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 $-$, $^{-1}$, $'$, $\overline{\ }$, ^{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. $\square$

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 $\overline{a} \in G$. $\square$

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). □

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. □

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 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[3]: $(\forall n \in \mathbb{N}^+)(\forall m \in \mathbb{Z})(\exists! r \in \mathbb{Z})\ (\ n \mid m - r\ ,\ 0 \leq r < n\ )$.

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:

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

Δ. Dokaz Leme euklidskom deljenju.

[3] Ako su $m, n \in \mathbb{Z}$, onda n *deli* m akko $(\exists q \in \mathbb{Z})\ m = nq$. Oznaka: $n \mid m$.

Δ. Prvi dokaz egzistencije q i r u lemi o euklidskom deljenju celih brojeva, razlikovanjem slučajeva i indukcijom po $m \geq 0$.

1. slučaj: $m \geq 0$.

(BI)[4] Ako je $m < n$, onda je $q = 0$, $r = m < n$.

(IK)[5] Neka je $m \geq n$ i pretpostavimo da

(IH)[6] Lema važi za prirodne brojeve manje od m.

Po (IH), postoje $q, r \in \mathbb{Z}$ tako da je $m - n = n \cdot q + r \ , \ 0 \leq r < n \ .$

Onda je $m = n \cdot (q+1) + r \ , \ 0 \leq r < n$, pa Lema važi i za m.

2. slučaj: $m < 0$.

Ako je $m < 0$, onda je $-m > 0$, pa na osnovu prethodnog slučaja postoje $q, r \in \mathbb{Z}$ tako da je $-m = n \cdot q + r \ , \ 0 \leq r < n \ .$

Ako je $r = 0$, onda je $m = n \cdot (-q) - r \ , \ 0 \leq -r < n \ .$

Ako je $n > r > 0$, onda je $m = n \cdot (-q-1) + (n-r) \ , \ 0 \leq n - r < n \ .$ $\square$

Δ. Drugi dokaz egzistencije q i r u lemi o euklidskom deljenju celih brojeva, koristeći da je $(\mathbb{N}, \leq)$ *dobro*[7] uređenje.

Skup $X := \{m - nq \mid q \in \mathbb{Z},\ m - nq \in \mathbb{N}_0\} \subseteq \mathbb{N}_0$ nije prazan.

Zaista: ako je $m \geq 0$, onda $m \in X$; inače $m - nm = -m(n-1) \in X$.

Postoji $\min X =: r = m - nq$, za neko q. Dokazujemo da je $0 \leq r < n$.

Iz $r \in X \subseteq \mathbb{N}_0$ sledi $0 \leq r$. Ako $r = m - nq \geq n$, onda $r - n = m - n(q+1) \geq 0$, to jest $r - n \in X$, što je kontradikcija sa $r - n < r = \min X$. Zato $r < n$. $\square$

Δ. Dokaz jedinstvenosti za q i r.

Neka je $m = n \cdot q + r \ , \ 0 \leq r < n$ i $m = n \cdot q_1 + r_1 \ , \ 0 \leq r < n$. Tada je $nq + r = nq_1 + r_1$, to jest $n(q - q_1) = r - r_1 \in \{0, \pm 1, \ldots, \pm(n-1)\}$. Otuda je $r_1 - r = 0$, i $q - q_1 = 0$. $\square$ Kraj dokaza Leme. $\square$

---

[4] Baza indukcije.

[5] Indukcijski korak.

[6] Indukcijska hipoteza.

[7] Uređenje $(S, \leq)$ je *dobro* akko svaki neprazan podskup $X \subseteq S$ ima minimum, $\min X$.

1.4 Jednakost ostataka

Definicija 4.1 Neka je $n \in \mathbb{N}^+$.

Definišemo binarnu relaciju, $=_n$, na skupu $\mathbb{Z}$:

$$(\forall x, y \in \mathbb{Z})\ (\ x =_n y \quad \Leftrightarrow \quad n \mid x - y \quad \Leftrightarrow \quad \varrho_n(x) = \varrho_n(y)\ ).$$

Lema 4.1 Osobine relacije $=_n$:

a) $=_n$ je relacija ekvivalencije; $\quad x =_n \varrho_n(x)$;

b) $x =_n y,\ \ x_1 =_n y_1 \quad \Rightarrow \quad x + x_1 =_n y + y_1,\ \ x \cdot x_1 =_n y \cdot y_1$;

c) $x =_n y \quad \Rightarrow \quad -x =_n -y,\ \ x^k =_n y^k$, za $k \geq 0$.

Δ. a) $n \mid x - \varrho_n(x) \quad \Rightarrow \quad x =_n \varrho_n(x)$.

Ref: $n \mid 0 = x - x \quad \Rightarrow \quad x =_n x$,

Sim: $x =_n y \quad \Rightarrow \quad n \mid x - y \quad \Rightarrow \quad n \mid y - x \quad \Rightarrow \quad y =_n x$,

Tran: $x =_n y,\ y =_n z \quad \Rightarrow \quad n \mid x - y,\ n \mid y - z$

$\Rightarrow \quad n \mid x - z = x - y + y - z \quad \Rightarrow \quad x =_n z$.

b) $x =_n y,\ \ x_1 =_n y_1 \quad \Rightarrow \quad n \mid x - y,\ \ n \mid x_1 - y_1$

$\Rightarrow \quad n \mid x - y + x_1 - y_1 = x + x_1 - (y + y_1)$,

$n \mid (x - y) \cdot x_1 + y \cdot (x_1 - y_1) = x \cdot x_1 - y \cdot y_1$

$\Rightarrow \quad x + x_1 =_n y + y_1,\ \ x \cdot x_1 =_n y \cdot y_1$,

c) $x =_n y \quad \Rightarrow \quad n \mid x - y \quad \Rightarrow \quad n \mid -(x - y) = -x - (-y) \quad \Rightarrow \quad -x =_n -y$.

$x =_n y \quad \Rightarrow \quad x^k =_n y^k$; za $k = 0$, jer je $x^0 = 1 = y^0$; i za $k = 1$.

$x =_n y \quad \Rightarrow \quad x^k =_n y^k$, za $k \geq 2$ sledi uzastopnom primenom b), $k - 1$ puta, kao i iz $x^k - y^k = (x - y) \cdot \sum_{s=0}^{k-1} x^{k-1-s} y^s$. $\square$

Napomena. Klasa ekvivalencije $x_{/=_n}$ elementa $x \in \mathbb{Z}$ jednaka je

$$x_{/=_n} = x + n\mathbb{Z}.$$

1.5 Tablice sabiranja i množenja u prstenu ostataka

Tablice komutativnih operacija su simetrične. Iz tablice se lako čita neutral (nula i jedinica), pa i invertibilnost elementa. Asocijativnost i distributivnost se ne vide neposredno. Treća tablica predstavlja Ojlerovu grupu.

$+_2$	0	1
0	0	1
1	1	0

$\cdot_2$	0	1
0	0	0
1	0	1

$\cdot_2$	0	1
0		
1		1

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\cdot_3$	0	1	2
0			
1		1	2
2		2	1

$x^{3-1} = 1$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\cdot_4$	0	1	2	3
0				
1		1		3
2				
3		3		1

$x^2 = 1$

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\cdot_5$	0	1	2	3	4
0					
1		1	2	3	4
2		2	4	1	3
3		3	1	4	2
4		4	3	2	1

1.6 Prsten ostataka

Definicija 6.1 Neka je $n \in \mathbb{N}^+$, $\mathbb{Z}_{/n} := \{0, 1, \ldots, n-1\}$.

Definišemo dve binarne $+_n$, $\cdot_n$ i jednu unarnu operaciju $-_n$ na $\mathbb{Z}_{/n}$:

$$x +_n y := \varrho_n(x+y), \qquad -_n x := \begin{cases} 0, & \text{ako je } x = 0; \\ n - x, & \text{ako } 0 < x < n. \end{cases}$$
$$x \cdot_n y := \varrho_n(x \cdot y),$$

Stav 6.1 $(\mathbb{Z}_{/n}, +_n, \cdot_n, -_n, 0, 1)$ je komutativan prsten sa jedinicom.

Δ. Ako je $n = 1$, onda je $\mathbb{Z}_{/n} = \{0\}$.

Neka je $n > 1$. Koristimo prethodnu definiciju, Lemu 4.1 a) $x =_n \varrho_n(x)$, zatim Lemu 4.1 b), i $(\forall s, t \in \mathbb{Z}_{/n})\ (s = t \ \Leftrightarrow\ s =_n t)$.

Asocijativnost za $+_n$:

$(x +_n y) +_n z =_n (x +_n y) + z =_n (x + y) + z =_n x + (y + z) =_n x + (y +_n z) =_n x +_n (y +_n z) \ \Rightarrow\ (x +_n y) +_n z = x +_n (y +_n z)$,

Asocijativnost za $\cdot_n$:

$(x \cdot_n y) \cdot_n z =_n (x \cdot_n y) \cdot z =_n (x \cdot y) \cdot z =_n x \cdot (y \cdot z) =_n x \cdot (y \cdot_n z) =_n x \cdot_n (y \cdot_n z) \ \Rightarrow\ (x \cdot_n y) \cdot_n z = x \cdot_n (y \cdot_n z)$,

Komutativnost za $+_n$ i $\cdot_n$ se vidi neposredno, iz definicije.

Nula 0 je neutral za $+_n$, a jedinica 1 je neutral za $\cdot_n$.

Za svako $x \in \mathbb{Z}_{/n}$ suprotni element je $-_n x$; vidi se neposredno, iz definicije.

Distributivnost $\cdot_n$ prema $+_n$:

$(x +_n y) \cdot_n z =_n (x +_n y) \cdot z =_n (x + y) \cdot z =_n x \cdot z + y \cdot z =_n x \cdot_n z + y \cdot_n z =_n x \cdot_n z +_n y \cdot_n z \ \Rightarrow\ (x +_n y) \cdot_n z = x \cdot_n z +_n y \cdot_n z$. $\square$

Napomena. Karakteristika prstena $\mathbb{Z}_{/n}$ je n; $\operatorname{char} \mathbb{Z}_{/n} = n$.

Teorema 6.2 $(\mathbb{Z}_{/n}, +_n, \cdot_n, -_n, 0, 1)$ je polje akko n je prost.

Δ. $\Rightarrow$: Karakteristika polja je 0 ili prost broj, prema Posledici Leme 2.7. Zato, ako je $\mathbb{Z}_{/n}$ polje, onda je $n = \operatorname{char} \mathbb{Z}_{/n}$ prost broj.

Direktan dokaz: ako je $n = m \cdot k$ složen, onda $m \cdot_n k = 0$, $m \neq 0$, $k \neq 0$, što je u polju nemoguće (Lema 2.7 Polje nema delitelje nule.).

$\Leftarrow$: Neka je $n =: p$ prost. Tada je $0 \neq 1$ u Z_p.

Dovoljno je dokazati da svaki $m \in \mathbb{Z}_{/p} \setminus \{0\}$ ima inverz za množenje.

Posmatramo funkciju $L_m : \mathbb{Z}_{/p} \to \mathbb{Z}_{/p} : x \mapsto m \cdot_p x$.

Dokazujemo da je „$1-1$”. Neka su $x, y \in \mathbb{Z}_{/p}$.

$$\begin{aligned} L_m(x) = L_m(y) \quad &\Rightarrow \quad m \cdot_p x = m \cdot_p y \quad \Rightarrow \quad m \cdot x =_p m \cdot y \\ &\Rightarrow \quad p \mid m \cdot (x-y) \\ &\Rightarrow \quad p \mid m \ \vee p \mid x - y \in \{0, \pm 1, \ldots, \pm(p-1)\} \\ &\Rightarrow \quad x - y = 0 \quad \Rightarrow \quad x = y. \end{aligned}$$

$\lceil$ Lema. Neka je $f : X \to Y$ funkcija, X i Y su konačni, $|X| = |Y|$.
Tada: f je „$1-1$” ($|f[X]| = |X|$) akko f je „na” ($|f[X]| = |Y|$). $\rfloor$

L_m je „$1-1$”, pa je (prema prethodnoj lemi) L_m i „na”.

Otuda sledi da postoji $k \in \mathbb{Z}_{/p}$ tako da je $m \cdot_p k = L_m(k) = 1$.

Znači da m ima inverz. $\square$

Primeri. Polje $\mathbb{Z}_p$ koje ima p elemenata, p je prost broj, i $\operatorname{char} \mathbb{Z}_p = p$.

Primeri. Neka polja čiji domeni su podskupovi skupa kompleksnih brojeva zatvoreni za sve operacije polja $\mathbb{C}$:

$\mathbb{Q}[\sqrt{3}] := \{a_0 + a_1\sqrt{3} \mid a_0, a_1 \in \mathbb{Q}\}$,

$\mathbb{Q}[\sqrt[3]{5}] := \left\{a_0 + a_1\sqrt[3]{5} + a_2\sqrt[3]{5}^2 \mid a_0, a_1, a_2 \in \mathbb{Q}\right\}$,

$\mathbb{Q}[\sqrt{2}, \sqrt{3}] := \{a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6} \mid a_0, a_1, a_2, a_2 \in \mathbb{Q}\}$.

1.7 Primer A^X (prenos strukture abelovske grupe)

Operacije skupa A^X definišemo *po koordinatama*.

Definicija 7.1 Neka je $X \neq \emptyset$, i neka je A komutativana grupa (Abelova grupa). Definišemo[8] operacije skupa $A^X := \{f \mid f : X \to A\}$:

0 u A^X: **Nula funkcija**,0, slika sve elemente skupa X u nulu $0 \in A$.

$+$ u A^X: **Zbir funkcija**$f, g \in A^X$ je funkcija $f + g \in A^X$, takva da je $(f+g)(x) := f(x) + g(x)$, za sve $x \in X$.

$-$ u A^X: Funkciji $f \in A^X$ je **suprotna funkcija**$-f \in A^X$ takva da je $(-f)(x) := -f(x)$[9], za sve $x \in X$.

Lema 7.1 Neka je $X \neq \emptyset$, A je komutativana grupa, i $f, g, h \in A^X$
Tada: $A^X1)$ $(f+g)+h = f+(g+h)$,

$A^X2)$ $f+g = g+f$,

$A^X3)$ $0+f = f = f+0$,

$A^X4)$ $-f+f = 0 = f+(-f)$.

Δ. Ako $f, g \in A^X$, onda $f = g \Leftrightarrow [(\forall x \in X)\ f(x) = g(x)]$.

A^X1: $((f+g)+h)(x) = (f+g)(x) + h(x) = (f(x)+g(x)) + h(x)$
$= f(x) + (g(x)+h(x)) = f(x) + (g+h)(x) = (f+(g+h))(x)$,

A^X2: $(f+g)(x) = f(x)+g(x) = g(x)+f(x) = (g+f)(x)$,

A^X3: $(f+0)(x) = f(x)+0(x) = f(x)+0 = f(x)$,

A^X4: $(f+(-f))(x) = f(x)+(-f)(x) = f(x)+(-f(x)) = 0 = 0(x)$. $\square$

[8] Koristimo algebraske operacije skupa A: $0 \in A$, sabiranje $+$, i unarnu operaciju $-$.
[9] Funkcije $f, g, ... \in A^X$ su „prioritetnije" od sabiranja, i od $-$, u A.

1.8 Polinomi

Definicija 8.1 Neka je $\mathbb{P}$ komutativan prsten sa jedinicom 1.
Definišemo $\mathbb{P}^{\mathbb{N}_0} = (P^{\mathbb{N}_0}, +, \cdot, -, \hat{0}, \hat{1})$:

$$(\forall a, b \in P^{\mathbb{N}_0})\ (\forall s \in \mathbb{N}_0)\ \begin{aligned}(a+b)(s) &:= a(s) + b(s) = a_s + b_s,\\ (-a)(s) &:= -a(s) = -a_s,\\ (a \cdot b)(s) &:= \sum_{k+l=s} a(k) \cdot b(l) = \sum_{k+l=s} a_k \cdot b_l,\end{aligned}$$

$(\forall s \in \mathbb{N}_0)\ \hat{0}(s) := 0$, zapisano kao niz $\hat{0} := (0, 0, 0, \ldots)$,
$\hat{1}(0) := 1$, $(\forall s \in \mathbb{N})\ \hat{1}(s) := 0$, kao niz $\hat{1} := (1, 0, 0, \ldots)$.

Napomena. Ako je $a = (a_0, a_1, \ldots, a_s, \ldots)$, $b = (b_0, b_1, \ldots, b_s, \ldots)$, onda je
$a + b = (a_0 + b_0, a_1 + b_1, \ldots, a_s + b_s, \ldots)$, $-a = (-a_0, -a_1, \ldots, -a_s, \ldots)$ i
$a \cdot b = (a_0 \cdot b_0,\ a_1 \cdot b_0 + a_0 \cdot b_1,\ \ldots,\ \sum_{k+l=s} a_k \cdot b_l, \ldots)$.

Lema 8.1 $(P^{\mathbb{N}_0}, +, \cdot, -, \hat{0}, \hat{1})$ je komutativan prsten sa jedinicom.

Δ. $(P^{\mathbb{N}_0}, +, -, \hat{0})$ je komutativna grupa, prema Lemi 7.1.

Asocijativnost množenja:

$$\begin{aligned}((a \cdot b) \cdot c)(s) &= \sum_{t+l=s} (a \cdot b)(t) \cdot c(l) = \sum_{t+l=s} \Big(\sum_{j+k=t} (a_j \cdot b_k)\Big) \cdot c_l\\ &= \sum_{t+l=s} \sum_{j+k=t} (a_j \cdot b_k) \cdot c_l = \sum_{j+k+l=s} a_j \cdot (b_k \cdot c_l)\\ &= \sum_{j+t=s} a_j \cdot \sum_{k+l=t} (b_k \cdot c_l) = \sum_{j+t=s} a(j) \cdot (b \cdot c)(t)\\ &= (a \cdot (b \cdot c))(s).\end{aligned}$$

Komutativnost množenja sledi neposredno iz definicije.

Jedinica: $(a \cdot \hat{1})(s) = \sum_{k+l=s} a_k \cdot \hat{1}_l = a_s \cdot \hat{1}_0 = a(s)$.

Distributivnost:

$$\begin{aligned}((a+b) \cdot c)(s) &= \sum_{k+l=s} (a+b)(k) \cdot c(l) = \sum_{k+l=s} (a_k + b_k) \cdot c_l\\ &= \sum_{k+l=s} (a_k \cdot c_l + b_k \cdot c_l) = \sum_{k+l=s} a_k \cdot c_l + \sum_{k+l=s} b_k \cdot c_l\\ &= (a \cdot c)(s) + (b \cdot c)(s) = (a \cdot c + b \cdot c)(s). \qquad \square\end{aligned}$$

Definicija 8.2 Neka je $\mathbb{P}$ komutativan prsten sa jedinicom 1, $\alpha \in P$, $\mathbb{P}^{\mathbb{N}_0} = (P^{\mathbb{N}_0}, +, \cdot, -, \hat{0}, \hat{1})$. Definišemo:

$P^{\mathbb{N}_0}_{fin} := \{\, a \in P^{\mathbb{N}_0} \;\mid\; (\exists n \in \mathbb{N})\,(\forall k > n)\;\; a_k := a(k) = 0 \,\}$,

$\widehat{\alpha} := (\alpha, 0, 0, 0, \ldots) \in P^{\mathbb{N}_0}_{fin}$ i $\widehat{P} := \{\, \widehat{\alpha} \mid \alpha \in P \,\}$,

$\mathrm{x} := (0, 1, 0, 0, \ldots) \in P^{\mathbb{N}_0}_{fin}$.

Lema 8.2 Neka su $\mathbb{P}$, $\mathbb{P}^{\mathbb{N}_0}$, $\alpha \in P$, x, $\widehat{\alpha}$, $\widehat{P}$, i $P^{\mathbb{N}_0}_{fin}$ kao gore. Tada:

a) $\widehat{\alpha + \beta} = \widehat{\alpha} + \widehat{\beta}$, $\widehat{-\alpha} = -\widehat{\alpha}$, $\widehat{\alpha \cdot \beta} = \widehat{\alpha} \cdot \widehat{\beta}$, $\widehat{0} = \hat{0}$, $\widehat{1} = \hat{1}$, pa pomoću funkcije $\widehat{\ }: P \to \widehat{P} : \alpha \mapsto \widehat{\alpha}$ poistovećujemo α i $\widehat{\alpha}$, P i $\widehat{P}$.

b) Za $k > 1$, $\mathrm{x}^k = (\underbrace{0, \ldots, 0}_{k \text{ nula}}, 1, 0, 0, \ldots)$, $\widehat{\alpha}\mathrm{x}^k = (\underbrace{0, \ldots, 0}_{k \text{ nula}}, \alpha, 0, 0, \ldots)$.

c) Ako je $a = (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots) \in P^{\mathbb{N}_0}_{fin}$, onda je
$a = (a_0, 0, 0, \ldots) + (0, a_1, 0, \ldots) + \cdots = \widehat{a}_0 + \widehat{a}_1\mathrm{x} + \widehat{a}_2\mathrm{x}^2 + \ldots + \widehat{a}_n\mathrm{x}^n$.
Primenom identifikacije iz a), imamo $a = a_0 + a_1\mathrm{x} + a_2\mathrm{x}^2 + \ldots + a_n\mathrm{x}^n$.

d) $P^{\mathbb{N}_0}_{fin}$ je zatvoren za sve operacije definisane u prstenu $\mathbb{P}^{\mathbb{N}_0}$, pa je u odnosu na njih i sam komutativan prsten sa jedinicom.

e) $P^{\mathbb{N}_0}_{fin}$ je najmanji prsten u $\mathbb{P}^{\mathbb{N}_0}$ koji sadrži prsten $\widehat{P}$ i element $\mathrm{x} := (0, 1, 0, 0, \ldots)$, primenom c). Poistovećujemo ga, koristeći c), sa
$\mathbb{P}[\mathrm{x}] := \{a_0 + a_1\mathrm{x} + a_2\mathrm{x}^2 + \ldots + a_n\mathrm{x}^n \mid n \geq 0,\; a_0, a_1, a_2, \ldots, a_n \in P\}$.

Δ. a) $\widehat{\alpha + \beta} = (\alpha + \beta, 0, 0, \ldots) = (\alpha, 0, 0, \ldots) + (\beta, 0, 0, \ldots) = \widehat{\alpha} + \widehat{\beta}, \ldots$.
b) Važi za $k = 1$, (BI). Neka je (IH): $\mathrm{x}^k(s) = \begin{cases} 1, & s = k; \\ 0, & s \neq k. \end{cases}$ Tada je

$\mathrm{x}^{k+1}(s) = \sum\limits_{j+l=s} \mathrm{x}^k(j)\mathrm{x}(l) = \begin{cases} 1 = \mathrm{x}^k(k)\mathrm{x}(1), & s = k+1; \\ 0, & s \neq k. \end{cases}$ Slično za $\widehat{\alpha}\mathrm{x}^k$.

d) Ako je $a_k = 0$ za $k > n$, i $b_l = 0$ za $l > m$, onda je $(-a)(k) = 0$ za $k > n$, $(a+b)(s) = 0$ za $s > \max(m, n)$, i $(ab)(s) = 0$ za $s > m + n$. $\square$