

Řešení předtermínové písemky

- (1) Necht' $\mathcal{A} = A(\alpha_i; i \in I)$, $\mathcal{B} = B(\alpha_i; i \in I)$ jsou algebry typu Ω . Zobrazení $f : A \rightarrow B$ se nazývá homomorfismus algeber $\mathcal{A}$ a $\mathcal{B}$, pokud pro každé $i \in I$ a $a_1, \dots, a_{\Omega(i)} \in A$ platí $f(\alpha_i(a_1, \dots, a_{\Omega(i)})) = \alpha_i(f(a_1), \dots, f(a_{\Omega(i)}))$. Jádrem tohoto homomorfismu rozumíme ekvivalenci $\ker(f) = \{(x, y) \in A^2; f(x) = f(y)\}$. V konkrétním případě π pak jest $\ker(\pi) = \{(x, y) \in \mathbb{Q}^2; x - y \in \mathbb{Q}\}$.

Definici homomorfismu měla většina z vás správně, u jádra pár lidí nesprávně uvedlo variantu $\text{Ker}(f)$, která v případě obecných algeber nedává smysl. Nejčastější chyba nastávala v aplikaci na konkrétní příklad, kdy jste často místo $x - y \in \mathbb{Q}$ psali $x^{-1}y \in \mathbb{Q}$ či prostě generické $\pi(x) = \pi(y)$, což jsem neuznával (napsat místo písmene A písmeno $\mathbb{Q}$ a místo f zase π není výkon hodný jednoho bodu).

- (2) Příklad testoval, zda znáte definici řádu prvku v (konečné) grupě a zda umíte počítat ve faktorokruhu. Označíme-li $I = u\mathbb{Z}_2[x]$, dověděli jste se na přednášce, že $f + I = (f \bmod u) + I$, a tedy $f + I = g + I \iff f \bmod u = g \bmod u$. Máme najít nejmenší $n \in \mathbb{N}$ takové, že $\alpha^n = 1 + I$. (V multiplikativní grupě tělesa $T = \mathbb{Z}_2[x]/I$ je totiž neutrálním prvkem právě $1 + I$, tj. jednotka okruhu T .)

Z Lagrangeovy věty si můžeme uvědomit, že řád prvku α může být pouze 1, 3, 5 či 15, jelikož $|T^*| = 15$. Ihned vidíme, že $x + I \neq 1 + I$ a stejně tak $(x + I)^3 = x^3 + I \neq 1 + I$. Dále $\alpha^5 = x^5 + I = (x^5 \bmod u) + I$, což vzhledem k tomu, že $x^4 \bmod u = x^3 + x^2 + x + 1$, se dále rovná $(x(x^3 + x^2 + x + 1) \bmod u) + I = (x^4 + x^3 + x^2 + x \bmod u) + I = 1 + I$, a řád prvku α v T^* je proto roven 5.

Tuto úlohu bohužel nikdo nevyřešil. Jedná se o relativně přímočarou aplikaci definic, ale chápu, že pokud jste na cvičení žádný výpočet ve faktorokruhu neprováděli, netušili jste často, jak to celé vlastně uchopit. Když už se někdo o něco pokusil, tak zase kupř. počítal chybně řád v aditivní grupě tělesa T .

- (3) Z vlastnosti $h\mathbb{R}[x] \subseteq g\mathbb{R}[x] \iff g|h$ mnozí z vás správně usoudili, že f by měl být nejmenším společným násobkem polynomů p a q . Jeho výpočet pak už byl pro některé trochu oříšek, ale vzhledem k tomu, že kořeny obou polynomů byly hezky celočíselné, nakonec se občas podařilo dosáhnout správného výsledku $p \cdot (x - 2) = x^5 - 2x^4 - 10x^3 + 20x^2 + 9x - 18$, popř. nějakého nenulového násobku tohoto polynomu (což bylo samozřejmě také správně).
- (4) Čínská věta o zbytcích vám většinou šla. Někdo ji zformuloval pouze jako jednu implikaci, za což jsem strhl bod. Nejčastějším prohřeškem bylo špatné psaní vztahu „a dělí b“, což se správně zapisuje jako $a|b$, ale několik z vás to otočilo (jeden to dokonce psal chvíli tak, a pak zase naopak, což už se nedá uznat ani s jedním okem přimhouřeným a druhým vypíchlým).
- (5) Už jsem uváděl na konci zkoušky. Z předpokladu plyne pro libovolná $x, y \in R$, že $x + y = (x + y)(x + y) = x^2 + xy + yx + y^2 = x + y + xy + yx$. Přičtením $-(x + y)$ k oběma stranám pak dostáváme $0 = xy + yx$, a tedy $-(xy) = yx$. Pro speciální volbu $a = x = y$ proto $a = -a$, což ale platí pro všechna $a \in R$, a tedy i pro prvek xy ; nakonec tedy obdržíme $xy = -(xy) = yx$.

Jak už jsem řekl po zkoušce, takovéto okruhy se nazývají booleovské a jedná se vlastně o převlečené booleovské algebry. Kromě tělesa $\mathbb{Z}_2$ už ale žádný další není obor (triviální okruh není obor dle definice na přednášce).

- (6) Bylo vidět, že máte už něco podobného nacvičeného. Řešila se soustava kongruencí $x \equiv_{17} 3, x \equiv_{16} 10, x \equiv_{15} 0$. Řešení jste hledali nejčastěji ve tvaru $\alpha + 17\beta + 17 \cdot 16\gamma$, přičemž jste ihned položili $\alpha = 3$, aby byla splněna první kongruence. Dále jste řešili $3 + 17\beta \equiv_{16} 10$, což vzhledem k tomu, že $17 \bmod 16 = 1$, dalo $\beta = 7$. Máme $3 + 17 \cdot 7 = 122$, a tak ještě musíme vyřešit $122 + 17 \cdot 16\gamma \equiv_{15} 0$. Modulo 15 je $17 \cdot 16$ rovno $2 \cdot 1$ a zároveň $122 \bmod 15 = 2$. Dostáváme proto $2 + 2\gamma \equiv_{15} 0$, což znamená, že γ je kongruentní s -1 modulo 15, tj. $\gamma \equiv_{15} 14$. Nakonec $x = 122 + 14 \cdot 16 \cdot 17 = 122 + 14 \cdot 272 = 122 + 3808 = 3930$.

Uznával jsem i nedovyčíslený poslední krok. Za početní chyby jsem strhával půlbody. Problémy jste si nejčastěji přivodili nešikovnými úpravami a zbytečným zdlouhavým počítáním inverzních prvků modulo 16, resp. 15.

- (7) Bonusovou úlohu rovněž nikdo nevyřešil. Možná jsem měl dát do nápovědy, že se nejedná o dva kořeny. Správný výsledek mohl být např. $5x^2 + 5x = 5x(x+1)$, který má za kořeny všechny prvky okruhu $\mathbb{Z}_{10}$. Úvaha, která k němu vedla, spočívala v tom, že $5x$ má za kořeny všechny sudé prvky ze $\mathbb{Z}_{10}$, a tedy $5(x+1)$ má za kořeny všechny liché. Jelikož $5 \cdot 5 = 5$ v $\mathbb{Z}_{10}$, je $5x(x+1)$ jejich součinem.