Osnove Algebre

Algebro ločimo na

- **klasično:** reševanje algebrajskih enačb, teorija števil
- **moderno:** raziskovanje algebrskih struktur

Obravnavali bomo:

1. grupoide, polgrupe, monoide, grupe
2. podgrupe, podgrupe edinke
3. ciklične končne, končne grupe
4. mreže
5. kolobarje, obsege, polja
6. polinome
7. teorija števil

Operacije

Naj bo $A \subseteq B$. Preslikava $f : A \times A \to B$ je **dvočlena operacija na** A.

Namesto $f(x, y)$ pišemo $x \cdot y$ oz. xy

Če je $\forall x, y \in A : x \cdot y \in A$, je f **notranja operacija v** A, množica A pa je za operacijo $\cdot$ **trdna** oz. **stabilna**.

Pogosto uporabljene operacije: $+$ seštevanje, $-$ odštevanje, $\cdot$ množenje, $/$ deljenje

Zgledi:

- $+$ je notranja operacija v $\mathbb{N}$;
- $-$ ni notranja operacija v $\mathbb{N}$;
- $-$ je operacija na $\mathbb{N}$ (vzamemo $A = \mathbb{N}$ in $B = \mathbb{Z}$);
- $-$ je notranja operacija v $\mathbb{Z}$.

Vprašanje 1 *Ali je deljenje notranja operacija?*

Odgovor:

Algebrske strukture

Štiri osnovne lastnosti

1. **notranjost**: če $\forall x, y \in A : x \cdot y \in A$;
2. **asociativnost**: $\forall x, y\, z \in A : x \cdot (y \cdot z) = (x \cdot y) \cdot z$;
3. **enota**: $e \in A$ je **enota**, če velja $\forall x \in A : x \cdot e = e \cdot x = x$;
4. **obrnljivost**: $x \in A$ je **obrnljiv**, če $\exists : y \in A : x \cdot y = y \cdot x = e$. Rečemo, da je y inverz x-a.

Algebrska struktura $(A, \cdot)$ je

- **grupoid**, če je $\cdot$ notranja operacija;
- **polgrupa**, če je $\cdot$ notranja in asociativna operacija;
- **monoid**, če je $\cdot$ notranja in asociativna operacija, obstaja enota;
- **grupa**, če je $\cdot$ notranja in asociativna operacija, obstaja enota, vsak element iz A je obrnljiv.

Algebrska struktura $(A, \cdot)$ je **komutativna** oz. **abelova**, če

$$\forall a, b \in A : a \cdot b = b \cdot a$$

Zgledi:

- $(\mathbb{R}, -)$ je grupoid;
- $(\mathbb{R}, +)$ je grupa;
- $(\mathbb{R}, \cdot)$ je monoid;
- $(\mathbb{R}^*, \cdot)$ za $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$;
- $(\mathbb{Z}_n, +_n)$ je grupa.

Naloga 1 *Kdaj je* $(\mathbb{Z}_n \setminus \{0\}, \cdot_n)$ *grupa?*

Velja:

- grupoid je polgrupa, če je $\cdot$ asociativna operacija;
- polgrupa je monoid, če ima operacija $\cdot$ enoto;
- monoid je grupa, če je vsak element iz A obrnljiv.

Vprašanje 2 *Kakšna algebrska struktura je* $(\{-1, 1\}, \cdot)$*?*

Odgovor:

Problem 1 *Naj bo* $Q\sqrt{2} = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$*. Ali je potem* $(Q\sqrt{2} \setminus \{0\}, \cdot)$ *grupa?*

Rešitev:

Trditev 1 *Grupoid* $(A, \cdot)$ *ima največ eno enoto.*

Dokaz: Recimo, da imamo dve enoti e_1, e_2. Obravnavajmo produkt $e_1 \cdot e_2$. Ker je e_1 enota, sledi $e_1 \cdot e_2 = e_2$. In, ker je e_2 enota, sledi $e_1 \cdot e_2 = e_1$. Torej $e_1 = e_2$.

□

Trditev 2 *V monoidu* $(A, \cdot)$ *ima vsak element največ en inverz.*

Dokaz: Recimo, da sta a', a'' inverza za a. Potem velja $a' \cdot a = a \cdot a' = e$ in $a'' \cdot a = a \cdot a'' = e$. Od tod velja:

$$a' = a' \cdot e = a' \cdot (a \cdot a'') = (a' \cdot a) \cdot a'' = e \cdot a'' = a''.$$

Torej velja $a' = a''$.

□

Potence v monoidu

Naj bo $(A, \cdot)$ monoid.

Potence elementa $a \in A$ definiramo takole:

$$a^0 = e, \quad a^1 = a, \quad a^n = a \cdot a \cdots a.$$

Velja:

$$a^n \cdot a^m = a^{n+m} \qquad \text{in} \qquad (a^n)^m = a^{nm}.$$

Inverz elementa $a \in A$ označimo z a^{-1} ter definiramo $a^{-n} = (a^{-1})^n$.

Kadar operacijo označimo s $+$, namesto o potencah govorimo o **večkratnikih**. V tem primeru enoto označimo z 0 ter večkratnike elementa $a \in A$ definiramo takole:

$$\begin{aligned} 0 \cdot a &= 0 \\ 1 \cdot a &= a \\ n \cdot a &= a + a + \cdots + a. \end{aligned}$$

Inverz elementa $a \in A$ označimo z $-a$ ter definiramo $(-n)a = n(-a)$.

Množico obrnljivih elementov iz A označimo z A^*.

Naloga 2 *Poišči $\mathbb{Z}_{12}^*$ za $(\mathbb{Z}_{12}, \cdot_{12})$, sestavi Cayleyevo tabelo za $(\mathbb{Z}_{12}^*, \cdot_{12})$ ter ugotovi kakšna je ta algebrska struktura.*

Trditev 3 *Naj bo* $(A, \cdot)$ *monoid. Potem,*

1. $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$;
2. *Če* $x, y \in A^*$, *potem* $x \cdot y \in A^*$;
3. $(A^*, \cdot)$ *je grupa.*

Dokaz: Prva trditev sledi takoj iz naslednjih dveh izpeljav:

$$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = (x \cdot (y \cdot y^{-1})) \cdot x^{-1} = (x \cdot e) \cdot x^{-1} = x \cdot x^{-1} = e$$

ter

$$(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = (y^{-1} \cdot (x \cdot x^{-1})) \cdot y = (y^{-1} \cdot e) \cdot y = x^{-1} \cdot x = e.$$

Posledica 4 *Algebrske strukure* $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, $(\{-1, 1\}, \cdot)$ *so grupe.*

Kongruenčne relacije

Naj bo $(A, \cdot)$ grupoid in R ekvivalenčna relacija v A.

V faktorski množici A/R želimo definirati operacijo $*$ takole:

$$R[x] * R[y] := R[x \cdot y] \tag{1}$$

Težava. Rezultat je lahko odvisen od izbire predstavnikov oz. operacija $*$ ni dobro definirana.

Definicija 1 *Ekvivalenčna relacija v grupoidu* $(A, \cdot)$ *je* **kongruenčna**, *če*

$$x\,R\,u \wedge y\,R\,v \;\Rightarrow\; x \cdot y\,R\,u \cdot v.$$

Trditev 5 *Če je* R *kongruenčna v* $(A, \cdot)$, *potem je operacija* $*$ *v* A/R *s predpisom iz* (1) *dobro definirana.*

Dokaz: Recimo $R[x] = R[u]$ in $R[y] = R[v]$ za poljubne x, y, u, v. Da bo operacija dobro definirana, mora veljati $R[x \cdot y] = R[u \cdot v]$.

Iz $R[x] = R[u]$ sledi $x\,R\,u$ ter iz $R[y] = R[v]$ sledi $y\,R\,v$. In ker je R kongurenčna, sledi $x \cdot y\,R\,u \cdot v$ in od tod $R[x \cdot y] = R[u \cdot v]$, kar je bilo potrebno pokazati. □

$(A/R, *)$ je **faktorski grupoid** za $(A, \cdot)$ glede na R.

Naloga 3 *Pokaži da je* $\equiv \pmod{12}$ *ekvivalenčna relacija v* $\mathbb{Z}$*. Kateri so ekvivalenčni razredi?*

Naloga 4 *Pokaži, da je* $\equiv \pmod{12}$ *kongruenčna relacija za grupo* $(\mathbb{Z}, +)$*. Kako definiramo operacijo* $*$*? Kakšna struktura je* $(\mathbb{Z}/ \equiv \pmod{12}, *)$*?*

Naloga 5 *Pokaži, da je* $\equiv \pmod{12}$ *kongruenčna relacija za monoid* $(\mathbb{Z}, \cdot)$*. Kako definiramo operacijo* $*$*? Kakšna struktura je* $(\mathbb{Z}/ \equiv \pmod{12}, *)$*?*

Izrek 6 *Naj bo R kongruenčna relacija v grupoidu $(A, \cdot)$. Potem velja*

1. $\cdot$ komutativna v $A \Rightarrow$ $*$ komutativna v A/R;

2. $\cdot$ asociativna v $A \Rightarrow$ $*$ asociativna v A/R;

3. e enota v $A \Rightarrow R[e]$ enota v A/R;

4. x obrnljiv v $A \Rightarrow R[x]$ obrnljiv v A/R in $R[x]^{-1} = R[x^{-1}]$.

Dokaz: Vsako trditev obravnavamo posebej:

1. $R[x] * R[y] = R[x \cdot y] = R[y \cdot x] = R[y] * R[x]$.

2. Izpeljimo:

$$\begin{aligned}(R[x] * R[y]) * R[z] &= R[x \cdot y] * R[z] = R[(x \cdot y) \cdot z] \\ &= R[x \cdot (y \cdot z)] = R[x] * (R[y] * R[z])\end{aligned}$$

3. Velja:

$$R[x] * R[e] = R[x \cdot e] = R[x] \quad \text{ter} \quad R[e] * R[x] = R[e \cdot x] = R[x].$$

Od tod sledi, da je $R[e]$ enota v A/R.

4. Velja:

$$R[x] * R[x^{-1}] = R[x \cdot x^{-1}] = R[e] \quad \text{ter} \quad R[x^{-1}] * R[x] = R[x^{-1} \cdot x] = R[e].$$

Od tod sledi, da je $R[x^{-1}]$ inverz za $R[x]$ v A/R, tj. $R[x]^{-1} = R[x^{-1}]$. □

Posledica 7 *Veljajo naslednje implikacije*

1. $(A, \cdot)$ je grupoid $\Rightarrow$ $(A/R, *)$ je grupoid;

2. $(A, \cdot)$ je polgrupa $\Rightarrow$ $(A/R, *)$ je polgrupa;

3. $(A, \cdot)$ je monoid $\Rightarrow$ $(A/R, *)$ je monoid;

4. $(A, \cdot)$ je grupa $\Rightarrow$ $(A/R, *)$ je grupa;

5. $(A, \cdot)$ je komutativna struktura $\Rightarrow$ $(A/R, *)$ je komutativna struktura.

Algebrska struktura $(\mathbb{Z}_m, +_m)$

$(\mathbb{Z}, +)$ je abelova grupa

$\equiv (\text{mod } m)$ je ekvivalenčna relacija v $\mathbb{Z}$

Faktorska množica $\mathbb{Z}/[\equiv (\text{mod } m)] = \{0, 1, \ldots, m-1\} = Z_m$

Velja

$$x \equiv u \pmod{m} \text{ in } y \equiv v \pmod{m} \Rightarrow x + y \equiv u + v \pmod{m}.$$

Torej $\equiv (\text{mod } m)$ je kongruenčna relacija v $(\mathbb{Z}, +)$.

Ustrezno operacijo $*$ v Z_m označimo s $+_m$ (seštevanje po modulu m)

Velja

$$x +_m y = (x + y) \pmod{m}$$

($x +_m y$ izračunamo tako, da seštejemo x in y, nato vzamemo ostanek pri deljenju z m)

Ker je $(\mathbb{Z}, +)$ abelova grupa, po posledici 7 sledi, da je $(\mathbb{Z}_m, +_m)$ abelova grupa.

Algebrska struktura $(\mathbb{Z}_m, \cdot_m)$

$(\mathbb{Z}, \cdot)$ je abelov monoid

Velja

$$x \equiv u \pmod{m} \text{ in } y \equiv v \pmod{m} \Rightarrow x \cdot y \equiv u \cdot v \pmod{m}.$$

Torej $\equiv \pmod{m}$ je kongruenčna relacija v $(\mathbb{Z}, \cdot)$.

Ustrezno operacijo $*$ v Z_m označimo z $\cdot_m$ (množenje po modulu m)

Velja

$$x \cdot_m y = (x \cdot y) \pmod{m}$$

($x \cdot_m y$ izračunamo tako, da zmnožimo x in y, nato vzamemo ostanek pri deljenju z m)

Ker je $(\mathbb{Z}, +)$ abelov monoid, po posledici 7 sledi, da je $(\mathbb{Z}_m, +_m)$ abelov monoid.

Algebrska struktura $(\mathbb{Z}_m^*, \cdot_m)$

$\mathbb{Z}_m^*$ je množica obrnljivih elementov iz $(\mathbb{Z}_m, \cdot_m)$. Potem, je $(\mathbb{Z}_m^*, \cdot_m)$ grupa.

Vprašanje 3 *Kateri elementi so v* $\mathbb{Z}_m^*$*?*

Velja,

$$a \in \mathbb{Z}_m^*, \text{ tj. } a \in \mathbb{Z}_m \text{ obrnljiv za } \cdot_m \Leftrightarrow$$

$$\exists x \in \mathbb{Z}_m : a \cdot_m x = 1 \Leftrightarrow$$

$$\exists x \in \mathbb{Z}_m : a \cdot x \equiv 1 \pmod{m} \Leftrightarrow$$

$$\exists x, y \in \mathbb{Z}_m : ax - 1 = my \Leftrightarrow$$

$$\exists x \in \mathbb{Z}_m : ax - my = 1 \Leftrightarrow$$

$$\gcd(a, m) = 1.$$

Torej,

$$\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m, a \perp m\} \quad \text{in} \quad |\mathbb{Z}_m^*| = \varphi(m).$$