

# Algebra, každý začátek je lehký

---

## Výsledky cvičení

In: Herbert Kästner (author); Peter Göthner (author); Karel Horák (translator): Algebra, každý začátek je lehký. (Czech). Praha: Mladá fronta, 1986. pp. 163–173.

Persistent URL: <http://dml.cz/dmlcz/404150>

### Terms of use:

© ÚV matematické olympiady

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://dml.cz>

# VÝSLEDKY CVIČENÍ

## Kapitola 1

1.  $M_1 = \{x: x \in \mathbb{Q} \text{ a } |x| > 2\}$ ,

$M_2 = \{x: x \in \mathbb{Z} \text{ a } x^2 = 1\}$ ,

$M_3 = \{x: x \in \mathbb{Q} \text{ a } \frac{22}{7} < x < \pi\} = \emptyset$ .

2. Průnikem je množina, která obsahuje jediný bod  $(2; 1)$ .

3.

$A$	$B$	$A \cap B$	$A \cup (A \cap B)$
1	1	1	1
1	0	0	1
0	1	0	0
0	0	0	0

Porovnáním 1. a 4. sloupce dostáváme tvrzení a); b) dokážeme analogicky.

4. Z  $A \subset B \subset C$  plyne  $A \cup B = B$  a  $B \cap C = B$ , je tedy  $A \cup B = B \cap C$ .

Obráceně, z  $A \cup B = B \cap C$  plyne, že  $A \cup B \subset B$ ; leží tedy každé  $x \in A$  také v  $B$ . Z uvedeného předpokladu ale dostaneme i  $B \cap C \supset B$ , tj. každé  $x \in B$  leží také v  $C$ .

5. Jsou-li  $A_i, A_k$  disjunktní, tedy  $A_i \cap A_k = \emptyset$ , plyne tvrzení bezprostředně z toho, že  $A \cap \emptyset = \emptyset$ . Obrácené tvrzení neplatí, jak se snadno přesvědčíme konstrukcí protipříkladu.

6. Všechny výroky jsou navzájem ekvivalentní.

7. Necht  $x \in A \cup B$ , pak je  $x \in A$  nebo  $x \in B$ . V obou případech dostáváme  $x \in Z$ , je tedy  $A \cup B \subset Z$ .

8. Pravdivé jsou výroky c) a d).
9. a)  $A \cap C$ , b)  $A \cap B$ , c)  $A$ , d)  $A \cap B$ , e)  $\emptyset$ .
10.  $A \times B$  má  $rs$  prvků.
11. Je-li  $x \in A$  a  $y \in C$ , tj.  $(x, y) \in A \times C \subset B \times C$ , je také  $x \in B$ , neboli  $A \subset B$ . Stejně dostaneme i obrácenou inkluzi, tudíž  $A = B^{13)}$ .
12.  $F_1, F_2$  a  $F_4$  jsou zobrazení, pouze  $F_4$  je vzájemně jednoznačné.
13. Hledané funkce můžeme popsat následujícími vztahy:  
 $(f \circ f)(x) = x^4 + 2x^2 + 2$ ,  $(g \circ g)(x) = 9x + 8$ ,  
 $(f \circ g)(x) = 3x^2 + 5$ ,  $(g \circ f)(x) = 9x^2 + 12x + 5$ ,  
 $f^{-1}(x) = \sqrt{x-1}$ ,  $g^{-1}(x) = \frac{1}{3}(x-2)$ .

14. Pouze c) a d) jsou rozklady.
15. Uvedené rozdělení je rozklad. To plyne z toho, že víme o podobných zobrazeních:  
 (1) složením dvou podobností dostaneme podobnost;  
 (2) inverzním zobrazením k podobnosti je podobnost;  
 (3) identické zobrazení je podobnost.
16. Jenom  $M_3$  a  $M_6$  jsou konečné množiny.
17. Vzájemně jednoznačné zobrazení  $\varphi$  množiny všech kmenových zlomků na  $N_0 \setminus \{0\}$  můžeme definovat takto:

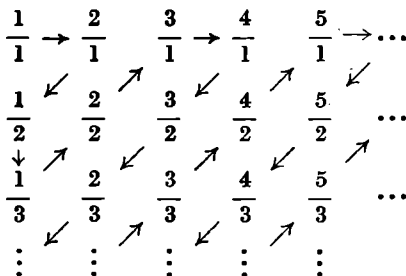
$$\varphi\left(\frac{1}{n}\right) = n.$$

Pro důkaz druhého tvrzení použijte návodů ke cvičení 18.

18. Očíslujme zlomky po řadě tak, jak ukazuje následující

<sup>13)</sup> Předpoklad  $C \neq \emptyset$  je podstatný, neboť klademe  $A \times \emptyset = \emptyset$  pro libovolnou množinu  $A$ . (Pozn. překl.)

schéma. Dostaneme tak vzájemně jednoznačné zobrazení  $Q^*$  na  $N_0$ .



Takovéto zobrazení můžeme použít i na množinu všech uspořádaných dvojic přirozených čísel.

## Kapitola 2

1. a)  $\{(1; 0), (2; 1), (3; 2), (4; 3), (5; 4)\}$ .

b) Označme  $M_1 = \{1\}$ ,  $M_2 = \{2\}$ ,  $M_3 = \{3\}$ ,  $M_4 = \{1; 2\}$ ,

$M_5 = \{1; 3\}$ ,  $M_6 = \{2; 3\}$ , pak je

$R = \{(\emptyset, M_1), (\emptyset, M_2), (\emptyset, M_3), (\emptyset, M_4), (\emptyset, M_5), (\emptyset, M_6),$   
 $(\emptyset, M), (M_1, M_4), (M_1, M_5), (M_1, M), (M_2, M_4),$   
 $(M_2, M_5), (M_2, M), (M_3, M_5), (M_3, M_6), (M_3, M),$   
 $(M_4, M), (M_5, M), (M_6, M)\}$ .

c)  $R = \{(2; 2), (2; 4), (2; 8), (2; 60), (4; 4), (4; 8), (4; 60),$   
 $(5; 5), (5; 45), (5; 60), (8; 8), (45; 45), (60; 60)\}$ .

2.  $M \times M = \{(1; 1), (1; 2), (2; 1), (2; 2)\}$ . Označíme-li  $a = (1; 1)$ ,  $b = (1; 2)$ ,  $c = (2; 1)$  a  $d = (2; 2)$ , dají se všechny relace v  $M$  znázornit takto:

$R_1 = \emptyset, R_2 = \{a\}, R_3 = \{b\}, R_4 = \{c\}, R_5 = \{d\}, R_6 = \{a, b\},$

$R_7 = \{a, c\}, R_8 = \{a, d\}, R_9 = \{b, c\}, R_{10} = \{b, d\}, R_{11} =$

$= \{c, d\}, R_{12} = \{a, b, c\}, R_{13} = \{a, b, d\}, R_{14} = \{a, c, d\},$

$R_{15} = \{b, c, d\}, R_{16} = M \times M.$

Každá relace v  $M$  je podle definice podmnožina  $M \times M$ . Existuje tedy tolik relací v  $M$ , kolik je podmnožin množiny  $M \times M$ . Obsahuje-li  $M$   $n$  prvků, má  $M \times M$   $n^2$  prvků a  $\mathcal{P}(M \times M)$  má podle 1. kapitoly  $2^{n^2}$  prvků.

$$3. R_1 = \{(1; 1), (1; 3), (1; 5), (3; 1), (3; 3), (3; 5), (5; 1), (5; 3), (5; 5)\},$$

$$R_2 = \{(1; 3), (2; 4), (3; 5), (4; 6)\}.$$

Nyní můžeme uzlový či kartézský graf uvedených relací nakreslit.

4. a) např. relace „ $<$ “ v  $N_0$ ,

b) např.  $R = \{(1; 1), (1; 2), (2; 1), (2; 2)\}$  v  $M = \{1, 2, 3\}$ ,

c)  $R \subset S$  a  $R \neq S$  platí např. pro relaci  $R$ : „je vlastní dělitel“ a  $S$ : „je dělitel“ v  $N_0$ ,

d) relace „bezprostředně následuje po“

a „stojí bezprostředně před“ jsou příkladem navzájem inverzních relací v  $N_0$ .

5. a) Vždy platí  $(x, y) \in R \Rightarrow (y, x) \in R^{-1}$ . Je-li  $R = R^{-1}$ , pak je pro  $(x, y) \in R$  také  $(y, x) \in R$ , tj.  $R$  je symetrická. Je-li obráceně  $R$  symetrická, platí  $R = R^{-1}$ , neboť všechny předchozí implikace lze obrátit. Jsou tedy výroky „ $R$  je symetrická“ a „ $R = R^{-1}$ “ ekvivalentní.

b)  $R_i \subset R$  znamená, že pro všechna  $x \in M$  platí  $(x, x) \in R$ , takže  $R$  je reflexivní. Obráceně, pro reflexivní  $R$  platí  $R_i \subset R$ .

c) Je-li  $(x, y) \in R$  a  $(y, z) \in R$ , pak platí  $(x, z) \in R \circ R$  (skládání přiřazení). Je-li nyní  $R \circ R \subset R$ , znamená to tranzitivitu  $R$ . Obráceně, z tranzitivity  $R$  vyplývá výrok  $R \circ R \subset R$ .

Předchozí výsledky můžeme shrnout:

$R$  reflexivní  $\Leftrightarrow R_i \subset R$ ;  $R$  symetrická  $\Leftrightarrow R = R^{-1}$ ;

$R$  tranzitivní  $\Leftrightarrow R \circ R \subset R$ .

6. „Odůvodnění“ začíná předpokladem, že pro prvek  $x$  existuje (alespoň) jedno  $y$  takové, že  $xRy$ ; tj. uvedený závěr

je možný jen pro taková  $x$ , která jsou v relaci s nějakým prvkem  $y \in M$ . Abychom dostali reflexivitu, museli bychom mít  $xRx$  pro všechna  $x$  ( $z M$ ).

7. Až na relaci c) jsou všechny relace reflexivní, symetrické a tranzitivní, tedy relace ekvivalence. Relace v c) není symetrická.

Třída ekvivalence relace f), která obsahuje prvek  $(2; 5)$ , je  $\{(x, x + 3) : x \in \mathbb{N}_0\}$ .

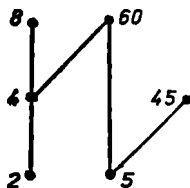
8. a) Podle V (2.3) se reflexivita a tranzitivita přenáší z  $R$  na  $R^{-1}$ ; je tedy také  $R \cap R^{-1}$  reflexivní a tranzitivní. Kromě toho je  $R \cap R^{-1}$  symetrická:

$(x, y) \in R \cap R^{-1} \Rightarrow (x, y) \in R$  a  $(x, y) \in R^{-1} \Rightarrow (y, x) \in R^{-1}$   
 a  $(y, x) \in R \Rightarrow (y, x) \in R \cap R^{-1}$ .

b) Protože  $(x, x) \in R$  a  $(x, x) \in S$  pro všechna  $x \in M$ , je také  $(x, x) \in R \cap S$ ; tj.  $R \cap S$  je reflexivní. Je-li  $(x, y) \in R \cap S$ , je  $(x, y) \in R$  a  $(x, y) \in S$  a na základě předpokládané symetrie  $R$  a  $S$  odtud plyne  $(y, x) \in R$  a  $(y, x) \in S$ , neboli  $(y, x) \in R \cap S$ . Je tedy  $R \cap S$  také symetrická, a podobně se ukáže, že je tranzitivní.

Pro  $R \cup S$  to neplatí, jak ukazuje protipříklad  $R = \{(a, a), (a, b), (b, a), (b, b)\}$ ,  $S = \{(a, a), (a, c), (c, a), (c, c)\}$  pro  $b \neq c$ :  $R \cup S$  obsahuje  $(b, a)$  a  $(a, c)$ , ale neobsahuje  $(b, c)$ , nemůže tedy být tranzitivní, a tudíž ani relací ekvivalence.

9. a)



b) Z grafu v cvičení 9a) vidíme, že výrok „v  $M$  neexistuje prvek, který by ležel pod 5“ je pravdivý, zatímco „všech-

ny prvky  $y \neq 5$  jsou nad 5“ pravdivý není, neboť 2 a 5 jsou nesrovnatelné.

10. a) Tvzení dostaneme použitím V(2.3). Protože některé zde použité výroky z V(2.3) nebyly v odstavci 2.2 dokázány, dožeňte to zde!

b) Platí  $xRx$  pro všechna  $x \in M$  a  $ySy$  pro všechna  $y \in N$ , podle definice  $T$  je tedy také  $(x, y)T(x, y)$  pro všechny  $(x, y) \in M \times N$ .  $T$  je tedy reflexivní. Ze vztahů

$$(x_1, y_1)T(x_2, y_2) \text{ a } (x_2, y_2)T(x_3, y_3)$$

plyne  $x_1Rx_2$  a  $x_2Rx_3$  stejně jako  $y_1Sy_2$  a  $y_2Sy_3$ . Předpokládaná tranzitivita  $R$  a  $S$  dovoluje závěr, že  $x_1Rx_2$  a  $y_1Sy_3$ , tedy také  $(x_1, y_1)T(x_3, y_3)$ .  $T$  je tudíž tranzitivní, a antisymetrie  $T$  se ukáže stejně.

11. a) Relace slučitelné nejsou; v  $\mathcal{P}(\{1, 2, 3, 4\})$  např. platí:  $\{1; 2\} \subset \{1, 2, 3\}$ ,  $\{1, 2\}$  má právě tolik prvků jako  $\{3; 4\}$  a  $\{1, 2, 4\}$  právě tolik prvků jako  $\{1, 2, 3\}$ , ale neplatí  $\{3; 4\} \subset \{1, 2, 4\}$ .

b) Pro  $x \leq y$  musí být každý prvek úplného vzoru  $x$  při  $f$  menší nebo rovný každému prvku úplného vzoru  $y$  při  $f$ . Tuto podmínku kupříkladu splňuje funkce  $f(x) = [x]$  ( $[x]$  je největší celé číslo  $\leq x$ ).

## Kapitola 3

1. Zúžení sčítání číselných posloupností na množiny  $M_1$  a  $M_2$  je neomezeně definovaná operace, neboť součet dvou aritmetických (resp. rostoucích) posloupností je opět aritmetická (resp. rostoucí) posloupnost. Pro geometrické posloupnosti tento výrok neplatí.
2. Obě operace jsou komutativní, ale jenom  $\circ_1$  je invertibilní. Např. rovnice  $b \circ_1 x = c$  nemá v  $\{a, b, c, d\}$  řešení. Neutrálním prvkem uvedených operací je  $a$ , resp.  $d$ .

3. Důkaz můžeme provést probráním všech možných případů, jež mohou vzhledem k relaci  $\leq$  pro  $a, b, c$  nastat.
4. Psaní číslic přirozených čísel za sebou je nezávislé na uzávorkování: je tedy  $\circ_3$  asociativní. Příklad  $12 \circ_3 45 = 1\ 245 \neq 4\ 512 = 45 \circ_3 12$  ukazuje nekomutativnost  $\circ_3$ . Operace  $\circ_3$  není ani invertibilní, neboť např. rovnice  $1\ 467 \circ_3 x = 347$  nemá zřejmě řešení. Naproti tomu má  $\circ_3$  vlastnost krácení; z  $a \circ_3 x_1 = a \circ_3 x_2$  vždy plyne  $x_1 = x_2$ , neboť rovnají-li se dvě přirozená čísla, rovnají se i příslušné číslice (v téže číselné soustavě). Pravý nebo levý neutrální prvek operace  $\circ_3$  nemá.
5. Operace  $\Delta$  není ani komutativní, ani asociativní, ale je invertibilní. Také má vlastnost krácení.
6. Všechny tři operace jsou komutativní, zato není žádná z nich asociativní.  $\circ_4$  je invertibilní,  $\circ_5$  a  $\circ_6$  invertibilní nejsou, což lze doložit neřešitelností rovnic  $0 \circ_5 x = 9$ , resp.  $3 \circ_6 x = 6$ . Vlastnost krácení mají  $\circ_4$  a  $\circ_6$ ;  $\circ_5$  ji nemá, neboť z rovnosti  $\sqrt{0 \cdot x_1} = \sqrt{0 \cdot x_2}$  nevyplývá nutně  $x_1 = x_2$ . Že žádná z operací nemá neutrální prvek, dokážeme nepřímo, idempotence se ověří výpočtem.
7. Návod: Necht  $t_1 = D(a, D(b, c))$  a  $t_2 = D(D(a, b), c)$ , pak platí  $t_1|a$  a  $t_1|D(b, c)$ , tj.  $t_1$  dělí  $a, b$  i  $c$ , platí tedy také  $t_1|D(a, b)$  a  $t_1|c$ , odkud plyne  $t_1|t_2$ . Právě tak ukážeme, že  $t_2|t_1$ . Ze vztahů  $t_1|t_2$  a  $t_2|t_1$  však plyne (v  $\mathbb{N}$ )  $t_1 = t_2$ .
8.  $\uparrow$  má 1 jako pravý neutrální prvek, nemá ale levý neutrální. 0 je neutrální prvek  $\square$  a  $-7$  je neutrální prvek  $\circ$ .
9. Z  $a^{x_1} = a^{x_2}$ , resp.  $y_1^a = y_2^a$  plyne  $x_1 = x_2$ , resp.  $y_1 = y_2$ . Uvědomte si přitom, že 0 a 1 nepatří do nosiče operace. Neřešitelnost rovnice např.  $2^x = 7$  v  $\mathbb{N} \setminus \{1\}$  ukazuje, že operace není invertibilní.
10. Pouze operace uvedené v d) a f) jsou komutativní; aso-



ciativní jsou jen e) a f). Neřešitelnost rovnic  $2^x = 5$  (pro b),  $1 \circ x = 4$  (pro d),  $4 \circ x = 5$  (pro e) a  $y \circ 4 = 1$  (pro f) dokládá, že příslušné operace nejsou invertibilní. V c) má každá rovnice  $a \circ x = 2a + x = c$  řešení  $x = c - 2a$ , zato  $y \circ 2 = 2y + 2 = 3$  nemá řešení (v Z). Pouze d) má neutrální prvek, a to 0.

11. Tabulkou operace je následující tabulka

	<i>n</i>	<i>p</i>	<i>q</i>	<i>m</i>
<i>n</i>	<i>n</i>	<i>p</i>	<i>q</i>	<i>m</i>
<i>p</i>	<i>p</i>	<i>n</i>	<i>m</i>	<i>q</i>
<i>q</i>	<i>q</i>	<i>m</i>	<i>n</i>	<i>p</i>
<i>m</i>	<i>m</i>	<i>q</i>	<i>p</i>	<i>n</i>

Uvedený součin je roven  $p$ . Soustava rovnic má řešení  $x = n$ ,  $y = p$ . Neobyčejné zjednodušení rovnic a rovností dostaneme ze vztahů  $p^2 = q^2 = m^2 = n$ , kde  $n$  je neutrální prvek.

12. Řešení je  $\mathbf{X} = \begin{pmatrix} 1 & -1 \\ 1 & 2 \end{pmatrix}$ . Při řešení je třeba využít toho, že násobení matic je vzhledem ke sčítání distributivní. Všechny v úloze uvedené matice jsou regulární.

## Kapitola 4

1. Multiplikativní grupa nesoudělných zbytkových tříd modulo 12:  $p, p, p, p$ ;  
množina všech reálných funkcí vzhledem ke sčítání:  $p, p, p, p$ ;  
množina  $\{1, 2, 3, 6\}$  s operací  $\wedge : p, p, p, n$ .
2. Objekty a, b, c, d jsou pologrupy; e, f, g jsou komutativní grupy; h je grupa (ačkoli násobení matic není obecně komutativní, ukazuje se, že h je komutativní grupa).

3. a) Tabulka nepopisuje grupu, neboť operace není asociativní; je např.  $(ab)d = cd = a$ , ale  $a(bd) = ac = d$ .

b)

	$a_1$	$a_2$	$a_3$	$a_4$	$a_5$
$a_1$	$a_1$	$a_2$	$a_3$	$a_4$	$a_5$
$a_2$	$a_2$	$a_3$	$a_4$	$a_5$	$a_1$
$a_3$	$a_3$	$a_4$	$a_5$	$a_1$	$a_2$
$a_4$	$a_4$	$a_5$	$a_1$	$a_2$	$a_3$
$a_5$	$a_5$	$a_1$	$a_2$	$a_3$	$a_4$

- c) Vyznačené řádky, resp. sloupce necht' „přísluší“ prvkům  $x$  a  $y$ , resp.  $z$  a  $u$ . Pak je  $xz = e$ , tj.  $z = x^{-1}$ , a  $xu = a$ ,  $yz = b$ . Pro hledaný součin dostaneme  $yu = yeu = yx^{-1}xu = (yx^{-1})(xu) = (yz)(xu) = ba$ .
4. Objekty  $c, e, f$  jsou okruhy;  $d$  je těleso;  $a$  je okruh, jestliže prvky matic jsou racionální nebo reálná čísla (obecněji: jestliže jsou prvky nějakého tělesa);  $b$  není ani okruh, ani těleso.
5. a) Podle V(4.3) je třeba ještě ukázat invertibilitu operace. Rovnice  $ax = b$  je vždy řešitelná, protože necháme-li  $x$  probíhat všech  $n$  prvků  $M$  ( $M$  je podle předpokladu konečná, má tedy  $n$  prvků), dostaneme  $n$  součinů  $ax \in M$ , mezi nimiž nemohou být dva stejné. Z  $ax_1 = ax_2$  totiž plyne podle vlastnosti krácení  $x_1 = x_2$ . Dostaneme tedy pro  $n$  možných činitelů  $x$  právě  $n$  navzájem různých součinů  $ax$  z  $M$ , to ale znamená, že každý prvek z  $M$  (řekněme  $b$ ) dostaneme jako nějaký součin  $ax_0$ .  $x_0$  je tedy řešením rovnice  $ax = b$ . Analogicky se ukáže, že i rovnice  $ya = b$  je vždy řešitelná.
- b) Je-li  $a \in U$  ( $U \neq \emptyset!$ ), je podle definice podgrupy také  $a^{-1} \in U$ , a tudíž  $a \cdot a^{-1} = e \in U$ .  $e$  neovlivňuje žádný prvek z  $G$ , a tím spíš ani z  $U$ . Je tedy  $e$  neutrální prvek  $U$ , a protože  $U$  je grupa, nemůže v  $U$  žádný jiný neutrální prvek existovat.
- c) Je-li např.  $G$  podgrupa všech celých čísel dělitelných

dvěma (v aditivní grupě celých čísel) a  $H$  podgrupa všech celých čísel dělitelných třemi, je  $4 \in G \cup H$  (neboť  $4 \in G$ ) i  $9 \in G \cup H$  (neboť  $9 \in H$ ), ale  $4 + 9 = 13 \notin G \cup H$ , neboť je  $13 \notin G$  i  $13 \notin H$ . Není tedy  $G \cup H$  podgrupa.

d) Rovnice  $ab + x = 0$  má podle definice inverzního prvku řešení  $-(ab)$ . Další řešení je  $(-a)b$ , jak ukazuje zkouška:  $ab + (-a)b = (a + (-a))b = 0 \cdot b = 0$ , přičemž jsme postupně použili distributivní zákon, definici inverzního prvku a úlohu nulového prvku při násobení. Protože ale rovnice  $ab + x = 0$  je v okruhu řešitelná jednoznačně, platí tedy  $-(ab) = (-a)b$ . Analogicky se dokážou ostatní tvrzení.

e) Dostaneme ji přímým roznásobením na základě distributivního zákona; protože násobení v tělese je komutativní, můžeme jako obvykle místo  $ab + ba$  psát  $2ab$  (což by v případě  $ab \neq ba$  nebylo možné).

$$6. \quad \begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array} \quad \begin{array}{c|ccc} + & 0 & 1 & a \\ \hline 0 & 0 & 1 & a \\ 1 & 1 & a & 0 \\ a & a & 0 & 1 \end{array} \quad \begin{array}{c|ccc} \cdot & 0 & 1 & a \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & a \\ a & 0 & a & 1 \end{array}$$

7. c) je homomorfismus, ale ostatní zobrazení jsou izomorfismy.

8. a) Izomorfii zjistíme porovnáním tabulek obou grup; izomorfí zobrazení  $\varphi$  je dáno vztahy  $\varphi(f_1) = (1)_8$ ,  $\varphi(f_2) = (3)_8$ ,  $\varphi(f_3) = (5)_8$ ,  $\varphi(f_4) = (7)_8$ .

b) Označíme-li oba prvky  $(H, +)$  jako 0 a  $a$ , bude zobrazení  $\varphi$ ,

$$\varphi(g) = \begin{cases} 0, & \text{je-li } g \text{ sudé,} \\ a, & \text{je-li } g \text{ liché,} \end{cases}$$

homomorfismus  $(\mathbb{Z}, +)$  na  $(H, +)$ .

c) Aditivní grupa zbytkových tříd modulo 6 je izomorfní s multiplikativní grupou nesoudělných zbytkových tříd modulo 7 díky zobrazení  $\varphi$ , kde  $\varphi((0)_6) = (1)_7$ ,

$\varphi((1)_6) = (3)_7$ ,  $\varphi((2)_6) = (2)_7$ ,  $\varphi((3)_6) = (6)_7$ ,  $\varphi((4)_6) = (4)_7$ ,  
 $\varphi((5)_6) = (5)_7$ .

Aditivní grupa zbytkových tříd modulo 6 je izomorfní s multiplikativní grupou nesoudělných zbytkových tříd modulo 9 díky zobrazení  $\eta$ , kde  $\eta((0)_6) = (1)_9$ ,  $\eta((1)_6) = (2)_9$ ,  $\eta((2)_6) = (4)_9$ ,  $\eta((3)_6) = (8)_9$ ,  $\eta((4)_6) = (7)_9$ ,  $\eta((5)_6) = (5)_9$ . Odtud dostaneme izomorfii grup nesoudělných zbytkových tříd modulo 7 a modulo 9 díky zobrazení  $\varphi^{-1}\eta$ . Protože aditivní grupa zbytkových tříd modulo 6 je cyklická, jsou cyklické i obě další grupy; jejich vytvářející prvky jsou  $(3)_7$ , resp.  $(2)_9$ .

d) Především je  $\varphi$  vzájemně jednoznačné zobrazení  $G$  na  $G$ . Aby  $\varphi$  byl izomorfismus, musí platit:  $\varphi(ab) = \varphi(a)\varphi(b)$ , to ale znamená, že  $(ab)^{-1} = a^{-1}b^{-1}$ . Obecně v každé grupě platí  $(ab)^{-1} = b^{-1}a^{-1}$ . Je tedy  $\varphi$  izomorfismus, právě když  $G$  je komutativní.

9. a)  $U_1 = \{1\}$ ,  $U_2 = \{1; 4\}$ ,  $U_3 = \{1; 11\}$ ,  $U_4 = \{1; 14\}$ ,

$U_5 = \{1, 2, 4, 8\}$ ,  $U_6 = \{1, 4, 7, 13\}$ .

b) Řád 12:  $\{a^0, a^1, \dots, a^{11}\} = \langle a \rangle$ ,

řád 6:  $\{a^0, a^2, a^4, a^6, a^8, a^{10}\} = \langle a^2 \rangle = \langle a^{10} \rangle$ ,

řád 4:  $\{a^0, a^3, a^6, a^9\} = \langle a^3 \rangle = \langle a^9 \rangle$ ,

řád 3:  $\{a^0, a^4, a^8\} = \langle a^4 \rangle = \langle a^8 \rangle$ ,

řád 2:  $\{a^0, a^5\} = \langle a^5 \rangle$ ,

řád 1:  $\{a^0\} = \langle a^0 \rangle$ .

c) Každý homomorfní obraz grupy sestává z úplných obrazů při odpovídajícím homomorfním zobrazení, tedy podle cvičení 9a:

$G/U_1 = G$ ,  $G/U_2 = \{\{1; 4\}, \{2; 8\}, \{7; 13\}, \{11; 14\}\}$ ,

$G/U_3 = \{\{1; 11\}, \{2; 7\}, \{4; 14\}, \{8; 13\}\}$ ,

$G/U_4 = \{\{1; 14\}, \{2; 13\}, \{4; 11\}, \{7; 8\}\}$ ,

$G/U_5 = \{\{1, 2, 4, 8\}, \{7, 11, 13, 14\}\}$ ,

$G/U_6 = \{\{1, 4, 7, 13\}, \{2, 8, 11, 14\}\}$ .