# Uvod v univerzalno algebro in Mal'cev pogoj
## Povzetek diplomske naloge

Andraž Kukovičič
Mentorica: izr. prof. dr. Ganna Kudryavtseva

Študijsko leto 2024/25

## 1 Uvod

V diplomski nalogi in njenem povzetku bom predstavil osnovne pojme univerzalne algebre skupaj s primeri, ki smo jih v dosedanjem študijumatematike že srečali. Postopno bom predstavil pojme in rezultate, ki bodo vodili do srža diplomske naloge: formulaciji in dokazu Mal'cevega izreka in terma, ki se imenuje po njem. Eden od ciljev univerzalne algebre je iskanje in uporaba skupnih lastnosti na prvi pogled popolnoma različnih algebrskih struktur. To nam da nov, splošnejši in poenoten pogled na že znane strukture, hkrati pa lahko posamezne primere na ta način predstavimo bolj ekonomično, z manj pisanja. Spomnimo se naprimer primera dokazovanja izreka o izomorfizmu, ki smo ga v pri Algebri II prvič dokazali za grupe, nato smo ga formulirali še za druge strukture npr. kolobarje, algebre, module. Pri tem smo običajno rekli, da dokaz poteka enako le da ustrezno spremenimo oznake. Z uporabo univerzalne algebre bomo lahko tak dokaz za več različnih struktur naredili popolnoma formalno. Pred definicijo in poglobitvijo v glavno temo naloge si bomo ogledali še nekaj osnovnih rezultatov o mrežah, ki bodo kasneje uporabljeni v nekaterih izrekih in dokazih.

## 2 Mreže

**Definicija 1.** *Neprazna množica $M$ z dvema binarnima operacijama, ki ju označimo $z \vee$ in $\wedge$ je* mreža*, če za vsaka dva elementa iz $M$ veljajo naslednjim pogojem:*

*M1* $x \vee y = y \vee x$ *in* $x \wedge y = y \wedge x$ *(komutativnost)*

*M2* $x \vee (y \vee z) = (x \vee y) \vee z$ *in* $\wedge (y \wedge z) = (x \wedge y) \wedge z$ *(asociativnost)*

*M3* $x \vee x = x$ *in* $x \wedge x = x$ *(idempotentnost)*

*M4* $x = x \vee (x \wedge y)$ *in* $x = x \wedge (x \vee y)$ *(absorbcijsko pravilo).*

Pokažimo sedaj, da je definicija mreže ekvivalentna naslednji trditvi.

**Trditev 1.** *Delno urejena množica* $M$ *je mreža natanko takrat, ko za vsaka* $x, y \in M$*, v* $M$ *obstajata* $\sup x, y$ *in* $inf x, y$*.*

*Dokaz.* Spomnimo se najprej kaj je delno urejena množica. To je množica $m$ z relacijo $\leq$, da za vse elemente $x, y, z \in M$ velja:

1. $x \leq x$ (refleksivnost)
2. Če je $x \leq y$ in $y \leq x$, sledi $x = y$. (antisimetričnost)
3. Če je $x \leq y$ in $y \leq z$, sledi $x \leq z$. (tranzitivnost)

Dokazali bomo implikaciji v obe smeri. Najprej predpostavimo, da je $M$ mreža po definiciji in dokažimo trditev. Definirajmo relacijo $\leq$: za $a, b \in M$ velja $a \leq b$ natanko takrat, ko je $a = a \wedge b$. Najprej bomo preverili, da tako definirana relacija podaja delno ureditev na $M$, nato pa še obstoj $supa, b$ in $inf a, b$. Za prvi del moramo preveriti refleksivnost, antisimetričnost in tranzitivnost.

(r) Ker je $a \wedge a = a$ sledi $a \leq a$.

(a) Če je $a \leq b$ in $b \leq a$ to pomeni, da je $a = a \wedge b$ in $b = b \wedge a$, torej je $a = b$.

(t) Če je $a \leq b$ in $b \leq c$ to pomeni, da je $a = a \wedge b$ in $b = b \wedge c$, torej je $a = a \wedge b = a \wedge (b \wedge c)$ zaradi asociativnosti je slednje enako $(a \wedge b) \wedge c = a \wedge c$. Dobili smo $a = a \wedge c$, od tod pa po definiciji relacije $\leq a \leq c$.

Pokazali smo, da je $M$ z relacijo $\leq$ delno urejena. Sedaj pokažimo še obsotoj supremov in infimov. Iz $a = a \wedge (a \vee b)$ in $b = b \wedge (a \vee b)$ sledi $a \leq a \vee b$ in $b \leq a \vee b$ torej je $a \vee b$ zgornja meja tako za $a$, kot za $b$. Pokažimo še, da je $a \vee b$ najmanjša zgornja meja Če je $a \leq u$ in $b \leq u$ z neki $u \in M$, je po definiciji $\leq a = a \wedge u$ in zato $a \vee u = (a \wedge u) \vee u = u$ in podobno $b \vee u = u$, torej je $(a \wedge u) \wedge (b \wedge u) = u \wedge u = u$. In zato $(a \vee b) \vee u = u$, od tu pa vstavimo $u$ v $(a \vee b) \wedge u = (a \vee b) \wedge ((a \vee b) \vee u) = a \vee b$ pri zadnji enakosti smo uporabili absorbcijsko pravilo. To nam da $a \vee b \leq u$. Torej je res $a \vee b = sup\{a, b\}$. Podobno pokažemo, da je $a \wedge b = inf\{a, b\}$.
Dokažimo še obratno implikacijo torej, da iz trditve sledi definicija. Predpostavimo, da drži naša trditev in definirajmo operaciji $\wedge$ in $\vee$ takole: $a \wedge b := inf\{a, b\}$ in $a \vee b := sup\{a, b\}$. Pokažimo, da tako definirana operacija $\vee$ zadošča pogojem M1 - M4.

M1 Res velja $sup\{a,b\} = sup\{b,a\}$.

M2 Imamo $a \vee (b \vee c)$ torej je $sup\{a, sup\{b,c\}\}$, kar je enako $sup\{sup\{a,b\}, c\}$ in zato $a \vee (b \vee c) = (a \vee b) \vee c$.

M3 Ker je $a = sup\{a,a\}$ je res $a \vee a = a$.

M4 $a = a \vee (a \wedge b)$ zapišemo kot $a = sup\{a, inf\{a,b\}\}$ kar je res, saj je $inf\{a,b\} \leq a$.

Podobno preverimo za operacijo $\wedge$. □

# 3 Algebra

Poglejmo si sedaj definicijo algebre. Najprej definirajmo tip ali jezik algebre.

Definicija: *tip* ali *jezik* algebre $A$ je množica funkcij oziroma operacij $f : A^n \to A$, označimo jo z $\mathcal{F}$. Število $n \in \mathbb{N}_0$ imeneujemo *rang* ali -arnost funkcije $f$.

Vaska $f \in \mathcal{F}$ ima prirejeno tako nenegativno število.

Sledi definicija algebre, ki bo zaobjela večino znanih algebrskih struktur, zato se na prvi pogled zdi zapletena in zelo formalna, vendar bomo kasneje skozi primere videli, da lahko algebrske strukture enostavno predstavimo kot primere algeber.

Definicija: *Algebra* $A$ tipa $\mathcal{F}$ je urejeni par $(A, \mathcal{F})$, kjer je $A$ neprazna množica, imenujemo jo tudi *univerzalna množica* algebre $A$, $\mathcal{F}$ pa tip algebre. Elemente $f \in \mathcal{F}$ imenujemo *fundamentalne operacije* algebre $A$.

Če je množica $\mathcal{F}$ končna, torej $\mathcal{F} = \{f_1, f_2, \ldots, f_k\}$ običajno algebro $A$ zapišemo kot $(A, f_1, \ldots, f_k)$. Fundamentalnim operacijam z rangom 1 pravimo unitarne, za rangom 2 pa binarne operacije.

Kot obljubljeno si sedaj definicijo oglejmo še na oprijemljivejši način z nekaj osnovnimi primeri, ki jih iz dosedanjega študija algebre že dobro poznamo.

**Primer 1.** *:*

1. *Grupa $G$ je algebra $(G, \cdot, ^{-1}, 1)$ v kateri veljajo naslednje identitete:*

   *G1* $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

   *G2* $x \cdot 1 = 1 \cdot x = x$

   *G3* $x \cdot x^{-1} = x^{-1} \cdot x = 1$.

   *Omenimo še, da je množenje: $\cdot$ binarna, invertiranje: $^{-1}$ unitarna operacija, enota 1 pa operacija z rangom 0.*

2. *Podobno so polgrupe algebre $(G, \cdot)$ in monoidi algebre $(M, \cdot, 1)$.*

3. *Tudi mreže, ki smo jih predstavili na začetku so algebre* $(M, \vee, \wedge)$ *v katerih veljajo identitete M1 - M4.*

4. *Kolobar je algebra* $(R, +, \cdot, -, 0, 1)$*, kjer sta* $+$ *in* $\cdot$ *binarni,* $-$ *unitarna in* $0$ *ter* $1$ *z rangom 0. V kolobarju pa veljajo naslednje identitete:*

   *R1* $(R, +, -, 0)$ *je Abelova grupa,*
   *R2* $(R, \cdot)$ *je polgrupa,*
   *R3* $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ *in* $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$
   *G2* $x \cdot 1 = 1 \cdot x = x$

Podobno lahko predstavimo še druge algebrske strukture npr. module in algebre nad kolobarjem. Za formulacijo Mal'cevega izreka potrebujemo pojem kongruenc, zato ga predstavimo.

**Definicija 2.** *Naj bo* $A$ *algebra tipa* $\mathcal{F}$ *in naj bo* $\theta$ *ekvivalenčna relacija na* $A$*. Tedaj je* $\theta$ kongruenca *na* $A$*, če zadošča naslednjemu pogoju: Za vsako* $n$*-arno operacijo* $f \in \mathcal{F}$ *in vse elemente* $a_i, b_i \in A$*, če velja* $a_i \theta b_i$ *za vse* $1 \leq i \leq n$*, potem velja* $f(a_1, \ldots, a_n)\, \theta\, f(b_i, \ldots, b_n)$*.*

Ponovno si na primeru oglejmo kaj naj definicija pove, videli bomo, da kongruence v nekaterih primerih že dobro poznamo.

**Primer 2.** *Pokazali bomo, da so kongruence na grupah v bijektivni korespodenci s podgrupami edinkami. Naj bo* $G$ *grupa in* $\theta$ *kongruenca na* $G$*. Označimo z* $[1]_\theta$ *ekvivalenčni razred enote v grupi* $G$ *glede na ekvivalenčno relacijo* $\theta$*. Pokažimo, da je* $[1]_\theta$ *edinka grupe* $G$*. Vzemimo poljubna elementa* $a, b \in [1]_\theta$*, torej zanju velja* $a\theta 1$ *in* $b\theta 1$*, produkt* $ab^{-1} = 11^{-1} = 1\theta 1$ *torej res leži v* $[1]_\theta$*. Zato je* $[1]_\theta$ *podgrupa. Vzemimo sedaj poljuben element* $g \in G$ *in si oglejmo produkt* $ghg^{-1}$ *za neki* $h \in [1]_\theta$*. Ker je* $h$ *ekvivalenten* $1$ *je* $ghg^{-1} = g1g^{-1} = 1 \in [1]_\theta$*. Torej je* $[1]_\theta$ *res edinka v* $G$*.*
*Obratno vzemimo* $H$ *podgrupo edinko grupe* $G$*. In definirajmo relacijo* $\theta$ *takole:* $a\theta b \Leftrightarrow ab^{-1} \in H$*. Pokažimo, da je tako definirana relacija kongruenca.*
$\theta$ *je res ekvivalnečna relacija:* $(r)$ $aa^{-1} = 1 \in H$*,* $(s)$ *če je* $ab^{-1} \in H$ *za vsaka* $a, b \in H$ *je tudi* $ba^{-1} \in H$ *in še* $(t)$ *če sta* $ab^{-1}$ *in* $bc^{-1}$ *iz* $H$ *je tudi* $ab^{-1}bc^{-1} = ac^{-1} \in H$*. Pokažimo še, da je* $\theta$ *kongruenca. Vzemimo* $a, a', b, b' \in H$ *take, da velja* $a\theta a'$ *in* $b\theta b'$*. Pokazati moramo, da velja* $ab\theta a'b'$*. Ker je* $H$ *pogrupa obstajata taka* $h_1, h_2 \in H$*, da je* $a' = ah_1$ *in* $b' = bh_2$*, ker je* $H$ *edinka obstaja tak* $h_3 \in H$*, da je* $h_1 b = bh_3$*. Oglejmo si sedaj produkt* $a'b' = ah_1bh_2 = abh_3h_2$*, torej je* $a'b'\theta ab$*. Torej je preslikava, ki kongruenci priredi podgrupo edinko* $\theta \mapsto [1]_\theta$ *bijekcija.*

Za formulacijo Mal'cevega izreka moramo definirati še nekaj pojmov.

**Definicija 3.** Identiteta *tipa* $\mathcal{F}$ *nad* $X$ *je izraz oblike* $p \approx q$*, kjer sta* $p, q \in T(X)$*.*

Pri tem je $T(X)$ množica vseh termov tipa $\mathcal{F}$ nad $X$, kjer je $X$ množica spremenljivk. Termi tipa $\mathcal{F}$ so izrazi, ki jih lahko sestavimo iz spremenljivk in operacij iz $\mathcal{F}$. Naprimer če za našo algebro vzamemo grupe so nekateri termi: $xy$, $x1$, $xyx^{-1}$, $x1xyxyy$. Na splošno če ima algebra tip $\mathcal{F} = \{\cdot, +\}$, kjer sta $\cdot$ in $+$ binarni operaciji, so termi naprimer: $x+y, (x+y)\cdot z, xyz, \ldots$

Pravimo da algebra $A$ tipa $\mathcal{F}$ zadošča $p(x_1, \ldots, x_n) \approx q(x_1, \ldots, x_n)$, če za vsako izbiro $a_1, \ldots, a_n \in A$ velja: $p(a_1, \ldots, a_n) \approx q(a_1, \ldots, a_n)$. To relacijo označimo takole: $A \models p \approx q$. Dodatno, pravimo da razred algeber $K$ zadošča $p \approx q$, če vsaka algebra iz $K$ zadošča $p \approx q$, kar označimo: $K \models p \approx q$.

Nadaljujmo z definicijama, ki bosta imeli pomembni vlogi pri našem izreku.

**Definicija 4.** *Algebra $A$ je* kongruenčno-permutabilna*, če vsak par kongruenc komutira: $\theta_1 \circ \theta_2 = \theta_2 \circ \theta_1$.*

**Definicija 5.** *Neprazen razred $K$ algeber tipa $\mathcal{F}$ imenujemo* raznoterost*, če je zaprt za podalgebre, slike homomorfizmov in direktne produkte.*

Sedaj smo pripravljeni, da brez dokaza navedemo ciljni izrek diplomske naloge.

**Izrek 1** (Mal'cev)**.** *Naj bo $V$ raznoterost tipa $\mathcal{F}$. Raznoterost $V$ je kongruenčno-permutabilna natanko takrat, ko obstaja term $p(x, y, z)$, da:*

$$V \models p(x, x, y) \approx y$$

*in*

$$V \models p(x, y, y) \approx x.$$

Za konec ponazorimo vsebino izreka za dvema preprostima primeroma.

**Primer 3.** *Grupe so kongruenčno-permutabilne, saj obstaja term $p(x, y, z) = xy^{-1}z$, ki zadošča navedenima identitetama: $p(x, x, y) = xx^{-1}y = y$ in $p(x, y, y) = xy^{-1}y = x$.*
*Tudi kolobarji so kongruenčno-permutabilne algebre, za $p$ vzamemo $p(x, y, z) = x - y + z$.*

# 4 Literatura