{2}, \frac{\pi}{2}), \leq)$ ir $(\mathbb{R}, \leq)$ yra to paties tipo: funkcija $\operatorname{tg} : (-\frac{\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$ yra bijekcija ir bet kuriems $x, y \in (-\frac{\pi}{2}, \frac{\pi}{2})$, $\operatorname{tg} x \leq \operatorname{tg} y$ tada ir tik tada, kai $x \leq y$.

1.5.37 pavyzdys. Sutvarkytosios aibės $(-\mathbb{N}, \leq)$ ir $(\mathbb{N}, \leq)$, čia

$$-\mathbb{N} = \{-n \mid n \in \mathbb{N}\},$$

nėra to paties tipo, nes sutvarkytoje aibėje $-\mathbb{N}$ egzistuoja galinis elementas, o sutvarkytoje aibėje $\mathbb{N}$ tokio elemento nėra.

1.5.38 apibrėžimas. Tarkime, $(A, \leq)$ – sutvarkytoji aibė. Bijekcija $f : A \to A$ vadinama sutvarkytosios aibės $(A, \leq)$ *automorfizmu*, jei f ir f^{-1} – monotoniniai atvaizdžiai. Sutvarkytosios aibės $(A, \leq)$ visų automorfizmų aibę žymėsime

$$\mathcal{A}ut(A, \leq).$$

Aibėje $\mathcal{A}ut(A, \leq)$ apibrėžtas atvaizdžių kompozicijos dėsnis $\circ$, kuris tenkina šias sąlygas:

1) $\circ$ – asociatyvus kompozicijos dėsnis;

2) $\mathrm{id} \in \mathcal{A}ut(A, \leq)$;

3) $f \in \mathcal{A}ut(A, \leq) \Longrightarrow f^{-1} \in \mathcal{A}ut(A, \leq)$.

Aibė $\mathcal{A}ut(A, \leq)$ kompozicijos dėsnio $\circ$, tenkinančio išvardytas sąlygas, atžvilgiu yra vadinama grupe. Kitaip tariant, sutvarkytosios aibės automorfizmas – tai tos aibės simetrija. Vėliau (5 skyriuje) grupes nagrinėsime išsamiau.

1.6 Cermelo-Frenkelio aibių teorijos aksiomatika

Aibių teorijos Cermelo-Frenkelio Z F aksiomų sistemos sąrašą galite rasti sudarytą įvairiai. Pateiksime kelias šių aksiomų sistemos versijas.

Cermelo-Frenkelio aibių teorijos Z F sistema gali būti aprašoma štai taip. Ši sistema yra sudaryta iš kintamųjų $x, y, \ldots$, kuriais žymimos aibės, ir pirmykščio predikato $\in$, reiškiančio priklausomumo sąryšį („priklauso“). Atomarinės formulės turi pavidalą: $x \in y$. Iš atomarinių formulių naudojant elementariosios logikos jungtis: $\Longrightarrow$ – implikaciją („jei $\ldots$, tai $\ldots$“), $\neg$ – neigimą („ne“), $\vee$ – disjunkciją („arba“), $\wedge$ – konjunkciją („ir“) ir kvantorius: $\forall$ – bendrumo kvantorių („kiekvienam“), $\exists$ – egzistavimo kvantorių („egzistuoja“), sudaromos kitos formulės ir teiginiai. Matematinėje logikoje užrašas „$\equiv$“ žymi ekvivalentumą („jei, $\ldots$, tai $\ldots$ ir atvirkščiai“). Be to, priimamos elementariosios logikos aksiomos bei išvedimo taisyklės. Aibių teorijos Z F sistemos aksiomos yra šios:

Z F 1. *Aibių lygumo aksioma.* Šia aksioma teigiama, kad dvi aibės yra lygios, jei jos sudarytos iš tų pačių elementų. Lygybės ženklas $=$ pakeičia užrašą $(\forall z)(z \in x \equiv z \in y)$. Aksioma simbolių kalba užrašoma taip:

$$x = y \Longrightarrow (\forall w)(x \in w \Longrightarrow y \in w).$$

Z F 2. *Sąjungos arba poros aksioma.* Jei x ir y – aibės, tai $\{x, y\}$ taip pat yra aibė, t. y.

$$(\exists w)(\forall z)(z \in w \equiv (z = x \vee z = y)).$$

Z F 3. *Išskyrimo aksioma.* Kiekvienai aibei z ir kiekvienai Z F sistemos formulei $F(x)$ egzistuoja aibės z poaibis, kuriam priklauso tos ir tik tos aibės x, kurioms teisinga formulė $F(x)$. Simbolių kalba aksioma užrašoma taip:

$$(\forall z)(\exists y)(\forall x)(x \in y \equiv (x \in z \wedge F(x))),$$

čia y neįeina į $F(x)$. Remiantis šia aksioma galima įrodyti tuščiosios aibės $\emptyset$ egzistavimą, jei egzistuoja bent viena aibė. Iš tikrųjų, tegu z yra aibė, o sistemos Z F formulė $F(x) = (x \in x) \wedge \neg(x \in x)$. Tuomet tuščioji aibė $\emptyset$, remiantis išskyrimo aksioma, apibrėžiama kaip aibės z poaibis

$$\emptyset = \{x \in z \mid (x \in x) \wedge \neg(x \in x)\}.$$

Z F 4. *Poaibių aibės arba laipsnio aksioma.* Kiekvienai aibei egzistuoja jos poaibių aibė:

$$(\forall z)(\exists y)(\forall x)\big(x \in y \equiv (\forall w)(w \in x \Longrightarrow w \in z)\big).$$

Z F 5. *Sumos aksioma.* Kiekvienai aibei egzistuoja aibė-suma:

$$(\forall z)(\exists y)(\forall x)\big(x \in y \equiv (\exists w)(x \in w \wedge w \in z)\big).$$

Z F 6. *Cermelo arba parinkimo aksioma.* Ši aksioma dar yra vadinama sandaugos aksioma. Jei x – aibė, kurios elementai netuščios, neturinčios bendrų elementų aibės, tai jos aibė-suma turi bent vieną poaibį, kuris su kiekvienu x elementu turi tik vieną bendrą elementą:

$$(\forall x)\Big((\forall y)(\forall z)\big((y \in x \wedge z \in x) \Longrightarrow$$

$$\Longrightarrow \big((\exists w)w \in y \wedge \neg(\exists w)(w \in y \wedge w \in z)\big)\big) \Longrightarrow$$

$$\Longrightarrow (\exists u)(\forall y)(y \in x \Longrightarrow (\exists v)(\forall t)\big(t = v \equiv (t \in u \wedge t \in y)\big))\Big).$$

Z F 7. *Begalybės aksioma.* Egzistuoja aibė, kuriai priklauso tuščioji aibė ir kurios kiekvienam elementui x aibė $\{x\}$, sudaryta iš vieno elemento, taip pat priklauso jai. Simbolių kalba aksioma atrodo taip:

$$(\exists z)\big(\emptyset \in z \wedge (\forall x)(x \in z \Longrightarrow \{x\} \in z)\big).$$

Z F 8. *Apribojimo aksioma.* Kiekvienai tokiai Z F sistemos formulei $F(x)$, kad $(\exists x)F(x)$, egzistuoja tokia aibė y, kad $F(y)$ teisinga, bet nė vienam jos elementui z formulė $F(z)$ nėra teisinga. Simbolių kalba:

$$(\exists x)F(x) \Longrightarrow (\exists y)(F(y) \wedge (\forall z)\neg\big(z \in y \wedge F(z)\big)).$$

.

Z F 9. *Pakeitimo aksioma.* Jei tarp dviejų klasių yra abipus vienareikšmė atitiktis ir viena šių klasių yra aibė, tai ir kita klasė yra aibė. Simbolių kalba:

$$(\forall x)(\forall y)(\forall w)(\big(F(x,y) \wedge F(z,w)\big) \Longrightarrow \big((x = z) \equiv (y = w)\big)).$$

Dabar pateiksime kitą Cermelo-Frenkelio Z F aksiomų sistemos apibrėžimą.

Z F 1'. *Aibių lygumo aksioma (apimties aksioma).* Šia aksioma teigiama, kad dvi aibės yra lygios, jei jos sudarytos iš tų pačių elementų. Lygybės ženklas $=$ pakeičia užrašą $(\forall z)(z \in x \equiv z \in y)$. Aksioma simbolių kalba užrašoma taip:

$$(\forall x)(x \in y \equiv x \in z) \Longrightarrow (y = z).$$

Z F 2'. *Tuščios aibės egzistavimo aksioma.* Aksioma simbolių kalba užrašoma taip:

$$\exists y \forall x (x \notin y).$$

Tuščia aibė yra žymima $\emptyset$.

Z F 3'. *Sąjungos arba poros aksioma.* Jei x ir y – aibės, tai $\{x, y\}$ taip pat yra aibė, t. y.

$$(\exists w)(\forall z)(z \in w \equiv (z = x \vee z = y)).$$

Z F 4'. *Sumos aksioma.* Kiekvienai aibei egzistuoja aibė-suma:

$$(\exists z)(\forall x)(x \in z \equiv (\exists y)(y \in v)(x \in y)).$$

Z F 5'. *Aibės poaibių arba laipsnio aksioma.* Kiekvienai aibei egzistuoja jos poaibių aibė:

$$\exists z \forall x (x \in z \equiv (x \subseteq y)).$$

Z F 6'. *Begalybės aksioma.* Simbolių kalba aksioma atrodo taip:

$$\exists u \forall z (\forall x (x \notin z) \Longrightarrow z \in u) \wedge (\forall z \in u)$$

$$(\forall v (\forall x (x \in v \equiv (x \in z \vee x = z)) \Longrightarrow v \in u)).$$

Z F 7'. *Išskyrimo aksioma.* Kiekvienai aibei z ir kiekvienai Z F sistemos formulei $F(x)$ egzistuoja aibės z poaibis, kuriam priklauso tos ir tik tos aibės x, kurioms teisinga formulė $F(x)$. Simbolių kalba aksioma užrašoma taip:

$$\exists u \forall z (z \in u \equiv (z \in x \wedge F(z))),$$

čia į formulę $F(x)$ nėra laisvai įeinančio kintamojo u.

Z F 8'. *Pakeitimo aksioma.* Simbolių kalba:

$$\exists u \forall z (z \in u \equiv (\exists x \in v)(F(x,\ z) \wedge \forall w (F(x,\ w) \Longrightarrow z = w))),$$

čia į formulę $F(x,\ z)$ nėra laisvai įeinančių kintamųjų u ir v.

Z F 9'. *Cermelo arba parinkimo aksioma.* Ši aksioma dar yra vadinama sandaugos aksioma. Jei x – aibė, kurios elementai netuščios, neturinčios bendrų elementų aibės, tai jos aibė-suma turi bent vieną poaibį, kuris su kiekvienu x elementu turi tik vieną bendrą elementą:

$$\forall x, y \in u ((x \neq \emptyset) \wedge ((x \neq y) \Longrightarrow (x \cap y = \emptyset))) \Longrightarrow$$

$$\Longrightarrow \exists v \forall u \exists x \forall y((y \in v \cap x) \equiv (y = x)).$$

Kartais į aksiomų sąrašą įtraukiama dar viena aksioma – tai *reguliarumo aksioma.* Ji formuluojama taip:

$$\exists z(z \in x) \Longrightarrow (\exists z \in x) \neq \exists u(u \in z \wedge u \in x).$$

1.6.1 pastaba. Kartais į aksiomų sąrašą neįtraukiama parinkimo aksioma ir toks aksiomų sąrašas yra vadinamas Z F sistema, o įtraukus į sąrašą parinkimo aksiomą – Z F C sistema.

Šioje Z F aibių teorijos sistemoje galima įrodyti, kad egzistuoja vienintelė natūraliųjų skaičių aibė, tenkinanti Peano aksiomas. Paskui galima apibrėžti racionaliųjų skaičių aibę ir Dedekindo pjūviais – realiųjų skaičių aibę.

Bet ši Z F aibių teorijos sistemos kalba yra formali. Norint suteikti šiai kalbai prasmę, būtina nagrinėti šios aksiomų sistemos interpretaciją. Pirmiausia, pasirodo, kad ši aksiomų sistema turi be galo daug interpretacijų. Kita vertus, egzistuoja tokios interpretacijos, kuriose natūraliųjų skaičių aibės, žiūrint iš išorės, nėra ekvivalenčios tarpusavyje ir nėra ekvivalenčios intuityviai suvokiamai natūraliųjų skaičių aibei. Taigi susidarė nepaprastai įdomi situacija. Kol kas nėra žinoma nė viena aibių teorijos aksiomų sistema, kuri turėtų vienintelę interpretaciją ir kuri būtų tiek galinga, kad jos terminais būtų galima suformuluoti šiuolaikinės matematikos teorijas.

1.7 Trumpa aibių teorijos raidos apžvalga

Kantoras, tyrinėdamas trigonometrines eilutes, 1872 m. pabandė klasifikuoti trigonometrinių eilučių teorijoje nagrinėjamas „ypatingas“ aibes. Pradėjęs taip tyrinėti aibes, Kantoras 1872–1897 m. sukūrė aibių teoriją.

Paprastomis aibių teorijos sąvokomis, kaip antai elemento priklausomumas visumai (aibei), visumos dalis, visumos dalių bendra dalis ir kitomis, matematikai ir filosofai visais laikais naudojosi sąmoningai. Šios sąvokos suvokiamos intuityviai ir dėl jų nebuvo diskutuojama. Todėl nesukėlė jokių diskusijų ir aibės apibrėžimas, kurį pateikė Kantoras: aibę suprasime kaip objektų, kuriuos vieną nuo kito gerai galime atskirti savo intuicija arba mintimis, sujungimą į vieną visumą.

Nepaprastai svarbus Kantoro atradimas – tai visiškai sutvarkytosios aibės. Remdamasis visiškai sutvarkytųjų aibių teorija, jis išplėtojo kardinaliųjų skaičių aritmetiką, suformulavo transfiničiosios indukcijos principą (tai matematinės indukcijos principo apibendrinimas) ir kontinuumo hipotezę. Be to, Kantoras yra bendrosios topologijos ir mato teorijos pradininkas. Visi šie atradimai, dėl kurių Kantoras vadinamas aibių teorijos kūrėju, matematikoje pasirodė pirmą kartą.

Kantoro kurta aibių teorija to laiko matematikos požiūriu atrodė labai keistai. Nors įrodymai ir griežti, rezultatai neįtikėtini ir keisti. Iki tol matematikoje nieko panašaus nebuvo. Todėl daugelis žymių to laiko matematikų aibių teorijos nepripažino. Ypač aštriai šią teoriją kritikavo Kronekeris. Tik Veijerštrasas gana palankiai vertino savo mokinio veiklą. Bet palaipsniui aibių teorija buvo pradėta taikyti daugelyje matematikos sričių, XIX a. pabaigoje buvo panaudotas transfiničiosios indukcijos principas, o 1904 m. įrodžius Cermelo įžymiąją teoremą (kiekvienoje aibėje galima apibrėžti visiškai sutvarkytosios aibės struktūrą), transfiničiosios indukcijos principas tapo svarbus visose šiuolaikinės matematikos srityse.

Kai aibių teorija tapo šiuolaikinės matematikos pagrindu, joje buvo aptikti paradoksai, kurie sukrėtė šiuos pagrindus.

Štai Bertrano Raselo paradoksas, paprasčiausias iš žinomų paradoksų: pažymėkime C visų aibių, kurios nėra savo pačios elementas, visumą. Tarę, kad C yra aibė, pabandykime išsiaiškinti, ar C yra C elementas, ar ne? Jei C yra C elementas, tai C nepriklauso C pagal C apibrėžimą. Jei C nėra C elementas, tai C priklauso C pagal C apibrėžimą. Kaip matome, iš tikrųjų paprastas paradoksas.

Šis paradoksas rodo, kad aibės apibrėžimas, pagrįstas intuicija, nėra korektiškas, o intuicija besąlygiškai pasitikėti negalima. Jau Bolcanas ir Veijerštrasas anksčiau buvo sukonstravę tolydžių funkcijų, nediferencijuojamų nė viename taške, pavyzdžių, rodančių, kad, remiantis vien tik intuicija, galima labai klysti. Taigi aibių teoriją reikėjo peržiūrėti ir griežtai pagrįsti.

Matematikai, norėdami išvengti paradoksų ir išsaugoti Kantoro aibių teorijos laimėjimus, stengėsi aibių teoriją pagrįsti aksiomatiškai. Taip buvo sukurtos įvairios aibių teorijos sistemos: Raselo tipų teorija (1908 m.), Cermelo (1908 m.), Cermelo-Frenkelio (1922 m.), Noimano-Bernaiso (1925, 1937, 1941–1943 m.), Bernaiso-Giodelio (1940 m.) sistemos, Kuaino „Naujieji pagrindai“. Labiausiai pritaikytos šiuolaikinės matematikos tikslams – tai Cermelo-Frenkelio ir Bernaiso-Giodelio aibių teorijų sistemos.

Kuriant matematinę teoriją aksiomatiškai, iškyla vienas svarbiausių klausimų: kaip įrodyti, kad aksiomatiškai grindžiama teorija yra neprieštaringa? Į šį klausimą atsakymas yra žinomas, jei kalbama ne apie aibių, o apie kurią nors kitą matematinę teoriją, grindžiamą aksiomatiškai. Norint įrodyti aksiomatiškai grindžiamos teorijos neprieštaringumą, reikia sukurti matematinį modelį, tenkinantį tam tikrą aksiomų sistemą. Matematinių modelių, tenkinančių tokias aksiomų sistemas, konstravimas, kiek yra žinoma, atliekamas aibių teorijos terminais. Aibių teorijos, grindžiamos aksiomų sistema, neprieštaringumui įrodyti minėtas būdas netinka. Jei pabandytume taip išspręsti aibių teorijos, grindžiamos aksiomatiškai, neprieštaringumą, patektume į užburtą ratą: aibių teorijos terminais konstruotume modelį aibių teorijos neprieštaringumui įrodyti.

Hilbertas pasiūlė programą šiam sunkiam klausimui išspręsti. Aibių ir kitų matematinių teorijų semantika nepaprastai sudėtinga. Jis pasiūlė formalizuoti aksiomatiškai kuriamą teoriją, t. y. atsisakyti aiškinti matematinių simbolių, naudojamų aksiomų sistemoje, prasmę, o jų savybes grįsti tik aksiomomis ir apibrėžti taisykles, kaip jais operuoti. Remiantis logikos išvedimo taisyklėmis ir aksiomomis, formaliai įrodytos teoremos turi prasmę bet kurioje aksiomatizuotos teorijos interpretacijoje. Hilbertas tikėjosi, kad, tuo keliu eidamas, įrodys aibių teorijos neprieštaringumą. Jis ir Bernaisas atkakliai ėmėsi įgyvendinti šią programą. Jo ir jo mokinio Bernaiso tyrimų, vykdant šią programą, rezultatai paskelbti jų fundamentiniame dviejų tomų veikale „Įrodymų teorija“.

Bet tikslo jie nepasiekė. 1934 m. Giodeliui įrodžius metamatematikos teoremą tapo aišku, kad Hilberto programa neįgyvendinama. Giodelio teorema teigia, kad kiekvienoje teorijoje, grindžiamoje pakankamai „galinga“formalia aksiomų sistema, galima suformuluoti teiginį (šios teorijos terminais), kurio šios teorijos terminais negalima nei įrodyti, nei paneigti.

Savaime suprantama, kad aibių teorijoje, taip pat visoje matematikoje susidarė gana įdomi situacija. Be to, aibių teorijos, grindžiamos formalia aksiomų sistema, yra be galo daug interpretacijų. Kol kas nėra žinoma nė viena aibių teorijos aksiomų sistema, kuri turėtų vienintelę interpretaciją ir būtų tiek galinga, kad joje būtų galima suformuluoti visas žinomas šiuolaikinės matematikos teorijas.

2 skyrius

Kompozicijos dėsniai

2.1 Vidiniai kompozicijos dėsniai

Viena pagrindinių sąvokų, norint apibrėžti algebrines struktūras aibėse, yra kompozicijos dėsnio sąvoka. Apibrėžiami dviejų tipų kompozicijos dėsniai: vidiniai ir išoriniai. Dabar nagrinėsime tik vidinius kompozicijos dėsnius, kurie dažnai dar yra vadinami ir binariosiomis operacijomis. Vidinius kompozicijos dėsnius paprastumo dėlei vadinsime kompozicijos dėsniais. Vėliau nagrinėsime ir išorinius kompozicijos dėsnius.

2.1.1 apibrėžimas. Atvaizdis $f : X \times X \to X$ yra vadinamas aibės X elementų *kompozicijos dėsniu* (*binariąja operacija*), apibrėžtu (apibrėžta) aibėje X. Elementas $f(x_1, x_2) \in X$ yra vadinamas aibės X elementų x_1, x_2 kompozicija, o x_1, x_2 – komponuojamaisiais elementais.

2.1.2 pastaba. Yra nagrinėjami ir iš dalies apibrėžti kompozicijos dėsniai, t. y., kai atvaizdžio f apibrėžimo sritis yra aibės $X \times X$ poaibis. Pavyzdžiui, atimtis $-$ natūraliųjų skaičių aibėje $\mathbb{N}$ iš dalies apibrėžta: atvaizdžio $- : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ apibrėžimo sritis yra $D(-) = \{(a, b) \mid \ a \geq b, \ a, b \in \mathbb{N}\}$. Mes iš dalies apibrėžtų kompozicijos dėsnių nenagrinėsime. Kompozicijos dėsnį f, apibrėžtą aibėje X, paprastumo dėlei vadinsime kompozicijos dėsniu aibėje X.

Jei f – komozicijos dėsnis aibėje X, tai kiekvienam sutvarkytam aibės X elementų dvejetui (x_1, x_2), remiantis f apibrėžimu, yra priskiriamas vienas ir tik vienas aibės X elementas $f(x_1, x_2)$. Pavyzdžiui, sudėtis $+$, daugyba $\cdot$ skaičių aibėse $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ yra kompozicijos dėsniai. Tik skaičių sudėties, daugybos atvejais vietoje $+(a, b)$, $\cdot(a, b)$ įprasta rašyti $a + b$, $a \cdot b$. Mes dažniausiai kompozicijos dėsnius žymėsime $+$, $\cdot$, $\circ$, $*$ ar dar kitokiais ženklais ir, kaip ir skaičių sudėties ir daugybos atvejais, rašysime juos tarp komponuojamųjų elementų: $x + y$, $x \cdot y$, $x*y$, $x \circ y$ ir t. t. (kai aišku, kokį kompozicijos dėsnį nagrinėjame, to dėsnio ženklą tarp komponuojamųjų elementų dažnai praleisime,). Kartais kompozicijos ženklą patogu rašyti ir prieš komponuojamųjų elementų porą: $\min(a, b)$, $\max(a, b)$ ir t. t. Aibę X su joje apibrėžtu kompozicijos dėsniu $*$ sutarkime žymėti $(X, *)$.

2.1.3 pavyzdys. Anksčiau minėjome, kad skaičių sudėtis $+$ ir skaičių daugyba $\cdot$ yra kompozicijos dėsniai aibėse $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$. Skaičių daugyba $\cdot$ yra kompozicijos dėsnis ir aibėse $\mathbb{Q}^* =: \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$.

2.1.4 pavyzdys. Tarkime, kad $X = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$. Atvaizdis

$$\min : X \times X \to X,\ \min(x, y) = \begin{cases} x, & \text{jei } x \leq y, \\ y, & \text{jei x>y}, \end{cases}$$

$x, y \in X$, yra kompozicijos dėsnis aibėje X. Atvaizdis

$$\max : X \times X \to X,\ \max = \begin{cases} x, & \text{jei } x \geq y, \\ y, & \text{jei } x < y, \end{cases}$$

$x, y \in X$, taip pat yra kompozicijos dėsnis aibėje X.

2.1.5 pavyzdys. Skaičių atimtis nėra kompozicijos dėsnis aibėje $\mathbb{N}$, bet yra kompozicijos dėsnis aibėse $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$.

2.1.6 pavyzdys. Apibrėžkime atvaizdį

$$\sqcup : \mathbb{N} \times \mathbb{N} \to \mathbb{N},\ (a, b) \mapsto a \sqcup b,\ a, b \in \mathbb{N},$$

$a \sqcup b$ – skaičių a ir b didžiausias bendrasis daliklis. $\sqcup$ yra kompozicijos dėsnis aibėje $\mathbb{N}$.

2.1.7 pavyzdys. Apibrėžkime atvaizdį

$$\sqcap : \mathbb{N} \times \mathbb{N} \to \mathbb{N},\ (a, b) \mapsto a \sqcap b,\ a, b \in \mathbb{N},$$

$a \sqcap b$ – skaičių a ir b mažiausias bendrasis kartotinis. $\sqcap$ yra kompozicijos dėsnis aibėje $\mathbb{N}$.

Štai keletas kompozicijos dėsnių, svarbių aibių teorijoje, pavyzdžių. Tarkime, kad X – aibė, $P(X)$ – aibės X visų poaibių aibė ($P(X)$ yra žymima ir 2^X).

2.1.8 pavyzdys. Aibių sudėtis (sąjunga) $\cup$ – kompozicijos dėsnis aibėje $P(X)$.

2.1.9 pavyzdys. Aibių daugyba (sankirta) $\cap$ – kompozicijos dėsnis aibėje $P(X)$.

2.1.10 pavyzdys. Aibių atimtis $\setminus$ – kompozicijos dėsnis aibėje $P(X)$.

2.1.11 pavyzdys. Aibių simetrinė atimtis $\ominus$ – kompozicijos dėsnis aibėje $P(X)$.

2.1.12 pavyzdys. Atvaizdžių kompozicija $\circ$ – kompozicijos dėsnis aibėje X^X, čia X^X – visų atvaizdžių $f : X \to X$ aibė.

2.1.13 pavyzdys. Pavyzdžiui, jei $X = \{a, b\}$, tai visus kompozicijos dėsnius aibėje X apibrėžkime lentelėmis.

$*_1$	a	b
a	a	a
b	a	a

$*_2$	a	b
a	b	a
b	a	a

$*_3$	a	b
a	a	b
b	a	a

$*_4$	a	b
a	a	a
b	b	a

$*_5$	a	b
a	a	a
b	a	b

$*_6$	a	b
a	b	b
b	a	a

$*_7$	a	b
a	b	a
b	b	a

$*_8$	a	b
a	a	b
b	b	a

$*_9$	a	b
a	b	a
b	a	b

$*_{10}$	a	b
a	a	a
b	b	b

$*_{11}$	a	b
a	a	b
b	a	b

$*_{12}$	a	b
a	a	b
b	b	b

$*_{13}$	a	b
a	b	a
b	b	b

$*_{14}$	a	b
a	b	b
b	b	a

$*_{15}$	a	b
a	b	b
b	a	b

$*_{16}$	a	b
a	b	b
b	b	b

Dar sykį atidžiai pažiūrėkime į 16-ą lentelių, kuriomis apibrėžiami kompozicijos dėsniai aibėje $X = \{a, b\}$. Pavyzdžiui, kompozicijos dėsniai $*_1$ ir $*_{16}$, $*_2$ ir $*_{14}$, $*_3$ ir $*_{15}$ ir t. t. tam tikra prasme mažai kuo skiriasi. Aibės X elementai a ir b yra lygiaverčiai ir, jei elementą a pažymėtume raide b, o b – raide a, tai lentelė, kuria yra apibrėžiamas $*_1$, apibrėžtų kompozicijos dėsnį $*_{16}$, o lentelė, kuri apibrėžia $*_{16}$, apibrėžtų kompozicijos dėsnį $*_1$ ir t. t.

Jei aibė X turi n elementų, tai galime sudaryti iš viso n^{n^2} lentelių, kuriomis yra apibrėžiami visi atvaizdžiai $f : X \times X \to X$, t. y. visi kompozicijos dėsniai aibėje X. Bet ne visi taip apibrėžti kompozicijos dėsniai yra iš esmės skirtingi.

Pateiksime apibrėžimą, kuriuo remiantis skirtingai apibrėžti kompozicijos dėsniai ir net skirtingose aibėse struktūriniu požiūriu yra tapatūs.

2.1.14 apibrėžimas (izomorfiniai kompozicijos dėsniai)**.** Aibė X su joje apibrėžtu kompozicijos dėsniu $*$ yra vadinama *izomorfine* aibei Y su joje apibrėžtu kompozicijos dėsniu $\circ$, jei egzistuoja tokia bijekcija $f : X \to Y$, kad bet kuriems $x_1, x_2 \in X$, $f(x_1 * x_2) = f(x_1) \circ f(x_2)$.

Bijekcija f vadinama *izomorfizmu* iš aibės $(X,*)$ į aibę $(Y,\circ)$. Jei $(X,*)$ yra izomorfinė $(Y,\circ)$, tai sutarkime žymėti $(X,*) \cong (Y,\circ)$. Tuo atveju, kai $X = Y$ ir $(X,*)$ yra izomorfinė $(X,\circ)$, paprastumo dėlei kompozicijos dėsnius $*$ ir $\circ$ vadinsime izomorfiniais.

Pavyzdžiui, anksčiau aibėje $\{a,b\}$ lentelėmis apibrėžti kompozicijos dėsniai $*_1$ ir $*_{16}$, $*_2$ ir $*_{14}$, $*_3$ir $*_{15}$ yra izomorfiniai.

Jei aibė X turi n elementų, tai, kaip minėjome, galima sudaryti iš viso n^{n^2} lentelių, apibrėžiančių visus kompozicijos dėsnius aibėje X. Akivaizdu, kad neizomorfinių kompozicijos dėsnių aibėje X yra mažiau nei n^{n^2}, bet kiek, nėra žinoma.

2.2 Asociatyvūs kompozicijos dėsniai

2.2.1. Reikėtų pasakyti, kad aibėje $(X,*)$, remiantis kompozicijos dėsnio apibrėžimu, galima sukomponuoti tik bet kuriuos du aibės X elementus. Norėdami apibrėžti trijų aibės X elementų x_1, x_2, x_3 kompoziciją, privalome nurodyti, kuria tvarka turi būti atliekami kompozicijos veiksmai. Pavyzdžiui, užrašas $x_1 * x_2 * x_3$ neturi prasmės. Užrašui $x_1 * x_2 * x_3$ galime suteikti prasmę, vienaip ar kitaip suskliaudę elementus: $(x_1 * x_2) * x_3$ ar $x_1 * (x_2 * x_3)$. Pavyzdžiui, pirmuoju atveju iš pradžių atliekame kompozicijos veiksmą $x_1 * x_2$ su elementais x_1, x_2, o paskui sukomponuojame elementus $x_1 * x_2$ ir x_3. Antruoju atveju iš pradžių atliekame kompozicijos veiksmą $x_2 * x_3$ su elementais x_2, x_3, o tada sukomponuojame elementus x_1 ir $x_2 * x_3$. Rezultatai, taip atlikus veiksmus, gali skirtis. Nagrinėkime, pavyzdžiui, atimtį $-$ sveikųjų skaičių aibėje $\mathbb{Z}$. Akivaizdu, kad $(5-3)-4 \neq 5-(3-4)$.

Kaip minėjome, užrašas $x_1*x_2*x_3$ neturi prasmės, jei skliausteliais nenurodyta, kokia tvarka turi būti atlikti kompozicijos veiksmai. Tuo labiau prasmės neturi užrašas $x_1*x_2*\cdots*x_n$. Norėdami apibrėžti n elementų $x_1, x_2, \ldots, x_n$ kompoziciją, tai galime padaryti reiškinyje $x_1 * x_2 * \cdots * x_n$ kuriuo nors būdu sudėlioję skliaustelius, pavyzdžiui,

$$\underbrace{((\ldots(}_{n-1} x_1 * x_2) * x_3) * \cdots * x_{n-1}) * x_n$$

ar

$$x_1 * (x_2 * (\cdots * (x_{n-1} * x_n \underbrace{))\ldots)}_{n-1},$$

ar dar kaip nors kitaip. Taigi nuo skliaustelių sudėliojimo tvarkos reiškinyje $x_1 * x_2 * \cdots * x_n$ priklauso n elementų, $n \geq 3$, kompozicijos apibrėžimas.

2.2.2 apibrėžimas. Kompozicijos dėsnis $*$ aibėje X yra vadinamas *asociatyviuoju*, jei bet kuriems x, y, $z \in X$,

$$(x * y) * z = x * (y * z).$$

Jei kompozicijos dėsnis $*$ aibėje X asociatyvus, tai bet kurių trijų elementų x, y, $z \in X$ kompozicija $x * y * z$ vienareikšmiškai apibrėžta ir nuo skliaustelių sudėliojimo tvarkos nepriklauso, t. y. skliausteliai nebūtini veiksmų tvarkai nurodyti. Kalbant apie aibės X n elementų x_1, x_2, $\dots$, x_n kompoziciją, kai $n > 3$, visiškai neakivaizdu, ar rezultatas priklauso nuo skliaustelių sudėliojimo tvarkos reiškinyje $x_1 * x_2 * \cdots * x_n$.

2.2.3 teorema. *Jei kompozicijos dėsnis $*$ aibėje X yra asociatyvusis, tai bet kurių n elementų x_1, x_2, $\dots$, $x_n \in X$, $n \geq 3$, kompozicija $x_1 * x_2 * \cdots * x_n$ vienareikšmiškai apibrėžta, t. y. nuo skliaustelių išdėstymo tvarkos reiškinyje $x_1 * x_2 * \cdots * x_n$ nepriklauso.*

Įrodymas. Teoremos teiginį įrodysime matematinės indukcijos metodu pagal komponuojamųjų elementų skaičių n. Kai $n = 3$, teoremos teiginys teisingas (tai asociatyvaus kompozicijos dėsnio apibrėžimas). Tarkime, kad teoremos teiginys yra teisingas, kai komponuojamųjų elementų yra mažiau nei n. Įrodysime, kad teoremos teiginys yra teisingas ir tuo atveju, kai komponuojamųjų elementų yra n.

Kuriuo nors būdu apibrėžiant n elementų x_1, x_2, $\dots$, x_n kompoziciją, skliausteliai reiškinyje $x_1 * x_2 * \cdots * x_n$ yra išdėstomi taip, kad kiekvieno žingsnio metu kompozicijos veiksmą galėtume atlikti tik su dviem gretimais suskliaustais elementais. Po kiekvieno žingsnio komponuojamųjų elementų skaičius sumažėja vienetu. Tarkime, kad pasirinkome kuriuos nors du skirtingus skliaustelių išdėstymo būdus reiškinyje $x_1 * x_2 * \cdots * x_n$ ir paskutinio žingsnio metu vienu ir kitu atveju kompozicijos veiksmai yra atliekami taip:

i) $(x_1 * \cdots * x_i) * (x_{i+1} * \cdots * x_n)$ ir

ii) $(x_1 * \cdots * x_j) * (x_{j+1} * \cdots * x_n)$, čia $1 \leq i, j \leq n$.

Pagal indukcinę prielaidą elementai

$$x_1 * \cdots * x_i,\ x_{i+1} * \cdots * x_n,\ x_1 * \cdots * x_j,\ x_{j+1} * \cdots * x_n$$

yra vienareikšmiškai apibrėžti. Tarkime, kad $i < j$. Tuomet

$$(x_1 * \cdots * x_i) * ((x_{i+1} * \cdots * x_j) * (x_{j+1} * \cdots * x_n))$$

ir

$$((x_1 * \cdots * x_i) * (x_{i+1} * \cdots * x_j)) * (x_{j+1} * \cdots * x_n).$$

Pažymėję $x = x_1 * \cdots * x_i$, $y = x_{i+1} * \cdots * x_j$ ir $z = x_{j+1} * \cdots * x_n$, gauname:

$$(x_1 * \cdots * x_i) * ((x_{i+1} * \cdots * x_j) * (x_{j+1} * \cdots * x_n)) = x * (y * z)$$

ir

$$((x_1 * \cdots * x_i) * (x_{i+1} * \cdots * x_j)) * (x_{j+1} * \cdots * x_n) = (x * y) * z.$$

Kadangi kompozicijos dėsnis $*$ aibėje X yra asociatyvus, tai $x*(y*z) = (x*y)*z$, t. y.

$$(x_1 * \cdots * x_i) * (x_{i+1} * \cdots * x_n) = (x_1 * \cdots * x_j) * (x_{j+1} * \cdots * x_n).$$

$\square$

2.2.4 pavyzdys. Atimtis aibėse $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ nėra asociatyvi.

2.2.5 pavyzdys. Dalyba aibėse $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ nėra asociatyvi.

2.2.6 pavyzdys. Aibių atimtis $\setminus$ aibėje $P(X)$, čia X – kuri nors aibė, nėra asociatyvi.

2.2.7 pavyzdys. Kompozicijos dėsniai min, max aibėse $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ yra asociatyvūs.

2.2.8 pavyzdys. Kompozicijos dėsniai $\sqcup$, $\sqcap$ aibėje $\mathbb{N}$ yra asociatyvūs.

2.2.9 pavyzdys. Simetrinė aibių atimtis $\ominus$ aibėje $P(X)$, čia X – kuri nors aibė, yra asociatyvi. Įsitikinkite!

2.2.10 pavyzdys. Aibių sudėtis (sąjunga) $\cup$ ir daugyba (sankirta) $\cap$ aibėje $\mathbb{P}(X)$, čia X – kuri nors aibė, yra asociatyvūs kompozicijos dėsniai.

2.2.11 pavyzdys. Apibrėžkime kompozicijos dėsnį aibėje $\mathbb{N}$ taip:

$$* : \mathbb{N} \times \mathbb{N} \to \mathbb{N},\ (a, b) \mapsto a * b = a^b,\ a, b \in \mathbb{N}.$$

Šis kompozicijos dėsnis nėra asociatyvus.

2.2.12 pavyzdys. Tegu X – kuri nors netuščia aibė. Atvaizdžių kompozicija $\circ$ aibėje X^X yra asociatyvi (čia X^X – visų atvaizdžių $f : X \to X$ aibė).

2.3 Indukuotieji kompozicijos dėsniai

Sakykime, Y yra aibės X netuščias poaibis, $*$ – aibės X elementų kompozicijos dėsnis.

2.3.1 apibrėžimas. Aibės X poaibis Y yra vadinamas *stabiliu* aibės X elementų kompozicijps dėsnio $*$ atžvilgiu, jei bet kuriems y_1, $y_2 \in Y$, $y_1 * y_2 \in Y$.

Jei aibės X poaibis Y yra stabilus kompozicijos dėsnio $*$ aibėje X atžvilgiu, tai kompozicijos dėsnio $* : X \times X \to X$ siaurinys $*\big|_{Y\times Y} : Y \times Y \to Y$ yra kompozicijos dėsnis aibėje Y, vadinamas kompozicijos dėsnio $*$ *indukuotuoju dėsniu* aibėje Y. Indukuotąjį kompozicijos dėsnį aibėje Y žymėsime taip pat kaip aibės X elementų kompozicijos dėsnį $*$, t. y. nerašysime atvaizdžio siaurinio ženklo $\big|_{Y\times Y}$. Jei aibės X netuščias poaibis Y yra stabilus aibės X elementų kompozicijos dėsnio $*$ atžvilgiu, tai rašysime $(Y, *) \subset (X, *)$.

2.3.2 pavyzdys. Nagrinėkime skaičių sudėtį $+$ aibėje $\mathbb{Z}$. Poaibis $n\mathbb{Z}$ (priminsime, kad $n\mathbb{Z} = \{nl \mid l \in \mathbb{Z}\}$), čia n – kuris nors fiksuotas natūralusis skaičius, yra stabilus sudėties $+$ atžvilgiu. Poaibis $1 + 2\mathbb{Z}$ (nelyginių skaičių poaibis) nėra stabilus sudėties $+$ atžvilgiu.

2.3.3 pavyzdys. Nagrinėkime skaičių daugybą $\cdot$ aibėje $\mathbb{Z}$. Poaibis $n\mathbb{Z}$, čia n – kuris nors fiksuotas natūralusis skaičius, yra stabilus daugybos $\cdot$ atžvilgiu. Poaibis $1+2\mathbb{Z}$ taip pat stabilus daugybos $\cdot$ atžvilgiu, o poaibis $2+3\mathbb{Z}$ ($2+3\mathbb{Z} = \{2+3l \mid l \in \mathbb{Z}\}$) nėra stabilus daugybos $\cdot$ atžvilgiu.

2.3.4 pavyzdys. Tarkime, X – netuščia aibė, o X^X – visų atvaizdžių $f : X \to X$ aibė. Pažymėkime $\mathcal{A}ut(X)$ aibės X^X poaibį, sudarytą iš visų bijekcijų $f : X \to X$. Aibės X^X poaibis $\mathcal{A}ut(X)$ yra stabilus atvaizdžių kompozicijos $\circ$ atžvilgiu, t. y., jei $f, g \in \mathcal{A}ut(X)$, tai $f \circ g \in \mathcal{A}ut(X)$.

2.3.5 pavyzdys. Akivaizdu, kad jei Y – aibės X netuščias poaibis, tai $P(Y)$ stabilus aibės $P(X)$ poaibis aibių sudėties (sąjungos) $\cup$ ir daugybos (sankirtos) $\cap$ atžvilgiu.

2.3.6 teiginys. *Aibės X elementų asociatyvus kompozicijos dėsnis $*$ stabiliame aibės X $*$ atžvilgiu poaibyje Y indukuoja asociatyvų kompozicijos dėsnį.*

Įrodymas. Šio teiginio įrodymas akivaizdus ir paliekamas skaitytojui. □

2.4 Faktorkompozicijos dėsniai

Sakykime, aibėje X yra apibrėžtas kompozicijos dėsnis $*$ ir ekvivalentumo sąryšis R.

2.4.1 apibrėžimas. Kompozicijos dėsnis $*$ ir ekvivalentumo sąryšis R, apibrėžti aibėje X, yra vadinami *suderintais*, jei

$$x_1 \equiv x_2 \pmod R,\ x_3 \equiv x_4 \pmod R \Longrightarrow x_1 * x_3 \equiv x_2 * x_4 \pmod R.$$

Jei kompozicijos dėsnis $*$ ir ekvivalentumo sąryšis R, apibrėžti aibėje X, yra suderinti, tai galima apibrėžti kompozicijos dėsnį $*$ aibės X pagal ekvivalentumo sąryšį R faktoraibėje X/R:

$$(x_1 \pmod R) * (x_2 \pmod R) = x_1 * x_2 \pmod R.$$

Šis apibrėžimas nepriklauso nuo atstovų x_1 ir x_2 iš ekvivalentumo klasių

$$x_1 \pmod R \quad \text{ir} \quad x_2 \pmod R$$

išrinkimo. Taip apibrėžtas kompozicijos dėsnis $*$ faktoraibėje X/R yra vadinamas kompozicijos dėsnio $*$, apibrėžto aibėje X, pagal ekvivalentumo sąryšį R *faktordėsniu.*

2.4.2 pavyzdys. Skaičių sudėtis $+$ ir ekvivalentumo sąryšis $R_n = \{(a,b) \mid a,b \in \mathbb{Z},\ a-b \in n\mathbb{Z}\}$, čia n – fiksuotas natūralusis skaičius, aibėje $\mathbb{Z}$ yra suderinti. Sudėtis faktoraibėje

$$Z_n = \mathbb{Z}/R_n = \{n\mathbb{Z}, 1+n\mathbb{Z}, \dots, n-1+n\mathbb{Z}\}$$

apibrėžiama taip: $(i+n\mathbb{Z}) + (j+n\mathbb{Z}) =: i+j+n\mathbb{Z}$, $i,j \in \mathbb{Z}$ (priminsime, kad $a+n\mathbb{Z} = b+n\mathbb{Z}$ tada ir tik tada, kai $n|\ a-b$, t. y. n dalija $a-b$).

Skaičių daugyba $\cdot$ ir tas pats ekvivalentumo sąryšis R_n aibėje $\mathbb{Z}$ yra suderinti. Daugyba $\cdot$ faktoraibėje $Z_n = \mathbb{Z}/R_n$ apibrėžiama taip: $(i+n\mathbb{Z})\cdot(j+n\mathbb{Z}) =: i\cdot j+n\mathbb{Z}$, $i,j \in \mathbb{Z}$.

Aibė $i+n\mathbb{Z} = \{i+nt \mid t \in \mathbb{Z}\}$ vadinama *likinių klase* arba *likinių aibe* moduliu n.

2.4.3 teiginys. *Jei aibės X elementų kompozicijos dėsnis $*$ yra asociatyvus ir suderintas su ekvivalentumo sąryšiu R, apibrėžtu aibėje X, tai kompozicijos dėsnio $*$ pagal R faktorkompozicijos dėsnis $*$ faktoraibėje X/R yra asociatyvus.*

Įrodymas. Šio teiginio įrodymas akivaizdus ir paliekamas skaitytojui. □

2.5 Neutralus elementas. Simetriniai elementai

2.5.1 Neutralus elementas

2.5.1 apibrėžimas. Tarkime, kad $*$ yra aibės X elementų kompozicijos dėsnis. Aibės X elementas e yra vadinamas *neutraliu* kompozicijos dėsnio $*$ atžvilgiu, jei kiekvienam $x \in X$, $e * x = x * e = x$.

2.5.2 teiginys. *Aibėje X šios aibės elementų kompozicijos dėsnio $*$ atžvilgiu gali egzistuoti ne daugiau kaip vienas neutralus elementas.*

Įrodymas. Sakykime, e ir e' aibės X elementų kompozicijos dėsnio $*$ atžvilgiu yra neutralūs elementai. Tuomet $e' = e' * e = e$. $\square$

2.5.3 pavyzdys. Aibėje $\mathbb{Z}$ (taip pat aibėse $\mathbb{Z}$, $\mathbb{R}$) skaičių sudėties $+$ atžvilgiu 0 yra neutralus elementas.

2.5.4 pavyzdys. Aibėje $\mathbb{Z}$ (taip pat aibėse $\mathbb{Q}$, $\mathbb{Q}^*$, $\mathbb{R}$, $\mathbb{R}^*$) skaičių daugybos $\cdot$ atžvilgiu 1 yra neutralus elementas.

2.5.5 pavyzdys. Tuščia aibė yra aibės $P(X)$ neutralus elementas simetrinės atimties $\ominus$ atžvilgiu.

2.5.6 pavyzdys. Tapatusis atvaizdis $\mathrm{id} \in \mathcal{A}ut(X)$, čia X – netuščia aibė, $\mathcal{A}ut(X)$ – visų bijekcijų $f : X \to X$ aibė, yra neutralus elementas atvaizdžių kompozicijos $\circ$ atžvigiu.

Susitarimas. Tuo atveju, kai aibės X elementų kompozicijos dėsnį žymėsime $+$ (arba $\cdot$) ir šio kompozicijos dėsnio atžvilgiu aibėje X egzistuos neutralus elementas, šį elementą žymėsime 0 (arba 1) ir vadinsime nuliu (arba vienetu).

2.5.2 Simetrinis elementas

2.5.7 apibrėžimas. Tarkime, $*$ yra aibės X elementų kompozicijos dėsnis, e – šio kompozicijos dėsnio atžvilgiu neutralus elementas. Elementas $x' \in X$ yra vadinamas *simetriniu elementu* elementui $x \in X$, jei $x' * x = x * x' = e$.

2.5.8 teiginys. *Sakykime, aibės X elementų kompozicijos dėsnis $*$ yra asociatyvus ir šio kompozicijos dėsnio atžvilgiu egzistuoja neutralus elementas e. Tuomet kiekvienam aibės X elementui gali egzistuoti ne daugiau kaip vienas simetrinis elementas.*

Įrodymas. Tarkime, kad elementui $x \in X$ egzistuoja simetriniai elementai $x', x'' \in X$. Tuomet $x' = x' * e = x' * (x * x'') = (x' * x) * x'' = e * x'' = x''$. $\square$

2.5.9 pavyzdys. Kiekvienam aibės $(\mathbb{Z}, +)$ (taip pat aibių $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$) elementui a egzistuoja simetrinis elementas $-a$.

2.5.10 pavyzdys. Kiekvienam aibės $(\mathbb{Q}^*, \cdot)$ (taip pat aibės $(\mathbb{R}^*, \cdot)$) elementui a egzistuoja simetrinis elementas a^{-1}.

2.5.11 pavyzdys. Nagrinėkime aibę $P(X)$ ir joje simetrinę aibių atimtį $\ominus$. Kiekvienam aibės $P(X)$ elementui A simetrinis elementas egzistuoja ir yra lygus A. Iš tikrųjų, $A \ominus A = \emptyset$.

2.5.12 pavyzdys. Nagrinėkime aibę $\mathcal{A}ut(X)$, čia X – netuščia aibė, ir joje apibrėžtą atvaizdžių kompoziciją $\circ$. Kiekvienam aibės $\mathcal{A}ut(X)$ elementui f egzistuoja simetrinis elementas $f^{-1} \in \mathcal{A}ut(X)$. Iš tikrųjų, $f \in \mathcal{A}ut(X)$ tada ir tik tada, kai atvaizdis $f : X \to X$ yra bijekcija. Vadinasi, egzistuoja $f^{-1} \in \mathcal{A}ut(X)$ ir $f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}$.

Susitarimas. Sakykime, kad aibės X elementų kompozicijos dėsnis yra žymimas $+$ (arba $\cdot$) ir šio kompozicijos dėsnio atžvilgiu egzistuoja neutralus elementas 0 (arba 1). Tuomet elementui $x \in X$ simetrinį elementą, jei jis egzistuoja, žymėsime $-x$ (arba x^{-1}) ir vadinsime *priešingu* (*atvirkštiniu*) elementu elementui x.

2.5.3 Komutatyvūs kompozicijos dėsniai

2.5.13 apibrėžimas. Aibės X elementų kompozicijos dėsnis $*$ yra vadinamas *komutatyviuoju*, jei bet kuriems elementams $x, y \in X$, $x * y = y * x$.

2.5.14 pavyzdys. Skaičių sudėtis $+$ aibėje $\mathbb{N}$ (taip pat aibėse $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$) yra komutatyvus kompozicijos dėsnis.

2.5.15 pavyzdys. Skaičių daugyba $\cdot$ aibėje $\mathbb{N}$ (taip pat aibėse $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{Z}^*$, $\mathbb{Q}^*$, $\mathbb{R}^*$) yra komutatyvus kompozicijos dėsnis.

2.5.16 pavyzdys. Simetrinė aibių atimtis $\ominus$ aibėje $P(X)$, čia$X$ – kuri nors aibė, yra komutatyvus kompozicijos dėsnis.

2.5.17 pavyzdys. Aibės $\mathcal{A}ut(X)$ elementų kompozicijos dėsnis $\circ$ ($\circ$ – atvaizdžių kompozicijos dėsnis) nėra komutatyvus, kai $|X| \geq 3$. Iš tikrųjų. Imkime tris skirtingus aibės X elementus x_1, x_2, x_3 ir nagrinėkime bijekcijas $f : X \to X$, $g : X \to X$, apibrėžtas taip:

$$f(x_1) = x_2,\ f(x_2) = x_1,\ f(x) = x,\ \text{kai } x \in X \setminus \{x_1, x_2\} \text{ ir}$$
$$g(x_2) = x_3,\ g(x_3) = x_2,\ g(x) = x,\ \text{kai } x \in X \setminus \{x_2, x_3\}.$$

Tada

$$(f \circ g)(x_1) = f(g(x_1)) = f(x_1) = x_2,$$
$$(g \circ f)(x_1) = g(f(x_1)) = g(x_2) = x_3,$$

t. y. $f \circ g \neq g \circ f$.

2.6 Išoriniai kompozicijos dėsniai

2.6.1 apibrėžimas (išorinio kompozicijos dėsnio apibrėžimas)**.** Aibės Ω, vadinamos operatorių aibe, elementų ir aibės X elementų *išoriniu kompozicijos dėsniu* yra vadinamas atvaizdis $f : \Omega \times X \to X$. Aibės Ω elementai yra vadinami *operatoriais*. Operatoriaus $\alpha \in \Omega$ ir aibės X elemento x kompozicija yra vadinama funkcijos f reikšmė $f(\alpha, x) \in X$.

Kaip ir vidinio kompozicijos dėsnio atveju sakysime, kad išorinis kompozicijos dėsnis f apibrėžtas aibėje X, o Ω – išorinio kompozicijos dėsnio f operatorių aibė.

Kai $\Omega = X$, išorinis kompozicijos dėsnis f yra vidinis kompozicijos dėsnis, apibrėžtas aibėje X. Taigi vidinio kompozicijos dėsnio sąvoka yra išorinio kompozicijos dėsnio sąvokos atskiras atvejis.

Išorinius kompozicijos dėsnius, kaip ir vidinius, žymėsime $\cdot$, $*$, $\circ$ ar dar kitokiais ženklais ir rašysime (o dažniausiai praleisime) tarp komponuojamųjų elementų: operatoriaus $\alpha \in \Omega$ ir elemento $x \in X$. Kai kuriais atvejais apibrėšime ir kitokius išorinio kompozicijos dėsnio ženklus, patogius konkrečiose situacijose. Pavyzdžiui, elementų $\alpha \in \Omega$ ir $x \in X$ kompoziciją galima žymėti x^α.

Sakykime, $*$ – opratorių aibės Ω ir aibės X elementų išorinis kompozicijos dėsnis, $A \subset \Omega$, $Y \subset X$. Apibrėžkime $A * Y = \{\alpha y \mid \alpha \in \Omega, y \in Y\}$. Akivaizdu, kad $A * X \subset X$. Šiuo atveju operatorių aibę Ω susiaurinome iki aibės A.

2.6.2 apibrėžimas (stabilus poaibis)**.** Sakykime, $*$ – operatorių aibės Ω ir aibėsX elementų išorinis kompozicijos dėsnis. Aibės X poaibis $Y \neq \emptyset$ yra vadinamas *stabiliu* išorinio kompozicijos dėsnio $*$ atžvilgiu, jei $\Omega * Y \subset Y$. Jei aibės X netuščias poaibis Y yra stabilus išorinio kompozicijos dėsnio $*$ atžvilgiu, tai išorinis kompozicijos dėsnis $*$ aibėje X apibrėžia išorinį kompozicijos dėsnį aibėje Y, vadinamą *indukuotu išoriniu kompozicijos dėsniu* aibėje Y.

Tarkime, kad aibėje X apibrėžtas ekvivalentumo sąryšis R, $*$ – išorinis kompozicijos dėsnis tarp Ω ir X elementų.

2.6.3 apibrėžimas. Išorinis kompozicijos dėsnis $*$ yra vadinamas *suderintu su ekvivalentumo sąryšiu* R aibėje X, jei kiekvienam $\alpha \in \Omega$,

$$x \equiv y \pmod R \Longrightarrow \alpha * x \equiv \alpha * y \pmod R.$$

Šiuo atveju galima apibrėžti išorinį kompozicijos dėsnį $*$ tarp operatorių aibės Ω ir faktoraibės X/R elementų:

$$\alpha * (x \pmod R) = \alpha * x \pmod R,\ \alpha \in \Omega,\ x \in X.$$

2.6.4 pavyzdys. Tarkime, X – netuščia aibė, $\Omega = X^X$. Operatorių aibės Ω ir aibės X elementų išorinį kompozicijos dėsnį $*$ apibrėškime taip:

$$\Omega \times X \to X,\ (f, x) \mapsto f * x = f(x),\ f \in \Omega,\ x \in X.$$

2.6.5 pavyzdys. Tegu $\Omega = X^X$, X – netuščia aibė, $A \subset \Omega$, $A \neq \emptyset$. Operatorių $f \in A$ ir aibės X elementų išorinis kompozicijos dėsnis apibrėžiamas kaip ir 2.6.4 pavyzdyje (kitaip tariant, operatorių aibę Ω susiaurinome iki aibės A). Dažnai pasitaiko svarbus atvejis, kai $A = \mathcal{A}ut(X)$. Vėliau šį atvejį nagrinėsime nuodugniau.

2.6.6 pavyzdys. Sakykime, S, X – netuščios aibės, $\Omega = X^X$, $\psi : S \to \Omega$ – atvaizdis. Operatorių aibės S ir aibės X elementų išorinį kompozicijos dėsnį $*$ apibrėžkime taip:

$$S \times X \to X,\ (\alpha, x) \mapsto \alpha * x = \psi(\alpha)(x),\ \alpha \in S,\ x \in X.$$

2.7 Algebrinės struktūros

Pagrindiniai algebros objektai, intensyviai pradėti tirti maždaug nuo XIX a. vidurio, yra algebrinės struktūros. Pusgrupės, grupės, žiedai, kūnai, tiesinės erdvės, algebros, moduliai – tai tik nedaugelio algebrinių struktūrų pavadinimai. Dabar apibrėšime abstrakčią, bendrą algebrinės struktūros sąvoką, o vėliau, apsiribodami kompozicijos dėsniais, kurie ir yra algebrinės struktūros aibės pagrindas, apibrėšime konkrečias algebrines struktūras ir suteiksime joms pavadinimus.

2.7.1 apibrėžimas. Algebrinę aibės X struktūrą apibrėžia vienas ar keletas aibės X elementų vidinių kompozicijos dėsnių ir vienas ar keletas operatorių aibių Ω_1, Ω_2, ... ir aibės X elementų išorinių kompozicijos dėsnių. Be to, šie kompozicijos dėsniai gali tenkinti vienokią ar kitokią aksiomų sistemą ir gali būti susiję vieni su kitais įvairiais sąryšiais. Dažniausiai X yra vadinama pagrindine aibe, o operatorių aibės Ω_1, Ω_2, ... – pagalbinėmis.

Galima nagrinėti aibės X poaibius Y, $Y \neq \emptyset$, stabilius visų kompozicijos dėsnių aibėje X atžvilgiu, ir tuose poaibiuose Y apibrėžti indukuotąsias algebrines struktūras. Panašiai galima nagrinėti ekvivalentumo sąryšius R aibėje X, suderintus su visais kompozicijos dėsniais, apibrėžtais aibėje X, ir apibrėžti algebrines faktorstruktūras aibėje X/R. Kai nagrinėsime konkrečias algebrines struktūras, išsamiai, kiek tai bus įmanoma, ir aptarsime indukuotąsias algebrines struktūras ir algebrines faktorstruktūras tais konkrečiais atvejais.

3 skyrius

Natūralieji ir sveikieji skaičiai

3.1 Elementari dalumo teorija

3.1.1. Šiame skyriuje išdėstysime natūraliųjų, sveikųjų skaičių elementariąją dalumo teoriją, Euklido algoritmą ir įrodysime pagrindinę aritmetikos teoremą.

Natūraliųjų skaičių aibę, taip pat skaičių sudėties, daugybos veiksmus ir tvarkos sąryšį joje būtų galima apibrėžti aksiomatiškai. Paskui to būtų galima natūraliųjų skaičių aibę praplėsti iki sveikųjų skaičių aibės ir vienareikšmiškai pratęsti sudėties, daugybos veiksmus bei tvarkos sąryšį, apibrėžtus natūraliųjų skaičių aibėje, į sveikųjų skaičių aibę, išlaikant pagrindines jų savybes. Bet mes taip nedarysime. Skaitytojui, be jokios abejonės, yra žinomi skaičių sudėties, daugybos veiksmų ir tvarkos sąryšio, apibrėžtų tiek natūraliųjų, tiek sveikųjų skaičių aibėse, pagrindinės savybės.

Natūraliųjų skaičių aibę žymėsime $\mathbb{N}$, o sveikųjų skaičių aibę – $\mathbb{Z}$. Nulis 0 priklauso natūraliųjų skaičių aibei $\mathbb{N}$. Skaičių sudėties ir daugybos veiksmus žymėsime $+$ ir $\cdot$. Dažniausiai daugybos ženklą tarp dauginamųjų praleisime, o rašysime tik tais atvejais, kai, šį ženklą praleidus, gali iškilti dviprasmybių.

Taip pat tariame, kad skaitytojui yra žinomi egzistencijos ir pilnosios indukcijos principai. Priminsime juos.

3.1.2 (egzistencijos principas)**.** Kiekvienas netuščias natūraliųjų skaičių aibės poaibis turi mažiausią natūralųjį skaičių.

Skaičių teorijoje daugelis egzistencijos įrodymų grindžiami egzistencijos principu.

3.1.3 (pilnosios indukcijos principas)**.** Tarkime, kad $A(n)$ žymi teiginį, priklausantį nuo natūraliojo skaičiaus n. Norėdami įsitikinti, ar šis teiginys teisingas kiekvienam natūraliajam skaičiui n, galime pasinaudoti matematinės indukcijos metodu. Matematinės indukcijos metodas susideda iš trijų dalių.

Pirmas žingsnis. Pirmiausia patikriname, ar teiginys teisingas skaičiui $n = 1$ (arba kuriam nors konkrečiam skaičiui $n = n_0$, nes mažesniems natūraliems skaičiams teiginys $A(n)$ gali būti neapibrėžtas).

Antras žingsnis. Darome indukcinę prielaidą, kad teiginys $A(m)$ teisingas kiekvienam natūraliajam skaičiui $m < n$ (arba kiekvienam natūraliajam skaičiui m, tenkinančiam sąlygą $n_0 \leq m < n$).

Trečias žingsnis. Remdamiesi indukcine prielaida, įrodome, kad teisingas ir teiginys $A(n)$.

Atlikę minėtus tris žingsnius, darome išvadą, kad teiginys $A(n)$ teisingas visiems natūraliesiems skaičiams $n \geq 1$ $(n \geq n_0)$.

Elementarioji dalumo teorija remiasi skaičiaus daliklio apibrėžimu.

3.1.4 apibrėžimas. Sveikasis skaičius b vadinamas sveikojo skaičiaus a *dalikliu* ir žymima $b \mid a$, jei egzistuoja toks sveikasis skaičius c, kad $a = bc$. Skaičius c yra vadinamas skaičiaus a daliklio b papildomu dalikliu.

Tuo atveju, kai skaičius b yra skaičiaus a daliklis, dažnai rašoma: skaičius b dalija skaičių a; skaičius a dalijasi iš skaičiaus b; skaičius a yra skaičiaus b kartotinis.

Sutarkime rašyti $b \nmid a$ tuo atveju, kai skaičius b nėra skaičiaus a daliklis (skaičius b nedalija skaičiaus a).

Remiantis skaičiaus daliklio apibrėžimu, galima įrodyti šias skaičių dalumo savybes:

1. Kiekvienam $a \in \mathbb{Z}$, $\pm 1 \mid a$.
2. Kiekvienam $a \in \mathbb{Z}$, $a \mid 0$ (yra susitarta, kad $0 \mid 0$).
3. Kiekvienam $a \in \mathbb{Z}$, $a \mid a$.
4. Jei $a \mid 1$, tai $a = \pm 1$.
5. Jei $0 \mid a$, tai $a = 0$.
6. Jei $b \mid a$ ir $a \mid b$, tai $a = \pm b$.
7. Jei $c \mid b$ ir $b \mid a$, tai $c \mid a$.
8. Jei $b \mid a_1$ ir $b \mid a_2$, tai bet kuriems $u_1, u_2 \in \mathbb{Z}$, $b \mid a_1u_1 + a_2u_2$.

Šias skaičių dalumo savybes gali įrodyti skaitytojas.

3.1.5 (skaičių didžiausias bendrasis daliklis)**.** Remdamiesi skaičių dalumo sąvoka, galime apibrėžti skaičių didžiausią bendrąjį daliką.

3.1.6 apibrėžimas. Sveikasis skaičius d vadinamas sveikųjų skaičių a_1, a_2, …, a_n *didžiausiu bendruoju dalikliu*, jei

1. $d \mid a_1$, $d \mid a_2$, …, $d \mid a_n$;
2. Jei $d' \mid a_1$, $d' \mid a_2$, …, $d' \mid a_n$, tai $d' \mid d$.

Šis apibrėžimas remiasi tik skaičių dalumo sąvoka ir nesiremia tokiomis sąvokomis kaip „didesnis“, „mažesnis“, „didžiausias“ir panašiai. Dažnai skaičių a_1, a_2, …, a_n didžiausias bendrasis daliklis yra apibrėžiamas kaip didžiausias natūralusis skaičius d, kuris dalija skaičius $a_1, a_2, \ldots, a_n$. Daugeliu atvejų dalumo sąvoką galima apibrėžti ne tik natūraliųjų ir sveikųjų, bet ir kitų skaičių aibėse, o tvarkos sąryšio, suderinto su sudėties ir daugybos savybėmis, tose aibėse apibrėžti negalima.

3.1.7 pastaba. Jei d yra skaičių $a_1, a_2, \ldots, a_n$ didžiausias bendrasis daliklis (dbd), tai akivaizdu, kad ir $-d$ taip pat yra skaičių a_1, a_2, …, a_n dbd. Taigi iš dviejų skaičių $a_1, a_2, \ldots, a_n$ dbd, besiskiriančių ženklu, galime išsirinkti neneigiamąjį ir jį žymėti $\mathrm{dbd}(a_1, a_2, \ldots, a_n)$ arba $a_1 \sqcup a_2 \sqcup \cdots \sqcup a_n$. Pavyzdžiui, $5 \sqcup 6 \sqcup 12 = 1$, $0 \sqcup (-7) = 7$, $0 \sqcup a = |a|$, čia $a \in \mathbb{Z}$.

Remdamiesi skaičių dbd apibrėžimu, gauname $a_1 \sqcup a_2 \sqcup \cdots \sqcup a_n = a_1 \sqcup (a_2 \sqcup \cdots \sqcup a_n)$. Vadinasi, n skaičių a_1, a_2, …, a_n dbd, $n \geq 2$, galima apskaičiuoti, mokant apskaičiuoti dviejų skaičių dbd.

Prielaida. Sutarkime, kad $0 \sqcup 0 = 0$.

Kadangi $0 \sqcup a = |a|$, tai galima apsiriboti skaičių $a_1 \neq 0$, $a_2 \neq 0$ dbd radimu. Nesusiaurindami bendrumo, galime tarti, kad $a_1 > 0$, $a_2 > 0$, nes $a_1 \sqcup a_2 = (-a_1) \sqcup a_2 = a_1 \sqcup (-a_2) = (-a_1) \sqcup (-a_2)$.

3.1.8 (dalybos su liekana formulė)**.** Dviejų skaičių a_1 ir a_2 didžiausią bendrąjį daliklį $a_1 \sqcup a_2$ galima rasti remiantis Euklido algoritmu. Euklido algoritmas pagrįstas dalybos su liekana formule.

3.1.9 teiginys (dalybos su liekana formulė)**.** *Bet kuriems $a_1, a_2 \in \mathbb{Z}$, $a_2 > 0$, egzistuoja tokie vieninteliai skaičiai $b_2, a_3 \in \mathbb{Z}$, $0 \leq a_3 < a_2$, kad $a_1 = a_2 b_2 + a_3$.*

Įrodymas. Kadangi $a_2 > 0$, tai egzistuoja toks $b_2 \in \mathbb{Z}$, kad

$$a_2 b_2 \leq a_1 < a_2(b_2 + 1).$$

Pažymėkime $a_3 =: a_1 - a_2 b_2$. Akivaizdu, kad $0 \leq a_3 < a_2$ ir $a_1 = a_2 b_2 + a_3$. Jei egzistuotų kita tokia skaičių pora $b_2', a_3' \in \mathbb{Z}$, $0 \leq a_3' < a_2$, kad $a_1 = a_2 b_2' + a_3'$, tai gautume lygybę:

$$a_2 b_2' + a_3' = a_2 b_2 + a_3.$$

Pertvarkę šią lygybę, gautume: $a_2(b_2' - b_2) = a_3 - a_3'$. Vadinasi, būtų tesinga lygybė $a_2|b_2' - b_2| = |a_3 - a_3'|$. Bet $0 \leq |a_3 - a_3'| < a_2$. Taigi $b_2' = b_2$, $a_3' = a_3$. $\square$

3.2 Euklido algoritmas

3.2.1. Tarkime, a_1, a_2 – sveikieji skaičiai, $a_2 > 0$. Keletą kartų pasinaudoję dalybos su liekana formule, gauname:

$$\begin{array}{ll} a_1 = a_2 b_2 + a_3, & 0 \leq a_3 < a_2, \\ a_2 = a_3 b_3 + a_4, & 0 \leq a_4 < a_3, \\ \vdots \qquad \vdots & \qquad \vdots \\ a_{l-3} = a_{l-2} b_{l-2} + a_{l-1}, & 0 \leq a_{l-1} < a_{l-2}, \\ a_{l-2} = a_{l-1} b_{l-1} + a_l, & 0 \leq a_l < a_{l-1}, \\ a_{l-1} = a_l b_l + 0. & \end{array}$$

Šių lygybių seka ir sudaro *Euklido algoritmo* esmę.

Įrodysime, kad paskutinė nelygi nuliui liekana a_l yra skaičių a_1, a_2 didžiausias bendrasis daliklis. Tam reikia įrodyti, kad

1. $a_l \mid a_1$, $a_l \mid a_2$.

2. Jei $d' \mid a_1$, $d' \mid a_2$, tai $d' \mid a_l$.

Iš paskutinės Euklido algoritmo lygybės matome, kad $a_l \mid a_{l-1}$, iš priešpaskutinės – $a_l \mid a_{l-2}$ ir t. t. Taigi $a_l \mid a_2$, $a_l \mid a_1$.

Lieka įsitikinti, kad a_l tenkina ir antrąją didžiausio bendrojo daliklio apibrėžimo savybę. Sakykime, $d' \mid a_1$, $d' \mid a_2$. Iš pirmosios Euklido algoritmo lygybės matome, kad $d' \mid a_3$, iš antrosios – $d' \mid a_4$ ir t. t. Taigi galų gale gauname $d' \mid a_l$.

3.2.2 išvada. *Jei d yra skaičių a_1 ir a_2 didžiausias bendrasis daliklis, tai egzistuoja tokie sveikieji skaičiai u_1, u_2, kad*

$$d = a_1 u_1 + a_2 u_2. \tag{3.1}$$

Įrodymas. Pritaikę skaičiams a_1, a_2 Euklido algoritmą, tarkime, gauname $d = a_l$. Remdamiesi anksčiau parašytomis lygybėmis, gauname:

$$d = a_l = a_{l-2} - a_{l-1} b_{l-1} = a_{l-2} - (a_{l-3} - a_{l-2} b_{l-2}) b_{l-1} =$$

$$= -a_{l-3} b_{l-1} + a_{l-2}(1 + b_{l-1} b_{l-2}) = \cdots = a_1 u_1 + a_2 u_2.$$

□

3.2.3 apibrėžimas. (3.1) išraiška vadinama skaičių a_1 ir a_2 didžiausio bendrojo daliklio *tiesine išraiška*.

3.2.4 pavyzdys. Rasime skaičių 1147 ir 899 didžiausą bendrąjį daliklį ir jį išreikšime duotaisiais skaičiais. Užrašome lygybes:

$$\begin{aligned}
1147 &= 899 \cdot 1 + 248,\\
899 &= 248 \cdot 3 + 155,\\
248 &= 155 \cdot 1 + 93,\\
155 &= 93 \cdot 1 + 62,\\
93 &= 62 \cdot 1 + 31,\\
62 &= 31 \cdot 2 + 0.
\end{aligned}$$

Taigi skaičių 1147 ir 899 didžiausias bendrasis daliklis yra lygus 31.
$31 = 93-62 = 93-(155-93) = 93\cdot 2-155 = (248-155)\cdot 2-155 = 248\cdot 2-155\cdot 3 = 248 \cdot 2 - (899 - 248 \cdot 3) \cdot 3 = 248 \cdot 11 - 899 \cdot 3 = (1147 - 899) \cdot 11 - 899 \cdot 3 = 1147 \cdot 11 - 899 \cdot 14.$

Kaip matome, $a_1 = 1147$, $u_1 = 11$, $a_2 = 899$, $u_2 = -14$.

3.2.5 pavyzdys. Rasime skaičių 47561 ir 3911 didžiausą bendrąjį daliklį ir jį išreikšime duotaisiais skaičiais. Užrašome lygybes:

$$\begin{aligned}
47561 &= 3911 \cdot 12 + 629,\\
3911 &= 629 \cdot 6 + 137,\\
629 &= 137 \cdot 4 + 81,\\
137 &= 81 \cdot 1 + 56,\\
81 &= 56 \cdot 1 + 25,\\
56 &= 25 \cdot 2 + 6,\\
25 &= 6 \cdot 4 + 1.
\end{aligned}$$

$1 = 25 - 6 \cdot 4 = 25 - (56 - 25 \cdot 2) \cdot 4 = 25 \cdot 9 - 56 \cdot 4 = (81 - 56) \cdot 9 - 56 \cdot 4 = 81\cdot 9-56\cdot 13 = 81\cdot 9-(137-81)\cdot 13 = 81\cdot 22-137\cdot 13 = (629-137\cdot 4)\cdot 22-137\cdot 13 = 629 \cdot 22 - 137 \cdot 101 = 629 \cdot 22 - (3911 - 629 \cdot 6) \cdot 101 = 629 \cdot 628 - 3911 \cdot 101 = (47561 - 3911 \cdot 12) \cdot 628 - 3911 \cdot 101 = 47561 \cdot 628 - 3911 \cdot 7637.$

Šiuo atveju $a_1 = 47561$, $u_1 = 628$, $a_2 = 3911$, $u_2 = -7637$.

Skaičių a ir b didžiausio bendrojo daliklio ir jo tiesinės išraiškos patogu ieškoti naudojant matricas (lenteles). Nagrinėkime skaičių matricą (skaičių lentelę)

$$\begin{pmatrix} x_1 & y_1 & r_1 \\ x_2 & y_2 & r_2 \end{pmatrix}.$$

3.2.6 apibrėžimas. Operacija, kai viena šios matricos eilutė padauginama iš skaičiaus ir pridedama prie kitos eilutės, vadinama *elementariąja*.

3.2.7 teiginys. *Tegu a, b – skaičiai. Tarkime, kad skaičių matricai*

$$\begin{pmatrix} x_1 & y_1 & r_1 \\ x_2 & y_2 & r_2 \end{pmatrix} \tag{3.2}$$

teisingos lygybės $ax_1 + by_1 = r_1$ *ir* $ax_2 + by_2 = r_2$*. Pažymėkime*

$$\begin{pmatrix} x_1' & y_1' & r_1' \\ x_2' & y_2' & r_2' \end{pmatrix} \tag{3.3}$$

matricą, gautą iš (3.2) *matricos, atlikus elementariąją operaciją. Tuomet* $ax_1' + by_1' = r_1'$ *ir* $ax_2' + by_2' = r_2'$*.*

Įrodymas. Nemažindami bendrumo tarkime, kad (3.3) matrica gauta iš (3.2) matricos, pirmą jos eilutę padauginus iš skaičiaus c ir pridėjus prie antros eilutės. Tuomet

$$\begin{pmatrix} x_1' & y_1' & r_1' \\ x_2' & y_2' & r_2' \end{pmatrix} = \begin{pmatrix} x_1 & y_1 & r_1 \\ x_2 + cx_1 & y_2 + cy_1 & r_2 + cr_1 \end{pmatrix}.$$

Kadangi $ax_1 + by_1 = r_1$ ir $ax_2 + by_2 = r_2$, tai

$$ax_1' + by_1' = ax_1 + by_1 = r_1 = r_1',$$

$$ax_2' + by_2' = a(x_2 + cx_1) + b(y_2 + cy_1) =$$

$$c(ax_1 + by_1) + ax_2 + by_2 = cr_1 + r_2 = r_2'.$$

□

Tarkime, kad reikia rasti skaičių $a_1 > 0$ ir $a_2 > 0$ didžiausią bendrąjį daliklį. Nagrinėkime matricą (skaičių lentelę)

$$\begin{pmatrix} 1 & 0 & a_1 \\ 0 & 1 & a_2 \end{pmatrix}. \tag{3.4}$$

Skaičių a_1 padalijame su liekana iš skaičiaus a_2: $a_1 = a_2b_2 + a_3$, $0 \leq a_3 < a_2$. Iš (3.4) matricos pirmosios eilutės atimame antrąją eilutę, padaugintą iš b_2 (elementarioji operacija). Gauname matricą

$$\begin{pmatrix} 1 & -b_2 & a_3 \\ 0 & 1 & a_2 \end{pmatrix}. \tag{3.5}$$

Sakykime, kad $a_3 > 0$ ir skaičių a_2 padalijame su liekana iš skaičiaus a_3: $a_2 = a_3b_3 + a_4$, $0 \leq a_4 < a_3$. Iš (3.5) matricos antrosios eilutės atimame pirmąją eilutę, padaugintą iš b_3 (elementarioji operacija). Gauname matricą

$$\begin{pmatrix} 1 & -b_2 & a_3 \\ -b_3 & 1 + b_2b_3 & a_4 \end{pmatrix}.$$

Šį dalybos procesą tęsiame, kol pirmą kartą matricos trečiame stulpelyje gausime nulį:

$$\begin{pmatrix} u & v & a_l \\ p & q & 0 \end{pmatrix}. \tag{3.6}$$

Nesunku įsitikinti, kad šios matricos skaičius a_l sutampa su Euklido algoritmo (žr. 3.2.1), pritaikyto skaičiams a_1 ir a_2, paskutine nenuline liekana, kuri lygi $\mathrm{dbd}(a_1, a_2)$. Taigi

$$a_l = \mathrm{dbd}(a_1, a_2).$$

(3.6) matrica gaunama iš (3.4) matricos, atliekant elementariąsias operacijas. Kadangi (3.4) matrica tenkina 3.2.7 teiginio sąlygą, tai ir (3.6) matrica tenkina šio teiginio sąlygą, todėl

$$a_1 u + a_2 v = a_l.$$

3.2.8 pavyzdys. Rasime skaičių 1147 ir 899 didžiausią bendrąjį daliklį ir jo tiesinę išraišką.

Sprendimas. Matricai

$$\begin{pmatrix} x_1 & y_1 & r_1 \\ x_2 & y_2 & r_2 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 899 \\ 0 & 1 & 1147 \end{pmatrix}$$

teisingos lygybės $899x_1 + 1147y_1 = 899$ ir $899x_2 + 1147y_2 = 1147$. Šioje matricoje atliekame elementariąsias operacijas:

$$\begin{pmatrix} 1 & 0 & 899 \\ 0 & 1 & 1147 \end{pmatrix} \Big\downarrow^{(-1)} \begin{pmatrix} 1 & 0 & 899 \\ -1 & 1 & 248 \end{pmatrix} \Big\uparrow_{(-3)} \begin{pmatrix} 4 & -3 & 155 \\ -1 & 1 & 248 \end{pmatrix} \Big\downarrow^{(-1)}$$

$$\begin{pmatrix} 4 & -3 & 155 \\ -5 & 4 & 93 \end{pmatrix} \Big\uparrow_{(-1)} \begin{pmatrix} 9 & -7 & 62 \\ -5 & 4 & 93 \end{pmatrix} \Big\downarrow^{(-1)} \begin{pmatrix} 9 & -7 & 62 \\ -14 & 11 & 31 \end{pmatrix} \Big\uparrow_{(-2)}$$

$$\begin{pmatrix} 37 & -29 & 0 \\ -14 & 11 & 31 \end{pmatrix}.$$

Taigi skaičius 31 yra skaičių 889 ir 1147 didžiausias bendrasis daliklis, kurio tiesinė išraiška, remiantis 3.2.7 teiginiu ir paskutine matrica, yra

$$899 \cdot (-14) + 1147 \cdot 11 = 31.$$

□

3.3 Pagrindinė aritmetikos teorema

3.3.1 apibrėžimas. Natūralusis skaičius $p > 1$ vadinamas *pirminiu*, jei skaičiai 1 ir p yra vieninteliai teigiami skaičiaus p dalikliai.

Taigi pats mažiausias pirminis skaičius yra 2. Skaičiai 3, 5, 7, 11, 13 yra pirminiai, o skaičius $15 = 3 \cdot 5$ nėra pirminis.

3.3.2 teorema. *Pirminių skaičių yra be galo daug.*

Įrodymas. Tarkime priešingai – kad pirminių skaičių aibė yra baigtinė. Tuomet egzistuoja toks skaičius N, kad kiekvienas pirminis skaičius yra ne didesnis už N. Nagrinėkime skaičių $N!+1$. Tegu $d > 1$ – mažiausias skaičiaus $N!+1$ daliklis. Tada d – pirminis skaičius. Vadinasi, $d \leq N$, todėl $d \mid N!$. Bet iš $d \mid N! + 1$ ir $d \mid N!$ gauname $d \mid N! + 1 - N! = 1$, t. y. $d = 1$. Prieštara. □

Įrodysime svarbią pirminių skaičių savybę.

3.3.3 teorema. *Jei pirminis skaičius p yra natūraliųjų skaičių a ir b sandaugos daliklis, tai p yra bent vieno skaičiaus a ar b daliklis.*

Įrodymas. Jei $p \mid a$, tai teoremos įrodymas baigtas. Jei $p \nmid a$, tai skaičių p ir a didžiausias bendrasis daliklis yra lygus 1. Vadinasi, remiantis anksčiau įrodyta išvada, egzistuoja tokie $u_1, u_2 \in \mathbb{Z}$, kad

$$1 = pu_1 + au_2.$$

Padauginę šią lygybę iš skaičiaus b, gauname

$$b = pbu_1 + abu_2.$$

Kadangi $p \mid p$, $p \mid ab$, tai, remiantis 8-ąja skaičių dalumo savybe, $p \mid pbu_1 + abu_2$, t. y. $p \mid b$. □

3.3.4 teorema (pagrindinė aritmetikos teorema)**.** *Kiekvienas natūralusis skaičius a, $a \neq 0$, vienareikšmiškai yra išskaidomas pirminių skaičių sandauga, jei nekreipiame dėmesio į dauginamųjų tvarką.*

Įrodymas. Pirmiausia matematinės indukcijos metodu įrodysime, kad kiekvienas natūralusis skaičius yra išskaidomas pirminių skaičių sandauga, o tada – išskaidymo vienatinumą.

Skaičiaus 1 skaidinys pirminiais skaičiais tuščias. Sakykime, kiekvienas natūralusis skaičius b, $1 < b < a$, yra išskaidomas pirminių skaičių sandauga. Įrodysime, kad ir skaičius a yra išskaidomas pirminių skaičių sandauga.

Galimi du atvejai: i) a – pirminis skaičius; ii) a – nėra pirminis skaičius. Pirmuoju atveju a išskaidytas pirminio skaičiaus sandauga. Antruoju atveju egzistuoja tokie natūralieji skaičiai $1 < a' < a$ ir $1 < a'' < a$, kad $a = a' \cdot a''$. Kadangi remiantis padaryta prielaida natūralieji skaičiai a' ir a'' yra išskaidomi pirminių skaičių sandauga, tai ir natūralusis skaičius a yra išskaidomas pirminių skaičių sandauga.

Vienatinumas. Natūraliojo skaičiaus skaidinio pirminių skaičių sandauga vienatinumą įrodysime matematinės indukcijos metodu.

Skaičiaus 1 skaidinys pirminiais skaičiais tuščias.

Sakykime, kad kiekvienas natūralusis skaičius a', $1 < a' < a$, vienareikšmiškai išskaidomas pirminių skaičių sandauga (indukcinė prielaida).

Įrodysime, kad ir skaičius a vienareikšmiškai išskaidomas pirminių skaičių sandauga.

Tarkime,

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot \dots \cdot q_s, \tag{3.7}$$

čia p_i, q_j, $1 \le i \le r$, $1 \le j \le s$, – pirminiai skaičiai. Įrodysime, kad $r = s$ ir $p_i = q_{j_i}$, $1 \le i \le r$, čia $j_1, j_2, \dots, j_r$ yra skaičių $1, 2, \dots, r$ perstatinys.

Kadangi $p_1 \mid a$, tai $p_1 \mid q_1 \cdot q_2 \cdot \dots \cdot q_s$. Jei $p_1 \ne q_1$, tai $p_1 \mid q_2 \cdot \dots \cdot q_s$. Pakartoję šį samprotavimą, gauname, kad egzistuoja toks j_1, kad $p_1 = q_{j_1}$. (3.7) lygybės abi puses suprastinę iš p_1, gauname:

$$a' = p_2 \cdot \dots \cdot p_r = q_1 \cdot \ldots \hat{q}_{j_1} \cdot \dots \cdot q_s,$$

čia stogelis virš q_{j_1}, t. y. $\hat{q}_{j_1}$ reiškia, kad pirminio skaičiaus q_{j_1} sandaugoje nėra. Kadangi $a' < a$, tai, remdamiesi indukcine prielaida, gauname: $r = s$, $p_i = q_{j_i}$, $2 \le i \le r$. □

3.3.5 pastaba. Kaip žinome, į skaičiaus 1 skaidinį neįeina nė vienas pirminis skaičius.

3.3.6 pastaba. Pirminis skaičius p skaičiaus a skaidinyje pirminiais skaičiais gali pasikartoti. Skaičiaus p pasikartojimų skaičius α skaičiaus a skaidinyje yra vadinamas pirminio skaičiaus p *kartotinumu.* Atsižvelgę į pirminių skaičių kartotinumus skaičiaus a skaidinyje pirminiais skaičiais, galime parašyti

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_m^{\alpha_m},$$

čia p_1, p_2, $\dots$, p_m – skirtingi pirminiai skaičiai, $\alpha_1 > 0$, $\alpha_2 > 0$, $\dots$, $\alpha_m > 0$ – jų kartotinumai. Šis vienintelis skaičiaus a skaidinys pirminiais skaičiais yra vadinama *kanoniniu skaidiniu* (*kanonine išraiška*). Analogiškai kiekvienas sveikasis skaičius $a \ne 0$ vienareikšmiškai yra užrašomas taip:

$$a = \pm p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_m^{\alpha_m}.$$

3.3.7 pastaba. Jei $a \ne 0$ yra racionalusis skaičius, tai jis vieninteliu būdu užrašomas taip:

$$a = \pm \frac{p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_r^{\alpha_r}}{q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \dots \cdot q_s^{\beta_s}},$$

čia p_1, p_2, $\dots$, p_r, q_1, q_2, $\dots$, q_s – skirtingi pirminiai skaičiai, $\alpha_1 > 0$, $\alpha_2 > 0$, $\dots$, $\alpha_r > 0$, $\beta_1 > 0$, $\beta_2 > 0$, $\dots$, $\beta_s > 0$ – natūralieji skaičiai. Tarus, kad sveikieji skaičiai $\alpha_1 \ne 0$, $\alpha_2 \ne 0$, $\dots$, $\alpha_t \ne 0$ gali būti tiek teigiami, tiek neigiami, racionaliojo skaičiaus $a \neq 0$ skaidinys pirminiais skaičiais gali būti užrašomas ir taip:

$$a = \pm p_1^{\alpha_1} \cdot p^{\alpha_2} \cdot \ldots \cdot p_t^{\alpha_t}.$$

Žymėjimai. Sutarkime naudoti tokius žymėjimus:

1. $a_1 + a_2 + \cdots + a_n = \sum_{j=1}^{n} a_j$.
2. $\binom{n}{j} = C_n^j = \frac{n!}{j!(n-j)!}, \quad 0 \leq j \leq n, \quad 0! = 1.$
3. Jei $\mathbf{j} = (j_1, j_2, \ldots, j_r),\ j_1,\ j_2, \ldots,\ j_r \geq 0$, tai $\mathbf{j}! = j_1! \cdot j_2! \cdot \cdots \cdot j_r!$.
4. $\binom{n}{\mathbf{j}} = \frac{n!}{\mathbf{j}!}$, čia $\mathbf{j} = (j_1, j_2, \ldots, j_r)$, $j_1 + j_2 + \cdots + j_r = n$.
5. Jei $\mathbf{j} = (j_1, j_2, \ldots, j_r),\ j_1,\ j_2, \ldots,\ j_r \geq 0$, $\mathbf{a} = (a_1, a_2, \ldots, a_r)$, tai

$$\mathbf{a}^{\mathbf{j}} = a_1^{j_1} \cdot a_2^{j_2} \cdot \cdots \cdot a_r^{j_r}.$$

Niutono binomo koeficientą $\binom{n}{j} = \frac{n!}{j!(n-j)!}, \quad 0 \leq j \leq n, \quad 0! = 1$, galima apibrėžti ir neigiamiems sveikiesiems skaičiams $-n$, čia $n > 0$. Tik šiuo atveju naudokimės tokia lygybe:

$$\binom{n}{j} = \frac{n \cdot (n-1) \cdot \cdots \cdot (n-j+1)}{j!}, \quad 0 \leq j \leq n.$$

Tuomet

$$\binom{-n}{j} = \frac{-n \cdot (-n-1) \cdot \cdots \cdot (-n-j+1)}{j!} =$$

$$(-1)^j \frac{(n+j-1) \cdot (n+j-2) \cdot \cdots \cdot n)}{j!} = (-1)^j \binom{n+j-1}{j}.$$

Pratimai.

1. Matematinės indukcijos metodu įrodykite Niutono binomo formulę:

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^j b^{n-j}.$$

2. Matematinės indukcijos metodu įrodykite formulę:

$$(a_1 + a_2 + \cdots + a_r)^n = \sum_{\substack{j_1,\ j_2, \ldots,\ j_r \geq 0 \\ j_1 + j_2 + \cdots + j_r = n}} \binom{n}{\mathbf{j}} \mathbf{a}^{\mathbf{j}},$$

čia $\mathbf{a} = (a_1, a_2, \ldots, a_r)$.

3. Matematinės indukcijos metodu įrodykite lygybę:

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

4. Raskite lygties $x_1 + x_2 + \cdots + x_n = N$ sveikaisiais neneigiamais skaičiais sprendinių skaičiaus formulę.

   Nurodymas: pirmiausia raskite ieškomos formulės išraišką, kai $n = 1$, $n = 2$, $n = 3$, tada pabandykite atspėti galutinę formulės išraišką ir matematinės indukcijos metodu įrodyti, kad ją atspėjote teisingai.

   4-ąjį pratimą galima spręsti ir kitaip. Lygties $x_1 + x_2 + \cdots + x_n = N$ sprendinių skaičius sveikaisiais neneigiamais skaičiais yra lygus nelygybės

$$x_1 + x_2 + \cdots + x_{n-1} \leq N \tag{3.8}$$

   sprendinių skaičiui sveikaisiais neneigiamais skaičiais. Tegu skaičių rinkinys $(a_1, a_2, \ldots, a_{n-1})$ yra 1-os nelygybės sprendinys. Sudarykime tokią skaičių seką:

$$1 \leq a_1 + 1 = b_1 < a_1 + a_2 + 2 = b_2 < \ldots$$
$$< a_1 + a_2 + \cdots + a_{n-1} = b_{n-1} \leq N + n - 1.$$

   Akivaizdu, kad, žinodami skaičių b_j, $1 \leq j \leq n-1$, seką

$$1 \leq b_1 < b_2 < \cdots < b_{n-1} \leq N + n - 1, \tag{3.9}$$

   vieninteliu būdu galime apibrėžti (3.8) nelygybės sprendinį $(a_1, a_2, \ldots, a_{n-1})$. Keliais būdais galime išrinkti skaičių b_j, $1 \leq j \leq n-1$, seką, tenkinančią (3.9) nelygybes? Galima ir kitaip paklausti: keliais būdais galime išrinkti $n-1$ skaičių iš $N+n-1$ skaičių? Atsakymas: $\binom{N+n-1}{n-1}$.

5. Tegu $|a| < 1$. Tuomet begalinės mažėjančios geometrinės progresijos

$$1, a, a^2, a^3, \ldots, a^n, \ldots$$

   narių suma yra lygi

$$\sum_{j=0}^{\infty} a^j = (1-a)^{-1}.$$

   Įrodykite, kad

$$(1-a)^{-n} = \sum_{j=0}^{\infty} \binom{-n}{j} (-1)^j a^j = \sum_{j=0}^{\infty} \binom{n+j-1}{j} a^j.$$

4 skyrius

Tiesinių lygčių sistemos

Nagrinėkime lygtį

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \tag{4.1}$$

čia $a_1, a_2, \ldots, a_n, b$ – fiksuoti realieji skaičiai, o $x_1, x_2, \ldots, x_n$ – kintamieji.

4.0.8 apibrėžimas. (4.1) lygtis vadinama *tiesine lygtimi*. Jei skaičius $b = 0$, tai ši lygtis vadinama *homogenine*. Realiųjų skaičių rinkinys $(c_1, c_2, \ldots, c_n)$ vadinamas (4.1) lygties *sprendiniu*, jei

$$a_1c_1 + a_2c_2 + \cdots + a_nc_n = b.$$

Tiesinių lygčių rinkinys

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \quad\cdots \quad \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{4.2}$$

vadinamas *tiesinių lygčių sistema*. Realieji skaičiai a_{ij} vadinami šios sistemos koeficientais, o skaičiai b_i – jos laisvaisiais nariais. Realiųjų skaičių rinkinys $(c_1, c_2, \ldots, c_n)$ vadinamas (4.2) sistemos *sprendiniu*, jei jis yra kiekvienos šios sistemos lygties sprendinys. Tiesinių lygčių sistema vadinama *suderinta*, jei ji turi bent vieną sprendinį. Dvi kintamųjų $x_1, x_2, \ldots, x_n$ tiesinių lygčių sistemos vadinamos *ekvivalenčiomis*, jei jų sprendinių aibės sutampa.

Tiesinių lygčių sistema, kurios visi laisvieji nariai yra nuliai, vadinama *homogenine*.

4.0.9 pavyzdys. Rinkinys $(2, 1)$ yra lygčių sistemos

$$\begin{cases} 3x + 2y = 8 \\ 2x - 3y = 1 \end{cases}$$

sprendinys.

4.0.10 pavyzdys. Lygčių sistema

$$\begin{cases} 3x + y = 2 \\ 3x + y = 1 \end{cases}$$

neturi sprendinių.

4.0.11 pavyzdys. Lygčių sistema

$$\begin{cases} 2x + y = 3 \\ 2x + y = 3 \end{cases}$$

turi be galo daug sprendinių. Visų sprendinių aibė yra

$$\{(x, 3 - 2x) \mid x \in \mathbb{R}\}.$$

4.0.12 teiginys. *Bet kuriai kintamųjų $x_1, x_2, \ldots, x_n$ tiesinių lygčių sistemai galimi tik šie atvejai:*

(i) sistema neturi sprendinių;

(ii) sistema turi tiktai vieną sprendinį;

(iii) sistema turi be galo daug sprendinių.

Įrodymas. Pakanka įrodyti, kad, jei sistema turi du skirtingus sprendinius, tai ji jų turi be galo daug. Iš tikrųjų, tarkime, kad realiųjų skaičių rinkiniai $(c_1, c_2, \ldots, c_n)$ ir $(c_1', c_2', \ldots, c_n')$ yra du skirtingi sistemos

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \cdots \quad \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{4.3}$$

sprendiniai. Tada rinkinys $(c_1 - c_1',\, c_2 - c_2',\, \ldots, c_n - c_n')$ yra homogeninių lygčių sistemos

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \cdots \quad \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases}$$

nenulinis sprendinys. Be to, kiekvienam $t \in \mathbb{R}$ rinkinys

$$\big((c_1 - c_1')t,\, (c_2 - c_2')t,\, \ldots,\, (c_n - c_n')t \big)$$

taip pat yra šios homogeninių lygčių sistemos sprendinys. Tada realiųjų skaičių rinkinys

$$\left(c_1 + (c_1 - c_1')t,\, c_2 + (c_2 - c_2')t,\, \ldots,\, c_n + (c_n - c_n')t \right)$$

su kiekvienu $t \in \mathbb{R}$ yra 4.3 lygčių sistemos sprendinys. Taigi 4.3 lygčių sistema turi be galo daug sprendinių. □

Lieka išsiaiškinti, kaip išspręsti bendrą tiesinių lygčių sistemą. Pirmiausia aptarsime, kaip bendrą tiesinių lygčių sistemą galima pertvarkyti į paprastesnę tiesinių lygčių sistemą taip, kad nagrinėjamos lygčių sistemos sprendinių aibė nepakistų. Tam pateiksime tiesinių lygčių sistemos elementariųjų pertvarkymų apibrėžimą.

4.0.13 apibrėžimas. Nagrinėkime tokius tiesinių lygčių sistemos pertvarkymus:

1. Sistemos lygtis padauginama iš nenulinio realaus skaičiaus.

2. Sistemos lygtis pakeičiama jos ir kitos lygties, padaugintos iš realaus skaičiaus, suma.

Šie pertvarkymai vadinami *elementariaisiais*.

4.0.14 teiginys. *Tiesinių lygčių sistemoje atliekant elementariuosius pertvarkymus sistemos sprendinių aibė nesikeičia. Kitaip sakant, jei viena tiesinių lygčių sistema gaunama iš kitos, atlikus baigtinį skaičių elementariųjų pertvarkymų, tai šios dvi sistemos yra ekvivalenčios.*

Įrodymas*.* Įrodymą paliekame skaitytojui. □

4.1 Gauso metodas

4.0.14 teiginiu paremtas tiesinių lygčių sistemų sprendimas Gauso metodu. Iš pradžių pateiksime šio metodo algoritmą (žr. 4.1.1 poskyrį), o tada (žr. 4.1.2 poskyrį) šį metodą paaiškinsime smulkiau.

4.1.1 Gauso metodas. Algoritmas

Algoritmas taikomas norint išspręsti bendrąją tiesinių lygčių sistemą. Išsirinkę vieną kurią nors lygtį, pavyzdžiui, pirmąją, ir joje kurį nors nežinomąjį, prie kurio esantis koeficientas nelygus nuliui, pavyzdžiui, x_1, sudarome naują sistemą. Šį pasirinktą nežinomąjį pašaliname iš kitų lygčių. Tai darome taip: pirmąją lygtį padauginame iš tokio skaičiaus, kad gautą padaugintą iš skaičiaus lygtį pridėję prie antros lygties gautume lygtį, kurioje nebeliktų pasirinkto eliminuoti nežinomojo. Tokiu pat būdu pasirinktas nežinomasis pašalinamas iš trečios ir visų kitų tolesnių lygčių. Padarę šiuos pertvarkymus gauname naują tiesinių lygčių sistemą, kurioje pasirinktas nežinomasis yra tik pirmoje lygtyje, o kitose lygtyse jo nebėra. Aprašytą nežinomojo eliminavimo procedūrą taikome naujai gautai tiesinių lygčių sistemai, išskyrus pirmąją lygtį. Pritaikę šiuos elementarius pertvarkymus pradinei tiesinių lygčių sistemai, gauname tiesinių lygčių sistemą, ekvivalenčią pradinei ir turinčią pavidalą

$$\begin{cases} a_{11}x_1 + \ldots + a_{1k_2}x_{k_2} + \ldots + a_{1k_r}x_{k_r} + \ldots + a_{1n}x_n = b_1, \\ \qquad a'_{2k_2}x_{k_2} + \ldots + a'_{2k_r}x_{k_r} + \ldots + a'_{2n}x_n = b'_2, \\ \qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \qquad\qquad a'_{p_rk_r}x_{k_r} + \ldots + a'_{p_rn}x_n = b'_{p_r}, \\ \qquad\qquad\qquad 0 = b'_{p_r+1}, . \\ \qquad\qquad\qquad \ldots\ldots \\ \qquad\qquad\qquad 0 = b'_l, \\ \qquad\qquad\qquad \ldots\ldots \\ \qquad\qquad\qquad 0 = b'_m. \end{cases}$$

Jei, spręsdami konkrečią lygčių sistemą, kuriame nors žingsnyje gauname lygtį $0 = 0$, tai ją iš sistemos išmetame. Jei kuriame nors žingsnyje gauname lygtį $0 = \alpha$, o $\alpha \neq 0$, tai baigiame spręsti lygčių sistemą ir padarome išvadą, kad lygčių sistema neturi sprendinių. Atsižvelgus į šias pastabas, sakykime, paskutinė netriviali pertvarkytos sistemos lygtis būtų

$$a'_{p_rk_r}x_{k_r} + \ldots + a'_{p_rn}x_n = b'_{p_r},$$

čia $a'_{p_rk_r} \neq 0$. Gautą tiesinių lygčių sistemą pradedama spręsti nuo nurodytos paskutinės lygties. Kadangi $a'_{p_rk_r} \neq 0$, kintamąjį x_{k_r} iš pakutinės lygties išreiškiame kintamaisiais x_j, $j > k_r$. Į priešpaskutinę lygtį įrašome kintamojo x_{k_r} išraišką kintamaisiais x_j, $j > k_r$. Kadangi $a'_{p_r-1k_{r-1}} \neq 0$, priešpaskutinėje lygtyje kintamąjį $x_{k_{r-1}}$ išreiškiame kintamaisiais x_j, $j > k_{r-1}$, tarp kurių jau nėra kintamojo x_{k_r}. Tęsdami šią procedūrą, gausime kintamųjų

$$x_1, x_{k_2}, \ldots, x_{k_r}$$

išraiškas likusiais kintamaisiais

$$x_j,\ j \neq k_1,\ \ldots, k_r,\ \text{čia } k_1 = 1.$$

Surašome visus kintamuosius į n ilgio rinkinį: į j-ąją vietą įrašome x_j, jei

$$j \neq k_1,\ \ldots, k_r,\ \text{čia } k_1 = 1,$$

o į k_j vietas, čia $1 \leq j \leq r$, surašome kintamųjų x_{k_j}, $1 \leq j \leq r$, išraiškas kintamaisiais

$$x_j,\ j \neq k_1,\ \ldots, k_r,\ \text{čia } k_1 = 1.$$

Gautas n ilgio rinkinys yra nagrinėjamos tiesinių lygčių sistemos bendrasis sprendinys. Kintamieji

$$x_j,\ j \neq k_1,\ \ldots, k_r,\ \text{čia } k_1 = 1,$$

yra vadinami laisvaisiais parametrais. Laisviesiems parametrams galima suteikti bet kurias skaitines reikšmes. Suteikę laisviesiems parametrams, kurių yra $n - r$, kurias nors konkrečias reikšmes, gauname nagrinėjamos tiesinių lygčių sistemos konkretų sprendinį.

4.1.1 pastaba. Pažymėtina, kad laisvų parametrų pasirinkimas nėra vienareikšmiškas. Tai priklauso nuo pasirinktų eliminuoti nežinomųjų. Bet sprendinių visuma, suteikint laisviesiems parametrams visas galimas reikšmes iš nagrinėjamos skaitinės srities, visais atvejais gaunama ta pati. Be to, skaičiai r ir $n-r$ taip pat nesikeičia sprendžiant Gauso algoritmu, nepriklausomai nuo to, kurie kintamieji būtų pasirinkti eliminuoti.

4.1.2 pastaba. Aprašytas algoritmas vadinamas įžymaus vokiečių matematiko Gauso (C. F. Gauss) vardu. Gausas buvo tituluojamas matematikų karaliumi.

4.1.2 Gauso metodas. Trapecinė lygčių sistema

4.1.3 apibrėžimas. Tiesinių lygčių sistema

$$\left\{\begin{array}{r} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1r}x_r + \cdots + a_{1n}x_n = b_1 \\ a_{22}x_2 + \cdots + a_{2r}x_r + \cdots + a_{2n}x_n = b_2 \\ \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \\ a_{rr}x_r + \cdots + a_{rn}x_n = b_r \\ 0 = b_{r+1} \\ \cdots\ \cdots \\ 0 = b_m \end{array}\right. , \tag{4.4}$$

kurioje $r = 0$ arba $r \geq 1$ ir $a_{11}a_{22} \cdot \ldots \cdot a_{rr} \neq 0$, vadinama *trapecine*. Jei $r = n$, tai ši lygčių sistema vadinama *trikampe*, o jei $r < n$, tai – *griežtai trapecine.*

4.1.4 pavyzdys. Lygčių sistema

$$\left\{\begin{array}{r} x_1 + 3x_2 - 5x_3 + 7x_4 = 5 \\ 3x_2 + 2x_3 + 2x_4 = 1 \\ 4x_3 + 9x_4 = 6 \end{array}\right.$$

yra griežtai trapecinė ($r = 3 < 4 = n$); lygčių sistema

$$\begin{cases} x_1 + 3x_2 - 5x_3 = 5 \\ \qquad 3x_2 + 2x_3 = 1 \\ \qquad\qquad 4x_3 = 6 \end{cases}$$

yra trikampė, o lygčių sistema

$$\begin{cases} x_1 + 2x_2 - 6x_3 + 3x_4 = 5 \\ \qquad x_2 + 2x_3 + 2x_4 = 4 \\ \qquad\qquad\qquad 2x_4 = 3 \end{cases}$$

nėra trapecinė (ir nėra trikampė). Šioje sistemoje, sukeitę kintamuosius x_3 ir x_4 vietomis, gausime griežtai trapecinę tiesinių lygčių sistemą

$$\begin{cases} x_1 + 2x_2 + 3x_4 - 6x_3 = 5 \\ \qquad x_2 + 2x_4 + 2x_3 = 4 \\ \qquad\qquad 2x_4 \qquad\quad = 3 \end{cases} .$$

4.1.5 teorema. *Kiekviena tiesinių lygčių sistema yra ekvivalenti (pakeitus galbūt kintamųjų tvarką) tam tikrai trapecinei tiesinių lygčių sistemai.*

Įrodymas. Teoremą įrodysime matematinės indukcijos būdu pagal sistemos lygčių skaičių m. Iš tikrųjų, įrodysime, kad kiekvieną tiesinių lygčių sistemą, atlikus baigtinį skaičių elementariųjų pertvarkymų, galima užrašyti kaip trapecinę lygčių sistemą.

Jei $m = 1$, tai turime sistemą iš vienos lygties. Tokia sistema yra trapecinė.

Tarkime, kad bet kurią tiesinių lygčių sistemą, kurioje yra $m - 1$ ($m \geq 2$) arba mažiau lygčių, atlikus baigtinį skaičių elementariųjų pertvarkymų, galima užrašyti kaip trapecinę lygčių sistemą.

Nagrinėkime tiesinių lygčių sistemą iš m ($m \geq 2$) lygčių:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \qquad \cdots \quad \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases} . \tag{4.5}$$

Jei šios sistemos visi koeficientai lygūs nuliui, tai ji yra trapecinė. Todėl toliau laikysime, kad bent vienas šios sistemos koeficientas yra nenulinis. Nemažindami bendrumo galime laikyti, kad bent vienas iš kintamojo x_1 koeficientų a_{11}, a_{21}, $\ldots$, a_{m1} yra nenulinis (priešingu atveju galime sukeisti kintamųjų tvarką). Kadangi lygčių tvarką sistemoje galime laisvai keisti (nuo to sistemos sprendinių aibė nesikeičia), tai laikysime, kad koeficientas $a_{11} \neq 0$.

Prie antrosios (4.5) sistemos lygties pridėję pirmąją, padaugintą iš skaičiaus $-a_{21}/a_{11}$, gauname lygčių sistemą

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ \qquad\qquad a'_{22}x_2 + \cdots + a'_{2n}x_n = b'_2 \\ a_{31}x_1 + a_{32}x_2 + \cdots + a_{3n}x_n = b_3 \\ \qquad\qquad \cdots \quad \cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases},$$

čia $a'_{2j} = a_{2j} - a_{21}a_{1j}/a_{11}$, $b'_2 = b_2 - a_{21}b_1/a_{11}$. Tą patį atlikę su trečiąja, ketvirtąja ir t. t. šios sistemos lygtimis, gauname sistemą

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ \qquad\qquad a'_{22}x_2 + \cdots + a'_{2n}x_n = b'_2 \\ \qquad\qquad a'_{32}x_2 + \cdots + a'_{3n}x_n = b'_3 \\ \qquad\qquad \cdots \quad \cdots \\ \qquad\qquad a'_{m2}x_2 + \cdots + a'_{mn}x_n = b'_m \end{cases}, \tag{4.6}$$

kuri, remiantis 4.0.14 teiginiu, yra ekvivalenti (4.5) lygčių sistemai.

Tiesinių lygčių sistema

$$\begin{cases} a'_{22}x_2 + \cdots + a'_{2n}x_n = b'_2 \\ a'_{32}x_2 + \cdots + a'_{3n}x_n = b'_3 \\ \qquad \cdots \quad \cdots \\ a'_{m2}x_2 + \cdots + a'_{mn}x_n = b'_m \end{cases}$$

turi mažiau nei m lygčių, todėl, remiantis indukcijos prielaida, atlikus baigtinį skaičių elementariųjų pertvarkymų (ir galbūt pakeitus kintamųjų tvarką), ši lygčių sistema užrašoma kaip jai ekvivalenti trapecinė sistema

$$\begin{cases} a''_{22}x_2 + \cdots + a''_{2r}x_r + \cdots + a''_{2n}x_n = b''_2 \\ \qquad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \quad \cdots \\ \qquad\qquad a''_{rr}x_r + \cdots + a''_{rn}x_n = b''_r \\ \qquad\qquad\qquad\qquad 0 = b''_{r+1} \\ \qquad\qquad\qquad\qquad \cdots \quad \cdots \\ \qquad\qquad\qquad\qquad 0 = b''_m \end{cases}.$$

Taigi (4.5) lygčių sistema ekvivalenti trapecinei lygčių sistemai

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1r}x_r + \cdots + a_{1n}x_n = b_1 \\ \qquad a''_{22}x_2 + \cdots + a''_{2r}x_r + \cdots + a''_{2n}x_n = b''_2 \\ \qquad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ \qquad\qquad a''_{rr}x_r + \cdots + a''_{rn}x_n = b''_r \, . \\ \qquad\qquad\qquad 0 = b''_{r+1} \\ \qquad\qquad\qquad \ldots \; \ldots \\ \qquad\qquad\qquad 0 = b''_m \end{cases}$$

□

Vadinasi, iš 4.1.5 teoremos įrodymo išplaukia, kad bet kurią tiesinių lygčių sistemą, atlikus baigtinį skaičių elementariųjų pertvarkymų, visada galima užrašyti kaip jai ekvivalenčią trapecinę tiesinių lygčių sistemą. Tai ir yra *Gauso metodo* esmė.

Suformuluosime dvi išvadas, kurias įrodyti paliekame skaitytojui.

4.1.6 išvada. *Teisingi tokie teiginiai:*

(i) (4.4) *trapecinė tiesinių lygčių sistema turi sprendinių tada ir tik tada, kai* $b_{r+1} = b_{r+2} = \ldots = b_m = 0$.

(ii) (4.4) *trapecinė tiesinių lygčių sistema turi vienintelį sprendinį tada ir tik tada, kai ji yra trikampė ir* $b_{r+1} = b_{r+2} = \ldots = b_m = 0$.

(iii) (4.4) *trapecinė tiesinių lygčių sistema turi be galo daug sprendinių tada ir tik tada, kai ji yra griežtai trapecinė ir* $b_{r+1} = b_{r+2} = \ldots = b_m = 0$.

4.1.7 išvada. *Tiesinių homogeninių lygčių sistema, kurioje kintamųjų yra daugiau nei lygčių, turi be galo daug sprendinių.*

4.2 Pavyzdžiai

4.2.1 pavyzdys. Kadangi tiesinių homogeninių lygčių sistema

$$\begin{cases} x_1 + x_2 + 6x_3 + x_4 = 0 \\ 2x_1 + 3x_2 + 3x_3 + 2x_4 = 0 \\ x_1 + 2x_2 + 4x_3 + 7x_4 = 0 \end{cases}$$

kintamųjų turi daugiau nei lygčių, tai jos sprendinių aibė yra begalinė. Vadinasi, ši sistema turi nenulinį sprendinį.

4.2.2 pavyzdys. Jei tiesinių lygčių sistema turi be galo daug sprendinių, tai, remiantis 4.1.6 išvada, ji ekvivalenti griežtai trapecinei lygčių sistemai

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1r}x_r + a_{1r+1}x_{r+1} + \cdots + a_{1n}x_n = b_1 \\ \qquad\quad a_{22}x_2 + \cdots + a_{2r}x_r + a_{2r+1}x_{r+1} + \cdots + a_{2n}x_n = b_2 \\ \qquad\qquad\qquad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ \qquad\qquad\qquad\quad a_{rr}x_r + a_{rr+1}x_{r+1} + \cdots + a_{rn}x_n = b_r \end{cases},$$

čia $a_{11}a_{22}\cdots a_{rr} \neq 0$ ir $r < n$. Šią lygčių sistemą perrašykime taip:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1r}x_r = b_1 - a_{1r+1}x_{r+1} - \cdots - a_{1n}x_n \\ \qquad\quad a_{22}x_2 + \cdots + a_{2r}x_r = b_2 - a_{2r+1}x_{r+1} - \cdots - a_{2n}x_n \\ \qquad\qquad\qquad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ \qquad\qquad\qquad\quad a_{rr}x_r = b_r - a_{rr+1}x_{r+1} - \cdots - a_{rn}x_n \end{cases}.$$

Gauta sistema kintamųjų $x_1, x_2, \ldots, x_r$ atžvilgiu yra trikampė, todėl šie kintamieji vienareikšmiškai išreiškiami kintamaisiais $x_{r+1}, x_{r+2}, \ldots, x_n$:

$$\begin{cases} x_1 = b'_1 + a'_{1r+1}x_{r+1} + \cdots + a'_{1n}x_n \\ x_2 = b'_2 + a'_{2r+1}x_{r+1} + \cdots + a'_{2n}x_n \\ \qquad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ x_r = b'_r + a'_{rr+1}x_{r+1} + \cdots + a'_{rn}x_n \end{cases}.$$

Šios lygybės ir nusako pradinės lygčių sistemos sprendinius (kintamuosius x_{r+1}, x_{r+2}, $\ldots$, x_n laikome parametrais, kurių reikšmes galima pasirinkti laisvai).

Dabar parodysime, kaip spręsti tiesinių lygčių sistemas Gauso metodu.

4.2.3 pavyzdys. Išspręsime lygčių sistemą Gauso metodu:

$$\begin{cases} x_1 + x_2 + 2x_3 + x_4 = 7 \\ 3x_1 + 4x_2 + 8x_3 + 5x_4 = 29 \\ x_1 + 3x_2 + 7x_3 + 8x_4 = 30 \\ 2x_1 + 2x_2 + 5x_3 + 6x_4 = 23 \end{cases}. \tag{4.7}$$

Pirmame etape iš 2-osios, 3-iosios ir 4-osios lygčių pašalinsime kintamąjį x_1: pirmąją lygtį padauginsime iš -3 ir pridėsime prie 2-osios; pirmąją lygtį padauginsime iš -1 ir pridėsime prie 3-iosios; pirmąją lygtį padauginsime iš -2 ir pridėsime prie 4-osios :

$$\begin{cases} x_1 + x_2 + 2x_3 + x_4 = 7 & {\scriptstyle (-3)} \quad {\scriptstyle (-1)} \quad {\scriptstyle (-2)} \\ 3x_1 + 4x_2 + 8x_3 + 5x_4 = 29 \\ x_1 + 3x_2 + 7x_3 + 8x_4 = 30 \\ 2x_1 + 2x_2 + 5x_3 + 6x_4 = 23 \end{cases}$$

$$
\left\{\begin{array}{rl}
x_1 + x_2 + 2x_3 + x_4 & = 7 \\
x_2 + 2x_3 + 2x_4 & = 8 \quad (-2) \\
2x_2 + 5x_3 + 7x_4 & = 23 \\
x_3 + 4x_4 & = 9
\end{array}\right.
\qquad
\left\{\begin{array}{rl}
x_1 + x_2 + 2x_3 + x_4 & = 7 \\
x_2 + 2x_3 + 2x_4 & = 8 \\
x_3 + 3x_4 & = 7 \quad (-1) \\
x_3 + 4x_4 & = 9
\end{array}\right.
$$

$$
\left\{\begin{array}{rl}
x_1 + x_2 + 2x_3 + x_4 & = 7 \\
x_2 + 2x_3 + 2x_4 & = 8 \\
x_3 + 3x_4 & = 7 \\
x_4 & = 2\,.
\end{array}\right. .
$$

Ši trikampė lygčių sistema ir yra Gauso metodo tikslas. Šioje sistemoje, nuo apačios kildami aukštyn, suskaičiuojame visus kintamuosius: iš 4-os lygties $x_4 = 2$ statome į 3-iąją, gauname $x_3 = 1$, šias reikšmes statome į 2-ąją lygtį ir gauname $x_2 = 2$. Galiausiai iš 1-osios lygties gauname $x_1 = 1$. Taigi (4.8) sistema turi vienintelį sprendinį $(1, 2, 1, 2)$.

4.2.4 pavyzdys. Išspręsime lygčių sistemą Gauso metodu:

$$
\left\{\begin{array}{rl}
x_1 + 2x_2 + x_3 + x_4 & = 1 \quad (-2)\ (-1)\ (-3) \\
2x_1 + 5x_2 + 4x_3 + 5x_4 & = 4 \\
x_1 + 4x_2 + 6x_3 + 10x_4 & = 6 \\
3x_1 + 7x_2 + 6x_3 + 9x_4 & = 7
\end{array}\right. \tag{4.8}
$$

$$
\left\{\begin{array}{rl}
x_1 + 2x_2 + x_3 + x_4 & = 1 \\
x_2 + 2x_3 + 3x_4 & = 2 \quad (-2)\ (-1) \\
2x_2 + 5x_3 + 9x_4 & = 5 \\
x_2 + 3x_3 + 6x_4 & = 4
\end{array}\right.
\qquad
\left\{\begin{array}{rl}
x_1 + 2x_2 + x_3 + x_4 & = 1 \\
x_2 + 2x_3 + 3x_4 & = 2 \\
x_3 + 3x_4 & = 1 \quad (-1) \\
x_3 + 3x_4 & = 2
\end{array}\right.
$$

$$
\left\{\begin{array}{rl}
x_1 + 2x_2 + x_3 + x_4 & = 1 \\
x_2 + 2x_3 + 3x_4 & = 2 \\
x_3 + 3x_4 & = 1 \\
0 & = 1\,.
\end{array}\right. .
$$

Taigi iš 4-osios lygties matome, kad sistema sprendinių neturi.

4.2.5 pavyzdys. Išspręsime lygčių sistemą Gauso metodu:

$$
\left\{\begin{array}{rl}
x_1 + 3x_2 + x_3 + 2x_4 & = 7 \quad (-2)\ (-4)\ (-3) \\
2x_1 + 7x_2 + 4x_3 + 5x_4 & = 18 \\
4x_1 + 14x_2 + 9x_3 + 11x_4 & = 38 \\
3x_1 + 12x_2 + 10x_3 + 10x_4 & = 35
\end{array}\right.
$$

$$
\left\{\begin{array}{rl}
x_1 + 3x_2 + x_3 + 2x_4 & = 7 \\
x_2 + 2x_3 + x_4 & = 4 \quad (-2)\ (-3) \\
2x_2 + 5x_3 + 3x_4 & = 10 \\
3x_2 + 7x_3 + 4x_4 & = 14
\end{array}\right.
\qquad
\left\{\begin{array}{rl}
x_1 + 3x_2 + x_3 + 2x_4 & = 7 \\
x_2 + 2x_3 + x_4 & = 4 \\
x_3 + x_4 & = 2 \quad (-1) \\
x_3 + x_4 & = 2
\end{array}\right.
$$

$$\begin{cases} x_1 + 3x_2 + x_3 + 2x_4 & = 7 \\ x_2 + 2x_3 + x_4 & = 4 \\ x_3 + x_4 & = 2\,. \end{cases} .$$

Gavome griežtai trapecinę tiesinių lygčių sistemą. Vadinasi, sistema turės be galo daug sprendinių (žr. 4.1.6 išvadą). Užrašysime visus sistemos sprendinius. Paskutinę lygčių sistemą perrašykime taip:

$$\begin{cases} x_1 + 3x_2 + x_3 & = 7 - 2x_4 \\ x_2 + 2x_3 & = 4 - x_4 \\ x_3 & = 2 - x_4 \end{cases} .$$

Jei kintamąjį x_4 laikysime parametru, tai ši lygčių sistema (kintamųjų x_1, x_2 ir x_3 atžvilgiu) yra trikampė, todėl kintamieji x_1, x_2 ir x_3 vienareikšmiškai išreiškiami parametru x_4: $x_3 = 2-x_4$, $x_2 = x_4$ ir $x_1 = 5-4x_4$. Taigi visi sistemos sprendiniai sudaro aibę

$$\{(5-4x_4,\, x_4,\, 2-x_4,\, x_4) \mid x_4 \in \mathbb{R}\}\,.$$

4.3 Tiesinių lygčių sistemos sprendinių aibės sandara

Nagrinėkime bendrą tiesinių lygčių sistemą

$$\begin{cases} a_{11}x_1 \;+ a_{12}x_2 \;+ \ldots \;+ a_{1n}x_n = b_1 \\ a_{21}x_1 \;+ a_{22}x_2 \;+ \ldots \;+ a_{2n}x_n = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{cases} . \tag{4.9}$$

Bet kuriems dviem šios sistemos sprendiniams

$$u = (c_1, c_2, \ldots, c_n) \quad \text{ir} \quad v = (c'_1, c'_2, \ldots, c'_n)$$

pažymėkime

$$u + v := (c_1 + c'_1, c_2 + c'_2, \ldots, c_n + c'_n)$$

ir

$$u - v := (c_1 - c'_1, c_2 - c'_2, \ldots, c_n - c'_n).$$

Nesunku įsitikinti, kad minėtos sistemos bet kurių dviejų sprendinių u ir v skirtumas $u - v$ yra tiesinių homogeninių lygčių sistemos

$$\begin{cases} a_{11}x_1 \;+ a_{12}x_2 \;+ \ldots \;+ a_{1n}x_n = 0 \\ a_{21}x_1 \;+ a_{22}x_2 \;+ \ldots \;+ a_{2n}x_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = 0 \end{cases} \tag{4.10}$$

sprendinys. Iš tikrųjų, kadangi $u = (c_1, c_2, \ldots, c_n)$ ir $v = (c'_1, c'_2, \ldots, c'_n)$ yra (4.9) lygčių sistemos sprendiniai, tai bet kuriam $i \in \{1, 2, \ldots, m\}$ teisingos lygybės

$$a_{i1}c_1 \ + a_{i2}c_2 \ + \ldots \ + a_{in}c_n = b_i$$

ir

$$a_{i1}c'_1 \ + a_{i2}c'_2 \ + \ldots \ + a_{in}c'_n = b_i.$$

Iš pirmosios lygybės atėmę antrąją, gauname

$$a_{i1}(c_1 - c'_1) \ + a_{i2}(c_2 - c'_2) \ + \ldots \ + a_{in}(c_n - c'_n) = 0, \quad 1 \le i \le m.$$

Vadinasi, rinkinys

$$u - v = (c_1 - c'_1, c_2 - c'_2, \ldots, c_n - c'_n)$$

yra (4.10) homogeninių lygčių sistemos sprendinys.

Panašiai galima įsitikinti, kad bet kurio (4.9) lygčių sistemos sprendinio

$$u = (c_1, c_2, \ldots, c_n)$$

ir bet kurio (4.10) homogeninių lygčių sistemos sprendinio

$$h = (h_1, h_2, \ldots, h_n)$$

suma

$$u + h = (c_1 + h_1, c_2 + h_2, \ldots, c_n + h_n)$$

yra (4.9) lygčių sistemos sprendinys.

Taigi teisinga tokia teorema (bendros tiesinių lygčių sistemos sprendinių sandara):

4.3.1 teorema. *Bendros tiesinių lygčių sistemos*

$$\begin{cases} a_{11}x_1 \ + a_{12}x_2 \ + \ldots \ + a_{1n}x_n = b_1 \\ a_{21}x_1 \ + a_{22}x_2 \ + \ldots \ + a_{2n}x_n = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{cases}$$

sprendinių aibė S yra gaunama prie atskiro šios sistemos sprendinio (jei bent vienas toks sprendinys egzistuoja) pridėjus atitinkamos tiesinių homogeninių lygčių sistemos (4.10 sistemos) sprendinius. Simboliškai galime užrašyti taip:

$$S = v_0 + V := \{v_0 + v \mid v \in V\},$$

čia v_0 – atskiras bendros tiesinių lygčių sistemos sprendinys, o V – atitinkamos tiesinių homogeninių lygčių sistemos sprendinių aibė.

Taigi ši teorema tvirtina, kad žinant bent vieną tiesinių lygčių sistemos sprendinį, toliau užtenka nagrinėti atitinkamą homogeninių lygčių sistemą. Tiesinių homogeninių lygčių sistemos sprendinių struktūrai nusakyti reikia tiesinės erdvės, jos dimensijos ir matricos rango sąvokų. Jos yra išdėstytos antrojoje vadovėlio dalyje. Todėl ir teoremą, nusakančią homogeninių lygčių sistemos sprendinius, įrodysime antrojoje knygos dalyje. Čia pateikiame tik šios teoremos formuluotę:

4.3.2 teorema. *Tiesinių homogeninių lygčių sistemos*

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = 0 \end{cases}$$

sprendinių tiesinės erdvės V dimensija

$$\dim_{\mathbb{R}} V = n - \operatorname{rg} A,$$

čia $\operatorname{rg} A$ *– matricos $A := (a_{ij})$ rangas.*

Taip pat pateikiame Kronekerio-Kapelio teoremą be įrodymo (jos įrodymą galima rasti vadovėlio antrojoje dalyje):

4.3.3 teorema (Kronekerio-Kapelio)**.** *Tiesinių lygčių sistema*

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m \end{cases}$$

yra suderinta (turi bent vieną sprendinį) tada ir tik tada, kai šios sistemos matricos

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

rangas sutampa su išplėstinės matricos

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} & b_1 \\ a_{21} & a_{22} & \cdots & a_{2n} & b_2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} & b_m \end{pmatrix}$$

rangu.

5 skyrius

Grupės

5.1 Bendros sąvokos

Šiame skyriuje nagrinėsime grupes, vieną iš labai svarbių algebrinių struktūrų, apibrėžiamų vienu aibės elementų vidiniu kompozicijos dėsniu, tenkinančiu tam tikras aksiomas. Tai paprasčiausias atvejis ta prasme, kad struktūra aibėje yra apibrėžiama vienu kompozicijos dėsniu.

5.1.1 apibrėžimas. Aibė G joje apibrėžto kompozicijos dėsnio $*$ atžvilgiu yra vadinama *grupe*, jei

1. Kompozicijos dėsnis $*$ yra asociatyvus, t. y. bet kuriems g_1, g_2, $g_3 \in G$, teisinga lygybė
$$(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3).$$

2. Egzistuoja *neutralus elementas* $1 \in G$ kompozicijos dėsnio $*$ atžvilgiu, t. y. kiekvienam $g \in G$ teisinga lygybė
$$1 * g = g * 1 = g.$$
Elementas 1 yra vadinamas grupės *vienetu* ir, kaip žinome (žr.2.5.2), yra vienintelis.

3. Kiekvienam elementui $g \in G$ egzistuoja simetrinis elementas g^{-1} kompozicijos dėsnio $*$ atžvilgiu:
$$g * g^{-1} = g^{-1} * g = 1.$$
Elementas g^{-1} yra vadinamas *atvirkštiniu elementu* elementui g ir, kaip žinome (žr.2.5.8), yra vienintelis.

5.1.2 apibrėžimas. Grupė $(G, *)$ yra vadinama *komutatyviąja* (arba *Abelio*) grupe, jei kompozicijos dėsnis $*$ yra komutatyvus, t. y. bet kuriems $g_1, g_2 \in G$, teisinga lygybė $g_1 * g_2 = g_2 * g_1$.

Abelio grupės sudaro svarbią grupių klasę, bet grupės, vaidinančios ypatingą vaidmenį teorinėje fizikoje, fizikinės chemijos, kristalų bei kitose teorijose, jau nekalbant apie matematiką, beveik be išimčių yra nekomutatyvios. Todėl apsiriboti tik komutatyviosiomis grupėmis netikslinga.

Grupės apibrėžime 2-ąją ir 3-iąją aksiomas galima pakeisti silpnesnėmis.

5.1.3 apibrėžimas (antrasis grupės apibrėžimas)**.** Aibė G joje apibrėžto jos elementų kompozicijos dėsnio $*$ atžvilgiu vadinama grupe, jei

1'. Kompozicijos dėsnis $*$ yra asociatyvus.

2'. Egzistuoja toks aibės G elementas e, kad kiekvienam $g \in G$

$$e * g = g.$$

Šiuo atveju e yra vadinamas kairiuoju grupės vienetu.

3'. Kiekvienam aibės G elementui g egzistuoja toks aibės G elementas h, kad

$$h * g = e.$$

Šiuo atveju h yra vadinamas kairiuoju atvirkštiniu elementu elementui g.

5.1.4. Įrodysime, kad šie grupės apibrėžimai yra ekvivalentūs. Visiškai akivaizdu, kad jei $(G, *)$ yra grupė pirmojo apibrėžimo prasme, tai $(G, *)$ yra grupė ir antrojo apibrėžimo prasme. Atvirkščiojo teiginio įrodymą sudaro keleto atskirų teiginių įrodymai.

5.1.5 teiginys. *Jei $(G, *)$ yra grupė antrojo apibrėžimo prasme, tai lygties $x * x = x$ sprendinys grupėje $(G, *)$ yra $x = e$.*

Įrodymas. Jei grupės $(G, *)$ elementas x tenkina sąlygą $x * x = x$, tai šios lygybės abi puses iš kairės padauginę iš elementui x kairiojo atvirkštinio elemento y, gauname: $y * (x * x) = y * x$. Bet $y * (x * x) = (y * x) * x = e * x = x$, o $y * x = e$. Vadinasi, $x = e$. □

5.1.6 teiginys. *Jei $(G, *)$ yra grupė antrojo apibrėžimo prasme, tai kiekvienam $g \in G$*

1. *$g * e = g$(kitaip tariant, e yra grupės vienetas).*

2. *Jei h yra kairysis atvirkštinis elementas elementui g, tai h yra ir dešinysis atvirkštinis elementas elementui g.*

Įrodymas. Pirmiausia įrodysime antrąją teiginio dalį. Jei h yra kairysis atvirkštinis elementas elementui g, tai galime parašyti lygybes:

$$g * h = g * e * h = g * (h * g) * h = (g * h) * (g * h),$$

t. y. elementas $g * h$ tenkina sąlygą: $(g * h) * (g * h) = g * h$. Remdamiesi 5.1.5 teiginiu, gauname, kad $g * h = e$. Vadinasi, h yra tiek kairysis, tiek dešinysis atvirkštinis elementas elementui g.

Dabar įrodysime pirmąją teiginio dalį. Remdamiesi 2-ąja įrodyta teiginio dalimi, galime parašyti:

$$g * e = g * (h * g) = (g * h) * g = e * g = g,$$

t. y. $g * e = g$, čia h – atvirkštinis elementas elementui g. □

5.1.7 (dviejų grupės apibrėžimų ekvivalentumas)**.** Taigi grupės $(G, *)$ antrojo apibrėžimo prasme kairysis vienetas e tenkina pirmojo grupės apibrėžimo 2-ąją aksiomą, o elementui g kairysis atvirkštinis elementas h tenkina pirmojo grupės apibrėžimo 3-iąją aksiomą. Todėl abu grupės apibrėžimai yra ekvivalentūs.

Būtų galima pateikti ir trečiąjį grupės apibrėžimą, antrajame žodį „kairysis“pakeitus žodžiu „dešinysis“, ir įrodyti visų apibrėžimų ekvivalentumą. Tai padaryti paliekame skaitytojui.

Įrodysime paprastą faktą.

5.1.8 teiginys. *Tarkime, $(G, *)$ – grupė, $g, h \in G$. Tuomet $(g * h)^{-1} = h^{-1} * g^{-1}$.*

Įrodymas. Elementas $(g * h)^{-1}$ yra atvirkštinis elementui $g * h$. Įsitikinsime, kad ir $h^{-1} * g^{-1}$ taip pat yra atvirkštinis elementas elementui $g * h$. Iš tikrųjų,

$$(g * h) * (h^{-1} * g^{-1}) = g * (h * h^{-1}) * g^{-1} = g * 1 * g^{-1} = g * g^{-1} = 1.$$

Kadangi kiekvienam grupės elementui egzistuoja tik vienas atvirkštinis elementas, tai $(g * h)^{-1} = h^{-1} * g^{-1}$. □

5.1.9. Apibrėšime grupės elementų laipsnius sveikaisiais skaičiais. Sakykime, kad g yra grupės $(G, *)$ elementas. Sutarkime, jog $g^0 = 1, g^1 = g$. Elemento g $n-$tąjį laipsnį, $n > 0$, galima apibrėžti induktyviai: $g^n := g * g^{n-1}$. Jei $n < 0$, tai elemento g $n-$tąjį laipsnį apibrėžiame taip: $g^n = (g^{-1})^{-n}$ (čia $-n > 0$).

Pratimai.

Įrodykite lygybes:

1. $g^m * g^n = g^{m+n}, m, n \in \mathbb{Z}$.
2. $(g^m)^n = g^{m \cdot n}, m, n \in \mathbb{Z}$.

5.1.10 pastaba. Abelio grupės kompozicijos dėsnis dažniausiai yra žymimas $+$ ir vadinamas grupės elementų sudėtimi, neutralus elementas – 0 ir vadinamas nuliu, o elementui g simetrinis elementas yra žymimas $-g$ ir vadinamas priešingu elementu elementui g. Šie žymėjimai yra vadinami adiciniais, o ankstesni, kuriais iki šiol naudojomės, – multiplikaciniais. Pereiti nuo multiplikacinių žymėjimų prie adicinių ir atvirkščiai – labai paprasta:

grupės elementas

$$x_1^{n_1} * x_2^{n_2} * \cdots * x_s^{n_s}$$

multiplikaciniame žymėjime yra pakeičiamas grupės elementu

$$n_1 * x_1 + n_2 * x_2 + \cdots + n_s * x_s$$

adiciniame žymėjime ir atvirkščiai, 1 – elementu 0 ir t. t.

5.1.11 apibrėžimas. Jei grupės $(G, *)$ aibė G yra baigtinė, tai grupė $(G, *)$ yra vadinama *baigtine*, o aibės G elementų skaičius $|G|$ yra vadinamas grupės $(G, *)$ *eile*. Jei grupės $(G, *)$ aibė G yra begalinė, tai grupė $(G, *)$ yra vadinama *begaline*.

5.1.12 pastaba. Dažniausiai paprastumo dėlei naudodami multiplikacinius žymėjimus tarp komponuojamųjų elementų nerašysime kompozicijos dėsnio ženklo.

5.1.13 pavyzdys. Akivaizdu, kad

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

yra begalinės Abelio grupės.

5.1.14 pavyzdys. Akivaizdu, kad

$$(\mathbb{Q}_+^*, \cdot), \quad (\mathbb{R}_+^*, \cdot), \quad (\mathbb{Q}^*, \cdot), \quad (\mathbb{R}^*, \cdot)$$

yra begalinės Abelio grupės.

5.1.15 pavyzdys. X – aibė, $P(X)$ – aibės X visų poaibių aibė. $(P(X), \ominus)$ – Abelio grupė, nes

1. $\ominus$ – simetrinė aibių atimtis yra asociatyvus kompozicijos dėsnis.
2. $\emptyset$ – neutralus elementas simetrinės aibių atimties $\ominus$ atžvilgiu.
3. Elementui $Y \in P(X)$ (t. y. $Y \subset X$) simetrinis elementas yra Y (nes $Y \ominus Y = \emptyset$).

Jei X – baigtinė aibė ir $|X| = n$, tai grupės $P(X)$ eilė lygi $|P(X)| = 2^n$.

5.1.16 pavyzdys (simetrinė grupė)**.** Tarkime, kad X – netuščia aibė. Įsitikinsime, kad $(\mathcal{A}ut X, \circ)$ – grupė. Iš tikrųjų, kaip žinome:

1. $\circ$ – asociatyvus kompozicijos dėsnis.

2. $\mathcal{A}utX \ni \mathrm{id}$ – neutralus elementas atvaizdžių kompozicijos $\circ$ atžvilgiu (priminsime, kad $\mathrm{id}(x) = x, x \in X$).

3. $f \in \mathcal{A}utX \Rightarrow f^{-1} \in \mathcal{A}utX, \quad f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}.$

Jei X – begalinė aibė, tai ir grupė $(\mathcal{A}utX, \circ)$ – begalinė. Jei $|X| = n$, tai šiuo atveju grupė $(\mathcal{A}utX, \circ)$ yra žymima S_n (arba Σ_n) ir vadinama n-tojo laipsnio *simetrine grupe*. n-ojo laipsnio simetrinės grupės S_n elementus galima nagrinėti kaip bijekcijas

$$f : \mathbb{N}_n \to \mathbb{N}_n, \text{ čia } \mathbb{N}_n = \{1, 2, \dots, n\}.$$

Vietoj $\mathbb{N}_n$ galima imti bet kurią baigtinę aibę, turinčią n elementų. Dažnai bijekcija $f : X \to X$, kai X – baigtinė aibė, yra vadinama aibės X elementų *keitiniu*. Bijekciją

$$f : \mathbb{N}_n \to \mathbb{N}_n$$

galima pavaizduoti lentele

$$\begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix},$$

pirmoje eilutėje bet kuria tvarka surašius visus aibės $\mathbb{N}_n$ elementus (šioje lentelėje aibės $\mathbb{N}_n$ elementai surašyti natūralia tvarka), o antroje eilutėje po kiekvienu pirmos eilutės elementu j parašius jo vaizdą $f(j)$. Kadangi f – bijekcija, tai $f(1), f(2), \dots, f(n)$, – visi tarpusavy skirtingi elementai. Dar kartą pabrėžiame, kad lentelės pirmoje eilutėje aibės $\mathbb{N}_n$ elementų tvarka nesvarbi, bet svarbu, kas parašyta po kiekvienu pirmos eilutės elementu! Pavyzdžiui, lentelės

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \text{ ir } \begin{pmatrix} 3 & 2 & 1 \\ 1 & 3 & 2 \end{pmatrix}$$

apibrėžia tą patį atvaizdį

$$f : \mathbb{N}_3 \to \mathbb{N}_3.$$

Tarp lentelių, vaizduojančių tą patį atvaizdį, rašysime lygybės ženklą. Pavyzdžiui,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 3 & 2 \end{pmatrix},$$

bet

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Dabar nesunku suskaičiuoti, kiek elementų turi grupė S_n. Tam reikia suskaičiuoti, kiek galima sudaryti lentelių

$$\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix},$$

vaizduojančių visas skirtingas bijekcijas

$$f : \mathbb{N}_n \to \mathbb{N}_n.$$

Akivaizdu, kad po 1-uoju galima parašyti bet kurį aibės $\mathbb{N}_n$ elementą, po 2-uoju galima parašyti bet kurį vieną iš likusių $n-1$ aibės $\mathbb{N}_n$ elementų ir t. t. Vadinasi, galima sudaryti iš viso $n \cdot (n-1) \cdot \dots \cdot 2 \cdot 1 = n!$ skirtingų lentelių, t. y. $|S_n| = n!$.

Tarkime, kad

$$f = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & \dots & n \\ g(1) & g(2) & \dots & g(n) \end{pmatrix}$$

– bijekcijos. Tuomet

$$f \circ g = f \circ \begin{pmatrix} 1 & 2 & \dots & n \\ g(1) & g(2) & \dots & g(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ f(g(1)) & f(g(2)) & \dots & f(g(n)) \end{pmatrix},$$

nes kiekvienam j:

$$j \xrightarrow{g} g(j) \xrightarrow{f} f(g(j)).$$

Atkreipsime dėmesį, kad

$$f^{-1} = \begin{pmatrix} f(1) & f(2) & \dots & f(n) \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Iš tikrųjų:

$$f \circ f^{-1} = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix} \circ \begin{pmatrix} f(1) & f(2) & \dots & f(n) \\ 1 & 2 & \dots & n \end{pmatrix} =$$

$$\begin{pmatrix} f(1) & f(2) & \dots & f(n) \\ f(1) & f(2) & \dots & f(n) \end{pmatrix} = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} = \mathrm{id}.$$

5.1.17 pavyzdys (grupė S_3)**.**

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \right.$$

$$\left. \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

Pažymėkime

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Tuomet

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \sigma^2 \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$$

$\sigma^3 = \mathrm{id}, \ \ \tau^2 = \mathrm{id}$. Taigi

$$S_3 = \{\mathrm{id}, \ \ \sigma, \ \ \sigma^2, \ \ \tau, \ \ \sigma \circ \tau, \ \ \sigma^2 \circ \tau\},$$

t. y. grupės S_3 elementai yra išreiškiami elementų σ ir τ sandaugomis. Elementus σ ir τ sieja lygybės

$$\sigma^3 = \tau^2 = \mathrm{id}, \quad \tau \circ \sigma \circ \tau = \sigma^2.$$

Šių lygybių pakanka tam, kad galėtume atkurti grupės S_3 elementų daugybos lentelę. Pavyzdžiui,

$$\tau \circ \sigma = \tau \circ \sigma \circ (\tau \circ \tau) = (\tau \circ \sigma \circ \tau) \circ \tau = \sigma^2 \circ \tau;$$

$$(\sigma \circ \tau) \circ (\sigma^2 \circ \tau) = \sigma \circ \tau \circ \sigma \circ \sigma \circ \tau = \sigma \circ \tau \circ \sigma \circ \tau \circ \tau \circ \sigma \circ \tau =$$

$$= \sigma \circ (\tau \circ \sigma \circ \tau) \circ (\tau \circ \sigma \circ \tau) = \sigma \circ \sigma^2 \circ \sigma^2 = \sigma^3 \circ \sigma^2 = \mathrm{id} \circ \sigma^2 = \sigma^2;$$

$$\tau \circ (\sigma^2 \circ \tau) = \tau \circ \sigma \circ \sigma \circ \tau = \tau \circ \sigma \circ \tau \circ \tau \circ \sigma \circ \tau = \sigma^2 \circ \sigma^2 = \sigma^3 \circ \sigma = \sigma$$

ir t. t.

5.1.18 pastaba. Atvaizdžių kompozicijos dėsnis yra žymimas $\circ$. Šiuo ženklu žymėjome ir simetrinės grupės elementų kompoziciją, nes simetrinės grupės elementus interpretavome kaip bijekcijas. Bet vietoje žymens $\circ$ renkant formules kompiuteriu patogiau rašyti $*$. Todėl dažnai, nors kai kurių grupių elementus ir interpretuosime kaip atvaizdžius, tarp komponuojamų elementų vietoje žymens $\circ$ rašysime $*$.

5.1.19 pavyzdys (Diedro grupė D_n (abstrakčiojo arba kombinatorinio taisyklingojo n-kampio simetrijų grupė))**.** Tarkime, kad aibė

$$\mathcal{F} = \{\{1,2\},\{2,3\},\dots\{n-1,n\},\{n,1\}\},$$

t. y. sudaryta iš aibės $\mathbb{N}_n$ nurodytų poaibių. Porą $(\mathbb{N}_n, \mathcal{F})$ pavadinsime *abstrakčiuoju taisyklinguoju n-kampiu.* Bijekciją $f : \mathbb{N}_n \to \mathbb{N}_n$, tenkinančią sąlygą

$$X \in \mathcal{F} \iff f(X) \in \mathcal{F},$$

pavadinkime abstrakčiojo taisyklingojo n-kampio $(\mathbb{N}_n, \mathcal{F})$ *simetrija*. Nesunku įsitikinti (o iš tikrųjų akivaizdu), kad abstrakčiojo taisyklingojo n-kampio $(\mathbb{N}_n, \mathcal{F})$ visos simetrijos atvaizdžių kompozicijos $*$ atžvilgiu sudaro grupę. Ši grupė yra vadinama *diedro grupe*. Sutarkime šią grupę žymėti D_n.

Norint apibrėžti $(\mathbb{N}_n, \mathcal{F})$ simetriją f, pakanka nurodyti, pavyzdžiui, aibės $\mathbb{N}_n$ elementų 1 ir 2 vaizdus: $f(1), f(2)$. Elemento 1 vaizdas gali būti bet kuris aibės $\mathbb{N}_n$ elementas i, o 2 – tik toks j, kad $\{i, j\} \in \mathcal{F}$. Jei elementų 1 ir 2 vaizdai nurodyti, tai kitų aibės $\mathbb{N}_n$ elementų vaizdai vienareikšmiškai nurodomi (įrodykite).

Ypač lengvai yra aprašoma abstrakčiojo taisyklingojo n-kampio $(\mathbb{N}_n, \mathcal{F})$ simetrijų grupė, pavaizdavus $(\mathbb{N}_n, \mathcal{F})$ plokštumoje kaip geometrinį taisyklingąjį n-kampį. Iš geometrinės prasmės nesunku suvokti, iš kokių atvaizdžių sudaryta grupė D_n. Ši grupė turi n posūkių apie n-kampio simetrijos centrą O ir n atspindžių taisyklingojo n-kampio simetrijos ašių atžvilgiu. Pažymėję posūkį

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1 \end{pmatrix},$$

kitus posūkius galime užrašyti σ laipsniais:

$$\sigma = \sigma^1, \sigma^2, \dots, \sigma^{n-1}, \sigma^n = \mathrm{id}.$$

Pažymėję atspindį

$$\tau = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & n & n-1 & \dots & 3 & 2 \end{pmatrix},$$

visus atspindžius galime užrašyti taip: τ, $\sigma * \tau$, $\sigma^2 * \tau, \dots, \sigma^{n-1} * \tau$. Iš geometrinės prasmės akivaizdu, kad $\tau * \sigma * \tau = \sigma^{-1} = \sigma^{n-1}$. Remdamiesi šia lygybe, galime užrašyti grupės D_n elementų daugybos lentelę:

$$\sigma^i * \sigma^j = \begin{cases} \sigma^{i+j}, & \text{jei } i+j < n, \\ \sigma^{i+j-n}, & \text{jei } i+j \geq n; \end{cases}$$

$$\sigma^i * (\sigma^j * \tau) = \begin{cases} \sigma^{i+j} * \tau, & \text{jei } i+j < n, \\ \sigma^{i+j-n} * \tau, & \text{jei } i+j \geq n; \end{cases}$$

$$(\sigma^i * \tau) * \sigma^j = \begin{cases} \sigma^{i-j} * \tau, & \text{jei } i-j \geq 0, \\ \sigma^{i-j+n} * \tau, & \text{jei } i-j < 0; \end{cases}$$

$$(\sigma^i * \tau) * (\sigma^j * \tau) = \begin{cases} \sigma^{i-j}, & \text{jei } i-j \geq 0, \\ \sigma^{i-j+n}, & \text{jei } i-j < 0. \end{cases}$$

Dabar glaustai galime apibrėžti diedro grupę:

$$D_n = \{\sigma^i * \tau^j \mid 0 \leq i < n,\ 0 \leq j \leq 1,\ \sigma^n = \tau^2 = \mathrm{id},\ \tau * \sigma * \tau = \sigma^{-1} = \sigma^{n-1}\},$$

t. y. grupė D_n turi $2n$ elementų, o šios grupės elementų daugybos lentelė yra apibrėžiama iš lygybių, siejančių elementus σ ir τ:

$$\sigma^n = \tau^2 = \mathrm{id}, \quad \tau * \sigma * \tau = \sigma^{-1}.$$

5.1.20 pavyzdys (tetraedro simetrijų grupė)**.** Tetraedro simetrijų grupė turi 24 elementus ir šią simetrijų grupę galima sutapatinti su grupe S_4 (įrodykite).

5.1.21 pavyzdys. Panašiai galima nagrinėti ir kitų iškilųjų taisyklingųjų kūnų (kubo, oktaedro, dodekaedro, ikosaedro) simetrijų grupes. Pažymėtina, kad kai kurių iškilųjų taisyklingųjų kūnų simetrijų grupės sutampa – tai kubo ir oktaedro, taip pat ikosaedro ir dodekaedro. Kubas ir oktaedras, ikosaedras ir dodekaedras yra vadinami dualiais kūnais. Tetraedras dualus sau. Pavyzdžiui, jei sujungsite atkarpomis kubo sienų centrus, tai gausite oktaedrą, o jei sujungsite atkarpomis oktaedro sienų centrus, tai gausite kubą. Visiškai taip pat yra susiję ikosaedras ir dodekaedras. Norint aprašyti minėtų iškilųjų taisyklingųjų kūnų simetrijų grupes, pakanka, pavyzdžiui, aprašyti tik kubo ir dodekaedro simetrijų grupes.

5.1.1 Taisyklingųjų kūnų simetrijų grupės

5.1.22 (kubo simetrijų grupė)**.** Dabar sužinosime, kiek yra kubo simetrijų. Pirmiausia suskaičiuokime, kiek yra posūkių, pervedančių kubą į save. Yra trys ašys, jungiančios kubo priešingų sienų centrus. Sukdami kubą apie kiekvieną jų, gauname po tris skirtingas simetrijas (tapačiojo atvaizdžio id – neįskaičiuojame). Yra keturios ašys, jungiančios kubo priešingas viršūnes. Sukdami kubą apie kiekvieną jų, gauname po dvi skirtingas simetrijas. Yra šešios ašys, jungiančios kubo priešingų briaunų centrus. Sukdami kubą apie kiekvieną jų, gauname po vieną simetriją.

Taigi sukdami kubą iš viso gauname

$$3 \times 3 + 4 \times 2 + 6 \times 1 + 1 = 9 + 8 + 6 + 1 = 24$$

(čia priskaičiuojame ir tapatųjį atvaizdį) simetrijas.

Paėmę vieną kubo veidrodinį atspindį kurios nors kubo simetrijos plokštumos atžvilgiu ir paėmę šio veidrodinio atspindžio kompoziciją su kiekviena kubo posūkio simetrija, gauname dar 24 kubo simetrijas. Taigi iš viso kubas turi 48 simetrijas.

Pratimas. Kubas turi keturias įstrižaines. Įrodykite, kad kubo posūkių grupės elementai perstato kubo įstrižaines. Kadangi kubo posūkių yra 24, o keturių skirtingų elementų perstatinių – taip pat 24, tai kubo posūkių grupę galite sutapatinti su kubo keturių įstrižainių visų perstatinių grupe.

5.1.23 (dodekaedro simetrijų grupė)**.** Įrodykite, kad, sukdami dodekaedrą apie jo centrą, gausite 60 dodekaedro simetrijų. Iš viso dodekaedras turi 120 simetrijų (įskaičiuojant ir jo veidrodinius atspindžius). Simetrinė grupė S_5 taip pat turi 120 elementų. Tai, kad šios grupės struktūriniu požiūriu yra vienodos, – labai svarbus faktas.

5.1.2 Tiesės afiniųjų atvaizdžių grupė

5.1.24. Apibrėžkime atvaizdį

$$T_{\alpha,a} : \mathbb{R} \to \mathbb{R}, \ \ T_{\alpha,a}(x) = \alpha x + a,$$

čia $\alpha \in \mathbb{R}^*, \ \ a, \ x \in \mathbb{R}$.

Įsitikinkime, kad atvaizdžių $T_{\alpha,a}$ ir $T_{\beta,b}$ kompozicija yra atvaizdis

$$T_{\alpha\beta,a+\alpha b}.$$

Iš tikrųjų, kiekvienam $x \in \mathbb{R}$ galima parašyti lygybes:

$$(T_{\alpha,a} \circ T_{\beta,b})(x) = T_{\alpha,a}(T_{\beta,b}(x)) = T_{\alpha,a}(\beta x + b)$$
$$= \alpha(\beta x + b) + a = (\alpha\beta)x + a + \alpha b = T_{\alpha\beta,a+\alpha b}(x).$$

Taigi atvaizdžių aibė

$$\mathcal{A}ff(\mathbb{R}) := \{T_{\alpha,a} \mid \ \alpha \in \mathbb{R}^*, \ \ a \in \mathbb{R}\}$$

yra stabili atvaizdžių kompozicijos $\circ$ atžvilgiu.

$\mathcal{A}ff(\mathbb{R})$ atvaizdžių kompozicijos $\circ$ atžvilgiu yra grupė. Iš tikrųjų, nes:

1. Atvaizdžių kopozicija $\circ$ yra asociatyvi.
2. $\mathrm{id} = T_{1,0} \in \mathcal{A}ff(\mathbb{R})$, id – neutralus elementas atvaizdžių kompozicijos $\circ$ atžvilgiu.
3. Atvaizdžiui $T_{\alpha,a}, \ \ \alpha \in \mathbb{R}^*, \ \ a \in \mathbb{R}$, atvirkštinis atvaizdis yra

   $$T_{\alpha^{-1},-\alpha^{-1}a}$$

   (įsitikinkite).

Grupė $(\mathcal{A}ff(\mathbb{R}), \circ)$ nėra komutatyvi (įsitikinkite).

Atvaizdžiai $T_{\alpha,a}, \ \ \alpha \in \mathbb{R}^*, \ \ a \in \mathbb{R}$, vadinami realiosios tiesės $\mathbb{R}$ *afiniosiomis transformacijomis*, o grupė $(\mathcal{A}ff(\mathbb{R}), \circ)$ – realiosios tiesės $\mathbb{R}$ *afiniųjų transformacijų grupe.*

Realiosios tiesės $\mathbb{R}$ afiniosios transformacijos $T_{\alpha,a}, \alpha \in \mathbb{R}_*, a \in \mathbb{R}$, specialioms parametrų α ir a reikšmėms turi atskirus pavadinimus. Pavyzdžiui, transformacija $T_{-1,a}$, čia $a \in \mathbb{R}$, yra vadinama tiesės $\mathbb{R}$ *veidrodiniu atspindžiu* taško $\frac{a}{2}$ atžvilgiu. Transformacija $T_{\alpha,0}, \ \ \alpha > 0$, yra vadinama *homotetija* centro 0 atžvilgiu, o jos koeficientas yra α, ir t. t.

5.1.25 pavyzdys. Galima nagrinėti tiesę, sudarytą iš racionaliųjų skaičių $\mathbb{Q}$. Šios tiesės afiniosios transformacijos sudaro grupę

$$\mathcal{A}ff(\mathbb{Q}) := \{T_{\alpha,a} \mid \alpha \in \mathbb{Q}^*, \ \ a \in \mathbb{Q}\}.$$

5.1.26. Anksčiau nagrinėti grupių pavyzdžiai yra bendros situacijos atskiras atvejis.

Tarkime, kad X – netuščia aibė, $\mathcal{F}$ – aibės X kai kurių poaibių aibė (t. y. $\mathcal{F} \subset P(X)$). Šiuo atveju sakysime, kad aibės X poaibių aibė $\mathcal{F}$ apibrėžia aibėje X struktūrą $\mathcal{F}$. Sutarkime aibę X su joje apibrėžta struktūra $\mathcal{F}$ žymėti $(X, \mathcal{F})$.

5.1.27 apibrėžimas. Aibės X su joje apibrėžta *struktūra* $\mathcal{F}$ *simetrija* yra vadinama bijekcija $f : X \to X$, tenkinanti sąlygas:

- $Y \in \mathcal{F} \Rightarrow f(Y) \in \mathcal{F}$;
- $Y \in \mathcal{F} \Rightarrow f^{-1}(Y) \in \mathcal{F}$.

5.1.28 teiginys. *Aibės X su joje apibrėžta struktūra $\mathcal{F}$ visos simetrijos atvaizdžių kompozicijos $*$ atžvilgiu sudaro grupę, kurią žymėsime $(\mathcal{A}ut(X, \mathcal{F}), *)$.*

Įrodymas. Šį teiginį paliekame įrodyti skaitytojui.

Savaime suprantama, kad, bet kaip parinkę aibės X poaibių aibę $\mathcal{F}$, nieko įdomaus negausime. Žinomos svarbios aibėje X struktūros yra apibrėžiamos tokiomis aibės X poaibių aibėmis $\mathcal{F}$, kurios tenkina vienokias ar kitokias aksiomų sistemas. Dabar pailiustruosime pavyzdžiais konkrečias aibės X struktūras.

5.1.3 Afinioji plokštuma

Sutarkime aibės X elementus vadinti taškais, o aibės X poaibius, priklausančius $\mathcal{F}$, – tiesėmis. Tiesės $l, m \in \mathcal{F}$ (t. y. l, m yra aibės X poaibiai) yra vadinamos *lygiagrečiomis* ir žymimos $l||m$, jei $l \cap m = \emptyset$ arba $l = m$.

5.1.29 apibrėžimas. Aibės X poaibių aibė $\mathcal{F}$ apibrėžia aibėje X *afiniosios plokštumos struktūrą*, jei $\mathcal{F}$ tenkina aksiomų sistemą:

1. Kiekvienai aibės X skirtingų taškų porai A ir B egzistuoja vienintelė tiesė $l \in \mathcal{F}$ tokia, kad $\{A, B\} \subset l$ (t. y. $A, B \in l$).

2. Kiekvienai tiesei $l \in \mathcal{F}$ ir kiekvienam taškui $A \in X$ egzistuoja vienintelė tokia tiesė m, kad $A \in m$ ir $m||l$.

3. Egzistuoja trys taškai $A, B, C \in X$, kartu nepriklausantys nė vienai tiesei $l \in \mathcal{F}$.

Pora $(X, \mathcal{F})$ yra vadinama *afiniąja plokštuma.* Afiniosios plokštumos $(X, \mathcal{F})$ simetrijos yra vadinamos plokštumos X *afiniosiomis transformacijomis.*

5.1.30 pavyzdys (baigtinės afiniosios plokštumos pavyzdys)**.** Tegu

$$\mathbb{N}_4 = \{1, 2, 3, 4\}, \quad \mathcal{F} = \big\{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 4\}, \{1, 3\}, \{2, 4\}\big\}.$$

$(\mathbb{N}_4, \mathcal{F})$ – afinioji plokštuma, turinti 4 taškus ir 6 tieses. Afiniosios plokštumos $(\mathbb{N}_4, \mathcal{F})$ simetrijų grupė yra S_4 (įrodykite).

Pratimai.

Tarkime, kad $(X, \mathcal{F})$ – baigtinė afinioji plokštuma (aibė X – baigtinė), tiesė $l \in \mathcal{F}$ turi n taškų.

1. Įrodykite, kad bet kuri afiniosios plokštumos $(X, \mathcal{F})$ tiesė taip pat turi n taškų.

2. Įrodykite, kad kiekvienai afiniosios plokštumos $(X, \mathcal{F})$ tiesei $l \in \mathcal{F}$, lygiagrečių tiesių tiesei l yra taip pat n. Taigi $|X| = n^2$.

3. Įrodykite, kad afinioji plokštuma $(X, \mathcal{F})$ turi $n^2 + n$ tiesių (nurodymas: iš pradžių įrodykite, kad tiesių, turinčių bendrą tašką A, yra $n + 1$, o paskui pasinaudokite 2-uoju pratimu).

5.1.4 Projekcinė plokštuma

Aibės X elementus sutarkime vadinti taškais, o aibės X poaibius, priklausančius $\mathcal{F}$, – tiesėmis.

5.1.31 apibrėžimas. Aibės X poaibių aibė $\mathcal{F}$ apibrėžia aibėje X *projekcinės plokštumos struktūrą*, jei $\mathcal{F}$ tenkina aksiomų sistemą:

1. Kiekvienai aibės X skirtingų taškų porai A ir B egzistuoja tokia vienintelė tiesė $l \in \mathcal{F}$, kad $\{A, B\} \subset l$ (t. y. $A, B \in l$).

2. Bet kurios dvi tiesės $l, m \in \mathcal{F}$ turi bent vieną bendrą tašką.

3. Egzistuoja aibės X trys taškai A, B, C, kartu nepriklausantys nei vienai tiesei $l \in \mathcal{F}$.

4. Kiekviena tiesė $l \in \mathcal{F}$ turi bent tris taškus.

Pora $(X, \mathcal{F})$ yra vadinama *projekcine plokštuma.* Projekcivinės plokštumos $(X, \mathcal{F})$ simetrijos yra vadinamos *projekcinėmis transformacijomis.*

5.1.32 pavyzdys (baigtinės projekcinės plokštumos pavyzdys)**.** Tegu

$$\mathbb{N}_7 = \{1,2,3,4,5,6,7\},$$

$$\mathcal{F} = \big\{\{1,2,7\},\{2,3,6\},\{1,4,6\},\{3,4,7\},\{2,4,5\},\{1,3,5\},\{5,6,7\}\big\}.$$

Projekcinė plokštuma $(\mathbb{N}_7, \mathcal{F})$ turi 7 taškus ir 7 tieses. Vėliau įrodysime, kad projekcinės plokštumos $(\mathbb{N}_7, \mathcal{F})$ simetrijų grupė $(\mathcal{A}ut(\mathbb{N}_7, \mathcal{F}), \circ)$ turi 168 elementus.

Pratimai.

Tarkime, kad $(X, \mathcal{F})$ – baigtinė projekcinė plokštuma (aibė X – baigtinė), jos tiesė $l \in \mathcal{F}$ turi $n+1$ tašką.

1. Įrodykite, kad kiekviena projekcinės plokštumos $(X, \mathcal{F})$ tiesė turi $n+1$ tašką (nurodymas: pirmiausia įrodykite, kad egzistuoja taškas A nepriklausantis tiesei l ir kuriai nors tiesei m, o paskui nagrinėkite tiesių, kurioms priklauso taškas A ir kuris nors tiesės l taškas B, susikirtimą su tiese m).

2. Įrodykite, kad projekcinės plokštumos $(X, \mathcal{F})$ tiesių, turinčių bendrą tašką A, yra $n+1$.

3. Įrodykite, kad projekcinė plokštuma $(X, \mathcal{F})$ turi n^2+n+1 tašką ir tiek pat tiesių.

5.1.33. Tarp afiniųjų ir projekcinių plokštumų yra glaudus ryšys.

Pratimai.

1. Tarkime, kad $(X, \mathcal{F})$ – projekcinė plokštuma, l – kuri nors šios plokštumos tiesė (t. y. $l \in \mathcal{F}$). Įrodykite, kad $(X \setminus l, \mathcal{F} \setminus \{l\})$ – afinioji plokštuma.

2. Tarkime, kad $(X, \mathcal{F})$ – afinioji plokštuma. Afiniosios plokštumos $(X, \mathcal{F})$ visas tarpusavyje lygiagrečias tieses pavadinkime lygiagrečių tiesių pluoštu. Kiekvieną afiniosios plokštumos $(X, \mathcal{F})$ tiesę l atitinka jai lygiagrečių tiesių pluoštas, kurį pavadinkime „idealiu“tašku ir žymėkime $[l]$. Matyti, kad jei afiniosios plokštumos $(X, \mathcal{F})$ tiesės l ir m yra lygiagrečios, tai $[l] = [m]$. Aibę, gautą prie aibės X prijungus visus „idealius“taškus $[l]$, pažymėkime $\tilde{X}$. Aibės $\tilde{X}$ poaibį, sudarytą iš visų aibės $\tilde{X}$ „idealių“taškų pavadinkime „idealia“tiese (ji dažnai yra vadinama „be galo nutolusia“tiese) ir pažymėkime $\tilde{q}$. Prie kiekvienos afiniosios plokštumos $(X, \mathcal{F})$ tiesės l prijungę „idealų“tašką $[l]$, gauname „tiesę“, kurią pažymėkime $\tilde{l}$. Apibrėžkime aibės $\tilde{X}$ poaibių aibę $\tilde{\mathcal{F}}$, sudarytą iš visų tiesių $\tilde{l}$, t. y. iš visų afiniosios plokštumos $(X, \mathcal{F})$ tiesių l, papildytų „idealiais“taškais $[l]$, ir „idealiosios“tiesės $\tilde{q}$. Įsitikinkite, kad $(\tilde{X}, \tilde{\mathcal{F}})$ – projekcinė plokštuma.

5.1.34. Afiniųjų ir projekcinių plokštumų struktūras aibėje X apibrėžėme aibės X poaibių aibėmis $\mathcal{F}$, tenkinančiomis atitinkamas aksiomų sistemas. Panašiai galima apibrėžti orientuotus ir neorientuotus grafus, topologines, mačiąsias erdves ir kitus matematinius objektus. Bet į šią matematinių struktūrų apibrėžimų schemą nepatenka, pavyzdžiui, algebrinės struktūros apibrėžimas. Todėl naudinga apibrėžti bendresnę struktūros aibėje sąvoką. Tai galima padaryti, pavyzdžiui, tariant, kad aibės $\mathcal{F}$ elementais gali būti aibių $X^n, P^k(X^n)$, čia $k, n \in \mathbb{N}$, kurie nors elementai ar poaibiai, tenkinantys vienokią ar kitokią aksiomų sistemą. Grupės $(X, *)$ struktūra šia prasme yra apibrėžiama aibe

$$\mathcal{F} = \{\Gamma_* | \ \Gamma_* \subset X \times X \times X\},$$

čia Γ_* grupės X elementų kopozicijos dėsnio grafikas. Šia bendresne apibrėžiamų aibėse struktūrų prasme tų struktūrų simetrijos apibrėžiamos panašiai kaip ir anksčiau.

5.2 Pogrupiai

5.2.1 apibrėžimas. Netuščias grupės $(G, *)$ poaibis H yra vadinamas grupės $(G, *)$ *pogrupiu*, jei

1. $g_1, g_2 \in H \Rightarrow g_1 * g_2 \in H$ (t. y. bet kurių dviejų poaibio H elementų sandauga priklauso H).
2. $g \in H \Rightarrow g^{-1} \in H$ (t. y. kiekvienam poaibio H elementui atvirkštinis elementas priklauso H).

5.2.2 teiginys. *Grupės $(G, *)$ pogrupis H yra grupė.*

Įrodymas. Remdamiesi pogrupio apibrėžimo 1-ąja sąlyga, gauname, kad pogrupis H stabilus kompozicijos dėsnio $*$ atžvilgiu. Kadangi grupės $(G, *)$ elementų kompozicijos dėsnis $*$ yra asociatyvus, tai ir indukuotas kompozicijos dėsnis pogrupyje H yra asociatyvus. Įrodysime, kad grupės vienetas 1 priklauso H. Kadangi $H \neq \emptyset$, tai egzistuoja $g \in H$. Remdamiesi pogrupio apibrėžimo 2-ąja sąlyga, gauname: $g, g^{-1} \in H$. Remdamiesi 1-ąja pogrupio apibrėžimo sąlyga, gauname: $1 = g * g^{-1} \in H$. Remdamiesi pogrupio apibrėžimo 2-ąja sąlyga, matome, kad pogrupio H kiekvienam elementui atvirkštinis elementas priklauso H. $\square$

Jei H yra grupės $(G, *)$ pogrupis, tai sutarkime rašyti $(H, *) \subset (G, *)$ ar $(G, *) \supset (H, *)$. Paprastumo dėlei, kalbėdami apie grupę, nerašysime grupės elementų kopozicijos dėsnio ženklo.

5.2.3 apibrėžimas (antrasis pogrupio apibrėžimas)**.** Netuščias grupės $(G, *)$ poaibis H yra vadinamas grupės $(G, *)$ pogrupiu, jei bet kuriems $g_1, g_2 \in H$, sandauga $g_1 * g_2^{-1} \in H$.

Pratimas. Įrodykite abiejų pogrupio apibrėžimų ekvivalentumą.

5.2.4 pavyzdys. Gupės $(\mathbb{Z}, +)$ poaibis $\mathbb{N}_n = \{1, 2, \ldots, n\}$ nėra pogrupis. Šiuo atveju netenkinama pogrupio apibrėžimo 1-oji sąlyga, nes, pavyzdžiui, $1, n \in \mathbb{N}_n$, bet $1+n \notin \mathbb{N}_n$. 2-oji pogrupio apibrėžimo sąlyga taip pat nėra tenkinama: $1 \in \mathbb{N}_n$, bet $-1 \notin \mathbb{N}_n$.

5.2.5 pavyzdys. Grupės $(\mathbb{Z}, +)$ poaibis $\mathbb{N}$ nėra pogrupis, nes 1-oji pogrupio apibrėžimo sąlyga yra tenkinama, bet 2-oji – ne: $1 \in \mathbb{N}$, o $-1 \notin \mathbb{N}$.

5.2.6 pavyzdys. Grupės $(\mathbb{Z}, +)$ poaibis $X = \{-2, -1, 0, 1, 2\}$ nėra pogrupis, nes, pavyzdžiui, $1, 2 \in X$, bet $1 + 2 = 3 \notin X$. 2-oji pogrupio apibrėžimo sąlyga yra tenkinama.

5.2.7 pavyzdys. Grupės $(\mathbb{Q}, +)$ poaibis $\mathbb{Z}$ yra pogrupis.

5.2.8 pavyzdys. Grupės $(\mathbb{Q}^*, \cdot)$ poaibis $\mathbb{Q}^*_+$ yra pogrupis.

5.2.9 pavyzdys. Grupės $(\mathbb{Z}, +)$ poaibis $n\mathbb{Z}$, čia n – fiksuotas natūralusis skaičius, yra pogrupis.

5.2.10 pavyzdys. Poaibis $\{2^n | \; n \in \mathbb{Z}\}$ yra grupės $(\mathbb{Q}^*, \cdot)$ pogrupis.

5.2.11 pavyzdys. $(\mathbb{Q}^*, \cdot)$ yra grupė, $\mathbb{Q}^* \subset \mathbb{Q}$, bet grupė $(\mathbb{Q}^*, \cdot)$ nėra grupės $(\mathbb{Q}, +)$ pogrupis. $\mathbb{Q}^*$ – grupė daugybos atžvilgiu, o $\mathbb{Q}$ – grupė sudėties atžvilgiu.

5.2.12 pavyzdys. $(\mathbb{Q}^*, \cdot)$ yra grupės $(\mathbb{R}^*, \cdot)$ pogrupis.

5.2.13 pavyzdys. Tarkime, kad X – netuščia aibė, Y – aibės X poaibis. Tuomet $(P(Y), \ominus)$ yra grupės $(P(X), \ominus)$ pogrupis.

5.2.14 pavyzdys. $(\mathbb{Z}[\frac{1}{m}], +)$ yra grupės $(\mathbb{Q}, +)$ pogrupis.

5.2.15 pavyzdys.

$$\{T_{\alpha,0} \mid \alpha \in \mathbb{Q}^*\}$$

yra grupės

$$\mathcal{A}ff(\mathbb{Q}) = \{T_{\alpha,a} \mid \alpha \in \mathbb{Q}^*, \;\; a \in \mathbb{Q}\}$$

pogrupis. Priminsime, kad

$$T_{\alpha,a} : \mathbb{Q} \to \mathbb{Q}, \;\; T_{\alpha,a}(x) = \alpha x + a, \;\; x \in \mathbb{Q}.$$

5.2.16 pavyzdys.

$$\{T_{1,a} \mid a \in \mathbb{Q}\}$$

yra grupės $\mathcal{A}ff(\mathbb{Q})$ pogrupis.

5.2.17 pavyzdys.

$$\{T_{\alpha,a} \mid \alpha \in \mathbb{Q}^*, \ \ a \in \mathbb{Q}\}$$

yra grupės

$$\mathcal{A}ff(\mathbb{R}) = \{T_{\alpha,a} \mid \alpha \in \mathbb{R}^*, \ \ a \in \mathbb{R}\}$$

pogrupis.

5.2.18 pavyzdys. Grupės

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \right.$$

$$\left. \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$$

pogrupiai yra šie:

$$H_1 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}, \ H_2 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\},$$

$$H_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\},$$

$$H_4 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

ir dar du trivialūs pogrupiai: $\{\mathrm{id}\}$ ir S_3.

Pratimai.

1. Išrašykite grupės D_4 visus pogrupius.
2. Išrašykite grupės D_5 visus pogrupius.
3. Išrašykite grupės D_6 visus pogrupius.
4. Įrodykite: jei G yra grupės $(\mathbb{R}^*, \cdot)$ pogrupis, tai ir

   $$\{T_{\alpha,a} \mid \alpha \in G, \ \ a \in \mathbb{R}\}$$

   yra grupės $\mathcal{A}ff(\mathbb{R})$ pogrupis.

5. Grupės $\mathcal{A}ff(\mathbb{R})$ pogrupis
$$\{T_{\alpha,a} \mid \alpha \in \{1,-1\},\ \ a \in \mathbb{R}\}$$
yra vadinamas atspindžių generuotu pogrupiu. Įrodykite: jei H yra grupės $(\mathbb{R},+)$ pogrupis, tai ir
$$\{T_{\alpha,a} \mid \alpha \in \{1,-1\},\ \ a \in H\}$$
yra grupės
$$\{T_{\alpha,a} \mid \alpha \in \{1,-1\},\ \ a \in \mathbb{R}\}$$
pogrupis.

6. Ar bet kuriam grupės $(\mathbb{R}^*,\cdot)$ pogrupiui G ir bet kuriam grupės $(\mathbb{R},+)$ pogrupiui H aibė
$$\{T_{\alpha,a} \mid \alpha \in G,\ \ a \in H\}$$
atvaizdžių kompozicijos atžvilgiu yra grupės $\mathcal{A}ff(\mathbb{R})$ pogrupis? Kokias sąlygas turi tenkinti pogrupiai G ir H, kad ši atvaizdžių aibė atvaizdžių kompozicijos atžvilgiu būtų grupė?

5.2.19 teiginys. *Jei H yra grupės $(G,*)$ pogrupis, o K – grupės H pogrupis, tai K yra grupės G pogrupis.*

Įrodymas. Įrodymas akivaizdus. □

5.2.20 teiginys. *Grupės $(G,*)$ pogrupių šeimos $\{H_\alpha\}_{\alpha\in I}$ sankirta $\bigcap\limits_{\alpha\in I} H_\alpha$ yra grupės $(G,*)$ pogrupis.*

Įrodymas. Grupės vienetas $1 \in \bigcap\limits_{\alpha\in I} H_\alpha$, nes kievienam $\alpha \in I$, $1 \in H_\alpha$. Vadinasi, $\bigcap\limits_{\alpha\in I} H_\alpha \neq \emptyset$. Jei $g_1, g_2 \in \bigcap\limits_{\alpha\in I} H_\alpha$, tai ir $g_1 * g_2^{-1} \in \bigcap\limits_{\alpha\in I} H_\alpha$. Iš tikrųjų, jei $g_1, g_2 \in \bigcap\limits_{\alpha\in I} H_\alpha$, tai kiekienam $\alpha \in I$, $g_1, g_2 \in H_\alpha$. Kadangi kiekvienam $\alpha \in I$ aibė H_α yra pogrupis, tai $g_1 * g_2^{-1} \in H_\alpha$. Vadinasi, $g_1 * g_2^{-1} \in \bigcap\limits_{\alpha\in I} H_\alpha$. □

5.2.21 teiginys. *Tarkime, kad X yra grupės $(G,*)$ poaibis. Egzistuoja grupės $(G,*)$ pogrupis H, tenkinantis sąlygas:*

1. $X \subset H$;

2. Jei K grupės G pogrupis ir $X \subset K$, tai $H \subset K$.

5.2.22 apibrėžimas. Pogrupis H yra vadinamas aibės X elementų arba aibės X *generuotu pogrupiu* ir žymimas $\langle X\rangle$. Aibės X elementai yra vadinami pogrupio H *sudaromosiomis* arba *generuojančiaisiais elementais.*

5.2.23 pastaba. Grupės pogrupių aibė aibių įdėties $\subset$ atžvilgiu yra sutvarkytoji aibė. Pogrupis H yra mažiausias šios tvarkos atžvilgiu tarp tų pogrupių, kuriems aibė X yra jų poaibis.

5.2.21 teiginio įrodymas. Kadangi $X \subset G$, tai grupės $(G, *)$ pogrupių K, tenkinančių sąlygą $X \subset K$, aibė netuščia. Šių pogrupių sankirta $H =: \bigcap_{X \subset K} K$ ir yra pogrupis (5.2.20 teiginys), tenkinantis teiginyje išvardytas sąlygas. $\square$

5.2.24 pastaba. Jei $X = \{x_1, x_2, \ldots, x_n\}$, tai vietoje $\langle\{x_1, x_2, \ldots, x_n\}\rangle$ rašysime $\langle x_1, x_2, \ldots, x_n\rangle$ arba $\langle X\rangle$.

5.2.25 apibrėžimas. Jei grupė $(G, *) = \langle g_1, g_2, \ldots, g_n\rangle$, tai G yra vadinama *baigtinai generuota grupe.* Šiuo atveju kiekvienas grupės G elementas g yra užrašomas elementų g_1, g_2, ..., g_n sveikųjų laipsnių sandauga:

$$g = g_{i_1}^{\alpha_1} g_{i_2}^{\alpha_2} \ldots g_{i_r}^{\alpha_r},$$

čia $\alpha_j \in \mathbb{Z}$, o elementai g_{i_j}, $1 \leq j \leq r$, nebūtinai tarp savęs skirtingi. Be to, elementas g nebūtinai vienareikšmiškai taip užrašomas.

5.3 Cikliniai pogrupiai

5.3.1 apibrėžimas. Grupės $(G, *)$ pogrupį $\langle g\rangle$, generuotą vieno elemento g, vadinsime *cikliniu.* Jei $G = \langle g\rangle$, tai G yra vadinama *cikline* grupe.

Pažymėsime, kad grupės $(G, *)$ pogrupiui $\langle g\rangle$ priklauso visi elemento g sveikieji laipsniai.

5.3.2 teiginys. *Grupės $(G, *)$ bet kurio elemento g sveikųjų laipsnių aibė yra grupės G ciklinis pogrupis $\langle g\rangle$.*

Įrodymas. Pastebėsime, kad elemento g sveikųjų laipsnių aibė netuščia. Jei imsime elemento g sveikuosius laipsnius g^r, g^s, tai $g^r * (g^s)^{-1} = g^{r-s}$ yra taip pat elemento g sveikasis laipsnis. $\square$

5.3.3 apibrėžimas. Jei grupės $(G, *)$ ciklinis pogrupis $\langle g\rangle$ begalinis, tai g yra vadinamas *begalinės eilės elementu.* Jei $\langle g\rangle$ – baigtinis pogrupis, tai pogrupio eilė $|\langle g\rangle|$ yra vadinama elemento g *eile.*

5.3.4 teiginys. *Jei grupės $(G, *)$ elemento g eilė yra lygi n, tai n yra toks mažiausias teigiamas sveikasis skaičius, kad $g^n = 1$. Be to,*

$$\langle g\rangle = \{1, g, g^2, \ldots, g^{n-1}\}.$$

Įrodymas. Kadangi pogrupis $\langle g\rangle$ yra baigtinis ($|\langle g\rangle| = n$), tai egzistuoja tokie $r, s \in \mathbb{N}, r < s$, kad $g^s = g^r$. Šios lygybės abi puses padauginę iš $(g^r)^{-1} = g^{-r}$, gauname: $g^{s-r} = 1, s - r \in \mathbb{N}$. Tarkime, m – toks mažiausias teigiamas sveikasis skaičius, kad $g^m = 1$. Poaibis $\{1, g, g^2, \dots, g^{m-1}\}$ yra grupės G pogrupis. Iš tikrųjų:

$$g^i * g^j = \begin{cases} g^{i+j}, & \text{jei } i + j < m, \\ g^{i+j-m}, & \text{jei } i + j \geq m \end{cases},$$

čia $0 \leq i, j < m$. Elementui $g^i, 0 < i < m$, atvirkštinis yra g^{m-i}, čia, kaip matome, $0 < m - i < m$. Vadinasi, $\langle g\rangle = \{1, g, g^2, \dots, g^{m-1}\}$. Kadangi $|\langle g\rangle| = n$, tai $m = n$. □

5.3.5 pavyzdys. $(\mathbb{Z}, +)$ – begalinės eilės ciklinė grupė, 1 – šios grupės sudaromoji (-1 – taip pat šios grupės sudaromoji; kitų sudaromųjų ši grupė neturi).

5.3.6 pavyzdys. Aibė (žr. 2.4.2 pavyzdį)

$$\mathbb{Z}_n = (\{n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, n - 1 + n\mathbb{Z}\}, +),$$

čia n – fiksuotas natūralusis skaičius, yra n-tosios eilės ciklinė grupė, $1 + n\mathbb{Z}$ – šios grupės sudaromoji.

5.3.7 pastaba. Iš 5.3.5 ir 5.3.6 pavyzdžių matome, kad egzistuoja bet kurios eilės ciklinės grupės.

Pratimai.

1. Raskite grupės $\mathbb{Z}_5$ visas sudaromąsias.

2. Raskite grupės $\mathbb{Z}_6$ visas sudaromąsias.

3. Kiek sudaromųjų turi grupė $\mathbb{Z}_n$?

4. Tarkime, kad grupės $(G, *)$ elemento g eilė yra lygi n. Įrodykite: jei kuriam nors $m \in \mathbb{Z}$, $g^m = 1$, tai $n \mid m$.

5. Tarkime, kad grupės $(G, *)$ elementų g_1 ir g_2 eilės yra lygios n_1 ir n_2 ir šie elementai yra perstatomi, t. y. $g_1 * g_2 = g_2 * g_1$ ir, be to, $\langle g_1\rangle \cap \langle g_2\rangle = \{1\}$. Įrodykite, kad elemento $g_1 * g_2$ eilė yra lygi skaičių n_1 ir n_2 mažiausiam bendrajam kartotiniui.

6. Kam yra lygios grupės $(\mathcal{A}ff(\mathbb{R}), \circ)$ elementų $T_{-1,2}, T_{-1,4}$ ir $T_{-1,2} \circ T_{-1,4}$ eilės? Priminsime, kad

$$T_{\alpha,a} : \mathbb{R} \to \mathbb{R}, \ \ T_{\alpha,a}(x) = \alpha x + a, \ x \in \mathbb{R}.$$

7. Kam lygios diedro grupės

$$D_n = \{\sigma^i * \tau^j \mid 0 \le i < n,\ 0 \le j \le 1,\ \sigma^m = \tau^2 = 1,\ \tau * \sigma * \tau = \sigma^{-1}\}$$

elementų $\sigma * \tau,\ \ \sigma^2 * \tau$ ir $\sigma * \tau * \sigma^2 * \tau$ eilės?

5.4 Grupės skaidinys pogrupio gretutinėmis klasėmis

Dabar nagrinėsime grupės $(G, *)$ išskaidymą į pogrupio H kairiąsias, dešiniąsias gretutines klases.

5.4.1 apibrėžimas. Tarkime, X, Y – grupės $(G, *)$ poaibiai. Tuomet $X * Y := \{x * y \mid x \in X, y \in Y\}$. Jei, pavyzdžiui, $X = \{g\}$, tai vietoje $\{g\} * Y$ rašysime $g * Y$. Analogiškai, vietoje $X * \{g\}$ rašysime $X * g$.

5.4.2 apibrėžimas. Grupės $(G, *)$ pogrupio H *kairiąja (dešiniąja) gretutine klase* yra vadinamas gupės $(G, *)$ poaibis $g*H$ (atitinkamai $H*g$), $g \in G$, o elementas g – šios *klasės atstovu*.

5.4.3 teiginys. *Tarkime, kad H yra grupės $(G, *)$ pogrupis. Tuomet $g_1 * H = g_2 * H$ tada ir tik tada, kai $g_1^{-1} * g_2 \in H$ ($H * g_1 = H * g_2$ tada ir tik tada, kai $g_1 * g_2^{-1} \in H$).*

Įrodymas. Jei $g_1 * H = g_2 * H$, tai $g_2 \in g_1 * H$. Vadinasi, egzistuoja toks elementas $h \in H$, kad $g_2 = g_1 * h$. Šios lygybės abi puses iš kairės padauginę iš g_1^{-1}, gauname: $g_1^{-1} * g_2 = h \in H$, t. y. $g_1^{-1} * g_2 \in H$. Pažymėsime: $g_1^{-1} * g_2 \in H \iff g_2^{-1} * g_1 \in H$.

Jei $g_1^{-1} * g_2 = h \in H$, tai $g_2 = g_1 * h$. Tuomet kiekvienam $h' \in H$, $g_2 * h' = g_1 * h * h' \in g_1 * H$, t. y. $g_2 * H \subset g_1 * H$. Lygybę $g_2 = g_1 * h$ perrašę taip: $g_1 = g_2 * h^{-1}$, gauname, panašiai kaip ir anksčiau, $g_1 * H \subset g_2 * H$. Vadinasi, $g_1 * H = g_2 * H$.

Panašiai teiginys įrodomas ir pogrupio H dešiniosioms gretutinėms klasėms. □

5.4.4 išvada. *Tarkime, kad H yra grupės $(G, *)$ pogrupis. Jei $g' \in g * H$, tai $g' * H = g * H$ (analogiškai: jei $g' \in H * g$, tai $H * g' = H * g$).*

Įrodymas. Jei $g' \in g * H$, tai egzistuoja toks $h \in H$, kad $g' = g * h$. Tada $g^{-1} * g' = h \in H$ ir, remdamiesi ankščiau įrodytu teiginiu, gauname: $g' * H = g * H$ (analogiškai įrodoma lygybė $H * g' = H * g$). □

5.4.5 pastaba. Taigi grupės $(G, *)$ pogrupio H kairiosios (arba dešiniosios) gretutinės klasės $g * H$ (arba $H * g$) bet kuris elementas gali būti vadinamas šios klasės atstovu.

5.4.6 teiginys. *Grupės $(G, *)$ pogrupio H kairiosios gretutinės klasės $g_1 * H$ ir $g_2 * H$ arba neturi bendrų elementų, arba sutampa (teiginio tvirtinimas teisingas ir pogrupio H dešiniosioms gretutinėms klasėms).*

Įrodymas. Jei $g_1 * H \cap g_2 * H = \emptyset$, tai teiginys įrodytas. Tarkime, kad $g \in g_1 * H \cap g_2 * H$. Tuomet, remdamiesi 5.4.4 išvada, gauname $g_1 * H = g * H = g_2 * H$. □

5.4.7. Kaip matome, grupės $(G, *)$ pogrupio H kairiosios (dešiniosios) gretutinės klasės suskaido grupę G į netuščius, neturinčius bendrų elementų, poaibius. Kaip žinome (žr.1.4.9), aibės skaidinys netuščiais, neturinčiais bendrų elementų, poaibiais yra gaunamas apibrėžus aibėje atitinkamą ekvivalentumo sąryšį ir atvirkščiai: apibrėžus aibės skaidinį netuščiais, neturinčiais bendrų elementų poaibiais, yra apibrėžiamas aibėje ekvivalentumo sąryšis. Tik pasakysime, kad grupės skaidiniai pogrupio kairiosiomis ir dešiniosiomis gretutinėmis klasėmis bendruoju atveju yra skirtingi. Tai pailiustruosime paprasčiausiais pavyzdžiais.

5.4.8 pavyzdys. Tegu

$$S_3 = D_3 = \{1,\ \sigma,\ \sigma^2,\ \tau,\ \sigma * \tau,\ \sigma^2 * \tau \mid \sigma^3 = \tau^2 = 1,\ \tau * \sigma * \tau = \sigma^2\}.$$

Tegu šios grupės pogrupis $H = \{1, \tau\}$. Tuomet

$$1 * H = \{1, \tau\},\quad \sigma * H = \{\sigma, \sigma * \tau\},\quad \sigma^2 * H = \{\sigma^2, \sigma^2 * \tau\},$$

o

$$H * 1 = \{1, \tau\},\ H * \sigma = \{\sigma, \tau * \sigma\} = \{\sigma, \sigma^2 * \tau\},$$
$$H * \sigma^2 = \{\sigma^2, \tau * \sigma^2\} = \{\sigma^2, \sigma * \tau\}.$$

Grupės $S_3 = D_3$ skaidinys pogrupio H kairiosiomis gretutinėmis klasėmis yra:

$$S_3 = D_3 = \{1, \tau\} \cup \{\sigma, \sigma * \tau\} \cup \{\sigma^2, \sigma^2 * \tau\},$$

o šios grupės skaidinys pogrupio H dešiniosiomis gretutinėmis klasėmis yra:

$$S_3 = D_3 = \{1, \tau\} \cup \{\sigma, \sigma^2 * \tau\} \cup \{\sigma^2, \sigma * \tau\}.$$

Kaip matome, šie grupės $S_3 = D_3$ skaidiniai yra skirtingi.

5.4.9 pastaba. Jei grupė $(G, *)$ yra komutatyvi, tai grupės G skaidiniai pogrupio H kairiosiomis ir dešiniosiomis gretutinėmis klasėmis sutampa, nes šiuo atveju kiekvienam $g \in G$, $g * H = H * g$ (iš tikrųjų: $g * H = \{g * h \mid h \in H\} = \{h * g \mid h \in H\} = H * g$).

5.4.10. Galime nurodyti ekvivalentumo sąryšius grupėje G, susijusius su grupės G skaidiniais pogrupio H kairiosiomis ir dešiniosiomis gretutinėmis klasėmis. Šie ekvivalentumo sąryšiai atrodo taip:

$$_{H}R = \{(g_1, g_2) \in G \times G |\ g_1^{-1} * g_2 \in H\}$$

ir

$$R_H = \{(g_1, g_2) \in G \times G |\ g_1 * g_2^{-1} \in H\}.$$

5.4.11 teiginys. *Faktoraibės $G/_{H}R$ ir G/R_H, apibrėžiamos grupės $(G, *)$ skaidiniais pogrupio H kairiosiomis ir dešiniosionis gretutinėmis klasėmis, kaip aibės yra ekvivalenčios.*

Įrodymas. Tarkime,

$$G = \bigcup_{\alpha \in I} g_\alpha * H$$

yra grupės G skaidinys pogrupio H skirtingomis kairiosiomis gretutinėmis klasėmis (t. y., $g_\alpha * H \cap g_\beta * H = \emptyset$, jei $\alpha \neq \beta, \alpha, \beta \in I$). Įrodysime, kad

$$\bigcup_{\alpha \in I} H * g_\alpha^{-1}$$

yra grupės G skaidinys pogrupio H skirtingomis dešiniosiomis gretutinėmis klasėmis. Tam reikia įrodyti:

1. $G = \bigcup\limits_{\alpha \in I} H * g_\alpha^{-1}$.

2. Jei $H * g_\alpha^{-1} = H * g_\beta^{-1}$, tai $\alpha = \beta$.

Tarkime, $g \in G$. Tada $g^{-1} \in G = \bigcup\limits_{\alpha \in I} g_\alpha * H$. Vadinasi, egzistuoja toks $\alpha_0 \in I$, kad $g^{-1} \in g_{\alpha_0} * H$. Taigi $g^{-1} = g_{\alpha_0} * h$ su kuriuo nors $h \in H$. Pastarosios lygybės abi puses pakėlę -1 laipsniu, gauname: $g = h^{-1} * g_{\alpha_0}^{-1}$, čia $h^{-1} \in H$. Taigi $g \in H * g_{\alpha_0}^{-1} \subset \bigcup\limits_{\alpha \in I} H * g_\alpha^{-1}$, t. y. $G = \bigcup\limits_{\alpha \in I} H * g_\alpha^{-1}$.

Tarkime, kad $H * g_\alpha^{-1} = H * g_\beta^{-1}$. Tuomet egzistuoja toks $h \in H$, kad $g_\alpha^{-1} = h * g_\beta^{-1}$. Taigi $g_\alpha = g_\beta * h^{-1}$, čia $h^{-1} \in H$, t. y. $g_\alpha * H = g_\beta * H$. Ši lygybė galima tik tuo atveju, kai $\alpha = \beta$. □

5.4.12 apibrėžimas. Faktoraibes $G/_{H}R$ ir G/R_H žymėsime $H \backslash G$ ir G/H.

5.4.13 apibrėžimas. Grupės $(G, *)$ pogrupio H skirtingų kairiųjų gretutinių klasių skaičius yra vadinamas pogrupio H *indeksu* grupėje G ir žymimas $[G : H]$. Šis skaičius taip pat yra lygus pogrupio H skirtingų dešiniųjų gretutinių klasių skaičiui.

5.4.14 teiginys. *Grupės $(G, *)$ pogrupio H kieviena kairioji (taip pat ir dešinioji) gretutinė klasė $g * H$ $(H * g)$, $g \in G$, kaip aibė yra ekvivalenti aibei H.*

Įrodymas. Įrodysime, kad $g * H$ ir H yra ekvivalenčios aibės. Štai bijekcija $f : H \to g * H, f(h) = g * h, h \in H$. Pirmiausia įsitikinsime, kad f – injekcija. Jei $f(h_1) = f(h_2)$, tai $g * h_1 = g * h_2$. Lygybės $g * h_1 = g * h_2$ abi puses padauginę iš kairės iš g^{-1}, gauname $h_1 = h_2$. Taigi f – injekcija.

Pagaliau įsitikinsime, kad f – siurjekcija. Jei $y \in g * H$, tai egzistuoja toks $h \in H$, kad $y = g * h$. Vadinasi, $f(h) = g * h = y$.

Panašiai įrodoma, kad atvaizdis $f : H \to H * g, f(h) = h * g, h \in H$, – bijekcija. □

5.4.15 išvada. *Jei grupė $(G, *)$ baigtinė, tai grupės G pogrupio H kairiosios (taip pat ir dešiniosios) gretutinės klasės turi tą patį elementų skaičių, lygų pogrupio H elementų skaičiui.*

5.4.16 teorema (Lagranžo teorema)**.** *Baigtinės grupės $(G, *)$ pogrupio H eilė $|H|$ dalija grupės G eilę $|G|$.*

Įrodymas. Grupės G pogrupio H skirtingos kairiosios gretutinės klasės apibrėžia grupės G skaidinį

$$G = H \cup g_2 * H \cup \cdots \cup g_r * H,$$

čia $1, g_2, \ldots, g_r$ tarp savęs neekvivalentūs ekvivalentumo klasių atstovai. Kadangi $|H| = |g_2 * H| = \cdots = |g_r * H|$, tai $|G| = r|H|$ (r – pogrupio H indeksas grupėje G). □

5.4.17 išvada. *Baigtinės grupės $(G, *)$ elemento g eilė dalija grupės G eilę.*

Įrodymas. Elemento g eilė yra lygi ciklinio pogrupio $[g]$ eilei, o pogrupio eilė dalija grupės eilę. □

5.4.18 išvada. *Jei $(G, *)$ – baigtinė grupė, $g \in G$, tai $g^{|G|} = 1$.*

Pastarąją išvadą baigtinėms Abelio grupėms galima įrodyti tiesiogiai.

5.4.19 teiginys. *Tarkime, $(G, *)$ – baigtinė Abelio grupė. Tada $g^{|G|} = 1$, $g \in G$.*

Įrodymas. Sakykime, $G = \{g_1, g_2, \ldots, g_n\}$. Imkime $g \in G$. Tuomet $G = \{g * g_1, g * g_2, \ldots, g * g_n\}$, nes atvaizdis $f : G \to G, f(g_j) = g * g_j, 1 \le j \le n$, – bijekcija. Vadinasi, $(g * g_1) * (g * g_2) * \cdots * (g * g_n) = g_1 * g_2 * \cdots * g_n$. Kairioji šios lygybės pusė yra lygi $g^n * g_1 * g_2 * \cdots * g_n$. Taigi $g^n * g_1 * g_2 * \cdots * g_n = g_1 * g_2 * \cdots * g_n$. Suprastinę šios lygybės abi puses iš $g_1 * g_2 * \cdots * g_n$, gauname: $g^{|G|} = 1$. □

5.4.20. Bet kuriam baigtinės grupės $(G, *)$ eilės $|G|$ dalikliui d nebūtinai egzistuoja grupės G d eilės elementas. Pavyzdžiui, diedro grupės D_n, $n \geq 3$, eilė yra lygi $2n$, bet ši grupė neturi $2n$ eilės elemento. Jei toks elementas egzistuotų, tai grupė D_n būtų ciklinė ir kartu – komutatyvi. Bet grupė D_n nėra komutatyvi, kai $n \geq 3$. Kitus pavyzdžius rasite pratimuose.

Pratimai.

1. Diedro grupės D_{15} eilė yra lygi 30. Nors $6|30, 10|30$, ši grupė neturi nei 6-osios, nei 10-osios eilės elementų. Įsitikinkite, kad šioje grupėje yra 1 elementas 1-osios eilės (tai grupės vienetas 1), 2 elementai 3-iosios eilės, 4 elementai 5-osios eilės, 8 elementai 15-osios eilės ir 15 elementų 2-osios eilės.
2. Kiek ir kokios eilės elementų yra grupėje D_{16}?
3. Kiek ir kokios eilės elementų yra grupėje D_{12}?
4. Kiek ir kokios eilės elementų yra grupėje S_4?

Atsakymai.

2. Grupėje D_{16} yra: 1 elementas 1-osios eilės; 9 elementai 2-osios eilės; 2 elementai 4-osios eilės ir 4 elementai 8-osios eilės.
3. Grupėje D_{12} yra: 1 elementas 1-osios eilės; 13 elementų 2-osios eilės; 2 elementai 3-iosios eilės; 2 elementai 4-osios eilės; 2 elementai 6-osios eilės ir 4 elementai 12-osios eilės.
4. Grupėje S_4 yra: 1 elementas 1-osios eilės; 9 elementai 2-osios eilės; 8 elementai 3-iosios eilės ir 6 elementai 4-osios eilės.

5.4.21 pastaba. Lagranžo teoremą įrodėme baigtinėms grupėms. Begalinių grupių atveju ši teorema praranda prasmę, bet ir šiuo atveju begalinės grupės pogrupio indeksas grupėje gali būti baigtinis. Pavyzdžiui, $(\mathbb{Z}, +)$ – begalinė grupė, $n\mathbb{Z}$ – grupės $(\mathbb{Z}, +)$ pogrupis. Grupės $(\mathbb{Z}, +)$ skaidinys pogrupio $n\mathbb{Z}$ kairiosiomis (ar dešiniosiomis) klasėmis atrodo taip:

$$\mathbb{Z} = n\,\mathbb{Z} \cup (1 + n\,\mathbb{Z}) \cup (2 + n\,\mathbb{Z}) \cup \cdots \cup (n - 1 + n\,\mathbb{Z}).$$

Kaip matome, pogrupio $n\,\mathbb{Z}$ skirtingų gretutinių klasių skaičius yra bagtinis ir lygus n. Taigi $[\mathbb{Z} : n\,\mathbb{Z}] = n$.

Pratimai.

1. Užrašykite grupės

$$S_3 = D_3 = \{\sigma^i * \tau^j \mid 0 \le i < 3,\ 0 \le j \le 1,\ \sigma^3 = \tau^2 = 1,\ \tau * \sigma * \tau = \sigma^{-1}\}$$

skaidinį pogrupio H kairiosiomis gretutinėmis klasėmis, kai

$$\text{a) } H = \{1, \tau\};\ \text{ b) } H = \{1, \sigma * \tau\};\ \text{ c) } H = \{1, \sigma, \sigma^2\}.$$

2. Tegu grupė

$$G = (\{T_{\alpha,a} \mid \alpha \in \{1, -1\},\ \ a \in \mathbb{Z}\}, \circ)$$

ir jos pogrupis

$$H = \{T_{\alpha,a} \mid \alpha \in \{1, -1\},\ \ a \in n\mathbb{Z}\}.$$

Priminsime, kad

$$T_{\alpha,a} : \mathbb{R} \to \mathbb{R},\ \ T_{\alpha,a}(x) = \alpha x + a,\ x \in \mathbb{R}.$$

Raskite $[G : H]$.

3. Grupė G tokia pat, kaip ir 2-me pratime, o

$$H = \{T_{1,a} \mid a \in n\,\mathbb{Z}\}.$$

Raskite $[G : H]$.

4. Užrašykite grupės $(P(\{1, 2, 3, 4\}), \ominus)$ skaidinį pogrupio $P(\{1, 2\})$ kairiosiomis (ar dešiniosiomis) gretutinėmis klasėmis (čia $P(X)$ – aibės X visų poaibių aibė, $\ominus$ – simetrinė aibių atimtis).

5. Tarkime, K – grupės H pogrupis, o H – grupės $(G, *)$ pogrupis, $[H : K] < \infty, [G : H] < \infty$. Įrodykite: $[G : K] = [G : H][H : K]$.

6. Tarkime, kad H ir K – grupės $(G, *)$ baigtinio indekso pogrupiai. Įrodykite, kad $H \cap K$ – grupės G baigtinio indekso pogrupis.

   Nuoroda. Įrodykite: jei $k_1 * (H \cap K) \ne k_2 * (H \cap K)$, tai $k_1 * H \ne k_2 * H$, čia $k_1, k_2 \in K, H \cap K \subset K \subset G$. Dabar galima padaryti išvadą: $[K : H \cap K] \le [G : H]$ ir pasinaudoti 5-uoju pratimu.

7. Jei $H_1, H_2, \ldots, H_s$ – grupės $(G, *)$ baigtinio indekso pogrupiai, tai ir

$$H_1 \cap H_2 \cap \cdots \cap H_s$$

yra grupės G baigtinio indekso pogrupis.

5.4.22. Dabar apibrėšime svarbius grupės pogrupius: grupės centrą ir grupės komutantą.

5.4.23 apibrėžimas. Grupės $(G, *)$ poibis

$$Z(G) = \{g \in G \mid \forall x \in G,\, g * x = x * g\}$$

vadinamas grupės G *centru.*

5.4.24 teiginys. *Grupės* $(G, *)$ *centras* $Z(G)$ *yra grupės* G *pogrupis.*

Įrodymas. Pirmiausia pastebėsime, kad $Z(G) \neq \emptyset$, nes $1 \in Z(G)$. Dabar patrikrinsime abi pogrupio apibrėžimo sąlygas.

1. Sakykime, $g_1, g_2 \in Z(G)$. Tuomet kiekvienam $x \in G$,

$$(g_1 * g_2) * x = g_1 * (g_2 * x) = g_1 * (x * g_2) = (g_1 * x) * g_2 = (x * g_1) * g_2 = x * (g_1 * g_2).$$

Įrodėme: jei $g_1, g_2 \in Z(G)$, tai ir $g_1 * g_2 \in Z(G)$.

2. Lieka įrodyti: jei $g \in Z(G)$, tai ir $g^{-1} \in Z(G)$. Jei $g \in Z(G)$, tai kiekvienam $x \in G$, $g * x = x * g$. Pastaroji lygybė ekvivalenti lygybei: kiekvienam $x \in G$, $x * g^{-1} = g^{-1} * x$. Vadinasi, $g^{-1} \in Z(G)$. □

5.4.25 apibrėžimas. Grupės $(G, *)$ elementų g ir h *komutatoriumi* yra vadinamas elementas $g*h*g^{-1}*h^{-1}$ ir žymimas $[g, h]$. Grupės G pogrupis, generuotas grupės G elementų komutatorių $[g, h]$, $g, h \in G$, yra vadinamas grupės G *komutantu* ir žymimas G'. Kitaip tariant:

$$G' = \langle \{[g, h] \mid g, h \in G\} \rangle.$$

5.4.26 pastaba. Bendruoju atveju grupės dviejų komutatorių sandauga nėra šios grupės komutatorius. Pateikite pavyzdžių.

Pratimai.

1. Įrodykite, kad grupės S_4 centras $Z(S_4) = \{\mathrm{id}\}$.

2. Raskite grupių $\mathcal{A}ff(\mathbb{Q})$, $\mathcal{A}ff(\mathbb{R})$ centrus $Z(\mathcal{A}ff(\mathbb{Q})$, $Z(\mathcal{A}ff(\mathbb{R}))$.

3. Raskite grupių $\mathcal{A}ff(\mathbb{Q})$, $\mathcal{A}ff(\mathbb{R})$ komutantus $\mathcal{A}ff(\mathbb{Q})'$, $\mathcal{A}ff(\mathbb{R})'$.

4. Raskite diedro grupių D_n, $n \geq 3$ centrus ir komutantus.

5.5 Normalieji pogrupiai

5.5.1. Kaip matėme anksčiau, grupės $(G,*)$ skaidiniai pogrupio H kairiosiomis ir dešiniosiomis gretutinėmis klasėmis bendru atveju yra skirtingi. Specialiu atveju, kai G – komutatyvi grupė, grupės G skaidiniai bet kurio pogrupio kairiosiomis ar dešiniosiomis gretutinėmis klasėmis sutampa. Bet ir nekomutatyviųjų grupių $(G,*)$ skaidiniai tam tikrų pogrupių H kairiosiomis ir dešiniosiomis gretutinėmis klasėmis, kaip pamatysime, taip pat sutampa ir šiuo atveju galėsime apibrėžti naują grupę – grupės G fatorgrupę G/H pagal pogrupį H.

5.5.2 apibrėžimas. Grupės $(G,*)$ pogrupis H yra vadinamas *normaliuoju* (invariantiniu), jei kiekvienam $g \in G$, $g*H = H*g$.

5.5.3 pastaba. Kadangi $g*H = H = H*g$, jei $g \in H$, tai normaliojo pogrupio H apibrėžime pakanka reikalauti, kad kiekvienam $g \in G \setminus H$ būtų $g*H = H*g$.

5.5.4 pastaba. Normaliojo pogrupio apibrėžime kiekvienam $g \in G$ lygybės $g*H = H*g$ yra suprantamos kaip aibių lygybės. Remdamiesi lygybe $g*H = H*g$ negalime daryti išvados, kad bet kuriems $g \in G$ ir $h \in H$ teisinga lygybė $g*h = h*g$. Pavyzdžiui, imkime

$$G = S_3 = \{1, \sigma, \sigma^2, \tau, \sigma*\tau, \sigma^2*\tau \,|\, \sigma^3 = \tau^2 = 1, \tau*\sigma*\tau = \sigma^2\},\ H = \{1, \sigma, \sigma^2\}.$$

Tuomet

$$\tau*H = \{\tau, \tau*\sigma, \tau*\sigma^2\} = \{\tau, \sigma^2*\tau, \sigma*\tau\} = H*\tau,$$

bet $\tau*\sigma \neq \sigma*\tau$.

5.5.5 teiginys. *Grupės* $(G,*)$ *pogrupis* H *yra normalusis, jei*

$$g \in G, h \in H \Rightarrow g*h*g^{-1} \in H.$$

Įrodymas. Jei

$$g \in G, h \in H \Rightarrow g*h*g^{-1} \in H,$$

tai kiekvienam $g \in G$, $g*H*g^{-1} \subset H$. Bet jei kiekvienam $g \in G$,

$$g*H*g^{-1} \subset H, \tag{5.1}$$

tai ir

$$g^{-1}*H*g = g^{-1}*H*(g^{-1})^{-1} \subset H.$$

Tačiau $g^{-1}*H*(g^{-1})^{-1} \subset H$ ekvivalentu

$$H \subset g*H*g^{-1}.$$

Iš čia ir iš (5.1) gauname, jog kiekvienam $g \in G$, $g*H*g^{-1} = H$, o ši lygybė ekvivalenti lygybei $g*H = H*g, g \in G$. □

5.5.6 pavyzdys. Kiekvienas Abelio grupės $(G, *)$ pogrupis yra normalusis.

5.5.7 pavyzdys. Diedro grupės

$$D_n = \{\sigma^i * \tau^j \mid 0 \leq i < n,\ 0 \leq j \leq 1,\ \sigma^n = \tau^2 = 1,\ \tau * \sigma * \tau = \sigma^{-1}\},\ n \geq 3,$$

ciklinis pogrupis

$$[\sigma] = \{\sigma^j \mid 0 \leq j < n,\ \sigma^n = 1\}$$

yra normalusis, o pogrupiai

$$H_j = \{1, \sigma^j * \tau\},\ \text{čia}\ 0 \leq j < n,$$

nėra normalieji. Pavyzdžiui,

$$\sigma * H_j * \sigma^{-1} = \{1, \sigma^{j+2} * \tau\} \neq H_j,\ \ 0 \leq j < n.$$

Priminsime: $\sigma^n = 1, n \geq 3$.

5.5.8 pavyzdys. Afiniosios grupės

$$\mathcal{A}ff(\mathbb{R}) = (\{T_{\alpha,a} \mid \alpha \in \mathbb{R}^*,\ a \in \mathbb{R}\},\ \circ)$$

pogrupis $H = \{T_{1,a} | \ a \in \mathbb{R}\}$ yra normalusis. Iš tikrųjų: jei

$$T_{\alpha,a} \in \mathcal{A}ff(\mathbb{R}),\ \ T_{1,b} \in H,$$

tai

$$T_{\alpha,a} \circ T_{1,b} \circ T_{\alpha,a}^{-1} = T_{\alpha,a+\alpha b} \circ T_{\alpha^{-1},-\alpha^{-1}a} = T_{1,\alpha b} \in H.$$

Priminsime, kad

$$T_{\alpha,a} \circ T_{\beta,b} = T_{\alpha\beta,a+\alpha b},\ \ T_{\alpha,a}^{-1} = T_{\alpha^{-1},-\alpha^{-1}a}.$$

Grupės $\mathcal{A}ff(\mathbb{R})$ pogrupis

$$K = \{T_{\alpha,0} \mid \alpha \in \mathbb{R}^*\}$$

nėra normalusis, nes, pavyzdžiui,

$$T_{1,a} \circ T_{\alpha,0} \circ T_{1,a}^{-1} = T_{\alpha,a} \circ T_{1,-a} = T_{\alpha,a-\alpha a} \not\subset K,$$

jei tik $a \neq 0, \alpha \neq 1$.

Pratimai.

1. Įrodykite, kad grupės $(G, *)$ indekso 2 pogrupis H grupėje G yra normalusis.

2. Įrodykite: jei H yra grupės $(G, *)$ normalusis pogrupis, K – grupės G pogrupis, tai $H * K = K * H$ yra grupės G pogrupis.

3. Įrodykite: jei H, K yra grupės $(G, *)$ normalieji pogrupiai, tai $H * K$ yra grupės G normalusis pogrupis.

4. Įrodykite: jei H yra grupės $(G, *)$ normalusis pogrupis, K – grupės G pogrupis, tai $H \cap K$ yra grupės K normalusis pogrupis.

5. Įrodykite: jei H yra grupės $(G, *)$ pogrupis, tai $\bigcap\limits_{g \in G} g * H * g^{-1}$ yra grupės G normalusis pogrupis.

6. Įrodykite: jei H yra grupės $(G, *)$ baigtinio indekso pogrupis, tai ir

$$\bigcap_{g \in G} g * H * g^{-1} = \bigcap_{i=1}^{r} g_i * H * g_i^{-1}$$

yra grupės G baigtinio indekso normalusis pogrupis, čia $G = g_1 * H \cup g_2 * H \cup \cdots \cup g_r * H$ – grupės G skaidinys pogrupio H skirtingomis kairiosiomis gretutinėmis klasėmis.

7. Įrodykite, kad grupės $(G, *)$ centras $Z(G)$ yra grupės G normalusis pogrupis.

8. Įrodykite, kad grupės $(G, *)$ komutantas G' yra grupės G normalusis pogrupis.

5.6 Grupės faktorgrupė pagal normalųjį pogrupį

5.6.1. Tarkime, kad H yra grupės $(G, *)$ normalusis pogrupis. Tuomet faktoraibės G/H ir $H \backslash G$ yra lygios. Faktoraibėje G/H apibrėšime jos elementų kompozicijos dėsnį (daugybą) $*$ taip:

$$(g_1 * H) * (g_2 * H) =: g_1 * g_2 * H.$$

Galite įsitikinti, kad taip apibrėžtas faktoraibės G/H elementų kompozicijos dėsnis nepriklauso nuo pogrupio H gretutinių klasių atstovų. Be to, pogrupio H gretutinių klasių $g_1 * H$ ir $g_2 * H$ sandaugą galime apibrėžti kaip grupės G poaibį, sudarytą iš poaibių $g_1 * H$ ir $g_2 * H$ elementų sandaugų $x * y, x \in g_1 * H, y \in g_2 * H$. Visais atvejais gauname tą patį rezultatą. Galite įsitikinti, kad taip apibrėžę faktoraibės G/H elementų sandaugą, gauname grupę $(G/H, *)$.

5.6.2 apibrėžimas. Tarkime, kad H yra grupės $(G, *)$ normalusis pogrupis. Grupė $(G/H, *)$ yra vadinama grupės G *faktorgrupe* pagal normalųjį pogrupį H.

5.6.3 teiginys. *Grupės $(G, *)$ faktorgrupė $(G/G', *)$ pagal grupės G komutantą G' yra komutatyvi grupė.*

Įrodymas. Tarkime, kad $x * G', y * G' \in G/G', x, y \in G$. Tada $(x * G') * (y * G') = x * y * G' = y * x * G' = (y * G') * (x * G')$, nes $(x * y) * (y * x)^{-1} = x * y * x^{-1} * y^{-1} = [x, y] \in G'$. □

5.6.4 teiginys. *Jei grupės $(G, *)$ faktorgrupė $(G/H, *)$ pagal grupės G normalųjį pogrupį H yra komutatyvi grupė, tai $G' \subset H$, čia G' – grupės G komutantas.*

Įrodymas. Kadangi bet kuriems $x, y \in G$, $(x * H) * (y * H) = (y * H) * (x * H)$, tai bet kuriems $x, y \in G$, $x * y * H = y * x * H$. Iš pastarosios lygybės gauname: bet kuriems $x, y \in G$, $(x * y) * (y * x)^{-1} = x * y * x^{-1} * y^{-1} = [x, y] \in H$. Kadangi bet kuriems $x, y \in G$, $[x, y] \in H$, tai $G' \subset H$. □

Pratimai.

1. Raskite diedro grupių D_n, $n \geq 3$ faktorgrupes pagal jų centrus ir komutantus.

2. Raskite grupių $\mathcal{A}ff(\mathbb{Q})$ ir $\mathcal{A}ff(\mathbb{R})$ faktorgrupes pagal jų komutantus $\mathcal{A}ff(\mathbb{Q})'$ ir $\mathcal{A}ff(\mathbb{R})'$.

5.7 Homomorfizmai

5.7.1. Nagrinėsime tokius atvaizdžius, vadinamus homomorfizmais, apibrėžtus vienoje grupėje ir įgyjančius reikšmes kitoje grupėje, kurie išsaugo grupės struktūrą. Izomorfizmas – tai bijektyvus homomorfizmas. Jei tarp dviejų tiriamų objektų egzistuoja izomorfizmas, tai tie objektai struktūriniu teorijos požiūriu identiški. Nagrinėjami izomorfiniai objektai gali būti labai skirtingai apibrėžiami. Todėl nepaprastai svarbu sugebėti atpažinti izomorfinius objektus ir skirti neizomorfinius. Idealiausias atvejis būtų visus tiriamus objektus suklasifikuoti, t. y. sudaryti tokį visų tarp savęs neizomorfinių objektų sąrašą, kad kiekvienas toje teorijoje tiriamas objektas būtų izomorfinis vienam ir tik vienam objektui iš pateikto sąrašo. Bet, deja, grupių klasifikacija, – neišsprendžiamas uždavinys. Neegzistuoja algoritmas, leidžiantis bendru atveju atsakyti, ar skirtingai apibrėžtos grupės yra izomorfinės, ar ne. Šį nepaprastai svarbų faktą griežtai įrodė Novikovas.

Daug yra pasiekta tiriant tik atskiras grupių klases.

5.7.2 apibrėžimas. Tarkime, kad $(G, *), (H, \circ)$ – grupės. Atvaizdis $f : G \to H$ yra vadinamas *homomorfizmu*, jei bet kuriems $g_1, g_2 \in G$,

$$f(g_1 * g_2) = f(g_1) \circ f(g_2).$$

Homomorfizmas f yra vadinamas *izomorfizmu*, jei f – bijekcija. Grupės $(G, *)$ ir $(H, \circ)$ yra vadinamos *izomorfinėmis* ir rašoma $(G, *) \cong (H, \circ)$, jei egzistuoja bent vienas izomorfizmas $f : G \to H$. Izomorfizmas $f : G \to G$ yra vadinamas grupės $(G, *)$ *automorfizmu*.

5.7.3 pavyzdys. Grupės $(\mathbb{R}_+^*, *)$ ir $(\mathbb{R}, +)$ yra izomorfinės, nes

$$\ln : \mathbb{R}_+^* \to \mathbb{R}$$

– izomorfizmas. Įsitikinkite.

5.7.4 pavyzdys. $(\mathbb{R}^*, *)$ – grupė, atvaizdis

$$f : \mathbb{R}^* \to \mathbb{R}^*, f(\alpha) = \alpha^3, \alpha \in \mathbb{R}^*,$$

yra izomorfizmas.

5.7.5 pavyzdys. $(\mathbb{R}^*, *)$ – grupė, atvaizdis

$$f : \mathbb{R}^* \to \mathbb{R}^*, f(\alpha) = \alpha^{2n+1}, \;\; n \in \mathbb{Z}, \;\; \alpha \in \mathbb{R}^*,$$

yra izomorfizmas.

5.7.6 pavyzdys. $(\mathbb{R}^*, *)$ – grupė, atvaizdis

$$f : \mathbb{R}^* \to \mathbb{R}^*, f(\alpha) = \alpha^{2n}, \;\; n \in \mathbb{Z}, \;\; \alpha \in \mathbb{R}^*,$$

yra tik homomorfizmas, nei injekcinis, nei siurjekcinis.

5.7.7 pavyzdys. $(\mathbb{Q}^*, *)$ – grupė, atvaizdis

$$f : \mathbb{Q}^* \to \mathbb{Q}^*, \;\; f(\alpha) = \alpha^3, \;\; \alpha \in \mathbb{Q}^*,$$

yra injekcinis homomorfizmas, bet nėra siurjekcinis.

5.7.8 pavyzdys. $(\mathbb{Z}, +)$ – grupė, atvaizdis

$$f : \mathbb{Z} \to \mathbb{Z}, \;\; f(n) = 5\,n, \;\; n \in \mathbb{Z},$$

yra homomorfizmas.

5.7.9 pavyzdys. Grupės $(\mathbb{Z}, +)$ ir $(5\,\mathbb{Z}, +)$ – izomorfinės,

$$f : \mathbb{Z} \to 5\,\mathbb{Z}, \;\; f(n) = 5n, \;\; n \in \mathbb{Z},$$

– izomorfizmas.

5.7.10 pavyzdys. $(\mathbb{Z}, +)$, $(\{1, -1\}, *)$ – grupės, atvaizdis

$$f : \mathbb{Z} \to \{1, -1\}, \;\; f(n) = (-1)^n, \;\; n \in \mathbb{Z}$$

yra homomorfizmas.

5.7.11 pavyzdys. Atvaizdis

$$f : \mathbb{Q} \to \mathbb{Q}, \;\; f(\alpha) = 5\,\alpha, \;\; \alpha \in \mathbb{Q},$$

yra grupės $(\mathbb{Q}, +)$ automorfizmas.

5.7.12 pavyzdys. Atvaizdis

$$f : \mathbb{Q} \to \mathbb{Q}, \;\; f(\alpha) = a\,\alpha, \;\; \alpha, \; a \in \mathbb{Q}, \;\; a \neq 0,$$

yra grupės $(\mathbb{Q}, +)$ automorfizmas.

5.7.13 pavyzdys. Atvaizdis

$$f : \mathbb{R} \to \mathbb{R}, \;\; f(\alpha) = a\,\alpha, \;\; \alpha, \; a \in \mathbb{R}, \;\; a \neq 0,$$

yra grupės $(\mathbb{R}, +)$ automorfizmas.

5.7.14. Įrodysime keletą paprastų faktų apie homomorfizmus.

5.7.15 teiginys. *Jei $(G, *), (H, \circ)$ – grupės, $f : G \to H$ – homomorfizmas, tai:*
1. $f(1_G) = 1_H$, čia 1_G – grupės G vienetas, 1_H – grupės H vienetas.
2. Kiekvienam $g \in G$, $f(g^{-1}) = f(g)^{-1}$.

Įrodymas. 1. $f(1_G) = f(1_G * 1_G) = f(1_G) \circ f(1_G)$. Lygybės $f(1_G) \circ f(1_G) = f(1_G)$ abi puses padauginę, pavyzdžiui, iš kairės iš elemento $f(1_G)^{-1}$, gauname:

$$f(1_G)^{-1} \circ ((1_G) \circ f(1_G)) = f(1_G)^{-1} \circ f(1_G) = 1_H.$$

Kairioji šios lygybės pusė, kaip nesunku matyti, yra $f(1_G)$. Taigi $f(1_G) = 1_H$.

2. Kadangi $f(1_G) = 1_H$, tai $f(g{*}g^{-1}) = f(g){\circ}f(g^{-1}) = 1_H$. Panašiai galima gauti lygybę: $f(g^{-1}) \circ f(g) = 1_H$. Vadinasi, kiekvienam $g \in G$, $f(g^{-1}) = f(g)^{-1}$ (remiantis elementui atvirkštinio elemento apibrėžimu). $\square$

5.7.16 apibrėžimas. Tarkime, $(G, *), (H, \circ)$ – grupės, $f : G \to H$ – homomorfizmas. Grupės G poaibis

$$\ker f := \{g \in G \mid f(g) = 1_H\}$$

yra vadinamas homomorfizmo f *branduoliu.*

5.7.17 teiginys. *Tarkime,* $(G, *), (H, \circ)$ *– grupės,* $f : G \to H$ *– homomorfizmas. Homomorfizmo* f *branduolys* $\ker f$ *yra grupės* G *normalusis pogrupis.*

Įrodymas. $1_G \in \ker f$, nes $f(1_G) = 1_H$. Vadinasi, $\ker f \neq \emptyset$. Pirmiausia įrodysime, kad $\ker f$ yra grupės G pogrupis.

1. Sakykime, $g_1, g_2 \in \ker f$, t. y. $f(g_1) = 1_H, f(1_H) = 1_H$. Tuomet $f(g_1 * g_2) = f(g_1) \circ f(g_2) = 1_H \circ 1_H = 1_H$, t. y. $g_1 * g_2 \in \ker f$.

2. Sakykime, $g \in \ker f$, t. y. $f(g) = 1_H$. Tuomet $f(g^{-1}) = f(g)^{-1} = 1_H^{-1} = 1_H$, t. y. $g^{-1} \in \ker f$.

Taigi $\ker f$ – grupės G pogrupis. Dabar įsitikinsime, kad $\ker f$ yra grupės G normalusis pogrupis. Tam įrodysime: jei $g \in G, g' \in \ker f$, tai $g * g' * g^{-1} \in \ker f$. Tikriname: $f(g * g' * g^{-1}) = f(g) \circ f(g') \circ f(g^{-1}) = f(g) \circ 1_H \circ f(g^{-1}) = f(g) \circ f(g^{-1}) = 1_H$ (nes $f(g^{-1}) = f(g)^{-1}$). □

5.7.18 teiginys. *Tarkime,* $(G, *), (H, \circ)$ *– grupės,* $f : G \to H$ *– homomorfizmas. Jei* $\ker f = \{1_G\}$*, tai* f *– injekcinis homomorfizmas.*

Įrodymas. Jei $f(g_1) = f(g_2)$, tai $f(g_1) \circ f(g_2)^{-1} = 1_H$. Bet $f(g_1) \circ f(g_2)^{-1} = f(g_1) \circ f(g_2^{-1}) = f(g_1 * g_2^{-1}) = 1_H$. Vadinasi, $g_1 * g_2^{-1} \in \ker f = \{1_G\}$, t. y. $g_1 * g_2^{-1} = 1_G$ arba $g_1 = g_2$. □

5.7.19 išvada. *Baigtinės izomorfinės grupės* $(G, *), (H, \circ)$ *turi tokį patį tos pačios eilės elementų skaičių.*

Įrodymas. Tarkime, kad $f : G \to H$ – izomorfizmas, $g \in G$, – n-tosios eilės elementas (t. y. $g^n = 1_G$, bet $g^j \neq 1_G$, jei $0 < j < n$). Tuomet $f(g^n) = f(g)^n = 1_H$, bet $f(g^j) = f(g)^j \neq 1_H$, kai $0 < j < n$, nes $g^j \neq 1_G$ ir f – bijekcija. □

5.7.20. Pavyzdžiui, remdamiesi pastarąja išvada, įsitikinsime, kad diedro grupė D_{12} nėra izomorfinė grupei S_4 (kiekviena šių grupių turi po 24 elementus). Iš tikrųjų: grupė D_{12} 2-osios eilės elementų turi 13, o grupė S_4 2-osios eilės elementų turi tik 9. Grupės $D_{2^{n-1}}$ ir $(P(\mathbb{N}_n), \ominus)$, čia $n > 2$, taip pat nėra izomorfinės, nors $|D_{2^{n-1}}| = |(P(\mathbb{N}_n)| = 2^n$. Grupė $(P(\mathbb{N}_n), \ominus)$ – komutatyvi, o grupė $D_{2^{n-1}}$ nėra komutatyvi.

Pratimai.

1. Įrodykite, kad grupės $(G, *)$ automorfizmų aibė $\mathcal{A}ut(G, *)$ atvaizdžių kompozicijos $\circ$ atžvilgiu sudaro grupę $(\mathcal{A}ut(G, *), \circ)$.

   5.7.21 pastaba. Priminsime, kad anksčiau pakankamai bendru atveju apibrėžėme aibės X su struktūta $\mathcal{F}$ (algebrine ar kitokia) simetrijų grupę $(\mathcal{A}ut(X, \mathcal{F}), \circ)$ (žr. 5.1.27). Aibės X atveju $\mathcal{A}ut(X)$ žymėjome visų bijekcijų $f : X \to X$ aibę. Ir šiuo atveju $(\mathcal{A}ut(X), \circ)$ galime interpretuoti kaip aibės X simetrijų grupę ir šis žymėjimas yra suderintas su ankstesniu žymėjimu $(\mathcal{A}ut(X, \mathcal{F}), \circ)$, kai $\mathcal{F} = \emptyset$. Jei aibėje G yra apibrėžta grupės struktūra, tai $\mathcal{A}ut(G, *)$ žymime visų bijekcijų $f : G \to G$, išsaugančių grupės G struktūrą, aibę. Ir šiuo atveju grupę $(\mathcal{A}ut(G, *), \circ)$ galime interpretuoti kaip grupės G simetrijų grupę. Kaip matome, visi žymėjimai yra suderinti ir jokių dviprasmybių iškilti negali. Sutarsime grupės G automorfizmų grupės $(\mathcal{A}ut(G, *), \circ)$ žymėjimą sutrumpinti ir vietoje $(\mathcal{A}ut(G, *), \circ)$ rašyti $\mathcal{A}ut(G)$.

2. Kiekvienam grupės $(G, *)$ elementui g galime priskirti izomorfizmą

   $$f_g : G \to G,\ f_g(x) = g * x * g^{-1},\ x \in G,$$

   vadinamą grupės G *vidiniu automorfizmu*. Įsitikinkite, kad f_g iš tikrųjų yra grupės G automorfizmas. Visų grupės G vidinių automorfizmų aibė $\mathcal{I}nt(G)$ atvaizdžių kompozicijos $\circ$ atžvilgiu sudaro grupę $(\mathcal{I}nt(G), \circ)$, vadinamą grupės G vidinių automorfizmų grupe. Šią grupę sutarkime žymėti $\mathcal{I}nt(G)$. Grupė $\mathcal{I}nt(G)$ yra izomorfinė grupei $G/Z(G)$.

3. Įrodykite, kad atvaizdis $F : G \to \mathcal{I}nt(G), F(g) = f_g, g \in G$, čia

   $$f_g : G \to G,\ f_g(x) = g * x * g^{-1},\ x \in G,$$

   – grupės G vidinis automorfizmas, yra homomorfizmas. Įrodykite, kad šio homomorfizmo branduolys $\ker F$ yra grupės G centras $Z(G)$. Priminsime: $Z(G) := \{g \in G |\ g * x = x * g, x \in G\}$. Galima apibrėžti grupės G *išorinių automorfizmų grupę* kaip $\mathcal{A}ut(G)/\mathcal{I}nt(G)$.

4. Įrodykite, kad grupės $(G, *)$ vidinių automorfizmų grupė $\mathcal{I}nt(G)$ yra grupės G visų automorfizmų grupės $\mathcal{A}ut(G)$ normalusis pogrupis.

5. Raskite diedro grupių D_6, D_7, D_8 vidinių automorfizmų grupes (raskite šių grupių centrus, o paskui faktogrupes $D_6/Z(D_6)$, $D_7/Z(D_7)$, $D_8/Z(D_8)$).

6. Raskite grupių $\mathcal{A}ff(\mathbb{Q}), \mathcal{A}ff(\mathbb{R})$ vidinių automorfizmų grupes.

7. Raskite grupės S_4 vidinių automorfizmų grupę.

8. Įrodykite, kad Abelio grupės G vidinių automorfizmų grupė $\mathcal{I}nt(G) = \{\mathrm{id}\}$.
9. Tarkime, kad $f : X \to X$ – bijekcija. Ar aibės X bijekcija f generuoja grupės $(P(X), \ominus)$ automorfizmą?

5.7.22 teiginys. *Tarkime,* $(G, *), (H, \circ)$ *– grupės,* $f : G \to H$ *– homomorfizmas. Tuomet:*

1. *Jei K – grupės G pogrupis, tai $f(K)$ yra grupės H pogrupis.*
2. *Jei N – grupės H pogrupis, tai $f^{-1}(N)$ yra grupės G – pogrupis ir* $\ker f \subset f^{-1}(N)$.
3. *Jei N – grupės H normalusis pogrupis, tai $f^{-1}(N)$ yra grupės G normalusis pogrupis.*
4. *Jei f – siurjekcinis homomorfizmas (t. y. f(G)=H), K – grupės G normalusis pogrupis, tai ir $f(K)$ yra grupės H normalusis pogrupis.*

Įrodymas. 1. Sakykime, $y_1, y_2 \in f(K)$. Tada egzistuoja tokie $k_1, k_2 \in K$, kad $f(k_1) = y_1, f(k_2) = y_2$. Vadinasi, $y_1 * y_2^{-1} = f(k_1) \circ f(k_2)^{-1} = f(k_1) \circ f(k_2^{-1}) = f(k_1 * k_2^{-1}) \in f(K)$, nes $k_1 * k_2^{-1} \in K$.

2. Sakykime, $x_1, x_2 \in f^{-1}(N)$, t. y. $f(x_1), f(x_2) \in N$. Tada $x_1 * x_2^{-1} \in f^{-1}(N)$, nes $f(x_1 * x_2^{-1}) = f(x_1) \circ f(x_2)^{-1} \in N$ (priminsime: N yra pogrupis ir jei $f(x_1), f(x_2) \in N$, tai $f(x_1) \circ f(x_2)^{-1} \in N$). Kadangi $1_H \in N$, tai $f^{-1}(1_H) = \ker f \subset f^{-1}(N)$.

3. Sakykime, $g \in G,\ x \in f^{-1}(N)$. Tada $g*x*g^{-1} \in f^{-1}(N)$, nes $f(g*x*g^{-1}) = f(g) \circ f(x) \circ f(g)^{-1} \in N$ (N –normalusis pogrupis, $f(x) \in N$).

4. Sakykime, $h \in H, y \in f(K)$. Vadinasi, egzistuoja toks $g \in G$, kad $f(g) = h$, ir egzistuoja toks $k \in K$, kad $f(k) = y$. Tada $h \circ y \circ h^{-1} = f(g) \circ f(k) \circ f(g)^{-1} = f(g * k * g^{-1}) \in f(K)$, nes $g * k * g^{-1} \in K$ (priminsime, kad K – normalusis pogrupis, $k \in K$). □

5.7.23 teorema. *Jei H, K yra grupės $(G, *)$ pogrupiai, H – normalusis pogrupis, tai $H * K = K * H$ yra grupės G pogrupis.*

Įrodymas. Priminsime, kad $H * K = \{h * k \mid h \in H, k \in K\}$. Sakykime, $h_1 * k_1,\ h_2 * k_2 \in H * K$. Tuomet

$$h_1 * k_1 (h_2 * k_2)^{-1} = h_1 * k_1 * k_2^{-1} * h_2^{-1} =$$

$$\underbrace{h_1 * (k_1 * k_2^{-1}) * h_2^{-1} * (k_1 * k_2^{-1})^{-1}} * (k_1 * k_2^{-1}).$$

Kadangi H – normalusis pogrupis, tai

$$(k_1 * k_2^{-1}) * h_2^{-1} * (k_1 * k_2^{-1})^{-1} \in H \Rightarrow$$

$$h_1 * (k_1 * k_2^{-1}) * h_2^{-1} * (k_1 * k_2^{-1})^{-1} \in H \Rightarrow$$
$$\underbrace{h_1 * (k_1 * k_2^{-1}) * h_2^{-1} * (k_1 * k_2^{-1})^{-1}} * (k_1 * k_2^{-1}) \in H * K,$$

nes $k_1 * k_2^{-1} \in K$ (K – pogrupis, vadinasi, jei $k_1, k_2 \in K$, tai ir $k_1 * k_2^{-1} \in K$). Taigi įrodėme, kad $H * K$ yra grupės G pogrupis. Jei $k * h \in K * H$, tai $(k * h * k^{-1}) * k \in H * K$, t. y. $K * H \subset H * K$. Panašiai įrodoma, kad $H * K \subset K * H$. Taigi $H * K = K * H$. □

5.7.24 teiginys. *Tarkime,* $(G, *), (H, \circ)$ *– grupės,* N *– grupės* G *pogrupis,* $f : G \to H$ *– homomorfizmas. Tuomet*

$$f^{-1}(f(N)) = N * \ker f = \ker f * N$$

Įrodymas. Akivaizdu, kad $N \subset f^{-1}(f(N))$ ir $\ker f \subset f^{-1}(f(N))$ (kadangi $1_H \in f(N)$, o $\ker f = f^{-1}(1_H)$). Vadinasi, $N * \ker f \subset f^{-1}(f(N))$, nes $f^{-1}(f(N))$ – grupės G pogrupis. Tarkime, kad $x \in f^{-1}(f(N))$. Tada $f(x) \in f(N)$. Vadinasi, egzistuoja toks $k \in N$, kad $f(k) = f(x)$. Lygybę $f(k) = f(x)$, čia $k \in N, x \in f^{-1}(f(N))$, perrašome taip: $1_H = f(k)^{-1} \circ f(x) = f(k^{-1} * x)$. Matome, kad $k^{-1} * x \in \ker f$, čia $k \in N, x \in f^{-1}(f(N))$. Vadinasi, $x \in k * \ker f \subset N * \ker f$. Įrodėme: $f^{-1}(f(N)) = N * \ker f = \ker f * N$. □

5.7.25 išvada. *Jei* $(G, *), (H, \circ)$ *– grupės,* $f : G \to H$ *– siurjekcinis homomorfizmas, tai atvaizdis* F*, apibrėžtas grupės* H *visų pogrupių aibėje*

$$H \supset K \overset{F}{\mapsto} f^{-1}(K) \subset G,$$

čia K *– grupės* H *pogrupis, yra bijekcija tarp grupės* H *visų pogrupių ir grupės* G *visų tokių pogrupių* N*, kad* $\ker f \subset N$*. Be to,* $f^{-1}(K)$ *– grupės* G *normalusis pogrupis tada ir tik tada, kai* K *yra grupės* H *normalusis pogrupis.*

Įrodymas. Sakykime, K, K_1, K_2 – grupės H pogrupiai. Akivaizdu, kad jei $K_1 \neq K_2$, tai $F(K_1) = f^{-1}(K_1) \neq f^{-1}(K_2) = F(K_2), \ker f \subset f^{-1}(K) = F(K)$. Jei N yra toks grupės G pogrupis, kad $\ker f \subset N$, tai $f(N)$ yra grupės H pogrupis ir $F(f(N)) = f^{-1}(f(N)) = N * \ker f = N$. Paskutinis išvados teiginys išplaukia iš 5.7.22 teiginio trečiosios ir ketvirtosios dalių. □

5.7.26 teorema (pirmoji teorema apie izomorfizmą)**.** *Tarkime, kad* $(G, *)$, $(H, \circ)$ *– grupės,* $f : G \to H$ *– homomorfizmas. Tuomet grupės* G *faktorgrupė* $G/\ker f$ *pagal homomorfizmo* f *branduolį* $\ker f$ *yra izomorfinė grupei* $f(G) \subset H$.

Įrodymas. Kadangi homomorfizmo f branduolys $\ker f$ yra grupės G normalusis pogrupis, tai galima nagrinėti grupės G faktorgrupę $G/\ker f$ pagal $\ker f$. Apibrėžkime atvaizdį

$$\bar{f} : G/\ker f \to H, \ \bar{f}(g * \ker f) := f(g), \ g \in G.$$

Įsitikinsime, kad atvaizdis $\bar{f}$ korektiškai apibrėžtas, t. y. nepriklauso nuo normaliojo pogrupio $\ker f$ kairiosios gretutinės klasės $g * \ker f$ atstovo parinkimo. Jei $g_1 * \ker f = g_2 * \ker f$, $g_1^{-1} * g_2 \in \ker f$. Vadinasi, $f(g_1^{-1} * g_2) = 1_H$ arba $f(g_1) = f(g_2)$. Iš pastoriosios lygybės gauname: jei $g_1 * \ker f = g_2 * \ker f$, tai $\bar{f}(g_1 * \ker f) = \bar{f}(g_2 * \ker f)$.

Atvaizdis $\bar{f} : G/\ker f \to H$ yra homomorfizmas. Iš tikrųjų: bet kuriems $g_1, g_2 \in G$,

$$\bar{f}((g_1 * \ker f) * (g_2 * \ker f)) = \bar{f}(g_1 * g_2 * \ker f) =$$

$$= f(g_1 * g_2) = f(g_1) \circ f(g_2) = \bar{f}(g_1 * \ker f) \circ \bar{f}(g_2 * \ker f).$$

Dabar įsitikinsime, kad $\bar{f}$ – injekcinis homomorfizmas. Sakykime, $\bar{f}(g_1 * \ker f) = \bar{f}(g_2 * \ker f)$, t. y. $f(g_1) = f(g_2)$. Lygybę $f(g_1) = f(g_2)$ perrašykime taip: $1_H = f(g)^{-1} \circ f(g_2) = f(g_1^{-1} * g_2)$. Vadinasi, $g_1^{-1} * g_2 \in \ker f$, t. y. $g_1 * \ker f = g_2 * \ker f$.

Grupės $G/\ker f$ vaizdas yra $\bar{f}(G/\ker f) = f(G)$. Taigi $\bar{f} : G/\ker f \to f(G)$ – bijekcinis homomorfizmas, t. y. izomorfizmas. □

5.7.27 išvada. *Jei $(G, *), (H, \circ)$ – grupės, $f : G \to H$ – siurjekcinis homomorfizmas, tai grupė $G/\ker f$ yra izomorfinė grupei H.*

5.7.28 teorema (antroji teorema apie izomorfizmą)**.** *Jei H, K yra grupės $(G, *)$ pogrupiai, H – normalusis pogrupis, tai $H \cap K$ yra grupės K normalusis pogrupis ir grupė $K/K \cap H$ yra izomorfinė grupei $H * K/H$.*

Įrodymas. Atvaizdis $j : G \to G/H$, $j(g) = g * H$, $g \in G$, yra grupių homomorfizmas. Iš tikrųjų:

$$j(g_1 * g_2) = g_1 * g_2 * H = (g_1 * H) * (g_2 * H) = j(g_1) * j(g_2), g_1, g_2 \in G.$$

Akivaizdu, kad $\ker j = H$. Rasime pogrupio K vaizdą

$$j(K) = \{k * H \mid k \in K\}.$$

Aibė $j(K)$ sudaryta iš pogrupio H kairiųjų (tas pats, kas ir iš dešiniųjų) gretutinių klasių $k * H, k \in K$. Taigi $j(K) = K * H/H$. Homomorfizmo

$$j\big|_K : K \to G/H$$

branduolys $\ker j\big|_K = K \cap H$. Remiantis pirmąja teorema apie izomorfizmą, grupė $K/K \cap H$ yra izomorfinė grupei $K * H/H$. □

5.7.29 išvada. *Jei K, H – baigtinės grupės $(G, *)$ pogrupiai, H – normalusis pogrupis, tai $|K * H||K \cap H| = |H||K|$.*

Įrodymas. Kadangi grupės $K/K\cap H$ ir $K*H/H$ yra izomorfinės, tai $\big|K/K\cap H\big| = \big|K*H/H\big|$. Iš šios lygybės gauname: $|K|/|K\cap H| = |K*H|/|H|$ arba $|K*H||K\cap H| = |K||H|$. □

5.7.29 išvada teisinga bet kuriems baigtiniams pogrupiams H ir K. Priminsime, kad grupės G netuščių poaibių S ir T sandauga yra

$$ST := \{st \mid s\in S,\ t\in T\}.$$

5.7.30 teiginys. *Tarkime, kad H ir K yra baigtiniai grupės $(G,*)$ pogrupiai. Tuomet*

$$|K*H| = \frac{|K||H|}{|K\cap H|}.$$

Įrodymas. Tegu $h_1,\ h_2\in H$ ir $k_1,\ k_2\in K$. Įrodysime, kad lygybė

$$h_1k_1 = h_2k_2$$

yra teisinga tada ir tik tada, kai egzistuoja toks elementas $l\in K\cap H$, kad $h_2 = h_1l^{-1}$ ir $k_2 = lk_1$. Iš tikrųjų, jei $h_2 = h_1l^{-1}$, $k_2 = lk_1$ ir $l\in K\cap H$, tai $h_2\in H$, $k_2\in K$ ir $h_2k_2 = h_1k_1$. Dabar tarkime, kad $h_1k_1 = h_2k_2$, $h_1,\ h_2\in H$, $k_1,\ k_2\in K$. Tuomet $h_2^{-1}h_1 = k_2k_1^{-1}$. Pažymėkime $l := h_2^{-1}h_1 = k_2k_1^{-1}$. Tada $l\in K\cap H$. Be to, iš lygybės $l = k_2k_1^{-1}$ matyti, kad $k_2 = lk_1$, o iš lygybės $l = h_2^{-1}h_1$ – kad $h_2 = h_1l^{-1}$.

Taigi kiekvienas aibės $K*H = \{kh \mid k\in K, h\in H\}$ elementas užrašomas pavidalu kh, $k\in K$, $h\in H$, lygiai $|K\cap H|$ kartų, t. y.

$$|K*H| = \frac{|K||H|}{|K\cap H|}.$$

□

5.7.31 pastaba. 5.7.30 teiginyje pogrupių H ir K sandauga KH nebūtinai yra grupės G pogrupis.

5.7.32 teorema (trečioji teorema apie izomorfizmą)**.** *Jei K, H – grupės $(G,*)$ normalieji pogrupiai ir $K\subset H$, tai H/K yra grupės G/K normalusis pogrupis ir grupė $G/K\big/H/K$ yra izomorfinė grupei G/H.*

Įrodymas. Šią teoremą įrodyti paliekame skaitytojui. □

5.8 Grupių tiesioginės sandaugos

Jei grupė $(G, *)$ turi normalųjį pogrupį H, pagal kurį grupės G faktorgrupė G/H yra izomorfinė grupei K, tai grupė G yra vadinama *grupės H plėtiniu grupe K*. Bendruoju atveju aprašyti grupės H plėtinius grupe K – gana sudėtingas uždavinys. Šio bendrojo uždavinio paprastesni variantai, – tai grupių H ir K pusiau tiesioginės ir tiesioginė sandaugos. Dabar aptarsime grupių tiesioginę sandaugą.

5.8.1. Tarkime, $(H, *)$, $(K, \circ)$ – grupės. Apibrėžkime aibių H ir K Dekarto sandaugos $H \times K$ elementų daugybą $\bullet$:

$$(h_1, k_1) \bullet (h_2, k_2) := (h_1 * h_2, k_1 \circ k_2), \quad (h_1, k_1), (h_2, k_2) \in H \times K.$$

Akivaizdu, kad aibės $H \times K$ elementų daugyba $\bullet$ yra asociatyvi, $(1_H, 1_K)$ – šios daugybos atžvilgiu vienetas, elementui (h, k) atvirkštinis elementas yra (h^{-1}, k^{-1}). Kaip matome, aibė $H \times K$ jos elementų daugybos $\bullet$ atžvilgiu yra grupė.

5.8.2 apibrėžimas. Grupė $(H \times K, \bullet)$ yra vadinama grupių $(H, *), (K, \circ)$ *išorine tiesiogine sandauga*, o grupės $(H, *)$, $(K, \circ)$ – tiesioginės sandaugos komponentėmis.

5.8.3 pastaba. Tikriausiai pastebėjote, kad grupių tiesioginės sandaugos apibrėžime skirtingoms grupėms naudojome skirtingus grupių elementų daugybos ženklus. Tai darėme norėdami pabrėžti, kad gali būti imamos bet kokios grupės, o šias grupes tiesiogiai sudauginę, gauname visiškai naują grupę. Grupių $(H, *)$, $(K, \circ)$ tiesioginės sandaugos elementų daugybos ženklą būtų logiška žymėti $* \times \circ$. Bet tai per daug gremėzdiška. Sutarkime nuo šiol grupių elementų daugybos ženklus vėl žymėti žvaigždute, tašku ar kokiu nors kitokiu simboliu arba visiškai praleisti. Tarp tiesioginės sandaugos komponenčių elementų kompozicijos ženklų dažniausiai nerašysime. Grupių H ir K išorinę tiesioginę sandaugą dažniausiai žymėsime $H \times K$.

5.8.4 pastaba. Grupės $H \times K$ ir $K \times H$ yra izomorfinės: atvaizdis

$$f : H \times K \to K \times H, \ \ f((h, k)) = (k, h), \ \ h \in H, \ \ k \in K$$

yra izomorfizmas.

5.8.5. Jei $(H \times K, *)$ yra grupių H ir K išorinė tiesioginė sandauga, tai grupės $H \times K$ pogrupiai $\tilde{H} := \{(h, 1_K) \mid h \in H\}$ ir $\tilde{K} := \{(1_H, k) \mid k \in K\}$ yra izomorfiniai grupėms H ir K. Grupės $H \times K$ pogrupiai $\tilde{H}$ ir $\tilde{K}$ tenkina sąlygas:

1. Kiekvienas grupės $H \times K$ elementas (h, k) yra išreiškiamas pogrupių $\tilde{H}$ ir $\tilde{K}$ elementų $(h, 1_K)$ ir $(1_H, k)$ sandauga: $(h, k) = (h, 1_K) * (1_H, k)$.

2. $\tilde{H}$ ir $\tilde{K}$ yra normalieji pogrupiai.

3. $\tilde{H} \cap \tilde{K} = \{(1_H, 1_K)\}$.

Įrodysime 2-ąją iš šių savybių.
Jei $(h', k') \in H \times K$, $(h, 1_K) \in \tilde{H}$, tai

$$(h', k') * (h, 1_K) * (h', k')^{-1} = (h'hh'^{-1}, 1_K) \in \tilde{H}.$$

Panašiai įrodoma, kad $\tilde{K}$ taip pat yra grupės $H \times K$ normalusis pogrupis.

Grupės $H \times K$ pogrupių $\tilde{H}$ ir $\tilde{K}$ 1-ąją, 2-ąją ir 3-iąją savybes galima pakeisti ekvivalenčiomis savybėmis:

1'. Kiekvienas grupės $H \times K$ elementas (h, k) yra vienareikšmiškai išreiškiamas pogrupių $\tilde{H}$ ir $\tilde{K}$ elementų $(h, 1_K)$ ir $(1_H, k)$ sandauga: $(h, k) = (h, 1_K) * (1_H, k)$.

2'. Kievienas pogrupio $\tilde{H}$ elementas yra perstatomas su kiekvienu pogrupio $\tilde{K}$ elementu.

5.8.6 apibrėžimas. Grupė $(G, *)$ yra vadinama pogrupių H ir K (*vidine*) *tiesiogine sandauga* ir žymima $G = H \times K$, jei:

1. $G = H * K$.

2. H, K – grupės G yra normalieji pogrupiai.

3. $H \cap K = \{1\}$.

5.8.7 teiginys. *Jei grupė $(G, *)$ yra pogrupių H ir K tiesioginė sandauga, tai kiekvienas grupės G elementas vienareikšmiškai yra išreiškiamas pogrupių H ir K elementų sandauga ir, be to, kiekvienas pogrupio H elementas yra perstatomas su kiekvienu pogrupio K elementu.*

Įrodymas. Kadangi grupė G yra pogrupių tiesioginė sandauga, tai pogrupiai H, K yra normalieji, jų sankirta sudaryta iš grupės vieneto ir kievienas grupės G elementas yra išreiškiamas pogrupių H ir K elementų sandauga.

Jei $h \in H, k \in K$, tai elementų h, k komutatorius

$$[h, k] = h * k * h^{-1} * k^{-1} \in H \cap K.$$

Iš tikrųjų, kadangi H normalusis pogrupis ir $h \in H$, tai gauname, kad $h^{-1} \in H$, $k * h^{-1} * k^{-1} \in H$, vadinasi, ir $h * k * h^{-1} * k^{-1} \in H$. Kadangi K yra normalusis pogrupis ir $k \in K$, tai, panašiai kaip ir anksčiau, gauname, kad $h * k * h^{-1} * k^{-1} \in K$. Įrodėme, kad $[h, k] \in H \cap K$. Remdamiesi 3-iąja pogrupių H, K tiesioginės sandaugos savybe, gauname $[h, k] = 1$, t. y. $h * k = k * h$. Dabar įrodysime, kad kiekvienas grupės G elementas vienareikšmiškai išreiškiamas pogrupių H ir K elementų sandauga. Jei $g = h * k = h' * k'$, tai $h'^{-1} * h = k' * k^{-1} \in H \cap K$, nes kairiojoje lygybės pusėje esantis elementas priklauso pogrupiui H, o dešiniojoje – pogrupiui K. Vadinasi, $h'^{-1} * h = k' * k^{-1} = 1$, t. y. $h = h', k = k'$. □

5.8.8 pastaba. Jei grupė $(G, *)$ yra pogrupių H ir K tiesioginė sandauga, tai kiekvienam grupės G elementui g egzistuoja tokie vieninteliai $h \in H$ ir $k \in K$, kad $g = h * k = k * h$. Ir šiuo atveju rašysime $G = H \times K = K \times H$.

5.8.9 teiginys. *Jei kiekvienas grupės G elementas vienareikšmiškai yra išreiškiamas pogrupių H ir K elementų sandauga ir, be to, kiekvienas pogrupio H elementas yra perstatomas su kiekvienu pogrupio K elementu, tai grupė G yra pogrupių H ir K tiesioginė sandauga.*

Įrodymas. Kadangi kiekvienas grupės G elementas vienareikšmiškai yra išreiškiamas pogrupių H ir K elementų sandauga, tai $G = H * K$. Iš sąlygos, kad kiekvienas pogrupio H elementas yra perstatomas su kiekvienu pogrupio K elementu, gauname: kiekvienam $k \in K$, $k * H = \{k * h \mid h \in H\} = \{h * k \mid h \in H\} = H * k$. Panašiai kiekvienam $h \in H$ teisinga lygybė: $h * K = K * h$. Kadangi kiekvienam $h \in H$, $h * H = H = H * h$ ir kiekvienam $k \in K$, $k * K = K = K * k$, tai kiekvienam grupės G elementui g, $g * H = h * k * H = h * H * k = H * h * k = H * g$ (čia elementas g yra išreikštas pogrupių H, K elementų sandauga: $g = h * k$). Panašiai įrodoma lygybė $g * K = K * g, g \in G$. Kaip matome, pogrupiai H, K yra grupės G normalieji pogrupiai.

Įrodysime, kad pogrupių H ir K sankirta $H \cap K = \{1\}$. Jei būtų $q \in H \cap K$, $q \neq 1$, tai grupės G elemento g išraišką pogrupių H, K elementų h ir k sandauga $g = h*k$ galėtume užrašyti taip: $g = h*k = h*(q*q^{-1}*k) = (h*q)*(q^{-1}*k)$. Taigi matome, kad $h, h*q \in H$, $h \neq h*q$, $k, q^{-1}*k \in K$, t. y. grupės G elementas g yra išreiškiamas pogrupių H ir K elementų sandauga bent dviem skirtingais būdais. Tai prieštarauja teiginio sąlygai, kad kiekvienas grupės G elementas vienareikšmiškai yra išreiškiamas pogrupių H ir K elementų sandauga. □

5.8.10 pastaba. Kad grupė yra tiesioginė pogrupių sandauga, galima apibrėžti dviem skirtingais ekvivalenčiais būdais. Pirmasis grupės tiesioginės sandaugos apibrėžimas nusakomas šiomis sąlygomis:

(i) kiekvienas grupės elementas išreiškiamas pogrupių elementų sandauga;

(ii) šie pogrupiai yra grupės normalieji pogrupiai;

(iii) šių pogrupių sankirta sudaryta tik iš grupės vieneto.

Antrasis apibrėžimas, ekvivalentus pirmajam, nusakomas taip:

(i) kiekvienas grupės elementas vienareikšmiškai išskaidomas į pogrupių elementų sandaugą;

(ii) šių pogrupių elementai tarpusavyje perstatomi.

5.8.11 pastaba. Grupių išorinės tiesioginės sandaugos ir tiesioginės sandaugos sąvokos yra ekvivalenčios. Jei grupė $(H\times K,*)$ yra grupių H ir K išorinė tiesioginė sandauga, tai ji yra anksčiau apibrėžtų pogrupių $\tilde{H}$ ir $\tilde{K}$, izomorfinių atitinkamai grupėms H, K, tiesioginė sandauga. Teisingas ir toks teiginys: jei grupė $(G,*)$ yra pogrupių H ir K tiesioginė sandauga, tai ji yra izomorfinė grupių H ir K išorinei tiesioginei sandaugai $H\times K$. Pastarąjį teiginį įrodysime.

Įrodymas. Kiekvienam grupės G elementui g egzistuoja tokia vienintelė sutvarkyta pora (h_g,k_g), $h_g\in H$, $k_g\in K$, kad $g=h_g*k_g$. Kiekvienam elementui $g\in G$ priskyrę porą $(h_g,k_g)\in H\times K$, gauname bijekciją $f:G\to H\times K$ (čia $G\to H\times K$ suprantame kaip išorinę grupių G ir H tiesioginę sandaugą). Jei $g_1=h_{g_1}*k_{g_1}$, $g_2=h_{g_2}*k_{g_2}$, tai

$$f(g_1*g_2)=f((h_{g_1}*k_{g_1})*(h_{g_2}*k_{g_2}))=f((h_{g_1}*h_{g_2})*(k_{g_1}*k_{g_2}))=$$

$$(h_{g_1}*h_{g_2},k_{g_1}*k_{g_2})=(h_{g_1},k_{g_1})*(h_{g_2},k_{g_2})=f(g_1)*f(g_2).$$

Kaip matome, bijekcija $f:G\to H\times K$ yra homomorfizmas. □

5.8.12. Dabar galime apibrėžti baigtinio grupių skaičiaus tiesioginę sandaugą.

Sakykime, $(H_1,*_1),(H_2,*_2),\dots,(H_n,*_n)$ yra grupės. Apibrėžkime aibių H_1, H_2, …, H_n Dekarto sandaugos

$$H_1\times H_2\times\cdots\times H_n$$

elementų daugybą $*$:

$$(h_1,h_2,\dots,h_n)*(h_1',h_2',\dots,h_n'):=(h_1*_1h_1',\ h_2*_2h_2',\ \dots,\ h_n*_nh_n'),$$

$$(h_1,h_2,\dots,h_n),\ (h_1,h_2,\dots,h_n)\in H_1\times H_2\times\cdots\times H_n.$$

Panašiai kaip ir dviejų grupių atveju įrodoma, kad $H_1\times H_2\times\cdots\times H_n$ jos elementų apibrėžtos daugybos $*$ atžvilgiu yra grupė.

5.8.13 apibrėžimas. Grupė $(H_1\times H_2\times\cdots\times H_n,*)$ yra vadinama grupių $(H_1,*_1)$, $(H_2,*_2)$, …, $(H_n,*_n)$ *išorine tiesiogine sandauga.*

5.8.14 apibrėžimas. Grupė $(G,*)$ yra vadinama pogrupių $H_1,H_2,\dots,H_n$ *tiesiogine sandauga*, jei:

1. $G=H_1*H_2*\cdots*H_n$.

2. Grupės G pogrupiai $H_1, H_2, \dots, H_n$ yra normalieji.

3. Kiekvienam j, $1 \le j \le n$,

$$(H_1 * H_2 * \cdots * \hat{H}_j * \cdots * H_n) \cap H_j = \{1\},$$

čia stogelis virš pogrupio reiškia, kad to pogrupio pogrupių sandaugoje nėra.

5.8.15. Panašiai kaip ir dviejų pogrupių atveju, kad grupė yra pogrupių tiesioginė sandauga, galima apibrėžti ir kitaip.

5.8.16 apibrėžimas. Grupė $(G, *)$ yra vadinama pogrupių H_1, H_2, $\dots$, H_n, tiesiogine sandauga, jei:

1. Kiekvienas grupės G elementas vienareikšmiškai išskaidomas pogrupių H_1, H_2, $\dots$, H_n elementų sandauga, t. y. kiekvienam grupės G elementui g egzistuoja vieninteliai tokie elementai $h_1 \in H_1, h_2 \in H_2, \dots, h_n \in H_n$, kad

$$g = h_1 * h_2 * \cdots * h_n.$$

2. Bet kurių dviejų skirtingų pogrupių H_i ir H_j, $1 \le i, j \le n, i \ne j$, elementai tarpusavyje perstatomi:

$$h_i \in H_i, h_j \in H_j \Rightarrow h_i * h_j = h_j * h_i,\ 1 \le i, j \le n, i \ne j.$$

Kaip ir dviejų grupių atveju, grupių išorinės tiesioginės sandaugos ir tiesioginės sandaugos sąvokos yra ekvivalenčios.

Pratimai.

1. Įrodykite, kad abu grupių tiesioginės sandaugos apibrėžimai yra ekvivalentūs.

2. Įrodykite, kad jei grupės $(H_1, *_1), (H_2, *_2), \dots, (H_n, *_n)$ yra komutatyvios, tai šių grupių išorinė tiesioginė sandauga – taip pat komutatyvi.

3. Įrodykite, kad dviejų baigtinių ciklinių grupių, kurių eilės yra tarpusavyje pirminiai skaičiai (didžiausias bendrasis daliklis lygus 1), tiesioginė sandauga yra ciklinė grupė.

4. Apibendrinkite 3-iąjį pratimą baigtinio skaičiaus baigtinių ciklinių grupių atvejui.

5.8.17. Grupių tiesioginę sandaugą galima apibrėžti ir begalinio grupių skaičiaus atveju.

Sakykime, $\{(G_\alpha, *)\}_{\alpha\in I}$ yra grupių šeima. Aibių šeimos $\{G_\alpha\}_{\alpha\in I}$ tiesioginės sandaugos $\prod\limits_{\alpha\in I} G_\alpha$ elementų daugybą $*$ apibrėžkime taip: jei

$$\{g_\alpha\}_{\alpha\in I}, \{h_\alpha\}_{\alpha\in I} \in \prod_{\alpha\in I} G_\alpha,$$

tai

$$\{g_\alpha\}_{\alpha\in I} * \{h_\alpha\}_{\alpha\in I} := \{g_\alpha * h_\alpha\}_{\alpha\in I}.$$

Akivaizdu, kad aibė $\prod\limits_{\alpha\in I} G_\alpha$ apibrėžtos jos elementų daugybos $*$ atžvilgiu sudaro grupę, kurią žymėsime $(\prod\limits_{\alpha\in I} G_\alpha, *)$.

5.8.18 apibrėžimas. Grupę

$$(\prod_{\alpha\in I} G_\alpha, *)$$

vadinsime grupių šeimos $\{(G_\alpha, *)\}_{\alpha\in I}$ *tiesiogine sandauga.*

Ši grupių tiesioginė sandauga yra vadinama *išorine.* Galima apibrėžti ir grupių vidinę tiesioginę sandaugą. Bet tuo atveju, kai grupių šeima yra begalinė, grupių išorinės ir vidinės tiesioginių sandaugų apibrėžimai nėra ekvivalentūs.

5.8.19 teiginys. *Tarkime, $\{G_\alpha\}_{\alpha\in I}$ yra grupės $(G, *)$ normaliųjų pogrupių šeima, generuojanti grupę G, ir kiekvienam $\alpha_0 \in I$,*

$$G_{\alpha_0} \cap \prod_{\alpha\in I\setminus\alpha_0} G_\alpha = \{1\}.$$

Tada kiekvienas grupės $(G, *)$ elementas vieninteliu būdu išreiškiamas normaliųjų pogrupių šeimos $\{G_\alpha\}_{\alpha\in I}$ elementų baigtine sandauga.

Įrodymas. Pirmiausia įrodysime, kad šeimos $\{G_\alpha\}_{\alpha\in I}$ bet kurių dviejų skirtingų pogrupių G_α, G_β elementai $g_\alpha \in G_\alpha, g_\beta \in G_\beta$ yra perstatomi, t. y. , bet kuriems $g_\alpha \in G_\alpha, g_\beta \in G_\beta, \alpha \neq \beta$,

$$g_\alpha * g_\beta = g_\beta * g_\alpha.$$

Imkime elementų $g_\alpha \in G_\alpha, g_\beta \in G_\beta$ komutatorių $[g_\alpha, g_\beta] = g_\alpha * g_\beta * g_\alpha^{-1} * g_\beta^{-1}$. Kadangi G_α ir G_β yra normalieji pogrupiai, tai $g_\beta * g_\alpha^{-1} * g_\beta^{-1} \in G_\alpha$, vadinasi, ir

$g_\alpha * g_\beta * g_\alpha^{-1} * g_\beta^{-1} \in G_\alpha$. Panašiai gauname, kad $g_\alpha * g_\beta * g_\alpha^{-1} * g_\beta^{-1} \in G_\beta$. Vadinasi, elementas $[g_\alpha, g_\beta] \in G_\alpha \cap G_\beta, \alpha \neq \beta$. Bet, remdamiesi sąlyga: kiekvienam $\alpha_0 \in I$,

$$G_{\alpha_0} \cap \prod_{\alpha \in I \setminus \alpha_0} G_\alpha = \{1\},$$

gauname, kad $G_\alpha \cap G_\beta = \{1\}$, jei tik $\alpha \neq \beta$. Taigi $[g_\alpha, g_\beta] = g_\alpha * g_\beta * g_\alpha^{-1} * g_\beta^{-1} = 1$ arba $g_\alpha * g_\beta = g_\beta * g_\alpha$.

Remdamiesi teoremos sąlyga, gauname, kad grupės $(G, *)$ kiekvienas elementas yra išreiškiamas pogrupių šeimos $\{G_\alpha\}_{\alpha \in I}$ elementų baigtine sandauga. Daugiklių tvarka nesvarbi, nes įrodėme, kad skirtingų šeimos pogrupių elementai yra perstatomi. Lieka įrodyti, kad kiekvienas grupės G elementas vieninteliu būdu išreiškiamas pogrupių šeimos $\{G_\alpha\}_{\alpha \in I}$ elementų sandauga. Tarkime, kad

$$g = \prod_{\alpha \in I} g_\alpha = \prod_{\alpha \in I} h_\alpha,$$

čia beveik visiems $\alpha \in I$ (išskyrus baigtinį skaičių), $g_\alpha = 1$. Reikia įrodyti, kad kiekvienam $\alpha \in I$, $g_\alpha = h_\alpha$. Nagrinėkime elementą

$$(\prod_{\alpha \in I} g_\alpha) * (\prod_{\alpha \in I} h_\alpha)^{-1} = \prod_{\alpha \in I} (g_\alpha * h_\alpha^{-1}) = 1.$$

Jei kuriam nors $\alpha_0 \in I$ būtų $g_{\alpha_0} * h_{\alpha_0}^{-1} \neq 1$, tai, remdamiesi lygybe

$$\prod_{\alpha \in I} (g_\alpha * h_\alpha^{-1}) = 1,$$

gautume:

$$1 \neq g_{\alpha_0}^{-1} * h_{\alpha_0} \in G_{\alpha_0} \cap \prod_{\alpha \in I \setminus \alpha_0} G_\alpha = \{1\},$$

o tai prieštarautų teoremos sąlygai. □

5.9 Grupės veikimas aibėje

5.9.1. Tegu G – grupė, X – aibė. Nagrinėkime grupės G, kaip operatorių aibės, ir aibės X elementų išorinį kompozicijos dėsnį (žr. 2.6.1 apibrėžimą) $F : G \times X \to X$, tenkinantį sąlygas:

1. Kiekvienam $x \in X$, $F(1, x) = x$, čia 1 – grupės G vienetas.

2. Bet kuriems $g_1, g_2 \in G$, $x \in X$, $F(g_1 g_2, x) = F(g_1, F(g_2, x))$.

Jei išorinį kompozicijos dėsnį F pažymėtume $*$ ir rašytume tarp komponuojamųjų elementų, tai anksčiau užrašytos sąlygos atrodytų taip:

1. Kiekvienam $x \in X$, $1 * x = x$, čia 1 – grupės G vienetas.

2. Bet kuriems $g_1, g_2 \in G$, $x \in X$, $(g_1 g_2) * x = g_1 * (g_2 * x)$.

5.9.2 pastaba. Tegu apibrėžtas grupės G ir aibės X elementų išorinis kompozicijos dėsnis, kurio reikšmių aibėjė yra X. Tuomet patogu pasakyti: „aibės X elementą x, *paveikę* grupės G elementu g, gauname $g * x$ “.

5.9.3. Grupės G, kaip operatorių aibės, ir aibės X elementų išorinis kompozicijos dėsnis $*$ apibrėžia aibėje X ekvivalentumo sąryšį: aibės X elementas x_2 yra vadinamas ekvivalenčiu elementui x_1, jei egzistuoja toks grupės G elementas g, kad $x_2 = g * x_1$. Įsitikinsime, kad tai iš tikrųjų ekvivalentumo sąryšis.

Pirma, kiekvienam aibės X elementui x, x yra ekvivalentus x, nes, remiantis pirmąja išorinio kompozicijos dėsnio $*$ savybe, $x = 1 * x$.

Antra, tegu x_2 yra ekvivalentus x_1, t. y. egzistuoja toks grupės G elementas g, kad $x_2 = g * x_1$. Tuomet, šios lygybės abi puses paveikę grupės G elementu g^{-1}, gauname: $g^{-1} * x_2 = g^{-1} * (g * x_1) = (g^{-1} g) * x_1 = 1 * x_1 = x_1$, t. y. x_1 yra ekvivalentus x_2.

Trečia, tarkime, x_3 yra ekvivalentus x_2, o x_2 yra ekvivalentus x_1, t. y. egzistuoja tokie $g, h \in G$, kad $x_3 = g * x_2$, $x_2 = h * x_1$. Tuomet, remdamiesi antrąja išorinio kompozicijos dėsnio $*$ savybe, gauname: $x_3 = g * x_2 = g * (h * x_1) = (gh) * x_1$, t. y. x_3 yra ekvivalentus x_1.

5.9.4 apibrėžimas. Kiekvienam aibės X elementui x apibrėžkime aibės X poaibį $G * x := \{g * x \mid g \in G\}$. Aibės X poaibis $G * x$ yra vadinamas elemento x *orbita.* Elemento x orbita $G * x$ yra elemento x ekvivalentumo klasė, ekvivalentumo sąryšio, apibrėžto išorinio kompozicijos dėsnio $*$, atžvilgiu.

5.9.5 pastaba. Tegu apibrėžtas grupės G ir aibės X elementų išorinis kompozicijos dėsnis, kurio reikšmių aibė yra X. Tuomet galime užrašyti lygybę:

$$X = \bigcup_{\alpha \in I} G * x_\alpha,$$

čia x_α, $\alpha \in I$, – skirtingų ekvivalentumo klasių atstovai. Kaip žinome, $G * x_\alpha \neq G * x_\beta$, jei $\alpha \neq \beta$, $\alpha \in I$.

5.9.6. Tarkime, kad apibrėžtas grupės G ir aibės X elementų išorinis kompozicijos dėsnis, kurio reikšmių aibė yra X.

5.9.7 apibrėžimas. Tegu $x \in X$. Grupės G poaibis $\{g \in G \mid g * x = x\}$ yra vadinamas elemento x *stabilizatoriumi* ir žymimas $\mathrm{st}_G(x)$.

5.9.8 teiginys. *Aibės X elemento x stabilizatorius $st_G(x)$ yra grupės G pogrupis.*

Įrodymas. Tarkime, $g_1, g_2 \in \mathrm{st}_G(x)$. Tuomet

$$(g_1 * g_2) * x = g_1 * (g_2 * x) = g_1 * x = x,$$

todėl $g_1 * g_2 \in \mathrm{st}_G(x)$. Be to, kadangi

$$g_1^{-1} * x = g_1^{-1} * (g_1 * x) = (g_1^{-1} * g_1) * x = \mathrm{id} * x = x,$$

$g_1^{-1} \in \mathrm{st}_G(x)$. Vadinasi, elemento $x \in X$ stabilizatorius $\mathrm{st}_G(x)$ yra grupės G pogrupis. $\square$

5.9.9 teiginys. *Jei aibės X elementas y priklauso elemento x orbitai $G * x$, tai elemento y stabilizatorius $st_G(y)$ yra sujungtinis grupės G pogrupis pogrupiui $st_G(x)$.*

Įrodymas. Priminsime, kad grupės G pogrupis H yra vadinamas *sujungtiniu pogrupiu* pogrupiui N, jei egzistuoja toks grupės G elementas g, kad $H = gNg^{-1}$.

Kadangi elementas $y \in G * x$, tai egzistuoja toks grupės G elementas g, kad $y = g * x$. Tuomet kiekvienam pogrupio $\mathrm{st}_G(x)$ elementui h elementas ghg^{-1} priklauso elemento y stabilizatoriui $\mathrm{st}_G(y)$, nes

$$(ghg^{-1}) * y = (gh) * (g^{-1} * y) = (gh) * x = g * (h * x) = g * x = y.$$

Vadinasi,

$$g\,\mathrm{st}_G(x)\,g^{-1} \subset \mathrm{st}_G(y).$$

Panašiai galima įsitikinti, kad $g\,\mathrm{st}_G(x)\,g^{-1} \supset \mathrm{st}_G(y)$. $\square$

5.9.10 teiginys. *Aibės X elemento x orbitos $G * x$ elementų skaičius yra lygus elemento x stabilizatoriaus $st_G(x)$ indeksui $[G : st_G(x)]$ grupėje G.*

Įrodymas. Nagrinėkime grupės G skaidinį pogrupio $\mathrm{st}_G(x)$ kairiosiomis gretutinėmis klasėmis:

$$G = \mathrm{st}_G(x) \cup g_2\,\mathrm{st}_G(x) \cup \cdots \cup g_r\,\mathrm{st}_G(x).$$

Įrodysime, kad elemento x orbitą $G * x$ sudaro aibės X elementai x, $g_2 * x$, …, $g_r * x$.

Pirmiausia pastebėsime, kad $h_1 * x = h_2 * x$ tada ir tik tada, kai grupės G elementai h_1 ir h_2 priklauso tai pačiai pogrupio $\mathrm{st}_G(x)$ kairiajai gretutinei klasei. Iš tikrųjų, lygybės $h_1 * x = h_2 * x$ abi puses paveikę grupės elementu h_2^{-1}, gauname

$$h_2^{-1} * (h_1 * x) = h_2^{-1} * (h_2 * x) = (h_2^{-1} h_2) * x = x,$$

t. y. $(h_2^{-1}h_1) * x = x$. Vadinasi, jei $h_1 * x = h_2 * x$, tai $h_2^{-1}h_1 \in \mathrm{st}_G(x)$, t. y. h_1 ir h_2 priklauso tai pačiai pogrupio $\mathrm{st}_G(x)$ kairiajai gretutinei klasei. Kadangi grupės G elementai $1, g_2, \ldots, g_r$ yra skirtingų pogrupio $\mathrm{st}_G(x)$ kairiųjų gretutinių klasių atstovai, tai aibės X elementai $x, g_1 * x, \ldots, g_r * x$ yra tarpusavyje skirtingi. Lieka įrodyti, kad kiekvienas orbitos $G * x$ elementas sutampa su kuriuo nors aibės $\{x,\ g_1 * x,\ \ldots,\ g_r * x\}$ elementu.

Tarkime, $y \in G * x$. Tuomet egzistuoja toks grupės G elementas g, kad $y = g * x$. Jei grupės G elementas g priklauso pogrupio $\mathrm{st}_G(x)$ kairiajai gretutinei klasei $g_j\,\mathrm{st}_G(x)$, tai $y = g * x = g_j * x$. □

5.9.11 pavyzdys. Tarkime, G – baigtinė grupė. Apibrėžkime atvaizdį

$$* : G \times G \to G,\ (g,\ h) \mapsto g * h := ghg^{-1},\ g, h \in G.$$

5.9.12 apibrėžimas. Grupės G elemento $h \in G$ ekvivalentumo klasė

$$\{ghg^{-1} \mid g \in G\}$$

vadinama elementui h *sujungtinių elementų klase* ir yra žymima $C_G(h)$.

Elemento $h \in G$ stabilizatorius $\mathrm{st}_G(h)$ yra sudarytas iš visų tokių grupės G elementų g, kurių kiekvienas yra perstatomas su elementu h. Grupių teorijoje elemento h stabilizatorius $\mathrm{st}_G(h)$ yra vadinamas elemento h *centralizatoriumi* ir yra žymimas $Z_G(h)$. Remiantis 5.9.10 teiginiu, grupės G elementui h sujungtinių elementų skaičius yra lygus elemento h centralizatoriaus $Z_G(h)$ indeksui $[G : Z_G(h)]$ grupėje G. Taigi kiekvienam elementui $h \in G$ sujungtinių elementų skaičius $|C_G(h)|$ dalija grupės G eilę $|G|$. Galime parašyti:

$$G = C_G(h_1) \cup C_G(h_2) \cup \cdots \cup C_G(h_s),$$

čia $h_1, h_2, \ldots, h_s$ – sujungtinių elementų skirtingų klasių atstovai.

5.9.13 pavyzdys. Tarkime, G – grupė, $X = P_0(G)$ – grupės G visų pogrupių aibė. Apibrėžkime grupės G ir aibės X elementų išorinį kompozicijos dėsnį taip:

$$* : G \times X \to X,\ (g, H) \mapsto g * H := gHg^{-1},\ g \in G,\ G \supset H - \text{ pogrupis.}$$

Aibės X elemento H ekvivalentumo klasė yra sudaryta iš vieno elemento H tada ir tik tada, kai H yra grupės G normalusis pogrupis. Aibės X elementai H ir N yra ekvivalentūs tada ir tik tada, kai grupės G pogrupiai H ir N yra sujungtiniai. Kitaip tariant, aibės X elementai H ir N yra ekvivalentūs tada ir tik tada, jei egzistuoja toks grupės G elementas g, kad $H = gNg^{-1}$. Taigi aibės X elemento H orbita sudaryta iš grupės G pogrupių, kurie yra sujungtiniai pogrupiui H.

Aibės X elemento H stabilizatorius $\mathrm{st}_G(H)$ grupių teorijoje yra vadinamas grupės G pogrupio H *normalizatoriumi* ir yra žymimas $N_G(H)$. Kaip ir 5.9.11 pavyzdyje, grupės G pogrupiui H sujungtinių pogrupių skaičius dalija grupės G eilę $|G|$.

Šiuo atveju 5.9.10 teiginį galima perrašyti taip:

5.9.14 teiginys. *Baigtinės grupės G pogrupiui H sujungtinių pogrupių skaičius lygus to pogrupio normalizatoriaus $N_G(H)$ indeksui $[G : N_G(H)]$ grupėje G.*

5.9.15 pavyzdys. Remdamiesi grupės G ir aibės X elementų išorinio kompozicijos dėsnio sąvoka, įrodysime svarbų faktą apie p-grupes.

5.9.16 apibrėžimas. Grupė G yra vadinama *p-grupe*, jei šios grupės kiekvieno elemento eilė yra lygi pirminio skaičiaus p laipsniui.

5.9.17 pastaba. Jei p-grupė G yra baigtinė, tai, remdamiesi Koši teorema (kurią įrodysime vėliau): jei baigtinės grupės eilė dalijasi iš pirminio skaičiaus p, tai grupė turi p eilės elementą, gauname, kad grupės G eilė $|G|$ yra lygi pirminio skaičiaus p laipsniui p^n. Taigi baigtinės grupės atveju p-grupę galima apibrėžti kaip grupę G, kurios eilė $|G|$ yra lygi pirminio skaičiaus laipsniui p^n.

5.9.18 teorema. *Kiekviena baigtinė p-grupė G turi netrivialų centrą $Z(G)$ (t. y. $Z(G) \neq \{1\}$).*

Įrodymas. Apibrėžkime p-grupės G, kaip operatorių aibės, ir aibės $X = G$ išorinį kompozicijos dėsnį:

$$* : G \times G \to G,\ g * h = ghg^{-1},\ g, h \in G.$$

Šiuo atveju aibės G elemento h orbita $G * h = \{ghg^{-1} \mid g \in G\}$ yra grupės G elementui h sujungtinių elementų klasė. Sakykime, $G * h_1$, $G * h_2$, $\dots$, $G * h_s$ – visos skirtingos G elementų orbitos, t. y.

$$G = G * h_1 \cup G * h_2 \cup \dots \cup G * h_s.$$

Remdamiesi šia lygybe, galime užrašyti

$$|G| = |G * h_1| + |G * h_2| + \dots + |G * h_s|. \tag{5.2}$$

Kadangi kiekvienos orbitos elementų skaičius yra lygus šios orbitos bet kurio elemento stabilizatoriaus indeksui, kiekvienos orbitos elementų skaičius yra pirminio skaičiaus p laipsnis (p-grupės tiek kiekvieno pogrupio eilė, tiek pogrupio indeksas yra pirminio skaičiaus p laipsnis). Vadinasi, jei kurio nors p-grupės G elemento h orbita $G * h$ sudaryta daugiau nei iš vieno elemento, tai $p \mid |G * h|$. Grupės G vieneto 1 orbita yra $\{1\}$. Kadangi $p \mid |G|$, tai pirminis skaičius p dalija ir dešiniąją (5.2) lygybės pusę. Kadangi (5.2) lygybės dešinėje pusėje yra vienas dėmuo, lygus 1, tai dešinėje pusėje turi būti dar bent vienas dėmuo, lygus $1 = p^0$. Tarkime, $|G * h_j| = 1$, čia h_j nėra grupės G vienetas. $|G * h_j| = 1$ tada ir tik tada, kai $G * h_j = \{h_j\}$, t. y., kai kiekvienam $g \in G$, $gh_jg^{-1} = h_j$. O tai ir reiškia, kad $h_j \in Z(G)$. □

5.9.19. Sakykime, apibrėžtas grupės G ir aibės X elementų išorinis kompozicijos dėsnis $*$. Galima užrašyti aibės X elementų skirtingų orbitų skaičiaus formulę. Pažymėkime $N(g)$ aibės X elementų, tenkinančių sąlygą $g * x = x$, skaičių. Nagrinėkime sumą

$$\sum_{g \in G} N(g).$$

Imkime $x \in X$. Elementas x į užrašytą sumą yra įskaičiuojamas $|\mathrm{st}_G(x)|$ kartų, nes kiekvienam $g \in \mathrm{st}_G(x)$, $g * x = x$. Į anksčiau užrašytą sumą $|\mathrm{st}_G(x)|$ kartų yra įskaičiuojamas ir kiekvienas elemento x orbitos $G * x$ elementas. Taigi elemento x orbitos $G * x$ elementų indėlis į nagrinėjamą sumą yra lygus

$$|G * x| \cdot |\mathrm{st}_G(x)| = [G : \mathrm{st}_G(x)] \cdot |\mathrm{st}_G(x)| = |G|.$$

Vadinasi, aibės X elementų skirtingų orbitų skaičius lygus

$$\frac{1}{|G|} \sum_{g \in G} N(g).$$

5.10 Baigtinių Abelio grupių struktūra

Nagrinėsime baigtines Abelio grupes.

5.10.1 apibrėžimas. Grupė G, kurios kiekvieno elemento eilė yra lygi pirminio skaičiaus p laipsniui, yra vadinama *p-grupe*. Abelio p-grupė dažnai yra vadinama *primariąja p-grupe*.

5.10.2 teorema (Koši teorema)**.** *Jei Abelio grupės G eilė n dalijasi iš pirminio skaičiaus p, tai grupė G turi p eilės elementą.*

Įrodymas. Teoremą įrodysime matematinės indukcijos metodu. Jei $n = 1$, tai teoremos teiginys teisingas, nes 1 nesidalija iš jokio pirminio skaičiaus. Tarkime, kad teoremos teiginys teisingas kiekvienai Abelio grupei, kurios eilė $m < n$. Imkime grupės G elementą $g \neq 1$ ir nagrinėkime ciklinę grupę $\langle g \rangle$. Jei $\langle g \rangle = G$, tai elemento $g^{\frac{n}{p}}$ eilė yra p. Jei $\langle g \rangle \subset G$, $\langle g \rangle \neq G$, tai galimi du atvejai:

- $p \big| |\langle g \rangle|$ ir

- $p \not| |\langle g\rangle|$.

Pirmuoju atveju pogrupio $\langle g\rangle$ eilė $|\langle g\rangle| < n$ ir dalijasi iš skaičiaus p. Vadinasi, remdamiesi indukcine prielaida, gauname, kad šiuo atveju teorema įrodyta. Antruoju atveju grupės G faktorgrupės $G/\langle g\rangle$ pagal pogrupį $\langle g\rangle$ eilė $|G/\langle g\rangle| = \frac{|G|}{|\langle g\rangle|} < n$ ir dalijasi iš skaičiaus p. Remdamiesi indukcine prielaida, gauname, kad grupė $G/\langle g\rangle$ turi p eilės elementą $h * \langle g\rangle$, t. y. $(h * \langle g\rangle)^p = \langle g\rangle$, $(h * \langle g\rangle)^j \neq \langle g\rangle$, kai $0 < j < p$. Lygybė $(h * \langle g\rangle)^p = \langle g\rangle$ ekvivalenti sąlygai $h^p \in \langle g\rangle$, t. y. egzistuoja toks $s \in \mathbb{N}$, kad $h^p = g^s$. Elemento h eilė yra lygi pt, čia t – toks mažiausias teigiamas skaičius, kad $(g^s)^t = 1$. Vadinasi, elemento h^t eilė yra lygi p. □

5.10.3 išvada. *Baigtinės Abelio p-grupės G eilė yra lygi pirminio skaičiaus p laipsniui.*

Įrodymas. Iš tikrųjų, jei Abelio p-grupės G eilė $|G|$ dalytųsi iš pirminio skaičiaus $q \neq p$, tai, remiantis įrodyta teorema, grupė G turėtų q eilės elementą. O tai prieštarautų sąlygai, kad G yra p-grupė. □

Dabar įrodysime Koši teoremą bendruoju atveju.

5.10.4 teorema (Koši teorema)**.** *Jei baigtinės grupės G eilė dalijasi iš pirminio skaičiaus p, tai grupė G turi p eilės elementą.*

Įrodymas. Šią teoremą įrodysime taip pat matematinės indukcijos metodu. Jei grupės G eilė lygi 1, tai teoremos teiginys teisingas. Tarkime, kad teoremos teiginys teisingas kiekvienai grupei, kurios eilė $m < n$. Jei egzistuoja grupės G pogrupis H, $H \neq G$, kurio eilė dalijasi iš pirminio skaičiaus p, tai, remdamiesi indukcine prielaida, gauname, kad teoremos teiginys teisingas. Nagrinėkime atvejį, kai nė vieno grupės G pogrupio eilė nesidalija iš skaičiaus p. Sudarykime grupės G skaidinį sujungtinių elementų klasėmis

$$G = \bigcup_{j=1}^{r} C(g_j) \cup \bigcup_{z \in Z(G)} \{z\},$$

čia g_j sujungtinių elementų skirtingų klasių atstovai, nepriklausantys grupės G centrui $Z(G)$. Taigi galime užrašyti lygybę:

$$|G| = |Z(G)| + \sum_{j=1}^{r} |C(g_j)|.$$

Grupės G elementui g sujungtinių elementų skaičius $|C(g)|$ yra lygus elemento g centralizatoriaus $Z_G(g)$ indeksui $[G : Z_G(g)]$ grupėje G. Grupės G elemento z, priklausančio grupės G centrui, sujungtinių elementų klasė sudaryta tik iš vieno elemento $\{z\}$, nes kiekvieno grupės centro elemento centralizatorius sutampa su grupe G. Elemento g, nepriklausančio centrui, centralizatorius $Z_G(g)$ yra grupės G pogrupis, nesutampantis su grupe G. Kadangi pogrupio $Z_G(g)$ eilė pagal padarytą prielaidą nesidalija iš pirminio skaičiaus p, o grupės G eilė dalijasi iš p, tai ir pogrupio $Z_G(g)$ indeksas $[G : Z_G(g)]$ grupėje G dalijasi iš p. Vadinasi, kiekvienas sumos

$$\sum_{j=1}^{r} |C(g_j)|$$

dėmuo $|C(g_j)|$, $1 \le j \le r$, dalijasi iš p. Gauname, kad iš skaičiaus p dalijasi ir grupės G centro $Z(G)$ eilė. Tai įmanoma, remiantis padaryta prielaida (kad grupės G kiekvieno netrivialaus pogrupio (t. y. $\neq G$) eilė nesidalija iš pirminio skaičiaus p), tik tuo atveju, jei $Z(G) = G$. O Abelio grupėms šią teoremą įrodėme. □

5.10.5 išvada. *Jei G yra baigtinė p-grupė, tai grupės G eilė $|G|$ yra pirminio skaičiaus p laipsnis.*

5.10.6 teorema. *Sakykime, kad baigtinės Abelio grupės G eilė yra n,*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

– skaičiaus n kanoninis skaidinys pirminiais skaičiais. Tuomet grupė G yra vienareikšmiškai išskaidoma į p_j-pogrupių G_j, $1 \le j \le r$, tiesioginę sandaugą

$$G = \prod_{j=1}^{r} G_j$$

(t. y. pogrupiai G_j, $1 \le j \le r$, yra nusakomi vienareikšmiškai). Pogrupio G_j eilė yra lygi $p_j^{\alpha_j}$, $1 \le j \le r$.

Įrodymas. Sudarykime skaičius $n_j = n/p_j^{\alpha_j}$, $1 \le j \le r$. Šių skaičių didžiausias bendrasis daliklis yra lygus 1 (akivaizdu: $p_i \mid n_j$, $i \neq j$, bet $p_i \nmid n_i$, $1 \le i, j \le r$). Vadinasi, egzistuoja tokie sveikieji skaičiai q_j, $1 \le j \le r$, kad

$$\sum_{j=1}^{r} n_j q_j = 1.$$

Kadangi G yra Abelio grupė, tai grupės G elementų g, pakeltų n_j laipsniais, aibė

$$G_j = \{g^{n_j} \mid g \in G\}, \ \ 1 \le j \le r,$$

yra grupės G pogrupis. Iš tikrųjų, jei $g_1^{n_j}, g_2^{n_j} \in G_j$, tai

$$g_1^{n_j}(g_2^{n_j})^{-1} = (g_1 g_2^{-1})^{n_j} \in G_j, \ \ 1 \le j \le r.$$

Kiekvienam j, $1 \leq j \leq r$, G_j yra grupės G p_j-pogrupis, nes kiekvienas pogrupio G_j elementas, pakeltas $p_j^{\alpha_j}$ laipsniu, yra grupės G vienetas 1. Iš tikrųjų, jei $g^{n_j} \in G_j$, tai

$$(g^{n_j})^{p_j^{\alpha_j}} = g^n = 1$$

(priminsime, kad grupės elemento eilė dalija grupės eilę). Dabar įrodysime, kad kiekvienas grupės G elementas g yra vienareikšmiškai išreiškiamas pogrupių G_j, $1 \leq j \leq r$, elementų sandauga. Imkime $g \in G$. Tuomet

$$g^1 = g^{n_1 q_1 + \cdots + n_r q_r} = \prod_{j=1}^{r} (g^{n_j})^{q_j}.$$

Kiekvienam j, $1 \leq j \leq r$, elementas g^{n_j} priklauso pogrupiui G_j, vadinasi, ir $(g^{n_j})^{q_j} \in G_j$. Pažymėję $g_j := (g^{n_j})^{q_j}$, gauname lygybę

$$g = \prod_{j=1}^{r} g_j.$$

Lieka įrodyti šios sandaugos vienatį.

Tarkime, kad

$$g = \prod_{j=1}^{r} g_j = \prod_{j=1}^{r} g'_j,$$

$g_j, g'_j \in G_j$, $j = 1, 2, \ldots, r$. Bet kuriam $s \in \{1, 2, \ldots, r\}$ pastarąją lygybę galime perrašyti

$$g_s^{-1} {g'}_s = \prod_{\substack{j=1 \\ j \neq s}}^{r} g_j {g'}_j^{-1}.$$

Kadangi $g_s^{-1} {g'}_s \in G_s$,

$$(g_s^{-1} {g'}_s)^{p_s^{\alpha_s}} = 1.$$

Iš kitos pusės,

$$(g_s^{-1} {g'}_s)^{n_s} = (\prod_{\substack{j=1 \\ j \neq s}}^{r} g_j {g'}_j^{-1})^{n_s} = \prod_{\substack{j=1 \\ j \neq s}}^{r} (g_j {g'}_j^{-1})^{n_s} = \prod_{\substack{j=1 \\ j \neq s}}^{r} g_j^{n_s} ({g'}_j^{-1})^{n_s} = 1,$$

nes kiekvienam j, $1 \leq j \leq r$, $j \neq s$, skaičius n_s dalijasi iš $p_j^{\alpha_j}$. Kadangi kiekvienam s, $1 \leq s \leq r$, skaičiai $p_s^{\alpha_s}$ ir n_s yra tarpusavyje pirminiai, tai egzistuoja tokie sveikieji skaičiai a_s ir b_s, kad

$$p_s^{\alpha_s} a_s + n_s b_s = 1.$$

Taigi kiekvienam s, $1 \le s \le r$, teisinga lygybė

$$g_s {g'}_s^{-1} = (g_s {g'}_s^{-1})^{p_s^{\alpha_s} a_s + n_s b_s} = (g_s {g'}_s^{-1})^{p_s^{\alpha_s} a_s} \cdot (g_s {g'}_s^{-1})^{n_s b_s} = 1,$$

t. y. $g_s = g'_s$. Įrodėme, kad grupė G yra pogrupių G_j, $1 \le j \le r$, tiesioginė sandauga. Remdamiesi lygybe

$$|G| = n = \prod_{j=1}^{r} p_j^{\alpha_j} = \prod_{j=1}^{r} |G_j|$$

gauname, kad kiekvienam j, $1 \le j \le r$, $|G_j| = p_j^{\alpha_j}$, nes pogrupio G_j eilė yra lygi pirminio skaičiaus p_j, $1 \le j \le r$, laipsniui.

Visiškai akivaizdu, kad pogrupiai G_j, $1 \le j \le r$, yra vienareikšmiškai apibrėžiami: kiekvienam j, $1 \le j \le r$, pogrupis G_j yra sudarytas iš tų grupės G elementų, kurių eilė yra pirminio skaičiaus p_j laipsnis. □

5.10.7. Ką tik įrodyta teorema dažnai yra formuluojama ir įrodoma adiciniais žymėjimais. Mes taip pat pateiksime šios teoremos formuluotę vartodami adicinę terminiją. Štai perėjimo nuo multiplikacinių žymėjimų ir terminų prie adicinių žymėjimų ir terminų žodynėlis:

- Sandaugos ženklas $\prod$ pakeičiamas sumos ženklu $\sum$.
- Elementas g^n pakeičiamas elementu ng.
- Elementų sandauga
  $$g_1^{n_1} g_2^{n_2} \dots g_s^{n_s}$$
  pakeičiama elementų suma
  $$n_1 g_1 + n_2 g_2 + \dots + n_s g_s.$$
- Grupės vienetas 1 pakeičiamas grupės nuliu 0.
- Daugybos ženklas $*$ (ar $\cdot$) pakeičiamas sudėties ženklu $+$.
- Terminas „tiesioginė sandauga“ pakeičiamas terminu „tiesioginė suma“.
- Ženklą $\oplus$ naudosime tiesioginei sumai žymėti.

Dabar suformuluosime anksčiau įrodytą teoremą adiciniais žymėjimais.

5.10.8 teorema. *Sakykime, kad baigtinės Abelio grupės G eilė yra n. Tegu*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$$

– skaičiaus n kanoninis skaidinys pirminiais skaičiais. Tuomet grupė G yra vieninteliu būdu išskaidoma į p_j-pogrupių G_j, $1 \le j \le r$, tiesioginę sumą

$$G = \bigoplus_{j=1}^{r} G_j$$

(t. y. pogrupiai G_j, $1 \le j \le r$, yra apibrėžiami vienareikšmiškai). Pogrupio G_j eilė yra lygi $p_j^{\alpha_j}$, $1 \le j \le r$.

Dabar įrodysime, kad kiekvieną baigtinę Abelio p-grupę G galima išskaidyti į ciklinių pogrupių tiesioginę sandaugą.

5.10.9 teorema. *Kiekviena baigtinė Abelio p-grupė G yra išskaidoma į ciklinių p-pogrupių tiesioginę sandaugą $\prod_{j=1}^{r} G_j$.*

Įrodymas. Sakykime, kad g_1 yra grupės G didžiausios eilės p^{n_1} elementas. Jei ciklinis pogrupis $\langle g_1 \rangle = G$, tai teoremos įrodymas baigtas. Jei $\langle g_1 \rangle \ne G$, tai išrinkime grupės G tokį elementą g_2', kad elementas $g_2'\langle g_1 \rangle$ faktorgrupėje $G/\langle g_1 \rangle$ turėtų didžiausią eilę p^{n_2}. Tuomet ${g'}_2^{p^{n_2}} \in \langle g_1 \rangle$, t. y. kuriam nors j, $0 \le j < p^{n_1}$, ${g'}_2^{p^{n_2}} = g_1^j$. Kadangi kiekvieno grupės G elemento eilė yra pirminio p laipsnis, o elementas g_1 grupėje G yra didžiausios eilės, tai

$$(g_1^j)^{p^{n_1-n_2}} = g_1^{jp^{n_1-n_2}} = {g_2'}^{p^{n_1}} = 1.$$

Vadinasi, $p^{n_1} \mid jp^{n_1-n_2}$, t. y. $p^{n_2} \mid j$. Taigi $j = p^{n_2}j'$. Įrašę šią j išraišką į lygybę ${g'}_2^{p^{n_2}} = g_1^j$, gauname: ${g'}_2^{p^{n_2}} = g_1^{p^{n_2}j'}$ arba ${g'}_2^{p^{n_2}} g_1^{-p^{n_2}j'} = ({g'}_2 g_1^{-j'})^{p^{n_2}} = 1$. Pažymėkime elementą ${g'}_2 g_1^{-j'}$ ženklu g_2. Tuomet gauname: $g_2^{p^{n_2}} = 1$. Įrodysime, kad elemento g_2 eilė yra lygi p^{n_2} (vadinasi, šiuo atveju teisinga nelygybė $n_2 \le n_1$) ir $\langle g_1 \rangle \cap \langle g_2 \rangle = 1$. Jei būtų $g_2^{p^m} = 1$ ir $0 < m < n_2$, tai gautume

$$g_2^{p^m} = ({g'}_2 g_1^{-j'})^{p^m} = 1 \quad \text{arba} \quad {g'}_2^{p^m} = g_1^{j'p^m},$$

t. y. $(g_2'\langle g_1 \rangle)^{p^m} = \langle g_1 \rangle$, o tai prieštarautų tam, kad elemento $g_2'\langle g_1 \rangle$ eilė yra p^{n_2}. Jei būtų $\langle g_1 \rangle \cap \langle g_2 \rangle \ne 1$, tai kuriam nors m, $0 < m < n_2$, gautume $g_2^{p^m} \in \langle g_1 \rangle$. Vėl gautume prieštarą tam, kad elemento $g_2'\langle g_1 \rangle$ eilė yra p^{n_2}.

Jei $\langle g_1 \rangle \times \langle g_2 \rangle \ne G$, tai galime išrinkti grupės G tokį elementą g_3', kad faktorgrupės $G/(\langle g_1 \rangle \times \langle g_2 \rangle)$ elemento $g_3'\langle g_1 \rangle\langle g_2 \rangle$ eilė p^{n_3} būtų didžiausia. Vėl galime parašyti ${g'}_3^{p^{n_3}} \in \langle g_1 \rangle \times \langle g_2 \rangle$, t. y. egzistuoja tokie i, j, $0 \le i < p^{n_1}$, $0 \le j < p^{n_2}$, kad ${g'}_3^{p^{n_3}} = g_1^i g_2^j$. Panašiai kaip ir anksčiau,

$$g_1^{ip^{n_1-n_3}} g_2^{jp^{n_1-n_3}} = (g_1^i g_2^j)^{p^{n_1-n_3}} = {g'}_3^{p^{n_1}} = 1,$$

t. y. $g_1^{ip^{n_1-n_3}} = 1$, $g_2^{jp^{n_1-n_3}} = 1$. Taigi $p^{n_1} \mid ip^{n_1-n_3}$ ir $p^{n_2} \mid jp^{n_1-n_3}$, o tai reiškia, kad $p^{n_3} \mid i$, $p^{n_3} \mid j$. Sakykime, $i = p^{n_3}i'$, $j = p^{n_3}j'$. Tuomet lygybę ${g'}_3^{p^{n_3}} = g_1^i g_2^j$ galime perrašyti taip:

$$ {g'}_3^{p^{n_3}} g_1^{-p^{n_3}i'} g_2^{-p^{n_3}j'} = ({g'}_3 g_1^{-i'} g_2^{-j'})^{p^{n_3}} = 1. $$

Pažymėkime $g_3 = {g'}_3 g_1^{-i'} g_2^{-j'}$. Panašiai kaip ir anksčiau, galima įrodyti, kad elemento g_3 eilė yra lygi p^{n_3} ir

$$ (\langle g_1 \rangle \times \langle g_2 \rangle) \cap \langle g_3 \rangle = 1. $$

Elementų $g_1, g_2, \ldots, g_r$, tenkinančių sąlygą: elemento

$$ g_j \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_{j-1} \rangle $$

faktorgrupėje

$$ G/(\langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_{j-1} \rangle) $$

eilė p^{n_j} yra didžiausia ir

$$ (\langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_{j-1} \rangle) \cap \langle g_j \rangle = 1, \ 1 \leq j \leq r, $$

išrinkimą galime tęsti iki gausime

$$ G = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_r \rangle. $$

□

Antras teoremos įrodymas. Sakykime, $g_1 \in G$ – didžiausios eilės elementas, jo eilė yra lygi p^{n_1}. Jei $\langle g_1 \rangle = G$, tai teoremos įrodymas baigtas. Jei $\langle g_1 \rangle \neq G$, tai išrinkime didžiausios eilės grupės G pogrupį H, tenkinantį sąlygą: $\langle g_1 \rangle \cap H = \{1\}$. Įrodysime, kad $G = \langle g_1 \rangle \times H$. Įrodę šią lygybę, teoremos įrodymą galėsime užbaigti matematinės indukcijos metodu, tarę, kad teoremos teiginys teisingas kiekvienai baigtinei Abelio p-grupei, kurios eilė yra mažesnė nei grupės G.

Sakykime, kad $\langle g_1 \rangle \times H \neq G$. Imkime mažiausios eilės elementą $a \in G$, nepriklausantį pogrupiui $\langle g_1 \rangle \times H \neq G$. Sakykime, kad elemento a eilė yra lygi p^m. Jei būtų $m = 1$, tai, remdamiesi sąlyga $a \notin \langle g_1 \rangle \times H$, gautume: kiekvienam j, $0 < j < p$, $a^j \notin \langle g_1 \rangle \times H$ (bet kuriam j, $0 < j < p$, elementas a^j generuoja ciklinį pogrupį $\langle a \rangle$). Tuomet grupės G pogrupis $H' := H \times \langle a \rangle$ tenkintų sąlygą $\langle g_1 \rangle \cap H' = \{1\}$ ir jo eilė būtų $|H'| = |H|p$, o tai prieštarautų pogrupio H parinkimui. Taigi būtinai $m > 1$. Elemento $a^p \neq 1$ eilė yra mažesnė už elemento a eilę. Vadinasi, $a^p \in \langle g_1 \rangle \times H$, t. y. egzistuoja tokie j, $1 \leq j < p^{n_1}$ ir $h \in H$, kad $a^p = g_1^j h$. Šios lygybės abi puses pakėlę p^{m-1} laipsniu, gauname:

$$ (g_1^j h)^{p^{m-1}} = g_1^{jp^{m-1}} h^{p^{m-1}} = a^{p^m} = 1, $$

t. y. $g_1^{jp^{m-1}} = 1$ ir $h^{p^{m-1}} = 1$. Remdamiesi lygybe $g_1^{jp^{m-1}} = 1$, darome išvadą, kad $p^{n_1} \mid jp^{m-1}$, t. y. $p^{n_1-m+1} \mid j$. Kadangi $n_1 - m + 1 > 0$, tai $p \mid j$. Sakykime, kad $j = pj'$. Tuomet lygybę $a^p = g_1^j h$ galime perrašyti taip:

$$a^p g_1^{-j} = a^p (g_1^{-j'})^p = (a g_1^{-j'})^p = h.$$

Pažymėję elementą $a g_1^{-j'}$ raide h', gauname: $h' \notin \langle g_1 \rangle \times H$, $h'^p \in H$. Nagrinėkime grupės G pogrupį $\langle h', H \rangle$. Šio pogrupio eilė yra didesnė už pogrupio H eilę. Vadinasi, $\langle h', H \rangle \cap \langle g_1 \rangle \neq \{1\}$, t. y. egzistuoja tokie i, j, $0 < i < p$, $0 < j < p^{n_1}$, $h \in H$, kad $h'^i h = g_1^j$. Remdamiesi šia lygybe, darome išvadą, kad $h'^i \in \langle g_1 \rangle \times H$. Bet $h'^p \in H \subset \langle g_1 \rangle \times H$. Kadangi skaičiai i ir p tarpusavyje pirminiai, tai egzistuoja tokie $u, v \in \mathbb{Z}$, kad $1 = iu + pv$. Vadinasi,

$$h' = h'^{iu+pv} = (h'^i)^u (h'^p)^v \in \langle g_1 \rangle \times H.$$

Gavome prieštarą prielaidai, kad $\langle g_1 \rangle \times H \neq G$. Vadinasi, $G = \langle g_1 \rangle \times H$. Kaip anksčiau minėjome, teoremos įrodymą galima užbaigti matematinės indukcijos metodu. Jei $H = \langle g_2 \rangle \times \cdots \times \langle g_r \rangle$, tai $G = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_r \rangle$. □

5.10.10 pastaba. Grupės G skaidinio $G = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_r \rangle$ ciklinių pogrupių tiesiogine sandauga cikliniai pogrupiai $\langle g_j \rangle$, $1 \leq j \leq r$, apibrėžiami nevienareikšmiškai. Du grupės G skaidiniai ciklinių pogrupių tiesiogine sandauga gali neturėti nė vieno to paties ciklinio pogrupio. Išnagrinėkime keletą pavyzdžių.

5.10.11 pavyzdys. Grupė

$$G = \{1, a, b, ab \mid a^2 = b^2 = 1, ab = ba\}$$

yra išskaidoma į pogrupių tiesioginę sandaugą taip:

1. $G = \{1, a \mid a^2 = 1\} \times \{1, b \mid b^2 = 1\}$.
2. $G = \{1, a \mid a^2 = 1\} \times \{1, ab \mid (ab)^2 = 1\}$.
3. $G = \{1, b \mid b^2 = 1\} \times \{1, ab \mid (ab)^2 = 1\}$.

Kaip matome, grupės G skaidiniai ciklinių pogrupių tiesiogine sandauga skiriasi, bet visuose skaidiniuose tų pogrupių eilės yra lygios skaičiams 2, 2.

5.10.12 pavyzdys. Nagrinėkime grupės

$$G = \{a^i b^j \mid 0 \leq i, j < 3, a^3 = b^3 = 1, ab = ba\}$$

skaidinius ciklinių pogrupių tiesiogine sandauga:

1. $G = \{1, a, a^2\} \times \{1, b, b^2\} = \langle a \rangle \times \langle b \rangle$.

2. $G = \{1, ab, a^2b^2\} \times \{1, ab^2, a^2b\} = \langle ab \rangle \times \langle a^2b \rangle$.

Kaip matome, šie grupės G skaidiniai ciklinių pogrupių tiesiogine sandauga neturi bendrų ciklinių pogrupių. Bet ir šį kartą kiekviename grupės G skaidinyje yra po du ciklinius pogrupius, kurių eilės tiek viename, tiek kitame skaidinyje yra lygios 3 ir 3.

Kaip matome iš pavyzdžių, baigtinės Abelio p-grupės bet kurie du skaidiniai ciklinių pogrupių tiesiogine sandauga turi tą patį skaičių ciklinių pogrupių. Be to, fiksuotos eilės ciklinių pogrupių skaičius yra tas pats kiekviename skaidinyje. Kitaip tariant, baigtinės Abelio p-grupės skaidinio ciklinių pogrupių tiesiogine sandauga vienareikšmiškai yra apibrėžiamas ciklinių pogrupių skaičius tame skaidinyje, o šie cikliniai pogrupiai vienareikšmiškai nusakomi tik izomorfizmo tikslumu. Grupių teorijos požiūriu to pakanka, kad galėtume suklasifikuoti baigtines Abelio grupes.

5.10.13 (Abelio p-grupės skaidinio ciklinių pogrupių tiesiogine sandauga vienatis)**.** Įrodėme, kad grupę G galima išskaidyti į ciklinių pogrupių $\langle g_j \rangle$, $1 \le j \le r$, tiesioginę sandaugą $G = \langle g_1 \rangle \langle g_2 \rangle \dots \langle g_r \rangle$. Lieka įrodyti, kad grupės G kiekviename skaidinyje ciklinių pogrupių tiesiogine sandauga fiksuotos eilės ciklinių pogrupių yra tas pats skaičius.

Įrodymas. Įrodysime matematinės indukcijos metodu. Tarkime, kad teorema įrodyta visoms Abelio p-grupėms, kurių eilė mažesnė už p^n. Tegu G – Abelio p-grupė, kurios eilė lygi p^n. Sakykime, kad grupė G išskaidyta į ciklinių pogrupių tiesioginę sandaugą dviem skirtingais būdais:

$$G = \langle g_1 \rangle \times \langle g_2 \rangle \times \dots \times \langle g_r \rangle, \;\; m_1 \ge m_2 \ge \dots \ge m_r,$$

ir

$$G = \langle h_1 \rangle \times \langle h_2 \rangle \times \dots \times \langle h_s \rangle, \;\; n_1 \ge n_2 \ge \dots \ge n_s,$$

čia $p^{m_1}, p^{m_2}, \dots, p^{m_r}$ – elementų $g_1,\; g_2, \dots, g_r$ eilės, o $p^{n_1}, p^{n_2}, \dots, p^{n_s}$ – elementų $h_1,\; h_2, \dots, h_s$ eilės. Nagrinėkime homomorfizmą

$$f_p : G \to G,\; f_p(g) = g^p, \;\; g \in G.$$

Šio homomorfizmo branduolys sudarytas iš grupės G p eilės elementų ir vieneto 1. Pirmojo skaidinio atvejų jų yra p^r, o antrojo skaidinio atveju – p^s. Taigi $r = s$, t. y. tiek viename, tiek kitame grupės G skaidiniuose cikliniais pogrupiais į tiesioginę sandaugą ciklinių pogrupių skaičius tas pats. Nagrinėkime homomorfizmo f_p vaizdą $f_p(G)$. Galime užrašyti šio pogrupio skaidinius cikliniais pogrupiais

$$f_p(G) = \langle g_1^p \rangle \times \langle g_2^p \rangle \times \dots \times \langle g_r^p \rangle,$$

ir
$$f_p(G) = \langle h_1^p \rangle \times \langle h_2^p \rangle \times \cdots \times \langle h_r^p \rangle.$$
Šiuo atveju ciklinių pogrupių eilės yra
$$p^{m_1-1},\ p^{m_2-1},\ \ldots,\ p^{m_r-1}, \text{ ir } p^{n_1-1},\ p^{n_2-1},\ \ldots,\ p^{n_s-1}.$$
Kadangi pogrupio $f_p(G)$ eilė mažesnė nei p^n, tai
$$m_1 - 1 = n_1 - 1,\ \ m_2 - 1 = n_2 - 1, \ldots, m_r - 1 = n_r - 1,$$
t. y. $m_1 = n_1$, $m_2 = n_2$, $\ldots$, $m_r = n_r$. □

Taigi, jei grupė G yra ciklinių pogrupių tiesioginė sandauga
$$G = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_r \rangle,$$
$|\langle g_i \rangle| = p^{n_i}$, $1 \leq i \leq r$, ir
$$n_1 \geq n_2 \geq \ldots \geq n_r,$$
tai grupės G terminais vienareikšmiškai yra apibrėžiamas ciklinių pogrupių skaičius r ir vienareikšmiškai apibrėžiamos šių ciklinių pogrupių eilės p^{n_i}, $1 \leq i \leq r$.

5.10.14 apibrėžimas. Jei baigtinė Abelio p-grupė G yra ciklinių pogrupių $\langle g_j \rangle$, $1 \leq j \leq r$, kurių eilės atitinkamai yra lygios p^{n_j}, $1 \leq j \leq r$, tiesioginė sandauga
$$G = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_r \rangle,$$
tai skaičiai $n_1, n_2, \ldots, n_r$ yra vadinami grupės G *invariantais.* Ciklinius pogrupius tiesioginėje sandaugoje galima surašyti tokia tvarka, kad grupės G invariantai tenkintų sąlygą: $n_1 \geq n_2 \geq \cdots \geq n_r$.

5.10.15 teorema. *Baigtinės Abelio p-grupės G ir H yra izomorfinės tada ir tik tada, kai jų invariantai yra lygūs.*

Įrodymas. Akivaizdu, kad jei baigtinės Abelio p-grupės G ir H yra izomorfinės, tai jų invariantai yra lygūs.

Sakykime, baigtinių Abelio p-grupių G ir H invariantai yra $n_1 \geq n_2 \geq \cdots \geq n_r$. Tuomet grupės G ir H yra išskaidomos ciklinių pogrupių tiesiogine sandauga:
$$G = \langle g_1 \rangle \times \langle g_2 \rangle \times \cdots \times \langle g_r \rangle$$
ir
$$H = \langle h_1 \rangle \times \langle h_2 \rangle \times \cdots \times \langle h_r \rangle.$$
Ciklinių pogrupių $\langle g_1 \rangle$ ir $\langle h_1 \rangle$, $\langle g_2 \rangle$ ir $\langle h_2 \rangle$, $\ldots$, $\langle g_r \rangle$ ir $\langle h_r \rangle$ eilės yra lygios p^{n_1}, p^{n_2}, $\ldots$, p^{n_r}. Apibrėžkime atvaizdį
$$f : G \to H,\ \ f(g_1^{a_1} g_2^{a_2} \ldots g_r^{a_r}) = h_1^{a_1} h_2^{a_2} \ldots h_r^{a_r},\ 0 \leq a_j < p^{n_j},\ 1 \leq j \leq r.$$
Akivaizdu, kad f yra izomorfizmas. □

5.11 Simetrinė grupė

5.11.1. Pažymėkime $\mathbb{N}_n := \{1, 2, \ldots, n\}$ ir nagrinėkime visų bijekcijų $\sigma : \mathbb{N}_n \to \mathbb{N}_n$ aibę S_n. Bijekcija $\sigma : \mathbb{N}_n \to \mathbb{N}_n$ dažnai yra vadinama aibės $\mathbb{N}_n$ elementų *keitiniu* arba *perstatiniu*. Kadangi dviejų bijekcijų $\sigma, \tau \in S_n$ kompozicija $\tau \circ \sigma$ yra bijekcija, tai galima apibrėžti aibės S_n elementų kompozicijos dėsnį $\circ$:

$$\circ : S_n \times S_n \to S_n,\ (\sigma, \tau) \mapsto \tau \circ \sigma,\ \sigma, \tau \in S_n.$$

Priminsime, kad dviejų atvaizdžių $\sigma, \tau \in S_n$ kompozicija $\tau \circ \sigma$ apibrėžiama taip:

$$(\tau \circ \sigma)(j) := \tau(\sigma(j)),\ \ j \in \mathbb{N}_n.$$

Tapatusis atvaizdis id: $\mathbb{N}_n \to \mathbb{N}_n$, $\mathrm{id}(j) = j$, $j \in \mathbb{N}_n$, taip pat yra keitinys.

Aibė S_n kompozicijos dėsnio $\circ$ atžvilgiu yra grupė, nes

1. Kompozicijos dėsnis $\circ$ yra asociatyvus.
2. $S_n \ni \mathrm{id}$ – neutralus elementas $\circ$ atžvilgiu (grupės vienetas).
3. Kiekvienam $\sigma \in S_n$ egzistuoja $\sigma^{-1} \in S_n$ ir $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \mathrm{id}$ (σ^{-1} – atvirkštinis elementas elementui σ).

5.11.2 apibrėžimas. Grupė $(S_n, \circ)$ vadinama *n-tojo laipsnio simetrine grupe.* Jos eilė yra lygi $n!$.

5.11.3. Bijekciją $\sigma : \mathbb{N}_n \to \mathbb{N}_n$ galima pavaizduoti lentele

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix};$$

pirmoje lentelės eilutėje bet kuria tvarka surašomi visi aibės $\mathbb{N}_n$ elementai (šioje lentelėje aibės $\mathbb{N}_n$ elementai surašyti natūralia tvarka), o antroje lentelės eilutėje po kiekvienu pirmos eilutės elementu j parašomas jo vaizdas $\sigma(j)$. Kadangi σ – bijekcija, tai elementai $\sigma(1)$, $\sigma(2)$, …, $\sigma(n)$ yra paporiui skirtingi. Pabrėžiame, kad lentelės pirmoje eilutėje aibės $\mathbb{N}_n$ elementų tvarka nesvarbi, bet svarbu, kas parašyta po kiekvienu pirmos eilutės elementu! Jei bijekcijos $\sigma, \tau \in S_n$ pavaizduojamos atitinkamai lentelėmis

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix} \text{ ir } \begin{pmatrix} 1 & 2 & \ldots & n \\ \tau(1) & \tau(2) & \ldots & \tau(n) \end{pmatrix},$$

tai bijekcija $\tau \circ \sigma$ pavaizduojama lentele

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ \tau(\sigma(1)) & \tau(\sigma(2)) & \ldots & \tau(\sigma(n)) \end{pmatrix}.$$

Pavyzdžiui,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 4 & 2 & 5 \end{pmatrix}.$$

5.11.4. Sakykime, σ yra grupės S_n elementas. Grupės S_n elementą

$$\underbrace{\sigma \circ \sigma \circ \cdots \circ \sigma}_{m}$$

žymėsime σ^m ir vadinsime elemento σ m-tuoju laipsniu. Kadangi grupė S_n baigtinė, tai kiekvieno grupės S_n elemento eilė yra baigtinė, t. y., jei $\sigma \in S_n$, tai egzistuoja toks mažiausias teigiamas sveikasis skaičius r, kad $\sigma^r = \mathrm{id}$, $\sigma^j \neq \mathrm{id}$, jei $0 < j < r$. Elemento $\sigma \in S_n$, kurio eilė yra lygi r, laipsniai $\{\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{r-1}\}$ sudaro grupės S_n ciklinį pogrupį $\langle \sigma \rangle$.

5.11.5 apibrėžimas. Elementas $\sigma \in S_n$ vadinamas *ciklu* ir žymimas

$$(j_1\ j_2\ \ldots\ j_r),$$

jei j_1, j_2, $\ldots$, j_r – tarpusavyje skirtingi aibės $\mathbb{N}_n$ elementai,

$$\sigma(j_1) = j_2,\ \sigma(j_2) = j_3,\ \ldots,\ \sigma(j_{r-1}) = j_r,\ \sigma(j_r) = j_1,$$

o kiekvienam aibės $\mathbb{N}_n$ elementui $j \notin \{j_1, j_2, \ldots, j_r\}$, $\sigma(j) = j$. Skaičius r vadinamas ciklo $(j_1\ j_2\ \ldots\ j_r)$ *ilgiu.* Dažnai ilgio r ciklas vadinamas r-ciklu. Ciklai $(i\ j)$ (jų ilgis lygus 2) vadinami *transpozicijomis.*

5.11.6 pastaba. Remiantis ciklo apibrėžimu, akivaizdu, kad

$$(j_1\ j_2\ \ldots\ j_r) = (j_2\ j_3\ \ldots\ j_r\ j_1) = \cdots = (j_r\ j_1\ \ldots\ j_{r-2}\ j_{r-1}).$$

Be to, r ilgio ciklo $(j_1\ j_2\ \ldots\ j_r)$ eilė yra lygi r.

5.11.7 apibrėžimas. Ciklai $(i_1\ i_2\ \ldots\ i_s)$ ir $(j_1\ j_2\ \ldots\ j_r)$ vadinami *nepriklausomais*, jei

$$\{i_1,\ i_2,\ \ldots,\ i_s\} \cap \{j_1,\ j_2,\ \ldots,\ j_r\} = \emptyset.$$

Sakykime, kad keitinys $\sigma \in S_n$, $\sigma \neq \mathrm{id}$, yra išskaidytas ciklų $\sigma_1, \sigma_2, \ldots, \sigma_t \in S_n \setminus \{\mathrm{id}\}$ sandauga:

$$\sigma = \sigma_1 \sigma_2 \cdots \sigma_t.$$

Šis išskaidymas vadinamas keitinio σ išraiška *nepriklausomų ciklų sandauga*, jei bet kurie du šios išraiškos ciklai σ_i ir σ_j, $i \neq j$, yra nepriklausomi.

Lygybė $\mathrm{id} = (1)$ vadinama grupės S_n vieneto id išraiška *nepriklausomų ciklų sandauga.*

5.11.8 pavyzdys. Keitinio $\sigma \in S_9$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 1 & 4 & 9 & 8 & 7 & 6 & 2 \end{pmatrix},$$

išraiška nepriklausomų ciklų sandauga yra:

$$\sigma = (1\ 3)(6\ 8)(2\ 5\ 9).$$

5.11.9 teiginys. *Grupės S_n nepriklausomi ciklai yra perstatomi. Kitaip sakant, jei σ ir τ – nepriklausomi ciklai, tai $\sigma\tau = \tau\sigma$.*

Įrodymas. Įrodyti paliekame skaitytojui. □

5.11.10. Kiekvienam grupės S_n elementui σ aibėje $\mathbb{N}_n$ apibrėžkime ekvivalentumo sąryšį $\underset{\sigma}{\sim}$: $i \underset{\sigma}{\sim} j$, jei egzistuoja toks elemento σ sveikasis laipsnis σ^m, kad $\sigma^m(i) = j$.

5.11.11 apibrėžimas. Aibės $\mathbb{N}_n$ elementų ekvivalentumo klasės pagal ekvivalentumo sąryšį $\underset{\sigma}{\sim}$ vadinamos elemento σ *orbitomis*.

Elemento $\sigma \in S_n$ orbita, kuriai priklauso aibės $\mathbb{N}_n$ elementas j, sudaryta iš elementų j, $\sigma(j)$, $\sigma^2(j)$, ..., $\sigma^{p-1}(j)$, čia p – toks mažiausias teigiamas sveikasis skaičius, kad $\sigma^p(j) = j$.

5.11.12 apibrėžimas. Jei elemento $\sigma \in S_n$ orbita sudaryta iš vieno aibės $\mathbb{N}_n$ elemento j (t. y. $\sigma(j) = j$), tai j vadinamas *σ-nejudamu elementu.*

Dabar ciklą galime apibūdinti ir kitaip. Grupės S_n elementas σ yra ciklas, jei elemento σ visos orbitos, išskyrus vieną, sudarytos iš aibės $\mathbb{N}_n$ σ-nejudamų elementų.

5.11.13 teiginys. *Jei neatsižvelgiama į dauginamųjų tvarką, tai kiekvienas grupės S_n elementas vienareikšmiškai užrašomas nepriklausomų ciklų sandauga.*

Įrodymas. Grupės S_n vienetui id teiginys akivaizdžiai teisingas, todėl toliau nagrinėsime tik keitinius $\sigma \in S_n$, $\sigma \neq \mathrm{id}$.

Sakykime, $\sigma \in S_n$, o X_1, X_2, ..., X_t – elemento σ orbitos. Taigi $X_i \cap X_j = \emptyset$, jei $i \neq j$, $1 \leq i, j \leq t$, $X_1 \cup X_2 \cup \cdots \cup X_t = \mathbb{N}_n$. Apibrėžkime atvaizdžius $\sigma_i : \mathbb{N}_n \to \mathbb{N}_n$, $1 \leq i \leq t$:

$$\sigma_i(j) = \begin{cases} \sigma(j), & \text{jei } j \in X_i \\ j, & \text{jei } j \in \mathbb{N}_n \setminus X_i \end{cases}.$$

Remdamiesi atvaizdžių σ_i, $1 \leq i \leq t$, apibrėžimu, matome, kad kiekvienam i, $1 \leq i \leq t$, σ_i – ciklai. Įrodysime, kad

$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_t. \tag{5.3}$$

Pakanka įrodyti, kad kiekvienam $j \in \mathbb{N}_n$,

$$\sigma(j) = (\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_t)(j).$$

Iš tikrųjų, nagrinėkime skaičių

$$j \in \mathbb{N}_n = X_1 \cup X_2 \cup \cdots \cup X_t.$$

Kadangi jokios dvi skirtingos elemento σ orbitos neturi bendrų elementų, tai egzistuoja toks vienintelis indeksas i, $1 \leq i \leq t$, kad $j \in X_i$. Tuomet

$$(\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_t)(j) = \sigma_i(j) = \sigma(j).$$

Taigi įrodėme, kad teisinga (5.3) lygybė. Joje praleidę ilgio 1 ciklus (kurie lygūs id), gausime keitinio σ išraišką nesikertančių ciklų sandauga.

(5.3) išskaidymo (praleidus ilgio 1 ciklus) vienareikšmiškumą galima įrodyti matematinės indukcijos metodu pagal t. Įrodymą paliekame skaitytojui. $\square$

5.11.14 pastaba. Sutarkime tarp ciklų nerašyti grupės S_n elementų kompozicijos dėsnio ženklo $\circ$.

5.11.15. Kiekvienas ciklas $(j_1\ j_2\ \ldots\ j_r)$ gali būti užrašomas transpozicijų sadauga:

$$(j_1\ j_2\ \ldots\ j_r) = (j_1\ j_r)(j_1\ j_{r-1})\ldots(j_1\ j_2).$$

Ciklai transpozicijų sandauga užrašomi nevienareikšmiškai. Pavyzdžiui, grupės S_n, $n \geq 3$, ciklą $(1\ 2\ 3)$ galime išskaidyti transpozicijų sandauga taip:

$$(1\ 2\ 3) = (1\ 3)(1\ 2) = (1\ 2)(2\ 3) = (2\ 3)(1\ 3) = (2\ 3)(1\ 2)(1\ 3)(2\ 3).$$

Be to, kaip matome, ciklą dviem skirtingais būdais išskaidžius transpozicijų sandauga, transpozicijų skaičius viename ir kitame išskaidyme gali skirtis.

5.11.16 išvada. *Kiekvienas grupės S_n elementas yra išskaidomas transpozicijų sandauga. Grupės S_n transpozicijos yra šios grupės sudaromosios.*

Įrodymas. Nagrinėkime keitinį $\sigma \in S_n$. Remiantis 5.11.13 teiginiu, keitinį σ galima išreikšti nepriklausomų ciklų sandauga:

$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_t.$$

Kadangi kiekvieną ciklą galima užrašyti transpozicijų sandauga (žr. 5.11.15 pastraipą), tai ir patį keitinį σ galima išreikšti transpozicijų sandauga. $\square$

5.11.1 Keitinio lyginumas I

5.11.17 apibrėžimas. Sakoma, kad užrašytų skirtingų natūraliųjų skaičių pora $i\ j$ sudaro *inversiją* arba *netvarką*, jei $i > j$. Grupės S_n elementas

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$$

vadinamas *lyginiu* (*nelyginiu*), jei šio keitinio antroje eilutėje

$$j_1\, j_2\, \dots\, j_n$$

esančių netvarkų skaičius yra lyginis (nelyginis).

5.11.18 pavyzdys. Nagrinėkime keitinį

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}.$$

Šio keitinio antrojoje eilutėje skaičių poros, sudarančios inversijas, yra šios:

$$3\ 1;\ 3\ 2;\ 4\ 2.$$

Taigi σ – nelyginis keitinys.

5.11.19 pavyzdys. Nagrinėkime keitinį

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Šio keitinio antrojoje eilutėje skaičių poros, sudarančios inversijas, yra šios:

$$4\ 3;\ 4\ 2;\ 4\ 1;\ 3\ 2;\ 3\ 1;\ 2\ 1.$$

Taigi τ – lyginis keitinys.

5.11.20 teiginys. *Jei keitinys $\sigma \in S_n$ yra lyginis (nelyginis), o $\tau \in S_n$ – transpozicija, tai keitinys $\sigma\tau$ yra nelyginis (lyginis).*

Įrodymas. Sakykime, kad transpozicija $\tau = (i\ j)$, $i < j$, o keitinys

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}.$$

Tuomet

$$\sigma\tau = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} (i\ j) =$$

$$= \begin{pmatrix} 1 & \cdots & i & \cdots & j & \cdots & n \\ a_1 & \cdots & a_j & \cdots & a_i & \cdots & a_n \end{pmatrix}$$

(šis keitinys gaunamas iš keitinio σ, antrojoje jo eilutėje sukeičiant skaičius $\sigma(i)$ ir $\sigma(j)$ vietomis). Iš pradžių teiginį įrodysime tuo atveju, kai i ir j – du gretimi natūralieji skaičiai.

Tarkime, kad $j = i + 1$. Tuomet

$$\sigma\tau = \sigma \circ (i\; i+1) = \begin{pmatrix} 1 & \cdots & i-1 & i & i+1 & i+2 & \cdots & n \\ a_1 & \cdots & a_{i-1} & a_{i+1} & a_i & a_{i+2} & \cdots & a_n \end{pmatrix}.$$

Jei $a_i > a_{i+1}$, tai skaičių pora $a_i\; a_{i+1}$ yra keitinio σ antrosios eilutės

$$a_1 \;\cdots\; a_i\; a_{i+1} \;\cdots\; a_n$$

inversija, o skaičių pora $a_{i+1}\; a_i$ keitinio $\sigma\tau$ antrojoje eilutėje

$$a_1 \;\cdots\; a_{i-1}\; a_{i+1}\; a_i\; a_{i+2} \;\cdots\; a_n$$

inversijos nesudaro. Visos kitos keitinio σ antrosios eilutės inversijos sutampa su keitinio $\sigma\tau$ atitinkamomis antrosios eilutės inversijomis. Taigi šiuo atveju keitinio $\sigma\tau$ antrojoje eilutėje yra viena inversija mažiau nei keitinio σ antrojoje eilutėje. Vadinasi, keitiniai σ ir $\sigma\tau$ yra skirtingo lyginumo, t. y., jei σ – lyginis (nelyginis) keitinys, tai $\sigma\tau$ – nelyginis (lyginis). Analogiškai galima įsitikinti, kad, jei $a_i < a_{i+1}$, tai keitinio $\sigma\tau$ antrojoje eilutėje yra viena inversija daugiau nei keitinio σ antrojoje eilutėje, todėl ir šiuo atveju keitiniai σ ir $\sigma\tau$ yra skirtingo lyginumo.

Sakykime, kad $j \geq i + 2$. Galima įsitikinti, kad transpozicija $(i\; j)$ išreiškiama pavidalo $(k\; k+1)$ transpozicijų sandauga:

$$(i\; j) =$$

$$= (i\; i+1)(i+1\; i+2)\cdots(j-2\; j-1)(j-1\; j)(j-2\; j-1)\cdots(i+1\; i+2)(i\; i+1).$$

Šioje išraiškoje yra lygiai $2(j-i)-1$ transpozicijų. Taigi keitinys $\sigma\tau$ gaunamas keitinį σ iš dešinės pusės $2(j-i)-1$ kartų dauginant iš pavidalo $(k\;\; k+1)$ transpozicijų. Remiantis jau įrodyta teiginio dalimi (atvejis $j = i+1$), kiekvieną kartą keitinį iš dešinės dauginant iš pavidalo $(k\;\; k+1)$ transpozicijos keičiasi jo lyginumas. Kadangi skaičius $2(j-i)-1$ nelyginis, tai keitinio $\sigma\tau$ lyginumas bus priešingas keitinio σ lyginumui. □

5.11.21 išvada. *Bet kuri transpozicija yra nelyginis keitinys.*

Įrodymas. Tegu $\tau \in S_n$ – transpozicija. Kadangi identiškas keitinys id yra lyginis (inversijų skaičius lygus nuliui), tai, remiantis 5.11.20 teiginiu, transpozicija $\tau = \mathrm{id} \circ \tau$ yra nelyginis keitinys. □

Apibrėžkime atvaizdį sgn : $S_n \to \{1, -1\}$ taip:

$$\operatorname{sgn}(\sigma) = \begin{cases} 1, & \text{jei } \sigma \text{ – lyginis keitinys,} \\ -1, & \text{jei } \sigma \text{ – nelyginis keitinys.} \end{cases}$$

Kitaip sakant, keitinys $\sigma \in S_n$ yra lyginis tada ir tik tada, kai $\operatorname{sgn}(\sigma) = 1$. Pavyzdžiui, remiantis 5.11.21 išvada, bet kuriai transpozicijai τ teisinga lygybė $\operatorname{sgn}(\tau) = -1$.

5.11.22 teiginys. *Jei keitinį $\sigma \in S_n$ galima išreikšti s transpozicijų sandauga, tai*

$$\operatorname{sgn}(\sigma) = (-1)^s.$$

Įrodymas. Tegu $\tau_1, \tau_2, \ldots, \tau_s \in S_n$ – transpozicijos ir

$$\sigma = \tau_1 \tau_2 \cdots \tau_s.$$

Remiantis 5.11.20 teiginiu, galima parašyti

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_1 \tau_2 \cdots \tau_s) = -\operatorname{sgn}(\tau_1 \tau_2 \cdots \tau_{s-1}) =$$

$$= \operatorname{sgn}(\tau_1 \tau_2 \cdots \tau_{s-2}) = -\operatorname{sgn}(\tau_1 \tau_2 \cdots \tau_{s-3}) = \cdots = (-1)^s.$$

$\square$

5.11.23 teiginys. *Bet kuriems keitiniams $\sigma, \tau \in S_n$ teisinga lygybė*

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma) \operatorname{sgn}(\tau).$$

Įrodymas. Remiantis 5.11.16 išvada, keitinius σ ir τ galima išreikšti transpozicijų sandauga:

$$\sigma = \mu_1 \mu_2 \cdots \mu_s,$$

$$\tau = \nu_1 \nu_2 \cdots \nu_t,$$

čia μ_i, ν_j – transpozicijos. Todėl, remiantis 5.11.22 teiginiu, $\operatorname{sgn}(\sigma) = (-1)^s$ ir $\operatorname{sgn}(\tau) = (-1)^t$. Kita vertus, keitinio $\sigma\tau$ išraiška transpozicijų sandauga yra:

$$\sigma\tau = \mu_1 \mu_2 \cdots \mu_s \nu_1 \nu_2 \cdots \nu_t.$$

Remdamiesi šia išraiška ir 5.11.22 teiginiu, galime parašyti

$$\operatorname{sgn}(\sigma\tau) = (-1)^{s+t} = (-1)^s (-1)^t = \operatorname{sgn}(\sigma) \operatorname{sgn}(\tau).$$

$\square$

Taigi iš 5.11.23 teiginio matyti, kad atvaizdis sgn: $S_n \to \{-1, 1\}$ yra homomorfizmas ($\{-1, 1\}$ – multiplikatyvioji grupė). Šio homomorfizmo branduolys $\ker \operatorname{sgn}$, žymimas A_n, sudarytas iš visų simetrinės grupės S_n lyginių keitinių. Be to, A_n yra grupės S_n indekso 2 pogrupis. Kaip žinome, grupės indekso 2 pogrupis visada yra normalusis pogrupis. Taigi simetrinėje grupėje S_n yra $n!/2$ lyginių ir tiek pat nelyginių keitinių.

5.11.24 išvada. *Dviejų to paties lyginumo keitinių sandauga yra lyginis keitinys, o dviejų skirtingo lyginumo keitinių sandauga yra nelyginis keitinys.*

Įrodymas. Ši išvada išplaukia iš 5.11.23 teiginio. □

5.11.25 išvada. *Jei grupės S_n elementas σ užrašomas transpozicijų sandaugomis*

$$\sigma = (i_1\ j_1)(i_2\ j_2) \dots (i_r\ j_r) = (l_1\ m_1)(l_2\ m_2) \dots (l_s\ m_s), \tag{5.4}$$

tai $r \equiv s \pmod 2$.

Įrodymas. Kadangi atvaizdis $\operatorname{sgn} : S_n \to \{1, -1\}$ yra homomorfizmas, tai, remiantis 5.11.22 teiginiu ir (5.4) lygybe,

$$\operatorname{sgn}(\sigma) = (-1)^r = (-1)^s.$$

Gauname $r \equiv s \pmod 2$. □

5.11.26. Taigi remiantis 5.11.22 teiginiu ir 5.11.25 išvada, simetrinės grupės lyginio keitinio bet kuriame skaidinyje transpozicijomis yra lyginis dauginamųjų skaičius, o nelyginio keitinio bet kuriame skaidinyje transpozicijomis – nelyginis dauginamųjų skaičius.

5.11.27 išvada. *Jei* $\tau = (j_1\ j_2\ \dots\ j_r)$ *–* r*-ciklas, tai* $\operatorname{sgn}(\tau) = (-1)^{r-1}$.

Įrodymas. Kadangi

$$\tau = (j_1\ j_2\ \dots\ j_r) = (j_1\ j_r)(j_1\ j_{r-1}) \dots (j_1\ j_2),$$

tai, remiantis 5.11.22 teiginiu, $\operatorname{sgn}(\tau) = (-1)^{r-1}$. □

Iš šios išvados paaiškėja, kad nelyginio ilgio ciklas yra lyginis keitinys, o lyginio ilgio ciklas yra nelyginis keitinys.

5.11.28 išvada. *Jei keitinys σ išreikštas ciklų sandauga, o šių ciklų ilgiai yra $k_1, k_2, \dots, k_s$, tai*

$$\operatorname{sgn}(\sigma) = (-1)^{k_1+k_2+\dots+k_s-s}.$$

Įrodymas. Sakykime, kad keitinio σ išraiška ciklų sandauga yra:

$$\sigma = \tau_1 \tau_2 \cdots \tau_s,$$

čia τ_i – ciklas, kurio ilgis k_i. Tada, remiantis 5.11.23 teiginiu ir 5.11.27 išvada,

$$\operatorname{sgn}(\sigma) = \operatorname{sgn}(\tau_1)\operatorname{sgn}(\tau_2) \cdots \operatorname{sgn}(\tau_s) =$$

$$(-1)^{k_1-1}(-1)^{k_2-1}\cdots(-1)^{k_s-1} = (-1)^{k_1+k_2+\cdots+k_s-s}.$$

$\square$

5.11.29 teiginys. *Grupę S_n generuoja transpozicijos $(1\ 2)$, $(1\ 3)$, $\dots$, $(1\ n)$, o grupės S_n normalųjį pogrupį A_n (sudarytą iš visų lyginių keitinių) generuoja 3-ciklai $(1\ i\ j)$, $1 < i < j \le n$.*

Įrodymas. Grupę S_n generuoja transpozicijos $(i\ j)$, $1 \le i < j \le n$. Kadangi bet kuriems i, j, $1 \le i < j \le n$,

$$(i\ j) = (1\ i)(1\ j)(1\ i),$$

tai, kaip matome, grupę S_n generuoja transpozicijos $(1\ 2)$, $(1\ 3)$, $\dots$, $(1\ n)$.

Grupės S_n normalųjį pogrupį $A_n = \ker\operatorname{sgn}$ generuoja transpozicijų sandaugos $(i\ j)(l\ m)$, $1 \le i < j \le n$, $1 \le l < m \le n$. Kadangi bet kuriems $1 < i, j \le n$, $i \ne j$, teisinga lygybė

$$(1\ i)(1\ j) = (1\ j\ i) = (1\ i\ j)^2,$$

galime parašyti:

$$(i\ j)(l\ m) = (1\ i)(1\ j)(1\ i)(1\ l)(1\ m)(1\ l).$$

Jei $i = l$, tai

$$(i\ j)(l\ m) = (1\ i)(1\ j)(1\ m)(1\ l) = (1\ i\ j)^2(1\ l\ m),$$

o jei $i \ne l$, tai

$$(i\ j)(l\ m) = (1\ i)(1\ j)(1\ i)(1\ l)(1\ m)(1\ l) =$$

$$= (1\ j\ i)(1\ l\ i)(1\ l\ m) = (1\ i\ j)^2(1\ l\ i)(1\ l\ m).$$

(Jei $l > i$, tai galime parašyti $(1\ l\ i) = (1\ i\ l)^2$.) Kaip matome, grupės S_n normalųjį pogrupį A_n generuoja 3-ciklai $(1\ i\ j)$, $1 < i < j \le n$. $\square$

5.11.2 Keitinio lyginumas II

Šiame skyrelyje kitaip apibrėšime simetrinės grupės S_n elementų lyginumo sąvoką. (Skaitytojas, susipažinęs su 5.11.1 skyreliu „Keitinio lyginumas I“, šį skyrelį gali praleisti.) Naująjį apibrėžimą susiesime tiek su keitinio išskaidymo transpozicijomis skaičiaus lyginumu, tiek su viršutinėje ir apatinėje eilutėse esančių skaičių porų inversijų skaičių sumos lyginumu.

Apibrėžkime aibės $\{1,\ 2,\ \ldots, n\}$ elementų keitinio

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}$$

lyginumą. Tam apibrėžkime skaičių

$$A = \prod_{1 \leqslant i < j \leqslant n} (i - j).$$

Keitinio σ veikimą į skaičių A apibrėžkime taip:

$$\sigma A = \prod_{1 \leqslant i < j \leqslant n} (\sigma(i) - \sigma(j)).$$

Įsitikinsime, kad skaičiai A ir σA skiriasi daugikliu $+1$ arba -1, t. y.

$$\sigma A = \operatorname{sgn}(\sigma) A, \text{ čia } \operatorname{sgn}(\sigma) = \pm 1.$$

Tai iš tikrųjų akivaizdu, nes

$$\prod_{1 \leqslant i < j \leqslant n} |i - j| = \prod_{1 \leqslant i < j \leqslant n} |\sigma(i) - \sigma(j)|.$$

5.11.30 apibrėžimas. Aibės $\{1,\ 2,\ \ldots, n\}$ elementų keitinių grupėje S_n apibrėžta funkcija

$$\operatorname{sgn} : S_n \to \{\pm 1\},\ \sigma \mapsto \operatorname{sgn}(\sigma).$$

Keitinys σ vadinamas *lyginiu* (*nelyginiu*), jei $\operatorname{sgn}(\sigma) = 1$ ($\operatorname{sgn}(\sigma) = -1$).

5.11.31 teiginys. *Funkcija*

$$\operatorname{sgn} : S_n \to \{\pm 1\},\ \sigma \mapsto \operatorname{sgn}(\sigma)$$

yra grupių homomorfizmas, t. y. bet kuriems aibės $\{1,\ 2,\ \ldots, n\}$ *elementų keitiniams* σ *ir* τ *teisinga lygybė*

$$\operatorname{sgn}(\sigma \cdot \tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau).$$

Įrodymas. Remdamiesi keitinių lyginumo apibrėžimu, galime užrašyti lygybes:

$$(\sigma \cdot \tau)A = (\sigma \cdot (\tau)A) = \sigma(\operatorname{sgn}(\tau)A) = \operatorname{sgn}(\tau)\sigma A = \operatorname{sgn}(\tau) \cdot \operatorname{sgn}(\sigma)A.$$

Iš šių lygybių matome, kad

$$\operatorname{sgn}(\sigma \cdot \tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau),$$

nes $A \neq 0$. $\square$

Šią naująją lyginumo sąvoką susiesime su skaičių poros inversijos sąvoka. Tam į skaičių A ir σA apibrėžimą žvilgtelėkime atidžiau.

Pirmiausia įsižiūrėkime, kaip sudaryti skaičiai A ir σA. Tam nagrinėkime aibės $\{1,\ 2,\ \ldots, n\}$ dvielemenčių poaibių aibę

$$\{\{i,\ j\}\ |1 \leqslant i < j \leqslant n\}.$$

Kiekvienam šios dvielemenčių poaibių aibės elementui $\{i,\ j\}$, jei $i < j$, priskiriamas skaičiaus A daugiklis $i - j$, t. y. mažesnio ir didesnio poaibio $\{i,\ j\}$ elementų i ir j skirtumas. Taigi kiekvienas skaičiaus A daugiklis taip gaunamas iš vieno ir tiktai vieno aibės $\{1,\ 2,\ \ldots, n\}$ dvielemenčio poaibio. Išsiaiškinkime, kokius daugiklius sudauginę gauname skaičių σA? Kadangi

$$\{1,\ 2,\ \ldots, n\} = \{\sigma(1),\ \sigma(2),\ \ldots, \sigma(n)\},$$

tai ir šių aibių dvielemenčių poaibių aibės sutampa:

$$\{\{i,\ j\}\ |1 \leqslant i < j \leqslant n\} = \{\{\sigma(i),\ \sigma(j)\}\ |1 \leqslant i < j \leqslant n\}.$$

Taigi kiekvienas skaičiaus σA daugiklis susiejamas su vienu ir tik vienu dvielemenčiu poaibiu $\{\sigma(i),\ \sigma(j)\}$ ir gaunamas kaip skirtumas $\sigma(i) - \sigma(j)$, jei $i < j$. Jei $\sigma(i) < \sigma(j)$, kai $i < j$, tai $\sigma(i) - \sigma(j)$ yra tiek skaičiaus σA, tiek skaičiaus A daugiklis. Jei $\sigma(i) > \sigma(j)$, kai $i < j$, tai $\sigma(i) - \sigma(j)$ yra skaičiaus σA daugiklis, o $\sigma(j) - \sigma(i)$ yra skaičiaus A daugiklis. Darome išvadą, kad

$$\sigma A = (-1)^r A = \operatorname{sgn}(\sigma)A, \text{ t. y. } \operatorname{sgn}(\sigma) = (-1)^r,$$

čia r lygus skaičiui porų $(i,\ j)$, tenkinančių nelygybes $i < j$ ir $\sigma(i) > \sigma(j)$.

Ir vėl galime išskirti skaičių poros inversijos sąvoką, kuri buvo apibrėžta anksčiau. Ši sąvoka patogi apskaičiuojant konkrečių keitinių lyginumą.

5.11.32 apibrėžimas. Sakoma, kad skaičių $\sigma(i)$ ir $\sigma(j)$ pora $(\sigma(i),\ \sigma(j))$, tenkinanti sąlygą $\sigma(i) > \sigma(j)$, kai $i < j$, sudaro *inversiją*, t. y. netvarką. Atkreipkite dėmesį: skaičiaus $\sigma(i)$ užimamos vietos indeksas i mažesnis nei skaičiaus $\sigma(j)$ užimamos vietos indeksas j, bet pats skaičius $\sigma(i)$ didesnis nei skaičius $\sigma(j)$.

5.11.33 išvada. *Kaip matome,*

$$\sigma A = \operatorname{sgn}(\sigma)A = (-1)^r A,$$

čia r yra lygus skaičių porų $(\sigma(i),\ \sigma(j))$, $i < j$, apatinėje keitinio

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$$

eilutėje, sudarančių inversijas, skaičiui. Viršutinės keitinio eilutės skaičiai užrašyti natūralia tvarka ir jokia skaičių pora nesudaro inversijos.

Remiantis skaičių poros inversijos apibrėžimu nesunku apskaičiuoti aibės elementų keitinio lyginumą.

5.11.34 pavyzdys. Tegu

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 2 & 4 \end{pmatrix}.$$

Čia

$$\sigma(1) = 3,\ \sigma(2) = 5,\ \sigma(3) = 1.\ \sigma(4) = 6,\ \sigma(5) = 2,\ \sigma(6) = 4.$$

Išrašykime visas apatinės eilutės skaičių poras, sudarančias inversijas:

$$(3,\ 1),\ (3,\ 2),\ (5,\ 1),\ (5,\ 2),\ (5,\ 4),\ (6,\ 2),\ (6,\ 4).$$

Kadangi jų skaičius nelyginis (jų 7), tai užrašytas keitinys yra nelyginis.

5.11.35 teiginys. *Dviejų skaičių transpozicija*

$$(i\ j) = \begin{pmatrix} 1 & \dots & i & \dots & j & \dots & n \\ 1 & \dots & j & \dots & i & \dots & n \end{pmatrix}$$

yra nelyginė.

Įrodymas. Apskaičiuokime apatinėje eilutėje skaičių porų, sudarančių inversijas, skaičių. Tegu $i < j$. Tuomet skaičių poros $(j,\ l)$, čia $i \leqslant l \leqslant j-1$, taip pat skaičių poros $(m,\ i)$, čia $i+1 \leqslant m \leqslant j-1$, sudaro inversijas. Tokių porų skaičius

$$(j-i) - (i-1) + (j-1) - i = 2(j-i) - 1$$

yra nelyginis. □

Kaip žinome, kiekvieną keitinį galima užrašyti transpozicijų sandauga (žr. 5.11.16 išvadą). Kadangi transpozicija yra nelyginis ketinys, o funkcija sgn – homomorfizmas, tai galime suformuluoti išvadą.

5.11.36 išvada. *Lyginio (nelyginio) keitinio bet kuriame užraše transpozicijų sandauga transpozicijų skaičius yra lyginis (nelyginis).*

5.11.37 išvada. *Kiekvienas aibės* $\{1,\ 2,\ \ldots, n\}$ *elementų keitinys* σ *užrašomas transpozicijų sandauga. Bet kurioje lyginio (nelyginio) keitinio išraiškoje transpozicijų sandauga transpozicijų skaičius yra lyginis (nelyginis).*

5.11.38 teiginys. *Keitinio*

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}$$

apatinėje eilutėje bet kuriuos du skaičius sukeitus vietomis, pasikeičia keitinio lyginumas.

Įrodymas. Sudauginkime transpoziciją (j_r, j_s) ir keitinį σ:

$$(j_r, j_s)\begin{pmatrix} 1 & \ldots & r & \ldots & s & \ldots & n \\ j_1 & \ldots & j_r & \ldots & j_s & \ldots & j_n \end{pmatrix} = \begin{pmatrix} 1 & \ldots & r & \ldots & s & \ldots & n \\ j_1 & \ldots & j_s & \ldots & j_r & \ldots & j_n \end{pmatrix}.$$

Iš pastarosios lygybės matome, kad

$$\operatorname{sgn}\begin{pmatrix} 1 & \ldots & r & \ldots & s & \ldots & n \\ j_1 & \ldots & j_s & \ldots & j_r & \ldots & j_n \end{pmatrix} = \operatorname{sgn}((j_r,\ j_s)) \cdot \operatorname{sgn}(\sigma) = -\operatorname{sgn}(\sigma).$$

□

Kaip žinome, keitinio viršutinės eilutės skaičius nebūtina surašyti natūralia tvarka. Svarbu, kad po kiekvienu viršutinės eilutės skaičiumi būtų parašytas jo vaizdas.

5.11.39 teiginys. *Keitinio*

$$\sigma = \begin{pmatrix} i_1 & \ldots & i_r & \ldots & i_s & \ldots & n \\ j_1 & \ldots & j_r & \ldots & j_s & \ldots & j_n \end{pmatrix}$$

viršutinėje eilutėje bet kuriuos du skaičius sukeitus vietomis, pasikeičia jo lyginumas.

Įrodymas. Sudauginkme keitinį σ ir transpoziciją (i_r, i_s):

$$\begin{pmatrix} i_1 & \ldots & i_r & \ldots & i_s & \ldots & i_n \\ j_1 & \ldots & j_r & \ldots & j_s & \ldots & j_n \end{pmatrix}(i_r, i_s) = \begin{pmatrix} i_1 & \ldots & i_s & \ldots & i_r & \ldots & i_n \\ j_1 & \ldots & j_r & \ldots & j_s & \ldots & j_n \end{pmatrix}.$$

Iš pastarosios lygybės matome, kad

$$sgn\begin{pmatrix} i_1 & \ldots & i_s & \ldots & i_r & \ldots & i_n \\ j_1 & \ldots & j_r & \ldots & j_s & \ldots & j_n \end{pmatrix} = \operatorname{sgn}((i_r,\ i_s)) \cdot \operatorname{sgn}(\sigma) = -\operatorname{sgn}(\sigma).$$

□

5.11.40 išvada. *Aibės* $\{1,\ 2,\ \ldots, n\}$ *elementų keitinio*

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}$$

stulpelius sukeitus vietomis, keitinio lyginumas nesikeičia. (Keičiant du stulpelius vietomis keitinio viršutinėje ir apatinėje eilutėse du skaičiai sukeičiami vietomis, todėl, remiantis 5.11.38 ir 5.11.39 teiginiais, keitinio lyginumas nepasikeičia.)

5.11.41 išvada. *Norint praktiškai apskaičiuoti keitinio lyginumą, reikia suskaičiuoti viršutinės ir apatinės eilučių skaičių porų, sudarančių inversijas, skaičius ir juos sudėti. Jei suma lyginė(nelyginė), tai keitinys lyginis(nelyginis).*

5.12 Sujungtinių elementų klasės

5.12.1 apibrėžimas. Grupės S_n elementai x ir y vadinami *sujungtiniais*, jei egzistuoja toks grupės S_n elementas σ, kad $y = \sigma x \sigma^{-1}$. Tarp grupės S_n sujungtinių elementų x ir y sutarkime rašyti ženklą $\sim$: $x \sim y$.

5.12.2 teiginys. *Sąryšis* $\sim$ *yra ekvivalentumo sąryšis grupėje* S_n*.*

Įrodymas. Įsitikinsime, kad sąryšis $\sim$ tenkina tris ekvivalentumo sąryšio apibrėžimo sąlygas.

1. Kiekvienam $x \in S_n$, $x \sim x$, nes $x = \mathrm{id} \circ x \circ \mathrm{id}$ (id – grupės S_n vienetas).

2. Jei $x \sim y$, t. y. egzistuoja toks $\sigma \in S_n$, kad $y = \sigma x \sigma^{-1}$, tai ir $y \sim x$, nes $x = \sigma^{-1} y \sigma = \sigma^{-1} y (\sigma^{-1})^{-1}$.

3. Jei $x \sim y$, $y \sim z$, tai ir $x \sim z$. Iš tikrųjų, kadangi egzistuoja tokie $\sigma, \tau \in S_n$, kad $z = \tau y \tau^{-1}$, $y = \sigma x \sigma^{-1}$, tai $z = \tau \sigma x \sigma^{-1} \tau^{-1} = \tau \sigma x (\tau \sigma)^{-1}$.

□

5.12.3 apibrėžimas. Elemento $x \in S_n$ ekvivalentumo klasė pagal ekvivalentumo sąryšį $\sim$ yra vadinama elementui x *sujungtinių elementų klase.*

5.12.4. Apibrėžkime grupės S_n poaibį K_x, sudarytą iš visų tokių elementų σ, kurie yra perstatomi su elementu $x \in S_n$:

$$K_x := \{\sigma \in S_n |\ \sigma x = x \sigma\}.$$

5.12.5 teiginys. *Kiekvienam grupės* S_n *elementui* x *grupės* S_n *poaibis* K_x *yra grupės* S_n *pogrupis.*

Įrodymas. Visų pirma pastebėsime, kad, jei τ yra perstatomas su x, tai ir τ^{-1} yra perstatomas su x. Iš tikrųjų, lygybė $\tau x = x\tau$ yra ekvivalenti lygybei $x\tau^{-1} = \tau^{-1}x$.

Sakykime, $\sigma, \tau \in K_x$. Tada

$$(\sigma\tau^{-1})x = \sigma x\tau^{-1} = x(\sigma\tau^{-1}).$$

Vadinasi, jei $\sigma, \tau \in K_x$, tai $\sigma\tau^{-1} \in K_x$. Taigi K_x yra grupės S_n pogrupis. □

5.12.6 apibrėžimas. K_x vadinamas grupės S_n elemento x *stacionariuoju pogrupiu.*

Apibrėžkime grupės S_n veikimą aibėje $X = S_n$:

$$* : S_n \times S_n \to S_n,\ g * x = gxg^{-1},\ g, x \in S_n.$$

Šiuo atveju aibės S_n elemento x orbita $S_n * x = \{gxg^{-1} \mid g \in S_n\}$ yra grupės S_n elementui x sujungtinių elementų klasė, o elemento $x \in S_n$ stabilizatorius $\mathrm{st}_{S_n}(x) = \{g \in S_n \mid g * x = x\}$ sutampa su to elemento stacionariuoju pogrupiu K_x (žr. 5.9.4 apibrėžimą).

5.12.7 teiginys. *Grupės S_n elementui x sujungtinių elementų klasės elementų skaičius lygus elemento x stacionariojo pogrupio K_x indeksui grupėje S_n.*

Šis teiginys, turint galvoje po 5.12.6 apibrėžimo pateiktą grupės S_n veikimą aibėje $X = S_n$, yra kitais terminais suformuluotas 5.9.10 teiginys. Vis dėlto pateikiame tiesioginį šio teiginio įrodymą.

Įrodymas. Sakykime, $\{x_1, x_2, \ldots, x_r\}$ – elementui $x = x_1$ sujungtinių elementų klasė (elementai $x_1, x_2, \ldots, x_r$ yra skirtingi), o $g_1 = (1)$, g_2, …, g_r – tokie grupės S_n elementai, kad $x_1 = g_1x_1g_1^{-1}$, $x_2 = g_2x_1g_2^{-1}$, …, $x_r = g_rx_1g_r^{-1}$.

Kiekvienam $h \in S_n$ egzistuoja vienintelis toks j, $1 \le j \le r$, kad $hx_1h^{-1} = x_j$. Taigi $hx_1h^{-1} = g_jx_1g_j^{-1}$. Šią lygybę iš kairės padauginę iš g_j^{-1}, o iš dešinės – iš g_j, gauname: $g_j^{-1}hx_1h^{-1}g_j = x_1$ arba

$$g_j^{-1}hx_1(g_j^{-1}h)^{-1} = x_1.$$

Vadinasi, $g_j^{-1}h \in K_x$ arba $h \in g_jK_x$. Ir atvirkščiai, jei $h \in g_jK_x$, tai $g_j^{-1}h \in K_x$. Tuomet $g_j^{-1}hx_1(g_j^{-1}h)^{-1} = x_1$ arba $hx_1h^{-1} = g_jx_1g_j^{-1} = x_j$.

Kaip matome, kiekvieną kairiąją pogrupio K_x gretutinę klasę g_jK_x, $1 \le j \le r$, atitinka elementui $x = x_1$ sujungtinis elementas $x_j = hx_1h^{-1}$, $h \in g_jK_x$, $1 \le j \le r$. Kadangi $S_n = \bigcup_{j=1}^{r} g_jK_x$, tai teoremos įrodymas baigtas. □

5.12.8 apibrėžimas. Nedidėjanti sveikųjų skaičių seka

$$\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \cdots \geq \lambda_s \geq 1$$

yra vadinama skaičiaus $n \in \mathbb{N}$ *skaidiniu*, jei $\sum\limits_{j \geq 1} \lambda_j = n$. Skaičiaus n visų skaidinių skaičius yra žymimas $p(n)$.

5.12.9 pavyzdys. Skaičiaus 7 skaidiniai yra šie:

$$\begin{array}{llll}
7 & & & \\
6 & 1 & & \\
5 & 2 & & \\
5 & 1 & 1 & \\
4 & 3 & & \\
4 & 2 & 1 & \\
4 & 1 & 1 & 1 \\
3 & 3 & 1 &
\end{array}
\qquad
\begin{array}{lllllll}
3 & 2 & 2 & & & & \\
3 & 2 & 1 & 1 & & & \\
3 & 1 & 1 & 1 & 1 & & \\
2 & 2 & 2 & 1 & & & \\
2 & 2 & 1 & 1 & 1 & & \\
2 & 1 & 1 & 1 & 1 & 1 & \\
1 & 1 & 1 & 1 & 1 & 1 & 1
\end{array}$$

Taigi $p(7) = 15$.

Skaičiaus $n \in \mathbb{N}$ skaidinį $\lambda_1 \geq \lambda_2 \geq \lambda_3 \geq \cdots \geq \lambda_m \geq 1$ sutarkime užrašyti trumpiau. Sakykime,

$$\lambda_1 = \lambda_2 = \cdots = \lambda_{s_1} > \lambda_{s_1+1} = \cdots = \lambda_{s_1+s_2} > \ldots$$

$$> \lambda_{s_1+s_2+\cdots+s_{r-1}+1} = \cdots = \lambda_{s_1+s_2+\cdots+s_{r-1}+s_r}.$$

Pažymėję $\lambda_1 = \mu_1$, $\lambda_{s_1+1} = \mu_2$, $\ldots$, $\lambda_{s_1+s_2+\cdots+s_{r-1}+1} = \mu_r$, anksčiau nurodytą skaičiaus n skaidinį galime užrašyti taip:

$$(\mu_1^{(s_1)}, \mu_2^{(s_2)}, \ldots, \mu_r^{(s_r)}), \quad \mu_1 > \mu_2 > \cdots > \mu_r, \quad \sum_{j=1}^{r} s_j \mu_j = n. \tag{5.5}$$

(5.5) skaidinį trumpumo dėlei pažymėkime $\widehat{\mu}$.

5.12.10. Kiekvienas grupės S_n elementas σ yra išskaidomas į nepriklausomų ciklų sandaugą $\sigma = \sigma_1 \sigma_2 \ldots \sigma_m$. Į grupės S_n elemento sandaugą nepriklausomais ciklais, kaip susitarta, neįrašomi ciklai, kurių ilgis lygus 1. Kadangi nepriklausomi ciklai yra perstatomi, tai sakykime, kad σ_1, σ_2, $\ldots$, σ_m šiame skaidinyje yra išdėstyti jų ilgių nedidėjimo tvarka. Surašę šių ciklų ilgius ir prirašę tiek vienetų, kiek elemento σ skaidinyje praleista ilgio 1 ciklų, gauname skaičiaus n skaidinį:

$$(\lambda_1^{(s_1)}, \lambda_2^{(s_2)}, \ldots, \lambda_r^{(s_r)}),$$

čia $\lambda_1 > \lambda_2 > \cdots > \lambda_r \geq 1$.

Taigi kiekvieną grupės S_n elementą σ atitinka skaičiaus n skaidinys

$$\widehat{\lambda} = (\lambda_1^{(s_1)}, \lambda_2^{(s_2)}, \ldots, \lambda_r^{(s_r)}), \quad \lambda_1 > \lambda_2 > \cdots > \lambda_r \geq 1,$$

čia s_j – ilgio λ_j ciklų skaičiai elemento σ skaidinyje nepriklausomais ciklais, įskaitant ir ilgio 1 ciklus.

5.12.11 apibrėžimas. Jei grupės S_n elementą σ atitinka skaičiaus n skaidinys $\widehat{\lambda}$, tai σ vadinamas *ciklinio tipo* $\widehat{\lambda}$ *elementu.*

Pratimas. Sakykime,

$$\widehat{\lambda} = (\lambda_1^{(s_1)}, \lambda_2^{(s_2)}, \ldots, \lambda_r^{(s_r)}),$$

čia $\lambda_1 > \lambda_2 > \cdots > \lambda_r \geq 1$, yra skaičiaus n skaidinys (t. y. $\sum\limits_{j=1}^{r} s_j\lambda_j = n$). Įrodykite, kad grupėje S_n yra

$$\frac{n!}{\lambda_1^{s_1}\lambda_2^{s_2}\ldots\lambda_r^{s_r}s_1!s_2!\ldots s_r!}$$

ciklinio tipo $\widehat{\lambda}$ elementų.

5.12.12 teiginys. *Grupės S_n ciklui $(j_1\ j_2\ \ldots\ j_r)$ sujungtinis elementas*

$$\pi(j_1\ j_2\ \ldots\ j_r)\pi^{-1}, \quad \pi \in S_n,$$

yra ciklas $(\pi(j_1)\ \pi(j_2)\ \ldots\ \pi(j_r))$ (čia $\pi(j)$ – bijekcijos $\pi : \mathbb{N}_n \to \mathbb{N}_n$ reikšmė taške $j \in \mathbb{N}_n$).

Įrodymas. Bijekcija $\alpha = \pi(j_1\ j_2\ \ldots\ j_r)\pi^{-1}$ aibės $\mathbb{N}_n$ elementą $\pi(j_i)$ perveda į $\pi(j_{i+1})$, $1 \leq i \leq r-1$, elementą $\pi(j_r)$ – į $\pi(j_1)$, o elementai

$$\pi(l) \in \mathbb{N}_n \setminus \{\pi(j_1), \pi(j_2), \ldots, \pi(j_r)\}$$

yra α-nejudami. □

5.12.13 teiginys. *Grupės S_n elementai σ ir τ yra sujungtiniai tada ir tik tada, kai jų cikliniai tipai sutampa.*

Įrodymas. Jei elementai σ ir τ yra sujungtiniai, tai egzistuoja toks $\pi \in S_n$, kad $\sigma = \pi\tau\pi^{-1}$. Sakykime, $\tau = \tau_1\tau_2\ldots\tau_m$ – keitinio τ išraiška nepriklausomų ciklų sandauga, joje ciklai $\tau_1, \tau_2, \ldots, \tau_m$ surašyti jų ilgių nedidėjimo tvarka. Tuomet

$$\sigma = \pi\tau\pi^{-1} = (\pi\tau_1\pi^{-1})(\pi\tau_2\pi^{-1})\ldots(\pi\tau_m\pi^{-1}).$$

Remiantis 5.12.12 teiginiu, ciklui τ_j sujungtinis elementas $\pi\tau_j\pi^{-1}$ yra tokio pat ilgio ciklas kaip ir ciklas τ_j, $1 \le j \le m$. Vadinasi, grupės S_n sujungtiniai elementai yra to paties ciklinio tipo.

Sakykime, grupės S_n elementai σ ir τ yra to paties ciklinio tipo

$$\widehat{\lambda} = (\lambda_1^{(s_1)}, \lambda_2^{(s_2)}, \dots, \lambda_r^{(s_r)}),$$

čia $\lambda_1 > \lambda_2 > \cdots > \lambda_r \ge 1$, $\sum\limits_{j=1}^{r} s_j\lambda_j = n$. Užrašykime elementus σ ir τ nepriklausomų ciklų sandaugomis, įskaitant ir ilgio 1 ciklus, surašydami ciklus jų ilgių nedidėjimo tvarka. Tada parašę elementą σ po elementu τ taip, kad atitinkamo ilgio ciklai būtų vienas po kitu, ir praleidę ciklų skliaustelius, gauname tokį keitinį $\pi : \mathbb{N}_n \to \mathbb{N}_n$, kad $\sigma = \pi\tau\pi^{-1}$. □

5.12.14 pavyzdys. Imkime grupės S_8 elementus $\sigma = (1\ 3\ 7)(2\ 8\ 5\ 4)$ ir $\tau = (2\ 6\ 5)(4\ 1\ 7\ 8)$. Šių elementų cikliniai tipai sutampa. Vadinasi, šie elementai yra sujungtiniai, t. y. egzistuoja toks elementas π, kad $\sigma = \pi\tau\pi^{-1}$. Remdamiesi teoremos įrodymu, gauname:

$$\pi = \begin{pmatrix} 4 & 1 & 7 & 8 & 2 & 6 & 5 & 3 \\ 2 & 8 & 5 & 4 & 1 & 3 & 7 & 6 \end{pmatrix} = (1\,8\,4\,2)(3\,6)(5\,7).$$

Iš tikrųjų,

$$\pi\tau\pi^{-1} = (1\,8\,4\,2)(3\,6)(5\,7)(2\,6\,5)(4\,1\,7\,8)(1\,2\,4\,8)(3\,6)(5\,7) =$$

$$= (1\,3\,7)(2\,8\,5\,4) = \sigma.$$

Pažymėsime, kad egzistuoja ne vienas toks elementas π, kad $\sigma = \pi\tau\pi^{-1}$. Pavyzdžiui, jei imtume

$$\pi_2 = \begin{pmatrix} 4 & 1 & 7 & 8 & 2 & 6 & 5 & 3 \\ 8 & 5 & 4 & 2 & 1 & 3 & 7 & 6 \end{pmatrix} = (1\,5\,7\,4\,8\,2)(3\,6),$$

tai $\sigma = \pi_2\tau\pi_2^{-1}$. Iš tikrųjų,

$$(1\,5\,7\,4\,8\,2)(3\,6)(2\,6\,5)(4\,1\,7\,8)(1\,2\,8\,4\,7\,5)(3\,6) = (1\,3\,7)(2\,8\,5\,4).$$

Įrodykite, kad egzistuoja 12 tokių elementų $\pi \in S_8$, kad $\sigma = \pi\tau\pi^{-1}$ ir nurodykite visus juos.

Pratimai.

1. Raskite grupės S_7 elementų $(1\ 2)(3\ 4\ 5)$ ir $(1\ 2\ 3)(4\ 5\ 6\ 7)$ eiles.

2. Sakykime, σ_1, σ_2, ..., σ_m yra nepriklausomi grupės S_n ciklai, kurių ilgiai yra lygūs λ_1, λ_2, ..., λ_m. Įrodykite, kad elemento $\sigma_1\sigma_2\ldots\sigma_m$ eilė yra lygi skaičių λ_1, λ_2, ..., λ_m mažiausiam bendrajam kartotiniui.

3. Raskite grupėje S_7 didžiausios eilės elementą. Kiek grupėje S_7 yra didžiausios eilės elementų? Kokia šių elementų eilė?

4. Raskite grupėje S_8 didžiausios eilės elementą. Kiek grupėje S_8 yra didžiausios eilės elementų? Kokia šių elementų eilė?

5. Raskite grupės S_7 elemento $(1\ 2)(3\ 4\ 5)$ stacionarųjį pogrupį. Kokia šio pogrupio eilė? Kiek elementų turi elementui $(1\ 2)(3\ 4\ 5)$ sujungtinių elementų klasė.

6. Įrodykite, kad grupėje S_n yra $\frac{n!}{l(n-l)!}$ ilgio l $(l \leq n)$ ciklų.

5.13 Sylovo teoremos

5.13.1. Nagrinėkime grupę G, kurios eilė yra lygi n. Sakykime, skaičiaus n kanoninis skaidinys pirminiais skaičiais yra $n = \prod\limits_{j=1}^{s} p_j^{a_j}$. Ką galime pasakyti apie grupės G pogrupius, žinodami grupės eilės kanoninį skaidinį pirminiais skaičiais? Anksčiau įrodėme (Koši teorema), kad jei grupės G eilę n dalija pirminis skaičius p, tai egzistuoja grupės G elementas, kurio eilė yra lygi p. Kiekvienas grupės G eilės p elementas g generuoja grupės G p eilės ciklinį pogrupį $\langle g\rangle$. Anksčiau, nagrinėdami pavyzdžius, įsitikinome, kad ne kiekvienam grupės eilės n dalikliui d egzistuoja grupės d eilės elementas. Bendruoju atveju į šį klausimą atsako trys Sylovo teoremos, kurias šiame skyrelyje suformuluosime ir įrodysime.

5.13.2 teorema (pirmoji Sylovo teorema)**.** *Jei pirminio skaičiaus p laipsnis p^r dalija grupės G eilę n, tai egzistuoja grupės G pogrupis, kurio eilė yra p^r.*

5.13.3 apibrėžimas. Sakykime, grupės G eilė yra lygi n, p – pirminis skaičius. Jei $p^a \mid n$, $p^{a+1} \nmid n$, tai grupės G pogrupis, kurio eilė yra p^a, vadinamas grupės G *Sylovo p-pogrupiu.*

5.13.4 išvada. *Jei pirminis skaičius p dalija grupės G eilę n, tai egzistuoja bent vienas grupės G Sylovo p-pogrupis.*

5.13.5 teorema (antroji Sylovo teorema)**.** *Bet kurie baigtinės grupės G Sylovo p-pogrupiai yra sujungtiniai.*

5.13.6 teorema (trečioji Sylovo teorema)**.** *Sakykime, pirminis skaičius p dalija grupės G eilę n. Grupės G Sylovo p-pogrupių skaičius l tenkina sąlygas:*

i) $l \equiv 1 \pmod p$*;*

ii) $l \mid n$*.*

5.13.7. Pirmosios Sylovo teoremos įrodymo planas yra toks. Iš pradžių įrodysime pirmąją Sylovo teoremą atskiru atveju, pirminiam skaičiui p ir simetrinei grupei S_{p^n}. Paskui įrodysime, kad kiekviena baigtinė grupė G yra izomorfinė simetrinės grupės S_{p^n} pogrupiui, kai $n \in \mathbb{N}$ yra pakankamai didelis. Pagaliau įrodysime, kad jei grupė G yra grupės H pogrupis ir grupėje H egzistuoja Sylovo p-pogrupis, tai ir grupėje G egzistuoja Sylovo p-pogrupis.

5.13.8. Dabar nagrinėsime p^n-tojo laipsnio simetrinę grupę S_{p^n}, čia p – pirminis skaičius. Įrodysime, kad šioje grupėje egzistuoja Sylovo p-pogrupis. Išsiaiškinkime, kokia grupės S_{p^n} Sylovo p-pogrupio eilė. Tam išsiaiškinkime, koks didžiausias pirminio skaičiaus p laipsnis dalija grupės S_{p^n} eilę $p^n!$.

Kadangi skaičius $p^n!$ yra visų skaičių j, $1 \leq j \leq p^n$, sandauga, tai daugikliai, kurie dalijasi iš pirminio skaičiaus p, yra šie: pj, $1 \leq j \leq p^{n-1}$. Šių daugiklių sandauga yra lygi $p^{p^{n-1}}p^{n-1}!$. Tarę, kad didžiausias pirminio skaičiaus p laipsnis, kuris dalija $p^n!$, $n \geq 1$, yra $p^{t(n)}$, galime parašyti lygybę:

$$p^{t(n)} = p^{p^{n-1}+t(n-1)}, \; n \geq 1.$$

Vadinasi,

$$t(n) = p^{n-1} + t(n-1) = \cdots = p^{n-1} + p^{n-2} + \cdots + p + t(1).$$

Kadangi skaičių $p!$ dalija tik p^1, tai

$$t(n) = 1 + p + \cdots + p^{n-1} = \frac{p^n - 1}{p - 1}.$$

5.13.9. Matematinės indukcijos metodu pagal skaičių n įrodysime, kad simetrinėje grupėje S_{p^n} egzistuoja Sylovo p-pogrupis, t. y. pogrupis, kurio eilė yra lygi $p^{t(n)} = p^{p^{n-1}+p^{n-2}+\cdots+1}$.

5.13.10 teorema. *Simetrinėje grupėje S_{p^n} egzistuoja Sylovo p-pogrupis.*

Įrodymas. Pirmasis žingsnis. Atvejis, kai $n = 1$, akivaizdus. Grupėje S_p elementas $(1\ 2\ \ldots\ p)$ generuoja p eilės pogrupį.

Antrasis žingsnis. Sakykime, kad simetrinėje grupėje $S_{p^{n-1}}$ egzistuoja Sylovo p-pogrupis. Šio pogrupio eilė yra lygi

$$p^{t(n-1)} = p^{p^{n-2}+p^{n-3}+\cdots+1}.$$

Trečiasis žingsnis. Įrodysime, kad ir simetrinėje grupėje S_{p^n} egzistuoja Sylovo p-pogrupis, t. y. pogrupis, kurio eilė yra lygi

$$p^{t(n)} = p^{p^{n-1}+p^{n-2}+\cdots+1}.$$

Suskirstykime aibės $\mathbb{N}_{p^n}$ elementus į p poaibių:

$$A_0 = \{1, 2, \ldots, p^{n-1}\},$$

$$A_1 = \{p^{n-1}+1,\ p^{n-1}+2, \ldots, 2p^{n-1}\},$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots$$

$$A_j = \{jp^{n-1}+1,\ jp^{n-1}+2, \ldots, (j+1)p^{n-1}\},$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots$$

$$A_{p-1} = \{(p-1)p^{n-1}+1,\ (p-1)p^{n-1}+2, \ldots, p^n\}.$$

Nagrinėkime tokius simetrinės grupės S_{p^n} keitinius $f : \mathbb{N}_{p^n} \to \mathbb{N}_{p^n}$, kad $f(j) = j$, kai $p^{n-1} < j \leq p^n$. Šie elementai sudaro grupės S_{p^n} pogrupį H_0, izomorfinį grupei $S_{p^{n-1}}$. Kitaip tariant, H_0 sudaro tik tie aibės $\mathbb{N}_n$ elementų keitiniai, kurie perstatinėja tik poaibio A_0 elementus, o kitų poaibių A_j, $1 \leq j \leq p-1$, elementus palieka nejudamus. Pagal indukcinę prielaidą grupėje H_0 egzistuoja Sylovo p-pogrupis P_0, kurio eilė yra lygi $p^{t(n-1)}$. Imkime simetrinės grupės S_{p^n} elementą

$$\pi = \big(1\ p^{n-1}+1\ 2p^{n-1}+1\ \ldots\ (p-1)p^{n-1}+1\big)\circ$$

$$\ldots \quad \ldots \quad \ldots$$

$$\circ\big(j\ \ p^{n-1}+j\ \ 2p^{n-1}+j\ \ldots\ (p-1)p^{n-1}+j\big)\circ$$

$$\ldots \quad \ldots \quad \ldots$$

$$\circ\big(p^{n-1}\ \ 2p^{n-1}\ \ 3p^{n-1}\ \ldots\ p^n\big).$$

Šis keitinys poaibio A_0 elementus perveda į poaibio A_1 elementus, poaibio A_1 elementus – į poaibio A_2 elementus ir t. t. ir pagaliau poaibio A_{p-1} elementus – į poaibio A_0 elementus. Kitaip tariant, aibės $\mathbb{N}_n$ elementų keitinys π perstato cikliškai poaibius A_j, $0 \leq j \leq p-1$. Elemento π eilė yra lygi p. Pažymėsime, kad kiekvienam $f \in H_0$ keitinys $\pi^j f \pi^{-j}$, $0 \leq j \leq p-1$, perstatinėja tik aibės A_j elementus, o aibės $\mathbb{N}_{p^n}$ elementus, nepriklausančius poaibiui A_j, palieka nejudamus. Vadinasi, grupės S_{p^n} pogrupiai

$$H_j := \pi^j H_0 \pi^{-j},\ \ 0 \leq j \leq p-1$$

yra izomorfiniai grupei $S_{p^{n-1}}$ ir kiekviename pogrupyje H_j egzistuoja Sylovo p-pogrupis $P_j = \pi^j P_0 \pi^{-j}$, $0 \leq j \leq p-1$. Grupės S_{p^n} pogrupių H_i ir H_j elementai, kai $i \neq j$, yra perstatomi, nes šių pogrupių elementai perstatinėja nesikertančių aibių A_i ir A_j elementus. Vadinasi, grupės S_{p^n} pogrupis $P' = P_0 P_1 \ldots P_{p-1}$, generuotas pogrupių $P_j \subset H_j$, $0 \leq j \leq p-1$, yra izomorfinis tiesioginei sandaugai

$$P_0 \times P_1 \times \cdots \times P_{p-1}.$$

Taigi pogrupio P' eilė yra lygi $p^{t(n-1)p} = p^{t(n)-1}$. Kadangi $P_j = \pi^j P_0 \pi^{-j}$, $0 \leq j \leq p-1$, tai

$$\pi P_j = \pi^{j+1} P_0 \pi^{-j} = \pi^{j+1} P_0 \pi^{-(j+1)} \pi = P_{j+1}\pi,$$

čia $P_p := P_0$. Todėl $\pi P' = P'\pi$. Vadinasi, grupės S_{p^n} pogrupio P, generuoto ciklinio pogrupio $\langle\pi\rangle$ ir pogrupio P', kiekvienas elementas vieninteliu būdu užrašomas taip:

$$\pi^j \sigma_0 \sigma_1 \dots \sigma_{p-1},$$

čia $\sigma_i \in P_i$, $0 \leq i, j \leq p-1$. Simetrinės grupės S_{p^n} pogrupio P eilė yra lygi $p^{t(n)}$, todėl P ir yra simetrinės grupės S_{p^n} ieškomas Sylovo p-pogrupis. □

5.13.11 teorema (Keilio teorema)**.** *Grupė, kurios eilė yra lygi n, yra izomorfinė simetrinės grupės S_n pogrupiui.*

Įrodymas. Sakykime, grupės G eilė yra lygi n, $\{g_1, g_2, \dots, g_n\}$ – grupės G elementai. Grupės G elementui x priskirkime atvaizdį

$$f_x : G \to G, \quad f_x(g_j) = xg_j, \ 1 \leq j \leq n.$$

Atvaizdis $f_x : G \to G$ yra injekcinis. Iš tikrųjų, jei $f_x(g_i) = f_x(g_j)$, tai $xg_i = xg_j$ arba $g_i = g_j$ (priminsime, kad grupėje galima prastinti tiek iš kairės, tiek iš dešinės). Vadinasi, atvaizdis $f_x : G \to G$ yra aibės G elementų keitinys, t. y. $f_x \in S_n$. Taigi gavome atvaizdį

$$F : G \to S_n, \quad F(x) := f_x, \ x \in G.$$

Šis atvaizdis yra homomorfizmas, nes bet kuriems grupės G elementams x ir y ir bet kuriam $g_j \in G$ teisinga lygybė

$$f_{xy}(g_j) = xyg_j = f_x(yg_j) = f_x(f_y(g_j)) = (f_x \circ f_y)(g_j),$$

t. y.

$$F(xy) = f_{xy} = f_x \circ f_y = F(x) \circ F(y).$$

Be to, homomorfizmas $F : G \to S_n$ yra injekcinis. Iš tikrųjų, jei kuriems nors $x, y \in G$ teisinga lygybė $F(x) = F(y)$, tai kiekvienam $z \in G$, $f_x(z) = f_y(z)$, t. y. $xz = yz$ arba $x = y$ (grupėje G lygybę $xz = yz$ suprastinome iš dešinės iš elemento z).

Kadangi homomorfizmas $F : G \to S_n$ yra injekcinis, tai grupė G yra izomorfinė grupei $F(G)$ (žr. 5.7.26 teoremą), kuri yra grupės S_n pogrupis (žr. 5.7.22 teiginį). □

5.13.12 teorema. *Sakykime, grupė G yra grupės H pogrupis ir grupėje H egzistuoja Sylovo p-pogrupis P. Tuomet ir grupėje G egzistuoja Sylovo p-pogrupis.*

Įrodymas. Sakykime, $|G| = p^s a$, $p \nmid a$, $|H| = p^m b$, $p \nmid b$, P – grupės H Sylovo p-pogrupis, t. y. toks pogrupis, kurio eilė yra lygi p^m. Įrodysime, kad egzistuoja bent vienas toks grupės H elementas x, kad

$$G \cap xPx^{-1}$$

yra grupės G Sylovo p-pogrupis, t. y. toks pogrupis, kurio eilė yra lygi p^s.

Nagrinėkime grupėje H dvigubas gretutines klases

$$GxP = \{gxh \mid g \in G,\, h \in P\}, \quad x \in H.$$

Įrodysime, kad dvi tokios klasės arba sutampa arba neturi bendrų elementų. Sakykime, $z \in GxP \cap GyP$. Tuomet elementą z galime užrašyti taip:

$$z = g_1 x h_1 = g_2 y h_2, \quad g_1, g_2 \in G, \quad h_1, h_2 \in P.$$

Remdamiesi lygybe $g_1 x h_1 = g_2 y h_2$, gauname $x = g_1^{-1} g_2 y h_2 h_1^{-1} \in GyP$, t. y. $GxP \subset GyP$. Panašiai gauname, kad $y = g_2^{-1} g_1 x h_1 h_2^{-1} \in GxP$, t. y. $GyP \subset GxP$.

Taigi įrodėme, kad, jei grupės H dvigubos gretutinės klasės GxP ir GyP turi bendrą elementą, tai jos ir sutampa. Vadinasi, grupės H dvigubos gretutinės klasės GxP, $x \in H$ suskaido grupę H į netuščius, paporiui neturinčius bendrų elementų poaibius. Tada galime užrašyti

$$H = \bigcup_{j=1}^{r} G x_j P,$$

čia x_j, $1 \le j \le r$, yra skirtingų dvigubų gretutinių klasių atstovai. Iš čia gauname lygybę

$$|H| = |Gx_1P| + |Gx_2P| + \cdots + |Gx_rP|. \tag{5.6}$$

Grupės H pogrupiams G ir $x_j P x_j^{-1}$ pritaikę 5.7.30 teiginį, gauname, kad dviguboje gretutinėje klasėje Gx_jP elementų skaičius yra lygus

$$|Gx_jP| = |Gx_jPx_j^{-1}| = \frac{|G||x_jPx_j^{-1}|}{|G \cap x_jPx_j^{-1}|} = \frac{|G||P|}{|G \cap x_jPx_j^{-1}|}, \quad 1 \le j \le r.$$

Sakykime, $|G \cap x_jPx_j^{-1}| = p^{t_j}$, $0 \le t_j < s$, $1 \le j \le r$. Tuomet dviguboje gretutinėje klasėje Gx_jP elementų skaičius yra lygus

$$|Gx_jP| = \frac{|G||P|}{|G \cap x_jPx_j^{-1}|} = \frac{p^s p^m ab}{p^{t_j}} = p^{s-t_j+m} ab, \quad 1 \le j \le r.$$

Dabar įsitikinsime, kad bent vienam j, $1 \le j \le r$, $|G \cap x_j P x_j^{-1}| = p^s$. Iš tikrųjų, jei kiekvienam j, $1 \le j \le r$, būtų teisinga lygybė

$$|G \cap x_j P x_j^{-1}| = p^{t_j}$$

ir $0 \le t_j < s$, tai kiekvienos dvigubos gretutinės klasės Gx_jP elementų skaičius $p^{s-t_j+m}ab$ dalytųsi iš p^{m+1}, todėl, remiantis (5.6) lygybe, iš p^{m+1} dalytųsi ir grupės H eilė $|H|$. Taip negali būti, nes $|H| = p^m b$ ir $p \nmid b$. Taigi egzistuoja bent vienas toks j_0, $1 \le j_0 \le r$, kad $|G \cap x_{j_0} P x_{j_0}^{-1}| = p^s$, t. y.

$$G \cap x_{j_0} P x_{j_0}^{-1}$$

yra grupės G Sylovo p-pogrupis. □

Pirmosios Sylovo teoremos įrodymas. Sakykime, G – grupė, $|G| = p^s a = n$, $p \nmid a$. Teigiame, kad grupėje G egzistuoja Sylovo p-pogrupis. Remiantis Keilio teorema (žr. 5.13.11 teoremą), grupė G yra izomorfinė simetrinės grupės S_n pogrupiui G'. Parinkime tokį m, kad būtų teisinga nelygybė $n < p^m$. Simetrinę grupę S_n galime nagrinėti kaip simetrinės grupės S_{p^m} pogrupį. Taigi

$$G' \subset S_n \subset S_{p^m}.$$

Kadangi grupėje S_{p^m} egzistuoja Sylovo p-pogrupis (žr. 5.13.10 teoremą), tai, remiantis 5.13.12 teorema, ir grupės S_{p^m} pogrupyje G' taip pat egzistuoja Sylovo p-pogrupis P'. Jei $f : G' \to G$ – izomorfizmas, tai $f(P') = P$ yra grupės G Sylovo p-pogrupis. □

Antrosios Sylovo teoremos įrodymas. Sakykime, G – grupė, P ir P' – grupės G Sylovo p-pogrupiai. Įrodysime, kad pogrupiai P ir P' yra sujungtiniai, t. y. egzistuoja toks grupės G elementas g, kad $P' = gPg^{-1}$.

Sakykime, $|G| = p^s a = n$, $p \nmid a$, $|P| = |P'| = p^s$. Nagrinėkime grupės G dvigubas gretutines klases

$$P'xP = \{gxh \mid g \in P',\, h \in P\}, \quad x \in G.$$

Panašiai kaip ir 5.13.12 teoremos įrodyme galima įsitikinti, kad dvi tokios klasės, arba sutampa arba neturi bendrų elementų. Užrašykime grupės skaidinį dvigubomis gretutinėmis klasėmis:

$$G = \bigcup_{j=1}^{r} P'x_jP,$$

čia x_j, $1 \le j \le r$, yra skirtingų dvigubų gretutinių klasių atstovai. Iš čia gauname lygybę

$$|H| = |P'x_1P| + |P'x_2P| + \cdots + |P'x_rP|. \tag{5.7}$$

Remiantis 5.7.30 teiginiu, dvigubos gretutinės klasės $P'x_jP$ elementų skaičius lygus

$$|P'x_jP| = |P'x_jPx_j^{-1}| = \frac{|P'||x_jPx_j^{-1}|}{|P' \cap x_jPx_j^{-1}|} = \frac{|P'||P|}{|P' \cap x_jPx_j^{-1}|},\ 1 \leq j \leq r.$$

Sakykime,

$$|P' \cap x_jPx_j^{-1}| = p^{t_j},$$

$0 \leq t_j \leq s$, $1 \leq j \leq r$. Tada $|P'x_jP| = p^{2s-t_j}$, $1 \leq j \leq r$. Jei kiekvienam j, $1 \leq j \leq r$, būtų $0 \leq t_j < s$, tai skaičius p^{2s-t_j} dalytųsi iš p^{s+1}, todėl, remiantis (5.7) lygybe, iš p^{s+1} dalytųsi ir grupės G eilė $|G|$. Taip negali būti, nes $|G| = p^s a$, $p \nmid a$. Taigi egzistuoja toks j_0, $1 \leq j_0 \leq r$, kad

$$|P' \cap x_{j_0}P\,x_{j_0}^{-1}| = p^s,$$

t. y. $P' = x_{j_0}P\,x_{j_0}^{-1}$. □

Trečiosios Sylovo teoremos įrodymas. Sakykime, G – grupė, $n = |G| = p^s a$, $p \nmid a$, P – grupės G Sylovo p-pogrupis, t. y. P – grupės G pogrupis, kurio eilė yra lygi $|P| = p^s$. Nagrinėkime pogrupio P normalizatorių $N_G(P)$ grupėje G. Pagal apibrėžimą

$$N_G(P) = \{x \in G|\ xPx^{-1} = P\}.$$

Sakykime, kad grupės G skaidinys kairiosiomis gretutinėmis klasėmis pagal pogrupį $N_G(P)$ yra

$$G = \bigcup_{j=1}^{l} x_jN_G(P),$$

čia x_j, $1 \leq j \leq l$ – skirtingų kairiųjų gretutinių klasių atstovai. Teigiame, kad grupės G visi skirtingi Sylovo p-pogrupiai yra šie: $x_jPx_j^{-1}$, $1 \leq j \leq l$. Iš tikrųjų, tarkime, kad P' yra grupės G Sylovo p-pogrupis. Remiantis antrąja Sylovo teorema, pogrupis P' yra sujungtinis pogrupiui P, todėl egzistuoja toks $x \in G$, kad

$$P' = xPx^{-1}.$$

Sakykime, kad elementas x priklauso kairiajai gretutinei klasei $x_jN_G(P)$. Tuomet egzistuoja toks $h \in N_G(P)$, kad $x = x_jh$. Tada teisinga lygybė

$$P' = xPx^{-1} = x_jhP(x_jh)^{-1} = x_jhPh^{-1}x_j^{-1} = x_jPx_j^{-1}.$$

Taigi kiekvienas grupės G Sylovo p-pogrupis sutampa su vienu iš pogrupių $x_jPx_j^{-1}$, $1 \leq j \leq l$. Lieka įsitikinti, kad Sylovo p-pogrupiai $x_jPx_j^{-1}$, $1 \leq j \leq l$ yra skirtingi. Iš tikrųjų, tarkime, kad $x_jPx_j^{-1} = x_iPx_i^{-1}$. Tuomet $x_i^{-1}x_jP(x_i^{-1}x_j)^{-1} = P$, todėl

$x_i^{-1}x_j \in N_G(P)$, t. y. $x_j \in x_iN_G(P)$. Kadangi gretutinės klasės $x_iN_G(P)$ ir $x_jN_G(P)$ turi bendrą elementą x_j, tai jos sutampa. Vadinasi, $i = j$.

Kaip matome, egzistuoja abipus vienareikšmė atitiktis tarp grupės G Sylovo p-pogrupių ir grupės G kairiųjų gretutinių klasių pagal Sylovo p-pogrupio P normalizatorių $N_G(P)$ grupėje G. Vadinasi, gupės G Sylovo p-pogrupių yra l. Kadangi pogrupio indeksas dalija grupės G eilę, tai $l \mid n$. Lieka įrodyti, kad $l \equiv 1 \pmod p$.

Užrašykime grupės G skaidinį dvigubomis gretutinėmis klasėmis PxP, $x \in G$:

$$G = \bigcup_{j=1}^{r} Px_jP,$$

čia x_j, $1 \le j \le r$, – skirtingų dvigubų gretutinių klasių atstovai. Panašiai kaip ir 5.13.12 teoremos įrodyme galima įsitikinti, kad dvi dvigubos gretutinės klasės arba sutampa, arba neturi bendrų elementų. Jei $x_j \in N_G(P)$, tai

$$Px_jP = PPx_j = Px_j.$$

Jei $x_j \notin N_G(P)$, tai

$$P \cap x_jPx_j^{-1} \subset P, \;\; P \cap x_jPx_j^{-1} \ne P.$$

Vadinasi, jei $x_j \notin N_G(P)$, tai dvigubos gretutinės klasės Px_jP elementų skaičius yra lygus

$$|Px_jP| = \frac{|P||x_jPx_j^{-1}|}{|P \cap x_jPx_j^{-1}|} = p^{2s-t_j},$$

čia $|P \cap x_jPx_j^{-1}| = p^{t_j}$, $t_j < s$, ir, kaip matome, dalijasi iš p^{s+1}. Grupės G skaidinį dvigubomis gretutinėmis klasėmis suskirstykime į dvi sumas: į vieną sudėkime dvigubas gretutines klases, kurių atstovai priklauso Sylovo p-pogrupio normalizatoriui $N_G(P)$, o į kitą – dvigubas gretutines klases, kurių atstovai nepriklauso Sylovo p-pogrupio normalizatoriui $N_G(P)$:

$$G = \bigcup_{x_j \in N_G(P)} Px_jP \;\cup \bigcup_{x_j \notin N_G(P)} Px_jP.$$

Kadangi $P \subset N_G(P)$, tai pirmoji sąjunga

$$\bigcup_{x_j \in N_G(P)} Px_jP$$

yra $N_G(P)$ skaidinys pogrupio P dešiniosiomis gretutinėmis klasėmis (grupėje $N_G(P)$ kairiosios ir dešiniosios pogrupio P klasės sutampa, nes P yra normalusis pogrupis grupėje $N_G(P)$). Vadinasi, galime parašyti lygybę:

$$|G| = |N_G(P)| + \sum_{\substack{j \\ x_j \notin N_G(P)}} p^{2s-t_j} = |N_G(P)| + p^{s+1}q.$$

Šią lygybę padaliję iš $|N_G(P)|$, gauname

$$l = 1 + \frac{p^{s+1}q}{|N_G(P)|}. \tag{5.8}$$

Kadangi $p^s = |P|$ dalija $|N_G(P)|$, o $|N_G(P)|$ dalija $|G| = p^s a$, $p \nmid a$, tai skaičius $|N_G(P)|$ dalijasi tik iš p^s ir nesidalija iš pirminio skaičiaus p didesnio laipsnio. Taigi sveikasis skaičius

$$\frac{p^{s+1}q}{|N_G(P)|}$$

dalijasi iš p, todėl iš (5.8) gauname $l \equiv 1 \pmod p$. □

5.13.13 pavyzdys. Įrodysime, kad grupė G, kurios eilė lygi 15, yra ciklinė.

Kadangi $15 = 3 \cdot 5$, tai, remiantis pirmąja Sylovo teorema, egzistuoja grupės G Sylovo 3-pogrupis H_1 ir 5-pogrupis H_2. Sylovo 3-pogrupių yra $1 + 3m$ ir, be to, $1 + 3m \mid 15$ (trečioji Sylovo teorema). Tai galima tik tuo atveju, kai $m = 0$. Kitaip tariant, egzistuoja tik vienas Sylovo 3-pogrupis H_1. Kadangi kiekvienam $x \in G$, xH_1x^{-1} yra 3-pogrupis, tai kiekvienam $x \in G$, $xH_1x^{-1} = H_1$. Taigi H_1 yra grupės G normalusis pogrupis. Panašiai įrodoma, kad H_2 taip pat yra grupės G normalusis pogrupis.

Įrodysime, kad pogrupių H_1 ir H_2 elementai komutuoja, t. y. bet kuriems $h_1 \in H_1$, $h_2 \in H_2$, teisinga lygybė $h_1h_2 = h_2h_1$. Iš tikrųjų, kadangi H_1 yra grupės G normalusis pogrupis, tai $h_2h_1^{-1}h_2^{-1} \in H_1$, todėl ir $h_1h_2h_1^{-1}h_2^{-1} \in H_1$. Analogiškai, kadangi H_2 yra grupės G normalusis pogrupis, tai $h_1h_2h_1^{-1} \in H_2$, todėl ir $h_1h_2h_1^{-1}h_2^{-1} \in H_2$. Taigi elementas $h_1h_2h_1^{-1}h_2^{-1}$ priklauso sankirtai $H_1 \cap H_2 = \{1\}$, t. y. $h_1h_2 = h_2h_1$.

Vadinasi, grupė G yra ciklinių pogrupių H_1 ir H_2 tiesioginė sandauga. Kadangi ciklinių pogrupių H_1 ir H_2 eilės yra 3 ir 5, t. y. tarpusavyje pirminiai skaičiai, tai G taip pat yra ciklinė grupė.

Panašiai įrodysime bendresnį teiginį:

5.13.14 teiginys. *Tarkime, kad grupės G eilė yra pq, kur p ir q yra tokie pirminiai skaičiai, kad $p < q$ ir $q \not\equiv 1 \pmod p$. Tuomet grupė G yra ciklinė.*

Įrodymas. Remiantis pirmąja Sylovo teorema, egzistuoja grupės G Sylovo p-pogrupis H_p ir q-pogrupis H_q. Pagal trečiąją Sylovo teoremos, grupės G Sylovo p-pogrupių skaičius n_p dalija tos grupės eilę pq ir $n_p \equiv 1 \pmod p$. Kadangi $q \not\equiv 1 \pmod p$, tai $n_p = 1$, t. y. grupėje G yra vienintelis p eilės pogrupis.

Kiekvienam grupės G elementui g, pogrupis gH_pg^{-1} taip pat yra grupės G Sylovo p-pogrupis. Kadangi $n_p = 1$, tai $gH_pg^{-1} = H_p$, t. y. pogrupis H_p yra normalusis grupės G pogrupis.

Analogiškai įrodoma, kad H_q yra grupės G normalusis pogrupis.

Sankirta $H_p \cap H_q$ yra grupės H_p pogrupis, todėl, remiantis Lagranžo teorema, pogrupio $H_p \cap H_q$ eilė dalija grupės H_p eilę p. Analogiškai įrodoma, kad pogrupio $H_p \cap H_q$ eilė dalija grupės H_q eilę q. Kadangi p ir q yra skirtingi pirminiai skaičiai, tai $|H_p \cap H_q| = 1$, t. y. $H_p \cap H_q = \{1\}$.

Įrodysime, kad pogrupių H_p ir H_q elementai komutuoja, t. y. bet kuriems $g \in H_p$, $h \in H_q$, teisinga lygybė $gh = hg$. Iš tikrųjų, kadangi H_p yra grupės G normalusis pogrupis, tai $hg^{-1}h^{-1} \in H_p$, todėl ir $ghg^{-1}h^{-1} \in H_p$. Analogiškai, kadangi H_q yra grupės G normalusis pogrupis, tai $ghg^{-1} \in H_q$, todėl ir $ghg^{-1}h^{-1} \in H_q$. Taigi elementas $ghg^{-1}h^{-1}$ priklauso sankirtai $H_p \cap H_q = \{1\}$, t. y. $gh = hg$.

Vadinasi, grupė G yra ciklinių pogrupių H_p ir H_q tiesioginė sandauga. Kadangi ciklinių pogrupių H_p ir H_q eilės yra p ir q, t. y. tarpusavyje pirminiai skaičiai, tai G taip pat yra ciklinė grupė. □

5.13.15 pavyzdys. Remiantis 5.13.14 teiginiu, grupės, kurių eilės yra 33, 35, 51, 65, 69, 77, 85, 87, 91 arba 95, yra ciklinės.

6 skyrius

Žiedai ir žiedų homomorfizmai

6.1 Žiedai

6.1.1. Tarkime, kad netuščioje aibėje A apibrėžti jos elementų kompozicijos dėsniai $+$ ir $*$, vadinami aibės A elementų sudėtimi ir daugyba.

6.1.2 apibrėžimas. Aibę A, joje apibrėžtų jos elementų sudėties $+$ ir daugybos $*$ atžvilgiu, vadinsime *žiedu*, jei

1. Sudėtis $+$ yra asociatyvi: bet kuriems $x, y, z \in A$,
$$(x + y) + z = x + (y + z).$$
2. Egzistuoja neutralus elementas 0 sudėties $+$ atžvilgiu: kiekvienam $x \in A$,
$$x + 0 = 0 + x = x.$$
3. Kiekvienam aibės A elementui x egzistuoja simetrinis elementas y sudėties $+$ atžvilgiu:
$$x + y = y + x = 0.$$
Elementui x sudėties $+$ atžvilgiu simetrinį elementą žymėsime $-x$ ir vadinsime priešingu elementu elementui x.
4. Sudėtis $+$ yra komutatyvi: bet kuriems $x, y \in A$,
$$x + y = y + x.$$
5. Daugyba $*$ yra asociatyvi: bet kuriems $x, y, z \in A$,
$$(x * y) * z = x * (y * z).$$

6. Sudėtis $+$ ir daugyba $*$ yra susijusios distributyvumo dėsniais: bet kuriems $x, y, z \in A$,
$$(x+y)*z = x*z + y*z,$$
$$z*(x+y) = z*x + z*y.$$

6.1.3. Žiedo $(A, +, *)$ elementas 0 yra vadinamas nuliu. Remdamiesi 1-4 aksiomomis, matome, kad $(A, +)$ – Abelio grupė. Taigi nereikalaujama, kad žiedo $(A, +, *)$ daugyba $*$ būtų komutatyvi.

6.1.4 apibrėžimas. Jei žiedo $(A, +, *)$ daugyba $*$ yra komutatyvi (t. y. bet kuriems $x, y \in A$, $x*y = y*x$), tai $(A, +, *)$ yra vadinamas *komutatyviuoju žiedu.*

Kaip matome, nereikalaujama, kad žiede $(A, +, *)$ egzistuotų neutralus elementas daugybos $*$ atžvilgiu.

6.1.5 apibrėžimas. Jei žiede $(A, +, *)$ egzistuoja neutralus elementas daugybos $*$ atžvilgiu, tai jį žymėsime 1 ir vadinsime *žiedo vienetu*, o $(A, +, *)$ – *žiedu su vienetu.*

6.1.6. Mes nagrinėsime tiktai žiedus $(A, +, *)$ su vienetu. Jei žiedas neturi vieneto, tai yra žinoma, kaip galima prijungti vienetą ir gauti žiedą su vienetu.

Labai svarbi yra speciali klasė žiedų, kurių kiekvienam nenuliniam elementui egzistuoja nenulinis simetrinis elementas daugybos atžvilgiu.

6.1.7 apibrėžimas. Nekomutatyvus žiedas $(A, +, *)$ su vienetu 1 yra vadinamas *žiedu su dalyba* arba *nekomutatyviuoju kūnu*, jei kiekvienam $x \in A$, $x \neq 0$, egzistuoja toks $y \in A$, $y \neq 0$, kad $x*y = y*x = 1$. Komutatyvus žiedas $(A, +, *)$ su dalyba yra vadinamas *kūnu.*

Elementui $x \in A, x \neq 0$, simetrinis elementas daugybos atžvilgiu $*$, jei jis tik egzistuoja, yra žymimas x^{-1} ir yra vadinamas *atvirkštiniu elementu* elementui x.

6.1.8. Dabar apibrėšime požiedžio, idempotenčiojo, nilpotenčiojo elementų ir nulio daliklių sąvokas. Vėliau šias sąvokas pailiustruosime pavyzdžiais.

6.1.9 apibrėžimas. Netuščias žiedo $(A, +, *)$ poaibis B, stabilus sudėties $+$ ir daugybos $*$ atžvilgiu, yra vadinamas žiedo $(A, +, *)$ *požiedžiu*, jei $(B, +, *)$ yra žiedas.

6.1.10 apibrėžimas. Žiedo $(A, +, *)$ nenulinis elementas a yra vadinamas *idempotentu* arba *idempotenčiuoju* elementu, jei $a*a = a^2 = a$.

6.1.11 apibrėžimas. Žiedo $(A, +, *)$ nenulinis elementas a yra vadinamas *kairiuoju žiedo nulio dalikliu*, jei egzistuoja toks nenulinis elementas b, kad $a*b = 0$. Panašiai apibrėžiamas dešinysis žiedo nulio daliklis. Komutatyvaus žiedo atveju šios sąvokos sutampa ir toks elementas yra vadinamas žiedo *nulio dalikliu.*

6.1.12 apibrėžimas. Žiedo $(A, +, *)$ nenulinis elementas a yra vadinamas *nilpotentu* arba nilpotenčiuoju elementu, jei egzistuoja toks sveikasis skaičius $n > 0$, kad $a^n = 0$.

6.1.13 apibrėžimas. Komutatyvus žiedas su vienetu be nulio daliklių yra vadinamas *sveikumo* arba *integralumo sritimi.*

6.1.14 pastaba. Kūno požiedis bendruoju atveju nėra kūnas.

6.1.15 pastaba. Žiedo nilpotentas yra tiek kairysis, tiek dešinysis žiedo nulio daliklis.

6.1.16 pavyzdys. Sveikųjų skaičių aibė $\mathbb{Z}$ skaičių sudėties $+$ ir daugybos $\cdot$ atžvilgiu yra komutatyvus žiedas su vienetu. Jį žymėsime $(\mathbb{Z}, +, \cdot)$.

6.1.17 pavyzdys. Racionaliųjų skaičių aibė $\mathbb{Q}$ skaičių sudėties $+$ ir daugybos $\cdot$ atžvilgiu yra kūnas $(\mathbb{Q}, +, \cdot)$.

6.1.18 pavyzdys. Realiųjų skaičių aibė $\mathbb{R}$ skaičių sudėties $+$ ir daugybos $\cdot$ atžvilgiu yra kūnas $(\mathbb{R}, +, \cdot)$.

6.1.19 pavyzdys. Tarkime, kad $A = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, čia $\bar{j} = j (\operatorname{mod} 4)$. Likinių moduliu 4 aibė (žr. 2.4.2 pavyzdį) A sudėties ir daugybos atžvilgiu yra žiedas. Akivaizdu, kad $\bar{2}^2 = \bar{0}$. Taigi $\bar{2}$ yra nilpotentinis nagrinėjamo žiedo elementas.

6.1.20 pavyzdys. Apibrėžkime aibę

$$\mathbb{H}(\mathbb{R}) = \{\alpha + \beta \cdot i + \gamma \cdot j + \delta \cdot k \mid \alpha, \beta, \gamma, \delta \in \mathbb{R}\},$$

kurios elementai yra formalūs simboliai $\alpha + \beta \cdot i + \gamma \cdot j + \delta \cdot k$. Elementai

$$\alpha + \beta \cdot i + \gamma \cdot j + \delta \cdot k \ \text{ ir } \ \alpha' + \beta' \cdot i + \gamma' \cdot j + \delta' \cdot k$$

yra lygūs pagal apibrėžimą tada ir tik tada, kai $\alpha = \alpha'$, $\beta = \beta'$, $\gamma = \gamma'$, $\delta = \delta'$. Be to, koeficientai prie simbolių i, j, k, gali būti parašyti ir dešinėje pusėje, t. y.

$$\alpha + \beta \cdot i + \gamma \cdot j + \delta \cdot k = \alpha + i \cdot \beta + j \cdot \gamma + k \cdot \delta.$$

Apibrėšime aibės $\mathbb{H}(\mathbb{R})$ elementų sudėtį ir daugybą.

Sudėtis $+$ aibėje $\mathbb{H}(\mathbb{R})$.

Pagal apibrėžimą

$$(\alpha+\beta\cdot i+\gamma\cdot j+\delta\cdot k)+(\alpha'+\beta'\cdot i+\gamma'\cdot j+\delta'\cdot k) := \alpha+\alpha'+(\beta+\beta')\cdot i+(\gamma+\gamma')\cdot j+(\delta+\delta')\cdot k.$$

Akivaizdu, kad $(\mathbb{H}(\mathbb{R}), +)$ – Abelio grupė.

Daugyba $\cdot$ aibėje $\mathbb{H}(\mathbb{R})$.

Norint apibrėžti aibės $\mathbb{H}(\mathbb{R})$ elementų daugybą, pakanka apibrėžti elementų i, j ir k daugybos lentelę ir remtis žiedo apibrėžimo 6-ąja aksioma. Elementų i, j, k daugybos lentelę apibrėžkime taip:

$$i \cdot i = j \cdot j = k \cdot k = -1, \quad i \cdot j = -j \cdot i = k,$$

$$j \cdot k = -k \cdot j = i, \quad k \cdot i = -i \cdot k = j.$$

Dabar, remdamiesi elementų i, j ir k daugybos lentele ir žiedo apibrėžimo 6-ąja aksioma, galime užrašyti aibės $\mathbb{H}(\mathbb{R})$ dviejų elementų sandaugos išraišką:

$$(\alpha + \beta \cdot i + \gamma \cdot j + \delta \cdot k) \cdot (\alpha' + \beta' \cdot i + \gamma' \cdot j + \delta' \cdot k)$$

$$= \alpha\alpha' - \beta\beta' - \gamma\gamma' - \delta\delta' + (\alpha\beta' + \beta\alpha' + \gamma\delta' - \delta\gamma') \cdot i$$

$$+(\alpha\gamma' + \gamma\alpha' + \delta\beta' - \beta\delta') \cdot j + (\alpha\delta' + \delta\alpha' + \beta\gamma' - \gamma\beta') \cdot k.$$

Iš čia gauname

$$(\alpha + \beta \cdot i + \gamma \cdot j + \delta \cdot k) \cdot (\alpha - \beta \cdot i - \gamma \cdot j - \delta \cdot k) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2.$$

Remdamiesi pastarąja lygybe matome, kad kiekvienam nenuliniam elementui $\alpha + \beta \cdot i + \gamma \cdot j + \delta \cdot k$ (t. y., kai bent vienas koeficientų α, β, γ, δ yra nelygus nuliui) egzistuoja atvirkštinis elementas

$$(\alpha + \beta \cdot i + \gamma \cdot j + \delta \cdot k)^{-1} = (\alpha^2 + \beta^2 + \gamma^2 + \delta^2)^{-1} \cdot (\alpha - \beta \cdot i - \gamma \cdot j - \delta \cdot k).$$

Kaip matome, $(\mathbb{H}(\mathbb{R}), +, \cdot)$ yra nekomutatyvus žiedas su dalyba arba nekomutatyvus kūnas. Šis nekomutatyvus kūnas dar yra vadinamas *kvaternionų kūnu.* Pirmas kvaternionų kūną pradėjo tirti anglų matematikas Hamiltonas. Kvaternionų kūnas dažniausiai yra žymimas $\mathbb{H}(\mathbb{R})$ pabrėžiant, kad kvaternionai yra gaunami simbolius $1, i, j, k$ dauginant iš realiųjų skaičių ir paskui sudedant. Galima nagrinėti kvaternionus $\alpha + \beta \cdot i + \gamma \cdot j + \delta \cdot k$, kurių koeficientai $\alpha, \beta, \gamma, \delta$ yra racionalūs skaičiai. Taigi galime apibrėžti

$$\mathbb{H}(\mathbb{Q}) = \{\alpha + \beta \cdot i + \gamma \cdot j + \delta \cdot k \mid \alpha, \beta, \gamma, \delta \in \mathbb{Q}\}.$$

Nesunku įsitikinti, kad $(\mathbb{H}(\mathbb{Q}), +, \cdot)$ taip pat yra nekomutatyvus kūnas. Jis yra vadinamas *racionaliųjų kvaternionų kūnu.*

6.1.21 pavyzdys. Šiame pavyzdyje nagrinėsime racionaliųjų kvaternionų kūno $(\mathbb{H}(\mathbb{Q}), +, \cdot)$ požiedį $(\mathbb{Q}(i), +, \cdot)$, čia

$$\mathbb{Q}(i) := \{\alpha + \beta \cdot i \mid \alpha, \beta \in \mathbb{Q}\}.$$

Galite įsitikinti, kad racionaliųjų kvaternionų kūno $(\mathbb{H}(\mathbb{Q}), +, \cdot)$ poaibis $\mathbb{Q}(i)$ yra stabilus sudėties $+$ ir daugybos $\cdot$ atžvilgiu, taigi yra nekomutatyvaus kūno $(\mathbb{H}(\mathbb{Q}), +, \cdot)$ požiedis. Įrodysime, kad $(\mathbb{Q}(i), +, \cdot)$ yra kūnas. Pirmiausia pastebėsime, kad aibės $\mathbb{Q}(i)$ elementų daugyba $\cdot$ yra komutatyvi, nes

$$(\alpha+\beta\cdot i)\cdot(\alpha'+\beta'\cdot i) = \alpha\cdot\alpha' - \beta\cdot\beta' + (\alpha\cdot\beta' + \beta\cdot\alpha')\cdot i = (\alpha'+\beta'\cdot i)\cdot(\alpha+\beta\cdot i).$$

Kiekvienam nenuliniam žiedo $(\mathbb{Q}(i), +, \cdot)$ elementui $\alpha+\beta\cdot i$, t. y. kai bent vienas koeficientų α, β nelygus 0, egzistuoja atvirkštinis elementas

$$(\alpha^2+\beta^2)^{-1}\cdot(\alpha-\beta\cdot i).$$

Kaip matome, $(\mathbb{Q}(i), +, \cdot)$ yra kūnas. Šis kūnas yra vadinamas *Gauso skaičių kūnu*.

6.1.22 pavyzdys. Panašiai kaip ir 6.1.21 pavyzdyje, nagrinėkime realiųjų kvaternionų kūno $(\mathbb{H}(\mathbb{R}), +, \cdot)$ požiedį $(\mathbb{C}, +, \cdot)$, čia $\mathbb{C} := \{\alpha+\beta\cdot i \mid \alpha, \beta \in \mathbb{R}\}$. Kaip ir 6.1.21 pavyzdyje galima įsitikinti, kad $(\mathbb{C}, +, \cdot)$ yra kūnas. Šis kūnas yra vadinamas *kompleksinių skaičių kūnu*. Kompleksinių skaičių kūnas labai svarbus matematikoje. Vėliau šį kūną tirsime išsamiau (žr. 6.7 skyrelį).

6.1.23. Dabar įrodysime teoremą apie baigtines sveikumo (integralumo) sritis, o paskui aptarsime labai svarbų žiedo pavyzdį.

Priminsime, kad komutatyvaus žiedo $(A, +, *)$ nenulinis elementas a yra vadinamas nulio dalikliu, jei egzistuoja toks nenulinis elementas $b \in A$, kad $a * b = 0$. Komutatyvus žiedas $(A, +, *)$ yra vadinamas sveikumo (integralumo) sritimi, jei žiedas A neturi nulio daliklių.

6.1.24 teorema. *Baigtinis komutatyvus žiedas* $(A, +, *)$ *be nulio daliklių yra kūnas.*

Įrodymas. Kadangi $(A, +, *)$ yra žiedas, tai, norint įrodyti teoremą, reikia įrodyti, kad žiede $(A, +, *)$ yra vienetas ir kiekvienam nenuliniam žiedo $(A, +, *)$ elementui egzistuoja atvirkštinis elementas daugybos atžvilgiu. Pabrėžiame, jog formuluodami teoremą nereikalavome, kad žiedo vienetas egzistuotų.

Tarkime, kad $A = \{a_1, a_2, \ldots, a_n\}$, o $a_1 = 0$. Pirmiausia įrodysime, kad, žiedo A nenulinius elementus $a_2, \ldots, a_n$, padauginę iš kurio nors fiksuoto nenulinio elemento $a_s, 2 \le s \le n$, gauname visus nenulinius žiedo A elementus $a_2, \ldots, a_n$, tik galbūt, surašytus kita tvarka nei $a_2, \ldots, a_n$. Iš tikrųjų, visi elementai $a_2, a_3, \ldots, a_n$ yra tarpusavyje skirtingi ir tarp jų nėra žiedo nulio. Jei būtų

$$a_i * a_s = a_j * a_s, \quad i \ne j, \quad 2 \le s \le n,$$

tai gautume

$$a_i * a_s - a_j * a_s = (a_i - a_j)a_s = 0,$$

o tai žiede be nulio daliklių įmanoma tik tuo atveju, kai $a_i - a_j = 0$. Bet, jei $i \neq j$, tai ir $a_i \neq a_j$. Vadinasi, sudauginę elementus

$$a_2, \ldots, a_n, \quad \text{ar} \quad a_2 * a_s, \ldots, a_n * a_s, \quad 2 \leq s \leq n,$$

gauname tą patį elementą. Taigi

$$a_2 * a_3 * \cdots * a_n = a_s^{n-1} * a_2 * a_3 * \cdots * a_n,\ 2 \leq s \leq n,$$

čia a_s^{n-1} reikia suprasti kaip a_s, sudaugintą su savimi $n-1$ kartą. Šią lygybę galime perrašyti ir taip:

$$a_2 * a_3 * \cdots * \hat{a}_r * \cdots * a_n(a_r - a_s^{n-1} * a_r) = 0,$$

čia stogelis virš elemento žymi, kad šio elemento sandaugoje nėra. Kadangi

$$a_2 * a_3 * \cdots * \hat{a}_r * \cdots * a_n \neq 0,$$

o žiedas A be nulio daliklių, tai bet kuriems r, s, $2 \leq r, s \leq n$, $a_r = a_s^{n-1} * a_r$. Vadinasi, a_s^{n-1}, $2 \leq s \leq n$, yra žiedo A vienetas, t. y. kiekvienam s, $2 \leq s \leq n$, $a_s^{n-1} = 1$. Taigi įrodėme lygybes:

$$a_s^{n-1} = a_r^{n-1}, \ \ 2 \leq r, s \leq n.$$

Pastarąsias lygybes galima įrodyti ir taip: iš anksčiau įrodytų lygybių

$$a_2 * a_3 * \cdots * a_n = a_s^{n-1} * a_2 * a_3 * \cdots * a_n, \ \ 2 \leq s \leq n,$$

gauname: jei

$$a_s^{n-1} * a_2 * a_3 * \cdots * a_n = a_r^{n-1} * a_2 * a_3 * \cdots * a_n, \ \ 2 \leq r, s \leq n,$$

tai

$$(a_s^{n-1} - a_r^{n-1}) * a_2 * a_3 * \cdots * a_n = 0$$

arba $a_s^{n-1} = a_r^{n-1}$, $2 \leq r, s \leq n$.

Lieka įrodyti, kad kiekvienam nenuliniam žiedo A elementui a_s, $2 \leq s \leq n$, egzistuoja atvirkštinis elementas. Remdamiesi lygybe $a_s^{n-1} = 1$, $2 \leq s \leq n$, gauname, kad

$$a_s^{-1} = a_s^{n-2}, \ \ 2 \leq s \leq n.$$

□

6.1.25 pastaba. Remdamiesi teoremos įrodymu, matome, kad kiekvienas baigtinio kūno, turinčio n elementų, nenulinis elementas, pakeltas $n-1$-uoju laipsniu, yra lygus šio kūno vienetui, kitaip tariant, kiekvienas šio kūno nenulinis elementas yra lygties $x^{n-1} = 1$ šaknis. Šis faktas gali būti įrodytas remiantis grupių teorija. Baigtinio kūno nenuliniai elementai sudaro Abelio grupę. Šios grupės eilė yra lygi $n - 1$. Kiekvienas Abelio grupės elementas, pakeltas laipsniu, lygiu grupės eilei, yra lygus grupės vienetui. Vėliau įrodysime, kad baigtinis kūnas gali turėti tik p^m, čia p – kuris nors pirminis skaičius, m – kuris nors natūralusis skaičius, elementų.

6.1.26 pavyzdys. Tarkime, kad $(A, +, *)$ – sveikumo sritis su vienetu 1, t. y. komutatyvusis žiedas be nulio daliklių su vienetu. Apibrėšime mažiausią kūną, kuriam priklauso (yra jo poaibis) žiedas A. Nagrinėkime aibę

$$A \times A := \{(a, b) \,|\, a \in A,\, b \in A \setminus \{0\}\}.$$

Joje apibrėžkime sąryšį R taip:

$$(a_1, b_1) \underset{R}{\sim} (a_2, b_2) \Longleftrightarrow a_1 b_2 = a_2 b_1.$$

Pavyzdžiui, bet kuriems $a, b, t \in A$, $b \neq 0$, $t \neq 0$, $(a, b) \underset{R}{\sim} (at, bt)$. Nesunku įsitikinti, kad R yra ekvivalentumo sąryšis (žr. 1.4.1 apibrėžimą) aibėje $A \times A$. Faktoraibę $(A \times A)/R$ pažymėkime K (žr. 1.4 skyrelį), o ekvivalentumo klasę, kuriai priklauso aibės $A \times A$ elementas (a, b), pažymėkime

$$\frac{a}{b} \quad \text{arba tiesiog} \quad a/b.$$

Dabar apibrėšime aibės K elementų sudėtį ir daugybą. Tegu $a_1/b_1, a_2/b_2 \in K$. Tuomet

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} := \frac{a_1 b_2 + a_2 b_1}{b_1 b_2},$$
$$\frac{a_1}{b_1} \cdot \frac{a_2}{b_2} := \frac{a_1 a_2}{b_1 b_2}.$$

Paliekame skaitytojui įsitikinti, kad aibės K elementų sudėtis ir daugyba suderintos su ekvivalentumo sąryšiu R (žr. 2.4.1 apibrėžimą), t. y. operacijos rezultatas nepriklauso nuo ekvivalentumo klasių atstovų parinkimo (t. y., jei $a_1/b_1 = a_1'/b_1'$ ir $a_2/b_2 = a_2'/b_2'$, tai $a_1/b_1 + a_2/b_2 = a_1'/b_1' + a_2'/b_2'$ ir $a_1/b_1 \cdot a_2/b_2 = a_1'/b_1' \cdot a_2'/b_2'$).

Nesunku įsitikinti, kad aibė K joje apibrėžtos sudėties ir daugybos atžvilgiu yra kūnas. Šio kūno nulis yra $0/1$, o vienetas – $1/1$. Kiekvieną žiedo A elementą a sutapatinę su elementu $a/1 \in K$, gauname, kad žiedas A yra kūno K požiedis. (Sutapatinama naudojantis injekciniu homomorfizmu $f : A \to K$, $f(a) = a/1 \in K$, $a \in A$ (žr. 6.5 skyrelį).)

6.1.27 pastaba. 6.1.26 pavyzdyje sukonstruotas kūnas K vadinamas žiedo A (sveikumo sritis su vienetu) *santykių kūnu*.

6.2 Matricų algebra

6.2.1. Nagrinėsime svarbų žiedą, kuris yra vadinamas *matricų algebra.* Algebra yra vadinama tiesinė erdvė, kurioje apibrėžta žiedo struktūra, suderinta su tiesinės erdvės struktūra.

6.2.2 apibrėžimas. Abelio grupė $(V, +)$ yra vadinama *tiesine erdve* virš kūno $(k, +, *)$, jei apibrėžtas atvaizdis (išorinis kompozicijos dėsnis)

$$\circ : k \times V \to V,$$

tenkinantis sąlygas: bet kuriems $\alpha, \beta \in k$, $u, v \in V$,

1. $(\alpha * \beta) \circ u = \alpha \circ (\beta \circ u)$.
2. $1 \circ u = u$, 1– kūno k vienetinis elementas.
3. $(\alpha + \beta) \circ u = \alpha \circ u + \beta \circ u$.
4. $\alpha \circ (u + v) = \alpha \circ u + \alpha \circ v$.

6.2.3 apibrėžimas. Tiesinė erdvė $(V, +)$ virš kūno $(k, +, *)$ yra vadinama *algebra*, jei tiesinėje erdvėje apibrėžtas kompozicijos dėsnis $\cdot$, tenkinantis sąlygas: bet kuriems α, β, $\gamma \in k$, $u, v, w \in V$,

$$(\alpha \circ u + \beta \circ v) \cdot (\gamma \circ w) = (\alpha * \gamma) \circ (u \cdot w) + (\beta * \gamma) \circ (v \cdot w),$$

$$(\gamma \circ w) \cdot (\alpha \circ u + \beta \circ v) = (\gamma * \alpha) \circ (w \cdot u) + (\gamma * \beta) \circ (w \cdot v).$$

Jei kompozicijos dėsnis $\cdot$ aibėje V asociatyvus, tai algebra $(V, +, \cdot)$ yra vadinama *asociatyviąja.* Vėliau nagrinėsime ir neasociatyviųjų algebrų pavyzdžius.

6.2.4 pastaba. Norėdami pabrėžti algebros apibrėžime dalyvaujančių kompozicijos dėsnių įvairovę, juos žymėjome įvairiais simboliais. Tik ženklą „+“naudojome tiek sudėčiai aibėje k, tiek aibėje V žymėti. Tokios žymėjimų įvairovės ateityje atsisakysime. Daugybai žymėti naudosime $*$ arba $\cdot$ arba tarp komponuojamų elementų nerašysime jokių ženklų.

6.2.5 apibrėžimas. Kūno k elementų šeima $(\alpha_{ij}), 1 \le i \le m, 1 \le j \le n$, sunumeruota dviem indeksais ir surašyta į lentelę

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{m1} & \alpha_{m2} & \dots & \alpha_{mn} \end{pmatrix}$$

yra vadinama $m \times n$ *matrica*, o α_{ij} – šios matricos ij-elementu arba ij-komponente (α_{ij} – matricos elementas, užrašytas matricos i-osios eilutės ir j-tojo stulpelio sankirtoje).

Sutarkime $m \times n$ matricą žymėti (α_{ij}). Norėdami pabrėžti, kad matrica A turi m eilučių ir n stulpelių, rašysime $A = (\alpha_{ij})_{ij=1}^{m,n}$. $m \times n$ matricos (α_{ij}) ir (β_{ij}) yra lygios tada ir tik tada, kai bet kuriems i, j, $1 \leq i \leq m$, $1 \leq j \leq n$,

$$\alpha_{ij} = \beta_{ij}.$$

Visų $m \times n$ matricų, kurių elementai priklauso kūnui k, aibę žymėsime $M_{m \times n}(k)$. Jei $m = n$, tai $n \times n$ matricos dar vadinamos *n-tos eilės kvadratinėmis matricomis.* Visų $n \times n$ matricų su koeficientais kūne k aibę žymėsime $M_n(k)$.

6.2.1 Matricų sudėtis

$m \times n$ matricų (α_{ij}) ir (β_{ij}) suma vadinama $m \times n$ matrica $(\alpha_{ij} + \beta_{ij})$ ir žymima $(\alpha_{ij}) + (\beta_{ij})$. Taigi sudedant matricas sudedami atitinkami jų elementai, t. y.

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ & \cdots & \cdots & \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{pmatrix} + \begin{pmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1n} \\ \beta_{21} & \beta_{22} & \cdots & \beta_{2n} \\ & \cdots & \cdots & \\ \beta_{m1} & \beta_{m2} & \cdots & \beta_{mn} \end{pmatrix}$$

$$= \begin{pmatrix} \alpha_{11} + \beta_{11} & \alpha_{12} + \beta_{12} & \cdots & \alpha_{1n} + \beta_{1n} \\ \alpha_{21} + \beta_{21} & \alpha_{22} + \beta_{22} & \cdots & \alpha_{2n} + \beta_{2n} \\ & \cdots & \cdots & \\ \alpha_{m1} + \beta_{m1} & \alpha_{m2} + \beta_{m2} & \cdots & \alpha_{mn} + \beta_{mn} \end{pmatrix}.$$

Nesunku įsitikinti, kad $(M_{m \times n}(k), +)$ – Abelio grupė. $m \times n$ matrica

$$\begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ & \cdots & \cdots & \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

vadinama nuline matrica ir žymima $\mathcal{O}$. Nulinė matrica yra šios grupės $(M_{m \times n}(k), +)$ neutralus elementas.

6.2.2 Matricų daugyba iš kūno k elementų

Apibrėžkime atvaizdį $k \times M_{m \times n}(k) \to M_{m \times n}(k)$ – skaičiaus $\lambda \in k$ ir $m \times n$ matricos (α_{ij}) sandaugą:

$$\lambda \cdot \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ & \cdots & \cdots & \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{pmatrix} = \begin{pmatrix} \lambda\alpha_{11} & \lambda\alpha_{12} & \cdots & \lambda\alpha_{1n} \\ \lambda\alpha_{21} & \lambda\alpha_{22} & \cdots & \lambda\alpha_{2n} \\ & \cdots & \cdots & \\ \lambda\alpha_{m1} & \lambda\alpha_{m2} & \cdots & \lambda\alpha_{mn} \end{pmatrix}.$$

6.2.6. Galima įsitikinti, kad apibrėžtas išorinis kompozicijos dėsnis tenkina tokias savybes:

1. Bet kuriems $\lambda, \mu \in k,\ A \in M_{m\times n}(k)$
$$(\lambda \cdot \mu) \cdot A = \lambda \cdot (\mu \cdot A).$$
2. Kiekvienai matricai $A \in M_{m\times n}(k))$
$$1 \cdot A = A,\ \ 1 \in k.$$
3. Bet kuriems $\lambda, \mu \in k,\ A \in M_{m\times n}(k)$
$$(\lambda + \mu) \cdot A = \lambda \cdot A + \mu \cdot A.$$
4. Bet kuriems $\lambda \in k,\ A, B \in M_{m\times n}(k)$
$$\lambda \cdot (A + B) = \lambda \cdot A + \lambda \cdot B.$$

Sutarkime, kad $(\alpha_{ij}) \cdot \lambda = (\alpha_{ij} \cdot \lambda)$. Tuomet akivaizdu, kad $\lambda \cdot A = A \cdot \lambda$, $\lambda \in k, A \in M_{m\times n}(k)$.

6.2.7 apibrėžimas. Apibrėžkime $m \times n$ matricą e_{ij}, kurios ij-elementas lygus $1 \in k$, o visi kiti yra lygūs $0 \in k$. Tuomet kiekvieną $m \times n$ matricą (α_{ij}) galima vienareikšmiškai užrašyti taip:
$$(\alpha_{ij}) = \sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} \cdot e_{ij}.$$

Šis užrašas patogus atliekant matricų sudėties ir daugybos veiksmus.

6.2.8 pastaba. Prisiminę anksčiau pateiktą tiesinės erdvės apibrėžimą, pažymėsime, kad visų $m \times n$ matricų grupė $(M_{m\times n}(k), +)$ yra tiesinė erdvė virš kūno k, o e_{ij}, $1 \le i \le m, 1 \le j \le n$, – šios tiesinės erdvės bazė (žiūrėkite tiesinės erdvės bazės apibrėžimą).

6.2.3 Matricų daugyba

Apibrėšime atvaizdį
$$M_{m\times n}(k) \times M_{n\times p}(k) \to M_{m\times p}(k),$$

kuris yra vadinamas *matricų daugyba.*

Tarkime, kad

$$A = (\alpha_{ij}) \in M_{m\times n}(k),\ B = (\beta_{ij}) \in M_{n\times p}(k).$$

Tuomet matricų

$$(\alpha_{ij}) \quad \text{ir} \quad (\beta_{ij})$$

sandauga yra vadinama $m \times p$ matrica

$$(\alpha_{ij}) \cdot (\beta_{ij}) := (\gamma_{ij}),$$

kurios ij-elementas γ_{ij} apibrėžiamas taip:

$$\gamma_{ij} = \sum_{s=1}^{n} \alpha_{is} \cdot \beta_{sj}, \quad 1 \le i \le m,\ 1 \le j \le p.$$

Pavyzdžiui,

$$\begin{pmatrix} 1 & 2 & 1 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 4 & 3 & 5 \\ 1 & 5 & 4 & 7 \\ 3 & 9 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 7 & 23 & 12 & 23 \\ 10 & 32 & 19 & 35 \end{pmatrix}.$$

Paprastai tariant, matricos (γ_{ij}) ij-elementas yra gaunamas pirmosios matricos i eilutę paelemenčiui sudauginant su antrosios matricos j stulpeliu ir gautus rezultatus sudedant.

6.2.9. Nesunku įsitikinti šiomis matricų daugybos savybėmis:

1. $(A \cdot B) \cdot C = A \cdot (B \cdot C),\ A \in M_{m\times n}(k),\ B \in M_{n\times p}(k),\ C \in M_{p\times r}(k).$

2. $(A + B) \cdot C = A \cdot C + B \cdot C,\ A, B \in M_{m\times n}(k),\ C \in M_{n\times p}(k).$

3. $C \cdot (A + B) = C \cdot A + C \cdot B,\ C \in M_{m\times n}(k),\ A, B \in M_{n\times p}(k).$

4. Kiekvienai matricai $A \in M_{m\times n}(k)$

   $$\mathbf{1}_m \cdot A = A,$$

   čia $\mathbf{1}_m := (\delta_{ij})_{i,j=1}^{m}$, vadinama m eilės vienetine matrica, o

   $$\delta_{ij} = \begin{cases} 1, & \text{jei } i = j, \\ 0, & \text{jei } i \ne j, \end{cases}$$

   yra vadinama *Kronekerio δ funkcija.*

5. Kiekvienai matricai $A \in M_{m\times n}(k)$

$$A \cdot \mathbf{1}_n = A.$$

6.2.10. Atidžiau panagrinėkime $M_n(k)$. Kaip žinome, $(M_n(k), +)$ – Abelio grupė. Matricų daugyba $\cdot$ apibrėžta aibėje $M_n(k)$.

$$\mathbf{1}_n := \sum_{j=1}^{n} e_{jj}$$

– neutralus aibės $M_n(k)$ elementas daugybos atžvilgiu. Taigi $(M_n(k), +, \cdot)$ – žiedas (netgi algebra virš kūno k, nes $M_n(k)$ – tiesinė erdvė virš kūno k, o matricų daugyba yra suderinta su tiesinės erdvės struktūra).

Algebros $(M_n(k), +, \cdot)$ elementų e_{ij}, $1 \le i, j \le n$, daugybos lentelė atrodo taip:

$$e_{ij} \cdot e_{pq} = \delta_{jp} e_{iq}, \;\; 1 \le i, j, p, q \le n,$$

čia δ_{jp} – Kronekerio simbolis (funkcija). Kaip matome, elementai e_{ij}, $1 \le i, j \le n$, yra matricų algebros $M_n(k)$ tiek kairieji, tiek dešinieji nulio dalikliai, o e_{ii}, $1 \le i \le n$, – šio algebros idempotentai.

Algebros $(M_n(k), +, \cdot)$ elementų daugyba vienareikšmiškai apibrėžiama žinant elementų e_{ij}, $1 \le i, j \le n$, daugybos lentelę:

$$\left(\sum_{i,j=1}^{n} \alpha_{ij} \cdot e_{ij} \right) \cdot \left(\sum_{r,s=1}^{n} \beta_{rs} \cdot e_{rs} \right) = \sum_{i,r,s=1}^{n} \alpha_{ir} \cdot \beta_{rs} \cdot e_{is}.$$

Algebros $(M_n(k), +, \cdot)$, $n > 1$, elementų daugyba nėra komutatyvi, nes, pavyzdžiui, $e_{11} \cdot e_{12} = e_{12}$, o $e_{12} \cdot e_{11} = 0$. Kaip matome, elementai e_{ij}, $1 \le i, j \le n$, yra matricų algebros $(M_n(k), +, \cdot)$ tiek kairieji, tiek dešinieji nulio dalikliai, o e_{ii}, $1 \le i \le n$, – šio algebros idempotentai.

Pratimai.

1. Tarkime, $u = \sum_{j=1}^{n-1} e_{jj+1} \in M_n(k)$. Įrodykite, kad $u^s = \sum_{j=1}^{n-s} e_{jj+s}$. Atskiru atveju $u^{n-1} = e_{1n}, u^n = 0$.

2. Apibrėžkime atvaizdį:

$$\mathrm{Tr} : M_n(k) \to k, \;\; \mathrm{Tr}(\sum_{i,j=1}^{n} \alpha_{ij} e_{ij}) = \sum_{j=1}^{n} \alpha_{jj}.$$

Skaičius $\mathrm{Tr}(A)$, $A \in M_n(k)$, vadinamas matricos A *pėdsaku*. Įrodykite, kad

i) $\mathrm{Tr}(A \cdot B) = \mathrm{Tr}(B \cdot A)$;

ii) $\mathrm{Tr}(\lambda \cdot A + \mu \cdot B) = \lambda \cdot \mathrm{Tr}(A) + \mu \cdot \mathrm{Tr}(B)$;

iii) $\mathrm{Tr}(\mathbf{1}_n) = n \cdot 1$, čia $\lambda, \mu, 1 \in k,\ A, B \in M_n(k)$.

3. Tarkime, kad atvaizdis $f : M_n(\mathbb{Q}) \to \mathbb{Q}$ tenkina sąlygas:

   i) $f(\mathbf{1})_n = n$;

   ii) $f(\lambda \cdot A + \mu \cdot B) = \lambda \cdot f(A) + \mu \cdot f(B),\ \lambda, \mu \in \mathbb{Q},\ A, B \in M_n(\mathbb{Q})$;

   iii) $f(A \cdot B) = f(B \cdot A)$.

   Įrodykite, kad $f = \mathrm{Tr}$.

   Patarimas. Pasinaudokite lygybėmis:

$$e_{ii} = e_{ij} \cdot e_{ji},\ e_{ij} = e_{ii} \cdot e_{ij} = e_{ij} \cdot e_{jj},\ 1 \leq i, j \leq n,$$

$$\mathbf{1}_n = \sum_{j=1}^{n} e_{jj},\ e_{ij} \cdot e_{pq} = 0, j \neq p.$$

4. Įrodykite, kad lygtis $X \cdot Y - Y \cdot X = \mathbf{1}_n$ algebroje $(M_n(k), +, \cdot)$ neišprendžiama.

5. Tarkime, kad $A = \mathbb{Q}[x]$,

$$\frac{d}{dx} : \mathbb{Q}[x] \to \mathbb{Q}[x],\ \frac{d}{dx} f(x) := f'(x),$$

   yra diferencijavimo atvaizdis,

$$m : \mathbb{Q}[x] \to \mathbb{Q}[x],\ m(f(x)) := x \cdot f(x),$$

   yra dauginimo iš kitamojo x operatorius. Įrodykite:

$$\frac{d}{dx} \circ m - m \circ \frac{d}{dx} = \mathrm{id},$$

   čia $\mathrm{id} : \mathbb{Q}[x] \to \mathbb{Q}[x], \mathrm{id}(f(x)) = f(x)$, – tapatusis atvaizdis.

6. Tarkime, kad žiedo $(A, +, *)$ elementai a ir b turi savybę: $b * a = q * a * b$, čia $q * a = a * q, q * b = b * q$. Įrodykite Niutono binomo formulės analogą:

$$(a + b)^n = \sum_{j=0}^{n} \begin{bmatrix} n \\ j \end{bmatrix}_q * a^{n-j} * b^j,$$

   čia

$$\begin{bmatrix} n \\ j \end{bmatrix}_q = \frac{[n]_q!}{[j]_q! * [n-j]_q!},\ [m]_q! := (q^m - 1) * (q^{m-1} - 1) * \cdots * (q - 1).$$

Įrodykite, kad

$$\lim_{q\to 1} \begin{bmatrix} n \\ j \end{bmatrix}_q = \binom{n}{j}.$$

7. Įrodykite, kad aibę

$$\mathbb{H}(\mathbb{C}) = \{\alpha + \beta \cdot i + \gamma \cdot j + \delta \cdot k \mid \alpha, \beta, \gamma, \delta \in \mathbb{C}\}$$

(sudėtis ir daugyba šioje aibėje apibrėžiamos taip pat kaip ir aibėje $\mathbb{H}(\mathbb{R})$) galima sutapatinti su matricų algebra $M_2(\mathbb{C})$, t. y. egzistuoja bijekcija $f : \mathbb{H}(\mathbb{C}) \to M_2(\mathbb{C})$, turinti savybes: bet kuriems $\alpha \in \mathbb{C}$, $a, b \in \mathbb{H}$,

i) $f(\alpha \cdot a) = \alpha \cdot f(a)$;

ii) $f(a + b) = f(a) + f(b)$;

iii) $f(a \cdot b) = f(a) \cdot f(b)$.

Kaip matome, algebra $\mathbb{H}(\mathbb{C})$ nėra kūnas.

6.3 Žiedo idealai

Tarkime, kad $(A, +, *)$ – žiedas su vienetu.

6.3.1 apibrėžimas. Netuščias žiedo $(A, +, *)$ poaibis $\mathfrak{a}$ yra vadinamas *kairiuoju (dešiniuoju) žiedo idealu*, jei:

1. $x, y \in \mathfrak{a} \Rightarrow x \pm y \in \mathfrak{a}$.
2. $a \in A, x \in \mathfrak{a} \Rightarrow a * x \in \mathfrak{a}$ ($a \in A, x \in \mathfrak{a} \Rightarrow x * a \in \mathfrak{a}$).

Antrąją žiedo idealo apibrėžimo sąlygą galima užrašyti ir taip:

$$A * \mathfrak{a} \subset \mathfrak{a} \quad (\mathfrak{a} * A \subset \mathfrak{a}),$$

čia $A * \mathfrak{a} = \{a * x \mid a \in A, x \in \mathfrak{a}\}$ $(\mathfrak{a} * A = \{x * a \mid x \in \mathfrak{a}, a \in A\})$.

6.3.2 apibrėžimas. Netuščias žiedo $(A, +, *)$ poaibis $\mathfrak{a}$ yra vadinamas *abipusiu žiedo idealu*, jei:

1. $x, y \in \mathfrak{a} \Rightarrow x \pm y \in \mathfrak{a}$;
2. $a \in A, x \in \mathfrak{a} \Rightarrow a * x, x * a \in \mathfrak{a}$.

Komutatyvaus žiedo atveju kairiojo, dešiniojo ir abipusio žiedo idealo sąvokos sutampa.

6.3.3 teiginys. *Tarkime,* $(A, +, *)$ *– žiedas,* $a \in A$*. Tuomet* $A*a = \{x*a \mid x \in A\}$ *yra kairysis žiedo* A *idealas,* $a * A = \{a * x \mid x \in A\}$ *– dešinysis žiedo idealas, o poaibis* $A * a * A = \{x * a * y \mid x, y \in A\}$ *– abipusis žiedo* A *idealas.*

Įrodymas. 1. Jei $x, y \in A*a$, tai egzistuoja tokie $u, v \in A$, kad $x = u*a, y = v * a$. Vadinasi, $x \pm y = u * a \pm v * a = (u \pm v) * a \in A * a$.

2. Jei $x \in A*a$, tai egzistuoja toks $u \in A$, kad $x = u*a$. Vadinasi, kiekvienam $b \in A, b * x = b * (u * a) = (b * u) * a \in A * a$.

Įrodėme, kad $A * a$ yra kairysis žiedo idealas. Panašiai įrodoma, kad $a * A$ – dešinysis, o $A * a * A$ – abipusis žiedo idealas. □

6.3.4 apibrėžimas. Idealas $A * a$ (arba $a * A$ ir $A * a * A$), generuotas vieno elemento a, yra vadinamas kairiuoju (arba dešiniuoju ir abipusiu) *pagrindiniu žiedo A idealu.*

Idealų sudėtis. Tarkime, kad $\mathfrak{a}$ ir $\mathfrak{b}$ – žiedo $(A, +, *)$ kairieji idealai. Apibrėšime idealų $\mathfrak{a}$ ir $\mathfrak{b}$ sumą

$$\mathfrak{a} + \mathfrak{b} = \{x + y \mid x \in \mathfrak{a}, y \in \mathfrak{b}\},$$

t. y. aibė $\mathfrak{a} + \mathfrak{b}$, sudaryta iš sumų $x+y$, čia $x \in \mathfrak{a}$, $y \in \mathfrak{b}$. Panašiai yra apibrėžiama dešiniųjų ir abipusių idealų suma.

6.3.5 teiginys. *Žiedo* $(A, +, *)$ *kairiųjų (dešiniųjų, abipusių) idealų* $\mathfrak{a}$ *ir* $\mathfrak{b}$ *suma* $\mathfrak{a} + \mathfrak{b}$ *yra kairysis (dešinysis, abipusis) žiedo* $(A, +, *)$ *idealas.*

Įrodymas. 1. Tarkime, kad $x, y \in \mathfrak{a} + \mathfrak{b}$. Vadinasi, egzistuoja tokie $u_1, u_2 \in \mathfrak{a}$ ir $v_1, v_2 \in \mathfrak{b}$, kad $x = u_1 + v_1$, $y = u_2 + v_2$. Taigi

$$x \pm y = (u_1 + v_1) \pm (u_2 + v_2) = (u_1 \pm u_2) + (v_1 \pm v_2) \in \mathfrak{a} + \mathfrak{b},$$

nes $u_1 \pm u_2 \in \mathfrak{a}$, $v_1 \pm v_2 \in \mathfrak{b}$.

2. Tarkime, kad $x \in \mathfrak{a} + \mathfrak{b}$, t. y. egzistuoja tokie $u \in \mathfrak{a}$, $v \in \mathfrak{b}$, kad $x = u + v$. Tuomet, jei $a \in A$, tai

$$a * x = a * (u + v) = a * u + a * v \in \mathfrak{a} + \mathfrak{b},$$

nes $a * u \in \mathfrak{a}, a * v \in \mathfrak{b}$.

Panašiai teiginys įrodomas dešiniesiems ir abipusiems idealams. □

6.3.6 apibrėžimas. Įdealas $A * a_1 + A * a_2 + \dots A * a_s$, čia a_1, a_2, …, $a_s \in A$, yra vadinamas kairiuoju žiedo $(A, +, *)$ *idealu, generuotu elementų* a_1, a_2, …, a_s. Panašiai apibrėžiami dešinieji ir abipusieji idealai, generuoti elementų a_1, a_2, …, a_s. Komutatyvaus žiedo atveju idealas $A * a_1 + A * a_2 + \cdots + A * a_s$ yra žymimas $(a_1, a_2, \dots, a_s)$, o elementai a_1, a_2, …, a_s vadinami *idealo sudaromosiomis.*

6.3.7 pastaba. Idealo žymėjimą $(a_1, a_2, \ldots, a_s)$ galima supainioti su Dekarto sandaugos A^s elementu. Bet tikėkimės, kad iš konteksto bus aišku, apie ką kalbama.

6.3.8 pavyzdys. Kūno $(k, +, *)$ idealai yra tik nulinis (0) ir k. Iš tikrųjų, jei $\mathfrak{a}$ – nenulinis kūno idealas, tai egzistuoja $\alpha \neq 0, \alpha \in \mathfrak{a}$. Tuomet $\alpha^{-1} \in k, \alpha \in \mathfrak{a} \Rightarrow \alpha^{-1} * \alpha = 1 \in \mathfrak{a} \Rightarrow k \subset \mathfrak{a}$. Vadinasi, $\mathfrak{a} = k$.

6.3.9 teiginys. *Sveikųjų skaičių žiedo* $(\mathbb{Z}, +, \cdot)$ *kiekvienas idealas yra pagrindinis.*

Įrodymas. Idealas (0) yra pagrindinis. Tarkime, $\mathfrak{a} \neq (0)$. Kadangi $\mathfrak{a}$ idealas, tai $x \in \mathfrak{a} \Rightarrow (-1) \cdot x = -x \in \mathfrak{a}$. Vadinasi, idealui $\mathfrak{a}$ priklauso mažiausias nenulinis natūralusis skaičius n. Įrodysime, kad $\mathfrak{a} = (n) = n\mathbb{Z}$. Akivaizdu, kad $(n) \subset \mathfrak{a}$. Reikia tik įrodyti, kad $\mathfrak{a} \subset (n)$. Jei $x \in \mathfrak{a}$, tai, remdamiesi dalybos su liekana formule (žr. 3.1.9 teiginį), galime parašyti $x = n \cdot y + z, 0 \leq z < n$. Jei būtų $z \neq 0$, tai, kadangi $x, n \in \mathfrak{a}$, gautume $z = x - n \cdot y \in \mathfrak{a}$. O tai prieštarautų skaičiaus n parinkimui (priminsime: n – idealo $\mathfrak{a}$ mažiausias nenulinis natūralusis skaičius). Taigi $x = n \cdot y \in (n)$, t. y. $\mathfrak{a} \subset (n)$. □

6.3.10 teiginys. *Matricų algebra* $M_n(k)$*, čia* k *– kūnas, neturi abipusių idealų, išskyrus* (0) *ir* $M_n(k)$*.*

Įrodymas. Priminsime, kad

$$M_n(k) = \{\sum_{i,j=1}^{n} \alpha_{ij} e_{ij} \mid \alpha_{ij} \in k,\ 1 \leq i, j \leq n\}.$$

Pirmiausia įrodysime, kad, jei $\mathfrak{a}$ yra abipusis idealas, kuriam priklauso kuris nors elementas $e_{i_0 j_0}$, tai $\mathfrak{a} = M_n(k)$. Iš tikrųjų, jei $e_{i_0 j_0} \in \mathfrak{a}$ ir $\mathfrak{a}$ – abipusis idealas, tai

$$e_{rs} = e_{r i_0} \cdot e_{i_0 j_0} \cdot e_{j_0 s} \in \mathfrak{a},\ 1 \leq r, s \leq n.$$

Vadinasi, ir $\sum\limits_{i,j=1}^{n} \alpha_{ij} e_{ij} \in \mathfrak{a}$, kad ir kokie būtų koeficientai $\alpha_{ij} \in k$, $1 \leq i, j \leq n$.

Dabar tarkime, kad $\mathfrak{a}$ – nenulinis abipusis algebros $M_n(k)$ idealas. Įrodysime, kad idealui $\mathfrak{a}$ priklauso bent vienas elementas $e_{i_0 j_0}$ ir, remdamiesi anksčiau įrodytu faktu, užbaigsime teiginio įrodymą.

Kadangi $\mathfrak{a} \neq (0)$, tai idealui $\mathfrak{a}$ priklauso nenulinis elementas $a = \sum_{i,j=1}^{n} \alpha_{ij} \cdot e_{ij}$. Tarkime, kad $\alpha_{i_0 j_0} \neq 0$. Elementas

$$e_{i_0 i_0} \cdot a \cdot e_{j_0 j_0} = \alpha_{i_0 j_0} e_{i_0 j_0} \in \mathfrak{a},$$

nes $a \in \mathfrak{a}$ ir $\mathfrak{a}$ – abipusis idealas. Kadangi $\alpha_{i_0 j_0} \neq 0$, tai

$$\alpha_{i_0 j_0}^{-1} \cdot (\alpha_{i_0 j_0} \cdot e_{i_0 j_0}) = e_{i_0 j_0} \in \mathfrak{a}\,.$$

□

6.3.11. Algebra $M_n(k)$ turi kairiųjų ir dešiniųjų idealų, nesutampančių nei su (0), nei su $M_n(k)$. Pavyzdžiui, $e_{ij} \cdot M_n(k)$ – dešinysis idealas, kurio kiekvienas elementas turi pavidalą

$$\sum_{s=1}^{n} \alpha_{is} \cdot e_{is}.$$

Kaip matome, $e_{ij} \cdot M_n(k) \neq M_n(k)$. Be to, akivaizdu, kad $e_{ij} \cdot M_n(k) = e_{i1} \cdot M_n(k)$.

Pratimas. Įrodykite, kad komutatyvus žiedas $(A, +, *)$, kurio idealai yra tik (0) ir A, yra kūnas.

6.4 Žiedo faktoržiedas pagal idealą

6.4.1. Tarkime, kad $(A, +, *)$ – žiedas, $\mathfrak{a}$ – šio žiedo abipusis idealas. Apibrėšime faktoržiedą $(A/\mathfrak{a}, +, *)$. Tam apibrėžkime ekvivalentumo sąryšį aibėje A:

$$x \underset{\mathfrak{a}}{\sim} y \iff x - y \in \mathfrak{a}\,.$$

Vietoje $x \underset{\mathfrak{a}}{\sim} y$ galima rašyti $x \equiv y (\operatorname{mod} \mathfrak{a})$. Aibės A faktoraibę pagal apibrėžtą ekvivalentumo sąryšį pažymėkime $A/\mathfrak{a}$. Faktoraibės $A/\mathfrak{a}$ elementai užrašomi $x + \mathfrak{a}$ (elementas $x + \mathfrak{a}$ dažnai yra žymimas $x (\operatorname{mod} \mathfrak{a})$). Remiantis ekvivalentumo sąryšio apibrėžimu,

$$x + \mathfrak{a} = y + \mathfrak{a} \iff x - y \in \mathfrak{a}\,.$$

Aibės $A/\mathfrak{a}$ elementų sudėtis.

Apibrėžkime elementų $x + \mathfrak{a}$ ir $y + \mathfrak{a}, x, y \in A$ sumą taip:

$$(x + \mathfrak{a}) + (y + \mathfrak{a}) := x + y + \mathfrak{a}\,.$$

Įsitikinsime, kad elementų $x + \mathfrak{a}$ ir $y + \mathfrak{a}$ suma $x + y + \mathfrak{a}$ nepriklauso nuo atstovų x ir y parinkimo. Tarkime, kad $x' + \mathfrak{a} = x + \mathfrak{a}, y' + \mathfrak{a} = y + \mathfrak{a}$. Tuomet $x' - x \in \mathfrak{a}, y' - y \in \mathfrak{a}$. Vadinasi, $x' + y' + \mathfrak{a} = x + y + \mathfrak{a}$, nes $(x' + y') - (x + y) = (x' - x) + (y' - y) \in \mathfrak{a}$ (priminsime: $x' - x \in \mathfrak{a}, y' - y \in \mathfrak{a} \Rightarrow (x' - x) + (y' - y) \in \mathfrak{a}$, nes $\mathfrak{a}$ yra idealas).

Nesunku įsitikinti, kad $(A/\mathfrak{a}, +)$ – Abelio grupė, $\mathfrak{a}$ – šios grupės neutralus elementas sudėties atžvilgiu.

Aibės $A/\mathfrak{a}$ elementų daugyba.

Apibrėžkime elementų $x + \mathfrak{a}$ ir $y + \mathfrak{a}, x, y \in A$ sandaugą taip:

$$(x + \mathfrak{a}) * (y + \mathfrak{a}) := x * y + \mathfrak{a}\,.$$

Įsitikinsime, kad elementų $x + \mathfrak{a}$ ir $y + \mathfrak{a}$ sandauga $x * y + \mathfrak{a}$ nepriklauso nuo atstovų x ir y parinkimo. Tarkime, kad $x' + \mathfrak{a} = x + \mathfrak{a}, y' + \mathfrak{a} = y + \mathfrak{a}$. Tuomet

$$(x' + \mathfrak{a}) * (y' + \mathfrak{a}) = x' * y' + \mathfrak{a}, \quad \text{o} \quad (x + \mathfrak{a}) * (y + \mathfrak{a}) = x * y + \mathfrak{a}\,.$$

Teigiame, kad $x' * y' + \mathfrak{a} = x * y + \mathfrak{a}$. Iš tikrųjų, nes

$$x' * y' - x * y = x' * y' - x' * y + x' * y - x * y = x' * (y' - y) + (x' - x) * y \in \mathfrak{a}$$

(priminsime: $\mathfrak{a}$ – abipusis idealas, $x' - x \in \mathfrak{a}, y' - y \in \mathfrak{a} \Rightarrow x' * (y' - y) \in \mathfrak{a}, (x' - x) * y \in \mathfrak{a} \Rightarrow x' * (y' - y) + (x' - x) * y \in \mathfrak{a}$).

Nesunku įsitikinti, kad aibės $A/\,\mathfrak{a}$ elementų daugyba yra asociatyvi. Įrodysime, kad aibės $A/\,\mathfrak{a}$ elementų sudėtis ir daugyba yra susijusios distributyvumo dėsniais:

$$((x + \mathfrak{a}) + (y + \mathfrak{a})) * (z + \mathfrak{a}) = (x + \mathfrak{a}) * (z + \mathfrak{a}) + (y + \mathfrak{a}) * (z + \mathfrak{a}),$$

$$(z + \mathfrak{a}) * ((x + \mathfrak{a}) + (y + \mathfrak{a})) = (z + \mathfrak{a}) * (x + \mathfrak{a}) + (z + \mathfrak{a}) * (y + \mathfrak{a}).$$

Įrodysime tik pirmąją lygybę, nes antroji lygybė įrodoma panašiai.

$$((x + \mathfrak{a}) + (y + \mathfrak{a})) * (z + \mathfrak{a}) = (x + y + \mathfrak{a}) * (z + \mathfrak{a}) = (x + y) * z + \mathfrak{a} =$$

$$= x * z + y * z + \mathfrak{a} = (x * z + \mathfrak{a}) + (y * z + \mathfrak{a}) = (x + \mathfrak{a}) * (z + \mathfrak{a}) + (y + \mathfrak{a}) * (z + \mathfrak{a}).$$

Taigi aibė $A/\,\mathfrak{a}$ apibrėžtų jos elementų sudėties $+$ ir daugybos $*$ atžvilgiu yra žiedas. Jei žiedas $(A, +, *)$ turi vienetą 1, tai $1 + \mathfrak{a}$ yra žiedo $(A/\,\mathfrak{a}, +, *)$ vienetas.

6.4.2 apibrėžimas. Žiedas $(A/\,\mathfrak{a}, +, *)$ yra vadinamas žiedo $(A, +, *)$ *faktoržiedu* pagal abipusį idealą $\mathfrak{a}$.

6.5 Žiedų homomorfizmai

Tarkime, kad $(A, +, *)$ ir $(B, +, *)$ – žiedai, 0_A ir 0_B yra žiedo A ir žiedo B nuliai.

6.5.1 apibrėžimas. Atvaizdis $f : A \to B$ yra vadinamas *homomorfizmu*, jei bet kuriems $x, y \in A$:

1. $f(x + y) = f(x) + f(y)$;

2. $f(x * y) = f(x) * f(y)$.

Įrodysime keletą paprastų faktų.

6.5.2 teiginys. *Jei $f : A \to B$ – homomorfizmas, tai:*

1. $f(0_A) = 0_B$;

2. $f(-x) = -f(x), x \in A$.

Įrodymas. 1. Galime parašyti: $f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A)$. Pirmoji iš šių lygybių gaunama remiantis tuo, kad $(0_A = 0_A + 0_A)$, o antroji – remiantis tuo, kad f – homomorfizmas. Prie lygybės $f(0_A) + f(0_A) = f(0_A)$ abiejų pusių pridėję elementui $f(0_A)$ priešingą elementą $-f(0_A)$, gauname:

$$(f(0_A) + f(0_A)) + (-f(0_A)) = f(0_A) + (-f(0_A)) = 0_B.$$

Bet kairėje lygybės pusėje esantis elementas yra lygus:

$$f(0_A) + ((f(0_A) + (-f(0_A)) = f(0_A) + 0_B = f(0_A).$$

Vadinasi, $f(0_A) = 0_B$.

2. Remdamiesi anksčiau įrodyta lygybe, gauname: $0_B = f(0_A) = f(x + (-x)) = f(x) + f(-x)$. Paskutinė lygybė gaunama remiantis tuo, kad f – homomorfizmas. Vadinasi, $f(-x)$ yra elementui $f(x)$ priešingas elementas, t. y. $f(-x) = -f(x)$. □

6.5.3 teiginys. *Jei $f : A \to B$ – nenulinis homomorfizmas, 1_A – žiedo A vienetas, tai $f(1_A)$ yra žiedo B idempotentas (idempotentas – tai nenulinis elementas, tenkinantis lygtį: $x^2 = x$).*

Įrodymas. Panašiai kaip ir įrodant 6.5.2 teiginį, galime parašyti: $f(1_A) = f(1_A * 1_A) = f(1_A) * f(1_A)$. Žiede lygtį $x * x = x$ tenkina idempotentai. Kadangi $f(1_A) * f(1_A) = f(1_A)$, tai galime teigti tik kad $f(1_A)$ yra žiedo B idempotentas. □

6.5.4 pastaba. Štai paprastas pavyzdys, iliustruojantis, kad $f(1_A)$ gali ir nebūti žiedo B vienetas. Apibrėžkime žiedą

$$A = \mathbb{Q} * e_1 + \mathbb{Q} * e_2 := \{\alpha * e_1 + \beta * e_2 \mid \alpha, \beta \in \mathbb{Q}\},$$

čia $\alpha * e_1 + \beta * e_2 = \gamma * e_1 + \delta * e_2$ tada ir tik tada, kai $\alpha = \gamma, \beta = \delta$. Apibrėžkime aibės A elementų sudėtį taip:

$$(\alpha_1 * e_1 + \alpha_2 * e_2) + (\beta_1 * e_1 + \beta_2 * e_2) := (\alpha_1 + \beta_1) * e_1 + (\alpha_2 + \beta_2) * e_2.$$

Galima nesunkiai įsitikinti, kad $(A, +)$ yra Abelio grupė, o $0 := 0 * e_1 + 0 * e_2$ – šios grupės nulis. Apibrėžkime elementų e_1, e_2 daugybos lentelę taip:

$$e_1^2 = e_1 * e_1 = e_1, e_2^2 = e_2 * e_2 = e_2, e_1 * e_2 = e_2 * e_1 = 0.$$

Remdamiesi 6-ąja žiedo apibrėžimo aksioma, daugybą galime išplėsti iki aibės A elementų daugybos. Taigi $(A, +, *)$ – žiedas. Apibrėžkime atvaizdį $f : A \to A$ taip:

$$f(\alpha_1 * e_1 + \alpha_2 * e_2) = \alpha_1 * e_1.$$

Žiedo $(A, +, *)$ vienetas daugybos atžvilgiu yra $e_1 + e_2$. Kaip matome, $f(e_1 + e_2) = e_1$, o e_1 yra žiedo A idempotentas.

6.5.5 pastaba. Dažnai yra nagrinėjami žiedų homomorfizmai $f : A \to B$ siauresne prasme, kai reikalaujama, kad žiedo A vieneto 1_A vaizdas $f(1_A)$ būtų žiedo B vienetas.

6.5.6 teiginys. *Jei $f : A \to B$ – siurjekcinis homomorfizmas, tai žiedo $(A, +, *)$ vieneto 1_A vaizdas $f(1_A)$ yra žiedo $(B, +, *)$ vienetas.*

Įrodymas. Pažymėkime žiedo B elementą $f(1_A)$ raide e. Norint įrodyti, kad e yra žiedo B vienetas, reikia įrodyti, kad bet kuriam žiedo B elementui b teisingos lygybės $e * b = b * e = b$. Kadangi $f : A \to B$ – siurjekcinis homomorfizmas, tai kiekvienam žiedo B elementui b egzistuoja toks žiedo A elementas a, kad $f(a) = b$. Lygybės $1_A * a = a * 1_A = a$ abi puses paveikę atvaizdžiu f, gauname: $f(1_A * a) = f(a * 1_A) = f(a)$. Šią lygybę pertvarkę, gauname: $f(1_A) * f(a) = f(a) * f(1_A) = f(a)$, t. y. $e * b = b * e = b$. □

6.5.7 teiginys. *Tarkime, kad $(A, +, *)$ ir $(B, +, *)$ – žiedai. Jei $f : A \to B$ – homomorfizmas, tai $f(A)$ yra žiedo B požiedis.*

Įrodymas. Jei $x, y \in f(A)$, tai egzistuoja tokie $a, b \in A$, kad $f(a) = x, f(b) = y$. Vadinasi, $x + y = f(a) + f(b) = f(a + b) \in f(A)$. Taigi žiedo B poaibis $f(A)$ yra stabilus sudėties atžvilgiu, $f(0_A) = 0_B \in f(A)$. Jei $x \in f(A)$, tai egzistuoja toks $a \in A$, kad $f(a) = x$. Tuomet $f(-a) = -f(a) = -x$. Vadinasi, $(f(A), +)$ yra Abelio grupė. Poaibis $f(A)$ taip pat yra stabilus ir daugybos atžvilgiu:

$$x * y = f(a) * f(b) = f(a * b) \in f(A),$$

čia $a, b \in A$ tokie, kad $f(a) = x, f(b) = y$. □

6.5.8 apibrėžimas. Tarkime, kad $f : A \to B$ – homomorfizmas. Žiedo A poaibis $\ker f := \{x \in A \mid f(x) = 0_B\}$ (t. y. $\ker f = f^{-1}(0_B)$) yra vadinamas homomorfizmo f *branduoliu*.

6.5.9 teorema. *Homomorfizmo $f : A \to B$ branduolys* $\ker f$ *yra žiedo A abipusis idealas. Žiedo A faktoržiedas $A/\ker f$ yra izomorfinis žiedo A vaizdui $f(A)$.*

Įrodymas. Pažymėsime , kad $\ker f \neq \emptyset$, nes $0_A \in \ker f$ (žr. 6.5.2 teiginį). Dabar patikrinsime abipusio idealo apibrėžimo aksiomas.

1. Jei $x, y, \in \ker f$, tai $f(x) = 0_B, f(y) = 0_B$. Vadinasi, $f(x \pm y) = f(x) \pm f(y) = 0_B + 0_B = 0_B$, t. y. $x \pm y \in \ker f$.

2. Jei $x \in \ker f, a \in A$, tai $f(x * a) = f(x) * f(a) = 0_B * f(a) = 0_B$. Panašiai $f(a * x) = f(a) * f(x) = f(a) * 0_B = 0_B$. Taigi $\ker f$ yra žiedo A abipusis idealas.

Kadangi $\ker f$ yra žiedo A abipusis idealas, galima nagrinėti žiedo A faktoržiedą $A/\ker f$ pagal idealą $\ker f$. Lieka įrodyti, kad $A/\ker f$ yra izomorfinis žiedo A vaizdui $f(A)$.

Homomorfizmas $f: A \to B$ generuoja atvaizdį

$$\bar{f}: A/\text{ker } \to f(A),\ \bar{f}(x + \text{ker } f) := f(x),\ x \in A.$$

Įrodysime, kad atvaizdis $\bar{f}: A/\text{ker } f \to f(A)$ yra korektiškai apibrėžtas, t. y. nepriklauso nuo ekvivalentumo klasės $x + \text{ker } f$ atstovo x parinkimo: jei $x + \text{ker } f = y + \text{ker } f$, tai ir $\bar{f}(x + \text{ker } f) = \bar{f}(y + \text{ker } f)$. Tarkime, kad $x + \text{ker } f = y + \text{ker } f$, t. y. $x - y \in \text{ker } f$. Tuomet $\bar{f}(x + \text{ker } f) = f(x)$, o $\bar{f}(y + \text{ker } f) = f(y)$. Kadangi $x - y \in \text{ker } f$, tai $f(x - y) = 0_B$. Vadinasi, $f(x) - f(y) = 0_B$, t. y. $f(x) = f(y)$.

Atvaizdis $\bar{f}: A/\text{ker } f \to f(A)$ yra siurjekcinis. Jei $b \in f(A)$, tai egzistuoja toks $a \in A$, kad $f(a) = b$ (kadangi atvaizdis $f: A \to B$ yra siurjekcija). Tuomet $\bar{f}(a + \text{ker } f) = f(a) = b$.

Įsitikinsime, kad atvaizdis $\bar{f}: A/\text{ker } f \to f(A)$ yra ir injekcinis. Jei $\bar{f}(a + \text{ker } f) = \bar{f}(a' + \text{ker } f)$, tai $f(a) = f(a')$ arba $f(a) - f(a') = 0_B$. Remdamiesi pastarąja lygybe, gauname: $f(a - a') = 0_B$,t. y. $a - a' \in \text{ker } f$, o tai ir reiškia, kad $a + \text{ker } f = a' + \text{ker } f$.

Atvaizdis $\bar{f}: A/\text{ker } f \to f(A)$ yra homomorfizmas, nes

$$\bar{f}((a + \text{ker } f) * (a' + \text{ker } f)) = \bar{f}(a * a' + \text{ker } f) =$$

$$= f(a * a') = f(a) * f(a') = \bar{f}(a + \text{ker } f) * \bar{f}(a' + \text{ker } f).$$

Kadangi $\bar{f}$ yra bijekcinis homomorfizmas, tai teorema įrodyta. □

6.5.10 teiginys. *Tarkime, kad* $(A, +, *)$ *ir* $(B, +, *)$ *– žiedai,* $f: A \to B$ *– siurjekcinis homomorfizmas. Tuomet žiedo A kairiojo (dešiniojo, abipusio) idealo* $\mathfrak{a}$ *vaizdas* $f(\mathfrak{a})$ *yra kairysis (dešinysis, abipusis) žiedo B idealas.*

Įrodymas. Sakykime, $\mathfrak{a}$ – kairysis žiedo A idealas, $f(\mathfrak{a})$ – jo vaizdas. Jei $x, y \in f(\mathfrak{a})$, tai egzistuoja tokie $a, b \in \mathfrak{a}$, kad $f(a) = x$, $f(b) = y$. Tuomet $x \pm y = f(a) \pm f(b) = f(a \pm b) \in f(\mathfrak{a})$, nes $a \pm b \in \mathfrak{a}$. Jei $x \in f(\mathfrak{a})$, $y \in B$, tai egzistuoja tokie $a \in \mathfrak{a}$, $b \in A$, kad $f(a) = x$, $f(b) = y$. Tuomet $y * x = f(b) * f(a) = f(b * a) \in f(\mathfrak{a})$, nes $b * a \in \mathfrak{a}$.

Panašiai įrodoma, kad žiedo A dešiniojo (abipusio) idealo vaizdas yra žiedo B dešinysis (abipusis) idealas. □

6.5.11 teiginys. *Tarkime, kad* $(A, +, *)$ *ir* $(B, +, *)$ *– žiedai,* $f: A \to B$ *– homomorfizmas. Tuomet žiedo B kairiojo (dešiniojo, abipusio) idealo* $\mathfrak{b}$ *pirmavaizdis* $f^{-1}(\mathfrak{b})$ *yra žiedo A kairysis (dešinysis, abipusis) idealas.*

Įrodymas. Sakykime, kad $\mathfrak{b}$ – žiedo B kairysis idealas, $f^{-1}(\mathfrak{b})$ – jo pirmavaizdis. Jei $x, y \in f^{-1}(\mathfrak{b})$, t. y. $f(x), f(y) \in \mathfrak{b}$, tai $x \pm y \in f^{-1}(\mathfrak{b})$, nes $f(x \pm y) = f(x) \pm f(y) \in \mathfrak{b}$. Jei $x \in f^{-1}(\mathfrak{b})$, $y \in A$, tai $y * x \in f^{-1}(\mathfrak{b})$. Iš tikrųjų: $f(y * x) = f(y) * f(x) \in \mathfrak{b}$, nes $f(y) \in B$, $f(x) \in \mathfrak{b}$, o kadangi $\mathfrak{b}$ idealas, tai ir $f(y) * f(x) \in \mathfrak{b}$.

Panašiai įrodoma, kad žiedo B dešiniojo (abipusio) idealo pirmavaizdisas yra žiedo A dešinysis (abipusis) idealas. □

Pratimas. Tarkime, kad $(A, +, *)$ ir $(B, +, *)$ – žiedai, $f : A \to B$ – siurjekcinis homomorfizmas, $\mathfrak{a}$ – žiedo A abipusis idealas. Įrodykite: $(f^{-1} \circ f)(\mathfrak{a}) = \mathfrak{a} + \ker f$.

6.5.12 teiginys. *Sakykime, kad $\mathfrak{a} \subset \mathfrak{b}$ yra žiedo A abipusieji idealai. Tuomet $\mathfrak{b}/\mathfrak{a}$ yra faktoržiedo $A/\mathfrak{a}$ abipusis idealas.*

Įrodymas. Šį teiginį siūlome įrodyti skaitytojui. □

Nagrinėsime žiedo idealus, nesutampančius su pačiu žiedu.

6.5.13 teiginys. *Tarkime, kad $(A, +, *)$ ir $(B, +, *)$ – žiedai, $f : A \to B$ – siurjekcinis homomorfizmas. Tuomet žiedo B abipusių idealų aibė $I(B)$ yra ekvivalenti žiedo A abipusių idealų $\mathfrak{a}$, tenkinančių sąlygą $\mathfrak{a} \supset \ker f$, ir $I(A/\ker f)$.*

Įrodymas. Jei $\mathfrak{b}$ yra žiedo B abipusis idealas, tai $f^{-1}(\mathfrak{b})$ yra žiedo A abipusis idealas ir $\ker f \subset f^{-1}(\mathfrak{b})$. Taigi galime apibrėžti atvaizdį $F : I(B) \to I(A/\ker f)$, $F(\mathfrak{b}) = f^{-1}(\mathfrak{b})$, $\mathfrak{b} \in I(B)$. Įsitikinsime, kad F yra bijekcija.

Jei $\mathfrak{a}$ yra žiedo A abipusis idealas ir $\ker f \subset \mathfrak{a}$, t. y. $\mathfrak{a} \in I(A/\ker f)$, tai $\mathfrak{b} := f(\mathfrak{a})$ yra žiedo B abipusis idealas. Be to, $F(\mathfrak{b}) = f^{-1}(f(\mathfrak{a})) = \mathfrak{a} + \ker f = \mathfrak{a}$. Kaip matome, F yra siurjekcinis atvaizdis. Akivaizdu, kad F – injekcinis atvaizdis: jei $\mathfrak{b}_1 \neq \mathfrak{b}_2$, tai $f^{-1}(\mathfrak{b}_1) \neq f^{-1}(\mathfrak{b}_2)$, t. y. $F(\mathfrak{b}_1) \neq F(\mathfrak{b}_2)$. □

6.5.14. Sakykime, $(A, +, *)$ – žiedas, $I(A)$ yra šio žiedo visų abipusių idealų, nesutampančių su žiedu A, aibė. $I(A)$ įdėties $\subset$ atžvilgiu yra sutvarkytoji aibė. Remdamiesi Corno lema (žr. 1.5.25 teoremą), įrodysime, kad aibėje $I(A)$ egzistuoja bent vienas maksimalus elementas.

6.5.15 teiginys. *Žiedo $(A, +, *)$ su vienetu visų abipusių idealų, nelygių žiedui A, aibėje $I(A)$ egzistuoja bent vienas maksimalus elementas įdėties $\subset$ atžvilgiu.*

Įrodymas. Įsitikinsime, kad aibė $I(A)$ tenkina Corno lemos sąlygą. Sakykime, $\{\mathfrak{a}_\alpha\}_{\alpha \in P}$ yra žiedo A įdėties $\subset$ atžvilgiu tiesiškai sutvarkytų abipusių idealų šeima. Reikia įrodyti, kad žiedo A abipusių idealų šeima $\{\mathfrak{a}_\alpha\}_{\alpha \in P}$ aibėje $I(A)$ yra aprėžta iš viršaus. Tam įrodysime, kad aibė $\cup_{\alpha \in P} \mathfrak{a}_\alpha$ yra žiedo A abipusis idealas, nelygus žiedui A.

Sakykime,

$$x, y \in \cup_{\alpha \in P} \mathfrak{a}_\alpha.$$

Tuomet egzistuoja toks $\alpha_0 \in P$, kad $x, y \in \mathfrak{a}_{\alpha_0}$. Kadangi $\mathfrak{a}_{\alpha_0}$ yra žiedo A abipusis idealas, tai

$$x \pm y \in \mathfrak{a}_{\alpha_0} \subset \cup_{\alpha \in P} \mathfrak{a}_\alpha.$$

Jei

$$x \in \cup_{\alpha \in P} \mathfrak{a}_\alpha, y \in A,$$

tai egzistuoja toks $\alpha_0 \in P$, kad $x \in \mathfrak{a}_{\alpha_0}$. Kadangi $\mathfrak{a}_{\alpha_0}$ yra žiedo A abipusis idealas, tai

$$x * y, y * x \in \mathfrak{a}_{\alpha_0} \subset \cup_{\alpha \in P} \mathfrak{a}_\alpha.$$

Kaip matome, $\cup_{\alpha \in P} \mathfrak{a}_\alpha$ yra žiedo A abipusis idealas ir kiekvienam $\alpha \in P$,

$$\mathfrak{a}_\alpha \in \cup_{\alpha \in P} \mathfrak{a}_\alpha.$$

Be to, šis idealas nesutampa su žiedu A. Priešingu atveju žiedo vienetas 1 priklausytų kuriam nors $\mathfrak{a}_\alpha$, $\alpha \in P$, o tai prieštarautų sąlygai, kad visi aibės $I(A)$ elementai yra žiedo A idealai, nesutampantys su A. Dabar, remdamiesi Corno lema, gauname, kad aibė $I(A)$ turi bent vieną maksimalų elementą $\mathfrak{m}$. $\square$

6.5.16. Nuo šiol nagrinėsime tik komutatyvius žiedus $(A, +, *)$ su vienetu. Tegu $(A, +, *)$ toks žiedas, o $\mathfrak{m}$ – šio žiedo *maksimalus idealas*, t. y. toks idealas $\mathfrak{m} \neq A$, kad tarp idealų $\mathfrak{m}$ ir A nėra jokio kito idealo, t. y., jei $\mathfrak{a}$ – žiedo A idealas ir $\mathfrak{m} \subset \mathfrak{a} \subset A$, tai $\mathfrak{a} = \mathfrak{m}$ arba $\mathfrak{a} = A$.

Įrodysime svarbią komutatyvaus žiedo maksimalaus idealo savybę.

6.5.17 teiginys. *Jei komutatyvaus žiedo $(A, +, *)$ su vienetu elementų x ir y sandauga $x * y$ priklauso maksimaliam šio žiedo idealui $\mathfrak{m}$, tai bent vienas iš elementų x ar y priklauso $\mathfrak{m}$.*

Įrodymas. Sakykime, kad žiedo A elementų x ir y sandauga $x * y$ priklauso maksimaliam idealui $\mathfrak{m}$. Jei elementas $x \in \mathfrak{m}$, tai teiginio įrodymas baigtas. Sakykime, kad $x \notin \mathfrak{m}$. Tuomet $A * x + \mathfrak{m}$ yra žiedo A idealas, nes $A * x$ ir $\mathfrak{m}$ yra idealai, o idealų suma, kaip žinome, yra idealas. Kadangi $x \in A * x + \mathfrak{m}$, bet $x \notin \mathfrak{m}$, tai $A * x + \mathfrak{m} = A$. Vadinasi, egzistuoja tokie $a \in A$, $m \in \mathfrak{m}$, kad $1 = a * x + m$. Padauginę šios lygybės abiejų pusių elementus iš y, gauname $y = a * x * y + m * y$. Remdamiesi sąlyga $x * y \in \mathfrak{m}$, gauname, kad ir $a * x * y \in \mathfrak{m}$. Kadangi $m \in \mathfrak{m}$, tai ir $m * y \in \mathfrak{m}$. Taigi ir elementas y priklauso idealui $\mathfrak{m}$, nes yra dviejų elementų $a * x * y$ ir $m * y$, priklausančių idealui $\mathfrak{m}$, suma. $\square$

Žiedo $(A, +, *)$ idealas $\mathfrak{p} \neq A$ vadinamas *pirminiu*, jei iš $x, y \in A$ ir $xy \in \mathfrak{p}$ išplaukia, kad $x \in \mathfrak{p}$ arba $y \in \mathfrak{p}$. Iš 6.5.17 teiginio matyti, kad kiekvienas maksimalus idealas yra pirminis.

6.5.18 teiginys. *Komutatyvaus žiedo $(A, +, *)$ su vienetu 1 faktoržiedas $A/\mathfrak{m}$ pagal žiedo A idealą $\mathfrak{m}$ yra kūnas tada ir tik tada, kai $\mathfrak{m}$ yra maksimalus idealas.*

Įrodymas. Kaip žinome, komutatyvaus žiedo $(A, +, *)$ su vienetu 1 faktoržiedas $A/\mathfrak{m}$ pagal žiedo A idealą $\mathfrak{m}$ yra žiedas. Sakykime, kad $\mathfrak{m}$ yra maksimalus idealas. Įrodysime, kad faktoržiedo $A/\mathfrak{m}$ kiekvienam nenuliniam elementui egzistuoja atvirkštinis elementas. Imkime $x + \mathfrak{m} \in A/\mathfrak{m}$, $x \notin \mathfrak{m}$. Idealas $A * x + \mathfrak{m}$ tenkina sąlygas:

(i) $\mathfrak{m} \subset A * x + \mathfrak{m}$;

(ii) $\mathfrak{m} \neq A * x + \mathfrak{m}$, $x \in A * x + \mathfrak{m}$, $x \notin \mathfrak{m}$.

Vadinasi, $A = A * x + \mathfrak{m}$. Taigi egzistuoja tokie $a \in A$, $m \in \mathfrak{m}$, kad $a * x + m = 1$. Teigiame, kad faktoržiedo $A/\mathfrak{m}$ elementas $a + \mathfrak{m}$ yra atvirkštinis elementui $x + \mathfrak{m}$. Iš tikrųjų:

$$(a + \mathfrak{m}) * (x + \mathfrak{m}) = a * x + \mathfrak{m} = 1 - m + \mathfrak{m} = 1 + \mathfrak{m}\,.$$

Sakykime, kad faktoržiedas $A/\mathfrak{m} = k$ yra kūnas. Atvaizdis $f : A \to k$, $f(x) := x + \mathfrak{m}$, $x \in A$, yra siurjekcinis homomorfizmas, kurio branduolys yra $\mathfrak{m}$. Pagal 6.5.13 teiginį, yra abipus vienareikšmė atitiktis tarp k idealų ir žiedo A idealų $\mathfrak{a}$, tenkinančių sąlygą: $\mathfrak{m} \subset \mathfrak{a}$. Kaip žinome, kūnas k neturi tarpinių idealų tarp $\{0\}$ ir paties kūno k. Vadinasi, nėra žiedo A tarpinių idealų tarp $\mathfrak{m}$ ir A. Taigi $\mathfrak{m}$ yra žiedo A maksimalus idealas. □

6.6 Dalumas žieduose

Nagrinėsime dalumo sąvoką žieduose.

6.6.1 apibrėžimas. Sakykime, $(A, +, *)$ yra komutatyvus žiedas su vienetu 1, $a, b \in A$. Elementas b yra vadinamas elemento a *dalikliu* (dažnai sakoma ir taip: *elementas b dalija elementą a*) ir žymimas $b \mid a$, jei egzistuoja toks elementas $c \in A$, kad $a = b * c$.

Nagrinėjant kurio nors žiedo savybes, svarbu žinoti šio žiedo vieneto daliklius.

6.6.2 teiginys. *Komutatyvaus žiedo $(A, +, *)$ su vienetu 1 žiedo vieneto daliklių aibė A^* žiedo elementų daugybos $*$ atžvilgiu sudaro grupę.*

Įrodymas. Aibė A^* netuščia, nes $1 \in A^*$ $(1|1$, nes $1 * 1 = 1)$. Sakykime, kad $a, b \in A^*$, t. y. egzistuoja tokie $c, d \in A$, kad $a * c = 1$, $b * d = 1$. Tuomet $(a * b) * (c * d) = (a * c) * (b * d) = 1 * 1 = 1$, t. y., jei a ir b yra vieneto 1 dalikliai, tai elementas $a * b$ taip pat yra vieneto daliklis. Vadinasi, žiedo A poaibis A^* yra stabilus žiedo elementų daugybos $*$ atžvilgiu. Daugyba $*$ yra asociatyvi, $1 \in A^*$. Jei $a \in A^*$, tai egzistuoja toks $b \in A$, kad $a * b = 1$. Bet šią lygybę galima ir taip užrašyti: $b * a = 1$. Taigi $b \in A^*$ ir yra atvirkštinis elementas elementui a. Grupė $(A^*, *)$ yra komutatyvi, nes žiedas A yra komutatyvus. □

6.6.3 apibrėžimas. Komutatyvaus žiedo $(A,+,*)$ su vienetu 1 elementai a ir b yra vadinami *asocijuotais* (*ekvivalenčiais*), jei egzistuoja toks žiedo vieneto daliklis u (t. y. $u \in A^*$), kad $a = b * u$. Jei a ir b yra asocijuoti, tai rašysime $a \approx b$.

Kitaip tariant, elementai a ir b yra asocijuoti (ekvivalentūs), jei $a|b$ ir $b|a$.

6.6.4 teiginys. *Binarusis sąryšis $\approx$ aibėje A yra ekvivalentumo sąryšis.*

Įrodymas. 1. Kiekvienam $a \in A$, $a \sim a$, nes $a = a * 1$, $1 \in A^*$.

2. Jei $a \approx b$, tai $b \approx a$. Iš tikrųjų, jei $a \approx b$, tai egzistuoja toks $u \in A^*$, kad $a = b * u$. Bet $u^{-1} \in A^*$. Vadinasi, $b = a * u^{-1}$, t. y. $b \approx a$.

3. Jei $a \approx b$ ir $b \approx c$, tai ir $a \approx c$. Iš tikrųjų, jei $a \approx b$ ir $b \approx c$, tai egzistuoja tokie $u, v \in A^*$, kad $a = b*u$, $b = c*v$. Iš šių lygybių gauname: $a = b*u = c*(v*u)$, t. y. $a \approx c$, nes, kadangi $u, v \in A^*$, tai ir $u * v \in A^*$. □

6.6.5 apibrėžimas. Komutatyvaus žiedo $(A,+,*)$ su vienetu 1 elementas π, kuris nėra lygus jokiam vieneto dalikliui, yra vadinamas *pirminiu*, jei elemento π dalikliai yra tik žiedo A vieneto 1 dalikliai ir elementai, ekvivalentūs elementui π.

6.6.6 pavyzdys. Sveikųjų skaičių žiedo $(\mathbb{Z},+,\cdot)$ vieneto dalikliai yra $\{1,-1\}$. Ekvivalentūs pirminiai skaičiai skiriasi ženklu. Kalbant apie pirminius skaičius, iš dviejų tarpusavyje ekvivalenčių pirminių skaičių visuomet galime pasirinkti teigiamąjį.

6.6.7 pavyzdys. Skaičių aibė $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} | a, b \in \mathbb{Z}\}$ skaičių sudėties $+$ ir daugybos $*$ atžvilgiu sudaro komutatyvų žiedą su vienetu $1 = 1 + 0\sqrt{2}$. Šis žiedas turi be galo daug vieneto daliklių. Pavyzdžiui, $\varepsilon = 1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ yra žiedo vieneto dakiklis. Iš tikrųjų: $-1 + \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, o $(-1 + \sqrt{2})(1 + \sqrt{2}) = -(-1)^2 + (\sqrt{2})^2 = 1$. Elementai ε^n, $n \in \mathbb{Z}$ yra vieneto dalikliai. Visų žiedo $\mathbb{Z}[\sqrt{2}]$ vieneto daliklių grupė yra $\{\pm\varepsilon^n | n \in \mathbb{Z}\}$.

Pavyzdžiui, žiedo $\mathbb{Z}[\sqrt{2}]$ elementai $\sqrt{2}$, 3, 5, $3 + \sqrt{2}$, $3 - \sqrt{2}$, 11, 13, $5 + 2\sqrt{2}$, $5 - 2\sqrt{2}$, 19, $5 + \sqrt{2}$, $5 - \sqrt{2}$ ir t. t., yra pirminiai, tarpusavyje neekvivalentūs. Be įrodymo paaiškinsime, kaip rasti žiedo $\mathbb{Z}[\sqrt{2}]$ tarpusavy neekvivalenčius pirminius elementus. Teigiami sveikieji pirminiai skaičiai p, tenkinantys sąlygą $p \equiv \pm 1 \pmod 8$, yra pirminiai ir žiede $\mathbb{Z}[\sqrt{2}]$. Teigiami sveikieji pirminiai skaičiai p, tenkinantys sąlygą $p \equiv 3, 5 (\operatorname{mod} 8)$, yra išskaidomi dviejų neekvivalenčių pirminių elementų $a + b\sqrt{2}$ ir $a - b\sqrt{2}$, priklausančių žiedui $\mathbb{Z}[\sqrt{2}]$, sandauga: $p = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2$. Elementai $a + b\sqrt{2}$ ir $a - b\sqrt{2}$ yra apibrėžti daugiklių $\pm\varepsilon^n$, $n \in \mathbb{Z}$, tikslumu. Pareikalaukime, kad pirminio skaičiaus p, $p \equiv 3, 5 (\operatorname{mod} 8)$, pirminių daugiklių $a + b\sqrt{2}$ ir $a - b\sqrt{2}$ sveikosios dalys a būtų teigiamos ir mažiausios. Taip apibrėžtus žiedo $\mathbb{Z}[\sqrt{2}]$ pirminius elementus $a + b\sqrt{2}$, $a - b\sqrt{2}$ ir pirminius skaičius p, $p \equiv \pm 1 (\operatorname{mod} 8)$ vadinsime žiedo $\mathbb{Z}[\sqrt{2}]$ *normuotais pirminiais elementais.*

Dabar suformuluosime svarbią teoremą apie žiedo $\mathbb{Z}[\sqrt{2}]$ nenulinių elementų išskaidymą pirminių elementų sandauga. Šios teoremos neįrodysime.

6.6.8 teorema. *Žiedo $\mathbb{Z}[\sqrt{2}]$ kiekvienas nenulinis elementas yra vienareikšmiškai išskaidomas vieneto daliklio ir normuotų pirminių elementų sandauga, jei nekreipiame dėmesio į dauginamųjų tvarką.*

6.6.9 pavyzdys. Panašiai kaip ir 6.6.7 pavyzdyje, nagrinėkime žiedą $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} | a, b \in \mathbb{Z}\}$ skaičių sudėties $+$ ir daugybos $\cdot$ atžvilgiu. Šio žiedo vieneto daliklių grupė yra $\{1, -1\}$. Tai įrodysime.

Sakykime, $a + b\sqrt{-5}|1$. Tuomet egzistuoja toks $c + d\sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$, kad $(a + b\sqrt{-5})(c + d\sqrt{-5}) = 1$, t. y. $ac - 5bd = 1$, $ad + bc = 0$. Remdamiesi šiomis lygybėmis matome, kad ir $(a - b\sqrt{-5})(c - d\sqrt{-5}) = 1$. Vadinasi,

$$(a + b\sqrt{-5})(c + d\sqrt{-5})(a - b\sqrt{-5})(c - d\sqrt{-5}) = 1$$

arba

$$(a + b\sqrt{-5})(a - b\sqrt{-5})(c + d\sqrt{-5})(c - d\sqrt{-5}) = (a^2 + 5b^2)(c^2 + 5d^2) = 1.$$

Ši lygybė galima tik tuo atveju, jei $a^2 + 5b^2 = 1$, $a, b \in \mathbb{Z}$. Lygtis $a^2 + 5b^2 = 1$ sveikaisiais skaičiais turi tik šiuos sprendinius: $a = 1, b = 0$ ir $a = -1, b = 0$. Taigi įrodėme, kad žiedo $\mathbb{Z}[\sqrt{-5}]$ vieneto dalikliai yra tik 1 ir -1.

Žiedo $\mathbb{Z}[\sqrt{-5}]$ elementai 3, 7, $4 + \sqrt{-5}$ ir $4 - \sqrt{-5}$ yra pirminiai. Pavyzdžiui, įrodysime, kad 3 yra pirminis elementas. Sakykime, kad $(a + b\sqrt{-5})(c + d\sqrt{-5}) = 3$. Panašiai kaip ir anksčiau, galime įrodyti, kad $(a - b\sqrt{-5})(c - d\sqrt{-5}) = 3$. Vadinasi,

$$(a + b\sqrt{-5})(a - b\sqrt{-5})(c + d\sqrt{-5})(c - d\sqrt{-5}) = (a^2 + 5b^2)(c^2 + 5d^2) = 9.$$

Kadangi $a^2 + 5b^2 | 9$, tai skaičius $a^2 + 5b^2$ gali būti lygus 1, 3 arba 9. Jei $a^2 + 5b^2 = 1$, tai $a = \pm 1, b = 0$. Šiuo atveju $c + d\sqrt{-5} = \pm 3$. Lygtis $a^2 + 5b^2 = 3$ sprendinių sveikaisiais skaičiais neturi. Jei $a^2 + 5b^2 = 9$, tai $a = \pm 3, b = 0$. Pagaliau išnagrinėjome visus atvejus ir įsitikinome, kad 3 yra pirminis elementas. Panašiai įrodoma, kad 7 yra žiedo $\mathbb{Z}[\sqrt{-5}]$ pirminis elementas.

Dabar įrodysime, kad $4 + \sqrt{-5}$ taip pat yra žiedo $\mathbb{Z}[\sqrt{-5}]$ pirminis elementas. Sakykime, kad

$$(a + b\sqrt{-5})(c + d\sqrt{-5}) = 4 + \sqrt{-5}.$$

Tada $ac - 5bd = 4$, $ad + bc = 1$. Remdamiesi šiomis lygybėmis, galite įsitikinti, kad

$$(a - b\sqrt{-5})(c - d\sqrt{-5}) = 4 - \sqrt{-5}.$$

Vadinasi,

$$(a + b\sqrt{-5})(c + d\sqrt{-5})(a - b\sqrt{-5})(c - d\sqrt{-5}) = (4 + \sqrt{-5})(4 - \sqrt{-5}) = 21.$$

Sudauginę šios lygybės kairėje pusėje esančius reiškinius, gauname: $(a^2+5b^2)(c^2+5d^2)=21$. Vadinasi, a^2+5b^2 gali būti lygus 1, 3, 7, 21. Bet lygtys $a^2+5b^2=3$ ir $a^2+5b^2=7$ sprendinių sveikaisiais skaičiais neturi. Jei $a^2+5b^2=1$, tai $a=\pm1, b=0$. Šiuo atveju $c+d\sqrt{-5}=\pm(4+\sqrt{-5})$. Jei $a^2+5b^2=21$, tai tuomet $c^2+5d^2=1$. Šiuo atveju $a+b\sqrt{-5}=\pm(4+\sqrt{-5})$. Panašiai įrodoma, kad žiedo $\mathbb{Z}[\sqrt{-5}]$ elementas $4-\sqrt{-5}$ yra taip pat pirminis.

Bet štai staigmena:

$$3\cdot7=(4+\sqrt{-5})(4-\sqrt{-5})=21.$$

Žiedo $\mathbb{Z}[\sqrt{-5}]$ elementas 21 yra išskaidomas pirminiais elementais dviem visiškai skirtingais būdais! Žiede $\mathbb{Z}[\sqrt{-5}]$ nenuliniai elementai pirminiais elementais gali būti išskaidomi ne vienu būdu.

6.7 Kompleksinių skaičių kūnas

6.7.1. Apibrėžkime aibę

$$\mathbb{C}=\{a+bi|\ a,\ b\in\mathbb{R},\ i^2=-1\}.$$

Aibės $\mathbb{C}$ elementas $a+bi$, $a,b\in\mathbb{R}$, vadinamas *kompleksiniu skaičiumi*. Skaičius a vadinama kompleksinio skaičiaus $a+bi$ *realiąja dalimi* ir žymimas $\mathrm{Re}(a+bi)$, t. y. $a=\mathrm{Re}(a+bi)$, o b – šio kompleksinio skaičiaus *menamąja dalimi* ir žymimas $\mathrm{Im}(a+bi)$, t. y. $b=\mathrm{Im}(a+bi)$. Du kompleksiniai skaičiai $a+bi$ ir $c+di$ yra lygūs pagal apibrėžimą tada ir tik tada, kai jų realiosios ir menamosios dalys yra lygios: $a=c, b=d$. Kompleksinis skaičius $0:=0+0\cdot i$ vadinamas nuliniu kompleksiniu skaičiumi arba tiesiog nuliu. Nenulinis kompleksinis skaičius $0+bi$, $b\in\mathbb{R}$, vadinamas *grynai menamuoju* skaičiumi.

Apibrėšime kompleksinių skaičių sudėtį ir daugybą ir įsitikinsime, kad kompleksinių skaičių aibė $\mathbb{C}$ apibrėžtų veiksmų atžvilgiu yra kūnas.

Aibės $\mathbb{C}$ elementų sudėtį apibrėžkime taip:

$$(a+bi)+(c+di):=(a+c)+(b+d)i,\ a,b,c,d\in\mathbb{R}.$$

Akivaizdu, kad kompleksinių skaičių aibė sudėties atžvilgiu sudaro Abelio grupę.

Aibės $\mathbb{C}$ elementų daugybą apibrėžkime taip:

$$(a+bi)(c+di):=(ac-bd)+(ad+bc)i,\ a,b,c,d\in\mathbb{R}.$$

1. Įsitikinkite, kad taip apibrėžta kompleksinių skaičių daugyba asociatyvi.

2. Akivaizdu, kad kompleksinis skaičius $1=1+0i$ daugybos atžvilgiu yra neutralus elementas, t. y. vienetas.

3. Kiekvienam nenuliniam kompleksinam skaičiui $a+bi$ egzistuoja atvirkštinis kompleksinis skaičius:

$$(a+bi)^{-1} = \frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)}$$
$$= \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}\, i \in \mathbb{C},$$

nes $\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2} \in \mathbb{R}$.

4. Kompleksinių skaičių daugyba komutatyvi: $(a+bi)(c+di) = (c+di)(a+bi)$. Įsitikinkite sudauginę šiuos kompleksinius skaičius.

Dabar akivaizdu, kad kompleksinių skaičių aibė be nulinio elemento $\mathbb{C}^*$ daugybos atžvilgiu sudaro Abelio grupę. Kadangi kompleksinių skaičių sudėtis ir daugyba yra susijusios distributyvumo dėsniu:

$$(\alpha+\beta)\gamma = \alpha\gamma + \beta\gamma,\ \alpha, \beta, \gamma \in \mathbb{C}$$

(įsitikinkite atlikę veiksmus), tai kompleksinių skaičių aibė $\mathbb{C}$ kompleksinių skaičių sudėties ir daugybos atžvilgiu sudaro kūną.

6.7.1 Kompleksinių skaičių geometrinė interpretacija

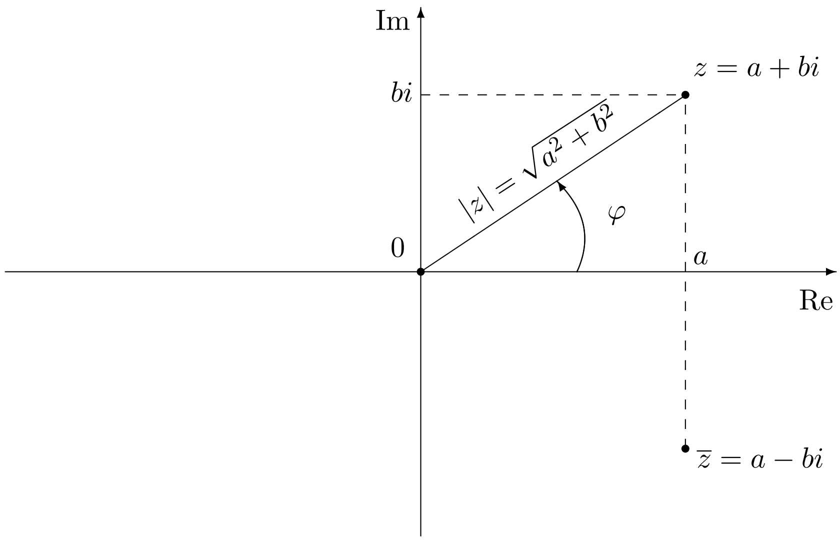
6.7.2. Kompleksinius skaičius galima pavaizduoti plokštumos $\mathbb{R}^2 = \mathbb{R}\times\mathbb{R}$ taškais: kompleksinį skaičių $a+bi$ atitinka plokštumos $\mathbb{R}^2$ taškas, kurio koordinatės yra (a, b) (žr. 6.1 pav.). Realiuosius skaičius $a = a+0i$, $a \in \mathbb{R}$, atitinka plokštumos $\mathbb{R}^2$ tiesė $\{(a, 0)|\ a \in \mathbb{R}\}$, vadinama *realiąja tiese* ir žymima Re, o grynai menamuosius kompleksinius skaičius $0+bi$, $b \in \mathbb{R}$, atitinka plokštumos $\mathbb{R}^2$ tiesė $\{(0, b)|\ b \in \mathbb{R}\}$, vadinama *menamąja tiese* ir žymima Im.

Plokštumos $\mathbb{R}^2$ taško (a, b), atitinkančio kompleksinį skaičių $a+bi$, atstumas $\sqrt{a^2+b^2}$ iki koordinačių pradžios $(0, 0)$ vadinamas kompleksinio skaičiaus $a+bi$ *moduliu* ir žymimas $|a+bi|$. Įsitikinsime, kad funkcija $|\cdot| : \mathbb{C} \to \mathbb{R}_+$ (čia $\mathbb{R}_+$ – neneigiamų realiųjų skaičių aibė) yra multiplikatyvi (funkcija $f : \mathbb{C} \to \mathbb{C}$ vadinama *multiplikatyvia*, jei bet kuriems $z_1, z_2 \in \mathbb{C}$, $f(z_1z_2) = f(z_1)f(z_2)$.):

$$|(a+bi)(c+di)| = |a+bi| \cdot |c+di|,\ a, b, c, d \in \mathbb{R}.$$

Norint įrodyti pastarąją lygybę, patogu vietoje kompleksinio skaičiaus $a+bi$ modulio $|a+bi| = \sqrt{a^2+b^2}$ nagrinėti šio kompleksinio skaičiaus modulio kvadratą $|a+bi|^2 = a^2+b^2$. Taigi

$$|(a+bi)(c+di)|^2 = (ac-bd)^2 + (bc+ad)^2 = a^2c^2 + b^2d^2 + b^2c^2 + a^2d^2$$
$$= (a^2+b^2)c^2 + (a^2+b^2)d^2 = (a^2+b^2)(c^2+d^2) = |a+bi|^2|c+di|^2.$$



6.1 pav.: Kompleksinių skaičių plokštuma

6.7.3 apibrėžimas. Kompleksinis skaičius $a - bi$ vadinamas *jungtiniu* kompleksiniam skaičiui $a + bi$ ir yra žymimas $\overline{a + bi}$.

Jei kompleksinį skaičių $a+bi$ atitinka plokštumos $\mathbb{R}^2$ taškas (a, b), tai jungtinį kompleksinį skaičių $a - bi$ skaičiui $a + bi$ atitinka plokštumos $\mathbb{R}^2$ taškas $(a, -b)$, simetrinis taškui (a, b) realiosios tiesės $\{(a, 0)|\ a \in \mathbb{R}\}$ atžvilgiu.

Pratimai.

1. Įrodykite, kad bet kuriems kompleksiniams skaičiams α, β teisingos lygybės $\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$ ir $\overline{\alpha\beta} = \bar{\alpha}\bar{\beta}$.

2. Įrodykite, kad bet kuriam nenuliniam kompleksiniam skaičiui α teisinga lygybė $\overline{\alpha^{-1}} = (\bar{\alpha})^{-1}$.

6.7.2 Kompleksinių skaičių trigonometrinė išraiška

6.7.4 apibrėžimas. Kompleksinį skaičių $a+bi \neq 0$ galima užrašyti trigonometrine išraiška. Nagrinėkime nenulinį vektorių v, kurio pradžia yra taške $(0, 0)$, o galas – taške (a, b). Realiąją teigiamą pusašę $\{(a, 0)|a \geq 0\}$ pasukime apie tašką $(0, 0)$ prieš laikrodžio rodyklę tokiu kampu $\varphi \in [0, 2\pi)$, kad vektoriaus v ir pasuktos pusašės kryptys sutaptų. Kampas $\varphi \in [0, 2\pi)$ vadinamas kompleksinio skaičiaus

$a + bi \neq 0$ *argumentu* ir žymimas $\arg(a+bi)$. Taip pat apibrėžkime aibę

$$\mathrm{Arg}\,(a+bi) := \{\arg(a+bi) + 2\pi n \mid n \in \mathbb{Z}\}.$$

6.7.5 pastaba. Kompleksinio skaičiaus 0 argumentas neapibrėžtas.

Kompleksinio skaičiaus $a + ib$ modulį $\sqrt{a^2+b^2}$ pažymėkime raide r. Nesunku įsitikinti, kad teisingos lygybės $a = r\cos\varphi$, $b = r\sin\varphi$ (žr. 6.1 pav.). Taigi galime parašyti:

$$a + bi = r(\cos\varphi + i\sin\varphi). \tag{6.1}$$

Ši lygybė vadinama kompleksinio skaičiaus $a + bi$ *trigonometrine išraiška.*

Kompleksinio skaičiaus $a + bi$ argumentas, atsižvelgiant į taško $(a, b) \neq (0, 0)$ padėtį koordinačių ašių atžvilgiu, apskaičiuojamas šitaip:

$$\arg(a+bi) = \begin{cases} \arccos\left(\frac{a}{\sqrt{a^2+b^2}}\right) & \text{I ir II ketvirtyje,} \\ 2\pi - \arccos\left(\frac{a}{\sqrt{a^2+b^2}}\right) & \text{III ir IV ketvirtyje, } b \neq 0\,. \end{cases}$$

Trigonometrinės išraiškos kompleksinius skaičius patogu dauginti.

6.7.6 teiginys. *Sakykime,* $z_1, z_2 \in \mathbb{C} \setminus \{0\}$, $\varphi_1 := \arg z_1$, $\varphi_2 := \arg z_2$. *Tuomet*

$$\begin{aligned} &1) \quad (z_1)^{-1} = |z_1|^{-1}\big(\cos(-\varphi_1) + i\sin(-\varphi_1)\big); \\ &2) \quad z_1 \cdot z_2 = |z_1| \cdot |z_2|\big(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)\big); \\ &3) \quad \tfrac{z_1}{z_2} = \tfrac{|z_1|}{|z_2|}\big(\cos(\varphi_1-\varphi_2) + i\sin(\varphi_1-\varphi_2)\big). \end{aligned}$$

Įrodymas. 1) Kompleksinio skaičiaus z_1 trigonometrinė išraiška yra

$$z_1 = |z_1|(\cos\varphi_1 + i\sin\varphi_1),$$

todėl galime parašyti

$$\begin{aligned} \frac{1}{z_1} = \frac{1}{|z_1|(\cos\varphi_1 + i\sin\varphi_1)} &= \frac{\cos\varphi_1 - i\sin\varphi_1}{|z_1|(\cos\varphi_1 + i\sin\varphi_1)(\cos\varphi_1 - i\sin\varphi_1)} \\ &= \frac{1}{|z_1|}\frac{\cos\varphi_1 - i\sin\varphi_1}{\cos^2\varphi_1 + \sin^2\varphi_1} = \frac{1}{|z_1|}(\cos\varphi_1 - i\sin\varphi_1) \\ &= \frac{1}{|z_1|}\big(\cos(-\varphi_1) + i\sin(-\varphi_1)\big). \end{aligned}$$

Taigi, 1) lygybė teisinga.

2) Pasinaudoję kompleksinių skaičių z_1 ir z_2 trigonometrinėmis išraiškomis (žr. 6.1 lygybę), galime parašyti

$$z_1 \cdot z_2 = |z_1|(\cos\varphi_1 + i\sin\varphi_1) \cdot |z_2|(\cos\varphi_2 + i\sin\varphi_2)$$

$$= |z_1| \cdot |z_2| \Big(\cos\varphi_1 \cos\varphi_2 - \sin\varphi_1 \sin\varphi_2 + i\big(\cos\varphi_1 \sin\varphi_2 + \sin\varphi_1 \cos\varphi_2\big)\Big)$$

$$= |z_1| \cdot |z_2| \big(\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)\big).$$

Taigi 2) teiginio lygybė taip pat teisinga.

3) Trečioji teiginio lygybė išplaukia iš pirmųjų dviejų. □

6.7.7 pastaba. Nenuliniam kompleksiniam skaičiui z sutarkime žymėti $z^0 := 1$.

6.7.8 išvada (Muavro formulė)**.** *Sakykime, z – nenulinis kompleksinis skaičius, kurio argumentas yra φ. Tuomet bet kuriam $n \in \mathbb{Z}$ teisinga lygybė*

$$z^n = |z|^n \big(\cos(n\varphi) + i \sin(n\varphi)\big). \tag{6.2}$$

Įrodymas. Iš pradžių įrodysime (6.2) lygybę natūraliesiems skaičiams. Kai $n = 1$, tai (6.2) lygybė yra kompleksinio skaičiaus z trigonometrinė išraiška:

$$z = |z|(\cos\varphi + i \sin\varphi).$$

Tarkime, kad (6.2) lygybė teisinga su visais natūraliaisiais skaičiais k, $k \le n - 1$. Taigi teisinga lygybė

$$z^{n-1} = |z|^{n-1} \big(\cos((n-1)\varphi) + i \sin((n-1)\varphi)\big).$$

Kompleksiniams skaičiams z ir z^{n-1} pritaikę 6.7.6 teiginio antrąją lygybę, gauname

$$z^n = z \cdot z^{n-1} = |z|^n \big(\cos(n\varphi) + i \sin(n\varphi)\big),$$

t. y. (6.2) lygybė teisinga, kai $k = n$. Remiantis matematinės indukcijos principu, (6.2) lygybė teisinga bet kuriam natūraliajam n.

Dabar tarkime, kad n – neigiamas sveikasis skaičius. Pritaikę (6.2) lygybę kompleksiniam skaičiui z ir natūraliajam skaičiui $-n$, gauname

$$z^{-n} = |z|^{-n} \big(\cos(-n\varphi) + i \sin(-n\varphi)\big).$$

Remdamiesi šia lygybe ir 6.7.6 teiginio pirmąja lygybe, galime parašyti

$$z^n = \big(z^{-n}\big)^{-1} = |z|^n \big(\cos(n\varphi) + i \sin(n\varphi)\big).$$

Pagaliau, jei $n = 0$, tai (6.2) lygybė akivaizdi (žr. 6.7.7 pastabą). □

Iš 6.7.6 teiginio 2) lygybės ir kompleksinio skaičiaus apibrėžimo išplaukia tokia lygybė:

$$\arg(\alpha\beta) = \begin{cases} \arg\alpha + \arg\beta, & \text{jei } \arg\alpha + \arg\beta < 2\pi, \\ \arg\alpha + \arg\beta - 2\pi, & \text{jei } \arg\alpha + \arg\beta \ge 2\pi \end{cases}, \tag{6.3}$$

$\alpha, \beta \in \mathbb{C} \setminus \{0\}$.

6.7.9. Sakykime, $A, B \subset \mathbb{R}$. Apibrėžkime aibių A ir B sumą:

$$A + B := \{a + b \mid a \in A,\, b \in B\}.$$

Remdamiesi aibės $\operatorname{Arg}\alpha$, $\alpha \in \mathbb{C} \setminus \{0\}$, apibrėžimu ir (6.3) lygybe, galime parašyti:

$$\operatorname{Arg}(\alpha\beta) = \operatorname{Arg}\alpha + \operatorname{Arg}\beta,\ \ \alpha, \beta \in \mathbb{C} \setminus \{0\}.$$

6.7.3 Kompleksinių skaičių rodiklinė išraiška

Oileris pasiūlė tokį žymėjimą:

$$e^{i\varphi} := \cos\varphi + i\sin\varphi, \quad \varphi \in \mathbb{R}. \tag{6.4}$$

Tuomet kompleksinio skaičiaus $a + bi \neq 0$ trigonometrinę išraišką (6.1) galima perrašyti taip:

$$a + bi = re^{i\varphi}.$$

Ši lygybė vadinama kompleksinio skaičiaus $a+bi \neq 0$ *rodikline išraiška*. (6.4) lygybę galima „paaiškinti“ tokiu būdu: į funkcijos e^x skleidinį eilute:

$$e^x = \sum_{j=0}^{\infty} \frac{x^j}{j!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!} + \ldots$$

vietoje x-o įrašę $i\varphi$, $\varphi \in \mathbb{R}$, gauname:

$$e^{i\varphi} = 1 + i\varphi - \frac{\varphi^2}{2!} - \frac{i\varphi^3}{3!} + \frac{\varphi^4}{4!} + \ldots$$

$$= \sum_{j=0}^{\infty} \frac{(-1)^j \varphi^{2j}}{(2j)!} + i \sum_{j=1}^{\infty} \frac{(-1)^{j-1}\varphi^{2j-1}}{(2j-1)!} = \cos\varphi + i\sin\varphi.$$

Vadinasi, $a + bi = r(\cos\varphi + i\sin\varphi) = re^{i\varphi}$, čia $r = |a + bi|$, $\varphi = \arg(a + bi)$.

6.7.6 teiginį galima užrašyti rodikline forma.

6.7.10 teiginys. *Sakykime,* $z_1, z_2 \in \mathbb{C} \setminus \{0\}$, $\varphi_1 := \arg z_1$, $\varphi_2 := \arg z_2$. *Tuomet*

1) $(z_1)^{-1} = |z_1|^{-1} e^{-i\varphi_1}$;

2) $z_1 \cdot z_2 = |z_1| \cdot |z_2|\, e^{i(\varphi_1 + \varphi_2)}$;

3) $\frac{z_1}{z_2} = \frac{|z_1|}{|z_2|}\, e^{i(\varphi_1 - \varphi_2)}$.

6.7.4 Šaknies traukimas

6.7.11 apibrėžimas. Sakykime, $a + bi$ – nenulinis kompleksinis skaičius, o n – natūralusis skaičius. *n-tojo laipsnio šaknimi* iš skaičiaus $a + bi$ vadinamas kiekvienas kompleksinis skaičius z, kurio n-tasis laipsnis lygus $a + bi$, t. y.

$$z^n = a + bi.$$

6.7.12 teiginys. *Sakykime, z_0 – nenulinis kompleksinis skaičius, n – natūralusis skaičius, ir $\varphi_0 \in \operatorname{Arg} z_0$. Yra lygiai n skirtingų n-tojo laipsnio šaknų iš kompleksinio skaičiaus z_0 ir bet kuri iš jų užrašoma pavidalu*

$$\sqrt[n]{|z_0|} \cdot \left(\cos\left(\frac{\varphi_0 + 2\pi k}{n}\right) + i \sin\left(\frac{\varphi_0 + 2\pi k}{n}\right)\right), \tag{6.5}$$

$k = 0, 1, 2, \ldots, n - 1$.

Įrodymas. Tarkime, kad z yra n-tojo laipsnio šaknis iš kompleksinio skaičiaus z_0. Tegu $\varphi = \arg z$. Tuomet $z^n = z_0$, ir iš Muavro formulės (žr. 6.7.8 išvadą) išplaukia lygybė

$$z^n = |z|^n\big(\cos(n\varphi) + i \sin(n\varphi)\big) = |z_0|(\cos \varphi_0 + i \sin \varphi_0).$$

Taigi

$$\left\{\begin{array}{rl} |z|^n & = |z_0| \\ \cos(n\varphi) & = \cos \varphi_0 \\ \sin(n\varphi) & = \sin \varphi_0 \end{array}\right. \Leftrightarrow \left\{\begin{array}{ll} |z| & = \sqrt[n]{|z_0|} \\ n\varphi & = \varphi_0 + 2\pi k, \quad k \in \mathbb{Z} \end{array}\right.$$

$$\Leftrightarrow \left\{\begin{array}{ll} |z| & = \sqrt[n]{|z_0|} \\ \varphi & = \frac{\varphi_0 + 2\pi k}{n}, \quad k \in \mathbb{Z} \end{array}\right. .$$

Lieka pastebėti, kad visi (6.5) lygybėje nurodyti skaičiai yra skirtingi. t. y. egzistuoja lygiai n skirtingų n-tojo laipsnio šaknų iš nenulinio kompleksinio skaičiaus z_0. □

6.7.13 pavyzdys. Ištrauksime 5-ojo laipsnio šaknį iš kompleksinio skaičiaus $z = -\sqrt{3} + i$ ir pavaizduosime gautas šaknis kompleksinėje plokštumoje.

Sprendimas. Kompleksinio skaičiaus z modulis $|z| = 2$, o jo argumentas $\arg z = \arccos(-\sqrt{3}/2) = 5\pi/6$, todėl jo trigonometrinė forma yra

$$z = 2\left(\cos\frac{5\pi}{6} + i \sin\frac{5\pi}{6}\right).$$

Taigi

$$z_k = \sqrt[5]{2}\left(\cos\left(\frac{\pi}{6} + \frac{2\pi k}{5}\right) + i\ \sin\left(\frac{\pi}{6} + \frac{2\pi k}{5}\right)\right), \quad k = 0, 1, 2, 3, 4.$$

Vadinasi, kompleksinėje plokštumoje reikia pavaizduoti tokius skaičius:

$$z_0 = \sqrt[5]{2}\left(\cos\left(\frac{\pi}{6}\right) + i\,\sin\left(\frac{\pi}{6}\right)\right),$$

$$z_1 = \sqrt[5]{2}\left(\cos\left(\frac{17\pi}{30}\right) + i\,\sin\left(\frac{17\pi}{30}\right)\right),$$

$$z_2 = \sqrt[5]{2}\left(\cos\left(\frac{29\pi}{30}\right) + i\,\sin\left(\frac{29\pi}{30}\right)\right),$$

$$z_3 = \sqrt[5]{2}\left(\cos\left(\frac{41\pi}{30}\right) + i\,\sin\left(\frac{41\pi}{30}\right)\right),$$

$$z_4 = \sqrt[5]{2}\left(\cos\left(\frac{53\pi}{30}\right) + i\,\sin\left(\frac{53\pi}{30}\right)\right).$$

Šie skaičiai, pažymėti kompleksinėje plokštumoje, yra taisyklingojo penkiakampio, įbrėžto į apskritimą su centru taške 0 ir spinduliu $\sqrt[5]{2}$, viršūnės (žr. 6.2 paveikslėlį). $\square$

6.7.5 Kompleksinės plokštumos vienetinis apskritimas

6.7.14. Visi kompleksiniai skaičiai α, kurių modulis $|\alpha|$ yra lygus 1, sudaro kompleksinėje plokštumoje $\mathbb{C}$ apskritimą S^1, kurio centras yra koordinačių pradžioje $(0, 0)$, o spindulys lygus 1. Įrodysime, kad apskritimas S^1 kompleksinių skaičių daugybos atžvilgiu yra Abelio grupė.

Akivaizdu, aibė S^1 yra stabili kompleksinių skaičių daugybos atžvilgiu. Iš tikrųjų, jei $\alpha, \beta \in S^1$, tai $\alpha\beta \in S^1$, nes $|\alpha\beta| = |\alpha||\beta| = 1$.

Akivaizdu, kad

i) daugyba asociatyvi;

ii) 1 – daugybos atžvilgiu vienetinis elementas;

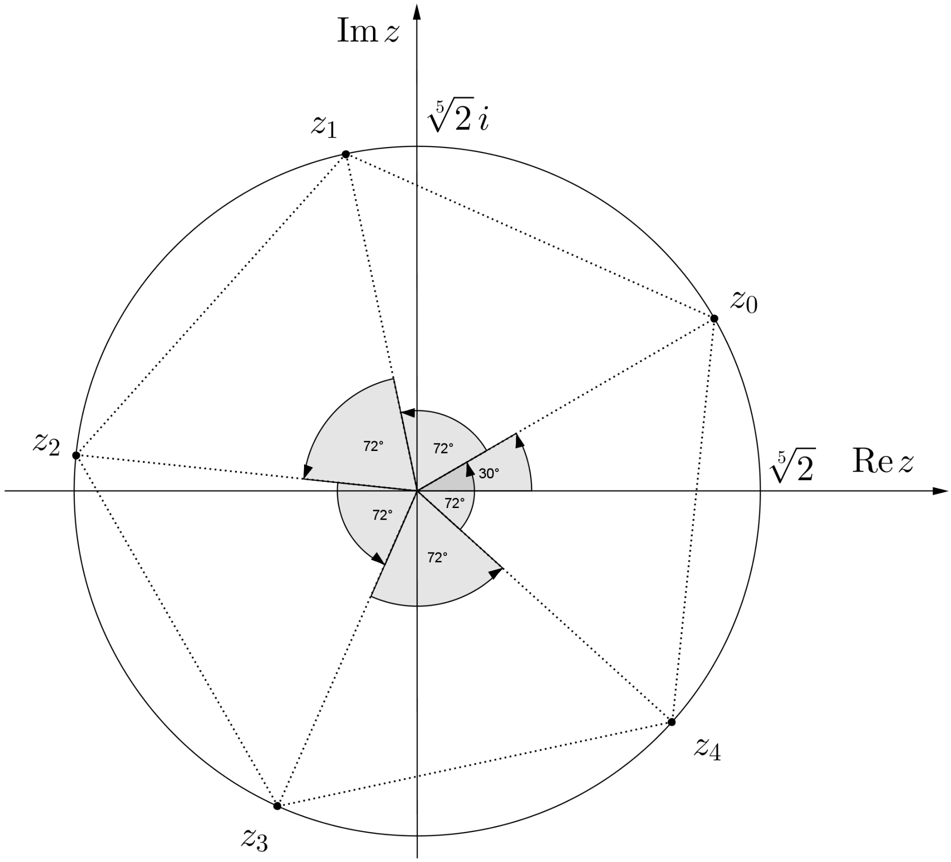
iii) jei $\alpha \in S^1$, tai $\alpha^{-1} \in S^1$;

iv) daugyba komutatyvi.

Taigi S^1 kompleksinių skaičių daugybos atžvilgiu yra Abelio grupė.

6.7.15. Kompleksinė plokštuma be nulio $\mathbb{C}^*$ kompleksinių skaičių daugybos atžvilgiu yra grupė, $\mathbb{R}^*_+$ ir S^1 – šios grupės pogrupiai. Kiekvienas nenulinis kompleksinis skaičius α vieninteliu būdu užrašomas

$$\alpha = |\alpha| e^{i \arg \alpha}, \quad |\alpha| \in \mathbb{R}^*_+, \quad e^{i \arg \alpha} \in S^1.$$



6.2 pav.: penktojo laipsnio šaknys iš skaičiaus $z = -\sqrt{3} + i$

Kitais žodžiais galima pasakyti taip: grupė $\mathbb{C}^*$ yra savo pogrupių $\mathbb{R}_+^*$ ir S^1 tiesioginė sandauga: $\mathbb{C}^* = \mathbb{R}_+^* \times S^1$.

Apibūdinant Abelio grupę S^1 nuodugniau, reikia kai kurių matematinės analizės sąvokų. Tarsime, kad tos sąvokos, kurias paminėsime, yra žinomos.

Kompleksinę plokštumą $\mathbb{C}$, kaip metrinę erdvę atstumo funkcijos $d(\alpha, \beta) = |\alpha - \beta|$ atžvilgiu, galima sutapatinti su Euklido plokštuma $\mathbb{R}^2$. n-matės Euklido erdvės $\mathbb{R}^n$ poaibis yra kompaktinis tada ir tik tada, kai jis yra aprėžtas ir uždaras. Kadangi apskritimas S^1 kompleksinėje plokštumoje yra aprėžtas ir uždaras, tai S^1 yra kompaktinė aibė.

Daugybos operacija $S^1 \times S^1 \dot{\to} S^1$ yra tolydus atvaizdis. Galima pasakyti ir tiksliau: daugybos funkcija $x + yi = (a + ib) \cdot (c + id)$, $a, b, c, d \in \mathbb{R}$, $a^2 + b^2 = 1$, $c^2 + d^2 = 1$, yra glodi (o iš tikrųjų analizinė) funkcija. Todėl grupė S^1 yra vadinama kompaktine realiąja Li grupe.

6.7.16 teiginys. *Nenulinių kompleksinių skaičių grupės $\mathbb{C}^*$ kiekvienas kompaktinis pogrupis G yra grupės S^1 pogrupis.*

Įrodymas. Sakykime, G – grupės $\mathbb{C}^*$ kompaktinis pogrupis, bet $G \not\subset S^1$. Vadinasi, egzistuoja toks kompleksinis skaičius $\alpha \in G$, bet $\alpha \notin S^1$. Tuomet $|\alpha| \neq 1$. Kadangi G – grupė, tai kiekvienam $n \in \mathbb{Z}$, $\alpha^n \in G$. Aibė $\{\alpha^n \mid n \in \mathbb{Z}\}$ nėra kompaktinė. Iš tikrųjų. Apibrėžtumo dėlei tarkime, kad $|\alpha| > 1$. Tuomet

$$\lim_{n\to\infty} |\alpha|^n = \infty,$$

t. y. aibė G nėra aprėžta, vadinasi, nėra kompaktinė. Gavome prieštarą prielaidai. Taigi $G \subset S^1$. $\square$

6.7.17. Kadangi kiekvienas grupės $\mathbb{C}^*$ baigtinis pogrupis G yra kompaktinis, tai remdamiesi įrodytu teiginiu, gauname $G \subset S^1$. Kitame skyrelyje aprašysime visus grupės S^1 baigtinius pogrupius (ir kartu visus grupės $\mathbb{C}^*$ kompaktinius pogrupius).

6.7.6 n-tojo laipsnio šaknys iš vieneto

6.7.18. Pirmiausia šiame skyrelyje išnagrinėsime lygties $x^n - 1 = 0$ sprendinius kompleksiniais skaičiais. Sakykime, kompleksinis skaičius α yra šios lygties sprendinys, t. y. $\alpha^n = 1$. Remdamiesi kompleksinio skaičiaus modulio multiplikatyviąja savybe, galime parašyti: $|\alpha^n| = |\alpha|^n = 1$. Kadangi kompleksinio skaičiaus α modulis $|\alpha|$ yra neneigiamas realusis skaičius, tai gauname $|\alpha| = 1$. Vadinasi, lygties $x^n - 1 = 0$ sprendinį trigonometrine išraiška galime užrašyti taip: $\alpha = \cos\varphi + i\sin\varphi$. Įrašę šį skaičių į lygybę $\alpha^n - 1 = 0$, gauname:

$$(\cos\varphi + i\sin\varphi)^n = 1,$$

$$\cos(n\varphi) + i\sin(n\varphi) = 1 + 0 \cdot i,$$

$$\begin{cases} \cos(n\varphi) = 1 \\ \sin(n\varphi) = 0 \end{cases}.$$

Taigi $n\varphi = 2\pi s$, $s \in \mathbb{Z}$. Iš šios lygybės gauname: $\varphi = \frac{2\pi s}{n}$, $s \in \mathbb{Z}$. Kintamajam s suteikę reikšmes $s = 0, 1, \ldots, n-1$, gauname n skirtingų φ reikšmių:

$$0,\ \frac{2\pi}{n},\ \frac{4\pi}{n},\ \frac{6\pi}{n},\ \ldots,\ \frac{2\pi(n-1)}{n},$$

kurios priklauso intervalui $[0, 2\pi)$. Kitaip tariant, gavome n skirtingų kompleksinių lygties $x^n - 1 = 0$ šaknų:

$$\cos\left(\frac{2\pi j}{n}\right) + i\,\sin\left(\frac{2\pi j}{n}\right) = e^{2\pi i j/n},\ \ 0 \le j \le n-1.$$

Bet, kaip žinome, n-tojo laipsnio lygtis kūne negali turėti daugiau negu n šaknų. Vadinasi, suradome visas lygties $x^n - 1 = 0$ kompleksines šaknis.

Lygties $x^n - 1 = 0$ šaknys $e^{2\pi ij/n}$, $0 \le j \le n-1$, priklauso vienetiniam apskritimui $S^1 \subset \mathbb{C}$ ir šį apskritimą dalija į n lygių dalių.

6.7.19 teiginys. *Lygties* $x^n - 1 = 0$ *šaknys* $e^{2\pi ij/n}$, $0 \le j \le n-1$, *sudaro ciklinę grupę (t. y. grupę, kurią generuoja vienas šios grupės elementas).*

Įrodymas. Apibrėžkime atvaizdį

$$f : \mathbb{Z} \to \{e^{2\pi ij/n} \mid 0 \le j \le n-1\} \subset S^1,\ f(j) = e^{2\pi ij/n},\ j \in \mathbb{Z}.$$

Šis atvaizdis yra siurjekcinis ir tenkina sąlygą: $f(j+l) = f(j) \cdot f(l)$, $j, l \in \mathbb{Z}$. Iš tikrųjų,

$$f(j+l) = e^{2\pi i(j+l)/n} = e^{2\pi ij/n} \cdot e^{2\pi il/n} = f(j) \cdot f(l),\ j, l \in \mathbb{Z}.$$

Kitaip tariant, atvaizdis $f : \mathbb{Z} \to S^1$ yra homomorfizmas. Kadangi $\mathbb{Z}$ skaičių sudėties atžvilgiu yra begalinės eilės ciklinė grupė, tai šios grupės vaizdas

$$f(\mathbb{Z}) = \{e^{2\pi ij/n} \mid 0 \le j \le n-1\}$$

yra n-tos eilės grupės S^1 ciklinis pogrupis. Šio pogrupio sudaromoji yra $e^{2\pi i/n}$, t. y. šis elementas generuoja pogrupį $\{e^{2\pi ij/n} \mid 0 \le j \le n-1\}$.

Homomorfizmo f branduolys $\ker f = n\mathbb{Z} = \{nl \mid l \in \mathbb{Z}\}$. Remdamiesi pirmąja teorema apie izomorfizmą (žr. 5.7.26 teoremą ir 5.7.27 išvadą), matome, kad lygties $x^n - 1 = 0$ šaknų grupė (multiplikacinė) $\{e^{2\pi ij/n} \mid 0 \le j \le n-1\}$ yra izomorfinė ciklinei grupei $\mathbb{Z}/n\mathbb{Z} = Z_n$. □

6.7.20. Galime susumuoti grupės S^1 baigtinių pogrupių rezultatus. Šios grupės baigtiniai pogrupiai – tai baigtinio laipsnio šaknų iš vieneto grupės ir šių grupių pogrupiai.

6.8 Polinomų žiedai

Šiame skyrelyje nagrinėsime polinomų žiedą.

6.8.1 apibrėžimas. Tarkime, $(A, +, *)$ – komutatyvus žiedas su vienetu 1. Begalinę formalią sumą

$$\sum_{j \ge 0} a_j x^j = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m + \ldots,\quad a_j \in A,\ j \ge 0,$$

vadinsime kintamojo x *polinomu* (*daugianariu*) su koeficientais žiede A, jei egzistuoja toks neneigiamas sveikasis skaičius n, kad kiekvienam $j > n$, $a_j = 0$.

6.8.2 apibrėžimas. Kintamojo x polinomus

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_mx^m + \ldots$$

ir

$$g(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m + \ldots$$

su koeficientais žiede A vadinsime lygiais ir žymėsime $f(x) = g(x)$ tada ir tik tada, kai kiekvienam $j \geq 0$, $a_j = b_j$. Visų kintamojo x polinomų su koeficientais žiede A aibę žymėsime $A[x]$.

6.8.3 pastaba. Polinomą

$$0 + 0x + 0x^2 + \cdots + 0x^m + \ldots$$

vadinsime nuliniu ir sutapatinsime su žiedo A nuliu 0.

6.8.4 pastaba. Polinomą

$$1 + 0x + 0x^2 + \cdots + 0x^m + \ldots$$

sutapatinsime su žiedo A vienetu 1.

6.8.5 pastaba. Jei polinomo $f(x) = \sum_{j\geq 0} a_jx^j$, $f(x) \in A[x]$, visi koeficientai $a_j = 0$, kai $j > n$, tai vietoje begalinės sumos $\sum_{j\geq 0} a_jx^j$ rašysime baigtinę sumą $\sum_{j=0}^{n} a_jx^j$.

6.8.6 apibrėžimas. Sakysime, kad nenulinio polinomo $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in A[x]$ *laipsnis* yra n, jei $a_n \neq 0$. Polinomo $f(x)$ laipsnį žymėsime $\deg f(x)$. Sutarkime, kad nulinio polinomo laipsnis yra $-\infty$, t. y. $\deg 0 := -\infty$. (Šis susitarimas leidžia supaprastinti kai kurias formules (žr. 6.8.10 išvadą).)

6.8.1 Polinomų sudėtis ir daugyba

Nagrinėkime du polinomus su koeficientais žiede A:

$$f(x) = \sum_{j\geq 0} a_jx^j \quad \text{ir} \quad g(x) = \sum_{j\geq 0} b_jx^j.$$

Šių polinomų suma ir sandauga apibrėžiamos taip:

$$f(x) + g(x) := \sum_{j\geq 0}(a_j + b_j)x^j,$$

$$f(x) \cdot g(x) := \sum_{j\geq 0}\Big(\sum_{\substack{r+s=j\\ r,s\geq 0}} a_r \cdot b_s\Big)x^j.$$

Nesunku įsitikinti, kad $(A[x], +)$ yra Abelio grupė. Be to, akivaizdu, kad dviejų polinomų sandauga taip pat yra polinomas.

Pratimas. Įrodykite, kad polinomų daugyba yra asociatyvi.

6.8.7 teiginys. *Aibė $A[x]$ polinomų sudėties ir daugybos atžvilgiu yra komutatyvus žiedas su vienetu 1.*

Įrodymas. Kaip minėjome, $(A[x], +)$ yra Abelio grupė. Polinomų daugyba yra asociatyvi, 1 – vienetas daugybos atžvilgiu. Polinomų daugyba komutatyvi, nes žiedo A elementų daugyba komutatyvi. Lieka įsitikinti, kad polinomų sudėtis ir daugyba yra susijusios distributyvumo dėsniu

$$(f(x) + g(x)) \cdot h(x) = f(x) \cdot h(x) + g(x) \cdot h(x), \quad f(x),\ g(x),\ h(x) \in A[x].$$

Iš tikrųjų, nagrinėkime polinomus

$$f(x) = \sum_{j \geq 0} a_j x^j, \quad g(x) = \sum_{j \geq 0} b_j x^j, \quad h(x) = \sum_{j \geq 0} c_j x^j.$$

Tuomet

$$\begin{aligned}(f(x) + g(x)) \cdot h(x) &= \sum_{j \geq 0} \Big(\sum_{\substack{r+s=j \\ r,s \geq 0}} (a_r + b_r) \cdot c_s \Big) x^j = \sum_{j \geq 0} \Big(\sum_{\substack{r+s=j \\ r,s \geq 0}} (a_r \cdot c_s + b_r \cdot c_s) \Big) x^j \\ &= \sum_{j \geq 0} \Big(\sum_{\substack{r+s=j \\ r,s \geq 0}} a_r \cdot c_s \Big) x^j + \sum_{j \geq 0} \Big(\sum_{\substack{r+s=j \\ r,s \geq 0}} b_r \cdot c_s \Big) x^j = f(x) \cdot h(x) + g(x) \cdot h(x).\end{aligned}$$

□

6.8.8 apibrėžimas. $(A[x], +, \cdot)$ yra vadinamas kintamojo x *polinomų žiedu* su koeficientais žiede A.

6.8.9 teiginys. *Jei žiedas $(A, +, *)$ neturi nulio daliklių, tai ir polinomų žiedas $A[x]$ neturi nulio daliklių.*

Įrodymas. Sakykime,

$$f(x) = \sum_{j \geq 0}^{n} a_j x^j \quad \text{ir} \quad g(x) = \sum_{j \geq 0}^{m} b_j x^j$$

yra atitinkamai n-tojo ir m-tojo laipsnių polinomai (t. y. $a_n \neq 0$ ir $b_m \neq 0$) su koeficientais žiede A. Tuomet

$$\begin{aligned}f(x) \cdot g(x) &= (a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) \cdot (b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0) \\ &= a_n * b_m x^{n+m} + (a_n * b_{m-1} + a_{n-1} * b_m) x^{n+m-1} + \cdots + a_0 * b_0.\end{aligned}$$

Kadangi $a_n \neq 0$ ir $b_m \neq 0$, tai $a_n * b_m \neq 0$ (nes žiedas A neturi nulio daliklių). Vadinasi, jei $f(x) \neq 0$, $g(x) \neq 0$, tai ir $f(x) \cdot g(x) \neq 0$. □

6.8.10 išvada. *Jei žiedas $(A, +, *)$ neturi nulio daliklių ir polinomai $f(x), g(x) \in A[x]$, tai*
$$\deg\left(f(x) \cdot g(x)\right) = \deg f(x) + \deg g(x).$$

6.8.11. Polinomų dalumo sąvoka yra dalumo sąvokos žiede atskiras atvejis.

6.8.12 apibrėžimas. Tarkime, kad $f(x), g(x) \in A[x]$. Sakysime polinomas $g(x)$ *dalija* polinomą $f(x)$ (arba polinomas $g(x)$ yra polinomo $f(x)$ *daliklis*) ir žymėsime $g(x)|f(x)$, jei egzistuoja toks polinomas $h(x) \in A[x]$, kad $f(x) = g(x) \cdot h(x)$.

6.8.13 teiginys. *Jei komutatyvus žiedas $(A, +, *)$ su vienetu 1 neturi nulio daliklių, tai kintamojo x polinomų žiedo $A[x]$ vieneto daliklių grupė $(A[x])^*$ sutampa su žiedo A vieneto daliklių grupe A^*.*

Įrodymas. Sakykime, $f(x) \in A[x]$ ir $f(x)|1$, t. y. egzistuoja toks $g(x) \in A[x]$, kad $f(x) \cdot g(x) = 1$. Remdamiesi šia lygybe, matome, kad $\deg f(x) + \deg g(x) = \deg 1 = 0$. Kadangi $\deg f(x) \geq 0$, $\deg g(x) \geq 0$, tai $\deg f(x) = 0$, t. y. $f(x) = a \in A$. Remdamiesi sąlyga $a|1$ gauname, kad $f(x) = a \in A^*$. Įrodėme: $(A[x])^* \subset A^*$. Įdėtis $A^* \subset (A[x])^*$ – akivaizdi. Taigi $(A[x])^* = A^*$. □

6.8.14. Dabar išnagrinėsime kintamojo x polinomų su koeficientais kūne k žiedą $k[x]$. Šio žiedo struktūra gana paprasta.

6.8.2 Dalybos su liekana formulė

Tegu k – kūnas. Kiekvienas šiame skyrelyje paminėtas polinomas priklauso žiedui $k[x]$.

6.8.15 teiginys. *Sakykime, kad $f(x), g(x) \in k[x]$, $g(x) \neq 0$ (nėra nulinis polinomas). Tada egzistuoja tokie vieninteliai polinomai $h(x)$ ir $r(x)$, priklausantys žiedui $k[x]$, kad*
$$f(x) = g(x) \cdot h(x) + r(x)$$
ir $\deg r(x) < \deg g(x)$.

Įrodymas. Tegu $n := \deg f(x)$ ir $m := \deg g(x)$. Jei $n < m$, tai imkime $h(x) = 0$, $r(x) = f(x)$. Tuomet dalybos su liekana formulę galime užrašyti taip: $f(x) = g(x) \cdot 0 + f(x)$, $\deg f(x) < \deg g(x)$.

Sakykime, kad $n \geq m$ ir
$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,\ a_n \neq 0,$$
$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0,\ b_m \neq 0.$$
Polinomą $g(x)$ padauginę iš $\frac{a_n}{b_m}x^{n-m}$ ir atėmę iš polinomo $f(x)$, gauname:
$$f(x) - g(x) \cdot \frac{a_n}{b_m}x^{n-m} = \left(a_{n-1} - \frac{a_n}{b_m} \cdot b_{m-1}\right) x^{n-1} + \cdots =: f_1(x).$$

Šią lygybę perrašykime taip:

$$f(x) = g(x) \cdot \frac{a_n}{b_m} x^{n-m} + f_1(x).$$

Polinomo $f_1(x)$ laipsnis nėra didesnis už $n-1$. Jei $\deg f_1(x) < m$, tai šiuo atveju polinomo $f(x)$ dalyba iš polinomo $g(x)$ baigta ir dalybos su liekana formulė atrodo taip:

$$f(x) = g(x) \cdot (c_1 x^{n-m}) + f_1(x), \quad c_1 = a_n/b_m.$$

Jei $\deg\ f_1(x) \geq m$, tai, panašiai kaip ir anksčiau, polinomą $f_1(x)$ dalijame iš polinomo $g(x)$ ir gauname lygybę:

$$f_1(x) = g(x) \cdot (c_2 x^{\deg\ f_1 - m}) + f_2(x), \ \ \deg\ f_2(x) < \deg\ f_1(x) < n.$$

Atlikę šiuos veiksmus, gauname:

$$f(x) = g(x) \cdot (c_1 x^{n-m} + c_2 x^{\deg\ f_1 - m}) + f_2(x).$$

Jei $\deg\ f_2(x) < m$, tai polinomo $f(x)$ dalyba iš polinomo $g(x)$ baigta. Jei $\deg\ f_2(x) \geq m$, tai, kaip ir anksčiau, polinomą $f_2(x)$ dalijame iš polinomo $g(x)$. Šį procesą tęsiame tol, kol gauname, kad liekanos laipsnis yra mažesnis už polinomo $g(x)$ laipsnį m. Taigi, po baigtinio žingsnių skaičiaus, gausime:

$$f(x) = g(x) \cdot h(x) + r(x), \ \ \deg\ r(x) < \deg\ g(x).$$

Lieka įrodyti, kad polinomai $h(x)$ ir $r(x)$ apibrėžiami vienareikšmiškai. Sakykime, kad $f(x) = g(x) \cdot h'(x) + r'(x)$, $\deg\ r'(x) < \deg\ g(x)$. Tuomet, iš lygybės $f(x) = g(x) \cdot h(x) + r(x)$ atėmę lygybę $f(x) = g(x) \cdot h'(x) + r'(x)$, gauname:

$$g(x) \cdot (h(x) - h'(x)) = r'(x) - r(x). \tag{6.6}$$

Tarkime, kad $h(x) - h'(x) \neq 0$. Tuomet $\deg\,(h(x) - h'(x)) \geq 0$ ir iš (6.6) lygybės, remdamiesi 6.8.10 išvada, gauname

$$\deg(r'(x) - r(x)) = \deg\big(g(x) \cdot (h(x) - h'(x))\big)$$
$$= \deg g(x) + \deg\big(h(x) - h'(x)\big) \geq \deg g(x) = m.$$

Tačiau polinomo $r'(x) - r(x)$ laipsnis griežtai mažesnis už m, nes $\deg r'(x) < m$ ir $\deg r(x) < m$. Prieštara! Taigi $h(x) = h'(x)$, o tada ir $r(x) = r'(x)$.

$\square$

6.8.16 apibrėžimas. Polinomas $f(x) \in k[x]$ vadinamas nenulinių polinomų $g_1(x)$, $g_2(x)$, …, $g_s(x) \in k[x]$ *didžiausiu bendruoju dalikliu* ir žymimas

$$\mathrm{dbd}\big(g_1(x), g_2(x), \ldots, g_s(x)\big),$$

jei

1. $f(x)|g_1(x)$, $f(x)|g_2(x)$, ..., $f(x)|g_s(x)$, t. y. polinomas $f(x)$ yra polinomų $g_1(x)$, $g_2(x)$, ..., $g_s(x)$ bendrasis daliklis;

2. Jei $h(x) \in k[x]$ – toks polinomas, kad $h(x)|g_1(x)$, $h(x)|g_2(x)$, ..., $h(x)|g_s(x)$, tai $h(x)|f(x)$.

6.8.17 teiginys. *Polinomų $g_1(x)$, $g_2(x)$, ..., $g_s(x)$ didžiausias bendrasis daliklis vienareikšmiškai apibrėžiamas daugiklio $\varepsilon \in k^*$ tikslumu.*

Įrodymas. Jei $f_1(x)$ ir $f_2(x)$ yra polinomų $g_1(x)$, $g_2(x)$, ..., $g_s(x)$ didžiausi bendrieji dalikliai, tai, remdamiesi polinomų $g_1(x)$, $g_2(x)$, ..., $g_s(x)$ didžiausio bendrojo daliklio apibrėžimu, gauname, kad $f_1(x)|f_2(x)$ ir $f_2(x)|f_1(x)$. Vadinasi, egzistuoja tokie $g_1(x) \in k[x]$ ir $g_2(x) \in k[x]$, kad $f_2(x) = f_1(x) \cdot h_1(x)$ ir $f_1(x) = f_2(x) \cdot h_2(x)$. Remdamiesi šiomis lygybėmis, gauname:

$$f_2(x) = f_1(x) \cdot h_1(x) = f_2(x) \cdot h_2(x) \cdot h_1(x)$$

arba $f_2(x) \cdot (1 - h_2(x) \cdot h_1(x)) = 0$. Kadangi žiedas $k[x]$ neturi nulio daliklių ir $f_2(x) \neq 0$, tai $h_1(x) \cdot h_2(x) = 1$, t. y. $h_1(x), h_2(x) \in k^*$. Pažymėję $h_2(x) = \varepsilon \in k^*$, gauname $f_1(x) = \varepsilon \cdot f_2(x)$. □

6.8.18. Dviejų nenulinių polinomų didžiausią bendrąjį daliklį galima rasti pasitelkus *Euklido algoritmą.* Sakykime, nenuliniai polinomai $f_1(x), f_2(x) \in k[x]$. Remdamiesi dalybos su liekana formule, galime parašyti lygybes:

$$\begin{array}{rll}
f_1(x) & = f_2(x) \cdot h_2(x) + f_3(x), & \deg f_3(x) < \deg f_2(x), \\
f_2(x) & = f_3(x) \cdot h_3(x) + f_4(x), & \deg f_4(x) < \deg f_3(x), \\
f_3(x) & = f_4(x) \cdot h_4(x) + f_5(x), & \deg f_5(x) < \deg f_4(x), \\
\dots & \dots & \dots \\
f_{m-3}(x) & = f_{m-2}(x) \cdot h_{m-2}(x) + f_{m-1}(x), & \deg f_{m-1}(x) < \deg f_{m-2}(x), \\
f_{m-2}(x) & = f_{m-1}(x) \cdot h_{m-1}(x) + f_m(x), & \deg f_m(x) < \deg f_{m-1}(x), \\
f_{m-1}(x) & = f_m(x) \cdot h_m(x) + 0. &
\end{array}$$

Paskutinė, nelygi nuliui, liekana $f_m(x)$ ir yra polinomų $f_1(x)$ ir $f_2(x)$ didžiausias bendrasis daliklis. Tai įrodysime. Polinomas $f_m(x)$ dalija polinomą f_{m-1}. Remdamiesi priešpaskutine lygybe, matome, kad $f_m(x)$ dalija polinomą f_{m-2}. Kildami parašytomis lygybėmis aukštyn, gauname, kad $f_m(x)$ dalija polinomus $f_{m-3}(x)$, $\dots$, $f_2(x)$ ir $f_1(x)$. Jei polinomas $h(x)$ dalija polinomus $f_1(x)$ ir $f_2(x)$, tai, remdamiesi pirmąja lygybe, matome, kad $f_1(x)$ dalija $f_3(x)$. Leisdamiesi lygybėmis žemyn, gausime, kad $f_1(x)$ dalija ir $f_m(x)$. Taigi $f_m(x)$ yra polinomų $f_1(x)$ ir $f_2(x)$ didžiausias bendrasis daliklis.

6.8.19 apibrėžimas. Polinomai $g_1(x)$, $g_2(x)$, $\dots$, $g_s(x)$ vadinami *tarpusavyje pirminiais*, jei jų didžiausias bendrasis daliklis yra lygus 1.

6.8.20 išvada. *Jei polinomų $f_1(x)$ ir $f_2(x)$, priklausančių žiedui $k[x]$, didžiausias bendrasis daliklis yra $d(x)$, tai egzistuoja tokie žiedo $k[x]$ polinomai $g_1(x)$ ir $g_2(x)$, kad*

$$d(x) = f_1(x) \cdot g_1(x) + f_2(x) \cdot g_2(x).$$

Įrodymas. Polinomams $f_1(x)$ ir $f_2(x)$ pritaikę Euklido algoritmą, gauname:

$$\begin{array}{ll}
f_1(x) = f_2(x) \cdot h_2(x) + f_3(x), & \deg f_3(x) < \deg f_2(x),\\
f_2(x) = f_3(x) \cdot h_3(x) + f_4(x), & \deg f_4(x) < \deg f_3(x),\\
f_3(x) = f_4(x) \cdot h_4(x) + f_5(x), & \deg f_5(x) < \deg f_4(x),\\
\dots \quad \dots & \dots\\
f_{m-3}(x) = f_{m-2}(x) \cdot h_{m-2}(x) + f_{m-1}(x), & \deg f_{m-1}(x) < \deg f_{m-2}(x),\\
f_{m-2}(x) = f_{m-1}(x) \cdot h_{m-1}(x) + f_m(x), & \deg f_m(x) < \deg f_{m-1}(x),\\
f_{m-1}(x) = f_m(x) \cdot h_m(x) + 0. &
\end{array}$$

Kaip žinome, $f_m(x)$ yra polinomų $f_1(x)$ ir $f_2(x)$ didžiausias bendrasis daliklis, t. y. $d(x) = \varepsilon f_m(x)$. Iš priešpaskutinės Euklido algoritmo lygybės gauname:

$$f_m(x) = f_{m-2}(x) - f_{m-1}(x) \cdot h_{m-1}(x).$$

Į šią lygybę įrašę polinomo f_{m-1} išraišką, gautą iš Euklido algoritmo aukščiau esančios lygybės, gauname:

$$\begin{aligned}
f_m(x) &= f_{m-2}(x) - (f_{m-3}(x) - f_{m-2}(x) \cdot h_{m-2}(x)) \cdot h_{m-1}(x)\\
&= -f_{m-3}(x) \cdot h_{m-1}(x) + f_{m-2}(x) \cdot (1 + h_{m-2}(x) \cdot h_{m-1}(x)).
\end{aligned}$$

Į šią lygybę įrašę polinomo $f_{m-2}(x)$ išraišką polinomais f_{m-3} ir f_{m-4}, gausime polinomo $f_m(x)$ išraišką polinomais f_{m-3} ir f_{m-4}. Darydami tokius pertvarkymus ir toliau, galų gale gausime $f_m(x)$ išraišką polinomais $f_1(x)$ ir $f_2(x)$:

$$f_m(x) = f_1(x) \cdot g_1'(x) + f_2(x) \cdot g_2'(x).$$

Remdamiesi šia lygybe, gauname:

$$d(x) = \varepsilon \cdot (f_1(x) \cdot g_1'(x) + f_2(x) \cdot g_2'(x)) = f_1(x) \cdot g_1(x) + f_2(x) \cdot g_2(x),$$

čia $g_1(x) = \varepsilon \cdot g_1'(x)$, $g_2(x) = \varepsilon \cdot g_2'(x)$. □

6.8.3 Polinomų šaknys

6.8.21 apibrėžimas. Tarkime, $(A, +, \cdot)$ – komutatyvus žiedas su vienetu 1, $a \in A$. Tegu polinomas $p(x) \in A[x]$, $p(x) = c_n x^n + \cdots + c_1 x + c_0$. Žiedo A elementas

$$c_n a^n + c_{n-1} a^{n-1} + \cdots + c_1 a + c_0$$

vadinamas *polinomo* $p(x)$ *reikšme* taške a ir žymimas $p(a)$. Elementas $a \in A$ vadinamas nenulinio polinomo $p(x) \in A[x]$ *šaknimi žiede* A, jei $p(a) = 0$.

6.8.22 pavyzdys. Skaičius 2 yra polinomo $p(x) = x^2-5x+6$ šaknis, nes $p(2) = 0$. Polinomas $x^2-2 \in \mathbb{Q}[x]$ neturi šaknų kūne $\mathbb{Q}$. Iš tikrųjų, jei x^2-2 turėtų racionalią šaknį $r \in \mathbb{Q}$, tai būtų teisinga lygybė $r^2 - 2 = 0$, todėl $\sqrt{2} = \pm r$, t. y. skaičius $\sqrt{2}$ būtų racionalus. Tačiau $\sqrt{2} \notin \mathbb{Q}$. Tuo tarpu kūne $\mathbb{R}$ polinomas $x^2 - 2$ turi dvi skirtingas šaknis: $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

6.8.23 teiginys. *Tarkime, kad k – kūnas, polinomas $p(x) \in k[x]$ ir $a \in k$. Tuomet egzistuoja toks polinomas $q(x) \in k[x]$, kad*

$$p(x) = q(x)(x - a) + p(a).$$

Įrodymas. Pritaikę 6.8.15 teiginį polinomams $p(x)$ ir $x - a$, gauname, kad egzistuoja toks polinomas $q(x) \in k[x]$ ir elementas $r \in k$, kad

$$p(x) = q(x)(x - a) + r. \tag{6.7}$$

Šioje lygybėje, sulyginę polinomų $p(x)$ ir $q(x)(x-a)+r$ reikšmes taške a, gauname $r = p(a)$. □

6.8.24 (Hornerio schema)**.** Dalijant polinomą iš pirmojo laipsnio polinomo $x - a$ (t. y. ieškant (6.7) išraiškos) patogu naudoti vadinamąją *Hornerio schemą.* Taigi tarkime, kad polinomą $p(x) \in k[x]$ (k – kūnas) reikia padalinti su liekana iš polinomo $x - a$, $a \in k$, t. y. ieškome tokio polinomo $q(x) \in k[x]$ ir tokio elemento $r \in k$, kad

$$p(x) = q(x)(x - a) + r.$$

Sakykime, kad

$$p(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$$

ir

$$q(x) = b_{n-1}\, x^{n-1} + b_{n-2}\, x^{n-2} + \ldots + b_1\, x + b_0.$$

Polinomų $p(x)$ ir $q(x)$ koeficientus surašome į lentelę:

	a_n	a_{n-1}	a_{n-2}	$\cdots$	a_1	a_0
a	b_{n-1}	b_{n-2}	b_{n-3}	$\cdots$	b_0	r

Koeficientai b_j ir r randami iš rekurentinių formulių:

$$b_{n-1} = a_n,$$

$$b_j = a \cdot b_{j+1} + a_{j+1}, \quad 0 \le j \le n - 2,$$

$$r = a \cdot b_0 + a_0.$$

6.8.25 pavyzdys. Polinomą $x^4 + x^3 - 2x^2 + 3x + 2$ padalinsime su liekana iš polinomo $x + 1$.

Sprendimas. Pagal Hornerio schemą užpildome lentelę:

	1	1	-2	3	2
-1	1	0	-2	5	-3

Taigi

$$x^4 + x^3 - 2x^2 + 3x + 2 = (x^3 - 2x + 5)(x + 1) - 3.$$

□

6.8.26 pavyzdys. Polinomą $x^4 + x^3 - 2x^2 + 3x + 2$ padalinsime su liekana iš polinomo $x + 1$.

Sprendimas. Pagal Hornerio schemą užpildome lentelę:

	1	0	2	-1	0	-1	3	2
2	1	2	6	11	22	43	89	180

Taigi

$$x^7 + 2x^5 - x^4 - x^2 + 3x + 2 = (x^6 + 2x^5 + 6x^4 + 11x^3 + 22x^2 + 43x + 89)(x - 2) + 180.$$

□

6.8.27 išvada (Bezu teorema)**.** *Sakykime, kad k – kūnas. Elementas $a \in k$ yra nenulinio polinomo $p(x) \in k[x]$ šaknis tada ir tik tada, kai $x - a \mid p(x)$.*

Įrodymas. *Būtinumas.* Tarkime, kad elementas $a \in k$ yra polinomo $p(x) \in k[x]$ šaknis. Remiantis 6.8.23 teiginiu, egzistuoja toks polinomas $q(x) \in k[x]$, kad $p(x) = q(x)(x - a) + p(a) = q(x)(x - a)$. Taigi $x - a \mid p(x)$.

Pakankamumas. Sakykime, kad $x - a \mid p(x)$. Tuomet egzistuoja toks polinomas $q(x) \in k[x]$, kad $p(x) = q(x)(x - a)$. Sulyginę polinomų $p(x)$ ir $q(x)(x - a)$ reikšmes taške a, gauname $p(a) = 0$, t. y. elementas a yra polinomo $p(x)$ šaknis. □

6.8.28 apibrėžimas. Tarkime, kad k – kūnas, $m \in \mathbb{N}$. Elementas $a \in k$ vadinamas nenulinio polinomo $p(x) \in k[x]$ *m-tojo kartotinumo šaknimi*, jei polinomas $p(x)$ dalijasi iš polinomo $(x - a)^m$, bet nesidalija iš polinomo $(x - a)^{m+1}$. Polinomo $p(x)$ 1-ojo kartotinumo šaknys vadinamos *paprastosiomis*, o šaknys, kurių kartotinumas yra mažiausiai 2, vadinamos *kartotinėmis šaknimis*.

6.8.29 pavyzdys. Skaičius 3 yra polinomo $p(x) = x^3 - 5x^2 + 3x + 9 \in \mathbb{Q}[x]$ 2-ojo kartotinumo šaknis, nes $(x - 3)^2 \mid p(x)$ ir $(x - 3)^3 \nmid p(x)$. O skaičius -1 yra šio polinomo paprastoji šaknis, nes $x + 1 \mid p(x)$ ir $(x + 1)^2 \nmid p(x)$.

6.8.30. Iš 6.8.28 apibrėžimo matyti, kad elementas $a \in k$ yra nenulinio polinomo $p(x) \in k[x]$ m-tojo kartotinumo šaknis tada ir tik tada, kai $p(x) = (x-a)^m g(x)$ ir $x - a \nmid g(x)$. Paskutinė sąlyga, remiantis Bezu teorema (žr. 6.8.27 išvadą), ekvivalenti sąlygai $g(a) \neq 0$.

6.8.31 teorema. *Tarkime, kad k – kūnas, $p(x) \in k[x]$ – nenulinis polinomas, o elementai a_1, a_2, ..., $a_r \in k$ yra šio polinomo skirtingos šaknys, kurių kartotinumai atitinkamai yra m_1, m_2, ..., m_r. Tuomet žiede $k[x]$ egzistuoja toks polinomas $g(x)$, kad*

$$p(x) = (x-a_1)^{m_1}(x-a_2)^{m_2}\cdots(x-a_r)^{m_r}g(x)$$

ir $g(a_j) \neq 0$, $j = 1, 2, \ldots, r$.

Įrodymas. Įrodysime matematinės indukcijos būdu pagal r. Kai $r = 1$, teoremos tvirtinimas išplaukia iš kartotinės šaknies apibrėžimo (žr. 6.8.30 pastraipą). Tarkime, kad teorema teisinga, kai $r = t-1$, $t \geq 2$. Įrodysime, jog teorema teisinga kai, $r = t$. Nagrinėkime nenulinį polinomą $p(x) \in k[x]$. Sakykime, kad elementai a_1, a_2, ..., $a_t \in k$ yra šio polinomo skirtingos šaknys, kurių kartotinumai atitinkamai yra m_1, m_2, ..., m_t. Remiantis indukcijos prielaida (taikoma polinomui $p(x)$ ir jo šaknims a_1, a_2, ..., a_{t-1}), egzistuoja toks polinomas $h(x) \in k[x]$, kad

$$p(x) = (x-a_1)^{m_1}(x-a_2)^{m_2}\cdots(x-a_{t-1})^{m_{t-1}}h(x) \tag{6.8}$$

ir $h(a_j) \neq 0$, $j = 1, 2, \ldots, t-1$. Lieka įrodyti, kad

$$(x-a_t)^{m_t} \mid h(x) \;\text{ ir }\; (x-a_t)^{m_t+1} \nmid h(x).$$

Kadangi $c_t - c_1 \neq 0$, $c_t - c_2 \neq 0$, ..., $c_t - c_{t-1} \neq 0$, tai polinomas

$$(x-a_1)^{m_1}(x-a_2)^{m_2}\cdots(x-a_{t-1})^{m_{t-1}} \tag{6.9}$$

nesidalija iš polinomo $x - a_t$. Vadinasi, (6.9) polinomas ir polinomas $(x-a_t)^{m_t}$ yra tarpusavyje pirminiai, todėl, remiantis 6.8.20 išvada, egzistuoja tokie polinomai $u(x)$, $v(x) \in k[x]$, kad

$$u(x)(x-a_1)^{m_1}(x-a_2)^{m_2}\cdots(x-a_{t-1})^{m_{t-1}} + v(x)(x-a_t)^{m_t} = 1.$$

Iš (6.8) lygybės ir iš paskutinės lygybės, padaugintos iš $h(x)$, gauname

$$u(x)p(x) + v(x)(x-a_t)^{m_t}h(x) = h(x). \tag{6.10}$$

Kadangi polinomo $p(x)$ šaknies a_t kartotinumas yra m_t, tai $(x-a_t)^{m_t} \mid p(x)$, todėl (6.10) lygybės kairėje pusėje esantis polinomas dalijasi iš $(x-a_t)^{m_t}$. Vadinasi, ir dešinėje šios lygybės pusėje esantis polinomas $h(x)$ dalijasi iš $(x-a_t)^{m_t}$. Taigi egzistuoja toks polinomas $g(x) \in k[x]$, kad $h(x) = (x - a_t)^{m_t} g(x)$ ir $g(a_j) \neq 0$, $j = 1, 2, \dots, t-1$. Tada (6.8) lygybę galime perrašyti

$$p(x) = (x - a_1)^{m_1}(x - a_2)^{m_2} \cdots (x - a_t)^{m_t} g(x).$$

Belieka pažymėti, kad $g(a_t) \neq 0$, nes priešingu atveju polinomo $p(x)$ šaknies a_t kartotinumas būtų didesnis už m_t. Įrodėme teoremą, kai $r = t$, todėl, remiantis indukcijos principu, teorema teisinga kiekvienam $r \in \mathbb{N}$. □

6.8.32 išvada. *Tarkime, kad k – kūnas, $n \in \mathbb{N}$. Kiekvienas n-tojo laipsnio polinomas $p(x) \in k[x]$ turi ne daugiau kaip n šaknų (kiekviena šaknis skaičiuojama tiek kartų koks jos kartotinumas) kūne k.*

Įrodymas. Tarkime, kad elementai a_1, a_2, …, $a_r \in k$ yra polinomo $p(x)$ skirtingos šaknys, kurių kartotinumai atitinkamai yra m_1, m_2, …, m_r. Remiantis 6.8.31 teorema, egzistuoja toks polinomas $g(x) \in k[x]$, kad

$$p(x) = (x - a_1)^{m_1}(x - a_2)^{m_2} \cdots (x - a_r)^{m_r} g(x).$$

Iš šios lygybės, remdamiesi 6.8.10 išvada, gauname

$$\deg p(x) = m_1 + m_2 + \cdots + m_r + \deg g(x). \tag{6.11}$$

Kadangi polinomo $p(x)$ laipsnis $n \geq 1$, tai polinomas $g(x)$ nenulinis, todėl jo laipsnis $\deg g(x) \geq 0$. Taigi iš (6.11) lygybės išplaukia

$$m_1 + m_2 + \cdots + m_r \leq \deg p(x) = n.$$

□

6.8.33 išvada. *Tarkime, kad k – kūnas, $n \in \mathbb{N}$, o $p(x), q(x) \in k[x]$ – polinomai, kurių laipsniai $\leq n$. Jei egzistuoja skirtingi kūno k elementai a_1, a_2, …, a_{n+1}, kuriuose polinomų $p(x)$ ir $q(x)$ reikšmės sutampa, tai šie polinomai yra lygūs.*

Įrodymas. Tarkime, kad polinomai $p(x)$ ir $q(x)$ nėra lygūs. Nagrinėkime nenulinį polinomą $h(x) := p(x) - q(x)$. Šio polinomo laipsnis ne didesnis už n, nes $\deg p(x) \leq n$ ir $\deg q(x) \leq n$. Be to,

$$h(a_1) = h(a_2) = \cdots = h(a_{n+1}) = 0,$$

t. y. polinomas $h(x)$, kurio laipsnis $\leq n$, turi $n+1$ skirtingą šaknį kūne k. Tačiau, remiantis 6.8.32 išvada, polinomas $h(x)$ negali turėti daugiau kaip n šaknų kūne k. Prieštara. Vadinasi, $h(x)$ – nulinis polinomas, t. y. polinomai $p(x)$ ir $q(x)$ yra lygūs. □

6.8.34 pastaba. Galima būtų įrodyti 6.8.31 teoremą ir 6.8.32 ir 6.8.33 išvadas bendresniu atveju – kūną k pakeitus bet kokia sveikumo sritimi (t. y. komutatyviu žiedu su vienetu be nulio daliklių) A. Tačiau minėti teiginiai nebus teisingi, jei kūną k pakeisime bet kokiu žiedu. Pavyzdžiui, polinomas $p(x) := x^3 \in \mathbb{Z}_8[x]$ turi keturias skirtingas šaknis kūne $\mathbb{Z}_8$: $p(0) = p(2) = p(4) = p(6) = 0$.

6.8.35 išvada (Lagranžo interpoliacinė formulė)**.** *Tarkime, kad k – kūnas, a_0, a_1, a_2, ..., a_n, b_0, b_1, b_2, ..., $b_n \in k$ ir elementai a_0, a_1, a_2, ..., a_n – skirtingi. Tuomet egzistuoja vienintelis polinomas $p(x) \in k[x]$, $\deg p(x) \leq n$, tenkinantis sąlygą*

$$p(a_j) = b_j, \quad j = 0, 1, 2, \ldots, n. \tag{6.12}$$

Šis polinomas turi išraišką

$$p(x) = \sum_{j=0}^{n} b_j \frac{(x - a_1) \cdots (x - a_{j-1})\,(x - a_{j+1}) \cdots (x - a_n)}{(a_j - a_1) \cdots (a_j - a_{j-1})(a_j - a_{j+1}) \cdots (a_j - a_n)}. \tag{6.13}$$

Įrodymas. Nesunku įsitikinti, kad (6.13) polinomas tenkina (6.12) sąlygą. Vienatis išplaukia iš 6.8.33 išvados. □

6.8.36 teiginys (Vijeto formulės)**.** *Tarkime, kad kūno k elementai a_1, a_2, ..., a_n (nebūtinai skirtingi) yra n-tojo laipsnio polinomo*

$$p(x) = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0 \in k[x]$$

šaknys:

$$p(x) = c_n (x - a_1)(x - a_2) \cdots (x - a_n).$$

Tuomet

$$\begin{aligned} a_1 + a_2 + \cdots + a_n &= -\frac{c_{n-1}}{c_n}, \\ \ldots \qquad \ldots & \qquad \ldots \\ \sum_{i_1 < i_2 < \cdots < i_r} a_{i_1} a_{i_2} \cdots a_{i_r} &= (-1)^r \frac{c_{n-r}}{c_n}, \\ \ldots \qquad \ldots & \qquad \ldots \\ a_1 a_2 \cdots a_n &= (-1)^n \frac{c_0}{c_n}. \end{aligned} \tag{6.14}$$

Įrodymas. (6.14) formulės gaunamos sudauginus narius polinomo $p(x)$ išraiškoje

$$c_n (x - a_1)(x - a_2) \cdots (x - a_n)$$

ir koeficientus prie x laipsnių sulyginus su atitinkamais koeficientais išraiškoje

$$c_n x^n + c_{n-1} x^{n-1} + \cdots + c_0.$$

Paliekame skaitytojui tuo įsitikinti. □

6.8.4 Polinomo išvestinė

6.8.37 apibrėžimas. Tarkime, kad k – kūnas, $n \in \mathbb{N}$. Tegu $p(x) \in k[x]$ – n-tojo laipsnio polinomas,

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Polinomo $p(x)$ *išvestine* vadinamas polinomas

$$p'(x) := na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1. \tag{6.15}$$

Jei $\deg p(x) \leq 0$, tai apibrėžkime $p'(x) := 0$, t. y. polinomo, kurio laipsnis ≤ 0, išvestinė yra nulinis polinomas.

6.8.38 teiginys. *Jei* $p(x),\ q(x) \in k[x]$, $\alpha, \beta \in k$, *tai*

$$\big(\alpha p + \beta q\big)' = \alpha p' + \beta q'; \tag{6.16}$$

$$\big(pq\big)' = p'q + pq'. \tag{6.17}$$

Įrodymas. (6.16) lygybė išplaukia iš (6.15) ir polinomų sumos apibrėžimo. (6.17) lygybės įrodymą, pasinaudojus (6.16) lygybe ir polinomų sandaugos apibrėžimu, galima redukuoti iki atvejo $p(x) = x^n$, $q(x) = x^m$:

$$\begin{aligned}(x^n x^m)' = (x^{n+m})' = (n+m)x^{n+m-1} &= (nx^{n-1})x^m + (mx^{m-1})x^n \\ &= (x^n)'x^m + x^n(x^m)'.\end{aligned}$$

□

Dabar apibrėšime aukštesnės eilės polinomo išvestines.

6.8.39 apibrėžimas. Polinomas $\big(p'(x)\big)'$ vadinamas polinomo $p(x)$ *antrosios eilės išvestine* ir žymimas $p''(x)$ arba $p^{(2)}(x)$. Indukcijos būdu apibrėžiama polinomo $p(x)$ *n-tosios eilės išvestinė*:

$$p^{(n)}(x) := \big(p^{(n-1)}(x)\big)', \quad n \in \mathbb{N},$$

$$p^{(0)}(x) := p(x).$$

6.8.40 teiginys (Leibnico formulė)**.** *Bet kuriam natūraliajam skaičiui n ir bet kuriems polinomams $p(x)$ ir $q(x)$ teisinga lygybė*

$$\big(pq\big)^{(n)} = \sum_{j=0}^{n} \binom{n}{j} p^{(j)} q^{(n-j)}.$$

Įrodymas. Įrodyti paliekame skaitytojui. □

6.8.41 teorema. *Tarkime, kad k – kūnas. Elementas $a \in k$ yra nenulinio polinomo $p(x)$ kartotinė šaknis tada ir tik tada, kai $p(a) = p'(a) = 0$.*

Įrodymas. *Būtinumas.* Tarkime, kad elementas a yra polinomo $p(x)$ kartotinė šaknis. Tada $(x-a)^2 \mid p(x)$. Taigi egzistuoja toks polinomas $g(x) \in k[x]$, kad $p(x) = (x-a)^2 g(x)$. Tuomet $p(a) = 0$ ir polinomo $p(x)$ išvestinė

$$p'(x) = 2(x-a)g(x) + (x-a)^2 g'(x).$$

Vadinasi, $p(a) = p'(a) = 0$.

Pakankamumas. Tarkime, kad nenulinis polinomas $p(x)$ tenkina sąlygą $p(a) = p'(a) = 0$. Polinomą $p(x)$ padalinkime iš polinomo $(x-a)^2$ ir liekaną užrašykime pavidalu $Ax + B$, A, $B \in k$:

$$p(x) = (x-a)^2 g(x) + Ax + B, \tag{6.18}$$

čia $g(x) \in k[x]$. Tuomet polinomo $p(x)$ išvestinė

$$p'(x) = 2(x-a)g(x) + (x-a)^2 g'(x) + A.$$

Šioje lygybėje, paėmę $x = a$, gauname $A = p'(a) = 0$. Tuomet (6.18) lygybėje, paėmę $x = a$, gauname $B = p(a) = 0$. Taigi iš (6.18) lygybės matome, kad polinomas $p(x)$ dalijasi iš $(x-a)^2$. Vadinasi, elementas a yra polinomo $p(x)$ kartotinė šaknis. □

Kūnas vadinamas *nulinės charakteristikos kūnu*, jei jo vienetui e teisinga nelygybė $ne \neq 0$ su kiekvienu natūraliuoju $n \geq 1$. Pavyzdžiui, kūnai $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ yra nulinės charakteristikos kūnai. O kūnas $\mathbb{Z}_p$, p – pirminis, nėra nulinės charakteristikos, nes

$$p \cdot \overline{1} = \underbrace{\overline{1} + \overline{1} + \cdots + \overline{1}}_{p} = \overline{p} = \overline{0}.$$

Jei k – nulinės charakteristikos kūnas ir $p(x) \in k[x]$, tai

$$\deg p' = \deg p - 1.$$

Tačiau ši lygybė negalioja, kai k nėra nulinės charakteristikos kūnas. Pavyzdžiui, polinomo $x^9 + x^3 + 1 \in \mathbb{Z}_3[x]$ išvestinė

$$(x^9 + x^3 + 1)' = 9x^8 + 3x^2 = 0$$

yra nulinis polinomas.

6.8.42 teiginys (Teiloro formulė)**.** *Sakykime, kad k – nulinės charakteristikos kūnas. Bet kuriam n-tojo laipsnio polinomui $p(x) \in k[x]$ ir bet kuriam kūno k elementui a teisinga lygybė*

$$p(x) = p(a) + p'(a)(x-a) + \frac{p''(a)}{2!}(x-a)^2 + \cdots + \frac{p^{(n)}(a)}{n!}(x-a)^n. \tag{6.19}$$

Įrodymas. Įrodyti paliekame skaitytojui. $\square$

Polinomo $p(x)$ (6.19) išraiškos $x-a$ laipsniais patogu ieškoti naudojant Hornerio schemą.

6.8.43 pavyzdys. Užrašysime polinomą $x^5+2x^4+8x^3+6x^2+x+10$ dvinario $x+2$ laipsniais.

Sprendimas. Naudojame Hornerio schemą:

	1	2	8	6	1	10
-2	1	0	8	-10	21	-32
-2	1	-2	12	-34	89	
-2	1	-4	20	-74		
-2	1	-6	32			
-2	1	-8				
-2	1					

Nesunku įsitikinti, kad gautos lentelės įstrižainės skaičiai yra ieškomos išraiškos atitinkamų $x+2$ laipsnių koeficientai. Taigi

$$\begin{gathered}x^5+2x^4+8x^3+6x^2+x+10\\ =1\cdot(x+2)^5-8(x+2)^4+32(x+2)^3-74(x+2)^2+89(x+2)-32.\end{gathered}$$

$\square$

6.8.44 teorema. *Tarkime, kad k – nulinės charakteristikos kūnas, $m\in\mathbb{N}$. Elementas $a\in k$ yra nenulinio polinomo $p(x)\in k[x]$ m-tojo kartotinumo šaknis tada ir tik tada, kai*

$$p(a)=p'(a)=\cdots=p^{(m-1)}(a)=0 \quad \textit{ir} \quad p^{(m)}(a)\neq 0. \tag{6.20}$$

Įrodymas. *Būtinumas.* Kadangi elementas $a\in k$ yra polinomo $p(x)$ m-tojo kartotinumo šaknis, tai egzistuoja toks polinomas $g(x)\in k[x]$, kad

$$p(x)=(x-a)^m g(x) \quad \text{ir} \quad g(a)\neq 0.$$

Taigi $p^{(0)}(a)=p(a)=0$. Fiksuokime skaičių $r\in\{1,2,\ldots,m-1\}$. Įrodysime, kad $p^{(r)}(a)=0$. Iš tikrųjų, pritaikę Leibnico formulę (žr. 6.8.40 teiginį) polinomams $(x-a)^m$ ir $g(x)$, gauname

$$\begin{aligned}p^{(r)}(x)=\Big((x-a)^m\cdot g(x)\Big)^{(r)}&=\sum_{j=0}^{r}\binom{r}{j}\big((x-a)^m\big)^{(j)}g^{(r-j)}(x)\\ &=\sum_{j=0}^{r}\binom{r}{j}m(m-1)\cdots(m-j+1)\,(x-a)^{m-j}g^{(r-j)}(x).\end{aligned}\tag{6.21}$$

Kadangi $1 \le r < m$, tai (6.21) sumos kiekvienas polinomas dalijasi iš $x-a$, todėl ir polinomas $p^{(r)}(x)$ dalijasi iš $x-a$, t. y. $p^{(r)}(a)=0$. Be to, (6.21) lygybė taip pat galioja paėmus $r=m$:

$$\begin{aligned} p^{(m)}(x) = \sum_{j=0}^{m-1} \binom{r}{j} m \cdots (m-j+1)\,(x-a)^{m-j} g^{(r-j)}(x) \; + g(x) \\ = (x-a)h(x) + g(x), \end{aligned}$$

čia $h(x) \in k[x]$. Taigi $p^{(m)}(a) = g(a) \neq 0$.

Pakankamumas. Tarkime, kad polinomas $p(x) \in k[x]$ tenkina (6.20) sąlygą. Parašykime Teiloro formulę šiam polinomui (žr. 6.8.42 teiginį):

$$p(x) = p(a) + p'(a)(x-a) + \frac{p''(a)}{2!}(x-a)^2 + \cdots + \frac{p^{(n)}(a)}{n!}(x-a)^n,$$

čia $n = \deg p(x)$. Tuomet iš (6.20) sąlygos ir paskutinės lygybės gauname:

$$\begin{aligned} p(x) &= \frac{p^{(m)}(a)}{m!}(x-a)^m + \cdots + \frac{p^{(n)}(a)}{n!}(x-a)^n \\ &= (x-a)^m \cdot \Big(\frac{p^{(m)}(a)}{m!} + \frac{p^{(m+1)}(a)}{(m+1)!}(x-a) + \cdots + \frac{p^{(n)}(a)}{n!}(x-a)^{n-m}\Big). \end{aligned}$$

Paskutiniuose skliaustuose esantį polinomą pažymėkime $g(x)$. Tada galime parašyti $p(x) = (x-a)^m g(x)$. Be to, $g(a) = p^{(m)}(a)/m! \neq 0$. Vadinasi, elementas a yra polinomo $p(x)$ m-tojo kartotinumo šaknis. □

6.8.45 pavyzdys. Įrodysime, kad skaičius 2 yra polinomo

$$p(x) = x^4 - 5x^3 + 6x^2 + 4x - 8 \in \mathbb{R}[x]$$

trečiojo kartotinumo šaknis.

Sprendimas. Skaičiuojame išvestines:

$$p'(x) = 4x^3 - 15x^2 + 12x + 4,$$

$$p''(x) = 12x^2 - 30x + 12,$$

$$p'''(x) = 24x - 30.$$

Kadangi $p(2) = p'(2) = p''(2) = 0$ ir $p'''(2) \neq 0$, tai, remiantis 6.8.44 teorema, skaičius 2 yra polinomo $p(x)$ trečiojo kartotinumo šaknis. □

6.8.5 Pirminiai polinomai

6.8.46 apibrėžimas. Tarkime, $(A, +, \cdot)$ – komutatyvus žiedas su vienetu 1. Polinomas $p(x) \in A[x]$ vadinamas *pirminiu (neredukuojamu) virš žiedo* A, jei $p(x)$ neišskaidomas dviejų polinomų $f(x), g(x) \in A[x]$, kurių laipsniai mažesni už polinomo $p(x)$ laipsnį, sandauga $f(x) \cdot g(x)$. Kitaip tariant, polinomas $p(x)$ yra pirminis virš žiedo A, jei lygybė $p(x) = f(x) \cdot g(x)$, $f(x), g(x) \in A[x]$, yra galima tik tuo atveju, kai $p(x) = \varepsilon \cdot f(x)$, $g(x) = \varepsilon^{-1}$ arba $p(x) = \varepsilon \cdot g(x)$, $f(x) = \varepsilon^{-1}$, $\varepsilon \in A^*$. (Priminsime, kad A^* – žiedo A vieneto daliklių aibė.)

Taip pat sakoma, jog polinomas $p(x) \in A[x]$ yra *redukuojamas* virš žiedo A, jei jis nėra neredukuojamas, t. y. egzistuoja tokie polinomai $f(x), g(x) \in A[x]$, kad $p(x) = f(x)g(x)$, $\deg f(x) < \deg p(x)$ ir $\deg g(x) < \deg p(x)$.

Toliau nagrinėsime polinomus su koeficientais kūne k.

Jei kūnas k yra kūno K pokūnis, tai polinomų žiedas $k[x]$ yra žiedo $K[x]$ požiedis. Polinomas $p(x) \in k[x]$ pirminis virš kūno k gali nebūti pirminis virš kūno K, t. y. gali būti išskaidomas dviejų polinomų $f(x), g(x) \in K[x]$, $\deg f(x) < \deg p(x)$, $\deg g(x) < \deg p(x)$, sandauga $f(x) \cdot g(x)$.

Pavyzdžiui, polinomas $x^2 - 2 \in \mathbb{Q}[x]$ yra pirminis virš kūno $\mathbb{Q}$, nes $\sqrt{2} \notin \mathbb{Q}$ ir todėl šis polinomas nėra išskaidomas dviejų pirmojo laipsnio polinomų su racionaliais koeficientais sandauga. Bet šis polinomas nėra pirminis virš kūno $\mathbb{R}$ (arba virš kūno $\mathbb{Q}(\sqrt{2})$), nes $x^2 - 2 = (x - \sqrt{2}) \cdot (x + \sqrt{2})$.

6.8.47 teiginys. *Tarkime, kad $p(x)$ – antrojo arba trečiojo laipsnio polinomas su koeficientais iš kūno k. Polinomas $p(x)$ redukuojamas virš kūno k tada ir tik tada, kai jis turi šaknį šiame kūne.*

Įrodymas. *Būtinumas.* Tarkime, jog polinomas $p(x) \in k$ redukuojamas virš kūno k. Tuomet egzistuoja tokie teigiamo laipsnio polinomai $u(x)$, $v(x) \in k[x]$, kad $p(x) = u(x)v(x)$. Remdamiesi 6.8.10 išvada, galime parašyti

$$\deg u(x) + \deg v(x) = \deg p(x).$$

Kadangi polinomas $p(x)$ yra antrojo arba trečiojo laipsnio, tai bent vienas iš polinomų $u(x)$ arba $v(x)$ yra tiesinis, t. y. pirmojo laipsnio. Tarkime, jog $\deg u(x) = 1$. Tuomet $u(x) = ax + b$, čia a, $b \in k$, $a \neq 0$. Taigi elementas $-b/a$ yra polinomo $u(x)$ šaknis. Vadinasi, polinomas $p(x)$ turi šaknį kūne k.

Pakankamumas išplaukia iš Bezu teoremos (žr. 6.8.27 išvadą). $\square$

6.8.48 apibrėžimas. Polinomą $f(x) \in k[x]$ vadinsime *normuotu* (angl. *monic*), jei jo koeficientas prie aukščiausiojo x laipsnio yra lygus 1, t. y. jei $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, $n \geq 0$.

Nagrinėkime žiedą $k[x]$. Kaip ir bendruoju žiedų teorijos atveju, polinomus $f(x)$ ir $g(x)$ vadinsime ekvivalenčiais, jei $f(x) = \varepsilon \cdot g(x)$, $\varepsilon \in k^*$. Tarpusavyje ekvivalenčių polinomų aibėje $\{\varepsilon \cdot f(x) | \varepsilon \in k^*\}$ egzistuoja vienintelis normuotas polinomas. Jei

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0,$$

tai, polinomą $f(x)$ padauginę iš a_n^{-1}, gausime normuotą polinomą

$$a_n^{-1} \cdot f(x) = x^n + a_n^{-1} a_{n-1} x^{n-1} + \cdots + a_n^{-1} a_1 x + a_n^{-1} a_0,$$

priklausantį polinomo $f(x)$ ekvivalentumo klasei. Kalbėdami apie polinomų didžiausią bendrąjį daliklį apibrėžtumo dėlei galime turėti omenyje polinomų normuotą didžiausią bendrąjį daliklį.

Įrodysime labai svarbią pirminių polinomų $p(x) \in k[x]$ savybę.

6.8.49 teorema. *Jei žiedo $k[x]$ pirminis polinomas $p(x)$ dalija polinomų $f(x)$, $g(x) \in k[x]$ sandaugą $f(x) \cdot g(x)$, tai $p(x)$ dalija bent vieną iš polinomų: $f(x)$ ar $g(x)$.*

Įrodymas. Jei $p(x) | f(x)$, tai teoremos teiginys įrodytas. Jei $p(x) \nmid f(x)$, tai polinomų $p(x)$ ir $f(x)$ didžiausias bendrasis daliklis yra lygus 1. Vadinasi, egzistuoja tokie polinomai $u(x), v(x) \in k[x]$, kad $p(x) \cdot u(x) + f(x) \cdot v(x) = 1$. Padauginę šią lygybę iš $g(x)$, gauname: $p(x) \cdot u(x) \cdot g(x) + f(x) \cdot g(x) \cdot v(x) = g(x)$. Polinomas $p(x)$ dalija polinomą, esantį kairėje šios lygybės pusėje, vadinasi, $p(x)$ dalija ir $g(x)$. □

6.8.50 teorema. *Kiekvienas nenulinis polinomas $f(x) \in k[x]$ išskaidomas vieneto daliklio ir normuotų pirminių polinomų virš kūno k sandauga. Šis išskaidymas randamas vienareikšmiškai, jei dauginamųjų tvarka nesvarbi.*

Įrodymas. Visų pirma įrodysime, kad kiekvieną nenulinį polinomą $f(x) \in k[x]$ galima išskaidyti vieneto daliklio ir normuotų pirminių polinomų virš kūno k sandauga.

Nulinio laipsnio nenulinis polinomas yra vieneto daliklis. Šiuo atveju teiginys yra teisingas. Pirmojo laipsnio polinomą $a_1 x + a_0$, $a_1 \neq 0$, galime užrašyti taip: $a_1 x + a_0 = a_1(x + a_1^{-1} a_0)$. Tai ir yra polinomo $a_1 x + a_0$ skaidinys vieneto daliklio a_1 ir normuoto pirminio polinomo $x + a_1^{-1} a_0$ sandauga. Sakykime, teiginys yra įrodytas kiekvienam nenuliniam polinomui $f(x) \in k[x]$, kurio laipsnis yra mažesnis nei n. Įrodysime, kad ir kiekvienas n-tojo laipsnio polinomas yra išskaidomas vieneto daliklio ir normuotų pirminių polinomų virš kūno k sandauga. Imkime n-tojo laipsnio polinomą $f(x) \in k[x]$. Jei $f(x)$ yra pirminis virš kūno k, tai, iškėlę prieš skliaustus polinomo $f(x)$ koeficientą prie aukščiausiojo x laipsnio, gausime ieškomą polinomo $f(x)$ skaidinį. Jei $f(x)$ nėra pirminis virš kūno k, tai egzistuoja tokie $g(x), h(x) \in k[x]$, deg $g(x) <$ deg $f(x)$, deg $h(x) <$ deg $f(x)$, kad $f(x) = g(x) \cdot h(x)$. Polinomai $g(x), h(x)$ pagal prielaidą yra išskaidomi vieneto daliklio ir normuotų pirminių polinomų virš kūno k sandauga. Taigi tokia sandauga yra išskaidomas ir polinomas $f(x)$.

Dabar įrodysime skaidinio vienatį. Sakykime, kad

$$f(x) = \varepsilon \cdot p_1(x) \cdot p_2(x) \cdot \dots \cdot p_r(x) = \eta \cdot q_1(x) \cdot q_2(x) \cdot \dots \cdot q_s(x),$$

$\varepsilon, \eta \in k^*$, $p_1(x)$, $p_2(x)$, $\dots$, $p_r(x)$, $q_1(x)$, $q_2(x)$, $\dots$, $q_s(x)$ – normuoti pirminiai polinomai virš k. Reikia įrodyti, kad $r = s$, $\varepsilon = \eta$ ir egzistuoja toks skaičių $1, 2, \dots, r$ keitinys $j_1, j_2, \dots, j_r$, kad $p_1(x) = q_{j_1}(x)$, $p_2(x) = q_{j_2}(x)$, $\dots$, $p_r(x) = q_{j_r}(x)$.

Visiškai akivaizdu, kad $\varepsilon = \eta = a_n$ – polinomo $f(x)$ koeficientas prie aukščiausiojo x laipsnio. Polinomas $p_1(x)$ yra pirminis virš k ir

$$p_1(x) | q_1(x) \cdot q_2(x) \cdot \dots \cdot q_s(x).$$

Jei $p_1(x) \nmid q_1(x)$, tai, remdamiesi įrodyta pirminių polinomų savybe, gauname:

$$p_1(x) | q_2(x) \cdot \dots \cdot q_s(x).$$

Taip tęsdami toliau, po baigtinio žingsnių skaičiaus, gausime, kad $p_1(x) | q_{j_1}(x)$. Kadangi $p_1(x)$ ir $q_{j_1}(x)$ yra normuoti pirminiai polinomai virš k ir $p_1(x) | q_{j_1}(x)$, tai $p_1(x) = q_{j_1}(x)$. Polinomų žiedas $k[x]$ neturi nulio daliklių, vadinasi,

$$\varepsilon \cdot p_1(x) \cdot (p_2(x) \cdot \dots \cdot p_r(x) - q_1(x) \cdot q_2(x) \cdot \dots \cdot \hat{q}_{j_1}(x) \cdot \dots \cdot q_s(x)) = 0$$

tik tuo atveju, kai

$$p_2(x) \cdot \dots \cdot p_r(x) - q_1(x) \cdot q_2(x) \cdot \dots \cdot \hat{q}_{j_1}(x) \cdot \dots \cdot q_s(x) = 0,$$

t. y., kai

$$p_2(x) \cdot \dots \cdot p_r(x) = q_1(x) \cdot q_2(x) \cdot \dots \cdot \hat{q}_{j_1}(x) \cdot \dots \cdot q_s(x)$$

(stogelis virš polinomo rodo, kad to polinomo sandaugoje nėra). Baigti įrodyti teoremą galima matematinės indukcijos metodu, tarus, kad kiekvieno polinomo, kurio laipsnis yra mažesnis nei polinomo $f(x)$ laipsnis, skaidinio pirminiais polinomais vienatis įrodyta. □

6.8.51 apibrėžimas. Iš 6.8.50 teoremos matyti, kad kiekvieną nenulinį polinomą $p(x) \in k[x]$ vieninteliu būdu (jei nekreipsime dėmesio į dauginamųjų tvarką) galima išreikšti

$$p(x) = a \cdot p_1(x)^{n_1} p_2(x)^{n_2} \cdots p_m(x)^{n_m},$$

čia $a \in k^*$, o p_1, p_2, $\dots$, p_m – skirtingi normuoti pirminiai polinomai. Ši išraiška vadinama polinomo $p(x)$ *kanoniniu skaidiniu* (*kanonine išraiška*).

6.8.52 teorema. *Tegu k ir K – nulinės charakteristikos kūnai ir $k \subset K$. Jei polinomas $p(x) \in k[x]$ yra pirminis virš k, tai jis kūne K neturi kartotinių šaknų.*

Įrodymas. Tarkime, kad $p(x) \in k[x]$ – pirminis virš k polinomas. Kadangi k – nulinės charakteristikos kūnas, tai išvestinė $p'(x)$ yra nenulinis polinomas, kurio laipsnis mažesnis už polinomo $p(x)$ laipsnį. Taigi polinomai $p(x)$ ir $p'(x)$ yra tarpusavyje pirminiai, todėl, remiantis 6.8.20 išvada, egzistuoja tokie polinomai $u(x), v(x) \in k[x]$, kad

$$p(x)u(x) + p'(x)v(x) = 1. \tag{6.22}$$

Dabar tarkime, kad polinomas $p(x)$ turi kartotinę šaknį $a \in K$. Tada, remiantis 6.8.44 teorema, $p'(a) = 0$. Kadangi $k \subset K$, tai (6.22) lygybė galioja ir žiede $K[x]$. Įstatę $x = a$ į (6.22) lygybę, gauname $0 = 1$. Prieštara. □

6.8.53 pastaba. 6.8.52 teoremos įrodyme yra frazė „Įstatę $x = a$ į (6.22) lygybę, gauname …“ Šią frazę reikia suprasti taip: sulyginę kairėje ir dešinėje (6.22) lygybės pusėse esančių polinomų reikšmes taške $x = a$, gauname …

Pratimas. Tegu k ir K – kūnai ir $k \subset K$. Įsitikinkite, kad jei polinomai $f(x) \in k[x]$ ir $g(x) \in k[x]$ yra tarpusavyje pirminiai žiede $k[x]$, tai jie tarpusavyje pirminiai ir žiede $K[x]$.

6.8.6 Racionaliųjų trupmenų kūnas

Tegu k – kūnas. Remiantis 6.8.9 teiginiu, polinomų žiedas $k[x]$ yra sveikumo sritis (neturi nulio daliklių), todėl galima nagrinėti šio žiedo santykių kūną (žr. 6.1.26 pavyzdį), kuris šiuo atveju vadinamas kintamojo x *racionaliųjų trupmenų kūnu* virš k ir žymimas $k(x)$. Plačiau panagrinėsime šį kūną.

Racionaliųjų trupmenų kūno $k(x)$ elementai yra trupmenos

$$\frac{f(x)}{g(x)},$$

čia $f(x), g(x) \in k[x]$, $g(x)$ – nenulinis polinomas. Šios trupmenos vadinamos *racionaliosiomis trupmenomis*. Polinomas $f(x)$ vadinamas racionaliosios trupmenos $f(x)/g(x)$ *skaitikliu*, o polinomas $g(x)$ – šios trupmenos *vardikliu*. Priminsime (žr. 6.1.26 pavyzdį), kaip kūne $k(x)$ apibrėžta elementų lygybė, sudėtis ir daugyba:

$$\frac{f(x)}{g(x)} = \frac{f_1(x)}{g_1(x)} \iff f(x)g_1(x) = g(x)f_1(x),$$

$$\frac{f(x)}{g(x)} + \frac{f_1(x)}{g_1(x)} := \frac{f(x)g_1(x) + f_1(x)g(x)}{g(x)g_1(x)},$$

$$\frac{f(x)}{g(x)} \cdot \frac{f_1(x)}{g_1(x)} := \frac{f(x)f_1(x)}{g(x)g_1(x)}.$$

Be to, trupmena $f(x)/1$, $f(x) \in k[x]$, sutapatinama su polinomu $f(x)$. Tuomet žiedas $k[x]$ yra trupmenų kūno $k(x)$ požiedis.

Racionalioji trupmena $f(x)/g(x)$ vadinama *nesuprastinama*, jei polinomų $f(x)$ ir $g(x)$ didžiausias bendrasis daliklis lygus 1. Nesunku įsitikinti, kad bet kurią racionaliąją trupmeną galima išreikšti nesuprastinama trupmena (užtenka trupmenos skaitiklį ir vardiklį padalinti iš jų didžiausio bendrojo daliklio).

Racionalioji trupmena $f(x)/g(x)$ vadinama *taisyklingąja*, jei

$$\deg f(x) < \deg g(x).$$

6.8.54 teiginys. *Kiekviena racionalioji trupmena $f(x)/g(x) \in k(x)$ vieninteliu būdu išreiškiama polinomo ir taisyklingosios racionaliosios trupmenos suma.*

Įrodymas. Padalinkime trupmenos $f(x)/g(x)$ skaitiklį iš vardiklio su liekana:

$$f(x) = g(x)q(x) + r(x), \quad \deg r(x) < \deg g(x),$$

čia $q(x)$, $r(x) \in k[x]$. Tada trupmeną $f(x)/g(x)$ galime išreikšti polinomo $q(x)$ ir taisyklingosios trupmenos $r(x)/g(x)$ suma:

$$\frac{f(x)}{g(x)} = \frac{g(x)q(x) + r(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)}. \tag{6.23}$$

Įrodysime, kad ši išraiška randama vienareikšmiškai, t. y., jei

$$\frac{f(x)}{g(x)} = q_1(x) + \frac{r_1(x)}{g_1(x)}, \tag{6.24}$$

čia $q_1(x) \in k[x]$, o $r_1(x)/g_1(x)$ – taisyklingoji trupmena, tai

$$q(x) = q_1(x) \quad \text{ir} \quad \frac{r(x)}{g(x)} = \frac{r_1(x)}{g_1(x)}.$$

Iš tikrųjų, tarkime, kad racionaliosios trupmenos $f(x)/g(x)$ (6.23) ir (6.24) išraiškos yra skirtingos, t. y. $q(x) \neq q_1(x)$. Sulyginę abi šias išraiškas, gauname

$$q(x) - q_1(x) = \frac{r_1(x)}{g_1(x)} - \frac{r(x)}{g(x)} = \frac{r_1(x)g(x) - r(x)g_1(x)}{g(x)g_1(x)},$$

$$g(x)g_1(x)\big(q(x) - q_1(x)\big) = r_1(x)g(x) - r(x)g_1(x).$$

Šios lygybės kairėje pusėje esančio polinomo laipsnis ne mažesnis už polinomo $g(x)g_1(x)$ laipsnį (nes $q(x) \neq q_1(x)$), o dešinėje pusėje esančio polinomo laipsnis mažesnis už $\deg\big(g(x)g_1(x)\big)$, nes

$$\deg\big(r_1(x)g(x)\big) = \deg r_1(x) + \deg g(x) < \deg g_1(x) + \deg g(x) = \deg\big(g_1(x)g(x)\big)$$

ir

$$\deg\big(r(x)g_1(x)\big) = \deg r(x) + \deg g_1(x) < \deg g(x) + \deg g_1(x) = \deg\big(g_1(x)g(x)\big).$$

Prieštara! Taigi racionaliosios trupmenos $f(x)/g(x)$ (6.23) išraiška randama vienareikšmiškai. $\square$

6.8.55 apibrėžimas. Tegu k – kūnas. Taisyklingoji racionalioji trupmena

$$f(x)/g(x) \in k(x)$$

vadinama *paprastąja*, jei egzistuoja toks neredukuojamas virš k polinomas $p(x) \in k[x]$ ir toks polinomas $q(x) \in k[x]$, kad

$$\frac{f(x)}{g(x)} = \frac{q(x)}{p(x)^n},$$

$n \in \mathbb{N}$, ir $\deg q(x) < \deg p(x)$.

6.8.56 teorema. *Kiekviena taisyklingoji racionalioji trupmena vieninteliu būdu išreiškiama paprastųjų trupmenų suma.*

Įrodymas. Iš pradžių įrodysime egzistavimą, o tuomet – vienatį. Paprastumo dėlei toliau polinomą $p(x)$ žymėsime tiesiog p.

Egzistavimas. Tegu $f/g \in k(x)$ – taisyklingoji racionalioji trupmena, t. y. f, $g \in k[x]$ ir $\deg f < \deg g$. Sakykime, jog polinomas g išreiškiamas dviejų tarpusavyje pirminių polinomų g_1 ir $g_2 \in k[x]$ sandauga $g = g_1g_2$. Tuomet egzistuoja tokie polinomai u_1, $u_2 \in k[x]$, kad

$$u_1g_1 + u_2g_2 = 1.$$

Šios lygybės abi puses padauginame iš f:

$$fu_1g_1 + fu_2g_2 = f. \tag{6.25}$$

Polinomą fu_1 padalinkime su liekana iš polinomo g_2:

$$fu_1 = qg_2 + r_2, \qquad \deg r_2 < \deg g_2.$$

Šią išraišką įstatę į (6.25) lygybę, gauname

$$f = r_1g_2 + r_2g_1, \tag{6.26}$$

čia $r_1 := fu_2 + qg_1$. Įrodysime, kad $\deg r_1 < \deg g_1$. Iš tikrųjų,

$$\deg f < \deg g = \deg(g_1g_2) = \deg g_1 + \deg g_2.$$

Be to,

$$\deg(r_2 g_1) = \deg r_2 + \deg g_1 < \deg g_1 + \deg g_2.$$

Todėl

$$\begin{aligned}\deg r_1 + \deg g_2 = \deg(r_1 g_2) = \deg(f - r_2 g_1) \le \max\{\deg f, \deg(r_2 g_1)\} \\ < \deg g_1 + \deg g_2.\end{aligned}$$

Taigi $\deg r_1 < \deg g_1$.

Padaliję (6.26) lygybės abi puses iš $g_1 g_2$, gauname

$$\frac{f}{g} = \frac{f}{g_1 g_2} = \frac{r_1}{g_1} + \frac{r_2}{g_2}.$$

Abi šios lygybės dešiniojoje pusėje esančios trupmenos yra taisyklingosios, nes $\deg r_1 < \deg g_1$ ir $\deg r_2 < \deg g_2$. Jei kurios nors šių trupmenų vardiklis g_j išreiškiamas dviejų tarpusavyje pirminių polinomų sandauga $g_j = h_1 h_2$, tai galima pritaikyti anksčiau aprašytą samprotavimą ir išskaidyti šią trupmeną dviejų taisyklingųjų trupmenų, kurių vardikliai yra polinomai h_1 ir h_2, suma. Tęsdami šį procesą, rasime trupmenos f/g išraišką taisyklingųjų racionaliųjų trupmenų suma

$$\frac{f}{g} = \sum_{i=1}^{m} \frac{v_i}{p_i^{n_i}}, \tag{6.27}$$

čia $v_i, p_i \in k[x]$, $\deg v_i < \deg p_i^{n_i}$, o p_i – normuoti (vyriausiasis koeficientas $= 1$) pirminiai virš k polinomai, įeinantys į polinomo g kanoninį skaidinį:

$$g = \varepsilon \cdot p_1^{n_1} \cdot p_2^{n_2} \cdots p_m^{n_m}, \quad \varepsilon \in k.$$

Toliau įrodysime, kad taisyklingąją racionaliąją trupmeną $v/p^n \in k(x)$, $p \in k[x]$ – pirminis polinomas, $v \in k[x]$, $\deg v < \deg p^n$, galima išreikšti paprastųjų racionaliųjų trupmenų suma. Iš tikrųjų, dalindami polinomus su liekana, gauname

$$\begin{aligned} v &= q_1 p^{n-1} + r_1, \\ r_1 &= q_2 p^{n-2} + r_2, \\ \ldots &\quad \ldots \quad \ldots \\ r_{n-2} &= q_{n-1} p + r_{n-1}, \\ r_{n-1} &= q_n, \end{aligned}$$

čia $\deg r_i < \deg p^{n-i}$, $i = 1, 2, \ldots, n-1$. Nesunku įsitikinti, kad $\deg q_i < \deg p$, $i = 1, 2, \ldots, n$. Taigi

$$v = q_1 p^{n-1} + q_2 p^{n-2} + \cdots + q_{n-1} p + q_n.$$

Šios lygybės abi puses padaliję iš p^n, gauname racionaliosios trupmenos v/p^n išraišką paprasčiausių trupmenų suma

$$\frac{v}{p^n} = \frac{q_1}{p} + \frac{q_2}{p^2} + \cdots + \frac{q_{n-1}}{p^{n-1}} + \frac{q_n}{p^n}. \tag{6.28}$$

Vienatis. Dabar įrodysime, kad taisyklingosios trupmenos f/g išraiška paprastųjų trupmenų suma randama vienareikšmiškai. Iš tikrųjų, iš (6.27) ir (6.28) lygybių išplaukia, kad taisyklingąją racionaliąją trupmeną f/g galima išreikšti paprastųjų trupmenų suma

$$\frac{f}{g} = \sum_{i=1}^{m} \Big(\sum_{j=1}^{n_i} \frac{a_{ij}}{p_i^j} \Big), \tag{6.29}$$

čia a_{ij}, $p_i \in k[x]$, $\deg a_{ij} < \deg p_i$, o p_1, p_2, …, p_m – skirtingi normuoti pirminiai polinomai. Tarkime, kad trupmeną f/g dar vienu būdu galima išreikšti paprastųjų trupmenų suma:

$$\frac{f}{g} = \sum_{s=1}^{\mu} \Big(\sum_{t=1}^{\nu_s} \frac{b_{st}}{q_s^t} \Big), \tag{6.30}$$

čia b_{st}, $q_s \in k[x]$, $\deg b_{st} < \deg q_s$, o q_1, q_2, …, q_μ – skirtingi normuoti pirminiai polinomai. Dabar suvienodinsime (6.29) ir (6.30) užrašus: nagrinėkime visų (6.30) išraiškos trupmenų vardiklių aibę

$$\Big\{ q_s^t \Big\}.$$

Jei kokio nors šios aibės elemento q_s^t nepasitaiko tarp (6.29) išraiškos trupmenų vardiklių, tai (6.29) išraišką papildome trupmena $0/q_s^t$. Tą patį atliekame ir su (6.30) išraiška. Papildę, jei reikia, pirminių polinomų aibę

$$\{p_1, p_2, \ldots, p_m\}$$

naujais nariais p_{m+1}, …, p_M, (6.29) ir (6.30) išraiškas galime perrašyti atitinkamai

$$\frac{f}{g} = \sum_{i=1}^{M} \Big(\sum_{j=1}^{N_i} \frac{a_{ij}}{p_i^j} \Big), \tag{6.31}$$

ir

$$\frac{f}{g} = \sum_{i=1}^{M} \Big(\sum_{j=1}^{N_i} \frac{b_{ij}}{p_i^j} \Big), \tag{6.32}$$

čia a_{ij}, b_{ij}, $p_i \in k[x]$, $\deg a_{ij} < \deg p_i$, $\deg b_{ij} < \deg p_i$, o p_1, p_2, …, p_M – skirtingi normuoti pirminiai polinomai.

Tarkime, kad (6.31) ir (6.32) išraiškos yra skirtingos, t. y. aibės

$$\left\{\frac{a_{ij}}{p_i^j}\right\} \quad \text{ir} \quad \left\{\frac{b_{ij}}{p_i^j}\right\}$$

yra skirtingos. Nemažindami bendrumo tarkime, kad

$$\frac{a_{1u}}{p_1^u} \notin \left\{\frac{b_{st}}{q_s^t}\right\}, \tag{6.33}$$

čia $u \in \{1, 2, \ldots, n_1\}$. Be to, tegu u – didžiausias skaičius, kuriam teisingas (6.33) teiginys. Iš (6.31) lygybės atėmę (6.32) lygybę, gauname

$$\frac{c_1}{p_1} + \cdots + \frac{c_u}{p_1^u} + \sum_{i=2}^{M}\left(\sum_{j=1}^{N_i}\frac{a_{ij} - b_{ij}}{p_i^j}\right) = 0, \tag{6.34}$$

čia $c_j = a_{1j} - b_{1j}$, $j = 1, 2, \ldots, u$. Be to, $c_u \neq 0$. (6.34) lygybę padauginę iš $p_1^u \prod_{i=2}^{M} p_i^{N_i}$ ir surinkę visus gautos išraiškos narius, kurie dalijasi iš p_1, galime parašyti

$$c_u \prod_{i=2}^{M} p_i^{N_i} + p_1 P = 0, \tag{6.35}$$

čia $P \in k[x]$. Kadangi polinomai p_1 ir $\prod_{i=2}^{M} p_i^{N_i}$ yra tarpusavyje pirminiai, tai iš (6.35) lygybės matyti, jog polinomas c_u dalijasi iš p_1. Tačiau polinomo c_u laipsnis mažesnis už polinomo p_1 laipsnį, nes $c_u = a_{1u} - b_{1u}$ ir $\deg a_{1u} < \deg p_1$, $\deg b_{1u} < \deg p_1$. Taigi $c_u = 0$. Prieštara. □

6.8.57. Parodysime, kaip atskirti tiesinio daugiklio laipsnį $(x-a)^n$. Nagrinėkime racionaliąją trupmeną $f/g \in k(x)$. Tegu $g = (x-a)^n h$, $h \in k[x]$, $h(a) \neq 0$. Tada bet kuriam $b_n \in k$ teisinga lygybė

$$\frac{f}{g} = \frac{b_n}{(x-a)^n} + \frac{f - b_n h}{(x-a)^n h}. \tag{6.36}$$

Šioje lygybėje parenkame $b_n = f(a)/h(a)$. Tada $f(a) - b_n h(a) = 0$, todėl, remiantis Bezu teorema, $x - a \mid f - b_n h$. Taigi egzistuoja toks polinomas $f_1 \in k[x]$, kad

$$\frac{f - b_n h}{(x-a)^n h} = \frac{f_1}{(x-a)^{n-1} h}.$$

dabar (6.36) lygybę galime perrašyti

$$\frac{f}{g} = \frac{b_n}{(x-a)^n} + \frac{f_1}{(x-a)^{n-1} h}. \tag{6.37}$$

Pirmiau išdėstytą samprotavimą pritaikę trupmenai

$$\frac{f_1}{(x-a)^{n-1}h}$$

gauname, kad egzistuoja toks elementas $b_{n-1} \in k$ ir toks polinomas $f_2 \in k[x]$, kad

$$\frac{f_1}{(x-a)^{n-1}h} = \frac{b_{n-1}}{(x-a)^{n-1}} + \frac{f_2}{(x-a)^{n-2}h}.$$

Taigi (6.37) lygybę galime perrašyti

$$\frac{f}{g} = \frac{b_n}{(x-a)^n} + \frac{b_{n-1}}{(x-a)^{n-1}} + \frac{f_2}{(x-a)^{n-2}h}.$$

Tęsdami šį procesą, gausime išraišką

$$\frac{f}{g} = \frac{b_n}{(x-a)^n} + \frac{b_{n-1}}{(x-a)^{n-1}} + \cdots + \frac{b_1}{x-a} + \frac{f_n}{h},$$

čia $f_n \in k[x]$.

Pirmiau pateiktu būdu galima „atskelti“kiekvieną trupmenos f/g vardiklio g tiesinio daliklio laipsnį $(x-a)^n$. Jei kiekvienas vardiklio g pirminis daliklis yra tiesinis, tai šiuo būdu galima rasti trupmenos f/g išraišką paprastųjų trupmenų suma.

Taisyklingosios trupmenos $f/g \in k(x)$ išraiškai paprastųjų trupmenų suma rasti dažniausiai taikomas *neapibrėžtųjų koeficientų metodas*, kuris remiasi faktu, kad kiekviena taisyklingoji trupmena $f/g \in k(x)$ turi išraišką

$$\frac{f}{g} = \sum_{i=1}^{m} \Big(\sum_{j=1}^{n_i} \frac{a_{ij}}{p_i^j} \Big), \tag{6.38}$$

čia $a_{ij},\ p_i \in k[x]$, $\deg a_{ij} < \deg p_i$, o $p_1,\ p_2,\ \ldots,\ p_m$ – skirtingi normuoti (vyriausiasis koeficientas $= 1$) pirminiai polinomai, įeinantys į vardiklio g kanoninį skaidinį:

$$g = a \cdot p_1^{n_1} p_2^{n_2} \cdots p_m^{n_m}, \quad a \in k.$$

Taigi ieškodami trupmenos f/g išraiškos paprastųjų trupmenų suma, sudarome formalią (6.38) išraišką, kurioje polinomų a_{ij} koeficientai yra ieškomi nežinomieji. Šios išraiškos abi lygybės puses padauginę iš polinomo g, gauname polinomų lygybę. Sulyginę gautų polinomų koeficientus prie atitinkamų x laipsnių, gauname tiesinių lygčių sistemą. (Remiantis 6.8.56 teorema, ši sistema turi vienintelį sprendinį.) Išsprendę šią sistemą, rasime (6.38) išraišką ir pamatysime, kad joje iš viso yra

$$\sum_{i=1}^{m} n_i \deg p_i = \deg g$$

nežinomų koeficientų.

Atskirai aptarsime svarbų atvejį $\mathbb{R}(x)$. Kiekvienas pirminis žiedo $\mathbb{R}[x]$ polinomas yra pirmojo arba antrojo laipsnio (žr. 6.8.71 teiginį). Taigi taisyklingosios trupmenos $f/g \in \mathbb{R}(x)$ išraiška paprastųjų trupmenų suma šiuo atveju yra tokio pavidalo

$$\frac{f}{g} = \sum_{i=1}^{r} \left(\frac{t_{i1}}{x-a_i} + \frac{t_{i2}}{(x-a_i)^2} + \cdots + \frac{t_{in_i}}{(x-a_i)^{n_i}} \right) + \sum_{j=1}^{s} \left(\frac{u_{j1}x+v_{j1}}{x^2+b_jx+c_j} + \frac{u_{j2}x+v_{j2}}{(x^2+b_jx+c_j)^2} + \cdots + \frac{u_{jm_j}x+v_{jm_j}}{(x^2+b_jx+c_j)^{m_j}} \right), \tag{6.39}$$

čia $x-a_i$, $x^2+b_jx+c_j \in \mathbb{R}[x]$ yra skirtingi pirminiai polinomai, įeinantys į vardiklio g kanoninį skaidinį (virš $\mathbb{R}$)

$$g = a \cdot \prod_{i=1}^{r} (x-a_i)^{n_i} \prod_{j=1}^{s} (x^2+b_jx+c_j)^{m_j}, \quad a \in \mathbb{R}.$$

(Kiekvienas pirminis žiedo $\mathbb{R}[x]$ polinomas yra pirmojo arba antrojo laipsnio (žr. 6.8.71 teiginį).)

6.8.58 pavyzdys. Rasime taisyklingosios trupmenos $f(x)/g(x)$ išraišką paprastųjų trupmenų suma; čia

$$f(x) = x^4 + 6\,x^3 - 4\,x^2 - 3,$$
$$g(x) = x^5 - 2\,x^3 - 2\,x^2 - 3\,x - 2.$$

Pirmas sprendimas. Nesunku įsitikinti, kad polinomo $g(x)$ kanoninis skaidinys yra

$$g(x) = (x-2)(x+1)^2(x^2+1).$$

Žinome (žr. 6.8.56 teoremos įrodymą), kad taisyklingosios trupmenos $f(x)/g(x)$ išraiška paprastųjų trupmenų suma turi (6.39) pavidalą:

$$\frac{f(x)}{g(x)} = \frac{A}{x-2} + \frac{B}{x+1} + \frac{C}{(x+1)^2} + \frac{Dx+E}{x^2+1}, \tag{6.40}$$

čia A, B, C, D, E – ieškomi (neapibrėžti) realieji skaičiai.

(6.40) lygybę padauginę iš $g(x)$, gauname lygybę

$$f(x) = A(x+1)^2(x^2+1) + B(x-2)(x+1)(x^2+1) + C(x-2)(x^2+1) + (Dx+E)(x-2)(x+1)^2. \tag{6.41}$$

Šios lygybės dešinėje pusėje atlikę veiksmus, gauname

$$f(x) = (A + B + D)x^4 + (2A - B + C + E)x^3 + (2A - B - 2C - 3D)x^2 \\ + (2A - B + C - 2D - 3E)x + A - 2B - 2C - 2E.$$

Ši lygybė yra polinomų lygybė, todėl koeficientai prie atitinkamų x laipsnių sutampa. Taigi sulyginę paskutinės lygybės dešinėje ir kairėje pusėje esančių polinomų koeficientus prie atitinkamų x laipsnių, gauname lygčių sistemą

$$\begin{cases} A + B + D = 1 \\ 2A - B + C + E = 6 \\ 2A - B - 2C - 3D = -4 \\ 2A - B + C - 2D - 3E = 0 \\ A - 2B - 2C - 2E = -3 \end{cases}.$$

Išsprendę šią lygčių sistemą, gauname $A = 1$, $B = -1$, $C = 2$, $D = 1$ ir $E = 1$. Šias reikšmes įstatę į (6.40) lygybę, gauname, kad trupmenos $f(x)/g(x)$ išraiška paprastųjų trupmenų suma yra

$$\frac{f(x)}{g(x)} = \frac{1}{x-2} - \frac{1}{x+1} + \frac{2}{(x+1)^2} + \frac{x+1}{x^2+1}. \tag{6.42}$$

Antras sprendimas. Kaip ir pirmame sprendime sudarome (6.41) lygybę, bet skliaustų neatskliaudžiame. Nežinomuosius A, B, C, D, E rasime į minėtąją lygybę įstatę tam tikras x reikšmes. Iš tikrųjų, įstatę $x = 2$ į (6.41) lygybę, gauname $f(2) = 45A$, t. y. $A = 1$. Įstatę į minėtą lygybę $x = -1$, gauname $C = 2$. Į (6.41) lygybę įstatę $x = 0$ ir atlikę aritmetinius veiksmus, gauname ($A = 1$, $C = 2$) lygtį

$$B + E = 0, \tag{6.43}$$

o įstatę $x = 1$, gauname lygtį

$$B + D + E = 1.$$

Iš paskutinių dviejų lygčių randame $D = 1$. Į (6.41) lygybę įstatę $x = -2$, gauname ($A = 1$, $C = 2$, $D = 1$) lygtį

$$5B - E = -6.$$

Iš šios lygybės ir iš (6.43) lygybės randame $B = -1$, $E = 1$. Taigi gauname (6.42) išraišką.

Trečias sprendimas. (6.42) išraišką rasime 6.8.57 skyrelyje pateiktu metodu. Bet kuriam skaičiui $A \in \mathbb{R}$ teisinga lygybė

$$\frac{f(x)}{g(x)} = \frac{f(x)}{(x-2)h(x)} = \frac{A}{x-2} + \frac{f(x) - A \cdot h(x)}{(x-2)h(x)}, \tag{6.44}$$

čia $h(x) = (x+1)^2(x^2+1) = x^4+2x^3+2x^2+2x+1$. Parinkę $A = f(2)/h(2) = 1$, gauname, kad skaičius 2 yra polinomo

$$f(x) - A \cdot h(x) = 4x^3 - 6x^2 - 2x - 4$$

šaknis, todėl šis polinomas dalijasi iš $x - 2$:

$$4x^3 - 6x^2 - 2x - 4 = (x-2)(4x^2+2x+2).$$

Taigi (6.44) lygybę galime perrašyti

$$\frac{f(x)}{g(x)} = \frac{1}{x-2} + \frac{(x-2)(4x^2+2x+2)}{(x-2)h(x)} = \frac{1}{x-2} + \frac{4x^2+2x+2}{(x+1)^2(x^2+1)}. \tag{6.45}$$

Toliau ieškome trupmenos

$$\frac{4x^2+2x+2}{(x+1)^2(x^2+1)}$$

išraiškos paprastųjų trupmenų suma. Kiekvienam $C \in \mathbb{R}$ teisinga lygybė

$$\frac{4x^2+2x+2}{(x+1)^2(x^2+1)} = \frac{C}{(x+1)^2} + \frac{4x^2+2x+2-C(x^2+1)}{(x+1)^2(x^2+1)}. \tag{6.46}$$

Parinkę $C = 2$ (polinomų $4x^2+2x+2$ ir x^2+1 reikšmių taške $x = -1$ santykis), gauname, kad skaičius -1 yra polinomo

$$4x^2+2x+2 - B(x^2+1) = 2x^2+2x$$

šaknis, todėl šis polinomas dalijasi iš $x+1$: $2x^2+2x = 2x(x+1)$. Dabar (6.46) lygybę galime perrašyti

$$\begin{aligned} \frac{4x^2+2x+2}{(x+1)^2(x^2+1)} &= \frac{2}{(x+1)^2} + \frac{2x(x+1)}{(x+1)^2(x^2+1)} = \\ &= \frac{2}{(x+1)^2} + \frac{2x}{(x+1)(x^2+1)}. \end{aligned} \tag{6.47}$$

Belieka trupmenos vardiklyje

$$\frac{2x}{(x+1)(x^2+1)}$$

„atskelti“daugiklį $x+1$. Bet kuriam $B \in \mathbb{R}$ teisinga lygybė

$$\frac{2x}{(x+1)(x^2+1)} = \frac{B}{x+1} + \frac{2x - B\cdot(x^2+1)}{(x+1)(x^2+1)}. \tag{6.48}$$

Parinkę $B = -1$ (polinomų $2x$ ir x^2+1 reikšmių taške $x = -1$ santykis) gauname, kad skaičius -1 yra polinomo

$$2x - B \cdot (x^2+1) = x^2 + 2x + 1$$

šaknis: $x^2 + 2x + 1 = (x+1)^2$. Taigi (6.48) lygybę galime perrašyti

$$\frac{2x}{(x+1)(x^2+1)} = \frac{-1}{x+1} + \frac{(x+1)^2}{(x+1)(x^2+1)} = \frac{-1}{x+1} + \frac{x+1}{x^2+1}. \tag{6.49}$$

Pagaliau iš (6.45), (6.47) ir (6.49) lygybių užrašome pradinės trupmenos $f(x)/g(x)$ išraišką paprastųjų trupmenų suma:

$$\frac{f(x)}{g(x)} = \frac{1}{x-2} + \frac{2}{(x+1)^2} - \frac{1}{x+1} + \frac{x+1}{x^2+1}.$$

6.8.7 Polinomai su kompleksiniais koeficientais

Šiame skyrelyje nagrinėsime polinomus, kurių koeficientai yra kompleksiniai skaičiai. Iš pradžių apibrėšime algebriškai uždarą kūną, o paskui suformuluosime vadinamąją „pagrindinę algebros teoremą“.

6.8.59 apibrėžimas (algebriškai uždaras kūnas I)**.** Kūnas k vadinamas *algebriškai uždaru*, jei kiekvienas teigiamo laipsnio polinomas $p(x) \in k[x]$ žiede $k[x]$ išsiskaido pirmojo laipsnio polinomų sandauga, t. y.

$$p(x) = a \cdot (x - a_1)(x - a_2) \cdots (x - a_n), \quad a,\, a_j \in k.$$

6.8.60 apibrėžimas (algebriškai uždaras kūnas II)**.** Kūnas k vadinamas *algebriškai uždaru*, jei kiekvienas teigiamo laipsnio polinomas šiame kūne turi bent vieną šaknį.

Galima nesunkiai įsitikinti, kad abu šie apibrėžimai yra ekvivalentūs. Dabar be įrodymo suformuluosime vadinamąją „pagrindinę algebros teoremą“. Pateiksime dvi (ekvivalenčias) šios teoremos formuluotes.

6.8.61 teorema (pagrindinė algebros teorema. Pirmoji formuluotė)**.** *Kompleksinių skaičių kūnas $\mathbb{C}$ yra algebriškai uždaras.*

6.8.62 teorema (pagrindinė algebros teorema. Antroji formuluotė)**.** *Kiekvienas teigiamo laipsnio polinomas su kompleksiniais koeficientais turi bent vieną šaknį kūne $\mathbb{C}$.*

Pirmas šią teoremą 1799 metais griežtai įrodė Gausas. Skambus pavadinimas „pagrindinė algebros teorema“suteiktas dar tais laikais, kai viena svarbiausių algebros užduočių buvo polinominių lygčių sprendimas. Nors 6.8.61 teorema tebėra svarbus teiginys, šiais laikais algebroje ji priskiriama „eilinių“teiginių grupei.

6.8.63 pavyzdys. Pasistengsime paaiškinti, kodėl polinomas

$$p(z) = z^4 - 3z^3 + z^2 - 2z + 6$$

turi bent vieną kompleksinę šaknį. (Toks paaiškinimas tinka bet kokiam teigiamo laipsnio polinomui.)

Fiksuokime pakankamai didelį realųjį skaičių R ir nagrinėkime, kaip kinta funkcija $p(Re^{it})$, kai kintamasis t prabėga visas realiąsias reikšmes tarp 0 ir 2π. Kai $t \in [0, 2\pi]$, kompleksinės plokštumos taškas Re^{it} nubrėžia apskritimą, kurio spindulys R, o centras – 0. O taškas $p(Re^{it})$, kai $t \in [0, 2\pi]$, nubrėžia uždarą (nes $p(Re^{i\cdot 0}) = p(Re^{i2\pi}) = p(R)$) kreivę $\Gamma(R)$. Pakankamai dideliems R skaičius 0 priklausys kreivės $\Gamma(R)$ „vidui“ (žr. 6.3 pav.; $R = 3$). Iš kitos pusės, jei skaičius $R > 0$ pakankamai mažas, tai kiekvienas kreivės $\Gamma(R)$ taškas bus labai artimas skaičiui $p(0) = 6$ ir skaičius 0 bus uždarosios kreivės $\Gamma(R)$ „išorėje“ (žr. 6.4 pav.; $R = 1$). Spinduliui R kintant nuo 1 iki 3, kreivė $\Gamma(1)$ „tolygiai pereina“ į kreivę $\Gamma(3)$, todėl egzistuoja tokia spindulio reikšmė $R_0 \in (1, 3)$, kad kreivė $\Gamma(R_0)$ eina per nulį. Tuomet egzistuoja toks $t_0 \in [0, 2\pi]$, kad $p(R_0 e^{it_0}) = 0$, t. y. kompleksinis skaičius $R_0 e^{it_0}$ yra polinomo $p(z)$ šaknis.

6.8.64 pastaba. 6.3 ir 6.4 pav. matyti, kad $\Gamma(3)$ pereinant į $\Gamma(1)$, kreivė $\Gamma(R)$ tašką 0 kirs lygiai keturis kartus.

6.8.65 išvada. *Kiekvinas n-tojo laipsnio polinomas*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,\ a_j \in \mathbb{C},\ 0 \le j \le n,\ n \ge 1,$$

yra išskaidomas pirmojo laipsnio polinomų sandauga:

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = a_n(x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n),$$

čia $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{C}$ – polinomo $f(x)$ šaknys.

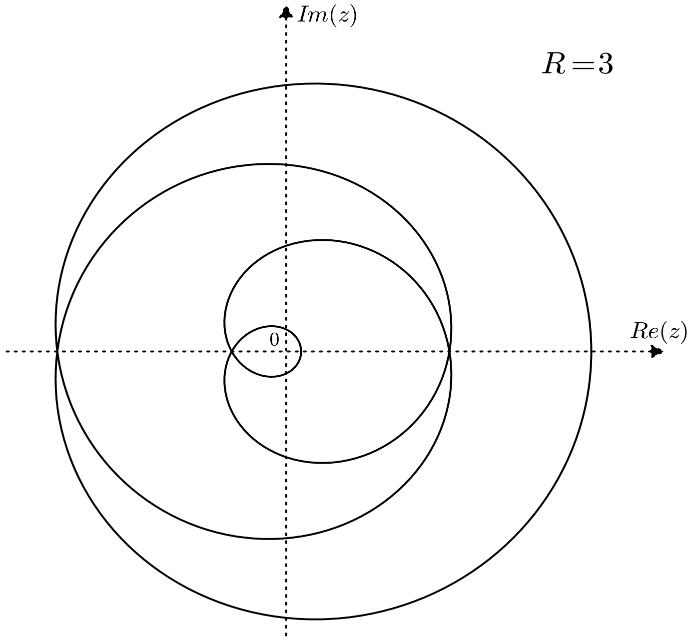
6.8.66 išvada. *Kiekvienas n-tojo, $n \ge 1$, laipsnio polinomas su kompleksiniais (arba realiaisiais) koeficientais turi lygiai n kompleksinių šaknų, jei kiekvieną šaknį skaičiuosime tiek kartų, koks jos kartotinumas.*

6.8.8 Polinomai su realiaisiais koeficientais

6.8.67 teiginys. *Jei kompleksinis skaičius $a \in \mathbb{C}$ yra polinomo su realiaisiais koeficientais šaknis, tai jungtinis skaičius $\overline{a}$ taip pat yra šio polinomo šaknis. Be to, šaknų a ir $\overline{a}$ kartotinumai sutampa.*

Įrodymas. Tarkime, kad $c \in \mathbb{C}$, $p(x) \in \mathbb{R}[x]$,

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0,$$



6.3 pav.: Kreivė $p(3e^{it})$, $t \in [0, 2\pi]$; čia $p(z) = z^4 - 3z^3 + z^2 - 2z + 6$

ir $p(c) = 0$, t. y.

$$a_n c^n + a_{n-1}c^{n-1} + \cdots + a_0 = 0. \tag{6.50}$$

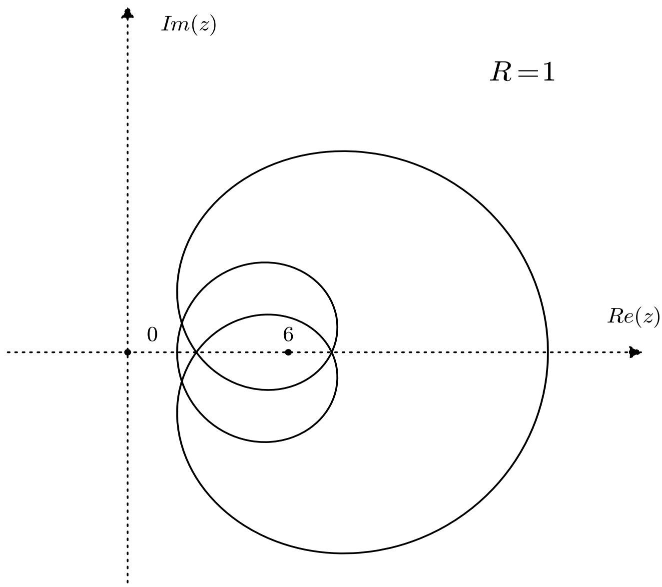
Žinome, kad kompleksiniams skaičiams α, $\beta \in \mathbb{C}$ teisingos lygybės $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$ ir $\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}$ (žr. 1 pratimą po 6.7.3 apibrėžimo). Tuomet

$$0 = \overline{a_n c^n + a_{n-1}c^{n-1} + \cdots + a_0} = \overline{a_n c^n} + \overline{a_{n-1}c^{n-1}} + \cdots + \overline{a_0}$$

$$= \overline{a_n} \cdot \overline{c}^n + \overline{a_{n-1}} \cdot \overline{c}^{n-1} + \cdots + \overline{a_0} = a_n \overline{c}^n + a_{n-1}\overline{c}^{n-1} + \cdots + a_0 = p(\overline{c}),$$

čia $\overline{a_j} = a_j$, nes $a_j \in \mathbb{R}$. Taigi $p(\overline{c}) = 0$, t. y. jungtinis skaičius $\overline{c}$ yra polinomo $p(x)$ šaknis.

Dabar įrodysime, kad polinomo $p(x)$ šaknų a ir $\overline{a}$ kartotinumai sutampa. Jei $a \in \mathbb{R}$, tai $a = \overline{a}$ ir minėtas tvirtinimas šiuo atveju akivaizdus. Tarkime, kad kompleksinis skaičius a yra grynai menamas, t. y. $a \in \mathbb{C} \setminus \mathbb{R}$. Tegu s – šaknies a kartotinumas, o t – šaknies $\overline{a}$ kartotinumas. Sakykime, kad $s \neq t$. Nemažindami bendrumo galime laikyti, kad $s < t$. Remiantis 6.8.31 teorema, egzistuoja toks



6.4 pav.: Kreivė $p(e^{it})$, $t \in [0, 2\pi]$; čia $p(z) = z^4 - 3z^3 + z^2 - 2z + 6$

polinomas $q(x) \in \mathbb{C}[x]$, kad

$$p(x) = (x - a)^s (x - \overline{a})^t q(x)$$

ir $q(a) \neq 0$ ir $q(\overline{a}) \neq 0$. Kadangi polinomo $(x - a)(x - \overline{a}) = x^2 - (a + \overline{a})x + a\overline{a}$ koeficientai yra realūs skaičiai, tai

$$(x - a)^s (x - \overline{a})^s \in \mathbb{R}[x].$$

Padaliję polinomą $p(x)$ iš polinomo $(x - a)^s (x - \overline{a})^s$ gauname, kad polinomo $(x-\overline{a})^{t-s} q(x)$ koeficientai taip pat yra realūs skaičiai. Be to, kompleksinis skaičius $\overline{a}$ yra polinomo $(x - \overline{a})^{t-s} q(x)$ šaknis. Tačiau jungtinis skaičius $\overline{\overline{a}} = a$ nėra šio polinomo šaknis. Tai prieštarauja nagrinėjamo teiginio pirmajai daliai, kurią jau įrodėme. Taigi $s = t$. □

6.8.68 išvada. *Polinomo su realiaisiais koeficientais visų šaknų aibė kompleksinėje plokštumoje yra simetriška realiosios ašies atžvilgiu.*

6.8.69 teiginys. *Nelyginio laipsnio polinomas su realiaisiais koeficientais turi bent vieną realią šaknį.*

Įrodymas. Tarkime, kad $p(x) \in \mathbb{R}$ – polinomas, kurio laipsnis n yra nelyginis skaičius. Iš pagrindinės algebros teoremos (žr. 6.8.66 išvadą) išplaukia, kad polinomas $p(x)$ turi lygiai n kompleksinių šaknų (kiekvieną šaknį skaičiuojant tiek kartų, koks jos kartotinumas). Be to, iš 6.8.67 teiginio žinome, kad polinomo $p(x)$ grynai menamų šaknų skaičius yra lyginis. Vadinasi, polinomas $p(x)$ turi bent vieną realią šaknį. □

6.8.70 pastaba. 6.8.69 teiginį galima įrodyti nesinaudojant pagrindine algebros teorema (kurios įrodymo šiame vadovėlyje nepateikiame). Trumpai paaiškinsime, kaip tai padaryti. Tarkime, kad $p(x) \in \mathbb{R}[x]$ – nelyginio laipsnio polinomas. Be to, laikysime, kad šio polinomo vyriausiasis koeficientas yra teigiamasis skaičius. Tuomet $\lim_{x\to-\infty} p(x) = -\infty$ ir $\lim_{x\to\infty} p(x) = \infty$, nes polinomo $p(x)$ laipsnis yra nelyginis. Taigi egzistuoja tokie realieji skaičiai a ir b, $a < b$, kad $p(a) < 0$ ir $p(b) > 0$. Kadangi polinomas (polinominė funkcija $p : \mathbb{R} \to \mathbb{R}$, $\mathbb{R} \ni a \mapsto p(a)$) yra tolydi visoje realiųjų skaičių aibėje funkcija, tai, remiantis tarpinių reikšmių teorema, egzistuoja realusis skaičius $c \in (a,\ b)$, kad $p(c) = 0$. Taigi polinomas $p(x)$ turi bent vieną realią šaknį.

6.8.71 teiginys. *Kiekvienas pirminis žiedo $\mathbb{R}[x]$ polinomas yra pirmojo arba antrojo laipsnio.*

Įrodymas. Tarkime, kad $p(x) \in \mathbb{R}[x]$ – pirminis polinomas ir $n := \deg p(x) > 2$. Remiantis pagrindine algebros teorema, polinomas $p(x)$ turi lygiai n kompleksinių šaknų. Tegu $a \in \mathbb{C}$ – polinomo $p(x)$ šaknis. Tuomet $a \notin \mathbb{R}$, nes priešingu atveju polinomas $p(x)$ dalintųsi iš $x-a \in \mathbb{R}[x]$ ir nebūtų pirminis. Iš 6.8.67 teiginio išplaukia, kad kompleksinis jungtinis skaičius $\overline{a}$ taip pat yra polinomo $p(x)$ šaknis. Remiantis 6.8.31 teorema, polinomas $p(x)$ dalijasi iš $(x-a)(x-\overline{a})$. Taigi egzistuoja toks polinomas $q(x) \in \mathbb{C}[x]$, kad

$$p(x) = (x-a)(x-\overline{a})q(x). \tag{6.51}$$

Polinomo $(x-a)(x-\overline{a}) = x^2-(a+\overline{a})x+a\overline{a}$ visi koeficientai yra realieji skaičiai, nes $a+\overline{a} \in \mathbb{R}$ ir $a\overline{a} \in \mathbb{R}$. Tuomet iš (6.51) lygybės gauname (dalindami „kampu“), kad $q(x) \in \mathbb{R}[x]$. Be to, kadangi $\deg p(x) > 2$, tai $\deg q(x) > 0$. Vadinasi, polinomas $p(x)$ nėra pirminis. Prieštara. □

6.8.72 teorema. *Kiekvienas n-tojo laipsnio normuotas polinomas su realiaisiais koeficientais vieninteliu būdu (jei nekreipsime dėmesio į dauginamųjų tvarką) išreiškiamas m tiesinių polinomų $x - a_j$, atitinkančių realiąsias šaknis $a_1, \ldots, a_m$, ir $(n-m)/2$ kvadratinių polinomų, neturinčių realiųjų šaknų, sandauga.*

Įrodymas. Įrodoma remiantis 6.8.50 teorema ir 6.8.71 teiginiu. □

6.8.9 Polinomai su racionaliaisiais koeficientais

6.8.73 teiginys. *Jei racionalusis skaičius u/v, $u \in \mathbb{Z}$, $v \in \mathbb{N}$, $dbd(u, v) = 1$, yra nenulinio polinomo*

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] \tag{6.52}$$

šaknis, tai $u \mid a_0$ ir $v \mid a_n$.

Įrodymas. Kadangi racionalusis skaičius u/v, $u \in \mathbb{Z}$, $v \in \mathbb{N}$, yra (6.52) polinomo šaknis, tai

$$a_n \left(\frac{u}{v}\right)^n + a_{n-1}\left(\frac{u}{v}\right)^{n-1} + \cdots + a_1 \frac{u}{v} + a_0 = 0.$$

Šią lygybę padauginę iš v^n, gauname

$$a_n u^n + a_{n-1}u^{n-1}v + \cdots + a_1 u v^{n-1} + a_0 v^n = 0. \tag{6.53}$$

Pertvarkę pastarąją lygybę, galime parašyti

$$u \cdot \left(a_n u^{n-1} + a_{n-1}u^{n-2}v + \cdots + a_1 v^{n-1}\right) = -a_0 v^n,$$

todėl skaičius $a_0 v^n$ dalijasi iš u. Kadangi skaičiai u ir v tarpusavyje pirminiai, tai $u \mid a_0$.

(6.53) lygybę perrašę

$$v \cdot \left(a_{n-1}u^{n-1} + \cdots + a_1 u v^{n-2} + a_0 v^{n-1}\right) = -a_n u^n$$

matome, kad skaičius $a_n u^n$ dalijasi iš v. Kadangi skaičiai u ir v tarpusavyje pirminiai, tai $v \mid a_n$. □

6.8.74 išvada. *Jei polinomas*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] \tag{6.54}$$

turi racionalią šaknį, tai ši šaknis yra sveikasis skaičius, kuris dalija polinomo laisvąjį narį a_0.

Įrodymas. Jei racionalusis skaičius u/v, $u \in \mathbb{Z}$, $v \in \mathbb{N}$, $\mathrm{dbd}(u, v) = 1$, yra (6.54) polinomo šaknis, tai, remiantis 6.8.73 teiginiu, $u \mid a_0$, o skaičius v dalija šio polinomo vyriausiąjį koeficientą 1. Taigi $v = 1$ ir $u/v = u \in \mathbb{Z}$. □

6.8.74 išvadą galima šiek tiek apibendrinti.

6.8.75 teiginys. *Jei sveikasis skaičius c yra polinomo*

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

šaknis, tai $c \mid a_0$, $c - 1 \mid p(1)$ ir $c + 1 \mid p(-1)$.

Įrodymas. Kadangi $c \in \mathbb{Z}$ yra polinomo $p(x)$ šaknis, tai $x - c \mid p(x)$. Todėl egzistuoja toks polinomas $g(x) \in \mathbb{Z}[x]$, kad $p(x) = (x-c)g(x)$. Į šią lygybę įstatę $x = 0$, $x = 1$, $x = -1$, atitinkamai gauname lygybes:

$$p(0) = -cg(0), \quad p(1) = -(c-1)g(1), \quad p(-1) = -(c+1)g(-1).$$

Taigi $c \mid p(0) = a_0$, $c - 1 \mid p(1)$ ir $c + 1 \mid p(-1)$. □

6.8.76 apibrėžimas. Polinomas $p(x) = a_n x^n + \ldots + a_1 x + a_0 \in \mathbb{Z}[x]$ vadinamas *primityviuoju*, jei jo koeficientų didžiausias bendrasis daliklis lygus 1, t. y.

$$\mathrm{dbd}(a_n, \ldots, a_1, a_0) = 1.$$

6.8.77 teiginys (Gauso lema)**.** *Dviejų primityviųjų polinomų su sveikaisiais koeficientais sandauga yra primityvusis polinomas.*

Įrodymas. Tarkime, kad $f(x), g(x) \in \mathbb{Z}[x]$ – primityvieji polinomai,

$$f(x) = a_m x^m + \ldots + a_1 x + a_0,$$

$$g(x) = b_n x^n + \ldots + b_1 x + b_0,$$

o sandauga

$$f(x)g(x) = c_{m+n} x^{m+n} + \ldots + c_1 x + c_0$$

nėra primityvusis polinomas, t. y. egzistuoja pirminis skaičius, p iš kurio dalijasi visi polinomo $f(x)g(x)$ koeficientai c_{m+n}, …, c_1, c_0. Tegu a_i – polinomo $f(x)$ koeficientas, nesidalijantis iš p, kurio indeksas i – didžiausias. (Toks koeficientas egzistuoja, nes $f(x)$ – primityvusis polinomas.) Analogiškai, tegu b_j – polinomo $g(x)$ koeficientas, nesidalijantis iš p, kurio indeksas j – didžiausias. Nagrinėkime sandaugos $f(x)g(x)$ koeficientą c_{i+j} :

$$\begin{aligned} c_{i+j} &= a_i b_j + a_{i-1} b_{j+1} + a_{i-2} b_{j+2} + \cdots + \\ &\quad + a_{i+1} b_{j-1} + a_{i+2} b_{j-2} + \cdots \end{aligned} \tag{6.55}$$

Šios lygybės dešiniosios pusės visi dėmenys, išskyrus $a_i b_j$, dalijasi iš p, nes, remiantis skaičių a_i ir b_j parinkimu, skaičiai b_{i+1}, b_{i+2}, … ir a_{j+1}, a_{j+2}, … dalijasi iš p. Taigi (6.55) lygybės dešinioji pusė nesidalija iš p. Tačiau šios lygybės karioji pusė (skaičius c_{i+j}) dalijasi iš p. Prieštara. Vadinasi, primityviųjų polinomų sandauga taip pat yra primityvusis polinomas. □

6.8.78 išvada. *Jei polinomas su sveikaisiais koeficientais redukuojamas virš racionaliųjų skaičių kūno, tai jis redukuojamas ir virš sveikųjų skaičių žiedo.*

Įrodymas. Tarkime, kad polinomas $p(x) \in \mathbb{Z}[x]$ yra redukuojamas virš racionaliųjų skaičių kūno $\mathbb{Q}$. (Akivaizdu, kad $\mathbb{Z}[x] \subset \mathbb{Q}[x]$.) Tada egzistuoja tokie polinomai $f_1(x), f_2(x) \in \mathbb{Q}[x]$, kad

$$p(x) = f_1(x)f_2(x),$$

$\deg f_1(x) < \deg p(x)$ ir $\deg f_2(x) < \deg p(x)$. Tada egzistuoja tokie sveikieji skaičiai a_i, b_i, $\mathrm{dbd}(a_i, b_i) = 1$, kad

$$f_i(x) = \frac{a_i}{b_i}\, h_i(x), \quad i = 1, 2,$$

čia $h_i(x) \in \mathbb{Z}[x]$ – primityvusis polinomas. (Prieš skliaustus iškeliame polinomo $f_i(x)$ koeficientų bendrąjį vardiklį ir skaitiklių didžiausią bendrąjį daliklį.) Taigi

$$p(x) = \frac{a_1a_2}{b_1b_2}\, h_1(x)h_2(x). \tag{6.56}$$

Tvirtiname, kad skaičius $a_1a_2/(b_1b_2)$ yra sveikasis. Iš tikrųjų, jei $a_1a_2/(b_1b_2) \notin \mathbb{Z}$, tai egzistuoja tokie $a, b \in \mathbb{Z}$, $b > 1$, $\mathrm{dbd}(a, b) = 1$, kad $a_1a_2/(b_1b_2) = a/b$. Kadangi $h_1(x)$ ir $h_2(x)$ – primityvieji polinomai, tai, pagal Gauso lemą (6.8.77 teiginį), polinomas $h_1(x)h_2(x)$ taip pat yra primityvusis. Vadinasi, egzistuoja polinomo $h_1(x)h_2(x)$ koeficientas, kuris nesidalija iš b. Tačiau tada $p(x) \notin \mathbb{Z}[x]$. Prieštara. Taigi $a_1a_2/(b_1b_2) \in \mathbb{Z}$, todėl iš (6.56) lygybės išplaukia, kad polinomas $p(x)$ redukuojamas ir virš sveikųjų skaičių žiedo.

□

6.8.79 teiginys (Eizenšteino kriterijus)**.** *Tarkime, kad $p \in \mathbb{Z}$ – pirminis skaičius, o polinomo*

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in \mathbb{Z}[x],$$

$n \geq 2$, *koeficientai* a_j, $0 \leq j \leq n-1$, *dalijasi iš* p. *Jei laisvasis narys* a_0 *nesidalija iš* p^2, *tai polinomas* $f(x)$ *yra neredukuojamas virš* $\mathbb{Q}$.

Įrodymas. Tarkime, kad polinomas $f(x)$ yra redukuojamas virš $\mathbb{Q}$. Tuomet, pagal 6.8.78 išvadą, polinomas $f(x)$ taip pat redukuojamas virš $\mathbb{Z}$. Todėl egzistuoja tokie polinomai $g(x), h(x) \in \mathbb{Z}[x]$, kad

$$f(x) = g(x)h(x) \quad \text{ir} \quad \deg g(x) < n,\ \deg g(x) < n.$$

Kadangi polinomas $f(x)$ yra normuotasis (vyriausiasis koeficientas 1), tai polinomus $g(x)$ ir $h(x)$ galima parinkti taip, kad jie būtų normuoti. Tegu

$$g(x) = x^r + b_{r-1}x^{r-1} + \ldots + b_1x + b_0 \in \mathbb{Z},$$

$$h(x) = x^s + c_{s-1}x^{s-1} + \ldots + c_1x + c_0 \in \mathbb{Z},$$

$r < n$, $s < n$. Kadangi laisvasis narys $a_0 = b_0c_0$ nesidalija iš p^2, tai arba b_0 arba c_0 nesidalija iš p. Nemažindami bendrumo tarkime, kad skaičius b_0 nesidalija iš p. Tuomet c_0 dalijasi iš p, nes $p \mid a_0$. Tegu t – mažiausias natūralusis skaičius su kuriuo $p \nmid c_t$. Aišku, kad $1 \leq t \leq s < n$. Sulyginę polinomų $f(x)$ ir $g(x)h(x)$ koeficientus prie x^t, gauname

$$a_t = b_0c_t + b_1c_{t-1} + \dots. \tag{6.57}$$

Iš teiginio sąlygos matyti, kad a_t dalijasi iš p $(1 \leq t \leq s < n)$. Be to, iš skaičiaus t apibrėžimo aišku, kad $p \mid c_k$, $0 \leq k \leq t-1$. Tada iš (6.57) lygybės gauname, kad skaičius b_0c_t dalijasi iš p. Kadangi p – pirminis skaičius, tai $p \mid b_0$ arba $p \mid c_t$ (žr. 3.3.3 teoremą). Prieštara. □

6.8.80 pavyzdys. Remiantis Eizenšteino kriterijumi $(p = 3)$, polinomas

$$x^5 - 12x^3 + 6x - 15$$

yra neredukuojamas virš $\mathbb{Q}$.

6.8.81 pavyzdys. Eizenšteino kriterijaus sąlyga $p^2 \nmid a_0$ yra svarbi: polinomo $x^2 + 2x + 4 = (x+2)(x+2)$ visi koeficientai, išskyrus vyriausiąjį, dalijasi iš 2, o laisvasis narys dalijasi iš $4 = 2^2$.

6.8.10 Polinomo šaknų lokalizavimas

Bet kuriam nenuliniam polinomui galima nurodyti kompleksinės plokštumos skritulį, kuriam priklauso visos nagrinėjamo polinomo šaknys.

6.8.82 teorema. *Jei kompleksinis skaičius c yra nenulinio polinomo*

$$a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{C}[x] \tag{6.58}$$

šaknis, tai

$$|c| < 1 + \frac{A}{|a_n|}, \tag{6.59}$$

čia $A = \max\{|a_i| \mid 0 \leq i \leq n\}$.

Įrodymas. Kadangi skaičius $c \in \mathbb{C}$ yra (6.58) polinomo šaknis, tai

$$a_nc^n + a_{n-1}c^{n-1} + \dots + a_1c + a_0 = 0.$$

Jei $|c| \leq 1$, tai (6.59) nelygybė teisinga. Toliau laikysime, kad $|c| > 1$. Iš paskutinės lygybės gauname

$$\begin{aligned}|a_nc^n| = |-a_{n-1}c^{n-1} - \dots - a_1c - a_0| &\leq |a_{n-1}| \cdot |c|^{n-1} + \dots + |a_1| \cdot |c| + |a_0| \\ &\leq A(|c|^{n-1} + \dots + |c| + 1) = A\frac{|c|^n - 1}{|c| - 1} < A\frac{|c|^n}{|c| - 1}.\end{aligned}$$

Taigi
$$|a_n| \cdot |c|^n < A\frac{|c|^n}{|c|-1}.$$
Iš šios nelygybės išvedama (6.59) nelygybė. □

Toliau kalbėsime tik apie polinomo su realiaisiais koeficientais realiąsias šaknis. Nagrinėkime tokį uždavinį:

Nustatyti kiek polinomas $p(x) \in \mathbb{R}[x]$ turi realiųjų šaknų intervale $[a, b]$, $a < b$.

Šį uždavinį 1829 metais išsprendė prancūzų matematikas Šturmas. Suformuluosime teoremą, kuria remiantis išsprendžiamas minėtas uždavinys. Ši teorema vadinama Šturmo vardu. (Prancūzų matematikas Furjė šį uždavinį išsprendė dar ankščiau, tačiau jo publikacija, paruošta prieš pat Prancūzijos revoliuciją buvo pamiršta.)

Tarkime, kad kompleksinis skaičius c yra nenulinio polinomo $p(x) \in \mathbb{R}[x]$ šaknis. Jei c – paprastoji polinomo $p(x)$ šaknis, tai, remiantis 6.8.41 teiginiu, išvestinė $p'(x)$ nesidalija iš $x - c$. Vadinasi, kiekviena polinomo $p(x)$ šaknis yra ir polinomo
$$\frac{p(x)}{\mathrm{dbd}(p(x), p'(x))} \tag{6.60}$$
paprastoji šaknis.

Dabar tarkime, kad c – kartotinė polinomo $p(x)$ šaknis, kurios kartotinumas lygus $m \geq 2$. Iš 6.8.44 teoremos išplaukia, kad skaičius c yra išvestinės $p'(x)$ $(m-1)$-tojo kartotinumo šaknis. Taigi ir šiuo atveju skačius c yra (6.60) polinomo paprastoji šaknis. Vadinasi, (6.60) polinomas neturi kartotinių šaknų. Be to, visų (6.60) polinomo šaknų aibė sutampa su polinomo $p(x)$ visų šaknų aibe.

Taigi ieškant polinomo visų šaknų aibės pakanka apsiriboti polinomais, kurie neturi kartotinių šaknų.

6.8.83 apibrėžimas. Tarkime, kad $p(x)$ – nenulinis polinomas su realiaisiais koeficientais, kuris neturi kartotinių šaknų. Nenulinių polinomų su realiaisiais koeficientais šeima
$$p_0(x) = p(x),\ p_1(x),\ p_2(x),\ \ldots,\ p_s(x) \tag{6.61}$$
vadinama polinomo $p(x)$ *Šturmo sistema*, jei

(i) gretimi (6.61) sistemos polinomai neturi bendrų šaknų, t. y. su kiekvienu $j \in \{0, 1, \ldots, s-1\}$ polinomai $p_j(x)$ ir $p_{j+1}(x)$ neturi bendrų šaknų;

(ii) paskutinis sistemos polinomas $p_s(x)$ neturi realiųjų šaknų;

(iii) jei a – (6.61) sistemos polinomo $p_j(x)$, $1 \leq j \leq s-1$, realioji šaknis, tai $p_{j-1}(a) \cdot p_{j+1}(a) < 0$;

(iv) jei realusis skaičius a yra polinomo $p(x)$ šaknis, tai sandauga $p(x)p_1(x)$ yra *didėjanti* taške $x = a$, t. y. egzistuoja tokia taško $x = a$ aplinka $(a-\varepsilon, a+\varepsilon)$, $\varepsilon > 0$, kad intervale $(a-\varepsilon, a)$ sandauga $p(x)p_1(x)$ yra neigiama, o intervale $(a, a+\varepsilon)$ ši sandauga yra teigiama.

6.8.84 pavyzdys. Tarkime, kad $p(x)$ – nenulinis polinomas su realiaisiais koeficientais, neturintis kartotinių šaknų (kompleksinių). Sukonstruosime polinomo $p(x)$ Šturmo sistemą. Tegu $p_1(x) := p'(x)$. Polinomai $p(x)$ ir $p_1(x)$ tenkina 6.8.83 apibrėžimo (iv) sąlygą. Iš tikrųjų, tarkime, kad realusis skaičius a yra polinomo $p(x)$ šaknis. Kadangi skaičius a yra paprastoji šio polinomo šaknis, tai $p'(a) \neq 0$. Todėl egzistuoja taško $x = a$ aplinka $(a-\varepsilon, a+\varepsilon)$, $\varepsilon > 0$, kurioje išvestinė $p'(x) \neq 0$. Vadinasi, išvestinė $p'(x)$ visame intervale $(a-\varepsilon, a+\varepsilon)$ yra to paties ženklo (nes $p'(x)$ yra tolydi funkcija). Jei $p'(a) > 0$, tai $p'(x) > 0$ visame intervale $(a-\varepsilon, a+\varepsilon)$ ir polinomas $p(x)$ yra didėjanti funkcija šiame intervale. Todėl $p(x)p_1(x) = p(x)p'(x) < 0$ intervale $(a-\varepsilon, a)$ ir $p(x)p_1(x) > 0$ intervale $(a, a+\varepsilon)$. O jeigu $p'(a) < 0$, tai $p'(x) < 0$ visame intervale $(a-\varepsilon, a+\varepsilon)$ ir polinomas $p(x)$ yra mažėjanti funkcija šiame intervale. Todėl $p(x)p_1(x) < 0$ intervale $(a-\varepsilon, a)$ ir $p(x)p_1(x) > 0$ intervale $(a, a+\varepsilon)$.

Padalinkime polinomą $p(x)$ iš polinomo $p_1(x)$ ir liekaną pažymėkime $-p_2(x)$:

$$p(x) = p_1(x)q_1(x) - p_2(x),$$

čia $q_1(x) \in \mathbb{R}[x]$. Tarkime, kad polinomai $p_{k-1}(x)$ ir $p_k(x)$ jau sukonstruoti. Tada polinomo $p_{k-1}(x)$ dalybos iš polinomo $p_k(x)$ liekaną pažymėkime $-p_{k+1}(x)$:

$$p_{k-1}(x) = p_k(x)q_k(x) - p_{k+1}(x), \tag{6.62}$$

čia $q_k(x) \in \mathbb{R}[x]$. Jei polinomas $p_k(x)$ yra nenulinis, tai polinomo $p_{k+1}(x)$ laipsnis yra mažesnis už polinomo $p_k(x)$ laipsnį. Todėl tęsiant 6.62 dalybos procedūrą atsiras toks natūralusis skaičius s, kad $p_s(x) \neq 0$, o polinomas $p_{s+1}(x)$ yra nulinis:

$$\begin{aligned} p(x) &= p_1(x)q_1(x) - p_2(x),\\ p_1(x) &= p_2(x)q_2(x) - p_3(x),\\ &\cdots\ \cdots\ \cdots\\ p_{s-2}(x) &= p_{s-1}(x)q_{s-1}(x) - p_s(x),\\ p_{s-1}(x) &= p_s(x)q_s(x). \end{aligned} \tag{6.63}$$

Įrodysime, kad taip sukonstruota polinomų šeima

$$p_0(x) = p(x),\ p_1(x),\ p_2(x),\ \ldots,\ p_s(x) \tag{6.64}$$

yra polinomo $p(x)$ Šturmo sistema. Nagrinėjamo pavyzdžio pradžioje įsitikinome, kad ši sistema tenkina 6.8.83 apibrėžimo (iv) sąlygą. Įsitikinsime, kad (6.64) polinomų sistema tenkina 6.8.83 apibrėžimo (ii) sąlygą, t. y. polinomas $p_s(x)$ neturi realiųjų šaknų. Iš tikrųjų, iš (6.63) paskutinės lygybės matyti, kad polinomas $p_{s-1}(x)$ dalijasi iš polinomo $p_s(x)$, o iš priešpaskutinės lygybės – kad ir polinomas $p_{s-2}(x)$ dalijasi iš polinomo $p_s(x)$. Taip kildami (6.63) lygybėmis į viršų gausime, kad polinomas $p_s(x)$ yra polinomų $p(x)$ ir $p_1(x) = p'(x)$ bendrasis daliklis. Tačiau $\mathrm{dbd}(p(x), p'(x)) = 1$, nes polinomas $p(x)$ neturi kartotinių šaknų (kompleksinių). Vadinasi, polinomas $p_s(x)$ yra nenulinis skaičius ir realiųjų šaknų neturi.

Dabar įsitikinsime, kad (6.64) polinomų šeima tenkina 6.8.83 apibrėžimo (i) sąlygą. Tarkime, kad (6.64) sistemos polinomai $p_k(x)$ ir $p_{k+1}(x)$ turi bendrą šaknį a. Tuomet iš (6.63) lygybės

$$p_{k-1}(x) = p_k(x)q_k(x) - p_{k+1}(x)$$

paaiškėja, kad skaičius a yra ir polinomo $p_{k-1}(x)$ šaknis, o iš (6.63) lygybės

$$p_{k-2}(x) = p_{k-1}(x)q_{k-1}(x) - p_k(x)$$

matyti, kad skaičius a yra ir polinomo $p_{k-2}(x)$ šaknis. Taip kildami (6.63) lygybėmis į viršų gausime, kad skaičius a yra polinomų $p(x)$ ir $p_1(x) = p'(x)$ bendroji šaknis, t. y. skaičius a yra polinomo $p(x)$ kartotinė šaknis. Prieštara.

Tarkime, kad realusis skaičius a yra polinomo $p_j(x)$, $1 \leq j \leq s-1$, šaknis. Iš 6.8.83 apibrėžimo (i) sąlygos žinome, kad $p_{j-1}(a) \neq 0$ ir $p_{j+1}(a) \neq 0$. Įstatę $x = a$ į (6.63) lygybę

$$p_{j-1}(x) = p_j(x)q_j(x) - p_{j+1}(x),$$

gauname $p_{j-1}(a) = -p_{j+1}(a)$. Vadinasi, $p_{j-1}(a)p_{j+1}(a) < 0$. Taigi (6.64) polinomų šeima tenkina 6.8.83 apibrėžimo (iii) sąlygą.

Įsitikinome, kad (6.64) polinomų šeima yra polinomo $p(x)$ Šturmo sistema.

6.8.85 pastaba. (6.64) sistemos bet kurį polinomą padauginę iš teigiamo skaičiaus vėl gausime polinomo $p(x)$ Šturmo sistemą.

6.8.86 apibrėžimas. Nagrinėkime realiųjų skaičių seką

$$a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n. \tag{6.65}$$

Išbraukę nulinius šios sekos narius, gauname seką

$$a_{i_1},\ a_{i_2},\ a_{i_3},\ \ldots,\ a_{i_m},$$

čia $0 \leq i_1 < i_2 < i_3 < \cdots < i_m \leq n$. Jei $a_{i_k}a_{i_{k+1}} < 0$, tai sakome, kad (6.65) sekos i_{k+1}-jame naryje yra *ženklo pokytis*. Pavyzdžiui, sekoje

$$1,\ 2,\ -5,\ 0,\ 4,\ 0,\ 0,\ -3$$

yra lygiai trys ženklo pokyčiai, o sekose

$$1,\ 2,\ 7,\ 0,\ 5$$

ir

$$0,\ 0,\ 0,\ 0,\ 0,\ 0$$

iš viso nėra ženklo pokyčių.

Tarkime, kad $p(x) \in \mathbb{R}[x]$ – nenulinis polinomas, neturintis kartotinių šaknų (kompleksinių), realusis skaičius c nėra šio polinomo šaknis, o polinomų šeima

$$p_0(x) = p(x),\ p_1(x),\ p_2(x),\ \ldots,\ p_s(x) \tag{6.66}$$

yra polinomo $p(x)$ Šturmo sistema. Realiųjų skaičių sekoje

$$p(c),\ p_1(c),\ p_2(c),\ \ldots,\ p_s(c)$$

esančių ženklo pokyčių skaičių pažymėkime $W(c)$. Skaičius $W(c)$ vadinamas (6.66) *Šturmo sistemos ženklo pokyčių skaičiumi taške* $x = c$.

6.8.87 teorema (Šturmo teorema)**.** *Tarkime, kad $p(x) \in \mathbb{R}[x]$ – polinomas, neturintis kartotinių šaknų (kompleksinių), o realieji skaičiai a ir b, $a < b$, nėra šio polinomo šaknys. Tuomet $W(a) \geq W(b)$. Be to, skirtumas $W(a) - W(b)$ sutampa su polinomo $p(x)$ realiųjų šaknų skaičiumi intervale (a, b).*

Įrodymas. Žiūrėsime, kaip keičiasi (6.66) Šturmo sistemos ženklo pokyčių skaičius $W(x)$, kai x didėja. Raide $\mathcal{S}$ pažymėkime (6.66) sistemos polinomų realiųjų šaknų aibę, t. y. realusis skaičius a priklauso aibei $\mathcal{S}$ tada ir tik tada, kai jis yra kurio nors (6.66) sistemos polinomo šaknis. Tegu

$$\mathcal{S} = \{a_1 < a_2 < \ldots < a_m\}.$$

Kiekviename intervale $(-\infty, a_1)$, (a_1, a_2), …, (a_{m-1}, a_m), (a_m, ∞) funkcija $W(x)$ yra pastovi, nes šiuose intervaluose kiekvienas (6.66) sistemos polinomas turi pastovų ženklą (nes neturi šaknies šiuose intervaluose). Pažymėję $a_0 := -\infty$ ir $a_{m+1} := \infty$, minėtą intervalų sistemą galime užrašyti taip:

$$(a_0, a_1),\ (a_1, a_2),\ \ldots,\ (a_{m-1}, a_m),\ (a_m, a_{m+1}). \tag{6.67}$$

Taigi pakanka išnagrinėti, kiek skiriasi funkcijos $W(x)$ reikšmė gretimuose (6.67) intervaluose. Nagrinėkime du gretimus (6.67) intervalus (a_{i-1}, a_i) ir (a_i, a_{i+1}). Galimi du atvejai:

1) skaičius a_i nėra polinomo $p(x)$ šaknis;

2) skaičius a_i yra polinomo $p(x)$ šaknis.

1) atvejis. Tarkime, kad skaičius a_i nėra polinomo $p(x)$ šaknis. Įrodysime, kad funkcijos $W(x)$ reikšmė, kai x pereina iš intervalo (a_{i-1}, a_i) į intervalą (a_i, a_{i+1}), nepasikeičia (t. y. funkcijos $W(x)$ reikšmės intervaluose (a_{i-1}, a_i) ir (a_i, a_{i+1}) sutampa). Iš tikrųjų, jei kiekvienas (6.66) Šturmo sistemos polinomas nekeičia savo ženklo, kai x pereina iš intervalo (a_{i-1}, a_i) į intervalą (a_i, a_{i+1}), tai ir funkcijos $W(x)$ reikšmės intervaluose (a_{i-1}, a_i) ir (a_i, a_{i+1}) sutampa. Tarkime, kad atsiras (6.66) sistemos polinomas $p_k(x)$, kurio ženklai intervaluose (a_{i-1}, a_i) ir (a_i, a_{i+1}) yra priešingi. Tuomet skaičius a_i yra šio polinomo šaknis. Be to, $k \geq 1$ (nes skaičius a_i nėra polinomo $p(x)$ šaknis). Iš Šturmo sistemos apibrėžimo (iii) sąlygos gauname nelygybę

$$p_{k-1}(a_i)p_{k+1}(a_i) < 0. \tag{6.68}$$

Taigi polinomai $p_{k-1}(x)$ ir $p_{k+1}(x)$ neturi šaknų intervale (a_{i-1}, a_{i+1}), todėl jie nekeičia ženklo šiame intervale. Be to, iš (6.68) nelygybės matyti, kad polinomų $p_{k-1}(x)$ ir $p_{k+1}(x)$ ženklai intervale (a_{i-1}, a_{i+1}) yra priešingi. Taigi polinomų šeima

$$p_{k-1}(x),\ p_k(x),\ p_{k+1}(x) \tag{6.69}$$

abiejuose intervaluose (a_{i-1}, a_i) ir (a_i, a_{i+1}) turi lygiai vieną ženklo pokytį. Pavyzdžiui, jei polinomas $p_{k-1}(x)$ intervale (a_{i-1}, a_{i+1}) yra neigiamas, o polinomas $p_k(x)$, pereinant iš intervalo (a_{i-1}, a_i) į intervalą (a_i, a_{i+1}), keičia ženklą iš $+$ į $-$, tai (6.69) polinomų sistemos ženklai intervaluose (a_{i-1}, a_i) ir (a_i, a_{i+1}) yra atitinkamai

$$\begin{array}{ccc} - & + & + \\ - & - & + \end{array}$$

Taigi funkcijos $W(x)$ reikšmės intervaluose (a_{i-1}, a_i) ir (a_i, a_{i+1}) sutampa.

2) atvejis. Tarkime, kad skaičius a_i yra polinomo $p_0(x) = p(x)$ šaknis. Iš Šturmo sistemos apibrėžimo (i) sąlygos matyti, kad polinomas $p_1(x)$ intervale (a_{i-1}, a_{i+1}) neturi šaknų, todėl šiame intervale nekeičia ženklo. Remiantis Šturmo sistemos apibrėžimo (iv) sąlyga, egzistuoja toks realusis skaičius $\varepsilon > 0$, kad sandauga $p_0(x)p_1(x)$ yra neigiama intervale $(a_i - \varepsilon, a_i)$ ir teigiama intervale $(a_i, a_i + \varepsilon)$. Vadinasi, polinomai $p_0(x)$ ir $p_1(x)$ yra priešingų ženklų intervale (a_{i-1}, a_i) ir to paties ženklo intervale (a_i, a_{i+1}). Taigi polinimų šeima

$$p_0(x),\ p_1(x)$$

intervale (a_{i-1}, a_i) turi vieną ženklo pokytį, o intervale (a_i, a_{i+1}) neturi ženklo pokyčio. Be to, lygiai taip pat kaip ir 1) atvejui, galima įsitikinti, kad polinomų šeima

$$p_1(x),\ p_2(x),\ \ldots,\ p_s(x)$$

turi tą patį ženklo pokyčių skaičių intervaluose (a_{i-1}, a_i) ir (a_i, a_{i+1}). Vadinasi, funkcijos $W(x)$ reikšmė intervale (a_{i-1}, a_i) vienetu didesnė už reikšmę intervale (a_i, a_{i+1}).

Taigi polinomo $p(x)$ Šturmo sistemos ženklo pokyčių skaičius $W(x)$ kiekviename iš (6.67) intervalų yra pastovi funkcija. Funkcijos $W(x)$ reikšmės gretimuose (6.67) intervaluose (a_{i-1}, a_i) ir (a_i, a_{i+1}) skiriasi tada ir tik tada, kai skaičius a_i yra polinomo $p(x)$ šaknis. Be to, minėtas skirtumas lygus vienetui: funkcijos $W(x)$ reikšmė intervale (a_{i-1}, a_i) yra vienetu didesnė už reikšmę intervale (a_i, a_{i+1}). Vadinasi, teisinga nelygybė $W(a) \geq W(b)$, o skirtumas $W(a) - W(b)$ lygus polinomo $p(x)$ šaknų, priklausančių intervalui (a, b), skaičiui. □

6.8.88 pavyzdys. Nustatysime, kiek polinomas

$$p(x) = x^4 - 3x^3 + 4x^2 - 3x - 2 \in \mathbb{R}[x]$$

turi realiųjų šaknų intervale $(-2,\ 3)$.

Sprendimas. Nesunku įsitikinti, kad polinomai $p(x)$ ir $p'(x)$ yra tarpusavyje pirminiai, todėl (remiantis 6.8.41 teiginiu) polinomas $p(x)$ neturi kartotinių šaknų. Sudarome polinomo $p(x)$ Šturmo sistemą (žr. 6.8.84 pavyzdį ir 6.8.85 pastabą):

$$\begin{aligned}
p_0(x) &= x^4 - 3x^3 + 4x^2 - 3x - 2 \\
p_1(x) &= 4x^3 - 9x^2 + 8x - 3 \\
p_2(x) &= -5x^2 + 12x + 41 \\
p_3(x) &= -22x - 1 \\
p_4(x) &= -1
\end{aligned}$$

Iš čia gauname tokią lentelę:

	$p_0(x)$	$p_1(x)$	$p_2(x)$	$p_3(x)$	$p_4(x)$	Ženklo pokyčių skaičius $W(x)$
$x = -2$	$+$	$-$	$-$	$+$	$-$	3
$x = 3$	$+$	$+$	$+$	$-$	$-$	1

Remiantis Šturmo teorema, polinomas $p(x)$ intervale $(-2,\ 3)$ turi lygiai dvi $(W(-2) - W(3) = 2)$ realiąsias šaknis. □

6.8.89 pastaba. Norėdami suskaičiuoti, kiek iš viso polinomas $p(x)$ turi realiųjų šaknų, turėtume rasti tokį intervalą (a, b), kuriam priklausytų visos šio polinomo šaknys, ir tada suskaičiuoti skirtumą $W(a) - W(b)$.

Nurodysime būdą, kaip suskaičiuoti, kiek polinomas turi realiųjų šaknų, kai žinoma kokia nors jo Šturmo sistema. Tarkime, kad polinomas $p(x) \in \mathbb{R}[x]$, $\deg p(x) > 0$, neturi kartotinių šaknų ir

$$p_0(x) = p(x),\ p_1(x),\ p_2(x),\ \ldots,\ p_s(x) \tag{6.70}$$

yra šio polinomo Šturmo sistema. Be to, sakykime, kad polinomo

$$p_j(x) = a_j x^{n_j} + \cdots, \quad 0 \le j \le s,$$

laipsnis $\deg p_j(x) = n_j$. Jei skaičiaus $x_0 \in \mathbb{R}$ modulis $|x_0|$ yra pakankamai didelis, tai kiekvieno (6.70) Šturmo sistemos polinomo $p_j(x)$ reikšmės taške $x = x_0$ ženklas priklauso tik nuo to polinomo vyriausiojo nario $a_j x^{n_j}$ ženklo taške $x = x_0$, t. y.

$$\operatorname{sgn}\big(p_j(x_0)\big) = \begin{cases} \operatorname{sgn}\big(a_j(-1)^{n_j}\big) & \text{jei } x_0 < 0, \\ \operatorname{sgn}\big(a_j\big) & \text{jei } x_0 > 0. \end{cases} \tag{6.71}$$

Ženklo pokyčių skaičių sekose

$$a_0(-1)^{n_0}, \quad a_1(-1)^{n_1}, \quad \ldots, \quad a_s(-1)^{n_s}$$

ir

$$a_0, \quad a_1, \quad \ldots, \quad a_s$$

atitinkamai pažymėkime $W_{-\infty}$ ir W_{∞}. Tuomet, remiantis Šturmo teorema ir (6.71) lygybe, polinomo $p(x)$ visų realiųjų šaknų skaičius lygus

$$W_{-\infty} - W_{\infty}.$$

6.8.90 pavyzdys. Nustatysime, kiek polinomas

$$p(x) = x^4 - 3x^3 + 4x^2 - 3x - 2 \in \mathbb{R}[x]$$

iš viso turi realiųjų šaknų. Be to, kiekvienai šio polinomo šakniai nurodysime tokį baigtinį intervalą, kuriam priklauso tik viena polinomo $p(x)$ šaknis.

Sprendimas. Kaip ir 6.8.88 pavyzdyje, sudarome polinomo $p(x)$ Šturmo sistemą:

$$\begin{aligned} p_0(x) &= x^4 - 3x^3 + 4x^2 - 3x - 2 \\ p_1(x) &= 4x^3 - 9x^2 + 8x - 3 \\ p_2(x) &= -5x^2 + 12x + 41 \\ p_3(x) &= -22x - 1 \\ p_4(x) &= -1. \end{aligned}$$

6.8.89 pastaboje aptarėme, kaip rasti polinomo $p(x)$ visų realiųjų šaknų skaičių. Randame ženklo pokyčių skaičius $W_{-\infty}$ ir W_{∞}:

	$p_0(x)$	$p_1(x)$	$p_2(x)$	$p_3(x)$	$p_4(x)$	Ženklo pokyčių skaičiai $W_{\pm\infty}$
$-\infty$	$+$	$-$	$-$	$+$	$-$	3
∞	$+$	$+$	$-$	$-$	$-$	1

Taigi polinomas $p(x)$ iš viso turi dvi realiąsias šaknis. Šią lentelę papildome eilutėmis, atitinkančiomis reikšmes $x = -2$, $x = 0$ ir $x = 3$:

	$p_0(x)$	$p_1(x)$	$p_2(x)$	$p_3(x)$	$p_4(x)$	Ženklo pokyčių skaičius
$-\infty$	$+$	$-$	$-$	$+$	$-$	3
$x = -2$	$+$	$-$	$-$	$+$	$-$	3
$x = 0$	$-$	$-$	$+$	$-$	$-$	2
$x = 3$	$+$	$+$	$+$	$-$	$-$	1
∞	$+$	$+$	$-$	$-$	$-$	1

Iš šios lentelės matyti, kad viena polinomo realioji šaknis priklauso intervalui $(-2, 0)$, o kita – intervalui $(0, 3)$.

□

6.8.91 pavyzdys. Nustatysime, kiek polinomas

$$p(x) = x^5 + 7x^4 + 13x^3 + 15x^2 + 7x - 4 \in \mathbb{R}[x]$$

iš viso turi realiųjų šaknų ir kiekvienai realiajai šakniai nurodysime tokį baigtinį intervalą, kuriam priklauso tik viena polinomo $p(x)$ šaknis.

Sprendimas. Nesunku įsitikinti, kad polinomai $p(x)$ ir $p'(x)$ yra tarpusavyje pirminiai, todėl (remiantis 6.8.41 teiginiu) polinomas $p(x)$ neturi kartotinių šaknų. Sudarome polinomo $p(x)$ Šturmo sistemą (žr. 6.8.84 pavyzdį ir 6.8.85 pastabą):

$$\begin{aligned}
p_0(x) &= x^5 + 7x^4 + 13x^3 + 15x^2 + 7x - 4\\
p_1(x) &= 5x^4 + 28x^3 + 39x^2 + 30x + 7\\
p_2(x) &= 66x^3 + 48x^2 + 70x + 149\\
p_3(x) &= -464x^2 + 207x + 1394\\
p_4(x) &= -269417x - 339550\\
p_5(x) &= -1.
\end{aligned}$$

Iš čia gauname tokią lentelę:

	$p_0(x)$	$p_1(x)$	$p_2(x)$	$p_3(x)$	$p_4(x)$	$p_5(x)$	Ženklo pokyčių skaičius
$-\infty$	$-$	$+$	$-$	$-$	$+$	$-$	4
-5	$-$	$+$	$-$	$-$	$+$	$-$	4
-3	$+$	$-$	$-$	$-$	$+$	$-$	3
-1	$-$	$-$	$+$	$+$	$-$	$-$	2
1	$+$	$+$	$+$	$+$	$-$	$-$	1
∞	$+$	$+$	$+$	$-$	$-$	$-$	1

Iš šios lentelės antrosios ir septintosios eilučių matome, kad polinomas $p(x)$ iš viso turi tris realiąsias šaknis $x_1 < x_2 < x_3$. Be to, iš trečiosios – šeštosios eilučių matyti, kad

$$x_1 \in (-5,\,-3),\;\; x_2 \in (-3,\,-1) \quad \text{ir} \quad x_3 \in (-1,\,1).$$

$\square$

6.9 Polinomų žiedo $k[x]$ idealų struktūra

Polinomų žiedo $k[x]$ idealų struktūra yra paprasta.

6.9.1 teiginys. *Polinomų žiedas $k[x]$ yra pagrindinių idealų žiedas, t. y., jei $\mathfrak{a}$ yra žiedo $k[x]$ idealas, tai egzistuoja toks polinomas $f(x) \in k[x]$, kad*

$$\mathfrak{a} = f(x) \cdot k[x].$$

Kaip įprasta, $f(x) \cdot k[x] = \{f(x)g(x) |\; g(x) \in k[x]\}$.

Įrodymas. Jei $\mathfrak{a} = \{0\}$, tai

$$\mathfrak{a} = \{0\} = 0 \cdot k[x].$$

Jei $\mathfrak{a} \neq \{0\}$, tai egzistuoja mažiausio laipsnio nenulinis polinomas $f(x)$, priklausantis idealui $\mathfrak{a}$. Remdamiesi idealo apibrėžimu, gauname, kad

$$f(x) \cdot k[x] \subset \mathfrak{a}\,.$$

Įrodysime, jog kiekvienas idealo $\mathfrak{a}$ polinomas priklauso $f(x) \cdot k[x]$, t. y. $f(x)$ dalija kiekvieną polinomą, priklausantį idealui $\mathfrak{a}$. Sakykime, $g(x) \in \mathfrak{a}$. Polinomams $f(x)$ ir $g(x)$ pritaikę dalybos su liekana formulę, galime parašyti:

$$g(x) = f(x) \cdot h(x) + r(x),\;\; \deg r(x) < \deg f(x).$$

Kadangi $g(x) \in \mathfrak{a}$, $f(x) \in \mathfrak{a}$ ir $r(x) = g(x) - f(x) \cdot h(x)$, tai polinomas $r(x)$ priklauso idealui $\mathfrak{a}$. Tačiau $\deg r(x) < \deg f(x)$, todėl $r(x) = 0$, nes priešingu atveju gautume prieštaravimą polinomo $f(x)$ išrinkimui (kaip mažiausio laipsnio nenulinio polinomo, priklausančio idealui $\mathfrak{a}$). Iš lygybės $r(x) = 0$ gauname

$$g(x) = f(x) \cdot h(x),$$

t. y. $g(x) \in f(x) \cdot k[x]$. Taigi $\mathfrak{a} = f(x) \cdot k[x]$. □

Akivaizdu, kad $f(x)\cdot k[x] \subset g(x)\cdot k[x]$ tada ir tik tada, kai $g(x)|f(x)$. Vadinasi, $f(x) \cdot k[x] = g(x) \cdot k[x]$ tada ir tik tada, kai $f(x)|g(x)$ ir $g(x)|f(x)$, t. y., kai polinomai $f(x)$ ir $g(x)$ yra ekvivalentūs.

6.9.2 teiginys. *Polinomų žiedo $k[x]$ idealas $f(x)\cdot k[x]$ yra maksimalus tada ir tik tada, kai $f(x)$ yra pirminis virš kūno k polinomas.*

Įrodymas. *Būtinumas.* Sakykime, kad idealas $f(x) \cdot k[x]$ nėra maksimalus. Tuomet egzistuoja toks idealas $g(x) \cdot k[x]$, kad

$$f(x) \cdot k[x] \subset g(x) \cdot k[x] \subset k[x],$$

bet

$$f(x) \cdot k[x] \neq g(x) \cdot k[x] \quad \text{ir} \quad g(x) \cdot k[x] \neq k[x]. \tag{6.72}$$

Iš sąlygos $f(x) \cdot k[x] \subset g(x) \cdot k[x]$ gauname, kad $g(x)|f(x)$, o iš (6.72) sąlygų išplaukia nelygybės $\deg g(x) > 0$ ir $\deg g(x) < \deg f(x)$. Taigi šiuo atveju $f(x)$ nėra pirminis virš kūno k.

Pakankamumas. Tarkime, kad $f(x)$ yra pirminis polinomas virš kūno k. Sakykime, kad $g(x) \in k[x]$ yra toks polinomas, kad

$$f(x) \cdot k[x] \subset g(x) \cdot k[x].$$

Tuomet $g(x)|f(x)$. Kadangi $f(x)$ yra pirminis polinomas virš kūno k, tai arba $g(x) \in k^*$, arba $f(x)$ ir $g(x)$ yra ekvivalentūs. Pirmuoju atveju idealas $g(x) \cdot k[x]$ sutampa su visu žiedu $k[x]$, o antruoju – $f(x)\cdot k[x] = g(x)\cdot k[x]$. Kaip matome, jei $f(x)$ yra pirminis polinomas virš kūno k, tai idealas $f(x)\cdot k[x]$ yra maksimalus. □

Anksčiau įrodėme, kad žiedo faktoržiedas pagal maksimalų idealą yra kūnas. Sakykime, $f(x)$ – žiedo $k[x]$ pirminis polinomas virš kūno k. Kaip žinome, $f(x) \cdot k[x]$ yra žiedo $k[x]$ maksimalus idealas. Trumpumo dėlei šį idealą pažymėkime raide $\mathfrak{f}$.

6.9.3. Dabar tirsime polinomų žiedo $k[x]$ faktoržiedą $k[x]/\mathfrak{f}$ pagal maksimalų idealą $\mathfrak{f} = f(x) \cdot k[x]$.

6.9.4 teorema. *Tarkime, kad $f(x) \in k[x]$ pirminis polinomas virš kūno k. Polinomų žiedo $k[x]$ faktoržiedas $k[x]/\mathfrak{f}$ pagal maksimalų idealą $\mathfrak{f} = f(x) \cdot k[x]$ yra kūno k plėtinys (kūnas, kurio pokūnis yra k), kuriame polinomas $f(x)$ turi šaknį.*

Įrodymas. Polinomų žiedo $k[x]$ faktoržiedas $k[x]/\mathfrak{f}$ pagal maksimalų idealą $\mathfrak{f} = f(x) \cdot k[x]$ yra kūnas. Nagrinėkime faktoržiedo $k[x]/\mathfrak{f}$ elementus $\alpha + \mathfrak{f}$, $\alpha \in k$. Įsitikinsime, kad atvaizdis

$$F : k \to k[x]/\mathfrak{f}, \quad \alpha \to \alpha + \mathfrak{f}, \quad \alpha \in k,$$

yra injekcinis homomorfizmas. Sakykime, kad $F(\alpha) = F(\beta)$, $\alpha, \beta \in k$. Kadangi $F(\alpha) = \alpha + \mathfrak{f}$, $F(\beta) = \beta + \mathfrak{f}$, tai iš lygybės $F(\alpha) = F(\beta)$ gauname lygybę $\alpha + \mathfrak{f} = \beta + \mathfrak{f}$, t. y. $\alpha - \beta \in \mathfrak{f}$. Sąlyga $\alpha - \beta \in \mathfrak{f}$ ekvivalenti sąlygai $f(x)|\alpha - \beta$. Bet $f(x)|\alpha - \beta$ tik tuo atveju, jei $\alpha - \beta = 0$, nes deg $f(x) > 0$, o deg $(\alpha - \beta) \leq 0$. Įrodėme, kad F – injekcinis atvaizdis.

Dabar įsitikinsime, kad F yra homomorfizmas. Bet kuriems $\alpha, \beta \in k$, gauname $F(\alpha + \beta) = \alpha + \beta + \mathfrak{f} = (\alpha + \mathfrak{f}) + (\beta + \mathfrak{f}) = F(\alpha) + F(\beta)$. Panašiai bet kuriems $\alpha, \beta \in k$, gauname $F(\alpha \cdot \beta) = \alpha \cdot \beta + \mathfrak{f} = (\alpha + \mathfrak{f}) \cdot (\beta + \mathfrak{f}) = F(\alpha) \cdot F(\beta)$.

Kadangi $F : k \to k[x]/\mathfrak{f}$ injekcinis homomorfizmas, tai galime sutapatinti kūną k su jo vaizdu $F(k) \in k[x]/\mathfrak{f}$. Pažymėję kūną $k[x]/\mathfrak{f}$ raide K, kūną k galime nagrinėti kaip kūno K pokūnį. Taigi $f(x) \in k[x] \subset K[x]$. Pažymėkime raide θ kūno $K = k[x]/\mathfrak{f}$ (priminsime, kad $\mathfrak{f} = f(x) \cdot k[x]$) elementą $x + \mathfrak{f}$. Sakykime, kad

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0,$$

$a_j \in k \subset K$, $0 \leq j \leq n$. Tuomet

$$f(\theta) = a_n \theta^n + a_{n-1} \theta^{n-1} + \cdots + a_1 \theta + a_0 = f(x) + \mathfrak{f} = \mathfrak{f}.$$

Tačiau $\mathfrak{f}$ yra kūno K nulinis elementas, todėl $f(\theta) = 0$, t. y. $\theta \in K$ yra polinomo $f(x)$ šaknis. □

6.9.5 pavyzdys. Nagrinėkime $\mathbb{Q}[x]$ ir polinomą $x^2 - 2$. Šis polinomas yra pirminis virš $\mathbb{Q}$. Faktoržiedo $\mathbb{Q}[x]/((x^2 - 2) \cdot \mathbb{Q}[x])$ elementai vienareikšmiškai gali būti užrašomi taip: $a + bx + (x^2 - 2) \cdot \mathbb{Q}[x]$. Sudauginkime šio faktoržiedo du elementus :

$$(a + bx + (x^2 - 2) \cdot \mathbb{Q}[x]) \cdot (c + dx + (x^2 - 2) \cdot \mathbb{Q}[x]) =$$

$$= ac + (ad + bc)x + bdx^2 + (x^2 - 2) \cdot \mathbb{Q}[x] =$$

$$= ac + (ad + bc)x + bd(x^2 - 2 + 2) + (x^2 - 2) \cdot \mathbb{Q}[x] =$$

$$ac + 2bd + (ad + bc)x + (x^2 - 2) \cdot \mathbb{Q}[x].$$

Kita vertus, aibė

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

skaičių sudėties ir daugybos atžvilgiu yra kūnas. Tuo įsitikinsime. Akivaizdu, kad ši aibė yra stabili sudėties ir daugybos atžvilgiu (t. y., jei $u, v \in \mathbb{Q}(\sqrt{2})$, tai $u+v,\, uv \in \mathbb{Q}(\sqrt{2}))$. Vadinasi, $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ yra komutatyvus žiedas. Jei $a + b\sqrt{2} \neq 0$, tai

$$\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{(a-b\sqrt{2})\cdot(a+b\sqrt{2})} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2} + \frac{-b\sqrt{2}}{a^2-2b^2}.$$

Įsitikinome, kad $(\mathbb{Q}(\sqrt{2}), +, \cdot)$ yra kūnas. Dabar įrodysime, kad faktoržiedas

$$\mathbb{Q}[x]/((x^2-2)\cdot\mathbb{Q}[x])$$

yra izomorfinis kūnui $(\mathbb{Q}(\sqrt{2}), +, \cdot)$. Atvaizdis

$$F : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}[x]/((x^2-2)\cdot\mathbb{Q}[x]),$$

$F(a+b\sqrt{2}) = a+bx+(x^2-2)\cdot\mathbb{Q}[x]$, $a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, yra izomorfizmas. Iš tikrųjų, akivaizdu, kad F yra bijekcija. Iš anksčiau sudaugintų kūno $\mathbb{Q}[x]/((x^2-2)\cdot\mathbb{Q}[x])$ elementų matome, kad F išsaugo sudėties ir daugybos veiksmus.

6.9.6 pavyzdys. Nagrinėkime $\mathbb{Q}[x]$ ir polinomą x^3-2. Polinomas x^3-2 yra pirminis virš racionaliųjų skaičių kūno $\mathbb{Q}$. Iš tikrųjų, jei šis polinomas nebūtų pirminis virš $\mathbb{Q}$, tai jį būtų galima išskaidyti arba į trijų pirmos eilės polinomų, arba į pirmos ir antros eilės polinomų su racionaliaisiais koeficientais sandaugą. Vienu ar kitu atveju šis polinomas turėtų racionalią šaknį. Bet kubinė šaknis iš dviejų nėra racionalusis skaičius, o kitos šio polinomo šaknys yra kompleksinės.

Faktoržiedo $\mathbb{Q}[x]/((x^3-2)\cdot\mathbb{Q}[x])$ elementai vienareikšmiškai užrašomi taip:

$$a + bx + cx^2 + (x^3-2)\cdot\mathbb{Q}[x].$$

Prieš sudaugindami kūno $\mathbb{Q}[x]/((x^3-2)\cdot\mathbb{Q}[x])$ du elementus, sutarkime idealą $(x^3-2)\cdot\mathbb{Q}[x]$ žymėti $\mathfrak{m}$, o faktoržiedą $\mathbb{Q}[x]/((x^3-2)\cdot\mathbb{Q}[x])$ – K. Sudauginkime šio kūno du elementus:

$$(a+bx+cx^2+\mathfrak{m})\cdot(a'+b'x+c'x^2+\mathfrak{m}) =$$

$$= aa' + (ab'+ba')x + (ac'+bb'+ca')x^2 + (bc'+cb')x^3 + cc'x^4 + \mathfrak{m} =$$

$$= aa' + (ab'+ba')x + (ac'+bb'+ca')x^2 +$$

$$+ (bc'+cb')(x^3-2+2) + cc'(x^4-2x+2x) + \mathfrak{m} =$$

$$= aa' + 2(bc'+cb') + (ab'+ba'+2cc')x + (ac'+bb'+ca')x^2 + \mathfrak{m},$$

nes $x^3-2,\, x^4-2x = (x^3-2)\cdot x \in \mathfrak{m}$.

Kaip ir 6.9.5 pavyzdyje, galima įsitikinti, kad aibė

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a,b,c \in \mathbb{Q}\}$$

yra kūnas, kuris izomorfinis kūnui K. Atvaizdis

$$F : \mathbb{Q}(\sqrt[3]{2}) \to K = \mathbb{Q}[x]/((x^3 - 2) \cdot \mathbb{Q}[x]),$$

$F(a + b\sqrt[3]{2} + c\sqrt[3]{4}) = a + bx + cx^2 + \mathfrak{m}$, $a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$, yra šių kūnų izomorfizmas.

Pratimas. Pasinaudoję Euklido algoritmu, raskite elementui

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \neq 0,$$

$a, b, c \in \mathbb{Q}$, atvirkštinį elementą.

7 skyrius

Matricos ir determinantai

7.1 Antrosios eilės matricos determinantas

7.1.1. Nagrinėkime tiesinių lygčių sistemą:

$$\begin{cases} a_{11}x & + a_{12}y = b_1 \\ a_{21}x & + a_{22}y = b_2 \end{cases}. \tag{7.1}$$

Šią lygčių sistemą galime išspręsti taip: pirmąją lygtį padauginę iš a_{22} ir pridėję prie antrosios, padaugintos iš $-a_{12}$, gauname lygtį

$$(a_{11}a_{22} - a_{12}a_{21})x = b_1a_{22} - b_2a_{12}.$$

(7.1) lygčių sistemos pirmąją lygtį padauginę iš $-a_{21}$ ir pridėję prie antrosios, padaugintos iš a_{11}, gauname lygtį

$$(a_{11}a_{22} - a_{12}a_{21})y = a_{11}b_2 - a_{12}b_1.$$

Taigi (7.1) lygčių sistemos sprendinys yra toks:

$$x = \frac{b_1a_{22} - b_2a_{12}}{a_{11}a_{22} - a_{12}a_{21}}, \ y = \frac{a_{11}b_2 - a_{12}b_1}{a_{11}a_{22} - a_{12}a_{21}}.$$

7.1.2. Patogu nagrinėti matricas (skaičių lenteles)

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}, \begin{pmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{pmatrix}, \begin{pmatrix} a_{11} & b_1 \\ a_{21} & b_2 \end{pmatrix}.$$

Pirmoji matrica yra sudaryta iš (7.1) lygčių sistemos koeficientų prie nežinomųjų. Antroji matrica gauta iš pirmosios, pakeitus joje pirmąjį stulpelį (7.1) lygčių sistemos laisvaisiais nariais. Analogiškai trečioji matrica gauta iš pirmosios, pakeitus joje antrąjį stulpelį (7.1) lygčių sistemos laisvaisiais nariais. Reiškinys $a_{11}a_{22} - a_{12}a_{21}$ vadinamas pirmosios matricos *determinantu*. Reiškiniai

$$b_1a_{22} - b_2a_{12} \;\text{ ir }\; a_{11}b_2 - a_{12}b_1$$

yra antrosios ir trečiosios matricų determinantai. Matricos

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

determinantas $a_{11}a_{22} - a_{12}a_{21}$ yra žymimas

$$\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad \text{arba} \quad \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}.$$

7.1.3. Taigi (7.1) lygčių sistemos srendinį galime užrašyti taip:

$$x = \frac{\det \begin{pmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{pmatrix}}{\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}}, \quad y = \frac{\det \begin{pmatrix} a_{11} & b_1 \\ a_{21} & b_2 \end{pmatrix}}{\det \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}}.$$

Šios (7.1) lygčių sistemos sprendinio formulės universalios. Nagrinėjant bendrosios lygčių sistemos sprendinio formules, nebūtina nurodyti, kad

$$a_{11}a_{22} - a_{12}a_{21} \neq 0.$$

Kaip matome, šis raidinis reiškinys yra nesuprastinamas ir todėl nėra lygus 0. Rūpintis, kad vardiklis nevirstų nuliu, reikia tik tada, kai dydžius $a_{11}, a_{22}, a_{12}, a_{21}$ pakeičiame, pavyzdžiui, skaitinėmis reikšmėmis.

7.2 Trečiosios eilės matricos determinantas

7.2.1. Dabar nagrinėkime bendrąją trijų tiesinių lygčių su trimis nežinomaisiais sistemą:

$$\begin{cases} a_{11}x + a_{12}y + a_{13}z = b_1 \\ a_{21}x + a_{22}y + a_{23}z = b_2 \\ a_{31}x + a_{32}y + a_{33}z = b_3 \end{cases}. \tag{7.2}$$

Šią lygčių sistemą pertvarkysime. Pirmąją lygtį, padauginę iš a_{22} ir pridėję prie antrosios lygties, padaugintos iš $-a_{12}$, gauname:

$$(a_{11}a_{22} - a_{12}a_{21})x + (a_{13}a_{22} - a_{23}a_{12})z = b_1a_{22} - b_2a_{12}.$$

Pirmąją lygtį, padauginę iš $-a_{32}$ ir pridėję prie trečiosios lygties, padaugintos iš a_{12}, gauname:

$$(-a_{11}a_{32} + a_{12}a_{31})x + (-a_{13}a_{32} + a_{33}a_{12})z = -b_1a_{32} + b_3a_{12}.$$

Antrąją lygtį padauginę iš $-a_{32}$ ir pridėję prie trečiosios lygties, padaugintos iš a_{22}, gauname:

$$(-a_{21}a_{32} + a_{22}a_{31})x + (-a_{23}a_{32} + a_{33}a_{22})z = -b_2a_{32} + b_3a_{22}.$$

Gavome tokias tris lygtis:

$$\begin{cases} (a_{11}a_{22} - a_{12}a_{21})x & +(a_{13}a_{22} - a_{23}a_{12})z & = b_1a_{22} - b_2a_{12} \\ (a_{12}a_{31} - a_{11}a_{32})x & +(a_{33}a_{12} - a_{13}a_{32})z & = b_3a_{12} - b_1a_{32} \\ (a_{22}a_{31} - a_{21}a_{32})x & +(a_{33}a_{22} - a_{23}a_{32})z & = b_3a_{22} - b_2a_{32} \end{cases}$$

Pirmąją iš šių lygčių padauginę iš a_{33}, antrąją – iš a_{23}, trečiąją – iš $-a_{13}$ ir sudėję gautus rezultatus, gauname:

$$(a_{11}a_{22}a_{33} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} - a_{11}a_{23}a_{32} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31})x =$$

$$= b_1(a_{22}a_{33} - a_{23}a_{32}) - b_2(a_{12}a_{33} - a_{13}a_{32}) + b_3(a_{12}a_{23} - a_{13}a_{22}).$$

Tuomet

$$x = \frac{b_1(a_{22}a_{33} - a_{23}a_{32}) - b_2(a_{12}a_{33} - a_{13}a_{32}) + b_3(a_{12}a_{23} - a_{13}a_{22})}{a_{11}a_{22}a_{33} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} - a_{11}a_{23}a_{32} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}} =$$

$$= \frac{b_1(a_{22}a_{33} - a_{23}a_{32}) - b_2(a_{12}a_{33} - a_{13}a_{32}) + b_3(a_{12}a_{23} - a_{13}a_{22})}{a_{11}(a_{22}a_{33} - a_{23}a_{32}) - a_{21}(a_{12}a_{33} - a_{13}a_{32}) + a_{31}(a_{12}a_{23} - a_{13}a_{22})} =$$

$$= \frac{b_1\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - b_2\begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + b_3\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}}{a_{11}\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{21}\begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + a_{31}\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}}.$$

7.2.2. Apibrėžkime matricos (skaičių lentelės)

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

determinantą taip:

$$\det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11}\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{21}\begin{vmatrix} a_{12} & a_{13} \\ a_{32} & a_{33} \end{vmatrix} + a_{31}\begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} =$$

$$= a_{11}a_{22}a_{33} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} - a_{11}a_{23}a_{32} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}.$$

Tada (7.2) lygčių sistemos sprendinio x-komponentės reikšmę galima užrašyti taip:

$$x = \frac{\det\begin{pmatrix} b_1 & a_{12} & a_{13} \\ b_2 & a_{22} & a_{23} \\ b_3 & a_{32} & a_{33} \end{pmatrix}}{\det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}}.$$

Panašiai galima užrašyti (7.2) lygčių sistemos sprendinio y ir z-komponenčių reikšmes:

$$y = \frac{\det\begin{pmatrix} a_{11} & b_1 & a_{13} \\ a_{21} & b_2 & a_{23} \\ a_{31} & b_3 & a_{33} \end{pmatrix}}{\det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}}, \quad z = \frac{\det\begin{pmatrix} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \\ a_{31} & a_{32} & b_3 \end{pmatrix}}{\det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}}.$$

Panagrinėję šiuos pavyzdžius, galime tikėtis, kad ir n lygčių su n nežinomaisiais sistemos atveju egzistuoja universalios formulės sprendinio komponentėms užrašyti. Iš tikrųjų, taip ir yra. Visų pirma, apibrėšime n-tos eilės kvadratinės matricos determinanto sąvoką ir įrodysime pagrindines determinanto savybes. Paskui rasime n lygčių su n nežinomaisiais sistemos sprendinio išraišką, vadinamą Kramerio taisykle.

7.3 Aritmetinė tiesinė erdvė k^n

Tegu k – kūnas, o n – natūralusis skaičius. Nagrinėkime aibę

$$k^n := \{(x_1, x_2, \dots, x_n) \mid x_j \in k,\ j = 1, 2, \dots, n\}.$$

Aibė k^n vadinama n-mate *aritmetine tiesine erdve* virš kūno k (plačiau apie tiesines erdves skaitykite antroje vadovėlio dalyje). Šios aibės elementai

$$(x_1, x_2, \dots, x_n)$$

vadinami *vektoriais*. Apibrėžkime erdvės k^n vektorių $u = (x_1, x_2, \dots, x_n)$ ir $v = (y_1, y_2, \dots, y_n)$ *sumą* ir *daugybą iš skaliaro* $\alpha \in k$:

$$\begin{aligned} u + v &:= (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n), \\ \alpha u &:= (\alpha x_1, \alpha x_2, \dots, \alpha x_n). \end{aligned}$$

Vektorius $(0, 0, \ldots, 0)$ vadinamas erdvės k^n *nuliniu vektoriumi* ir žymimas $\mathcal{O}$. Aritmetinę tiesinę erdvę k^1 įprasta sutapatinti su kūnu k.

Paliekame skaitytojui įsitikinti, kad bet kuriems aritmetinės erdvės k^n vektoriams u, v, w ir skaliarams $\alpha, \beta \in k$ teisingos lygybės:

1) $u + v = v + u$;

2) $(u + v) + w = u + (v + w)$;

3) $u + \mathcal{O} = \mathcal{O} + u = u$;

4) $u + (-1) \cdot u = \mathcal{O}$;

5) $1 \cdot u = u$;

6) $(\alpha\beta)u = \alpha(\beta u)$;

7) $(\alpha + \beta)u = \alpha u + \beta u$;

8) $\alpha(u + v) = \alpha u + \alpha v$.

Vektorius $(-1) \cdot v$ žymimas $-v$ ir vadinamas *priešingu* vektoriui v. Pažymėkime

$$\begin{aligned} e_1 &= (1, 0, 0, \ldots, 0), \\ e_2 &= (0, 1, 0, \ldots, 0), \\ &\ldots \quad \ldots \quad \ldots \quad \ldots \\ e_n &= (0, 0, 0, \ldots, 1). \end{aligned}$$

Nesunku įsitikinti, kad bet kurį aritmetinės erdvės k^n vektorių $(x_1, x_2, \ldots, x_n)$ galima išreikšti vektoriais $e_1, e_2, \ldots, e_n$:

$$(x_1, x_2, \ldots, x_n) = x_1 e_1 + x_2 e_2 + \cdots + x_n e_n.$$

Vektorių šeima $e_1, e_2, \ldots, e_n$ vadinama erdvės k^n *standartine baze*.

7.4 Matricos

7.4.1. Priminsime (žr. 6.2 skyrelį), kad kūno k elementų šeima $(\alpha_{ij}), 1 \leq i \leq m, 1 \leq j \leq n$, sunumeruota dviem indeksais ir surašyta į lentelę

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_{m1} & \alpha_{m2} & \ldots & \alpha_{mn} \end{pmatrix},$$

yra vadinama $m \times n$ *matrica*, o α_{ij} – šios matricos ij-elementu arba ij-komponente (α_{ij} – matricos elementas, užrašytas matricos i-tosios eilutės ir j-ojo stulpelio sankirtoje).

7.4.2. Priminsime, kad $m \times n$ matricą, nurodydami jos elementus, sutarėme sutrumpintai žymėti (α_{ij}). $m \times n$ matricos (α_{ij}) ir (β_{ij}) yra lygios tada ir tik tada, kai $\alpha_{ij} = \beta_{ij}$ visiems $i, j, 1 \leq i \leq m, 1 \leq j \leq n$. Visų $m \times n$ matricų, kurių elementai priklauso kūnui k, aibę žymime $M_{m \times n}(k)$.

Jei $m = n$, tai $n \times n$ matricos dar yra vadinamos n-tos eilės *kvadratinėmis matricomis.* Visų $n \times n$ matricų su koeficientais kūne k aibę žymime $M_n(k)$. n-tos eilės kvadratinių matricų aibės $M_n(k)$ matrica

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

žymima $\mathbf{1}_n$ ir vadinama *vienetine matrica.* Šią matricą galima dar ir taip išreikšti:

$$\mathbf{1}_n = (\delta_{ij}),$$

čia δ_{ij} – Kronekerio simbolis, apibrėžiamas taip:

$$\delta_{ij} = \begin{cases} 1, & \text{jei } \ i = j, \\ 0, & \text{jei } \ i \neq j \end{cases}.$$

Priminsime, kokius veiksmus galima atlikti su matricomis, ir tų veiksmų savybes (žr. 6.2 skyrelį).

$m \times n$ matricų (α_{ij}) ir (β_{ij}) *suma* vadinama $m \times n$ matrica $(\alpha_{ij} + \beta_{ij})$ ir žymima $(\alpha_{ij}) + (\beta_{ij})$. Taigi sudedant matricas sudedami atitinkami jos elementai, t. y.

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \cdots & \alpha_{2n} \\ & \cdots & \cdots & \\ \alpha_{m1} & \alpha_{m2} & \cdots & \alpha_{mn} \end{pmatrix} + \begin{pmatrix} \beta_{11} & \beta_{12} & \cdots & \beta_{1n} \\ \beta_{21} & \beta_{22} & \cdots & \beta_{2n} \\ & \cdots & \cdots & \\ \beta_{m1} & \beta_{m2} & \cdots & \beta_{mn} \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha_{11} + \beta_{11} & \alpha_{12} + \beta_{12} & \cdots & \alpha_{1n} + \beta_{1n} \\ \alpha_{21} + \beta_{21} & \alpha_{22} + \beta_{22} & \cdots & \alpha_{2n} + \beta_{2n} \\ & \cdots & \cdots & \\ \alpha_{m1} + \beta_{m1} & \alpha_{m2} + \beta_{m2} & \cdots & \alpha_{mn} + \beta_{mn} \end{pmatrix}.$$

Nesunku įsitikinti, kad $(M_{m \times n}(k), +)$ – Abelio grupė. $m \times n$ matrica

$$\begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ & \cdots & \cdots & \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

vadinama *nuline* matrica ir žymima $\mathcal{O}$. Nulinė matrica yra grupės $(M_{m\times n}(k), +)$ neutralus elementas, t. y. bet kuriai $m \times n$ matricai teisinga lygybė $A + \mathcal{O} = A$.

7.4.3. Skaičiaus $\lambda \in k$ ir $m \times n$ matricos (α_{ij}) sandauga vadinama matrica

$$\begin{pmatrix} \lambda\alpha_{11} & \lambda\alpha_{12} & \cdots & \lambda\alpha_{1n} \\ \lambda\alpha_{21} & \lambda\alpha_{22} & \cdots & \lambda\alpha_{2n} \\ & \cdots & \cdots & \\ \lambda\alpha_{m1} & \lambda\alpha_{m2} & \cdots & \lambda\alpha_{mn} \end{pmatrix}$$

ir žymima $\lambda\cdot(\alpha_{ij})$. Nesunku įsitikinti, kad bet kuriems $\lambda, \mu \in k$, $A, B \in M_{m\times n}(k)$ teisingos lygybės:

1. $\lambda \cdot (\mu A) = (\lambda\mu) \cdot A$.
2. $1 \cdot A = A$, čia 1 – kūno k vienetas.
3. $\lambda \cdot (A + B) = \lambda \cdot A + \lambda \cdot B$.
4. $(\lambda + \mu) \cdot A = \lambda \cdot A + \mu \cdot A$.

$m \times n$ matricos (α_{ij}) eilutes

$$(\alpha_{i1},\ \alpha_{i2},\ \ldots,\ \alpha_{in})$$

surašę vieną šalia kitos į vieną ilgą eilutę, šią matricą galime sutapatinti su aritmetinės tiesinės erdvės (žr. 7.3 skyrelį)

$$\underbrace{k^n \times k^n \times \cdots \times k^n}_{m} = k^{nm} \tag{7.3}$$

vektoriumi

$$(\alpha_{11},\ \ldots,\ \alpha_{1n},\ \alpha_{21},\ \ldots,\ \alpha_{2n},\ \ldots,\ \alpha_{m1},\ \ldots,\ \alpha_{mn}).$$

Taigi matricų aibę $M_{m\times n}(k)$ galime sutapatinti su (7.3) aritmetine tiesine erdve.

7.4.4. Apibrėšime matricų daugybą

$$\cdot : M_{m\times n}(k) \times M_{n\times p}(k) \to M_{m\times p}(k).$$

$m\times n$ matricos (α_{ij}) ir $n\times p$ matricos (β_{ij}) *sandauga* vadinama $m\times p$ matrica

$$(\alpha_{ij}) \cdot (\beta_{ij}) := (\gamma_{ij}),$$

kurios ij-elementas γ_{ij} apibrėžiamas taip:

$$\gamma_{ij} = \sum_{s=1}^{n} \alpha_{is} \cdot \beta_{sj}.$$

Pavyzdžiui,

$$\begin{pmatrix} 1 & 2 & 1 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 4 & 3 & 5 \\ 1 & 5 & 4 & 7 \\ 3 & 9 & 1 & 4 \end{pmatrix} = \begin{pmatrix} 7 & 23 & 12 & 23 \\ 10 & 32 & 19 & 35 \end{pmatrix}.$$

Kitaip sakant, matricos (γ_{ij}) ij-elementas yra gaunamas pirmosios matricos i eilutę paelemenčiui sudauginant su antrosios matricos j stulpeliu ir gautus rezultatus sudedant.

Paliekame skaitytojui įsitikinti, kad matricų daugyba turi tokias savybes:

1. $(A \cdot B) \cdot C = A \cdot (B \cdot C), \quad A \in M_{m\times n}(k),\ B \in M_{n\times p}(k),\ C \in M_{p\times r}(k).$
2. $(A + B) \cdot C = A \cdot C + B \cdot C, \quad A, B \in M_{m\times n}(k),\ C \in M_{n\times p}(k).$
3. $C \cdot (A + B) = C \cdot A + C \cdot B,\ C \in M_{m\times n}(k), \quad A, B \in M_{n\times p}(k).$
4. Kiekvienai matricai $A \in M_{m\times n}(k)$
$$\mathbf{1}_m \cdot A = A,$$
čia $\mathbf{1}_m$ – vienetinė matrica.
5. Kiekvienai matricai $A \in M_{m\times n}(k)$
$$A \cdot \mathbf{1}_n = A.$$

7.4.5 apibrėžimas. Nagrinėkime $m \times n$ matricą $A = (\alpha_{ij})$. Tada $n \times m$ matrica $A^t = (\beta_{ij})$, kurios elementai
$$\beta_{ij} = \alpha_{ji},$$
vadinama *transponuota* matricai A.

Pavyzdžiui,

$$\begin{pmatrix} 3 & 7 & 7 \\ 4 & 1 & 6 \\ 0 & 2 & 5 \end{pmatrix}^t = \begin{pmatrix} 3 & 4 & 0 \\ 7 & 1 & 2 \\ 7 & 6 & 5 \end{pmatrix}, \quad \begin{pmatrix} 3 & 7 & 2 \\ 4 & 1 & 5 \end{pmatrix}^t = \begin{pmatrix} 3 & 4 \\ 7 & 1 \\ 2 & 5 \end{pmatrix},$$

$$\begin{pmatrix} 3 & 7 & 7 \end{pmatrix}^t = \begin{pmatrix} 3 \\ 7 \\ 7 \end{pmatrix}.$$

Mus domins matricų daugyba kvadratinių matricų aibėje $M_n(k)$.

7.5 Kvadratinės matricos determinanto funkcija

7.5.1. Dabar nagrinėsime tik n-tos eilės kvadratines matricas $A \in M_n(k)$. Matricos

$$A = (\alpha_{ij})$$

i-tąją eilutę pažymėkime v_i, t. y.

$$v_i = (\alpha_{i1}\ \alpha_{i2}\ \ldots\ \alpha_{in}),\ 1 \leq i \leq n.$$

Tada matricą $A = (\alpha_{ij})$ galima užrašyti taip:

$$A = (\alpha_{ij}) = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} = \begin{pmatrix} v_1^t & v_2^t & \ldots & v_n^t \end{pmatrix}^t.$$

7.5.2. Artimiausias mūsų tikslas – apibrėžti atvaizdį

$$\det : M_n(k) \to k,\ A \mapsto \det A,\ \ A = (\alpha_{ij}) \in M_n(k),$$

tenkinantį sąlygas, kurias suformuluosime vėliau. Norėdami pabrėžti, kad šio atvaizdžio det reikšmė $\det A$ priklauso nuo matricos A eilučių, turėtume rašyti

$$\det \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix} \quad \text{arba} \quad \det\begin{pmatrix} v_1^t & v_2^t & \ldots & v_n^t \end{pmatrix}^t.$$

Bet šie užrašai nepatogūs. Norėdami pabrėžti, kad $\det A$ priklauso nuo matricos A eilučių, sutarkime rašyti $\det(v_1,\ v_2,\ \ldots,\ v_n)$, t. y. atvaizdį det traktuoti kaip matricos A eilučių funkciją.

7.5.3 teiginys. *Egzistuoja vienintelė funkcija*

$$\det : M_n(k) \to k,\ A \mapsto \det A,\ A = (\alpha_{ij}) \in M_n(k),$$

tenkinanti sąlygas:

1. det *yra matricos A eilučių n-tiesinė funkcija, t. y. funkcija* det *yra tiesinė pagal n-tos eilės kvadratinės matricos kiekvieną eilutę: kiekvienam j, $1 \leq j \leq n$,*

$$\det(v_1, \ldots, \lambda v_j' + \mu v_j'', \ldots, v_n) =$$
$$= \lambda \cdot \det(v_1, \ldots, v_j', \ldots, v_n) + \mu \cdot \det(v_1, \ldots, v_j'', \ldots, v_n).$$

2. det *yra matricos A eilučių alternuojanti funkcija, t. y., jei matricos $A = (\alpha_{ij})_{i,j=1}^{n}$ kurios nors dvi eilutės v_i ir v_j, $i \neq j$, $1 \leq i, j \leq n$, yra lygios, tai*

$$\det(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = 0.$$

3. Teisinga lygybė

$$\det \mathbf{1}_n = 1,$$

*čia $\mathbf{1}_n$ – vienetinė matrica (*det *– normuota funkcija, – vienetinės matricos determinantas lygus* 1*).*

Įrodymas. Tarkime, kad funkcija det egzistuoja. Visų pirma įrodysime, kad det turi tokią savybę: matricos determinantas keičia ženklą, sukeitus vietomis matricos dvi eilutes. Paskui įrodysime, kad tik vienintelė funkcija gali tenkinti išvardintas sąlygas, ir pagaliau įrodysime funkcijos det egzistavimą.

Remiantis antrąja sąlyga, bet kuriems i, j, $i \neq j$, $1 \leq i, j \leq n$, teisinga lygybė

$$0 = \det(v_1,\ \ldots,\ v_i + v_j,\ \ldots,\ v_i + v_j,\ \ldots,\ v_n) =$$

$$= \det(v_1,\ \ldots,\ v_i,\ \ldots,\ v_i,\ \ldots,\ v_n) + \det(v_1,\ \ldots,\ v_i,\ \ldots,\ v_j,\ \ldots,\ v_n) +$$

$$+ \det(v_1,\ \ldots,\ v_j,\ \ldots,\ v_i,\ \ldots,\ v_n) + \det(v_1,\ \ldots,\ v_j,\ \ldots,\ v_j,\ \ldots,\ v_n) =$$

$$= \det(v_1,\ \ldots,\ v_i,\ \ldots,\ v_j,\ \ldots,\ v_n) + \det(v_1,\ \ldots,\ v_j,\ \ldots,\ v_i,\ \ldots,\ v_n),$$

todėl

$$\det(v_1,\ \ldots,\ v_i,\ \ldots,\ v_j,\ \ldots,\ v_n) = -\det(v_1,\ \ldots,\ v_j,\ \ldots,\ v_i,\ \ldots,\ v_n).$$

Taigi sukeitus vietomis matricos dvi eilutes, jos determinantas keičia ženklą. Vadinasi, kiekvienam aibės $\mathbb{N}_n$ elementų keitiniui σ teisinga lygybė:

$$\det(v_{\sigma(1)},\ v_{\sigma(2)},\ \ldots,\ v_{\sigma(n)}) = \operatorname{sgn}(\sigma) \cdot \det(v_1,\ v_2,\ \ldots,\ v_n).$$

Dabar įrodysime funkcijos det vienatį. Užrašykime matricos $A = (\alpha_{ij})$ i-tąją eilutę v_i, $1 \leq i \leq n$, tiesinės erdvės k^n standartinės bazės vektoriais e_1, e_2, $\ldots$, e_n:

$$v_i = (\alpha_{i1},\ \alpha_{i2},\ \ldots,\ \alpha_{in}) = \alpha_{i1}e_1 + \alpha_{i2}e_2 + \cdots + \alpha_{in}e_n,$$

čia

$$e_1 = (1, 0, 0, \ldots, 0),$$

$$e_2 = (0, 1, 0, \ldots, 0),$$

$$\ldots \quad \ldots \quad \ldots \quad \ldots$$

$$e_n = (0, 0, 0, \ldots, 1).$$

Įrašę v_i, $1 \leq i \leq n$, išraiškas į $\det(v_1,\ v_2,\ \ldots,\ v_n)$ ir, remdamiesi pirmąja bei antrąja funkcijos det savybėmis, gauname:

$$\det\left(\sum_{j_1=1}^{n}\alpha_{1j_1}e_{j_1},\ \sum_{j_2=1}^{n}\alpha_{2j_2}e_{j_2},\ \sum_{j_3=1}^{n}\alpha_{3j_3}e_{j_3},\ \ldots,\ \sum_{j_n=1}^{n}\alpha_{nj_n}e_{j_n}\right) =$$

$$= \sum_{j_1=1}^{n}\alpha_{1j_1}\det\left(e_{j_1},\ \sum_{j_2=1}^{n}\alpha_{2j_2}e_{j_2},\ \sum_{j_3=1}^{n}\alpha_{3j_3}e_{j_3},\ \ldots,\ \sum_{j_n=1}^{n}\alpha_{nj_n}e_{j_n}\right) =$$

$$= \sum_{j_1=1}^{n}\alpha_{1j_1}\sum_{j_2=1}^{n}\alpha_{2j_2}\det\left(e_{j_1},\ e_{j_2},\ \sum_{j_3=1}^{n}\alpha_{3j_3}e_{j_3},\ \ldots,\ \sum_{j_n=1}^{n}\alpha_{nj_n}e_{j_n}\right) =$$

$$\ldots\ \ldots\ \ldots$$

$$= \sum_{j_1=1}^{n}\alpha_{1j_1}\sum_{j_2=1}^{n}\alpha_{2j_2}\cdots\sum_{j_n=1}^{n}\alpha_{nj_n}\det(e_{j_1},\ e_{j_2},\ \ldots,\ e_{j_n}) =$$

$$= \sum_{\sigma\in S_n}\alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\ldots\alpha_{n\sigma(n)}\det(e_{\sigma(1)},\ e_{\sigma(2)},\ \ldots,\ e_{\sigma(n)}) =$$

$$= \sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\ldots\alpha_{n\sigma(n)}\det(e_1,\ e_2,\ \ldots,\ e_n),$$

čia

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & r & \ldots & s & \ldots & n \\ j_1 & j_2 & \ldots & j_r & \ldots & j_s & \ldots & j_n \end{pmatrix}.$$

Taigi

$$\det((\alpha_{ij})_{ij=1}^{n}) = \sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\ldots\alpha_{n\sigma(n)},$$

nes $\det(e_1,\ e_2,\ \ldots,\ e_n) = 1$ (trečioji det savybė).

Pagaliau matematinės indukcijos metodu įrodysime determinanto funkcijos det egzistavimą.

Pirmos eilės matricai (α) apibrėžkime $\det(\alpha) = \alpha$. Sakykime, kad kiekvienai $n-1$-os eilės kvadratinei matricai A funkcija det, tenkinanti teiginyje išvardytas sąlygas, egzistuoja. Tegu $A = (\alpha_{ij}) \in M_n(k)$ – n-tos eilės matrica. Apibrėžkime bet kuriam r, $1 \leq r \leq n$,

$$\begin{aligned}\det(\alpha_{ij}) = (-1)^{r+1}\alpha_{1r}M^{1r} + (-1)^{r+2}\alpha_{2r}M^{2r} + \cdots +\\ +(-1)^{r+n}\alpha_{nr}M^{nr},\end{aligned} \tag{7.4}$$

čia M^{jr} – $n-1$-os eilės matricos, gautos matricoje $A = (\alpha_{ij})$ išbraukus j-ąją eilutę ir r-tąjį stulpelį, determinantas. Lieka įrodyti, kad ši funkcija tenkina teoremoje išvardytas sąlygas.

Išsirinkime matricos A s-tąją eilutę, $1 \leq s \leq n$. Jei $j \neq s$, $1 \leq j \leq n$, tai matricos A s-tosios eilutės elementai, išskyrus elementą, esantį r-tajame stulpelyje, sudaro ir determinanto M^{jr}, $1 \leq j \leq n$, $j \neq s$, kurią nors eilutę. Kadangi $n-1$-os eilės determinantai yra tiesinės funkcijos pagal kiekvieną eilutę, tai ir

$$\det(\alpha_{ij})_{ij=1}^{n} = (-1)^{r+s}\alpha_{sr}M^{sr} + \sum_{\substack{j=1\\ j\neq s}}^{n}(-1)^{r+j}\alpha_{jr}M^{jr},$$

yra tiesinė funkcija pagal s eilutę, nes ir dėmuo $(-1)^{r+s}\alpha_{sr}M^{sr}$ tiesiškai priklauso nuo s eilutės koordinatės α_{sr}.

Dabar įrodysime, kad, jei matricos A kurios nors dvi eilutės yra lygios, tai ir apibrėžtas n-tos eilės matricos A determinantas $\det(A)$ yra lygus nuliui. Tarkime, kad matricos A p-toji ir q-toji eilutės yra lygios, $p < q$. Tada sumos

$$\det A = \det(\alpha_{ij})_{ij=1}^{n} = \sum_{j=1}^{n}(-1)^{r+j}\alpha_{jr}M^{jr}$$

dėmenys $(-1)^{r+j}\alpha_{jr}M^{jr}$ lygūs 0, jei $j \neq p,\ q$, nes šiuo atveju determinantai M^{jr} turi po dvi lygias eilutes. Taigi iš šios sumos lieka tik dviejų dėmenų suma:

$$(-1)^{r+p}\alpha_{pr}M^{pr} + (-1)^{r+q}\alpha_{qr}M^{qr} = (-1)^{r+p}\alpha_{pr}(M^{pr} + (-1)^{q-p}M^{qr}).$$

Determinantas M^{pr} yra gaunamas iš determinanto M^{qr}, pastorojo determinanto eilutes sukeitus vietomis taip, kad šį sukeitimą atitinka keitinys

$$\sigma(j) = \begin{cases} j, & \text{jei } 1 \leq j \leq p-1, \\ j+1, & \text{jei } p \leq j \leq q-2, \\ p, & \text{jei } j = q-1, \\ j, & \text{jei } q \leq j \leq n-1. \end{cases}$$

Šį keitinį užrašę

$$\sigma = \begin{pmatrix} 1 & \ldots & p-1 & p & \ldots & q-1 & q & \ldots & n-1 \\ 1 & \ldots & p-1 & p+1 & \ldots & p & q & \ldots & n-1 \end{pmatrix},$$

suskaičiuokime, kiek skaičių porų antrojoje eilutėje sudaro inversijas. Kaip matome, skaičių poros, kurios sudaro inversijas, yra tik šios:

$$p+1\,p;\ \ p+2\,p;\ \ \ldots\ \ q-1\,p.$$

Šių porų yra $q-2-(p-1)=q-p-1$. Taigi suma

$$M^{pr}+(-1)^{q-p}M^{qr}=M^{pr}+(-1)^{q-p}(-1)^{q-p-1}M^{pr}=M^{pr}-M^{pr}=0.$$

Lieka įrodyti, kad $\det \mathbf{1}_n = 1$. Bet tai akivaizdu, nes

$$\det(e_1,\ e_2,\ \ldots,\ e_n)=\delta_{rr}\cdot\det(e_1',\ \ldots,\ \hat{e_r},\ \ldots,\ e_n')=1,$$

čia stogelis virš e_r žymi, kad e_r praleistas, o e_j', $j\neq r$, žymi, kad praleista vektoriaus e_j r-toji koordinatė. □

Įrodinėdami determinanto funkcijos (žr. 7.5.3 teiginį) vienatį, įrodėme, kad

$$\det A=\det(\alpha_{ij})=\sum_{\sigma\in S_n}\mathrm{sgn}(\sigma)\alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\ldots\alpha_{n\sigma(n)}. \tag{7.5}$$

7.5.4 apibrėžimas. Skaičius $\det A$, apibrėžtas (7.5) lygybe, vadinamas kvadratinės matricos A *determinantu.*

7.5.5 pastaba. Šią lygybę būtų galima panaudoti determinanto apibrėžimui. Tačiau, taip apibrėžę n-tos eilės kvadratinės matricos determinantą, turėtume įrodyti, kad ši determinanto funkcija tenkina tris sąlygas, suformuluotas 7.5.3 teiginyje.

Pratimas. Apibrėžę matricos $A=(\alpha_{ij})$ determinantą formule

$$\det A=\sum_{\sigma\in S_n}\mathrm{sgn}(\sigma)\alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\ldots\alpha_{n\sigma(n)},$$

įrodykite, kad ši funkcija tenkina tris determinanto funkcijos savybes (žr. 7.5.3 teiginį).

7.5.6. Remdamiesi (7.4) rekurenčiąja formule, n-tos eilės matricos determinantą galime apskaičiuoti, mokėdami apskaičiuoti $n-1$-os eilės determinantą. Remdamiesi šia formule, n-tos eilės matricos determinantą galime išskleisti bet kuriuo determinanto sulpeliu. Dabar įrodysime, kad n-tos eilės matricos A ir šios matricos transponuotos matricos A^t determinantai yra lygūs: $\det A=\det A^t$. Tada n-os eilės matricos determinantą galima išskleisti ir bet kuria determinanto eilute.

7.5.7 teiginys. *Tarkime, kad $A=(\alpha_{ij})$ – kvadratinė matrica. Tada*

$$\det A=\det A^t,$$

čia A^t – matricai A transponuota matrica.

Įrodymas. 7.5.3 teiginio įrodyme (įrodinėdami determinanto funkcijos vienatį) gavome lygybę:

$$\det A = \det(\alpha_{ij}) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\dots\alpha_{n\sigma(n)}.$$

Taigi

$$\det A^t = \det(\beta_{ij}) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\beta_{1\sigma(1)}\beta_{2\sigma(2)}\dots\beta_{n\sigma(n)},$$

čia $\beta_{ij} = \alpha_{ji}$, $i, j \in \{1, 2, \dots, n\}$. Kiekvienas šio determinanto dėmuo

$$\operatorname{sgn}(\sigma)\beta_{1\sigma(1)}\beta_{2\sigma(2)}\dots\beta_{n\sigma(n)} = \operatorname{sgn}(\sigma)\alpha_{\sigma(1)1}\alpha_{\sigma(2)2}\dots\alpha_{\sigma(n)n}.$$

Bet

$$\operatorname{sgn}(\sigma)\alpha_{\sigma(1)1}\alpha_{\sigma(2)2}\dots\alpha_{\sigma(n)n} = \operatorname{sgn}(\sigma)\alpha_{1\sigma^{-1}(1)}\alpha_{2\sigma^{-1}(2)}\dots\alpha_{n\sigma^{-1}(n)}.$$

Kadangi $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$, tai

$$\det A^t = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma^{-1})\alpha_{1\sigma^{-1}(1)}\alpha_{2\sigma^{-1}(2)}\dots\alpha_{n\sigma^{-1}(n)} =$$

$$= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)\alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\dots\alpha_{n\sigma(n)} = \det A.$$

□

7.5.8 išvada. *Tegu $A = (\alpha_{ij})$ – n-tos eilės kvadratinė matrica. Tada bet kuriam r, $1 \le r \le n$,*

$$\det(\alpha_{ij}) = (-1)^{r+1}\alpha_{r1}M^{r1} + (-1)^{r+2}\alpha_{r2}M^{r2} + \dots + (-1)^{r+n}\alpha_{rn}M^{rn}.$$

7.5.9 apibrėžimas. Nagrinėkime n-tos eilės kvadratinę matricą $A = (\alpha_{ij})$. $n-1$-os eilės matricos, gautos matricoje A išbraukus i-tąją eilutę ir j-ąjį stulpelį, determinantas žymimas M^{ij} ir vadinamas matricos A ij-tojo elemento α_{ij} *papildomu minoru*. Skaičius $A^{ij} := (-1)^{i+j}M^{ij}$ vadinamas matricos A ij-tojo elemento α_{ij} *algebriniu adjunktu*.

Matricos $A = (\alpha_{ij}) \in M_n(k)$ determinanto $\det A$ skleidinį r-tąja eilute arba r-tuoju stulpeliu galime užrašyti taip:

$$\det(\alpha_{ij}) = \alpha_{r1}A^{r1} + \alpha_{r2}A^{r2} + \dots + \alpha_{rn}A^{rn}$$

arba

$$\det(\alpha_{ij}) = \alpha_{1r}A^{1r} + \alpha_{2r}A^{2r} + \dots + \alpha_{nr}A^{nr}.$$

7.5.10 pavyzdys. Apskaičiuosime matricos

$$A = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 2 & 1 & 1 & 0 \\ 3 & -1 & 1 & 2 \\ 2 & 2 & 1 & 0 \end{pmatrix}$$

determinantą $\det A$. Skaičiuojame pagal ketvirtą stulpelį (nes ten daugiausia nulių):

$$\det A = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 2 & 1 & 1 & 0 \\ 3 & -1 & 1 & 2 \\ 2 & 2 & 1 & 0 \end{pmatrix} = 2 \cdot A^{14} + 0 \cdot A^{24} + 2 \cdot A^{34} + 0 \cdot A^{44} =$$

$$= 2 \cdot (-1)^{1+4} \cdot \begin{vmatrix} 2 & 1 & 1 \\ 3 & -1 & 1 \\ 2 & 2 & 1 \end{vmatrix} + 2 \cdot (-1)^{3+4} \cdot \begin{vmatrix} 1 & 0 & 1 \\ 2 & 1 & 1 \\ 2 & 2 & 1 \end{vmatrix} =$$

$$= (-2)(-2 + 2 + 6 + 2 - 3 - 4) - 2(1 + 0 + 4 - 2 - 0 - 2) = -4.$$

7.5.11. Matricos $A = (\alpha_{ij}) \in M_n(k)$ r-tosios eilutės elementus α_{rj} pakeiskime x_{rj}, $1 \leq j \leq n$, ir užrašykime gautos matricos $\tilde{A}$ determinanto skleidinį r-tąja eilute:

$$\det\tilde{A} = x_{r1}A^{r1} + x_{r2}A^{r2} + \cdots + x_{rn}A^{rn}. \tag{7.6}$$

Jei (7.6) lygybėje vietoje x_{rj} įrašytume, pavyzdžiui, α_{sj}, $s \neq r$, $1 \leq j \leq n$, tai gautume matricos, kurios r-toji ir s-toji eilutės yra lygios, determinanto skleidinio r-tąja eilute formulę. Kadangi matricos, kurios dvi eilutės yra lygios, determinantas lygus nuliui, tai gauname lygybę:

$$\alpha_{s1}A^{r1} + \alpha_{s2}A^{r2} + \cdots + \alpha_{sn}A^{rn} = 0, \quad \text{jei} \quad s \neq r,\ 1 \leq r, s \leq n.$$

7.6 Determinantų savybės

Išvardysime determinanto savybes (jos išplaukia iš 7.5.3 teiginio ir jo įrodymo), užrašytas eilučių terminais. Šios savybės teisingos ir tuo atveju, jei suformuluotume jas stulpelių terminais (žr. 7.5.7 teiginį). Matricos determinantą vadinsime tiesiog determinantu.

1. Jei determinanto kuri nors eilutė sudaryta iš nulių, tai determinantas lygus nuliui.

2. Jei determinanto dvi eilutės yra lygios, tai determinantas lygus nuliui.

3. Jei determinanto dvi eilutės yra proporcingos, tai determinantas lygus nuliui.

4. Determinanto dvi eilutes sukeitus vietomis, pasikeičia determinanto ženklas.

5. Jei determinanto kuri nors eilutė yra padauginta iš skaičiaus λ, tai šį skaičių galima iškelti prieš determinanto ženklą:

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda a_{j1} & \lambda a_{j2} & \dots & \lambda a_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \lambda \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

6. Jei determinanto i-tąją eilutę padauginsime iš skaičiaus λ ir pridėsime prie determinanto j-osios eilutės, $j \neq i$, tai determinanto reikšmė nepasikeis:

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda a_{i1} + a_{j1} & \lambda a_{i2} + a_{j2} & \dots & \lambda a_{in} + a_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} =$$

$$= \begin{vmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{i1} & a_{i2} & a_{i3} & \dots & a_{in} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{j1} & a_{j2} & a_{j3} & \dots & a_{jn} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{vmatrix}.$$

7. Jei kurią nors determinanto eilutę užrašysime dviejų eilučių suma, tai determinantą galėsime užrašyti dviejų determinantų, kurių kitos eilutės tokios

pačios, kaip ir pradinio determinanto, suma:

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{j1}+b_{j1} & a_{j2}+b_{j2} & \dots & a_{jn}+b_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} =$$

$$= \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{j1} & b_{j2} & \dots & b_{jn} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

8. Jei matricos determinantas lygus nuliui, tai matricos eilutės yra tiesiškai priklausomos.

7.7 Determinanto skaičiavimas

Šiame skyrelyje paaiškinsime, kaip praktiškai skaičiuoti determinantą. Aprašomas metodas labai panašus į Gauso metodą tiesinių lygčių sistemoms, todėl jį vadinsime tiesiog Gauso metodu. Šio metodo esmė – su matricos eilutėmis atliekant elementariuosius pertvarkymus, matricai suteikti trikampį pavidalą (trikampio pavidalo matricos determinantas lygus pagrindinės istrižainės elementų sandaugai).

7.7.1 apibrėžimas. Nagrinėkime tokius matricos eilučių pertvarkymus:

1. dvi matricos eilutės sukeičiamos vietomis;

2. matricos eilutė pakeičiama jos ir kitos eilutės, padaugintos iš realaus skaičiaus, suma.

Šie pertvarkymai vadinami *elementariaisiais*.

Kvadratinėje matricoje atliekant pirmą elementarųjį pertvarkymą, tos matricos determinantas keičia ženklą, o atliekant antrą elementarųjį pertvarkymą, determinantas nepasikeičia (žr. ketvirtą ir šeštą determinanto savybes 7.6 skyrelyje).

7.7.2 apibrėžimas. Jei $n \times n$ matricos $A = (a_{ij})$ visi elementai, esantys žemiau pagrindinės istrižainės (t. y. visi elementai a_{ij}, kurių indeksai tenkina nelygybę

$i > j$), lygūs nuliui, tai tokia matrica vadinama *trikampe matrica*. Kitaip sakant, trikampė matrica – tai tokia matrica, kuri turi pavidalą

$$\begin{pmatrix} a_{11} & a_{12} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & a_{23} & \dots & a_{2n} \\ 0 & 0 & \ddots & \ddots & \vdots \\ & & & \ddots & \\ 0 & 0 & 0 & \dots & a_{nn} \end{pmatrix}.$$

7.7.3 teiginys. *Teisingi tokie teiginiai:*

(i) *Bet kurią kvadratinę matricą, atlikus baigtinį skaičių elementariųjų pertvarkymų, galima paversti trikampe matrica.*

(ii) *Trikampės matricos $A = (a_{ij})$ determinantas lygus pagrindinės įstrižainės elementų sandaugai $a_{11}a_{22}\dots a_{nn}$.*

Įrodymas. Teiginį įrodyti paliekame skaitytojui. Kvadratinė matrica, atliekant elementariuosius pertvarkymus, paverčiama trikampe matrica labai panašiai kaip sprendžiant tiesinių lygčių sistemą Gauso metodu (žr. 4.1.5 teoremą). □

7.7.4 pastaba. Sakykime, kad matrica A, atlikus baigtinį skaičių elementariųjų pertvarkymų, paverčiama trikampe matrica $B = (b_{ij})$. Be to, sakykime, kad buvo atlikta lygiai r matricos eilučių sukeitimų (elementariųjų pertvarkymų nr. 1). Tada

$$\det A = (-1)^r \cdot b_{11}b_{22}\dots b_{nn}.$$

7.7.5 pavyzdys. Determinantą

$$\begin{vmatrix} 1 & 1 & 2 & 1 \\ 2 & 3 & 5 & 4 \\ 2 & 4 & 7 & 9 \\ 3 & 4 & 8 & 10 \end{vmatrix}$$

suskaičiuosime Gauso metodu.

Gauso metodo tikslas – atliekant elementariuosius pertvarkymus paversti determinanto matricą trikampe matrica, kurios pagrindinės įstrižainės

$$(a_{11}, a_{22}, a_{33}, \dots)$$

apačioje būtų vien nuliai. Toks determinantas lygus istrižainės elementų sandaugai (žr. 7.7.3 teiginį).

Padauginame pirmą eilutę iš -2 ir pridedame prie antros (kad elementas a_{21} virstų nuliu). Tada pirmą eilutę dauginame iš -2 ir pridedame prie trečios. Pirmą eilutę padauginę iš -3 pridedame prie ketvirtos:

$$\begin{vmatrix} 1 & 1 & 2 & 1 \\ 2 & 3 & 5 & 4 \\ 2 & 4 & 7 & 9 \\ 3 & 4 & 8 & 10 \end{vmatrix} \begin{matrix} \downarrow^{(-2)} & \downarrow^{(-2)} & \downarrow^{(-3)} \end{matrix} = \begin{vmatrix} 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 2 & 3 & 7 \\ 0 & 1 & 2 & 7 \end{vmatrix} \begin{matrix} \downarrow^{(-2)} & \downarrow^{(-1)} \end{matrix}$$

$$= \begin{vmatrix} 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 1 & 5 \end{vmatrix} \downarrow^{(-1)} = \begin{vmatrix} 1 & 1 & 2 & 1 \\ 0 & 1 & 1 & 2 \\ 0 & 0 & 1 & 3 \\ 0 & 0 & 0 & 2 \end{vmatrix} = 1 \cdot 1 \cdot 1 \cdot 2 = 2.$$

Kai kurių n-tosios eilės determinantų reikšmes galima rasti pasinaudojus rekurentinėmis formulėmis. Nagrinėkime n-tosios eilės determinantą

$$D_n := \begin{vmatrix} a & b & 0 & \cdots & 0 & 0 \\ c & a & b & \cdots & 0 & 0 \\ 0 & c & a & \cdots & 0 & 0 \\ 0 & 0 & c & \cdots & 0 & 0 \\ & & \vdots & \vdots & & \\ 0 & 0 & 0 & \cdots & a & b \\ 0 & 0 & 0 & \cdots & c & a \end{vmatrix},$$

čia a ir b – realieji skaičiai. Skleidžiant pagal pirmą eilutę galima įsitikinti, kad šis determinantas tenkina rekurentinį sąryšį

$$D_n = aD_{n-1} - bcD_{n-2}, \quad n \geq 3. \tag{7.7}$$

Be to,

$$D_1 = a, \quad D_2 = \begin{vmatrix} a & b \\ c & a \end{vmatrix} = a^2 - bc.$$

Remdamiesi šia rekurentine formule galime paeiliui suskaičiuoti determinantus D_3, D_4, D_5 ir t. t. Tačiau, remiantis tiesinių rekurentinių sąryšių teorija (žr. [11], 5.4 skyrelį), determinantą D_n galima išreikšti per kvadratinės lygties

$$x^2 - ax + bc = 0$$

((7.7) rekurentinio sąryšio charakteristinės lygties) šaknis x_1 ir x_2:

$$D_n = \begin{cases} c_1 x_1^n + c_2 x_2^n, & \text{jei } x_1, x_2 \in \mathbb{R},\ x_1 \neq x_2 \\ x_1^n (c_1 + c_2 n), & \text{jei } x_1, x_2 \in \mathbb{R},\ x_1 = x_2 \\ c_1 x_1^n + c_2 x_2^n, & \text{jei } x_1, x_2 \in \mathbb{C},\ x_1 \neq x_2 \end{cases},$$

čia c_1, c_2 – konstantos, $c_1, c_2 \in \mathbb{C}$, o $\mathbb{C}$ – kompleksinių skaičių kūnas (žr. 6.7 skyrelį). Kaip rasti c_1 ir c_2, paaiškinsime pavyzdžiais.

7.7.6 pastaba. Pagal apibrėžimą

$$\mathbb{C} := \{\alpha + \beta i \mid \alpha, \beta \in \mathbb{R},\ i^2 = -1\}.$$

Sudėties ir daugybos veiksmai aibėje $\mathbb{C}$ atliekami panašiai kaip ir realiųjų skaičių aibėje, tik dauginant kompleksinius skaičius, skaičiaus i kvadratas i^2 pakeičiamas -1.

7.7.7 pavyzdys. Apskaičiuosime determinantą

$$D_n = \begin{vmatrix} 5 & 2 & 0 & \dots & 0 & 0 \\ 2 & 5 & 2 & \dots & 0 & 0 \\ 0 & 2 & 5 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 5 & 2 \\ 0 & 0 & 0 & \dots & 2 & 5 \end{vmatrix}.$$

Išskleidę šį determinantą pagal pirmąją eilutę, gauname

$$D_n = 5D_{n-1} - 2 \begin{vmatrix} 2 & 2 & \dots & 0 & 0 \\ 0 & 5 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 5 & 2 \\ 0 & 0 & \dots & 2 & 5 \end{vmatrix} = 5D_{n-1} - 2 \cdot 2D_{n-2}.$$

Perkėlę visus narius į kairę pusę, gauname

$$D_n - 5D_{n-1} + 4D_{n-2} = 0.$$

Kvadratinės lygties

$$x^2 - 5x + 4 = 0$$

šaknys yra 1 ir 4. Vadinasi,

$$D_n = 1^n \cdot c_1 + 4^n \cdot c_2 = c_1 + 4^n \cdot c_2.$$

Kadangi $D_1 = 5$, $D_2 = 21$, tai gauname lygčių sistemą

$$\begin{cases} c_1 + 4c_2 &= 5 \\ c_1 + 4^2 c_2 &= 21 \end{cases}$$

koeficientams c_1 ir c_2 rasti. Išsprendę šią lygčių sistemą, gauname

$$c_1 = -\frac{1}{3},\ c_2 = \frac{4}{3}.$$

Taigi

$$D_n = \frac{4^{n+1} - 1}{3}.$$

7.7.8 pavyzdys. Apskaičiuosime determinantą

$$D_n = \begin{vmatrix} 2 & 1 & 0 & \dots & 0 & 0 \\ 1 & 2 & 1 & \dots & 0 & 0 \\ 0 & 1 & 2 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 2 & 1 \\ 0 & 0 & 0 & \dots & 1 & 2 \end{vmatrix}.$$

Panašiai kaip ir praeitame pavyzdyje gauname

$$D_n - 2D_{n-1} + D_{n-2} = 0.$$

Kvadratinės lygties

$$x^2 - 2x + 1 = 0$$

abi šaknys yra lygios 1. Vadinasi,

$$D_n = 1^n \cdot c_1 + 1^n \cdot n \cdot c_2 = c_1 + n \cdot c_2.$$

Kadangi $D_1 = 2$, $D_2 = 3$, gauname lygčių sistemą

$$\begin{cases} c_1 + \ c_2 = 2 \\ c_1 + 2c_2 = 3 \end{cases}$$

koeficientams c_1 ir c_2 rasti. Išsprendę šią lygčių sistemą, gauname

$$c_1 = c_2 = 1.$$

Vadinasi,

$$D_n = 1 + n.$$

7.7.9 pavyzdys. Apskaičiuosime determinantą

$$D_n = \begin{vmatrix} 2 & 5 & 0 & \dots & 0 & 0 \\ 1 & 2 & 5 & \dots & 0 & 0 \\ 0 & 1 & 2 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 2 & 5 \\ 0 & 0 & 0 & \dots & 1 & 2 \end{vmatrix}.$$

Panašiai kaip ir praeitame pavyzdyje gauname:

$$D_n - 2D_{n-1} + 5D_{n-2} = 0.$$

Kvadratinės lygties

$$x^2 - 2x + 5 = 0$$

šaknys yra kompleksinės ir yra lygios $1 + 2i$ ir $1 - 2i$. Vadinasi,

$$D_n = (1 + 2i)^n \cdot c_1 + (1 - 2i)^n \cdot c_2.$$

Kadangi $D_1 = 2$, $D_2 = -1$, gauname lygčių sistemą

$$\begin{cases} (1 + 2i) \cdot c_1 + (1 - 2i) \cdot c_2 = 2 \\ (1 + 2i)^2 \cdot c_1 + (1 - 2i)^2 \cdot c_2 = -1 \end{cases}.$$

Išspręsime šią lygčių sistemą. Pirmąją lygtį padauginę iš $1+2i$ ir iš gautos lygties atėmę antrąją lygtį, gauname

$$((1 + 2i)(1 - 2i) - (1 - 2i)^2) \cdot c_2 = 2 + 4i - (-1),$$

t. y.

$$(8 + 4i) \cdot c_2 = 3 + 4i.$$

Iš šios lygybės gauname

$$c_2 = \frac{3 + 4i}{8 + 4i} = \frac{(3 + 4i)(8 - 4i)}{(8 + 4i)(8 - 4i)} = \frac{2 + i}{4}.$$

Galite įsitikinti (pasinaudojome simetrija), kad

$$c_1 = \frac{2 - i}{4}.$$

Galutinai gauname

$$D_n = (1 + 2i)^n \cdot \frac{2 - i}{4} + (1 - 2i)^n \cdot \frac{2 + i}{4}.$$

Sutvarkę pastarąjį reiškinį, galime parašyti:

$$D_n = \sum_{j \geqslant 0} (-1)^j \left(\binom{n}{2j} + \binom{n}{2j + 1} \right) 2^{2j},$$

čia

$$\binom{n}{j} = \frac{n!}{j!(n - j)!}, \quad 0 \leqslant j \leqslant n,$$

Niutono binomo koeficientai. Jie dar žymimi ir kitaip:

$$\mathrm{C}_n^j = \binom{n}{j} = \frac{n!}{j!(n - j)!}, \quad 0 \leqslant j \leqslant n.$$

7.7.10 apibrėžimas. Tarkime, kad $a_1, a_2, \ldots, a_n$ – bet kokie realieji (arba kompleksiniai) skaičiai. Determinantas

$$W_n(a_1, a_2, \ldots, a_n) := \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ a_1 & a_2 & a_3 & \cdots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \cdots & a_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & \cdots & a_n^{n-1} \end{vmatrix}$$

vadinamas *Vandermondo determinantu.*

7.7.11 teiginys. *Vandermondo determinantas $W_n(a_1, a_2, \ldots, a_n)$ lygus skaičiui*

$$\prod_{1 \le i < j \le n} (a_j - a_i), \quad n \ge 2.$$

Įrodymas. Teiginį įrodyti paliekame skaitytojui. (Teiginį galima įrodyti matematinės indukcijos būdu.) $\square$

7.7.12 išvada. *Vandermondo determinantas $W_n(a_1, a_2, \ldots, a_n)$ yra nenulinis skaičius tada ir tik tada, kai visi skaičiai $a_1, a_2, \ldots, a_n$ yra skirtingi.*

7.8 Matricų sandaugos determinantas

7.8.1 apibrėžimas. Sakykime, kad k – kūnas, $m, n \in \mathbb{N}$. Atvaizdis

$$F : \underbrace{k^m \times k^m \times \cdots \times k^m}_{n} \to k$$

vadinamas *n-tiesiniu*, jei bet kuriems $v_1, \ldots, v_j, v_j', \ldots, v_n \in k^m$, $1 \le j \le n$, λ, $\mu \in k$,

$$F(v_1, \ldots, \lambda v_j + \mu v_j', \ldots, v_n) = \lambda \cdot F(v_1, \ldots, v_j, \ldots, v_n) +$$
$$+ \mu \cdot F(v_1, \ldots, v_j', \ldots, v_n).$$

Atvaizdis F vadinamas *alternuojančiuoju*, jei jo reikšmė $F(v_1, v_2, \ldots, v_n)$ lygi nuliui, kai kurie nors du vektoriai $v_1, v_2, \ldots, v_n$ sutampa.

7.8.2 teiginys. *Jei*

$$F : \underbrace{k^m \times k^m \times \cdots \times k^m}_{n} \to k$$

yra n-tiesinis, alternuojantysis atvaizdis, tai

$$F(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = -F(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_n).$$

Įrodymas. Kadangi atvaizdis F yra alternuojantysis, tai

$$F(v_1, \ldots, v_i + v_j, \ldots, v_i + v_j, \ldots, v_n) = 0.$$

Kadangi atvaizdis F yra n-tiesinis, tai

$$0 = F(v_1, \ldots, v_i + v_j, \ldots, v_j + v_i, \ldots, v_n) =$$

$$= F(v_1, \ldots, v_i, \ldots, v_i, \ldots, v_n) + F(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) +$$

$$+ F(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_n) + F(v_1, \ldots, v_j, \ldots, v_j, \ldots, v_n) =$$

$$= F(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) + F(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_n).$$

Taigi

$$F(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = -F(v_1, \ldots, v_j, \ldots, v_i, \ldots, v_n).$$

□

7.8.3 išvada. *Sakykime, kad*

$$F : \underbrace{k^m \times k^m \times \cdots \times k^m}_{n} \to k$$

yra n-tiesinis, alternuojantysis atvaizdis, o $\sigma \in S_n$. Tada bet kuriems vektoriams $v_1, v_2, \ldots, v_n \in V$ teisinga lygybė

$$F(v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(n)}) = \operatorname{sgn}(\sigma) F(v_1, v_2, \ldots, v_n).$$

Įrodymas. Išvadą įrodyti paliekame skaitytojui. □

7.8.4 teiginys. *Tegu k^n – aritmetinė tiesinė erdvė virš kūno k. Sakykime, kad*

$$F : \underbrace{k^n \times k^n \times \cdots \times k^n}_{n} \to k$$

yra n-tiesinis, alternuojantysis atvaizdis, $A = (\alpha_{ij}) \in M_n(k)$ – n-tos eilės kvadratinė matrica, o $v_1, v_2, \ldots, v_n \in k^n$ – bet kokie vektoriai. Tada

$$F\left(\sum_{j_1=1}^{n} \alpha_{1j_1} v_{j_1},\ \sum_{j_2=1}^{n} \alpha_{2j_2} v_{j_2},\ \ldots,\ \sum_{j_n=1}^{n} \alpha_{nj_n} v_{j_n}\right) =$$

$$= \det(A) \cdot F(v_1,\ v_2,\ \ldots,\ v_n).$$

Įrodymas. Kadangi F – n-tiesinis, alternuojantysis atvaizdis, tai, remdamiesi 7.8.3 išvada, galime parašyti

$$F\left(\sum_{j_1=1}^{n}\alpha_{1j_1}v_{j_1},\ \sum_{j_2=1}^{n}\alpha_{2j_2}v_{j_2},\ \sum_{j_3=1}^{n}\alpha_{3j_3}v_{j_3},\ \dots,\ \sum_{j_n=1}^{n}\alpha_{nj_n}v_{j_n}\right)=$$

$$=\sum_{j_1=1}^{n}\alpha_{1j_1}F\left(v_{j_1},\ \sum_{j_2=1}^{n}\alpha_{2j_2}v_{j_2},\ \sum_{j_3=1}^{n}\alpha_{3j_3}v_{j_3},\ \dots,\ \sum_{j_n=1}^{n}\alpha_{nj_n}v_{j_n}\right)=$$

$$=\sum_{j_1=1}^{n}\alpha_{1j_1}\sum_{j_2=1}^{n}\alpha_{2j_2}F\left(v_{j_1},\ v_{j_2},\ \sum_{j_3=1}^{n}\alpha_{3j_3}v_{j_3},\ \dots,\ \sum_{j_n=1}^{n}\alpha_{nj_n}v_{j_n}\right)=$$

$$\dots\quad\dots\quad\dots$$

$$=\sum_{j_1=1}^{n}\alpha_{1j_1}\sum_{j_2=1}^{n}\alpha_{2j_2}\cdots\sum_{j_n=1}^{n}\alpha_{nj_n}F(v_{j_1},\ v_{j_2},\ \dots,\ v_{j_n})=$$

$$=\sum_{\sigma\in S_n}\alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\dots\alpha_{n\sigma(n)}F(v_{\sigma(1)},\ v_{\sigma(2)},\ \dots,\ v_{\sigma(n)})=$$

$$=\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\dots\alpha_{n\sigma(n)}F(v_1,\ v_2,\ \dots,\ v_n)=$$

$$=\det(\alpha_{ij})\cdot F(v_1,\ v_2,\ \dots,\ v_n)=\det(A)\cdot F(v_1,\ v_2,\ \dots,\ v_n).$$

□

7.8.5 teiginys. *Bet kurių n-tos eilės kvadratinių matricų A ir B sandaugos determinantas lygus tų matricų determinantų sandaugai, t. y.*

$$\det(AB)=\det A\cdot\det B.$$

Įrodymas. Matricų $A=(\alpha_{ij})$ ir $B=(\beta_{ij})$ sandaugos matricą AB pažymėkime (γ_{ij}). Tada

$$\gamma_{ij}=\sum_{r=1}^{n}\alpha_{ir}\beta_{rj}$$

ir

$$\det(AB)=\det(\gamma_{ij})=\det\left(\sum_{j_1=1}^{n}\gamma_{1j_1}e_{j_1},\ \sum_{j_2=1}^{n}\gamma_{2j_2}e_{j_2},\ \dots,\ \sum_{j_n=1}^{n}\gamma_{nj_n}e_{j_n}\right),\quad(7.8)$$

čia $e_1, e_2, \ldots, e_n$ – standartinė erdvės k^n bazė. Sandaugos matricos $AB = (\gamma_{ij})$ i-toji eilutė

$$(\gamma_{i1}, \gamma_{i2}, \ldots, \gamma_{in}) = \sum_{j=1}^{n} \gamma_{ij} e_j = \sum_{j=1}^{n} \left(\sum_{r=1}^{n} \alpha_{ir} \beta_{rj} \right) e_j. \tag{7.9}$$

Paskutinėje sumoje sukeitę sumavimo tvarką (pergrupavę dėmenis), gauname

$$\sum_{j=1}^{n} \left(\sum_{r=1}^{n} \alpha_{ir} \beta_{rj} \right) e_j = \sum_{r=1}^{n} \alpha_{ir} \left(\sum_{j=1}^{n} \beta_{rj} e_j \right). \tag{7.10}$$

Pažymėkime $v_r = \sum_{j=1}^{n} \beta_{rj} e_j$. Tada $v_r \in k^n$ yra matricos $B = (\beta_{ij})$ r-toji eilutė, t. y.

$$B = \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}.$$

Taigi iš (7.9) ir (7.10) lygybių išplaukia, kad sandaugos matricos $AB = (\gamma_{ij})$ i-tąją eilutę galima išreikšti taip:

$$\sum_{j=1}^{n} \gamma_{ij} e_j = \sum_{r=1}^{n} \alpha_{ir} v_r.$$

Šias išraiškas įstatę į (7.8) ir du kartus iš eilės pritaikę 7.8.4 teiginį (determinantas $\det : k^n \times k^n \times \cdots \times k^n \to k$ yra n-tiesinis ir alternuojantysis atvaizdis), gauname lygybę

$$\det(AB) = \det \left(\sum_{j_1=1}^{n} \alpha_{1j_1} v_{j_1},\ \sum_{j_2=1}^{n} \alpha_{2j_2} v_{j_2},\ \ldots,\ \sum_{j_n=1}^{n} \alpha_{nj_n} v_{j_n} \right) =$$

$$= \det(\alpha_{ij}) \det(v_1, v_2, \ldots, v_n) =$$

$$= \det(A) \det \left(\sum_{j_1=1}^{n} \beta_{1j_1} e_{j_1},\ \sum_{j_2=1}^{n} \beta_{2j_2} e_{j_2},\ \ldots,\ \sum_{j_n=1}^{n} \beta_{nj_n} e_{j_n} \right) = \det(A) \det(B).$$

$\square$

7.9 Atvirkštinė matrica

Tegu k – kūnas.

7.9.1 apibrėžimas. Matrica $A \in M_n(k)$ vadinama *atvirkštine* matricai $B \in M_n(k)$ ir žymima $A = B^{-1}$, jei

$$AB = BA = \mathbf{1}_n.$$

7.9.2 teiginys. *n-tos eilės kvadratinei matricai $A \in M_n(k)$ egzistuoja atvirkštinė matrica A^{-1} tada ir tik tada, kai* $\det A \neq 0$.

Įrodymas. *Būtinumas.* Tegu n-tos eilės kvadratinei matricai $A \in M_n(k)$ egzistuoja atvirkštinė matrica A^{-1}, t. y. $AA^{-1} = \mathbf{1}_n$. Tada

$$\det A \cdot \det A^{-1} = \det(AA^{-1}) = \det \mathbf{1}_n = 1,$$

t. y. $\det A \neq 0$.

Pakankamumas. Sakykime, kad matricos $A \in M_n(k)$ determinantas $\det A \neq 0$. Tegu M^{ij} – matricos $A = (\alpha_{ij})$ ij-ojo elemento α_{ij} papildomas minoras (priminsime: M^{ij} – $(n-1)$-os eilės matricos, gautos matricoje A išbraukus i-tąją eilutę ir j-tąjį stulpelį, determinantas), $A^{ij} := (-1)^{i+j}M^{ij}$ – šio elemento algebrinis adjunktas. Apibrėžkime matricą

$$B = \frac{1}{\det A}\begin{pmatrix} A^{11} & A^{21} & \dots & A^{n1} \\ A^{12} & A^{22} & \dots & A^{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A^{1n} & A^{2n} & \dots & A^{nn} \end{pmatrix}. \tag{7.11}$$

Sudauginę matricas A ir B, galime įsitikinti, kad $AB = BA = \mathbf{1}_n$. Taigi $B = A^{-1}$. □

7.9.3 pavyzdys. Remdamiesi (7.11) išraiška rasime matricos

$$A = \begin{pmatrix} 1 & 2 & 1 \\ 2 & 3 & 4 \\ 3 & 4 & 8 \end{pmatrix}$$

atvirkštinę matricą A^{-1}.

$$|A| = -1, \ A^{11} = (-1)^{1+1}\begin{vmatrix} 3 & 4 \\ 4 & 8 \end{vmatrix} = 8, \ A^{12} = (-1)^{1+2}\begin{vmatrix} 2 & 4 \\ 3 & 8 \end{vmatrix} = -4,$$

$$A^{13} = (-1)^{1+3}\begin{vmatrix} 2 & 3 \\ 3 & 4 \end{vmatrix} = -1, \ A^{21} = (-1)^{2+1}\begin{vmatrix} 2 & 1 \\ 4 & 8 \end{vmatrix} = -12,$$

$$A^{22} = (-1)^{2+2}\begin{vmatrix} 1 & 1 \\ 3 & 8 \end{vmatrix} = 5,\ A^{23} = (-1)^{2+3}\begin{vmatrix} 1 & 2 \\ 3 & 4 \end{vmatrix} = 2,$$

$$A^{31} = (-1)^{3+1}\begin{vmatrix} 2 & 1 \\ 3 & 4 \end{vmatrix} = 5,\ A^{32} = (-1)^{3+2}\begin{vmatrix} 1 & 1 \\ 2 & 4 \end{vmatrix} = -2,$$

$$A^{33} = (-1)^{3+3}\begin{vmatrix} 1 & 2 \\ 2 & 3 \end{vmatrix} = -1.$$

Taigi, remdamiesi atvirkštinės matricos (7.11) išraiška, galime parašyti

$$A^{-1} = \begin{pmatrix} A^{11} & A^{12} & A^{13} \\ A^{21} & A^{22} & A^{23} \\ A^{31} & A^{32} & A^{33} \end{pmatrix}^t = \begin{pmatrix} -8 & 12 & -5 \\ 4 & -5 & 2 \\ 1 & -2 & 1 \end{pmatrix}.$$

7.9.4 pastaba. Tarkime, reikia suskaičiuoti ketvirtos eilės matricos atvirkštinę matricą. Jei šios matricos ieškotume remdamiesi (7.11) išraiška, tai reikėtų suskaičiuoti 16 trečios eilės determinantų (nemažai darbo). Todėl šį atvirkštinės matricos skaičiavimo metodą galima būtų pavadinti „darbas puošia žmogų“.

Atvirkštinės matricos skaičiavimas, paremtas (7.11) išraiška, yra nepraktiškas, todėl aptarsime kitą metodą, kuris vadinamas *Gauso metodu.*

7.9.5 pastaba. Matricai $A \in M_n(\mathbb{R})$, kai $\det A \neq 0$, atvirkštinę matricą galima rasti ir Gauso metodu. Gauso metodas pagrįstas tiesinių lygčių sistemos

$$AX = \mathbf{1}_n,$$

čia X – n-os eilės nežinomųjų kvadratinė matrica, sprendimu Gauso metodu. Akivaizdu, kad šios lygčių sistemos sprendinys yra $X = A^{-1}$. Praktiškai Gauso metodu matricai atvirkštinė matrica ieškoma taip: pirmiausia sudaroma matrica

$$(A \mid \mathbf{1}_n).$$

Užrašytos matricos eilutėms taikant elementarius pertvarkymus, matrica A paverčiama vienetine. Tada ilgos matricos dešinėje pusėje gauname matricą A^{-1}, t. y. gauta matrica yra pavidalo

$$(\mathbf{1}_n \mid A^{-1}).$$

7.9.6 pavyzdys. Gauso metodu apskaičiuosime matricai

$$A = \begin{pmatrix} 3 & -2 & 2 \\ -1 & 5 & 6 \\ 2 & 3 & 5 \end{pmatrix}$$

atvirkštinę matricą. Pirmiausia įsitikinkime, kad $\det A \neq 0$. Galite įsitikinti, kad $\det A = -39$. Norėdami rasti matricai A atvirkštinę matricą Gauso metodu, kaip nurodyta 7.9.5 pastaboje, sudarome matricą

$$\left(\begin{array}{ccc|ccc} 3 & -2 & 2 & 1 & 0 & 0 \\ -1 & 5 & 6 & 0 & 1 & 0 \\ 2 & 3 & 5 & 0 & 0 & 1 \end{array}\right).$$

Šią matricą elementariaisiais pertvarkymais, taikomais eilutėms, reikia paversti į tokią matricą, kad kairėje pusėje gautume vienetinę matricą. Tada dešinėje pusėje, kaip parašyta pastaboje, gauta matrica ir bus atvirkštinė matricai A. Tam antrąją eilutę padauginę iš 3 ir 2 ir pridėję atitinkamai prie pirmos ir trečios eilučių, gauname matricą

$$\left(\begin{array}{ccc|ccc} 0 & 13 & 20 & 1 & 3 & 0 \\ -1 & 5 & 6 & 0 & 1 & 0 \\ 0 & 13 & 17 & 0 & 2 & 1 \end{array}\right).$$

Pirmąją eilutę padauginę iš -1 ir pridėję prie trečios eilutės, paskui pirmąją eilutę padauginę iš 5 ir pridėję prie antros eilutės, padaugintos iš -13, gauname matricą

$$\left(\begin{array}{ccc|ccc} 0 & 13 & 20 & 1 & 3 & 0 \\ 13 & 0 & 22 & 5 & 2 & 0 \\ 0 & 0 & -3 & -1 & -1 & 1 \end{array}\right).$$

Panašiai pasinaudoję trečiąja eilute, išnaikiname elementus, kurie užima vietas, numeruojamas indeksais (13) ir (23). Tai atlikę, gauname matricą

$$\left(\begin{array}{ccc|ccc} 0 & 39 & 0 & -17 & -11 & 20 \\ 39 & 0 & 0 & -7 & -16 & 22 \\ 0 & 0 & -3 & -1 & -1 & 1 \end{array}\right).$$

Šios matricos trečiąją eilutę padauginę iš -13, o paskui sukeitę pirmąją ir antrąją eilutes vietomis, gauname matricą

$$\left(\begin{array}{ccc|ccc} 39 & 0 & 0 & -7 & -16 & 22 \\ 0 & 39 & 0 & -17 & -11 & 20 \\ 0 & 0 & 39 & 13 & 13 & -13 \end{array}\right).$$

Pagaliau galime užrašyti matricai A atvirkštinę matricą:

$$A^{-1} = \frac{1}{39}\begin{pmatrix} -7 & -16 & 22 \\ -17 & -11 & 20 \\ 13 & 13 & -13 \end{pmatrix}.$$

7.9.7 pavyzdys. Rasime matricai

$$A = \begin{pmatrix} 1 & 2 & 2 & 1 \\ 2 & 5 & 5 & 4 \\ 3 & 8 & 9 & 8 \\ 1 & 3 & 4 & 5 \end{pmatrix}$$

atvirkštinę matricą A^{-1}. Užrašome dvigubą matricą:

$$\left(\begin{array}{cccc|cccc} 1 & 2 & 2 & 1 & 1 & 0 & 0 & 0 \\ 2 & 5 & 5 & 4 & 0 & 1 & 0 & 0 \\ 3 & 8 & 9 & 8 & 0 & 0 & 1 & 0 \\ 1 & 3 & 4 & 5 & 0 & 0 & 0 & 1 \end{array}\right)$$

kairėje pusėje parašyta matrica A, o dešinėje – vienetinė matrica E. Galima atlikti tokius veiksmus (eilučių elementariuosius pertvarkymus):

- padauginti eilutę iš skaičiaus;
- vieną eilutę padauginti iš skaičiaus ir pridėti prie kitos;
- sukeisti eilutes vietomis.

(Iš tikrųjų, trečią pertvarkymą galima išreikšti pirmais dviem.) Atlikdami šiuos veiksmus kairiąją dvigubos matricos pusę paverčiame vienetine. Tada dešinėje pusėje gauta matrica bus atvirkštinė matricai A.

$$\left(\begin{array}{cccc|cccc} 1 & 2 & 2 & 1 & 1 & 0 & 0 & 0 \\ 2 & 5 & 5 & 4 & 0 & 1 & 0 & 0 \\ 3 & 8 & 9 & 8 & 0 & 0 & 1 & 0 \\ 1 & 3 & 4 & 5 & 0 & 0 & 0 & 1 \end{array}\right) \; (-2) \; (-3) \; (-1)$$

$$\left(\begin{array}{cccc|cccc} 1 & 2 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 & -2 & 1 & 0 & 0 \\ 0 & 2 & 3 & 5 & -3 & 0 & 1 & 0 \\ 0 & 1 & 2 & 4 & -1 & 0 & 0 & 1 \end{array}\right) \; (-2) \; (-1)$$

$$\left(\begin{array}{cccc|cccc} 1 & 2 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 & -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & -2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 & -1 & 0 & 1 \end{array}\right) \; (-1)$$

$$\left(\begin{array}{cccc|cccc} 1 & 2 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 2 & -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & -2 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & -1 & 1 \end{array}\right) \; (-1) \; (-2) \; (-1)$$

$$\left(\begin{array}{cccc|rrrr} 1 & 2 & 2 & 0 & 1 & -1 & 1 & -1 \\ 0 & 1 & 1 & 0 & -2 & -1 & 2 & -2 \\ 0 & 0 & 1 & 0 & 1 & -3 & 2 & -1 \\ 0 & 0 & 0 & 1 & 0 & 1 & -1 & 1 \end{array}\right) \uparrow_{(-1)} \uparrow_{(-2)}$$

$$\left(\begin{array}{cccc|rrrr} 1 & 2 & 0 & 0 & -1 & 5 & -3 & 1 \\ 0 & 1 & 0 & 0 & -3 & 2 & 0 & -1 \\ 0 & 0 & 1 & 0 & 1 & -3 & 2 & -1 \\ 0 & 0 & 0 & 1 & 0 & 1 & -1 & 1 \end{array}\right) \uparrow_{(-2)}$$

$$\left(\begin{array}{cccc|rrrr} 1 & 0 & 0 & 0 & 5 & 1 & -3 & 3 \\ 0 & 1 & 0 & 0 & -3 & 2 & 0 & -1 \\ 0 & 0 & 1 & 0 & 1 & -3 & 2 & -1 \\ 0 & 0 & 0 & 1 & 0 & 1 & -1 & 1 \end{array}\right).$$

Kairėje pusėje gavome vienetinę matricą, todėl dešinėje pusėje esanti matrica bus atvirkštinė matricai A, t. y.

$$A^{-1} = \begin{pmatrix} 5 & 1 & -3 & 3 \\ -3 & 2 & 0 & -1 \\ 1 & -3 & 2 & -1 \\ 0 & 1 & -1 & 1 \end{pmatrix}.$$

Matricos atvirkštinę matricą galima panaudoti sprendžiant tiesinių lygčių sistemas.

7.9.8 pavyzdys. Išspręsime tiesinių lygčių sistemą

$$\begin{cases} 3x_1 - 2x_2 + 2x_3 = 39 \\ -x_1 + 5x_2 + 6x_3 = -78 \\ 2x_1 + 3x_2 + 5x_3 = -39 \end{cases}.$$

Šią sistemą galime užrašyti matricų žymenimis

$$AX = B,$$

čia matrica

$$A = \begin{pmatrix} 3 & -2 & 2 \\ -1 & 5 & 6 \\ 2 & 3 & 5 \end{pmatrix},$$

sudaryta iš koeficientų prie kintamųjų, o matricos X ir B yra

$$X = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \quad B = \begin{pmatrix} 39 \\ -78 \\ -39 \end{pmatrix}.$$

Lygtį

$$AX = B$$

galime išspręsti abi lygybės puses padauginę iš kairės iš matricos A^{-1}. Matrica A^{-1} mums žinoma:

$$A^{-1} = \frac{1}{39}\begin{pmatrix} -7 & -16 & 22 \\ -17 & -11 & 20 \\ 13 & 13 & -13 \end{pmatrix}$$

(žr. 7.9.6 pavyzdį). Taigi

$$X = A^{-1} \cdot B = \frac{1}{39}\begin{pmatrix} -7 & -16 & 22 \\ -17 & -11 & 20 \\ 13 & 13 & -13 \end{pmatrix} \cdot \begin{pmatrix} 39 \\ -78 \\ -39 \end{pmatrix} = \begin{pmatrix} 3 \\ -15 \\ 0 \end{pmatrix}.$$

7.10 Atvirkštinės matricos skaičiavimo pavyzdžiai

Tarkime, kad n-tos eilės matricą A galima užrašyti pavidalu

$$A = \mathbf{1_n} + U,$$

čia $\mathbf{1_n}$ – vienetinė matrica, o matrica U tokia, kurios n-tasis laipsnis U^n yra nulinė matrica. Tada matricai A atvirkštinė matrica yra

$$A^{-1} = \mathbf{1_n} - U + U^2 - U^3 + \ldots + (-1)^{n-1}U^{n-1}.$$

Tuo galima įsitikinti tiesiogiai:

$$AA^{-1} = (\mathbf{1_n} + U)(\mathbf{1_n} - U + U^2 - U^3 + \ldots + (-1)^{n-1}U^{n-1}) = \mathbf{1_n}.$$

7.10.1 pavyzdys. Apskaičiuosime matricai

$$A = \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

atvirkštinę matricą.

Akivaizdu, kad

$$A = \mathbf{1_n} + U,$$

čia

$$U = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}. \tag{7.12}$$

Keliant matricą U laipsniais, vienetai virš pagrindinės įstrižainės tolsta nuo jos lygiagrečiai su šia įstrižaine ir $U^n = \mathcal{O}$. Taigi

$$A^{-1} = \begin{pmatrix} 1 & -1 & 1 & \cdots & (-1)^{n-2} & (-1)^{n-1} \\ 0 & 1 & -1 & \cdots & (-1)^{n-3} & (-1)^{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -1 \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}.$$

Pratimas. Tegu U – matrica apibrėžta (7.12) lygybe. Raskite matricos

$$A = \mathbf{1_n} + \alpha_1 U + \alpha_2 U^2 + \ldots + \alpha_{n-1} U^{n-1}, \quad \alpha_1,\ \alpha_2, \ldots, \alpha_{n-1} \in \mathbb{R},$$

atvirkštinę matricą.

Patarimas: atvirkštinę matricą užrašykite pavidalu

$$A^{-1} = \mathbf{1_n} + x_1 U + x_2 U^2 + \ldots + x_{n-1} U^{n-1},$$

čia $x_1,\ x_2, \ldots, x_{n-1}$ – nežinomieji, kuriuos reikia rasti. Įsitikinkite, kad lygtis

$$(\mathbf{1_n} + \alpha_1 U + \alpha_2 U^2 + \ldots + \alpha_{n-1} U^{n-1})\cdot$$
$$\cdot(\mathbf{1_n} + x_1 U + x_2 U^2 + \ldots + x_{n-1} U^{n-1}) = \mathbf{1_n}$$

išsprendžiama.

7.10.2 pavyzdys. Tarkime, kad J_n – n-tos eilės matrica, sudaryta iš vienetų. Įsitikinsime, kad

$$(\mathbf{1_n} - J_n)^{-1} = \mathbf{1_n} - \frac{1}{n-1} J_n.$$

Iš tikrųjų,

$$J_n^2 = J_n \cdot J_n = n \cdot J_n.$$

Vadinasi,

$$(\mathbf{1_n} - J_n) \cdot (\mathbf{1_n} - J_n)^{-1} = (\mathbf{1_n} - J_n) \cdot \left(\mathbf{1_n} - \frac{1}{n-1} J_n\right) =$$
$$= \mathbf{1_n} - \frac{1}{n-1} J_n - J_n + \frac{n}{n-1} = \mathbf{1_n}.$$

Pratimas. Remdamiesi 7.10.2 pavyzdžiu, apskaičiuokite matricai

$$A = \begin{pmatrix} a & b & b & \cdots & b & b \\ b & a & b & \cdots & b & b \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ b & b & b & \cdots & a & b \\ b & b & b & \cdots & b & a \end{pmatrix}, \quad \text{kai} \quad a \neq b, \quad a \neq (1-n)b,$$

atvirkštinę matricą.

7.11 Kramerio taisyklė

Sakykime, kad k – kūnas.

7.11.1 teorema (Kramerio taisyklė)**.** *Tarkime, tiesinių lygčių sistemos*

$$\begin{cases} \alpha_{11}x_1 & + & \alpha_{12}x_2 & + & \ldots & + & \alpha_{1n}x_n & = & \beta_1 \\ \alpha_{21}x_1 & + & \alpha_{22}x_2 & + & \ldots & + & \alpha_{2n}x_n & = & \beta_2 \\ \vdots & & \vdots & & \ddots & & \vdots & & \vdots \\ \alpha_{n1}x_1 & + & \alpha_{n2}x_2 & + & \ldots & + & \alpha_{nn}x_n & = & \beta_n \end{cases}$$

matricos $A = (\alpha_{ij}) \in M_n(k)$*, sudarytos iš koeficientų prie nežinomųjų, determinantas* $\det A \neq 0$*. Tada ši tiesinių lygčių sistema turi vienintelį sprendinį* $(\gamma_1, \gamma_2, \ldots, \gamma_n)$*, kurio* j*-oji koordinatė*

$$\gamma_j = \frac{d_j}{\det A}, \quad 1 \leq j \leq n,$$

čia d_j*,* $1 \leq j \leq n$ *– matricos, gautos matricoje* A j*-ąjį stulpelį pakeitus lygčių sistemos laisvaisiais nariais, determinantas.*

Įrodymas. Šią tiesinių lygčių sistemą užrašykime taip:

$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}. \tag{7.13}$$

Kadangi $\det A \neq 0$, tai egzistuoja atvirkštinė matrica A^{-1}, kuri lygi

$$\frac{1}{\det A} \begin{pmatrix} A^{11} & A^{21} & \ldots & A^{n1} \\ A^{12} & A^{22} & \ldots & A^{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A^{1n} & A^{2n} & \ldots & A^{nn} \end{pmatrix}.$$

(7.13) lygybės abi puses padauginę iš kairės iš A^{-1}, gauname:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \frac{1}{\det A} \begin{pmatrix} A^{11} & A^{21} & \ldots & A^{n1} \\ A^{12} & A^{22} & \ldots & A^{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A^{1n} & A^{2n} & \ldots & A^{nn} \end{pmatrix} \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}.$$

Taigi

$$x_j = \frac{\beta_1 A^{1j} + \beta_2 A^{2j} + \cdots + \beta_n A^{nj}}{\det A}.$$

Kaip matome, $\beta_1 A^{1j} + \beta_2 A^{2j} + \cdots + \beta_n A^{nj}$ – matricos, gautos matricoje A j-ąjį stulpelį pakeitus lygčių sistemos laisvaisiais nariais, determinanto skleidinys j-uoju stulpeliu. $\square$

7.11.2 pavyzdys. Išspręsime tiesinių lygčių sistemą

$$\begin{cases} 3x_1 - 2x_2 + 2x_3 = 39 \\ -x_1 + 5x_2 + 6x_3 = -78 \\ 2x_1 + 3x_2 + 5x_3 = -39 \end{cases}$$

remdamiesi Kramerio taisykle. Kadangi sistemos determinantas

$$d = \begin{vmatrix} 3 & -2 & 2 \\ -1 & 5 & 6 \\ 2 & 3 & 5 \end{vmatrix} = -39$$

yra nenulinis skaičius, tai, remiantis Kramerio taisykle (žr. 7.11.1 teoremą), nagrinėjama lygčių sistema turi vienintelį sprendinį. Šis sprendinys randamas iš formulių

$$x_i = \frac{d_i}{d}, \quad i \in \{1, 2, 3\},$$

čia

$$d_1 = \begin{vmatrix} 39 & -2 & 2 \\ -78 & 5 & 6 \\ -39 & 3 & 5 \end{vmatrix} = -117, \quad d_2 = \begin{vmatrix} 3 & 39 & 2 \\ -1 & -78 & 6 \\ 2 & -39 & 5 \end{vmatrix} = 585,$$

$$d_3 = \begin{vmatrix} 3 & -2 & 39 \\ -1 & 5 & -78 \\ 2 & 3 & -39 \end{vmatrix} = 0.$$

Taigi nagrinėjama lygčių sistema turi vienintelį sprendinį $(3, -15, 0)$.

7.12 Hamiltono-Keilio teorema

7.12.1 apibrėžimas. Tarkime, kad k – kūnas, o matrica $A = (\alpha_{ij}) \in M_n(k)$. Kintamojo t polinomas $\varphi_A(t)$, apibrėžtas lygybe

$$\varphi_A(t) = \det(A - t\mathbf{1}_n) = \det \begin{pmatrix} \alpha_{11} - t & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} - t & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} - t \end{pmatrix},$$

vadinamas matricos A *charakteristiniu polinomu*.

n-tosios eilės kvadratinei matricai A su koeficientais iš kūno k ir polinomui

$$p(t) = a_m t^m + a_{m-1}t^{m-1} + \cdots + a_1 t + a_0 \in k[t]$$

pažymėkime

$$p(A) := a_m A^m + a_{m-1}A^{m-1} + \cdots + a_1 A + a_0 \cdot \mathbf{1}_n.$$

Taigi $p(A)$ yra n-tosios eilės kvadratinė matrica.

7.12.2 pavyzdys. Nagrinėkime matricą

$$A = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

ir polinomą $p(t) = t^2 - t + 3$. Tada

$$p(A) = A^2 - A + 3 \cdot \mathbf{1}_2 = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} - \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} = \begin{pmatrix} 5 & 2 \\ 1 & 5 \end{pmatrix}.$$

7.12.3 teorema (Hamiltono-Keilio teorema). *n-tosios eilės kvadratinės matricos A su koeficientais iš kūno k charakteristiniam polinomui $\varphi_A(t)$ teisinga lygybė*

$$\varphi_A(A) = \mathcal{O},$$

čia $\mathcal{O}$ – nulinė matrica.

Įrodymas. Nagrinėkime n-tos eilės kvadratinę matricą

$$B(t) = (A_{ij}(t)),$$

čia $A_{ij}(t)$ yra matricos

$$A - t\mathbf{1}_n = \begin{pmatrix} \alpha_{11} - t & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} - t & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} - t \end{pmatrix}$$

ji elemento algebrinis adjunktas. Kiekvienas matricos $B(t)$ elementas $A_{ij}(t)$ yra kintamojo t polinomas, kurio laipsnis $\deg A_{ij}(t) \le n-1$. Tegu

$$B(t) = B_{n-1}t^{n-1} + \cdots + B_1 t + B_0,$$

čia B_j, $0 \le j \le n-1$, matricos su pastoviaisiais koeficientais. Be to, tegu

$$\varphi_A(t) = (-1)^n t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0.$$

Tada

$$(A - t\mathbf{1}_n)B(t) = \varphi_A(t)\mathbf{1}_n.$$

Sudauginę ir sulyginę koeficientus prie t laipsnių, gauname:

$$\begin{array}{ccccc} & & B_{n-1} & = & (-1)^n \\ AB_{n-1} & - & B_{n-2} & = & a_{n-1} \\ AB_{n-2} & - & B_{n-3} & = & a_{n-2} \\ \cdots\cdots & \cdots & \cdots & \cdots & \cdots\cdots \\ AB_1 & - & B_0 & = & a_1 \\ AB_0 & & & = & a_0 \end{array}$$

Pirmąją lygybę iš kairės padauginę iš A^n, antrąją – iš A^{n-1} ir t. t. ir sudėję, gauname:

$$\mathcal{O} = (-1)^n A^n + a_{n-1}A^{n-1} + \cdots + a_1 A + A_0 = \varphi_A(A).$$

□

Hamiltono-Keilio teoremoje tvirtinama, kad matrica A yra jos chrakteristinio polinomo šaknis.

Literatūra

[1] D. S. Dummit, R. M. Foote, *Abstract algebra,* 3rd ed., Wiley International Edition. Chichester: Wiley, 2004.

[2] E. Gaigalas, *Algebros užduotys ir rekomendacijos,* 1992, tinklalapis: http://www.mif.vu.lt/katedros/mmk/gaig/files/algebra1.html

[3] T. Gowers (ed.), J. Barrow-Green (ed.), I. Leader (ed.), *The Princeton companion to mathematics,* Princeton, NJ: Princeton University Press, 2008.

[4] W. H. Greub, *Linear algebra,* 4th ed., Springer, 451 p., 1975.

[5] J. Hefferon, *Linear algebra,* CreateSpace, 446 p., 2011, tinklalapis: http://joshua.smcvt.edu/linearalgebra/book.pdf, tinklalapis: http://joshua.smcvt.edu/linearalgebra

[6] K. M. Hoffman, *Linear algebra,* 2nd ed., Prentice Hall, 407 p., 1971.

[7] A. I. Kostrikin, *Introduction to algebra (Iš rusų kalbos vertė Neal Koblitz.),* New York-Heidelberg-Berlin: Springer-Verlag, 1982.

[8] S. Lang, *Linear algebra,* 3rd ed., Undergraduate Texts in Mathematics, Springer, 305 p., 1987.

[9] S. Lang, *Introduction to linear algebra,* 2nd ed. (corrected 2nd printing), New York, NY: Springer, 305 p., 1988.

[10] D. C. Lay, *Linear algebra and its applications,* 4th ed., Addison Wesley, 576 p., 2011.

[11] E. Manstavičius, *Analizinė ir tikimybinė kombinatorika,* TEV, Vilnius, 2007.

[12] K. Matthews, *Elementary linear algebra,* Lecture notes, 2011, tinklalapis: http://www.numbertheory.org/book/mp103.pdf

[13] A. Matuliauskas, *Algebra,* Vilnius: Mokslas, 1985.

[14] R. Messer, *Linear algebra: gateway to mathematics,* Addison Wesley, 560 p., 1997.

[15] G. Strang, *Linear algebra: video lectures,* 1999, tinklalapis: http://ocw.mit.edu/courses/mathematics/18-06-linear-algebra-spring-2010/video-lectures

[16] G. Strang, *Introduction to linear algebra,* 4th ed., Wellesley Cambridge Press, 584 p., 2009.

[17] H. Weyl, *Symmetry,* Princeton, NJ: Princeton University Press, 1989.

Pavardžių rodyklė

ABELIS (Niels Henrik Abel, 1802–1829)

BANACHAS (Stefan Banach, 1892–1945)

BERNAISAS (Paul Bernays, 1888–1977)

BEZU (Étienne Bézout, 1730–1783)

BOLCANAS (Bernard Bolzano, 1781–1848)

CERMELAS (Ernst Zermelo, 1871–1953)

CORNAS (Max Zorn, 1906–1993)

DEDEKINDAS (Richard Dedekind, 1831–1916)

DEKARTAS (René Descartes, 1596–1650)

De MORGANAS (Augustus De Morgan, 1806–1871)

De FRYZAS (Gustav de Vries, 1866–1934)

EIZENŠTEINAS (Ferdinand Gotthold Max Eisenstein, 1823–1852)

EŠERAS (Maurits Cornelis Escher, 1898–1972)

FRENKELIS (Abraham Fraenkel, 1891–1965)

FURJĖ (Jean Baptiste Joseph Fourier, 1768–1830)

GALUA (Évariste Galois, 1811–1832)

GAUSAS (Carl Friedrich Gauss, 1777–1855)

GORDONAS (Walter Gordon, 1893–1939)

GIODELIS (Kurt Gödel, 1906–1978)

HAMILTONAS (William Rowan Hamilton, 1805–1865)

HANAS (Hans Hahn, 1879–1934)

HORNERIS (William George Horner, 1786–1837)

KADOMCIAVAS (Boris Kadomtsev, 1928–1998)

KAPELIS (Alfredo Capelli, 1855–1910)

KEILIS (Arthur Cayley, 1821–1895)

KORTEVEGAS (Diederik Korteweg, 1848–1941)

KRAMERIS (Gabriel Cramer, 1704–1752)

KRONEKERIS (Leopold Kronecker, 1823–1891)

KUAINAS (Willard Van Orman Quine, 1908–2000)

KURATOVSKIS (Kazimierz Kuratowski, 1896–1980)

KANTORAS (Georg Cantor, 1845–1918)

KOŠI (Augustin Louis Cauchy, 1789–1857)

LAGRANŽAS (Joseph Louis Lagrange, 1736–1813)

LEIBNICAS (Gottfried Wilhelm Leibniz, 1646–1716)

LI (Sophus Lie, 1842–1899)

MUAVRAS (Abraham de Moivre, 1667–1754)

NOIMANAS (John von Neumann, 1903–1957)

OILERIS (Leonhard Euler, 1707–1783)

PEANAS (Giuseppe Peano, 1858–1932)

PETIAŠVILIS (Vladimir Petviashvili, 1936–1993)

RASELAS (Bertrand Russell, 1872–1970)

SYLOVAS (Peter Ludwig Mejdell Sylow, 1832–1918)

ŠTURMAS (Jacques Charles François Sturm, 1803–1855)

TEILORAS (Brook Taylor, 1685–1731)

VANDERMONDAS (Alexandre-Théophile Vandermonde, 1735–1796)

VEILIS (Hermann Weyl, 1885–1955)

VEJERŠTRASAS (Karl Weierstrass, 1815–1897)

VIJETAS (François Viète, 1540–1603)

Rodyklė

adjunktas
  algebrinis, 266
afinioji plokštuma, 91
afiniosios transformacijos, 89
aibė
  kryptinė, 36
  skaiti, 26
  tiesiškai sutvarkyta, 33
  visiškai sutvarkyta, 35
aibės
  ekvivalenčios, 25
  papildinys, 16
  to paties tipo, 37
aibių
  junginys, 13
  lygybė, 12
  sąjunga, 13
  sandauga, 14
  sankirta, 14
  šeima, 13
  simetrinis skirtumas, 15
  skirtumas, 15
  suma, 13
aksiomų sistema
  Bernaiso-Giodelio, 11
  Cermelo-Frenkelio, 11, 38
aksioma
  Cermelo, 35
  ėmimo, 35
  parinkimo, 35
algebra, 173
  asociatyvioji, 173
algebriškai uždaras kūnas, 231
algebrinis adjunktas, 266
algoritmas
  Euklido, 59, 207
apibrėžimo sritis, 18
argumentas
  kompleksinio skaičiaus, 195
asociatyvumas, 14
asocijuoti žiedo elementai, 190
atitiktis
  binarioji, 18
  dvivietė, 18
atvaizdis, 21
  alternuojantysis, 275
  bijekcinis, 24
  injekcinis, 24
  monotoninis, 37
  n-tiesinis, 275
  siurjekcinis, 24
atvirkštinis elementas, 53, 80
atvirkštinis sąryšis, 19
atvirkštinė matrica, 279
atvirkštinis elementas, 167
automorfizmas
  grupės, 110
  vidinis, 113

baigtinė grupė, 83

baigtinai generuota grupė, 97
begalinės eilės elementas, 97
bijekcija, 24
branduolys, 185
    grupių homomorfizmo, 112

centralizatorius, 127
centras
    grupės, 105
Cermelo teorema, 35
charakteristinis polinomas, 287
ciklai
    nepriklausomi, 140
ciklas, 140
ciklinė grupė, 97
ciklinis pogrupis, 97
ciklinis tipas, 154
ciklo ilgis, 140
Corno lema, 35

dėsnis
    De Morgano, 15
dalíklis, 57, 189
    vieneto, 189
dalybos su liekana formulė, 58
daugianaris, 202
dešinioji gretutinė klasė, 99
Dekarto sandauga, 23
determinantas, 265
    Vandermondo, 275
didžiausias bendrasis daliklis
    polinomų, 206
    skaičių, 58
diedro grupė, 86
distributyvumas, 15

eilė
    grupės, 83
    grupės elemento, 97
Eizenšteino kriterijus, 238
ekvivalenčios aibės, 25
ekvivalentumo klasė, 29
elementarieji pertvarkymai, 69, 269
elementas
    atvirkštinis, 53
    begalinės eilės, 97
    galinis, 34
    maksimalusis, 33
    minimalusis, 33
    neutralus, 51
    pradinis, 34
    priešingas, 53
    simetrinis, 52
elemento eilė, 97
Euklido algoritmas, 59, 207

faktoržiedas, 183
faktoraibė, 31
faktordėsnis, 51
faktorgrupė, 109
formulė
    dalybos su liekana, 58
    Lagranžo interpoliacinė, 213
    Leibnico, 214
    Teiloro, 215
formulės
    Vijeto, 213
funkcija, 20
    Kronekerio, 176

Gauso lema, 237
Gauso metodas, 74, 280
generuojantieji elementai, 96
generuotas pogrupis, 96
grafikas
    atvaizdžio, 24
gretutinė klasė, 99
griežtai trapecinė lygčių sistema, 71
grupė, 80
    Abelio, 81
    afiniųjų transformacijų, 89
    baigtinė, 83
    baigtinai generuota, 97
    ciklinė, 97

diedro, 86
komutatyvioji, 81
simetrinė, 84
grupės
izomorfinės, 110
grupės centras, 105
grupės eilė, 83
grupės elemento eilė, 97
grupės plėtinys, 118
grupės vienetas, 80
grynai menamasis skaičius, 192

Hamiltono-Keilio teorema, 288
homogeninė lygtis, 67
homogeninių lygčių sistema, 67
homomorfizmas
grupių, 110
žiedų, 183
homotetija, 89
Hornerio schema, 209

idealas, 179
maksimalus, 188
pagrindinis, 180
pirminis, 188
idempotentas, 167
idempotentumas, 14
indeksas
pogrupio, 101
indukcijos principas, 57
injekcija, 24
integralumo sritis, 168
invariantai
grupės, 138
inversija, 142
išorinė tiesioginė sandauga, 118
išorinė tiesioginė sandauga, 121, 123
išorinis kompozicijos dėsnis, 54
išraiška
kanoninė
polinomo, 220
skaičiaus, 64
išvestinė
polinomo, 214
izomorfizmas, 47
grupių, 110

jungtinis kompleksinis skaičius, 194

kairioji gretutinė klasė, 99
kanoninė išraiška
polinomo, 220
skaičiaus, 64
kanoninis skaidinys
polinomo, 220
skaičiaus, 64
kartotinumas
šaknies, 210
Keilio teorema, 159
keitinys, 84, 139
ciklas, 140
lyginis, 142
nelyginis, 142
transpozicija, 140
kitimo sritis, 18
klasės atstovas, 99
kompleksinis skaičius, 192
grynai menamasis, 192
jungtinis, 194
kompozicija
atvaizdžių, 22
sąryšių, 19
kompozicijos dėsnis, 44
asociatyvusis, 48
indukuotas, 54
indukuotasis, 50
išorinis, 53
komutatyvus, 53
suderintas, 54
komutantas, 105
komutatorius, 105
komutatyvumas, 14
konstrukcija
Kuratovskio, 18

Kramerio taisyklė, 286
Kronekerio funkcija, 176
Kronekerio-Kapelio teorema, 79
kūnas, 167
  algebriškai uždaras, 231
  Gauso skaičių, 170
  kompleksinių skaičių, 170
  kvaternionų, 169
  nekomutatyvusis, 167
  nulinės charakteristikos, 215
  racionaliųjų kvaternionų, 169
  racionaliųjų trupmenų, 221
  santykių, 172
kvaternionų kūnas, 169

Lagranžo teorema, 102
laipsnis
  polinomo, 203
Leibnico formulė, 214
lema
  Corno, 35
  Gauso, 237
likinių aibė, 51
likinių klasė, 51
lyginis keitinys, 142

maksimalus idealas, 188
matematinės indukcijos principas, 57
matrica, 173, 258
  atvirkštinė, 279
  kvadratinė, 174
  nulinė, 259
  transponuota, 260
  vienetinė, 258
matricos pėdsakas, 177
menamoji dalis, 192
menamoji tiesė, 193
metodas
  Gauso, 74, 280
  neapibrėžtųjų koeficientų, 227
minoras
  papildomas, 266
modulis
  kompleksinio skaičiaus, 193
multiplikatyvi funkcija, 193

neapibrėžtųjų koeficientų metodas, 227
nelyginis keitinys, 142
nepriklausomi ciklai, 140
neredukuojamas polinomas, 218
nesutvarkytasis dvejetas, 17
nesutvarkytoji pora, 17
netvarka, 142
neutralus elementas, 51
nilpotentas, 168
normalizatorius, 128
normalusis pogrupis, 106
normuotas polinomas, 218
n-tiesinis atvaizdis, 275
nulinės charakteristikos kūnas, 215
nulio daliklis, 167

orbita, 125, 141

pagrindinė algebros teorema, 231
pagrindinė aritmetikos teorema, 63
pagrindinių idealų žiedas, 248
pagrindinis idealas, 180
papildinys, 16
papildomas minoras, 266
paprastoji trupmena, 223
paradoksas
  Bertrano Raselo, 11
pėdsakas, 177
perstatinys, 139
p-grupė, 128
pirminis žiedo elementas, 190
pirminis idealas, 188
pirminis polinomas, 218
pirminis skaičius, 62
pirmvaizdis, 21
  pilnasis, 21
plėtinys
  grupės, 118

sąryšio, 20
požiedis, 167
poaibis, 12
aprėžtas iš apačios, 34
aprėžtas iš viršaus, 34
stabilus, 50, 54
pogrupio indeksas, 101
pogrupis, 93
ciklinis, 97
generuotas, 96
normalusis, 106
stacionarusis, 152
sujungtinis, 126
polinomų žiedas, 204
polinomai
tarpusavyje pirminiai, 207
polinomas, 202
charakteristinis, 287
neredukuojamas, 218
normuotas, 218
pirminis, 218
primityvusis, 237
redukuojamas, 218
polinomo laipsnis, 203
polinomo šaknis, 208
priešingas elementas, 53
primarioji p-grupė, 129
principas
egzistencijos, 56
pilnosios indukcijos, 57
projekcija
Dekarto sandaugos, 23
projekcinė plokštuma, 91

racionaliųjų trupmenų kūnas, 221
racionalioji trupmena, 221
realioji dalis, 192
realioji tiesė, 193
refleksyvumas, 27
reikšmių aibė, 18
rodiklinė išraiška, 197

šaknis
iš kompleksinio skaičiaus, 198
kartotinė, 210
paprastoji, 210
polinomo, 208
santykių kūnas, 172
sąryšis
binarusis, 18
dvivietis, 18
ekvivalentumo, 27
funkcinis, 20
siaurinys
sąryšio, 19
σ-nejudamas elementas, 141
simetriškumas, 27
simetrija, 87, 90
simetrinė grupė, 84, 139
simetrinis elementas, 52
siurjekcija, 24
skaičius
kompleksinis, 192
skaidinys
kanoninis
polinomo, 220
skaičiaus, 64
skaičiaus, 153
skaiti aibė, 26
stabilizatorius, 125
stabilus poaibis, 54
stacionarusis pogrupis, 152
standartinė bazė, 257
struktūra
afiniosios plokštumos, 90
aibėje, 90
projekcinės plokštumos, 91
Šturmo teorema, 243
sudaromosios, 96
idealo, 180
sujungtinių elementų klasė, 127, 152
sujungtiniai elementai, 151
sujungtinis pogrupis, 126

sutvarkytoji aibė, 32
sutvarkytasis dvejetas, 18
sutvarkytoji pora, 18
sveikumo sritis, 168
Sylovo p-pogrupis, 156
Sylovo teorema, 156, 157

taisyklingoji trupmena, 222
Teiloro formulė, 215
teorema
  Cermelo, 35
  Hamiltono-Keilio, 288
  Keilio, 159
  Kronekerio-Kapelio, 79
  Lagranžo, 102
  pagrindinė algebros, 231
  pagrindinė aritmetikos, 63
  Šturmo, 243
  Sylovo, 156, 157
tiesiškai sutvarkyta aibė, 33
tiesinė erdvė, 173
tiesinė erdvė, 256
tiesinė lygtis, 67
tiesinių lygčių sistema, 67
tiesioginė sandauga
  pogrupių, 119, 121
tiesioginė suma, 133
transformacija
  afinioji, 89, 91
  projekcinė, 91
transpozicija, 140
tranzityvumas, 27
trapecinė lygčių sistema, 71
trigonometrinė išraiška, 195
trikampė lygčių sistema, 71
trupmena
  paprastoji, 223
  taisyklingoji, 222
tvarka, 33

vaizdas
  elemento, 21
  poaibio, 21
Vandermondo determinantas, 275
vektorius, 256
vidinis automorfizmas, 113
vieneto daliklis, 189
Vijeto formulės, 213
visiškai sutvarkyta aibė, 35

žiedas, 166
  integralumo sritis, 168
  komutatyvusis, 167
  pagrindinių idealų, 248
  polinomų, 204
  su dalyba, 167
  su vienetu, 167
  sveikumo sritis, 168

Paulius Drungilas, Hamletas Markšaitis
Algebra. I dalis. – Vilniaus universiteto leidykla, 2013. – 310 p.

ISBN 978-609-459-128-0

Šis algebros vadovėlis (pirmoji dalis) parašytas Vilniaus universiteto Matematikos ir informatikos fakulteto matematikos specialybės studentams skaitomų algebros paskaitų pagrindu.

Viršelio dailininkė *Audronė Uzielaitė*
Kalbos redaktorė *Gražina Indrišiūnienė*

Išleido Vilniaus universiteto leidykla
Universiteto g. 3, LT-01513 Vilnius