## 1. teorie (1 bod)

Definujte relaci uspořádání. Co je to lineární uspořádání?

Buď $(X, \leq)$ uspořádaná množina a $A \subseteq X$. Definujte supremum množiny $A$.

Buď $(X, \leq)$ uspořádaná množina a $A \subseteq X$. Definujte infimum množiny $A$.

Buď $(X, \leq)$ uspořádaná množina. Definujte maximální a největší prvek.

Buď $(X, \leq)$ uspořádaná množina. Definujte minimální a nejmenší prvek.

Uveďte definici svazu a úplného svazu pomocí relace uspořádání.

Uveďte definici svazu jako algebry $(X, \vee, \wedge)$.

Definujte Booleovu algebru.

Uveďte definici Lindenbaumovy algebry dané teorie.

## 2. teorie (1 bod)

Buď $\mathbf{A} = (A, *)$ algebra typu (2) a $X \subseteq A$. Co značí $\langle X \rangle_{\mathbf{A}}$?

Buď $\mathbf{A} = (A, ', c)$ algebra typu (1,0) a $X \subseteq A$. Co značí $\langle X \rangle_{\mathbf{A}}$?

Uveďte definici podalgebry algebry $(A, *, +)$ typu (2,2).

Uveďte definici podalgebry algebry $(A, -, c)$ typu (1,0).

Uveďte definici podalgebry algebry $(A, +, a)$ typu (2,0).

Uveďte definici direktního součinu algeber $(A, *, +)$ a $(B, \circ, \cdot)$ typu (2,2).

Uveďte definici direktního součinu algeber $(A, ', u)$ a $(B, f, v)$ typu (1,0).

Uveďte definici homomorfismu mezi algebrami $(A, *, \cdot)$ a $(B, +, \circ)$ typu (2,2).

Uveďte definici homomorfismu mezi algebrami $(A, f, a)$ a $(B, ', b)$ typu (1,0).

Uveďte definici homomorfismu mezi algebrami $(A, +, a)$ a $(B, \circ, b)$ typu (2,0).

Uveďte definici izomorfismu. Co to znamená, že jsou dvě algebry izomorfní?

Definujte podgrupu dané grupy $\mathbf{G} = (G, \cdot, ^{-1}, 1)$.

Buď $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ grupa a $X \subseteq G$. Co značí $\langle X \rangle_{\mathbf{G}}$?

Buď $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ a $\mathbf{H} = (H, *, ', e)$ grupy. Definujte homomorfismus $\mathbf{G} \to \mathbf{H}$.

Buď $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ a $\mathbf{H} = (H, *, ', e)$ grupy a $\varphi : \mathbf{G} \to \mathbf{H}$ homomorfismus. Co se rozumí jeho jádrem a obrazem?

Buď $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ a $\mathbf{H} = (H, *, ', e)$ grupy. Definujte direktní součin $\mathbf{G} \times \mathbf{H}$.

## 3. teorie (1 bod)

Uveďte definici kongruence dané algebry $(A, \circ, *)$ typu (2,2).

Uveďte definici kongruence dané algebry $(A, f, a)$ typu (1,0).

Uveďte definici kongruence dané algebry $(A, \cdot, c)$ typu (2,0).

Uveďte definici normální podgrupy dané grupy $\mathbf{G} = (G, *, ', e)$.

Jak souvisí normální podgrupy s kongruencemi?

Uveďte definici faktorgrupy grupy $\mathbf{G} = (G, *, ', e)$ podle normální podgrupy $\mathbf{H}$ (včetně definice operací).

Uveďte definici faktoralgebry algebry $(A, \cdot, \circ)$ typu (2,2) podle kongruence $\sim$ (včetně definice operací).

Uveďte definici faktoralgebry algebry $(A, f, a)$ typu (1,0) podle kongruence $\sim$ (včetně definice operací).

Uveďte definici faktoralgebry algebry $(A, \cdot, c)$ typu (2,0) podle kongruence $\sim$ (včetně definice operací).

Uveďte 1. větu o izomorfismu pro grupy.

Uveďte 1. větu o izomorfismu pro obecné algebry.

## 4. teorie (1 bod)

Uveďte definici termu a uzavřené formule daného typu (jazyka).

Uveďte definici absolutně volné algebry daného typu (jazyka).

Definujte, co znamená zápis $a \equiv b \pmod{n}$, a uveďte základní vlastnosti.

Definujte Eulerovu funkci a napište Eulerovu větu.

Definujte Eulerovu funkci a uveďte vzorec pro její výpočet.

Uveďte definici abelovské grupy.

Uveďte definici grupy.

Napište nějakou množinu generátorů grupy $\mathbf{S}_n$ velikosti $\leq n^2$.

Napište nějakou množinu generátorů grupy $\mathbf{A}_n$ velikosti $\leq n^3$.

Definujte znaménko permutace a grupu $\mathbf{A}_n$.

## 5. teorie (1 bod)

Definujte grupu $\mathbf{T}^*$ pro dané těleso $\mathbf{T}$. Za jakých podmínek je cyklická?

Definujte grupu $\mathbb{Z}_n^*$. Jaké má prvky?

Uveďte nějaký postup na výpočet inverzního prvku v grupě $\mathbb{Z}_n^*$.

Definujte řád prvku $a$ grupy $\mathbf{G} = (G, \cdot, ^{-1}, 1)$.

Definujte cyklickou grupu.

Uveďte všechny (až na izomorfismus) cyklické grupy.

Kolik má daná cyklická grupa generátorů?

Uveďte větu o cykličnosti podgrup multiplikativních grup těles.

Definujte diskrétní logaritmus o základu $a$ v cyklické grupě $\mathbf{G} = (G, *, ', e)$.

Uveďte Diffie-Helmanův protokol na výměnu klíče.

## 6. teorie (1 bod)

Napište, co rozumíme rozkladem grupy $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ podle podgrupy $\mathbf{H}$. Co rozumíme rozkladovou třídou a transverzálou?

Napište, co rozumíme rozkladem grupy $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ podle podgrupy $\mathbf{H}$ a uveďte základní vlastnosti.

Napište Lagrangeovu větu. Co přesně značí $[\mathbf{G} : \mathbf{H}]$ ?

Jaký je vztah řádu grupy a řádů jejích prvků?

Jaký je vztah řádu grupy a řádů jejích podgrup?

Definujte relaci tranzitivity a orbitu daného působení grupy $\mathbf{G}$ na množině $X$.

Nechť grupa $\mathbf{G}$ působí na množinu $X$. Definujte $X_g$ a $G_x$ pro dané $g \in G$ a $x \in X$. Co je to pevný bod?

Nechť grupa $\mathbf{G}$ působí na množinu $X$ a buď $x \in X$. Napište vztah mezi velikostmi $G$, $G_x$ a $[x]$.

Napište Burnsideovu větu.

## 7. příklady (1 bod)

Uveďte příklad lineárního uspořádání na čtyřech prvcích.

Uveďte příklad uspořádání na dvou prvcích, které není lineární.

Uveďte příklad tříprvkového svazu.

Uveďte dva (neizomorfní) příklady čtyřprvkového svazu.

Uveďte příklad osmiprvkové Booleovy algebry.

Uveďte příklad úplného svazu, který není Booleovou algebrou.

Uveďte příklad lineárně uspořádané množiny, která není úplným svazem.

Tvoří konečné podmnožiny množiny $\mathbb{N}$ svaz vzhledem k uspořádání $\subseteq$? Stručně zdůvodněte.

Tvoří konečné podmnožiny množiny $\mathbb{N}$ úplný svaz vzhledem k uspořádání $\subseteq$? Stručně zdůvodněte.

Tvoří konečné podmnožiny množiny $\mathbb{N}$ Booleovu algebru vzhledem k uspořádání $\subseteq$? Stručně zdůvodněte.

Je každá lineárně uspořádaná množina svaz? Stručně zdůvodněte.

Je každá lineárně uspořádaná množina úplný svaz? Stručně zdůvodněte.

Existuje Booleova algebra, která je lineárně uspořádaná? Pokud ano, uveďte příklad, pokud ne, stručně zdůvodněte.

Existuje svaz, jehož každá podmnožina má infimum, ale nějaká podmnožina nemá supremum? Pokud ano, uveďte příklad, pokud ne, stručně zdůvodněte.

Nakreslete nejmenší uspořádanou množinu, která má maximální i minimální prvek, ale nemá největší ani nejmenší prvek.

Nakreslete nejmenší uspořádanou množinu, ve které má každá podmnožina supremum, ale nějaká podmnožina nemá infimum.

Nakreslete nejmenší uspořádanou množinu, která má aspoň tři maximální prvky a aspoň jeden nejmenší.

Nakreslete nejmenší uspořádanou množinu, která má aspoň tři maximální prvky a žádný nejmenší.

Nakreslete nejmenší uspořádanou množinu, která má aspoň tři maximální prvky a žádný největší.

Existuje uspořádaná množina, která má aspoň tři maximální prvky a jeden největší? Pokud ano, uveďte příklad, pokud ne, stručně zdůvodněte.

Existuje uspořádaná množina, která má aspoň tři maximální prvky a žádný minimální? Pokud ano, uveďte příklad, pokud ne, stručně zdůvodněte.

Existuje uspořádaná množina, která má aspoň tři maximální prvky a žádný nejmenší? Pokud ano, uveďte příklad, pokud ne, stručně zdůvodněte.

Existuje uspořádaná množina, která nemá žádný minimální ani maximální prvek? Pokud ano, uveďte příklad, pokud ne, stručně zdůvodněte.

Existuje uspořádaná množina taková, že každá její podmnožina má dolní i horní mez, ale přitom není svazově uspořádaná? Pokud ano, uveďte příklad, pokud ne, stručně zdůvodněte.

Existuje uspořádaná množina taková, že každá její podmnožina má dolní i horní mez, ale přitom není svazově uspořádaná? Pokud ano, uveďte příklad, pokud ne, stručně zdůvodněte.

Existuje uspořádaná množina, která má největší prvek, aspoň jeden minimální prvek a přitom není svaz? Pokud ano, uveďte příklad, pokud ne, stručně zdůvodněte.

Existuje uspořádaná množina s jedním největším a dvěma nejmenšími prvky? Pokud ano, uveďte příklad, pokud ne, stručně zdůvodněte.

Existuje svaz bez nejmenšího prvku? Pokud ano, uveďte příklad, pokud ne, stručně zdůvodněte.

Existuje svaz, který má právě tři minimální prvky? Pokud ano, uveďte příklad, pokud ne, stručně zdůvodněte.

Nakreslete nejmenší uspořádanou množinu, která není svazem.

Nakreslete nejmenší svaz, který není Booleovou algebrou.

Nakreslete svaz podmnožin tříprvkové množiny. Je to Booleova algebra?

Nakreslete svaz dělitelů čísla 42. Je to Booleova algebra?

Nakreslete svaz dělitelů čísla 81. Je to Booleova algebra?

Nakreslete svaz dělitelů čísla 100. Je to Booleova algebra?

Nakreslete svaz dělitelů čísla 48. Je to Booleova algebra?

Nakreslete svaz dělitelů čísla 70. Je to Booleova algebra?

## 8. příklady (1 bod)

Rozhodněte, zda konečné podmnožiny $\mathbb{N}$ tvoří podsvaz svazu $\mathbf{P}(\mathbb{N})$ podmnožin množiny $\mathbb{N}$. Stručně zdůvodněte.

Rozhodněte, zda podmnožiny sudé velikosti tvoří podsvaz svazu $\mathbf{P}(\{0,1,2,3\})$ podmnožin množiny $\{0,1,2,3\}$. Stručně zdůvodněte.

Rozhodněte, zda podmnožiny liché velikosti tvoří podsvaz svazu $\mathbf{P}(\{0,1,2,3\})$ podmnožin množiny $\{0,1,2,3\}$. Stručně zdůvodněte.

Rozhodněte, zda podmnožiny obsahující prvek 2 tvoří podsvaz svazu $\mathbf{P}(\{0,1,2,3\})$ podmnožin množiny $\{0,1,2,3\}$. Stručně zdůvodněte.

Rozhodněte, zda množina $\{\emptyset,\{0,1,2,3\},\{0\}\}$ tvoří podsvaz svazu $\mathbf{P}(\{0,1,2,3\})$ podmnožin množiny $\{0,1,2,3\}$. Stručně zdůvodněte.

Rozhodněte, zda množina $\{\emptyset,\{0,1,2,3\},\{0,1\},\{2\},\{3\}\}$ tvoří podsvaz svazu $\mathbf{P}(\{0,1,2,3\})$ podmnožin množiny $\{0,1,2,3\}$. Stručně zdůvodněte.

Rozhodněte, zda $\mathbf{P}(\{0,1,2\})$ tvoří podsvaz svazu $\mathbf{P}(\{0,1,2,3,4\})$. Zde $\mathbf{P}(X)$ značí svaz podmnožin množiny $X$. Stručně zdůvodněte.

Rozhodněte, zda $\mathbf{D}(12)$ tvoří podsvaz svazu $\mathbf{D}(168)$. Zde $\mathbf{D}(n)$ značí svaz dělitelů čísla $n$. Stručně zdůvodněte.

Rozhodněte, zda $\mathbf{D}(16)$ tvoří podsvaz svazu $\mathbf{D}(168)$. Zde $\mathbf{D}(n)$ značí svaz dělitelů čísla $n$. Stručně zdůvodněte.

Rozhodněte, zda sudé dělitele čísla 120 tvoří podsvaz svazu $\mathbf{D}(120)$ všech dělitelů čísla 120. Stručně zdůvodněte.

Rozhodněte, zda liché dělitele čísla 120 tvoří podsvaz svazu $\mathbf{D}(120)$ všech dělitelů čísla 120. Stručně zdůvodněte.

Rozhodněte, zda konečné podmnožiny $\mathbb{N}$ tvoří podalgebru Booleovy algebry $\mathbf{P}(\mathbb{N})$ podmnožin množiny $\mathbb{N}$. Stručně zdůvodněte.

Rozhodněte, zda podmnožiny sudé velikosti tvoří podalgebru Booleovy algebry $\mathbf{P}(\{0,1,2,3\})$ podmnožin množiny $\{0,1,2,3\}$. Stručně zdůvodněte.

Rozhodněte, zda podmnožiny liché velikosti tvoří podalgebru Booleovy algebry $\mathbf{P}(\{0,1,2,3\})$ podmnožin množiny $\{0,1,2,3\}$. Stručně zdůvodněte.

Rozhodněte, zda podmnožiny obsahující prvek 2 tvoří podalgebru Booleovy algebry $\mathbf{P}(\{0,1,2,3\})$ podmnožin množiny $\{0,1,2,3\}$. Stručně zdůvodněte.

Rozhodněte, zda $\mathbf{P}(\{0,1,2\})$ tvoří podalgebru Booleovy algebry $\mathbf{P}(\{0,1,2,3,4\})$. Zde $\mathbf{P}(X)$ značí algebru podmnožin množiny $X$. Stručně zdůvodněte.

Rozhodněte, zda množina $\{\emptyset, \{0,1,2,3\}, \{0,1\}, \{2,3\}\}$ tvoří podalgebru Booleovy algebry $\mathbf{P}(\{0,1,2,3\})$ podmnožin množiny $\{0,1,2,3\}$. Stručně zdůvodněte.

Rozhodněte, zda množina $\{\emptyset, \{0,1,2,3\}, \{0,3\}\}$ tvoří podalgebru Booleovy algebry $\mathbf{P}(\{0,1,2,3\})$ podmnožin množiny $\{0,1,2,3\}$. Stručně zdůvodněte.

Rozhodněte, zda vektory se sudým počtem jedniček tvoří podalgebru Booleovy algebry $\mathbf{2}^6$, kde $\mathbf{2}$ značí dvouprvkovou Booleovu algebru s prvky $0 < 1$. Stručně zdůvodněte.

Rozhodněte, zda vektory $\{(0,0,0), (0,1,0), (1,0,1), (1,1,1)\}$ tvoří podalgebru Booleovy algebry $\mathbf{2}^4$, kde $\mathbf{2}$ značí dvouprvkovou Booleovu algebru s prvky $0 < 1$. Stručně zdůvodněte.

Rozhodněte, zda iracionální čísla tvoří podgrupu grupy $\mathbb{C}^*$. Stručně zdůvodněte.

Rozhodněte, zda celá čísla tvoří podgrupu grupy $\mathbb{C}$. Stručně zdůvodněte.

Rozhodněte, zda celá čísla tvoří podgrupu grupy $\mathbb{C}^*$. Stručně zdůvodněte.

Rozhodněte, zda racionální čísla tvoří podgrupu grupy $\mathbb{R}$. Stručně zdůvodněte.

Rozhodněte, zda kladná čísla tvoří podgrupu grupy $\mathbb{R}$. Stručně zdůvodněte.

Rozhodněte, zda kladná čísla tvoří podgrupu grupy $\mathbb{R}^*$. Stručně zdůvodněte.

Rozhodněte, zda sudá celá čísla tvoří podgrupu grupy $\mathbb{Q}$. Stručně zdůvodněte.

Rozhodněte, zda sudá celá čísla tvoří podgrupu grupy $\mathbb{Q}^*$. Stručně zdůvodněte.

Rozhodněte, zda přirozená čísla tvoří podgrupu grupy $\mathbb{Q}$. Stručně zdůvodněte.

Rozhodněte, zda permutace splňující $\pi^2 = id$ tvoří podgrupu grupy $\mathbf{S}_3$.

Rozhodněte, zda liché permutace tvoří podgrupu grupy $\mathbf{S}_n$.

Rozhodněte, zda množina $\{1,7\}$ tvoří podgrupu grupy $\mathbb{Z}_9^*$. Stručně zdůvodněte.

Rozhodněte, zda množina $\{1,3\}$ tvoří podgrupu grupy $\mathbb{Z}_{10}^*$. Stručně zdůvodněte.

Rozhodněte, zda množina $\{1,2,4,5,10\}$ tvoří podgrupu grupy $\mathbb{Z}_{11}^*$. Stručně zdůvodněte.

Rozhodněte, zda množina $\{1,3,9\}$ tvoří podgrupu grupy $\mathbb{Z}_{13}^*$. Stručně zdůvodněte.

Rozhodněte, zda množina $\{1,4,7\}$ tvoří podgrupu grupy $\mathbb{Z}_9^*$. Stručně zdůvodněte.

Rozhodněte, zda množina $\{1,5\}$ tvoří podgrupu grupy $\mathbb{Z}_{12}^*$. Stručně zdůvodněte.

Rozhodněte, zda lichá čísla tvoří podgrupu grupy $\mathbb{Z}$. Stručně zdůvodněte.

Rozhodněte, zda otočení tvoří podgrupu grupy $\mathbf{D}_8$ (= grupa všech symetrií čtverce). Stručně zdůvodněte.

Rozhodněte, zda osové symetrie tvoří podgrupu grupy $\mathbf{D}_8$ (= grupa všech symetrií čtverce). Stručně zdůvodněte.

Rozhodněte, zda otočení tvoří podgrupu grupy $\mathbf{D}_{10}$ (= grupa všech symetrií pětiúhelníka). Stručně zdůvodněte.

Rozhodněte, zda osové symetrie tvoří podgrupu grupy $\mathbf{D}_{10}$ (= grupa všech symetrií pětiúhelníka). Stručně zdůvodněte.

Rozhodněte, zda iracionální čísla tvoří podalgebru algebry $(\mathbb{C}, f)$, kde $f(x) = x^2$. Stručně zdůvodněte.

Rozhodněte, zda racionální čísla tvoří podalgebru algebry $(\mathbb{C}, f)$, kde $f(x) = x^2$. Stručně zdůvodněte.

Rozhodněte, zda $\{p^k : p \text{ prvočíslo}, k \in \mathbb{N}\}$ tvoří podalgebru algebry $(\mathbb{Z}, f)$, kde $f(x) = x^2$. Stručně zdůvodněte.

Rozhodněte, zda čísla s normou 1 tvoří podalgebru algebry $(\mathbb{C}, f)$, kde $f(x) = xi$. Stručně zdůvodněte.

## 9. příklady (1 bod)

Jsou algebry $(\mathbb{Z}, f)$ a $(\mathbb{N}, g)$, kde $f(x) = x + 1$ a $g(x) = x + 1$, izomorfní? Stručně zdůvodněte.

Jsou algebry $(\mathbb{N}, f)$ a $(\mathbb{N}, g)$, kde $f(x) = x + 1$ a $g(x) = x + 2$, izomorfní? Stručně zdůvodněte.

Jsou algebry $(\mathbb{N}, f)$ a $(\mathbb{N}, g)$, kde $f(x) = x + 1$ a $g(x) = x^2$, izomorfní? Stručně zdůvodněte.

Jsou algebry $(\mathbb{Z}, f)$ a $(\mathbb{Z}, g)$, kde $f(x) = x + 1$ a $g(x) = 2x$, izomorfní? Stručně zdůvodněte.

Jsou algebry $(\mathbb{Q}, f)$ a $(\mathbb{Q}, g)$, kde $f(x) = x + 1$ a $g(x) = x + 2$, izomorfní? Stručně zdůvodněte.

Jsou svazy $\mathbf{P}(\{0, 1, 2\})$ a $\mathbf{D}(30)$ izomorfní? Zde $\mathbf{D}(n)$ značí svaz dělitelů čísla $n$ a $\mathbf{P}(X)$ značí svaz podmnožin množiny $X$. Stručně zdůvodněte.

Jsou svazy $\mathbf{P}(\{0, 1, 2\})$ a $\mathbf{D}(50)$ izomorfní? Zde $\mathbf{D}(n)$ značí svaz dělitelů čísla $n$ a $\mathbf{P}(X)$ značí svaz podmnožin množiny $X$. Stručně zdůvodněte.

Jsou svazy $\mathbf{D}(30)$ a $\mathbf{D}(105)$ izomorfní? Zde $\mathbf{D}(n)$ značí svaz dělitelů čísla $n$.

Jsou svazy $\mathbf{D}(105)$ a $\mathbf{D}(175)$ izomorfní? Zde $\mathbf{D}(n)$ značí svaz dělitelů čísla $n$.

Jsou svazy $\mathbf{D}(8)$ a $\mathbf{D}(125)$ izomorfní? Zde $\mathbf{D}(n)$ značí svaz dělitelů čísla $n$.

Jsou svazy $\mathbf{P}(\{0, 1\}) \times \mathbf{P}(\{0, 1, 2\})$ a $\mathbf{P}(\{0, 1, 2, 3, 4\})$ izomorfní? Zde $\mathbf{P}(X)$ značí svaz podmnožin množiny $X$. Stručně zdůvodněte.

Jsou grupy $\mathbb{R}$ a $\mathbb{R}^+$ (podgrupa kladných čísel grupy $\mathbb{R}^*$) izomorfní? Stručně zdůvodněte.

Jsou grupy $\mathbb{R}$ a $\mathbb{R}^*$ izomorfní? Stručně zdůvodněte.

Jsou grupy $\mathbb{Q}$ a $\mathbb{Q}^*$ izomorfní? Stručně zdůvodněte.

Jsou grupy $\mathbb{C}$ a $\mathbb{R} \times \mathbb{R}$ izomorfní? Stručně zdůvodněte.

Jsou grupy $\mathbb{C}^*$ a $\mathbb{R}^* \times \mathbb{R}^*$ izomorfní? Stručně zdůvodněte.

Jsou grupy $\mathbb{Q}$ a $\mathbb{Z} \times \mathbb{Z}$ izomorfní? Stručně zdůvodněte.

Jsou grupy $\mathbb{Z}_{29}$ a $\mathbb{Z}_{29}^*$ izomorfní? Stručně zdůvodněte.

Jsou grupy $\mathbb{Z}_{19}$ a $\mathbb{Z}_{20}^*$ izomorfní? Stručně zdůvodněte.

Jsou grupy $\mathbb{Z}_{12}$ a $\mathbb{Z}_3 \times \mathbb{Z}_4$ izomorfní? Stručně zdůvodněte.

Jsou grupy $\mathbb{Z}_{16}$ a $\mathbb{Z}_4 \times \mathbb{Z}_4$ izomorfní? Stručně zdůvodněte.

Jsou grupy $\mathbb{Z}_{12}$ a $\mathbb{Z}_2 \times \mathbb{Z}_6$ izomorfní? Stručně zdůvodněte.

Jsou grupy $\mathbb{Z}_{15}$ a $\mathbb{Z}_3 \times \mathbb{Z}_5$ izomorfní? Stručně zdůvodněte.

Jsou grupy $\mathbf{A}_4$ a $\mathbb{Z}_2 \times \mathbf{S}_3$ izomorfní? Stručně zdůvodněte.

Jsou grupy $\mathbf{A}_4$ a $\mathbf{D}_{12}$ izomorfní? Stručně zdůvodněte.

Jsou grupy $\mathbf{S}_4$ a $\mathbb{Z}_2 \times \mathbf{A}_4$ izomorfní? Stručně zdůvodněte.

Jsou grupy $\mathbf{S}_3$ a $\mathbb{Z}_2 \times \mathbf{A}_3$ izomorfní? Stručně zdůvodněte.

Jsou grupy $\mathbb{Z}_3$ a $\mathbf{A}_3$ izomorfní? Stručně zdůvodněte.

## 10. příklady (1 bod)

Existuje abelovská grupa s neabelovskou podgrupou? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Existuje neabelovská grupa s abelovskou vlastní podgrupou? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Je grupa $\mathbf{S}_3$ abelovská? Stručně zdůvodněte.

Je grupa $\mathbf{A}_4$ (=sudé permutace) abelovská? Stručně zdůvodněte.

Je grupa $\mathbf{A}_3$ (=sudé permutace) abelovská? Stručně zdůvodněte.

Je grupa $\mathbf{D}_8$ (symetrie čtverce) abelovská? Stručně zdůvodněte.

Je grupa $\mathbb{Z}^*$ abelovská? Stručně zdůvodněte.

Je $(\mathbb{Z}, \cdot, ^{-1}, 1)$ grupa? Stručně zdůvodněte.

Je $(\mathbb{Q}, \cdot, ^{-1}, 1)$ grupa? Stručně zdůvodněte.

Je $(\{0, 1, -1\}, \cdot, ^{-1}, 1)$ grupa? Stručně zdůvodněte.

Je $(\{1, -1\}, \cdot, ^{-1}, 1)$ grupa? Stručně zdůvodněte.

Tvoří matice s násobením grupu? Stručně zdůvodněte.

Tvoří všechny funkce $\mathbb{R} \to \mathbb{R}$ se skládáním grupu? Stručně zdůvodněte.

Existuje neabelovská 6-prvková grupa? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Existuje neabelovská 7-prvková grupa? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Existuje neabelovská 8-prvková grupa? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Existuje neabelovská 12-prvková grupa? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Existuje neabelovská nekonečná grupa? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Napište aspoň čtyři neizomorfní osmiprvkové grupy.

Napište aspoň dvě neizomorfní devítiprvkové grupy.

Napište aspoň dvě neizomorfní desetiprvkové grupy.

Napište aspoň dvě neizomorfní 24-prvkové grupy.

Existuje cyklická nekonečná grupa? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Existuje cyklická osmiprvková grupa? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Existuje necyklická osmiprvková grupa? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Existuje necyklická 11-prvková grupa? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Existuje 100-prvková grupa obsahující prvek řádu 12? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Existuje 99-prvková grupa obsahující prvek řádu 8? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Existuje 99-prvková grupa obsahující prvek řádu 9? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Existuje 74-prvková grupa obsahující prvek řádu 10? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Existuje 64-prvková grupa, která má 16-prvkovou podgrupu? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Existuje 70-prvková grupa, která má 15-prvkovou podgrupu? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Existuje 60-prvková grupa, která má 15-prvkovou podgrupu? Pokud ano, uveďte příklad. Pokud ne, zdůvodněte.

Je faktorgrupa $\mathbf{S}_4/\mathbf{H}$, kde $H = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), id\}$, abelovská?

Kolik prvků má faktorgrupa $\mathbf{S}_4/\mathbf{H}$, kde $H = \{(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3), id\}$?

Kolik prvků má faktorgrupa $\mathbf{S}_6/\mathbf{A}_6$ ?

Kolik prvků má faktorgrupa $\mathbb{Z}/5\mathbb{Z}$ ?

Buď $\mathbf{G} = \mathbf{S}_4$ a $\mathbf{H} = \langle(1\ 2\ 3)\rangle$. Spočtěte prvky rozkladové třídy $(1\ 4)\mathbf{H}$.

Buď $\mathbf{G} = \mathbf{S}_4$ a $\mathbf{H} = \langle(1\ 2\ 3)\rangle$. Spočtěte prvky rozkladové třídy $(1\ 3\ 4)\mathbf{H}$.

Buď $\mathbf{G} = \mathbf{S}_4$ a $\mathbf{H} = \{\pi \in S_4 : \pi(4) = 4\}$. Spočtěte prvky rozkladové třídy $(1\ 4)\mathbf{H}$.

Buď $\mathbf{G} = \mathbf{D}_8$ a $\mathbf{H}$ podgrupa sestávající z otočení. Spočtěte prvky rozkladové třídy $o\mathbf{H}$, kde $o$ je vybraná osa.

Buď $\mathbf{G} = \mathbf{D}_8$ a $\mathbf{H}$ podgrupa generovaná vybranou osovou sysmetrií. Spočtěte prvky rozkladové třídy $s\mathbf{H}$, kde $s$ je středová symetrie.

Buď $\mathbf{G} = \mathbb{C}$ a $\mathbf{H} = \mathbb{R}$. Spočtěte prvky rozkladové třídy $i + \mathbf{H}$.

Buď $\mathbf{G} = \mathbb{C}^*$ a $\mathbf{H} = \{z : |z| = 1\}$. Spočtěte prvky rozkladové třídy $2i\mathbf{H}$.

Buď $\mathbf{G} = \mathbb{Z}_{14}^*$ a $\mathbf{H} = \{1, 9, 11\}$. Spočtěte prvky rozkladové třídy $3\mathbf{H}$.

## 11. příklady (1 bod)

Určete řád prvku 5 v grupě $\mathbb{Z}_{62}^*$.

Určete řád prvku 2 v grupě $\mathbb{Z}_{63}^*$.

Určete řád prvku 3 v grupě $\mathbb{Z}_{80}^*$.

Určete řád prvku 12 v grupě $\mathbb{Z}_{61}$.

Určete řád prvku 44 v grupě $\mathbb{Z}_{46}$.

Určete řád prvku 27 v grupě $\mathbb{Z}_{30}$.

Určete řád prvku $e^{6\pi i/7}$ v grupě $\mathbb{C}^*$.

Určete řád prvku $e^{3\pi i/8}$ v grupě $\mathbb{C}^*$.

Generuje prvek 8 grupu $\mathbb{Z}_{50}$? Generuje prvek 8 grupu $\mathbb{Z}_{51}$? Stručně zdůvodněte.

Generuje prvek 6 grupu $\mathbb{Z}_{70}$? Generuje prvek 6 grupu $\mathbb{Z}_{72}$? Stručně zdůvodněte.

Generuje prvek 2 grupu $\mathbb{Z}_9^*$? Stručně zdůvodněte.

Generuje prvek 4 grupu $\mathbb{Z}_{15}^*$? Stručně zdůvodněte.

Generuje prvek 7 grupu $\mathbb{Z}_{50}^*$? Stručně zdůvodněte.

Kolik podgrup má grupa $\mathbb{Z}_8$?

Kolik podgrup má grupa $\mathbb{Z}_{10}$?

Kolik podgrup má grupa $\mathbb{Z}_{12}$?

Kolik podgrup má grupa $\mathbb{Z}_6^*$?

Kolik podgrup má grupa $\mathbf{S}_3$?

Kolik prvků řádu 4 má grupa $\mathbf{S}_4$?

Kolik prvků řádu 5 má grupa $\mathbf{S}_4$?

Kolik prvků řádu 3 má grupa $\mathbf{S}_5$?

Kolik prvků řádu 4 má grupa $\mathbb{Z}_{12}$?

Kolik prvků řádu 5 má grupa $\mathbb{Z}_{25}$?

Kolik prvků řádu 9 má grupa $\mathbb{Z}_{18}$?

Kolik prvků řádu 13 má grupa $\mathbb{Q}^*$?

Kolik prvků řádu 2 má grupa $\mathbb{Q}^*$?

Kolik prvků řádu 3 má grupa $\mathbb{C}^*$?

Kolik prvků řádu 3 má grupa $\mathbb{Z}_9^*$?

Kolik prvků řádu 3 má grupa $\mathbb{Z}_{12}^*$?

Kolik prvků řádu 2 má grupa $\mathbb{Z}_{15}^*$?

Kolik prvků řádu 3 má grupa $\mathbb{Z}_{14}^*$?

Kolik prvků řádu nekonečno má grupa $\mathbb{Z}^*$?

Kolik prvků řádu 2 má grupa $\mathbb{Z}[i]^*$?

Kolik prvků řádu 4 má grupa $\mathbf{D}_8$ (= grupa všech symetrií čtverce)?

Kolik prvků řádu 3 má grupa $\mathbf{D}_8$ (= grupa všech symetrií čtverce)?

Kolik prvků řádu 2 má grupa $\mathbf{D}_8$ (= grupa všech symetrií čtverce)?

Kolik prvků řádu 5 má grupa $\mathbf{D}_{10}$ (= grupa všech symetrií pětiúhelníka)?

Kolik prvků řádu 4 má grupa sudých permutací $\mathbf{A}_4$?

Kolik prvků řádu 3 má grupa sudých permutací $\mathbf{A}_4$?

Kolik prvků řádu 2 má grupa $\mathbf{S}_4$?

Kolik prvků řádu 3 má grupa $\mathbf{S}_4$?

Kolik prvků řádu 4 má grupa $\mathbf{S}_4$?

Kolik prvků řádu 6 má grupa $\mathbf{S}_5$?

Kolik prvků řádu 5 má grupa $\mathbf{S}_5$?

Kolik prvků řádu 4 obsahuje grupa a) $\mathbb{C}$ b) $\mathbb{C}^*$ ?

Rozhodněte zda grupa a) $\mathbb{C}$, b) $\mathbb{C}^*$ obsahuje prvek řádu 5. Pokud ano, uveďte příklad.

Rozhodněte, zda grupa $\mathbf{S}_6$ obsahuje prvek řádu a) 5, b) 8. Pokud ano, uveďte příklad.

Rozhodněte, zda grupa $\mathbf{S}_5$ obsahuje prvek řádu a) 5, b) 6. Pokud ano, uveďte příklad.

Rozhodněte, zda grupa $\mathbf{S}_5$ obsahuje prvek řádu a) 4, b) 7. Pokud ano, uveďte příklad.

Rozhodněte, zda grupa $\mathbf{A}_4$ (= sudé permutace) obsahuje prvek řádu a) 4, b) 5. Pokud ano, uveďte příklad.

Rozhodněte, zda grupa $\mathbf{A}_5$ (= sudé permutace) obsahuje prvek řádu a) 4, b) 5. Pokud ano, uveďte příklad.

Určete řád prvku $(1\ 2\ 5)(3\ 6)(4\ 7)$ v grupě $\mathbf{S}_7$.

Určete řád prvku $(3\ 1\ 2\ 5)(7\ 6)(4)$ v grupě $\mathbf{S}_7$.

Určete řád prvku $(3\ 1\ 6\ 5)(7\ 4\ 2\ 8)$ v grupě $\mathbf{S}_8$.

Určete řád prvku $(1\ 3\ 9\ 5)(2\ 4\ 8)(6\ 7)$ v grupě $\mathbf{S}_9$.

Určete řád prvku $(1\ 3)(4\ 8\ 7\ 6\ 5)$ v grupě $\mathbf{S}_8$.

Je grupa $\mathbf{S}_3$ cyklická? Stručně zdůvodněte.

Je grupa $\mathbf{S}_4$ cyklická? Stručně zdůvodněte.

Je grupa $\mathbf{A}_4$ (= sudé permutace) cyklická? Stručně zdůvodněte.

Je grupa $\mathbf{D}_8$ (= grupa všech symetrií čtverce) cyklická? Stručně zdůvodněte.

Je grupa všech otočení krychle cyklická? Stručně zdůvodněte.

Je grupa všech otočení čtverce cyklická? Stručně zdůvodněte.

Je grupa všech otočení pětiúhelníka cyklická? Stručně zdůvodněte.

Je grupa $\mathbb{Q}$ cyklická? Stručně zdůvodněte.

Je grupa $\mathbb{Q}^*$ cyklická? Stručně zdůvodněte.

Je grupa $\mathbb{Z}$ cyklická? Stručně zdůvodněte.

Je grupa $\mathbb{Z}_9$ cyklická? Stručně zdůvodněte.

Je grupa $\mathbb{Z}_8^*$ cyklická? Stručně zdůvodněte.

Je grupa $\mathbb{Z}_{10}^*$ cyklická? Stručně zdůvodněte.

Je grupa $\mathbb{Z}^*$ cyklická? Stručně zdůvodněte.

Je podgrupa $3\mathbb{Z}$ grupy $\mathbb{Z}$ cyklická? Stručně zdůvodněte.

Je podgrupa $-6\mathbb{Z}$ grupy $\mathbb{Z}$ cyklická? Stručně zdůvodněte.

## 12. příklady (1 bod)

Vypište orbity působení grupy $\mathbf{D}_{10}$ všech symetrií pravidelného pětiúhelníka na množině jeho vrcholů.

Vypište orbity působení grupy $\mathbf{D}_{10}$ všech symetrií pravidelného pětiúhelníka na množině jeho hran.

Vypište orbity působení grupy $\mathbf{S}_8$ na množině $\{1, \ldots, 8\}$.

Vypište orbity působení grupy $\mathbf{S}_6$ na množině $\{(i, j) : i, j = 1, \ldots, 6\}$.

Nechť grupa $\mathbf{D}_{10}$ všech symetrií pravidelného pětiúhelníka působí na množině jeho vrcholů. Kolik pevných bodů má daná osová symetrie?

Nechť grupa $\mathbf{D}_{10}$ všech symetrií pravidelného pětiúhelníka působí na množině jeho hran. Kolik pevných bodů má daná osová symetrie?

Nechť grupa $\mathbf{D}_{12}$ všech symetrií pravidelného šestiúhelníka působí na množině jeho hran. Kolik pevných bodů má středová symetrie?

Kolik prvků má stabilizátor bodu 5 v působení grupy $\mathbf{S}_{10}$ na množinu $\{1, \ldots, 10\}$?

Kolik prvků má stabilizátor bodu 2 v působení grupy $\mathbf{S}_6$ na množinu $\{1, \ldots, 6\}$?

Kolik prvků má stabilizátor daného vrcholu v působení grupy $\mathbf{D}_{12}$ všech symetrií pravidelného šestiúhelníka na množině jeho vrcholů?

Kolik prvků má stabilizátor dané hrany v působení grupy $\mathbf{D}_{12}$ všech symetrií pravidelného šestiúhelníka na množině jeho hran?

Kolik prvků má stabilizátor daného vrcholu v působení grupy $\mathbf{D}_{10}$ všech symetrií pravidelného pětiúhelníka na množině jeho vrcholů?

Kolik prvků má stabilizátor dané hrany v působení grupy $\mathbf{D}_{10}$ všech symetrií pravidelného pětiúhelníka na množině jeho hran?

Uvažujme působení grupy otočení čtverce na množinu všech obarvení šachovnice $3\times 3$ dvěma barvami. Kolik prvků má stabilizátor obarvení, kde jsou všechna políčka bílá?

Uvažujme působení grupy otočení čtverce na množinu všech obarvení šachovnice $3\times 3$ dvěma barvami. Kolik prvků má stabilizátor obarvení, kde je prostřední políčko černé a ostatní bílá?

Uvažujme působení grupy otočení čtverce na množinu všech obarvení šachovnice $3 \times 3$ dvěma barvami. Kolik prvků má stabilizátor obarvení, kde je jedno rohové políčko černé a ostatní bílá?

Uvažujme působení grupy otočení čtverce na množinu všech obarvení šachovnice $4 \times 4$ dvěma barvami. Kolik prvků má stabilizátor obarvení, kde je jedno políčko černé a ostatní bílá?

Uvažujme působení grupy otočení čtverce na množinu všech obarvení šachovnice $4\times 4$ dvěma barvami. Kolik prvků má stabilizátor obarvení, kde jsou rohová políčka černá a ostatní bílá?

Uvažujme působení grupy $\mathbf{D}_8$ všech symetrií čtverce na množinu všech obarvení šachovnice $3 \times 3$ dvěma barvami. Kolik prvků má stabilizátor obarvení, kde jsou všechna políčka bílá?

Uvažujme působení grupy $\mathbf{D}_8$ všech symetrií čtverce na množinu všech obarvení šachovnice $3 \times 3$ dvěma barvami. Kolik prvků má stabilizátor obarvení, kde je prostřední políčko černé a ostatní bílá?

Uvažujme působení grupy $\mathbf{D}_8$ všech symetrií čtverce na množinu všech obarvení šachovnice $3 \times 3$ dvěma barvami. Kolik prvků má stabilizátor obarvení, kde je jedno rohové políčko černé a ostatní bílá?

Uvažujme působení grupy $\mathbf{D}_8$ všech symetrií čtverce na množinu všech obarvení šachovnice $4 \times 4$ dvěma barvami. Kolik prvků má stabilizátor obarvení, kde je jedno vnitřní políčko černé a ostatní bílá?

Uvažujme působení grupy $\mathbf{D}_8$ všech symetrií čtverce na množinu všech obarvení šachovnice $4 \times 4$ dvěma barvami. Kolik prvků má stabilizátor obarvení, kde jsou rohová políčka černá a ostatní bílá?

Uvažujme působení grupy $\mathbf{GL}_n(\mathbf{T})$ na vektorový prostor $T^n$, kde akce matice $A$ na vektoru $v$ je definovaná jako $Av$. Vypište orbity.

Nechť grupa $\mathbf{G}$ všech izometrií v rovině (tj. všechna otočení, translace a osové symetrie) působí na rovinu $X = \mathbb{R}^2$. Vypište orbity.

Nechť grupa $\mathbf{G}$ všech izometrií v rovině (tj. všechna otočení, translace a osové symetrie) působí na rovinu $X = \mathbb{R}^2$. Vypište prvky $G_x$ pro daný bod $x$.

Nechť grupa $\mathbf{G}$ všech izometrií v rovině (tj. všechna otočení, translace a osové symetrie) působí na rovinu $X = \mathbb{R}^2$. Vypište prvky $X_g$ pro dané otočení $g$.

Nechť grupa $\mathbf{G}$ všech izometrií v rovině (tj. všechna otočení, translace a osové symetrie) působí na rovinu $X = \mathbb{R}^2$. Vypište prvky $X_g$ pro danou translaci $g$.

Nechť grupa $\mathbf{G}$ všech izometrií v rovině (tj. všechna otočení, translace a osové symetrie) působí na rovinu $X = \mathbb{R}^2$. Vypište prvky $X_g$ pro danou osovou symetrii $g$.

## 13. úloha (2 body)

Spočtěte $13^{13^{13}} + 15^{15^{15}} \bmod 17$.

Spočtěte $123^{321} \bmod 8$.

Spočtěte $5^{444} \bmod 132$.

Spočtěte poslední dvě cifry čísla $13^{282}$.

Spočtěte poslední dvě cifry čísla $11^{441}$.

Spočtěte poslední dvě cifry čísla $11^{442}$.

Spočtěte poslední tři cifry čísla $3^{402}$.

Spočtěte poslední tři cifry čísla $3^{403}$.

Spočtěte <u>předposlední</u> cifru čísla $27^{4321}$.

Spočtěte <u>předposlední</u> cifru čísla $27^{3321}$.

Spočtěte poslední cifru čísla $3^{2007}$.

Spočtěte $10^{9^8} \bmod 6$.

Spočtěte $10^{11^{12}} \bmod 6$.

Spočtěte $9^{8^7} \bmod 7$.

Spočtěte $9^{7^5} \bmod 7$.

Spočtěte $11^{114} \cdot 13^{76} \bmod 6$.

Spočtěte $8^{1111} + 12^{1111} \bmod 10$.

Spočtěte $8^{333} + 12^{333} \bmod 10$.

Spočtěte $10^{444} + 14^{666} \bmod 12$.

Spočtěte $10^{333} + 14^{333} \bmod 12$.
Najděte všechna $x \in \mathbb{Z}$ splňující $2x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 4$, $3x \equiv 1 \pmod 5$.
Najděte všechna $x \in \mathbb{Z}$ splňující $x \equiv 1 \pmod 4$, $x \equiv 2 \pmod 5$, $2x \equiv 3 \pmod 7$.
Najděte všechna $x \in \mathbb{Z}$ splňující $x \equiv 1 \pmod 2$, $x \equiv 4 \pmod 5$, $x \equiv 6 \pmod 7$.
Najděte všechna $x \in \mathbb{Z}$ splňující $x \equiv 0 \pmod 4$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$.
Najděte všechna $x \in \mathbb{Z}$ splňující $x \equiv 1 \pmod 5$, $x \equiv 0 \pmod 6$, $x \equiv 4 \pmod 7$.
Najděte všechna $x \in \mathbb{Z}$ splňující $x \equiv 3 \pmod 4$, $3x \equiv 4 \pmod{11}$.
Najděte všechna $x \in \mathbb{Z}$ splňující $2x \equiv 5 \pmod 7$, $2x \equiv 5 \pmod 9$.
Najděte všechna $x \in \mathbb{Z}$ splňující $3x \equiv 5 \pmod 8$, $x \equiv 5 \pmod 9$.
Najděte všechna $x \in \mathbb{Z}$ splňující $2x \equiv 6 \pmod 7$, $x \equiv 3 \pmod 9$.
Najděte všechna $x \in \mathbb{Z}$ splňující $3x \equiv 7 \pmod{10}$, $2x \equiv 8 \pmod{11}$.
Najděte $0 \leq x \leq 31$ takové, že $28x \equiv 5 \pmod{31}$.
Najděte $0 \leq x \leq 33$ takové, že $29x \equiv 5 \pmod{33}$.
Najděte $0 \leq x \leq 35$ takové, že $9x \equiv 5 \pmod{35}$.
Najděte $0 \leq x \leq 37$ takové, že $4x \equiv 5 \pmod{37}$.
Spočtěte hodnotu Eulerovy funkce $\varphi(2250)$.
Spočtěte hodnotu Eulerovy funkce $\varphi(2310)$.
Spočtěte Bézoutovy koeficienty pro NSD(25,33).
Spočtěte Bézoutovy koeficienty pro NSD(21,30).
Spočtěte Bézoutovy koeficienty pro NSD(20,32).
Spočtěte Bézoutovy koeficienty pro NSD(19,27).
Spočtěte $11^{-1}$ v grupě $\mathbb{Z}_{24}^*$.
Spočtěte $13^{-1}$ v grupě $\mathbb{Z}_{19}^*$.
Spočtěte $5^{-1}$ v grupě $\mathbb{Z}_{22}^*$.
Spočtěte $7^{-1}$ v grupě $\mathbb{Z}_{23}^*$.