Řešení domácích úkolů na algebru 08/09 zima

Příklad 1. Najděte všechny ireducibilní (nerozložitelné) polynomy stupně 4 nad tělesem $\mathbb{Z}_2$ (a ukažte, že jsou ireducibilní a že jsou všechny). Vyberte si jeden z nich a v 16-tiprvkovkém tělese určeném tímto polynomem spočítejte pomocí Euiklidova algoritmu $(x^3+x+1)^{-1}$.

Řešení. Ireducibilní polynom p nemůže mít kořen (jinak je dělitelný polynomem $x-a$, kde a je kořen). Polynomy stupně čtyři nad $\mathbb{Z}_2$, které nemají kořen, jsou, jak snadno nahlédnete, následující:

$$x^4+x+1,\ x^4+x^2+1,\ x^4+x^3+1,\ x^4+x^3+x^2+x+1.$$

Pokud je některý z nich rozložitelný, pak je nutně součinem dvou nerozložitelných polynomů stupně 2. Nerozložitelný polynom stupně 2 je jen jeden, a to x^2+x+1. Takže polynom

$$(x^2+x+1)^2 = x^4+x^2+1$$

je jediný rozložitelný polynom ze seznamu výše.

Nad $\mathbb{Z}_2$ existují právě čtyři ireducibilní polynomy stupně 4, a to x^4+x+1, x^4+x^3+1 a $x^4+x^3+x^2+x+1$.

Vybereme si například $q = x^4+x+1$ a v příslušném tělese budeme počítat $(x^3+x+1)^{-1}$. Euklidovým algoritmem najdeme polynomy a, b takové, že $1 = aq + b(x^3+x+1)$. Pak $b \bmod q$ je hledaný inverzní prvek.

$$\begin{aligned} \underline{x^4+x+1} &= x\cdot(\underline{x^3+x+1}) + (\underline{x^2+1}) \\ \underline{x^3+x+1} &= x\cdot(\underline{x^2+1}) + \underline{1}. \end{aligned}$$

Z první rovnice dostaneme

$$\underline{x^2+1} = (\underline{x^4+x+1}) + x\cdot(\underline{x^3+x+1}).$$

Z druhé rovnice máme

$$\begin{aligned} \underline{1} &= (\underline{x^3+x+1}) + x\cdot(\underline{x^2+1}) \\ &= (\underline{x^3+x+1}) + x\cdot\big[(\underline{x^4+x+1}) + x\cdot(\underline{x^3+x+1})\big] \\ &= x\cdot(\underline{x^4+x+1}) + (x^2+1)\cdot(\underline{x^3+x+1}). \end{aligned}$$

Takže $(x^3+x+1)^{-1} = x^2+1$.

Příklad 2. Najděte všechny podalgebry a kongruence algebry $\mathbb{A} = \{a, b, c, d, e\}(\circ)$, kde

$\circ$	a	b	c	d	e
a	a	e	c	a	a
b	e	d	e	b	b
c	a	e	c	a	c
d	c	b	a	e	e
e	a	e	a	d	b

(Nezapomeňte napsat postup, z kterého plyne správnost výsledku. Samotný výsledek je bezcenný.)

Řešení. Neprve najdeme podalgebry. Jistě $\emptyset$ a $\{a, b, c, d, e\}$ jsou podalgebry. Nechť B je libovolná podalgebra $\mathbb{A}$. Pokud $b \in B$, pak $d \in B$ (protože $b \circ b = d$). Pokud $d \in B$, pak $e \in B$ (protože $d \circ d = e$). Pokud $e \in B$, pak $b \in B$ (protože $e \circ e = b$). Tedy buď $\{b, c, d\} \cap B = \emptyset$, nebo $\{b, d, e\} \subseteq B$. Jedinými adepty na podalgebry (kromě triviálních) jsou $\{a\}, \{c\}, \{a, c\}, \{b, d, e\}, \{a, b, d, e\}, \{b, c, d, e\}$. U každé z těchto množin ověříme, zda je uzavřená na $\circ$. Zjistíme, že $\{a\}$ a $\{c\}$, $\{b, d, e\}$ jsou podalgebry a zbývající dvě nikoliv.

Podalgebry algebry $\mathbb{A}$ jsou právě $\emptyset$, $\{a\}$, $\{c\}$, $\{a, c\}$, $\{b, d, e\}$, $\{a, b, c, d, e\}$.

Nyní nejdeme kongruence. Nechť $\sim$ je libovolná kongruence.

- Pokud $a \sim b$, pak $a \sim e$ (protože $a \circ a \sim b \circ a$), $e \sim d$ (protože $a \circ b \sim b \circ b$), $c \sim e$ (protože $a \circ c \sim b \circ c$). Tedy $\sim = A^2$.
- Pokud $a \sim d$, pak $a \sim e$ ($a \circ d \sim d \circ d$) a $a \sim b$ ($e \circ a \sim e \circ e$). Z předchozího již víme, že $\sim = A^2$
- Pokud $a \sim e$, pak $a \sim b$ ($e \circ a \sim e \circ e$) a opět $\sim = A^2$.
- Pokud $b \sim c$, pak $a \sim e$ ($b \circ a \sim c \circ a$) a $\sim = A^2$.
- ...

Podobně snadno nahlédneme, že z $b \sim d$ plyne $\sim = A^2$, z $b \sim e$ plyne $\sim = A^2$, z $c \sim d$ plyne $\sim = A^2$, z $c \sim e$ plyne $\sim = A^2$ a $d \sim e = A^2$.

Takže pokud $\sim \neq A^2$, tak buď $\sim = \{(a, a) : a \in A\}$ (triviální kongruence s třídami $\{a\}$, $\{b\}$, ...) nebo $\sim$ je kongruence s rozkladovými třídami $\{a, c\}$, $\{b\}$, $\{d\}$, $\{e\}$. První ekvivalence je vždy kongruencí. Druhá ekvivalence je rovněž kongruence — stačí ověřit, že $a \circ x \sim c \circ x$ a $x \circ a \sim x \circ c$ pro libovolné $x \in A$ (viz cvičení). To lze snadno vidět z tabulky.

Jediná netriviální kongruence algebry $\mathbb{A}$ je ekvivalence daná třídami $\{a, c\}$, $\{b\}$, $\{d\}$, $\{e\}$ (v zápisu ze cvičení je to $ac|b|d|e$).

Příklad 3. Nechť $N = \{1, 2, \dots, \}$ (tj. přirozená čísla bez nuly) a $\mathbb{N} = N(+)$, kde $+$ je běžná operace sčítání. Najděte všechny homomorfismy $\mathbb{N} \times \mathbb{N} \to \{1, -1\}(\cdot)$.

Řešení. Ukážeme, že homomorfismus $f : \mathbb{N} \times \mathbb{N} \to \{1, -1\}(\cdot)$ je jednoznačně určen hodnotami $f(1,1)$ a $f(2,1)$. Označme $a = f(1,1)$ a $b = f(2,1)$.

(i) **Pro libovolné** $k \in N$ **platí** $f(k,k) = a^k$. Dokážeme indukcí. Pro $k = 1$ jde o definici a. Předpokládejme, že tvrzení platí pro k. Z definice homomorfismu dostáváme $f(k+1, k+1) = f((k,k)+(1,1)) = f(k,k)f(1,1) =^{IP} a^k a = a^{k+1}$.

(ii) **Pro libovolné** $k \in N$ **platí** $f(k,1) = a^k b^{k-1}$. Dokážeme indukcí. Pro $k = 1$ tvrzení platí, protože $f(1,1) = a = a^1 b^0$. Předokládejme, že tvrzení platí pro k. Z definice homomorfismu dostáváme $f(k,1)f(2,1) = f((k,1)+(2,1)) = f(k+2,2) = f((k+1,1)+(1,1)) = f(k+1,1) \cdot f(1,1)$. Tedy $f(k+1,1) = f(k,1)f(1,1)f(2,1) = f(k,1)ab =^{IP} a^k b^{k-1} ab = a^{k+1} b^k$.

(iii) **Pro libovolné** $l \in N$ **platí** $f(1,l) = ab^{l-1}$. Z definice homomorfismu máme $f(1,l) \cdot f(l,1) = f((1,l) + (l,1)) = f(l+1, l+1) = a^{l+1}$, kde poslední rovnost plyne z (i). Takže $f(1,l) = f(l,1)a^{l+1}$. Dosazením (ii) dostáváme $f(1,l) = a^l b^{l-1} a^{l+1} = ab^{l-1}$

(iv) **Pro libovolná** $k, l \in N$ **platí** $f(k,l) = a^k b^{k+l}$. Pro $l = 1$ plyne tvrzení z (ii), pro $k = 1$ z (iii). Předpokládejme, že $k, l \geq 2$. Z definice homomorfismu a užitím (ii) a (iii) máme $f(k,l) = f((k-1,1) + (1,l-1)) = f(k-1,1)f(1,l-1) = a^{k-1} b^{k-2} ab^{l-2} = a^k b^{k+l}$.

Různé volby a a b dávají čtyři možné homomorfismy

- Pro $a = b = 1$ dostáváme $f(k,l) = 1$.
- Pro $a = 1$, $b = -1$ dostáváme $f(k,l) = (-1)^{k+l}$.
- Pro $a = -1$, $b = 1$ dostáváme $f(k,l) = (-1)^k$.
- Pro $a = b = -1$ dostáváme $f(k,l) = (-1)^k (-1)^{k+l} = (-1)^l$.

Je snadné (ale nutné !!!) ověřit, že všechna 4 zobrazení jsou skutečně homomorfismy.

Příklad 4. Zjistěte, zda grupa $\mathbb{Z}_{19}^*$ je izomorfní grupě $\mathbb{Z}_{18}$. Grupa $\mathbb{Z}_{19}$ má prvky $\{1, 2, \ldots, 18\}$ a binární operací je násobení modulo 19. Grupa $\mathbb{Z}_{18}$ má prvky $\{0, 1, \ldots, 17\}$ a binární operací je sčítání modulo 18.

Řešení. Nech f je homomorfismus $\mathbb{Z}_{18} \to \mathbb{Z}_{19}^*$. Protože 1 je generátorem grupy $\mathbb{Z}_{18}$, homomorfismus f je jednoznačně určen hodnotou $f(1)$. Označme ji a. Pak $f(2) = f(1 +_{\text{mod } 18} 1) = f(1) \cdot_{\text{mod } 19} f(1) = a^2 \bmod 19$. Dále $f(3) = a^3 \bmod 19$, atd. Indukcí snadno dokážeme, že

$$f(n) = a^n \bmod 19, \quad n \in \mathbb{Z}_{18}.$$

Zobrazení f je slučitelné s binární operací:

$$f(n +_{\mathrm{mod}\ 18} m) = a^{n+_{\mathrm{mod}\ 18} m} \mathrm{mod}\ 19 = a^{n+m+18k} \mathrm{mod}\ 19 = a^{n+m} a^{18^k} \mathrm{mod}\ 19 =$$

$$= a^{n+m} \mathrm{mod}\ 19 = (a^n \mathrm{mod}\ 19) \cdot_{\mathrm{mod}\ 19} (a^m \mathrm{mod}\ 19) = f(n) \cdot_{\mathrm{mod}\ 19} f(m)$$

Využili jsme toho, že $a^{18} \bmod 19 = 1$. To platí, protože řád a v grupě $\mathbb{Z}_{19}^*$ dělí počet prvků grupy $\mathbb{Z}_{19}^*$, což je 18. Takže $a^r \bmod 19 = 1$ pro jisté $r|18$ a tím spíše $a^{18} \bmod 19 = 1$. (Také se tomu říká Malá Fermatova věta.)

Slučitelnost s ostatními operacemi není potřeba ověřovat, protože každé zobrazení mezi grupami slučitelné s binární operací je již homomorfismem (ověřte!).

Našli jsme vlastně všechny homomorfismy $\mathbb{Z}_{18} \to \mathbb{Z}_{19}^*$.

Pokud najdeme v $\mathbb{Z}_{19}^*$ prvek a řádu 18, pak příslušné zobrazení f bude prosté (tedy i na, protože grupy mají stejný konečný počet prvků) – kdyby nebylo prosté budou existovat $n < m < 18$ pro které $a^m = a^n$ (v $\mathbb{Z}_{19}^*$). Pak ale $a^{m-n} = 1$, což je ve sporu s tím, že a má řád $18 > m - n$.

Zkusíme $a = 2$. Protože řád a dělí 18 musí to být buď 1,2,3,9 nebo 18. Ale $2^2 = 4 \neq 1$ a $2^9 = 2^4 \cdot 2^4 \cdot 2 \bmod 19 = (-3) \cdot (-3) \cdot 2 \bmod 19 = 18 \neq 1$, takže 2 má řád 18.

Dané grupy jsou izomorfní, například zobrazení $f(n) = 2^n \bmod 19$ je izomorfismem $\mathbb{Z}_{18} \to \mathbb{Z}_{19}^*$.

Poznámky.

- Cyklická grupa (= 1-generovaná grupa) mohutnosti n je izomorfní $\mathbb{Z}_n$. Pokud toto víme, stačí v grupě $\mathbb{Z}_{19}^*$ najít generátor, tj. prvek řádu 18.
- Lze ukázat, že grupy $\mathbb{Z}_p^*$ a $\mathbb{Z}_{p-1}$ jsou izomorfní pro libovolné prvočíslo p. K tomu stačí najít v $\mathbb{Z}_p^*$ prvek řádu $p - 1$. Obecně, multiplikativní grupa libovolného konečného tělesa je cyklická.

Příklad 5. Pro grupu D_6 (symetrie 6-tiúhelníka) najděte všechny podgrupy, všechny normální podgrupy a popište příslušné faktorgrupy.

Řešení. Řešení bylo probíráno na cvičení. Označme

$$r = (1\ 2\ 3\ 4\ 5\ 6), \quad d = (2\ 6)(3\ 5).$$

Platí

$$D_6 = \{id = r^0, r^1, r^2, \ldots, r^5, d = r^0 d, rd, r^2 d, \ldots, r^5 d\}.$$

Prvek r^i je otočení o $60i$ stupňů, prvek $r^i d$ je osová souměrnost podle osy, která s přímkou 14 svírá $30i$ stupňů. Zřejmě $r^i = r^{i \bmod 6}, d^i = d^{i \bmod 2}$. Snadno spočítáme, že $dr = r^5 d (= r^{-1} d)$, obecněji $dr^i = r^{-i} d$. Skládání dvou osových souměrností:

$$r^i d\ r^j d = r^i r^{-j} dd = r^{i-j}. \qquad (1)$$

Skládání rotace a osové souměrnosti:

$$r^i\ r^j d = r^{i+j} d, \quad r^j d\ r^i = r^j r^{-i} d = r^{j-i} d. \qquad (2)$$

Uvažujme libovolnou podgrupu $H \leq D_6$ a označme $R = \langle r \rangle = \{id, r, r^2, \ldots, r^5\}$ a $T = H \cap R$. T je podgrupou cyklické grupy R a jejich strukturu známe z přenášky. Jsou následující možnosti

- $T = \{id\}$. Pak H obsahuje nejvýše jednu osovou souměrnost, jinak by obsahovala neidentickou rotaci (viz (1)). Pro H máme následující možnosti: $X_1 = \{id\}$, $Y_i = \{id, r^i d\}$, $i = 0, \ldots, 5$, všechny tyto množiny jsou zřejmě podgrupy D_6.
- $T = \{id, r^3\}$. Pokud H obsahuje osovou souměrnost $r^i d$, pak i $r^{i+3}d$. Jiné osové souměrnosti v H být nemůžou kvůli (1) – vznikla by rotace, která není v T. Pro H máme následující možnosti: $X_2 = \{id, r^3\}$, $Z_i = \{id, r^3, r^i d, r^{i+3}d\}$, $i = 0, 1, 2$. Jsou to podgrupy D_6 jak je vidět z (1) a (2).
- $T = \{id, r^2, r^4\}$. Stejnou úvahou jako v předchozím případě dostáváme podgrupy $X_3 = \{id, r^2, r^4\}$, $W_i = \{id, r^2, r^4, r^i d, r^{i+2}d, r^{i+4}d\}$, $i = 0, 1$.
- $T = \{id, r^1, r^2, \ldots, r^5\}$. Máme podgrupy $X_6 = \{id, r^1, \ldots, r^5\}$ a D_6. V tomto případě stačí použít Lagrangovu větu.

Našli jsme celkem 16 podgrup. X_1, X_2, X_3, X_6 jsou normální: To plyne z výpočtu:

$$(r^i d)\ r^k\ (r^i d)^{-1} = r^i d r^k d r^{-i} = r^i r^{-k} d d r^{-i} = r^{-k}.$$

Výpočtem lze též ověřit, že W_0 a W_1 jsou normální a zbylé netriviální podgrupy normální nejsou. Máme celkem 7 normálních podgrup: $X_1, X_2, X_3, X_6, D_6, W_0, W_1$. Faktorgrupy jsou následující

$$D_6/X_1 \cong D_6, \quad D_6/D_6 \cong \mathbb{Z}_1, \quad D_6/W_i \cong \mathbb{Z}_2, \quad D_6/X_6 \cong \mathbb{Z}_2,$$

$$D_6/X_2 \cong S_3, \quad D_6/X_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

D_6/X_2 je izomorfní S_3 proto, že tato grupa není komutativní (např. $dr \not\sim rd$ v kongruenci odpovídající X_2) a S_3 je jediná nekomutativní grupa velikosti 6. D_6/X_3 je izomorfní $\mathbb{Z}_2 \times \mathbb{Z}_2$ proto, že v této grupě není prvek řádu 4 a jediné čtyřprvkové grupy jsou (až na izomorfismus) $\mathbb{Z}_4$ a $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Příklad 6. Najděte všechny kongruence algebry $\mathbb{P} = P(\cap, \cup)$, kde P je množina všech podmnožin množiny $\{0, 1, 2\}$ a $\cap, \cup$ jsou běžné (binární) operace průniku a sjednocení.

Řešení. Vyřešíme obecnější úlohu: budeme uvažovat svaz $P(X)$ všech podmožin obecné množiny X. Nejprve dvě pozorování o kongruencích svazů obecně. (Pozorování nejsou nutná pro vyřešení úlohy, ale je užitečné si toho všimnout.)

(S1) Pokud $\sim$ je kongruence svazu $L(\wedge, \vee)$ a $a \sim b$, pak $a \wedge b \sim a \vee b$. Důkaz: protože $\sim$ je kongruence, máme $a \wedge b \sim b \wedge b = b$ a $a \vee b \sim b \vee b = b$ a tvrzení plyne z tranzitivity $\sim$.

(S2) Pokud $\sim$ je kongruence svazu $L(\wedge, \vee)$, $a \sim b$ a $a \leq b$, pak $a \sim c$ pro libovolné c, pro něž $a \leq c \leq b$. Důkaz: $a = a \wedge c \sim b \wedge c = c$.

Čili pokud $a \sim b$ pro nějakou kongruenci $\sim$, pak všechny prvky mezi $a \wedge b$ a $a \vee b$ jsou v jedné $\sim$-třídě.

Uvažujme libovolnou kongruenci $\sim$ svazu všech podmnožin množiny X.

(P1) Nechť $Y, Z \subseteq X$. Pak $Y \sim Z$ právě tehdy, když $\emptyset \sim (Z - Y) \cup (Y - Z)$. Důkaz: Pokud $Y \sim Z$, pak $\emptyset = Y \cap (X - Y) \sim Z \cap (X - Y) = Z - Y$ a podobně $\emptyset \sim Y - Z$. Tedy (např. podle (S1)) $\emptyset \sim (Z - Y) \cup (Y - Z)$. Naopak, pokud $\emptyset \sim (Z - Y) \cup (Y - Z)$, pak $Y = \emptyset \cup Y \sim (Z - Y) \cup (Y - Z) \cup Y = Y \cup Z$ a podobně $Z \sim Y \cup Z$. Tedy $Y \sim Z$ (z tranzitivity).

(P2) Nechť $Y \subseteq X$. Pak $Y \sim \emptyset$ právě tehdy, když pro každé $y \in Y$ platí $\emptyset \sim \{y\}$. Důkaz: Plyne z (S1) a (S2).

Pro danou kongruenci $\sim$ označme

$$Q_\sim = \{x \in X : \emptyset \sim \{x\}\} \subseteq X.$$

Důsledkem (P1) a (P2) je, že kongruence $\sim$ je jednoznačně určená množinou $Q_\sim$, a to následujícím způsobem:

$$Y \sim Z \quad \text{právě když} \quad (Y - Z) \cup (Z - Y) \subseteq Q_\sim$$

Na druhou stranu, pro libovolnou podmožinu $Q \subseteq X$ relace definovaná vztahem

$$Y \sim Z \quad \text{právě když} \quad (Y - Z) \cup (Z - Y) \subseteq Q$$

je kongruence (ověřte!). Tedy kongruence svazu $P(X)$ vzájemně jednoznačně odpovídají podmnožinám X výše uvedeným způsobem. Lze snadno ukázat, že tato korespondence je izomorfismem svazů. Tedy svaz kongruencí svazu $P(X)$ je izomorfní svazu $P(X)$.

Příklad 7. Rozhodněte (zdůvodnění je opět nutné), zda svaz konvexních podmnožin roviny uspořádaných inkluzí je a) modulární b) distributivní.

Řešení. Položme

$$A = \{(0,0)\}, \quad B = \{(x,0) : x \in \langle 0,1\rangle\}, \quad C = \{(-1,x) : x \in \mathbb{R}\}.$$

Platí $A \subseteq B$, $(C \vee A) \wedge B = B$ a $(C \wedge B) \vee A = A$. Tedy daný svaz není modulární, čili ani distributivní.

Poznámky. Častou chybou bylo, že jste k důkazu nemodularity chtěli v daném svazu najít podsvaz izomorfní N_5, přičemž nalezených pět množin netvořilo podsvaz (natož aby to byl podsvaz izomorfní N_5).

Příklad 8. Spočtěte poslední dvě cifry v desítkovém zápisu čísla $87^{(85^{83})}$.

Řešení. Protože jsou čísla 87 a 100 nesoudělná, můžeme použít Eulerovu větu:

$$87^{85^{83}} \equiv 87^{85^{83} \bmod \varphi(100)} = 87^{85^{83} \bmod 40} \pmod{100}.$$

K výpočtu $85^{83} \bmod 40$ stejnou větu použít nejde kvůli soudělnosti čísel 85 a 40. Vypočteme

$$85^{83} \equiv 0^{83} = 0 \bmod 5$$

a užitím Eulerovy věty

$$85^{83} \equiv 5^{83} \equiv 5^{83 \bmod \varphi(8)} = 5^{83 \bmod 4} = 5^3 \equiv 5 \pmod{8}.$$

Použitím ČVZ dostaneme $85^{83} \equiv 5 \pmod{40}$, takže

$$87^{85^{83}} \equiv 87^5 \equiv 7 \pmod{100}.$$

Poslední dvě cifry jsou tedy 07.