Latvijas Universitāte
Fizikas un matemātikas fakultāte
Matemātiskās analīzes katedra

Jānis Buls

ABSTRAKTĀ ALGEBRA

Lekciju konspekts — 2008

SATURS

IEVADS

Abstraktā algebra — tas ir īpašs elegants domāšanas stils, kas pirmajā skatījumā neatšķiras no matemātikā vispārpieņemtām shēmām; tomēr tā ir pavisam cita fantastiska pasaule. Abstraktās algebras vadmotīvs — matemātiskie objekti kā tādi, paši par sevi, nav tik būtiski — svarīgi ir šo objektu savstarpējie sakari, attiecības.

Mēs sākam ar pašu vienkāršako, proti, ar kopām un tajās definētajām operācijām. Algebriskās operācijas pakļaujas konkrētiem likumiem — aksiomām. Šīs aksiomas izvēlas tā, lai tās aprakstītu lietojumos biežāk sastopamās īpašības, tādas kā: asociativitāte, komutativitāte, distributivitāte. Tā rezultātā mēs pakāpeniski virzāmies no vienkāršā uz sarežģīto: attēlojumi, operācijas; pusgrupas, grupas, gredzeni, lauki; moduļi, asociatīvas algebras; grupu algebras, pusgrupu algebras; polinomi, grupu reprezentācijas. Tās ir galvenās tēmas, kas tiks aplūkotas šajā kursā.

Tiem, kas ir pragmatiskāk noskaņoti, atgādināsim, ka abstraktā algebra kā pamatkurss parasti tiek iekļauta daudzu pasaules universitāšu matemātikas bakalaura studiju programmās, jo abstraktās algebras aparātu (galvenokārt tehniku) lieto citās matemātikas nozarēs, fizikā, inženierzinātnēs, datorzinātnēs; mūsdienās arī ekonomikā un bioloģijā. Tas viss izskaidrojams ar algebras pamatnostāju, pētīt algebriskas sistēmas ar precizitāti līdz izomorfismam, specifiskas interpretācijas un jautājumus bieži vien atstājot konkrēto zinātņu pārziņā.

APZĪMĒJUMI

$\neg$ — negācija,
$\vee$ — disjunkcija, $\wedge$ — konjunkcija,
$\Rightarrow$ — implikācija, $\Leftrightarrow$ — ekvivalence,
$\exists$ — eksistences kvantors, $\forall$ — universālkvantors,
$\exists! x\ P(x)$ — eksistē viens vienīgs tāds x, kam izpildās nosacījums $P(x)$,
$\overset{\infty}{\exists}\ x\ P(x)$ — bezgalīgi daudziem x izpildās nosacījums $P(x)$,
$\overset{\infty}{\forall}\ x\ P(x)$ — gandrīz visiem x izpildās nosacījums $P(x)$,

$x \in X$ — elements x pieder kopai X jeb x ir kopas X elements,
$A \subseteq B$ — kopa A ir kopas B apakškopa, $\mathfrak{P}(B) \leftharpoondown\!\!= \{A \mid A \subseteq B\}$,
$A \subset B$ — kopa A ir kopas B īsta apakškopa,
$A \cup B$, $A \cap B$, $A \setminus B$ — kopu A un B apvienojums, šķēlums, starpība,
$\min K$ — kopas K minimālais elements,
$\max K$ — kopas K maksimālais elements,

$\leftharpoondown\!\!=$, $=\!\!\rightharpoondown$ — vienādības saskaņā ar definīciju,
$\overline{1,n} \leftharpoondown\!\!= \{1, 2, \ldots, n\}$; $\overline{k,n} \leftharpoondown\!\!= \{k, k+1, \ldots, n\}$, te $k \leq n$,
$\mathbb{Z}$ — veselo skaitļu kopa,
$\mathbb{Z}_+ \leftharpoondown\!\!= \{x \mid x \in \mathbb{Z} \wedge x > 0\}$, $\mathbb{Z}_- \leftharpoondown\!\!= \{x \mid x \in \mathbb{Z} \wedge x < 0\}$,
$\mathbb{N} \leftharpoondown\!\!= \mathbb{Z}_+ \cup \{0\}$, $\mathbb{N}_- \leftharpoondown\!\!= \mathbb{Z} \setminus \mathbb{Z}_+$,
$\mathbb{Q}$ — racionālo skaitļu kopa,
$\mathbb{R}$ — reālo skaitļu kopa, $\mathbb{C}$ — komplekso skaitļu kopa,
$\mathbb{R}_+ \leftharpoondown\!\!= \{x \in \mathbb{R} \mid x \geq 0\}$, $\mathbb{R}_- \leftharpoondown\!\!= \{x \in \mathbb{R} \mid x \leq 0\}$,
$\mathbb{R}^* \leftharpoondown\!\!= \mathbb{R} \setminus \{0\}$, $\mathbb{R}^*_+ \leftharpoondown\!\!= \{x \in \mathbb{R}^* \mid x > 0\}$, $\mathbb{R}^*_- \leftharpoondown\!\!= \{x \in \mathbb{R}^* \mid x < 0\}$,
$\aleph_0$ — kopas $\mathbb{N}$ apjoms, $\mathfrak{c}$ — reālo skaitļu kopas $\mathbb{R}$ apjoms,

$\langle x, y \rangle \leftharpoondown\!\!= (x, y) \leftharpoondown\!\!= \{\{x\}, \{x, y\}\}$,
$(x_1, x_2, \ldots, x_n) \leftharpoondown\!\!= ((x_1, x_2, \ldots, x_{n-1}), x_n)$,

$A_1 \times A_2 \times \ldots \times A_n \leftharpoondown \{(x_1, x_2, \ldots, x_n) \,|\, \forall i \in \overline{1,n}\, (x_i \in A_i)\}, \quad A^n$,
$f : x \mapsto y, \quad f : X \multimap\!\!\to Y, \quad X \overset{f}{\multimap\!\!\to} Y$,
$\mathrm{Dom}(f) \leftharpoondown \{x \,|\, \exists y \in Y\ (f : x \mapsto y)\}, \quad \mathrm{Ran}(f) \leftharpoondown \{y \,|\, \exists x \in X\ (f : x \mapsto y)\}$,
$f : X \to Y, \quad X \xrightarrow{f} Y, \quad f : X \twoheadrightarrow Y, \quad f : X \hookrightarrow Y$,
$Y^\omega \leftharpoondown \{\psi \,|\, \psi : \mathbb{N} \to Y\}$,
$f|H$ — attēlojuma f sašaurinājums kopā H,
$\mathrm{pr}_i\rho$ — attiecības ρ vai operācijas ρ i–tā projekcija,

$a \diagdown b$ — skaitlis b ir skaitļa a daudzkārtnis,
$a \nmid b$ — skaitlis b nav skaitļa a daudzkārtnis,
$D(a_1, a_2, \ldots, a_n) \leftharpoondown \{q | \forall i \in \overline{1,n}\ q \diagdown a_i\}$,
$\mathrm{ld}(a_1, a_2, \ldots, a_n) \leftharpoondown \max D(a_1, a_2, \ldots, a_n)$,
$\mathrm{md}(a_1, a_2, \ldots, a_n)$ — skaitļu $a_1, a_2, \ldots, a_n$ mazākais kopīgais dalāmais,

$a \equiv b(\mathrm{mod}\ m)$ — skaitļi a un b ir kongruenti pēc moduļa m,
$[a] \leftharpoondown \{b \mid a \equiv b(\mathrm{mod}\ m)\}$,
$\mathbb{Z}_m \leftharpoondown \{[0], [1], \ldots, [m-1]\}$,
$\mathbb{Z}m \leftharpoondown \{x \in \mathbb{Z} \,|\, m \diagdown x\}$,

$\mathrm{Mat}_n^m(\mathbb{R})$ — visu $m \times n$ matricu kopa ar elementiem no lauka $\mathbb{R}$,
$\mathrm{Mat}_n(\mathbb{R}) \leftharpoondown \mathrm{Mat}_n^n(\mathbb{R})$,
$D_n(\mathbb{R})$ — visu n–tās kārtas diagonālmatricu kopa ar elementiem no lauka $\mathbb{R}$,
$GL_n(\mathbb{R})$ — pilna lineāra grupa pār lauku $\mathbb{R}$,
$SL_n(\mathbb{R})$ — speciāla lineāra grupa pār lauku $\mathbb{R}$,
$DL_n(\mathbb{R})$ — nesingulāro diagonālmatricu grupa pār lauku $\mathbb{R}$,
$\mathfrak{S}(A)$ — kopas A simetriskā grupa, $\quad \mathfrak{S}_n \leftharpoondown \mathfrak{S}(\overline{1,n})$,

$\mathrm{K\bar{e}r}f$ — attēlojuma f kodols,
$\mathrm{Im}f$ — attēlojuma f attēls,
$\mathrm{Hom}(M, M') \leftharpoondown \{f : M \to M' \,|\, f \text{ ir moduļu homomorfisms}\}$,
$\mathrm{End}(M)$ — moduļa M visu endomorfismu kopa,
$\mathrm{Aut}(M)$ — moduļa M visu automorfismu kopa,
$\mathcal{L}(\mathfrak{A})$ — sistēmas $\mathfrak{A}$ lineārā čaula,

$\square$ — pierādījuma sākums,
$\blacksquare$ — pierādījuma beigas;
$\Rightarrow$ — implikācijas zīmi pierādījuma sākumā mēs izmantojam, lai norādītu,

ka tagad sākas teorēmas nepieciešamā nosacījuma pierādījums,
$\Leftarrow$ — šo zīmi pierādījumos mēs izmantojam, lai norādītu, ka tagad sākas teorēmas pietiekamā nosacījuma pierādījums,
$\stackrel{A1.2.3}{=}$ — šo apzīmējumu pierādījumos mēs izmantojam, lai norādītu, ka vienādības pamatotība balstās uz apgalvojumu 1.2.3 (saprotams, ka apgalvojuma 1.2.3 vietā var būt jebkurš cits apgalvojums, teorēma, lemma, formula, utm.).

1. nodaļa

ATTĒLOJUMI

Attēlojumi un operācijas. Attēlojumu kompozīcijas asociativitāte. Injektīvu un sirjektīvu attēlojumu kategoriālais raksturojums. Injektīvo, sirjektīvo un bijektīvo attēlojumu kompozīcija. Inversais attēlojums, bijekcijas inversais attēlojums. Substitūcijas. Kopas sadalījums un ekvivalences tipa predikāts. Attēlojuma kodols. Faktorkopa, Neteres pirmā izomrfisma teorēma attēlojumiem.

1.1. Attēlojumi un operācijas

Attīstītas teorijas pamatiezīme ir "spēles noteikumu" fiksēšana. Tāpēc rodas uzdevums veidot teoriju ar vislielāko rūpību un loģisko precizitāti. Tie apgalvojumi, kurus izmanto kaut kādā pierādījumā, arī paši prasa pierādījumu ar kādu agrāku apgalvojumu palīdzību, savukārt agrākie apgalvojumi arī jāpierāda, utt. Kurā vietā šai spriedumu ķēdei būs gals (precīzāk — sākums)? Tāda vispār nav. Kāda ir izeja no aprakstītā šķietami bezcerīgā stāvokļa? Matemātiķi šo "Gordija mezglu" nav atraisījuši, bet vienkārši pārcirtuši. Proti, kādā vietā spriedumu ķēdē daži apgalvojumi tiek akceptēti *bez pierādījuma*. Tos sauc par *aksiomām*.

Līdzīga situācija ir ar jēdzieniem. Katrā definīcijā jaunais jēdziens tiek konstruēts ar citu jēdzienu palīdzību. Tā rezultātā katra definīcija saistās ar citām, kuras definētos jēdzienus, kas apskatāmajā definīcijā tiek uzskatīti par zināmiem. Piemēram, par taisnes nogriezni sauc taisnes daļu, kas atrodas starp diviem punktiem. Bet kā definēt jēdzienus "taisne" un "starp"? Tātad definīcijas veido tādu pašu bezgalīgu virkni kā pierādījumi. Tādēļ dažus jēdzienus izvēlas *bez definīcijas*. Tos sauc par *pamatjēdzieniem* jeb *sākotnējiem* *jēdzieniem.* Pārējos (definētos) jēdzienus sauc par *atvasinātiem jēdzieniem.* Pamatjēdzienu un aksiomu izvēles pamatotība daudzējādā ziņā ir ārpus matemātikas. Te jābalstās gan uz filozofiju, praksi, gan zinātnes metodoloģiju. Matemātikas sistematizācija deviņpadsmitā gadsimta beigu posmā ļāva secināt, ka viens no perspektīvākajiem pamatjēdzieniem matemātikā ir kopas jēdziens. To var izvēlēties par vienīgo pamatjēdzienu visā matemātikā.

Kopu $\{\{x\},\{x,y\}\}$ sauc par elementu $x \in X$ un $y \in Y$ *sakārtotu pāri* un lieto apzīmējumu (x,y) vai $\langle x,y\rangle$. Pāri $((x_1,x_2,\ldots,x_{n-1}),x_n)$, kur $\forall i \in \overline{1,n}$ $(x_i \in A_i)$ sauc par *n-dimensionālu kortežu* pār kopām $A_1, A_2, \ldots, A_n$. Turpmāk n-dimensionāla korteža apzīmēšanai lietosim pierakstu $(x_1,x_2,\ldots,x_n)$. Par kopu $A_1, A_2, \ldots, A_n$ *Dekarta reizinājumu* sauc visu n-dimensionālo kortežu kopu pār kopām $A_1, A_2, \ldots, A_n$, t.i.,

$$A_1 \times A_2 \times \ldots \times A_n \rightleftharpoons \{(x_1,x_2,\ldots,x_n) \,|\, \forall i \in \overline{1,n}\,(x_i \in A_i)\}.$$

Ja $A = A_1 = A_2 = \ldots = A_n$, tad lieto arī pierakstu $A^n \rightleftharpoons A_1 \times A_2 \times \ldots \times A_n$. Kopas $A_1 \times A_2 \times \ldots \times A_n$ apakškopu ϱ mēdz saukt arī par *n-vietīgu attieksmi (attiecību, predikātu)*, kas definēta kopā $A_1 \times A_2 \times \ldots \times A_n$. Šai situācijā kopu A_i, $i \in \overline{1,n}$, sauc par attieksmes ϱ *i-to projekciju* un lieto apzīmējumu $A_i = \mathrm{pr}_i \varrho$.

Trijnieku $f = \langle X, Y, F\rangle$, kur $F \subseteq X \times Y$ sauc par *attēlojumu* jeb *funkciju*, ja visiem kopas F elementiem $(x,y),(x,z)$ ir spēkā vienādība $y = z$. Kopu X sauc par attēlojuma f *starta* jeb *izejas* kopu, Y — par *finiša* jeb *ieejas* kopu, F sauc par *grafiku.* Ja $(x,y) \in F$, tad lieto pierakstu $f(x) = y$ jeb $f : x \mapsto y$. Vispārīgs pieraksts $f : X -\!\!\circ\!\!\!\longrightarrow Y$ (lieto arī pierakstu $X \overset{f}{-\!\!\circ\!\!\!\longrightarrow} Y$) norāda, ka f ir attēlojums ar starta kopu X un finiša kopu Y.

Kopu

$$\mathrm{Dom}(f) \rightleftharpoons \{x \,|\, \exists y \in Y\ (f : x \mapsto y)\}$$

sauc par attēlojuma $f : X -\!\!\circ\!\!\!\longrightarrow Y$ *definīcijas apgabalu.* Savukārt kopu

$$\mathrm{Ran}(f) \rightleftharpoons \{y \,|\, \exists x \in X\ (f : x \mapsto y)\}$$

sauc par attēlojuma f *vērtību apgabalu.* Attēlojumu $f : X -\!\!\circ\!\!\!\longrightarrow Y$ sauc par *visur definētu attēlojumu*, ja $\mathrm{Dom}(f) = X$. Šai gadījumā mēdz lietot vienu no apzīmējumiem

$$f : X \to Y \quad \text{vai} \quad X \xrightarrow{f} Y.$$

Pretējā gadījumā attēlojumu $f : X -\!\!\circ\!\!\!\longrightarrow Y$ sauc par *daļēji definētu,* proti, ja

$$\exists x \in X\ x \notin \mathrm{Dom}(f).$$

Visur definētu attēlojumu $g : X_1 \times X_2 \times \ldots \times X_n \to X_{n+1}$ sauc arī par *n-vietīgu algebrisku operāciju.* Šai situācijā kopu X_i, $i \in \overline{1, n+1}$, sauc par operācijas g *i-to projekciju* un lieto apzīmējumu $X_i = \mathrm{pr}_i g$.

1.1.1. Piemērs. Saskaitīšana $(+)$ un reizināšana $(\cdot)$ ir divvietīgas algebriskas operācijas reālo skaitļu kopā $\mathbb{R}$, taču dalīšana $(:)$ nav algebriska operācija reālo skaitļu kopā $\mathbb{R}$.

Mūsdienās termins "algebriska operācija" tiek lietots arī vispārīgākās situācijās. Tā rezultātā atšķirība starp attēlojumu un algebrisku operāciju ir nosacīta un bieži saistīta ar attiecīgās matemātikas nozares tradīcijām.

Turpmāk, ja tas netiks speciāli atrunāts, tad visi lietotie attēlojumi būs visur definēti attēlojumi.

1.2. Attēlojumu kompozīcija

1.2.1. Definīcija. *Ja $f : X \multimap\!\!\!\to Y$ un $g : Z \multimap\!\!\!\to W$ ir funkcijas, tad funkciju $h : X \multimap\!\!\!\to W$, kas definēta ar nosacījumu:*

$$\forall x \in X \quad h(x) = g(f(x)),$$

sauc par funkciju f un g kompozīciju (superpozīciju jeb saliktu funkciju) un apzīmē $g \circ f$.

Tātad funkciju kompozīcija $g \circ f$ ir trijnieks (X, W, H), kur

$$H = \{\, (x, w) \,|\, \exists y \in Y \cap Z \; (\, f : x \mapsto y \,\wedge\, g : y \mapsto w \,)\, \}.$$

Brīdinājums. (i) Dažkārt funkciju kompozīcijas $g \circ f$ apzīmēšanai mēdz lietot pierakstu fg vai arī pierakstu (fg). Šai gadījumā parasti pieraksta $h(x)$ vietā lieto pierakstu xh vai arī pierakstu $(x)h$. Tā rezultātā

$$xh = h(x) = g(f(x)) = (g \circ f)(x) = x(fg).$$

Savukārt

$$(xf)g = f(x)g = g(f(x)) = h(x) = xh.$$

Esam pierādījuši vienādību $x(fg) = (xf)g$.

(ii) Tā kā simbolu $\circ$ moduļu teorijā parasti lieto citiem mērķiem, tad situācijās, kad varētu rasties šaubas, mēs pieraksta $g \circ f$ vietā lietosim pierakstu $g \overset{\frown}{\cdot} f$.

1.2.2. Piemērs. Ja $f : \mathbb{R} \mathrel{-\!\!\circ\!\!\!\longrightarrow} \mathbb{R}$ un $g : \mathbb{R} \mathrel{-\!\!\circ\!\!\!\longrightarrow} \mathbb{R}$ ir reāla argumenta funkcijas, kur

$$f(x) = 6\sqrt{x} \quad \text{un} \quad g(x) = \cos^3 x,$$

tad

$$(g \circ f)(x) = g(f(x)) = \cos^3(6\sqrt{x}),$$

bet

$$(f \circ g)(x) = f(g(x)) = 6\sqrt{\cos^3 x}.$$

Tātad vispārīgā gadījumā $f \circ g \neq g \circ f$.

1.2.3. Apgalvojums. *Ja $f : X_1 \mathrel{-\!\!\circ\!\!\!\longrightarrow} Y_1$, $g : X_2 \mathrel{-\!\!\circ\!\!\!\longrightarrow} Y_2$ un $h : X_3 \mathrel{-\!\!\circ\!\!\!\longrightarrow} Y_3$ ir funkcijas, tad $(fg)h = f(gh)$.*

$\square$ No $(fg)h$ un $f(gh)$ definīcijas izriet, ka

$$(fg)h : X_1 \mathrel{-\!\!\circ\!\!\!\longrightarrow} Y_3 \quad \text{un} \quad f(gh) : X_1 \mathrel{-\!\!\circ\!\!\!\longrightarrow} Y_3,$$

t.i., šīm funkcijām ir vienas un tās pašas gan starta, gan finiša kopas. Savukārt vienādības

$$\begin{aligned} x((fg)h) &= (x(fg))h = ((xf)g)h = h(g(f(x))), \\ x(f(gh)) &= (xf)(gh) = ((xf)g)h = h(g(f(x))) \end{aligned}$$

demonstrē, ka šīm funkcijām sakrīt arī grafiki. $\blacksquare$

1.2.4. Apgalvojums. *Funkciju $f_1, f_2, \ldots, f_n$ kompozīcija jebkuram iekavu izvietojumam definē vienu un to pašu funkciju.*

$\square$ Pieņemsim, ka $f \leftharpoondown f_1(f_2(\ldots(f_{n-1}f_n)\ldots))$. Ja $n = 1$ vai $n = 2$, tad f_1, $f_1 f_2$ nesatur iekavas, un šai situācijā apgalvojums ir spēkā. Ja $n = 3$, tad tas ir iepriekšējais apgalvojums.

Tālākais pierādījums induktīvs, pieņemot, ka apgalvojums ir spēkā, ja reizinātāju skaits ir mazāks par n. Apskatīsim kompozicīju $f_1 f_2 \ldots f_n$ izdalot iekavas pēdējiem diviem reizinātājam. Iespējami šādi varianti:

$$\begin{aligned} g_1 &\leftharpoondown f_1(f_2 \ldots f_n), \\ g_2 &\leftharpoondown (f_1 f_2)(f_3 \ldots f_n), \\ &\cdots \\ g_{n-1} &\leftharpoondown (f_1 \ldots f_{n-1}) f_n. \end{aligned}$$

Mēs pieņemam, ka iekavu iekšpusē, ja reizinātāju skaits ir lielāks par 2, ir fiksēts konkrēts iekavu izvietojums. Tā kā saskaņā ar indukcijas pieņēmumu kompozīcija

$$f_2 f_3 \dots f_n$$

nav atkarīga no iekavu izvietojuma, tad $g_1 = f$.

Pieņemsim, ka jau pierādītas vienādības

$$f = g_1 = \dots = g_{i-1},$$

tad

$$\begin{aligned} g_{i-1} &= (f_1 \dots f_{i-1})(f_i f_{i+1} \dots f_n) \\ &= (f_1 \dots f_{i-1})(f_i(f_{i+1} \dots f_n)) \\ &\overset{A1.2.3}{=} ((f_1 \dots f_{i-1})f_i)(f_{i+1} \dots f_n) \\ &= (f_1 \dots f_i)(f_{i+1} \dots f_n) = g_i. \end{aligned}$$

Esam parādījuši, ka $g_{i-1} = g_i$. Balstoties uz indukcijas pieņēmumu tagad varam secināt $g_i = g_1 = f$. ■

1.3. Sirjekcijas un injekcijas

Attēlojumu $f : X \multimap\!\!\!\to Y$ sauc par *sirjekciju* un lieto apzīmējumu $f : X \twoheadrightarrow Y$, ja $\mathrm{Ran}(f) = Y$. Attēlojumu f sauc par *injekciju* un lieto apzīmējumu $f : X \hookrightarrow Y$, ja dažādiem elementiem x_1, x_2 atbilst dažādi y_1, y_2, t.i.,

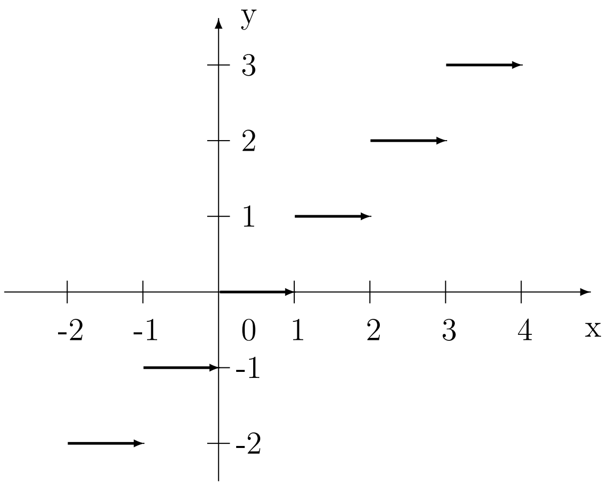
$$\forall (x_1, x_2) \in X^2\ [x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)].$$

Ja algebriska operācija $h : X \to Y$ ir gan sirjekcija, gan injekcija, tad to sauc par *bijekciju.*

1.3.1. Piemēri. Attēlojums $\mathbb{I}_A : A \to A : x \mapsto x$ ir bijekcija. Turpmāk, lai atslogotu apzīmējumus, ja no konteksta būs noprotama kopa A vai arī tās daba nebūs būtiska, mēs attēlojumam $\mathbb{I}_A$ lietosim arī pierakstu $\mathbb{I}$.

Funkcija

$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = x^3 + 1$$



1.1. zīm.: Funkcijas $y = \lfloor x \rfloor$ grafiks.

ir visur definēta, tā ir gan sirjekcija, gan injekcija, tāpēc bijekcija, taču

$$f : \mathbb{R} \to \mathbb{R}, \qquad f(x) = \lfloor x \rfloor$$

kaut arī ir visur definēta funkcija nav nedz sirjekcija, nedz injekcija (skatīt 1.1. zīm.). Vēlāk, runājot par inversajām funkcijām, mēs konstatēsim, ka injekcijas ir tās "labās" funkcijas, kurām var meklēt inversās funkcijas.

1.3.2. Apgalvojums. *Visur definēts attēlojums $f : B \to C$ ir injekcija tad un tikai tad, ja jebkuriem attēlojumiem*

$$g : A \multimap B, \qquad h : A \multimap B$$

no vienādības

$$gf = hf \qquad \text{seko} \qquad g = h.$$

$\square$ $\Rightarrow$ Pieņemsim, ka $x \in A$, tad

$$(xg)f = x(gf) = x(hf) = (xh)f.$$

No šejienes

$$x \in \mathrm{Dom}(g) \Leftrightarrow x \in \mathrm{Dom}(h),$$

jo $f : B \to C$ ir visur definēts attēlojums. Tā kā f ir injekcija, tad $xg = xh$, tātad $g = h$.

$\Leftarrow$ Pieņemsim, ka jebkuriem attēlojumiem

$$g : A \multimap B, \qquad h : A \multimap B$$

izpildās nosacījums:

$$gf = hf \Rightarrow g = h,$$

taču f nav injekcija. Ja reiz tā, tad

$$\exists a \in B \exists b \in B (a \neq b \wedge af = bf).$$

Tagad definēsim attēlojumus g un h:

$$\begin{aligned} g : B \to B \quad &: \quad x \mapsto a, \\ h : B \to B \quad &: \quad x \mapsto b. \end{aligned}$$

Šai situācijā

$$x(gf) = (xg)f = af = bf = (xh)f = x(hf).$$

Tātad $gf = hf$, un tāpēc $g = h$. Pretruna, jo

$$xg = a \neq b = xh. \blacksquare$$

1.3.3. Apgalvojums. *Attēlojums $f : A \multimap B$ ir sirjekcija tad un tikai tad, ja jebkuriem attēlojumiem*

$$g : B \multimap C, \qquad h : B \multimap C$$

no vienādības

$$fg = fh \qquad \text{seko} \qquad g = h.$$

$\square$ $\Rightarrow$ Pieņemsim, ka $fg = fh$. Ja reiz dots, ka f ir sirjekcija, tad

$$\forall b \in B \; \exists a \in A \;\; af = b,$$

un tāpēc

$$bg = (af)g = a(fg) = a(fh) = (af)h = bh.$$

No šejienes

$$b \in \mathrm{Dom}(g) \Leftrightarrow b \in \mathrm{Dom}(h).$$

Tā rezultātā $g = h$.

$\Leftarrow$ Pieņemsim, ka jebkuriem attēlojumiem

$$g : B \multimap\!\!\!\to C, \qquad h : B \multimap\!\!\!\to C$$

izpildās nosacījums:

$$fg = fh \Rightarrow g = h,$$

taču f nav sirjekcija. Saprotams, ka $\mathrm{Dom}(f) \neq \emptyset$, citādi neizpildās nosacījums: $fg = fh \Rightarrow g = h$. Ja reiz tā, tad

$$\exists b \in B\ \forall x \in A\ \ xf \neq b.$$

Nofiksējam $a \in \mathrm{Dom}(f)$, tad $b \neq af \mathrel{=\!\!\!\!\rightharpoondown} b_0$. Definējam attēlojumu

$$xg \mathrel{\leftharpoondown\!\!\!\!=} \begin{cases} x, & \text{ja} \quad x \neq b; \\ b_0, & \text{ja} \quad x = b. \end{cases}$$

Tā kā $b \neq b_0$, tad $g \neq \mathbb{I}_B$.

Mēs jau konstatējām, ka $\forall x \in A\ \ xf \neq b$, tāpēc

$$(xf)g = (xf)\mathbb{I}_B.$$

No šejienes

$$x(fg) = (xf)g = (xf)\mathbb{I}_B = x(f\mathbb{I}_B),$$

t.i., $fg = f\mathbb{I}_B$. Tas ļauj secināt, ka $g = \mathbb{I}_B$. Pretruna! $\blacksquare$

1.3.4. Apgalvojums. *Injektīvu attēlojumu kompozīcija ir injektīvs attēlojums.*

$\square$ Pieņemsim, ka $f : A \multimap\!\!\!\to B$, $g : C \multimap\!\!\!\to D$ ir injektīvi attēlojumi. Ja $\mathrm{Dom}(fg) = \emptyset$, tad nekas nav jāpierāda, tādēļ pieņemsim, ka $x, y \in \mathrm{Dom}(fg) \neq \emptyset$ un $x \neq y$. Ja reiz $x, y \in \mathrm{Dom}(fg)$, tad $x, y \in \mathrm{Dom}(f)$.

Tā kā f ir injekcija, tad $xf \neq yf$. Savukārt arī g ir injekcija, tāpēc $x(fg) = (xf)g \neq (yf)g = y(fg)$. $\blacksquare$

1.3.5. Apgalvojums. *Ja $f : A \to B$ un $g : B \to C$ ir visur definēti attēlojumi, tad $fg : A \to C$ ir visur definēts attēlojums.*

$\square$ Pieņemsim, ka $x \in A$. Tā kā f ir visur definēts attēlojums, tad $x \in \mathrm{Dom}(f)$ un $xf \in \mathrm{Ran}(f) \subseteq B$. Attēlojums g arī ir visur definēts, tāpēc $xf \in \mathrm{Dom}(g)$ un $(xf)g \in \mathrm{Ran}(g) \subseteq C$.

Tagad ņemam vērā, ka $(xf)g = x(fg)$. Tā rezultātā $x \in \mathrm{Dom}(fg)$. $\blacksquare$

1.3.6. Apgalvojums. *Ja $f : A \mathrel{-\!\!\circ\!\!\!\rightarrow} B$ un $g : B \mathrel{-\!\!\circ\!\!\!\rightarrow} C$ ir sirjekcijas, tad $fg : A \mathrel{-\!\!\circ\!\!\!\rightarrow} C$ arī ir sirjekcija.*

$\square$ Pieņemsim, ka $z \in C$, tad eksistē tāds $y \in B$, ka $yg = z$, jo

$$g : B \mathrel{-\!\!\circ\!\!\!\rightarrow} C$$

ir sirjekcija. Tā kā $f : A \mathrel{-\!\!\circ\!\!\!\rightarrow} B$ ir sirjekcija, tad eksistē tāds $x \in A$, ka $xf = y$. Tā rezultātā $x(fg) = (xf)g = yg = z$. Tātad $fg : A \mathrel{-\!\!\circ\!\!\!\rightarrow} C$ arī ir sirjekcija. $\blacksquare$

1.3.7. Apgalvojums. *Ja $f : A \to B$ un $g : B \to C$ ir bijekcijas, tad $fg : A \to C$ ir bijekcija.*

$\square$ Pieņemsim, ka $f : A \to B$ un $g : B \to C$ ir bijekcijas. Saskaņā ar Apgalvojumu 1.3.4 $fg : A \to C$ ir injekcija. Savukārt Apgalvojums 1.3.6 ļauj secināt, ka $fg : A \to C$ ir sirjekcija. Tātad $fg : A \to C$ ir bijekcija. $\blacksquare$

1.4. Inversais attēlojums

Viens no veidiem, kā palielināt pazīstamo funkciju skaitu, ir apskatīt tā saucamās inversās jeb apvērstās funkcijas. Ideja ir šāda. Funkcija f piekārto elementam x_0 no definīcijas apgabala $\mathrm{Dom}(f)$ vienu vērtību y_0 no funkcijas f vērtību apgabala $\mathrm{Ran}(f)$. Ja mums ir palaimējies, tad eksistē inversā funkcija f^{-1}, t.i., katram y no $\mathrm{Ran}(f)$ pretējā ceļā var atrast to x no $\mathrm{Dom}(f)$, ka $f(x) = y$; f^{-1} definīcijas apgabals ir $\mathrm{Ran}(f)$, bet vērtību apgabals ir $\mathrm{Dom}(f)$.

1.4.1. Piemēri.

$$\text{Ja} \qquad y = 3x, \qquad \text{tad} \qquad x = f^{-1}(y) = \frac{1}{3}\,y;$$

$$\text{ja} \qquad y = x^3 - 1, \qquad \text{tad} \qquad x = \sqrt[3]{y+1}.$$

Pieņemsim, ka F ir funkcijas $f : X \mathrel{-\!\!\circ\!\!\!\rightarrow} Y$ grafiks, tad

$$F^{-1} \leftharpoondown \{\,(y,x) \mid (x,y) \in F\,\}.$$

1.4.2. Definīcija. *Trijnieku $f^{-1} = (Y, X, F^{-1})$ sauc par funkcijas $f : X \mathrel{-\!\!\circ\!\!\!\rightarrow} Y$ inverso jeb apvērsto funkciju, ja f^{-1} ir funkcija.*

1.4.3. Apgalvojums. *Ja funkcijai f eksistē inversā funkcija f^{-1}, tad funkcijai f^{-1} arī eksistē inversā funkcija un $(f^{-1})^{-1} = f$.*

$\square$ Ja reiz funkcijai $f = (X, Y, F)$ eksistē inversā funkcija, tad trijnieks $f^{-1} = (Y, X, F^{-1})$ ir funkcija, un tādēļ ir jēga runāt par inversās funkcijas f^{-1} inverso funkciju

$$(f^{-1})^{-1} = (X, Y, (F^{-1})^{-1}).$$

Tā kā $(x, y) \in F \Leftrightarrow (y, x) \in F^{-1}$, tad

$$(F^{-1})^{-1} = \{ (x, y) \mid (y, x) \in F^{-1} \} = \{ (x, y) \mid (x, y) \in F \} = F .$$

Līdz ar to $(f^{-1})^{-1} = (X, Y, (F^{-1})^{-1}) = (X, Y, F) = f$. $\blacksquare$

1.4.4. Apgalvojums. *Ja funkcijai f eksistē inversā funkcija f^{-1}, tad*
(i) $\forall x \in \mathrm{Dom}(f)\ [\ (f^{-1} \circ f)(x) = x\ ]$ *un*
(ii) $\forall y \in \mathrm{Ran}(f)\ [\ (f \circ f^{-1})(y) = y\ ]$.

$\square$ Pieņemsim, ka $f = (X, Y, F)$, tad $f^{-1} = (Y, X, F^{-1})$, kur $F^{-1} = \{ (y, x) \mid (x, y) \in F \}$.

(i) Pieņemsim, ka $x \in \mathrm{Dom}(f)$, tad $(x, f(x)) \in F \wedge (f(x), x) \in F^{-1}$. No šejienes $(f^{-1} \circ f)(x) = f^{-1}(f(x)) = x$.

(ii) Pieņemsim, ka $y \in \mathrm{Ran}(f)$, tad $\exists x \in X\ [\ (x, y) \in F\ ]$, tāpēc $(y, x) \in F^{-1}$. No šejienes $(f \circ f^{-1})(y) = f(f^{-1}(y)) = f(x) = y$. $\blacksquare$

Taču ne katrai funkcijai eksistē inversā funkcija. Piemēram, $y = x^2$ vai $y = \sin x$. Būtisks kritērijs, lai funkcijai eksistētu inversā, ir šāds.

1.4.5. Teorēma. *Funkcijai f eksistē inversā funkcija f^{-1} tad un tikai tad, ja f ir injekcija.*

$\square$ $\Rightarrow$ Pieņemsim, ka funkcijai $f = (X, Y, F)$ eksistē inversā funkcija $f^{-1} = (Y, X, F^{-1})$, tad $F^{-1} = \{ (y, x) \mid (x, y) \in F \}$. Tā kā f^{-1} ir funkcija, tad [2.7. definīcija]

$$\forall (y_1, x_1) \in F^{-1}\ \forall (y_2, x_2) \in F^{-1}\ [\ y_1 = y_2 \Rightarrow x_1 = x_2\ ]. \tag{1.1}$$

Pieņemsim, ka funkcija f nav injekcija, tad

$$\exists u_1\ \exists u_2\ \exists v\ [\ u_1 \neq u_2 \wedge (u_1, v) \in F \wedge (u_2, v) \in F\ ].$$

Tas nozīmē, ka $(v, u_1) \in F^{-1}$ un $(v, u_2) \in F^{-1}$, kas ir pretrunā ar (1.1). Tātad pieņēmums, ka f nav injekcija ir bijis kļūdains.

$\Leftarrow$ Pieņemsim, ka $f = (X, Y, F)$ ir injekcija, tad saskaņā ar 1.4.2. definīciju atliek pierādīt, ka $f^{-1} = (Y, X, F^{-1})$ ir funkcija. Tas nozīmē, ka mums jāprot pierādīt nosacījums (2.1) jeb ekvivalentā formā

$$\forall (x_1, y_1) \in F \ \forall (x_2, y_2) \in F \ [\, x_1 \neq x_2 \ \Rightarrow \ y_1 \neq y_2 \,].$$

Bet tas taču nav nekas cits, kā apgalvojums, ka f ir injekcija. Tā kā f saskaņā ar doto ir injekcija, tad tas arī ir viss pierādījums. ■

1.4.6. Apgalvojums. *Ja $f : A \multimap B$ un $g : B \multimap A$ ir attēlojumi, kuriem spēkā vienādības*

$$fg = \mathbb{I}_A \qquad \text{un} \qquad gf = \mathbb{I}_B,$$

tad f un g ir bijekcijas un $g = f^{-1}$.

□ (i) Tā kā $fg = \mathbb{I}_A$, tad $\mathrm{Dom}(f) = A$ t.i., f ir visur definēts attēlojums. Līdzīgi, g ir visur definēts attēlojums.

(ii) Tā kā $gf = \mathbb{I}_B$ un attēlojuma f finiša kopa ir B, tad f ir sirjekcija. Līdzīgi, g ir sirjekcija.

(iii) Pieņemsim, ka $b \neq y$ ir kopas B elementi, tad

$$\exists a \in A \ af = b \ \wedge \ \exists x \in A \ xf = y,$$

jo f ir sirjekcija. Tā kā $b \neq y$, tad $a \neq x$, jo f ir attēlojums.

Ņemam vērā, ka $gf = \mathbb{I}_B$, tāpēc

$$bg = afg = a \neq x = xfg = yg.$$

Tātad g ir injekcija. Līdzīgi, f ir injekcija.

(iv) Iepriekš izklāstītais punktos (i)–(iii) pamato, ka f un g ir bijekcijas.

(v) Pieņemsim, ka F ir attēlojuma f grafiks, tad

$$(x, y) \in F \Leftrightarrow xf = y.$$

No šejienes $x = x\mathbb{I}_A = xfg = yg$. Tātad $(y, x) \in G$ — attēlojuma g grafikam. Tas nozīmē, ka $F^{-1} \subseteq G$.

Pieņemsim, ka $(b, a) \in G$, tad $bg = a$. No šejienes $b = b\mathbb{I}_B = bgf = af$, t.i., $(a, b) \in F$, un tāpēc $(b, a) \in F^{-1}$. Līdz ar to $G \subseteq F^{-1}$.

Visu savelkot kopā: $F^{-1} = G$. Tā rezultātā

$$f^{-1} = \langle B, A, F^{-1}\rangle = \langle B, A, G\rangle = g.$$

Tātad $f^{-1} = g$. ■

1.4.7. Apgalvojums. *Ja $f : A \to B$ ir bijekcija, tad*

$$ff^{-1} = \mathbb{I}_A \qquad \text{un} \qquad f^{-1}f = \mathbb{I}_B.$$

□ Tā kā f ir bijekcija, tad (Teorēma 1.4.5) tai eksistē inversais attēlojums f^{-1}. Tagad atliek tikai atsaukties uz Apgalvojumu 1.4.4. ■

1.5. Substitūcijas

1.5.1. Definīcija. *Bijektīvu attēlojumu $f : A \to A$ sauc par kopas A substitūciju.*

Visu kopas A substitūciju veidoto kopu apzīmēsim ar $\mathfrak{S}(A)$. Ja $A = \overline{1,n}$, tad $\mathfrak{S}(\overline{1,n})$ vietā parasti lieto pierakstu $\mathfrak{S}_n$. Uzskatāmi kopas $\overline{1,n}$ substitūcijas σ reprezentē ar $2 \times n$ matricām

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix},$$

pilnībā uzrādot visus elementu $1, 2, \dots, n$ attēlus

$$\sigma : \begin{array}{cccc} 1 & 2 & \dots & n \\ \downarrow & \downarrow & \dots & \downarrow \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{array}.$$

1.5.2. Piemērs.

Ja

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \qquad \text{tad}$$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = \begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 3 & 4 & 2 \end{array} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

Turpretī

$$\tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

Tātad $\sigma\tau \neq \tau\sigma$.

1.6. Kopas sadalījums

Terminu *kopu saime* $\{\mathcal{A}_i \mid i \in \mathcal{I}\}$ mēs lietosim kā ekvivalentu apgalvojumam: kopas $\{\mathcal{A}_i \mid i \in \mathcal{I}\}$ elementi ir kopas $\mathcal{A}_i$. Kopu saimi $\{\mathcal{A}_i \mid i \in \mathcal{I}\}$ sauc par *galīgu*, ja $\mathcal{I}$ ir galīga kopa vai arī tā ir tukša kopa. Saimi $\{\mathcal{A}_i \mid i \in \mathcal{I}\}$ sauc par *sanumurējamu*, ja $\mathcal{I}$ ir sanumurējama, galīga vai tukša kopa. Turpmāk, lai atslogotu apzīmējumus, ja no konteksta būs noprotama indeksu kopa $\mathcal{I}$ vai arī tās daba nebūs būtiska, mēs lietosim pierakstu

$$\{\mathcal{A}_i\} \leftharpoondown \{\mathcal{A}_i \mid i \in \mathcal{I}\}.$$

1.6.1. Definīcija. *Kopu saimi $\{\mathcal{A}_i\}$ sauc par kopas $\mathcal{A}$ sadalījumu, ja*

- $\forall i\ (\mathcal{A}_i \neq \emptyset\ \wedge\ \mathcal{A}_i \subseteq \mathcal{A})$*;*
- $\forall a \in \mathcal{A}\ \exists! i\ \ a \in \mathcal{A}_i$*.*

Kopas $\mathcal{A}_i$ sauc par sadalījuma $\{\mathcal{A}_i\}$ *blakusklasēm.* Blakusklasi, kas satur elementu a apzīmē ar $[a]_{\{\mathcal{A}_i\}}$. Elementu $a \in \mathcal{A}_j$ šai gadījumā sauc par blakusklases $\mathcal{A}_j$ *pārstāvi.* Ja no konteksta skaidrs, kurš sadalījums ir padomā, tad lieto īsāku apzīmējumu $[a]$. Kopu

$$\mathcal{A}/\{\mathcal{A}_i\} \leftharpoondown \{\mathcal{A}_i\}$$

šai situācijā sauc par kopas $\mathcal{A}$ *faktorkopu* pēc sadalījuma $\{\mathcal{A}_i\}$. Kā redzams $\{\mathcal{A}_i\}$ un $\mathcal{A}/\{\mathcal{A}_i\}$ ir viena un tā pati kopa, tikai vienā gadījumā runā par kopu saimi, bet otrā — par kopu, kuras elementi ir blakusklases.

1.6.2. Definīcija. *Attēlojumu $\pi : \mathcal{A} \to \mathcal{A}/\{\mathcal{A}_i\}$, kas katram kopas $\mathcal{A}$ elementam a piekārto blakusklasi $[a]$ sauc par dabīgo attēlojumu.*

1.6.3. Sekas. *Kopas $\mathcal{A}$ dabīgais attēlojums ir sirjekcija.*

$\square$ Katra blakusklase satur kādu kopas $\mathcal{A}$ elementu. $\blacksquare$

1.6.4. Piemēri. (i) Kopu saime $\{Z_0, Z_1\}$, kur

$Z_0 \rightleftharpoons \{$pārskaitļi$\}$, $Z_1 \rightleftharpoons \{$nepārskaitļi$\}$, ir veselo skaitļu kopas $\mathbb{Z}$ sadalījums. Savukārt

$$\pi(x) \rightleftharpoons \begin{cases} Z_0, & \text{ja} \quad x \text{ ir pārskaitlis;} \\ Z_1, & \text{ja} \quad x \text{ ir nepārskaitlis} \end{cases}$$

ir šī sadalījuma dabīgais attēlojums.

(ii) Kopu saime $\{N_\alpha \,|\, \alpha \geq 0\}$, kur

$$N_0 \rightleftharpoons \{0\}, \qquad \forall \alpha > 0 \;\; N_\alpha \rightleftharpoons \{\alpha, -\alpha\},$$

ir reālo skaitļu kopas $\mathbb{R}$ sadalījums. Savukārt

$$\pi(x) \rightleftharpoons \begin{cases} \{0\}, & \text{ja} \quad x = 0; \\ \{x, -x\}, & \text{ja} \quad x \neq 0 \end{cases}$$

ir šī sadalījuma dabīgais attēlojums.

(iii) Pieņemsim, ka $\varphi : A \twoheadrightarrow B$ ir sirjekcija, tad kopu saime $\{A_b \,|\, b \in B\}$, kur $A_b \rightleftharpoons \{a \in A \,|\, \varphi(a) = b\}$, ir kopas A sadalījums.

$\square$ (i) Ja reiz $\varphi : A \twoheadrightarrow B$ ir sirjekcija, tad $\forall b \in B \; A_b \neq \emptyset$.

(ii) Kopas A_b elementi ir arī kopas A elementi, tāpēc $A_b \subseteq A$.

(iii) Tā ka $\forall x \in A \; \exists! y \in B \; \varphi(x) = y$, tad $\forall x \in A \; \exists! b \; x \in A_b$.

Še mēs pārskaitījām visas sadalījuma īpašības un konstatējām, ka kopu saimei $\{A_b \,|\, b \in B\}$ tās visas piemīt. $\blacksquare$

1.6.5. Definīcija. *Kopā K definētu divvietīgu attiecību $E \subseteq K^2$ sauc par:*
(i) *refleksīvu, ja* $\forall x \in K \; (x, x) \in E$;
(ii) *simetrisku, ja* $\forall x \in K \; \forall y \in K \; [\,(x, y) \in E \Rightarrow (y, x) \in E\,]$;
(iii) *transitīvu, ja* $\forall x \in K \; \forall y \in K \; \forall z \in K \; [\,(x, y) \in E \wedge (y, z) \in E \Rightarrow (x, z) \in E\,]$.

Kopā K definētu attiecību E sauc par *ekvivalences tipa predikātu*, ja tā ir gan refleksīva, gan simetriska, gan transitīva. Parasti, ja E ir ekvivalences tipa predikāts, tad tā vietā, lai rakstītu $(x, y) \in E$ lieto pierakstu $x \equiv_E y$. Ja no konteksta ir noprotams konkrēts ekvivalences tipa predikāts vai arī tā specifiskās īpašības nav būtiskas, tad pieraksta $x \equiv_E y$ vietā mēdz lietot pierakstu $x \equiv y$.

1.6.6. Apgalvojums. *Katrs kopas $\mathcal{A}$ sadalījums $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$ kopā $\mathcal{A}$ definē ekvivalences tipa predikātu*

$$E \leftharpoondown\!\!\!- \{(x, y) \,|\, \exists i \in \mathcal{I}\,(x \in \mathcal{A}_i \,\wedge\, y \in \mathcal{A}_i)\}.$$

$\Box$ (i) $\forall x \in \mathcal{A}\;(x, x) \in E$, jo $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$ ir kopas $\mathcal{A}$ sadalījums; tāpēc

$$\forall x \in \mathcal{A}\;\exists i \in \mathcal{I}\,(x \in \mathcal{A}_i \,\wedge\, x \in \mathcal{A}_i).$$

(ii) $\forall x \in \mathcal{A}\;\forall y \in \mathcal{A}\;[\,(x, y) \in E \Rightarrow (y, x) \in E\,]$, jo vienmēr ir patiesa implikācija

$$\exists i \in \mathcal{I}\,(x \in \mathcal{A}_i \,\wedge\, y \in \mathcal{A}_i) \Rightarrow \exists i \in \mathcal{I}\,(y \in \mathcal{A}_i \,\wedge\, x \in \mathcal{A}_i).$$

(iii) Vispirms ņemam vērā:

$$\text{ja} \quad y \in \mathcal{A}_i \quad \text{un} \quad y \in \mathcal{A}_j, \quad \text{tad} \quad i = j,$$

jo $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$ ir kopas $\mathcal{A}$ sadalījums. Tātad

$$\begin{aligned} \exists i \in \mathcal{I}\,(x \in \mathcal{A}_i \,\wedge\, y \in \mathcal{A}_i) \quad \wedge \quad & \exists j \in \mathcal{I}\,(y \in \mathcal{A}_j \,\wedge\, z \in \mathcal{A}_j) \\ \Rightarrow \quad & \exists k \in \mathcal{I}\,(x \in \mathcal{A}_k \,\wedge\, z \in \mathcal{A}_k). \end{aligned}$$

Līdz ar to $\forall x \in \mathcal{A}\;\forall y \in \mathcal{A}\;\forall z \in \mathcal{A}\;[\,(x, y) \in E \wedge (y, z) \in E \Rightarrow (x, z) \in E\,]$.

Še mēs secīgi pārskaitījām visas ekvivalences tipa predikāta īpašības un konstatējām, ka attiecībai E tās visas piemīt. $\blacksquare$

Mūsu tuvākais mērķis pierādīt šī apgalvojuma apgriezto apgalvojumu, taču šim nolūkam mums nepieciešama izvēles aksioma. Pieņemsim, ka dota patvaļīgi fiksēta kopa $\mathfrak{M}$ un šīs kopas visu apakškopu kopa

$$\mathfrak{P}(\mathfrak{M}) \leftharpoondown\!\!\!- \{\mathcal{A} \,|\, \mathcal{A} \subseteq \mathfrak{M}\}.$$

Izvēles aksioma. Katrai netukšai kopai $\mathfrak{M}$ eksistē tāds kopas $\mathfrak{P}(\mathfrak{M})$ attēlojums φ kopā $\mathfrak{M}$, ka izpildās nosacījums:

$$\emptyset \neq \mathcal{A} \subseteq \mathfrak{M} \Rightarrow \varphi(\mathcal{A}) \in \mathcal{A}.$$

1.6.7. Apgalvojums. *Katram kopā $\mathcal{A}$ definētam ekvivalences tipa predikātam $\equiv$ eksistē tāds kopas $\mathcal{A}$ sadalījums $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$, ka*

$$\forall x \in \mathcal{A}\;\forall y \in \mathcal{A}\;[x \equiv y \Leftrightarrow \exists i \in \mathcal{I}\,(x \in \mathcal{A}_i \,\wedge\, y \in \mathcal{A}_i)].$$

$\square$ Katram kopas $\mathcal{A}$ elementam x definējam kopu

$$[x] \rightleftharpoons \{y \in \mathcal{A} \,|\, x \equiv y\}.$$

(i) Parādīsim: ja $[x] \cap [y] \neq \emptyset$, tad $[x] = [y]$.

Pieņemsim, ka $a \in [x] \cap [y]$ un $b \in [x]$, tad $b \equiv a$ un $a \equiv y$, tāpēc $b \equiv y$, jo $\equiv$ ir transitīva attiecība. Tātad $[x] \subseteq [y]$.

Līdzīgi secināms, ka $[y] \subseteq [x]$. Līdz ar to $[x] = [y]$.

(ii) Saskaņā ar izvēles aksiomu eksistē attēlojums $\varphi : \mathfrak{P}(\mathcal{A}) \to \mathcal{A}$ ar īpašību

$$\emptyset \neq K \subseteq \mathcal{A} \Rightarrow \varphi(K) \in K.$$

Definējam kopu

$$\mathcal{I} \rightleftharpoons \{\varphi(K) \,|\, [\varphi(K)] = K\}.$$

Pieņemsim, ka $i \in \mathcal{I}$, tad eksistē tāda kopa $K \subseteq \mathcal{A}$, ka $i = \varphi(K)$ un $[\varphi(K)] = K$. No šejienes $[i] = [\varphi(K)] = K$. Tātad $i = \varphi(K) = \varphi([i])$.

(iii) Izrādās, ka $\{\, [i] \,|\, i \in \mathcal{I} \,\}$ ir meklētais kopas $\mathcal{A}$ sadalījums.

- Vispirms parādīsim, ka $\forall i \in \mathcal{I}\ ([i] \neq \emptyset\ \wedge\ [i] \subseteq \mathcal{A})$.

Ja reiz $i \in \mathcal{I}$, tad $\exists K \subseteq \mathcal{A}\ \ i = \varphi(K)$. Tā kā $\varphi : \mathfrak{P}(\mathcal{A}) \to \mathcal{A}$, tad $\varphi(K) \in \mathcal{A}$; tāpēc $\varphi(K) \in [\varphi(K)] \neq \emptyset$, turklāt, saskaņā ar $[\varphi(K)]$ definīciju $[\varphi(K)] \subseteq \mathcal{A}$.

- Tagad parādīsim, ka $\forall a \in \mathcal{A}\ \exists! i \in \mathcal{I}\ \ a \in [i]$.

Pieņemsim, ka $a \in \mathcal{A}$, tad $a \in [a]$. Saskaņā ar φ definīciju $\varphi([a]) \in [a]$. Tas ļauj secināt (skatīt pierādījuma punktu (i)), ka $[\varphi([a])] = [a]$. Tātad, ja $i = \varphi([a])$, tad $i \in \mathcal{I}$ un $a \in [i]$.

Pieņemsim, ka $j \in \mathcal{I}$ un $a \in [j]$, tad (skatīt pierādījuma punktu (i)) $[j] = [a] = [i]$. Tā rezultātā (skatīt (ii)) $j = \varphi([j]) = \varphi([i]) = i$.

Še mēs pārskaitījām visas kopas $\mathcal{A}$ sadalījuma īpašības un konstatējām, ka kopu saimei $\{\, [i] \,|\, i \in \mathcal{I} \,\}$ tās visas piemīt.

- Pieņemsim, ka x un y ir kopas $\mathcal{A}$ elementi, un $x \equiv y$, tad $\exists i \in \mathcal{I}\ x \in [i]$. Tā kā $x \equiv y$, tad arī $y \in [i]$.

- Pieņemsim, ka eksistē tāds $i \in \mathcal{I}$, ka $x \in [i]$ un $y \in [i]$, tad saskaņā ar blakusklases $[i]$ definīciju $x \equiv y$.

Līdz ar to apgalvojums pierādīts pilnībā. ■

1.6.8. Vingrinājumi. (i) Pierādīt, ka katram kopā $\mathcal{A}$ definētam ekvivalences tipa predikātam $\equiv$ eksistē viens vienīgs kopas $\mathcal{A}$ sadalījums $\{\mathcal{A}_i\}$, kas apmierina nosacījumu:

$$\forall x \in \mathcal{A}\, \forall y \in \mathcal{A}\, [x \equiv y \Leftrightarrow \exists i\, (x \in \mathcal{A}_i \,\wedge\, y \in \mathcal{A}_i)]. \tag{1.2}$$

(ii) Pierādīt, ka katram kopas $\mathcal{A}$ sadalījumam $\{\mathcal{A}_i\}$ eksistē viens vienīgs kopā $\mathcal{A}$ definēts ekvivalences tipa predikātam $\equiv$, kas apmierina nosacījumu (1.2). Šai gadījumā saka, ka ekvivalences tipa predikāts $\equiv$ *atbilst kopas* $\mathcal{A}$ *sadalījumam* $\{\mathcal{A}_i\}$

Pieņemsim, ka $\equiv$ ir kopā $\mathcal{A}$ definēts ekvivalences tipa predikāts. Mēs teiksim, ka kopas $\mathcal{A}$ sadalījums $\{\mathcal{A}_i\}$ *atbilst ekvivalences tipa predikātam* $\equiv$, ja tas apmierina nosacījumu (1.2). Šai situācijā kopu

$$\mathcal{A}/\equiv \;\;\overline{\leftarrow}\;\; \mathcal{A}/\{\mathcal{A}_i\}$$

sauc par kopas $\mathcal{A}$ faktorkopu pēc ekvivalences tipa predikāta $\equiv$.

1.6.9. Definīcija. *Pieņemsim, ka* $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$ *ir kopas* $\mathcal{A}$ *sadalījums. Kopu* $\{a_i \,|\, i \in \mathcal{I}\}$ *sauc par sadalījuma* $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$ *pilnu pārstāvju sistēmu, ja* $\forall i \in \mathcal{I}\;\; a_i \in \mathcal{A}_i$.

Ja nerodas pārpratumi, tad lieto īsāku izteiksmes formu, proti, tā vietā, lai teiktu, ka $\{a_i \,|\, i \in \mathcal{I}\}$ ir sadalījuma $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$ pilna pārstāvju sistēma, saka: $\{a_i \,|\, i \in \mathcal{I}\}$ ir pilna pārstāvju sistēma.

1.6.10. Apgalvojums. *Katram sadalījumam eksistē pilna pārstāvu sistēma.*

□ Pieņemsim, ka $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$ ir kopas $\mathcal{A}$ sadalījums. Ja reiz mums jāpierāda, ka eksistē pilna pārstāvju sistēma $\{a_i \,|\, i \in \mathcal{I}\}$, tad tas nozīmē, ka jāpierāda, ka eksistē attēlojums

$$f : \mathcal{I} \to \mathcal{A} \quad \text{ar īpašību} \quad f(i) \in \mathcal{A}_i.$$

Mums dots kopas $\mathcal{A}$ sadalījums $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$. Šis pieraksts nozīmē, ka katram $i \in \mathcal{I}$ mūsu rīcībā ir kāda konkrēta kopas $\mathcal{A}$ apakškopa $\mathcal{A}_i$. Tātad dots attēlojums

$$\psi : \mathcal{I} \to \mathfrak{P}(\mathcal{A}) : i \mapsto \mathcal{A}_i.$$

Saskaņā ar izvēles aksiomu eksistē attēlojums $\varphi : \mathfrak{P}(\mathcal{A}) \to \mathcal{A}$ ar īpašību

$$\emptyset \neq K \subseteq \mathcal{A} \Rightarrow \varphi(K) \in K.$$

No šejienes: mūsu meklētais attēlojums $f = \varphi \circ \psi$. Tiešām, $\psi(i) = \mathcal{A}_i$; savukārt $\varphi(\mathcal{A}_i) \in \mathcal{A}_i$. ∎

1.6.11. Definīcija. *Pieņemsim, ka sadalījums $\{\mathcal{A}_i \,|\, i \in \mathcal{I}\}$ atbilst kopā $\mathcal{A}$ definētam ekvivalences tipa predikātam $\equiv$. Kopu $\{a_i \,|\, i \in \mathcal{I}\}$ sauc par pilnu pārstāvju sistēmu, kas atbilst ekvivalences tipa predikātam $\equiv$, ja*

$$\forall i \in \mathcal{I} \;\; a_i \in \mathcal{A}_i.$$

Ja nerodas pārpratumi, tad lieto īsāku izteiksmes formu, proti, tā vietā, lai teiktu, ka $\{a_i \,|\, i \in \mathcal{I}\}$ ir pilna pārstāvju sistēma, kas atbilst ekvivalences tipa predikātam $\equiv$, saka: $\{a_i \,|\, i \in \mathcal{I}\}$ ir ekvivalences pilna pārstāvju sistēma.

1.6.12. Vingrinājums. *Katram ekvivalences tipa predikātam eksistē pilna pārstāvju sistēma.*

1.6.13. Definīcija. *Attiecību*

$$\mathrm{K\overline{er}}f \leftrightharpoons \{(x, y) | f(x) = f(y)\}$$

sauc par attēlojuma $f : A \to B$ kodolu.

1.6.14. Vingrinājums. *Pierādīt, ka attēlojuma $f : A \to B$ kodols ir kopā A definēts ekvivalences tipa predikāts.*

1.6.15. Definīcija. *Attēlojumu $\pi : A \to A/\mathrm{K\overline{er}}f : a \mapsto [a]$ sauc par attēlojuma $f : A \to B$ dabīgo attēlojumu.*

Mēs teiksim, ka diagramma

$$\begin{tikzcd}
A \arrow[rr, "f"] \arrow[dr, "g"'] & & B \\
& C \arrow[ur, "h"'] &
\end{tikzcd}$$

ir *komutatīva*, ja $f = gh$; te $f : A \to B$, $g : A \to C$, $h : C \to B$ ir attēlojumi.

1.6.16. Teorēma. *Katram attēlojumam* $f : A \to B$ *eksistē viens vienīgs attēlojums* $f_* : A/\mathrm{K\overline{er}} f \to B$*, kam diagramma*

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "\pi"'] & & B \\ & A/\mathrm{K\overline{er}} f \arrow[ur, "f_*"'] & \end{tikzcd} \tag{D1}$$

ir komutatīva; turklāt šis attēlojums f_* *ir injekcija.*

□ (i) Definējam attēlojumu $f_* : A/\mathrm{K\overline{er}} f \to B : [a] \mapsto af$. Parādīsim, ka šī definīcija ir korekta, proti, ja $[x] = [a]$, tad $[x]f_* = [a]f_*$.

Pieņemsim, ka $[x] = [a]$, tad $(x, y) \in \mathrm{K\overline{er}} f$, t.i., $xf = af$. No šejienes $[x]f_* = xf = af = [a]f_*$. Tātad f_* definīcija ir atkarīga tikai no blakusklases $[a]$ izvēles, nevis no konkrētā elementa $x \in [a]$ izvēles.

(ii) Pieņemsim, ka $a \in A$, tad $a\pi f_* = (a\pi)f_* = [a]f_* = af$. Tas nozīmē, ka $\pi f_* = f$; tātad diagramma (D1) ir komutatīva.

(iii) Pieņemsim, ka $\varphi : A/\mathrm{K\overline{er}} f \to B$ ir attēlojums, kam diagramma (D1) ir komutatīva, proti, $\pi\varphi = f$, tad

$$\forall a \in A \quad [a]\varphi = a\pi\varphi = af = [a]f_*.$$

Tas demonstrē, ka eksistē tikai viens attēlojums $f_* : A/\mathrm{K\overline{er}} f \to B$, kam diagramma (D1) ir komutatīva.

(iv) Pieņemsim, ka $[x] \neq [a]$, tad $x \neq a$ un $xf \neq af$. No šejienes

$$[x]f_* = xf \neq af = [af].$$

Tātad $f_* : A/\mathrm{K\overline{er}} f \to B$ ir injekcija. ■

2. nodaļa

PUSGRUPAS

Algebriska sistēma. Grupoīds; Kelī tabula. Neitrālais elements, neitrālā elementa vienīgums grupoīdā. Asociatīva operācija, pusgrupa, piemēri; vispārīgais asociatīvais likums pusgrupā. Komutatīva operācija, komutatīva (Ābela) pusgrupa; vispārīgais komutatīvais likums Ābela pusgrupā. Duālais elements, monoīds, piemēri, duālā elementa vienīgums monoīdā. Grupa, simetriska grupa. Komutatīva (Ābela) grupa. Pusgrupu homomorfisms, endomorfisms, epimorfisms, monomorfisms, izomorfisms, automorfisms. Pusgrupu epimorfisms: neitrālā elementa attēls, duālā elementa attēls. Apakšpusgrupas, to šķēlums; homomorfisma attēls. Kongruence, faktorpusgrupa, kanoniskais homomorfisms, homomorfisma kodols, izomorfisma teorēma. Veidotājkopa, veidotājelements, cikliska pusgrupa, cikls ar asti, ciklisko pusgrupu klasifikācija.

2.1. Algebriskas sistēmas

2.1.1. Definīcija. *Trijnieku $\langle K, O, A\rangle$ sauc par n-sugu algebrisku sistēmu, ja*

(i) $K = \{K_1, K_2, \dots, K_n\}$, *kur* K_i, $i \in \overline{1,n}$, *ir dažādas netukšas kopas,*

(ii) O *ir algebrisku operāciju* $\circ_i : X_1 \times X_2 \times \dots \times X_{k(i)} \to Y$ *kopa, kur* $\forall j \in \overline{1,k(i)}\ (X_j \in K)$, *kā arī* $Y \in K$,

(iii) A *ir dažādu attiecību* $\varrho_i \subseteq X_1 \times X_2 \times \dots \times X_{m(i)}$ *kopa, kur* $\forall j \in \overline{1,m(i)}\ (X_j \in K)$,

(iv) $\forall i \in \overline{1,n}\,[\,\exists \circ \in O\, \exists j\,(\,K_i = \mathrm{pr}_j \circ) \vee \exists \varrho \in A\, \exists j\,(K_i = \mathrm{pr}_j\, \varrho)]$.

Ja kopas O un A ir galīgas, un nerodas pārpratumi, piemēram,

$$O = \{\circ_1, \circ_2, \ldots, \circ_k\}, \quad A = \{\varrho_1, \varrho_2, \ldots, \varrho_m\},$$

tad $\langle K, O, A\rangle$ vietā lieto pierakstu

$$\langle K_1, K_2, \ldots, K_n; \circ_1, \circ_2, \ldots, \circ_k; \varrho_1, \varrho_2, \ldots, \varrho_m\rangle.$$

Ja $O = \emptyset$, tad algebrisko sistēmu sauc par *modeli*, ja turpretī $A = \emptyset$, tad — par *algebru*. Šai situācijā $\langle K, O, A\rangle$ vietā attiecīgi lieto pierakstu $\langle K, A\rangle$ vai $\langle K, O\rangle$, vai arī attiecīgi

$$\langle K_1, K_2, \ldots, K_n; \varrho_1, \varrho_2, \ldots, \varrho_m\rangle \quad \text{vai} \quad \langle K_1, K_2, \ldots, K_n; \circ_1, \circ_2, \ldots, \circ_k\rangle.$$

2.1.2. Piemērs. Trīs sugu algebru $\langle Q, A, B; \circ, *\rangle$ sauc par *Mīlija mašīnu*, ja Q, A, B — galīgas netukšas kopas, $Q \times A \xrightarrow{\circ} Q$ un $Q \times A \overset{*}{\twoheadrightarrow} B$. Kopu Q sauc par mašīnas *iekšējo stāvokļu* kopu, A un B attiecīgi — par *ieejas* un *izejas* alfabētiem. Kopu A un B elementus sauc par *burtiem*. Operācijas $\circ$ un $*$ attiecīgi sauc par *pārejas* un *izejas* funkcijām.

Ja no kontesta būs noprotams, cik sugu algebra ir dotā algebra $\mathfrak{A}$, tad mēs lietosim īsāku terminu *algebra*, tai vietā, lai teiktu: n–sugu algebra. Šai nodaļā mūs interesēs tikai vienas sugas algebras.

2.2. Grupoīdi

2.2.1. Definīcija. *Algebru $\langle G, \odot\rangle$ sauc par grupoīdu, ja $\odot$ ir kopā G definēta divvietīga operācija.*

Parasti lieto īsāku izteiksmes formu. Tai vietā, lai teiktu: pieņemsim, ka $\langle G, \odot\rangle$ ir grupoīds, mēdz teikt: pieņemsim, ka G ir grupoīds. Tā rezultātā grupoīdu identificē ar kopu G un saka: kopu G sauc par grupoīdu, ja tajā definēta divvietīga operācija. Ja neradīsies pārpratumi un no konteksta būs noprotama operācija $\odot$ arī mēs pieturēsimies pie šāda izteiksmes veida.

Bieži pāra (a, b) attēlu $a \odot b$ sauc par reizinājumu, pašu operāciju sauc par reizināšanu un operācijas zīmi nelieto, t.i., $ab \leftharpoondown a \odot b$. Atzīmēsim, ka šai situācijā reizinājumam ab var arī nebūt nekāda sakara ar tik pierasto skaitļu reizināšanu.

Dažkārt termina *reizinājums* vietā lieto terminu *summa*. Parasti tad operācijas $a \odot b$ vietā lieto pierakstu $a+b$. Atkal jāatzīmē (līdzīgi kā reizinājuma gadījumā), ka summai $a+b$ var arī nebūt nekāda sakara ar tik pierasto skaitļu summu. Saprotams, ka mēdz būt situācijas, kurās lieto arī citus apzīmējumus, piemēram, $a \circ b$, $a * b$, $a \# b$ vai arī $[a, b]$.

2.2.2. Piemēri. *Apskatu sāksim ar tradicionāliem piemēriem.*

(i) Aritmētiskās operācijas $+$, $\times$ ir divvietīgas operācijas naturālo skaitļu kopā $\mathbb{N}$. Tā rezultātā mūsu rīcībā ir divi dažādi grupoīdi: $\langle \mathbb{N}, + \rangle$ un $\langle \mathbb{N}, \times \rangle$.

Atzīmēsim, ka atņemšana $-$ visiem naturālo skaitļu pāriem nav definēta. Līdz ar to atņemšana $-$ tradicionālā nozīmē nav operācija naturālo skaitļu kopā. Tātad $\langle \mathbb{N}, - \rangle$ nav grupoīds.

(ii) Aritmētiskās operācijas $+$, $-$, $\times$ ir divvietīgas operācijas veselo skaitļu kopā $\mathbb{Z}$. Tā rezultātā mūsu rīcībā ir trīs dažādi grupoīdi: $\langle \mathbb{Z}, + \rangle$, $\langle \mathbb{Z}, - \rangle$, $\langle \mathbb{Z}, \times \rangle$.

Atzīmēsim, ka dalīšana $:$ visiem veselo skaitļu pāriem nav definēta. Līdz ar to dalīšana $:$ tradicionālā nozīmē nav operācija veselo skaitļu kopā. Tātad $\langle \mathbb{Z}, : \rangle$ nav grupoīds. Šai ziņā nekas nemainās, ja kopas $\mathbb{Z}$ vietā aplūko racionālo $\mathbb{Q}$, reālo $\mathbb{R}$ vai komplekso $\mathbb{C}$ skaitļu kopu. Taču, ja mēs aplūkojam kopu

$$\mathbb{Q}^\circ \leftharpoondown \mathbb{Q} \setminus \{0\},$$

tad dalīšana šai kopā ir divvietīga operācija. Līdz ar to $\langle \mathbb{Q}^\circ, : \rangle$ ir grupoīds.

(iii) Vektoru saskaitīšana un atņemšana ir divvietīgas operācijas kopā $\mathbb{C}^n$. Secinājums: $\langle \mathbb{C}^n, + \rangle$ un $\langle \mathbb{C}^n, - \rangle$ ir grupoīdi.

(iv) Vektoru $(a_1, a_2, a_3), (b_1, b_2, b_3)$ vektoriālais reizinājums

$$(a_1, a_2, a_3) \times (b_1, b_2, b_3) \leftharpoondown \left(\begin{vmatrix} a_2 & a_3 \\ b_2 & b_3 \end{vmatrix}, - \begin{vmatrix} a_1 & a_3 \\ b_1 & b_3 \end{vmatrix}, \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} \right)$$

ir divvietīga operācija kopā $\mathbb{R}^3$. Tātad $\langle \mathbb{R}^3, \times \rangle$ ir grupoīds.

(v) Visur definētu attēlojumu $A : \overline{1, m} \times \overline{1, n} \to \mathbb{K}$ sauc par *taisnstūrveida* jeb m reiz n *matricu* (lieto arī pierakstu: $m \times n$ matrica). Attēlojuma A vērtību apgabala $\mathrm{Ran}(A)$ elementus sauc par matricas A elementiem. Tā kā kopa $\overline{1, m} \times \overline{1, n}$ ir galīga, tad matricu A parasti reprezentē ar tabulu

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ . & . & . & . \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix},$$

kur $A(i,j) = a_{ij}$. Šai situācijā izmanto arī apzīmējumu $A = ||a_{ij}||_n^m$ un saka, ka matricas A izmēri ir $m \times n$. Ja no konteksta ir skaidrs, kādi ir matricas A izmēri vai arī šai informācijai nav būtiskas nozīmes, tad lieto vienkāršāku apzīmējumu $A = ||a_{ij}||$. Elementa a_{ij} pirmo indeksu i sauc par *rindas* indeksu, bet otro indeksu j — par *ailes* jeb *kolonnas* indeksu. Matricu $(a_{i1}, a_{i2}, \ldots, a_{in})$ sauc par matricas A i-to *rindu*, savukārt matricu

$$\begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$$

sauc par matricas A j-to *aili* jeb *kolonnu*. Vietas taupīšanas nolūkos j-to aili mēdz pierakstīt arī šādi $'(a_{1j}, a_{2j}, \ldots, a_{mj})$. Matricu

$$'A = \begin{pmatrix} a_{11} & a_{21} & \ldots & a_{m1} \\ a_{12} & a_{22} & \ldots & a_{m2} \\ . & . & . & . \\ a_{1n} & a_{2n} & \ldots & a_{mn} \end{pmatrix}$$

sauc par matricas A *transponēto* matricu. Tā ir $n \times m$ matrica.

Pieņemsim, ka $\mathrm{Mat}_n^m(\mathbb{R})$ ir $m \times n$ izmēru matricas, kuru elementi ir reāli skaitļi, tad $+$ un $-$ ir divvietīgas operācijas matricu kopā $\mathrm{Mat}_n^m(\mathbb{R})$. Tā rezultātā $\langle \mathrm{Mat}_n^m(\mathbb{R}), + \rangle$ un $\langle \mathrm{Mat}_n^m(\mathbb{R}), - \rangle$ ir grupoīdi.

(vi) Pieņemsim, ka $\mathrm{Mat}_n(\mathbb{R})$ ir n–tās kārtas kvadrātiskas matricas pār reālo skaitļu lauku, t.i., $\mathrm{Mat}_n(\mathbb{R}) \leftharpoondown \mathrm{Mat}_n^n(\mathbb{R})$, tad matricu reizināšana šai kopā ir divvietīga operācija. Tas nozīmē, ka $\langle \mathrm{Mat}_n(\mathbb{R}), \cdot \rangle$ ir grupoīds.

Kopā $\mathrm{Mat}_n(\mathbb{R})$ definēsim jaunu operāciju $[A, B] \leftharpoondown AB - BA$. Tā rezultātā $\langle \mathrm{Mat}_n(\mathbb{R}),\ [,] \rangle$ ir grupoīds.

(vii) Pieņemsim, ka $A \neq \emptyset$ un $\mathrm{Fun}(A) \leftharpoondown \{f \mid f : A \to A\}$, t.i., $\mathrm{Fun}(A)$ ir kopā A visur definēto attēlojumu $f : A \to A$ kopa. Attēlojumu kompozīcija $\circ$ ir divvietīga operācija šai kopā $\mathrm{Fun}(A)$. Tātad $\langle \mathrm{Fun(A)}, \circ \rangle$ ir grupoīds.

Ja G ir galīga kopa, tad grupoīdu $\langle G, \odot \rangle$ sauc par *galīgu*; ja G ir bezgalīga kopa, tad grupoīdu $\langle G, \odot \rangle$ sauc par *bezgalīgu*.

Ja grupoīds $\langle G, \odot \rangle$ ir galīgs, teiksim, $G = \{g_1, g_2, \ldots, g_n\}$, tad grupoīdu var uzdot ar sarakstu, proti, jāuzdod attēlojuma $\odot$ grafiks. Tātad, ja

$$\odot = \langle G^2, G, G_\odot \rangle,$$

tad

$$G_\odot = \{(g_i, g_j, g_i \odot g_j) \mid i \in \overline{1,n} \wedge j \in \overline{1,n}\}.$$

Kelī tabula ir piedāvājums, kā pārskatāmi vizualizēt kopas $G_\odot$ pierakstu. Izvēlamies kvadrātisku tabulu ar $(n+1) \times (n+1)$ rūtiņām un definējam

$$ent_{ij} \leftharpoondown \begin{cases} \odot, & \text{ja} \quad i = j = 0, \\ g_j, & \text{ja} \quad i = 0, j \in \overline{1,n}, \\ g_i, & \text{ja} \quad i \in \overline{1,n}, j = 0, \\ g_i \odot g_j, & \text{pārējos gadījumos;} \end{cases}$$

te ent_{ij} ir ieraksts tabulas i–tās rindas un j–tās ailes krustpunktā. Vizuāli tas izskatās šādi:

$\odot$	g_1	g_2	$\ldots$	g_n
g_1	$g_1 \odot g_1$	$g_1 \odot g_2$	$\ldots$	$g_1 \odot g_n$
g_2	$g_2 \odot g_1$	$g_2 \odot g_2$	$\ldots$	$g_2 \odot g_n$
.	. . .	. . .	. .	. . .
g_n	$g_n \odot g_1$	$g_n \odot g_2$	$\ldots$	$g_n \odot g_n$

Piemēram,

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

sauc par *Kleina 4–grupu.*

2.3. Neitrālie elementi

2.3.1. Definīcija. *Grupoīda G elementu e sauc par* neitrālo *(vienības, nulles) elementu, ja*

$$\forall a \in G\, [\, e \odot a = a = a \odot e\,]\, .$$

Ja operācija $\odot$ ir summa $+$, tad neitrālo elementu parasti sauc par *nulli* un tam lieto apzīmējumu 0.

Grupīda $\langle \mathbb{N}, + \rangle$ (skatīt Piemērus 2.2.2) nulles elements ir skaitlis 0; grupoīda $\langle \mathbb{N}, \times \rangle$ vienības elements ir skaitlis 1. Līdzīgi grupoīda $\langle \mathbb{Z}, + \rangle$ nulles elements ir skaitlis 0; grupoīda $\langle \mathbb{Z}, \times \rangle$ vienības elements ir skaitlis 1.

Savukārt grupoīdā $\langle \mathbb{Z}, - \rangle$ vienības elements neeksistē. Tiešām, pieņemsim, ka e ir $\langle \mathbb{Z}, - \rangle$ neitrālais elements, tad

$$e - 0 = 0 \qquad \text{un} \qquad e - 1 = 1.$$

No pirmās vienādības seko, ka $e = 0$, no otrās izriet, ka $e = 2$. Tātad $0 = e = 2$. Pretruna.

2.3.2. Vingrinājumi. (i) Atrast grupoīdu $\langle \mathbb{C}^n, + \rangle$, $\langle \mathrm{Mat}_n^m(\mathbb{R}), + \rangle$, $\langle \mathrm{Mat}_n(\mathbb{R}), \cdot \rangle$, $\langle \mathrm{Fun(A)}, \circ \rangle$ netrālos elementus.

(ii) Pierādīt, ka grupoīdos $\langle \mathbb{Q}^\circ, : \rangle$, $\langle \mathbb{C}^n, - \rangle$, $\langle \mathbb{R}^3, \times \rangle$, $\langle \mathrm{Mat}_\mathrm{n}^\mathrm{m}(\mathbb{R}), - \rangle$, $\langle \mathrm{Mat_n}(\mathbb{R}), [\,,] \rangle$ neitrālie elementi neeksistē.

2.3.3. Apgalvojums. *Grupoīdā eksistē ne vairāk kā viens neitrālais elements.*

□ Pieņemsim, ka e un e' ir divi neitrālie elementi, tad

$$e = e \odot e' = e' \,. \blacksquare$$

2.4. Asociatīva operācija

2.4.1. Definīcija. *Kopā G definētu operāciju $\odot$ sauc par asociatīvu, ja*

$$\forall a \in G \;\forall b \in G \;\forall c \in G \;[\,(a \odot b) \odot c = a \odot (b \odot c)\,]\,.$$

Grupoīdu G, kurā operācija $\odot$ ir asociatīva, sauc par *pusgrupu.*

Grupīdi $\langle \mathbb{N}, + \rangle$, $\langle \mathbb{N}, \times \rangle$ (skatīt Piemērus 2.2.2) ir pusgrupas. Līdzīgi grupoīdi $\langle \mathbb{Z}, + \rangle$ un $\langle \mathbb{Z}, \times \rangle$ ir pusgrupas.

Savukārt grupoīds $\langle \mathbb{Z}, - \rangle$ nav pusgrupa, jo

$$(6 - 2) - 3 = 1 \neq 7 = 6 - (2 - 3).$$

2.4.2. Vingrinājumi. (i) Pierādīt, ka grupoīdi $\langle \mathbb{C}^n, + \rangle$, $\langle \mathrm{Mat}_n^m(\mathbb{R}), + \rangle$, $\langle \mathrm{Mat}_n(\mathbb{R}), \cdot \rangle$, $\langle \mathrm{Fun(A)}, \circ \rangle$ ir pusgrupas.

(ii) Pierādīt, ka grupoīdi $\langle \mathbb{Q}^{\circ}, : \rangle$, $\langle \mathbb{C}^n, - \rangle$, $\langle \mathbb{R}^3, \times \rangle$, $\langle \mathrm{Mat}_{\mathrm{n}}^{\mathrm{m}}(\mathbb{R}), - \rangle$, $\langle \mathrm{Mat}_{\mathrm{n}}(\mathbb{R}), [,] \rangle$ nav pusgrupas.

2.4.3. Piemērs. Pieņemsim, ka A — galīga kopa un

$$A^+ \leftharpoondown \bigcup_{n+1}^{\infty} A^n.$$

Kopā A^+ definēsim divvietīgu operāciju $\#$, ko sauc par *konkatenāciju*,

$$(a_1, a_2, \dots, a_k) \# (b_1, b_2, \dots, b_m) \leftharpoondown (a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_m).$$

Šo pusgrupu sauc par veidotājkopas A *brīvo pusgrupu.* Vārdu kombinatorikā un teorētiskajā datorzinātnē šai situācijā kopu A mēdz saukt par *alfabētu*, kopas A elementus — par *vārdiem*, un to apzīmēšanai mēdz lietot pierakstu

$$a_1 a_2 \dots a_k \leftharpoondown (a_1 a_2 \dots a_k).$$

2.4.4. Apgalvojums. *Pusgrupas elementu $a_1, a_2, \dots, a_n$ reizinājums nav atkarīgs no iekavu izvietojuma.*

$\square$ Ja $n = 1$ vai $n = 2$, tad a_1, $a_1 a_2$ nesatur iekavas, un šai situācijā apgalvojums ir spēkā. Ja $n = 3$, tad $a_1(a_2 a_3) = (a_1 a_2) a_3$, jo pusgrupā operācija ir asociatīva.

Turpmākais pierādījums ir induktīvs. Tas kopē Apgalvojuma 1.2.4 pierādījumu, tāpēc to atstājam kā vingrinājumu lasītājam. $\blacksquare$

2.5. Komutatīva operācija

2.5.1. Definīcija. *Kopā G definētu operāciju $\odot$ sauc par* komutatīvu*, ja*

$$\forall a \in G \; \forall b \in G \; [\, a \odot b = b \odot a \,] \, .$$

Pusgrupu G, kurā operācija $\odot$ ir komutatīva sauc par *komutatīvu* jeb *Ābela pusgrupu.*

Pusgrupas $\langle \mathbb{N}, + \rangle$, $\langle \mathbb{N}, \times \rangle$ (skatīt Piemērus 2.2.2) ir komutatīvas. Līdzīgi pusgrupas $\langle \mathbb{Z}, + \rangle$ un $\langle \mathbb{Z}, \times \rangle$ ir komutatīvas.

Pusgrupa $\langle \mathrm{Mat}_n(\mathbb{R}), \cdot \rangle$ nav komutatīva, ja vien $n > 1$. Tā, piemēram,

$$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 2 & 5 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

2.5.2. Vingrinājumi. (i) Pierādīt, ka pusgrupas $\langle \mathbb{C}^n, +\rangle$, $\langle \mathrm{Mat}_n^m(\mathbb{R}), +\rangle$, ir komutatīvas.

(ii) Pierādīt, ka pusgrupas $\langle \mathrm{Fun(A)}, \circ\rangle$, $\langle A^+, \#\rangle$ nav komutatīvas, ja vien $|A| > 1$.

2.5.3. Apgalvojums. *Ja pusgrupas P elementiem $a_1, a_2, \ldots, a_n$ ir spēkā nosacījums*

$$\forall i \quad \forall j \quad a_i a_j = a_j a_i, \tag{2.1}$$

tad jebkurai substitūcijai

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix},$$

$$a_1 a_2 \ldots a_n = a_{\sigma(1)} a_{\sigma(2)} \ldots a_{\sigma(n)}.$$

$\square$ Pierādījums induktīvs. Ja $n = 2$, tad vienādība

$$a_1 a_2 = a_{\sigma(1)} a_{\sigma(2)}$$

tieši seko no (2.1).

Pieņemsim, ka apgalvojums ir spēkā $n-1$ reizinātājam.

(i) Ja $\sigma(n) = n$, tad, ņemot vērā Apgalvojumu 2.4.4 un induktīvo pieņēmumu, iegūstam

$$\begin{aligned} a_{\sigma(1)} a_{\sigma(2)} \ldots a_{\sigma(n)} &= (a_{\sigma(1)} a_{\sigma(2)} \ldots a_{\sigma(n-1)}) a_n \\ &= a_1 \ldots a_{n-1} a_n. \end{aligned}$$

(ii) Ja $n = \sigma(k)$, kur $1 < k < n$, tad

$$\begin{aligned} a_{\sigma(1)} a_{\sigma(2)} \ldots a_{\sigma(n)} &= a_{\sigma(1)} \ldots a_{\sigma(k-1)} a_{\sigma(k)} a_{\sigma(k+1)} \ldots a_{\sigma(n)} \\ &= (a_{\sigma(1)} \ldots a_{\sigma(k-1)})(a_n (a_{\sigma(k+1)} \ldots a_{\sigma(n)})) \\ &= (a_{\sigma(1)} \ldots a_{\sigma(k-1)})((a_{\sigma(k+1)} \ldots a_{\sigma(n)}) a_n) \\ &= (a_{\sigma(1)} \ldots a_{\sigma(k-1)} a_{\sigma(k+1)} \ldots a_{\sigma(n)}) a_n \\ &= a_1 \ldots a_{n-1} a_n. \end{aligned}$$

(iii) Ja $n = \sigma(1)$, tad

$$\begin{aligned} a_{\sigma(1)}a_{\sigma(2)}\ldots a_{\sigma(n)} &= (a_n a_{\sigma(2)})a_{\sigma(3)}\ldots a_{\sigma(n)} \\ &= (a_{\sigma(2)}a_n)a_{\sigma(3)}\ldots a_{\sigma(n)} \\ &= a_{\sigma(2)}(a_n a_{\sigma(3)}\ldots a_{\sigma(n)}) \\ &= a_{\sigma(2)}(a_{\sigma(3)}\ldots a_{\sigma(n)}a_n) \\ &= (a_{\sigma(2)}a_{\sigma(3)}\ldots a_{\sigma(n)})a_n \\ &= a_1\ldots a_{n-1}a_n. \qquad \blacksquare \end{aligned}$$

2.5.4. Sekas. *Komutatīvā pusgrupā jebkuriem elementiem* $a_1, a_2, \ldots, a_n$ *un jebkurai substitūcijai*

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix},$$

izpildās vienādība

$$a_1a_2\ldots a_n = a_{\sigma(1)}a_{\sigma(2)}\ldots a_{\sigma(n)}.$$

Vienošanās. Pieņemsim, ka P ir pusgrupa un $a \in P$, tad

$$\begin{aligned} a^1 &\leftharpoondown a; \\ a^{n+1} &\leftharpoondown a(a^n). \end{aligned}$$

2.5.5. Vingrinājumi. (i) Ja a ir pusgrupas P elements, tad

$$\forall m \in \mathbb{Z}_+ \; \forall n \in \mathbb{Z}_+ \; a^m a^n = a^{m+n}.$$

(ii) Ja pusgrupas P elementi a un b komutē, t.i., $ab = ba$, tad

$$\forall n \in \mathbb{Z}_+ \; (ab)^n = a^n b^n.$$

2.6. Duālie elementi

2.6.1. Definīcija. *Pusgrupu* $\langle P, \odot \rangle$, *kurā eksistē neitrālais elements* $e \in P$, *sauc par monoīdu.*

Monoīda P elementu a sauc par *apgriežamu*, ja

$$\exists b \in P \; [\, b \odot a = e = a \odot b \,] \,.$$

Šo b sauc par elementa a *duālo* (apgriezto, pretējo) elementu un parasti apzīmē ar a^{-1} (ja operācija $\odot$ ir komutatīva, tad mēdz lietot arī apzīmējumu $-a$). Monoīdu P, kurā operācija $\odot$ ir komutatīva, sauc par *komutatīvu* jeb *Ābela monoīdu.*

Pusgrupas $\langle \mathbb{N}, + \rangle$, $\langle \mathbb{N}, \times \rangle$ (skatīt Piemērus 2.2.2) ir komutatīvi monoīdi. Monoīda $\langle \mathbb{N}, + \rangle$ neitrālais elements ir 0, savukārt monoīda $\langle \mathbb{N}, \times \rangle$ neitrālais elements ir 1. Līdzīgi pusgrupas $\langle \mathbb{Z}, + \rangle$ un $\langle \mathbb{Z}, \times \rangle$ ir komutatīvi monoīdi.

2.6.2. Vingrinājumi. (i) Pusgrupas $\langle \mathbb{C}^n, + \rangle$, $\langle \mathrm{Mat}_n^m(\mathbb{R}), + \rangle$ ir komutatīvi monoīdi. Atrast šo monoīdu neitrālos elementus.

(ii) Pusgrupa $\langle \mathrm{Fun(A)}, \circ \rangle$ nav komutatīva, ja vien $|A| > 1$, taču tā ir monoīds. Atrast šī monoīda neitrālo elementu.

Pusgrupa $\langle \mathrm{Mat}_n(\mathbb{R}), \cdot \rangle$ nav komutatīva, taču tā ir monoīds. Šī monoīda neitrālais elements ir vienības matrica

$$E \leftharpoondown \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ . & . & . & . & . \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

Matricu $A^{-1} \in \mathrm{Mat}_n(\mathbb{R})$ sauc par matricas $A \in \mathrm{Mat}_n(\mathbb{R})$ *inverso matricu,* ja $A^{-1}A = E = AA^{-1}$.

Matricas

$$A[ij] = \begin{pmatrix} a_{11} & \dots & a_{1j-1} & a_{1j+1} & \dots & a_{1n} \\ . & . & . & . & . & . \\ a_{i-11} & \dots & a_{i-1j-1} & a_{i-1j+1} & \dots & a_{i-1n} \\ a_{i+11} & \dots & a_{i+1j-1} & a_{i+1j+1} & \dots & a_{i+1n} \\ . & . & . & . & . & . \\ a_{m1} & \dots & a_{mj-1} & a_{mj+1} & \dots & a_{mn} \end{pmatrix},$$

$$A[i-] = \begin{pmatrix} a_{11} & \dots & a_{1j-1} & a_{1j} & a_{1j+1} & \dots & a_{1n} \\ . & . & . & . & . & . & . \\ a_{i-11} & \dots & a_{i-1j-1} & a_{i-1j} & a_{i-1j+1} & \dots & a_{i-1n} \\ a_{i+11} & \dots & a_{i+1j-1} & a_{i+1j} & a_{i+1j+1} & \dots & a_{i+1n} \\ . & . & . & . & . & . & . \\ a_{m1} & \dots & a_{mj-1} & a_{mj} & a_{mj+1} & \dots & a_{mn} \end{pmatrix},$$

$$A[-j] = \begin{pmatrix} a_{11} & \dots & a_{1j-1} & a_{1j+1} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{i-11} & \dots & a_{i-1j-1} & a_{i-1j+1} & \dots & a_{i-1n} \\ a_{i1} & \dots & a_{ij-1} & a_{ij+1} & \dots & a_{in} \\ a_{i+11} & \dots & a_{i+1j-1} & a_{i+1j+1} & \dots & a_{i+1n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{m1} & \dots & a_{mj-1} & a_{mj+1} & \dots & a_{mn} \end{pmatrix}$$

sauc par matricas $A = ||a_{ij}||_n^m$ *apakšmatricām.*

Tīri mehāniski apakšmatrica $A[ij]$ iegūstama, ja matricā A izsvītro i-to rindu un j-to aili; apakšmatrica $A[i-]$ iegūstama, ja matricā A izsvītro i-to rindu; apakšmatrica $A[-j]$ iegūstama, ja matricā A izsvītro j-to aili.

Determinantu $|A[ij]|$ sauc par *elementam a_{ij} atbilstošo minoru* un lieto apzīmējumu M_{ij}, ja $A = ||a_{ij}|| \in \mathrm{Mat}_n(\mathbb{R})$. Skaitli $A_{ij} = (-1)^{i+j} M_{ij}$ sauc par *elementam a_{ij} atbilstošo algebrisko papildinājumu* jeb *adjunktu.*

Matricu

$$A^* = \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \dots & \dots & \dots & \dots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{pmatrix}$$

sauc par matricas A *adjunktu matricu*, bet $'A^*$ — par *piesaistīto matricu.*

Ja $|A| \neq 0$, tad $A^{-1} = \dfrac{1}{|A|}\,'A^*$. Tātad, ja $|A| \neq 0$, tad šim monoīda elementam $A \in \mathrm{Mat}_n(\mathbb{R})$ monoīdā $\mathrm{Mat}_n(\mathbb{R})$ eksistē duālais elements A^{-1}, ko sauc par matricas A *inverso matricu.*

2.6.3. Piemērs. Ja

$$A = \begin{pmatrix} 0 & 2 & -1 \\ 0 & 1 & 1 \\ -1 & -3 & 0 \end{pmatrix}, \quad \text{tad} \quad |A| = -\begin{vmatrix} 2 & -1 \\ 1 & 1 \end{vmatrix} = -3,$$

$$A_{11} = \begin{vmatrix} 1 & 1 \\ -3 & 0 \end{vmatrix} = 3, \qquad A_{12} = -\begin{vmatrix} 0 & 1 \\ -1 & 0 \end{vmatrix} = -1,$$

$$A_{13} = \begin{vmatrix} 0 & 1 \\ -1 & -3 \end{vmatrix} = 1, \qquad A_{21} = -\begin{vmatrix} 2 & -1 \\ -3 & 0 \end{vmatrix} = 3,$$

$$A_{22} = \begin{vmatrix} 0 & -1 \\ -1 & 0 \end{vmatrix} = -1, \qquad A_{23} = -\begin{vmatrix} 0 & 2 \\ -1 & -3 \end{vmatrix} = -2,$$

$$A_{31} = \begin{vmatrix} 2 & -1 \\ 1 & 1 \end{vmatrix} = 3, \quad A_{32} = -\begin{vmatrix} 0 & -1 \\ 0 & 1 \end{vmatrix} = 0, \quad A_{33} = \begin{vmatrix} 0 & 2 \\ 0 & 1 \end{vmatrix} = 0.$$

No šejienes

$$A^* = \begin{pmatrix} 3 & -1 & 1 \\ 3 & -1 & -2 \\ 3 & 0 & 0 \end{pmatrix}, \qquad 'A^* = \begin{pmatrix} 3 & 3 & 3 \\ -1 & -1 & 0 \\ 1 & -2 & 0 \end{pmatrix},$$

un tāpēc

$$A^{-1} = \begin{pmatrix} -1 & -1 & -1 \\ \frac{1}{3} & \frac{1}{3} & 0 \\ -\frac{1}{3} & \frac{2}{3} & 0 \end{pmatrix}.$$

Lasītājam ieteicam pārliecināties, ka $A^{-1}A = E$.

2.6.4. Apgalvojums. *Katram monoīda elementam eksistē ne vairāk kā viens duālais elements.*

□ Pieņemsim, ka b un c ir elementa a duālie elementi un e ir neitrālais elements, tad

$$b = be = b(ac) = (ba)c = ec = c. \qquad \blacksquare$$

2.6.5. Sekas. *Ja b ir elementa a duālais elements, tad a ir elementa b duālais elements, t.i., $(a^{-1})^{-1} = a$.*

□ $\quad a^{-1}a = e = aa^{-1}$. $\quad$ No šejienes $a = (a^{-1})^{-1}$. $\blacksquare$

2.6.6. Definīcija. *Attēlojumu $f : X_1 \to Y$ sauc par attēlojuma $g : X_2 \to Y$ sašaurinājumu kopā X_1, ja $X_1 \subseteq X_2$ un $\forall x \in X_1\, f(x) = g(x)$. Šajā situācijā mēdz lietot apzīmējumu $f = g|X_1$.*

2.6.7. Apgalvojums. *Katru pusgrupu $\langle P, \odot \rangle$, tai pievienojot vienu jaunu elementu, var pārvērst par monoīdu $\langle M, \cdot \rangle$ tā, lai $\cdot|P = \odot$.*

□ Pieņemsim, ka P — pusgrupa un $e \notin P$. Kopā $M \leftharpoondown P \cup \{e\}$ definējam jaunu operāciju $\cdot$:

$$\begin{aligned} \forall x \in P\ \forall y \in P \quad x \cdot y &\leftharpoondown x \odot y; \\ \forall y \in P \quad e \cdot y &\leftharpoondown y \rightharpoondown y \cdot e; \\ e \cdot e &\leftharpoondown e. \end{aligned}$$

Saskaņā ar operācijas $\cdot$ definīciju $\cdot|P = \odot$. $\blacksquare$

2.6.8. Piemērs. Pieņemsim, ka $\lambda \notin A^+$ un $A^* \leftharpoondown A^+ \cup \{\lambda\}$, tad kopu A^* var sekojoši pārvērst par monoīdu:

$$\lambda \# \lambda \leftharpoondown \lambda, \quad \lambda \# u \leftharpoondown u \rightharpoondown u \# \lambda .$$

Šo monoīdu sauc par *kopas A veidoto brīvo monoīdu* A^*. Kopas A^* elementu λ sauc par *tukšo vārdu.* Ja $u = u_1 = u_2 = \ldots = u_n$, tad lieto arī pierakstu $u^n \leftharpoondown u_1 u_2 \ldots u_n$. Savukārt $u^0 \leftharpoondown \lambda$.

Vienošanās. Pieņemsim, ka M — monoīds un $a \in M$, tad $a^0 \leftharpoondown e$, kur e ir monoīda M neitrālais elements.

2.6.9. Vingrinājumi. (i) Ja a ir monoīda M elements, tad

$$\forall m \in \mathbb{N}\, \forall n \in \mathbb{N}\; a^m a^n = a^{m+n}.$$

(ii) Ja monoīda M elementi a un b komutē, t.i., $ab = ba$, tad

$$\forall n \in \mathbb{N}\; (ab)^n = a^n b^n.$$

2.7. Grupas

2.7.1. Definīcija. *Monoīdu $\langle G, \odot \rangle$, kurā katrs elements ir apgriežams, sauc par grupu. Grupu G, kurā operācija $\odot$ ir komutatīva, sauc par komutatīvu jeb Ābela grupu.*

2.7.2. Apgalvojums. *Attēlojums f, kas katram grupas G elementam a piekārto tā apgriezto elementu a^{-1}, ir kopas G substitūcija.*

□ (i) Ņemot vērā Apgalvojumu 2.6.4, attēlojums f ir definēts korekti. Tā kā grupā katram elementam eksistē apgrieztais elements, tad $\mathrm{Dom}(f) = G$, t.i., f ir visur definēts attēlojums.

(ii) Ja $f(a) = f(b)$, tad $f(f(a)) = f(f(b))$. Saskaņā ar apgrieztā elementa definīciju a ir elementa a^{-1} apgrieztais elements, tāpēc $a = (a^{-1})^{-1} = f(f(a)) = f(f(b)) = (b^{-1})^{-1} = b$. Tātad f ir injekcija.

(iii) Pieņemsim, ka $a \in G$, tad $a^{-1} \in G$ un $f(a^{-1}) = (a^{-1})^{-1} = a$. Tātad f ir sirjekcija.

(iv) Tagad atliek vairs tikai atsaukties uz bijekcijas definīciju, lai konstatētu, ka f ir bijekcija. ■

2.7.3. Sekas. *Ja G ir grupa, tad*

$$G^{-1} \rightleftharpoons \{a^{-1} \,|\, a \in G\} = G.$$

2.7.4. Apgalvojums. *Katram grupas G elementam a attēlojums*

$$\mathrm{T}_a \ : x \mapsto ax$$

ir kopas G substitūcija.

□ (i) Ja $ax = ay$, tad $x = a^{-1}(ax) = a^{-1}(ay) = y$. Tas nozīmē, ka $\mathrm{T}_a \ : G \to G$ ir injekcija.

(ii) Ja $y \in G$, tad $a^{-1}y \in G$ un $\mathrm{T}_a \ : a^{-1}y \mapsto aa^{-1}y = y$. Tas demonstrē, ka T_a ir sirjekcija. ■

2.7.5. Vingrinājums. Katram grupas G elementam a attēlojums

$$\mathrm{T}'_a \ : x \mapsto xa$$

ir kopas G substitūcija.

2.7.6. Teorēma. *Kopa $\mathfrak{S}(A)$ ar tajā definēto operāciju*

$$(\tau, \sigma) \mapsto \tau\sigma$$

ir grupa.

□ (i) Saskaņā ar Apgalvojumu 1.3.7 $(\tau, \sigma) \mapsto \tau\sigma$ ir kopā $\mathfrak{S}(A)$ definēta divvietīga operācija, un tāpēc $\mathfrak{S}(A)$ ir grupoīds.

(ii) Saskaņā ar Apgalvojumu 1.2.3 grupoīds $\mathfrak{S}(A)$ ir pusgrupa.

(iii) Attēlojums $\mathbb{I} : A \to A$, kas definēts ar nosacījumu $\mathbb{I} : x \mapsto x$, ir kopas A substitūcija. Pieņemsim, ka $f \in \mathfrak{S}(A)$ un $a \in A$, tad

$$a(\mathbb{I}f) = (a\mathbb{I})f = af = (af)\mathbb{I} = a(f\mathbb{I}).$$

Tas pamato vienādību $\mathbb{I}f = f = f\mathbb{I}$, t.i., $\mathbb{I}$ ir pusgrupas $\mathfrak{S}(A)$ neitrālais elements. Tātad pusgrupa $\mathfrak{S}(A)$ ir monoīds.

(iv) Pieņemsim, ka $f \in \mathfrak{S}(A)$, tad saskaņā ar Apgalvojumu 1.4.7

$$f^{-1}f = \mathbb{I}_A \qquad \text{un} \qquad ff^{-1} = \mathbb{I}_A.$$

Tagad atsaucoties uz Apgalvojumu 1.4.6 secināms: f^{-1} ir bijekcija. Līdz ar to $f^{-1} \in \mathfrak{S}(A)$ un tas ir elementa f apgrieztais elements.

Atliek vairs tikai pievērsties Definīcijai 2.7.1, lai konstatētu, ka monoīds $\mathfrak{S}(A)$ ir grupa. ■

2.7.7. Definīcija. *Kopu $\mathfrak{S}(A)$ ar tajā definēto operāciju*

$$(\tau, \sigma) \mapsto \tau\sigma$$

sauc par kopas A simetrisko grupu; $\mathfrak{S}_n$ sauc par n-tās pakāpes simetrisko grupu.

Grupā $\mathfrak{S}_n$ definēto operāciju $(\tau, \sigma) \mapsto \tau\sigma$ pieņemts saukt par *reizināšanu*, nevis — kompozīciju.

Lietojumi kristalogrāfijā un fizikā ir viens no nopietnākajiem argumentiem, kāpēc mēs tuvāk iepazīstamies ar simetriskām grupām. Mūsdienu lasītāju, protams, tas var arī neaizkustināt, taču simetriskās grupas nozīmīgas arī vēsturiski, jo tieši tās (Ābela un Galuā darbos par algebriskiem vienādojumiem) bija pirmās, kas parādījās matemātikā.

2.7.8. Vingrinājumi. (i) Ja $\langle G, \cdot \rangle$ ir grupa, tad $\langle G, \odot \rangle$ ir grupa, kur

$$\forall x \in G \; \forall y \in G \; x \odot y \leftharpoondown\!\!\!= yx.$$

(ii) Kopa $\mathfrak{S}(A)$ ar tajā definēto operāciju

$$(\tau, \sigma) \mapsto \tau \circ \sigma$$

ir grupa.

2.7.9. Piemērs. Komutatīvais monoīds $\langle \mathbb{Z}, + \rangle$ ir Ābela grupa, taču komutatīvais monoīds $\langle \mathbb{Z}, \times \rangle$ nav grupa. Piemēram, skaitlim 2 monoīdā $\langle \mathbb{Z}, \times \rangle$ neeksistē apgrieztais elements.

2.7.10. Vingrinājums. Pierādīt, ka komutatīvie monoīdi $\langle \mathbb{C}^n, + \rangle$ un $\langle \mathrm{Mat}_n^m(\mathbb{R}), + \rangle$ ir grupas.

2.7.11. Piemēri. (i) Grupoīdi $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{R}, + \rangle$, $\langle \mathbb{C}, + \rangle$ ir komutatīvas grupas.

(ii) Vienelementīgā kopa $\{e\}$ ar tajā definēto operāciju $(e, e) \mapsto e$ ir komutatīva grupa. Šo grupu sauc par *triviālo* grupu.

(iii) Kopa $\mathbb{Z}_m$ ar tajā definēto operāciju $(x, y) \mapsto x + y \mod m$ ir komutatīva grupa. Šo grupu sauc par m–tās kārtas *ciklisko* grupu.

(iv) Vienības riņķis $S^1 \leftharpoondown\!\!\!= \{z \mid z \in \mathbb{C} \wedge |z| = 1\}$ ar tajā definēto komplekso skaitļu reizināšanu ir komutatīva grupa.

2.7.12. Vingrinājums. Pierādīt, ka Kleina 4–grupa ir Ābela grupa. Šīs grupas Kelī tabulu skatīt 31. lappusē.

2.8. Homomorfismi

2.8.1. Definīcija. *Pieņemsim, ka* $\langle P, \odot \rangle$ *un* $\langle S, \oplus \rangle$ *ir divas pusgrupas. Attēlojumu* $f : P \to S$ *sauc par pusgrupu homomorfismu, ja*

$$\forall x \in P \, \forall y \in P \quad f(x \odot y) = f(x) \oplus f(y).$$

Parasti gan operāciju simbolus $\odot$ un $\oplus$ vispārīgā gadījumā nelieto. Šai gadījumā homomorfisma definīcija izskatās šādi:

$$f(xy) = f(x)f(y).$$

Ja P un S ir komutatīvas pusgrupas, tad mēdz lietot aditīvo pierakstu:

$$f(x + y) = f(x) + f(y).$$

Saprotams, ka vispārīgā gadījumā saskaitīšanas simbols $+$ katrā pusgrupā apzīmē citu operāciju, kaut arī šīm operācijām tiek lietots viens un tas pats pieraksts.

Bijektīvu homomorfismu sauc par *izomorfismu.* Šai situācijā pusgrupas P un S sauc par *izomorfām* pusgrupām.

2.8.2. Piemēri. (i) Attēlojums $f : x \mapsto 2^x$ ir pusgrupu $\langle \mathbb{R}, + \rangle$, $\langle \mathbb{R}, \cdot \rangle$ homomorfisms.

(ii) Kopa $\{-1, 0, 1\}$ ar tajā definēto skaitļu reizināšanu ir pusgrupa. Attēlojums $f : x \mapsto \operatorname{sgn} x$ ir pusgrupu $\langle \mathbb{Z}, \cdot \rangle$, $\langle \{-1, 0, 1\}, \cdot \rangle$ homomorfisms.

(iii) Attēlojums

$$f : x \mapsto \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$$

ir pusgrupu $\langle \mathbb{R}, \cdot \rangle$, $\langle \mathrm{Mat}_2(\mathbb{R}), \cdot \rangle$ homomorfisms.

2.8.3. Definīcija. *Sirjektīvu homomorfismu sauc par epimorfismu. Injektīvu homomorfismu sauc par monomorfismu.*

2.8.4. Apgalvojums. *Ja* $f : P \twoheadrightarrow S$ *ir pusgrupu epimorfisms un* e *ir neitrālais elements, tad* $f(e)$ *ir neitrālais elements.*

□ Pieņemsim, ka $x \in S$. Tā kā $f : P \twoheadrightarrow S$ ir sirjekcija, tad eksistē tāds $a \in P$, ka $f(a) = x$. Tagad ņemam vērā, ka f ir homomorfisms

$$\begin{aligned} f(e)x &= f(e)f(a) = f(ea) = f(a) \\ &= x = f(a) = f(ae) = f(a)f(e) \\ &= xf(e). \quad \blacksquare \end{aligned}$$

Brīdinājums. Nosacījums, ka $f : P \twoheadrightarrow S$ ir epimorfisms ir būtisks. Tā, piemēram, attēlojums

$$f : x \mapsto \begin{pmatrix} x & 0 \\ 0 & 0 \end{pmatrix}$$

ir pusgrupu $\langle \mathbb{R}, \cdot \rangle$, $\langle \mathrm{Mat}_2(\mathbb{R}), \cdot \rangle$ homomorfisms, taču

$$f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix},$$

kas nav monoīda $\langle \mathrm{Mat}_2(\mathbb{R}), \cdot \rangle$ neitrālais elements. Šī iemesla dēļ monoīdu homomorfismu definē citādi.

2.8.5. Definīcija. *Pieņemsim, ka M un N ir divi monoīdi. Pusgrupu homomorfismu $f : M \to N$ sauc par monoīdu homomorfismu, ja*

$$f(e) = e',$$

kur e ir monoīda M neitrālais elements un e' ir monoīda N neitrālais elements.

2.8.6. Apgalvojums. *Ja $f : P \twoheadrightarrow S$ ir pusgrupu epimorfisms un elementam $a \in P$ eksistē duālais elements, tad elementam $f(a)$ eksistē duālais elements un $f(a)^{-1} = f(a^{-1})$.*

□ Tā kā elementam $a \in P$ eksistē duālais elements, tad pusgrupa P ir monoīds. Pieņemsim, ka e ir monoīda P neitrālais elements, tad $f(e)$ (Apgalvojumus 2.8.4) ir pusgrupas S neitrālais elements. Tagad ņemam vērā, ka $f : P \twoheadrightarrow S$ ir pusgrupu homomorfisms. No šejienes

$$f(a^{-1})f(a) = f(a^{-1}a) = f(e) = f(aa^{-1}) = f(a)f(a^{-1}).$$

Tātad (Definīcija 2.6.1) $f(a^{-1}) = f(a)^{-1}$. $\blacksquare$

2.8.7. Definīcija. *Pieņemsim, ka P ir pusgrupa. Pusgrupu homomorfismu $f : P \to P$ sauc par endomorfismu. Ja endomorfisms ir bijekcija, tad to sauc par automorfismu.*

2.8.8. Piemērs. Attēlojums $f : x \mapsto 2x$ ir monoīda $\langle \mathbb{N}, + \rangle$ endomorfisms. Šis endomorfisms ir monomorfisms, taču tas nav nedz epimorfisms, nedz automorfisms.

2.9. Apakšpusgrupas

2.9.1. Definīcija. *Pusgrupas $\langle P, \odot \rangle$ netukšu apakškopu S sauc par apakšpusgrupu, ja*

$$\forall x \in S \; \forall y \in S \quad x \odot y \in S.$$

2.9.2. Vingrinājums. Pusgrupas P apakšpusgrupa S ir pusgrupa.

2.9.3. Piemēri. (i) Kopa $\mathbb{Z}2 \leftharpoondown \{x \mid \exists a \in \mathbb{Z} \; x = 2a\}$ *ir pusgrupas* $\langle \mathbb{Z}, \cdot \rangle$ *apakšpusgrupa.*

(ii) Kopa $\{-1, 0, 1\}$ ir pusgrupas $\langle \mathbb{R}, \cdot \rangle$ apakšpusgrupa.

(iii) Kopa

$$\tilde{\mathbb{C}} \leftharpoondown \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| \; (a, b) \in \mathbb{R}^2 \right\}$$

ir pusgrupas $\langle \mathrm{Mat}_2(\mathbb{R}), \cdot \rangle$ apakšpusgrupa.

2.9.4. Vingrinājums. Pierādīt, ka $\langle \tilde{\mathbb{C}}, \cdot \rangle$ ir komutatīvs monoīds.

2.9.5. Apgalvojums. *Pieņemsim, ka $\{P_i \mid i \in \mathcal{I}\}$ ir pusgrupas P apakšpusgrupu saime. Ja $S \leftharpoondown \bigcap_{i \in \mathcal{I}} P_i \neq \emptyset$, tad S ir apakšpusgrupa.*

$\square$ Pieņemsim, ka $x \in S$ un $y \in S$, tad

$$\forall i \in \mathcal{I} \; (x \in P_i \wedge y \in P_i).$$

Tā kā P_i ir pusgrupas, tad $\forall i \in \mathcal{I} \; xy \in P_i$. Līdz ar to $xy \in \bigcap_{i \in \mathcal{I}} P_i = S$. $\blacksquare$

Brīdinājums. Nosacījums, lai $S \neq \emptyset$ ir būtisks. Tā, piemēram, $\langle \mathbb{Z}_-, + \rangle$ un $\langle \mathbb{Z}_+, + \rangle$ ir pusgrupas $\langle \mathbb{Z}, + \rangle$ apakšpusgrupas, bet $\mathbb{Z}_- \cap \mathbb{Z}_+ = \emptyset$, kas nav apakšpusgrupa.

Vienošanās. Pieņemsim, ka $f : P \to S$ ir attēlojums. Abstraktā algebrā parasti lieto apzīmējumu

$$\mathrm{Im}(f) \leftharpoondown \mathrm{Ran}(f),$$

ko sauc par attēlojuma f *attēlu*.

2.9.6. Apgalvojums. *Ja* $f : P \to S$ *ir pusgrupu homomorfisms, tad* $\mathrm{Im}(f)$ *ir pusgrupas* S *apakšpusgrupa.*

□ Pieņemsim, ka $y \in \mathrm{Im}(f)$ un $y' \in \mathrm{Im}(f)$, tad eksistē $x \in P$ un $x' \in P$ tādi, ka $f(x) = y$ un $f(x') = y'$. No šejienes

$$yy' = f(x)f(x') = f(xx') \in \mathrm{Im}(f). \quad \blacksquare$$

2.10. Kongruences

2.10.1. Definīcija. *Pusgrupā* P *definētu ekvivalences tipa predikātu* $\equiv$ *sauc par kongruenci, ja*

$$\forall a \in P\ \forall x \in P\ \forall y \in P\ (x \equiv y \Rightarrow ax \equiv ay\ \wedge\ xa \equiv ya).$$

2.10.2. Vingrinājums. *Ekvivalences tipa predikāts* $\equiv$ *ir kongruence pusgrupā* P *tad un tikai tad, ja*

$$a \equiv b\ \wedge\ x \equiv y \Rightarrow ax \equiv by.$$

2.10.3. Piemēri. (i) Kopu saime $\{Z_0, Z_1\}$, kur

$Z_0 \leftharpoondown \{\text{pārskaitļi}\}$, $Z_1 \leftharpoondown \{\text{nepārskaitļi}\}$, ir veselo skaitļu kopas $\mathbb{Z}$ sadalījums. Šis sadalījums definē (Apgalvojums 1.6.6) ekvivalences tipa predikātu $\equiv$, kas patiesībā ir kongruence pusgrupā $\langle \mathbb{Z}, + \rangle$:

a	$x \equiv y$	$a + x \equiv a + y\ \wedge\ x + a \equiv y + a$
Z_0	Z_0	Z_0
Z_0	Z_1	Z_1
Z_1	Z_0	Z_1
Z_1	Z_1	Z_0

(ii) Kopu saime $\{\mathbb{Z}_-, \{0\}, \mathbb{Z}_+\}$ ir veselo skaitļu kopas $\mathbb{Z}$ sadalījums. Šis sadalījums definē (Apgalvojums 1.6.6) ekvivalences tipa predikātu $\equiv$, kas patiesībā ir kongruence pusgrupā $\langle \mathbb{Z}, \cdot \rangle$:

a	$x \equiv y$	$ax \equiv ay \wedge xa \equiv ya$
$\mathbb{Z}_-$	$\mathbb{Z}_-$	$\mathbb{Z}_+$
$\mathbb{Z}_-$	$\{0\}$	$\{0\}$
$\mathbb{Z}_-$	$\mathbb{Z}_+$	$\mathbb{Z}_-$
$\{0\}$	$\mathbb{Z}_-$	$\{0\}$
$\{0\}$	$\{0\}$	$\{0\}$
$\{0\}$	$\mathbb{Z}_+$	$\{0\}$
$\mathbb{Z}_+$	$\mathbb{Z}_-$	$\mathbb{Z}_-$
$\mathbb{Z}_+$	$\{0\}$	$\{0\}$
$\mathbb{Z}_+$	$\mathbb{Z}_+$	$\mathbb{Z}_+$

Taču šis pats ekvivalences tipa predikāts nav kongruence pusgrupā $\langle \mathbb{Z}, + \rangle$. Piemēram, $-2 \equiv -1$, bet $-2 + 2 = 0 \not\equiv 1 = -1 + 2$.

2.10.4. Apgalvojums. *Ja $\equiv$ ir kongruence pusgrupā P, tad $P/\equiv$ ir pusgrupa, kur*

$$[x][y] \leftharpoondown [xy]. \tag{2.2}$$

$\square$ (i) Vispirms parādīsim, ka reizināšana faktorkopā $P/\equiv$ definēta korekti. Pieņemsim, ka $[a] = [x]$ un $[b] = [y]$, tad $a \equiv x$ un $b \equiv y$. Tā kā $\equiv$ ir kongruence pusgrupā P, tad $ab \equiv xb$ un $xb \equiv xy$. No šejienes, ņemot vērā, ka $\equiv$ ir transitīva, seko:

$$ab \equiv xy, \qquad \text{t.i.,} \qquad [ab] = [xy].$$

Tātad reizinājums nav atkarīgs no konkrētu blakusklases pārstāvju izvēles, svarīgi tikai, lai tie piederētu vienai un tai pašai blakusklasei.

(ii) Atliek parādīt, ka reizināšana ir asociatīva.

$$[a]([b][c]) = [a][bc] = [a(bc)] = [(ab)c] = [ab][c] = ([a][b])[c]. \quad \blacksquare$$

2.10.5. Definīcija. *Pieņemsim, ka $\equiv$ ir kongruence pusgrupā P. Faktorkopu $P/\equiv$ ar tajā definēto reizināšanu* (2.2) *sauc par faktorpusgrupu pēc kongruences $\equiv$.*

2.10.6. Vingrinājums. Ja $\equiv$ ir kongruence pusgrupā P, tad attēlojums

$$\pi : P \to P/\equiv : x \mapsto [x] \tag{2.3}$$

ir pusgrupu epimorfisms.

2.10.7. Definīcija. *Pieņemsim, ka $\equiv$ ir kongruence pusgrupā P. Homomorfismu* (2.3) *sauc par dabīgo jeb kanonisko homomorfismu.*

2.10.8. Piemēri. (i) Kopu saime $\{Z_0, Z_1\}$ (skatīt Piemēru 2.10.3(i)) definē kongruenci pusgrupā $\langle \mathbb{Z}, + \rangle$. Dotajā gadījumā $\mathbb{Z}/\equiv$ Kelī tabula izskatās šādi:

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

Attēlojums

$$\pi(x) \leftharpoondown \begin{cases} [0], & \text{ja} \quad x \text{ pāra skaitlis,} \\ [1], & \text{ja} \quad x \text{ nepāra skaitlis} \end{cases}$$

ir dabīgais homomorfisms.

(ii) Kopu saime $\{\mathbb{Z}_-, \{0\}, \mathbb{Z}_+\}$ (skatīt Piemēru 2.10.3(ii)) definē kongruenci pusgrupā $\langle \mathbb{Z}, \cdot \rangle$. Dotajā gadījumā $\mathbb{Z}/\equiv$ Kelī tabula izskatās šādi:

$\cdot$	$[-1]$	$[0]$	$[1]$
$[-1]$	$[1]$	$[0]$	$[-1]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[-1]$	$[0]$	$[1]$

Attēlojums

$$\pi(x) \leftharpoondown \begin{cases} [-1], & \text{ja} \quad x < 0, \\ [0], & \text{ja} \quad x = 0, \\ [1], & \text{ja} \quad x > 0 \end{cases}$$

ir dabīgais homomorfisms.

2.10.9. Apgalvojums. *Ja $f : P \to S$ ir pusgrupu homomorfisms, tad* $\mathrm{K\overline{er}}f$ *ir kongruence.*

□ Saskaņā ar definīciju: ja $(x,y) \in \mathrm{K\overline{er}}\, f$, tad $f(x) = f(y)$. No šejienes

$$\begin{array}{rrcl}
 & f(a)f(x) = f(a)f(y) & \wedge & f(x)f(a) = f(y)f(a), \\
\Leftrightarrow & f(ax) = f(ay) & \wedge & f(xa) = f(xy), \\
\Leftrightarrow & (ax, ay) \in \mathrm{K\overline{er}}\, f & \wedge & (xa, ya) \in \mathrm{K\overline{er}}\, f. \quad \blacksquare
\end{array}$$

2.10.10. Teorēma. *Katram pusgrupu homomorfismam $f : P \to S$ eksistē viens vienīgs pusgrupu homomorfisms $f_* : P/\mathrm{K\overline{er}}\, f \to S$, kam diagramma*

$$\begin{tikzcd}
P \arrow[rr, "f"] \arrow[dr, "\pi"'] & & S \\
 & P/\mathrm{K\overline{er}}\, f \arrow[ur, "f_*"'] &
\end{tikzcd} \tag{D2}$$

ir komutatīva; turklāt šis homomorfisms f_* ir monomorfisms.

□ Teorēma 1.6.16 apgalvo, ka eksistē viens vienīgs attēlojums

$$f_* : P/\mathrm{K\overline{er}}\, f \to S,$$

kam diagramma (D2) ir komutatīva, turklāt f_* ir injekcija. Atliek pārliecināties, ka šis attēlojums ir pusgrupu homomorfisms.

Pieņemsim, ka $[x] \in P/\mathrm{K\overline{er}}\, f$ un $[y] \in P/\mathrm{K\overline{er}}\, f$. Saskaņā ar f_* definīciju

$$f_*([x]) = f(x) \qquad \text{un} \qquad f_*([y]) = f(y).$$

No šejienes

$$\begin{aligned}
f_*([x])f_*([y]) &= f(x)f(y) = f(xy) \\
&= f_*([xy]) \overset{(2.2)}{=} f_*([x][y]). \quad \blacksquare
\end{aligned}$$

2.11. Cikliskas pusgrupas

2.11.1. Definīcija. *Pusgrupu P sauc par monogēnu jeb ciklisku pusgrupu, ja*

$$\exists a \in P \; \forall x \in P \; \exists n \in \mathbb{Z}_+ \; x = a^n.$$

Šai situācijā elementu a sauc par monogēnās pusgrupas P *veidotājelementu.*

2.11.2. Piemēri. (i) $\langle \mathbb{Z}_+, +\rangle$ ir monogēna pusgrupa ar veidotājelementu 1. Šo pusgrupu dažkārt sauc par *aditīvo pusgrupu* $\mathbb{Z}_+$.

(ii) Fiksējam pozitīvus naturālus skaitļus d un m, un definējam kopas $\mathbb{Z}_+$ sadalījumu $S(d,m)$:

$$\begin{array}{rcl} [1] & \rightleftharpoons & \{1\}, \quad [2] \rightleftharpoons \{2\}, \ldots, [d-1] \rightleftharpoons \{d-1\}; \\ [d] & \rightleftharpoons & \{x \mid x = d + km \wedge k \in \mathbb{N}\}, \\ [d+1] & \rightleftharpoons & \{x \mid x = d + 1 + km \wedge k \in \mathbb{N}\}, \\ \ldots & \ldots & \ldots\ldots\ldots\ldots\ldots\ldots \\ [d+m-1] & \rightleftharpoons & \{x \mid x = d + m - 1 + km \wedge k \in \mathbb{N}\}. \end{array}$$

2.11.3. Lemma. *Ja kopas $\mathbb{Z}_+$ sadalījums $S(d,m)$ atbilst ekvivalences tipa predikātam $\varrho(d,m)$ (skatīt Vingrinājumus 1.6.8), tad $\varrho(d,m)$ ir kongruence pusgrupā $\langle \mathbb{Z}_+, +\rangle$.*

□ Tā kā $\langle \mathbb{Z}_+, +\rangle$ ir komutatīva pusgrupa, tad jāpierāda tikai nosacījums

$$\forall a \in \mathbb{Z}_+ \, \forall x \in \mathbb{Z}_+ \, \forall x \in \mathbb{Z}_+ \quad [(x,y) \in \varrho(d,m) \Rightarrow (a+x, a+y) \in \varrho(d,m)].$$

Pieņemsim, ka $x \in [j]$ un $y \in [j]$. Tālāko pierādījumu sadalīsim divās daļās.

(i) Ja $1 \leq j < d$, tad $x = j = y$. No šejienes $a + x = a + y$, tāpēc $(a+x, a+y) \in \varrho(d,m)$.

(ii) Ja $d \leq j < d + m$, tad eksistē tādi naturāli k un s, ka

$$x = j + km \quad \text{un} \quad y = j + sm.$$

Pieņemsim, ka $a \in [i]$, tad eksistē tāds naturāls skaitlis l, ka $a = i + lm$. No šejienes

$$\begin{array}{rcl} a + x & = & i + j + (l+k)m, \\ a + y & = & i + j + (l+s)m. \end{array}$$

Ja $i + j < d + m$, tad šīs vienādības ļauj secināt, ka

$$a + x \in [i+j] \quad \text{un} \quad a + y \in [i+j],$$

tātad $(a + x, a + y) \in \varrho(d, m)$.

Tagad izanalizēsim gadījumu, ja $i + j \geq d + m$. Šai situācijā

$$i + j - d \geq m > 0,$$

un tāpēc eksistē tādi naturāli q un r, ka

$$i + j - d = qm + r, \quad \text{kur} \quad r \in \overline{0, m-1}.$$

Atzīmēsim, ka pēdējā vienādība nav nekas cits, kā dalīšana ar atlikumu. No šejienes

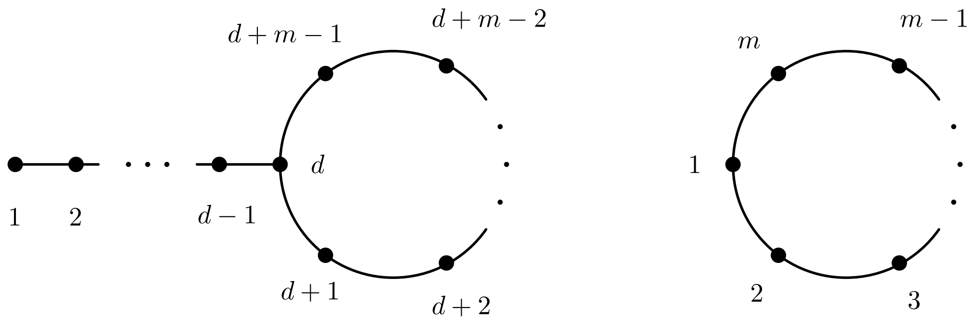
$$i + j = d + r + qm \quad \text{un} \quad d + r < d + m.$$

Tātad

$$\begin{aligned} a + x &= i + j + (l + k)m = d + r + qm + (l + k)m \\ &= d + r + (q + l + k)m \in [d + r], \\ a + y &= i + j + (l + s)m = d + r + qm + (l + s)m \\ &= d + r + (q + l + s)m \in [d + r]. \quad \blacksquare \end{aligned}$$

2.11.4. Definīcija. *Pusgrupas $\langle \mathbb{Z}_+, + \rangle$ faktorpusgrupu pēc kongruences $\varrho(d, m)$ sauc par ciklu ar asti.*

Ja $d = 1$, tad astes nav, un šai situācijā faktorpusgrupu $\mathbb{Z}_+ / \varrho(1, m)$ sauc par *ciklu.* Shematiski tas viss izskatās šādi:



2.11.5. Teorēma. *Jebkura monogēna pusgrupa ir izomorfa aditīvai pusgrupai $\mathbb{Z}_+$, ciklam, vai arī kādam ciklam ar asti.*

□ Pieņemsim, ka P — monogēna pusgrupa ar veidotājelementu a. Apskatīsim attēlojumu

$$\varphi : \mathbb{Z}_+ \to P : n \mapsto a^n.$$

Tā kā P — monogēna, tad φ — sirjekcija, turklāt

$$\varphi(m+n) = a^{m+n} \overset{\text{V2.5.5(i)}}{=} a^m a^n = \varphi(m)\varphi(n),$$

t.i., φ ir epimorfisms.

No Teorēmas 2.10.10 izriet, ka $\mathbb{Z}_+/\overline{\mathrm{Ker}}\varphi \cong \mathrm{Im}(\varphi)$, t.i., pusgrupas $\mathbb{Z}_+/\overline{\mathrm{Ker}}\varphi$ un $\mathrm{Im}(\varphi)$ ir izomorfas. Dotajā gadījumā $\mathrm{Im}(\varphi) = P$.

(i) Pieņemsim, ka sadalījums $\mathcal{A}$ atbilst kongruencei $\overline{\mathrm{Ker}}(\varphi)$. Ja visas sadalījuma $\mathcal{A}$ blakusklases ir vienelementīgas, tad $\mathbb{Z}_+ \cong \mathbb{Z}_+/\overline{\mathrm{Ker}}\varphi \cong P$.

(ii) Pretējā gadījumā eksistē klases $\mathcal{A}_i \in \mathcal{A}$, kas satur vismaz 2 elementus. Ar d apzīmēsim mazāko elementu, kas pieder šīm klasēm, t.i.,

$$d \leftharpoondown \min_i \mathcal{A}_i.$$

Tas nozīmē, ka klases $[1], [2], \ldots, [d-1]$ ir vienelementīgas un klase $[d]$ satur vismaz 2 elementus. Ar r apzīmēsim mazāko no skaitļa d atšķirīgo klases $[d]$ skaitli, t.i.,

$$r \leftharpoondown \min([d] \setminus \{d\}).$$

Pieņemsim, ka $m \leftharpoondown r - d$. Saskaņā ar $\overline{\mathrm{Ker}}(\varphi)$ definīciju no šejienes

$$\varphi(d) = \varphi(r) = \varphi(d+m). \tag{2.4}$$

Ņemot vērā skaitļa r definīciju secināms

$$[d] \neq [d+i], \qquad \text{ja} \qquad i \in \overline{1, m-1}.$$

Tiešām $d + i \notin [d]$, bet $d + i \in [d+i]$.

• Parādīsim, ka $\forall i \in \overline{0, m-1} \quad [d+i] \supseteq \{x \mid \exists k \in \mathbb{N}\ x = d + i + km\}$. Saskaņā ar $\overline{\mathrm{Ker}}(\varphi)$ definīciju mums jāparāda, ka

$$\varphi(d+i) = \varphi(d+i+km). \tag{2.5}$$

Ja $k = 0$, tad (2.5) ir acīm redzama. Tālākie spriedumi induktīvi

$$\begin{aligned}
\varphi(d+i+km) &= \varphi(d+i+(k-1)m+m) = \varphi(d+i+(k-1)m)\varphi(m) \\
&= \varphi(d+i)\varphi(m) = \varphi(d+i+m) \\
&= \varphi(d+m)\varphi(i) \overset{(2.4)}{=} \varphi(d)\varphi(i) = \varphi(d+i)
\end{aligned}$$

• Tagad parādīsim: ja $0 \le i < j < m$, tad $[d+i] \ne [d+j]$.
Pieņemsim pretējo, proti, $[d+i] = d+j$. Ja reiz tā, tad

$$\begin{aligned} [d] &\overset{(2.4)}{=} [d+m] = [d+j+m-j] \\ &= [d+j]+[m-j] = [d+i]+[m-j] \\ &= [d+(m-(j-i))] = [d+q], \end{aligned}$$

kur $q \leftharpoondown m-(j-i)$. No q definīcijas izriet, ka $0 < q < m$. Tātad

$$d < d+q < d+m = d+r-d = r \qquad \text{un} \qquad d+q \in [d].$$

Atceramies, ka r bija mazākais no d atšķirīgais blakusklases $[d]$ elements, bet $d+q < r$. Pretruna!

Mēs tikko konstatējām:

$$\text{ja} \qquad i \in \overline{0, m-1}, \qquad \text{tad} \qquad [d+i] = \{x \mid \exists k \in \mathbb{N}\ x = d+i+km\}.$$

Tātad $\mathcal{A} = S(d,m)$ (skatīt Piemēru 2.11.2(ii)), jo vienelementīgās blakusklases abiem šiem sadalījumiem arī sakrīt. Tā rezultātā

$$\mathbb{Z}_+/\varrho(d,m) = \mathbb{Z}_+/\overline{\mathrm{Ker}}(\varphi) \cong P,$$

t.i., P ir izomorfa ciklam, vai arī ciklam ar asti. ∎

Pieņemsim, ka P — pusgrupa un S — pusgrupas P apakšpusgrupa. Simboliski to pierakstīsim šadi: $S \le P$.
Pieņemsim, ka $\emptyset \ne X \subseteq P$, tad

$$\langle X \rangle \leftharpoondown \bigcap_{X \subseteq S \le P} S,$$

t.i., mēs aplūkojam šķēlumu pa visām pusgrupas P apakšpusgrupām, kas satur kopu X.

2.11.6. Apgalvojums. $\langle X \rangle$ *ir pusgrupa.*

□ (i) Tā kā $P \le P$, tad vismaz viena pusgrupa apmierina nosacījumu $\emptyset \ne X \subseteq P$.
(ii) Visas pusgrupas S satur kopu $X \ne \emptyset$, tāpēc $\langle X \rangle \supseteq X \ne \emptyset$. Tagad atsaucoties uz Apgalvojumu 2.9.5 secināms: $\langle X \rangle$ ir pusgrupa. ∎

2.11.7. Definīcija. *Pusgrupu* $\langle X\rangle$ *sauc par kopas* X *ğenerēto apakšpusgrupu.*

Ja $\langle X\rangle = P$, tad kopu X sauc par pusgrupas P *veidotājkopu.* Lai nesarežğītu apzīmējumus, ja $X = \{x_1, x_2, \dots, x_n\}$, parasti uzskata, ka

$$\langle x_1, x_2, \dots, x_n\rangle \leftharpoondown \langle X\rangle.$$

Pieņemsim, ka a ir pusgrupas P elements, tad

$$\forall n \in \mathbb{Z}_+ \; a^n \in P.$$

Tā rezultātā

$$P(a) \leftharpoondown \{x \mid \exists n \in \mathbb{Z}_+ \; x = a^n\}$$

ir pusgrupas P apakšpusgrupa, kas satur elementu a. Saskaņā ar $\langle a\rangle$ definīciju no šejienes izriet, ka $\langle a\rangle \subseteq P(a)$. Taču tā kā $\langle a\rangle$ ir pusgrupa un $a \in \langle a\rangle$, tad $P(a)$ ir pusgrupas $\langle a\rangle$ apakšpusgrupa, t.i., $P(a) \subseteq \langle a\rangle$. Līdz ar to $P(a) = \langle a\rangle$.

Tātad, ja pusgrupas P veidotājkopa sastāv no viena paša elementa, tad tā ir monogēna, jo $P(a)$ ir monogēna pusgrupa (skatīt monogēnas pusgrupas definīciju).

3. nodaļa

GRUPAS

Grupas, apakšgrupas, kreisās blakusklases, Lagranža teorēma. Elementa kārta, grupas kārta, apakšgrupas H indekss grupā G. Neitrālā, duālā elementa homomorfs attēls. Homomorfisma attēls. Faktorgrupa. Normālā apašgrupa un kongruence grupā. Faktorgrupa pēc normālās apakšgrupas. Kanoniskais homomorfisms, homomorfisma kodols, izomorfisma teorēma. Veidotājkopa, veidotājelements, cikliska grupa, ciklisko grupu klasifikācija. Kelī teorēma. Cikls, transpozīcija, neatkarīgi cikli, elementa i ğenerētā substitūcijas τ orbīta. Substitūcija kā neatkarīgu ciklu kompozīcija. Inversija, substitūcijas zīme, dekrements. Maiņzīmju grupa. Grupas komutants. Grupas centrs un saistīto elementu klases.

3.1. Pilna lineāra grupa

Atgādināsim (Definīcija 2.7.1), ka monoīdu $\langle G, \odot \rangle$, kurā katrs elements ir apgriežams, sauc par *grupu.* Grupu G, kurā operācija $\odot$ ir komutatīva, sauc par *komutatīvu* jeb *Ābela grupu.*

3.1.1. Piemēri. (i) Pieņemsim, ka $\mathbb{R}^* \rightleftharpoons \mathbb{R} \setminus \{0\}$, tad grupoīds $\langle \mathbb{R}^*, \cdot \rangle$ ir komutatīva grupa. Te operācija $\mathbb{R}^* \times \mathbb{R}^* \stackrel{\cdot}{\to} \mathbb{R}^*$ ir reālo skaitļu reizināšana.

(ii) Kopa

$$GL_n(\mathbb{R}) \rightleftharpoons \{\, A \in \mathrm{Mat}_n(\mathbb{R}) \mid |A| \neq 0 \,\}$$

ar tajā definēto matricu reizināšanas operāciju ir grupa.

Lai konstatētu, ka $GL_n(\mathbb{R})$ ir grupoīds mums nāksies pierādīt dažus rezultātus par determinantiem.

3.1.2. Lemma. *Ja*

$$B = \begin{pmatrix} 1 & b_{12} & b_{13} & \dots & b_{1n} \\ 0 & 1 & b_{23} & \dots & b_{2n} \\ . & . & . & . & . \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix},$$

tad $|A| = |BA|$ *jebkurai* n*-tās kārtas kvadrātiskai matricai* A*.*

□ Lielākas uzskatāmības labad matricas $A = ||a_{ij}||$ pieraksta vietā lietosim arī pierakstu

$$\begin{Vmatrix} \boldsymbol{a}_1 \\ \boldsymbol{a}_2 \\ \dots \\ \boldsymbol{a}_n \end{Vmatrix},$$

kur $\boldsymbol{a}_i = (a_{i1}, a_{i2}, \dots, a_{in})$ ir matricas A i-tā rinda. Šajos apzīmējumos

$$BA = \begin{Vmatrix} \boldsymbol{a}_1 + b_{12}\boldsymbol{a}_2 + \dots + b_{1n}\boldsymbol{a}_n \\ \boldsymbol{a}_2 + \dots + b_{2n}\boldsymbol{a}_n \\ \dots\dots\dots \\ \boldsymbol{a}_n \end{Vmatrix}.$$

Tagad pastāstīsim, kā matrica A elementāri pārveidojama par BA. Vispirms iegūst matricas BA pirmo rindu, tad — otro, trešo, utt., līdz iegūst priekšpēdējo rindu.

Detalizētāk aprakstīsim, kā iegūstama i-tā rinda. Vispirms $i+1$ rindu pareizina ar b_{ii+1} un rezultātu pieskaita i-tajai rindai, tad $i+2$ rindu pareizina ar b_{ii+2} un rezultātu pieskaita i-tajai rindai. Tā turpina, līdz iegūst $\boldsymbol{a}_i + b_{ii+1}\boldsymbol{a}_{i+1} + \dots + b_{in}\boldsymbol{a}_n$.

Tā kā visi aprakstītie pārveidojumi ir otrā veida elementāri pārveidojumi, tad $|BA| = |A|$. ■

Uzskatāmības labad matricas

$$H = \begin{pmatrix} a_{11} & \dots & a_{1m} & b_{11} & \dots & b_{1n} \\ . & . & . & . & . & . \\ a_{m1} & \dots & a_{mm} & b_{m1} & \dots & b_{mn} \\ c_{11} & \dots & c_{1m} & d_{11} & \dots & d_{1n} \\ . & . & . & . & . & . \\ c_{n1} & \dots & c_{nm} & d_{n1} & \dots & d_{nn} \end{pmatrix}$$

pieraksta vietā lietosim arī pierakstu

$$\left\| \begin{array}{cc} A & B \\ C & D \end{array} \right\|,$$

kur $\quad A = ||a_{ij}||_m^m, \quad B = ||b_{ij}||_n^m, \quad C = ||c_{ij}||_m^n, \quad D = ||d_{ij}||_n^n\,.$

3.1.3. Lemma.

$$\left| \begin{array}{cc} A & O \\ B & C \end{array} \right| = |A|\,|C|\,,$$

kur $\quad A = ||a_{ij}||_m^m, \quad O = ||0||_n^m, \quad B = ||b_{ij}||_m^n, \quad C = ||c_{ij}||_n^n\,.$

□ Pierādījuma metode — indukcija pēc m. Apzīmēsim

$$H \leftharpoondown \left\| \begin{array}{cc} A & O \\ B & C \end{array} \right\|.$$

Ja $m = 1$, tad

$$H = \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ b_{11} & c_{11} & \dots & c_{1n} \\ . & . & . & . \\ b_{n1} & c_{n1} & \dots & c_{nn} \end{pmatrix}.$$

Izvirzot $|H|$ pēc pirmās rindas,

$$|H| = a_{11} \left| \begin{array}{ccc} c_{11} & \dots & c_{1n} \\ . & . & . \\ c_{n1} & \dots & c_{nn} \end{array} \right| = |A|\,|C|\,.$$

Vispārīgā gadījumā, izvirzot H pēc pirmās rindas,

$$|H| = \sum_{j=1}^{m} a_{1j}\,H_{1j} = \sum_{j=1}^{m} (-1)^{j+1} a_{1j}\,|H[1j]|\,.$$

Ņemsim vērā (skatīt apakšmatricu definīcijas 36. lappusē), ka

$$H[1j] = \left\| \begin{array}{cc} A[1j] & O[1-] \\ B[-j] & C \end{array} \right\|,$$

un, tā kā matricas $A[1j]$ kārta ir $m-1$, tad saskaņā ar indukcijas pieņēmumu $|H[1j]| = |A[1j]|\,|C|$. No šejienes

$$|H| = \sum_{j=1}^{m}(-1)^{j+1}a_{1j}\,|A[1j]|\,|C| = |C|\sum_{j=1}^{m}(-1)^{j+1}a_{1j}\,|A[1j]| =$$

$$= |C|\sum_{j=1}^{m}a_{1j}\,A_{1j} = |C|\,|A| = |A|\,|C|\,. \blacksquare$$

3.1.4. Teorēma. *Ja A, B — kvadrātiskas matricas, tad*

$$|AB| = |A|\,|B|.$$

$\square$ Pieņemsim, ka $A, B \in \mathrm{Mat}_n(\mathbb{R})$, tad matricas

$$\left\| \begin{matrix} A & O \\ -E & B \end{matrix} \right\|$$

kārta ir $2n$. Saskaņā ar Lemmu 3.1.3

$$\left| \begin{matrix} A & O \\ -E & B \end{matrix} \right| = |A|\,|B|\,. \tag{3.1}$$

Savukārt, atsaucoties uz Lemmu 3.1.2

$$\left| \begin{matrix} A & O \\ -E & B \end{matrix} \right| = \left| \left\| \begin{matrix} E & A \\ O & E \end{matrix} \right\| \left\| \begin{matrix} A & O \\ -E & B \end{matrix} \right\| \right|.$$

Tā kā

$$\left\| \begin{matrix} E & A \\ O & E \end{matrix} \right\| \left\| \begin{matrix} A & O \\ -E & B \end{matrix} \right\| = \left\| \begin{matrix} O & AB \\ -E & B \end{matrix} \right\|,$$

tad

$$\left| \begin{matrix} A & O \\ -E & B \end{matrix} \right| = \left| \begin{matrix} O & AB \\ -E & B \end{matrix} \right|. \tag{3.2}$$

Pēdējā determinantā, mainot vietām pirmo aili ar $n+1$, tad otro — ar $n+2$, utt., līdz n-to aili nomaina ar $2n$, iegūst

$$\left| \begin{matrix} O & AB \\ -E & B \end{matrix} \right| = (-1)^n \left| \begin{matrix} AB & O \\ B & -E \end{matrix} \right|. \tag{3.3}$$

Atkal, atsaucoties uz Lemmu 3.1.3, var pamatot, ka

$$\begin{vmatrix} AB & O \\ B & -E \end{vmatrix} = |AB|\,|-E| = (-1)^n\,|AB|\,.$$

Tagad, ņemot vērā formulas (3.1–3.3), izvedams

$$|A|\,|B| = \begin{vmatrix} A & O \\ -E & B \end{vmatrix} = \begin{vmatrix} O & AB \\ -E & B \end{vmatrix} = (-1)^n \begin{vmatrix} AB & O \\ B & -E \end{vmatrix} =$$

$$= (-1)^n\,(-1)^n\,|AB| = |AB|\,. \;\blacksquare$$

3.1.5. Sekas. *$GL_n(\mathbb{R})$ ir grupoīds.*

$\square$ Pieņemsim, ka $A, B \in GL_n(\mathbb{R})$, tad $|A| \neq 0 \neq |B|$. No šejienes $|AB| = |A|\,|B| \neq 0$, tāpēc $AB \in GL_n(\mathbb{R})$. $\blacksquare$

Kā redzams, dažos gadījumos, lai konstatētu, ka dotā kopa ar tajā definēto operāciju ir grupa, nākas krietni papūlēties. Tikko aplūkotajā gadījumā mēs pamatojām, ka matricu reizināšanas sašaurinājums kopā $GL_n(\mathbb{R})$ arī ir operācija.

3.1.6. Teorēma. *Kopa $GL_n(\mathbb{R})$ ar tajā definēto matricu reizināšanas operāciju ir grupa.*

$\square$ (i) Tā kā $\mathrm{Mat}_n(\mathbb{R})$ ir monoīds, tad arī kopā $GL_n(\mathbb{R})$ izpildās asociatīvais likums. Līdz ar to $GL_n(\mathbb{R})$ ir monoīds.

(ii) Ņemsim vērā, ka $|A| \neq 0$, tādēļ (skatīt 37. lappusi) matricai A eksistē inversā matrica A^{-1}. Ja reiz tā, tad, balstoties uz Teorēmu 3.1.4, secināms $1 = |E| = |AA^{-1}| = |A|\,|A^{-1}|$. Tātad $|A^{-1}| = |A|^{-1} \neq 0$. Līdz ar to $A^{-1} \in GL_n(\mathbb{R})$. Tas nozīmē (Definīcija 2.7.1) [22.32. definīcija], ka $GL_n(\mathbb{R})$ ir grupa. $\blacksquare$

3.1.7. Definīcija. *Grupu $GL_n(\mathbb{R})$ sauc par pilnu lineāru grupu pār lauku $\mathbb{R}$.*

Lineāro grupu teorijas pirmsākumi attiecināmi uz XIX gadsimta vidu. Tie saistīti ar pētījumiem par ģeometriskām transformācijām, pirmām kārtām projektīvajā ģeometrijā. Lineāro grupu teorijas attīstība cieši saistīta ar Lī grupu teoriju, grupu reprezentācijām un Galuā teoriju. Mūsdienu teorētiskās fizikas problemātika būtiski paplašinājusi linearitātes lietojuma sfēru un tā ietekmējusi arī grupu teorijas attīstību.

3.1.8. Vingrinājums. Parādīt, ka kopa

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

ar tajā definēto matricu reizināšanas operāciju ir grupa.

3.1.9. Definīcija. *Grupu $SL_n(\mathbb{R})$ sauc par speciālu lineāru grupu pār lauku $\mathbb{R}$.*

3.2. Elementārās īpašības

3.2.1. Definīcija. *Pusgrupas P elementu e sauc par kreiso neitrālo elementu, ja*

$$\forall a \in P \quad ea = a.$$

Pusgrupas P elementu a' sauc par elementa $a \in P$ kreiso duālo elementu, ja

$$a'a = e.$$

3.2.2. Apgalvojums. *Pusgrupa G ir grupa tad un tikai tad, ja tajā eksistē kreisais neitrālais elements un katram $a \in G$ eksitē kreisais duālais elements.*

□ Nepieciešamais nosacījums uzreiz izriet no grupas definīcijas, jo neitrālais elements ir arī kreisais neitrālais un duālais elements ir arī kreisais duālais.

Pietiekamais nosacījums. Pieņemsim, ka e ir pusgrupas P kreisais neitrālais elements un a' ir elementa a kreisais duālais elements, tad elementam a' eksistē kreisais duālais elements a''. No šejienes

$$aa' = e(aa') = (a''a')(aa') = a''(a'a)a' = a''ea' = a''(ea') = a''a' = e.$$

Tas ļauj secināt, ka

$$ae = a(a'a) = (aa')a = ea = a.$$

Tātad e ir neitrālais elements un a' ir duālais elements. Tas nozīmē (skatīt grupas definīciju), ka G ir grupa. ■

3.2.3. Definīcija. *Pusgrupas P elementu e sauc par labo neitrālo elementu, ja*

$$\forall a \in P \quad ae = a.$$

Pusgrupas P elementu a' sauc par elementa $a \in P$ labo duālo elementu, ja

$$aa' = e.$$

3.2.4. Vingrinājums. *Pusgrupa G ir grupa tad un tikai tad, ja tajā eksistē labais neitrālais elements un katram $a \in G$ eksitē labais duālais elements.*

3.2.5. Apgalvojums. *Pusgrupa G ir grupa tad un tikai tad, ja*

$$\forall a \in G \, \forall b \in G \, \exists x \in G \, \exists y \in G \quad (xa = b \wedge ay = b).$$

$\square$ $\Rightarrow$ Izvēlamies $x = ba^{-1}$ un $y = a^{-1}b$, tad

$$xa = ba^{-1}a = b \qquad \text{un} \qquad ay = aa^{-1}b = b.$$

$\Leftarrow$ (i) Pieņemsim, ka e ir vienādojuma $xa = a$ atrisinājums un y_0 ir vienādojuma $ay = b$ atrisinājums, tad

$$eb = e(ay_0) = (ea)y_0 = ay_0 = b.$$

Līdz ar to e ir pusgrupas kreisais neitrālais elements.

(ii) Pieņemsim, ka b' ir vienādojuma $xb = e$ atrisinājums, tad b' ir elementa b kreisais apgrieztais elements. Tagad atsaucoties uz Apgalvojumu 3.2.2 secināms: P ir grupa. $\blacksquare$

Vienošanās. Pieņemsim, ka G ir grupa, $a \in G$ un $n \in \mathbb{N}$, tad

$$a^{-n} \leftharpoondown (a^{-1})^n.$$

3.2.6. Apgalvojums. *Katram grupas elementam a*

$$\forall m \in \mathbb{Z} \, \forall n \in \mathbb{Z} \quad a^m a^n = a^{m+n}.$$

$\square$ (i) Ja $m \geq 0$ un $n \geq 0$, tad tas ir Vingrinājums 2.6.9.

(ii) Ja $m \geq 0$ un $n \leq 0$, tad pierādījums induktīvs pa m.

Pieņemsim, ka e ir neitrālais elements un $m = 0$, tad apgalvojums ir spēkā, jo
$$a^m a^n = a^0 a^n = ea^n = a^n = a^{0+n} = a^{m+n}.$$

Tālākais pierādījums attiecas uz indukcijas pāreju.

$$a^{m+1}a^n = aa^m a^n = aa^{m+n}.$$

Ja $m + n \geq 0$, tad saskaņā ar Vingrinājumu 2.6.9 $\quad aa^{m+n} = a^{m+1+n}$.
Ja $m + n < 0$, tad $k \leftharpoondown -(m+n) > 0$ un

$$aa^{m+n} = aa^{-k} = a(a^{-1})^k \overset{\text{V2.6.9}}{=} aa^{-1}(a^{-1})^{k-1} = e(a^{-1})^{k-1} = a^{1-k} = a^{m+1+n}.$$

Indukcijas pāreja veikta pilnībā.

(iii) Ja $m \leq 0$ un $n \geq 0$, tad

$$a^m a^n = (a^{-1})^{-m}(a^{-1})^{-n} \overset{\text{(ii)}}{=} (a^{-1})^{-m-n}.$$

Ja $-m - n \geq 0$, tad $(a^{-1})^{-m-n} = a^{-(-m-n)} = a^{m+n}$.
Ja $-m - n < 0$, tad $(a^{-1})^{-m-n} = (a^{-1})^{-(m+n)} = ((a^{-1})^{-1})^{m+n} \overset{\text{S2.6.5}}{=} a^{m+n}$.
(iv) Ja $m \leq 0$ un $n \leq 0$, tad

$$a^m a^n = (a^{-1})^{-m}(a^{-1})^{-n} \overset{\text{(i)}}{=} (a^{-1})^{-m-n} = a^{-(-m-n)} = a^{m+n}. \quad \blacksquare$$

3.2.7. Vingrinājums. *Katram grupas elementam a*

$$\forall m \in \mathbb{Z}\ \forall n \in \mathbb{Z} \quad (a^m)^n = a^{mn}.$$

3.2.8. Apgalvojums. *Ja a un b ir grupas elementi, tad*

$$(ab)^{-1} = b^{-1}a^{-1}.$$

□ Pieņemsim, ka e ir grupas neitrālais elements, tad

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e.$$

Tātad $(ab)^{-1} = b^{-1}a^{-1}$. ■

3.2.9. Vingrinājums. *Ja a un b ir komutatīvi grupas elementi, t.i., $ab = ba$, tad*
$$\forall n \in \mathbb{Z} \quad (ab)^n = a^n b^n.$$

3.2.10. Apgalvojums (Saīsināšanas likumi). *Pieņemsim, ka a, b, c ir grupas G elementi.*

(i) *Ja $ab = ac$, tad $b = c$.*

(ii) *Ja $ba = ca$, tad $b = c$.*

$\square$ (i) $b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = c$.

(ii) Otra saīsināšanas likuma pierādījumu lasītājm piedāvājam kā vingrinājumu. $\blacksquare$

3.3. Apakšgrupas

3.3.1. Definīcija. *Grupas G apakškopu H sauc par apakšgrupu, ja*

(i) *H ir pusgrupas G apakšpusgrupa;*

(ii) $\forall x \in H \quad x^{-1} \in H$.

Šai situācijā līdzīgi kā pusgrupu gadījumā lieto apzīmējumu $H \leq G$.

3.3.2. Vingrinājumi. (i) Katra grupas G apakšgrupa H satur grupas G neitrālo elementu.

(ii) Katra grupas G apakšgrupa H ir grupa attiecībā pret to pašu grupas G operāciju.

(iii) Jebkurai netriviālai grupai G eksistē vismaz divas apakšgrupas: pati grupa G un grupa, kas sastāv no viena paša neitrālā elementa e. Šo vienelementīgo grupas G apakšgrupu $\{e\}$ sauc par grupas G *vienības apakšgrupu.*

3.3.3. Definīcija. *Grupas G vienības apakšgrupu, kā arī pašu grupu G sauc par grupas G triviālajām apakšgrupām.*

Brīdinājums. Jēdzieni *triviāla grupa* un *triviāla apakšgrupa* ir divi dažādi jēdzieni. Tā, piemēram, grupas $\langle \mathbb{Z}, + \rangle$ triviālās apakšgrupas ir grupas $\langle \{0\}, + \rangle$ un $\langle \mathbb{Z}, + \rangle$, taču pati grupa $\langle \mathbb{Z}, + \rangle$ nav triviāla.

3.3.4. Piemēri. (i) Grupas $\langle \mathbb{R}^*, \cdot \rangle$ apakšgrupas:

- $\mathbb{R}^*_+ \leftrightharpoons \{x \in \mathbb{R} \mid x > 0\}$;
- $\{-1; 1\}$;
- $\{x = 2^m \mid m \in \mathbb{Z}\}$.

(ii) Grupas $\langle \mathbb{Z}, + \rangle$ apakšgrupa ir

$$\mathbb{Z}2 \leftharpoondown \{x = 2n \,|\, n \in \mathbb{Z}\},$$

toties

$$\mathbb{Z}2 + 1 \leftharpoondown \{x = 2n + 1 \,|\, n \in \mathbb{Z}\}$$

nav šīs grupas apakšgrupa.

(iii) Grupas $GL_n(\mathbb{R})$ apakšgrupas:

- $SL_n(\mathbb{R})$;
- $$DL_n(\mathbb{R}) \leftharpoondown \left\{ \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ . & . & . & . \\ 0 & 0 & \dots & d_n \end{pmatrix} \middle| \, \forall i \; d_i \in \mathbb{R}^* \right\}.$$

3.3.5. Apgalvojums. *Ja $\{H_i \,|\, i \in \mathcal{I}\}$ ir grupas G apakšgrupu saime, tad $H \leftharpoondown \bigcap\limits_{i \in \mathcal{I}} H_i$ ir grupas G apakšgrupa.*

□ (i) Pieņemsim, ka e ir grupas G vienības elements, tad $e \in H$ (skatīt Vingrinājumu 3.3.2(i)). Līdz ar to $H \neq \emptyset$.

(ii) H ir pusgrupas G apakšpusgrupa (skatīt Apgalvojumu 2.9.5).

(iii) Pieņemsim, ka $h \in H$, tad $\forall i \in \mathcal{I}$ $h \in H_i$. Tā kā H_i ir grupas G apakšgrupa, tad $h^{-1} \in H_i$. No šejienes $h^{-1} \in \bigcap\limits_{i \in \mathcal{I}} H_i = H$.

(iv) Tagad atsaucoties uz (i)–(iii) un apaksğrupas definīciju secināms, ka H ir grupas G apakšgrupa. ■

3.3.6. Vingrinājums. Grupas G netukša apakškopa H ir grupas G apakšgrupa tad un tikai tad, ja tā apmierina šādus divus nosacījumus:

(i) ja a un b ir kopas H elementi, tad $ab \in H$;

(ii) ja $a \in H$, tad $a^{-1} \in H$.

3.4. Blakusklases

3.4.1. Vingrinājumi. (i) Pieņemsim, ka P — pusgrupa un K, H ir kopas P apakškopas, tad

$$KH \rightleftharpoons \{xy \,|\, x \in K \wedge x \in H\}.$$

Ja $K = \emptyset$ vai $H = \emptyset$, tad $KH \rightleftharpoons \emptyset$. Parādīt, ka šī operācija kopā $\mathfrak{P}(P)$ definē pusgrupu!

(ii) Pieņemsim, ka P — pusgrupa, $x \in P$ un $H \subseteq P$, tad

$$xH \rightleftharpoons \{x\}H \qquad \text{un} \qquad Hy \rightleftharpoons H\{y\}.$$

Pierādīt, ka attiecības

$$x \equiv_H^k y \overset{\text{def}}{\Leftrightarrow} xH = yH \qquad \text{un} \qquad x \equiv_H^l y \overset{\text{def}}{\Leftrightarrow} Hx = Hy$$

kopā P ir ekvivalences tipa predikāti.

3.4.2. Definīcija. *Pieņemsim, ka G — grupa, $H \leq G$ un $g \in G$, tad kopu gH sauc par elementa g definēto grupas G kreiso apkšgrupas H blakusklasi. Savukārt kopu Hg sauc par elementa g definēto grupas G labo apkšgrupas H blakusklasi.*

Dažkārt īsuma labad, ja nerodas pārpratumi, gH sauc par *kreiso blakusklasi pēc H*, bet Hg — par *labo blakusklasi pēc H.*

3.4.3. Piemēri. (i) Skaitļa -4 definētā grupas $\langle \mathbb{R}^*, \cdot \rangle$ kreisā apakšgrupas $\mathbb{R}^*_+$ blakusklase ir $\mathbb{R}^*_- \rightleftharpoons \{x \in \mathbb{R}^* \,|\, x < 0\}$.

(ii)

$$\begin{pmatrix} 1 & 3 \\ 2 & 3 \end{pmatrix} SL_2(\mathbb{R}) \quad = \quad \{A \in GL_2(\mathbb{R}) \,|\, |A| = -3\}.$$

Tātad matricas

$$\begin{pmatrix} 1 & 3 \\ 2 & 3 \end{pmatrix}$$

definētā pilnās lineārās grupas $GL_2(\mathbb{R})$ kreisā speciālās lineārās grupas $SL_2(\mathbb{R})$ blakusklase ir nesingulāro matricu kopa $\{A \in GL_2(\mathbb{R}) \,|\, |A| = -3\}$.

Atzīmēsim, ka matricu sauc par *singulāru* jeb *deģenerētu matricu*, ja tās determinants ir 0, ja tās determinants atšķiras no skaitļa 0, tad šādu matricu sauc par *nesingulāru* jeb *nedeģenerētu matricu.*

3.4.4. Lemma. *Ja H ir grupas G apakšgrupa un $xH \cap yH \neq \emptyset$, tad $xH = yH$.*

$\square$ (i) pieņemsim, ka $u \in xH \cap yH$, tad

$$\exists a \in H \; \exists b \in H \quad u = xa = yb.$$

No šejienes

$$x = yba^{-1} \qquad \text{un} \qquad y = xab^{-1}.$$

(ii) Pieņemsim, ka $v \in xH$, tad $\exists c \in H \;\; v = xc$. No šejienes

$$v = xc = yba^{-1}c \in yH,$$

jo H ir grupa un $a \in H, b \in H, c \in H$. Līdz ar to $xH \subseteq yH$.

(iii) Pieņemsim, ka $w \in yH$, tad $\exists d \in H \;\; w = yd$. No šejienes

$$w = yd = xab^{-1}d \in xH.$$

Tātad $yH \subseteq xH$.

(iv) Mēs parādījām, ka $xH \subseteq yH \subseteq xH$. Līdz ar to $xH = yH$. $\blacksquare$

3.4.5. Vingrinājums. *Ja H ir grupas G apakšgrupa un $Hx \cap Hy \neq \emptyset$, tad $Hx = Hy$.*

3.4.6. Lemma. *Ja H ir grupas G apakšgrupa, tad*

$$[x]_H^k \;\overline{\leftharpoondown}\; \{y \,|\, x \equiv_H^k y\} = xH.$$

$\square$ (i) Pieņemsim, ka e ir grupas G neitrālais elements, tad $x = xe$. Tas demonstrē, ka $x \in xH$.

Pieņemsim, ka $y \in xH$, tad saskaņā ar Lemmu 3.4.4 $xH = yH$, tāpēc $x \equiv_H^k y$. Līdz ar to $xH \subseteq [x]_H^k$.

(ii) Pieņemsim, ka $y \in [x]_H^k$, tad $x \equiv_H^k y$, t.i., $xH = yH$. No šejienes $y \in xH$, jo $y \in yH$. Tas demonstrē, ka $[x]_H^k \subseteq xH$.

(iii) Mēs parādījām, ka $xH \subseteq [x]_H^k \subseteq xH$. Līdz ar to $[x]_H^k = xH$. $\blacksquare$

3.4.7. Vingrinājumi. (i) Atrast tādu Kleina 4–grupas elementu x un apakškopu H, ka $[x]_H^k \neq xH$.

(ii) Ja H ir grupas G apakšgrupa, tad $[x]_H^l \;\overline{\leftharpoondown}\; \{y \,|\, x \equiv_H^l y\} = Hx$.

3.4.8. Lemma. *Pieņemsim, ka H ir grupas G apakšgrupa.*

$$aH = bH \Leftrightarrow a^{-1}b \in H.$$

$\Box$ $\Rightarrow$ Pieņemsim, ka $aH = bH$, tad eksistē tāds grupas H elements h, ka $ah = b$. No šejienes $a^{-1}b = h \in H$.

$\Leftarrow$ Pieņemsim, ka $h = a^{-1}b \in H$, tad $ah = b$. No šejienes $ah \in aH$ un saprotams $b \in bH$, jo H satur neitrālo elementu. Tātad $ah = b \in aH \cap bH$. Tagad atsaucoties uz Lemmu 3.4.4 secināms: $aH = bH$. $\blacksquare$

3.4.9. Vingrinājums. Pieņemsim, ka H ir grupas G apakšgrupa.

$$Ha = Hb \Leftrightarrow ab^{-1} \in H.$$

3.4.10. Apgalvojums. *Ja H ir grupas G apakšgrupa, tad attēlojums*

$$\phi : H \to aH : h \mapsto ah$$

ir bijekcija.

$\Box$ (i) Pieņemsim, ka $ah_1 = ah_2$, tad saskaņā ar saīsināšanas likumu (skatīt Apgalvojumu 3.2.10) secināms: $h_1 = h_2$. Tātad ϕ ir injekcija.

(ii) Pieņemsim, ka $x \in aH$, tad eksistē tāds $h \in H$, ka $x = ah$. No šejienes $\phi(h) = ah = x$. Tātad ϕ ir sirjekcija. $\blacksquare$

3.4.11. Vingrinājums. Ja H ir grupas G apakšgrupa, tad attēlojums

$$\phi : H \to Ha : h \mapsto ha$$

ir bijekcija.

3.4.12. Sekas. *Ja H ir grupas G apakšgrupa, tad*

$$\forall a \in G \quad |aH| = |H| = |Ha|.$$

Pieņemsim, ka H ir grupas G apakšgrupa un $\{a \,|\, a \in \mathcal{G}_k\}$ ir ekvivalences $\equiv^k_H$ pilna pārstāvju sistēma (skatīt Definīciju 1.6.11), tad kopas G sadalījumu $\mathcal{K} \leftharpoondown\rightharpoondown\!\!\!\!\!= \{aH \,|\, a \in \mathcal{G}_k\}$ sauc par *grupas G kreiso sadalījumu pēc apakšgrupas H*. Atbilstoši, ja $\{b \,|\, b \in \mathcal{G}_l\}$ ir ekvivalences $\equiv^l_H$ pilna pārstāvju sistēma, tad kopas G sadalījumu $\mathcal{L} \leftharpoondown\rightharpoondown\!\!\!\!\!= \{Hb \,|\, b \in \mathcal{G}_l\}$ sauc par *grupas G labo sadalījumu pēc apakšgrupas H*.

3.4.13. Definīcija. *Kopas $\mathcal{K}$ apjomu*

$$[G : H] \leftharpoondown |\mathcal{K}| = |\{aH \mid a \in \mathcal{G}_k\}|$$

sauc par apakšgrupas H indeksu grupā G.

Ja nerodas domstarpības tad lieto īsāku izteiksmes formu, un saka H indekss ir $[G : H]$.

3.4.14. Vingrinājumi. (i) Pieņemsim, ka G ir grupa un $K \subseteq G$, tad

$$K^{-1} \leftharpoondown \{x^{-1} \mid x \in K\}.$$

Pierādīt, ka $(KH)^{-1} = H^{-1}K^{-1}$ jebkurām kopas G apakškopām K un H.

(ii) Pieņemsim, ka H ir grupas G apakšgrupa. Pierādīt, ka

$$\phi : \mathcal{K} \to \mathcal{L} : aH \mapsto Ha^{-1}$$

ir bijekcija.

3.4.15. Sekas. *Pieņemsim, ka H ir grupas G apakšgrupa, tad*

$$[G : H] = |\mathcal{L}| = |\{Hb \mid b \in \mathcal{G}_l\}|.$$

3.4.16. Definīcija. *Pieņemsim, ka $\langle G, \odot \rangle$ ir grupa. Kopas G apjomu $|G|$ sauc par grupas G kārtu.*

Grupu G sauc par *galīgu grupu*, ja tās apjoms $|G|$ ir naturāls skaitlis. Šai situācijā lieto pierakstu $|G| < \aleph_0$. Pretējā gadījumā grupu G sauc par *bezgalīgu grupu* un mēdz lietot apzīmējumu $|G| \geq \aleph_0$.

3.4.17. Teorēma (Lagranžs). *Ja H ir galīgas grupas G apakšgrupa, tad*

$$[G : H] = \frac{|G|}{|H|}.$$

□ Pieņemsim, ka $\mathcal{K} = \{aH \mid a \in \mathcal{G}_k\}$ ir grupas G kreisais sadalījums pēc apakšgrupas H, tad $[G : H] = |\mathcal{K}|$ un (Sekas 3.4.12) katras apakšklases aH apjoms $|aH| = |H|$. Tā rezultātā $|G| = [G : H]\,|H|$. ■

3.4.18. Sekas. *Ja H ir galīgas grupas G apakšgrupa, tad $|H| \backslash |G|$, t.i., apakšgrupas H kārta dala grupas G kārtu.*

3.5. Homomorfismi

3.5.1. Definīcija. *Pieņemsim, ka G un G' ir grupas. Attēlojumu*

$$f : G \to G'$$

sauc par grupu homomorfismu, ja tas ir pusgrupu G, G' homomorfisms.

Līdzīgi kā pusgrupu gadījumā bijektīvu homomorfismu sauc par *izomorfismu.* Šai situācijā grupas G un G' sauc par *izomorfām* grupām. Sirjektīvu homomorfismu sauc par *epimorfismu.* Injektīvu homomorfismu sauc par *monomorfismu.*

Grupu homomorfismu $f : G \to G$ sauc par *endomorfismu.* Ja endomorfisms ir bijekcija, tad to sauc par *automorfismu.*

3.5.2. Apgalvojums. *Ja $f : G \to G'$ ir grupu homomorfisms, tad grupas G neitrālā elementa e attēls $f(e)$ ir grupas G neitrālais elements.*

□ Pieņemsim, ka e' ir grupas G' neitrālais elements, tad

$$e'f(e) = f(e) = f(ee) = f(e)f(e).$$

No šejienes saskaņā ar saīsināšana likumu (Apgalvojums 3.2.10) secinām: $e' = f(e)$. ■

3.5.3. Apgalvojums. *Ja $f : G \to G'$ ir grupu homomorfisms, tad*

$$\forall a \in G \;\; f(a^{-1}) = f(a)^{-1}.$$

□ Pieņemsim, ka e ir grupas G neitrālais elements un e' ir grupas G' neitrālais elements, tad

$$e' = f(e) = f(aa^{-1}) = f(a)f(a^{-1}).$$

No šejienes

$$f(a)^{-1} = f(a)^{-1}e' = f(a)^{-1}f(a)f(a^{-1}) = e'f(a^{-1}) = f(a^{-1}). \quad ■$$

3.5.4. Teorēma. *Ja $f : G \to G'$ ir pusgrupu homomorfisms, bet G ir grupa, tad* $\mathrm{Im} f$ *ir grupa.*

□ (i) Vispirms ievērojam (Apgalvojums 2.9.6), ka Imf ir pusgrupas G' apakšpusgrupa.

(ii) Pieņemsim, ka e ir grupas G neitrālais elements, tad saskaņā ar Apgalvojumu 2.8.4 secināms, ka $f(e)$ ir pusgrupas Imf neitrālais elements.

(iii) Apgalvojums 2.8.6 konstatē, ka

$$\forall a \in G \;\; f(a)^{-1} = f(a^{-1}).$$

Patvaļīgam $x \in \mathrm{Im}f$ eksistē tāds $a \in G$, ka $f(a) = x$. Tā kā $a \in G$, tad $a^{-1} \in G$. No šejienes $f(a^{-1}) \in \mathrm{Im}f$. Līdz ar to $x^{-1} \in \mathrm{Im}f$. ■

3.5.5. Sekas. *Ja $f : G \to G'$ ir pusgrupu epimorfisms, bet G ir grupa, tad G' ir grupa.*

3.5.6. Sekas. *Grupas G faktorpusgrupa $G/\equiv$ pēc kongruences $\equiv$ ir grupa.*

□ Atgādinām (Vingrinājums 2.10.6), ka

$$\pi : G \to G/{\equiv} : x \mapsto [x]$$

ir pusgrupu epimorfisms, tāpēc atliek tikai atsaukties uz iepriekš formulētajām sekām. ■

3.5.7. Definīcija. *Grupas G faktorpusgrupu $G/\equiv$ pēc kongruences $\equiv$ sauc par faktorgrupu.*

Kā mēs tikko konstatējām, tad faktorgrupa ir grupa.

3.5.8. Vingrinājums. Ja $f : G \to G'$ ir grupu homomorfisms, tad Im$f \leq G$.

3.6. Normālas apakšgrupas

Apskatīsim Vingrinājuma 3.4.1(i) modifikāciju.

3.6.1. Vingrinājums. (i) Pieņemsim, ka M — monoīds un K, H ir kopas M apakškopas, tad

$$KH \leftharpoondown \{xy \,|\, x \in K \wedge x \in H\}.$$

Parādīt, ka šī operācija kopā $\mathfrak{P}^+(M) \leftharpoondown \mathfrak{P}(M) \setminus \{\emptyset\}$ definē monoīdu!

Mājiens. Pieņemsim, ka $e \in M$ ir monoīda M neitrālais elements, tad kopa $\{e\}$ ir pusgrupas $\mathfrak{P}^+(M)$ neitrālais elements.

(ii) Pieņemsim, ka G nav triviāla grupa. Parādīt, ka $\mathfrak{P}^+(G)$ nav grupa!

3.6.2. Lemma. *Pieņemsim, ka K un H ir grupas G apakšgrupas.*

$$KH \leq G \Leftrightarrow KH = HK.$$

$\square \Rightarrow \quad HK \overset{S2.7.3}{=} H^{-1}K^{-1} \overset{A3.2.8}{=} (KH)^{-1} \overset{S2.7.3}{=} KH$

$\Leftarrow \quad (KH)(KH) = K(HK)H = K(KH)H = KKHH = KH$ un

$$(KH)^{-1} \overset{A3.2.8}{=} H^{-1}K^{-1} \overset{S2.7.3}{=} HK = KH$$

Tagad atliek tikai atsaukties uz Definīcijām 2.9.1 un 3.3.1, lai secinātu, ka $KH \leq G$. ■

Brīdinājums. Vienādība $KH = HK$ raksturo kopas G apakškopu vienādību, to nevajadzētu jaukt ar elementu komutativitāti. Saprotams, ja grupa G ir Ābela grupa, tad vienādība $KH = HK$ izpildās automātiski.

3.6.3. Lemma. *Pieņemsim, ka H ir grupas G apakšgrupa.*

$$\forall a \in G\ \forall b \in G\ \ (aH)(bH) = abH \Leftrightarrow \forall g \in G\ \ gH = Hg.$$

$\square \Rightarrow$ (i) $gHg^{-1} \subseteq gHg^{-1}H = gg^{-1}H = H$. No šejienes $gH \subseteq Hg$.
(ii) Līdzīgi

$$g^{-1}Hg \subseteq g^{-1}HgH = g^{-1}gH = H.$$

No šejienes $Hg \subseteq gH$.

(iii) Mēs parādījām, ka $gH \subseteq Hg \subseteq gH$. Tātad $gH = Hg$.

$\Leftarrow \quad (aH)(bH) = a(Hb)H = a(bH)H = ab(HH) = abH$ ■

3.6.4. Definīcija. *Grupas G apakšgrupu H sauc par normālu apakšgrupu, ja*

$$\forall g \in G\ \ gH = Hg.$$

Šai situācijā lieto apzīmējumu $H \trianglelefteq G$, un faktorkopu pēc ekvivalences tipa predikāta $\equiv_H^k$ pieraksta kā G/H.

3.6.5. Sekas. *Grupas G apakšgrupa H ir normāla tad un tikai tad, ja*

$$\forall g \in G\ \ gH \subseteq Hg.$$

□ $\Leftarrow$ Pieņemsim, ka $g \in G$, tad $g^{-1} \in G$, un tāpēc $g^{-1}H \subseteq Hg^{-1}$. No šejienes
$$H = gg^{-1}H \subseteq gHg^{-1}$$
un
$$Hg \subseteq gHgg^{-1} = gH.$$
Esam ieguvuši: $gH \subseteq Hg \subseteq gH$. Tātad $gH = Hg$.

$\Rightarrow$ Nepieciešamā nosacījuma pierādījumu atstājam lasītājam kā atjautības vingrinājumu. ■

3.6.6. Vingrinājumi. Grupas G apakšgrupa H ir normāla tad un tikai tad, ja izpildās kaut viens no sekojosiem nosacījumiem:

(i) $\forall g \in G \;\; H = gHg^{-1}$;

(ii) $\forall g \in G \;\; H = gHg^{-1}$;

(iii) $\forall g \in G \;\; H \subseteq gHg^{-1}$;

(iv) $\forall g \in G \;\; gHg^{-1} \subseteq H$.

3.6.7. Sekas. *Ja $H \trianglelefteq G$, tad G/H ir pusgrupas $\mathfrak{P}^+(G)$ ir apakšpusgrupa.*

□ Skatīt Lemmu 3.6.3. ■

3.6.8. Apgalvojums. *Ja $H \trianglelefteq G$, tad G/H ir grupa.*

□ (i) Pieņemsim, ka e ir grupas G neitrālais elements, tad (Lemma 3.6.3)
$$H(aH) = (eH)(aH) = eaH = aH.$$
Tas demonstrē, ka blakusklase H ir pusgrupas G/H kreisais neitrālais elements.

(ii) $(a^{-1}H)(aH) = aa^{-1}H = eH = H$. Tas demonstrē, ka blakusklase $a^{-1}H$ ir blakusklases aH kreisais duālais elements.

(iii) Ņemot vērā (i) un (ii) secināms (Apgalvojums 3.2.2): G/H ir grupa. ■

3.6.9. Piemēri. (i) Komutatīvas grupas jebkura apakšgrupa ir normāla.

(ii) Pieņemsim, ka $A \in SL_n(\mathbb{R})$ un $B \in GL_n(\mathbb{R})$, tad $|A| = 1$ un $|B| \neq 0$. No šejienes (Teorēma 3.1.4)

$$|BAB^{-1}| = |B||A||B^{-1}| = |B||B^{-1}| = |BB^{-1}| = |E| = 1.$$

Tātad $\forall B \in GL_n(\mathbb{R})\ \ B\,SL_n(\mathbb{R})\,B^{-1} \subseteq SL_n(\mathbb{R})$. Saskaņā ar Vingrinājumu 3.6.6 (iv) $SL_n(\mathbb{R}) \trianglelefteq GL_n(\mathbb{R})$.

(iii)

$$\begin{aligned}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} &= \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \neq DL_2(\mathbb{R}).\end{aligned}$$

Tātad $DL_2(\mathbb{R})$ nav pilnās lineārās grupas $GL_2(\mathbb{R})$ normāla apakšgrupa.

3.6.10. Apgalvojums. *Ja $H \trianglelefteq G$, tad $\equiv^k_H$ ir kongruence.*

□ (i) Pieņemsim, ka $x \in G$, tad saskaņā ar Lemmu 3.4.6 $[x]^k_H = xH$. Tas nozīmē, ka

$$a \equiv^k_H b \Leftrightarrow aH = bH$$

visiem grupas G elementiem a un b.

(ii) Pieņemsim, ka $a \equiv^k_H b$ un $g \in G$, tad $gaH = gbH$. Tātad $ga \equiv^k_H gb$.

Ņemsim vērā, ka $H \trianglelefteq G$, tāpēc $Ha = aH = bH = Hb$. No šejienes

$$\begin{aligned} Hag &= Hbg \\ agH &= bgH \\ ag &\equiv^k_H bg. \qquad \blacksquare \end{aligned}$$

3.6.11. Vingrinājums. *Ja $H \trianglelefteq G$, tad $\equiv^l_H$ ir kongruence.*

3.6.12. Teorēma. *Ja $\equiv$ ir kongruence grupā G un $e \in G$ ir neitrālais elements, tad*

$$[e] \trianglelefteq G \qquad \text{un} \qquad G/[e] = G/\equiv.$$

□ (i) Vispirms parādīsim, ka $[e] \leq G$.

Pieņemsim, ka a un b ir blakusklases $[e]$ elementi, tad $a \equiv e$ un $b \equiv e$. No šejienes

$$ab \equiv eb = b \equiv e.$$

Tātad $ab \in [e]$.

Tā kā $a \equiv e$, tad

$$e = a^{-1}a \equiv a^{-1}e = a^{-1}.$$

Tātad $a^{-1} \in [e]$. Tagad atliek tikai atsaukties uz Definīcijām 2.9.1 un 3.3.1, lai secinātu, ka $[e] \leq G$.

(ii) Pieņemsim, ka $x \in [e]$, tad $x \equiv e$; tāpēc

$$gx \equiv ge = g,$$
$$xg \equiv eg = g.$$

No šejienes $xg = gx$; tādēļ $x = xgg^{-1} \equiv gxg^{-1}$. Tas demonstrē, ka

$$gxg^{-1} \in [e], \qquad \text{tātad (skatīt Vingrinājumu 3.6.6 (iv))} \qquad [e] \trianglelefteq G.$$

(iii) Saskaņā ar Apgalvojumu 3.6.10 $\equiv^k_{[e]}$ ir kongruence. Tagad pievēršamies Definīcijai 3.6.4 un Apgalvojumam 3.6.8, lai secinātu, ka

$$G/\equiv^k_{[e]} = G/[e].$$

Atliek parādīt, ka kongruence $\equiv$ ir tā pati kongruence $\equiv^k_{[e]}$.

a) Pieņemsim, ka $x \equiv y$, tad $e = x^{-1}x \equiv x^{-1}y$. Tātad $x^{-1}y \in [e]$. Tas nozīmē (Lemma 3.4.8), ka $x[e] = y[e]$, proti, $x \equiv^k_{[e]} y$.

b) Pieņemsim, ka $x \equiv^k_{[e]} y$, tad $x[e] = y[e]$ jeb $y^{-1}x \in [e]$. Līdz ar to

$$\begin{aligned} y^{-1}x &\equiv e, \\ yy^{-1}x &\equiv ye, \\ x &\equiv y. \quad \blacksquare \end{aligned}$$

Šī teorēma parāda: katrai kongruencei $\equiv$ eksistē tāda grupas G normāla apakšgrupa H, ka $G/\equiv\, = G/H$. Mēs jau iepriekš konstatējām: katrai grupas normālai apakšgrupai H eksistē tāda kongruence $\equiv$, ka $G/\equiv\, = G/H$. Tāpēc parasti lieto nevis pierakstu $G/\equiv$, bet gan pierakstu G/H. Šo faktorgrupu pēc kongruences mēdz saukt par *faktorgrupu G/H pēc normālās apakšgrupas H*.

3.7. Kanoniskais homomorfisms

Ja $f : G \to G'$ ir grupu homomorfisms, tad f ir arī pusgrupu homomorfisms. Saskaņā ar Apgalvojumu 2.10.9 $\mathrm{K\overline{er}}f$ ir kongruence. Šī kongruence nosaka (skatīt Teorēmu 3.6.12) grupas G normālo apakšgrupu

$$[e] = \{x \mid (x, e) \in \mathrm{K\overline{er}}f\} = \{x \mid f(e) = f(x)\} = \{x \mid f(x) = e'\};$$

te $e \in G$ ir grupas G neitrālais elements un $e' \in G'$ ir grupas G' neitrālais elements. Grupu teorijā šo apakšgrupu sauc par *homomorfisma f kodolu* un lieto apzīmējumu $\mathrm{Ker}f$. Līdz ar to $\mathrm{Ker}f \rightleftharpoons [e]$.

Atšķirībā no pusgrupu teorijas, kur par homomorfisma kodolu sauc kongruenci $\mathrm{K\overline{er}}f$, grupu teorijā par homomorfisma kodolu sauc normālo apakšgrupu $\mathrm{Ker}f$.

Līdzīgi kā pusgrupu gadījumā, ja $\equiv$ ir kongruence grupā G, homomorfismu

$$\pi : G \to G/{\equiv} : a \mapsto [a]$$

sauc par *dabīgo* jeb *kanonisko homomorfismu.* Mēs jau atzīmējām (skatīt 73. lappusi), ka šai gadījumā eksistē tāda normāla grupas G apakšgrupa H, ka $G/{\equiv} = G/H$. Tā kā katrai grupas G normālai apakšgrupai H attiecība $\equiv^k_H$ ir kongruence (Apgalvojums 3.6.10), tad attēlojums

$$\pi : G \to G/\mathrm{Ker}f : a \mapsto [a]^k_{\mathrm{Ker}f}$$

ir dabīgais homomorfisms.

3.7.1. Teorēma. *Katram grupu homomorfismam $f : G \to G'$ eksistē viens vienīgs grupu homomorfisms $f_* : G/\mathrm{Ker}f \to G'$, kam diagramma*

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & G' \\ & G/\mathrm{Ker}f \arrow[ur, "f_*"'] & \end{tikzcd}$$

ir komutatīva; turklāt šis homomorfisms f_* ir monomorfisms.

□ Šis rezultāts pierādīts (Teorēma 2.10.10) pusgrupām. Turklāt (Apgalvojums 3.6.8) $G/\mathrm{Ker}f$ ir grupa. ■

3.7.2. Sekas (Izomorfisma teorēma). $G/\mathrm{Ker}f \cong \mathrm{Im}f$

3.7.3. Apgalvojums. *Grupu homomorfisms $f : G \to G'$ ir monomorfisms tad un tikai tad, ja $\mathrm{Ker}f = \{e\}$, kur $e \in G$ ir grupas G neitrālais elements.*

□ ⇒ Pieņemsim, ka $f : G \to G'$ ir monomorfisms, tad f ir gan homomorfisms, gan injekcija.

(i) Tā kā f ir homomorfisms, tad $f(e) = e'$, kur e' ir grupas G' neitrālais elements.

(ii) Tā kā f ir injekcija, tad $\forall a \in G\ (a \neq e \Rightarrow f(a) \neq f(e))$. Līdz ar to $\mathrm{Ker}f = \{e\}$.

⇐ (i) Pieņemsim, ka $f(a) = f(b)$, tad

$$a\mathrm{Ker}f \overset{\mathrm{T3.6.12}}{=} [a] = [b] \overset{\mathrm{T3.6.12}}{=} b\mathrm{Ker}f.$$

No šejienes $ab^{-1} \in \mathrm{Ker}f$.

(ii) Pieņemsim, ka $\mathrm{Ker}f = \{e\}$, tad $ab^{-1} = e$, tāpēc $a = b$. Esam pierādījuši, ka f ir injekcija. ■

3.8. Cikliskas grupas

Pieņemsim, ka $X \subseteq G$, tad

$$\langle X \rangle \leftharpoondown \bigcap_{X \subseteq H \leq G} H,$$

t.i., mēs aplūkojam šķēlumu pa visām grupas G apakšgrupām, kas satur kopu X.

Brīdinājums. Šai situācijā līdzīgi kā pusgrupu gadījumā lieto apzīmējumu $\langle X \rangle$.

3.8.1. Apgalvojums. $\langle X \rangle$ *ir grupa.*

□ Tā kā $G \leq G$, tad vismaz viena grupa apmierina nosacījumu $X \subseteq G$. Tālāk skatīt Apgalvojumu 3.3.5 un Vingrinājumu 3.3.2(ii). ■

3.8.2. Definīcija. *Grupu $\langle X \rangle$ sauc par kopas X ģenerēto apakšgrupu.*

Ja $\langle X\rangle = G$, tad kopu X sauc par grupas G *veidotājkopu.* Kopas X elementus sauc par *veidotājelementiem.* Lai nesarežģītu apzīmējumus, ja $X = \{x_1, x_2, \dots, x_n\}$, parasti uzskata, ka

$$\langle x_1, x_2, \dots, x_n\rangle \leftharpoondown \langle X\rangle.$$

3.8.3. Apgalvojums. *Ja X ir netukša grupas G apaškopa, tad*

$$\langle X\rangle = \{a \mid \exists n \in \mathbb{Z}_+ \, (a = a_1 a_2 \dots a_n \ \wedge \ \forall i \in \overline{1,n}\, (a_i \in X \ \vee \ a_i^{-1} \in X))\}.$$

□ Pieņemsim, ka $\quad X^{-1} \leftharpoondown \{a^{-1} \mid a \in X\} \quad$ un

$$\begin{array}{rcl} H & \leftharpoondown & \{a \mid \exists n \in \mathbb{Z}_+ \, (a = a_1 a_2 \dots a_n \ \wedge \ \forall i \in \overline{1,n} \ \ a_i \in X \cup X^{-1})\} \\ & = & \{ \text{ kopas } \ X \cup X^{-1} \ \text{ elementu galīgi reizinājumi } \}. \end{array}$$

(i) Pieņemsim, ka $a \in X$, tad $a^{-1} \in X^{-1}$. No šejienes $e = aa^{-1} \in H$, t.i., grupas G neitrālais elements arī pieder kopai H.

(ii) Pieņemsim, ka $a = a_1 a_2 \dots a_n$, tad $a^{-1} = a_n^{-1} \dots a_2^{-1} a_1^{-1}$. No šejienes, ja $a \in H$, tad $a^{-1} \in H$.

(iii) Pieņesim, ka $b = b_1 b_2 \dots a_k$, tad $ab = a_1 a_2 \dots a_n b_1 b_2 \dots b_k$. No šejienes, ja $a \in H$ un $b \in H$, tad $ab \in H$.

Tas ļauj secināt, ka H ir grupas G apakšgrupa, kas satur kopu X. Tātad $\langle X\rangle \subseteq H$.

Taču tā kā $\langle X\rangle$ ir grupa un $X \cup X^{-1} \subseteq \langle X\rangle$, tad $H \subseteq \langle X\rangle$. Līdz ar to $H = \langle X\rangle$. ■

3.8.4. Definīcija. *Grupu G sauc par ciklisku grupu, ja*

$$\exists g \in G \, \forall x \in G \, \exists n \in \mathbb{Z} \quad x = g^n.$$

Šai situācijā elementu g sauc par cikliskās grupas G *veidotājelementu.*

3.8.5. Sekas. *Ja g ir cikliskās grupas G veidotālelements, tad $G = \langle g\rangle$.*

□ Skatīt Apgalvojumu 3.8.3. ■

3.8.6. Vingrinājumi. (i) Katra cikliska grupa ir komutatīva.

(ii) Skaitļi -1 un 1 ir grupas $\langle \mathbb{Z}, +\rangle$ veidotājelementi.

3.8.7. Sekas. *$\langle \mathbb{Z}, + \rangle$ ir cikliska grupa.*

Aditīvo pierakstu + parasti lieto, ja grupa G ir komutatīva. Šai gadījumā elementa a duālo elementu mēdz saukt par pretējo un lieto pierakstu $-a$. Tā rezultātā Lemma 3.4.8 iegūst izskatu

$$a + H = b + H \Leftrightarrow a - b \in H.$$

Atgādinam, ka te $H \leq G$, un tā automātiski ir normāla apakšgrupa, jo komutatīvas grupas katra apakšgrupa ir normāla.

Aditīvajā variantā a^m vietā lieto pierakstu ma.

3.8.8. Lemma. *$\mathbb{Z}m \leftharpoondown \{x \in \mathbb{Z} \,|\, m \setminus x\}$ ir grupas $\langle \mathbb{Z}, + \rangle$ apakšgrupa.*

□ Pieņemsim, ka $\quad x \in \mathbb{Z}m \quad$ un $\quad y \in \mathbb{Z}m, \quad$ tad

$$\exists a \in \mathbb{Z}\ x = am \ \wedge\ \exists b \in \mathbb{Z}\ y = bm.$$

No šejienes $x + y = (a + b)m \in \mathbb{Z}m$ un $-x = -am \in \mathbb{Z}m$. ■

3.8.9. Definīcija. *Faktorgrupu $\mathbb{Z}/\mathbb{Z}m$ sauc par rezidiju grupu pēc moduļa m.*

3.8.10. Lemma. $\mathbb{Z}/\mathbb{Z}m = \{a + \mathbb{Z}m \,|\, a \in \overline{0, m-1}\}$.

□ Ja $0 \leq a < b < m$, tad $b - a \notin \mathbb{Z}m$, tāpēc $a + \mathbb{Z} \neq b + \mathbb{Z}$. Ja turpretī a ir patvaļīgs vesels skaitlis, tad eksistē tādi veseli skaitļi q un r, ka

$$a = mq + r \qquad \text{un} \qquad r \in \overline{0, m-1}.$$

No šejienes

$$a + \mathbb{Z}m = r + mq + \mathbb{Z}m = (r + \mathbb{Z}m) + (mq\mathbb{Z}m) = r + \mathbb{Z}m. \quad ■$$

Parasti kreisās blakusklases $a + \mathbb{Z}m$ apzīmēšamai lieto pierakstu $[a]$ un $\mathbb{Z}/\mathbb{Z}m$ apzīmēšanai lieto arī īsāku pierakstu $\mathbb{Z}_m \leftharpoondown \mathbb{Z}/\mathbb{Z}m$. Skaitļu teorijā pierāda, ka $\langle \mathbb{Z}_m, + \rangle$ ir komutatīva grupa. Mēs to izdarījām nedaudz citādāk.

3.8.11. Vingrinājums. Blakusklase [1] ir grupas $\langle \mathbb{Z}_m, + \rangle$ veidotājelements.

3.8.12. Sekas. *Grupa* $\langle \mathbb{Z}_m, +\rangle$ *ir cikliska.*

3.8.13. Lemma. *Ja* H *ir netriviāla grupas* $\langle \mathbb{Z}, +\rangle$ *apakšgrupa, tad*

$$\exists m \in \mathbb{Z}_+ \; H = \mathbb{Z}m.$$

$\square$ (i) Pieņemsim, ka $\{0\} \neq H \leq \mathbb{Z}$, tad H satur kādu pozitīvu skaitli. Pieņemsim, ka m ir mazākais pozitīvais skaitlis, kas pieder H, tad $\mathbb{Z}m \subseteq H$.

(ii) Pieņemsim, ka $a \in H$, tad tad eksistē tādi veseli skaitļi q un r, ka

$$a = mq + r \qquad \text{un} \qquad r \in \overline{0, m-1}.$$

No šejienes $r = a - mq \in H$.

Ja pieņem, ka $r \neq 0$, tad tas ir pretrunā ar m izvēli, jo m ir mazākais pozitīvais kopas H skaitlis. Atliek tikai viena iespēja, proti, $r = 0$, t.i., $a - mq \in \mathbb{Z}m$. Tātad $H \subseteq \mathbb{Z}m$.

(iii) Mēs parādījām, ka $\mathbb{Z}m \subseteq H \subseteq \mathbb{Z}m$. Tātad $H = \mathbb{Z}m$. $\blacksquare$

Turpmākajam mums nepieciešams viens rezultāts no skaitļu teorijas.

3.8.14. Teorēma. *Ja* $\mathrm{ld}(a, b) = d$*, tad* $\exists x \in \mathbb{Z} \, \exists y \in \mathbb{Z} \quad ax + by = d$.

Lasītājs šīs teorēmas pierādījumu var atrsat gandrīz katrā grāmatā, kas aplūko elementārās skaitļu teorijas jautājumus.

3.8.15. Teorēma. *Blakusklase* $[a]$ *ir grupas* $\langle \mathbb{Z}_m, +\rangle$ *veidotājelements tad un tikai tad, ja* $\mathrm{ld}(a, m) = 1$.

$\square$ $\Rightarrow$ Pieņemsim, ka blakusklase $[a]$ ir grupas $\mathbb{Z}_m$ veidotājelements un $\mathrm{ld}(a, m) = d$, tad

$$\exists x \in \mathbb{Z}_+ \; a = xd \;\wedge\; \exists y \in \mathbb{Z}_+ \; m = yd.$$

No šejienes $\quad [ay] = [xdy] = [xm] = [0]$.

Tagad apskatam klases

$$[0], [a], [2a], \ldots, [(y-1)a].$$

Pieņemam, ka c ir patvaļīgs kopas $\mathbb{Z}$ skaitlis, tad eksistē tādi veseli skaitļi q un r, ka

$$c = yq + r, \qquad \text{kur} \qquad r \in \overline{0, y-1}.$$

No šejienes

$$[ac] = [a(yq + r)] = [ayq + ar] = [ayq] + [ar] = [0q] + [ar] = [ar].$$

Līdz ar to

$$\mathbb{Z}_m = \{[0], [a], [2a], \ldots, [(y-1)a]\}.$$

Tas iespējams tikai tad, ja $y = m$. Tātad $d = 1$, jo $m = yd$.

$\Leftarrow$ Pieņemsim, ka $\mathrm{ld}(a, m) = 1$, tad saskaņā ar Teorēmu 3.8.14

$$\exists x \in \mathbb{Z}\, \exists y \in \mathbb{Z} \quad ax + my = 1.$$

No šejienes $[1] = [ax+my] = [ay]+[my] = [ax]+[0] = [ax]$. Ja $[c] \in \mathbb{Z}_m$, tad

$$[c] = c[1] = c[ax] = cx[a],$$

t.i., $[a]$ ir grupas $\mathbb{Z}_m$ veidotājelements. ■

3.8.16. Teorēma. *Katra cikliska grupa ir izomorfa veselo skaitļu aditīvai grupai $\langle \mathbb{Z}, + \rangle$, vai arī kādai rezidiju grupai pēc moduļa m.*

□ Pieņemsim, ka $G = \langle g \rangle$. Apskatīsim attēlojumu

$$f : \mathbb{Z} \to G : n \mapsto a^n.$$

Ja reiz G ir cikliska, tad f — sirjekcija.

(i) $f(m + n) = g^{m+n} \overset{\mathrm{A3.2.6}}{=} g^m g^n = f(m)f(n)$. Tātad f ir grupu homomorfisms.

(ii) Ja $\mathrm{Ker} f = \{0\}$, tad f ir monomorfisms (Apgalvojums 3.7.3). Tā kā f ir epimorfisms, tad no šejienes izriet, ka f ir izomorfisms.

(iii) Izomorfisma teorema 6.4.10 ļauj secināt, ka $G \cong \mathbb{Z}/\mathrm{Ker} f$. Ja $\mathrm{Ker} f \neq \{0\}$, tad atsaucoties uz Lemmu 3.8.13 iegūstam: $\mathrm{Ker} f = \mathbb{Z}m$. Mēs jau zinam, ka $\mathbb{Z}/\mathbb{Z}m = \mathbb{Z}_m$. ■

Ja a ir grupas G elements, tad $\forall n \in \mathbb{Z}\ a^n \in G$. Līdz ar to $\langle a \rangle \leq G$.

3.8.17. Definīcija. *Pieņemsim, ka a ir grupas G elements, tad apkšgrupas $\langle a \rangle$ kārtu sauc par elementa a kārtu.*

Parasti šai situācijā lieto apzīmējumu $o(a)$, proti, $o(a) \leftharpoondown\!\!\!\!\!\! = |\langle a \rangle|$.

3.8.18. Apgalvojums. *Ja grupas G elementa a kārta ir naturāls skaitlis, tad*

$$\langle a\rangle = \{a, a^2, \ldots, a^{o(a)}\} \qquad \text{un} \qquad a^{o(a)} = e,$$

kur e ir grupas G neitrālais elements.

□ Ja $a = e$, tad apgalvojums ir spēkā, tāpēc turpmākajā pierādījumā pieņemsim, ka $a \neq e$.

(i) Ņemam vērā, ka

$$\{a, a^2, \ldots, a^{k+1}\} \subseteq \langle a\rangle$$

jebkuram naturālam k. Pieņemsim, ka $o(a) = k$, tad saskaņā ar Dirihlē principu eksistē tādi naturāli skaitļi m un n, ka $a^m = a^n$, kur $1 \leq n < m \leq k+1$. No šejienes $a^{m-n} = e$. Tātad eksistē tāds naturāls skaitlis $\varkappa \in \overline{1,k}$, ka $a^{\varkappa} = e$.

(ii) Pieņemsim, ka

$$K \leftrightharpoons \{a, a^2, \ldots, a^{\varkappa}\},$$

tad $|K| \leq \varkappa \leq k$ un $K \subseteq \langle a\rangle$.

(iii) Pieņemsim, ka $x \in \langle a\rangle$, tad saskaņā ar $\langle a\rangle$ definīciju eksistē tāds vesels skaitlis u, ka $x = a^u$. No šejienes: eksistē tādi veseli skaitļi q un r, ka

$$u = \varkappa q + r \qquad \text{un} \qquad 0 \leq r < \varkappa.$$

Tā rezultātā

$$x = a^u = a^{\varkappa q + r} = a^{\varkappa q}a^r = (a^{\varkappa})^q a^r = e^q a^r = a^r \in K.$$

Līdz ar to $\langle a\rangle \subseteq K$.

(iv) Esam pierādījuši, ka $K \subseteq \langle a\rangle \subseteq K$. Tātad $K = \langle a\rangle$. Atliek tikai ņemt vērā visu iepriekš konstatēto, proti,

$$k \geq \varkappa \geq |K| = |\langle a\rangle| = o(a) = k.$$

Līdz ar to $\varkappa = k = o(a)$. Esam parādījuši, ka $a^{o(a)} = e$. ■

3.8.19. Sekas. *Ja $a \in G$ un grupas G kārta ir n, tad $a^n = e$, kur e ir grupas G neitrālais elements.*

□ Tā kā $\langle a\rangle \leq G$, tad (Sekas 3.4.18)

$$o(a) = |\langle a\rangle| \diagdown |G| = n.$$

Līdz ar to eksistē tāds naturāls skaitlis m, ka $m\, o(a) = n$. No šejienes

$$a^n = a^{o(a)m} = (a^{o(a)})^m = e^m = e. \quad ■$$

3.9. Kelī teorēma

3.9.1. Teorēma (Kelī). *Katra grupa G ir izomorfa kādai grupas $\mathfrak{S}(G)$ apakšgrupai.*

$\square$ (i) Katram $a \in G$ attēlojums $T'_a : x \mapsto xa$ ir kopas G substitūcija (Vingrinajums 2.7.5). Līdz ar to attēlojums

$$\varphi : a \mapsto T'_a$$

ir kopas G attēlojums kopā $\mathfrak{S}(G)$.

(ii) Pieņemsim, ka x, a un b ir kopas G elementi, tad

$$x(\varphi(a)\varphi(b)) = (x\varphi(a))\varphi(b) = xT'_aT'_b = xaT'_b = xab = xT'_{ab} = x\varphi(ab).$$

Tātad $\varphi(a)\varphi(b) = \varphi(ab)$, t.i., $\varphi : G \to \mathfrak{S}(G)$ ir grupu homomorfisms.

(iii) Pieņemsim, ka e ir grupas G neitrālais elements un $\varphi(a) = \varphi(b)$, tad

$$a = ea = eT'_a = e\varphi(a) = e\varphi(b) = eT'_b = eb = b.$$

Tātad $\varphi : G \to \mathfrak{S}(G)$ ir injekcija. Līdz ar to $G \cong \mathrm{Im}\varphi \leq \mathfrak{S}(G)$. Apmulsuma gadījumā skatīt Vingrinājumu 3.5.8. $\blacksquare$

Kelī teorēma principiālā nozīmē parāda, ka visu grupu teoriju var reducēt uz simetrisko grupu teoriju, taču grupas $\mathfrak{S}_n$ kārta jau pie maziem n ir liela, un tādēļ tās struktūra kļūst nepārskatāma.

3.9.2. Vingrinājums. $|\mathfrak{S}_n| = n!$

3.10. Neatkarīgi cikli

3.10.1. Definīcija. *Substitūciju*

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$$

sauc par ciklu $(i_1 i_2 \dots i_k)$, ja visi i_s ir dažādi un

$$\sigma(i) \quad = \quad \begin{cases} i, & \text{ja} \quad i \neq \{i_1, i_2, \dots, i_k\}, \\ i_{s+1} & \text{ja} \quad i = i_s \text{ un } s \neq k, \\ i_1 & \text{ja} \quad i = i_k. \end{cases}$$

Vienošanās. Katram ciklam $\varrho = (i_1 i_2 \dots i_k)$ mēs piekārtosim kopu $\bar{\varrho} \leftharpoondown \{i_1, i_2, \dots, i_k\}$.

3.10.2. Piemērs. Grupā $\mathfrak{S}_6$

$$(153) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 1 & 4 & 3 & 6 \end{pmatrix}$$

3.10.3. Definīcija. *Ciklu $(i_1 i_2)$ sauc par transpozīciju.*

3.10.4. Piemērs. Grupā $\mathfrak{S}_6$

$$(35) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 4 & 3 & 6 \end{pmatrix}$$

3.10.5. Definīcija. *Grupas $\mathfrak{S}_n$ ciklus $(i_1 i_2 \dots i_k)$, $(j_1 j_2 \dots j_m)$ sauc par neatkarīgiem cikliem, ja*

$$\{i_1, i_2, \dots, i_k\} \cap \{j_1, j_2, \dots, j_m\} = \emptyset.$$

3.10.6. Piemērs. Grupā $\mathfrak{S}_6$ cikli (135), (35) ir atkarīgi, bet cikli (126), (35) ir neatkarīgi.

3.10.7. Apgalvojums. *Ja ϱ un σ ir neatkarīgi cikli, tad $\varrho\sigma = \sigma\varrho$.*

□ (i) Pieņemsim, ka

$$\varrho = (i_1 i_2 \dots i_k) \qquad \text{un} \qquad \sigma = (j_1 j_2 \dots j_m),$$

tad

$$\bar{\varrho} = \{i_1, i_2, \dots, i_k\} \qquad \text{un} \qquad \bar{\sigma} = \{j_1, j_2, \dots, j_m\}.$$

(ii) Ja $i \in \bar{\varrho}$, tad $i\varrho \in \bar{\varrho} \wedge i \notin \bar{\sigma} \wedge i\varrho \notin \bar{\sigma}$.
Līdzīgi, ja $i \in \bar{\sigma}$, tad $i\sigma \in \bar{\sigma} \wedge i \notin \bar{\varrho} \wedge i\sigma \notin \bar{\varrho}$. Tātad

$$i(\varrho\sigma) = (i\varrho)\sigma = \left\{ \begin{array}{lll} i, & \text{ja} & i \notin \bar{\varrho} \cup \bar{\sigma}, \\ i\varrho & \text{ja} & i \in \bar{\varrho}, \\ i\sigma & \text{ja} & i \in \bar{\sigma}. \end{array} \right\} = (i\sigma)\varrho = i(\sigma\varrho). \quad \blacksquare$$

3.10.8. Teorēma. *Ja $\sigma_1, \sigma_2, \dots, \sigma_k$ ir pa pāriem neatkarīgi grupas $\mathfrak{S}_n$ cikli, tad*

$$\sigma_1 \sigma_2 \dots \sigma_k = \sigma_{\pi(1)} \sigma_{\pi(2)} \dots \sigma_{\pi(k)}$$

jebkurai substitūcijai $\pi \in \mathfrak{S}_k$.

$\square$ Skatīt Apgalvojumus 3.10.7 un 2.5.3 $\blacksquare$

Pieņemsim, ka $\tau \in \mathfrak{S}_n$ un $i \in \overline{1,n}$. Apskatīsim kopu

$$\{i\tau^0, i\tau^1, i\tau^2, \ldots, i\tau^n\}$$

kur $i\tau^0 \leftharpoondown i$ un $i\tau^{k+1} \leftharpoondown (i\tau^k)\tau$. Tā kā $\forall k\ i\tau^k \in \overline{1,n}$, tad saskaņā ar Dirihlē principu eksistē tādi skaitļi m un $\varkappa$, ka $\varkappa > 0$ un $i\tau^m = i\tau^{m+\varkappa}$. No šejienes $i\tau^\varkappa = i$. Pieņemsim, ka $\varkappa$ ir pats mazākais veselais pozitīvais skaitlis, kuram piemīt šī īpašība, tad elementi

$$i\tau^0, i\tau^1, i\tau^2, \ldots, i\tau^{\varkappa-1}$$

ir dažādi. Pretējā gadījumā eksistē tādi veseli skaitļi $\bar{m}$ un $\bar{\varkappa}$, ka $i\tau^{\bar{m}} = i\tau^{\bar{m}+\bar{\varkappa}}$, $0 \leq \bar{m} < \bar{m}+\bar{\varkappa} \leq \varkappa$ un $0 < \bar{\varkappa} < \varkappa$. No šejienes $i = i\tau^{\bar{\varkappa}}$, kas ir pretrunā ar $\varkappa$ izvēli, proti, $\varkappa$ ir mazākais veselais pozitīvais skaitlis, kuram izpildās īpašība $i\tau^\varkappa = i$.

3.10.9. Definīcija. *Ciklu* $(i\ i\tau\ i\tau^2 \ldots i\tau^{\varkappa-1})$ *sauc par elementa* i *ģenerēto substitūcijas* τ *orbītu.*

3.10.10. Lemma. *Ja* $\sigma = (i_1\ i_2\ \ldots\ i_{k-1}\ i_k)$ *ir elementa* i_1 *ģenerētā substitūcijas* τ *orbīta, tad*

$$\forall s \in \mathbb{Z} \quad \sigma = (\tau^s i_1\ \tau^s i_2\ \ldots\ \tau^s i_{k-1}\ \tau^s i_k)$$

$\square$ (i) Ja $s = 1$, tad

$$\begin{aligned}(\tau^s i_1\ \tau^s i_2\ \ldots\ \tau^s i_{k-1}\ \tau^s i_k) &= (\tau i_1\ \tau i_2\ \ldots\ \tau i_{k-1}\ \tau i_k)\\ &= (i_2\ i_3\ \ldots\ i_k\ i_1)\\ &= (i_1\ i_2\ \ldots\ i_{k-1}\ i_k) = \sigma.\end{aligned}$$

Tālākie spriedumi induktīvi pieņemot, ka

$$\sigma = (\tau^s i_1\ \tau^s i_2\ \ldots\ \tau^s i_{k-1}\ \tau^s i_k).$$

No šejienes

$$\begin{aligned}(\tau^{s+1} i_1\ \ldots\ \tau^{s+1} i_{k-1}\ \tau^{s+1} i_k) &= (\tau^s\tau i_1\ \ldots\ \tau^s\tau i_{k-1}\ \tau^s\tau i_k)\\ &= (\tau^s i_2\ \ldots\ \tau^s i_k\ \tau^s i_1)\\ &= (\tau^s i_1\ \tau^s i_2\ \ldots\ \tau^s i_k) = \sigma.\end{aligned}$$

(ii) Ja $s = -1$, tad

$$\begin{aligned}(\tau^s i_1\, \tau^s i_2 \,\ldots\, \tau^s i_{k-1}\, \tau^s i_k) &= (\tau^{-1} i_1\, \tau^{-1} i_2 \,\ldots\, \tau^{-1} i_{k-1}\, \tau^{-1} i_k)\\ &= (i_k\, i_1 \,\ldots\, i_{k-2}\, i_{k-1})\\ &= (i_1\, i_2 \,\ldots\, i_{k-1}\, i_k) = \sigma.\end{aligned}$$

Tālākie spriedumi induktīvi pieņemot, ka

$$\sigma = (\tau^{-s} i_1\, \tau^{-s} i_2 \,\ldots\, \tau^{-s} i_{k-1}\, \tau^{-s} i_k).$$

No šejienes

$$\begin{aligned}(\tau^{-s-1} i_1\;\; \tau^{-s-1} i_2 \,\ldots\, \tau^{-s-1} i_k) &= (\tau^{-s}\tau^{-1} i_1\;\; \tau^{-s}\tau^{-1} i_2 \,\ldots\, \tau^{-s}\tau^{-1} i_k)\\ &= (\tau^{-s} i_k\;\; \tau^{-s} i_1 \,\ldots\, \tau^{-s} i_{k-1})\\ &= (\tau^{-s} i_1\, \tau^{-s} i_2 \,\ldots\, \tau^{-s} i_k) = \sigma. \quad \blacksquare\end{aligned}$$

3.10.11. Vingrinājums. Ja $\sigma = (i\; i\tau\; i\tau^2 \ldots i\tau^{\varkappa-1})$ ir elementa i ģenerētā substitūcijas τ orbīta, tad

$$\forall k \in \mathbb{Z}\, \exists r \in \overline{0, \varkappa - 1}\; i\tau^k = i\tau^r \in \bar{\sigma}.$$

Mēs teiksim, ka σ ir *substitūcijas* $\tau \in \mathfrak{S}_n$ *orbīta*, ja eksistē tāds $i \in \overline{1, n}$, ka σ ir elementa i ģenerētā substitūcijas τ orbīta.

3.10.12. Lemma. *Substitūcijas $\tau \in \mathfrak{S}_n$ divas orbītas ϱ un σ sakrīt, vai arī tās ir neatkarīgas.*

□ Pieņemsim, ka $\sigma = (i\, i\tau \,\ldots\, i\tau^k)$, $\varrho = (j\, j\tau \,\ldots\, j\tau^m)$ un $d \in \bar{\sigma} \cap \bar{\varrho}$, tad eksistē tādi α un β, ka $d = i\tau^\alpha = j\tau^\beta$. No šejienes

$$i = j\tau^\beta\tau^{-\alpha} = j\tau^{\beta-\alpha} \overset{\text{V3.10.11}}{\in} \bar{\varrho}.$$

Tā rezultātā

$$\forall s \in \overline{1, k} \quad i\tau^s = j\tau^{\beta-\alpha}\tau^s = j\tau^{\beta-\alpha+s} \overset{\text{V3.10.11}}{\in} \bar{\varrho}.$$

Tātad $\bar{\sigma} \subseteq \bar{\varrho}$.

Līdzīgi

$$j = i\tau^\alpha\tau^{-\beta} = i\tau^{\alpha-\beta} \overset{\text{V3.10.11}}{\in} \bar{\sigma}$$

un

$$\forall s \in \overline{1,m} \quad j\tau^s = i\tau^{\alpha-\beta}\tau^s = i\tau^{\alpha-\beta+s} \overset{\mathrm{V3.10.11}}{\in} \bar{\sigma}.$$

Tātad $\bar{\varrho} \subseteq \bar{\sigma}$.

Visu savelkot kopā secināms: $\bar{\sigma} \subseteq \bar{\varrho} \subseteq \bar{\sigma}$, t.i., $\bar{\sigma} = \bar{\varrho}$. Tas iespējams tikai tad, ja $k = m$. Tā rezultātā

$$\begin{aligned} \varrho &= (j\, j\tau\, \ldots\, j\tau^m) = (j\, j\tau\, \ldots\, j\tau^k) \\ &= (i\tau^{\alpha-\beta}\ \ i\tau^{\alpha-\beta+1} \ldots\ i\tau^{\alpha-\beta+k}) \overset{\mathrm{L3.10.10}}{=} \sigma. \quad \blacksquare \end{aligned}$$

3.10.13. Lemma. *Ja σ ir elementa i ģenerēta substitūcijas $\tau \in \mathfrak{S}_n$ orbīta, tad*

$$\forall j \in \bar{\sigma} \quad j\tau = j\sigma.$$

$\square$ Pieņemsim, ka $\sigma = (i\ i\tau\ \ldots\ i\tau^k)$, tad $j = i\tau^r$, kur $0 \leq r \leq k$. No šejienes

$$j\sigma = (i\tau^r)\sigma = i\tau^{r+1} = (i\tau^r)\tau = j\tau. \quad \blacksquare$$

3.10.14. Teorēma. *Katru substitūciju $\tau \in \mathfrak{S}_n$ var uzrakstīt kā neatkarīgu ciklu reizinājumu.*

$\square$ Pieņemsim, ka $\sigma_1, \sigma_2, \ldots, \sigma_m$ ir visas iespējamās substitūcijas τ orbītas, kas satur vismaz 2 elementus, proti, $\forall k \in \overline{1,m}\ \ |\bar{\sigma}_k| > 1$. Ja

$$i \notin \bigcup_{k=1}^{m} \bar{\sigma}_k,$$

tad $\forall k\ \ i\sigma_k = i$. No šejienes

$$i\sigma_1\sigma_2\ldots\sigma_m = i = i\tau.$$

Pretējā gadījumā saskaņā ar Lemmu 3.10.12 $\quad \exists! s\ i \in \bar{\sigma}_s$. Tātad

$$i \notin \bigcup_{k=1}^{s-1} \bar{\sigma}_k,$$

un tāpēc $i\sigma_1 = i\sigma_2 = \ldots = i\sigma_{s-1} = i$.

No Lemmas 3.10.13 secināms, ka $\quad i\tau = i\sigma_s \in \bar{\sigma}_s$. Līdz ar to

$$i\tau \notin \bigcup_{k=s+1}^{m} \bar{\sigma}_k,$$

un tāpēc $(i\tau)\sigma_{s+1} = (i\tau)\sigma_{s+2} = \ldots = (i\tau)\sigma_m = i\tau$.

Visu savelkot kopā secināms:

$$i\sigma_1 \ldots \sigma_m = i\sigma_s\sigma_{s+1} \ldots \sigma_m = (i\sigma_s)\sigma_{s+1} \ldots \sigma_m = (i\tau)\sigma_{s+1} \ldots \sigma_m = i\tau.$$

Līdz ar to parādīts, ka

$$\forall i \quad i\tau = i(\sigma_1\sigma_2 \ldots \sigma_m),$$

t.i., $\tau = \sigma_1\sigma_2 \ldots \sigma_m$.

Visbeidzot atsaucoties uz Lemmu 3.10.12 secināms: $\sigma_1, \sigma_2, \ldots, \sigma_m$ ir neatkarīgi cikli. ■

3.10.15. Piemērs.

$$\mathfrak{S}_3 = \{e, (12), (13), (23), (123), (132)\}$$

3.10.16. Lemma. *Ja $\tau = \tau_1\tau_2 \ldots \tau_m$ ir neatkarīgu ciklu reizinājums, tad visi cikli τ_i ir substitūcijas τ orbītas.*

□ Pieņemsim, ka $\tau = \tau_1\tau_2 \ldots \tau_m$ ir neatkarīgu ciklu reizinājums un $\tau_i = (i_1\ i_2\ \ldots\ i_k)$, tad

$$\forall s \in \overline{1, k-1} \quad i_s\tau = i_s\tau_i = i_{s+1}$$

un $i_k\tau = i_k\tau_i = i_1$. Tā rezultātā $\tau_i = (i_1\ i_1\tau\ \ldots\ i_1\tau^{k-1})$. ■

3.10.17. Teorēma. *Katru substitūciju ar precizitāti līdz reizinātāju secībai var uzrakstīt vienā vienīgā veidā kā neatkarīgu ciklu reizinājumu, kur visi cikli satur vismaz 2 elementus.*

□ Saskaņā ar Teorēmu 3.10.14 katru substitūciju $\tau \in \mathfrak{S}_n$ var uzrakstīt kā neatkarīgu ciklu reizinājumu $\tau = \tau_1\tau_2 \ldots \tau_m$. Pieņemsim, ka šai reizinājumā visi cikli satur vismaz 2 elementus. Tos ciklus, kas satur tikai 1 elementu šai sarakstā var neiekļaut (no tā reizinājums nemainās).

Pieņemsim, ka $\tau = \sigma_1\sigma_2 \ldots \sigma_k$ ir kāds cits neatkarīgu ciklu reizinājums, piedevām visi cikli satur vismaz 2 elementus. Konkrētības labad pieņemsim, ka $k \leq m$.

Saskaņā ar Lemmu 3.10.16 visi cikli ir orbītas. Pieņemsim, ka

$$\sigma_1 = (j\ j\tau\ \ldots\ j\tau^{\omega}).$$

Tā kā elementa j ģenerētā substitūcijas τ orbīta nav vienelementīga, tad eksistē tada orbīta τ_s, ka $j \in \bar{\tau}_s$. Neatkarīgi cikli komutē (Teorēma 3.10.8), tāpēc var pieņemt, ka tieši $\bar{\tau}_1$ satur elementu j. Līdz ar to $\tau_1 = \sigma_1$ un $\tau_1\tau_2 \dots \tau_m = \sigma_1\sigma_2 \dots \sigma_k$. Tagad atsaucoties uz saīsināšanas likumu (Apgalvojums 3.2.10) secinām:

$$\tau_2 \dots \tau_m = \sigma_2 \dots \sigma_k.$$

Šos spriedumus atkārtojot k rezes iegūstam $\tau_{m-k} \dots \tau_{m-1}\tau_m = e$, kur e ir grupas $\mathfrak{S}_n$ neitrālais elememts, t.i., identiskais attēlojums $\mathbb{I}$.

Visbeidzot atliek konstatēt, ka $k = m$. Pieņemsim pretējo, proti, $k < m$, tad τ_m kā cikls satur vismaz 2 elementus, t.i., ja $i \in \tau_m$, tad $i\tau_m \neq i$. No šejienes, ņemot vērā, ka visi cikli ir neatkarīgi, iegūstam

$$i\mathbb{I} = i\tau_{m-k} \dots \tau_{m-1}\tau_m = i\tau_m \neq i.$$

Pretruna! ■

3.10.18. Definīcija. *Skaitli k sauc par substitūcijas τ neatkarīgo ciklu skaitu, ja τ uzrakstāma kā k neatkarīgu ciklu reizinājums.*

3.11. Maiņzīmju grupa

3.11.1. Definīcija. *Saka, ka pāris $u < v$ substitūcijā*

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

rada inversiju, ja $i_u > i_v$.

Konkrētajā gadījumā mēdz teikt arī, ka elements (var teikt arī skaitlis) i_u rada inversiju ar elementu i_v. Pretējā gadījumā saka, ka pāris $u < v$ nerada inversiju, t.i., ja $i_u < i_v$. Šai situācijā mēdz teikt arī, ka elements i_u nerada inversiju ar elementu i_v.

Pieņemsim, ka $\varkappa$ — pāru $u < v$ skaits, kas substitūcijā σ rada inversiju, tad skaitli $\varkappa$ sauc par *inversiju skaitu* substitūcijā σ, bet $(-1)^{\varkappa}$ sauc par *substitūcijas σ zīmi* un lieto apzīmējumu $\mathrm{sgn}(\sigma)$.

Tātad $\mathrm{sgn}(\sigma) = (-1)^{\varkappa}$. Ja $\mathrm{sgn}(\sigma) = 1$, tad σ sauc par *pāra* substitūciju, ja turpretī $\mathrm{sgn}(\sigma) = -1$, tad σ sauc par *nepāra* substitūciju.

3.11.2. Piemērs. Pāris $1 < 2$ substitūcijā

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ i_1 & i_2 & i_3 & i_4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

rada inversiju, jo $3 > 1$. Šoreiz $u = 1$, $v = 2$, tāpēc $(i_u, i_v) = (i_1, i_2) = (3, 1)$. Vēl tikai pāris $1 < 3$ substitūcijā σ rada inversiju, tādēļ σ ir pāra substitūcija.

3.11.3. Lemma. *Pāris $u < v$ substitūcijā σ rada inversiju tad un tikai tad, ja pāris $\sigma(v) < \sigma(u)$ inversajā substitūcijā σ^{-1} rada inversiju.*

$\square$ $\Rightarrow$ Pieņemsim, ka pāris $u < v$ substitūcijā σ rada inversiju, tad $\sigma(u) > \sigma(v)$. Tā kā $\sigma^{-1}(\sigma(v)) = v > u = \sigma^{-1}(\sigma(u))$, tad pāris $\sigma(v) < \sigma(u)$ substitūcijā σ^{-1} rada inversiju.

$\Leftarrow$ Pieņemsim, ka pāris $\sigma(v) < \sigma(u)$ inversajā substitūcijā σ^{-1} rada inversiju, tad $v = \sigma^{-1}(\sigma(v)) > \sigma^{-1}(\sigma(u)) = u$. Tātad $u < v$ un $\sigma(u) > \sigma(v)$, t.i., pāris $u < v$ substitūcijā σ rada inversiju. $\blacksquare$

3.11.4. Sekas. $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$.

$\square$ Pieņemsim, ka $\varkappa$ ir inversiju skaits substitūcijā σ, tad saskaņā ar Lemmu 3.11.3 arī substitūcijā σ^{-1} ir tikpat daudz inversiju. No šejienes $\operatorname{sgn}(\sigma) = (-1)^{\varkappa} = \operatorname{sgn}(\sigma^{-1})$. $\blacksquare$

3.11.5. Definīcija. *Saka, ka substitūcija τ iegūta no substitūcijas σ,* mainot vietām *k-to ar s-to* elementu*, ja $\tau(k) = \sigma(s)$, $\tau(s) = \sigma(k)$, toties visiem pārējiem i substitūciju vērtības sakrīt, t.i., $\tau(i) = \sigma(i)$.*

Speciālā gadījumā, ja $|k - s| = 1$, saka, ka τ iegūta no σ, *mainot vietām blakusesošos elementus.*

3.11.6. Piemērs. Substitūcija

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \quad \text{iegūta no} \quad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix},$$

mainot vietām blakusesošos elementus, proti, otro ar trešo. Skaitlis 3 ar skaitli 2 rada inversiju gan substitūcijā σ, gan substitūcijā τ. Tāpat gan skaitlis 2, gan 3, gan 4 ar skaitli 1 rada inversiju gan substitūcijā σ, gan substitūcijā τ, turpretī skaitlis 4 ar skaitli 2 rada inversiju tikai substitūcijā τ. Tā rezultātā substitūcijā σ inversiju skaits atšķiras no inversiju skaita substitūcijā τ tieši par skaitli 1, un tāpēc $\operatorname{sgn}(\tau) = -\operatorname{sgn}(\sigma)$.

3.11.7. Lemma. *Ja substitūcija τ iegūta no σ, mainot vietām blakus-esošos elementus, tad* $\operatorname{sgn}(\tau) = -\operatorname{sgn}(\sigma)$.

□ Mēs teiksim, ka elements $\sigma(u)$ substitūcijā σ atrodas pirms elementa $\sigma(v)$, ja $u < v$. Tikai šādā gadījumā ir saturīgi uzdot jautājumu:

— Vai elements $\sigma(u)$ rada inversiju ar elementu $\sigma(v)$?

Konkrētības labad pieņemsim, ka

$$\sigma = \begin{pmatrix} 1 & \dots & k-1 & k & k+1 & k+2 & \dots & n \\ i_1 & \dots & i_{k-1} & i_k & i_{k+1} & i_{k+2} & \dots & i_n \end{pmatrix},$$

bet

$$\tau = \begin{pmatrix} 1 & \dots & k-1 & k & k+1 & k+2 & \dots & n \\ i_1 & \dots & i_{k-1} & i_{k+1} & i_k & i_{k+2} & \dots & i_n \end{pmatrix}.$$

(i) Pieņemsim, ka nedz u, nedz v nav neviens no skaitļiem k, $k+1$, tad $\sigma(u) = i_u = \tau(u)$ un $\sigma(v) = i_v = \tau(v)$. Tātad šai situācijā pāris $u < v$ rada inversiju substitūcijā σ tad un tikai tad, ja tas rada arī inversiju substitūcijā τ.

(ii) Pieņemsim, ka elements i_u substitūcijā σ atrodas pirms elementa i_v un tikai viens no skaitļiem u vai v ir kopas $\{k,\, k+1\}$ elements, tad i_u arī substitūcijā τ atrodas pirms i_v. Tā rezultātā i_u substitūcijā σ rada inversiju ar i_v tad un tikai tad, ja i_u rada inversiju ar i_v arī substitūcijā τ.

(iii) Pieņemsim, ka $u = k$, bet $v = k+1$. Ja pāris $k < k+1$ substitūcijā σ rada inversiju, tad $i_k > i_{k+1}$. Tā kā $\tau(k) = i_{k+1}$ un $\tau(k+1) = i_k$, tad pāris $k < k+1$ nerada substitūcijā τ inversiju. Ja turpretī pāris $k < k+1$ nerada substitūcijā σ inversiju, tad $i_k < i_{k+1}$, un tāpēc pāris $k < k+1$ rada inversiju substitūcijā τ.

Tagad, visu apkopojot, varam apgalvot, ka inversiju skaits substitūcijās σ un τ iegūstams, saskaitot kopā visas inversijas, kas analizētas punktos (i), (ii), (iii). Tikai (iii) punktā aplūkoto inversiju skaits substitūcijā σ atšķiras no inversiju skaita substitūcijā τ par skaitli 1. Tātad, ja $\varkappa$ ir inversiju skaits substitūcijā σ, tad $\varkappa - 1$ vai $\varkappa + 1$ ir inversiju skaits substitūcijā τ. Līdz ar to

$$\operatorname{sgn}(\tau) = (-1)^{\varkappa \pm 1} = -(-1)^{\varkappa} = -\operatorname{sgn}(\sigma)\,. \blacksquare$$

Atgādināsim, ka ciklu (ks) sauc par *transpozīciju.*

3.11.8. Sekas. *Ja substitūcija τ iegūta no substitūcijas σ, mainot vietām k-to elementu ar s-to, tad* $\tau = (ks)\,\sigma$.

Šī iemesla dēļ, ja τ iegūta no σ, mainot vietām k-to elementu ar s-to, saka, ka substitūcijas σ un τ *atšķiras par transpozīciju.*

3.11.9. Apgalvojums. *Ja substitūcijas σ un τ atšķiras par transpozīciju, tad* $\operatorname{sgn}(\tau) = -\operatorname{sgn}(\sigma)$.

□ Pieņemsim, ka $\quad \tau = (uv)\,\sigma \quad$ un

$$\sigma = \begin{pmatrix} \dots & u & u_1 & \dots & u_s & v & \dots \\ \dots & i_u & i_{u_1} & \dots & i_{u_s} & i_v & \dots \end{pmatrix},$$

tad τ iegūstama no σ, mainot vietām tikai blakusesošos elementus, proti,

1	—	mainām vietām i_u ar i_{u_1};
2	—	mainām vietām i_u ar i_{u_2};
. . .	. . .	. . . .
s	—	mainām vietām i_u ar i_{u_s};
s+1	—	mainām vietām i_u ar i_v;
s	—	mainām vietām i_{u_s} ar i_v;
. . .	. . .	. . . .
2	—	mainām vietām i_{u_2} ar i_v;
1	—	mainām vietām i_{u_1} ar i_v.

Saskaņā ar Lemmu 3.11.7

$$\operatorname{sgn}(\tau) = (-1)^{2s+1}\operatorname{sgn}(\sigma) = -\operatorname{sgn}(\sigma)\,. \blacksquare$$

3.11.10. Sekas. *Katram $n > 1$ grupā $\mathfrak{S}_n$ pāra un nepāra substitūciju skaits sakrīt.*

□ Pieņemsim, ka $\mathfrak{N}$ ir nepāra substitūciju veidotā kopa, bet $\mathfrak{A}_n$ — pāra substitūciju veidotā kopa. Attēlojums $\mathrm{T}_{(ks)}$ ir kopas $\mathfrak{S}_n$ substitūcija (Apgalvojums 2.7.4 un Definīcija 3.10.3). Saskaņā ar tikko pierādīto apgalvojumu $\mathrm{T}_{(ks)}(\mathfrak{N}) \subseteq \mathfrak{A}_n$, un tāpēc $|\mathfrak{N}| \leq |\mathfrak{A}_n|$. Līdzīgi, $\mathrm{T}_{(ks)}(\mathfrak{A}_n) \subseteq \mathfrak{N}$, un tāpēc $|\mathfrak{P}| \leq |\mathfrak{N}|$. No šejienes, tā kā kopas $\mathfrak{N}$ un $\mathfrak{P}$ ir galīgas, tad $|\mathfrak{N}| = |\mathfrak{A}_n|$. $\blacksquare$

3.11.11. Sekas. $\qquad |\mathfrak{A}_n| = \frac{1}{2}n!$

□ Tā kā $|\mathfrak{S}_n| = n!$ (Vingrinājums 3.9.2), tad (Sekas 3.11.10)

$$|\mathfrak{A}_n| = \frac{1}{2}n! \quad \blacksquare$$

3.11.12. Apgalvojums. *Katra substitūcija uzrakstāma kā transpozīciju reizinājums.*

□ Teorēma 3.10.17 apgalvo, ka katra substitīcija τ ir uzrakstāma kā neatkarīgu ciklu reizinājums $\tau_1\tau_2\ldots\tau_n = \tau$. Pieņemsim, ka $\tau_i = (i_1\ i_2\ \ldots\ i_k)$.

Ievērojam

$$(i_1\ i_2\ i_3) = (i_1\ i_2)(i_1\ i_3).$$

No šejienes

$$\tau_i = (i_1\ i_2\ \ldots\ i_k) = (i_1\ i_2)(i_1\ i_3)\ldots(i_1\ i_k). \quad \blacksquare$$

3.11.13. Sekas. *Ja* $(i_1\ i_2\ \ldots\ i_k)$ *ir cikls, tad* $\operatorname{sgn}(i_1\ i_2\ \ldots\ i_k) = (-1)^k$.

3.11.14. Piemērs. $(13)(15) = (135) = (351) = (35)(31)$.

Tā kā $(15) \neq (35)$, tad dotais piemērs parāda, ka transpozīcijām Teorēmas 3.10.17 analogs nav spēkā.

3.11.15. Definīcija. *Elementu* i *sauc par substitūcijas* τ *nekustīgo punktu, ja* $i\tau = i$.

3.11.16. Definīcija. *Skaitli* $n - k - s$ *sauc par substitūcijas* $\tau \in \mathfrak{S}_n$ *dekrementu, ja*

- k *— substitūcijas* τ *neatkarīgo ciklu skaits,*
- s *— substitūcijas* τ *nekustīgo punktu skaits.*

3.11.17. Apgalvojums. $\operatorname{sgn}(\tau) = (-1)^d$, *kur* d *— substitūcijas* $\tau \in \mathfrak{S}_n$ *dekrements.*

□ (i) Pieņemsim, ka $\tau = \tau_1\tau_2\ldots\tau_k$ ir neatkarīgu ciklu reizinājums un $|\tau_i| = m_i$, tad (Sekas 3.11.13)

$$\operatorname{sgn}(\tau) = (-1)^{m_1-1}(-1)^{m_2-1}\ldots(-1)^{m_k-1} = (-1)^{\sum_{i=1}^{k}(m_i-1)}.$$

$$\sum_{i=1}^{k}(m_i - 1) = \sum_{i=1}^{k} m_i - k.$$

(ii) Ievērojam

$$|\bigcup_{i=1}^{n}\bar{\tau}_i| = \sum_{i=1}^{k} m_i.$$

No šejienes, ja s ir substitūcijas τ nekustīgo punktu skaits, tad

$$n - s = \sum_{i=1}^{k} m_i.$$

Līdz ar to $\sum_{i=1}^{k}(m_i - 1) = n - k - s$, t.i., šī summa ir vienāda ar dekrementu. ■

3.11.18. Piemērs.

$$\sigma \leftharpoondown \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 1 & 3 & 7 & 4 & 6 & 9 & 2 & 5 \end{pmatrix} = (182)(4795)$$

Tā kā dekrements $d = 9 - 2 - 2 = 5$, tad σ ir nepāru substitūcija.

3.11.19. Lemma. *Ja $H \leq G$ un $[G : H] = 2$, tad $H \trianglelefteq G$.*

□ (i) Tā kā $[G : H] = 2$, tad $G/H = \{H, xH\}$, kur $x \notin H$.

(ii) Ja $\in H$, tad $aH = H = Ha$.

(iii) Ja $a \notin H$, tad $aH \neq H \neq Ha$, tāpēc $aH = G \setminus H = Ha$.

(iv) Tagad, ņemot vērā (ii) un (iii), atliek tikai atsaukties uz Definīciju 3.6.4. ■

3.11.20. Teorēma. $\mathfrak{A}_n \trianglelefteq \mathfrak{S}_n$

□ (i) Pieņemsim, ka $\sigma \in \mathfrak{A}_n$, tad (Sekas 3.11.4) $\sigma^{-1} \in \mathfrak{A}_n$.

(ii) Pieņemsim, ka $\tau \in \mathfrak{A}_n$, tad to var uzrakstīt kā (Apgalvojums 3.11.12) transpozīciju reizinājumu $\tau = \tau_1\tau_2\ldots\tau_m$. Tā kā $\tau \in \mathfrak{A}_n$, tad m ir pārskaitlis. Līdzīgi, σ var uzrakstīt kā transpozīciju reizinājumu $\sigma_1\sigma_2\ldots\sigma_k$, kur k ir pārskaitlis. No šejienes $\sigma\tau = \sigma_1\sigma_2\ldots\sigma_k\tau_1\tau_2\ldots\tau_m$ ir transpozīciju reizinājums. Šai reizinājumā transpozīciju skaits ir pārskaitlis, tāpēc $\sigma\tau \in \mathfrak{A}_n$.

(iii) Ņemot vērā (i) un (ii) secināms: $\mathfrak{A}_n \leq \mathfrak{S}_n$.

(iv) Tagad atliek atsaukties uz Lemmu 3.11.19, Vingrinājumu 3.9.2 un Sekām 3.11.11, lai secinātu: $\mathfrak{A}_n \trianglelefteq \mathfrak{S}_n$. ■

3.11.21. Definīcija. *Grupu $\mathfrak{A}_n$ sauc par maiņzīmju grupu.*

3.12. Komutanti

3.12.1. Definīcija. *Grupas G elementu*

$$[a,b] \leftharpoondown a^{-1}b^{-1}ab$$

sauc par grupas G elementu a un b komutatoru.

Vienošanās.

- $\mathrm{Kom}G \leftharpoondown \{x \in G \mid \exists a \in G\ \exists b \in G\ \ x = [a,b]\}$,
- $[G,G] \leftharpoondown \langle \mathrm{Kom}G \rangle$.

[G,G] sauc par grupas G *komutantu.*

3.12.2. Teorēma. $[G,G] \trianglelefteq G$

$\square$ Pieņemsim, ka $x \in G$ un $u \in [G,G]$, tad

$$xux^{-1} = xux^{-1}u^{-1}uxx^{-1} = (xux^{-1}u^{-1})u \in [G,G].$$

Līdz ar to $x[G,G]x^{-1} \subseteq [G,G]$. Tātad $[G,G] \trianglelefteq G$. $\blacksquare$

3.12.3. Vingrinājums. Atrast grupas $\mathfrak{S}_3$ komutantu!

3.13. Grupas centrs

3.13.1. Definīcija. *Grupas G elementu c sauc par centrālo elementu, ja*

$$\forall g \in G \quad cg = gc.$$

Kopu C, kas sastāv no visiem grupas G centrālajiem elementiem, sauc par *grupas G centru.*

3.13.2. Apgalvojums. *Grupas G centrs C ir tās apakšgrupa.*

Ja $H \leq C$, tad $H \trianglelefteq G$.

□ (i) Pieņemsim, ka e ir grupas G neitrālais elements, tad $\forall g \in G \quad eg = ge$; tātad $e \in C$.

(ii) Pieņemsim, ka a, b ir centra elementi un $g \in G$, tad

$$(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab).$$

Līdz ar to $ab \in C$.

(iii) $a^{-1}g = a^{-1}gaa^{-1} = a^{-1}(ga)a^{-1} = a^{-1}(ag)a^{-1} = (a^{-1}a)ga^{-1} = ga^{-1}$; tātad $a^{-1} \in C$.

(iv) Ņemot vērā punktos (i)–(iii) pierādīto, secinām: $C \leq G$.

(v) Pieņemsim, ka $H \leq C$, $h \in H$ un $g \in G$, tad $ghg^{-1} = hgg^{-1} = h \in H$. Līdz ar to $H \trianglelefteq G$. ■

3.14. Saistītie elementi

3.14.1. Definīcija. *Grupas G elementus a un b sauc par saistītiem elementiem, ja*

$$\exists g \in G \quad b = gag^{-1}.$$

Kopu

$$S(a) \leftharpoondown \{b \,|\, \exists g \in G \;\; b = gag^{-1}\}$$

sauc par elementa a *saistīto elementu klasi.*

3.14.2. Vingrinājumi. (i) $a \in S(a)$

(ii) Ja a ir grupas G centrālais elements, tad $S(a) = \{a\}$.

3.14.3. Apgalvojums. *Grupas G saistīto elementu klases veido kopas G sadalījumu.*

□ Pieņemsim, ka $u \in S(a) \cap S(b)$, tad eksistē tādi grupas G elementi g un h, ka

$$u = gag^{-1} = hbh^{-1}.$$

(i) Pieņemsim, ka $v \in S(a)$, tad eksistē tāds $c \in G$, ka $v = cac^{-1}$. No šejienes

$$v = cac^{-1} = cg^{-1}ugc^{-1} = cg^{-1}hbh^{-1}gc^{-1} = (cg^{-1}h)b(cg^{-1}h)^{-1} \in S(b).$$

Līdz ar to $S(a) \subseteq S(b)$.
(ii) Lasītājam kā vingrinājumu piedāvājam pierādīt faktu, ka $S(b) \subseteq S(a)$.
(iii) No (i) un (ii) izriet, ka $S(a) \subseteq S(b) \subseteq S(a)$. Tātad $S(a) = S(b)$. ■

3.14.4. Vingrinājums. Atrast grupas $\mathfrak{S}_3$ saistīto elementu klases!

3.14.5. Definīcija. *Pieņemsim, ka g ir grupas G elements. Kopu*

$$C(g) \leftharpoondown \{a \in G \mid ag = ga\}$$

sauc par elementa g centralizatoru.

3.14.6. Sekas. $\forall g \in G \quad C \subseteq C(g)$

3.14.7. Apgalvojums. $\forall g \in G \quad C(g) \leq G.$

□ (i) Pieņemsim, ka $a \in C(g)$, tad $ag = ga$. No šejienes

$$a^{-1}g = a^{-1}aga^{-1} = a^{-1}(ag)a^{-1} = a^{-1}(ga)a^{-1} = a^{-1}g;$$

tātad $a^{-1} \in C(g)$.
(ii) Pieņemsim, ka $b \in C(g)$, tad $bg = gb$. Tagad varam secināt, ka

$$(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab);$$

tātad $ab \in C(g)$.
(iii) Ņemot vērā punktos (i)–(ii) pierādīto, secināms: $C(g) \leq G$. ■

3.14.8. Teorēma. $\forall g \in G \quad [G : C(g)] = |S(g)|.$

□ (i) Pieņemsim, ka $G/C(g)$ ir faktorkopa pēc ekvivalences tipa predikāta $\equiv^k_{C(g)}$ (skatīt Vingrinājumu 3.4.1(ii)), tad attēlojums

$$\varphi : S(g) \to G/C(g) : aga^{-1} \mapsto aC(g)$$

definēts korekti. Pierādīsim to!
Pieņemsim, ka $aga^{-1} = bgb^{-1}$. Mums jāparāda, ka $aC(g) = bC(g)$.

Veicam ekvivalentus pārveidojumus:

$$\begin{aligned} aga^{-1} &= bgb^{-1} \\ ag &= bgb^{-1}a \\ b^{-1}ag &= gb^{-1}a; \end{aligned}$$

tātad $b^{-1}a \in C(g)$. Saskaņā ar Lemmu 3.4.8 tas nozīmē, ka $aC(g) = bC(g)$.

(ii) Tagad parādīsim, ka attēlojums $\varphi : S(g) \to G/C(g)$ ir injekcija.

Pieņemsim, ka $u \neq v$, taču abi elementi ir kopas $S(g)$ elementi. Tas nozīmē, ka eksistē tādi grupas G elementi a un b, ka $u = aga^{-1}$ un $v = bgb^{-1}$.

Ja reiz $u \neq v$, tad $aga^{-1} \neq bgb^{-1}$, un ņemot vērā punktā (i) demonstrētos ekvivalentos pārveidojumus, secināms: $b^{-1}ag \neq gb^{-1}a$. Tātad $b^{-1}a \notin C(g)$, un tāpēc (skatīt Lemmu 3.4.8) $aC(g) \neq bC(g)$. Līdz ar to

$$\varphi(u) = aC(g) \neq bC(g) = \varphi(v),$$

t.i., φ ir injekcija.

(iii) Parādīsim, ka attēlojums $\varphi : S(g) \to G/C(g)$ ir sirjekcija.

Pieņemsim, ka $aC(g) \in G/S(g)$, tad $a \in G$. No šejienes

$$aga^{-1} \in S(g) \qquad \text{un} \qquad \varphi(aga^{-1}) = aC(g),$$

t.i., φ ir sirjekcija.

(iv) Tagad atsaucoties uz punktos (ii)–(iii) pierādīto, secināms:

$$\varphi : S(g) \to G/C(g)$$

ir bijekcija. Līdz ar to $|S(g)| = |G/C(g)| \overset{\text{D3.4.13}}{=} [G : C(g)]$. ■

4. nodaļa

GREDZENI

Gredzeni, piemēri, apakšgredzeni, gredzenu šķēlums; homomorfismi, homomorfisma attēls, kongruences, ideāli, faktorgredzeni, dabīgais homomorfisms, izomorfisma teorēma. Nulles dalītājs, integritātes apgabals, ķermenis, lauks, lauka raksturojums. Vienkāršs gredzens. Komplekso skaitļu lauks, kvaternionu ķermenis, matricu gredzens pār ķermeni. Gredzena centrs; matricu gredzens pār lauku, tā centrs.

4.1. Apakšgredzeni

4.1.1. Definīcija. *Algebru* $\langle R, +, \cdot \rangle$ *sauc par gredzenu, ja*

(i) $\langle R, + \rangle$ — *komutatīva grupa;*

(ii) $\langle R, \cdot \rangle$ — *pusgrupa;*

(iii) $(a+b)c = ac + bc \qquad un \qquad a(b+c) = ab + ac.$

$\langle R, + \rangle$ sauc par *gredzena* R *aditīvo grupu.* $\langle R, \cdot \rangle$ sauc par *gredzena* R *multiplikatīvo pusgrupu.* Gredzenu R sauc par *komutatīvu gredzenu*, ja multiplikatīvā pusgrupa ir komutatīva.

Ja gredzena R multiplikatīvā pusgrupa ir monoīds, tad šī monoīda neitrālo elementu sauc par *gredzena vieninieku.* Pašu monoīdu šai situācijā sauc par gredzena R *multiplikatīvo monoīdu.*

4.1.2. Piemēri. (i) Veselo skaitļu gredzens $\langle \mathbb{Z}, +, \cdot \rangle$ ir komutatīvs gredzens ar vieninieku.

(ii) Kvadrātisko matricu gredzens $\langle \mathrm{Mat}_n(\mathbb{R}), +, \cdot\rangle$ katram $n > 1$ ir nekomutatīvs gredzens ar vieninieku.

(iii) Pāru skaitļu gredzens $\mathbb{Z}2$ nesatur vieninieku.

(iv) Jebkuru komutatīvu grupu H var pārvērst par gredzenu tajā definējot reizināšanu ar nosacījumu: $ab \leftharpoondown 0$.

(v) Rezidiju gredzens $\mathbb{Z}_m$ ir komutatīvs gredzens. Šis gredzens ir galīgs, t.i., $|\mathbb{Z}_m| = m$.

4.1.3. Definīcija. *Gredzenu R, kuram reizināšana apmierina nosacījumu $ab = 0$, sauc par gedzenu ar nulles reizināšanu.*

4.1.4. Vingrinājumi. (i) Ja gredzens ar nulles reizināšanu sastāv no vismaz 2 elementiem, tad tas ir gredzens bez vieninieka.

(ii) Katrā gredzenā izpildā sekojošas izdentitātes:

- $0a - a0 = 0$,
- $a(-b) = (-a)b = -ab$,
- $(a-b)c = ac - bc \qquad \text{un} \qquad a(b-c) = ab - ac.$

4.1.5. Definīcija. *Grsdzena R apakškopu H sauc par apakšgredzenu, ja*

(i) *H ir aditīvās grupas apakšgrupa,*

(ii) *H ir multiplikatīvās pusgrupas apakšpusgrupa.*

4.1.6. Vingrinājumi. (i) Ja H ir gredzena R apakšgredzens, tad $\langle H, +|H, \cdot|H\rangle$ ir gredzens.

(ii) Pāra skaitļu gredzens $\mathbb{Z}2$ ir veselo skaitļu gredzena $\mathbb{Z}$ apakšgredzens.

(iii) Diagonālmatricas

$$D_n(\mathbb{R}) \leftharpoondown \left\{ \begin{pmatrix} d_1 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & \dots & d_n \end{pmatrix} \middle| \, \forall i \ d_i \in \mathbb{R} \right\}.$$

veido matricu gredzena $\mathrm{Mat}_n(\mathbb{R})$ apakšgredzenu.

(iv) Gredzena ar nulles reizināšanu aditīvās grupas katra apakšgrupa ir apakšgredzens.

4.1.7. Apgalvojums. *Ja* $\{R_i \mid i \in \mathcal{I}\}$ *ir gredzena* R *apakšgredzenu saime, tad* $R^0 \leftharpoondown \bigcap\limits_{i\in\mathcal{I}} R_i$ *ir gredzena* R *apakšgredzens.*

□ (i) R^0 ir gredzena R aditīvās grupas apakšgrupa (Apgalvojums 3.3.5).

(ii) Tā kā $R^0 \neq \emptyset$, jo $0 \in R^0$, tad R^0 ir multiplikatīvās pusgrupas apakšpusgrupa (Apgalvojums 2.9.5). ■

4.2. Homomorfismi

4.2.1. Definīcija. *Pieņemsim, ka* R *un* R' *ir gredzeni. Attēlojumu*

$$f : R \to R'$$

sauc par gredzenu homomorfismu, ja

- $f(x+y) = f(x) + f(y)$,
- $f(xy) = f(x)f(y)$.

Līdzīgi kā pusgrupu gadījumā bijektīvu homomorfismu sauc par *izomorfismu.* Šai situācijā gredzenus R un R' sauc par *izomorfiem* gredzeniem. Sirjektīvu homomorfismu sauc par *epimorfismu.* Injektīvu homomorfismu sauc par *monomorfismu.*

Gredzenu homomorfismu $f : R \to R$ sauc par *endomorfismu.* Ja endomorfisms ir bijekcija, tad to sauc par *automorfismu.*

4.2.2. Piemēri. (i) Attēlojums

$$f : D_2(\mathbb{R}) \to \mathbb{R} : \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mapsto a$$

ir gredzenu homomorfisms.

(ii) Pieņemsim, ka $C[a;b]$ ir segmentā $[a;b]$ nepārtraukto reāla argumenta funkciju gredzens. Attēlojums

$$\varphi : C[a;b] \to \mathbb{R} : f(x) \mapsto f(0)$$

ir gredzenu homomorfisms.

4.2.3. Apgalvojums. *Ja* $f : R \to R'$ *ir gredzenu homomorfisms, tad* $\mathrm{Im} f$ *ir gredzena* R' *apakšgredzens.*

$\Box$ (i) $\mathrm{Im} f$ ir gredzena R aditīvās grupas apakšgrupa (Vingrinājums 3.5.8).

(ii) $\mathrm{Im} f$ ir gredzena R multiplikatīvās pusgrupas apakšpusgrupa (Apgalvojums 2.9.6). $\blacksquare$

4.2.4. Definīcija. *Gredzenā* R *definētu ekvivalences tipa predikātu* $\equiv$ *sauc par kongruenci, ja tā ir gan gredzena aditīvās grupas kongruence, gan gredzena multiplikatīvās pusgrupas kongruence.*

4.2.5. Apgalvojums. *Ja* $\equiv$ *ir gredzena* R *kongruence, tad* $R/\equiv$ *ir gredzens, kur*

$$\begin{aligned} [x] + [y] &\leftharpoondown [x + y], \\ [x][y] &\leftharpoondown [xy]. \end{aligned}$$

$\Box$ (i) Šī kongruence definē aditīvo grupu $\langle R/\equiv, +\rangle$ (Sekas 3.5.6).

(ii) Šī kongruence definē multiplikatīvo pusgrupu $\langle R/\equiv, \cdot\rangle$ (Apgalvojums 2.10.4).

(iii) Parādīsim kā pierādāms viens distributīvais likums. Otra likuma pierādījumu atstājam lasītājam kā vingrinājumu.

$$\begin{aligned} [a]([b] + [c]) &= [a][b + c] = [a(b + c)] = [ab + ac] \\ &= [ab] + [ac] = [a][b] + [a][c]. \quad \blacksquare \end{aligned}$$

4.2.6. Definīcija. *Gredzenu* $R/\equiv$ *pēc kongruences* $\equiv$ *sauc par faktorgredzenu.*

4.2.7. Vingrinājums. Attēlojums $\pi : R \to R/\equiv : a \mapsto [a]$ ir gredzenu epimorfisms.

Līdzīgi kā pusgrupu gadījumā, attēlojumu

$$\pi : R \to R/\equiv : a \mapsto [a]$$

sauc par *dabīgo* jeb *kanonisko homomorfismu.*

4.2.8. Definīcija. *Gredzena* R *apakšgredzenu* I *sauc par ideālu, ja*

$$\forall a \in I\ \forall x \in R \quad (ax \in I \wedge xa \in I).$$

Īsāk to var pierakstīt šādi: $RI \subseteq I \supseteq IR$.

4.2.9. Teorēma. *Katrai gredzena kongruencei* $\equiv$ *eksistē tāds ideāls* I*, ka* $\quad R/I = R/{\equiv}$.

$\square$ Teorēma 3.6.12 apgalvo, ka

$$[0] \trianglelefteq R \qquad \text{un} \qquad R/[0] = R/{\equiv}\ .$$

Tas viss attiecas uz gredzena R aditīvo grupu.

Tagad kopā $R/[0]$ definējam reizināšanu:

$$(x + [0])(y + [0]) \leftharpoondown xy + [0].$$

Atliek konstatēt, ka $[0]$ ir ideāls, reizināšana definēta korekti, $R/[0]$ ir gredzens un tas sakrīt ar gredzenu $R/{\equiv}$.

(i) Pieņemsim, ka $a \in [0]$ un $x \in R$, tad $a \equiv 0$. Ja reiz $\equiv$ ir kongruence, tad $ax \equiv 0x = 0 = x0 \equiv xa$. Līdz ar to

$$ax \in [0] \qquad \text{un} \qquad xa \in [0].$$

Tātad $[0]$ ir gredzena R ideāls.

(ii) Parādīsim, ka $x + [0] = [x]$.

a) Pieņemsim, ka $y \in x+[0]$, tad (Lemmas 3.4.4 un 3.4.8), tad $y-x \in [0]$. Tas nozīmē, ka $y - x \equiv 0$ jeb $x \equiv y$. Tātad $y \in [x]$, t.i., $x + [0] \subseteq [x]$.

b) Pieņemsim, ka $y \in [x]$, tad $y \equiv x$ jeb $y - x \equiv 0$. Tātad $y - x \in [0]$. Tas saskaņā ar Lemmām 3.4.8 un 3.4.4 ļauj secināt, ka $y \in x + [0]$. Tātad $[x] \subseteq [x] + [0]$.

c) Mēs tikko parādījām (punkti a) un b)), ka $x + [0] \subseteq [x] \subseteq [x] + [0]$. Tātad $x + [0] = [x]$.

(iii) Tā rezultātā kopas $R/[0]$, $R/{\equiv}$ sakrīt un

$$(x + [0])(y + [0]) = xy + [0] = [xy] = [x][y],$$

t.i., reizināšana kopā $R/[0]$ definēta tāpat kā kopā $R/{\equiv}$. Tātad $R/{\equiv}$ un $R/[0]$ sakrīt arī kā gredzeni. $\blacksquare$

4.2.10. Teorēma. *Katram gredzena ideālam* I *eksistē tāda kongruence* $\equiv$*, ka* $\quad R/I = R/{\equiv}$.

□ (i) Saskaņā ar Apgalvojumu 3.6.10 ekvivalences tipa predikāts $\equiv_I^k$ ir kongruence gredzena R aditīvajā grupā.

(ii) Pieņemsim, ka $x \equiv_I^k y$ un $a \in R$, tad saskaņā ar $\equiv_I^k$ definīciju (Vingrinājums 3.4.1(ii)) $x + I = y + I$. No šejienes $x - y \in I$. Tā kā I ir ideāls, tad

$$\begin{aligned} ax - ay = a(x-y) \in I \quad &\text{un} \quad xa - ya = (x-y)a \in I, \\ ax + I = ay + I \quad &\text{un} \quad xa + I = ya + I, \\ ax \equiv_I^k ay \quad &\text{un} \quad xa \equiv_I^k ya. \end{aligned}$$

Tātad $\equiv_I^k$ ir gredzena R kongruence.

(iii) $[0]_I^k = \{x \mid x + I = 0 + I\} = I$. Tagad atsaucoties uz Teorēmas 4.2.9 pierādījumu, secināms $R/I = R/\equiv_I^k$. ■

4.2.11. Apgalvojums. *Ja $f : R \to R'$ ir gredzenu homomorfisms, tad*

$$\mathrm{Ker} f \leftharpoondown \{x \mid f(x) = 0\}$$

ir gredzena R ideāls.

□ (i) Saskaņā ar 74. lappusē izklāstīto $\mathrm{Ker} f$ ir gredzena R aditīvās grupas apakšgrupa.

(ii) Pieņemsim, ka $x \in \mathrm{Ker} f$ un $y \in \mathrm{Ker} f$, tad

$$f(xy) = f(x)f(y) = 0 \cdot 0 = 0.$$

Tātad $xy \in \mathrm{Ker} f$, t.i., $\mathrm{Ker} f$ ir gredzena R multiplikatīvās pusgrupas apakšpusgrupa.

(iii) Pieņemsim, ka $a \in \mathrm{Ker} f$ un $x \in R$, tad

$$f(ax) = f(a)f(x) = 0f(x) = 0 = f(x)0 = f(x)f(a) = f(xa).$$

Tātad gan $ax \in \mathrm{Ker} f$, gan $xa \in \mathrm{Ker} f$.

(iv) Tas viss kopumā (punti (i)–(iii)) demonstrē, ka $\mathrm{Ker} f$ ir gredzena R ideāls. ■

Gredzenu teorijā, līdzīgi kā grupu teorijā, šo ideālu $\mathrm{Ker} f$ sauc par *homomorfisma f kodolu.*

4.2.12. Teorēma. *Katram gredzenu homomorfismam $f : R \to R'$ eksistē viens vienīgs gredzenu homomorfisms $f_* : R/\mathrm{Ker} f \to R'$, kam diagramma*

$$\begin{tikzcd} R \arrow[rr, "f"] \arrow[dr, "\pi"'] & & R' \\ & R/\mathrm{Ker} f \arrow[ur, "f_*"'] & \end{tikzcd}$$

ir komutatīva; turklāt šis homomorfisms f_* ir monomorfisms.

□ Šis rezultāts pierādīts (Teorēma 3.7.1) grupām. Mums atliek parādīt, ka $f_* : R/\mathrm{Ker} f \to R'$ ir multiplikatīvo pusgrupu homomorfisms.

Pieņemsim, ka $[x] \in R/\mathrm{Ker}$ un $[y] \in R/\mathrm{Ker}$, tad

$$\begin{aligned} f_*([x][y]) &= f_*([xy]) = f_* \circ \pi(xy) = f(xy) = f(x)f(y) \\ &= f_* \circ \pi(x)\ f_* \circ \pi(y) = f_*([x])f_*([y]). \quad \blacksquare \end{aligned}$$

4.2.13. Sekas (Izomorfisma teorēma). $G/\mathrm{Ker} f \cong \mathrm{Im} f$

4.3. Integritātes apgabali

4.3.1. Definīcija. *Gredzena R nenulles elementu $a \neq 0$ sauc par nulles dalītāju, ja*

$$\exists b \in R\ (b \neq 0 \wedge (ab = 0 \vee ba = 0)).$$

Pieņemsim, ka R — gredzens ar 1. Gredzena R elementu a sauc par *apgriežamu*, ja

$$\exists b \in R\ ab = 1 = ba.$$

4.3.2. Apgalvojums. *Gredzena apgriežams elements nav nulles dalītājs.*

□ Pieņemsim pretējo, proti, ka eksistē tāds apgriežams gredzena R elements a, kas ir nulles dalītājs. No šejienes uzreiz seko, ka $a \neq 0$, jo ir nulles dalītājs. Ja reiz a ir nulles dalītājs, tad

$$\exists b \in R \quad (b \neq 0 \wedge (ab = 0 \vee ba = 0)).$$

Tā kā a ir apgriežams, tad

$$\exists x \in R \quad ax = 1 = xa.$$

Tas viss pamato sekojošas vienādības

$$\begin{aligned} b &= (xa)b = x(ab) = x0 = 0, \qquad \text{vai arī} \\ b &= b(ax) = (ba)x = 0x = 0. \qquad \text{Pretruna!} \ \blacksquare \end{aligned}$$

4.3.3. Definīcija. *Gredzenu R sauc par integritātes apgabalu, ja tas ir*

(i) *komutatīvs gredzens bez nulles dalītājiem;*

(ii) *gredzens ar* 1 *un* $1 \neq 0$.

Integritātes apgabalu R sauc par *lauku*, ja katrs gredzena R nenulles elements ir apgriežams gredzenā R.

4.3.4. Sekas. *Lauks nesatur nulles dalītājus.*

4.3.5. Sekas. *Lauka nenulles elementi veido komutatīvu multiplikatīvo grupu.*

4.3.6. Definīcija. *Pieņemsim, ka*

- R — *integritātes apgabals,*
- $\mathbb{Z}p$ *ir homomorfisma* $\lambda : \mathbb{Z} \to R : k \mapsto k1$ *kodols.*

Skaitli p sauc par gredzena R *raksturojumu* jeb *harakteristiku* un apzīmē ar $\mathrm{char} R$.

4.3.7. Teorēma. *Jebkura lauka raksturojums ir pirmskaitlis, vai arī* 0.

$\square$ Pieņemsim, ka $n = kl$ ir lauka L raksturojums, kur $1 < k < n$, tad

$$a \leftharpoondown k1 \qquad \text{un} \qquad b \leftharpoondown l1$$

ir no nulles atšķirīgi lauka L elementi. Taču

$$ab = (k1)(l1) = (kl)1 = n1 = 0,$$

kas ir pretrunā ar faktu, ka laukā nav nulles dalītāju. $\blacksquare$

4.3.8. Piemēri. (i)

$$\mathbb{C} \leftharpoondown \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a \in \mathbb{R} \wedge b \in \mathbb{R} \right\}$$

ir lauks.

(ii) Ja $p \in \mathbb{P}$, t.i., ja p ir pirmsksitlis, tad rezidiju gredzens $\mathbb{Z}_p$ ir lauks.

4.3.9. Definīcija. *Lauku $\mathbb{C}$ sauc par komplekso skaitļu lauku.*

4.3.10. Apgalvojums. *Attēlojums*

$$f : \mathbb{R} \to \mathbb{C} : a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

ir monomorfisms.

□ (i) Ja $a \neq b$, tad

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \neq \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix}.$$

(ii)

$$f(a) + f(b) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} + \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} a+b & 0 \\ 0 & a+b \end{pmatrix} = f(a+b).$$

(iii)

$$f(a)f(b) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & b \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & ab \end{pmatrix} = f(ab). \quad \blacksquare$$

Šis rezultāts attaisno identifikāciju

$$a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

Ja ar i apzīmējam matricu

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

tad

$$i^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1$$

un

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = a + bi.$$

Līdz ar to esam ieguvuši tradicionālo komplekso skaitļu pierakstu.

4.3.11. Definīcija. *Par kompleksa skaitļa $z = a + bi$ kompleksi saistīto skaitli sauc skaitli $\bar{z} \leftharpoondown a - bi$.*

4.3.12. Vingrinājums. Attēlojums $f : \mathbb{C} \to \mathbb{C} : z \mapsto \bar{z}$ ir automorfisms.

4.4. Ķermeņi

4.4.1. Definīcija. *Gredzenu sauc par ķermeni, ja tā multiplikatīvā pusgrupa bez* 0 *elementa ir grupa.*

4.4.2. Sekas. *Komutatīvs ķermenis ir lauks.*

4.4.3. Piemērs.

$$\mathbb{K} \leftharpoondown \left\{ \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \middle| u \in \mathbb{C} \wedge v \in \mathbb{C} \right\}$$

ir ķermenis.

Ja $u = a + bi$ un $v = c + di$, tad $u\bar{u} + v\bar{v} = a^2 + b^2 + c^2 + d^2 \geq 0$. Tātad,

$$\text{ja} \quad \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \neq 0, \qquad \text{tad} \quad \begin{vmatrix} u & v \\ -\bar{v} & \bar{u} \end{vmatrix} \neq 0.$$

No šejienes

$$\begin{aligned} \begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix} \begin{pmatrix} \bar{u} & -v \\ \bar{v} & u \end{pmatrix} &= \begin{pmatrix} u\bar{u} + v\bar{v} & -uv + vu \\ -\bar{v}\bar{u} + \bar{u}\bar{v} & \bar{v}v + \bar{u}u \end{pmatrix} \\ &= \begin{pmatrix} u\bar{u} + v\bar{v} & 0 \\ 0 & \bar{v}v + \bar{u}u \end{pmatrix}. \end{aligned}$$

Tas demonstrē, ka katra nenulles matrica $A \in \mathbb{K}$ ir apgriežama. Tai pašā laikā $\mathbb{K}$ nav komutatīvs gredzens, piemēram,

$$\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}.$$

4.4.4. Definīcija. *Ķermeni $\mathbb{K}$ sauc par kvaternionu ķermeni. Kopas $\mathbb{K}$ elementus sauc par kvaternioniem.*

4.4.5. Vingrinājums. Attēlojums

$$f : \mathbb{R} \to \mathbb{K} : a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

ir monomorfisms.

Līdzīgi kā komplekso skaitļu gadījumā šis rezultāts attaisno identifikāciju

$$a \mapsto \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

Ja ar i, j un k atbilstoši apzīmējam matricas

$$i \leftharpoondown \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad j \leftharpoondown \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k \leftharpoondown \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

tad iegūstam šadu reizināšanas tabulu:

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

No šejienes, ja $u = a+bi$ un $v = c+di$ (te i ir kompleksais skaitlis), iegūstam

$$\begin{aligned}
\begin{pmatrix} a+bi & c+di \\ -\overline{(c+di)} & \overline{a+bi} \end{pmatrix} &= \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \\
&= a\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \\
&+ c\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + d\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \\
&= a + bi + cj + dk.
\end{aligned}$$

4.4.6. Definīcija. *Gredzenu R, kas satur no 0 atšķirīgu 1, sauc par vienkāršu gredzenu, ja tā vienīgie ideāli ir R un $\{0\}$.*

4.4.7. Apgalvojums. *Ķermenis ir vienkāršs gredzens.*

□ Pieņemsim, ka $I \neq \{0\}$ ir ķermeņa K ideāls, tad (Definīcija 4.2.8)

$$\forall a \in I\ \forall x \in K \quad (ax \in I \wedge xa \in I).$$

Tā kā $I \neq \{0\}$, tad eksistē ideāla I nenulles elements a. No šejienes $1 = a^{-1}a \in I$. Ja reiz $1 \in I$, tad

$$\forall x \in K \quad x = x \cdot 1 \in I. \quad \blacksquare$$

Tagad pievērsīsimies matricu grdzenam $\mathrm{Mat}_n(K)$ pār ķermeni K, t.i., mūs interesēs kvadrātiskas matricas, kuru elementi ir ķemeņa K elementi. Ar $E_{ij} = ||e_{kl}|| \in \mathrm{Mat}_n(K)$ apzīmēsim matricu, kurai tikai viens elements e_{kl} atšķiras no 0, proti, $e_{ij} = 1$.

4.4.8. Lemma.

$$\forall A = ||a_{kl}|| \in \mathrm{Mat}_n(K) \quad E_{ip}AE_{qj} = a_{pq}E_{ij}.$$

□ (i) $E_{ip}A$ — tā ir matrica, kurai visas rindas, izņemot i–to rindu, sastāv tikai no 0. Savukārt i–tā rinda vienāda ar matrica A p–to rindu.

(ii) AE_{qj} — tā ir matrica, kurai visas ailes, izņemot j–to aili, sastāv tikai no 0. Savukārt j–tā aile vienāda ar matricas A q–to aili.

(iii) Tagad ņemot vērā (i) un (ii) secināms: $E_{ip}AE_{qj} = a_{pq}E_{ij}$. ■

4.4.9. Teorēma. *Matricu gredzens pār ķermeni ir vienkāršs.*

□ Pieņemsim, ka $I \neq \{0\}$ ir matricu gredzena $\mathrm{Mat}_n(K)$ ideāls, tad (Definīcija 4.2.8)

$$\forall A \in I\ \forall X \in \mathrm{Mat}_n(K) \quad (AX \in I \wedge XA \in I).$$

Tā kā $I \neq \{0\}$, tad eksistē ideāla I nenulles matrica $||a_{kl}||$. Pieņemsim, ka tieši $a_{pq} \neq 0$. Tagad ņemam vērā, ka

$$\forall i\ \forall j \quad a_{pq}E_{ij} \stackrel{\text{L4.4.8}}{=} E_{ip}||a_{kl}||E_{qj} \in I.$$

Tā rezultātā $E_{ij} = (a_{pq}^{-1}E)(a_{pq}E_{ij}) \in I$. Ja reiz tā, tad $\forall x \in K\ xE_{ij} \in I$. No šejienes, ja $X = ||x_{ij}|| \in \mathrm{Mat}_n(K)$, tad

$$X = \sum_{i=1}^{n}\sum_{j=1}^{n} x_{ij}E_{ij} \in I, \quad \text{t.i.,} \quad I = \mathrm{Mat}_n(K). \quad \blacksquare$$

4.5. Gredzena centrs

4.5.1. Definīcija. *Gredzena R elementu c sauc par centrālo elementu, ja*

$$\forall a \in R \quad ac = ca.$$

Kopu Z, kas sastāv no visiem gredzena R centrālajiem elementiem sauc par *gredzena R centru.*

4.5.2. Vingrinājumi. (i) Gredzena centrs ir tā apakšgredzens.

(ii) Pieņemsim, ka a un b ir gredzena R elementi, $E_{ij} \in \mathrm{Mat}_n(R)$ un $E_{kl} \in \mathrm{Mat}_n(R)$, tad

$$(aE_{ij})(bE_{kl}) = \begin{cases} abE_{il}, & \text{ja} \quad j = k \\ 0, & \text{ja} \quad j \neq k. \end{cases}$$

4.5.3. Teorēma. *Matricu gredzena* $\mathrm{Mat}_n(L)$ *pār lauku* L *centrs*

$$Z = \{\lambda E \mid \lambda \in L\}.$$

□ (i) $\qquad (\lambda E)A = \lambda A = (\lambda A)E = A(\lambda E).$
Šī vienādība ļauj konstatēt, ka $Z \supseteq \{\lambda E \mid \lambda \in L\}$.

(ii) Pieņemsim, ka $A \in Z$, tad $E_{ii}A = AE_{ii}$. Ja $A = ||a_{kl}||$, tad

$$E_{ii}A = \begin{pmatrix} 0 & \dots & 0 & \dots & 0 \\ . & . & . & . \\ a_{i1} & \dots & a_{ii} & \dots & a_{1n} \\ . & . & . & . \\ 0 & \dots & 0 & \dots & 0 \end{pmatrix}, \qquad AE_{ii} = \begin{pmatrix} 0 & \dots & a_{1i} & \dots & 0 \\ . & . & . & . \\ 0 & \dots & a_{ii} & \dots & 0 \\ . & . & . & . \\ 0 & \dots & a_{ni} & \dots & 0 \end{pmatrix}.$$

No šejienes redzams, ka vienādība iespējama tikai tad, ja visi $a_{il} = 0$ un visi $a_{ki} = 0$, izņemot vienīgi a_{ii}. Mainot indeksu i no 1 līdz n secināms, ka A ir diagonālmatrica, proti, A ir izskatā

$$A = \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ . & . & . & . \\ 0 & 0 & \dots & a_{nn} \end{pmatrix}.$$

(iii) Mēs pieņēmām, ka $A \in Z$, tāpēc $E_{ij}A = AE_{ij}$. No šejienes

$$\begin{aligned} E_{ij}A &= E_{ij}\sum_{k=1}^{n} a_{kk}E_{kk} = \sum_{k=1}^{n} a_{kk}E_{ij}E_{kk} \stackrel{\text{V4.5.2(ii)}}{=} a_{jj}E_{ij}, \\ AE_{ij} &= (\sum_{k=1}^{n} a_{kk}E_{kk})E_{ij} = \sum_{k=1}^{n} a_{kk}E_{kk}E_{ij} \stackrel{\text{V4.5.2(ii)}}{=} a_{ii}E_{ij}. \end{aligned}$$

Tā rezultātā $\forall i\ \forall j\ \ a_{ii} = a_{jj}$. Tātad $A = \lambda E$. ■

5. nodaļa

MODUĻI

Monoīda iedarbība uz kopu. Moduļi, piemēri. Apašmoduļi, to šķēlums. Lineāra kombinācija, vienas sistēmas izsakāmība ar citu sistēmu. Lineārā čaula. Moduļu homomorfismi, piemēri, homomorfisma attēls. Kongruence, faktormodulis, dabīgais homomorfisms, homomorfisma kodols, izomorfisma teorēma. Homomorfismu veidotā grupa, endomorfismu gredzens. Modulis pār endomorfismu gredzenu. Apašmoduļu summa, tiešā summa, tiešā ārējā summa, tiešais saskaitāmais. Minimālais apakšmodulis, gredzena minimālais ideāls, ireducibli moduļi, piemēri. Maksimālais apašmodulis, gredzena maksimālais ideāls, pusvienkāršs (pilnīgi reducējams) modulis. Galīgi ģenerēts modulis, tā raksturojums.

5.1. Apakšmoduļi

Šis nodaļas ietvaros, ja nekas speciāli netiks atrunāts, visi gredzeni ir gredzeni ar vieninieku.

5.1.1. Definīcija. *Divu sugu algebru $\langle R, M, \cdot, \circ\rangle$ sauc par monoīda R iedarbību uz kopu M no kreisās puses, ja*

(i) $\langle R, \cdot\rangle$ *— monoīds,*

(ii) $\circ$ *ir attēlojums* $R \times M \xrightarrow{\circ} M$*,*

(iii)

$$\begin{aligned} (ab)\circ x &= a\circ(b\circ x), \\ 1\circ x &= x. \end{aligned}$$

5.1.2. Definīcija. *Divu sugu algebru* $\langle R, M, +, \cdot, \oplus, \circ \rangle$ *sauc par kreiso* R*–moduli* M*, ja*

(i) $\langle R, +, \cdot \rangle$ — *gredzens ar vieninieku,*

(ii) $\langle M, \oplus \rangle$ — *komutatīva grupa,*

(iii) $\langle R, M, \cdot, \circ \rangle$ — *gredzena* R *multiplikatīvā monoīda iedarbība uz* M *no kreisās puses,*

(iv)

$$\begin{aligned} a \circ (x \oplus y) &= a \circ x \oplus a \circ y, \\ (a + b) \circ x &= a \circ x \oplus b \circ x. \end{aligned}$$

Literatūrā šādus moduļus sauc par *unitāriem* jeb *unitāliem* moduļiem. Kopas M elementus sauc par *vektoriem.* Parasti $+$ un $\oplus$ vietā lieto tikai simbolu $+$, bet simbolus $\cdot$ un $\circ$ vispār nelieto un uzskata, ka operācijas $\cdot$ un $\circ$ saista ciešāk par operācijām $+$ un $\oplus$. Tā rezultātā aksioma

$$(a + b) \circ x = (a \circ x) \oplus (b \circ x)$$

iegūst izskatu

$$(a + b)x = ax + bx.$$

Paralēli terminam R*–modulis* M mēs lietosim tai pašā nozīmē tādus terminus kā: M *ir* R*–modulis* vai arī M *ir modulis pār gredzenu* R. Ja no konteksta būs noprotams gredzens R, tad lietosim īsāku izteiksmes formu, proti, tā vietā, lai teiktu:
— M ir kreisais R–modulis, — teiksim:
— M ir modulis.

Analoģiski definē *labo* R*–moduli* M.

5.1.3. Definīcija. *Divu sugu algebru* $\langle R, M, \cdot, \circ \rangle$ *sauc par monoīda* R *iedarbību uz kopu* M *no labās puses, ja*

(i) $\langle R, \cdot \rangle$ — *monoīds,*

(ii) $\circ$ *ir attēlojums* $M \times R \xrightarrow{\circ} M$*,*

(iii)

$$\begin{aligned} x \circ (ab) &= x \circ (a \circ b), \\ x \circ 1 &= x. \end{aligned}$$

5.1.4. Definīcija. *Divu sugu algebru* $\langle R, M, +, \cdot, \oplus, \circ \rangle$ *sauc par labo* R*–moduli* M*, ja*

(i) $\langle R, +, \cdot \rangle$ — *gredzens ar vieninieku,*

(ii) $\langle M, \oplus \rangle$ — *komutatīva grupa,*

(iii) $\langle R, M, \cdot, \circ \rangle$ — *gredzena* R *multiplikatīvā monoīda iedarbība uz* M *no labās puses,*

(iv)

$$\begin{aligned} (x \oplus y) \circ a &= x \circ a \oplus y \circ a, \\ x \circ (a + b) &= x \circ a \oplus x \circ b. \end{aligned}$$

Tā kā kreiso R–moduļu M teorija ir analoga labo R–moduļu teorijai, tad parasti aplūko tikai vienu no šīm teorijām. Mēs turpmāk galvenokārt analizēsim kreisos R–moduļus M.

5.1.5. Piemēri. (i) Pieņemsim, ka R — gredzens ar vieninieku un M — šī gredzena aditīvā grupa, tad $\langle R, M, +, \cdot, +, \cdot \rangle$ ir gan kreisais R–modulis, gan labais R–modulis. Šai gadījumā parasti kreisajam modulim lieto apzīmējumu ${}_RR$, labajam — R_R.

(ii) Pieņmesim, ka R – gredzens ar vieninieku, tad R^n ir modulis, kur

$$\begin{aligned} (x_1, x_2, \ldots, x_n) \oplus (y_1, y_2, \ldots, y_n) &\leftharpoondown (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n), \\ a \circ (x_1, x_2, \ldots, x_n) &\leftharpoondown (ax_1, ax_2, \ldots, ax_n). \end{aligned}$$

(iii) Pieņemsim, ka $\langle M, \oplus \rangle$ — aditīva grupa un attēlojums $\mathbb{Z} \times M \xrightarrow{\circ} M$ definēts ar nosacījumu: $n \circ x \leftharpoondown nx$ (tiem, kas apjukuši, iesakam apskatīties komentāru 77. lappusē), tad $\langle \mathbb{Z}, M, +, \cdot, \oplus, \circ \rangle$ ir kreisais $\mathbb{Z}$-modulis M.

5.1.6. Vingrinājumi. Pieņemsim, ka $\langle R, M, +, \cdot, \oplus, \circ \rangle$ ir kreisais R–modulis M, tad

(i) $a \circ 0 = 0 \circ x = 0$, te izteiksmē $a \circ 0$ nulle ir aditīvās grupas M neitrālais elements, bet izteiksmē $0 \circ x$ nulle ir gredzena R aditīvās grupas neitrālais elements;

(ii) $a \circ (-x) = (-a) \circ x = -a \circ x$;

(iii) $a \circ (x - y) = a \circ x - a \circ y$;

(iv) $(a - b) \circ x = a \circ x - b \circ x$, te a un b ir gredzena R elementi, bet x, y ir vektori.

5.1.7. Definīcija. *Kreisā R–moduļa M apakškopu $N \subseteq M$ sauc par apakšmoduli, ja*

$$\forall a \in R\, \forall x \in N\, \forall y \in N \quad (ax \in N \wedge x + y \in N).$$

5.1.8. Vingrinājums. Ja N ir moduļa $\langle R, M, +, \cdot, \oplus, \circ\rangle$ apakšmodulis, tad $\langle R, N, +, \cdot, \oplus|N, \circ|R \times N\rangle$ ir modulis.

5.1.9. Apgalvojums. *Ja $\{M_i \,|\, i \in \mathcal{I}\}$ ir R–moduļa M apakšmoduļu saime, tad $M^0 \leftharpoondown \bigcap_{i \in \mathcal{I}} M_i$ ir moduļa M apakšmodulis.*

□ (i) M^0 ir grupas M apakšgrupa (Apgalvojums 3.3.5).

(ii) Pieņemsim, ka $a \in R$ un $x \in M^0$, tad $\forall i \in \mathcal{I}$ $x \in M_i$. Tā kā M_i ir moduļa M apakšmodulis, tad $ax \in M_i$. Līdz ar to $\forall i \in \mathcal{I}$ $ax \in M_i$. No šejienes $ax \in M^0$.

(iii) Tagad atsaucoties uz apakšmoduļa definīciju 5.1.7 un punktos (i), (ii) konstatēto secināms: M^0 ir moduļa M apakšmodulis. ■

5.2. Lineārā čaula

5.2.1. Definīcija. *Pieņemsim, ka M ir R–modulis, $a_i \in R$ un $x_i \in M$. Summu*

$$a_1 x_1 + a_n x_2 + \ldots + a_n x_n$$

sauc par vektoru $x_1, x_2, \ldots, x_n$ lineāru kombināciju.

Ja visi $a_i = 0$, tad lineāro kombināciju $a_1x_1 + a_nx_2 + \ldots + a_nx_n$ sauc par *triviālu* lineāru kombināciju. Ja vektors x ir vektoru $x_1, x_2, \ldots, x_n$ lineāra kombinācija, t.i., eksistē tādi gredzena R elementi $a_1, a_2, \ldots, a_n$, ka

$$x = a_1x_1 + a_nx_2 + \ldots + a_nx_n,$$

tad saka, ka vektors x *izsakāms ar sistēmu* $\{x_1, x_2, \ldots, x_n\}$. Kopas

$$\{x_1, x_2, \ldots, x_n\}$$

pieraksta vietā ļoti bieži mēdz tikai uzskaitīt elementus $x_1, x_2, \ldots, x_n$, proti, ja eksistē tādi gredzena R elementi $a_1, a_2, \ldots, a_n$, ka

$$x = a_1x_1 + a_nx_2 + \ldots + a_nx_n,$$

tad saka, ka vektors x *izsakāms ar sistēmu* $x_1, x_2, \ldots, x_n$.

Vispārīgā gadījumā pieņemsim, ka kopa $\mathfrak{A} = \{x_i \in M \mid i \in \mathcal{I}\}$. Saka, ka vektors x *izsakāms ar sistēmu* $\mathfrak{A}$, ja eksistē tādi $a_i \in R$, ka

$$x = \sum_{i \in \mathcal{I}} a_i x_i,$$

kur gandrīz visi $a_i = 0$. Tagad ir nepieciešams paskaidrot, ko nozīmē frāze "gandrīz visi $a_i = 0$".

Mēs sakam, ka kādas kopas $\mathfrak{K}$ gandrīz visiem elementiem piemīt īpašība $\mathcal{P}$, ja to kopas $\mathfrak{K}$ elementu skaits, kuriem nepiemīt īpašība $\mathcal{P}$ ir kāds naturāls skaitlis $n \in \mathbb{N}$. Skaitļa n lomā drīkst būt arī skaitlis 0. Formāli to visu var definēt šādi. Ja kopā $\mathfrak{K}$ definēts predikāts $\mathcal{P}(x)$ un

- $\mathfrak{K}_1 \leftharpoondown \{x \in \mathfrak{K} \mid \mathcal{P}(x) \sim p\}$,
- $\mathfrak{K}_2 \leftharpoondown \{x \in \mathfrak{K} \mid \mathcal{P}(x) \sim a\}$,
- $\mathfrak{K}_1 \cup \mathfrak{K}_2 = \mathfrak{K}$,
- $|\mathfrak{K}_2| < \aleph_0$,

tad saka, ka *gandrīz visiem* $x \in \mathfrak{K}$ *piemīt īpašība* $\mathcal{P}$. Šai situācijā mēdz lietot apzīmējumu $\overset{\infty}{\forall}\, x\ \mathcal{P}(x)$.

Kas attiecas uz summu $\sum_{i \in \mathcal{I}} a_i x_i$, tad tā ir definēta tikai galīgam saskaitāmo skaitam. Šai gadījumā frāze "gandrīz visi $a_i = 0$" nozīmē to, ka summācīja ir veikta tikai pa tiem kopas $\mathcal{I}$ elementiem i, kuriem $a_i \neq 0$. Formāli to visu var paskaidrot šādi. Pieņemsim, ka

- $\mathcal{J} \rightleftharpoons \{i \in \mathcal{I} \,|\, a_i \neq 0\}$,
- $|\mathcal{J}| < \aleph_0$,

tad
$$\sum_{i\in\mathcal{I}} a_i x_i \rightleftharpoons \sum_{i\in\mathcal{J}} a_i x_i.$$
Visbeidzot der atzīmēt, ka
$$\sum_{i\in\emptyset} a_i x_i \rightleftharpoons 0.$$

5.2.2. Definīcija. *Saka, ka sistēma $\mathfrak{A}$ izsakāma ar sistēmu $\mathfrak{A}'$, ja katrs sistēmas $\mathfrak{A}$ vektors izsakāms ar sistēmu $\mathfrak{A}'$.*

5.2.3. Apgalvojums (Lineārās izsakāmības transitivitāte). *Ja sistēma $\mathfrak{A}$ izsakāma ar sistēmu $\mathfrak{A}'$ un sistēma $\mathfrak{A}'$ izsakāma ar sistēmu $\mathfrak{A}''$, tad sistēma $\mathfrak{A}$ izsakāma ar sistēmu $\mathfrak{A}''$.*

□ Saskaņā ar doto, ja $x \in \mathfrak{A}$, tad eksistē tāda galīga kopas $\mathfrak{A}'$ apakškopa $\mathfrak{B}'$, ka
$$x = \sum_{y\in\mathfrak{B}'} a_y y,$$
kur visi a_y ir gredzena elementi. Savukārt katram $y \in \mathfrak{B}'$ eksistē tāda galīga kopas $\mathfrak{A}''$ apakškopa $\mathfrak{B}''_y$, ka
$$y = \sum_{z\in\mathfrak{B}''_y} b_z z,$$
kur visi a_z ir gredzena elementi. No šejienes
$$x = \sum_{y\in\mathfrak{B}'} a_y y = \sum_{y\in\mathfrak{B}'} a_y \sum_{z\in\mathfrak{B}''_y} b_z z = \sum_{y\in\mathfrak{B}'} \sum_{z\in\mathfrak{B}''_y} a_y b_z z.$$
Šajā summā saskaitāmo skaits ir galīgs, jo kopas $\mathfrak{B}'$ un $\mathfrak{B}''_y$ ir galīgas. ■

5.2.4. Definīcija. *Pieņemsim, ka M ir R–modulis un $\mathfrak{A} \subseteq M$. Kopu*
$$\mathcal{L}(\mathfrak{A}) \rightleftharpoons \{x \,|\, x \text{ ir izsakāms ar sistēmu } \mathfrak{A}\}$$
sauc par sistēmas $\mathfrak{A}$ lineāro čaulu.

Ja kopa $\mathfrak{A}$ ir galīga, teiksim, $\mathfrak{A} = \{x_1, x_2, \ldots, x_n\}$, tad lineārās čaulas $\mathcal{L}(\mathfrak{A})$ apzīmēšanai lieto pierakstu $\mathcal{L}(x_1, x_2, \ldots, x_n)$. Ja kopa $\mathfrak{A}$ ir vienelementīga kopa $\{x\}$, tad lineārās čaulas $\mathcal{L}(\mathfrak{A})$ apzīmēšanai lieto pierakstu Rx.

5.2.5. Vingrinājums. *Ja $\mathfrak{A}$ ir R–moduļa M apakškopa, tad lineārā čaula $\mathcal{L}(\mathfrak{A})$ ir apakšmodulis.*

5.2.6. Apgalvojums. *Ja $\mathfrak{A}$ ir R–moduļa M apakškopa, tad lineārā čaula*

$$\mathcal{L}(\mathfrak{A}) = \bigcap_{\mathfrak{A} \subseteq N \in \mathfrak{N}} N,$$

kur $\mathfrak{N}$ ir moduļa M visu apakšmoduļu saime.

$\square$ (i) Pieņemsim, ka $\mathcal{U} \leftharpoondown \bigcap_{\mathfrak{A} \subseteq N \in \mathfrak{N}} N$. Tā kā $\mathcal{L}(\mathfrak{A})$ ir viens no moduļiem, kas satur kopu kopu $\mathfrak{A}$, tad $\mathcal{U} \subseteq \mathcal{L}(\mathfrak{A})$.

(ii) Tā kā $\mathfrak{A} \subseteq \mathcal{U}$ un $\mathcal{U}$ ir moduļa M apakšmodulis, tad tas satur jebkuru sistēmas $\mathfrak{A}$ vektoru lineāru kombināciju. Tātad $\mathcal{L}(\mathfrak{A}) \subseteq \mathcal{U}$.

(iii) Mēs parādījām, ka $\mathcal{U} \subseteq \mathcal{L}(\mathfrak{A}) \subseteq \mathcal{U}$. Līdz ar to $\mathcal{L}(\mathfrak{A}) = \mathcal{U}$. $\blacksquare$

5.3. Homomorfismi

5.3.1. Definīcija. *Pieņemsim, ka M un M' ir R–moduļi. Attēlojumu*

$$f : M \to M'$$

sauc par moduļu homomorfismu, ja

$$\begin{aligned} f(x+y) &= f(x) + f(y), \\ f(ax) &= af(x). \end{aligned}$$

Līdzīgi kā pusgrupu gadījumā bijektīvu homomorfismu sauc par *izomorfismu.* Šai situācijā moduļus M un M' sauc par *izomorfiem* moduļiem. Sirjektīvu homomorfismu sauc par *epimorfismu.* Injektīvu homomorfismu sauc par *monomorfismu.*

Moduļu homomorfismu $f : M \to M$ sauc par *endomorfismu.* Ja endomorfisms ir bijekcija, tad to sauc par *automorfismu.*

5.3.2. Piemēri. (i) Pieņemsim, ka R — gredzens. Attēlojums

$$f : \mathrm{Mat}_n^m(R) \to R^n : \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ . & . & . & . \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \mapsto (a_{11}, a_{21}, \dots, a_{n1})$$

ir R–moduļu homomorfisms.

(ii) Pieņemsim, ka $A \in \mathrm{Mat}_n^m(\mathbb{R})$. Attēlojums

$$f : \mathbb{R}^n \to \mathbb{R}^n : (x_1, x_2, \dots, x_n) \mapsto (x_1, x_2, \dots, x_n)A$$

ir endomorfisms.

5.3.3. Apgalvojums. *Ja $f : M \to M'$ ir R–moduļu homomorfisms, tad* Imf *ir moduļa M' apakšmodulis.*

$\square$ (i) Pieņemsim, ka x' un y' ir kopas Imf vektori, tad eksistē tādi kopas M vektori x un y, ka $f(x) = x'$ un $f(y) = y'$. No šejienes

$$x' + y' = f(x) + f(y) = f(x + y) \in \mathrm{Im}f.$$

(ii) Pieņemsim, ka $a \in R$, tad $ax' = af(x) = f(ax) \in \mathrm{Im}f$. $\blacksquare$

5.4. Kongruences

5.4.1. Definīcija. *Kopā M definētu ekvivalences tipa predikātu $\equiv$ sauc par R–moduļa M kongruenci, ja tā ir grupas M kongruence, turklāt katram gredzena R elementam a un katram kopas M elementu pārim x, y izpildās nosacījums:*

$$x \equiv y \Rightarrow ax \equiv ay.$$

5.4.2. Apgalvojums. *Ja $\equiv$ ir R–moduļa M kongruence, tad $M/\!\equiv$ ir R–modulis M, kur*

$$[x] + [y] \leftharpoondown [x + y] \qquad \text{un} \qquad a[x] \leftharpoondown [ax].$$

□ (i) Tā kā $\equiv$ ir kongruence komutatīvajā grupā M, tad saskaitīšana definēta korekti.

(ii) Ja $[x] = [y]$, tad $x \equiv y$. Tā kā $\equiv$ ir kongruence, tad $\forall a \in R\ ax \equiv ay$; tātad $[ax] = [ay]$. Līdz ar to konstatēts, ka attēlojums

$$R \times M/{\equiv} \to\ M/{\equiv}$$

definēts korekti.

(iii)

$$(ab)[x] = [(ab)x] = [a(bx)] = a[bx] = a(b[x])$$

Tātad

$$\langle R, M/{\equiv}, \cdot, \circ\rangle, \qquad \text{kur} \qquad a \circ [x] \leftharpoondown [ax],$$

ir multiplikatīvā monoīda R iedarbība uz kopu $M/{\equiv}$ no kreisās puses.

(iv)

$$\begin{aligned} a([x] + [y]) &= a[x + y] = [a(x + y)] = [ax + ay] = [ax] + [ay] \\ &= a[x] + a[y], \\ (a + b)[x] &= [(a + b)x] = [ax + by] = [ax] + [by] = a[x] + b[x]. \end{aligned}$$

Tas demonstrē, ka izpildās abi distributīvie likumi.

(v) Visu savelkot kopā tagad varam secināt, ka $M/{\equiv}$ ir R–modulis. ■

5.4.3. Definīcija. *Moduli $M/\equiv$ pēc kongruences $\equiv$ sauc par faktormoduli pēc kongruences $\equiv$.*

5.4.4. Vingrinājums. Attēlojums $\pi : M \to M/{\equiv}: x \mapsto [x]$ ir R–moduļu epimorfisms.

Līdzīgi kā pusgrupu gadījumā, attēlojumu

$$\pi : M \to M/{\equiv}: x \mapsto [x]$$

sauc par *dabīgo* jeb *kanonisko homomorfismu.*

5.4.5. Teorēma. *Katrai moduļu kongruencei $\equiv$ eksistē tāds moduļa M apakšmodulis N, ka* $\qquad M/N = M/{\equiv}.$

□ Teorēma 3.6.12 apgalvo, ka

$$[0] \trianglelefteq M \qquad \text{un} \qquad M/[0] = M/\!\equiv .$$

Tas viss attiecas uz aditīvo grupu M.

Tagad kopā $R \times M/[0]$ definējam iedarbību:

$$a(x + [0]) \leftharpoondown ax + [0].$$

Atliek konstatēt, ka $[0]$ ir moduļa M apakšmodulis un $a(x + [0]) = a[x]$.

(i) Pieņemsim, ka $x \in [0]$ un $a \in R$, tad $x \equiv 0$. Ja reiz $\equiv$ ir kongruence, tad $ax \equiv a0 = 0$. Līdz ar to $ax \in [0]$. Tātad $[0]$ ir moduļa M apakšmodulis.

(ii) Parādīsim, ka $x + [0] = [x]$.

a) Pieņemsim, ka $y \in x+[0]$, tad (Lemmas 3.4.4 un 3.4.8), tad $y-x \in [0]$. Tas nozīmē, ka $y - x \equiv 0$ jeb $x \equiv y$. Tātad $y \in [x]$, t.i., $x + [0] \subseteq [x]$.

b) Pieņemsim, ka $y \in [x]$, tad $y \equiv x$ jeb $y - x \equiv 0$. Tātad $y - x \in [0]$. Tas saskaņā ar Lemmām 3.4.8 un 3.4.4 ļauj secināt, ka $y \in x + [0]$. Tātad $[x] \subseteq [x] + [0]$.

c) Mēs tikko parādījām (punkti a) un b)), ka $x + [0] \subseteq [x] \subseteq [x] + [0]$. Tātad $x + [0] = [x]$.

(iii) Tā rezultātā kopas $M/[0]$, $M/\!\equiv$ sakrīt un

$$a(x + [0]) = ax + [0] = [ax] = a[x],$$

t.i., iedarbība kopā $R\times M/[0]$ definēta tāpat kā kopā $R\times M/\!\equiv$. Tātad $M/\!\equiv$ un $M/[0]$ sakrīt arī kā moduļi. ■

5.4.6. Teorēma. *Katram R–moduļa M apakšmodulim N eksistē tāda kongruence $\equiv$, ka M/N un $M/\!\equiv$ sakrīt kā R–moduļi.*

□ (i) Saskaņā ar Apgalvojumu 3.6.10 ekvivalences tipa predikāts $\equiv_N^k$ ir kongruence grupā M.

(ii) Pieņemsim, ka $x \equiv_N^k y$ un $a \in R$, tad saskaņā ar $\equiv_N^k$ definīciju (Vingrinājums 3.4.1(ii)) $x + N = y + N$. No šejienes $x - y \in N$. Tā kā N ir moduļa M apakšmodulis, tad

$$\begin{aligned} ax - ay &= a(x - y) \in N, \\ ax + N &= ay + N, \\ ax &\equiv_N^k ay. \end{aligned}$$

Tātad $\equiv_I^k$ ir moduļa M kongruence.

(iii) $[0]_N^k = \{x \,|\, x + N = 0 + N\} = N$. Tagad atsaucoties uz Teorēmas 5.4.5 pierādījumu, secināms $M/N = M/\equiv_I^k$. ■

5.4.7. Apgalvojums. *Ja $f : M \to M'$ ir moduļu homomorfisms, tad*

$$\mathrm{Ker} f \leftharpoondown \{x \mid f(x) = 0\}$$

ir moduļa M apakšmodulis.

□ (i) Saskaņā ar 74. lappusē izklāstīto $\mathrm{Ker} f$ ir grupas M apakšgrupa.

(ii) Pieņemsim, ka $a \in R$ un $x \in \mathrm{Ker} f$, tad

$$f(ax) = af(x) = a0 = 0.$$

Tātad $ax \in \mathrm{Ker} f$.

(iii) Tas viss kopumā (punti (i)–(ii)) demonstrē, ka $\mathrm{Ker} f$ ir moduļa M apakšmodulis. ■

Moduļu teorijā, līdzīgi kā grupu teorijā, šo apakšmoduli $\mathrm{Ker} f$ sauc par *homomorfisma f kodolu.*

5.4.8. Teorēma. *Katram R–moduļu homomorfismam $f : M \to M'$ eksistē viens vienīgs moduļu homomorfisms $f_* : M/\mathrm{Ker} f \to M'$, kam diagramma*

$$\begin{tikzcd} M \arrow[rr, "f"] \arrow[dr, "\pi"'] & & M' \\ & M/\mathrm{Ker} f \arrow[ur, "f_*"'] & \end{tikzcd}$$

ir komutatīva; turklāt šis homomorfisms f_* ir monomorfisms.

□ Šis rezultāts pierādīts (Teorēma 3.7.1) grupām. Mums atliek parādīt, ka $f_* : M/\mathrm{Ker} f \to M'$ ir moduļu homomorfisms.

Pieņemsim, ka $a \in R$ un $[x] \in M/\mathrm{Ker}$, tad

$$\begin{aligned} f_*(a[x]) &= f_*([ax]) = f_* \circ \pi(ax) = f(ax) = af(x) \\ &= af \circ \pi(x) = af_*([x]). \quad ■ \end{aligned}$$

5.4.9. Sekas (Izomorfisma teorēma). $\quad G/\mathrm{Ker} f \cong \mathrm{Im} f$

5.5. Homomorfismu grupa

Pieņemsim, ka M un M' ir R–moduļi, tad

$$\mathrm{Hom}(M, M') \leftharpoondown \{f : M \to M' \mid f \text{ ir moduļu homomorfisms}\}.$$

Kopā $\mathrm{Hom}(M, M')$ definēsim operāciju $+$, ko sauksim par *homomorfismu summu.* Ja f un g ir kopas $\mathrm{Hom}(M, M')$ elementi, t.i., tie ir moduļu M, M' homomorfismi, tad

$$\forall x \in M \quad x(f+g) \leftharpoondown xf + xg.$$

5.5.1. Teorēma. $\langle \mathrm{Hom}(M, M'), +\rangle$ *ir komutatīva grupa.*

$\square$ (i) Vispirms parādīsim, ka $\langle \mathrm{Hom}(M, M'), +\rangle$ ir grupoīds.

a) Pieņemsim, ka $a \in R$, $x \in M$ un f, g ir moduļu M, M' homomorfismi, tad

$$\begin{aligned}(ax)(f+g) &= (ax)f + (ax)g = a(xf) + a(xg) = a((xf) + (xg)) \\ &= a(x(f+g)).\end{aligned}$$

b) Pieņemsim, ka $y \in M$, tad

$$\begin{aligned}(x+y)(f+g) &= (x+y)f + (x+y)g = (xf + yf) + (xg + yg) \\ &= (xf + xg) + (yf + yg) = x(f+g) + y(f+g).\end{aligned}$$

c) Ņemot vērā a) un b), secināms: $f + g \in \mathrm{Hom}(M, M')$.

(ii) Ievērojam, attēlojums $0 : M \to M' : x \mapsto 0'$ ir moduļu M, M' homomorfisms. Te $0 : M \to M'$ lietots attēlojuma apzīmēšanai, taču $0'$ nav attēlojums, bet apzīmē tikai grupas M' neitrālo elementu.

Saskaņā ar attēlojuma 0 definīciju $0 + f = f = f + 0$.

(iii) Parādīsim, ka attēlojums $-f : M \to M' : x \mapsto -xf$ ir moduļu M, M' homomorfisms.

$$\begin{aligned}(ax)(-f) &= -(axf) = -(a(xf)) = a(-xf) = a(x(-f)), \\ (x+y)(-f) &= -(x+y)f = -(xf + yf) = -xf + (-yf) \\ &= x(-f) + y(-f).\end{aligned}$$

(iv) Atliek parādīt, ka

$$\begin{aligned}f + (-f) &= 0, \\ f + (g+h) &= (f+g) + h, \\ f + g &= g + f,\end{aligned}$$

ko atstājam lasītājam kā vingrinājumu. $\blacksquare$

5.6. Endomorfismi

Pieņemsim, ka M ir R–modulis. Kopā $\mathrm{End}(M) \leftharpoondown \mathrm{Hom}(M, M)$ bez endomorfismu summas aplūkosim arī endomorfismu kompozīciju.

5.6.1. Teorēma. $\langle \mathrm{End}(M), +, \cdot \rangle$ *ir gredzens ar vieninieku. Te operācija* $\cdot$ *ir attēlojumu kompozīcija.*

□ (i) Teorēma 5.5.1 dod iespēju apgalvot, ka $\langle \mathrm{End}(M), + \rangle$ ir komutatīva grupa.

(ii) Parādīsim, ka $\langle \mathrm{End}(M), \cdot \rangle$ ir monoīds. Ņemot vērā Vingrinājumu 2.6.2(ii), mums atliek tikai konstatēt, ka $\langle \mathrm{End}(M), \cdot \rangle$ ir grupoīds un attēlojums $\mathbb{I}_M$ ir endomorfisms.

a) Pieņemsim, ka $a \in R$, $x \in M$ un f, g ir moduļa M endomorfismi, tad

$$(ax)(fg) \;=\; g(f(ax)) = g(af(x)) = ag(f(x)) = a(x(fg)).$$

b) Pieņemsim, ka $y \in M$, tad

$$\begin{aligned}(x+y)(fg) &= g(f(x+y)) = g(f(x) + f(y)) = g(f(x)) + g(f(y)) \\ &= x(fg) + y(fg).\end{aligned}$$

c) Ņemot vērā a) un b), secinām: $\langle \mathrm{End}(M), \cdot \rangle$ ir grupoīds.

d) Mēs atstājam lasītājam kā vingrinājumu pierādīt faktu, ka $\mathbb{I}_M$ ir endomorfisms.

(iii) Parādīsim kā pierādāms viens distributīvais likums. Otra likuma pierādījumu atstājam lasītājam kā vingrinājumu. Pieņemsim, ka $h \in \mathrm{End}(M)$, tad

$$\begin{aligned}x(f+g)h &= (x(f+g))h = (xf + xg)h = (xf)h + (xg)h \\ &= x(fh) + x(gh).\end{aligned}$$

Tātad $(f+g)h = fh + gh$. ■

5.6.2. Vingrinājums. $\langle \mathrm{End}(M), +, \circ \rangle$ ir gredzens ar vieninieku. Te operācija $\circ$ (skatīt 10. lappusi) ir attēlojumu kompozīcija.

Izrādās, ja M ir R–modulis, tad šo pašu grupu M var uztvert arī kā $\mathrm{End}(M)$–moduli. Mums tikai jānodefinē iedarbība:

$$\mathrm{End}(M) \times M \xrightarrow{\odot} M : f \odot x \leftharpoondown f(x).$$

5.6.3. Teorēma. *Ja M ir R–modulis, tad $\langle \mathrm{End}(M), M, +, \circ, \oplus, \odot \rangle$ ir $\mathrm{End}(M)$–modulis M. Te operācija $+$ ir endomorfismu summa, $\circ$ ir endomorfismu kompozīcija un $\oplus$ ir grupas M komutatīvā operācija.*

□ (i) Mēs jau zinam (Vingrinājums 5.6.2), ka $\langle \mathrm{End}(M), +, \circ \rangle$ ir gredzens ar vieninieku.

(ii) Saskaņā ar doto $\langle M, \oplus \rangle$ ir komutatīva grupa.

(iii) Pieņemsim, ka f, g ir endomorfismi un $x \in M$, tad

$$\begin{aligned} (f \circ g) \odot x &= (f \circ g)(x) = f(g(x)) = f \odot (g \odot x), \\ \mathbb{I} \odot x &= \mathbb{I}(x) = x, \end{aligned}$$

tātad $\langle \mathrm{End}(M), M, \circ, \odot \rangle$ ir $\mathrm{End}(M)$ iedarbība uz M no kreisās puses.

(iv) Pieņemsim, ka $y \in M$, tad

$$\begin{aligned} f \odot (x \oplus y) &= f(x \oplus y) = f(x) \oplus f(y) = (f \odot x) \oplus (f \odot y), \\ (f + g) \odot x &= (f + g)(x) = f(x) \oplus g(x) = (f \odot x) \oplus (g \odot x). \end{aligned}$$

(v) Tas viss kopumā (punti (i)–(iv)) demonstrē, ka

$$\langle \mathrm{End}(M), M, +, \circ, \oplus, \odot \rangle$$

ir kreisais $\mathrm{End}(M)$–modulis M. ■

Brīdinājums. Parasti $+$ un $\oplus$ vietā lieto tikai simbolu $+$, bet simbolus $\circ$ un $\odot$ vispār nelieto. Tai vietā, lai rakstītu $(f \circ g) \odot x$ vienkārši raksta $f(g(x))$. Arī mēs pieturēsimies pie šādas norunas.

5.7. Apakšmoduļu summa

5.7.1. Definīcija. *Moduļa S apakšmoduļu saimes $\{S_i \mid i \in \mathcal{I}\}$ apvienojuma $\bigcup\limits_{i \in \mathcal{I}} S_i$ lineāro čaulu sauc par apakšmoduļu saimes $\{S_i \mid i \in \mathcal{I}\}$ summu.*

Tātad saskaņā ar Definīciju 5.2.4 apakšmoduļu saimes $\{S_i \mid i \in \mathcal{I}\}$ summa ir $\mathcal{L}(\bigcup\limits_{i \in \mathcal{I}} S_i)$. Ja kopu saime $\bigcup\limits_{i \in \mathcal{I}} S_i$ nav pārāk liela, piemēram, tā sastāv no n apakšmoduļiem $S_1, S_2, \ldots, S_n$, tad $\mathcal{L}(\bigcup\limits_{i=1}^{n} S_i)$ sauc par apakšmoduļu

$S_1, S_2, \ldots, S_n$ summu. Šai gadījumā summas apzīmēšanai parasti lieto pierakstu $S_1 + S_2 + \ldots + S_n$, t.i,

$$S_1 + S_2 + \ldots + S_n \leftharpoondown \mathcal{L}(\bigcup_{i=1}^{n} S_i).$$

5.7.2. Apgalvojums.

$$S_1 + S_2 + \ldots + S_n = \{s_1 + s_2 + \ldots + s_n \,|\, \forall i \in \overline{1,n}\ s_i \in S_i\}.$$

□ Pieņemsim, ka

$$\begin{array}{rcl} S & \leftharpoondown & S_1 + S_2 + \ldots + S_n, \\ S' & \leftharpoondown & \{s_1 + s_2 + \ldots + s_n \,|\, \forall i \in \overline{1,n}\ s_i \in S_i\}. \end{array}$$

Uzreiz no S un S' definīcijas izriet, ka $S' \subseteq \mathcal{L}(\bigcup_{i=1}^{n} S_i) = S$. Mūsu mērķis: pārādīt, ka $S = S'$.

Ja $s \in \bigcup_{i=1}^{n} S_i$, tad eksistē tāds k, ka $s \in S_k$. No šejienes

$$s = \underbrace{0 + \ldots + 0}_{k-1 \text{ reizi}} + s + 0 + \ldots + 0 \in S'.$$

Tātad $\bigcup_{i=1}^{n} S_i \subseteq S'$. Atliek parādīt, ka S' ir modulis, tas saskaņā ar Apgalvojumu 5.2.6 $\mathcal{L}(\bigcup_{i=1}^{n} S_i) \subseteq S'$.

(i) Ja $a \in R$ un $s = s_1 + s_2 + \ldots + s_n \in S'$, tad

$$as = as_1 + as_2 + \ldots + as_n \in S'.$$

(ii) Ja $s' = s'_1 + s'_2 + \ldots + s'_n \in S'$, tad

$$s + s' = (s_1 + s'_1) + (s_2 + s'_2) + \ldots + (s_n + s'_n) \in S'. \quad \blacksquare$$

5.7.3. Definīcija. *Summu $S_1 + S_2 + \ldots + S_n$ sauc par tiešo summu, ja*

$$\forall i (S_1 + \ldots + S_{i-1} + S_{i+1} + \ldots + S_n) \cap S_i = 0.$$

Ja $S_1 + S_2 + \ldots + S_n$ ir tiešā summa, tad lieto apzīmējumu

$$S_1 \oplus S_2 \oplus \ldots \oplus S_n \qquad \text{vai arī} \qquad \bigoplus_{i=1}^{n} S_i.$$

5.7.4. Vingrinājums. $\bigoplus_{i=1}^{n} S_i = \bigoplus_{i=1}^{n} S_{\sigma(i)}$ *jebkurai substitūcijai* $\sigma \in \mathfrak{S}_n$.

5.7.5. Teorēma. *Pieņemsim, ka* $S = S_1 + S_2 + \ldots + S_n$*, tad sekojošie apgalvojumi ir ekvivalenti.*

(i) $S = S_1 \oplus S_2 \oplus \ldots \oplus S_n$*;*

(ii) $\forall i \in \overline{2,n}\ (S_1 + \ldots + S_{i-1}) \cap S_i = 0$*;*

(iii) *katram kopas* S *vektoram* s *eksistē viena vienīga reprezentācija izskatā* $s = s_1 + s_2 + \ldots + s_n$*, kur visi* $s_i \in S_i$*;*

(iv) *ja visi* $s_i \in S_i$ *un* $s_1 + s_2 + \ldots + s_n = 0$*, tad visi* $s_i = 0$.

□ (i) ⇒ (ii) Definīcija 5.7.3.
(ii) ⇒ (iii) Pieņemsim, ka

$$s_1 + s_2 + \ldots + s_n = s'_1 + s'_2 + \ldots + s'_n \qquad \text{un} \qquad k \leftharpoondown \max_i (s_i \neq s'_i).$$

No šejienes: ja $j > k$, tad $s_j = s'_j$. Tas nozīmē, ka

$$\begin{aligned} s'_k - s_k &= (s_1 - s'_1) + (s_2 - s'_2) + \ldots + (s_{k-1} - s'_{k-1}) \\ &\in S_k \cap (S_1 + \ldots + S_{k-1}) = 0. \end{aligned}$$

Tātad $s'_k - s_k = 0$, proti, $s_k = s'_k$, kas ir pretrunā ar indeksa k izvēli.

(iii) ⇒ (iv) Ievērojam $0 = 0 + 0 + \ldots + 0$, un tā kā saskaņā ar (iii) katram s eksistē viena vienīga reprezentācija izskatā $s = s_1 + s_2 + \ldots + s_n$, tad visi $s_i = 0$.

(iv) ⇒ (i) Pieņemsim pretējo, proti,

$$\exists s \neq 0\ \exists i \quad s \in (S_1 + \ldots + S_{i-1} + S_{i+1} + \ldots + S_n) \cap S_i.$$

Tātad eksistē tādi $s_j \in S_j$, ka $s = s_1 + \ldots + s_{i-1} + s_{i+1} + \ldots + s_n$. No šejienes

$$0 = s_1 + \ldots + s_{i-1} + (-s) + s_{i+1} + \ldots + s_n \qquad \text{un} \qquad -s \in S_i.$$

Saskaņā ar (iv) $-s = 0$, t.i., $s = 0$. Pretruna! ■

5.7.6. Sekas. *Divu apakšmoduļu summa* $S + T$ *ir tiešā summa tad un tikai tad, ja* $S \cap T = 0$.

5.7.7. Vingrinājums. Ja $S = \bigoplus\limits_{i=1}^{n} S_i$ un $S_i = \bigoplus\limits_{j=1}^{k_i} S_{ij}$, tad katram indeksam i

$$S = (S_1 \oplus S_2 \oplus \ldots \oplus S_{i-1}) \oplus (S_i \oplus S_{i+1} \oplus \ldots \oplus S_n)$$

un $\quad S = \bigoplus\limits_{i=1}^{n} \bigoplus\limits_{j=1}^{k_i} S_{ij}.$

5.7.8. Definīcija. *Pieņemsim, ka* $\{\langle R, M_i, +, \cdot, \overset{i}{+}, \overset{i}{\circ}\rangle \mid i \in \overline{1,k}\}$ *ir* R*–moduļu saime un*

$$M \rightleftharpoons M_1 \times M_2 \times \ldots \times M_k.$$

- *Definēsim iedarbību* $\circ$ *izmantojot iedarbības* $\overset{i}{\circ}$. *Ja* $a \in R$ *un* $(x_1, x_2, \ldots, x_k) \in M$, *tad*

$$a \circ (x_1, x_2, \ldots, x_k) \rightleftharpoons (a \overset{1}{\circ} x_1, a \overset{2}{\circ} x_2, \ldots, a \overset{k}{\circ} x_k).$$

- *Kopā* M *definēsim saskaitīšanas operāciju* $+$ *izmantojot saskaitīšanas operācijas* $\overset{i}{+}$ *kopās* M_i. *Ja* $(y_1, y_2, \ldots, y_k) \in M$, *tad*

$$(x_1, x_2, \ldots, x_k) + (y_1, y_2, \ldots, y_k) \rightleftharpoons (x_1 \overset{1}{+} y_1, x_2 \overset{2}{+} y_2, \ldots, x_k \overset{k}{+} y_k).$$

Šādi definēto moduli M *sauc par moduļu* $M_1, M_2, \ldots, M_k$ *tiešo ārējo summu.*

Brīdinājums. Parasti literatūrā tiešo ārējo summu apzīmē ar to pašu simbolu $\oplus$ kā tiešo summu, taču, lai lasītājam atvieglotu izpratni, mēs moduļu $M_1, M_2, \ldots, M_k$ tiešās ārējās summas apzīmēšanai lietosim pierakstu $\overline{\bigoplus}\limits_{i=1}^{k} M_i$.

5.7.9. Apgalvojums. *Ja* $\quad M = \overline{\bigoplus}\limits_{i=1}^{k} M_i,$

$$S_i \rightleftharpoons \{(x_1, x_2, \ldots, x_k) \in M \mid a_j = 0, \text{ ja } j \neq i\},$$

tad

(i) *katrs* S_i *ir moduļa* M *apakšmodulis;*

(ii) $S_i \cong M_i$*;*

(iii) $M = \bigoplus_{i=1}^{k} S_i$.

□ Attēlojums $f : M_i \to S_i : x \to (x_1, x_2, \ldots, x_k)$, kur

$$x_j \;=\; \begin{cases} x, & \text{ja} \quad j = i; \\ 0_{M_j}, & \text{ja} \quad j \neq i \end{cases}$$

ir moduļu izomorfisms $M_i \cong S_i$. Savukārt vienādība

$$(x_1, x_2, \ldots, x_k) = (x_1, 0, \ldots, 0) + (0, x_2, \ldots, 0) + \ldots + (0, 0, \ldots, x_k)$$

parāda, ka $M = \bigoplus_{i=1}^{k} S_i$. ■

5.7.10. Apgalvojums. *Ja* $M = \bigoplus_{i=1}^{k} M_i$*, katrs* N_i *ir moduļa* M_i *apakšmodulis un* $N = N_1 + N_2 + \ldots + N_k$*, tad faktormodulis*

$$M/N \cong \overline{\bigoplus_{i=1}^{k}} M_i/N_i.$$

□ Apskatīsim attēlojumu

$$f : M \to \overline{\bigoplus_{i=1}^{k}} M_i/N_i : x_1 + x_2 + \ldots + x_k \mapsto ([x_1], [x_2], \ldots, [x_k]),$$

kur $x_i \in M_i$ un $[x_i]$ — faktormoduļa M_i/N_i blakusklase. Saskaņā ar Teorēmu 5.7.5 attēlojums f definēts korekti. No f definīcijas izriet, ka šis attēlojums ir sirjekcija.

Ja $x = x_1 + x_2 + \ldots + x_k$, visi $x_i \in M_i$ un $f(x) = 0$, tad $\forall i \; x_i \in N_i$. Tas norāda, ka $x \in N$. Tāpēc $\mathrm{Ker} f \subseteq N$. Ja reiz $N = N_1 + N_2 + \ldots + N_k$, tad $N \subseteq \mathrm{Ker} f$. Tātad $N = \mathrm{Ker} f$.

Vairs atliek tikai atsaukties uz izomorfisma teorēmu. ■

5.7.11. Sekas. $(M_1 \oplus M_2)/M_2 \cong M_1$.

□ Tikko pierādītā teorēma ir spēkā, ja $k = 2$, $N_1 = 0$ un $N_2 = M_2$. ■

5.7.12. Definīcija. *Moduļa M apakšmoduli S sauc par moduļa M tiešo saskaitāmo, ja eksistē tāds moduļa M apakšmodulis N, ka $M = S \oplus N$.*

5.7.13. Apgalvojums. *Katram moduļa M tiešajam saskaitāmajam S eksistē faktormodulim M/S izomorfs moduļa M tiešs saskaitāmais.*

□ Ja S ir moduļa M tiešs saskaitāmais, tad eksistē tāds moduļa M apakšmodulis N, ka $M = S \oplus N$. Tagad ņemot vērā Sekas 5.7.11, iegūstam $(S \oplus N)/S \cong N$. Tātad $M/S \cong N$. ■

5.8. Ireducibli moduļi

5.8.1. Definīcija. *Moduļa M apakšmoduli $N \neq 0$ sauc par minimālu, ja katram moduļa M apakšmodulim H ir spēkā apgalvojums:*

$$0 \subseteq H \subset N \Rightarrow H = 0.$$

Moduli M sauc par *ireduciblu moduli*, ja tas ir moduļa M minimāls apakšmodulis.

Gredzena R apakšgredzenu I sauc par *kreiso ideālu*, ja

$$\forall a \in I \; \forall x \in R \quad ax \in I.$$

Gredzena R kreiso ideālu I sauc par *minimālu*, ja tas ir moduļa ${}_RR$ kreisais ideāls.

5.8.2. Piemēri. (i) Ja komutatīvas grupas G kārta ir pirmskaitlis, tad G ir minimāls $\mathbb{Z}$–modulis.

Pieņemsim, ka grupas G kārta ir pirmskaitlis p un N ir no 0 atšķirīgs $\mathbb{Z}$–moduļa G apakšmodulis, tad eksistē tāds $x \neq 0$, ka $x \in N$. Moduļa $\mathbb{Z}x$ kārta dala G kārtu, proti, pirmskaitli p. Tas iespējams tikai tad, ja paša $\mathbb{Z}x$ kārta ir vienāda ar p, t.i., $\mathbb{Z}x = G$.

(ii) Jebkurš ķermenis K kā modulis ${}_KK$ ir ireducibls.

Pieņemsim, ka $N = 0$ ir moduļa ${}_KK$ apakšmodulis, tad eksistē tāds $x \neq 0$, ka $x \in N$. Ja reiz $x \neq 0$, tad $x^{-1} \in K$. No šejienes $x_{-1}x = 1 \in N$.

Tālāk, patvaļīgam $a \in K$ elements $a = a1 \in N$, tāpēc $N = K$.

5.8.3. Teorēma. *Nenulles kreisais R–modulis M ir ireducibls tad un tikai tad, ja*

$$\forall x \in M \quad (x \neq 0 \Rightarrow M = Rx).$$

$\square$ $\Rightarrow$ Ja M ir ireducibls un $0 \neq x \in M$, tad Rx ir moduļa M nenulles apakšmodulis; tāpēc $Rx = M$.

$\Leftarrow$ Pieņemsim, ka M nav ireducibls, tad eksistē tāds moduļa M apakšmodulis N, ka $0 \neq N \subset M$. Izvēlamies $0 \neq x \in N$, tad $Rx \subseteq N$, tāpēc $m \neq Rx$. $\blacksquare$

5.9. Pilnīgi reducējami moduļi

5.9.1. Definīcija. *Moduļa M apakšmoduli $N \neq M$ sauc par maksimālo apakšmoduli, ja katram moduļa M apakšmodulim H ir spēkā izteikums:*

$$N \subset H \subseteq M \Rightarrow H = M.$$

Gredzena R kreiso ideālu I sauc par *maksimālo ideālu*, ja katram gredzena kreisajam ideālam J ir spēkā izteikums:

$$I \subset J \subseteq R \Rightarrow J = R.$$

5.9.2. Teorēma. *Kreisā R–moduļa M faktormodulis M/N ir ireducibls tad un tikai tad, ja N — maksimālais modulis.*

$\square$ $\Leftarrow$ Ja N — maksimālais apakšmodulis un $[0] \neq [x] \in M/N$, tad $x \notin N$. No šejienes $N \subset N + Rx \subseteq M$.

Ja reiz N ir maksimāls, tad $N + Rx = M$. No šejienes: ja $z \in M$, tad eksistē tādi $a \in R$ un $y \in N$, ka $z = y + ax$. Tā rezultātā

$$[z] = [y + ax] = [y] + [ax] = a[x],$$

t.i., $M/N = R[x]$. Saskaņā ar Teorēmu 5.8.3 tas nozīmē, ka M/N ir ireducibls.

$\Rightarrow$ Pieņemsim, ka M/N ir ireducibls, $N \subset H \subseteq M$, H ir moduļa M apakšmodulis un $x \in H \setminus N$, tad saskaņā ar Teorēmu 5.8.3 $M/N = R[x]$.

Brīvi izvēlētam $y \in M$ blaksusklase $[y] \in M/N = R[x]$, t.i., eksistē tāds $a \in R$, ka $[y] = a[x]$. No šejienes $[y] = [ax]$ jeb $y - ax \in N$. Tātad, eksistē tāds $z \in N$, ka $y - ax = z$. Tas nozīmē, ka

$$y = ax + z \in H.$$

Tātad $H = M$. $\blacksquare$

5.9.3. Definīcija. *Moduli M sauc par pilnīgi reducējamu jeb pusvienkāršu moduli, ja tas ir reprezentējams kā galīga skaita ireduciblu moduļu tiešā summa, t.i., eksistē tādi ireducibli moduļi $M_1, M_2, \ldots, M_k$, ka $M = \bigoplus_{i=1}^{k} M_i$.*

Vienošanās. Turpmāk šī paragrāfa ietvaros pieņemsim, ka M ir pilnīgi reducējams modulis un $M = \bigoplus_{i=1}^{k} M_i$ ir šī moduļa reprezentācija ar ireducibliem apakšmoduļiem.

5.9.4. Lemma. *Ja N ir moduļa M apakšmodulis un $0 \neq N \neq M$, tad pēc apakšmoduļu pārnumerācijas var panākt, ka*

$$\begin{aligned} M &= N \oplus M_1 \oplus M_2 \oplus \ldots \oplus M_\nu; \\ N &\cong M_{\nu+1} \oplus M_{\nu+2} \oplus \ldots \oplus M_k; \\ M/N &\cong M_1 \oplus M_2 \oplus \ldots \oplus M_\nu, \end{aligned}$$

kur $\nu \in \overline{1, k-1}$.

□ Pieņemsim, ka $M_1 \not\subseteq N$ (vajadzības gadījumā varam mainīt numerāciju). Tā rezultātā $M_1 \cap N \subseteq M_1$. Ja reiz M_1 ir ireducibls, tad $N \cap M_1 = 0$.

Ja $N + M_1 \neq M$, tad $(N + M_1) \cap M_2 = 0$ (vajadzības gadījumā varam mainīt numerāciju). Šo konstrukciju turpinam līdz

$$\begin{aligned} N + M_1 + \ldots + M_\nu &= M, \qquad \text{bet} \\ N + M_1 &= 0, \\ (N + M_1) \cap M_2 &= 0, \\ (N + M_1 + M_2) \cap M_3 &= 0, \\ \ldots \quad & \ldots \\ (N + M_1 + \ldots + M_{\nu-1}) \cap M_\nu &= 0. \end{aligned}$$

Saskaņā ar Teorēmu 5.7.5(ii) tas nozīmē, ka

$$M = N \oplus M_1 \oplus M_2 \oplus \ldots \oplus M_\nu.$$

Savukārt Vingrinājums 5.7.7 dod iespēju rakstīt

$$M = N \oplus (M_1 \oplus M_2 \oplus \ldots \oplus M_\nu),$$

t.i., N ir tiešs saskaitāmais. Tagad atsaucoties uz Sekām 5.7.11 varam apgalvot, ka

$$\begin{aligned} M/N &= N \oplus (M_1 \oplus M_2 \oplus \ldots \oplus M_\nu)/N \\ &\overset{\text{V5.7.4}}{=} (M_1 \oplus M_2 \oplus \ldots \oplus M_\nu) \oplus N/N \\ &\overset{\text{S5.7.11}}{=} M_1 \oplus M_2 \oplus \ldots \oplus M_\nu. \end{aligned}$$

Savukārt

$$\begin{aligned} & M/M_1 \oplus M_2 \oplus \ldots \oplus M_\nu \\ = \; & M_1 \oplus M_2 \oplus \ldots \oplus M_\nu \oplus M_{\nu+1} \oplus \ldots \oplus M_k/M_1 \oplus M_2 \oplus \ldots \oplus M_\nu \\ = \; & (M_1 \oplus M_2 \oplus \ldots \oplus M_\nu) \oplus (M_{\nu+1} \oplus \ldots \oplus M_k)/M_1 \oplus M_2 \oplus \ldots \oplus M_\nu \\ = \; & (M_{\nu+1} \oplus \ldots \oplus M_k) \oplus (M_1 \oplus M_2 \oplus \ldots \oplus M_\nu)/M_1 \oplus M_2 \oplus \ldots \oplus M_\nu \\ \cong \; & M_{\nu+1} \oplus \ldots \oplus M_k. \end{aligned}$$

Tātad

$$\begin{aligned} N &\cong N \oplus (M_1 \oplus M_2 \oplus \ldots \oplus M_\nu)/M_1 \oplus M_2 \oplus \ldots \oplus M_\nu \\ &= M/M_1 \oplus M_2 \oplus \ldots \oplus M_\nu \\ &\cong M_{\nu+1} \oplus \ldots \oplus M_k. \quad \blacksquare \end{aligned}$$

Vienošanās. Pieņemsim, ka N' ir moduļa M' apakšmodulis un

$$f : M'' \to M'$$

ir moduļu homomorfisms, tad

$$f^{-1}(N') \leftharpoondown \{x \in M'' \mid f(x) \in N'\}.$$

5.9.5. Vingrinājumi. (i) Ja N' ir moduļa M' apakšmodulis un $f : M'' \to M'$ ir moduļu homomorfisms, tad $f^{-1}(N')$ ir moduļa M'' apakšmodulis.

(ii) Ja

- $\varphi : N \to N_0$ ir moduļu izomorfisms;
- N_0 ir pilnīgi reducējams modulis;

- $N_0 = \bigoplus_{i=1}^{s}$ ir šī moduļa N_0 reprezentācija ar ireducibliem apakšmoduļiem,

tad

- N ir pilnīgi reducējams modulis un
- $N = \bigoplus_{i=1}^{s} \varphi^{-1}(N_i)$ ir šī moduļa N reprezentācija ar ireducibliem apakšmoduļiem.

5.9.6. Lemma. *Ja N ir moduļa M ireducibls apakšmodulis, tad*

$$\exists i\ N \cong M_i.$$

□ Saskaņā ar Lemmu 5.9.4 eksistē tāds indekss ν (vajadzības gadījumā mainot apakšmoduļu M_i numerāciju), ka

$$N \cong M_{\nu+1} \oplus M_{\nu+2} \oplus \ldots \oplus M_k.$$

Tā kā $N \cong M_{\nu+1} \oplus M_{\nu+2} \oplus \ldots \oplus M_k$, tad eksistē izomorfisms

$$\varphi : N \to M_{\nu+1} \oplus M_{\nu+2} \oplus \ldots \oplus M_k.$$

Saskaņā ar Vingrinājumu 5.9.5(ii)

$$N = \varphi^{-1}(M_{\nu+1}) \oplus \varphi^{-1}(M_{\nu+2}) \oplus \ldots \oplus \varphi^{-1}(M_k)$$

ir šī moduļa N reprezentācija ar ireducibliem apakšmoduļiem. Tā kā N pats ir ireducibls, tad šī summa satur tieši vienu saskaitāmo. ■

5.9.7. Teorēma. *Ja M ir pilnīgi reducējams modulis un $M = \bigoplus_{i=1}^{k} M_i$ ir šī moduļa reprezentācija ar ireducibliem apakšmoduļiem, tad*

- *moduļa M jebkurš apakšmodulis N ir pilnīgi reducējams;*
- *moduļa M jebkurš faktormodulis M/N ir pilnīgi reducējams;*
- *moduļa N katra ireduciblā komponente ir izomorfa kādam apakšmodulim M_i;*

- *moduļa M/N katra ireduciblā komponente ir izomorfa kādam apakšmodulim M_i;*
- *moduļa M katrs apakšmodulis ir moduļa M tiešs saskaitāmais;*
- *moduļa M katrs faktormodulis ir izomorfs kādam moduļa M apakšmodulim.*

□ Saskaņā ar Lemmu 5.9.4, ņemot vērā Vingrinājumu 5.9.5(ii), moduļa M katrs apakšmodulis N un arī faktormodulis M/N ir pilnīgi reducējams. Lemma 5.9.4 demonstrē, ka jebkurš moduļa M apakšmodulis N ir moduļa M tiešs saskaitāmis. Šī apakšmoduļa N ireduciblās komponentes (Lemma 5.9.6) ir izomorfas apakšmoduļiem M_i.

Tā kā eksistē tāds indekss ν (vajadzības gadījumā mainot apakšmoduļu M_i numerāciju), ka $M/N \cong M_1 \oplus M_2 \oplus \ldots \oplus M_\nu$, tad eksistē izomorfisms

$$\varphi : M/N \to M_1 \oplus M_2 \oplus \ldots \oplus M_\nu.$$

No šejienes (skatīt Vingrinājumu 5.9.5(ii))

$$M/N = \varphi^{-1}(M_1) \oplus \varphi^{-1}(M_2) \oplus \ldots \oplus \varphi^{-1}(M_\nu)$$

ir moduļa M/N reprezentācija ar ireducibliem apakšmoduļiem. Tagad atsaucoties uz Lemmu 5.9.6 secināms: moduļa M/N katrs ireducibls apakšmodulis N' ir izomorfs kādam apakšmodulim $\varphi^{-1}(M_i) \cong M_i$. Tātad moduļa M/N katra ireduciblā komponente ir izomorfa kādam no apakšmoduļiem M_i.

Ja reiz $M/N \cong M_1 \oplus M_2 \oplus \ldots \oplus M_\nu$, tad tas ir izomors moduļa M kādam apakšmodulim. ■

5.10. Galīgi ğenerēti moduļi

5.10.1. Definīcija. *R–moduli M sauc par galīgi ğenerētu moduli, ja eksistē tāda moduļa M galīga vektoru sistēma*

$$x_1, x_2, \ldots, x_n,$$

ka šīs sistēmas lineārā čaula $\mathcal{L}(x_1, x_2, \ldots, x_n) = M$.

5.10.2. Piemērs. Eksistē moduļi, kas nav galīgi ğenerēti.

Pieņemsim, ka R ir gredzens ar vieninieku un

$$R^\omega \leftharpoondown \{x \mid x : \mathbb{N} \to R\}.$$

Kopas R^ω elementus mēs sauksim par *ω–vārdiem.* Mēs lietosim šādus apzīmējumus: $x_i \leftharpoondown x(i), \qquad x \rightharpoondown (x_i) \rightharpoondown (x_0, x_1, \ldots, x_n, \ldots)$

Pieņemsim, ka

$$\begin{aligned} x &= (x_0, x_1, \ldots, x_n, \ldots) \in R^\omega, \\ y &= (y_0, y_1, \ldots, y_n, \ldots) \in R^\omega. \end{aligned}$$

Kopā R^ω definēsim divvietīgu operāciju

$$x + y \leftharpoondown (x_0 + y_0, x_1 + y_1, \ldots, x_n + y_n, \ldots)$$

Pieņemsim, ka $a \in R$, tad

$$ax \leftharpoondown (ax_0, ax_1, \ldots, ax_n, \ldots)$$

Līdz ar to R^ω ir pārvērsts par R–moduli.

5.10.3. Vingrinājums. *$V \leftharpoondown \{(x_0, x_1, \ldots, x_n, \ldots) \in R^\omega \mid \overset{\infty}{\forall} i \; x_i = 0\}$ ir moduļa R^ω apakšmodulis.*

Tagad parādīsim, ka V nav galīgi ğenerēts modulis. Pieņemsim pretējo, proti, $V = \mathcal{L}(v_1, v_2, \ldots, v_n)$, kur visi $v_i \in V$. No šejienes

$$\exists m \, \forall k > m \, \forall i \; v_k^i = 0, \qquad \text{kur} \qquad v_i = (v_0^i, v_1^i, \ldots, v_n^i, \ldots).$$

Tas nozīmē, ka nav iespējams iegūt vektoru

$$(\underbrace{1 + 1 + \ldots + 1}_{n+1 \text{ vieninieks}}, 0, 0, \ldots)$$

kā vektoru v_i lineāru kombināciju.

5.10.4. Teorēma. *Katrs galīgi ğenerēts R–modulis M ir izomorfs kādam moduļa R^n faktormodulim.*

$\square$ (i) Saskaņā ar doto eksistē galīgs skaits tādu vektoru $x_1, x_2, \ldots, x_n$, ka $M = \mathcal{L}(x_1, x_2, \ldots, x_n)$.

(ii) Parādīsim, ka attēlojums

$$f : R^n \to M : (a_1, a_2, \ldots, a_n) \mapsto a_1x_1 + a_2x_2 + \ldots + a_nx_n$$

ir moduļu sirjektīvs homomorfisms.

a) Ja $x \in M$, tad eksistē tādi gredzena R elementi $a_1, a_2, \ldots, a_n$, ka $x = a_1x_1 + a_2x_2 + \ldots + a_nx_n$. No šejienes $f(a_1, a_2, \ldots, a_n) = x$. Tātad f ir sirjekcija.

b) Pieņemsim, ka

$$\begin{aligned}
a &= (a_1, a_2, \ldots, a_n), \qquad \text{un} \\
b &= (b_1, b_2, \ldots, b_n), \qquad \text{tad} \\
f(a) + f(b) &= (a_1x_1 + a_2x_2 + \ldots + a_nx_n) + (b_1x_1 + b_2x_2 + \ldots + b_nx_n) \\
&= (a_1 + b_1)x_1 + (a_2 + b_2)x_2 + \ldots + (a_n + b_n)x_n \\
&= f(a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) = f(a + b).
\end{aligned}$$

c) Pieņemsim, ka $c \in R$, tad

$$\begin{aligned}
cf(a) &= c(a_1x_1 + a_2x_2 + \ldots + a_nx_n) \\
&= (ca_1x_1 + ca_2x_2 + \ldots + ca_nx_n) \\
&= f(ca_1, ca_2, \ldots, ca_n) = f(ca).
\end{aligned}$$

d) Tas viss kopumā (apakšpunkti a)–c)) demonstrē, ka $f : R^n \to M$ ir sirjektīvs moduļu homomorfisms.

(iii) Saskaņā ar izomorfisma teorēmu $R^n/\mathrm{Ker}f \cong M$. $\blacksquare$

6. nodaļa

ASOCIATĪVAS ALGEBRAS

Asociatīvas algebras, piemēri. Asociatīva algebra pār lauku. Apakšalgebras, to šķēlums. Algebras ideāli. Homomorfismi, algebras homomorfs attēls, kongruences, faktoralgebras, izomorfisma teorēma. Lineārās telpas endomorfismu algebra. Lineāri neatkarīga vektoru sistēma, moduļa bāze, brīvs modulis. Homomorfismi un matricas. Grupas algebra, tās centrs.

6.1. Asociatīvas algebras pār lauku

Šis nodaļas ietvaros, ja nekas speciāli netiks atrunāts, visi gredzeni ir gredzeni ar vieninieku. Simbolu R mēs rezervējam komutatīva gredzena ar vieninieku apzīmēšanai.

6.1.1. Definīcija. *Divu sugu algebru $\langle R, A, +, \cdot, \oplus, \circ, \odot\rangle$ sauc par asociatīvu algebru (lieto arī terminus: R–algebra A vai algebra A pār gredzenu R, ja*

(i) $\langle R, +, \cdot\rangle$ — *komutatīvs gredzens ar vieninieku,*

(ii) $\langle A, \oplus, \odot\rangle$ — *gredzens ar vieninieku,*

(iii) $\langle R, A, +, \cdot, \oplus, \circ\rangle$ — *kreisais R–modulis,*

(iv) $\forall a \in R\, \forall x \in A\, \forall y \in A \quad a \circ (x \odot y) = (a \circ x) \odot y = x \odot (a \circ y).$

Parasti $+$ un $\oplus$ vietā lieto tikai simbolu $+$, bet simbolus $\cdot$, $\circ$ un $\odot$ vispār nelieto un uzskata, ka operācijas $\cdot$, $\circ$ un $\odot$ saista ciešāk par operācijām $+$ un

$\oplus$. Tā rezultātā aksioma

$$a \circ (x \odot y) = (a \circ x) \odot y = x \odot (a \circ y)$$

iegūst izskatu

$$a(xy) = (ax)y = x(ay).$$

Šī aksioma nodrošina iespēju (līdzīgi kā asociatīvas operācijas gadījumā) nelietot iekavas, jo visas trīs izteiksmes

$$a \circ (x \odot y), \quad (a \circ x) \odot y, \quad x \odot (a \circ y)$$

definē vienu un to pašu kopas A elementu, ko turpmāk apzīmēsim ar axy vai xay.

Vienošanās. Lai nesajauktu gredzena R elementus ar gredzena A elementiem, turpmāk ar a, b, c apzīmēsim gredzena R elementus, bet ar x, y, z — gredzena A elementus.

6.1.2. Piemēri. (i) Komplekso skaitļu lauks $\mathbb{C}$ ir uztverams kā asociatīva algebra pār reālo skaitļu lauku $\mathbb{R}$.

(ii) Matricu gredzens $\mathrm{Mat}_n(R)$ uztverams kā asociatīva algebra pār R.

Ja gredzena R lomā ir lauks L, tad saka, ka dota *algebra pār lauku* L.

6.1.3. Teorēma. *Ja algebra A pār lauku L satur* 1 *atšķirīgu no* 0*, tad tā satur apakšlauku, kas ir izomorfs laukam L.*

Atzīmēsim, ka šai teorēmā domāts, ka 1 un 0 ir gredzena A elementi, nevis gredzena R elementi. Ja nerodas briesmas sajaukt gredzena R nulli ar gredzena A nulli, tad abus elementus parasti apzīmē ar vienu un to pašu simbolu 0. Ja tomēr radīsies risks, tad lietosim attiecīgi pierakstu 0_R, lai apzīmētu gredzena R nulli, un 0_A, lai apzīmētu gredzena A nulli. Tas pats attiecas arī uz gredzenu R un A vieniniekiem. Ievērot, ka R–algebras definīcija neprasa, lai A saturētu vieninieku atšķirīgu no nulles.

$\Box$ (i) Definēsim attēlojumu $f : L \to A : a \mapsto a \circ 1$.

$$\begin{aligned} f(a+b) &= (a+b)1 = a1 + b1 = f(a) + f(b), \\ f(ab) &= (ab)1 = (ab)(11) = a(b11) = a(1(b1)) = (a1)(b1) = f(a)f(b). \end{aligned}$$

Tātad f ir gredzenu homomorfisms.

(ii) Pieņemsim, ka $f(a) = f(b)$, tad $a1 = b1$, t.i., $0 = a1 - b1 = (a-b)1$. Ja nu izrādītos, ka $a - b \neq 0$, tad eksitētu $(a-b)^{-1}$. No šejienes

$$\begin{aligned} 1_A &= 1_R \circ 1_A = (a-b)^{-1}(a-b) \circ 1_A = (a-b)^{-1} \circ ((a-b) \circ 1_A) \\ &= (a-b)^{-1} \circ 0_A = 0_A. \qquad \text{Pretruna!} \end{aligned}$$

Tā rezultātā $L \cong Imf$. ■

6.2. Apakšalgebras

6.2.1. Definīcija. *Asociatīvu algebru $\langle R, B, +, \cdot, \oplus, \circ, \odot \rangle$ sauc par R–algebras A apakšalgebru, ja*

- *$\langle B, \oplus, \odot \rangle$ ir gredzena A apakšgredzens un $1_B = 1_A$;*
- *$\langle R, B, +, \cdot, \oplus, \circ \rangle$ ir moduļa A apakšmodulis.*

6.2.2. Apgalvojums. *Ja $\{A_i \,|\, i \in \mathcal{I}\}$ ir R–algebras A apakšalgebru saime, tad $A^0 \leftharpoondown \bigcap\limits_{i \in \mathcal{I}} M_i$ ir R–algebras A apakšalgebra.*

□ (i) Saskaņā ar Apgalvojumu 4.1.7 A^0 ir gredzena A apakšgredzens.

(ii) Saskaņā ar Apgalvojumu 5.1.9 A^0 ir moduļa A apakšmodulis. ■

6.3. Ideāli

6.3.1. Definīcija. *Gredzena A ideālu I sauc par R–algebras A ideālu.*

6.3.2. Vingrinājums. Ja I ir R–algebras A ideāls, tad I ir R–modulis.

Mājiens. Ja $x \in I$, tad $ax = a(x1_A) = x(a1_A) \in I$.

6.3.3. Apgalvojums. *R–algebras A faktorgredzens A/I pēc ideāla I ir R–algebra.*

□ Atliek pārliecināties, ka A/I apmierina visas Definīcijas 6.1.1 prasības.

(i) Saskaņā ar doto R ir komutatīvs gredzens ar vieninieku.

(ii) Saskaņā ar faktorgredzena definīciju 4.2.6 un Teorēmu 4.2.10 A/I ir gredzens. Tā kā

$$\forall x \in A \quad [1][x] = [1x] = [x] = [x1] = [x][1],$$

tad A/I ir gredzens ar vieninieku.

(iii) Saskaņā ar Vingrinājumu 6.3.2 ideāls I ir R–moduļa A apakšmodulis, tāpēc, ņemot vērā faktormoduļa A/I konstrukciju (Apgalvojums 5.4.2, Teorēma 5.4.5 un Teorēma 5.4.6), A/I ir kreisais R–modulis, kur

$$\forall a \in R \, \forall x \in A \quad a[x] \leftharpoondown [ax].$$

(iv) Visbeidzot pieņemsim, ka $a \in R$ un x, y ir kopas A elementi, tad

$$\begin{aligned} a([x][y]) &= a[xy] = [a(xy)] = [(ax)y] = [ax][y] = (a[x])[y], \\ a([x][y]) &= [a(xy)] = [x(ay)] = [x][ay] = [x](a[y]). \quad \blacksquare \end{aligned}$$

6.3.4. Definīcija. *R–algebras A faktorgredzenu A/I pēc ideāla I, kas ir R–algebra, sauc par R–algebras A faktoralgebru pēc ideāla I.*

6.4. Homomorfismi

6.4.1. Definīcija. *Attēlojumu $f : A \to A'$ sauc par R–algebru homomorfismu, ja*

- *f ir R–moduļu A, A' homomorfisms,*
- *f ir gredzenu A, A' homomorfisms un*
- *$f(1_A) = 1_{A'}$.*

Līdzīgi kā gredzenu gadījumā bijektīvu homomorfismu sauc par *izomorfismu.* Šai situācijā R–algebras A un A' sauc par *izomorfām* R–algebrām. Sirjektīvu homomorfismu sauc par *epimorfismu.* Injektīvu homomorfismu sauc par *monomorfismu.*

R–algebru homomorfismu $f : A \to A$ sauc par *endomorfismu.* Ja endomorfisms ir bijekcija, tad to sauc par *automorfismu.*

6.4.2. Apgalvojums. *Ja $f : A \to A'$ ir R–algebru homomorfisms, tad* $\mathrm{Im} f$ *ir algebras A' apakšalgebra.*

$\square$ (i) Tā kā $f : A \to A'$ ir R–moduļu homomorfisms, tad (Apgalvojums 5.3.3) $\mathrm{Im} f$ ir moduļa A' apakšmodulis.

(ii) Tā kā $f : A \to A'$ ir gredzenu homomorfisms, tad (Apgalvojums 4.2.3) $\mathrm{Im} f$ ir gredzena A' apakšgredzens.

(iii) Tā kā $f(1_A) = 1_{A'}$, tad $1_{A'} \in \mathrm{Im} f$ un $\mathrm{Im} f$ ir gredzens ar vienības elementu. $\blacksquare$

6.4.3. Definīcija. *Kopā definētu ekvivalences tipa predikātu $\equiv$ sauc par R–algebras A kongruenci, ja tā ir gan gredzena A kongruence, gan R–moduļa A kongruence.*

6.4.4. Apgalvojums. *Kopā A definēts ekvivalences tipa predikāts $\equiv$ ir R–algebras A kongruence tad un tikai tad, ja eksistē tāds R–algebras A ideāls I, ka*

$$[x] = x + I.$$

$\square$ $\Rightarrow$ Saskaņā ar Teorēmu 4.2.9 $[0_A]$ ir gredzena A ideāls. Ņemam vērā, ka $[x] = \{y \,|\, x \equiv y\}$ un $x + [0_A] = \{y \,|\, \exists z \in [0_A]\ y = x + z\}$.

(i) Pieņemsim, ka

$$\begin{aligned} y \in x + [0_A], &\qquad \text{tad} \\ y - x \in [0_A], &\qquad \text{t.i.,} \\ y - x \equiv 0_A. & \end{aligned}$$

No šejienes $y \equiv x$. Tātad $x + [0_A] \subseteq [x]$.

(ii) Pieņemsim, ka

$$\begin{aligned} y \in [x], &\qquad \text{tad} \\ y \equiv x, & \\ y - x \equiv 0_A, &\qquad \text{t.i.,} \\ y - x \in [0_A] &\qquad \text{jeb} \\ y \in x + [0_A]. & \end{aligned}$$

(iii) Mēs parādījām, ka $x + [0_A] \subseteq [x] \subseteq x + [0_A]$. Līdz ar to $x + [0_A] = [x]$.

$\Leftarrow$ Pieņemsim, ka eksistē tāds ideāls I, ka $\forall x \in A$ $[x] = x + I$. Pieņemsim, ka $x \equiv y$, tad

$$x + I = [x] = [y] = y + I.$$

No šejienes $x - y \in I$.

(i) Tā kā I ir ideāls, tad (Vingrinājums 6.3.2) I ir R–modulis, tāpēc

$$\begin{aligned} a(x-y) &\in I, \\ ax - ay &\in I, \\ ax &\in ay + I, \\ [ax] &= [ay], \\ ax &\equiv ay. \end{aligned}$$

Tā kā I ir ideāls, tad I ir gredzena A aditīvās grupas apakšgrupa. Gredzena A aditīvā grupa ir komutatīva, tāpēc

$$\begin{aligned} (x+z)-(y+z) \in I \quad &\text{un} \quad (z+x)-(z+y) \in I, \\ x+z \in (y+z)+I \quad &\text{un} \quad z+x \in (z+y)+I, \\ (x+z)+I = (y+z)+I \quad &\text{un} \quad (z+x)+I = (z+y)+I, \\ [x+z] = [y+z] \quad &\text{un} \quad [z+x] = [z+y], \\ x+z \equiv y+z \quad &\text{un} \quad z+x \equiv z+y. \end{aligned}$$

Esam parādījuši (skatīt Definīciju 5.4.1), ka $\equiv$ ir R–moduļa A kongruence.

(ii) Tā kā I ir ideāls, tad

$$\begin{aligned} z(x-y) \in I \quad &\text{un} \quad (x-y)z \in I, \\ zx - zy \in I \quad &\text{un} \quad xz - yz \in I, \\ zx \in zy + I \quad &\text{un} \quad xz \in yz + I, \\ zx + I = zy + I \quad &\text{un} \quad xz + i = yz + I, \\ [zx] = [zy] \quad &\text{un} \quad [xz] = [yz], \\ zx \equiv zy \quad &\text{un} \quad xz \equiv yz. \end{aligned}$$

Esam parādījuši (skatīt Definīciju 4.2.4), ka $\equiv$ ir gredzena A kongruence.

(iii) Saskaņā ar Definīciju 6.4.3 (skatīt punktus (i) un (ii)) $\equiv$ ir R–algebras A kongruence. ■

6.4.5. Definīcija. *Pieņemsim, ka $\equiv$ ir R–algebras A kongruence. Faktoralgebru $A/[0_A]$ sauc par faktoralgebru pēc kongruences $\equiv$.*

Šai situācijā $A/{\equiv} \leftharpoondown A/[0_A]$.

Atzīmēsim, ka katrs ideāls I gredzenā A definē (Teorēma 4.2.10) ekvivalences tipa predikātu $\equiv_I^k$ ar īpašību $[x]_I^k = x + I$. Līdz ar to (Apgalvojums 6.4.4) $\equiv_I^k$ ir R–algebras A kongruence. No šejienes iegūstam šādu rezultātu.

6.4.6. Sekas. *Katram R–algebras A ideālam I eksistē tāda kongruence $\equiv$, ka $A/{\equiv} = A/I$.*

6.4.7. Vingrinājums. Ja $f : A \to A'$ ir R–algebru homomorfisms, tad

$$\mathrm{Ker} f \leftharpoondown \{x \mid f(x) = 0_{A'}\}$$

ir R–algebras A ideāls.

Asociatīvo algebru teorijā, līdzīgi kā gredzenu teorijā, ideālu $\mathrm{Ker} f$ sauc par *homomorfisma f kodolu.*

6.4.8. Vingrinājums. Ja A ir R–algebra, tad attēlojums $\pi : A \to A/{\equiv}$: $x \mapsto [x]$ ir R–algebru epimorfisms.

6.4.9. Teorēma. *Katram R–algebru homomorfismam $f : A \to A'$ eksistē viens vienīgs R–algebru homomorfisms $f_* : A/\mathrm{Ker} f \to A'$, kam diagramma*

$$\begin{tikzcd} A \arrow[rr, "f"] \arrow[dr, "\pi"'] & & A' \\ & A/\mathrm{Ker} f \arrow[ur, "f_*"'] & \end{tikzcd}$$

ir komutatīva; turklāt šis homomorfisms f_* ir monomorfisms.

□ Šis rezultāts pierādīts (Teorēma 6.4.9) gredzeniem. Mums atliek parādīt, ka $f_*([1]) = 1_{A'}$ un $f_* : A/\mathrm{Ker} f \to A'$ ir R–moduļu homomorfisms.

$$f_*([1]) = f_* \circ \pi(1) = f(1) = 1_{A'}.$$

Pieņemsim, ka $a \in R$ un $[x] \in A/\mathrm{Ker}$, tad

$$\begin{aligned} f_*(a[x]) &= f_*([ax]) = f_* \circ \pi(ax) = f(ax) = af(x) \\ &= af_* \circ \pi(x) = af_*([x]). \quad \blacksquare \end{aligned}$$

6.4.10. Sekas (Izomorfisma teorēma). $A/\mathrm{Ker} f \cong \mathrm{Im} f$

6.5. Endomorfismi

Šai paragrāfā apskatīsim moduļus pār asociatīvām algebrām, proti, pieņemsim, ka A ir R–algebra un M ir modulis pār gredzenu A. Šai gadījumā, ja mēs aplūkojam A–moduli M, mums interesē tikai fakts, ka A ir gredzens. Saprotams tālākajās konstrukcijās mēs varam izmantot arī faktu, ka A īstenībā ir ne tikai gredzens, bet gan R–algebra.

Pieņemsim, ka N ir A–modulis, tad

$$\mathrm{Hom}_A(M,N) \leftharpoondown \{f : M \to N \mid f \text{ ir } A \text{ moduļu homomorfisms}\}.$$

Mēs jau zinam (Teorēma 5.5.1), ka $\mathrm{Hom}_A(M,N)$ ir komutatīva grupa.

6.5.1. Apgalvojums. $\mathrm{Hom}_A(M,N)$ *ir R–modulis, ja iedarbība*

$$R \times \mathrm{Hom}_A(M,N) \to \mathrm{Hom}_A(M,N)$$

definēta ar vienādību

$$\forall u \in M \quad af(u) \leftharpoondown (a1_A)f(u).$$

$$\begin{array}{rrcl} \square \text{ (i)} & (af)(xu) & = & (a1_A)f(xu) = (a1_A)(xf(u)) = ((a1_A)x)f(u) \\ & & = & (a(1_Ax))f(u) = (a(x1_A))f(u) = (x(a1_A))f(u) \\ & & = & x((a1_A)f(u)) = x(af(u)) = x(af)(u); \\ & (af)(u+v) & = & (a1_A)f(u+v) = (a1_A)(f(u)+f(v)) \\ & & = & (a1_A)f(u) + (a1_A)f(v) = (af)(u) + (af)(v). \end{array}$$

Esam parādījuši, ka $af \in \mathrm{Hom}_A(M,N)$.

$$\begin{array}{rrcl} \text{(ii)} & (ab)f(u) & = & ((ab)1_A)f(u) = (a(b1_A))f(u) = (a(b1_A1_A))f(u) \\ & & = & (a(1_A(b1_A)))f(u) = ((a1_A)(b1_A))f(u) \\ & & = & (a1_A)((b1_A)f(u)) = a(bf(u)); \\ & 1_Rf(u) & = & (1_R1_A)f(u) = 1_Af(u) = f(u). \end{array}$$

Esam parādījuši, ka R iedarbība uz kopu $\mathrm{Hom}_A(M,N)$ no kreisās puses definēta korekti.

$$\begin{aligned}
\text{(iii)}\quad a((f+g)(u)) &= (a1_A)((f+g)(u)) = (a1_A)(f(u)+g(u)) \\
&= (a1_A)f(u) + (a1_A)g(u) = af(u) + ag(u); \\
(a+b)f(u) &= ((a+b)1_A)f(u) = (a1_A + b1_A)f(u) \\
&= (a1_A)f(u) + (b1_A)f(u) = af(u) + bf(u).
\end{aligned}$$

Esam pamatojuši vienādības

$$\begin{aligned}
a(f+g) &= af + ag; \\
(a+b)f &= af + bf.
\end{aligned}$$

(iv) Visu savelkot kopā (punkti (i)–(iii) un Teorēma 5.5.1) secināms (Definīcija 5.1.2), ka $\mathrm{Hom}_A(M, N)$ ir R–modulis. ■

Pieņemsim, ka $\mathrm{End}_A(M) \rightleftharpoons \mathrm{Hom}_A(M, M)$.

6.5.2. Teorēma. $\mathrm{End}_A(M)$ *ir R–algebra.*

□ (i) Vispirms precizēsim kādā nozīmē mēs lietojam terminu $\mathrm{End}_A(M)$ ir R–algebra. Pieņemsim, ka

$$\langle R, A, +, \cdot, \oplus, \circ, \odot \rangle$$

ir R–algebra A un

$$\langle A, M, \oplus, \odot, \tilde{+}, \tilde{\circ} \rangle$$

ir A–modulis M, tad R–algebru $\mathrm{End}_A(M)$

$$\langle R, \mathrm{End}_A(M), +, \cdot, \overset{\frown}{+}, \overset{\frown}{\circ}, \overset{\frown}{\cdot} \rangle$$

definē šādi:

- saskaitīšanu $\overset{\frown}{+}$ definē ar vienādību

$$\forall u \in M \quad (f \overset{\frown}{+} g)(u) \rightleftharpoons f(u) \tilde{+} g(u);$$

- R–iedarbību uz $\mathrm{End}_A(M)$ definē ar vienādību

$$\forall u \in M \quad (a \overset{\frown}{\circ} f)(u) \rightleftharpoons (a \circ 1_A) \tilde{\circ} f(u);$$

- reizināšanu $\widehat{\cdot}$ definē ar vienādību

$$\forall u \in M \quad (f \,\widehat{\cdot}\, g)(u) \leftharpoondown f(g(u)).$$

Tātad reizināšana $\widehat{\cdot}$ ir attēlojumu kompozīcija (Definīcija 1.2.1).

(ii) Mēs tikko pierādījām (Apgalvojums 6.5.1), ka

$$\langle R, \mathrm{End}_A(M), +, \cdot, \widehat{+}, \widehat{\circ} \rangle$$

ir kreisais R–modulis $\mathrm{End}_A(M)$.

(iii) Vingrinājums 5.6.2 konstatē, ka

$$\langle \mathrm{End}_A(M), \widehat{+}, \widehat{\cdot} \rangle$$

ir gredzens ar vienības elementu $\mathbb{I}_M$.

(iv) Atliek tikai konstatēt, ka

$$\begin{array}{l} \forall a \in R \quad \forall f \in \mathrm{End}_A(M) \quad \forall g \in \mathrm{End}_A(M) \\ \qquad a \,\widehat{\circ}\, (f \,\widehat{\cdot}\, g) \quad = \quad (a \,\widehat{\circ}\, f) \,\widehat{\cdot}\, g \;=\; f \,\widehat{\cdot}\, (a \,\widehat{\circ}\, g). \end{array}$$

$$\begin{aligned} (a \,\widehat{\circ}\, (f \,\widehat{\cdot}\, g))(u) &= (a \circ 1_A)\tilde{\circ}(f \,\widehat{\cdot}\, g)(u) = (a \circ 1_A)\tilde{\circ}(f(g(u)) \\ &= (a \,\widehat{\circ}\, f)(g(u)) = ((a \,\widehat{\circ}\, f) \,\widehat{\cdot}\, g)(u); \\ (a \,\widehat{\circ}\, (f \,\widehat{\cdot}\, g))(u) &= (a \circ 1_A)\tilde{\circ}(f(g(u)) = f((a \circ 1_A)\tilde{\circ} g(u)) \\ &= f((a \,\widehat{\circ}\, g)(u)) = (f \,\widehat{\cdot}\, (a \,\widehat{\circ}\, g))(u). \quad \blacksquare \end{aligned}$$

6.5.3. Definīcija. $\mathrm{End}_A(M)$ *sauc par moduļa* M *endomorfismu algebru.*

Tagad aplūkosim mazāk samudžinātu konstrukciju. Pieņemsim, ka M un M' ir R–moduļi.

6.5.4. Apgalvojums. $\mathrm{Hom}(M, M')$ *ir* R*–modulis.*

$\square$ (i) Vispirms precizēsim kādā nozīmē mēs lietojam terminu $\mathrm{Hom}(M, M')$ ir R–modulis. Pieņemsim, ka

$$\langle R, M, +, \cdot, \oplus, \circ \rangle \qquad \text{un} \qquad \langle R, M, +, \cdot, \acute{\oplus}, \acute{\circ} \rangle$$

ir R–moduļi, tad R–moduli $\mathrm{Hom}(M,M')$

$$\langle R, \mathrm{Hom}(M,M'), +, \cdot, \widehat{+}, \widehat{\circ}\rangle$$

definē šādi:

- saskaitīšanu $\widehat{+}$ definē ar vienādību

$$\forall u \in M \quad (f \,\widehat{+}\, g)(u) \overline{\leftharpoondown} f(u)\acute{\oplus} g(u);$$

- R–iedarbību uz $\mathrm{Hom}(M,M')$ definē ar vienādību

$$\forall u \in M \quad (a \,\widehat{\circ}\, f)(u) \overline{\leftharpoondown} a\acute{\circ} f(u).$$

(ii) Mēs jau pierādījām (Teorēma 5.5.1), ka $\langle \mathrm{Hom}(M,M'), \widehat{+}\rangle$ ir komutatīva grupa.

(iii) Parādīsim, ka $\langle R, \mathrm{Hom}(M,M'), \cdot, \widehat{\circ}\rangle$ ir multiplikatīvā monoīda R iedarbība uz kopu $\mathrm{Hom}(M,M')$ no kreisās puses.

a) Vispirms parādīsim, ka $a \,\widehat{\circ}\, f \in \mathrm{Hom}(M,M')$.

$$\begin{aligned}
(a \,\widehat{\circ}\, f)(b \circ u) &= a\acute{\circ} f(b \circ u) = a\acute{\circ}(b\acute{\circ} f(u)) = (ab)\acute{\circ} f(u) = (ba)\acute{\circ} f(u) \\
&= b\acute{\circ}(a\acute{\circ} f(u)) = b\acute{\circ}(a \,\widehat{\circ}\, f)(u); \\
(a \,\widehat{\circ}\, f)(u \oplus v) &= a\acute{\circ} f(u \oplus v) = a\acute{\circ}(f(u)\acute{\oplus} f(v)) \\
&= a\acute{\circ} f(u) \,\acute{\oplus}\, a\acute{\circ} f(v) = (a \,\widehat{\circ}\, f)(u) \,\acute{\oplus}\, (a \,\widehat{\circ}\, f)(v).
\end{aligned}$$

b) Tagad parādīsim, ka $(ab) \,\widehat{\circ}\, f = a \,\widehat{\circ}\, (b \,\widehat{\circ}\, f)$ un $1 \,\widehat{\circ}\, f = f$.

$$\begin{aligned}
((ab) \,\widehat{\circ}\, f)(u) &= (ab)\acute{\circ} f(u) = a\acute{\circ}(b\acute{\circ} f(u)) \\
&= a\acute{\circ}(b \,\widehat{\circ}\, f)(u) = (a \,\widehat{\circ}\, (b \,\widehat{\circ}\, f))(u); \\
(1 \,\widehat{\circ}\, f)(u) &= 1\acute{\circ} f(u) = f(u).
\end{aligned}$$

(iv) Atliek tikai konstatēt, ka

$$\forall a \in R \; \forall b \in R \qquad \forall f \in \mathrm{Hom}(M,M') \; \forall g \in \mathrm{Hom}(M,M')$$

$$\begin{aligned}
a \,\widehat{\circ}\, (f \,\widehat{+}\, g) &= a \,\widehat{\circ}\, f \;\widehat{+}\; a \,\widehat{\circ}\, g, \\
(a+b) \,\widehat{\circ}\, f &= a \,\widehat{\circ}\, f \;\widehat{+}\; b \,\widehat{\circ}\, f.
\end{aligned}$$

$$
\begin{aligned}
(a \overset{\frown}{\circ} (f \overset{\frown}{+} g))(u) &= a\acute{\circ}(f \overset{\frown}{+} g)(u) = a\acute{\circ}(f(u)\acute{\oplus} g(u)) \\
&= a\acute{\circ} f(u) \acute{\oplus} a\acute{\circ} g(u) = (a \overset{\frown}{\circ} f)(u) \acute{\oplus} (a \overset{\frown}{\circ} g)(u) \\
&= (a \overset{\frown}{\circ} f \ \overset{\frown}{+} \ a \overset{\frown}{\circ} g)(u); \\
((a+b) \overset{\frown}{\circ} f)(u) &= (a+b)\acute{\circ} f(u) = a\acute{\circ} f(u) \acute{\oplus} b\acute{\circ} f(u) \\
&= (a \overset{\frown}{\circ} f)(u) \acute{\oplus} (b \overset{\frown}{\circ} f)(u) \\
&= (a \overset{\frown}{\circ} f \ \overset{\frown}{+} \ b \overset{\frown}{\circ} f)(u). \quad \blacksquare
\end{aligned}
$$

6.5.5. Apgalvojums. *Ja M ir R–modulis, tad* End(M) *ir R–algebra.*

$\square$ (i) Vispirms precizēsim kādā nozīmē mēs lietojam terminu End(M) ir R–algebra. Pieņemsim, ka

$$\langle R, M, +, \cdot, \oplus, \circ\rangle \quad \text{ir} \quad R\text{–modulis,}$$

tad R–algebru End(M)

$$\langle R, \mathrm{End}(M), +, \cdot, \overset{\frown}{+}, \overset{\frown}{\circ}, \overset{\frown}{\cdot}\rangle$$

definē šādi:

- saskaitīšanu $\overset{\frown}{+}$ definē ar vienādību

$$\forall u \in M \quad (f \overset{\frown}{+} g)(u) \mathrel{\overline{\leftharpoondown}} f(u) \oplus g(u);$$

- R–iedarbību uz End(M) definē ar vienādību

$$\forall u \in M \quad (a \overset{\frown}{\circ} f)(u) \mathrel{\overline{\leftharpoondown}} a \circ f(u);$$

- reizināšanu $\overset{\frown}{\cdot}$ definē ar vienādību

$$\forall u \in M \quad (f \overset{\frown}{\cdot} g)(u) \mathrel{\overline{\leftharpoondown}} f(g(u)).$$

Tātad reizināšana $\overset{\frown}{\cdot}$ ir attēlojumu kompozīcija (Definīcija 1.2.1).

(ii) Vingrinājums 5.6.2 konstatē, ka

$$\langle \mathrm{End}(M), \widehat{+}, \widehat{\cdot} \rangle$$

ir gredzens ar vienības elementu $\mathbb{I}_M$.

(iii) Apgalvojums 6.5.4 ļauj secināt, ka

$$\langle R, \mathrm{End}(M), +, \cdot, \widehat{+}, \widehat{\circ} \rangle$$

ir R–modulis End(M).

(iv) Atliek tikai konstatēt, ka

$$\begin{aligned} &\forall a \in R \quad \forall f \in \mathrm{End}(M) \quad \forall g \in \mathrm{End}(M) \\ &\qquad a \,\widehat{\circ}\, (f \,\widehat{\cdot}\, g) \;=\; (a \,\widehat{\circ}\, f) \,\widehat{\cdot}\, g \;=\; f \,\widehat{\cdot}\, (a \,\widehat{\circ}\, g). \end{aligned}$$

$$\begin{aligned} (a \,\widehat{\circ}\, (f \,\widehat{\cdot}\, g))(u) &= (a \circ (f \,\widehat{\cdot}\, g)(u) = a \circ (f(g(u)) \\ &= (a \,\widehat{\circ}\, f)(g(u)) = ((a \,\widehat{\circ}\, f) \,\widehat{\cdot}\, g)(u); \\ (a \,\widehat{\circ}\, (f \,\widehat{\cdot}\, g))(u) &= a \circ (f(g(u)) = f(a \circ g(u)) \\ &= f((a \,\widehat{\circ}\, g)(u)) = (f \,\widehat{\cdot}\, (a \,\widehat{\circ}\, g))(u). \quad \blacksquare \end{aligned}$$

Nekas principiāli nemainās, ja V ir lineāra telpa pār lauku L.

6.5.6. Sekas. *Ja V ir lineāra telpa pār lauku L, tad* End(V) *ir L–algebra.*

6.6. Brīvie moduļi

Šī paragrāfa ietvaros M ir R–modulis.

6.6.1. Definīcija. *Kopu $S \subseteq M$ sauc par lineāri atkarīgu, ja eksistē tādi kopas S dažādi elementi $x_1, x_2, \ldots, x_n$ un gredzena R elementi $a_1, a_2, \ldots, a_n$, ka*

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0_M$$

un vismaz viens no koeficientiem $a_i \neq 0_R$.

Ja kopa S nav lineāri atkarīga, tad to sauc par *lineāri neatkarīgu kopu.* Ja kopa S ir galīga, teiksim, $S = \{x_1, x_2, \ldots, x_k\}$, tad tā vietā, lai teiktu, ka S ir lineāri neatkarīga kopa, mēdz teikt, ka vektori

$$x_1, x_2, \ldots, x_k$$

ir lineāri neatkarīgi.

6.6.2. Vingrinājumi. (i) Kopa $S \subseteq M$ ir lineāri neatkarīga tad un tikai tad, ja jebkuriem dažādiem kopas S elementiem $x_1, x_2, \ldots, x_n$ vienādība

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0_M$$

izpildās tikai tad, ja $a_1 = a_2 = \ldots = a_n = 0_R$.

(ii) Ja $K \subseteq S \subseteq M$ un K ir lineāri atkarīga, tad arī S ir lineāri atkarīga.

(iii) Ja $K \subseteq S \subseteq M$ un S ir lineāri neatkarīga, tad arī K ir lineāri neatkarīga.

(iv) Ja $0_M \in S$, tad S ir lineāri atkarīga.

(v) Kopa $S \subseteq M$ ir lineāri neatkarīga tad un tikai tad, ja katra galīga kopas S apakškopa ir lineāri neatkarīga.

6.6.3. Definīcija. *Kopu $S \subseteq M$ sauc par moduļa M bāzi, ja kopa S ir lineāri neatkarīga un $\mathcal{L}(S) = M$.*

Ja $M = \{0\}$, tad $\emptyset$ sauc par moduļa M bāzi. Mēs sakam, ka bāze S ir galīga, ja $|S| < \aleph_0$.

6.6.4. Apgalvojums. *Ja S ir moduļa M bāze, tad katrs moduļa M vektors vienā vienīgā veidā izsakāms ar sistēmu S.*

$\square$ Pieņemsim, ka

$$\sum_{y \in S} a_y y = x = \sum_{y \in S} b_y y,$$

kur gandrīz visi $a_y = 0$ un gandrīz visi $b_y = 0$, un $x \in M$. No šejienes

$$\sum_{y \in S} (a_y - b_y)y = 0_M$$

un gandrīz visi $a_y = b_y = 0$. Tā rezultātā eksistē tāda galīga kopas S apakškopa S', ka

$$\sum_{y \in S'} (a_y - b_y) y = \sum_{y \in S} (a_y - b_y) y = 0_M.$$

Tā kā kopa S ir lineāri neatkarīga, tad (Vingrinājums 6.6.2(iii)) arī kopa S' ir lineāri neatkarīga, tāpēc (Vingrinājums 6.6.2(i)) $\forall y \in S'\ a_y - b_y = 0$. Līdz ar to $\forall y \in S\ a_y = b_y$. ■

6.6.5. Definīcija. *Moduli M sauc par brīvu moduli, ja tam eksistē bāze.*

6.6.6. Piemērs. $\mathrm{Mat}_n^m(R)$ ir brīvs modulis ar bāzi

$$S = \{E_{ij} \mid (i,j) \in \overline{1,m} \times \overline{1,n}\}.$$

Ar $E_{ij} = ||e_{kl}|| \in \mathrm{Mat}_n^m(R)$ apzīmēta matrica, kurai tikai viens elements e_{kl} atšķiras no 0, proti, $e_{ij} = 1$.

6.6.7. Apgalvojums. *Ja N ir R–modulis un M ir brīvs R–modulis ar bāzi S, tad katram attēlojumam $h : S \to N$ eksistē tāds moduļu homomorfisms $f \in \mathrm{Hom}(M, N)$, ka $f|S = h$.*

□ Tā kā S ir moduļa M bāze, tad katrs $x \in M$ viennozīmīgi reprezentējams izskatā $x = \sum_{y \in S} a_y y$, kur gandrīz visi $a_y = 0$. Attēlojumu $f : M \to N$ definējam ar vienādību

$$f(x) \leftharpoondown \sum_{y \in S} a_y h(y).$$

Atliek pārliecināties, ka tas ir homomorfisms.

(i) Pieņemsim, ka $a \in R$, tad

$$af(x) = a \sum_{y \in S} a_y h(y) = \sum_{y \in S} a a_y h(y) = f(ax).$$

(ii) Pieņemsim, ka $\sum_{y \in S} b_y y = z \in M$, tad

$$f(x) + f(z) = \sum_{y \in S} a_y h(y) + \sum_{y \in S} b_y h(y) = \sum_{y \in S} (a_y + b_y) h(y) = f(x + z). \quad ■$$

6.6.8. Lemma. *Ja M ir galīgi ģenerēts brīvs modulis, tad šī moduļa bāze ir galīga.*

$\Box$ Pieņemsim, ka S ir moduļa M bāze un $M = \mathcal{L}(x_1, x_2, \ldots, x_n)$. Tā kā S ir bāze, tad katrs x_i viennozīmīgi reprezentējams izskatā $x_i = \sum\limits_{y \in S} a_{iy}y$, kur gandrīz visi $a_{iy} = 0$. Tā rezultātā katram $i \in \overline{1, n}$ eksistē tāda galīga kopas S apakškopa S_i, ka

$$x_i = \sum_{y \in S} a_{iy}y = \sum_{y \in S_i} a_{iy}y.$$

No šejienes $x_i = \sum\limits_{y \in S_0} a_{iy}y$, kur $S_0 \leftharpoondown \bigcup\limits_{i=1}^{n} S_i$.

Tā kā $M = \mathcal{L}(x_1, x_2, \ldots, x_n)$, tad visi moduļa M elementi izsakāmi ar kopas S_0 elementiem. Tas attiecas arī uz kopas $S \setminus S_0$ elementiem, taču kopa S ir lineāri neatkarīga, tāpēc $S \setminus S_0 = \emptyset$. $\blacksquare$

6.6.9. Teorēma. *Ja M un N ir galīgi ģenerēti brīvie R–moduļi, tad* $\mathrm{Hom}(M, N)$ *ir galīgi ģenerēts brīvais R–modulis.*

$\Box$ (i) Mēs jau zinam, ka moduļu M un N bāzes ir galīgas (Lemma 6.6.8) un $\mathrm{Hom}(M, N)$ ir R–modulis (Apgalvojums 6.5.4).

(ii) Pieņemsim, ka $\mathcal{U} = \{u_1, u_2, \ldots, u_m\}$ un $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$ ir attiecīgi moduļu M un N bāzes. Katram indeksu pārim $(i, j) \in \overline{1, m} \times \overline{1, n}$ definējam attēlojumu

$$h_{ij} : \mathcal{U} \to \mathcal{V} : u_k \mapsto \begin{cases} v_j, & \text{ja} \quad k = i; \\ 0, & \text{ja} \quad k \neq i. \end{cases}$$

Saskaņā ar Apgalvojumu 6.6.7 eksistē tādi homomorfismi $f_{ij} \in \mathrm{Hom}(M, N)$, ka $f_{ij}|\mathcal{U} = h_{ij}$. Atliek parādīt, ka $S \leftharpoondown \{f_{ij} \,|\, (i, j) \in \overline{1, m} \times \overline{1, n}\}$ ir moduļa $\mathrm{Hom}(M, N)$ bāze.

Pieņemsim, ka $f \in \mathrm{Hom}(M, N)$, tad katrs $f(u_i) \in N$, un tāpēc izsakāms ar sistēmu $\mathcal{V}$. Konkrētības labad

$$f(u_i) = a_{i1}v_1 + a_{i2}v_2 + \ldots + a_{in}v_n.$$

Pieņemsim, ka

$$g \leftharpoondown \sum_{i=1}^{m} \sum_{j=1}^{n} a_{ij} f_{ij},$$

tad

$$\begin{aligned} g(u_k) &= \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}f_{ij}(u_k) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{ij}h_{ij}(u_k) = \sum_{j=1}^{n} a_{kj}h_{kj}(u_k) \\ &= \sum_{j=1}^{n} a_{kj}v_j = f(u_k). \end{aligned}$$

Pieņemsim, ka $x \in M$, tad x izsakāms ar sistēmu $\mathcal{U}$. Konkrētības labad $x = b_1u_1 + b_2u_2 + \ldots + b_mu_m$. No šejienes

$$g(x) = g(\sum_{k=1}^{m} b_ku_k) = \sum_{k=1}^{m} b_kg(u_k) = \sum_{k=1}^{m} b_kf(u_k) = f(\sum_{k=1}^{m} b_ku_k) = f(x).$$

Līdz ar to $f = g$, t.i., f ir izsakāms ar sistēmu S. Tādējādi $\mathcal{L}(S) = \mathrm{Hom}(M, N)$, un tāpēc tas ir galīgi ģenerēts modulis.

(iii) Parādīsim, ka S ir $\mathrm{Hom}(M, N)$ bāze. Pieņemsim, ka

$$h = \sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}f_{ij} = 0,$$

tad $\forall x \in M$ $h(x) = 0_N$. No šejienes

$$\forall k \in \overline{1,m} \quad 0_N = h(u_k) = \sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}f_{ij}(u_k) = \sum_{i=1}^{m}\sum_{j=1}^{n} b_{ij}h_{ij}(u_k) = \sum_{j=1}^{n} b_{kj}v_j.$$

Tā kā $\mathcal{V}$ ir lineāri neatkarīga kopa, tad $b_{k1} = b_{k2} = \ldots = b_{kn} = 0$. Līdz ar to $\mathrm{Hom}(M, N)$ ir brīvs modulis. ■

6.6.10. Teorēma. *Ja M un N ir galīgi ģenerēti brīvie R–moduļi, tad $\mathrm{Hom}(M, N)$ un $\mathrm{Mat}_n^m(R)$ ir izomorfi R–moduļi, kur m ir moduļa M bāzes apjoms un n ir moduļa N bāzes apjoms.*

□ (i) Pieņemsim, ka $\mathcal{U} = \{u_1, u_2, \ldots, u_m\}$ un $\mathcal{V} = \{v_1, v_2, \ldots, v_n\}$ ir attiecīgi moduļu M un N bāzes. Pieņemsim, ka $f \in \mathrm{Hom}(M, N)$ un

$$\forall k \in \overline{1,m} \quad f(u_k) = a_{k1}v_1 + a_{k2}v_2 + \ldots + a_{kn}v_n,$$

tad

$$||f|| \rightleftharpoons \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ . & . & . & . \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Definējam attēlojumu $\Phi : \mathrm{Hom}(M, N) \to \mathrm{Mat}_n^m(R) : f \mapsto ||f||$.

(ii) Pieņemsim, ka $a \in R$, tad

$$\begin{aligned} (af)(u_k) &= af(u_k) = a(a_{k1}v_1 + a_{k2}v_2 + \ldots + a_{kn}v_n) \\ &= aa_{k1}v_1 + aa_{k2}v_2 + \ldots + aa_{kn}v_n. \end{aligned}$$

Tas nozīmē, ka $||af|| = a||f||$. Līdz ar to

$$\Phi(af) = ||af|| = a||f|| = a\Phi(f).$$

Pieņemsim, ka $g \in \mathrm{Hom}(M, N)$ un

$$||g|| \rightleftharpoons \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ . & . & . & . \\ b_{m1} & b_{m2} & \dots & b_{mn} \end{pmatrix},$$

tad

$$\begin{aligned} (f+g)(u_k) &= f(u_k) + g(u_k) \\ &= (a_{k1}v_1 + a_{k2}v_2 + \ldots + a_{kn}v_n) + (b_{k1}v_1 + b_{k2}v_2 + \ldots + b_{kn}v_n) \\ &= (a_{k1} + b_{k1})v_1 + (a_{k2} + b_{k2})v_2 + \ldots + (a_{kn} + b_{kn})v_n. \end{aligned}$$

Tas nozīmē, ka $||f + g|| = ||f|| + ||g||$. Lidz ar to

$$\Phi(f + g) = ||f + g|| = ||f|| + ||g|| = \Phi(f) + \Phi(g).$$

Esam parādījuši, ka $\Phi : \mathrm{Hom}(M, N) \to \mathrm{Mat}_n^m(R)$ ir R–moduļu homomorfisms.

(iii) Pieņemsim, ka Φ nav injekcija, tad (Apgalvojums 3.7.3) eksistē tāds $f \neq 0$, ka $||f|| = \Phi(f) = ||0_R||$, t.i., $||f||$ ir nulles matrica. Līdz ar to

$$\forall k \, \forall j \quad a_{kj} = 0_R.$$

Ja reiz $f \neq 0$, tad eksistē tāds $x \in M$, ka $f(x) \neq 0_N$. Tā kā $\mathcal{U}$ ir moduļa M bāze, tad x izsakāms ar sistēmu $\mathcal{U}$. Konkrētības labad

$$x = a_1 u_1 + a_2 u_2 + \ldots + a_m u_m.$$

No šejienes

$$\begin{aligned} 0_N &\neq f(x) = f(\sum_{k=1}^{m} a_k u_k) = \sum_{k=1}^{m} a_k f(u_k) = \sum_{k=1}^{m} a_k \sum_{j=1}^{n} a_{kj} v_k \\ &= \sum_{k=1}^{m} a_k \sum_{k=1}^{m} 0_R v_k = \sum_{k=1}^{m} a_k 0_N = 0_N. \end{aligned}$$

Preteuna! Tātad Φ ir monomorfisms.

(iv) Pieņemsim, ka

$$C = \begin{pmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ \cdot & \cdot & \cdot & \cdot \\ c_{m1} & c_{m2} & \ldots & c_{mn} \end{pmatrix} \in \mathrm{Mat}_n^m(R).$$

Definējam attēlojumu $h : \mathcal{U} \to N$ ar vienādībām

$$\forall k \in \overline{1,m} \quad h(u_k) \leftharpoondown c_{k1} v_1 + c_{k2} v_2 + \ldots + c_{kn} v_n.$$

Saskaņā ar Apgalvojumu 6.6.7 eksistē tāds homomorfisms $\chi \in \mathrm{Hom}(M, N)$, ka $\chi | \mathcal{U} = h$. Savukārt saskaņā ar χ definīciju $C = ||\chi|| = \Phi(\chi)$. Tas demonstrē, ka Φ ir epimorfisms.

(v) Visu savelkot kopā (punkti (ii)–(iv)) secināms, ka

$$\Phi : \mathrm{Hom}(M, N) \to \mathrm{Mat}_n^m(R)$$

ir R–moduļu izomorfisms. Tātad $\mathrm{Hom}(M, N) \cong \mathrm{Mat}_n^m(R)$. ■

6.6.11. Vingrinājums. *R–moduļi* $\mathrm{Mat}_n^m(R)$ *un* $\mathrm{Mat}_m^n(R)$ *ir izomorfi.*

6.6.12. Teorēma. *Ja M ir galīgi ģenerēts brīvs modulis, tad* $\mathrm{End}(M)$ *un* $\mathrm{Mat}_m(R)$ *ir izomorfas R–algebras, kur m ir moduļa M bāzes apjoms.*

□ Mēs jau esam pazīstami (Apgalvojums 6.5.5) ar R–algebru $\mathrm{End}(M)$, turklāt mēs jau zinam (Teorēma 6.6.10), ka $\mathrm{End}(M)$ un $\mathrm{Mat}_m(R)$ ir izomorfi R–moduļi.

(i) Pieņemsim, ka $\mathcal{U} = \{u_1, u_2, \ldots, u_m\}$ ir moduļa M bāze. Pieņemsim, ka $f \in \mathrm{End}(M)$ un

$$\forall k \in \overline{1, m} \quad f(u_k) = a_{1k}u_1 + a_{2k}u_2 + \ldots + a_{mk}u_m,$$

tad

$$\overset{\triangledown}{||}\, f\, || \leftharpoondown \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ . & . & . & . \\ a_{m1} & a_{m2} & \ldots & a_{mm} \end{pmatrix}.$$

Definējam attēlojumu $\Psi : \mathrm{End}(M) \to \mathrm{Mat}_m(R) : f \mapsto \overset{\triangledown}{||}\, f\, ||$. Ņemot vērā Teorēmas 6.6.10 pierādījumu un Vingrinājumu 6.6.11, secināms: Ψ ir R–moduļu izomorfisms.

(ii) Pieņemsim, ka $g \in \mathrm{End}(M)$ un

$$\overset{\triangledown}{||}\, g\, || = \begin{pmatrix} b_{11} & b_{12} & \ldots & b_{1m} \\ b_{21} & b_{22} & \ldots & b_{2m} \\ . & . & . & . \\ b_{m1} & b_{m2} & \ldots & b_{mm} \end{pmatrix},$$

tad

$$\begin{aligned} f(g(u_j)) &= f(b_{1j}u_1 + b_{2j}u_2 + \ldots + b_{mj}u_m) \\ &= b_{1j}f(u_1) + b_{2j}f(u_2) + \ldots + b_{mj}f(u_m) \\ &= b_{1j}\sum_{i=1}^{m} a_{i1}u_i + b_{2j}\sum_{i=1}^{m} a_{i2}u_i + \ldots + b_{mj}\sum_{i=1}^{m} a_{im}u_i \\ &= \sum_{k=1}^{m} b_{kj}\sum_{i=1}^{m} a_{ik}u_i = \sum_{i=1}^{m}\sum_{k=1}^{m} b_{kj}a_{ik}u_i = \sum_{i=1}^{m}\Big(\sum_{k=1}^{m} b_{kj}a_{ik}\Big)u_i \\ &= \sum_{i=1}^{m}\Big(\sum_{k=1}^{m} a_{ik}b_{kj}\Big)u_i. \end{aligned}$$

No šejienes, ja

$$\overset{\triangledown}{||}\, f \mathbin{\overset{\frown}{\cdot}} g\, || = \begin{pmatrix} c_{11} & c_{12} & \ldots & c_{1m} \\ c_{21} & c_{22} & \ldots & c_{2m} \\ . & . & . & . \\ c_{m1} & c_{m2} & \ldots & c_{mm} \end{pmatrix},$$

tad $c_{ij} = \sum_{k=1}^{m} a_{ik}b_{kj}$, t.i., $\overset{\triangledown}{||}\ f \overset{\frown}{\cdot} g\ || = \overset{\triangledown}{||}\ f\ ||\ \overset{\triangledown}{||}\ g\ ||$.

Tātad $\Psi(f \overset{\frown}{\cdot} g) = \Psi(f)\Psi(g)$. Tā kā $\Psi(f+g) = \Psi(f) + \Psi(g)$, tad tas nozīmē, ka $\Psi : \mathrm{End}(M) \to \mathrm{Mat}_m(R)$ ir gredzenu homomorfisms.

(iii) Ņemam vērā, ka gredzena $\mathrm{End}(M)$ vienības elements ir $\mathbb{I}_{\mathbb{M}}$ (tiem, kas to aizmirsuši iesakam pievērsties Vingrinājumam 5.6.2). Tā rezultātā

$$\forall k \in \overline{1,m} \quad \mathbb{I}_M(u_k) = u_k.$$

No šejienes $\overset{\triangledown}{||}\ \mathbb{I}\ || = E$, t.i., $\Psi(\mathbb{I})$ ir vienāds ar vienības matricu.

(iv) Visu savelkot kopā (punkti (i)–(iii)) secināms, ka

$$\Psi : \mathrm{End}(M) \to \mathrm{Mat}_m(R)$$

ir R–algebru izomorfisms. Tātad $\mathrm{End}(M) \cong \mathrm{Mat}_m(R)$. ■

6.7. Grupu algebras

Pieņemsim, ka G — grupa, tad

$$R(G) \rightleftharpoons \{f : G \to R \mid \overset{\infty}{\forall}\, x\ f(x) = 0\}.$$

Pieņemsim, ka f un g ir kopas $R(G)$ elementi, tad

$$\begin{aligned} (f+g)(x) &\rightleftharpoons f(x) + g(x), \\ (fg)(x) &\rightleftharpoons \sum_{y \in G} f(y)g(y^{-1}x). \end{aligned}$$

Tā kā gandrīz visiem y attēlojums $f(y) = 0$, tad reizināšana fg ir definēta korekti.

6.7.1. Apgalvojums. *$R(G)$ ir gredzens ar vienības elementu.*

□ (i) Tas, ka $R(G)$ attiecībā pret saskaitīšanu ir komutatīva grupa izriet no fakta, ka R attiecībā pret saskaitīšanu ir komutatīva grupa. Te neitrālā elementa lomā ir attēlojums $0(x)$, kas katru $x \in G$ attēlo par $0 \in R$. Attēlojuma $f \in R(G)$ pretējais attēlojums ir $-f$, kas katru $x \in G$ attēlo par $-f(x)$.

(ii) Pieņemsim, ka grupas G neitrālais elements ir e, tad kopā $R(G)$ vienības elements ir attēlojums

$$1(x) \leftharpoondown \begin{cases} 1, & \text{ja} \quad x = e; \\ 0, & \text{ja} \quad x \neq e. \end{cases}$$

Šai situācijā

$$\begin{aligned} (1f)(x) &= \sum_{y\in G} 1(y)f(y^{-1}x) = f(x), \\ (f1)(x) &= \sum_{y\in G} f(y)1(y^{-1}x) = f(x)1(x^{-1}x) = f(x)1(e) = f(x). \end{aligned}$$

(iii) Parādīsim, ka reizināšana kopā $R(G)$ ir asociatīva. Pieņemsim, ka f, g un h ir kopas $R(G)$ elementi, tad

$$\begin{aligned} ((fg)h)(x) &= \sum_{y\in G}(fg)(y)h(y^{-1}x) \\ &= \sum_{y\in G}(\sum_{z\in G} f(z)g(z^{-1}y))h(y^{-1}x) \\ &= \sum_{z\in G} f(z)\sum_{y\in G} g(z^{-1}y)h(y^{-1}x). \end{aligned}$$

Ņemam vērā, ka attēlojums $G \to G : y \mapsto zy$ ir grupas bijekcija, tāpēc

$$\sum_{y\in G} g(z^{-1}y)h(y^{-1}x) = \sum_{y\in G} g(z^{-1}(zy))h((zy)^{-1}x) = \sum_{y\in G} g(y)h(y^{-1}z^{-1}x).$$

Līdz ar to

$$(fg)h)(x) = \sum_{z\in G} f(z)\sum_{y\in G} g(y)h(y^{-1}z^{-1}x).$$

Tagad pievēršamies reizinājumam

$$\begin{aligned} (f(gh))(x) &= \sum_{z\in G} f(z)(gh)(z^{-1}x) = \sum_{z\in G} f(z)\sum_{y\in G} g(y)h(y^{-1}(z^{-1}x)) \\ &= \sum_{z\in G} f(z)\sum_{y\in G} g(y)h(y^{-1}z^{-1}x). \end{aligned}$$

(iii) Visbeidzot jāparāda, ka kopā $R(G)$ izpildās distributīvie likumi.

$$\begin{aligned}((f+g)h)(x) &= \sum_{y\in G}(f+g)(y)h(y^{-1}x) = \sum_{y\in G}[f(y)+g(y)]h(y^{-1}x) \\ &= \sum_{y\in G} f(y)h(y^{-1}x) + \sum_{y\in G} g(y)h(y^{-1}x) \\ &= (fg)(x) + (gh)(x).\end{aligned}$$

Otrs distributīvais likums pierādāms pēc tās pašas shēmas, tāpēc to atstājam kā vingrinājumu lasītājam. ■

6.7.2. Definīcija. *$R(G)$ sauc par grupas G gredzenu ar koeficientiem no gredzena G. Reizinšanu gredzenā G sauc par tinumu.*

Pieņemsim, ka $\sigma \in G$, tad

$$\lfloor\sigma\rfloor(x) \rightleftharpoons \begin{cases} 1, & \text{ja} \quad x=\sigma; \\ 0, & \text{ja} \quad x \neq \sigma. \end{cases}$$

6.7.3. Piemērs. Pieņemsim, ka grupas G neitrālais elements ir e, tad

$$\lfloor e\rfloor(x) = \left\{ \begin{array}{lll} 1, & \text{ja} & x=e; \\ 0, & \text{ja} & x\neq e. \end{array} \right\} = 1(x).$$

Pieņemsim, ka $a \in R$, tad

$$\lfloor a\sigma\rfloor(x) \rightleftharpoons \begin{cases} a, & \text{ja} \quad x=\sigma; \\ 0, & \text{ja} \quad x \neq \sigma. \end{cases}$$

6.7.4. Piemēri.

$$\begin{aligned}\lfloor 1\sigma\rfloor(x) &\rightleftharpoons \left\{ \begin{array}{lll} 1, & \text{ja} & x=\sigma; \\ 0, & \text{ja} & x\neq\sigma. \end{array} \right\} = \lfloor\sigma\rfloor(x), \\ \lfloor 0\sigma\rfloor(x) &\rightleftharpoons \left\{ \begin{array}{lll} 0, & \text{ja} & x=\sigma; \\ 0, & \text{ja} & x\neq\sigma. \end{array} \right\} = 0(x).\end{aligned}$$

6.7.5. Vingrinājums. *Ja $a \in R$, $b \in R$ un $\sigma_1 \in G$, $\sigma_2 \in G$, tad*

$$\begin{aligned}\lfloor a\sigma_1\rfloor + \lfloor b\sigma_1\rfloor &= \lfloor (a+b)\sigma_1\rfloor, \\ (\lfloor a\sigma_1\rfloor)(\lfloor b\sigma_2\rfloor) &= \lfloor (ab)(\sigma_1\sigma_2)\rfloor.\end{aligned}$$

6.7.6. Apgalvojums. *Katram attēlojumam $f \in R(G)$ eksistē viena vienīga reprezentācija izskatā*

$$f = \sum_{\sigma \in G} \lfloor a_\sigma \sigma \rfloor,$$

kur gandrīz visi $a_\sigma = 0$.

$\square$ Pieņemsim, ka $a_\sigma \leftharpoondown f(\sigma)$. Saskaņā ar f definīciju $\overset{\infty}{\forall} \sigma\ f(\sigma) = 0$. Tā rezultātā summa $\sum_{\sigma \in G} \lfloor a_\sigma \sigma \rfloor$ definēta korekti un tāpēc $\sum_{\sigma \in G} \lfloor a_\sigma \sigma \rfloor \in R(G)$.

$$\begin{aligned}
(\sum_{\sigma \in G} \lfloor a_\sigma \sigma \rfloor)(x) &= \sum_{\sigma \in G} \lfloor a_\sigma \sigma \rfloor(x) = \sum_{\sigma \in G} \left\{ \begin{array}{cc} a_x, & \text{ja} \quad \sigma = x; \\ 0, & \text{ja} \quad \sigma \neq x. \end{array} \right\} \\
&= a_x = f(x).
\end{aligned}$$

Tas pamato eksistenci.

Pieņemsim, ka $f = \sum_{\sigma \in G} \lfloor b_\sigma \sigma \rfloor$, tad katram $x \in G$

$$a_x = f(x) = (\sum_{\sigma \in G} \lfloor b_\sigma \sigma \rfloor)(x) = \sum_{\sigma \in G} \lfloor b_\sigma \sigma \rfloor(x) = b_x.$$

Tas pamato unitāti. $\blacksquare$

6.7.7. Vingrinājumi. (i) Attēlojums $\varphi : R \to R(G) : a \mapsto \lfloor ae \rfloor$ ir gredzenu homomorfisms.

(ii) Attēlojums $R \times R(G) \to R(G) : (a, f) \mapsto \lfloor ae \rfloor f$ ir gredzena R multiplikatīvā monoīda iedarbība uz $R(G)$ no kreisās puses.

(iii) $R(G)$ ir R–modulis, kur R iedarbība uz $R(G)$ no kreisās puses definēta ar nosacījumu $(a, f) \mapsto \lfloor ae \rfloor f$.

(iv) Ja R — komutatīvs gredzens, tad $\{\lfloor ae \rfloor \mid a \in R\}$ ietilpst gredzena $R(G)$ centrā.

(v) Ja R — komutatīvs gredzens, tad $R(G)$ ir R–algebra, kur R iedarbība uz $R(G)$ no kreisās puses definēta ar nosacījumu $(a, f) \mapsto \lfloor ae \rfloor f$.

(vi) Ja G ir nekomutatīva grupa, tad $R(G)$ ir nekomutatīvs gredzens pat ja R ir komutatīvs gredzens.

Pieņemsim, ka $a \in R$ un $\sigma \in G$, tad pieraksta $\lfloor a\sigma \rfloor$ vietā lietosim pierakstu $a\sigma$. Parasti šāds pieraksts nerada pārpratumus, un tāpēc tas tiek plaši lietots. Tā rezultātā, ja $f = \sum\limits_{\sigma \in G} \lfloor a_\sigma \sigma \rfloor$, mēs iegūstam pierakstu

$$f = \sum_{\sigma \in G} a_\sigma \sigma.$$

6.7.8. Definīcija. *Gredzena $R(G)$ centru sauc par grupu algebras $R(G)$ centru.*

Tiem, kas jau aizmirsuši, kas ir gredzena centrs iesakam skatīt Definīciju 4.5.1.

6.7.9. Teorēma. *Grupu algebras $R(G)$ elements $f = \sum\limits_{\xi \in G} a_\xi \xi$ atrodas algebras $R(G)$ centrā Z tad un tikai tad, ja $a_\sigma = a_\tau$ katram grupas G saistīto elementu pārim (σ, τ).*

$\square$ $\Rightarrow$ Pieņemsim, ka $f \in Z$ un elementu pāris (σ, τ) ir saistīto elementu pāris. Atgādināsim (Definīcija 3.14.1), ka grupas G elementus σ un τ sauc par saistītiem elementiem, ja eksistē tāds grupas G elements η, ka $\tau = \eta\sigma\eta^{-1}$.

Tā kā $f \in Z$, tad $\lfloor \eta \rfloor f = f \lfloor \eta \rfloor$. No šejienes

$$\begin{aligned} \lfloor \eta \rfloor f \lfloor \eta^{-1} \rfloor &= f \lfloor \eta \rfloor \lfloor \eta^{-1} \rfloor \overset{\text{P6.7.4}}{=} f \lfloor 1\eta \rfloor \lfloor 1\eta^{-1} \rfloor \overset{\text{P6.7.5}}{=} f \lfloor (11)(\eta\eta^{-1}) \rfloor \\ &= f \lfloor e \rfloor \overset{\text{P6.7.3}}{=} f 1_{L(G)} = f. \end{aligned}$$

Savukārt

$$\begin{aligned} \lfloor \eta \rfloor f \lfloor \eta^{-1} \rfloor &= \lfloor 1\eta \rfloor \sum_{\xi \in G} \lfloor a_\xi \xi \rfloor \lfloor 1\eta^{-1} \rfloor = \sum_{\xi \in G} \lfloor 1\eta \rfloor \lfloor a_\xi \xi \rfloor \lfloor 1\eta^{-1} \rfloor \\ &\overset{\text{V6.7.5}}{=} \sum_{\xi \in G} \lfloor (1a_\xi 1)(\eta\xi\eta^{-1}) \rfloor = \sum_{\xi \in G} \lfloor a_\xi (\eta\xi\eta^{-1}) \rfloor. \end{aligned}$$

Tātad

$$\sum_{\xi \in G} \lfloor a_\xi \xi \rfloor = \sum_{\xi \in G} \lfloor a_\xi (\eta\xi\eta^{-1}) \rfloor.$$

No šejienes

$$\lfloor a_\tau \tau \rfloor = \lfloor a_\tau (\eta\sigma\eta^{-1}) \rfloor = \lfloor a_\sigma (\eta\sigma\eta^{-1}) \rfloor = \lfloor a_\sigma \tau \rfloor.$$

Tas iespējams tikai tad, ja $a_\sigma = a_\tau$.

$\Leftarrow$ Pieņemsim, ka jebkuram grupas G elementu pārim (σ, η) $\quad a_\sigma = a_{\eta\sigma\eta^{-1}}$, tad

$$\lfloor \eta \rfloor f \lfloor \eta^{-1} \rfloor = \sum_{\xi \in G} \lfloor a_\xi (\eta\xi\eta^{-1}) \rfloor = \sum_{\xi \in G} \lfloor a_{\eta\xi\eta^{-1}} (\eta\xi\eta^{-1}) \rfloor .$$

Tagad ņemot vērā Apgalvojumu 2.7.4 un Vingrinājumu 2.7.5 secināms, ka attēlojums $\xi \mapsto \eta\xi\eta^{-1}$ ir kopas G substitūcija, tāpēc

$$\sum_{\xi \in G} \lfloor a_{\eta\xi\eta^{-1}} (\eta\xi\eta^{-1}) \rfloor = \sum_{\zeta \in G} \lfloor a_\zeta \zeta \rfloor = f.$$

Līdz ar to $\forall \eta \in G \ \lfloor \eta \rfloor f = f \lfloor \eta \rfloor$.

Pieņemsim, ka $g = \sum_{\eta \in G} \lfloor b_\eta \eta \rfloor \in R(G)$, tad

$$\begin{aligned} gf &= \Big(\sum_{\eta \in G} \lfloor b_\eta \eta \rfloor \Big) f = \Big(\sum_{\eta \in G} b_\eta \lfloor \eta \rfloor \Big) f = \sum_{\eta \in G} (b_\eta \lfloor \eta \rfloor) f = \sum_{\eta \in G} b_\eta (\lfloor \eta \rfloor f) \\ &= \sum_{\eta \in G} b_\eta (f \lfloor \eta \rfloor) = \sum_{\eta \in G} f (b_\eta \lfloor \eta \rfloor) = f \sum_{\eta \in G} b_\eta \lfloor \eta \rfloor = f \sum_{\eta \in G} \lfloor b_\eta \eta \rfloor = fg. \end{aligned}$$

Tātad $f \in Z$. ■

7. nodaļa

POLINOMI

Bilineārs attēlojums, pusgrupu algebras, polinomi. Substitūcijas teorēma. Integritātes apgabals, polinomi pār integritātes apgabalu. Dalīšanas algoritms. Bezū teorēma. Galveno ideālu apgabals, polinomi pār lauku.

7.1. Pusgrupu algebras

Šis nodaļas ietvaros, ja nekas speciāli netiks atrunāts, visi gredzeni ir gredzeni ar vieninieku. Simbolu R mēs rezervējam komutatīva gredzena ar vieninieku apzīmēšanai.

7.1.1. Definīcija. *Pieņemsim, ka M un M' ir R–moduļi. Attēlojumu $\beta : M^2 \to M'$ sauc par bilineāru attēlojumu, ja*

- *katram $x \in M$ attēlojums $\beta^x(y) \leftharpoondown \beta(x, y)$ ir moduļu M, M' homomorfisms,*
- *katram $y \in M$ attēlojums $\beta_y(x) \leftharpoondown \beta(x, y)$ ir moduļu M, M' homomorfisms.*

Ja $\langle R, A, +, \cdot, \oplus, \circ, \odot \rangle$ ir asociatīva algebra, tad attēlojums $A^2 \overset{\odot}{\to} A$ ir bilineārs attēlojums.

Atzīmēsim, ka R–modulis A ir asociatīva algebra, ja kopā $A^2 \overset{\odot}{\to} A$ ir definēts bilineārs attēlojums, kas ir asociatīvs, proti,

$$\forall x \in A \, \forall y \in A \, \forall z \in A \quad (x \odot y) \odot z = x \odot (y \odot z);$$

bez tam kopā A eksistē tāds elements 1_A, ka

$$\forall x \in A \quad 1_A \odot x = x = x \odot 1_A.$$

Mēs atkārtosim konstrukcijas, kādas veicām definējot grupas algebru. Pieņemsim, ka P — pusgrupa, tad

$$R(P) \leftharpoondown \{f : P \to R \mid \overset{\infty}{\forall}\, x\; f(x) = 0\}.$$

Pieņemsim, ka f un g ir kopas $R(P)$ elementi, tad

$$\begin{aligned} (f+g)(x) &\leftharpoondown f(x) + g(x), \\ (fg)(x) &\leftharpoondown \sum_{yz=x} f(y)g(z). \end{aligned}$$

Tā kā gandrīz visiem y attēlojums $f(y) = 0$, tad reizināšana fg ir definēta korekti.

Pieņemsim, ka $y_1, y_2, \ldots, y_n$ ir tie pusgrupas P elementi, kuriem $f(y) \neq 0$. Attiecīgi $z_1, z_2, \ldots, z_m$ ir tie pusgrupas P elementi, kuriem $g(z) \neq 0$. Veidojot visus iespējamos reizinājumus $y_i z_j$ var iegūt ne vairāk kā nm pusgrupas P elementu. Tas nozīmē, ka $fg \in R(P)$.

7.1.2. Lemma. *Kopā $R(P)$ izpildās distributīvie likumi.*

□

$$\begin{aligned} ((f+g)h)(x) &= \sum_{yz=x} (f+g)(y)h(z) = \sum_{yz=x} [f(y) + g(y)]h(z) \\ &= \sum_{yz=x} f(y)h(z) + \sum_{yz=x} g(y)h(z) \\ &= (fg)(x) + (gh)(x). \end{aligned}$$

Otrs distributīvais likums pierādāms pēc tās pašas shēmas, tāpēc to atstājam kā vingrinājumu lasītājam. ■

Ja pusgrupas P neitrālais elements ir e, tad kopā $R(P)$ vienības elements ir attēlojums

$$1(x) \leftharpoondown \begin{cases} 1, & \text{ja } x = e; \\ 0, & \text{ja } x \neq e. \end{cases}$$

Šai situācijā

$$\begin{aligned}
(1f)(x) &= \sum_{yz=x} 1(y)f(z) = f(x), \\
(f1)(x) &= \sum_{yz=x} f(y)1(z) = f(x)1(e) = f(x).
\end{aligned}$$

Pieņemsim, ka $\sigma \in P$, tad

$$\lfloor \sigma \rfloor (x) \leftharpoondown \begin{cases} 1, & \text{ja} \quad x = \sigma; \\ 0, & \text{ja} \quad x \neq \sigma. \end{cases}$$

7.1.3. Piemērs. Pieņemsim, ka pusgrupas P neitrālais elements ir e, tad

$$\lfloor e \rfloor (x) = \left\{ \begin{array}{ll} 1, & \text{ja} \quad x = e; \\ 0, & \text{ja} \quad x \neq e. \end{array} \right\} = 1(x).$$

Pieņemsim, ka $a \in R$, tad

$$\lfloor a\sigma \rfloor (x) \leftharpoondown \begin{cases} a, & \text{ja} \quad x = \sigma; \\ 0, & \text{ja} \quad x \neq \sigma. \end{cases}$$

7.1.4. Piemēri.

$$\begin{aligned}
\lfloor 1\sigma \rfloor (x) &\leftharpoondown \left\{ \begin{array}{ll} 1, & \text{ja} \quad x = \sigma; \\ 0, & \text{ja} \quad x \neq \sigma. \end{array} \right\} = \lfloor \sigma \rfloor (x), \\
\lfloor 0\sigma \rfloor (x) &\leftharpoondown \left\{ \begin{array}{ll} 0, & \text{ja} \quad x = \sigma; \\ 0, & \text{ja} \quad x \neq \sigma. \end{array} \right\} = 0(x).
\end{aligned}$$

7.1.5. Apgalvojums. *Katram attēlojumam $f \in R(P)$ eksistē viena vienīga reprezentācija izskatā*

$$f = \sum_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor,$$

kur gandrīz visi $a_\sigma = 0$.

□ Pieņemsim, ka $a_\sigma \leftharpoondown f(\sigma)$. Saskaņā ar f definīciju $\overset{\infty}{\forall} \sigma \; f(\sigma) = 0$. Tā rezultātā summa $\sum\limits_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor$ definēta korekti un tāpēc $\sum\limits_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor \in R(P)$.

$$\begin{aligned}
\Big(\sum_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor\Big)(x) &= \sum_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor (x) = \sum_{\sigma \in P} \left\{ \begin{array}{ll} a_x, & \text{ja} \quad \sigma = x; \\ 0, & \text{ja} \quad \sigma \neq x. \end{array} \right\} \\
&= a_x = f(x).
\end{aligned}$$

Tas pamato eksistenci.

Pieņemsim, ka $f = \sum_{\sigma \in P} \lfloor b_\sigma \sigma \rfloor$, tad katram $x \in P$

$$a_x = f(x) = (\sum_{\sigma \in P} \lfloor b_\sigma \sigma \rfloor)(x) = \sum_{\sigma \in P} \lfloor b_\sigma \sigma \rfloor (x) = b_x.$$

Tas pamato unitāti. ∎

7.1.6. Lemma. *Ja $a \in R$, $b \in R$ un $\sigma_1 \in P$, $\sigma_2 \in P$, tad*

$$(\lfloor a\sigma_1 \rfloor)(\lfloor b\sigma_2 \rfloor) = \lfloor (ab)(\sigma_1\sigma_2) \rfloor.$$

□
$$\begin{aligned}
(\lfloor a\sigma_1 \rfloor)(\lfloor b\sigma_2 \rfloor))(x) &= \sum_{yz=x} \lfloor a\sigma_1 \rfloor (y) \lfloor b\sigma_1 \rfloor (z) \\
&= \begin{cases} ab, & \text{ja} \quad y = \sigma_1 \text{ un } z = \sigma_2, \text{ un } yz = x; \\ 0, & \text{pretējā gadījumā.} \end{cases} \\
&= \lfloor (ab)(\sigma_1\sigma_2) \rfloor (x). \qquad \blacksquare
\end{aligned}$$

7.1.7. Sekas. *Ja $f = \sum_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor$ un $g = \sum_{\tau \in P} \lfloor b_\tau \tau \rfloor$, tad*

$$fg = \sum_{\sigma \in P} \sum_{\tau \in P} \lfloor (a_\sigma b_\tau)(\sigma\tau) \rfloor.$$

7.1.8. Apgalvojums. *$R(P)$ ir gredzens. Ja P ir monoīds, tad $R(P)$ ir gredzens ar vienības elementu.*

□ Ņemot vērā iepriekš izklāstīto mums atliek tikai parādīt, ka reizināšana ir asociatīva. Pieņemsim, ka $f = \sum_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor$, $g = \sum_{\tau \in P} \lfloor b_\tau \tau \rfloor$ un $h = \sum_{\eta \in P} \lfloor c_\eta \eta \rfloor$, tad (Sekas 7.1.7)

$$\begin{aligned}
(fg)h &= \sum_{\sigma\in P}\sum_{\tau\in P}\lfloor(a_\sigma b_\tau)(\sigma\tau)\rfloor\sum_{\eta\in P}\lfloor c_\eta\eta\rfloor \\
&= \sum_{\sigma\in P}\sum_{\tau\in P}\sum_{\eta\in P}\lfloor(a_\sigma b_\tau)(\sigma\tau)\rfloor\lfloor c_\eta\eta\rfloor \\
&= \sum_{\sigma\in P}\sum_{\tau\in P}\sum_{\eta\in P}\lfloor((a_\sigma b_\tau)c_\eta)((\sigma\tau)\eta)\rfloor, \\
f(gh) &= \sum_{\sigma\in P}\lfloor a_\sigma\sigma\rfloor\sum_{\tau\in P}\sum_{\eta\in P}\lfloor(b_\tau c_\eta)(\tau\eta)\rfloor \\
&= \sum_{\sigma\in P}\sum_{\tau\in P}\sum_{\eta\in P}\lfloor a_\sigma\sigma\rfloor\lfloor(b_\tau c_\eta)(\tau\eta)\rfloor \\
&= \sum_{\sigma\in P}\sum_{\tau\in P}\sum_{\eta\in P}\lfloor(a_\sigma(b_\tau c_\eta))(\sigma(\tau\eta))\rfloor.
\end{aligned}$$

Tā kā $(a_\sigma b_\tau)c_\eta = a_\sigma(b_\tau c_\eta)$ un $(\sigma\tau)\eta = \sigma(\tau\eta)$, tad $(fg)h = f(gh)$. ■

7.1.9. Teorēma. *Ja R — komutatīvs gredzens un P — monoīds, tad $R(P)$ ir R–algebra, kur R iedarbība uz $R(P)$ no kreisās puses definēta ar nosacījumu $(a, f) \mapsto \lfloor ae\rfloor f$.*

□ (i) Mēs jau konstatējām, ka $R(P)$ ir gredzens ar vieninieku.

(ii) Pieņemsim, ka $f \in R(P)$, tad f var reprezentēt izskatā $f = \sum\limits_{\sigma\in P}\lfloor a_\sigma\sigma\rfloor$.

Pieņemsim, ka a un b ir gredzena R elementi, un e ir monoīda P neitrālais elements, tad

$$\begin{aligned}
(ab)f &= \lfloor(ab)e\rfloor\sum_{\sigma\in P}\lfloor a_\sigma\sigma\rfloor = \sum_{\sigma\in P}\lfloor((ab)a_\sigma)(e\sigma)\rfloor \\
&= \sum_{\sigma\in P}\lfloor(a(ba_\sigma))(e(e\sigma))\rfloor = \lfloor ae\rfloor\sum_{\sigma\in P}\lfloor(ba_\sigma)(e\sigma)\rfloor \\
&= \lfloor ae\rfloor(\lfloor be\rfloor\sum_{\sigma\in P}\lfloor a_\sigma\sigma\rfloor) = a(bf);
\end{aligned}$$

bez tam

$$\begin{aligned}
1f &= \lfloor 1e\rfloor\sum_{\sigma\in P}\lfloor a_\sigma\sigma\rfloor = \sum_{\sigma\in P}\lfloor(1a_\sigma)(e\sigma)\rfloor \\
&= \sum_{\sigma\in P}\lfloor a_\sigma\sigma\rfloor = f.
\end{aligned}$$

Līdz ar to esam parādījuši, ka $(a, f) \mapsto \lfloor ae \rfloor f$ ir R–iedarbība uz $R(P)$ no kreisās puses.

(iii) Pieņemsim, ka $g \in R(P)$, tad g var reprezentēt izskatā $g = \sum_{\sigma \in P} \lfloor b_\sigma \sigma \rfloor$.

$$\begin{aligned}
a(f+g) &= \lfloor ae \rfloor \Big(\sum_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor + \sum_{\sigma \in P} \lfloor b_\sigma \sigma \rfloor \Big) \\
&= \lfloor ae \rfloor \sum_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor + \lfloor ae \rfloor \sum_{\sigma \in P} \lfloor b_\sigma \sigma \rfloor = af + ag; \\
(a+b)f &= \big(\lfloor ae \rfloor + \lfloor be \rfloor \big) \sum_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor \\
&= \lfloor ae \rfloor \sum_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor + \lfloor be \rfloor \sum_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor = af + bf.
\end{aligned}$$

Tagad esam parādījuši, ka $R(P)$ ir R–modulis.

(iv)

$$\begin{aligned}
a(fg) &= \lfloor ae \rfloor \Big(\sum_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor \sum_{\tau \in P} \lfloor b_\tau \tau \rfloor \Big) = \lfloor ae \rfloor \sum_{\sigma \in P} \sum_{\tau \in P} \lfloor (a_\sigma b_\tau)(\sigma\tau) \rfloor \\
&= \sum_{\sigma \in P} \sum_{\tau \in P} \lfloor ae \rfloor \lfloor (a_\sigma b_\tau)(\sigma\tau) \rfloor = \sum_{\sigma \in P} \sum_{\tau \in P} \lfloor (a(a_\sigma b_\tau))(e(\sigma\tau)) \rfloor \\
&= \sum_{\sigma \in P} \sum_{\tau \in P} \lfloor ((aa_\sigma) b_\tau)(\sigma\tau) \rfloor = \sum_{\sigma \in P} \lfloor (aa_\sigma)\sigma \rfloor \sum_{\tau \in P} \lfloor b_\tau \tau \rfloor \\
&= \big(\lfloor ae \rfloor \sum_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor \big) \sum_{\tau \in P} \lfloor b_\tau \tau \rfloor = (af)g; \\
a(fg) &= \sum_{\sigma \in P} \sum_{\tau \in P} \lfloor ((aa_\sigma) b_\tau)(\sigma\tau) \rfloor = \sum_{\sigma \in P} \sum_{\tau \in P} \lfloor (a_\sigma (ab_\tau))(\sigma\tau) \rfloor \\
&= \sum_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor \sum_{\tau \in P} \lfloor (ab_\tau)\tau \rfloor = \sum_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor \big(\lfloor ae \rfloor \sum_{\tau \in P} \lfloor b_\tau \tau \rfloor \big) \\
&= f(ag).
\end{aligned}$$

Tātad $a(fg) = (af)g = f(ag)$.

(v) Tā kā R ir komutatīvs gredzens, tad, ņemot vērā punktos (i)–(iv) pierādīto, saskaņā ar Definīciju 6.1.1 secināms, ka $R(P)$ ir R–algabra. ∎

7.1.10. Definīcija. *Asociatīvo algebru $R(P)$ sauc par monoīda P algebru.*

Ja asociatīvās algebras definīcijā neprasa, lai $R(P)$ būtu gredzens ar vienības elementu, bet prasa tikai, lai $R(P)$ būtu gredzens, tad var pierādīt sekojošu rezultātu.

7.1.11. Vingrinājums. Ja R — komutatīvs gredzens un P — pusgrupa, tad $R(P)$ ir R–algebra, kur R iedarbība uz $R(P)$ no kreisās puses definēta ar nosacījumu $(a, f) \mapsto \sum\limits_{\sigma \in P} \lfloor (aa_\sigma)\sigma \rfloor$. Te attēlojums f ir reprezentēts izskatā $f = \sum\limits_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor$.

Šai gadījumā asociatīvo algebru $R(P)$ sauc par *pusgrupas P algebru.*

Pieņemsim, ka $a \in R$ un $\sigma \in P$, tad pieraksta $\lfloor a\sigma \rfloor$ vietā lietosim pierakstu $a\sigma$. Parasti šāds pieraksts nerada pārpratumus, un tāpēc tas tiek plaši lietots. Tā rezultātā, ja $f = \sum\limits_{\sigma \in P} \lfloor a_\sigma \sigma \rfloor$, mēs iegūstam pierakstu

$$f = \sum_{\sigma \in P} a_\sigma \sigma.$$

7.1.12. Vingrinājums. Ja P ir komutatīva pusgrupa, tad $R(P)$ ir komutatīvs gredzens.

7.2. Polinomu algebra

Ja gadījumā lauks ir galīgs, funkcionālā pieeja rada nepatikšanas. Tā, piemēram, funcijas $y_1 = x^2 + x + 1$ un $y_2 = x^3 + x + 1$ rezidiju laukā $\mathbb{Z}_2$ (Piemērs 4.3.8(ii)) definē vienu un to pašu funkciju. Tiešām,

$$\begin{aligned} y_1(0) &= 0^2 + 0 + 1 = 1 = 0^3 + 0 + 1 = y_2(0), \\ y_1(1) &= 1^2 + 1 + 1 = 1 = 1^3 + 1 + 1 = y_2(1). \end{aligned}$$

Lai pārvarētu šīs grūtības, vispārīgā gadījumā polinomus definē citādi.

7.2.1. Definīcija. *Monoīda $\mathbb{N}$ algebru $R(\mathbb{N})$ sauc par polinomu algebru pār gredzenu R.*

Šai gadījumā parasti lieto nevis apzīmējumu $R(\mathbb{N})$, bet gan apzīmējumu $R[X]$. Arī mēs pieturēsimies pie šīs tradīcijas. Kopas $R[X]$ elementus sauc par *polinomiem pār gredzenu R.* Ja no konteksta ir noprotams gredzens R

vai arī šāda informācija nav būtiska, tad lieto īsāku terminu, proti, kopas $R[X]$ elementus sauc par *polinomiem*.

Katram $n \in \mathbb{N}$ definējam attēlojumu $X^n \leftharpoondown \lfloor n \rfloor$.

7.2.2. Lemma. (i) $X^0 = 1_{R[X]}$,

(ii) $\forall m \in \mathbb{N}\, \forall n \in \mathbb{N} \quad X^m X^n = X^{m+n}$.

(iii) *Katram attēlojumam $f \in R[X]$ eksistē viena vienīga reprezentācija izskatā*

$$f = \sum_{k \in \mathbb{N}} a_k X^k,$$

kur gandrīz visi $a_k = 0$.

□ (i) $X^0 = \lfloor 0 \rfloor \overset{\text{P7.1.3}}{=} 1_{R[X]}$.
(ii) $X^m X^n = \lfloor m \rfloor \lfloor n \rfloor \overset{\text{L7.1.6}}{=} \lfloor m+n \rfloor = X^{m+n}$.
(iii) $f \overset{\text{A7.1.5}}{=} \sum\limits_{k \in \mathbb{N}} \lfloor a_k k \rfloor \overset{\text{T7.1.9}}{=} \sum\limits_{k \in \mathbb{N}} a_k \lfloor k \rfloor = \sum\limits_{k \in \mathbb{N}} a_k X^k$. ■

Tātad, ja $f \in R[X]$, tad $f = \sum\limits_{k \in \mathbb{N}} a_k X^k$, kur gandrīz visi $a_k = 0$. Ja reiz gandrīz visi $a_k = 0$, tad

$$\exists n \in \mathbb{N}\, \forall k > n \quad a_k = 0.$$

Līdz ar to

$$f = \sum_{k \in \mathbb{N}} a_k X^k = \sum_{k=0}^{n} a_k X^k.$$

Ja mēs elementu $a \in R$ identificējam ar $aX^0 \in R[X]$ un X^1 identificējam ar X, tad iegūstam šādu polinoma f pierakstu

$$f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0,$$

kas ir tradicionāls labi pzīstams polinoma pieraksts. Gredzena R elementus a_k sauc par *polinoma f koeficientiem.* Ja $a_n = 1_R$, tad polinomu f sauc par *unitāru polinomu.*

Reālo skaitļu gadījumā šīs abas pieejas dod vienu un to pašu rezultātu.

7.2.3. Vingrinājums. Ja

$$\mathrm{Pol}(\mathbb{R}) \leftharpoondown \{f : \mathbb{R} \to \mathbb{R} \mid \exists n \in \mathbb{N}\ f(x) = \sum_{k=0}^{n} a_k x^k\},$$

tad $\mathbb{R}$–algebras $\mathbb{R}[X]$ un $\mathrm{Pol}(\mathbb{R})$ ir izomorfas.

Mājiens. Vienīgās problēmas šī fakta konstatācijā saistāmas ar pierādījumu, ka attēlojums

$$\varphi : \mathbb{R}[X] \to \mathrm{Pol}(\mathbb{R}) : \sum_{k=0}^{n} a_k X^k \mapsto \sum_{k=0}^{n} a_k x^k$$

ir injekcija.

Tradicionāli polinomu apzīmēšanai lieto pierakstu $f(X)$, kas vizuāli saistīts ar algebras $\mathrm{Pol}(\mathbb{R})$ elementu pierakstu, proti, algebras $\mathrm{Pol}(\mathbb{R})$ elementi ir neatkarīgā mainīgā x funkcijas. Gadījumā, ja $f(X) \in R[X]$, tad f nav mainīgā $X \in R$ funkcija, kaut vai tā vienkāršā iemesla dēļ, ka $X \notin R$, bet gan $X \in R[X]$. Taču funkcionālo koncepciju var ieviest.

Pieņemsim, ka S ir komutatīvs gredzens ar vienības elementu 1_S un $\phi : R \to S$ ir tāds gredzenu homomorfisms, ka $\phi(1_R) = 1_S$. Katram $u \in S$ definējam attēlojumu

$$\phi_u : R[X] \to S$$

ar formulu

$$\phi_u(a_n X^n + \ldots + a_1 X + a_0) \leftharpoondown \phi(a_n)u^n + \ldots + \phi(a_1)u + \phi(a_0).$$

7.2.4. Vingrinājumi.

(i) $$\Big(\sum_{i=0}^{m} a_i X^i\Big)\Big(\sum_{j=0}^{n} b_j X^j\Big) = \sum_{k=0}^{m+n} c_k X^k, \quad \text{kur} \quad c_k = \sum_{i=0}^{k} a_i b_{k-i}.$$

(ii) $\phi_u : R[X] \to S$ ir gredzenu homomorfisms.

(iii) Attēlojums $\iota : R \to R[X] : a \mapsto aX^0$ ir gredzenu monomorfisms.

7.2.5. Definīcija. *Attēlojumu $\phi_u : R[X] \to S$ sauc par homomorfisma $\phi : R \to S$ un elementa $u \in S$ determinēto substitūcijas homomorfismu.*

Ja nerodas pārpratumi, tad lieto īsāku terminu, proti, ϕ_u sauc par *substitūcijas homomorfismu.*

7.2.6. Teorēma (Polinomu substitūcijas teorēma). *Pieņemsim, ka R, S — komutatīvi gredzeni, $\phi(1_R) = 1_S$ un $u \in S$. Katram gredzenu homomorfismam $\phi : R \to S$ eksistē viens vienīgs gredzenu homomorfisms $\phi_u : R[X] \to S$, ka $\phi_u|R = \phi$.*

□ Ņemsim vērā, ka polinomu gadījumā katru $aX^0 \in R[X]$ identificē ar $a \in R$. Ja mēs šo vienošanos ignorējam, tad $\phi_u|R = \phi$ vietā jāraksta

$$\forall a \in R \quad \phi_u(aX_0) = \phi(a).$$

(i) Eksistences pierādījumu mēs uzticējām lasītājam (skatīt Vingrinājumu 7.2.4(ii)).

(ii) Pieņemsim, ka $\tilde{\phi}_u : R[X] \to S$ ir tāds gredzenu homomorfisms, ka $\tilde{\phi}_u(X) = u$ un $\tilde{\phi}_u|R = \phi$, tad

$$\begin{aligned}
\tilde{\phi}_u(X^n) &= \tilde{\phi}_u(\underbrace{XX\dots X}_{n}) = \underbrace{\tilde{\phi}_u(X)\tilde{\phi}_u(X)\dots\tilde{\phi}_u(X)}_{n} \\
&= \underbrace{uu\dots u}_{n} = u^n = \phi_u(X^n), \\
\tilde{\phi}_u(aX^n) &= \tilde{\phi}_u((aX^0)X^n) = \tilde{\phi}_u(aX^0)\tilde{\phi}_u(X^n) \\
&= \phi(a)u^n = \phi_u(aX^n).
\end{aligned}$$

No šejienes

$$\begin{aligned}
\tilde{\phi}_u(a_nX^n + \dots + a_1X + a_0) &= \tilde{\phi}_u(a_nX^n) + \dots + \tilde{\phi}_u(a_1X) + \tilde{\phi}_u(a_0X^0) \\
&= \phi_u(a_nX^n) + \dots + \phi_u(a_1X) + \phi_u(a_0X^0) \\
&= \phi_u(a_nX^n + \dots + a_1X + a_0). \quad \blacksquare
\end{aligned}$$

Vienošanās. Gadījumā, ja $S = R$ un $\phi = \mathbb{I}_R$, tad $\phi_u(f)$ vietā lieto pierakstu $f(u)$.

7.3. Polinomi pār integritātes apgabalu

Polinomu $f(X) = \sum_{k=0}^{n} a_kX^k$ sauc par *nenulles polinomu*, ja

$$\exists i \in \overline{0, n} \quad a_i \neq 0.$$

7.3.1. Definīcija. *Skaitli* $\deg f \leftharpoondown\!\!\!\!\rightharpoondown \max\{k \mid a_k \neq 0\}$ *sauc par nenulles polinoma* $f(X) = \sum\limits_{k=0}^{n} a_k X^k$ *pakāpi. Ja* $f(X) = 0_{R[X]}$, *tad* $\deg f \leftharpoondown\!\!\!\!\rightharpoondown -\infty$.

Kopā $\mathbb{N} \cup \{-\infty\}$ definēsim saskaitīšanu izmantojot saskaitīšanas operāciju monoīdā $\mathbb{N}$:

$$a + b \leftharpoondown\!\!\!\!\rightharpoondown \begin{cases} a + b, & \text{ja} \quad a \in \mathbb{N} \text{ un } b \in \mathbb{N}; \\ -\infty, & \text{pretējā gadījumā.} \end{cases}$$

Elementu a_0 sauc par polinoma *brīvo locekli*, a_1X — par *lineāro locekli*, a_2X^2 — *kvadrātisko locekli*, a_3X^3 — *kubisko locekli*, a_kX^k — par *k–tās pakāpes locekli.* Ja $\deg f = n \in \mathbb{N}$, tad a_n sauc par polinoma $f(X)$ *vecāko koeficientu*, polinomu a_nX^n šai situācijā sauc par polinoma $f(X)$ *vecāko locekli* (lieto arī terminus: *galvenais loceklis, augstākās pakāpes loceklis*).

Polinomu aX^k sauc par *monomu.* Līdz ar to polinoms ir monomu summa.

7.3.2. Lemma. *Ja* $f(X) \in R[X]$ *un* $g(X) \in R[X]$, *tad*

(i) $\deg(f + g) \leq \max\{\deg f, \deg g\}$;

(ii) $\deg(fg) \leq \deg f + \deg g$.

□ (i) Pieņemsim, ka

$$\begin{aligned} f(X) &= a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0, \\ g(X) &= b_mX^m + a_{m-1}X^{m-1} + \ldots + b_1X + b_0. \end{aligned}$$

Pieņemsim, ka $d \leftharpoondown\!\!\!\!\rightharpoondown \max\{\deg f, \deg g\}$, tad

$$\begin{aligned} f(X) &= a_dX^d + a_{d-1}X^{d-1} + \ldots + a_1X + a_0, \\ g(X) &= b_dX^d + a_{d-1}X^{d-1} + \ldots + b_1X + b_0. \end{aligned}$$

Saprotams daži a_i vai b_j šai pierakstā var būt arī vienādi ar 0.

No šejienes

$$f(X) + g(X) = (a_d + b_d)X^d + (a_{d-1} + b_{d-1})X^{d-1} + \ldots + (a_1 + b_1)X + a_0 + b_0,$$

un tāpēc $\deg(f + g) \leq d = \max\{\deg f, \deg g\}$, jo nav izslēgts, ka $a_d + b_d = 0$.

(ii) $f(X)g(X) \overset{\text{V7.2.4(i)}}{=} a_nb_mX^{n+m} + \ldots + a_0b_0$, tāpēc

$$\deg(fg) \leq m + n = \deg f + \deg g,$$

jo nav izslēgts, ka a_n vai b_m ir nulles dalītājs, un tad $a_nb_m = 0$. ■

7.3.3. Sekas. *Ja $f(X) \in R[X]$, $g(X) \in R[X]$ un kaut viens no šo polinomu vecākajiem koeficientim ir apgriežams gredzenā R, tad* $\deg(fg) = \deg f + \deg g$.

□ Pieņemsim, ka

$$\begin{aligned} f(X) &= a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0, \qquad a_n \neq 0 \\ g(X) &= b_mX^m + a_{m-1}X^{m-1} + \ldots + b_1X + b_0, \qquad b_m \neq 0. \end{aligned}$$

No šejienes $f(X)g(X) \overset{\text{V7.2.4(i)}}{=} a_nb_mX^{n+m} + \ldots + a_0b_0$.

Pieņemsim, ka $\deg(fg) < \deg f + \deg g$, tad $a_nb_m = 0$.

(i) Pieņemsim, ka a_n ir apgriežams gredzenā R, tad $b_m = a_n^{-1}a_nb_m = 0$. Pretruna!

(ii) Pieņemsim, ka b_m ir apgriežams gredzenā R, tad $a_n = a_nb_mb_m^{-1} = 0$. Pretruna!

(iii) Esam konstatējuši (punkti (i) un (ii)), ka pieņemums $\deg(fg) \neq \deg f + \deg g$ rada pretrunas. Tātad tas ir nepareizs pieņemums. Atliek secināt, ka $\deg(fg) = \deg f + \deg g$. ■

7.3.4. Sekas. *Ja $f(X) \in R[X]$, $g(X) \in R[X]$ un kaut viens no šo polinomu vecākajiem koeficientim nav* 0 *dalītājs, tad* $\deg(fg) = \deg f + \deg g$.

□ Pieņemsim, ka

$$\begin{aligned} f(X) &= a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0, \\ g(X) &= b_mX^m + a_{m-1}X^{m-1} + \ldots + b_1X + b_0. \end{aligned}$$

No šejienes $f(X)g(X) \overset{\text{V7.2.4(i)}}{=} a_nb_mX^{n+m} + \ldots + a_0b_0$. Tā kā viens no koeficientiem a_n vai b_m nav nulles dalītājs, tad $a_nb_m \neq 0$, tāpēc

$$\deg(fg) = m + n = \deg f + \deg g. \quad ■$$

7.3.5. Sekas. *Ja R — integritātes apgabals, $f(X) \in R[X]$ un $g(X) \in R[X]$, tad* $\deg(fg) = \deg f + \deg g$.

□ Ja R ir integritātes apgabals, tad polinoma $f(X)$ vecākais koeficients nav nulles dalītājs, tāpēc (Sekas 7.3.4) $\deg(fg) = \deg f + \deg g$. ■

7.3.6. Apgalvojums. *Ja R — integritātes apgabals, tad $R[X]$ — integritātes apgabals.*

□ Ja $f(X) \neq 0_{R[X]}$ un $g(X) \neq 0_{R[X]}$, tad (Sekas 7.3.5)

$$\deg(fg) = \deg f + \deg g \geq 0 \neq -\infty.$$

Līdz ar to $fg \neq 0_{R[X]}$. ■

7.4. Dalīšanas algoritms

7.4.1. Teorēma. *Ja $f(X) \in R[X]$, $g(X) \in R[X]$ ir nenulles polinomi, bez tam polinoma $g(X)$ vecākais koeficients ir apgriežams gredzenā R, tad eksistē viens vienīgs polinomu pāris $q(X) \in R[X]$ un $r(X) \in R[X]$, kam*

$$f(X) = g(X)q(X) + r(X) \qquad \text{un} \qquad \deg r < \deg g.$$

□ Pieņemsim, ka

$$\begin{aligned} f(X) &= a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0, \qquad & n = \deg f, \\ g(X) &= b_m X^m + a_{m-1}X^{m-1} + \ldots + b_1 X + b_0, \qquad & m = \deg g. \end{aligned}$$

Saskaņā ar doto $a_n \neq 0 \neq b_m$ un b_m — apgriežams gredzenā R.

Tālākais pierādījums induktīvs pēc n.

(i) Ja $n = 0$ un $\deg g > \deg f$, tad ņemam

$$q(X) \leftrightharpoons 0_{R[X]} \qquad \text{un} \qquad r(X) \leftrightharpoons f(X).$$

(ii) Ja $n = 0$ un $\deg g = \deg f = 0$, tad ņemam

$$q(X) \leftrightharpoons a_n b_m^{-1} X^0 \qquad \text{un} \qquad r(X) \leftrightharpoons 0_{R[X]}.$$

(iii) Pieņemsim, ka teorēma pierādīta visiem polinomiem $f(X)$, kuru pakāpe $\deg f < n$.

a) Ja $\deg g > \deg f$, tad ņemam

$$q(X) \leftrightharpoons 0_{R[X]} \qquad \text{un} \qquad r(X) \leftrightharpoons f(X).$$

b) Ja $\deg g \leq \deg f$, tad

$$f(X) = a_n b_m^{-1} X^{n-m} g(X) + f_1(X), \qquad \text{kur} \qquad \deg f_1 < n.$$

Saskaņā ar indukcijas pieņēmumu

$$f(X) = a_n b_m^{-1} X^{n-m} g(X) + q_1(X)g(X) + r(X), \qquad \text{kur} \qquad \deg r < \deg g.$$

Ņemam $q(X) \leftrightharpoons a_n b_m^{-1} X^{n-m} + q_1(X)$.

Līdz ar to eksistences pierādījums veikts pilnībā. Pārejam pie unitātes pierādījuma.

Pieņemsim, ka $f(X) = q_1(X)g(X) + r_1(X) = q_2(X)g(X) + r_2(X)$, kur $\deg r_1 < \deg g$ un $\deg r_2 < \deg g$. No šejienes

$$(q_1(X) - q_2(X))g(X) = r_2(X) - r_1(X).$$

Polinoma $g(X)$ vecākais koeficients ir apgriežams, tāpēc (Sekas 7.3.3)

$$\deg((q_1 - q_2)g) = \deg(q_1 - q_2) + \deg g.$$

Tātad

$$\deg(q_1 - q_2) + \deg g = \deg(r_2 - r_1),$$

bet $\deg(r_2 - r_1) < \deg g$. Ja reiz tā, tad $\deg(r_2 - r_1)$ nav naturāls skaitlis. Atliek tikai $\deg(r_2 - r_1) = -\infty$, t.i., $r_2(X) = r_1(X)$.

Esam ieguvuši vienādības

$$\begin{aligned} (q_1(X) - q_2(X))g(X) &= 0_{R[X]}, \\ \deg(q_1 - q_2) + \deg g &= -\infty. \end{aligned}$$

Tā kā $\deg g \in \mathbb{N}$, tad atliek tikai, ka $\deg(q_1 - q_2) = -\infty$, t.i., $q_1(X) = q_2(X)$. ■

7.4.2. Definīcija. *Gadījumā, ja $r(X) = 0_{R[X]}$, tad saka, ka $g(X)$ dala $f(X)$ jeb $f(X)$ dalās ar $g(X)$ bez atlikuma. Šai gadījumā mēs lietojam pierakstu $g(X) \setminus f(X)$.*

7.4.3. Teorēma (Bezū). *Ja $a \in R$, tad katram polinomam $f(X) \in R[X]$ eksistē tāds polinoms $q(X) \in R[X]$, ka*

$$f(X) = (X - a)q(X) + f(a).$$

□ Saskaņā ar dalīšanas algoritmu

$$f(X) = (X - a)q(X) + r(X) \qquad \text{un} \qquad \deg r < \deg(X - 1) = 1.$$

Tādējādi eksistē $r \in R$, ka $r(X) = rX^0$.

Tagad, pielietojot substitūcijas teorēmu attēlojumam $X \mapsto a$, iegūstam

$$f(a) = (a - a)q(a) + r(a) = 0 + r = r.$$

No šejienes, ņemot vērā vienošanos $rX^0 = r$,

$$f(X) = (X - a)q(X) + f(a). \quad ■$$

7.4.4. Sekas. *Pieņemsim, ka $a \in R$ un $f(X) \in R[X]$.*

$$f(a) = 0 \Leftrightarrow (X - a) \diagdown f(X).$$

7.4.5. Definīcija. *Elementu $a \in R$ sauc par polinoma $f(X) \in R[X]$ sakni, ja $f(a) = 0$.*

7.4.6. Apgalvojums. *Ja R ir integritātes apgabals, tad katram nenulles polinomam $f(X) \in R[X]$ eksistē ne vairāk kā* $\deg f$ *saknes.*

$\square$ Pieņemsim, ka $\deg f = 0$, tad $f(X) = a \neq 0$. No šejienes

$$\forall b \in R \; f(b) = a \neq 0,$$

t.i., polinomam $f(X)$ nav sakņu, un tātad teorēma ir pareiza, jo

$$0 \leq 0 = \deg f.$$

Tālākais pierādījums induktīvs pēc $n \leftharpoondown \deg f$.

(i) Ja polinomam $f(X)$ nav sakņu, tad automātiski teorēma ir spēkā.

(ii) Pieņemsim, ka $a \in R$ ir polinoma $f(X)$ sakne, tad (Sekas 7.4.4) eksistē tāds polinoms $q(X) \in R[X]$, ka $f(X) = (X - a)q(X)$. No šejienes (Sekas 7.3.5) $\deg q = n - 1$. Saskaņā ar indukcijas pieņēmumu polinomam $q(X)$ ir ne vairāk par $n - 1$ sakni.

Pieņemsim, ka b ir kāda polinoma $f(X)$ sakne, tad

$$0 = f(b) = (b - a)q(b).$$

Tā kā R ir integritātes apgabals, tad $b - a = 0$ vai $q(b) = 0$. Tas nozīmē, ka $b = a$ vai arī b ir polinoma $q(X)$ sakne. Tā rezultātā polinoma $f(X)$ sakņu skaits gredzenā R nepārsniedz skaitli

$$1 + (n - 1) = n.$$

Līdz ar to indukcijas pāreja veikta pilnībā. $\blacksquare$

Atzīmēsim, ka šis rezultāts var būt arī kļūdains, ja R nav integritātes apgabals.

7.4.7. Piemērs. Gredzenā $\mathbb{Z}_2 \times \mathbb{Z}_2$ polinomam $X^2 - X$ ir četras saknes.

7.4.8. Sekas. *Pieņemsim, ka $f(X)$ un $g(X)$ ir polinomi pār integritātes apgabalu R, kuru pakāpes nepārsniedz skaitli n. Ja $f(a) = g(a)$ vismaz $n+1$ dažadam $a \in R$, tad $f(X) = g(X)$.*

□ Polinoma $h(X) \coloneqq f(X) - g(X)$ pakāpe nepārsniedz skaitli n, tāpēc (Apgalvojums 7.4.6) tam nevar būt vairāk par n saknēm. Izņemums ir tikai polinoms $0_{R[X]}$. Ja reiz polinomam $h(X)$ ir vismaz $n+1$ dažāda sakne, tad $h(X) = 0_{R[X]}$. Līdz ar to $f(X) = g(X)$. ■

7.4.9. Vingrinājums. Ja R ir bezgalīgs integritātes apgabals, proti, $|R| \geq \aleph_0$, un

$$\mathrm{Pol(R)} \coloneqq \{f : R \to R \,|\, \exists n \in \mathbb{N}\; f(x) = \sum_{k=0}^{n} a_k x^k\},$$

tad R–algebras $R[X]$ un Pol(R) ir izomorfas.

7.5. Galveno ideālu apgabals

7.5.1. Definīcija. *Gredzena R ideālu I sauc par galveno ideālu, ja eksistē tāds $a \in R$, ka $I = Ra$.*

7.5.2. Apgalvojums. *Katrs veselo skaitļu gredzena $\mathbb{Z}$ ideāls ir galvenais ideāls.*

□ (i) Ja $I = \{0\}$, tad $I = \mathbb{Z}0$, un tāpēc tas ir galvenais ideāls.

(ii) Turpmākajā pierādījumā pieņemsim, ka gredzena $\mathbb{Z}$ ideāls I bez 0 satur vēl kādu citu skaitli $n \in I$. Tā kā I ir gredzena $\mathbb{Z}$ ideāls, tad I ir gredzena $\mathbb{Z}$ apakšgredzens. Līdz ar to $-n \in I$. Tas nozīmē, ka I satur kādu pozitīvu skaitli p.

(iii) Pieņemsim, ka

$$d \coloneqq \min_{p \in \mathbb{Z}_+} I,$$

t.i., d ir mazākais pozitīvais veselais skaitlis, kas pieder ideālam I.

(iv) Pieņemsim, ka $m \in I$, tad saskaņā ar Eiklīda algoritmu eksistē tādi veseli skaitļi q un r, ka

$$m = dq + r \qquad \text{un} \qquad 0 \leq r < d.$$

Tā kā $d \in I$, tad $dq \in I$. Līdz ar to

$$r = m - dq \in I.$$

Taču d ir mazākais pozitīvais veselais skaitlis, kas pieder ideālam I, tāpēc $r = 0$. Līdz ar to $m = dq \in \mathbb{Z}d$.

(v) Esam parādījuši, ka $I \subseteq \mathbb{Z}d$, bet tā kā I ir ideāls un $d \in I$, tad $\mathbb{Z}d \subseteq \mathbb{Z}I \subseteq I$. Līdz ar to $I = \mathbb{Z}d$, proti, tas ir galvenais ideāls. ■

7.5.3. Definīcija. *Integritātes apgabalu, kura katrs ideāls ir galvenais sauc par galveno ideālu apgabalu.*

7.5.4. Teorēma. *Ja L ir lauks, tad $L[X]$ ir galveno ideālu apgabals.*

□ (i) Ja $I = \{0\}$, tad $I = L[X]0$, un tāpēc tas ir galvenais ideāls.

(ii) Turpmākajā pierādījumā pieņemsim, ka gredzena $L[X]$ ideāls I bez 0 satur vēl kādu citu polinomu $g(X)$. Pieņemsim, ka $0 \neq f(X) \in I$ izvēlēts tā, lai

$$\forall h(X) \in I \quad (h(X) \neq 0 \Rightarrow \deg f \leq \deg h).$$

(iii) Pieņemsim, ka $0 \neq h(X) \in I$, tad (Teorēma 7.4.1) eksistē tāds polinomu $q(X) \in L[X]$ un $r(X) \in L[X]$ pāris, ka

$$h(X) = f(X)q(X) + r(X) \qquad \text{un} \qquad \deg r < \deg f.$$

Tā kā $f(X) \in I$, tad $f(X)q(X) \in I$. Līdz ar to

$$r(X) = h(X) - f(X)q(X) \in I.$$

Taču ideālam I nepieder neviens nenulles polinoms, kura pakāpe ir mazāka par $\deg f$, tāpēc $r(X) = 0$. Līdz ar to $h(X) \in L[X]f(X)$.

(iv) Esam parādījuši, ka $I \subseteq L[X]f(X)$, bet tā kā I ir ideāls un $f(X) \in I$, tad $L[X]f(X) \subseteq L[X]I \subseteq I$. Līdz ar to $I = L[X]f(X)$, proti, tas ir galvenais ideāls. ■

8. nodaļa

GRUPU REPREZENTĀCIJAS

Grupas reprezentācija, triviāla reprezentācija, reprezentācijas kārta. Reprezentācijas modulis, ekvivalentas reprezentācijas. Piemēri, cikliskas grupas viendimensionāla reprezentācija, regulāra reprezentācija.

8.1. Automorfismu grupa

Šī paragrāfa ietvaros

- R — komutatīvs gredzens ar vienības elementu;
- M — brīvs R–modulis, kura bāzes apjoms ir m.

Atgādināsim

$$\mathrm{End}(M) \rightleftharpoons \{f : M \to M \mid f \text{ ir moduļa } M \text{ endomomorfisms}\}.$$

8.1.1. Apgalvojums.

$$\mathrm{Aut}(M) \rightleftharpoons \{f \in \mathrm{End}(M) \mid f \text{ ir moduļa } M \text{ automomorfisms}\}$$

ir grupa, kur grupas operācija $\overset{\frown}{\cdot}$ *ir attēlojumu kompozīcija.*

□ (i) Pieņemsim, ka $f \in \mathrm{Aut}(M)$, tad (Teorēma 1.4.5) inversais attēlojums f^{-1} ir kopas M substitūcija.

(ii) Pieņemsim, ka $x \in M$ un $y \in M$, tad eksistē tādi $x' \in M$ un $y' \in M$, ka $f(x') = x$ un $f(y') = y$. No šejienes

$$f^{-1}(x+y) = f^{-1}(f(x')+f(y')) = f^{-1}(f(x'+y')) = x'+y' = f^{-1}(x)+f^{-1}(y).$$

(iii) Pieņemsim, ka $a \in R$, tad

$$f^{-1}(ax) = f^{-1}(af(x')) = f^{-1}(f(ax')) = ax' = af^{-1}(x).$$

(iv) Esam parādījuši (punkti (ii) un (iii)), ka $f^{-1} \in \mathrm{End}(M)$, un tā kā f^{-1} ir kopas M substitūcija (punkts (i)), tad $f^{-1} \in \mathrm{Aut}(M)$.

(v) Atgādināsim (Apgalvojums 1.2.3), ka attēlojumu kompozīcija ir asociatīva. Triviāla pārbaude liecina, ka $\mathbb{I}_M \in \mathrm{Aut}(M)$. Tas kopā ar punktā (iv) konstatēto ļauj secināt, ka $\mathrm{Aut}(M)$ ir grupa. ■

Pieņemsim, ka $\mathcal{U} = \{u_1, u_2, \ldots, u_m\}$ ir moduļa M bāze. Ja $f \in \mathrm{End}(M)$ un

$$\forall k \in \overline{1,m} \quad f(u_k) = a_{1k}u_1 + a_{2k}u_2 + \ldots + a_{mk}u_m, \tag{8.1}$$

tad

$$\overset{\triangledown}{\|} f \| \rightleftharpoons \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ . & . & . & . \\ a_{m1} & a_{m2} & \ldots & a_{mm} \end{pmatrix}.$$

Attēlojums $\Psi : \mathrm{End}(M) \to \mathrm{Mat}_m(R) : f \mapsto \overset{\triangledown}{\|} f \|$ ir R–algebru izomorfisms (skatīt Teorēmas 6.6.12 pierādījumu).

8.1.2. Apgalvojums. *Endomomorfisms $f \in \mathrm{End}(M)$ ir automorfisms tad un tikai tad, ja matricai $\overset{\triangledown}{\|} f \|$ eksistē inversā matrica.*

□ ⇒ Pieņemsim, ka $f \in \mathrm{Aut}(M)$, tad (Apgalvojums 8.1.1) arī $f^{-1} \in \mathrm{Aut}(M)$. Līdz ar to $\mathbb{I}_M = f \overset{\frown}{\cdot} f^{-1}$ un tāpēc

$$E = \Psi(\mathbb{I}_M) = \Psi(f \overset{\frown}{\cdot} f^{-1}) = \Psi(f)\Psi(f^{-1}) = \overset{\triangledown}{\|} f \| \ \overset{\triangledown}{\|} f^{-1} \|.$$

No šejienes $\overset{\triangledown}{\|} f^{-1} \| = \overset{\triangledown}{\|} f \|^{-1}$.

⇐ Pieņemsim, ka $f \in \mathrm{End}(M)$ un matricai $\overset{\triangledown}{\|} f \|$ eksistē inversā matrica $\overset{\triangledown}{\|} f \|^{-1}$. Tā kā $\Psi : \mathrm{End}(M) \to \mathrm{Mat}_m(R)$ ir bijekcija, tad eksistē tāds homomorfisms $g \in \mathrm{End}(M)$, ka $\overset{\triangledown}{\|} g \| = \overset{\triangledown}{\|} f \|^{-1}$. No šejienes

$$\begin{aligned} \Psi(f \overset{\frown}{\cdot} g) &= \Psi(f)\Psi(g) = \overset{\triangledown}{\|} f \| \ \overset{\triangledown}{\|} g \| = \overset{\triangledown}{\|} f \| \ \overset{\triangledown}{\|} f \|^{-1} = E = \Psi(\mathbb{I}_M), \\ \Psi(g \overset{\frown}{\cdot} f) &= \Psi(g)\Psi(f) = \overset{\triangledown}{\|} g \| \ \overset{\triangledown}{\|} f \| = \overset{\triangledown}{\|} f \|^{-1} \ \overset{\triangledown}{\|} f \| = E = \Psi(\mathbb{I}_M). \end{aligned}$$

Tā kā $\Psi : \mathrm{End}(M) \to \mathrm{Mat}_m(R)$ ir bijekcija, tad

$$g \stackrel{\frown}{\cdot} f = \mathbb{I}_M \qquad \text{un} \qquad f \stackrel{\frown}{\cdot} g = \mathbb{I}_M.$$

Tas nozīmē (Apgalvojums 1.4.6), ka f ir bijekcija. Tātad f ir automorfisms. ■

8.1.3. Teorēma. *Grupas* $\mathrm{Aut}(M)$ *un*

$$GL_m(R) \rightleftharpoons \{\, A \in \mathrm{Mat}_m(R) \mid \text{ matricai } A \text{ eksistē inversā matrica} \,\}$$

ir izomorfas.

□ (i) Ievērojam (skatīt Teorēmas 6.6.12 pierādījumu), ka

$$\Psi : \mathrm{End}(M) \to \mathrm{Mat}_m(R) : f \mapsto \overset{\triangledown}{\|} f \,\|$$

ir pusgrupu $\langle\, \mathrm{End}(M), \stackrel{\frown}{\cdot} \,\rangle$ un $\langle\, \mathrm{Mat}_m(R), \cdot \,\rangle$ monomorfisms. Pieņemsim, ka $\Psi_a \rightleftharpoons \Psi|\mathrm{Aut}(M)$, tad

$$\Psi_a : \mathrm{Aut}(M) \to \mathrm{Mat}_m(R) : f \mapsto \overset{\triangledown}{\|} f \,\|$$

arī ir pusgrupu monomorfisms. Tā kā $\mathrm{Aut}(M)$ ir grupa, tad (Teorēma 3.5.4) $\mathrm{Im}\Psi_a$ ir grupa. Atliek parādīt, ka $\mathrm{Im}\Psi_a = GL_m(R)$.

(ii) Ja $f \in \mathrm{Aut}(M)$, tad $\overset{\triangledown}{\|} f \,\| \in GL_m(R)$ (Apgalvojums 8.1.2). Tātad $\mathrm{Im}\Psi_a \subseteq GL_m(R)$.

(iii) Pieņemsim, ka $A \in GL_m(R)$, tad $A \in \mathrm{Mat}_m(R)$. Tā kā

$$\Psi : \mathrm{End}(M) \to \mathrm{Mat}_m(R)$$

ir bijekcija, tad eksistē tāds $f \in \mathrm{End}(M)$, ka $\overset{\triangledown}{\|} f \,\| = A$.

Saskaņā ar pieņēmumu matricai A eksistē inversā matrica, tāpēc arī matricai $\overset{\triangledown}{\|} f \,\|$ eksistē inversā matrica. Apgalvojums 8.1.2 šai gadījumā konstatē, ka $f \in \mathrm{Aut}(M)$. Tātad $A = \overset{\triangledown}{\|} f \,\| \in \mathrm{Im}\Psi_a$. Līdz ar to $GL_m(R) \subseteq \mathrm{Im}\Psi_a$.

(iv) Mēs parādījām, ka $\mathrm{Im}\Psi_a \subseteq GL_m(R) \subseteq \mathrm{Im}\Psi_a$. No šejienes $\mathrm{Im}\Psi_a = GL_m(R)$. ■

8.2. Grupas reprezentācija

Vienošanās. Turpmāk šis nodaļas ietvaros, ja nekas speciāli netiks atrunāts, tad

- a, b, c mēs rezervējam lauka L elementu apzīmēšanai;
- x, y, z mēs rezervējam vektoru telpas V pār lauku L elementu apzīmēšanai;
- σ, τ, η mēs rezervējam grupas G elementu apzīmēšanai;
- f, g, h mēs rezervējam grupu algebras $L(G)$ elementu apzīmēšanai.

8.2.1. Definīcija. *Pieņemsim, ka V ir vektoru telpa pār lauku L un* $\mathrm{Aut}(V)$ *— šīs vektoru telpas automorfismu grupa. Katru homomorfismu*

$$\Phi : G \to \mathrm{Aut}(V)$$

sauc par grupas G reprezentāciju.

Vektoru telpu V šai gadījumā sauc par *reprezentācijas Φ telpu.* Reprezentāciju Φ sauc par *triviālu*, ja

$$\forall \sigma \quad \Phi(\sigma) = \mathbb{I}_V.$$

Reprezentāciju Φ sauc par *precīzu*, ja Φ ir monomorfisms.

Reprezentāciju Φ sauc par *reprezentāciju pār lauku L*, ja V ir vektoru telpa pār lauku L. Vektoru telpas dimensiju sauc par *reprezentācijas Φ dimensiju* jeb *kārtu.* Tātad $\dim\Phi \leftharpoondown\!\!\!\!\rightharpoonup \dim V$. Ja $\dim\Phi = n$, tad saka, ka Φ ir *n–dimensionāla reprezentācija.*

Atzīmēsim, ka ${}_L L$ (lasītājam, kas jūtas apmulsis, iesakam aplūkot Piemēru 5.1.5(i)) ir vektoru telpa pār lauku L. Dotajā situācijā $\dim_L L = 1$.

8.2.2. Lemma. *Ja $\Phi : G \to \mathrm{Aut}(V)$ ir viendimensionāla reprezentācija, tad*

$$\forall \sigma\, \forall \tau \quad \Phi(\sigma\tau) = \Phi(\tau\sigma).$$

□ Tā kā dim$\Phi = 1$, tad dim$V = 1$. Saskaņā ar Teorēmu 8.1.3

$$\mathrm{Aut}(V) \cong GL_1(L) = L^* \leftrightharpoons L \setminus \{0_L\}.$$

Te L^* ir lauka L multiplikatīvā grupa (skatīt Sekas 4.3.5).

Pieņemsim, ka $\Psi_a : \mathrm{Aut}(V) \to L^*$ ir grupu izomorfisms, tad

$$\begin{aligned}\Psi_a\big(\Phi(\sigma\tau)\big) &= \Psi_a\big(\Phi(\sigma)\Phi(\tau)\big) = \Psi_a\big(\Phi(\sigma)\big)\,\Psi_a\big(\Phi(\tau)\big) = \Psi_a\big(\Phi(\tau)\big)\,\Psi_a\big(\Phi(\sigma)\big) \\ &= \Psi_a(\Phi(\tau)\Phi(\sigma)) = \Psi_a\big(\Phi(\tau\sigma)\big).\end{aligned}$$

Tā kā $\Psi_a : \mathrm{Aut}(V) \to L^*$ ir bijekcija, tad no šejienes izriet, ka $\Phi(\sigma\tau) = \Phi(\tau\sigma)$. ■

8.2.3. Apgalvojums. *Ja $\Phi : G \to \mathrm{Aut}(V)$ ir viendimensionāla reprezentācija un grupas G elementi σ, τ ir saistīti, tad $\Phi(\sigma) = \Phi(\tau)$.*

□ Saskaņā ar doto σ un τ ir saistīti elementi, tāpēc (Definīcija 3.14.1) eksistē tāds η, ka $\sigma = \eta\tau\eta^{-1}$. No šejienes

$$\Phi(\sigma) = \Phi(\eta\tau\eta^{-1}) = \Phi(\eta\tau)\Phi(\eta^{-1}) \overset{\mathrm{L8.2.2}}{=} \Phi(\tau\eta)\Phi(\eta^{-1}) = \Phi(\tau\eta\eta^{-1}) = \Phi(\tau). \ ■$$

Ja Φ ir n–dimensionāla reprezentācija pār lauku L, tad (Teorēma 8.1.3) Aut$V \cong GL_n(L)$. Šī iemesla dēļ lietojumos reprezentāciju Φ parasti uzdod ar matricas $GL_n(L)$ elementiem, nevis automorfismiem. Tas viss saistīts ar ērtībām. Parasti aprēķinus veikt ar matricām ir vieglāk nekā ar automorfismiem, it īpaši, ja lauka L lomā ir reālo skaitļu $\mathbb{R}$ vai komplekso skaitļu $\mathbb{C}$ lauks. Taču nepieredzējušam lasītājam var rasties problēma:

— Kur te ir automorfismi?

Saprotams matricas nav automorfismi. Lai atrastu pašus automorfismus, jāveic papildus aprēķini. Tam visam izmantojama formula (8.1), taču tad ir jānofiksē vektoru telpas V bāze.

Atzīmēsim, ja lauks L un vektoru telpas V dimensija ir nofiksēta, tad $V \cong L^n$. Šis rezultāts var būtiski atvieglot aprēķinus, ja ir vēlme atrast pašus automorfismus.

8.2.4. Piemērs. Pieņemsim, ka C_2 ir otrās kārtas cikliska grupa. Mūsu mērķis: atrast visas šīs grupas viendimensionālās reprezentācijas pār reālo skaitļu lauku $\mathbb{R}$.

Ņemot vērā iepriekš teikto, mums jāatrod homomorfismi $\Gamma : C_2 \to \mathbb{R}^*$.

Grupa C_2 sastāv no 2 elementiem, teiksim e, kas ir grupas C_2 neitrālais elements, un vēl kāda elementa σ. Tā kā C_2 ir cikliska otrās kārtas grupa, tad $\sigma^2 = e$.

Pieņemsim, ka Γ ir homomorfisms, kas atbilst grupas C_2 viendimensionālai reprezentācijai pār reālo skaitļu lauku, tad $\Gamma(e) = 1$. Pieņemsim, ka $\Gamma(\sigma) = c \in \mathbb{R}^*$, tad

$$1 = \Gamma(e) = \Gamma(\sigma^2) = \Gamma(\sigma\sigma) = \Gamma(\sigma)\Gamma(\sigma) = cc = c^2.$$

Reālo skaitļu laukā vienādojumam $c^2 = 1$ ir divas saknes: 1 un -1. Esam ieguvuši divus homomorfismus:

C_2	e	σ
Γ_1	1	1
Γ_2	1	-1

Tā kā reālo skaitļu laukā vienādojumam $c^2 = 1$ ir tieši divas saknes, tad citu homomorfismu nav.

Parasti literatūrā ar šādu rezultātu arī apmierinās, taču, stingri runājot, šie homomorfismi Γ_i nav grupas C_2 reprezentācijas. Homomorfismam Γ_1 atbilst reprezentācija

C_2	e	σ
Φ_1	$\mathbb{I}_V$	$\mathbb{I}_V$

kur V ir patvaļīga viendimensionāla vektoru telpa pār reālo skaitļu lauku $\mathbb{R}$. Savukārt homomorfismam Γ_2 atbilst reprezentācija

C_2	e	σ
Φ_2	$\mathbb{I}_V$	$-\mathbb{I}_V$

Viegli pārliecināties, ka $-\mathbb{I}_V \in \mathrm{Aut}V$ un

$$(\Phi_2(\sigma))^2 = (-\mathbb{I}_V)^2 = (-\mathbb{I}_V) \overset{\frown}{\cdot} (-\mathbb{I}_V) = \mathbb{I}_V = \Phi_2(e) = \Phi_2(\sigma^2).$$

Atzīmēsim, ka Φ_1 mūsu gadījumā ir triviāla grupas C_2 reprezentācija, savukārt Φ_2 ir precīza grupas C_2 reprezentācija.

8.3. Reprezentācijas modulis

Pieņemsim, ka $\Phi : G \to \mathrm{Aut}(V)$ ir grupas G reprezentācija pār lauku L. Mūsu mērķis: pārvērst V par moduli pār grupas G algebru $L(G)$. Vispirms katram $\sigma \in G$ definējam attēlojumu $\lfloor\sigma\rfloor \breve{\circ} x \mapsto \Phi(\sigma)(x)$.

8.3.1. Lemma. (i) $\big(\lfloor\sigma\rfloor\lfloor\tau\rfloor\big)\breve{\circ} x = \lfloor\sigma\rfloor\breve{\circ}\big(\lfloor\tau\rfloor\breve{\circ} x\big)$*;*

(ii) $\lfloor\sigma\rfloor\breve{\circ}(x+y) = \lfloor\sigma\rfloor\breve{\circ} x + \lfloor\sigma\rfloor\breve{\circ} y$*.*

$$\begin{aligned} \square \quad \text{(i)} \quad \big(\lfloor\sigma\rfloor\lfloor\tau\rfloor\big)\breve{\circ} x &\overset{\text{V6.7.5}}{=} \lfloor\sigma\tau\rfloor\breve{\circ} x = \Phi(\sigma\tau)(x) = \Phi(\sigma)\big(\Phi(\tau)(x)\big) \\ &= \lfloor\sigma\rfloor\breve{\circ}\big(\lfloor\tau\rfloor\breve{\circ} x\big); \\ \text{(ii)} \quad \lfloor\sigma\rfloor\breve{\circ}(x+y) &= \Phi(\sigma)(x+y) = \Phi(\sigma)(x) + \Phi(\sigma)(y) \\ &= \lfloor\sigma\rfloor\breve{\circ} x + \lfloor\sigma\rfloor\breve{\circ} y. \quad \blacksquare \end{aligned}$$

8.3.2. Lemma. $\lfloor\sigma\rfloor\breve{\circ}(ax) = a\big(\lfloor\sigma\rfloor\breve{\circ} x\big)$.

$$\square \quad \lfloor\sigma\rfloor\breve{\circ}(ax) = \Phi(\sigma)(ax) = a\Phi(\sigma)(x) = a\big(\lfloor\sigma\rfloor\breve{\circ} x\big). \quad \blacksquare$$

Mēs jau zinam (Apgalvojums 6.7.6), ka katru $f \in L(G)$ var reprezentēt kā summu $f = \sum\limits_{\sigma\in G}\lfloor a_\sigma\sigma\rfloor$. Tagad definējam attēlojumu

$$L(G)\times V \xrightarrow{\breve{\circ}} V : f\breve{\circ} x \leftharpoondown \sum_{\sigma\in G}\lfloor\sigma\rfloor\breve{\circ}(a_\sigma x). \tag{8.2}$$

8.3.3. Lemma. *Attēlojums, kas definēts ar formulu* (8.2) *ir gredzena* $L(G)$ *multiplikatīvā monoīda iedarbība uz kopu* V *no kreisās puses.*

$\square$ Pieņemsim, ka $g = \sum\limits_{\tau\in G}\lfloor b_\tau\tau\rfloor$, tad

$$\begin{aligned} fg\breve{\circ} x &\overset{\text{S7.1.7}}{=} \Big(\sum_{\sigma\in G}\sum_{\tau\in G}\lfloor(a_\sigma b_\tau)\sigma\tau\rfloor\Big)\breve{\circ} x \overset{8.2}{=} \sum_{\sigma\in G}\sum_{\tau\in G}\lfloor\sigma\tau\rfloor\breve{\circ} a_\sigma b_\tau x; \\ f\breve{\circ}(g\breve{\circ} x) &\overset{8.2}{=} \sum_{\sigma\in G}\lfloor\sigma\rfloor\breve{\circ} a_\sigma(g\breve{\circ} x) \overset{8.2}{=} \sum_{\sigma\in G}\lfloor\sigma\rfloor\breve{\circ}(a_\sigma\sum_{\tau\in G}\lfloor\tau\rfloor\breve{\circ} b_\tau x) \\ &= \sum_{\sigma\in G}\lfloor\sigma\rfloor\breve{\circ}\sum_{\tau\in G}a_\sigma(\lfloor\tau\rfloor\breve{\circ} b_\tau x) \overset{\text{L8.3.2}}{=} \sum_{\sigma\in G}\lfloor\sigma\rfloor\breve{\circ}\sum_{\tau\in G}\lfloor\tau\rfloor\breve{\circ} a_\sigma b_\tau x \\ &\overset{\text{L8.3.1(ii)}}{=} \sum_{\sigma\in G}\sum_{\tau\in G}\lfloor\sigma\rfloor\breve{\circ}\lfloor\tau\rfloor\breve{\circ} a_\sigma b_\tau x \overset{\text{L8.3.1(i)}}{=} \sum_{\sigma\in G}\sum_{\tau\in G}\lfloor\sigma\tau\rfloor\breve{\circ} a_\sigma b_\tau x. \end{aligned}$$

Tātad $fg\breve{\circ}x = f\breve{\circ}(g\breve{\circ}x)$. Visbeidzot, pieņemsim, ka $e \in G$ ir grupas G neitrālais elements, tad

$$1_{L(G)}\breve{\circ}x \overset{\text{P6.7.3}}{=} \lfloor e \rfloor \circ x = \Phi(e)(x) = \mathbb{I}_V(x) = x. \quad \blacksquare$$

8.3.4. Apgalvojums. *Ja gredzena $L(G)$ multiplikatīvā monoīda iedarbība uz kopu V no kreisās puses definēta saskaņā ar formulu* (8.2)*, tad V ir kreisais $L(G)$–modulis.*

$\square$ Vispirms konstatēsim, kas mums īsti ir jāpierāda.

- Pieņemsim, ka $\langle L, V, +, \cdot, \breve{+}, \breve{\cdot} \rangle$ — vektoru telpa pār lauku L,
- $\langle L, L(G), +, \cdot, \oplus, \circ, \odot \rangle$ — grupas G algebra pār lauku L,
- $\Phi : G \to \mathrm{Aut}V$ — grupas G reprezentācija.

Mums jāparāda, ka $\langle L(G), V, \oplus, \odot, \breve{+}, \breve{\circ} \rangle$ ir kreisais $L(G)$–modulis.
Saskaņā ar doto

- $\langle L(G), \oplus, \odot \rangle$ ir gredzens,
- $\langle V, \breve{+} \rangle$ ir komutatīva grupa.

Mēs jau esam pierādījuši (Lemma 8.3.3), ka attēlojums $L(G) \times V \xrightarrow{\breve{\circ}} V$ ir gredzena $L(G)$ multiplikatīvā monoīda iedarbība uz kopu V no kreisās puses.

Ja tagad pievēršamies Definīcijai 5.1.2, tad vienīgais, ko vēl jāpierāda, ir abi distributīvie likumi. Tad daram to!

Vienosimies, ka pieraksts $\sum^{\oplus}$ norāda uz summēšanu gredzenā $L(G)$, bet $\sum^{\breve{+}}$ norāda uz summēšanu grupā $\langle V, \breve{+} \rangle$. Pieņemsim, ka $f = \sum\limits_{\sigma \in G}^{\oplus} \lfloor a_\sigma \sigma \rfloor$ un $g = \sum\limits_{\sigma \in G}^{\oplus} \lfloor b_\sigma \sigma \rfloor$, tad

$$\begin{aligned} f\breve{\circ}(x\breve{+}y) &= \Big(\sum_{\sigma \in G}^{\oplus} \lfloor a_\sigma \sigma \rfloor\Big)\breve{\circ}(x\breve{+}y) \overset{8.2}{=} \sum_{\sigma \in G}^{\breve{+}} \lfloor \sigma \rfloor \breve{\circ}(a_\sigma \breve{\cdot} (x\breve{+}y)) \\ &= \sum_{\sigma \in G}^{\breve{+}} \lfloor \sigma \rfloor \breve{\circ}(a_\sigma \breve{\cdot} x \breve{+} a_\sigma \breve{\cdot} y) \end{aligned}$$

$$
\begin{aligned}
&\overset{\text{L8.3.1(ii)}}{=} \sum_{\sigma\in G}^{\check{+}} \big(\lfloor\sigma\rfloor\breve{\circ}(a_\sigma \check{\cdot} x)\check{+}\lfloor\sigma\rfloor\breve{\circ}(a_\sigma \check{\cdot} y)\big)\\
&= \sum_{\sigma\in G}^{\check{+}} \lfloor\sigma\rfloor\breve{\circ}(a_\sigma \check{\cdot} x)\check{+}\sum_{\sigma\in G}^{\check{+}} \lfloor\sigma\rfloor\breve{\circ}(a_\sigma \check{\cdot} y)\\
&= \Big(\sum_{\sigma\in G}^{\oplus}\lfloor a_\sigma\sigma\rfloor\Big)\breve{\circ}x\check{+}\Big(\sum_{\sigma\in G}^{\oplus}\lfloor a_\sigma\sigma\rfloor\Big)\breve{\circ}y \overset{8.2}{=} f\breve{\circ}x\check{+}f\breve{\circ}y;
\end{aligned}
$$

$$
\begin{aligned}
(f\oplus g)\breve{\circ}x &= \Big(\sum_{\sigma\in G}^{\oplus}\lfloor a_\sigma\sigma\rfloor \oplus \sum_{\sigma\in G}^{\oplus}\lfloor b_\sigma\sigma\rfloor\Big)\breve{\circ}x\\
&= \Big(\sum_{\sigma\in G}^{\oplus}\lfloor (a_\sigma + b_\sigma)\sigma\rfloor\Big)\breve{\circ}x\\
&\overset{8.2}{=} \sum_{\sigma\in G}^{\check{+}} \lfloor\sigma\rfloor\breve{\circ}((a_\sigma + b_\sigma)\check{\cdot} x) = \sum_{\sigma\in G}^{\check{+}} \lfloor\sigma\rfloor\breve{\circ}(a_\sigma \check{\cdot} x\check{+}b_\sigma\check{\cdot} x)\\
&\overset{\text{L8.3.1(ii)}}{=} \sum_{\sigma\in G}^{\check{+}} \big(\lfloor\sigma\rfloor\breve{\circ}(a_\sigma \check{\cdot} x)\check{+}\lfloor\sigma\rfloor\breve{\circ}(b_\sigma \check{\cdot} x)\big)\\
&= \sum_{\sigma\in G}^{\check{+}} \lfloor\sigma\rfloor\breve{\circ}(a_\sigma \check{\cdot} x)\check{+}\sum_{\sigma\in G}^{\check{+}} \lfloor\sigma\rfloor\breve{\circ}(b_\sigma \check{\cdot} x)\\
&= \Big(\sum_{\sigma\in G}^{\oplus}\lfloor a_\sigma\sigma\rfloor\Big)\breve{\circ}x\check{+}\Big(\sum_{\sigma\in G}^{\oplus}\lfloor b_\sigma\sigma\rfloor\Big)\breve{\circ}x\\
&\overset{8.2}{=} f\breve{\circ}x\check{+}g\breve{\circ}x. \quad \blacksquare
\end{aligned}
$$

8.3.5. Definīcija. *Pieņemsim, ka*

- $\langle L, L(G), +, \cdot, \oplus, \circ, \odot\rangle$ — *grupas G algebra pār lauku L,*
- $\Phi : G \to \mathrm{Aut}V$ — *grupas G reprezentācija,*
- $\langle L, V, +, \cdot, \check{+}, \check{\cdot}\rangle$ — *reprezentācijas Φ telpa.*

Moduli $\langle L(G), V, \oplus, \odot, \check{+}, \breve{\circ}\rangle$, kur iedarbība $\breve{\circ}$ definēta saskaņā ar formulu (8.2)*, sauc par reprezentācijas Φ moduli.*

Pieņemsim, ka

- $\langle L, L(G), +, \cdot, \oplus, \circ, \odot\rangle$ ir grupas G algebra pār lauku L un

- $\langle L(G), M, \oplus, \odot, \breve{+}, \breve{\circ}\rangle$ ir $L(G)$–modulis.

Tagad parādīsim, kā, izmantojot šo informāciju, definējama grupas G reprezentācija pār lauku L.

8.3.6. Lemma. *Attēlojums*

$$L \times M \xrightarrow{\breve{\cdot}} M : a \breve{\cdot} x \quad \leftharpoondown \quad (a \circ 1_{L(G)}) \breve{\circ} x \tag{8.3}$$

ir lauka L multiplikatīvā monoīda iedarbība uz kopu M no kreisās puses.

□ Ievērojam (Teorēma 6.1.3), ka $\iota : L \to L(G) : a \mapsto a \circ 1_{L(G)}$ ir gredzenu monomorfisms, tāpēc

$$(ab) \circ 1_{L(G)} = (a \circ 1_{L(G)}) \odot (b \circ 1_{L(G)}).$$

No šejienes

$$\begin{aligned}(ab) \breve{\cdot} x &= ((ab) \circ 1_{L(G)}) \breve{\circ} x = ((a \circ 1_{L(G)}) \odot (b \circ 1_{L(G)})) \breve{\circ} x \\ &= (a \circ 1_{L(G)}) \breve{\circ} ((b \circ 1_{L(G)}) \breve{\circ} x) = a \breve{\cdot} (b \breve{\cdot} x).\end{aligned}$$

Savukārt

$$1 \breve{\cdot} x = (1 \circ 1_{L(G)}) \breve{\circ} x = 1_{L(G)} \breve{\circ} x = x. \quad \blacksquare$$

8.3.7. Apgalvojums. $\langle L, M, +, \cdot, \breve{+}, \breve{\cdot}\rangle$ *ir vektoru telpa.*

□ Saskaņā ar doto

- $\langle L, +, \cdot\, \rangle$ ir lauks,
- $\langle M, \breve{+}\, \rangle$ ir komutatīva grupa.

Mēs jau parādījām (Lemma 8.3.6), ka $\langle L, M, \cdot, \breve{\cdot}\rangle$ ir L iedarbība uz kopu M.

Atliek pierādīt distributīvos likumus. Pieņemsim, ka x un y ir kopas M elementi, tad

$$\begin{aligned}a \breve{\cdot} (x \breve{+} y) &= (a \circ 1_{L(G)}) \breve{\circ} (x \breve{+} y) = (a \circ 1_{L(G)}) \breve{\circ} x \breve{+} (a \circ 1_{L(G)}) \breve{\circ} y \\ &= a \breve{\cdot} x \breve{+} b \breve{\cdot} y, \\ (a+b) \breve{\cdot} x &= ((a+b) \circ 1_{L(G)}) \breve{\circ} x = (a \circ 1_{L(G)} \oplus b \circ 1_{L(G)}) \breve{\circ} x \\ &= (a \circ 1_{L(G)}) \breve{\circ} x \breve{+} (b \circ 1_{L(G)}) \breve{\circ} x = a \breve{\cdot} x \breve{+} b \breve{\cdot} x. \quad \blacksquare\end{aligned}$$

8.3.8. Apgalvojums. *Attēlojums* $\Psi(\sigma)(x) \leftharpoondown\!\!= \lfloor\sigma\rfloor\breve{\circ}x$ *ir grupas* G *reprezentācija. Reprezentācijas telpa šai gadījumā ir* $\langle L, M, +, \cdot, \breve{+}, \breve{\cdot}\rangle$.

$\square$ (i) Vispirms parādīsim, ka $\Psi(\sigma) \in \mathrm{End}(M)$.

$$\begin{aligned}
\Psi(\sigma)(x\breve{+}y) &= \lfloor\sigma\rfloor\breve{\circ}(x\breve{+}y) = \lfloor\sigma\rfloor\breve{\circ}x\breve{+}\lfloor\sigma\rfloor\breve{\circ}y = \Psi(\sigma)(x)\breve{+}\Psi(\sigma)(y),\\
\Psi(\sigma)(a\breve{\cdot}x) &= \lfloor\sigma\rfloor\breve{\circ}(a\breve{\cdot}x) = \lfloor\sigma\rfloor\breve{\circ}((a\circ 1_{L(G)})\breve{\circ}x) = (\lfloor\sigma\rfloor \odot (a\circ 1_{L(G)}))\breve{\circ}x\\
&= (a\circ(\lfloor\sigma\rfloor \odot 1_{L(G)}))\breve{\circ}x = (a\circ(1_{L(G)} \odot \lfloor\sigma\rfloor)\breve{\circ}x\\
&= ((a\circ 1_{L(G)}) \odot \lfloor\sigma\rfloor)\breve{\circ}x = (a\circ 1_{L(G)})\breve{\circ}(\lfloor\sigma\rfloor\breve{\circ}x)\\
&= a\breve{\cdot}\Psi(\sigma)(x).
\end{aligned}$$

(ii) Tagad parādīsim, ka

$$\Psi : G \to \mathrm{End}(M)$$

ir pusgrupu homomorfisms.

$$\Psi(\sigma\tau)(x) = \lfloor\sigma\tau\rfloor\breve{\circ}x = (\lfloor\sigma\rfloor \odot \lfloor\tau\rfloor)\breve{\circ}x = \lfloor\sigma\rfloor\breve{\circ}(\lfloor\tau\rfloor\breve{\circ}x) = \Psi(\sigma)\big(\Psi(\tau)(x)\big).$$

Tātad $\Psi(\sigma\tau) = \Psi(\sigma)\Psi(\tau)$.

(iii) Visbeidzot konstatēsim, ka $\Psi(\sigma)$ ir kopas M substitūcija. Pieņemsim, ka e ir grupas G neitrālais elements. Mēs jau zinam (Piemērs 6.7.3), ka $\lfloor e\rfloor = 1_{L(G)}$. No šejienes

$$\begin{aligned}
\Psi(e)(x) &= \lfloor e\rfloor\breve{\circ}x = 1_{L(G)}\breve{\circ}x = x = \mathbb{I}_M(x);\\
\mathbb{I}_M &= \Psi(e) = \Psi(\sigma\sigma^{-1}) = \Psi(\sigma)\Psi(\sigma^{-1}),\\
\mathbb{I}_M &= \Psi(e) = \Psi(\sigma^{-1}\sigma) = \Psi(\sigma^{-1})\Psi(\sigma).
\end{aligned}$$

Tas ļauj secināt (Apgalvojums 1.4.6), ka $\Psi(\sigma)$ ir bijekcija. Tātad $\Psi(\sigma) \in \mathrm{Aut}(M)$. $\blacksquare$

8.3.9. Sekas. *Reprezentācijas* Ψ *modulis ir* $\langle L(G), M, \oplus, \odot, \breve{+}, \breve{\circ}\rangle$.

$\square$ Pieņemsim, ka $\langle L(G), M, \oplus, \odot, \breve{+}, \acute{\circ}\rangle$ ir reprezentācijas Ψ modulis. Saskaņā ar reprezentācijas moduļa aprakstu iedarbība $L(G)\times M \xrightarrow{\acute{\circ}} M$ tiek definēta ar vienādību (8.2). Mūsu gadījumā tas izskatās šādi. Vispirms katram $\sigma \in G$ definējam attēlojumu

$$\lfloor\sigma\rfloor\acute{\circ}x \leftharpoondown\!\!= \Psi(\sigma)(x) \overset{\text{A8.3.8}}{=} \lfloor\sigma\rfloor\breve{\circ}x,$$

tad katram $f = \sum\limits_{\sigma\in G}^{\oplus} \lfloor a_\sigma \sigma \rfloor$ definējam

$$
\begin{aligned}
f \acute{\circ} x &\leftharpoondown \sum_{\sigma\in G}^{\breve{+}} \lfloor \sigma \rfloor \acute{\circ} (a_\sigma \breve{\cdot} x) = \sum_{\sigma\in G}^{\breve{+}} \lfloor \sigma \rfloor \breve{\circ} ((a_\sigma \circ 1_{L(G)}) \breve{\circ} x) \\
&= \sum_{\sigma\in G}^{\breve{+}} \big(\lfloor \sigma \rfloor \odot (a_\sigma \circ 1_{L(G)}) \big) \breve{\circ} x = \sum_{\sigma\in G}^{\breve{+}} \lfloor a_\sigma \sigma \rfloor \breve{\circ} x \\
&= \Big(\sum_{\sigma\in G}^{\oplus} \lfloor a_\sigma \sigma \rfloor \Big) \breve{\circ} x = f \breve{\circ} x.
\end{aligned}
$$

Tā rezultātā $\langle L(G), M, \oplus, \odot, \breve{+}, \acute{\circ} \rangle = \langle L(G), M, \oplus, \odot, \breve{+}, \breve{\circ} \rangle$. ■

Grupas G reprezentāciju Ψ sauksim par $L(G)$–modulim M *atbilstošo reprezentāciju.*

8.3.10. Sekas. *Reprezentācijas* $\Phi : G \to \mathrm{Aut}(V)$ *modulim* V *atbilstošā reprezentācija* Ψ *sakrīt ar* Φ.

□ Saskaņā ar reprezentācijas moduļa aprakstu (Definīcija 8.3.5) iedarbība $L(G) \times V \xrightarrow{\breve{\circ}} V$ tiek definēta izmantojot vienādību

$$\lfloor \sigma \rfloor \breve{\circ} x \leftharpoondown \Phi(\sigma)(x).$$

Tā rezultātā, ja $\langle L, L(G), +, \cdot, \oplus, \circ, \odot \rangle$ ir grupas G algebra pār lauku L un $\langle L, V, +, \cdot, \breve{+}, \breve{\cdot} \rangle$ ir reprezentācijas Φ telpa, iegūst reprezentācijas moduli $\langle L(G), V, \oplus, \odot, \breve{+}, \breve{\circ} \rangle$, kur

$$\lfloor a\sigma \rfloor \breve{\circ} x \leftharpoondown \lfloor \sigma \rfloor \breve{\circ} (a \breve{\cdot} x).$$

Savukārt $L(G)$–modulim V atbilstošo reprezentāciju Ψ definē šādi. Pieņemsim, ka e ir grupas G neitrālais elements, tad vispirms definē vektoru telpu $\langle L, V, +, \cdot, \breve{+}, \acute{\cdot} \rangle$, kur

$$
\begin{aligned}
a \acute{\cdot} x &\leftharpoondown (a \circ 1_{L(G)}) \breve{\circ} x = \lfloor ae \rfloor \breve{\circ} x = \lfloor e \rfloor \breve{\circ} (a \breve{\cdot} x) \\
&= \Phi(e)(a \breve{\cdot} x) = \mathbb{I}_V (a \breve{\cdot} x) = a \breve{\cdot} x.
\end{aligned}
$$

Līdz ar to $\langle L, V, +, \cdot, \breve{+}, \acute{\cdot} \rangle = \langle L, V, +, \cdot, \breve{+}, \breve{\cdot} \rangle$. Pašu reprezentāciju Ψ tagad definē ar vienādību

$$\Psi(\sigma)(x) \leftharpoondown \lfloor \sigma \rfloor \breve{\circ} x = \Phi(\sigma)(x).$$

Tas nozīmē, ka $\Psi = \Phi$. ■

Šie rezultāti pamato nostāju, kāpēc literatūrā par grupas G reprezentāciju sauc jebkuru $L(G)$–moduli M. Tā rezultātā mūsdienās grupu reprezentāciju teorijā nozīmīga loma atvēlēta $L(G)$–moduļu izpētei.

8.4. Ekvivalentas reprezentācijas

8.4.1. Definīcija. *Reprezentācijas*

$$\Phi : G \to \mathrm{Aut}(V), \qquad \Psi : G \to \mathrm{Aut}(W)$$

pār lauku L sauc par ekvivalentām reprezentācijām, ja eksistē tāds vektoru telpu izomorfisms

$$\varphi : V \to W,$$

ka

$$\forall \sigma \quad \Phi(\sigma) = \varphi \Psi(\sigma) \varphi^{-1}.$$

Brīdinājums. Definīcijā te mēs atļāvāmies pierakstu $x\Phi(\sigma) \leftharpoonup \Phi(\sigma)(x)$.

Atzīmēsim, ka reprezentācijas Φ un Ψ ir ekvivalentas tad un tikai tad, ja katram grupas G elementam σ diagramma

$$\begin{tikzcd} V \arrow[r, "\Phi(\sigma)"] \arrow[d, "\varphi"'] & V \arrow[d, "\varphi"] \\ W \arrow[r, "\Psi(\sigma)"'] & W \end{tikzcd} \tag{D3}$$

ir komutatīva. Tiešām, tā kā φ ir bijekcija, tad vienādība

$$\Phi(\sigma) = \varphi \Psi(\sigma) \varphi^{-1}$$

ir ekvivalenta vienādībai

$$\Phi(\sigma)\varphi = \varphi \Psi(\sigma).$$

Šī paragrāfa ietvaros pieņemsim, ka

- $\langle L, L(G), +, \cdot, \oplus, \circ, \odot \rangle$ — grupas G algebra pār lauku L;
- $\Phi : G \to \mathrm{Aut}(V)$ — grupas G reprezentācija,
- $\langle L, V, +, \cdot, \breve{+}, \breve{\cdot} \rangle$ — reprezentācijas Φ telpa,

- $\langle L(G), V, \oplus, \odot, \breve{+}, \breve{\circ}\rangle$ — reprezentācijas Φ modulis;
- $\Psi : G \to \mathrm{Aut}(W)$ — grupas G reprezentācija,
- $\langle L, W, +, \cdot, \acute{+}, \acute{\cdot}\rangle$ — reprezentācijas Ψ telpa,
- $\langle L(G), W, \oplus, \odot, \acute{+}, \acute{\circ}\rangle$ — reprezentācijas Ψ modulis.

8.4.2. Teorēma. *Reprezentācijas*

$$\Phi : G \to \mathrm{Aut}(V), \qquad \Psi : G \to \mathrm{Aut}(W)$$

ir ekvivalentas tad un tikai tad, ja atbilstošie reprezentācijas moduļi ir izomorfi.

$\square$ $\Rightarrow$ Pieņemsim, ka $f = \sum\limits_{\sigma\in G} \lfloor a_\sigma \sigma \rfloor$, tad

$$\begin{aligned}
(f \breve{\circ} x)\varphi &= \Big(\big(\sum_{\sigma\in G} \lfloor a_\sigma \sigma\rfloor\big)\breve{\circ} x\Big)\varphi = \Big(\sum_{\sigma\in G}\lfloor\sigma\rfloor \breve{\circ}(a_\sigma \check{\cdot} x)\Big)\varphi \\
&= \big(\sum_{\sigma\in G}(a_\sigma \check{\cdot} x)\Phi(\sigma)\big)\varphi = \big(\sum_{\sigma\in G} a_\sigma \check{\cdot}(x\Phi(\sigma)\big)\varphi \\
&= \sum_{\sigma\in G} a_\sigma \acute{\cdot}(x\Phi(\sigma)\varphi) = \sum_{\sigma\in G} a_\sigma \acute{\cdot}(x\varphi\Psi(\sigma)\varphi^{-1}\varphi) \\
&= \sum_{\sigma\in G} a_\sigma \acute{\cdot}(x\varphi\Psi(\sigma)) = \sum_{\sigma\in G}(a_\sigma \acute{\cdot}(x\varphi))\Psi(\sigma) \\
&= \sum_{\sigma\in G}\lfloor\sigma\rfloor \acute{\circ}(a_\sigma \acute{\cdot}(x\varphi)) = \big(\sum_{\sigma\in G}\lfloor a_\sigma\sigma\rfloor\big)\acute{\circ}(x\varphi) \\
&= f\acute{\circ}(x\varphi).
\end{aligned}$$

Tā kā $\varphi : V \to W$ ir vektoru telpu izomorfisms, tad φ ir bijekcija un

$$(x \breve{+} y)\varphi = x\varphi \acute{+} y\varphi.$$

Tā rezultātā reprezentācijas moduļi V un W ir izomorfi $L(G)$–moduļi.

$\Leftarrow$ Pieņemsim, ka $\varphi : V \to W$ ir reprezentācijas moduļu V un W izomorfisms. Ņemot vērā iepriekšējā paragrāfā izklāstīto (Sekas 8.3.10), saskaņā ar formulu (8.3)

$$\begin{aligned}
\forall x \in V \quad & a \check{\cdot} x = (a \circ 1_{L(G)})\breve{\circ} x, \\
\forall w \in W \quad & a \acute{\cdot} w = (a \circ 1_{L(G)})\acute{\circ} w.
\end{aligned}$$

No šejienes

$$(a \breve{\cdot} x)\varphi = ((a \circ 1_{L(G)})\breve{\circ} x)\varphi = ((a \circ 1_{L(G)})\acute{\circ}(x\varphi)) = a \acute{\cdot} (x\varphi).$$

Tā kā $\varphi : V \to W$ ir $L(G)$–moduļu izomorfisms, tad φ ir bijekcija un

$$(x \breve{+} y)\varphi = x\varphi \acute{+} y\varphi.$$

Tā rezultātā vektoru telpas V un W ir izomorfas. Turklāt

$$\begin{aligned} x\varphi\Psi(\sigma) &= (x\varphi)\Psi(\sigma) = \lfloor\sigma\rfloor \acute{\circ} x\varphi = (\lfloor\sigma\rfloor \breve{\circ} x)\varphi \\ &= (x\Phi(\sigma))\varphi = x\Phi(\sigma)\varphi. \end{aligned}$$

Tas nozīmē, ka $\forall\sigma\ \Phi(\sigma)\varphi = \varphi\Psi(\sigma)$, proti, diagramma (D3) ir komutatīva visiem $\sigma \in G$. Tātad reprezentācijas

$$\Phi : G \to \mathrm{Aut}(V), \qquad \Psi : G \to \mathrm{Aut}(W)$$

ir ekvivalentas. ■

8.5. Ciklisku grupu reprezentācijas

8.5.1. Piemērs. Pieņemsim, ka C_3 ir trešās kārtas cikliska grupa. Mūsu mērķis: atrast visas šīs grupas viendimensionālās reprezentācijas pār reālo skaitļu lauku $\mathbb{R}$.

Ņemot vērā otrajā paragrāfā izklāstīto, mums jāatrod homomorfismi

$$\Gamma : C_3 \to \mathbb{R}^*.$$

Grupa C_3 sastāv no 3 elementiem, teiksim e, kas ir grupas C_3 neitrālais elements, un vēl kāda elementa σ. Tā kā C_3 ir cikliska trešās kārtas grupa, tad

$$C_3 = \{e, \sigma, \sigma^2\},$$

turklāt $\sigma^3 = e$.

Pieņemsim, ka Γ ir homomorfisms, kas atbilst grupas C_3 viendimensionālai reprezentācijai pār reālo skaitļu lauku, tad $\Gamma(e) = 1$. Pieņemsim, ka $\Gamma(\sigma) = c \in \mathbb{R}^*$, tad

$$1 = \Gamma(e) = \Gamma(\sigma^3) = \Gamma(\sigma\sigma\sigma) = \Gamma(\sigma)\Gamma(\sigma)\Gamma(\sigma) = ccc = c^3.$$

Reālo skaitļu laukā vienādojumam $c^3 = 1$ ir tikai viena sakne: 1. Esam ieguvuši tikai vienu homomorfismu:

C_3	e	σ	σ^2
Γ	1	1	1

Tā kā reālo skaitļu laukā vienādojumam $c^3 = 1$ ir tieši viena sakne, tad citu homomorfismu nav.

Homomorfismam Γ atbilst triviālā reprezentācija

C_3	e	σ	σ^2
Φ	$\mathbb{I}_V$	$\mathbb{I}_V$	$\mathbb{I}_V$

kur V ir patvaļīga viendimensionāla vektoru telpa pār reālo skaitļu lauku $\mathbb{R}$, un citu cikliskās grupas C_3 reprezentāciju pār reālo skaitļu lauku $\mathbb{R}$ nav.

Aina krasi izmainās, ja lauka $\mathbb{R}$ vietā aplūkojam lauku $\mathbb{C}$. Komplekso skaitļu laukā vienādojumam $c^3 = 1$ ir trīs saknes: 1 un

$$\begin{aligned} e^{\frac{2\pi i}{3}} &= \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}\, i\,, \\ e^{\frac{4\pi i}{3}} &= \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} = -\frac{1}{2} - \frac{\sqrt{3}}{2}\, i\,. \end{aligned}$$

Tagad esam ieguvuši trīs homomorfismus:

C_3	e	σ	σ^2
Γ_1	1	1	1
Γ_2	1	$-\frac{1}{2} + \frac{\sqrt{3}}{2}\, i$	$-\frac{1}{2} - \frac{\sqrt{3}}{2}\, i$
Γ_3	1	$-\frac{1}{2} - \frac{\sqrt{3}}{2}\, i$	$-\frac{1}{2} + \frac{\sqrt{3}}{2}\, i$

Atzīmēsim, ka homomorfismam Γ_1 mūsu gadījumā atbilst triviāla grupas C_3 reprezentācija, savukārt homomorfismiem Γ_2 un Γ_3 atbilst precīzas grupas C_3 reprezentācijas.

Visumā jau lietojumos pētnieki nemīl operēt ar citiem laukiem, taču šai gadījumā arī fiziķi ir samierinājušies ar nepieciešamību izmantot komplekso skaitļu lauku.

8.5.2. Piemērs. Pieņemsim, ka C_n ir n–tās kārtas cikliska grupa. Mūsu mērķis: atrast visas šīs grupas viendimensionālās reprezentācijas pār komplekso skaitļu lauku $\mathbb{C}$.

Mēs sekosim iepriekšējā piemērā izklāstītajai shēmai. Pieņemsim, ka $\sigma \in C_n$ ir šīs grupas veidotājelements (Definīcija 3.8.4), tad

$$C_n = \{e, \sigma, \sigma^2, \ldots, \sigma^{n-1}\},$$

turklāt $\sigma^n = e$. Pieņemsim, ka Γ ir homomorfisms, kas atbilst grupas C_n viendimensionālai reprezentācijai pār komplekso skaitļu lauku, tad $\Gamma(e) = 1$. Pieņemsim, ka $\Gamma(\sigma) = c \in \mathbb{C}^*$, tad

$$1 = \Gamma(e) = \Gamma(\sigma^n) = \big(\Gamma(\sigma)\big)^n = c^n.$$

Komplekso skaitļu laukā vienādojumam $c^n = 1$ ir n dažādas saknes:

$$\zeta_k \leftharpoondown e^{\frac{2\pi k i}{n}}, \qquad k \in \overline{0, n-1}.$$

Esam ieguvuši n homomorfismus $\Gamma_k : C_n \to \mathbb{C}^*$:

C_n	e	σ	σ^2	$\ldots$	σ^{n-1}
Γ_0	1	1	1	$\ldots$	1
Γ_1	1	ζ_1	ζ_1^2	$\ldots$	ζ_1^{n-1}
Γ_2	1	ζ_2	ζ_2^2	$\ldots$	ζ_2^{n-1}
.	.	.	.	.	.
Γ_{n-1}	1	ζ_{n-1}	ζ_{n-1}^2	$\ldots$	ζ_{n-1}^{n-1}

8.6. Regulāras reprezentācijas

Pieņemsim, ka $\langle L, L(G), +, \cdot, \oplus, \circ, \odot\rangle$ — grupas G algebra pār lauku L. Ja algebru $L(G)$ mēs uztveram tikai kā gredzenu, tad ${}_{L(G)}L(G)$ ir $L(G)$–modulis. Šim modulim $\langle L(G), L(G), \oplus, \odot, \oplus, \odot\rangle$ atbilst (Apgalvojums 8.3.7) vektoru telpa

$$\langle L, L(G), +, \cdot, \oplus, \breve{\because}\rangle,$$

kur saskaņā ar formulu (8.3)

$$a \,\breve{\because}\, f \leftharpoondown (a \circ 1_{L(G)}) \odot f = a \circ f.$$

Tātad

$$\langle L, L(G), +, \cdot, \oplus, \breve{\because} \rangle = \langle L, L(G), +, \cdot, \oplus, \circ \rangle \rightleftharpoons \mathcal{R}_L(G).$$

Modulim $\mathcal{R}_L(G)$ atbilstošā reprezentācija Ψ definējama ar vienādību (Apgalvojums 8.3.8)

$$\Psi(\sigma)(f) \leftharpoondown \lfloor \sigma \rfloor \odot f. \tag{8.4}$$

8.6.1. Apgalvojums. *Ja G ir n–tās kārtas grupa, tad Ψ ir n–dimensionāla reprezentācija.*

$\square$ Saskaņā ar Definīciju 8.2.1 mums jāparāda, ka vektoru telpas $\mathcal{R}_L(G)$ dimensija $\dim \mathcal{R}_L(G) = n$.

Pieņemsim, ka $f \in L(G)$, tad f ir izsakāms izskatā

$$f = \sum_{\sigma \in G} \lfloor a_\sigma \sigma \rfloor = \sum_{\sigma \in G} a_\sigma \circ \lfloor \sigma \rfloor.$$

Līdz ar to $\dim \mathcal{R}_L(G) \leq |G| = n$.

Pieņemsim, ka $G = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ un

$$0_{L(G)} = a_1 \circ \lfloor \sigma_1 \rfloor \oplus a_2 \circ \lfloor \sigma_2 \rfloor \oplus \ldots \oplus a_n \circ \lfloor \sigma_n \rfloor = \sum_{i=1}^{n} \lfloor a_i \sigma_i \rfloor.$$

Tā kā

$$0_{L(G)} = \sum_{i=1}^{n} \lfloor 0 \sigma_i \rfloor$$

un katram $f \in L(G)$ eksistē (Apgalvojums 6.7.6) viena vienīga reprezentācija izskatā $f = \sum_{i=1}^{n} \lfloor b_i \sigma_i \rfloor$, tad visi $a_i = 0$. Līdz ar to vektori

$$\lfloor \sigma_1 \rfloor, \lfloor \sigma_2 \rfloor, \ldots, \lfloor \sigma_n \rfloor$$

ir lineāri neatkarīgi. Tas nozīmē, ka $\dim \mathcal{R}_L(G) \geq n$. $\blacksquare$

8.6.2. Definīcija. *Grupas G reprezentāciju Ψ, kas definēta saskaņā ar formulu* (8.4)*, sauc par regulāro reprezentāciju.*

8.6.3. Piemērs. Cikliskās grupas C_4 regulārā reprezentācija pār reālo skaitļu lauku $\mathbb{R}$. Pieņemsim, ka $C_4 = \{e, \sigma, \sigma^2, \sigma^3\}$, kur e ir grupas C_4 neitrālais elements un $\sigma^4 = e$, tad vektoru telpas

$$\langle \mathbb{R}, \mathbb{R}(G), +, \cdot, \oplus, \circ \rangle$$

bāze ir

$$\{\lfloor e \rfloor, \lfloor \sigma \rfloor, \lfloor \sigma^2 \rfloor, \lfloor \sigma^3 \rfloor\}$$

un saskaņā ar formulu (8.4) grupas C_4 regulārā reprezentācija Ψ definējama ar vienādību

$$\Psi(\tau)(f) \leftharpoondown \lfloor \tau \rfloor \odot f.$$

No šejienes

$$\begin{aligned} \Psi(\sigma)(\lfloor e \rfloor) &= \lfloor \sigma \rfloor, \qquad & \Psi(\sigma)(\lfloor \sigma \rfloor) &= \lfloor \sigma^2 \rfloor, \\ \Psi(\sigma)(\lfloor \sigma^2 \rfloor) &= \lfloor \sigma^3 \rfloor, \qquad & \Psi(\sigma)(\lfloor \sigma^3 \rfloor) &= \lfloor \sigma^4 \rfloor = \lfloor e \rfloor. \end{aligned}$$

Tagad pievēršoties formulai (8.1) iegūstam

$$\overset{\triangledown}{||}\ \Psi(\sigma)\ || \leftharpoondown \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Pārejās matricas aprēķināmas no $\overset{\triangledown}{||}\ \Psi(\sigma)\ ||$:

$$\overset{\triangledown}{||}\ \Psi(\sigma^2)\ || = \overset{\triangledown}{||}\ \Psi(\sigma)\Psi(\sigma)\ || = \overset{\triangledown}{||}\ \Psi(\sigma)\ ||\ \ \overset{\triangledown}{||}\ \Psi(\sigma)\ || = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix};$$

$$\overset{\triangledown}{||}\ \Psi(\sigma^3)\ || = \overset{\triangledown}{||}\ \Psi(\sigma^2)\Psi(\sigma)\ || = \overset{\triangledown}{||}\ \Psi(\sigma^2)\ ||\ \ \overset{\triangledown}{||}\ \Psi(\sigma)\ || = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix};$$

$$\overset{\triangledown}{||}\ \Psi(e)\ || \leftharpoondown \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

8.6.4. Apgalvojums. *Viendimensionālas triviālas reprezentācijas $L(G)$–modulim V eksistē izomorfs moduļa ${}_{L(G)}L(G)$ apakšmodulis tad un tikai tad, ja grupa G ir galīga.*

$\Box$ Vispirms noskaidrosim, kā izskatās triviālās reprezentācijas modulis. Pieņemsim, ka $\langle L, V, +, \cdot, \breve{+}, \breve{\cdot} \rangle$ ir reprezentācijas Φ telpa, tad triviālā reprezentācija Φ ir vektoru telpas V identiskais attēlojums $\mathbb{I}_V$, proti,

$$\forall \sigma \in G \quad \Phi(\sigma) = \mathbb{I}_V.$$

Tā rezultātā

$$\lfloor \sigma \rfloor \breve{\circ} x \leftharpoondown \Phi(\sigma)(x) = \mathbb{I}_V(x) = x.$$

Ja $f = \sum\limits_{\sigma \in G} \lfloor a_\sigma \sigma \rfloor$, tad

$$f \breve{\circ} x \leftharpoondown \sum_{\sigma \in G} \lfloor \sigma \rfloor \breve{\circ} (a_\sigma \breve{\cdot} x) = \sum_{\sigma \in G} a_\sigma \breve{\cdot} x.$$

Līdz ar to, ja $\langle L, L(G), +, \cdot, \oplus, \circ, \odot \rangle$ ir grupas G algebra, tad triviālās reprezentācijas Φ modulis ir

$$\langle L(G), V, \oplus, \odot, \breve{+}, \breve{\circ} \rangle.$$

Tā kā $\langle L, V, +, \cdot, \breve{+}, \breve{\cdot} \rangle$ ir viendimensionāla vektoru telpa, tad

$$\exists v \in V \quad \mathcal{L}(v) = V.$$

Tā rezultātā

$$\forall x \in V \; \exists a \in L \quad x = a \breve{\cdot} v.$$

$\Leftarrow$ Pieņemsim, ka G ir galīga grupa un

$$\psi : V \to_{L(G)} L(G) : a \breve{\cdot} v \mapsto a \circ \sum_{\sigma \in G} \lfloor \sigma \rfloor.$$

Parādīsim, ka ψ ir $L(G)$–moduļu monomorfisms. Pieņemsim, ka $y \in V$, tad eksistē tāds $b \in L$, ka $y = b \breve{\cdot} v$. No šejienes

$$\begin{aligned}
\psi(x \breve{+} y) &= \psi(a \breve{\cdot} v \breve{+} b \breve{\cdot} v) = \psi((a+b) \breve{\cdot} v) = (a+b) \circ \sum_{\sigma \in G} \lfloor \sigma \rfloor \\
&= a \circ \sum_{\sigma \in G} \lfloor \sigma \rfloor \oplus b \circ \sum_{\sigma \in G} \lfloor \sigma \rfloor = \psi(x) \oplus \psi(y). \\
\psi(f \breve{\circ} x) &= \psi(\sum_{\sigma \in G} a_\sigma \breve{\cdot} x) = \sum_{\sigma \in G} \psi(a_\sigma \breve{\cdot} x) = \sum_{\sigma \in G} \psi(a_\sigma \breve{\cdot} a \breve{\cdot} v) \\
&= \sum_{\sigma \in G} \psi((a_\sigma a) \breve{\cdot} v) = \sum_{\sigma \in G} (a_\sigma a) \circ \sum_{\tau \in G} \lfloor \tau \rfloor;
\end{aligned}$$

$$\begin{aligned} f \odot \psi(x) &= \Big(\sum_{\sigma\in G}\lfloor a_\sigma \sigma\rfloor\Big) \odot \sum_{\tau\in G}\lfloor a\tau\rfloor = \sum_{\sigma\in G}\sum_{\tau\in G}\lfloor (a_\sigma a)\sigma\tau\rfloor \\ &= \sum_{\sigma\in G}(a_\sigma a) \circ \sum_{\tau\in G}\lfloor \tau\rfloor. \end{aligned}$$

Tātad

$$\psi(x \breve{+} y) = \psi(x) \oplus \psi(y) \qquad \text{un} \qquad \psi(f \breve{\circ} x) = f \odot \psi(x),$$

t.i., $\psi : V \to_{L(G)} L(G)$ ir $L(G)$–moduļu homomorfisms.

Pieņemsim, ka $x \neq y$, tad $a \neq b$. No šejienes

$$\psi(x) = \sum_{\sigma\in G}\lfloor a\sigma\rfloor \overset{\text{A6.7.6}}{\neq} \sum_{\sigma\in G}\lfloor b\sigma\rfloor = \psi(y).$$

Tātad ψ ir injekcija. Līdz ar to $L(G)$–modulis V ir izomorfs $L(G)$–modulim $\mathcal{L}\big(\sum\limits_{\sigma\in G}\lfloor\sigma\rfloor\big)$.

$\Rightarrow$ Pieņemsim, ka

$$\varphi : V \to_{L(G)} L(G)$$

ir $L(G)$–moduļu homomorfisms un $\varphi(x) = \sum\limits_{\tau\in G}\lfloor b_\tau \tau\rfloor$, tad

$$\varphi(\lfloor\sigma\rfloor \breve{\circ} x) = \lfloor\sigma\rfloor \odot \varphi(x) = \lfloor\sigma\rfloor \odot \sum_{\tau\in G}\lfloor b_\tau\tau\rfloor = \sum_{\tau\in G}\lfloor b_\tau(\sigma\tau)\rfloor.$$

No otras puses $\lfloor\sigma\rfloor \breve{\circ} x = x$, tāpēc $\varphi(\lfloor\sigma\rfloor \breve{\circ} x) = \varphi(x)$, t.i.,

$$\sum_{\tau\in G}\lfloor b_\tau(\sigma\tau)\rfloor = \sum_{\tau\in G}\lfloor b_\tau\tau\rfloor = \sum_{\tau\in G}\lfloor b_{\sigma\tau}(\sigma\tau)\rfloor.$$

Tas nozīmē, ka

$$\forall\tau \in G\ \forall\sigma\in G \quad b_\tau = b_{\sigma\tau}.$$

Speciālā gadījumā

$$\forall\sigma\in G \quad b_e = b_\sigma, \tag{8.5}$$

kur e ir grupas G neitrālais elements. No šejienes

$$\varphi(x) = \sum_{\tau\in G}\lfloor b_\tau\tau\rfloor = \sum_{\sigma\in G}\lfloor b_\sigma\sigma\rfloor \overset{(8.5)}{=} \sum_{\sigma\in G}\lfloor b_e\sigma\rfloor = b_e \circ \sum_{\sigma\in G}\lfloor\sigma\rfloor.$$

Ja G ir bezgalīga grupa, tad $\sum\limits_{\sigma\in G}\lfloor\sigma\rfloor \notin L(G)$, tāpēc $b_e = 0$. Līdz ar to

$$\forall x \in V \quad \varphi(x) = 0_{L(G)}.$$

Tā kā $\langle L, V, +, \cdot, \breve{+}, \breve{\cdot}\rangle$ ir viendimensionāla vektoru telpa, tad $v \neq 0_V$. Tas demonstrē, ka $\varphi : V \to_{L(G)} L(G)$ nav monomorfisms. ■

Bibliogrāfija

[1] William A. Adkins, Steven H. Weintraub. (1999) *Algebra.* Springer–Verlag, — 526 p.

[2] Robert B. Ash. (2006) *Basic Abstract Algebra: For Graduate Students and Advance Undergraduates.* Dover Publications.

[3] Steve Roman. (2005) *Field Theory.* Springer–Verlag, — 272 p.

[4] Л. А. Скорняков. (1986) *Элементы алгебры*. Москва «Наука», — 240 с.