# АЛГЕБРА

## Елементи опште алгебре

Основни појмови и примери

Зоран Петровић

Прво предавање

На самом почетку овог курса пажњу ћемо посветити основним појмовима алгебре — појму алгебарске операције, алгебарске структуре, хомоморфизма и слично. Дефинишимо најпре појам алгебарске операције.

**Дефиниција 1** Нека је $A$ непразан скуп и $n$ природан број. Операција $f$ дужине $n$ на скупу $A$, или $n$-арна операција скупа $A$ је функција $f\colon A^n \to A$.

Уколико је $f$ $n$-арна операција, кажемо и да је $f$ операција дужине $n$. То можемо записати и овако $\#(f) = n$, где са $\#(f)$ означавамо дужину операције $f$.

Истакнимо одмах да ће нам посебно значајни бити случајеви када је $n = 0$, $n = 1$ и $n = 2$.

- У случају да је $n = 0$, имамо нуларну операцију $f\colon A^0 \to A$.
- У случају да је $n = 1$, говоримо о унарној операцији $f\colon A \to A$.
- Ако је $n = 2$, у питању је бинарна операција $f\colon A^2 \to A$.

Појаснимо најпре појам нуларне операције. Скуп $A^0$ је заправо једночлан (поновите мало знање из математичке логике). Стога се нуларна операција своди на избор једног елемента из скупа $A$ (елемент који је слика тог јединог елемента из $A^0$ је изабрани елемент). Из тог разлога, често се и не говори о нуларним операцијама, него о константама, тј. изабраним елементима датог скупа. Ми ћемо користити и један и други приступ, указујући на специфичности у појединим случајевима.

У случају бинарне операције, најчешће се не пише $f(a, b)$, него $(a\, f\, b)$. Уосталом, да ли збир два броја пишете као $+(a, b)$ или као $(a+b)$ (спољашње заграде морамо да пишемо због формирања сложенијих израза)? Бинарне операције обично ћемо означавати са $\cdot$, $*$, $\circ$ и слично управо због наведеног начина писања.

Наведимо неке примере.

1. Сабирање ($+$) и множење ($\cdot$) су примери бинарних операција у скуповима $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$.

2. Пресек ($\cap$), односно унија ($\cup$) су примери бинарних операција на партитивном скупу $\mathcal{P}(X)$ неког непразног скупа $X$.

3. На скупу позитивних целих бројева, тј. на скупу $\mathbb{N} \setminus \{0\}$, дефинишемо операције NZD (највећи заједнички делилац) и NZS (највећи заједнички садржалац). Ово нам је (добро) познато из школске математике. Овде имамо редак случај да бинарну операцију не пишемо у инфиксном запису, тј. писаћемо $\mathrm{NZD}(m, n)$, а не $m \,\mathrm{NZD}\, n$.

4. (**посебно важан пример**) Нека је $n \geq 2$ природан број. Посматрајмо скуп $Z_n = \{0, 1, \ldots, n-1\}$. На овом скупу можемо дефинисати две веома важне бинарне операције — сабирање по модулу $n$, у ознаци $+_n$ и множење по модулу $n$, у ознаци $\cdot_n$ на следећи начин. Означимо са $\rho(m, n)$, где је $m$ цео број, а $n \geq 2$ природан број, остатак при дељењу $m$ са $n$ (подсетимо се да се остатак при дељењу $m$ са $n$ дефинише као јединствени природан број $r$ за који важи $m = qn + r, 0 \leq r < n$ за неки цео број $q$). Тада, за $a, b \in Z_n$:

$$a +_n b := \rho(a + b, n);$$

$$a \cdot_n b := \rho(a \cdot b, n).$$

5. Налажење супротног елемента у $Z$ ($-$) је пример једне унарне операције: $m \mapsto -m$.

6. Налажење супротног елемента у $Z_n$ ($-_n$) је пример једне унарне операције:
$$-_n m = \begin{cases} 0 & m = 0 \\ n - m & m \neq 0 \end{cases}$$

7. Комплемент подскупа ( $^c$) је пример једне унарне операције у скупу $\mathcal{P}(X)$: $A \mapsto A^c$.

8. На скупу позитивних целих бројева $\mathbb{N} \setminus \{0\}$ можемо дефинисати и две $n$-арне операције (где је $n \geq 2$):

$$(m_1, \ldots, m_n) \mapsto \mathrm{NZD}(m_1, \ldots, m_n) \quad (m_1, \ldots, m_n) \mapsto \mathrm{NZS}(m_1, \ldots, m_n).$$

Дефинишимо сада и појам алгебарске структуре.

**Дефиниција 2** Алгебарска структура је уређена $(n+1)$-торка

$$\mathbb{A} = (A, f_1, \ldots, f_n),$$

где је $A$ непразан скуп, који се назива и носач структуре $\mathbb{A}$, а $f_1, \ldots, f_n$ су операције на скупу $A$ при чему је $\#(f_i) \geq \#(f_{i+1})$ за све $i = \overline{1, n-1}$.

Приметимо да неке од ових операција могу бити и дужине 0, тј. као део алгебарске структуре могу се појавити и константе. Уобичајено је да се операције пишу у опадајућем поретку својих дужина (зато је то и стављено у оквиру дефиниције). На пример, уколико у структури имамо само бинарне, унарне и нуларне операције, то најпре пишемо бинарне операције, потом унарне и на крају константе. У вези са овим је и појам сигнатуре дате структуре $\mathbb{A}$, у ознаци $\sigma(\mathbb{A})$, а која се дефинише са

$$\sigma(\mathbb{A}) := (\#(f_1), \ldots, \#(f_n)).$$

Јасно је да би две структуре биле једнаке, морају имати исту сигнатуру.

Наведимо и неке важне примере алгебарских структура.

1. $\mathbb{N} = (N, +, \cdot, 0, 1)$, $\sigma(\mathbb{N}) = (2, 2, 0, 0)$.
2. $\mathbb{Z} = (Z, +, \cdot, -, 0, 1)$, $\sigma(\mathbb{Z}) = (2, 2, 1, 0, 0)$.
3. $\mathbb{Z}_n = (Z_n, +_n, \cdot_n, -_n, 0, 1)$, $\sigma(\mathbb{Z}_n) = (2, 2, 1, 0, 0)$.
4. $\mathbb{P}(X) = (\mathcal{P}(X), \cup, \cap, ^c, \emptyset, X)$, $\sigma(\mathbb{P}(X)) = (2, 2, 1, 0, 0)$.

Да бисмо даље радили са алгебарским структура, тј. да бисмо испитали који закони важе у њима, морамо најпре увести појам алгебарског закона, а за то нам је потребан и појам алгебарског израза.

Појам алгебарског израза нам јесте познат из школске математике (појављује се чак и у укрштеним речима — једночлани алгебарски израз познат нам је као моном), али вероватно не баш у прецизној формулацији. У сваком случају, знамо да су алгебарски изрази неки записи у којима се појављују константе, променљиве и знаци алгебарских операција. Дакле, сам израз није неки број, него неки запис. Сваки запис је записан на неком језику, те нам је стога погодно да уведемо појам алгебарског језика.

**Дефиниција 3** Алгебарски језик је произвољан непразан скуп чије елементе називамо функцијски (операцијски) симболи. Осим тога, сваком симболу је придружен један природан број, који представља његову дужину.

Обично користимо $L$ као ознаку за алгебарски језик. Уколико $F \in L$, онда дужину симбола $F$ означавамо са $\#(F)$. На пример, уколико желимо да записујемо изразе у којима се појављује само сабирање, довољно је узети да је $L = \{+\}$, где је овде $+$ симбол за сабирање (а не сама операција!). Уколико је ситуација сложенија, па разматрамо и сабирање и множење, а и нулу и јединицу, онда радимо са алгебарским језиком $L = \{+, \cdot, 0, 1\}$, где су овде $+$ и $\cdot$ операцијски симболи дужине 2, а 0 и 1 операцијски симболи дужине 0, који се називају и симболи константи (писали смо већ да су константе заправо нуларне операције, тј. операције дужине 0). Наравно, да бисмо записивали алгебарске

изразе биће нам неопходни и зарези, као и заграде. Но, како су они увек потребни, не стављају се као део самог алгебарског језика (можда је ово добро место да поновите неке основне појмове логике првог реда, које сте обрадили у оквиру увода у математичку логику).

Као што нам је познато из школске математике, у оквиру израза се, поред заграда, знакова алгебарских операција и константи, такође појављују и променљиве. Дакле, потребан нам је и један скуп променљивих $\mathcal{V}ar = \{x_0, x_1, \ldots\}$. Овде је наведен скуп од пребројиво много променљивих, али наравно да ћемо ми у пракси најчешће користити и ознаке $x, y, z$ и слично за променљиве (просто је једноставније у формулама користити ове ознаке).

Сада можемо дефинисати и појам алгебарског израза (или само израза).

**Дефиниција 4** Нека је $L$ неки алгебарски језик. Алгебарски изрази језика $L$ дефинишу се са:

- Променљиве и симболи константи су алгебарски изрази.
- Ако су $t_1, \ldots, t_n$ алгебарски изрази и $F(\in L)$ операцијски симбол језика $L$ дужине $n$ $(n \geq 1)$, онда је и $F(t_1, \ldots, t_n)$ алгебарски израз.
- Алгебарски изрази се могу добити једино коначном применом претходна два правила.

Дакле, последње својство нам говори о коначности записа алгебарских израза. Нпр. ако је $L = \{+, \cdot, 0, 1\}$ где су $+$ и $\cdot$ операцијски симболи дужине 2, а 0 и 1 симболи константи, онда

$$(x + 0), ((1 + 1) \cdot (x + (1 \cdot y))), (1 \cdot (0 \cdot 1))$$

јесу алгебарски изрази, док

$$1 + 1 + \cdots$$

то није.

Као што знамо, алгебарске изразе можемо да израчунавамо, тј. можемо наћи вредност алгебарског израза чим знамо вредности свих променљивих које се у њему појављују. Наравно, морамо да будемо мало опрезнији. На пример, на шта прво помислите када угледате запис

$$A + B$$

на табли? Вероватно је прва асоцијација да је неко сабирао две матрице. Или можда два линеарна оператора. Али, зашто би то било тако? Можда је реч о сабирању два полинома, или чак два реална броја. Наравно да бројеве најчешће пишемо малим словима, али то што је најчешће, не значи и да је увек. Још је више нејасно о чему се ради ако угледате

$$A * B$$

на табли или у нечијој свесци. Шта је сад ово? Јасно је да морамо да знамо више да бисмо могли да израчунамо неки израз. Најпре, морамо да знамо у ком скупу радимо, затим морамо да знамо о којим се операцијама ради (дакле, морамо да знамо интерпретацију операцијских симбола који се ту појављују, нпр. којој операцији одговара симбол звездице из горњег израза). Наравно, симболу дужине $n$ одговара $n$-арна операција. Посебно, константном симболу (симболу дужине 0) одговара неки елемент из $A$. Напокон, морамо да знамо вредности промењљивих које се појављују у изразу (придруживање $\alpha\colon \mathcal{V}ar \to A$ обично се назива валуација (увод у математичку логику...) ).

**Дефиниција 5** Вредност алгебарског израза $t$ језика $L$ при датој валуацији $\alpha\colon \mathcal{V} \to A$, у ознаци $t^{\mathbb{A}}[\alpha]$, где је $\mathbb{A}$ алгебарска структура језика $L$ са скупом носачем $A$, дефинише се на следећи начин.

- Вредност симбола константе $c$ је онај елемент $c^{\mathbb{A}}$ скупа $A$ који је интерпретација константе $c$.
- Вредност промењљиве $x_i$ је $\alpha(x_i)$.
- Ако је $t = F(t_1, \ldots, t_n)$ где су $t_1, \ldots, t_n$ изрази и $F(\in L)$ операцијски симбол дужине $n$, онда је $t^{\mathbb{A}}[\alpha] = F^{\mathbb{A}}(t_1^{\mathbb{A}}[\alpha], \ldots, t_n^{\mathbb{A}}[\alpha])$, при чему је $F^{\mathbb{A}}$ интерпретација операцијског симбола $F$ (дакле операција дужине $n$, која одговара симболу $F$).

Ово можда делује компликовано, али заправо није. Урадимо два примера.

**Пример 6** Нека је $L = \{+, \cdot, 1\}$, где су $+$ и $\cdot$ операцијски симболи дужине 2, а 1 симбол константе. Ако је $\mathbb{A} = (M_2(\mathbb{R}), +, \cdot, E)$ алгебарска структура коју чине матрице реда 2 и у којима је $+$ операција сабирања матрица, $\cdot$ операција множења матрица, а $E$ јединична матрица, израчунати вредност израза $((x+1)\cdot(x+1))$ уколико је валуација $\alpha$ таква да је

$$\alpha(x) = \begin{bmatrix} 2 & 3 \\ 1 & -2 \end{bmatrix},$$

док се $+$ интепретира као сабирање матрица, $\cdot$ као множење матрица, а 1 као јединична матрица.

**Решење:** Вредност датог израза је заправо једнака матрици

$$(\alpha(x) + E) \cdot (\alpha(x) + E),$$

односно матрици

$$\left(\begin{bmatrix} 2 & 3 \\ 1 & -2 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) \cdot \left(\begin{bmatrix} 2 & 3 \\ 1 & -2 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right),$$

чију ће вредност читаоци лако израчунати. ♣

Приметимо да је знак + овде и операцијски симбол, а и сама операција! Уобичајен је случај да се користи иста ознака подразумевајући да се води рачуна о контексту у коме се дати симболи појављују. Уколико постоји могућност грешке, користе се различите ознаке.

**Пример 7** Нека је $L = \{*, \circ, n, j\}$, где су $*$ и $\circ$ операцијски симболи дужине 2, а $n$ и $j$ симболи константи. Дат је израз

$$((x_1 * j) \circ ((j * (j * n)) * j)).$$

Израчунати вредност овог израза ако знамо да је алгебарска структура о којој се ради структура $\mathbb{Z}_3 = (Z_3, +_3, \cdot_3, 0, 1)$ при валуацији $\alpha : \mathcal{V}ar \to Z_3$, где је $\alpha(x_1) = 1$, док се $*$ интерпретира као сабирање, а $\circ$ као множење по модулу 3 и интерпретација константног симбола $n$ је 0, а $j$ је 1.

**Решење:** Урадимо ово детаљно. Како се $*$ интерпретира са $+_3$, а $\circ$ са $\cdot_3$, док је интепретација за $n$ елемент 0, а за $j$ елемент 1, добијамо:

$$\begin{aligned}
&((x_1 * j) \circ ((j * (j * n)) * j))^{\mathbb{Z}_3}[\alpha] \\
&= (x_1 * j)^{\mathbb{Z}_3}[\alpha] \cdot_3 ((j * (j * n)) * j)^{\mathbb{Z}_3}[\alpha] \\
&= (x_1^{\mathbb{Z}_3}[\alpha] +_3 j^{\mathbb{Z}_3}[\alpha]) \cdot_3 ((j * (j * n))^{\mathbb{Z}_3}[\alpha] +_3 j^{\mathbb{Z}_3}[\alpha]) \\
&= (\alpha(x_1) +_3 1) \cdot_3 ((j^{\mathbb{Z}_3}[\alpha] +_3 (j * n)^{\mathbb{Z}_3}[\alpha]) +_3 1) \\
&= (1 +_3 1) \cdot_3 ((1 +_3 (j^{\mathbb{Z}_3}[\alpha] +_3 n^{\mathbb{Z}_3}[\alpha])) +_3 1) \\
&= 2 \cdot_3 ((1 +_3 (1 +_3 0)) +_3 1) \\
&= 2 \cdot_3 ((1 +_3 1) +_3 1) \\
&= 2 \cdot_3 (2 +_3 1) \\
&= 2 \cdot_3 0 \\
&= 0.
\end{aligned}$$

♣

Позабавимо се сада појмом алгебарског закона и појмом алгебарске теорије.

**Дефиниција 8** Нека је $L$ неки алгебарски језик. Алгебарски закон језика $L$ је формула облика $t_1 = t_2$, где су $t_1$ и $t_2$ алгебарски изрази језика $L$.

**Дефиниција 9** Уколико је $\mathbb{A}$ алгебарска структура језика $L$ и $t_1 = t_2$ неки алгебарски закон истог језика онда тај закон важи у алгебри $\mathbb{A}$, или да је $\mathbb{A}$ модел за тај закон, у ознаци

$$\mathbb{A} \models t_1 = t_2,$$

уколико за сваку валуацију $\alpha: \mathcal{V}ar \to A$ важи:

$$t_1^{\mathbb{A}}[\alpha] = t_2^{\mathbb{A}}[\alpha].$$

Другим речима, закон $t_1 = t_2$ важи у алгебри $\mathbb{A}$, уколико се вредности ових израза поклапају за све могуће вредности променљивих из скупа носача $A$.

**Дефиниција 10** Скуп алгебарских закона назива се алгебарска теорија, а елементи тог скупа називају се аксиоме те теорије.

**Дефиниција 11** Уколико је $T$ нека алгебарска теорија, онда се са $\mathfrak{M}(T)$ означава класа свих алгебри у којима важе сви закони из $T$.

Класа $\mathfrak{M}(T)$ зове се и варијетет теорије $T$. Нека класа $\mathfrak{M}$ алгебри истог језика је варијетет (или једнакосна класа) уколико постоји алгебарска теорија $T$ таква да је $\mathfrak{M} = \mathfrak{M}(T)$.

Овде је важно истаћи неколико чињеница. Најпре, ма каква била теорија $T$, увек постоји алгебра у којој су тачни сви закони из $T$. Наиме, ма која једночлана алгебра $\mathbb{A} = \{a\}$, где је $a$ произвољно је пример такве алгебре. Јасно је да су све операције у овој алгебри тривијалне и да сви алгебарски закони ту важе. Осим тога, $\mathfrak{M}(T)$ је заиста класа, а не скуп. Ово је већ опажање које је базирано на резултатима теорије скупова. Наиме, добро је познато да не постоји скуп чији су елементи сви скупови. Но, не постоји ни скуп који садржи све једночлане скупове (ово је питање из теорије скупова и тиме се нећемо бавити — читалац може консултовати неки основни уџбеник у коме се ово разматра). Како све једночлане алгебре (прецизније говорећи алгебре са једночланим базним скупом) припадају класи $\mathfrak{M}(T)$, то је та класа заиста сувише обимна да би представљала скуп.

**Пример 12** Нека језик $L$ садржи операцијски знак $\cdot$ дужине 2. тада је

$$((x \cdot y) \cdot z) = (x \cdot (y \cdot z)),$$

где су $x, y, z$ ма које променљиве један алгебарски закон и наравно да нам је он познат као закон асоцијативности. Уколико се у $L$ налази и операцијски знак $+$ дужине 2, онда је закон

$$(x \cdot (y + z)) = ((x \cdot y) + (x \cdot z)),$$

добро познат као закон дистрибутивности.

Наравно, у пракси ћемо избегавати писање непотребних заграда, па ћемо закон асоцијативности записивати у облику

$$(x \cdot y) \cdot z = x \cdot (y \cdot z),$$

а закон дистрибутивности у облику

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

Наведимо сада, у облику табеле, примере неких алгебарских теорија.

| **Теорија** | **Језик** | **Аксиоме** |
|---|---|---|
| групоида ($G$) | $L_G = \{\cdot\}$ | нема |
| полугрупа ($S$) | $L_S = L_G$ | $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ |
| моноида ($M$) | $L_M = L_S \cup \{1\}$ | $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $x \cdot 1 = x$, $1 \cdot x = x$ |
| група ($Grp$) | $L_{Grp} = L_M \cup \{'\}$ | $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $x \cdot 1 = x$, $1 \cdot x = x$, $x \cdot x' = 1$, $x' \cdot x = 1$ |
| Абелових група ($Ab$) | $L_{Ab} = \{+, -, 0\}$ | $(x + y) + z = x + (y + z)$, $x + 0 = x$, $0 + x = x$, $x + (-x) = 0$, $(-x) + x = 0$, $x + y = y + x$ |
| прстена ($Rng$) | $L_{Rng} = L_{Ab} \cup L_S$ | $(x + y) + z = x + (y + z)$, $x + 0 = x$, $0 + x = x$, $x + (-x) = 0$, $(-x) + x = 0$, $x + y = y + x$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $x \cdot (y + z) = x \cdot y + x \cdot z$, $(y + z) \cdot x = y \cdot x + z \cdot z$ |
| прстена са јединицом ($Ring$) | $L_{Ring} = L_{Ab} \cup L_M$ | $(x + y) + z = x + (y + z)$, $x + 0 = x$, $0 + x = x$, $x + (-x) = 0$, $(-x) + x = 0$, $x + y = y + x$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $x \cdot (y + z) = x \cdot y + x \cdot z$, $(y + z) \cdot x = y \cdot x + z \cdot x$, $x \cdot 1 = x$, $1 \cdot x = x$ |
| комутативних прстена ($ComRng$) | $L_{ComRng} = L_{Rng}$ | $(x + y) + z = x + (y + z)$, $x + 0 = x$, $0 + x = x$, $x + (-x) = 0$, $(-x) + x = 0$, $x + y = y + x$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $x \cdot (y + z) = x \cdot y + x \cdot z$, $x \cdot y = y \cdot x$ |
| комутативних прстена са јединицом ($ComRing$) | $L_{ComRing} = L_{Ring}$ | $(x + y) + z = x + (y + z)$, $x + 0 = x$, $0 + x = x$, $x + (-x) = 0$, $(-x) + x = 0$, $x + y = y + x$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $x \cdot (y + z) = x \cdot y + x \cdot z$, $x \cdot y = y \cdot x$, $x \cdot 1 = x$, $1 \cdot x = x$ |

Саме алгебарске теорије о којима је реч (подсетимо се да је алгебарска теорија скуп алгебарских закона) могу се краће и овако изразити:

- $G = \emptyset$;
- $S = G \cup \{(x \cdot y) \cdot z = x \cdot (y \cdot z)\}$;
- $M = S \cup \{x \cdot 1 = x, 1 \cdot x = x\}$;
- $Grp = M \cup \{x \cdot x' = 1, x' \cdot x = 1\}$
- $Ab = \{(x + y) + z = x + (y + z), x + 0 = x, 0 + x = x, x + (-x) = 0, (-x) + x = 0, x + y = y + x\}$;
- $Rng = Ab \cup S \cup \{x \cdot (y + z) = x \cdot y + x \cdot z, (y + z) \cdot x = y \cdot x + z \cdot x\}$;
- $Ring = Rng \cup M$;
- $ComRng = Rng \cup \{x \cdot y = y \cdot x\}$;

- $ComRing = ComRng \cup M$.

На пример, $\mathfrak{M}(Grp)$ означава класу свих група, док $\mathfrak{M}(ComRing)$ означава класу свих комутативних прстена са јединицом.