

# Algebra 2

Luka Horjak ([lukahorjak@student.uni-lj.si](mailto:lukahorjak@student.uni-lj.si))

5. november 2021

# Kazalo

<b>Uvod</b>	<b>3</b>
<b>1 Osnovne algebrske strukture</b>	<b>4</b>
1.1 Linearne operacije . . . . .	4
1.2 Polgrupe in monoidi . . . . .	5
1.3 Grupe . . . . .	6
1.4 Kolobarji in polja . . . . .	7
1.5 Vektorski prostori in algebre . . . . .	8
1.6 Podstrukture . . . . .	9
1.7 Generatorji . . . . .	11
1.8 Direktni produkti in vsote . . . . .	12
<b>2 Primeri grup in kolobarjev</b>	<b>13</b>
2.1 Cela števila . . . . .	13
<b>Stvarno kazalo</b>	<b>14</b>

## 2 Primeri grup in kolobarjev

### 2.1 Cela števila

**Izrek 2.1.1** (Osnovni izrek o deljenju). Naj bo  $m \in \mathbb{Z}$  in  $n \in \mathbb{N}$ . Potem obstajata taki enolični števili  $q$  in  $r$ , za kateri je

$$m = qn + r \quad \text{in} \quad 0 \leq r < n.$$

*Dokaz.* Naj bo

$$S = \{k \in \mathbb{Z} \mid kn \leq m\}.$$

$S$  je navzgor omejena, zato ima največji element  $q$ , ki ustreza zgornjim pogojem.  $\square$

**Posledica 2.1.1.1.** Podmnožica  $H$  aditivne grupe  $\mathbb{Z}$  je podgrupa natanko tedaj, ko je  $H$  oblike  $n\mathbb{Z}$  za  $n \in \mathbb{N}_0$ .

*Dokaz.*  $n\mathbb{Z}$  je očitno grupa za vsak  $n$ , opazimo pa, da najmanjši naravni element  $H$  deli vse ostale.  $\square$

**Definicija 2.1.2.**  $d \in \mathbb{N}$  je *največji skupni delitelj* celih števil  $m$  in  $n$ , če  $d \mid n$ ,  $d \mid m$  in vsak skupni delitelj  $m$  in  $n$  deli tudi  $d$ . Označimo  $d = \gcd(m, n)$ .

**Trditev 2.1.3.** Naj bo  $G$  aditivna grupa in  $H, K \leq G$ . Potem je tudi

$$H + K = \{h + k \mid h \in H \wedge k \in K\}$$

podgrupa  $G$ .

*Dokaz.* The proof is obvious and need not be mentioned.  $\square$

**Posledica 2.1.3.1.** Za vse pare celih števil  $m$  in  $n$ , ki nista obe 0, obstaja enoličen največji skupni delitelj, ki je oblike

$$d = mx + ny$$

za neka  $x, y \in \mathbb{Z}$ .

*Dokaz.* Grupa  $n\mathbb{Z} + m\mathbb{Z}$  je grupa oblike  $d\mathbb{Z}$ .  $\square$

**Definicija 2.1.4.** Če je  $\gcd(m, n) = 1$  pravimo, da sta si  $m$  in  $n$  *tuji*.

**Lema 2.1.5** (Evklid). Naj bo  $p \in \mathbb{P}$  in  $m, n \in \mathbb{Z}$ . Potem velja

$$p \mid m \cdot n \implies p \mid n \vee p \mid m.$$

*Dokaz.* Če  $p \nmid m$ , je  $\gcd(p, m) = 1$ , zato obstajata taka  $x$  in  $y$ , da je

$$px + my = 1.$$

Sledi, da je

$$p \cdot \left( nx + \frac{mn}{p} \right) = n. \quad \square$$

# Stvarno kazalo

## C

Cela števila

Največji skupni delitelj, [13](#)

Tujost, [13](#)

## I

Izrek

Evklidova lema, [13](#)

Osnovni izrek o deljenju, [13](#)