FUNDAMENTALNI PRIKLADY PRO CVICENI 1-6

PARAGRAF 1: zakladni logicke pojmy a matemat. indukce

[1.1.B12b]Matematickou indukci dokazte, ze plati pro vsechna prirozena:

$$2^{n-1} \leq n! \tag{1}$$

DUKAZ:
Pro $n = 1$ plati $2^0 \leq 1!$, tedy $1 = 1$, coz plati. Predpokladejme tedy, ze tvrzeni plati pro $n-1$ (indukcni predpoklad), tedy $2^{n-2} \leq (n-1)!$. Dokazme, ze odtud plyne (1). Plati $n! = n(n-1)! \geq 2 \cdot 2^{n-2} = 2^{n-1}$. Nerovnost uvnitr je platna z indukcniho predpokladu a z toho, ze $n \geq 2$.

[1.1.B13]Necht n znaci libovolne prirozene cislo. Uvazme tvrzeni:

$$2 + 4 + 6 + \cdots + 2n = (n+2)(n-1). \tag{2}$$

Pak ukazte, ze:
a) uvedene tvrzeni neplati pro zadne prirozene n
b) uvedene tvrzeni lze 'dokazat' matematickou indukci, vynechame - li v ni 1. krok (tzn. vidime, ze 1. krok nelze pri dukazu matematickou indukci vypustit).
DUKAZ:
a) Staci si na leve strane rovnosti (2) povsimnout, ze soucet prvniho a posledniho, druheho a predposledniho je porad stejne cislo (napr. pro 2+4+6+8+10+12, je 2+12=14,4+10=14, 6+8=14 atd.), tedy obecne pro n liche bude soucet na leve strane rovnice (2) roven $(2+2n)\frac{n-1}{2} + \frac{2+2n}{2} = n^2 + n$, coz neni rovno $(n+2)(n-1)$. Pro n sude bude soucet take $(2+2n)\frac{n}{2} = n^2 + n$. Tim je dukaz dokoncen.
b) Pokud v matemat. indukci vynechame 1.krok, rovnost skutecne 'dokazeme', tedy necht tvrzeni plati pro $n-1$ (indukcni predpoklad) $2 + 4 + 6 + \cdots + 2(n-1) = (n+1)(n-2)$. Dokazeme, ze plati $2 + 4 + 6 + \cdots + 2n = (n+1)(n-2)$. Tedy musime dokazat $(n+1)(n-2) + 2n = (n+2)(n-1)$, coz je $n^2 + n - 2 = n^2 + n - 2$. Dukaz timto zpusobem je ale nespravny, protoze jsme prave vynechali prvni krok.

[1.1.B15]Posloupnost prirozenych cisel $u_1, u_2, u_3, \ldots$ je definovana rekuretne takto:

$$u_1 = 1, u_2 = 1, u_{n+2} = u_{n+1} + u_n \text{ pro } n \geq 1$$

(tato posloupnost se nazyva Fibonacciho posloupnost a jeji cleny se nazyvaji Fibonacciho cisla). Dokazte, ze plati:

$$u_{n+s} = u_{n-1} \cdot u_s + u_n \cdot u_{s+1} \text{ pro } \forall n \geq 2 \text{ cele }, \forall s \in \mathbb{N}.$$

(Navod: dukaz vedte matematickou indukci vzhledem k s.)
DUKAZ:
Pro $s = 1$ dostavame $u_{n+1} = u_{n-1} \cdot u_1 + u_n \cdot u_2$, kde $u_1 = 1, u_2 = 1$, tedy $u_{n+1} = u_{n-1} + u_n$, coz je Fibonacciho posloupnost.

Predpokladejme, ze rovnost plati pro $s-1$, tedy plati, ze $u_{n+s-1} = u_{n-1} \cdot u_{s-1} + u_n \cdot u_s$ (indukcni predpoklad). Dokazme, ze odtud plyne $u_{n+s} = u_{n-1} \cdot u_s + u_n \cdot u_{s+1}$. Predevsim plati, ze $u_{n+s} = u_{n+s-1} + u_{n+s-2}$. Dosadme z indukcniho predpokladu za u_{n+s-1}, u_{n+s-2} a pocitejme. $u_{n+s} = u_{n+s-1} + u_{n+s-2} = u_{n-1} \cdot u_{s-1} + u_n \cdot u_s + u_{n-1} \cdot u_{s-2} + u_n \cdot u_{s-1} = u_{n-1} \cdot (u_{s-1} + u_{s-2}) + u_n \cdot (u_s + u_{s-1}) = u_{n-1} \cdot u_s + u_n \cdot u_{s+1}$, a dukaz je dokoncen.

PARAGRAF 2: zakladni mnozinove pojmy

[1.2.B3] Necht $A_n, B_n (n \in \mathbb{N})$ jsou mnoziny, splnujici podminky:

$$A_n \supseteq A_{n+1}, B_n \supseteq B_{n+1} \text{ pro kazde } n \in \mathbb{N}. \tag{3}$$

Potom:
a) dokazte, ze $\bigcap_{n=1}^{\infty}(A_n \cup B_n) = \bigcap_{n=1}^{\infty} A_n \cup \bigcap_{n=1}^{\infty} B_n$
b) ukazte, ze predchozi rovnost neplati, vynechame-li predpoklad (3).
Navod: Dukaz $\subseteq$ vedte neprimo.
DUKAZ:
a) Nejdrive dokazme $\bigcap_{n=1}^{\infty}(A_n \cup B_n) \supseteq \bigcap_{n=1}^{\infty} A_n \cup \bigcap_{n=1}^{\infty} B_n$, tedy (z definice podmnoziny) $x \in (\bigcap_{n=1}^{\infty} A_n \cup \bigcap_{n=1}^{\infty} B_n) \Rightarrow x \in \bigcap_{n=1}^{\infty}(A_n \cup B_n)$. Necht $x \in (\bigcap_{n=1}^{\infty} A_n \cup \bigcap_{n=1}^{\infty} B_n) \Rightarrow (x \in \bigcap_{n=1}^{\infty} A_n) \vee (x \in \bigcap_{n=1}^{\infty} B_n) \Rightarrow (\forall n : x \in A_n) \vee (\forall n : x \in B_n) \Rightarrow \forall n : (x \in A_n \vee x \in B_n) \Rightarrow \forall n : x \in (A_n \cup B_n) \Rightarrow x \in (\bigcap_{n=1}^{\infty}(A_n \cup B_n)$, coz jsme meli dokazat.

Nyni dokazme $\bigcap_{n=1}^{\infty}(A_n \cup B_n) \subseteq \bigcap_{n=1}^{\infty} A_n \cup \bigcap_{n=1}^{\infty} B_n$, tedy $x \in \bigcap_{n=1}^{\infty}(A_n \cup B_n) \Rightarrow x \in (\bigcap_{n=1}^{\infty} A_n \cup \bigcap_{n=1}^{\infty} B_n)$, ale neprimo. Budeme tedy dokazovat: $x \notin (\bigcap_{n=1}^{\infty} A_n \cup \bigcap_{n=1}^{\infty} B_n) \Rightarrow x \notin \bigcap_{n=1}^{\infty}(A_n \cup B_n)$. Postupne dostavame $x \notin (\bigcap_{n=1}^{\infty} A_n \cup \bigcap_{n=1}^{\infty} B_n) \Rightarrow (x \notin \bigcap_{n=1}^{\infty} A_n) \wedge (x \notin \bigcap_{n=1}^{\infty} B_n) \Rightarrow (\exists k : x \notin A_k) \wedge (\exists l : x \notin B_l) \Rightarrow$(diky podmince (3) nyni najdeme spolecny index $m =$max(k, l) tak, ze)$\Rightarrow \exists m : (x \notin A_m) \wedge (x \notin B_m) \Rightarrow \exists m : x \notin (A_m \cup B_m) \Rightarrow x \notin \bigcap_{n=1}^{\infty}(A_n \cup B_n)$, coz jsme meli dokazat.

b) Kdybychom nepredpokladali (3) nebylo by mozne nalezt spolecny index m, a tak pokracovat v dalsich implikacich. Na prikladu si skutecne overte, ze index m za danych podminek lze nalezt.

[1.2.B7b] Dokazte, ze plati: $A \div C = B \div C \Rightarrow A = B$.
DUKAZ:
Dokazujme neprimo tedy $A \neq B \Rightarrow A \div C \neq B \div C = ((A - C) \cup (C - A)) \neq ((B - C) \cup (C - B))$. S nerovnosti mnozin A a B plyne existence prvku x, ktery je v A a neni v B (pripadne obracene, ale to je jen otazka znaceni), tedy $\exists x : x \in A \wedge x \notin B$. Nyni mohou nastat dve moznosti, bud $x \in C$, anebo $x \notin C$. Necht $x \in C$, pak $x \notin (A - C) \wedge x \notin (C - A)$, ale $x \notin (B - C) \wedge x \in (C - B)$, tedy plati, ze $((A - C) \cup (C - A)) \neq ((B - C) \cup (C - B))$. Pokud $x \notin C$, pak $x \in (A - C) \wedge x \notin (C - A)$, ale $x \notin (B - C) \wedge x \notin (C - B)$, tedy opet plati, ze $((A - C) \cup (C - A)) \neq ((B - C) \cup (C - B))$. Tim je dukaz ukoncen.

[1.2.B14a]Necht A, B, C, D jsou mnoziny. Dokazte, ze plati:
$(A \cup B) \times (C \cup D) = (A \times C) \cup (A \times D) \cup (B \times C) \cup (B \times D)$.
DUKAZ:
Primo, obe implikace. Necht $[x, y] \in ((A \cup B) \times (C \cup D)) \Leftrightarrow$ (definice kartezkeho soucinu) $\Leftrightarrow (x \in (A \cup B)) \wedge (y \in (C \cup D)) \Leftrightarrow$
$((x \in A) \vee (x \in B)) \wedge ((y \in C) \vee (y \in D)) \Leftrightarrow$
$(((x \in A) \vee (x \in B)) \wedge (y \in C)) \vee (((x \in A) \vee (x \in B)) \wedge (y \in D)) \Leftrightarrow$
$((x \in A) \wedge (y \in C)) \vee ((x \in B) \wedge (y \in C)) \vee ((x \in A) \wedge (y \in D)) \vee ((x \in B) \wedge (y \in D)) \Leftrightarrow$
(definice kartezkeho soucinu)
$\Leftrightarrow [x, y] \in (A \times C) \cup (B \times C) \cup (A \times D) \cup (B \times D)$, a tim je dukaz ukoncen.

PARAGRAF 3: zakladni vlastnosti celych cisel

[1.3.B5b] Necht m je prirozene cislo; $a, b, c \in \mathbb{Z}$. Dokazte, ze plati:

$$a \equiv b(\text{mod } m) \wedge b \equiv c(\text{mod } m) \Rightarrow a \equiv c(\text{mod } m).$$

DUKAZ:
Dukaz povedeme primo, tedy predpoklad rika, ze existuji $q_1, q_2 \in \mathbb{Z}$ tak, ze $(b = q_1 m + a) \wedge (c = q_2 m + b)$, a mame dokazat, ze odtud plyne existence $q_3 \in \mathbb{Z}$, ze $c = q_3 m + a$. Z predpokladu plyne, ze $c = q_2 m + b = q_2 m + q_1 m + a = (q_2 + q_1)m + a$, tedy $q_3 = q_1 + q_2$, a protoze soucet celych cisel je opet cele cislo, je existence q_3 dokazana, a tim dukaz ukoncen. (Zkuste si priklad).

PARAGRAF 5: zobrazeni

[1.5.B9c]Necht $f : A \rightarrow B$, $g : B \rightarrow C$ jsou zobrazeni. Dokazte, ze plati:

$$g \circ f \text{ je injektivni} \Rightarrow f \text{ je injektivni.}$$

DUKAZ:
Z definice injektivity plati, ze pro $\forall x_1, x_2 \in D_f, x_1 \neq x_2 \Rightarrow g(f(x_1)) \neq g(f(x_2))$. To je predpoklad, tedy chceme dokazat, ze $(\forall x_1, x_2 \in D_f, x_1 \neq x_2 \Rightarrow g(f(x_1)) \neq g(f(x_2))) \Rightarrow (\forall x_1, x_2 \in D_f, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2))$. To ale musi vzdy platit, protoze pokud by platilo, ze $f(x_1)) = f(x_2)$ a soucastne $x_1 \neq x_2$, pak by jediny bod $f(x_1) = f(x_2)$ byl zobrazen na dve funkcni hodnoty $g(f(x_1)), g(f(x_2))$, coz je spor s predpokladem, ze g je zobrazeni.

[1.5.B10b] Necht $f : A \rightarrow B$ je zobrazeni. Dokazte, ze plati:

$$f \text{ je surjektivni} \Leftrightarrow \text{existuje zobrazeni } h : B \rightarrow A \text{ tak, ze } f \circ h = id_B$$

(Navod: pri dukazu '$\Rightarrow$' hledane zobrazeni h primo zkonstruujte).
DUKAZ:
Nejdriv '$\Leftarrow$'. Z existence zobrazeni $h : B \rightarrow A$ takoveho, ze $f \circ h = id_B$ je nutno dokazat surjektivitu f, tedy ze pro $\forall y \in B \exists x \in A : f(x) = y$. Pokud ale takove zobrazeni h existuje, pak symbolicky lze psat $h(B) \subseteq A$ a $f(h(B)) = B$, tedy zobrazeni f je jiste surjektivni.
Nyni '$\Rightarrow$'. Predpokladejme, ze f je surjektivni a zkonstruujeme zobrazeni h s pozadovanymi vlastnostmi. Uvedomme si, ze surjektivita f znamena, ze vsechny prvky v B musi mit svuj vzor, a protoze f je zobrazeni musi byt v A vsechny prvky zobrazeny. Pokud by tedy f byla bijekce, h bychom zkonstruovali tak, ze pokud $b = f(a)$, tak $h(b) = a$, tedy h by byla inverze k f. Dejme tomu, ze f neni bijekce. Pak se aspon dva prvky z A musi zobrazit na jeden prvek z B. Zobrazeni h pak zkonstuujeme tak, ze pro $a_1 \neq a_2 \in A : f(a_1) = f(a_2) = b$ bude $h(b) = a_1$, kde a_1 je zvoleno pevne. O a_2 se jiz nemusime starat. Pro $\forall b \in B$ bude platit $h(b) = a_1$ a $f(a_1) = b$, tedy $f(h(b)) = b$, tedy $f \circ h$ je identita na B.

PARAGRAF: komplexni cisla

Dokazte $\cos(\alpha \pm \beta) = \cos(\alpha)\cos(\beta) \mp \sin(\alpha)\sin(\beta)$ a $\sin(\alpha \pm \beta) = \sin(\alpha)\cos(\beta) \pm \cos(\alpha)\sin(\beta)$.
DUKAZ:
Obecne plati $(a_1 + ia_2)(b_1 + ib_2) = (a_1 b_1 - a_2 b_2) + i(a_2 b_1 + a_1 b_2)$n a take obecne plati

$(\cos(\alpha) + i\sin(\alpha))(\cos(\beta) + i\sin(\beta)) = \cos(\alpha+\beta) + i\sin(\alpha+\beta)$.

Nyni dosadme za $a_1 = \cos(\alpha), a_2 = \sin(\alpha), b_1 = \cos(\pm\beta) = \cos(\beta), b_2 = \sin(\pm\beta) = \pm\sin(\beta)$. Dostaneme $\cos(\alpha\pm\beta) + i\sin(\alpha\pm\beta) = \cos(\alpha)\cos(\pm\beta) - \sin(\alpha)\sin(\pm\beta) + i(\sin(\alpha)\cos(\pm\beta) + \cos(\alpha)\sin(\pm\beta)) = \cos(\alpha)\cos(\beta) \mp \sin(\alpha)\sin(\beta) + i(\sin(\alpha)\cos(\beta) \pm \cos(\alpha)\sin(\beta))$ a porovnanim realnych a komplexnich casti vyrazu na zacatku a konci rovnice dostavame tvrzeni.

PARAGRAF 6: usporadane mnoziny

[Priklad] Dokazte, ze $\liminf a_n \leq \limsup a_n$.
DUKAZ:
Mejme posloupnost prvku a_n a oznacme $c_n = \inf\{a_k, k \geq n\}$ a $d_n = \sup\{a_k, k \geq n\}$. Infimum je podle definice nejvetsi horni zavora, supremum nejmensi dolni zavora. Pro vsechna n tedy plati, ze $c_n \leq d_n$ a podle vety o limitach musi platit, ze $\lim_{n\to\infty} c_n \leq \lim_{n\to\infty d_n}$, z cehoz plyne tvrzeni.

Jeste lepe je to patrne na priklade. Mejme posloupnost $a_n = (-1)^n \frac{1}{n}$. Posloupnost hornich zavor je
$d_1 = \sup\{-\frac{1}{1}, \frac{1}{2}, -\frac{1}{3}, \frac{1}{4}, -\frac{1}{5}, \frac{1}{6}, \dots\} = \frac{1}{2}$
$d_2 = \sup\{\frac{1}{2}, -\frac{1}{3}, \frac{1}{4}, -\frac{1}{5}, \frac{1}{6}, \dots\} = \frac{1}{2}$
$d_3 = \sup\{-\frac{1}{3}, \frac{1}{4}, -\frac{1}{5}, \frac{1}{6}, \dots\} = \frac{1}{4}$
$d_4 = \sup\{\frac{1}{4}, -\frac{1}{5}, \frac{1}{6}, \dots\} = \frac{1}{4}$
$d_5 = \sup\{-\frac{1}{5}, \frac{1}{6}, \dots\} = \frac{1}{6}$
a dolnich zavor je
$c_1 = \inf\{-\frac{1}{1}, \frac{1}{2}, -\frac{1}{3}, \frac{1}{4}, -\frac{1}{5}, \frac{1}{6}, \dots\} = -\frac{1}{1}$
$c_2 = \inf\{\frac{1}{2}, -\frac{1}{3}, \frac{1}{4}, -\frac{1}{5}, \frac{1}{6}, \dots\} = -\frac{1}{3}$
$c_3 = \inf\{-\frac{1}{3}, \frac{1}{4}, -\frac{1}{5}, \frac{1}{6}, \dots\} = -\frac{1}{3}$
$c_4 = \inf\{\frac{1}{4}, -\frac{1}{5}, \frac{1}{6}, \dots\} = -\frac{1}{5}$
$c_5 = \inf\{-\frac{1}{5}, \frac{1}{6}, \dots\} = -\frac{1}{5}$

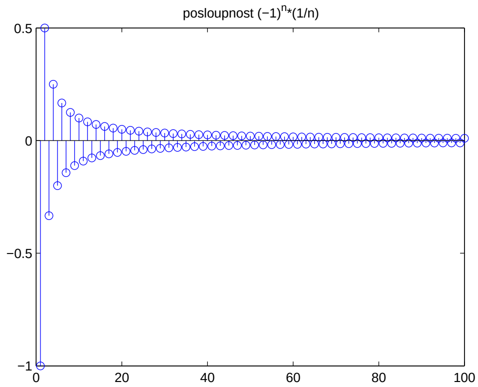

Figure 1:

Vsimnete si zajimave skutecnosti, ze infimum (minimum) zmensujici se mnoziny se muze jen zvetsovat, zatimco supremum (maximum) zmensujici se mnoziny se muze jen zmensovat. Z obrazku je take patrne, ze $\lim_{n\to\infty} a_n = 0$.

PARAGRAF 7: ekvivalence a rozklady

PARAGRAF 8: zakladni algebraicke struktury

[Priklad 2.76a] Dokazte, ze algebraicke struktury $(\mathbb{Z}, +, \cdot, 0, 1) \subset (\mathbb{Q}, +, \cdot, 0, 1) \subset (\mathbb{R}, +, \cdot, 0, 1) \subset (\mathbb{C}, +, \cdot, 0, 1)$ jsou do sebe vnorene obory integrity, z nichz posledni tri jsou dokonce pole nekonecne charakteristiky.
DUKAZ: Nejprve zopakujme vlastnosti oboru integrity (treba pro $(\mathbb{Z}, +, \cdot, 0, 1)$).
1. $(\mathbb{Z}, +, 0)$ je abelovska grupa, tedy
- 1a. $(\mathbb{Z}, +)$ je grupoid
- 1b. existuje jednotkovy prvek
- 1c. ke kazdemu prvku v $a \in \mathbb{N}$ existuje inverzni prvek a^{-1}
2. $(\mathbb{Z}, \cdot)$ je pologrupa
3. plati distributivni zakony, tedy pro libovolne a, b, c : $(a + b) \cdot c = a \cdot c + b \cdot c$ a

$c \cdot (a+b) = c \cdot a + c \cdot b$
4. $(\mathbb{Z}, \cdot, 1)$ monoid
5. $(\mathbb{Z}, \cdot)$ musi byt komutativni pologrupa
6. neexistuje delitel nuly

Jednotlive vlastnosti dokazme pro $(\mathbb{Z}, +, \cdot, 0, 1)$.
1a. pro $\forall a, b \in \mathbb{Z} : a + b \in \mathbb{Z}$ a je urceno jednoznacne
1b. musi existovat $e \in \mathbb{Z}$ tak, ze $\forall a \in \mathbb{Z} : a + e = e + a = a$, skutecne je to $e = 0$
1c. pro $\forall a \in \mathbb{Z}$ musi existovat $a^{-1} \in \mathbb{Z}$ tak, ze $a + a^{-1} = a^{-1} + a = e$, skutecne je to $a^{-1} = -a$
2. operace $+$ musi byt v $(\mathbb{Z}, +)$ asociativni, tedy pro $\forall a, b, c \in Z : a+(b+c) = (a+b)+c$, coz skutecne plati
3. pro cela cisla plati distributivni zakony
4. operace $\cdot$ musi byt asociativni (plati $\forall a, b, c \in Z : a \cdot (b \cdot c) = (a \cdot b) \cdot c$), navic musi existovat $e \in \mathbb{Z}$ tak, ze $\forall a \in \mathbb{Z} : a \cdot e = e \cdot a = a$, skutecne je to $e = 1$
5. pro $\forall a, b, c \in \mathbb{Z} : a \cdot (b \cdot c) = (a \cdot b) \cdot c$ a $a \cdot b = b \cdot a$, coz pro cela cisla plati
6. nesmi v $\mathbb{Z}$ existovat $a \neq 0, b \neq 0$ tak, aby $a \cdot b = 0$, coz pro cela cisla plati.
Z 1.-6. plyne, ze $(\mathbb{Z}, +, \cdot, 0, 1)$ je obor integrity. Neni to ale pole, protoze $(\mathbb{Z}, +, \cdot, 0, 1)$ je sice okruh s jednotkou, ale $(\mathbb{Z} - \{0\} \cdot, 1)$ neni abelovska grupa (v mnozine celych cisel nejsou inverzni prvky vzhledem k nasobeni, to jsou totiz pro cela cisla uz zlomky).

Pro ostatni algebraicke struktury $(\mathbb{Q}, +, \cdot, 0, 1) \subset (\mathbb{R}, +, \cdot, 0, 1) \subset (\mathbb{C}, +, \cdot, 0, 1)$ plati, ze jsou komutativnim telesem, takze to jsou pole. Je take jasne, ze maji nekonecnou charakteristiku ($(\mathbb{Z}, +, \cdot, 0, 1)$ ma take nekonecnou charakteristiku, ale pouze jako obor integrity). Pro zadne prirozene n z techto mnozin totiz neplati, ze $n \cdot 1 = 0$.

[Priklad 2.76b] $(\mathbb{Z}_N, \oplus, \odot, 0, 1)$ je komutativnim okruhem s jednotkou, ktery neni podokruhem zadneho z okruhu v prikladu 2.76a. $(\mathbb{Z}_N, \oplus, \odot, 0, 1)$ je oborem intergrity, jen kdyz N je prvocislo. Pak je to dokonce pole.
DUKAZ:
1. Dokazme, ze $(\mathbb{Z}_N, \oplus, \odot, 0, 1)$ je komutativnim okruhem s jednotkou. Mnozina $\mathbb{Z}_N = \{0, 1, \ldots, N-1\}$ je mnozina cisel, ktere vzniknou jako zbytky po deleni celeho cisla cislem N. Dokazujeme pro tuto mnozinu vlastnosti z prikladu 2.76a.
1a. pro $\forall a, b \in \mathbb{Z}_N : a \oplus b \in \mathbb{Z}_N$ a je urceno jednoznacne
1b. musi existovat $e \in \mathbb{Z}_N$ tak, ze $\forall a \in \mathbb{Z}_N : a \oplus e = e \oplus a = a$, skutecne je to $e = 0$
1c. pro $\forall a \in \mathbb{Z}_N$ musi existovat $a^{-1} \in \mathbb{Z}_N$ tak, ze $a \oplus a^{-1} = a^{-1} \oplus a = e$, skutecne je to $a^{-1} = N - a$
2. operace $\oplus$ musi byt v $(\mathbb{Z}_N, \oplus)$ asociativni, tedy pro $\forall a, b, c \in Z_N : a \oplus (b \oplus c) = (a \oplus b) \oplus c$, coz skutecne plati
3. pro cisla ze $\mathbb{Z}_N$ plati distributivni zakony
4. operace $\odot$ musi byt asociativni (plati $\forall a, b, c \in Z_N : a \odot (b \odot c) = (a \odot b) \odot c$, navic musi existovat $e \in \mathbb{Z}_N$ tak, ze $\forall a \in \mathbb{Z}_N : a \odot e = e \odot a = a$, skutecne je to $e = 1$
5. pro $\forall a, b, c \in \mathbb{Z}_N : a \odot (b \odot c) = (a \odot b) \odot c$ a $a \odot b = b \odot a$

Nektere rovnice nejsou primo videt, pomuzeme si tedy prikladem pro $\mathbb{Z}_3 = \{0, 1, 2\}$.
ad 1a. $0 \oplus 0 = 0, 0 \oplus 1 = 1, 0 \oplus 2 = 2, 1 \oplus 1 = 2, 1 \oplus 2 = 0, 2 \oplus 2 = 1$, tedy 1a plati
ad 1b. zrejme
ad 1c. $0 \oplus 3 = 0, 1 \oplus 2 = 0, 2 \oplus 1 = 0, 3 \oplus 0 = 0$, tedy 1c plati

ad 2 $(1 \oplus 2) \oplus 2 = 2 = 1 \oplus (2 \oplus 2)$ napriklad, plati i pro ostatni
ad 3 $0 = 2 \odot (1 \oplus 2) = (2 \odot 1) \oplus (2 \odot 2) = 2 \oplus 1 = 0$ napriklad
ad 4 $1 = 2 \odot (2 \odot 1) = (2 \odot 2) \odot 1 = 1$ napriklad, dale $a \odot 1 = a$
ad 5 overeno ve ad4 a dale $2 = 2 \odot 1 = 1 \odot 2 = 2$

2. $(\mathbb{Z}_N, \oplus, \odot, 0, 1)$ nemuze byt podokruh, protoze $(\mathbb{Z}_N, \oplus)$ neni dokonce ani podgrupoid $(\mathbb{Z}, +)$. Pro $(\mathbb{Z}_N, +)$ plati, ze $+$ neni operace, napr. pro $\mathbb{Z}_3$ bude $2 + 2 = 4 \notin \mathbb{Z}_3$.

3. $(\mathbb{Z}_N, \oplus, \odot, 0, 1)$ je oborem intergrity jen kdyz N je prvocislo. Overme si, ze kdyz N je provocislo, pak neexistuje delitel 0, tedy nesmi v $\mathbb{Z}_N$ existovat $a \neq 0, b \neq 0$ tak, aby $a \cdot b = 0$. Nejlepe na priklade. Pro $\mathbb{Z}_3 = \{0, 1, 2\}$ vzdy je $1 \odot 1 = 1 \neq 0, 2 \odot 1 = 2 \neq 0$, ale pro $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ je napriklad $2 \odot 2 = 0$, takze to neni obor integrity.

4. Podle chytre vety plati, ze kazdy konecny obor integrity je pole. (Overte si to ale na tomto priklade detailne).

PARAGRAF 9: vektorove prostory, podprostory, prime soucty prostoru, baze a dimenze prostoru

[3.1.B8] Necht V_1 a V_2 jsou vektorove prostory na ciselnym telesem T. Pro libovolne (u_1, u_2), $(v_1, v_2) \in V_1 \times V_2$ a $t \in T$ definujeme:

$$(u_1, u_2) + (v_1, v_2) = (u_1 + v_1, u_2 + v_2) \text{ resp. } t(u_1, u_2) = (tu_1, tu_2).$$

Dokazte, ze pak je $V_1 \times V_2$ je vektorovy prostor nad T.
DUKAZ:
Postupujeme podle definice vektoroveho prostoru. Zrejme plati, ze $t(u_1, u_2) = (tu_1, tu_2) \in V_1 \times V_2$. Dale $(V_1 \times V_2, +, 0)$ musi byt abelovska grupa. Skutecne $(u_1 + v_1, u_2 + v_2) \in V_1 \times V_2$, protoze V_1 a V_2 jsou vektorove prostory, jednotkovy a opacny prvek ve $V_1 \times V_2$ rovnez musi existovat. Staci poskladat do usporadane dvojice jednotkove a opacne prvky z jednotlivych V_1 a V_2. Nakonec overme distributivni zakon vzhledem ke scitani vektoru (ostatni jsou analogice).

$$\begin{gathered} t((u_1, u_2) + (v_1, v_2)) = t(u_1 + v_1, u_2 + v_2) = (t(u_1 + v_1), t(u_2 + v_2)) = \\ (tu_1 + tv_1, tu_2 + tv_2) = (tu_1, tu_2) + (tv_1, tv_2) = t(u_1, u_2) + t(v_1, v_2). \end{gathered}$$

Prvni rovnost je dana definici scitani ve $V_1 \times V_2$, druha je dana definici nasobeni skalarem ve $V_1 \times V_2$, treti je dana distributivnim zakonem vzhledem ke scitani vektoru v jednotlivych V_1 a V_2, ctvrta je dana opet definici scitani ve $V_1 \times V_2$, pata je dana definici nasobeni skalarem ve $V_1 \times V_2$.
Dodejme, ze tento priklad ma velky teoreticky vyznam, protoze rika, ze kartezky soucin vektorovych prostoru je opet vektorovym prostorem ovsem vetsi dimenze.

[3.2.B4] Rozhodnete, zda podmnozina $W \subseteq \mathbb{R}^n$ je podprostorem vektoroveho prostoru $\mathbb{R}^n$, je-li

$$W = \{(x_1, x_2, \ldots, x_n) \,|x_1 + x_2 + \cdots + x_n = 0\}.$$

DUKAZ:
Musi ve W lezet nulovy prvek $(0, 0, \ldots, 0)$, coz plati, protoze $0 + 0 + \cdots + 0 = 0$, zbyva

overit, jestli pro libovolne $a, b \in \mathbb{R}$ a libovolne $(x_1, x_2, \dots, x_n), (y_1, y_2, \dots, y_n) \in W$, plati $a(x_1, x_2, \dots, x_n) + b(y_1, y_2, \dots, y_n) \in W$. Pocitejme tedy $a(x_1, x_2, \dots, x_n) + b(y_1, y_2, \dots, y_n) = (ax_1, ax_2, \dots, ax_n) + (by_1, by_2, \dots, by_n) = (ax_1 + by_1, ax_2 + by_2, \dots, ax_n + by_n)$. Musime dokazat, ze $ax_1 + by_1 + ax_2 + by_2 + \dots + ax_n + by_n = 0$. To ale plati, pokud vytkneme a, b a dosadime za $x_1 + x_2 + \dots + x_n = 0$ a $y_1 + y_2 + \dots + y_n = 0$.

[3.2.B16b] Ve vektorovem prostoru V jsou dany podprostory W_1 a W_2. Rozhodnete, zda soucet $W_1 + W_2$ je primym souctem, je-li:
$V = \mathbb{R}^3$, $W_1 = \{(x, y, z) | x - 2y - 3z = 0\}$, $W_2 = \{(x, y, z) | x = z\}$.
DUKAZ:
Aby prostor V byl primym souctem prostoru W_1 a W_2, musi byt prunikem W_1 a W_2 pocatek a soucet dimenzi prostoru W_1 a W_2 musi dat dimenzi V. To ale v tomto pripade neplati, protoze W_1 je rovina v trojrozmernem prostoru s normalovym vektorem $(1, -2, -3)$ a W_2 je rovina v trojrozmernem prostoru s normalovym vektorem $(1, 0, -1)$. Jde tedy o ruznobezne roviny v trojrozmernem prostoru, a ty musi mit za spolecny prunik primku. Navic soucet dimenzi rovin $2 + 2 = 4$, coz neni tri.

[3.3.B14] Ve vektorovem prostoru $\mathbb{R}^{\mathbb{R}}$ (scitani funkci je dano jako soucet funkcnich hodnot v jednotlivych argumentech a nasobeni funkce skalarem jako soucin skalaru a jednotlivych funkcnich hodnot) jsou dany vektory (tj. zobrazeni $\mathbb{R} \to \mathbb{R}$) f, g, h. Dokazte, ze vektory f, g, h jsou linearne zavisle. Pritom:

$$f = \sin x,\ g = \cos x,\ h = \cos(x + \frac{\pi}{3}).$$

DUKAZ:
Linearni zavislost tri vektoru znamena, ze aspon jeden z nich lze vyjadrit jako linearni kombinaci ostatnich, tedy musi existovat $a, b \in \mathbb{R}$ tak, ze napr. $af + bg = h$. Pocitejme $a \sin x + b \cos x = \cos x \cos \frac{\pi}{3} - \sin x \sin \frac{\pi}{3} = \cos(x + \frac{\pi}{3})$. Odtud plyne, ze $a = -\frac{\sqrt{3}}{2}$ a $b = \frac{1}{2}$, takze vektory jsou linearne zavisle.

[3.4.B6] Naleznete bazi a dimenzi vektoroveho prostoru V, je-li: $V = \mathbb{K} \times \mathbb{K}$, nad tlesem $\mathbb{R}$. Scitani a nasobeni vektoru cislem je definovano po slozkach.
RESENI:
Musime umet vyjadrit jakoukoliv usporadanou dvojici $(a + bi, c + di)$. To muzeme naprikad tak, ze $a(1, 0) + b(i, 0) + c(0, 1) + d(0, i) = (a + bi, c + di)$. Dimenze je tedy 4 a bazi tvori 4 vektory $(1, 0), (i, 0), (0, 1), (0, i)$.