2. Tělesa

Buď v následujícím $n > 1$ přirozené číslo a položme $\mathbf{Z}_n = \{0, 1, \dots, n-1\}$. Nyní definujme na $\mathbf{Z}_n$ operace $+_n$ a $\cdot_n$ předpisem $a +_n b = (a+b) \bmod n$ a $a \cdot_n b = (a \cdot b) \bmod n$, kde mod n znamená zbytek po celočíselném dělení hodnotou n.

2.1. Ověřte, že pro všechna celá a, b a libovolné přirozené n platí, že $((a) \bmod n + (b) \bmod n) \bmod n = (a+b) \bmod n$ a $((a) \bmod n \cdot (b) \bmod n) \bmod n = (a \cdot b) \bmod n$.

Zvolme libovolně celá a, b a přirozené n. Předně si rozmyslíme význam zbytku po celočíselném dělení, tedy, že existují (jednoznačně určená) celá q a r, pro něž $(a) \bmod n + qn = a$ a $(b) \bmod n + rn = b$. Navíc připomeňme, že $0 \leq (a) \bmod n < n$ a $0 \leq (b) \bmod n < n$. Nyní počítejme:

$$(a+b) \bmod n = ((a) \bmod n + qn + (b) \bmod n + rn) \bmod n =$$

$$= ((a) \bmod n + (b) \bmod n + (q+r)n) \bmod n = ((a) \bmod n + (b) \bmod n) \bmod n.$$

Poznamenejme, že jsem využili elementárního faktu, že čísla, která se liší o násobek číslem n mají stejný zbytek po celočíselném dělení číslem n. $\square$

2.2. Dokažte, že $\mathbf{Z}_n$ spolu s operacemi $+_n$ a $\cdot_n$ splňuje axiomy (A0)–(A4), (M0)–(M3). (D) a (N).

Axiomy (A0) a (M0) požadují, aby obě operace $+_n$ i $\cdot_n$ byly dobře definované, tedy jejich výsledek ležel v množině $\mathbf{Z}_n$, což jsme zajistili definicí. S pomocí pozorování úlohy 2.1 a využitím asociativity sčítání na celých číslech spočítáme, že

$$(a +_n b) +_n c = ((a+b) \bmod n + c) \bmod n \overset{2.1}{=} ((a+b)+c) \bmod n =$$

$$(a + (b+c)) \bmod n \overset{2.1}{=} ((a+b) \bmod n + c) \bmod n = a +_n (b +_n c).$$

Stejnou úvahou pro násobení dostaneme

$$(a \cdot_n b) +_n c \overset{2.1}{=} ((a \cdot b) \cdot c) \bmod n = (a \cdot (b \cdot c)) \bmod n \overset{2.1}{=} a \cdot_n (b \cdot_n c).$$

Ukázali jsme, že jsou axiomy (A1) a (M1) splněny. Platnost komutativních zákonů, tedy axiomů (A2) a (M2) plyne okamžitě z definice operací a komutativity příslušných operací na celých číslech, podobně snadno z definice operací nahlédneme, že $0 +_n a = a$ a $1 \cdot_n a = a$ pro každé $a \in \mathbf{Z}_n$, tedy i axiomy (A3) a (M3) platí. Dále $-0 = 0$ a $-a = n - a$ pro všechna $a \in \mathbf{Z}_n \setminus \{0\}$, protože $(a + n - a) \bmod n = (n) \bmod n = 0$. odkud dostáváme platnost axiomu (A4). Distributivitu, tedy axiom (D), ověříme stejně jako asociativity pomocí úlohy 2.1 a s využitím distributivity na celých číslech:

$$(a +_n b) \cdot_n c \overset{2.1}{=} ((a+b) \cdot c) \bmod n = (a \cdot c + b \cdot c) \bmod n \overset{2.1}{=} a \cdot_n c +_n b \cdot_n c.$$

Konečně axiom netriviality je zřejmý z předpokladu, že $n > 1$. $\square$

2.3. Jsou-li $r, s \in \mathbf{N}$, $r > 1, s > 1$ a položme $n = rs$. Dokažte, že $\mathbf{Z}_n$ spolu s operacemi $+_n$ a $\cdot_n$ není těleso.

Ukázali jsme, že $\mathbf{Z}_n$ splňuje všechny axiomy tělesa s výjimkou axiomu (M4)- Protože víme, že v každém tělese musí podle Tvrzení 3.1 z přednášky platit pro $a \neq 0$ a $b \neq 0$, že $a \cdot b \neq 0$, stačí, abychom tuto podmínku vyvrátili. Položíme-li $a = r$ a $b = s$, pak vidíme, že $a \neq 0$ a $b \neq 0$, ovšem $a \cdot b = (n) \bmod n = 0$. $\square$

Nechť $a_0 \geq a_1$ jsou dvě přirozená čísla. Připomeňme **Eukleidův algoritmus** hledání největšího společného dělitele (NSD) čísel a_0 a a_1:

Známe-li a_{i-1} a a_i spočteme $a_{i+1} = (a_{i-1}) \bmod a_i$. Tedy víme, že existuje takové $q_i \in \mathbf{N}$ že $a_{i-1} = q_i a_i + a_{i+1}$ a $a_{i+1} < a_i$. Algoritmus skončí, když $a_{n+1} = 0$, potom $a_n = \mathrm{NSD}(a_0, a_1)$.

2.4. Najděte pomocí Euklidova algoritmu taková celá čísla x a y, aby $30x + 101y = 1$.

Nejprve si všimněme, že číslo 101 je prvočíslo, tedy největší společný dělitel čísel 30 a 101 je zcela jistě roven jedné. Euklidův algoritmus na nalezení největšího společného dělitele čísel 30 a 101 nám tedy samozřejmě musí dát výsledek 1. Přesto ho použijeme a budeme věnovat pozornost vztahu předchozích a následujících prvků:

$a_0 = 101$,
$a_1 = 30$,
$a_2 = 101 - 3 \cdot 30 = 11$,
$a_3 = 30 - 2 \cdot 11 = 8$,
$a_4 = 11 - 8 = 3$,
$a_5 = 8 - 2 \cdot 3 = 2$,
$a_6 = 3 - 2 = 1 = \mathrm{NSD}(101, 30)$.

Vidíme, že každé a_{i+1} je celočíselnou lineární kombinací prvků a_i a a_{i-1}, budeme-li postupně dosazovat předchozí vyjádření do následujících výrazů, dostaneme každé a_{i+1} jako celočíselnou lineární kombinací prvků a_0 a a_1:

$a_2 = 11 = 101 - 3 \cdot 30$,
$a_3 = 8 = 30 - 2 \cdot 11 = 30 - 2 \cdot (101 - 3 \cdot 30) = 7 \cdot 30 - 2 \cdot 101$,
$a_4 = 3 = 11 - 8 = (101 - 3 \cdot 30) - (7 \cdot 30 - 2 \cdot 101) = 3 \cdot 101 - 10 \cdot 30$,
$a_5 = 2 = 8 - 2 \cdot 3 = (7 \cdot 30 - 2 \cdot 101) - 2 \cdot (3 \cdot 101 - 10 \cdot 30) = 27 \cdot 30 - 8 \cdot 101$,
$a_6 = 1 = 3 - 2 = (3 \cdot 101 - 10 \cdot 30) - (27 \cdot 30 - 8 \cdot 101) = 11 \cdot 101 - 37 \cdot 30$.

Zjistili jsme, že $x = -37$ a $y = 11$. □

2.5. Najděte inverzní prvek k prvku 30 v tělese $\mathbf{Z}_{101}$.

Potřebujeme najít číslo $x \in \mathbf{Z}_{101}$, které by řešilo rovnici $(30 \cdot x) \bmod 101 = 1$, což můžeme reformulovat tak, že hledáme celá x a y, z nichž x má ležet v $\mathbf{Z}_{101}$, aby $30x + 101y = 1$. Podobnou úlohu už jsme řešili v předchozím příkladu, nyní si stačí uvědomit, že nalezené x, které neleží v požadovaném intervalu můžeme posunout pomocí vhodného násobku čísla 101. Dostaneme tedy zbytek po celočíselném dělení číslem 101, tj. $30^{-1} = (-37) \bmod 101 = 101 - 37 = 64$, protože

$$1 = 11 \cdot 101 - 37 \cdot 30 = 11 \cdot 101 - 30 \cdot 101 + 101 \cdot 30 - 37 \cdot 30 = (11 - 30) \cdot 101 + (101 - 37) \cdot 30.$$

Tedy jsme našli další a pro nás zajímavější řešení řešení $1 = 64 \cdot 30 - 19 \cdot 101$ rovnice z 2.4.

23./24.11.

2.6. Najděte nad tělesem $\mathbf{Z}_{101}$ prvky 63^{-1}, 20^{-1}, 2^{-1}, $(20 \cdot 63)^{-1}$, vyřešte nad ním rovnici $20 \cdot_{101} x = 7$ najděte inverzní matici k matici $\begin{pmatrix} 63 & 0 \\ 98 & 2 \end{pmatrix}$.

U prvních dvou hodnot postupujme stejně jako v předchozích úvahách, tedy využijeme Euklidův algoritmus:

$38 = 101 - 63,$
$25 = 63 - 38 = 2 \cdot 63 - 101,$
$13 = 38 - 25 = 2 \cdot 101 - 3 \cdot 63,$
$12 = 25 - 13 = 5 \cdot 63 - 3 \cdot 101,$
$1 = 13 - 12 = 5 \cdot 101 - 8 \cdot 63.$
Zjistili jsme, že $63^{-1} = (-8) \bmod 101 = 93$.

Podobně už v prvním kroku Euklidova algoritmu zjistíme, že $1 = 101 - 5 \cdot 20$, tedy $20^{-1} = (-5) \bmod 101 = 96$

Při určování hodnoty 2^{-1} můžeme udělat jednoduchou obecnou úvahu pro $\mathbf{Z}_p$, kde p je liché prvočíslo, že $\frac{p+1}{2} \in \mathbf{Z}_p$ a že $(2 \cdot \frac{p+1}{2}) \bmod p = (p+1) \bmod p = 1$, tedy $2^{-1} = \frac{101+1}{2} = 51$ v tělese $\mathbf{Z}_{101}$.

Uvážíme-li, že z axiomatiky tělesa plyne $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$ a $(-a) \cdot (-b) = a \cdot b$ pro všechny jeho prvky a a b (zkuste podrobně dokázat!), a využijeme-li vypočítaných hodnot, pak

$$(20 \cdot_{101} 63)^{-1} = 20^{-1} \cdot_{101} 63^{-1} = (-5) \cdot_{101} (-8) = 40.$$

Protože obvyklý způsob upravovaní rovnic je ekvivalentní (tj. vratný) i pro rovnice nad obecným tělesem, zjišťujeme, že hledané x je tvaru $x = 20^{-1} \cdot_{101} 7 = 96 \cdot_{101} 7 = 66$.

Konečně standardní cestou budeme upravovat řádky rozšířené matice nad tělesem $\mathbf{Z}_{101}$, přitom využijme znalosti $63^{-1} = 93$:

$$\left(\begin{array}{cc|cc} 63 & 0 & 1 & 0 \\ 98 & 2 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 93 & 0 \\ 98 & 2 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 93 & 0 \\ 0 & 2 & 77 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & 93 & 0 \\ 0 & 1 & 89 & 51 \end{array}\right).$$

Spočítali jsme, že $\begin{pmatrix} 63 & 0 \\ 98 & 2 \end{pmatrix}^{-1} = \begin{pmatrix} 93 & 0 \\ 89 & 51 \end{pmatrix}$. □

2.7. Dokažte, pomocí Euklidova algoritmu, že $\mathbf{Z}_p$ spolu s operacemi $+_p$ a $\cdot_p$ splňuje axiom 8.

Uvažujeme stejným způsobem jako v předchozích úlohách. Zvolme libovolně nenulové $a \in \mathbf{Z}_p$. Protože p je prvočíslo, jsou a a p nesoudělná, tedy pomocí Euklidova algoritmu lze najít celá x a y, pro něž $ax + py = \mathrm{NSD}(a,p) = 1$. Nyní stačí vzít $a^{-1} = (x) \bmod p$. □

Nadále budeme sčítání a násobení v tělese $\mathbf{Z}_p$ pro prvočíslo p psát bez indexu $_p$ (tj. jen $+$ a $\cdot$).

3. Aritmetické vektorové prostory a lineární nezávislost

3.1. Rozhodněte, zda je množina U podprostorem aritmetického vektorového prostoru $\mathbf{Z}_5^3$ nad tělesem $\mathbf{Z}_5$, jestliže
(a) $U = \{(0,0,0)^T\}$, (b) $U = \{(0,0,0)^T, (1,2,3)^T\}$, (c) $|U| = 4$,
(d) $U = \{(0,0,0)^T, (1,2,3)^T, (2,4,1)^T, (3,1,4)^T, (4,3,2)^T\}$,
(e) $|U| = 6$, (f) $|U| = 125$.

(a) Protože $(0,0,0)^T + (0,0,0)^T = (0,0,0)^T$ a $t(0,0,0)^T = (0,0,0)^T$ pro každé $t \in T$, je podle definice množina $\{(0,0,0)^T\}$ podprostorem $\mathbf{Z}_5^3$.

(b) Vidíme, že $(1,2,3)^T + (1,2,3)^T = 2(1,2,3)^T = (2,4,1)^T \notin U$, proto U není podprostorem.

(c) Je-li $\mathbf{u} = (u_1, u_2, u_3)$ nenulový vektor, potom množina $\mathbf{L}(\mathbf{u}) = \{a\,\mathbf{u} \mid a \in \mathbf{Z}_5\}$ obsahuje právě tolik různých vektorů,kolik prvků obsahuje těleso $\mathbf{Z}_5$. Proto čtyřprvkový podprostor (který by nutně obsahoval nenulový vektor) nad tělesem $\mathbf{Z}_5$ nemůže existovat.

(d) Snadno pomocí Tvrzení 4.3 z přednášky nahlédneme, že $U = \mathbf{L}((1,2,3)^T)$, tedy se jedná o podprostor.

(e) Kdyby existoval šestiprvkový podprostor nad tělesem $\mathbf{Z}_5$, pak obsahoval nějaký nenulový vektor $\mathbf{u}$ a pak ještě jeden vektor $\mathbf{v} \in U \setminus \mathbf{L}(\mathbf{u})$. Podle Tvrzení 4.7 by množin $\{\mathbf{u}, \mathbf{v}\}$ byla lineárně nezávislá, a proto by vektor $2\,\mathbf{u} \notin \mathbf{L}(\mathbf{u}) \cup \{\mathbf{v}\}$, což je spor s předpokladem $|U| = 6$. Tudíž žádný šestiprvkový podprostor nad tělesem $\mathbf{Z}_5$ neexistuje.

(f) Všimneme-li si, že 125 prvků má celý aritmetický prostor $\mathbf{Z}_5^3$, vidíme, že $U = \mathbf{Z}_5^3$ je podprostorem $\mathbf{Z}_5^3$. □

3.2. Rozhodněte, zda je posloupnost vektorů $(1,1,0,1)^T$, $(2,1,1,1)^T$, $(3,1,2,1)^T$ z aritmetického vektorového prostoru $\mathbf{R}^4$ nad tělesem R lineárně závislá či nezávislá.

Potřebujeme zjistit, zda existuje nějaké netriviální (tj. nenulové) řešení vektorové rovnice

$$x_1 \cdot (1,1,0,1)^T + x_2 \cdot (2,1,1,1)^T + x_3 \cdot (3,1,2,1)^T = (0,0,0,0)^T$$

Snadno nahlédneme, že řešení dané vektorové rovnice jsou právě řešení homogenní soustavy rovnic s maticí levých stran $\mathbf{A}$ (pravé strany jsou nulové, u matice homogenní soustavy rovnic vynecháváme sloupec nulových pravých stran, který se žádnými úpravami nemění). Tu následně obvyklým způsobem upravujeme:

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \\ 0 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & -1 & -2 \\ 0 & 1 & 2 \\ 0 & -1 & -2 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Aniž musíme nenulové řešení dopočítávat, ale zjevně jím jsou všechny násobky vektoru $(1,-2,1)$, zjišťujeme, že homogenní soustava rovnic s maticí $\mathbf{A}$, a tudíž i výše uvedená vektorová rovnice mají netriviální řešení, a proto jsou přímo podle definice vektory $(1,1,0,1)$, $(2,1,1,1)$, $(3,1,2,1)$ lineárně závislé. □

3.3. Rozhodněte, zda je posloupnost vektorů $(1,0,2,1)^T$, $(2,0,1,1)^T$, $(1,0,1,-1)^T$ v aritmetickém vektorovém prostoru $\mathbf{Q}^4$ nad tělesem $\mathbf{Q}$ lineárně závislá či nezávislá.

Stejně jako v předchozí úloze se ptáme, zda existuje, a v takovém případě půjde o lineárně závislé vektory, či neexistuje, což by znamenalo, že dané vektory by byly lineárně nezávislé, netriviální řešení vektorové rovnice

$$x_1 \cdot (1,0,2,1)^T + x_2 \cdot (2,0,1,1)^T + x_3 \cdot (1,0,1,-1)^T = (0,0,0,0)$$

Úlohu převedeme na otázku, zda existuje jednoznačné (tedy pouze triviální) řešení homogenní soustavy rovnic s maticí $\mathbf{A}$:

$$\mathbf{A} = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ 2 & 1 & 1 \\ 1 & 1 & -1 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & -3 & -1 \\ 0 & -1 & -2 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 5 \\ 0 & 0 & 0 \end{pmatrix}$$

Z upravené soustavy dostáváme jednoznačné řešení $x_1 = x_2 = x_3 = 0$, tedy vektory $(1,0,2,1)^T$, $(2,0,1,1)^T$, $(1,0,1,-1)^T$ jsou lineárně nezávislé. □

3.4. Najděte nějakou bázi podprostoru $U = \mathbf{L}((1,0,2,1)^T, (2,0,1,1)^T, (1,0,1,-1)^T)$ aritmetického vektorového prostoru $\mathbf{Q}^4$. Určete dimenzi U.

Protože množina $\{(1,0,2,1)^T, (2,0,1,1)^T, (1,0,1,-1)^T\}$ podle definice generuje U a v předchozím příkladu jsme dokázali, že jde o lineárně nezávislou množinu aritmetických vektorů, tvoří bázi množina $\{(1,0,2,1)^T, (2,0,1,1)^T, (1,0,1,-1)^T\}$. Počet prvků libovolné báze je dimenze, tedy $\dim U = 3$. □

3.5. Rozhodněte, zda je vektor $(1,1,4)^T$ lineární kombinací vektorů posloupnost vektorů $(1,4,3)^T$, $(3,1,1)^T$ ve vektorovém prostoru $\mathbf{Z}_5^3$ nad tělesem $\mathbf{Z}_5$. V případě kladné odpovědi najděte $x, y \in \mathbf{Z}_5$, pro něž $x \cdot (1,4,3) + y \cdot (3,1,1) = (1,1,4)$.

Ptáme se, zda existují hodnoty $x, y \in \mathbf{Z}_5$, které řeší vektorovou rovnici $x \cdot (1,4,3)^T + y \cdot (3,1,1)^T = (1,1,4)^T$, tedy řešíme soustavu 3 rovnic o 2 neznámých (pro každou souřadnici dostáváme jednu rovnici) s maticí, kterou snadno upravíme:

$$\left(\begin{array}{cc|c} 1 & 3 & 1 \\ 4 & 1 & 1 \\ 3 & 1 & 4 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 3 & 1 \\ 0 & 4 & 2 \\ 0 & 2 & 1 \end{array}\right) \sim \left(\begin{array}{cc|c} 1 & 3 & 1 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \end{array}\right)$$

Okamžitě vidíme, že řešení této soustavy existuje, proto $\begin{pmatrix} 1 \\ 1 \\ 4 \end{pmatrix} \in \mathbf{L}(\begin{pmatrix} 1 \\ 4 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \\ 1 \end{pmatrix})$ a $(x,y) = (2,3)$. □

30.11/1.12.

3.6. Spočítejte dimenzi podprostorů $\mathbf{U} = \mathbf{L}((2,1,1,1)^T, (4,2,1,3)^T, (3,4,3,0)^T, (1,3,4,2)^T)$ a $\mathbf{V} = \mathbf{L}((2,0,3,4)^T, (1,3,1,2)^T, (1,0,1,2)^T)$ aritmetického vektorového prostoru $\mathbf{Z}_5^4$ nad tělesem $\mathbf{Z}_5$

Uvědomme si, že oba podprostory můžeme chápat jako sloupcové vektorové prostory matic, které vzniknou sestavením příslušných generujících vektorů do sloupců, tedy $\mathbf{U} = \mathbf{S}(\mathbf{A})$ a $\mathbf{V} = \mathbf{S}(\mathbf{B})$ pro matice nad tělesem $\mathbf{Z}_5$

$$\mathbf{A} = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 1 & 2 & 4 & 3 \\ 1 & 1 & 3 & 4 \\ 1 & 3 & 0 & 2 \end{pmatrix} \quad \text{a} \quad \mathbf{B} = \begin{pmatrix} 2 & 1 & 1 \\ 0 & 3 & 0 \\ 3 & 1 & 1 \\ 4 & 2 & 2 \end{pmatrix}.$$

Nyní stačí využít Věty 4.23, která říká, že $\dim \mathbf{U} = \dim \mathbf{S}(\mathbf{A}) = r(\mathbf{A})$ a Důsledek 4.18, podle nějž stačí matice upravit posloupností elementárních úprav na odstupňovanou matici a v ní poté spočítat nenulové řádky:

$$\mathbf{A} = \begin{pmatrix} 2 & 4 & 3 & 1 \\ 1 & 2 & 4 & 3 \\ 1 & 1 & 3 & 4 \\ 1 & 3 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & 3 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 4 & 4 & 1 \\ 0 & 1 & 1 & 4 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & 3 & 1 \\ 0 & 4 & 4 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix},$$

proto $\dim \mathbf{U} = r(\mathbf{A}) = 2$ a

$$\mathbf{B} = \begin{pmatrix} 2 & 1 & 1 \\ 0 & 3 & 0 \\ 3 & 1 & 1 \\ 4 & 2 & 2 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & 1 \\ 0 & 3 & 0 \\ 0 & 2 & 2 \\ 0 & 0 & 0 \end{pmatrix} \sim \begin{pmatrix} 2 & 1 & 1 \\ 0 & 3 & 0 \\ 0 & 0 & 2 \\ 0 & 0 & 0 \end{pmatrix},$$

tudíž $\dim \mathbf{V} = r(\mathbf{B}) = 3$. □

3.7. Vyberte z množiny $X = \{(2,1,1,1)^T, (4,2,1,3)^T, (3,4,3,0)^T, (1,3,4,2)^T\}$, resp. $Y = \{(2,0,3,4)^T, (1,3,1,2)^T, (1,0,1,2)^T\}$ báze podprostorů $\mathbf{U} = \mathbf{L}(X)$, resp. $\mathbf{V} = \mathbf{L}(Y)$ aritmetického vektorového prostoru $\mathbf{Z}_5^4$.

Opět počítáme se sloupcovými vektorovými prostory $\mathbf{U} = \mathbf{S}(\mathbf{A})$ a $\mathbf{V} = \mathbf{S}(\mathbf{B})$ matic $\mathbf{A}$ a $\mathbf{B}$ z předchozí úlohy.

Můžeme využít Tvrzení 4.14. z přednášky, z kterého plyne, že bázové sloupcové vektory matice tvoří bázi sloupcového vektorového prostoru, protože bázové sloupce obecné matice jsou právě ty sloupce, které odpovídají bázový sloupcům odstupňovaného tvaru matice. Z odstupňovaných tvarů matic $\mathbf{A}$ a $\mathbf{B}$, které jsme našli v předchozí úloze, vidíme, že bázi $\mathbf{U}$ tvoří první dva sloupce matice $\mathbf{A}$, tedy vektory $\{(2,1,1,1)^T, (4,2,1,3)^T\}$ a bázi $\mathbf{U}$ tvoří všechny sloupce matice $\mathbf{B}$, tedy celá množina Y.

Díky spočítaným dimenzím $\mathbf{U}$ a $\mathbf{V}$, jsme v našem případě mohli postupovat přímočaře. Stačilo nahlédnout s využitím Tvrzení 4.10, že hledáme dvouprvkovou lineárně nezávislou množinu v $\mathbf{U}$, tedy dvojici vektorů, které nejsou svými násobky (to zřejmě splňuje například také dvojice vektorů $(2,1,1,1)^T, (3,4,3,0)^T$ či $(3,4,3,0)^T, (1,3,4,2)^T$) a tříprvkovou generující množinu, jíž je zřejmě celé Y. □

3.8. Spočítejte dimenze součtu $\mathbf{U} + \mathbf{V}$ a průniku $\mathbf{U} \cap \mathbf{V}$ podprostorů $\mathbf{Z}_5^4$ z předchozích dvou úloh.

Připomeňme, že $\mathbf{U} + \mathbf{V} = \{\mathbf{u} + \mathbf{v} \mid \mathbf{u} \in \mathbf{U}, \mathbf{v} \in \mathbf{V}\}$ je podprostor generovaný všemi vektory $\mathbf{U}$ i $\mathbf{V}$, ovšem stačí nám uvažovat jen báze $\mathbf{U}$ i $\mathbf{V}$, které už jsme nalezli, tedy platí, že $\mathbf{U} + \mathbf{V} = \mathbf{L}(\begin{pmatrix} 2 \\ 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 4 \\ 2 \\ 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 3 \\ 4 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \\ 2 \end{pmatrix})$. Dimenzi součtu $\mathbf{U} + \mathbf{V}$ nyní najdeme stejně jako v 3.6, tedy seřadíme generující vektory do sloupců matice a upravujeme

$$\mathbf{C} = \begin{pmatrix} 2 & 4 & 2 & 1 & 1 \\ 1 & 2 & 0 & 3 & 0 \\ 1 & 1 & 3 & 1 & 1 \\ 1 & 3 & 4 & 2 & 2 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & 2 & 1 & 1 \\ 0 & 0 & 4 & 0 & 2 \\ 0 & 4 & 2 & 3 & 3 \\ 0 & 1 & 3 & 4 & 4 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & 2 & 1 & 1 \\ 0 & 4 & 2 & 3 & 3 \\ 0 & 0 & 4 & 0 & 2 \\ 0 & 0 & 0 & 2 & 2 \end{pmatrix}.$$

Vidíme, že $\dim(\mathbf{U}+\mathbf{V}) = \dim(\mathbf{S}(\mathbf{C})) = r(\mathbf{C}) =$.

Konečně si zbývá uvědomit, že podle Věty 4.13 (o dimenzi součtu a průniku) je $\dim(\mathbf{U}+\mathbf{V}) = \dim(\mathbf{U}) + \dim(\mathbf{V}) - \dim(\mathbf{U} \vee \mathbf{V}) = 2 + 3 - 4 = 1$. □

3.9. Určete dimenzi průniku podprostorů $\mathbf{U}$ a $\mathbf{V}$ racionálního vektorového prostoru $\mathbf{Q}^3$, je-li $\mathbf{U} = \mathbf{L}((1,2,1),(1,0,2))$ a $\mathbf{V} = \mathbf{L}((1,1,0),(1,-1,1))$.

Snadno zjistíme, že $\dim \mathbf{U} = r(\begin{pmatrix} 1 & 1 \\ 2 & 0 \\ 1 & 2 \end{pmatrix}) = 2$, $\dim \mathbf{V} = r(\begin{pmatrix} 1 & 1 \\ 1 & -1 \\ 0 & 1 \end{pmatrix}) = 2$ a $\dim(\mathbf{U}+\mathbf{V}) = r(\begin{pmatrix} 1 & 1 & 1 & 1 \\ 2 & 0 & 1 & -1 \\ 1 & 2 & 0 & 1 \end{pmatrix}) = 3$, proto je díky Větě 4.13

$$\dim(\mathbf{U} \cap \mathbf{V}) = \dim \mathbf{U} + \dim \mathbf{V} - \dim(\mathbf{U}+\mathbf{V}) = 1.$$

□

3.10. Najděte nad tělesem $\mathbf{Z}_5$ všechna řešení homogenní soustavy rovnic s maticí $\mathbf{A} = \begin{pmatrix} 3 & 1 & 1 & 2 & 4 \\ 1 & 2 & 1 & 2 & 1 \\ 4 & 3 & 0 & 1 & 3 \end{pmatrix}$.

Připomeňme, že pro hledanou množinu všech řešení jsme zavedli značení $\mathbf{N}(\mathbf{A})$. Budeme tedy standardně upravovat matici $\mathbf{A}$ posloupností elementárních úprav odstupňovanou matici:

$$\begin{pmatrix} 3 & 1 & 1 & 2 & 4 \\ 1 & 2 & 1 & 2 & 1 \\ 4 & 3 & 0 & 1 & 3 \end{pmatrix} \sim \begin{pmatrix} 3 & 1 & 1 & 2 & 4 \\ 0 & 0 & 4 & 3 & 3 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix} \sim \begin{pmatrix} 3 & 1 & 1 & 2 & 4 \\ 0 & 0 & 1 & 3 & 4 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}.$$

Nyní si uvědomme, že jsme zjistili hodnost matice $\mathbf{A}$, konkrétně $h(\mathbf{A}) = 3$. Z Věty 4.23, víme, že $\mathbf{N}(\mathbf{A})$ je podprostor aritmetického vektorového prostoru $\mathbf{Z}_5^5$ dimenze $\dim \mathbf{N}(\mathbf{A}) = 5 - r(\mathbf{A}) = 2$. Potřebujme najít dvouprvkovou bázi podprostoru $\mathbf{N}(\mathbf{A})$. Vidíme, že získané Gaussova matice $\begin{pmatrix} \mathbf{3} & 1 & 1 & 2 & 4 \\ 0 & 0 & \mathbf{1} & 3 & 4 \\ 0 & 0 & 0 & \mathbf{1} & 2 \end{pmatrix}$ má 1., 3. a 4. bázový sloupec (t.j. sloupec s první nenulovou pozicí na řádku), proto můžeme volit hodnoty x_2 a x_5 a poté jednoznačně dopočítat zpětnou substitucí. Vezmeme-li za (x_2, x_5) postupně vektory standardní (nebo nějaké jiné) báze $\mathbf{Z}_5^2$ a dopočítáme-li hodnoty x_1, x_3 a x_4, budou nalezené vektory řešení lineárně nezávislé, tedy nutně půjde o hledanou bázi. Položíme-li tedy $x_2 = 1$ a $x_5 = 0$, pak snadno najdeme vektor $(3,1,0,0,0)^T$ řešící soustavu a podobně pro volbu $x_2 = 0$ a $x_5 = 1$ dostáváme řešení $(1,0,2,3,1)^T$.

Spočítali jsme, že množinou všech řešení homogenní soustavy rovnic s maticí $\mathbf{A}$ je podprostor $\mathbf{N}(\mathbf{A}) = \mathbf{L}((3,1,0,0,0)^T, (1,0,2,3,1)^T)$. □

3.11. Existuje nějaký vektor pravých stran $\mathbf{b} \in \mathbf{Z}_5^3$, pro který neexistuje žádné řešení soustavy $\mathbf{A}\mathbf{x}^T = \mathbf{b}^T$, kde $\mathbf{A}$ je matice z úlohy 3.10?

Stačí aplikovat Frobeniovu větu (Věta 4.24), která říká, že řešení obecné soustavy lineárních rovnic $\mathbf{A}\mathbf{x}^T = \mathbf{b}^T$ existuje právě tehdy, když je hodnost matice $\mathbf{A}$

stejná jako hodnost rozšířené matice $(\mathbf{A}|\mathbf{b}^T)$. Poznamenejme, že vždy platí nerovnost $r(\mathbf{A}) \leq r(\mathbf{A}|\mathbf{b}^T)$. Protože jsme zjistili, že $r(\mathbf{A}) = 3$ a matice $(\mathbf{A}|\mathbf{b}^T)$ má tři řádky, tedy $r(\mathbf{A}|\mathbf{b}^T) \leq 3$, vidíme, že $r(\mathbf{A}|\mathbf{b}^T) = 3$, a proto je soustava $\mathbf{A}\mathbf{x}^T = \mathbf{b}^T$ řešitelná pro každý vektor $\mathbf{b} \in \mathbf{Z}_5^3$. □

3.12. Najděte nad tělesem $\mathbf{Z}_5$ všechna řešení soustavy rovnic $\mathbf{A}\mathbf{x} = (1,2,4)^T$, kde $\mathbf{A}$ je matice z úlohy 3.10.

Díky Tvrzení 4.5 nám stačí najít jedno řešení $\mathbf{u}$ nehomogenní soustavy $\mathbf{A}\mathbf{x}^T = (1,2,4)^T$. Každé řešení potom budou právě tvaru $\mathbf{u} + \mathbf{w}$ pro vhodné $\mathbf{w} \in \mathbf{N}(\mathbf{A})$ podle Tvrzení 4.5.3. Postupujeme analogicky výpočtu v příkladu 3.10. Nejprve rozšířenou matici stejnými elementárními úpravami upravíme na Gaussovu matici a poté dopočítáme řešení například pro volbu $x_2 = 0$ a $x_5 = 0$:

$$\left(\begin{array}{ccccc|c} 3 & 1 & 1 & 2 & 4 & 1 \\ 1 & 2 & 1 & 2 & 1 & 2 \\ 4 & 3 & 0 & 1 & 3 & 4 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 3 & 1 & 1 & 2 & 4 & 1 \\ 0 & 0 & 4 & 3 & 3 & 0 \\ 0 & 0 & 1 & 3 & 4 & 1 \end{array}\right) \sim \left(\begin{array}{ccccc|c} 3 & 1 & 1 & 2 & 4 & 1 \\ 0 & 0 & 1 & 3 & 4 & 1 \\ 0 & 0 & 0 & 1 & 2 & 1 \end{array}\right).$$

Soustavu tedy řeší například vektor $(2,0,3,1,0)$, tedy využijeme-li nyní Tvrzení 4.5.3 a popisu podprostoru $\mathbf{N}(\mathbf{A})$ získané v 3.10, je množina všech řešení soustavy $\mathbf{A}\mathbf{x} = (1,2,4)^T$ tvaru

$$\{(1,0,3,1,0)^T\} + \mathbf{N}(\mathbf{A}) = \{(1,0,3,1,0)^T\} + \mathbf{L}((3,1,0,0,0)^T, (1,0,2,3,1)^T).$$

□

3.13. Najděte nad tělesem $\mathbf{Z}_7$ všechna řešení soustavy rovnic $\mathbf{A}\mathbf{x} = \mathbf{b}$ s maticí $\mathbf{A} = \begin{pmatrix} 3 & 1 & 5 & 2 \\ 3 & 2 & 4 & 6 \\ 2 & 5 & 6 & 0 \end{pmatrix}$ a) pro $\mathbf{b} = (1,1,1)^T$, b) pro $\mathbf{b} = (1,2,5)^T$

Opět upravíme rozšířenou matici soustavy na odstupňovanou matici.

a)

$$\left(\begin{array}{cccc|c} 3 & 1 & 5 & 2 & 1 \\ 3 & 2 & 4 & 6 & 1 \\ 2 & 5 & 6 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} 3 & 1 & 5 & 2 & 1 \\ 0 & 1 & 6 & 4 & 0 \\ 0 & 2 & 5 & 1 & 5 \end{array}\right) \sim \left(\begin{array}{cccc|c} 3 & 1 & 5 & 2 & 1 \\ 0 & 1 & 6 & 4 & 0 \\ 0 & 0 & 0 & 0 & 5 \end{array}\right)$$

Protože je hodnost matice homogenní soustavy rovnic menší než hodnost rozšířenou matici soustavy, díky Frobeniově větě (4.24) je množina všech řešení soustavy prázdná.

b)

$$\left(\begin{array}{cccc|c} 3 & 1 & 5 & 2 & 1 \\ 3 & 2 & 4 & 6 & 2 \\ 2 & 5 & 6 & 0 & 5 \end{array}\right) \sim \left(\begin{array}{cccc|c} 3 & 1 & 5 & 2 & 1 \\ 0 & 1 & 6 & 4 & 1 \\ 0 & 2 & 5 & 1 & 2 \end{array}\right) \sim \left(\begin{array}{cccc|c} 3 & 1 & 5 & 2 & 1 \\ 0 & 1 & 6 & 4 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Tentokrát řešení soustavy existuje a my snadno jedno najdeme $(0,1,0,0)^T$. Dále spočítáme bázi podprostoru $\mathbf{N}(\mathbf{A})$ a opět využijeme Tvrzení 4.5.3, podle nějž je množina všech řešení nehomogenní soustavy $\mathbf{A}\mathbf{x} = \mathbf{b}$ právě tvaru

$$\{\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}\} + \mathbf{N}(\mathbf{A}) = \{\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}\} + \mathbf{L}(\begin{pmatrix} 5 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \\ 0 \\ 1 \end{pmatrix}) = \{\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + r \cdot \begin{pmatrix} 5 \\ 1 \\ 1 \\ 0 \end{pmatrix} + s \cdot \begin{pmatrix} 3 \\ 3 \\ 0 \\ 1 \end{pmatrix} \mid r, s \in \mathbf{Z}_7\}.$$

□

3.14. Najděte nějakou bázi podprostorů $\mathbf{U}+\mathbf{V}$ a $\mathbf{U}\cap\mathbf{V}$ vektorového prostoru $\mathbf{Z}_5^4$ z příkladu 3.6.

V úloze 3.8 jsem zjistili, že dimenze podprostoru $\mathbf{U}+\mathbf{V}$ je 4, což podle Věty 4.11 z přednášky znamená, že $\mathbf{U}+\mathbf{V}=\mathbf{Z}_5^4$, protože $\dim \mathbf{Z}_5^4 = 4$. Tedy bázi $\mathbf{U}+\mathbf{V}$ tvoří například standardní báze $(1,0,0,0)^T, (0,1,0,0)^T, (0,0,1,0)^T, (0,0,0,1)^T$.

Nyní potřebujeme najít všechny vektory, které leží zároveň v $\mathbf{U}$ i ve $\mathbf{V}$, tedy které jsou zároveň lineárními kombinacemi generátorů $\mathbf{U}$ i $\mathbf{V}$. Připomeneme-li, že jsme v 3.7 našli bázi $\{(2,1,1,1)^T, (4,2,1,3)^T\}$ podprostoru $\mathbf{U}$ a bázi $\{(2,0,3,4)^T$, $(1,3,1,2)^T$, $(1,0,1,2)^T\}$ podprostoru $\mathbf{V}$ a že množina $\{-(2,0,3,4)^T, -(1,3,1,2)^T$, $-(1,0,1,2)^T\} = \{(3,0,2,1)^T, (4,2,4,3)^T, (4,0,4,3)^T\}$ je rovněž báze $\mathbf{V}$, pak hledáme lineární kombinace splňující

$$x_1\begin{pmatrix}2\\1\\1\\1\end{pmatrix}+x_2\begin{pmatrix}4\\2\\1\\3\end{pmatrix}=-y_1\begin{pmatrix}2\\0\\3\\4\end{pmatrix}-y_2\begin{pmatrix}1\\3\\1\\2\end{pmatrix}-y_3\begin{pmatrix}1\\0\\1\\2\end{pmatrix},$$

kterou upravíme do standardního tvaru

$$x_1\begin{pmatrix}2\\1\\1\\1\end{pmatrix}+x_2\begin{pmatrix}4\\2\\1\\3\end{pmatrix}+y_1\begin{pmatrix}2\\0\\3\\4\end{pmatrix}+y_2\begin{pmatrix}1\\3\\1\\2\end{pmatrix}+y_3\begin{pmatrix}1\\0\\1\\2\end{pmatrix}=\begin{pmatrix}0\\0\\0\\0\end{pmatrix}.$$

Hledáme tedy $\mathbf{N}(\mathbf{C})$ matice $\mathbf{C}=\begin{pmatrix}2&4&2&1&1\\1&2&0&3&0\\1&1&3&1&1\\1&3&4&2&2\end{pmatrix}\sim\begin{pmatrix}2&4&2&1&1\\0&4&2&3&3\\0&0&4&0&2\\0&0&0&2&2\end{pmatrix}$ z příkladu 3.8. Nyní snadno najdeme jedno netriviální řešení $(0,4,2,4,1)^T$ soustavy s maticí $\mathbf{C}$, tedy hledaným bázovým vektorem podprostoru $\mathbf{U}\cap\mathbf{V}$ je

$$\begin{pmatrix}1\\3\\4\\2\end{pmatrix}=0\cdot\begin{pmatrix}2\\1\\1\\1\end{pmatrix}+4\cdot\begin{pmatrix}4\\2\\1\\3\end{pmatrix}=3\cdot\begin{pmatrix}2\\0\\3\\4\end{pmatrix}+1\cdot\begin{pmatrix}1\\3\\1\\2\end{pmatrix}+4\cdot\begin{pmatrix}1\\0\\1\\2\end{pmatrix}.$$

□

7./8.12.

3.15. Najděte nějakou bázi průniku podprostorů $\mathbf{U}\cap\mathbf{V}$ vektorového prostoru $\mathbf{Z}_3^4$ nad tělesem $\mathbf{Z}_3$, jestliže $\mathbf{U}=\mathbf{L}((1,1,1,1)^T, (0,2,1,1)^T, (0,0,1,2)^T)$ a $\mathbf{V}=\mathbf{L}((1,2,2,1)^T$, $(0,1,2,1)^T$, $(0,0,2,2)^T)$.

Postupujeme stejně jako v předchozí úloze, tedy hledáme všechny vektory, které leží zároveň v $\mathbf{U}$ i ve $\mathbf{V}$, což si opět vyjádříme rovnicí:

$$x_1\begin{pmatrix}1\\1\\1\\1\end{pmatrix}+x_2\begin{pmatrix}0\\2\\1\\1\end{pmatrix}+x_3\begin{pmatrix}0\\0\\1\\2\end{pmatrix}=y_1\begin{pmatrix}1\\2\\2\\1\end{pmatrix}+y_2\begin{pmatrix}0\\1\\2\\1\end{pmatrix}+y_3\begin{pmatrix}0\\0\\2\\2\end{pmatrix},$$

kterou opět upravíme na

$$x_1\begin{pmatrix}1\\1\\1\\1\end{pmatrix}+x_2\begin{pmatrix}0\\2\\1\\1\end{pmatrix}+x_3\begin{pmatrix}0\\0\\1\\2\end{pmatrix}+y_1\begin{pmatrix}2\\1\\1\\2\end{pmatrix}+y_2\begin{pmatrix}0\\2\\1\\2\end{pmatrix}+y_3\begin{pmatrix}0\\0\\1\\1\end{pmatrix}=\begin{pmatrix}0\\0\\0\\0\end{pmatrix}.$$

Znovu počítáme všechna řešení homogenní soustavy s maticí:

$$\mathbf{D}=\begin{pmatrix}1&0&0&2&0&0\\1&2&0&1&2&0\\1&1&1&1&1&1\\1&1&2&2&2&1\end{pmatrix}\sim\begin{pmatrix}1&0&0&2&0&0\\0&2&0&2&2&0\\0&1&1&2&1&1\\0&1&2&0&2&1\end{pmatrix}\sim$$

$$\sim\begin{pmatrix}1&0&0&2&0&0\\0&2&0&2&2&0\\0&0&1&1&0&1\\0&0&2&2&1&1\end{pmatrix}\sim\begin{pmatrix}1&0&0&2&0&0\\0&2&0&2&2&0\\0&0&1&1&0&1\\0&0&0&0&1&2\end{pmatrix}.$$

Nyní snadno najdeme bázi $(1,2,2,1,0,0)^T$, $(0,2,2,0,1,1)^T$ podprostoru $\mathbf{N}(\mathbf{D})$. Zjistili jsme, že:

$$\begin{pmatrix}1\\2\\2\\1\end{pmatrix}=1\cdot\begin{pmatrix}1\\1\\1\\1\end{pmatrix}+2\cdot\begin{pmatrix}0\\2\\1\\1\end{pmatrix}+2\cdot\begin{pmatrix}0\\0\\1\\2\end{pmatrix}=1\cdot\begin{pmatrix}1\\2\\2\\1\end{pmatrix}+0\cdot\begin{pmatrix}0\\1\\2\\1\end{pmatrix}+0\cdot\begin{pmatrix}0\\0\\2\\2\end{pmatrix},$$

a

$$\begin{pmatrix}0\\1\\1\\0\end{pmatrix}=\begin{pmatrix}1\\2\\2\\1\end{pmatrix}=0\cdot\begin{pmatrix}1\\1\\1\\1\end{pmatrix}+2\cdot\begin{pmatrix}0\\2\\1\\1\end{pmatrix}+2\cdot\begin{pmatrix}0\\0\\1\\2\end{pmatrix}=0\cdot\begin{pmatrix}1\\2\\2\\1\end{pmatrix}+1\cdot\begin{pmatrix}0\\1\\2\\1\end{pmatrix}+1\cdot\begin{pmatrix}0\\0\\2\\2\end{pmatrix},$$

$$\begin{aligned}0\cdot(1,1,1,1)+2\cdot(0,2,1,1)+2\cdot(0,0,1,2)&=\\=0\cdot(1,2,2,1)+1\cdot(0,1,2,1)+1\cdot(0,0,2,2)&=(0,1,1,0).\end{aligned}$$

Tudíž vektory $(1,2,2,1)^T$ a $(0,1,1,0)^T$ leží v podprostoru $\mathbf{U}\cap\mathbf{V}$. Konečně si uvědomíme, že libovolné řešení soustavy lze napsat ve tvaru

$$a_1\cdot(1,2,2,1,0,0)^T+a_2\cdot(0,2,2,0,1,1)^T=(a_1,2a_1+2a_2,2a_1+2a_2,a_1,a_2,a_2)^T,$$

kde $a_1,a_2\in\mathbf{Z}_3$, proto lze každý vektor z průniku vyjádřit:

$$\begin{aligned}a_1\cdot(1,1,1,1)^T+(2a_1+2a_2)\cdot(0,2,1,1)^T+(2a_1+2a_2)\cdot(0,0,1,2)^T&=\\=a_1\cdot(1,2,2,1)^T+a_2\cdot(0,1,1,0)^T.\end{aligned}$$

Tím jsme zjistili, že každý vektor z podprostoru $\mathbf{U}\cap\mathbf{V}$ lze napsat ve tvaru $a_1\cdot(1,2,2,1)^T+a_2\cdot(0,1,1,0)^T$, tedy množina $\{(1,2,2,1)^T,(0,1,1,0)^T\}$ podprostor $\mathbf{U}\cap\mathbf{V}$ generuje. Zjevně se jedná o množinu lineárně nezávislou, tedy jde o bázi průniku. Není přitom těžké si uvědomit, že výsledné vektory budou jistě lineárně nezávislé, jestliže jsme hledali jejich souřadnice vzhledem k bázím prostorů $\mathbf{U}$ a $\mathbf{V}$.

Závěrem si ještě všimněme, že jsme soustavu nemuseli dopočítávat, neboť nám stačilo najít souřadnice báze řešení odpovídající proměnným y_i (tj. poslední 3 souřadnice) nebo x_i (tj. první 3 souřadnice). □

3.16. Doplňte lineárně nezávislou množinu $B=\{(2,4,0,1,4)^T,(1,2,1,0,3)^T\}$ na bázi aritmetického vektorového prostoru $\mathbf{Z}_5^5$.

Připomeňme, že podle Tvrzení 4.14.5 se řádkový vektorový prostor matice nezmění, upravíme-li ji posloupností elementárních řádkových úprav. Seřadíme-li vektory množiny B do řádků matice, kterou upravíme na odstupňovanou matici, vidíme, že

$$\mathbf{L}(B) = \mathbf{R}(\begin{pmatrix} 2 & 4 & 0 & 1 & 4 \\ 1 & 2 & 1 & 0 & 3 \end{pmatrix}) = \mathbf{R}(\begin{pmatrix} 2 & 4 & 0 & 1 & 4 \\ 0 & 0 & 1 & 2 & 1 \end{pmatrix})$$

Nyní snadno doplníme matici na odstupňovanou čtvercovou matici, jejíž všechny řádky jsou nenulové, například vektory standardní báze (i-tý přidáme, právě když i-tý sloupec matice není bázový) a přitom si všimneme, že:

$$\begin{pmatrix} 2 & 4 & 0 & 1 & 4 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & 0 & 1 & 4 \\ 0 & 0 & 1 & 2 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 2 & 4 & 0 & 1 & 4 \\ 1 & 2 & 1 & 0 & 3 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \mathbf{A}.$$

Zřejmě má řádkový prostor matice $\mathbf{A}$ dimenzi 5, proto je roven $\mathbf{Z}_5^5$. Tedy množina $\{(0,1,0,0,0)^T,\ (0,0,0,1,0)^T, (0,0,0,0,1)^T\}$ doplňuje množinu B na bázi $\mathbf{Z}_5^5$. $\square$

3.17. Najděte nějakou bázi podprostoru $\mathbf{U} = \mathbf{L}((3,1,4,2)^T, (2,3,5,1)^T, (1,5,6,1)^T)$ aritmetického vektorového prostoru $\mathbf{Z}_7^4$ a doplňte ji bázi celého prostoru $\mathbf{Z}_7^4$.

I tentokrát můžeme využít úvahy Tvrzení 4.14.5 o řádkovém vektorovém prostoru matice $\mathbf{M} = \begin{pmatrix} 3 & 1 & 4 & 2 \\ 2 & 3 & 5 & 1 \\ 1 & 5 & 6 & 1 \end{pmatrix}$, pro níž platí, že $\mathbf{U} = \mathbf{R}(\mathbf{M})$. Nejprve standardní cestou upravíme matici $\mathbf{M}$ na matici odstupňovanou:

$$\begin{pmatrix} 3 & 1 & 4 & 2 \\ 2 & 3 & 5 & 1 \\ 1 & 5 & 6 & 1 \end{pmatrix} \sim \begin{pmatrix} 3 & 1 & 4 & 2 \\ 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 3 \end{pmatrix} \sim \begin{pmatrix} 3 & 1 & 4 & 2 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \mathbf{N}.$$

Vidíme, že báze $\mathbf{R}(\mathbf{N}) = \mathbf{R}(\mathbf{M}) = \mathbf{U}$ je tvořena například nenulovými řádkovými vektory odstupňované matice $\mathbf{N}$. Tedy $\{(3,1,4,2)^T, (0,0,0,1)^T\}$ je báze $\mathbf{U}$. Nyní už postupujeme stejně jako v předchozí úloze, doplníme nenulové řádky matice $\mathbf{N}$ pomocí vektorů standardní báze, abychom dostali odstupňovanou regulární matici $\begin{pmatrix} 3 & 1 & 4 & 2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$. Tudíž množina $\{(0,1,0,0)^T,\ (0,0,1,0)^T\}$ doplňuje množinu $\{(3,1,4,2)^T, (0,0,0,1)^T\}$ na bázi $\mathbf{Z}_7^4$. $\square$

3.18. Určete nad tělesy $\mathbf{R}$ a $\mathbf{Z}_5$ hodnost matice $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 1 \\ 1 & 4 & 3 \end{pmatrix}$ a matice $\mathbf{A}^T$ a dimenze řádkového, sloupcového, nulového a levého nulového prostoru matice $\mathbf{A}$.

Podle Věty 4.23 stačí spočítat hodnost matice.

Upravujme matici posloupností elementárních úprav nejprve nad tělesem reálných čísel:

$$\begin{pmatrix}1&2&3\\2&1&1\\1&4&3\end{pmatrix}\sim\begin{pmatrix}1&2&3\\0&-3&-5\\0&2&0\end{pmatrix}\sim\begin{pmatrix}1&2&3\\0&1&0\\0&0&-5\end{pmatrix}.$$

Zjistili jsme, že nad tělesem $\mathbf{R}$ hodnost $r(\mathbf{A})=3$. Tedy že $r(\mathbf{A})=r(\mathbf{A}^T)=\dim\mathbf{R}(\mathbf{A})=\dim\mathbf{S}(\mathbf{A})=3$ a $\dim\mathbf{N}(\mathbf{A})=\dim\mathbf{N}(\mathbf{A}^T)=3-3=0$.

Podobně určíme hodnost $\mathbf{A}$ nad tělesem $\mathbf{Z}_5$:

$$\begin{pmatrix}1&2&3\\2&1&1\\1&4&3\end{pmatrix}\sim\begin{pmatrix}1&2&3\\0&1&0\\0&0&0\end{pmatrix}.$$

Tedy nad tělesem $\mathbf{Z}_5$ je $r(\mathbf{A})=r(\mathbf{A}^T)=\dim\mathbf{R}(\mathbf{A})=\dim\mathbf{S}(\mathbf{A})=2$ a $\dim\mathbf{N}(\mathbf{A})=\dim\mathbf{N}(\mathbf{A}^T)=3-2=1$. □

3.19. Najděte redukovaný odstupňovaný tvar matice $\mathbf{M}=\begin{pmatrix}3&3&2&6&4\\5&5&0&2&1\\2&2&5&3&4\end{pmatrix}$ nad tělesem $\mathbf{Z}_7$.

Nejprve obvyklým způsobem matici $\mathbf{M}$ upravíme na odstupňovanou matici a poté upravíme odstupňovanou matici tak, aby bázové sloupce byly právě vektory standardní báze:

$$\mathbf{M}\sim\begin{pmatrix}1&1&3&2&6\\0&0&6&6&6\\0&0&6&6&6\end{pmatrix}\sim\begin{pmatrix}1&1&3&2&6\\0&0&1&1&1\\0&0&0&0&0\end{pmatrix}\sim\begin{pmatrix}1&1&0&6&3\\0&0&1&1&1\\0&0&0&0&0\end{pmatrix}.$$

Spočítali jsme, že je matice $\begin{pmatrix}1&1&0&6&3\\0&0&1&1&1\\0&0&0&0&0\end{pmatrix}$ redukovaným odstupňovaným tvare matice $\mathbf{M}$ □

4. Permutace

4.1. Zapište v cyklickém zápisu a redukovaném cyklického zápisu permutace $p=\begin{pmatrix}1&2&3&4&5&6\\3&4&1&6&5&2\end{pmatrix}$, $q=\begin{pmatrix}1&2&3&4&5&6\\1&3&6&4&2&5\end{pmatrix}\in S_6$. Kolika různými způsoby lze v redukovaném a neredukovaném tvaru permutaci p a q zapsat?

Postupně vyčerpáme všechny prvky z množiny $\{1,2,3,4,5,6\}$, abychom zapsali cykly permutací $p=(13)(246)(5)$ a $q=(1)(2365)(4)$. V redukovaném cyklickém zápisu vynecháme všechny jednocykly, tedy pevné body daného zobrazení, a proto $p=(13)(246)$ a $q=(2365)$.

Zápis každého cyklu konkrétní permutace je určen svou první hodnotou, tedy n-cyklus lze zapsat n způsoby. Protože můžeme cykly v cyklickém zápisu ještě vzájemně libovolně permutovat, vidíme, že permutaci p lze v redukovaném cyklickém zápisu zapsat právě $2\cdot 3\cdot 2!=12$ způsoby a v neredukovaném cyklickém zápisu ji lze zapsat právě $2 \cdot 3 \cdot 1 \cdot 3! = 36$ způsoby. Stejnou úvahou dostaneme, že permutaci q můžeme v redukovaném cyklickém zápisu zapsat právě 4 způsoby a v neredukovaném cyklickém zápisu právě $4 \cdot 3! = 24$ způsoby. □

4.2. Mějme permutace $p = (1298)(36)(574)$ a $q = (34875)$ z množiny S_9 v redukovaném cyklickém zápisu. Určete jejich maticový zápis.

Z cyklického zápisu permutace p vidíme, že $p(1) = 2$, $p(2) = 9$, $p(9) = 8$, $p(8) = 1$, $p(3) = 6$, $p(6) = 3$, $p(5) = 7$, $p(7) = 4$ a $p(4) = 5$. Nyní snadno tyto údaje zaznamenáme do matice

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 9 & 6 & 5 & 7 & 3 & 4 & 1 & 8 \end{pmatrix}.$$

Snadno rozšíříme redukovaný cyklický zápis permutace q na neredukovaný zápis $q = (34875)(1)(2)(6)(9)$ a obdobným způsobem jako u permutace p najdeme matici

$$q = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 4 & 8 & 3 & 6 & 5 & 7 & 9 \end{pmatrix}.$$

□

4.3. Nechť $p = (135)(4798)(26)$ a $q = (18)(247693)$ jsou dvě permutace z S_9. Určete permutace $p \circ q$, $q \circ p$, p^{-1} a q^{-1}.

Nejprve přímo použitím definice snadno zjistíme hodnoty (skládáme zprava doleva):

$$p \circ q = (1495)(27)(368), \quad q \circ p = (129)(3587)(46).$$

Dále snadno nahlédneme, že inverzní permutací je právě „zrcadlový obraz" permutace, tedy

$$p^{-1} = (62)(8974)(531), \quad q^{-1} = (18)(239674).$$

□

4.4. Určete znaménka permutací p a q z předchozí úlohy.

Použijeme-li Lemma 5.6 z přednášky, stačí, abychom spočítali počet cyklů v neredukovaném cyklickém zápisu každé z permutací. V obou případech vidíme, že $p = (135)(4798)(26)$ i $q = (18)(247693)(5)$ obsahují 3 cykly, proto $\operatorname{sgn} p = \operatorname{sgn} q = (-1)^{9-3} = 1$. □

4.5. Určete znaménka permutací $p = (17)(36)(2458)$, p^{-1}, $q = (245)(3687)$, $r = (13)(2675), p \circ q \circ r, q^{-1} \circ r \circ p^{-1} \circ q \in S_8$.

Nejprve opět použijeme Lemma 5.6, abychom zjistili, že

$$\begin{aligned} \operatorname{sgn} p &= \operatorname{sgn}\ ((17)(36)(2458)) = (-1)^{8-3} = -1, \\ \operatorname{sgn} q &= \operatorname{sgn}\ ((1)(245)(3687)) = (-1)^{8-3} = -1, \\ \operatorname{sgn} r &= \operatorname{sgn}\ ((13)(2675)(4)(8)) = (-1)^{8-4} = 1. \end{aligned}$$

V předchozí úloze jsme si mohli všimnout, že inverzní permutace má stejně cyklů jako permutace původní, proto $\operatorname{sgn} p^{-1} = \operatorname{sgn} p = -1$. Konečně Tvrzení 5.5 nám říká, že znaménko složení permutací se rovná součinu znamének, proto

$$\operatorname{sgn}\ (p \circ q \circ r) = \operatorname{sgn} p \cdot \operatorname{sgn} q \cdot \operatorname{sgn} r = (-1) \cdot (-1) \cdot 1 = 1$$

Spojením posledních dvou pozorování dostáváme:

$$\text{sgn }(q^{-1}\circ r\circ p^{-1}\circ q) = \text{sgn }q\cdot\text{sgn }r\cdot\text{sgn }p\cdot\text{sgn }q = \text{sgn }r\cdot\text{sgn }p = -1.$$

□

4.6. Napište permutace $p = (13475)$ a $q = (19)(267)(3548)$ z S_9 jako součin transpozic.

Připomeňme, že transpozice je permutace, která vyměňuje právě dva prvky, tj. můžeme ji v redukovaném cyklickém zápisu zapsat ve tvaru (ab). Řešení úlohy pro permutaci p je zřejmé z Lemmatu 5.2, konkrétně

$$(13475) = (15)\circ(17)\circ(14)\circ(13) = (13)\circ(34)\circ(47)\circ(75).$$

Přímo z definice cyklického zápisu vidíme, že $(19)(267)(3548) = (19)\circ(267)\circ(3548)$, tedy nejprve úlohu vyřešíme pro každý z cyklů (19), (267) a (3548) pomocí Věty 6.9 a poté nalezené transpozice složíme, tedy

$$(19)(267)(3548) = (19)\circ(267)\circ(3548) =$$

$$= (19)\circ(27)\circ(26)\circ(38)\circ(34)\circ(35) = (19)\circ(26)\circ(67)\circ(35)\circ(54)\circ(48).$$

□

Další úlohy

(1) Buď T těleso $\cdot$ a nechť $a, b \in T$. Jestliže $a\cdot a = b\cdot b$, dokažte z axiomatiky tělesa, že nutně $a = b$ nebo $a = -b$.
(2) Spočítejte v tělese $\mathbf{Z}_{83}$ hodnoty 15^{-1} a $(3^{-1} + 6\cdot 53^{-1})^{-1}$.
(3) Vyřešte v tělese $\mathbf{Z}_{97}$ rovnici $7\cdot x + 3 = 51^{-1} + 17$.
(4) Existují-li najděte inverzní matice k maticím $\begin{pmatrix}11 & 12\\ 13 & 14\end{pmatrix}$, $\begin{pmatrix}8 & 9 & 9\\ 9 & 8 & 9\\ 9 & 9 & 8\end{pmatrix}$ a $\begin{pmatrix}15 & 16 & 3\\ 9 & 0 & 5\\ 12 & 0 & 15\end{pmatrix}$ nad tělesy $\mathbf{Z}_{17}$, $\mathbf{Z}_{19}$, $\mathbf{Z}_{53}$ a $\mathbf{Z}_{103}$.
(5) Rozhodněte, zda je posloupnost vektorů $(1,3,2,1)^T, (3,0,1,1)^T, (1,4,2,4)^T$ lineárně závislá ve vektorovém prostorech $\mathbf{R}^4$, $\mathbf{C}^4$, $\mathbf{Z}_5^4$ a $\mathbf{Z}_7^4$.
(6) Určete bázi a dimenzi podprostoru $\mathbf{L}((1,3,2,1)^T, (3,0,1,1)^T, (1,4,2,4)^T)$ vektorových prostorů $\mathbf{R}^4$, $\mathbf{C}^4$, $\mathbf{Z}_5^4$ a $\mathbf{Z}_7^4$.
(7) Najděte všechny podmnožiny množiny $X = \{(1,2,1,1,1)^T, (3,1,3,3,3)^T, (2,4,2,2,2)^T, (1,0,1,3,2)^T\}$, které tvoří bázi podprostoru $U = \mathbf{L}(X)$ vektorových prostorů $\mathbf{Q}^5$, $\mathbf{Z}_5^5$, $\mathbf{Z}_7^5$.
(8) Kolik existuje bází podprostoru $\mathbf{L}((1,1,2,0)^T, (4,1,3,1)^T, (1,3,2,1)^T)$ vektorových prostorů $\mathbf{Z}_5^4$ a $\mathbf{Z}_7^4$?
(9) Určete dimenze podprostorů $\mathbf{U}$, $\mathbf{V}$, $\mathbf{U}+\mathbf{V}$ a $\mathbf{U}\cap\mathbf{V}$ vektorových prostorů $\mathbf{Z}_5^4$ nad tělesem $\mathbf{Z}_5$ a $\mathbf{Z}_7^4$ nad tělesem $\mathbf{Z}_7$, jestliže $\mathbf{U} = \mathbf{L}((1,2,1,3)^T, (1,2,4,1)^T, (3,4,1,0)^T)$ a $\mathbf{V} = \mathbf{L}((4,1,2,3)^T, (0,3,3,1)^T, (1,2,1,3)^T)$.

(10) Určete nad tělesy $\mathbf{R}$, $\mathbf{Z}_5$ a $\mathbf{Z}_7$ hodnost matice $\mathbf{A} = \begin{pmatrix} 2 & 0 & 1 \\ 2 & 1 & 0 \\ 3 & 3 & 1 \end{pmatrix}$, matice $\mathbf{A}+\mathbf{A}$ a $\mathbf{A}\cdot\mathbf{A}$.

(11) Najděte nad tělesy $\mathbf{R}$, $\mathbf{Z}_5$ a $\mathbf{Z}_7$ všechna řešení homogenní soustavy rovnic s maticí $\mathbf{A}$ z předchozí úlohy.

(12) Najděte nad tělesy $\mathbf{Q}$, $\mathbf{Z}_3$ a $\mathbf{Z}_7$ všechna řešení nehomogenní soustavy rovnic s maticí $\left(\begin{array}{ccccc|c} 1 & 0 & 1 & 2 & 2 & 2 \\ 2 & 0 & 2 & 1 & 1 & 0 \end{array}\right)$.

(13) Je-li podprostor $\mathbf{U} = \mathbf{L}((2,4,0,1,4)^T, (1,2,1,0,3)^T)$ vektorového prostoru $\mathbf{Z}_5^5$ nad tělesem $\mathbf{Z}_5$, najděte bázi nějakého takového podprostoru $\mathbf{V}$, aby $\mathbf{U}+\mathbf{V} = \mathbf{Z}_5^5$ a $\mathbf{U}\cap\mathbf{V} = \{\mathbf{0}\}$.

(14) Uvažujme podprostor $\mathbf{W} = \mathbf{L}((1,6,2,4,5)^T)$ vektorového prostoru $\mathbf{Z}_7^5$ nad tělesem $\mathbf{Z}_7$. Najděte báze nějakých takových podprostorů $\mathbf{U}$ a $\mathbf{V}$, aby $\dim(\mathbf{U})^T = \dim(\mathbf{V})^T = 3$, $\mathbf{U}+\mathbf{V} = \mathbf{Z}_7^5$ a $\mathbf{U}\cap\mathbf{V} = \mathbf{W}$.

(15) Kolika způsoby lze lineárně nezávislou posloupnost $((1,2,2,1)^T, (2,1,1,0)^T)$ doplnit na bázi (chápanou jako posloupnost, tj. záleží na pořadí prvků) vektorového prostoru $\mathbf{Z}_3^4$?

(16) Buď $k \leq n$ přirozená čísla, p prvočíslo a $\mathbf{U}$ podprostor dimenze k vektorového prostoru $\mathbf{Z}_p^n$ nad tělesem $\mathbf{Z}_p$. Určete kolik existuje podprostorů $\mathbf{V}$ prostoru $\mathbf{Z}_p^n$, pro něž platí, že $\mathbf{U}+\mathbf{V} = \mathbf{Z}_5^5$ a $\mathbf{U}+\mathbf{V} = \{\mathbf{0}\}$.

(17) Dokažte, že lze nad tělesem racionálních čísel převést posloupností elementárních řádkových úprav matici $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \end{pmatrix}$ na matici $\mathbf{B} = \begin{pmatrix} 1 & 0 & -1 \\ 1 & 3 & 5 \end{pmatrix}$.

(18) Uvažujme matice $\mathbf{A}$ a $\mathbf{B}$ z předchozího příkladu. Najděte nějakou posloupností elementárních řádkových úprav, pomocí nichž lze převést matici $\mathbf{A}$ na matici $\mathbf{B}$.

(19) Rozhodněte, zda lze nad reálnými čísly převést posloupností elementárních řádkových úprav matici $\mathbf{A}$ na matici $\mathbf{B}$, kde $\mathbf{A} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 1 & 1 \end{pmatrix}$ a $\mathbf{B} = \begin{pmatrix} 1 & 0 & -1 \\ 1 & 2 & 1 \end{pmatrix}$.

(20) Mějme $p = (174)(256), q = (134765) \in S_7$. Určete permutace $p\circ q$, $q\circ p$, $p^{-1}\circ q$ a $q^{-1}\circ p^{-1}$ a $q\circ q$ najděte u všech těchto permutací jejich rozklad na transpozice.

(21) Mějme $p = (1278)(356), q = (13)(4765) \in S_8$. Určete znaménka permutací $p\circ q$, $q\circ p$, $p^{-1}\circ q$ a $q^{-1}\circ p^{-1}$ a $q\circ q$ najděte u všech těchto permutací jejich rozklad na transpozice.