4.10.

Buď n přirozené číslo a položme $\mathbf{Z}_n = \{0, 1, \ldots, n-1\}$. Definujme na $\mathbf{Z}_n$ binární operace $+$ a $\cdot$ předpisem $a + b = (a + b) \mathrm{mod} n$ a $a \cdot b = (a \cdot b) \mathrm{mod} n$, kde vlevo vždy uvažujeme standardní sčítání a násobení celých čísel a mod$n$ znamená zbytek po celočíselném dělení hodnotou n.

1.1. Najděte všechny podalgebry algebry $(\mathbf{Z}_5, +)$.

Připomeňme, že podalgebrou rozumíme jakoukoli neprázdnou podmnožinu P množiny $\mathbf{Z}_5$, která je uzavřená na všechny operace dané algebry, v daném případě tedy na jedinou operaci $+$. Dále připomeňme, že neprázdný průnik podalgeber je opět podalgebra, díky čemuž můžeme postupně uvažovat nejmenší podalgebry $(\mathbf{Z}_5, +)$ obsahující podmnožinu G, které budeme značit $\langle G \rangle$ (resp. $\langle g_1, \ldots, g_n \rangle$ místo $\langle \{g_1, \ldots, g_n\} \rangle$) a nazývat podalgebrami generovanými množinou G.

Nejprve uvážíme podalgebry generované jednoprvkovou množinou. Všimněme si, že

$$\langle 0 \rangle = \{0\} \text{ a } \langle 1 \rangle = \{1, 1+1, 1+1+1, 1+1+1+1, 1+1+1+1+1\} = \mathbf{Z}_5.$$

Nyní stačí nahlédnout, že součtem b kopií prvku a dostaneme právě hodnotu $a \cdot b$ (samozřejmě s násobením modulo 5) a že umíme pro každé $a \in \{2, 3, 4\}$ najít b, jímž je právě inverzní prvek v tělese $\mathbf{Z}_5$, pro který $a \cdot b = 1$. To znamená, že $1 \in \langle 2 \rangle$, $1 \in \langle 3 \rangle$ a $1 \in \langle 4 \rangle$, a proto

$$\mathbf{Z}_5 = \langle 1 \rangle = \langle 2 \rangle = \langle 3 \rangle = \langle 4 \rangle.$$

Konečně, všechny aspoň dvouprvkové množiny už zřejmě generují celé $\mathbf{Z}_5$. Zjistili jsme, že algebra $(\mathbf{Z}_5, +)$ obsahuje právě dvě podalgebry $\{0\}$ a $\mathbf{Z}_5$. □

1.2. Najděte všechny podalgebry algebry $(\mathbf{Z}_5, \cdot)$.

Uvažujeme podobně jako v předchozí úloze. Nejprve vidíme, že

$$\langle 0 \rangle = \{0\}, \quad \langle 1 \rangle = \{1\}, \quad \langle 2 \rangle = \{2, 4, 3, 1\}, \quad \langle 3 \rangle = \{3, 4, 2, 1\}, \quad \langle 4 \rangle = \{4, 1\}.$$

Snadno nahlédneme, že pro podlagbery $\langle a, b \rangle$, kde $a \neq 0 \neq b$, buď $\langle a, b \rangle = \langle a \rangle$ nebo $\langle a, b \rangle = \langle b \rangle$, a $\langle a, 0 \rangle = \langle a \rangle \cup \{0\}$. Konečně třígenerované podalgebry žádné nové příklady zřejmě nedají, tedy

$$\{0\}, \{1\}, \{0, 1\}, \{1, 4\}, \{0, 1, 4\}, \{1, 2, 3, 4\}, \mathbf{Z}_5$$

jsou právě všechny podalgebry $(\mathbf{Z}_5, \cdot)$. □

1.3. Najděte všechny podalgebry algebry $(\mathbf{Z}_5, +, \cdot, 0)$.

Tentokrát buď vezmem průnik systémů podalgeber z úloh 1.1, 1.2 a všimneme si, že obě podmnožiny obsahují 0 nebo uvážíme, že násobení i 0 dostaneme iterováním sčítání (u nuly právě pětkrát), tedy hledaný systém všech podalgeber je totožný s nalezeným systémem v úloze 1.1. □

1.4. Najděte všechny podalgebry algebry $(\mathbf{Z}_{10}, +, 0)$.

Postupujeme jako v 1.1. Snadno si opět uvědomíme, že $\langle 0\rangle = \{0\}$, každá podlagebra algebry $(\mathbf{Z}_{10}, +, 0)$ musí obsahovat 0 a dále, že

$$\langle 1\rangle = \langle 3\rangle = \langle 7\rangle = \langle 9\rangle = \mathbf{Z}_{10},\ \langle 2\rangle = \langle 4\rangle = \langle 6\rangle = \langle 8\rangle = \{0,2,4,6,8\},\ \langle 5\rangle = \{0,5\}$$

Připomeňme, že pomocí Eukleidova algoritmu umíme pro každá dvě kladná celá čísla a, b najít celá čísla u a v, aby $\mathrm{NSD}(a,b) = ua+vb$ a odtud snadno nahlédneme, že $\langle a,b\rangle = \langle \mathrm{NSD}(a,b)\rangle$. To ovšem znamená, že $\{0\}$, $\{0,5\}$, $\{0,2,4,6,8\}$ a $\mathbf{Z}_{10}$ jsou právě všechny podalgebry algebry $(\mathbf{Z}_{10}, +, 0)$. □

11.10.

Všimněm se, že bychom úvahou z předchozí úlohy uměli dokázat, že pro každou podalgebru P algebry $(\mathbf{Z}_n, +)$ existje takové $a \in \mathbf{Z}_n$, pro něž $P = \langle a\rangle$. Protože bude pozorování později dokázáno na přednášce, upustíme pro tento okamžik od důkazu a vezmeme ho jako fakt.

V následujícím textu budeme největšího společného dělitele čísel a_0 a a_1 značit $\mathrm{NSD}(a_0, a_1)$

1.5. Dokažte, že pro každé $a \in \mathbf{Z}_n$ existuje takové k, že buď k/n nebo $k = 0$ a $\langle a\rangle = \langle k\rangle$.

Předně poznamenejme, že pro $a = 0$ vezmeme $k = 0$. Předpokládejme, že $k > 0$, a položme $k = \mathrm{NSD}(a,b)$. Protože k/a, máme $a \in \langle k\rangle$, a tedy $\langle a\rangle \subseteq \langle k\rangle$, protože $\langle a\rangle$ je nejmenší podalgebra vzhledem k inkluzi obsahující prvek a a o podalgebře $\langle k\rangle$ jsme ukázali, že prvek a rovněž obsahuje. Eukleidův algoritmus nám zajišťuje existenci celých čísel u a v, pro něž $k = \mathrm{NSD}(a,n) = ua + vn$, navíc můžeme vzít u kladné, proto $k = (u \cdot a)\mathrm{mod}n \in \langle a\rangle$. Dostali jsme i druhou inkluzi $\langle k\rangle \subseteq \langle a\rangle$, tudíž $\langle a\rangle = \langle k\rangle$. □

1.6. Najděte všechny podalgebry algebry $(\mathbf{Z}_{15}, +, \cdot)$.

Předchozí úvahy nám říkají, že se stačí omezit na podmnožiny uzavřené na $+$ (viz 1.3) a hledané podalgebry jsou tvaru $\langle k\rangle = k\mathbf{Z}_{15} = \{k \cdot x |\ x \in \mathbf{Z}_{15/k}\}$ pro k/n nebo $k = 0$ (viz 1.4 a 1.5). To znamená, že

$$0\mathbf{Z}_{15} = \{0\},\ 5\mathbf{Z}_{15} = \{0,5,10\},\ 3\mathbf{Z}_{15} = \{0,3,6,9,12\},\ 1\mathbf{Z}_{15} = \mathbf{Z}_{15}$$

jsou právě všechny podalgebry algebry $(\mathbf{Z}_{15}, +, \cdot)$. □

1.7. Kolik existuje podalgeber algebry $(\mathbf{Z}_{1100}, +)$.

Uvážili jsme, že pro každý dělitel čísla 1100 existuje právě jedna podalgebra algebry $(\mathbf{Z}_{1100}, +)$. Protože $1100 = 2^2 \cdot 5^2 \cdot 11^1$, máme právě $3 \cdot 3 \cdot 2 = 18$ jeho dělitelů, tedy algebra $(\mathbf{Z}_{1100}, +)$ obsahuje 18 podalgeber. □

1.8. Najděte všechny podalgebry algebry $(\mathbf{Z}_6, 1)$.

Jediný požadavek, který tentokrát klademe na podalgebru, je, aby šlo o množinu obsahující prvek 1, snadno nahlédneme, že takových množin máme k dispozici právě $2^5 = 32$. □

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

Známe-li a_{i-1} a a_i spočteme $a_{i+1} = (a_{i-1}) mod\ a_i$. 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 $a_n = \mathrm{NSD}(a_0, a_1)$.

1.9. Najděte pomocí Eukleidova algoritmu největší společný dělitel čísel 72 a 93. Najděte dále taková celá čísla x a y, aby $\mathrm{NSD}(72, 93) = x.72 + y.93$.

První část úkolu je snadná, sepišme si i jakým způsobem jednotlivé zbytky po celočíselném dělení získáme:
$a_0 = 93$,
$a_1 = 72$,
$a_2 = 93 - 72 = 21$,
$a_3 = 72 - 3.21 = 9$,
$a_4 = 21 - 3.9 = 3 = \mathrm{NSD}(93, 72)$
$a_5 = 0$.
Druhou část úlohy vyřešíme rovněž pomocí Eukleidova algoritmu, stačí si uvědomit, že každé z čísel a_{i+1} dostaneme jako celočíselnou lineární kombinaci dvou předchozích hodnot a_{i-1} a a_i. Jednoduchou indukční úvahou zjistíme, že každé číslo a_{i+1} je celočíselnou lineární kombinaci hodnot a_0 a a_1. Konkrétně:
$a_2 = 93 - 72 = 21$,
$a_3 = 9 = 72 - 3.21 = 72 - 3.(93 - 72) = 4.72 - 3.93$,
$a_4 = 3 = \mathrm{NSD}(93, 72) = 21 - 2.9 = (93 - 72) - 2.(4.72 - 3.93) = 7.93 - 9.72$.
Zjistili jsme, že $x = -9$ a $y = 7$. □

1.10. Najděte celá čísla x a y tak, aby $x.18 + y.25 = 1$.

Protože $\mathrm{NSD}(18, 25) = 1$, zaručuje nám Eukleidův algoritmus existenci požadovaných čísel $x, y \in \mathbf{Z}$ a tento algoritmus použijeme podobně jako v předchozí úloze i k jejich nalezení:
$a_0 = 25$,
$a_1 = 18$,
$a_2 = 7 = 25 - 18$,
$a_3 = 4 = 18 - 2 \cdot 7 = 18 - 2 \cdot (25 - 18) = 3 \cdot 18 - 2 \cdot 25$,
$a_4 = 3 = 7 - 4 = 25 - 18 - (3 \cdot 18 - 2 \cdot 25) = 3 \cdot 25 - 4 \cdot 18$,
$a_5 = \mathrm{NSD}(25, 18) = 1 = 4 - 3 = 3 \cdot 18 - 2 \cdot 25 - (3 \cdot 25 - 4 \cdot 18) = 7 \cdot 18 - 5 \cdot 25$. □

18.10.

1.11. Najděte celočíselné řešení rovnice $x \cdot 18 + y \cdot 25 = 10$.

Vynásobíme-li již vyřešenou rovnici $7 \cdot 18 - 5 \cdot 25 = 1$ desítkou, okamžitě vidíme, že rovnici $x \cdot 18 + y \cdot 25 = 10$ řeší $x = 10 \cdot 7 = 70$ a $y = -5 \cdot 10 = -50$. □

Definujme nyní pro každé $k \in \mathbf{Z}_{217}$ zobrazení $f_k : \mathbf{Z}_{217} \to \mathbf{Z}_{217}$ ppředpisem $f_k(x) = (k \cdot x) \mathrm{mod} 217$.

1.12. Rozhodněte, zda existuje $x \in \mathbf{Z}_{217}$, aby $f_k(x) = 11$, jestliže a) $k = 100$, b) $k = 98$. Existuje-li řešení, najděte ho a rozhodněte, zda je určeno jednoznačně.

a) Hledáme $x \in \mathbf{Z}_{217}$, pro které existuje $y \in \mathbf{Z}$ splňující podmínku $100x + 217y = 11$. Díky Eukleidovu algoritmu a faktu, že $\mathrm{NSD}(100, 217) = 1$ dokonce víme, že lze vyřešit rovnici $100x + 217y = c$ opro každé $c \in \mathbf{Z}_{217}$, tedy zobrazení f_{100} je na

celou množinu $\mathbf{Z}_{217}$. Protože ovšem zobrazuje konečnou množinu do sebe, musí jít i o prosté zobrazení, tedy existuje pr8v2 jedno řešení vztahu $f_{100}(x) = 11$. Zbývá ho najít stejnou cestou jako v předchozí úloze:

$17 = 217 - 2 \cdot 100$,

$15 = 100 - 5 \cdot 17 = 100 - 5 \cdot (217 - 2 \cdot 100) = 11 \cdot 100 - 5 \cdot 217$,

$2 = 17 - 15 = 217 - 2 \cdot 100 - (11 \cdot 100 - 5 \cdot 217) = 6 \cdot 217 - 13 \cdot 100$,

$1 = 15 - 7 \cdot 2 = 11 \cdot 100 - 5 \cdot 217 - 7 \cdot (6 \cdot 217 - 13 \cdot 100) = 102 \cdot 100 - 47 \cdot 217$.

Proto $11 \cdot 102 \cdot 100 - 11 \cdot 47 \cdot 217 = 11$, tedy $x = (11 \cdot 102) \mathrm{mod} 217 = 37$. Všimněme si, že z druhého a třetího kroku Eukleidova algoritmu jsme přímo mohli dostat

$$11 = 15 - 2 \cdot 2 = 11 \cdot 100 - 5 \cdot 217 - 2 \cdot (6 \cdot 217 - 13 \cdot 100) = 37 \cdot 100 - 17 \cdot 217.$$

b) Tentokrát se ptáme, zda existuje $x \in \mathbf{Z}_{217}$ a $y \in \mathbf{Z}$, pro něž $98x + 217y = 11$. Protože 7 dělí 98 i 217, muselo by 7 dělit také číslo 11, což není pravda, proto takové x neexistuje. □

1.13. Rozhodněte, zda existuje a zda je určeno jednoznačně $x \in \mathbf{Z}_{217}$, aby $f_{98}(x) = 21$.

Uvažujem stejně jako v předchozí úloze. Hledáme tedy $x \in \mathbf{Z}_{217}$ a $y \in \mathbf{Z}$, pro něž $98x + 217y = 21$. Protože $\mathrm{NSD}(98, 217) = 7$ dělí 21 zaručuje nám Eukleidův algoritmus opět existenci řešení. Konkrétně hned v prvním kroku zjistíme, že $21 = 217 - 2 \cdot 98$, tedy $x = (-2) \mathrm{mod} 217 = 215$. Navíc $(98 \cdot 31) \mathrm{mod} 217 = 0$, proto $x = -2 + 31 = 29$ také řeší $f_{98}(x) = 21$. □

1.14. Rozhodněte, pro která k je zobrazení f_k homomorfismem a) algebry $(\mathbf{Z}_{217}, +)$ do sebe b) algebry $(\mathbf{Z}_{217}, +, \cdot)$ do sebe, kde uvažujeme operace modulo 217.

a) Snadno nahlédneme, že pro každé $a, b \in \mathbf{Z}_{217}$

$$f_k(a + b) = ((a + b) \cdot k) \mathrm{mod} 217 = (a \cdot k + b \cdot k) \mathrm{mod} 217 = f_k(a) + f_k(b),$$

tedy f_k je homomorfismus pro všechna $k \in \mathbf{Z}_{217}$.

b) Právě jsme ověřili, že vzhledem k první operaci je zobrazení f_k slučitelné pro všechna k. Dále je zjevně splněna podmínka $f_1(a \cdot b) = a \cdot b = f_1(a) \cdot f_1(b)$ a $f_0(a \cdot b) = 0 = f_0(a) \cdot f_0(b)$. Konečně jakmile $k = f_k(1 \cdot 1) = f_k(1) \cdot f_k(1) = k \cdot k$, tedy musí $217 / k^2 - k$. Snadno ovšem nahlédneme, že to platí pouze pro $k = 0$ nebo $k = 1$. Tedy jsme zjistili, že f_k je homomorfismus algebry $(\mathbf{Z}_{217}, +, \cdot)$ do sebe pouze pro $k \in \{0, 1\}$.

□

Uvažujme v dalším množinu $A = \{a, b, c\}$ s binárními operacemi $\circ$ a $\star$ danými tabulkami:

$\circ$	**a**	**b**	**c**
a	c	b	a
b	b	a	b
c	a	b	c

$\star$	**a**	**b**	**c**
a	a	b	c
b	b	c	a
c	c	a	b

1.15. Najděte všechny podalgebry algebry $(A, \circ)$.

Předně si uvědomme, že celá nosná množina A je podalgebrou každé algebry (s nosnou množinou A). Dále budeme postupně probírat podalgebry podle počtu prvků.

Je-li $\{x\}$ jednoprvková podalgebra A, zřejmě musí platit $x \circ x = x$, protože množina $\{x\}$ má být uzavřená na operaci $\circ$. Snadno z tabulky vyčeme, že takovou vlastnost (mluvíme o idempotenci) splňuje pouze prvek c. Tedy máme právě jednu jednoprvkovou podalgebru c algebry $A(\circ)$.

Dále uvažme, které z dvou prvkových podmnožin $\{a, b\}$, $\{a, c\}$ a $\{b, c\}$ jsou podalgebry. Zjevně podalgebra obsahující prvek a už musí obsahovat i prvek $c = a \circ a$, tedy $\{a, b\}$ není podalgebrou. Podobně podalgebra obsahující prvkek b musí obsahovat i prvek $a = b \circ b$, tedy ani $\{b, c\}$ není podalgebrou. Konečně z tabulky vidíme, že množina $\{a, c\} = \langle a \rangle$ je uzavřená na operaci $\circ$, tedy $\{a, c\}$ je jedinou dvouprvkovou podalgebra algebry $(A, \circ)$.

Dostáváme systém všech podalgeber: $\{c\}, \{a, c\}, \{a, b, c\}$. □

1.16. Najděte všechny podalgebry algebry $(A, \circ, a)$, kde a označuje nulární operaci vyznačující prvek a.

V předchozí úloze jsme našli všechny podmnožiny množiny A uzavřené na operaci $\circ$, z nichž potřebujeme nyní vybrat podmnožiny uzavřené na nulární operaci a, tedy právě ty, které obsahují prvek a. Podalgebry algebry $(A, \circ, a)$ jsou tedy zřejmě právě množiny $\{a, c\}, \{a, b, c\}$. □

1.17. Najděte všechny podalgebry algebry $(A, \circ, \star)$.

Tentokrát vybíráme ze systému množin uzavřených na operaci $\circ$ ty, které jsou navíc uzavřené na $\star$. Protože $c \star c = b$, zbývá nám pouze množina A. □

Další úlohy

(1) Najděte všechny podalgebry a kongruence algebry $C = \{a, b, c, d, e, f\}$ s jednou binární operací danou předpisem $x \odot y = x$.
(2) Uvažujme množinu $\mathbf{Z}_n$ s unární operací $^+$ definovanou předpisem $a^+ = (a+1) mod\ n$. Popište všechny podalgebry a všechny kongruence na $\mathbf{Z}_n(^+)$.
(3) Najděte všechna celočíselná řešení rovnice $324 \cdot x + 88 \cdot y = c$ postupně pro $c = 0, 2, 88, -4, -88$.
(4) Najděte všechna celočíselná řešení rovnice $15 \cdot x - 44 \cdot y = c$ postupně pro $c = 1, 2, -2$.
(5) Najděte (všechna) celočíselná řešení rovnice $15 \cdot x + 18 \cdot y + 10 \cdot z = 1$.
(6) Spočítejte v tělese $\mathbf{Z}_{83}$ hodnoty 15^{-1} a $(3^{-1} + 6 \cdot 53^{-1})^{-1}$.
(7) Vyřešte v tělese $\mathbf{Z}_{97}$ rovnici $7^{-1} \cdot x = 51^{-1}$.
(8) Ověřte, že Eukleidův algoritmus pracuje správně.