Glava 1

Algebarske strukture

1.1 Algebarske operacije i algebraske strukture

Defnicija 1.1 Neka su I i $A \neq \emptyset$ skupovi. ***I-familija elemenata skupa*** A, ili ***familija elemenata iz A indeksirana skupom*** I, je funkcija[1] $a : I \to A$ koju radije zapisujemo $a = (a_i)_{i \in I} \in A^I$, gde je $a_i := a(i)$.
Ako je $I = \emptyset$, onda je $A^I = \{\emptyset\}$, pa je svaka I-familija prazna.
Pojam familije uopštava pojam uređene n-torke (n je prirodan broj) i pojam niza.

Defnicija 1.2 Neka je A neprazan skup i n nenegativan ceo broj.

a) Definišemo ***n-ti stepen skupa*** A, u oznaci A^n:

$$A^0 := \{\emptyset\} \text{ i}$$

$$A^n := \{(a_1, \ldots, a_n) | a_1, \ldots, a_n \in A\}, \text{ ako je } n > 0.$$

A^n se formalizuje i kao skup svih funkcija iz skupa $\{1, 2, \ldots, n\}$ u skup A.

b) ***Algebarska operacija skupa*** A***, dužine*** n, ili ***n-arna operacija skupa*** A , je ma koja funkcija $f : A^n \to A$. Za n kažemo da je ***arnost*** ili ***dužina*** operacije f, u oznaci $\mathrm{ar}(f)$.

[1] Oznaka za skup svih funkcija iz skupa A u skup B je B^A, $A^\emptyset = \{\emptyset\}$.

Ako je f n-arna operacija i ako su $a_1, \ldots, a_n \in A$, onda za sliku $f(a_1, \ldots, a_n)$ iz A kažemo i da je rezultat operacije f, primenjene na $(a_1, \ldots, a_n)$.

Operacije f dužine 0 su određene slikom $f(\emptyset)$ jedinog elementa $\emptyset$ iz A^0, to jest fiksiranim elementom $a := f(\emptyset)$ iz A. Zato ćemo ***nularne*** operacije poistovećivati sa izabranim elementima skupa A i tako ih zapisivati. Zapravo, ***konstante*** iz A su našom definicijom formalno uvedene kao nularne operacije.

Ako je f operacija dužine 1, ili ***unarna*** operacija, i $a \in A$, rezultat pišemo $f(a)$; ali ne uvek, veoma retko. Neki znaci, na primer $-$, $^{-1}$, $'$, , ^{c}, ^{T}, se često koriste za označavanje unarnih operacija. Tada rezultat primene tih operacija na a pišemo $(-a)$, (a^{-1}), (a'), $\overline{a}$, (a^c), (a^T).

Ako je f operacija dužine 2, ili ***binarna*** operacija, i $a, b \in A$, rezultat u takozvanom prefiksnom zapisu pišemo $f(a, b)$, ali se takav zapis retko koristi. Neki znaci, na primer $+$, $\cdot$, $\cup$, $\cap$, $\vee$, $\wedge$, $\triangle$, pa čak i $\circ$, $*$, se često koriste za označavanje binarnih operacija i rezultat primene tih operacija na $a, b \in A$ se piše u takozvanom infiksnom zapisu. Na primer $(a * b)$.

Defnicija 1.3 ***Algebarska struktura***, ili kraće ***algebra***, je uređeni par $\mathbb{A} := (A, \Omega)$, gde je A neprazan skup, ***domen algebre*** $\mathbb{A}$, i Ω neka familija algebarskih operacija skupa A. ***Tip***, ili ***signatura***, ***algebre*** $\mathbb{A} = (A, \Omega)$ je Ω-familija $(\mathrm{ar}(f))_{f \in \Omega}$.
Kada je $\Omega = (f_i)_{i \in I}$, za neki skup I, onda pišemo i $\mathbb{A} := (A, f_i)_{i \in I}$. Tada je *tip*, ili *signatura*, *algebre* $\mathbb{A}$ I-familija $(\mathrm{ar}(f_i))_{i \in I}$.
Algebre $\mathbb{A}$ i $\mathbb{B}$ su ***istotipne*** ako imaju jednake tipove.

1.2 Pregled osnovnih algebarskih struktura

U ovom kursu osnovne algebarske strukture su: grupoidi, polugrupe (semigrupe), monoidi, grupe, prsteni i polja.

Defnicija 2.1 ***Grupoid*** je uređeni par $(G, *)$, gde je $*$ binarna operacija skupa $G \neq \emptyset$.

Defnicija 2.2 Neka je $(G, *)$ grupoid.
a) $e \in G$ je ***levi neutral grupoida*** G akko $(\forall x \in G)\ e * x = x$.
b) $e \in G$ je ***desni neutral grupoida*** G akko $(\forall x \in G)\ x * e = x$.
c) $e \in G$ je ***neutral grupoida*** G akko $(\forall x \in G)\ e * x = x = x * e$.
Umesto neutral, kažemo i neutralni element, identiteta, jedinica (posebno ako je binarna operacija $\cdot$), nula (posebno ako je binarna operacija $+$).

Lema 2.1 Grupoid $(G, *)$ ima najviše jedan neutral.

Δ. Pretpostavimo da su $e, f \in G$ neutrali. Tada je $f = e * f = e$. $\square$

Defnicija 2.3 ***Polugrupa (semigrupa)*** je grupoid $(S, *)$, u kome je binarna operacija $*$ asocijativna. Ekvivalentno, grupoid $(S, *)$ je ***semigrupa*** akko $(\forall x, y, z \in S)(x * y) * z = x * (y * z)$.

Defnicija 2.4 ***Monoid*** je semigrupa sa neutralom. Drugim rečima, semigrupa $(M, *)$ je ***monoid*** akko $(\exists z \in M)(\forall x \in M) z * x = x = x * z$. Ekvivalentno, $(M, *, e)$ je ***monoid*** akko $(M, *)$ je semigrupa, a $e \in M$ je njen neutral: $(\forall x \in M)\ e * x = x = x * e$.

Defnicija 2.5 Neka je $(M, *, e)$ monoid, $x \in M$.

a) $y \in M$ je ***levi inverz elementa*** x akko $y * x = e$.

b) $y \in M$ je ***desni inverz elementa*** x akko $x * y = e$.

c) $y \in M$ je ***inverz elementa*** x akko $y * x = e = x * y$.

Umesto inverz, kažemo i inverzni element, suprotni element (posebno ako je binarna operacija sabiranje, $+$).

Lema 2.2 Neka je $(M, *, e)$ monoid. Tada $x \in M$ ima najviše jedan inverz. (Ako element $x \in M$ ima inverz, označavaćmo ga $\overline{x}$.)

Δ. Pretpostavimo da su $y, z \in M$ inverzi elementa x.

Tada je $y = y * e = y * (x * z) = (y * x) * z = e * z = z$. $\square$

Lema 2.3 Neka je $(M, *, e)$ monoid. Ako su $a, b \in M$ invertibilni, onda su e, $a * b$ i $\overline{a}$ takođe invertibilni i važi:

a) $\overline{e} = e$, b) $\overline{a * b} = \overline{b} * \overline{a}$, c) $\overline{\overline{a}} = a$.

Δ. a) Sledi iz $e * e = e$.

b) Zaista $(\overline{b} * \overline{a}) * (a * b) = \overline{b} * (\overline{a} * (a * b)) = \overline{b} * ((\overline{a} * a) * b) = \overline{b} * (e * b) = \overline{b} * b = e$.

Slično je $(a * b) * (\overline{b} * \overline{a}) = e$. Otuda je $\overline{b} * \overline{a}$ inverz elementa $a * b$.

c) Sledi iz $a * \overline{a} = e = \overline{a} * a$. $\square$

Defnicija 2.6 ***Grupa*** je monoid u kome svaki element ima inverz. [Monoid $(G, *, e)$ je ***grupa*** akko $(\forall x \in G)(\exists y \in G)\ y * x = e = x * y$.] Ekvivalentno (Lema 2.2), $(G, *, ^{-}, e)$ je ***grupa*** akko $(G, *, e)$ je monoid i $(\forall x \in G)\ \overline{x} * x = e = x * \overline{x}$.

Defnicija 2.7 Grupa (semigrupa, grupoid) $(G, *)$ je ***komutativna*** akko

$$(\forall x, y \in G)\ x * y = y * x.$$

Napomena. Videli smo da se grupa može definisati na sledeće načine:

a) $(G, *)$ je grupa akko $(G, *)$ je semigrupa i

$(\exists z \in G)(\forall x \in G)(\ z * x = x = x * z\ \wedge\ (\exists y \in G)\ y * x = z = x * y)$,

b) $(G, *, ^-, e)$ je grupa akko $(G, *)$ je semigrupa,

$(\forall x \in G)\ e * x = x = x * e$, i $(\forall x \in G)\ \overline{x} * x = e = x * \overline{x}$.

Lema 2.4 Neka je $(G, *)$ semigrupa. Tada:

a) $(G, *)$ je grupa akko

$(\exists z \in G)(\forall x \in G)(\ z * x = x\ \wedge\ (\exists y \in G)\ y * x = z)$,

b) $(G, *, ^-, e)$ je grupa akko $(\forall x \in G)\ e * x = x$, i $(\forall x \in G)\ \overline{x} * x = e$.

Δ. Dovoljno je pokazati da desna strana povlači levu.

b) Prvo dokazujemo $(\forall x \in G)\ x * \overline{x} = e$, a zatim $(\forall x \in G)\ x * e = x$. Imamo da je $x * \overline{x} = (e * x) * \overline{x} = ((\overline{\overline{x}} * \overline{x}) * x) * \overline{x} = (\overline{\overline{x}} * (\overline{x} * x)) * \overline{x} = (\overline{\overline{x}} * e) * \overline{x} = \overline{\overline{x}} * (e * \overline{x}) = \overline{\overline{x}} * \overline{x} = e$, a onda je $x * e = x * (\overline{x} * x) = (x * \overline{x}) * x = e * x = x$.

a) Dovoljno je da neutral z označimo slovom e, inverz y elementa x slovom $\overline{x}$, a inverz elementa $\overline{x}$ slovom $\overline{\overline{x}}$ pa da ponovimo prethodni dokaz. $\Box$

Stav 2.1 Neka je $(M, *, e)$ monoid. Posmatramo skup invertibilnih elemenata $G := \{x \in M \mid (\exists y \in M)\ y * x = e = x * y\}$. Tada $e \in G$, skup G je zatvoren za binarnu operaciju $*$ i monoid $(G, *, e)$ je grupa.

Δ. Iz $e * e = e$ sledi $e \in G$. Dokazujemo zatvorenost. Neka su $a, b \in G$. Tada postoje neki $\overline{a}, \overline{b} \in M$ koji su inverzi elemenata a i b. Onda je $\overline{b} * \overline{a} = \overline{a * b}$ (Lema 2.3) inverz elementa $a * b$. Znači da $a * b \in G$. Ako je $a \in G$ i $\overline{a} \in M$ njegov inverz, onda je a inverz za $\overline{a}$ (Lema 2.3), pa $\overline{a} \in G$. $\Box$

Primeri. $(\mathbb{N}, +)$, $(\mathbb{N}, \mathrm{NZD})$ su komutativni grupoidi, $(\mathbb{N}, \cdot, 1)$, $(\mathbb{Z}, \cdot, 1)$,

$(\mathbb{N}_0, +, 0)$, $(\mathbb{N}, \mathrm{NZS}, 1)$ komutativni monoidi, $(\mathbb{Z}, +, -, 0)$, $(\mathbb{Q}, +, -, 0)$, $(\mathbb{R}, +, -, 0)$, $(\mathbb{C}, +, -, 0)$, $(\mathbb{Q}^\times, \cdot, {}^{-1}, 1)$, $(\mathbb{R}^\times, \cdot, {}^{-1}, 1)$, $(\mathbb{C}^\times, \cdot, {}^{-1}, 1)$ su komutativne grupe. Neka je X neprazan skup, $(X^X, \circ, \mathrm{id}_X)$ je nekomutativan monoid za $|X| \geq 2$, a njegova grupa svih inverzibilnih je $S_X := \{f \in X^X \mid f \text{ je bijekcija}\}$, nekomutativna je za $|X| > 2$.

Defnicija 2.7 Algebarska struktura $\mathbb{P} = (P, +, \cdot, -, 0)$ tipa $(2, 2, 1, 0)$ je ***prsten*** akko $(P, +, -, 0)$ je komutativna grupa, $(P, \cdot)$ je semigrupa i $(\forall x, y, z \in P)\ (x(y + z) = xy + xz\ \wedge\ (x + y)z = xz + yz)$ (važe oba zakona distributivnosti). Prsten $\mathbb{P}$ je ***komutativan*** akko je $\cdot$ komutativna, to jest akko je $(\forall x, y \in P)\ xy = yx$. $\mathbb{P}$ je prsten ***sa jedinicom*** 1 akko je $(\forall x \in P)\ 1 \cdot x = x = x \cdot 1$.

Lema 2.5 Neka je $(P, +, \cdot, -, 0)$ prsten. Tada:

a) $x\,0 = 0 = 0\,x$,

b) $x(-y) = -xy = (-x)y$, $(-x)(-y) = xy$,

c) Ako $x - y := x + (-y)$, onda $x(y - z) = xy - xz$, $(x - y)z = xz - yz$,

d) $(x_1 + \cdots + x_n)y = x_1 y + \cdots + x_n y$, $x(y_1 + \cdots + y_m) = xy_1 + \cdots + xy_m$,

e) $(x_1 + \cdots + x_n)(y_1 + \cdots + y_m) = \sum_{i=1}^{n} \sum_{j=1}^{m} x_i y_j = \sum_{j=1}^{m} \sum_{i=1}^{n} x_i y_j$.

Δ. a) Iz $x\,0 = x(0 + 0) = x\,0 + x\,0$ sledi $x\,0 = x\,0 + x\,0$. Onda je $x\,0 + (-x\,0) = (x\,0 + x\,0) + (-x\,0) = x\,0 + (x\,0 + (-x\,0))$, a ovo povlači $0 = x\,0$. Slično, $0 = 0\,x$.

b) Iz $0 = x\,0 = x(-y + y) = x(-y) + xy$ sledi $0 = x(-y) + xy$. Onda je $0 + (-xy) = (x(-y) + xy) + (-xy) = x(-y) + (xy + (-xy))$, a ovo povlači $-xy = x(-y)$. Slično, $-xy = (-x)y$.

Iz prethodnih jednakosti imamo $(-x)(-y) = -(-x)y = -(-xy) = xy$.

c) $(x - y)z = (x + (-y))z = xz + (-y)z = xz + (-yz) = xz - yz$.

d) Indukcijom, koristeći distributivnost.

e) Sledi iz d). $\square$

Primeri $(\{0\},+,\cdot,-,0)$, $(\mathbb{Z},+,\cdot,-,0)$, $(\mathbb{Q},+,\cdot,-,0)$, $(\mathbb{R},+,\cdot,-,0)$, $(\mathbb{Z}[x],+,\cdot,-,0)$, $(\mathbb{Q}[x],+,\cdot,-,0)$, $(\mathbb{R}[x],+,\cdot,-,0)$, $(\mathbb{P}(A),\triangle,\cap,\mathrm{id},\emptyset)$[2] su komutativni prsteni, sa jedinicom.

Defnicija 2.8 Definišemo ***karakteristiku prstena*** $\mathbb{P}$, u oznaci $\operatorname{char}\mathbb{P}$.

$$\operatorname{char}\mathbb{P} = \begin{cases} 0, & \text{ako je } C := \{n \in \mathbb{N} \mid (\forall x \in P)\ nx = 0\} = \emptyset; \\ \min C, & \text{ako je } C \neq \emptyset. \end{cases}$$

Ako je $\mathbb{P}$ prsten sa jedinicom 1, onda je $C = C_1 := \{n \in \mathbb{N} \mid n1 = 0\} \subseteq \mathbb{N}$. Neposredno imamo $C \subseteq C_1$. Za $C_1 \subseteq C$: ako je $n \in C_1$, onda za svako $x \in P$ imamo $nx = n(1x) = (n1)x = 0\,x = 0$, znači $n \in C$.

Defnicija 2.9 Prsten $\mathbb{P}$ je ***bez delitelja nule*** akko

$$(\forall x, y \in P)\ (xy = 0 \ \Rightarrow\ x = 0 \ \vee\ y = 0).$$

Lema 2.6 Ako je $\mathbb{P}$ prsten sa jedinicom 1, bez delitelja nule, onda je njegova karakteristika nula ili neki prost broj p.

Δ. Neka je $\operatorname{char}\mathbb{P} = m = kl$, gde su $k, l < m$. Tada iz $0 = m1 = (kl)1 = (kl)(11) = (k1)(l1)$ sledi $k1 = 0$ ili $l1 = 0$. Kontradikcija. $\square$

Defnicija 2.10 ***Polje*** je komutativan prsten sa jed. $1 \neq 0$ u kome svaki ne-nula element ima multiplikativni inverz. To jest, komutativan prsten $\mathbb{F}$ sa jed. 1 je ***polje*** akko $(\forall x \in F)\ (x \neq 0 \ \Rightarrow\ (\exists y \in F)\ xy = 1)$ i $1 \neq 0$. Inverz ne-nula elementa $x \in F$ označavamo x^{-1}.

[2] $\mathbb{P}(A) := \{X \mid X \subseteq A\}$ je *partitivni skup skupa* A, $\triangle$ je simetrična razlika.

Lema 2.7 U svakom polju važi $(\forall x, y)\ (xy = 0 \ \Rightarrow\ x = 0 \ \vee\ y = 0)$.

Δ. Dokazujemo ekvivalentnu formulu $(\forall x, y)\ (xy = 0 \ \wedge\ x \neq 0 \ \Rightarrow\ y = 0)$. Ako je $xy = 0$, i $x \neq 0$, onda je $y = (x^{-1}x)y = x^{-1}(xy) = x^{-1}0 = 0$. $\square$

Posledica. Svako polje $\mathbb{F}$ je prsten bez delitelja nule. Karakteristika polja je 0 ili prost broj $p \in \mathbb{N}$ (Lema 2.6).

Primeri $(\mathbb{Q}, +, \cdot, -, 0, 1)$, $(\mathbb{R}, +, \cdot, -, 0, 1)$ i $(\mathbb{C}, +, \cdot, -, 0, 1)$ su polja. Ali su $(\{0\}, +, \cdot, -, 0)$, $(\mathbb{Z}, +, \cdot, -, 0)$, $(\mathbb{Z}[x], +, \cdot, -, 0)$, $(\mathbb{Q}[x], +, \cdot, -, 0)$, $(\mathbb{R}[x], +, \cdot, -, 0)$, $(\mathbb{P}(A), \triangle, \cap, \mathrm{id}, \emptyset)$ prsteni koji nisu polja.

1.3 Euklidsko deljenje u $\mathbb{Z}$

Lema o euklidskom deljenju u $\mathbb{Z}$. Za svaki $m \in \mathbb{Z}$, i svaki $n \in \mathbb{N}^+$ postoje jedinstveni $q \in \mathbb{Z}$ i $r \in \{0, 1, \ldots n-1\}$ tako da je $m = n \cdot q + r$.
Tj. $(\forall m \in \mathbb{Z})(\forall n \in \mathbb{N}^+)(\exists! q \in \mathbb{Z})(\exists! r \in \mathbb{Z})\ (\ m = n \cdot q + r\ ,\ 0 \leq r < n\ )$.
Ekvivalentno: $(\forall n \in \mathbb{N}^+)(\forall m \in \mathbb{Z})(\exists! r \in \mathbb{Z})\ (\ n \mid m - r\ ,\ 0 \leq r < n\ )$.

Definicija 3.1 a) Za $n \in \mathbb{N}^+$, uvodimo $\mathbb{Z}_{/n} := \{0, 1, \ldots n-1\}$.

b) **Ostatak pri euklidskom deljenju brojem** $n \in \mathbb{N}^+$ je funkcija $\varrho_n : \mathbb{Z} \to \mathbb{Z}_{/n}$ definisana implicitno:

$$(\forall m \in \mathbb{Z})\ (\ \varrho_n(m) = r \Leftrightarrow (\ r \in \mathbb{Z}_{/n}\ \wedge\ n \mid m - r\ )\ ).$$