UNIVERZITA PALACKÉHO

PŘÍRODOVĚDECKÁ FAKULTA

I. Chajda, R. Halaš

CVIČENÍ Z ALGEBRY

OLOMOUC 1995

A UP

Ú V O D

Skriptum "Cvičení z algebry" je určeno zejména posluchačům základního třísemestrálního kursu algebry pro odborné studium matematiky a matematické informatiky na přírodovědecké fakultě Palackého university v Olomouci. Doplňuje přednáškový kurs a poskytuje dostatek příkladů pro přípravu na cvičení a pro samostatnou domácí přípravu.

Jednotlivé kapitoly skripta odpovídají kapitolám přednášek. Student může buď procházet tyto kapitoly paralelně s přednáškou, anebo vyhledávat příslušné části při přípravě na zkoušku či zápočet.

Jednotlivé příklady jsou rozdílně obtížné, od zcela elementárních příkladů, vhodných k ilustraci základních pojmů, až po dosti obtížné příklady, které může student konzultovat na cvičeních. U méně elementárních příkladů bývá uvedeno řešení či alespoň stručný návod, a to vždy na konci každé kapitoly.

Čtenáři se doporučuje procházet v každé kapitole všechna cvičení, a zejména pro studenty 1. semestru se doporučuje provádět i jednoduché příklady či důkazy v úplném formalismu. Po zvládnutí vždy určitého typu příkladů pak postupovat k další skupině, při neúspěchu se doporučuje konzultace na cvičeních či individuální.

Doufáme, že tento materiál umožní zejména zlepšit samostatnou přípravu studentů na jednotlivá cvičení z algebry a na písemné testy při udělování zápočtů.

V Olomouci 1993 Autoři

I. ČÁST

1. RELACE

Nechť A,B jsou množiny, $A\times B$ jejich kartézský součin. Relací mezi A a B nazveme každou podmnožinu $R\subseteq A\times B$. Relací na množině A nazveme každou podmnožinu kartézského součinu $A\times A$.

Relace R na množině A je reflexivní, jestliže pro každý prvek $x\in A$ platí $\langle x,x\rangle\in R$. Relace R je symetrická, jestliže pro každé $x,y\in A$, pokud $\langle x,y\rangle\in R$, pak také $\langle y,x\rangle\in R$. Relace R je tranzitivní, jestliže pro každé $x,y,z\in A$, pokud $\langle x,y\rangle\in R$ a $\langle y,z\rangle\in R$, pak také $\langle x,z\rangle\in R$. Relace R je antisymetrická, jestliže pro každé $x,y\in A$, pokud $\langle x,y\rangle\in R$ a $\langle y,x\rangle\in R$, pak $x=y$.

Symbolem ω_A označíme tzv. identickou relaci na A, neboli rovnost, t.j. $\langle x,y\rangle\in\omega_A$, právě když $x=y$. Symbolem ι_A označíme tzv. úplnou relaci na A, neboli úplný čtverec, t.j. $\iota_A=A\times A$. Je-li zřejmé, o jakou množinu A se jedná, můžeme index vynechat a psát pouze ω resp. ι. Je-li R relace na A, označme symbolem R^{-1} tzv. inverzní relaci k R, t.j.

$$R^{-1}=\{\langle x,y\rangle;\langle y,x\rangle\in R\}$$

Je-li R relace mezi A,B a S relace mezi B,C, označme symbolem $R\circ S$ tzv. relační součin, neboli složenou relaci, t.j. $\langle x,z\rangle\in R\circ S$, právě když existuje $y\in B$ tak, že $\langle x,y\rangle\in R$ a $\langle y,z\rangle\in S$. Násobení relací je asociativní, t.j. pro každé tři relace $R\subseteq A\times B$, $S\subseteq B\times C$, $T\subseteq C\times D$ je

$$R\circ(S\circ T)=(R\circ S)\circ T.$$

Dále budeme používat množinové symboly, t.j. $\cup$ označuje sjednocení, $\cap$ označuje průnik množin, $\emptyset$ označuje prázdnou množinu. Je-li Γ množina a pro každé $\gamma\in\Gamma$ je A_γ množina, označme symbolem $\{A_\gamma\ ;\gamma\in\Gamma\}$ tzv. systém množin (v systému množin se mohou množiny opakovat, t.j. pro $\gamma\neq\delta$, $\gamma\in\Gamma$, $\delta\in\Gamma$ může být $A_\gamma=A_\delta$). Naopak,

zapisujeme-li množinu A výčtem jejích prvků, t.j. $A=\{a,b,c\}$ nebo $A=\{a_1,a_2,\dots\}$ resp. $A=\{a_\gamma;\gamma\in\Gamma\}$, předpokládáme, že tyto prvky jsou po dvou různé, t.j. že se neopakují. Symbolem $\subseteq$ označíme množinovou inkluzi.

Příklady:

(1) Nechť R,S,T jsou relace na množině A. Dokažte:

(a) $(R\cup S)^{-1}=R^{-1}\cup S^{-1}$

(b) $(R\cap S)^{-1}=R^{-1}\cap S^{-1}$

(c) $R\subseteq S \Longrightarrow R^{-1}\subseteq S^{-1}$

(d) $R\circ(S\cup T)=(R\circ S)\cup(R\circ T)$

(e) $(S\cup T)\circ R=(S\circ R)\cup(T\circ R)$

(f) $R\circ(S\cap T)\subseteq(R\circ S)\cap(R\circ T)$

(g) $(S\cap T)\circ R\subseteq(S\circ R)\cap(T\circ R)$

(h) $R\circ\omega=\omega\circ R=R$.

(2) Nechť R je relace na množině $A\neq\emptyset$. Dokažte:

(a) R je reflexivní právě když $\omega\subseteq R$

(b) R je symetrická právě když $R=R^{-1}$

(c) R je tranzitivní právě když $R\circ R\subseteq R$

(d) R je antisymetrická právě když $R\cap R^{-1}\subseteq\omega$.

(3) Nechť R,S jsou tranzitivní relace na A. Dokažte, že také relace R^{-1} a $R\cap S$ jsou tranzitivní. Nechť R,S jsou symetrické relace na A. Dokažte, že také relace R^{-1}, $R\cap S$, $R\cup S$ jsou symetrické.

(4) Jsou-li R,S symetrické relace na A, pak $R\circ S$ je symetrická relace na A, právě když $R\circ S=S\circ R$. Dokažte!

(5) Jsou-li R,S reflexivní relace na $A\neq\emptyset$, pak

$$R\cup S\subseteq R\circ S.$$

(6) Které relace na množině A jsou současně symetrické i antisymetrické?

(7) Nechť R_i (pro $i\in I$) jsou reflexivní relace na $A\neq\emptyset$. Pak

$R=\cup\{R_i; i\in I\}$ je opět reflexivní relace na A. Dokažte!

(8) Nechť R_i $(i\in I)$ jsou symetrické relace na A. Pak $R=\cup\{R_i; i\in I\}$ je opět symetrická relace na A. Dokažte!

(9)(a) Je-li R reflexivní a tranzitivní relace na $A\neq\emptyset$, pak $R\circ R=R$. Dokažte!

(b) Ukažte příklad, kdy R je tranzitivní, ale nikoliv reflexivní, a $R\circ R\neq R$.

(10) Nechť A je množina všech lidí na Zemi. Nechť R je relace "býti bratrem", t.j. $\langle x,y\rangle\in R$, právě když x je bratr y. Nechť S je relace "býti rodičem", t.j. $\langle z,v\rangle\in S$, právě když z je rodič v. Co je relace $R\circ S$?

(11) Nechť $R_1,..,R_n,S$ jsou relace na množině A, nechť S je tranzitivní. Dokažte:

Jestliže $R_i\subseteq S$ (pro i=1,..,n), pak $R_1\circ R_2\circ..\circ R_n\subseteq S$.

(12) Dokažte, že pro libovolné relace S_i $(i\in I)$ a T na množině A platí:

(a) $(\cap\{S_i; i\in I\})^{-1}=\cap\{S_i^{-1}; i\in I\}$

(b) $(\cup\{S_i; i\in I\})^{-1}=\cup\{S_i^{-1}; i\in I\}$

(c) $(\cup\{S_i; i\in I\})\circ T=\cup\{S_i\circ T; i\in I\}$

$T\circ(\cup\{S_i; i\in I\})=\cup\{T\circ S_i; i\in I\}$

(d) $(\cap\{S_i; i\in I\})\circ T\subseteq\cap\{S_i\circ T; i\in I\}$

$T\circ(\cap\{S_i; i\in I\})\subseteq\cap\{T\circ S_i; i\in I\}$.

Ukažte příklad, kdy $\subseteq$ nelze nahradit rovností.

(13) Nechť A je n-prvková množina. Kolik existuje různých relací na A?

Návody k řešení:

(1)(a) Nechť $\langle x,y\rangle\in(R\cup S)^{-1}$; pak $\langle y,x\rangle\in R\cup S$, tedy $\langle y,x\rangle\in R$ nebo $\langle y,x\rangle\in S$, t.j. $\langle x,y\rangle\in R^{-1}$ nebo $\langle x,y\rangle\in S^{-1}$, neboli $\langle x,y\rangle\in R^{-1}\cup S^{-1}$. Analogicky se dokáže obrácená inkluze.

(f) Nechť $\langle x,y\rangle\in R\circ(S\cap T)$. Pak existuje $z\in A$ tak, že $\langle x,z\rangle\in R$ a $\langle z,y\rangle\in S\cap T$, t.j. $\langle z,y\rangle\in S$ a také $\langle z,y\rangle\in T$. Dle definice součinu relací $\langle x,y\rangle\in R\circ S$ a současně $\langle x,y\rangle\in R\circ T$, tedy $\langle x,y\rangle\in(R\circ S)\cap(R\circ T)$. Dokázali jsme $R\circ(S\cap T)\subseteq(R\circ S)\cap(R\circ T)$.

(h) Jestliže $\langle x,y\rangle\in R$, použijeme reflexivity relace ω, t.j. $\langle y,y\rangle\in\omega$, odkud $\langle x,y\rangle\in R\circ\omega$, t.j. $R\subseteq R\circ\omega$. Obráceně, jestliže $\langle x,y\rangle\in R\circ\omega$, pak existuje $z\in A$ tak, že $\langle x,z\rangle\in R$ a $\langle z,y\rangle\in\omega$. Ale $\langle z,y\rangle\in\omega$, právě když $z=y$, tedy $\langle x,y\rangle\in R$. Dokázali jsme $R\circ\omega\subseteq R$, dohromady $R\circ\omega=R$. Analogicky se dokáže druhá rovnost $\omega\circ R=R$.

(2)(c) Nechť R je tranzitivní, nechť $\langle x,y\rangle\in R\circ R$. Pak existuje $z\in A$ tak, že $\langle x,z\rangle\in R$ a $\langle z,y\rangle\in R$. Z tranzitivity R plyne $\langle x,y\rangle\in R$, tedy $R\circ R\subseteq R$. Obráceně, nechť $R\circ R\subseteq R$, a nechť $\langle x,y\rangle\in R$, $\langle y,z\rangle\in R$. Pak $\langle x,y\rangle\in R\circ R\subseteq R$, tedy R je tranzitivní.

(d) Nechť R je antisymetrická. Nechť $\langle x,y\rangle\in R\cap R^{-1}$, t.j. $\langle x,y\rangle\in R$ a $\langle x,y\rangle\in R^{-1}$, t.j. $\langle y,x\rangle\in R$. Z antisymetrie plyne $x=y$, t.j. $\langle x,y\rangle\in\omega$, neboli $R\cap R^{-1}\subseteq\omega$. Obráceně, nechť $R\cap R^{-1}\subseteq\omega$, a nechť $\langle x,y\rangle\in R$ a $\langle y,x\rangle\in R$. Pak $\langle x,y\rangle\in R^{-1}$, tedy $\langle x,y\rangle\in R\cap R^{-1}\subseteq\omega$, t.j. $x=y$, neboli R je antisymetrická.

(4)(i) Nechť $R\circ S=S\circ R$. Pak:

$$(R\circ S)^{-1}=(S\circ R)^{-1}=R^{-1}\circ S^{-1}=R\circ S,$$

tedy (viz příklad 2(b)) je i $R\circ S$ symetrická relace.

(ii) Nechť $R\circ S$ je symetrická. Pak $R\circ S=(R\circ S)^{-1}=S\circ R$. (Využívá se vlastnosti, že pro symetrické R,S platí $R=R^{-1}$, $S=S^{-1}$).

(5) Návod: využijte toho, že pro reflexivní R,S platí $R\subseteq R\circ S$, $S\subseteq R\circ S$ (Proč?).

(6) Je-li $A \neq \emptyset$, pak libovolná podmnožina relace ω je současně symetrická i antisymetrická relace.

(8) Nechť $\langle x,y\rangle \in R = \cup\{R_i; i \in I\}$. Pak existuje $j \in I$ tak, že $\langle x,y\rangle \in R_j$. Ale R_j je symetrická, tedy $\langle y,x\rangle \in R_j$, ale $R_j \subseteq \cup\{R_i; i \in I\} = R$, tedy $\langle y,x\rangle \in R$. Tedy R je symetrická.

(9)(a) Dle příkladu 2(c) je $R \circ R \subseteq R$. Je-li R navíc reflexivní, je dle 2(a) $\omega \subseteq R$, a tedy (dle 1(h)) $R = \omega \circ R \subseteq R \circ R$. Dohromady $R \circ R = R$.

(h) Stačí zvolit $A = \{a,b,c\}$, $R = \{\langle a,b\rangle, \langle b,c\rangle, \langle a,c\rangle\}$. Zřejmě R je tranzitivní, ale nikoliv reflexivní. Snadno ověříme $R \circ R = \{\langle a,c\rangle\} \subseteq R$, ale $R \circ R \neq R$.

(10) $R \circ S$ je relace býti strýcem.

(13) Má-li A právě n prvků, pak kartézský součin $A \times A$ obsahuje n^2 prvků a všech podmnožin $A \times A$ (t.j. všech relací na A) je tedy právě 2^{n^2}.

2. ZOBRAZENÍ

Relace R mezi množinami A,B se nazývá <u>zobrazení</u>, jestliže:

(i) $\langle x,y_1\rangle\in R$ a $\langle x,y_2\rangle\in R \Longrightarrow y_1=y_2$

(ii) pro každé $x\in A$ existuje $y\in B$ tak, že $\langle x,y\rangle\in R$.

Zobrazení budeme označovat malými písmeny latinské abecedy, t.j. např. $f,g,h,\ldots$, a místo zápisu $\langle x,y\rangle\in f$ budeme psát obvyklejší $y=f(x)$. Množinu všech $y\in B$ takových, že $y=f(x)$ pro některé $x\in A$ nazveme <u>úplný obraz</u> množiny A a označíme $f(A)$. Zobrazení $f:A\longrightarrow B$ nazveme <u>injekce</u>, jestliže $x\neq z$ pro $x,z\in A$ implikuje $f(x)\neq f(z)$. Zobrazení $f:A\longrightarrow B$ nazveme <u>surjekce</u>, jestliže $f(A)=B$. Zobrazení f se nazývá <u>bijekce</u>, je-li současně injekcí i surjekcí.

Zobrazení $id_A:A\longrightarrow A$ dané předpisem $id_A(x)=x$ se nazývá <u>identické zobrazení</u>.

Jsou-li $f:A\longrightarrow B$, $g:B\longrightarrow C$ zobrazení, pak symbolem $f\circ g$ označujeme (jak bylo v předchozí kapitole zavedeno) jejich relační součin. Relace $f\circ g$ je opět zobrazení (A do C) dané předpisem

$$f\circ g(x)=g(f(x)).$$

Nechť $f:A\longrightarrow B$. Zobrazení $f^{-1}:B\longrightarrow A$ se nazývá <u>inverzní</u> k f jestliže

$$f\circ f^{-1}=id_A \quad \text{a} \quad f^{-1}\circ f=id_B.$$

<u>Příklady:</u>

(1) Nechť R je relace mezi A,B. Dokažte, že R je zobrazení A do B právě když platí

(a) $R\circ R^{-1}\supseteq\omega_A$

(b) $R^{-1}\circ R\subseteq\omega_B$.

Dále, R je injekce, platí-li $R\circ R^{-1}=\omega_A$,

R je surjekce, platí-li $R^{-1}\circ R=\omega_B$.

(2) Nechť A,B jsou množiny a $f:A\longrightarrow B$ zobrazení. Pak je

ekvivalentní:

(a) f je surjekce

(b) $\forall C\ \forall g\ \forall h$: $f \circ g = f \circ h \Longrightarrow g = h$, kde C je libovolná množina, g, h zobrazení B do C.

(3) Nechť A, B jsou množiny a $f: A \longrightarrow B$ zobrazení. Pak je ekvivalentní:

(a) f je injekce

(b) $\forall C\ \forall g\ \forall h$: $g \circ f = h \circ f \Longrightarrow g = h$, kde C je libovolná množina, g, h zobrazení C do A.

(4) Nechť $f: A \longrightarrow B$ je zobrazení. Pak existuje nejvýše jedno inverzní zobrazení k f. Dokažte!

(5) Nechť $f: B \longrightarrow A$, $g: C \longrightarrow A$ jsou zobrazení, přičemž f je injekce. Dokažte:

(a) existuje zobrazení $h: C \longrightarrow B$ takové, že $h \circ f = g$ právě když $f(B) \supseteq g(C)$, přičemž h je jednoznačně určené.

$$\begin{tikzcd} B \arrow[r, "f"] & A \\ C \arrow[u, dotted, "h"] \arrow[ur, "g"'] & \end{tikzcd}$$

(b) h je injekce právě když g je injekce.

(c) h je surjekce právě když $f(B) = f(C)$.

(6) Nechť $f: A \longrightarrow B$, $g: B \longrightarrow C$ jsou zobrazení. Dokažte:

(a) Jsou-li f, g surjekce (injekce), pak je i $f \circ g$ surjekce (injekce).

(b) Je-li $f \circ g$ surjekce, pak je i g surjekce.

(c) Je-li $f \circ g$ injekce, pak je i f injekce.

(d) Ukažte na příkladě, že je-li $f \circ g$ surjekce, pak f nemusí být surjekce.

(e) Je-li $f \circ g$ surjekce a g je injekce, pak je f surjekce.

(f) Ukažte na příkladu, že je-li $f \circ g$ injekce, pak g nemusí být

injekce.

(g) Je-li $f \circ g$ injekce a f je surjekce, pak je i g injekce.

(7) Nechť A je <u>konečná</u> množina, $A \neq \emptyset$. Dokažte, že pro zobrazení $h: A \longrightarrow A$ je ekvivalentní:

(a) h je injekce

(b) h je surjekce

(c) h je bijekce.

Ukažte, že pro A nekonečnou toto tvrzení neplatí.

(8) Nechť $h: G \longrightarrow H$ je zobrazení a nechť $A \subseteq G, B \subseteq G$. Dokažte, že platí

$$h(A \cup B) = h(A) \cup h(B);$$

$$h(A \cap B) \subseteq h(A) \cap h(B).$$

Ukažte na příkladu, že $\subseteq$ nelze nahradit rovností.

(9) Určete všechna možná zobrazení tříprvkové množiny do dvouprvkové množiny.

(10) Určete všechny bijekce čtyřprvkové množiny

$$M = \{a, b, c, d\} \text{ na } M.$$

(11) Nechť $h: A \longrightarrow B$ je surjekce. Dokažte, že existuje $g: B \longrightarrow A$ tak, že $g \circ h = id_B$.

(12) Nechť $h: A \longrightarrow B$ je injekce. Dokažte, že existuje $f: B \longrightarrow A$ tak, že $h \circ f = id_A$.

(13) Ukažte příklad surjektivního zobrazení množiny celých čísel $\mathbb{Z}$ na $\mathbb{Z}$, které není bijekce.

(14) Nechť $f_i: A_i \longrightarrow B_i$ pro $i \in I$ jsou zobrazení. Za jakých předpokladů je relace $f = \cup\{f_i; i \in I\}$ zobrazením množiny $A = \cup\{A_i; i \in I\}$ do $B = \cup\{B_i; i \in I\}$?

(15) Nechť $A \subseteq G$ a $h_A: G \longrightarrow \{0, 1\}$ je zobrazení definované takto (tzv. charakteristická funkce):

$$h_A(x) = 1, \text{ jestliže } x \in A$$

$$h_A(x) = 0, \text{ jestliže } x \notin A.$$

Dokažte:

$$h_{A\cap B}(x)=h_A(x)\cdot h_B(x)=\min(h_A(x),h_B(x))$$

$$h_{A\cup B}(x)=\max(h_A(x),h_B(x)).$$

Jestliže $A\cap B=\emptyset$, pak $h_{A\cup B}(x)=h_A(x)+h_B(x)$.

(16) Nechť $f:A\longrightarrow B$ je zobrazení. Zkonstruujte zobrazení $h:B\longrightarrow A$ tak, aby platilo

$$f\circ h\circ f=f.$$

(17) Zobrazení $f:A\longrightarrow A$ se nazývá idempotentní, jestliže platí

$$f\circ f=f.$$

Dokažte, že jsou-li f,g idempotentní zobrazení A do A a platí-li $f\circ g=g\circ f$, pak $f\circ g$ je rovněž idempotentní zobrazení.

(18) Nechť A,B jsou neprázdné množiny. Dokažte, že projekce $pr_2:A\times B\longrightarrow B$ (t.j. $pr_2(\langle x,y\rangle)=y$) je bijekce, právě když A je jednoprvková množina.

Návody k řešení:

(1) Stačí si uvědomit, že podmínky (a),(b) jsou ekvivalentní s podmínkami (ii),(i) v definici zobrazení.

(2) **(a)$\Longrightarrow$(b).** Je-li f surjekce, $f\circ g=f\circ h$, pak $g(f(x))=h(f(x))$ pro každé $x\in A$. Ovšem $f(A)=B$, tedy $g=h$.
(b)$\Longrightarrow$(a) Není-li f surjekce, pak existuje $b\in B$: $f(a)\neq b$ pro každé $a\in A$. Definujme g,h takto:
$g(b)=c_1, h(b)=c_2$, $c_1\neq c_2$, pro $x\neq b$ nechť $g(x)=h(x)$. Pak $f\circ g=h\circ g$, ale $h\neq g$.

(4) Dokažte sporem!

(5)(a) Je-li $f(B)\supseteq g(C)$, pak pro každé $c\in C$ existuje $b\in B$ tak, že $f(b)=g(c)$. Jelikož f je prosté, existuje právě jedno takové b. Položíme $h(c)=b$ právě když, $f(b)=g(c)$.
Obráceně, existuje-li zobrazení h tak, že $h\circ f=g$, pak

$f(h(C))=g(C)\subseteq f(B)$.

(c) Je-li h surjekce, pak $h(C)=B$, tedy $f(h(C))=f(B)=g(C)$. Orácené, je-li $f(B)=g(C)$, pak pro každé $b\in B$ existuje $c\in C$ tak, že $f(b)=g(c)$. Dle definice h je $h(c)=b$, tedy h je surjekce.

(6)(b) Nechť $f:A\longrightarrow B$, $g:B\longrightarrow C$. Je-li $f\circ g$ surjekce, pak pro každé $c\in C$ existuje $a\in A$ tak, že $g(f(a))=c$. Pak ovšem pro každé $c\in C$ existuje $a'=f(a)$ tak, že $g(a')=c$.

(e) dle (b) je g surjekce, tedy g je bijekce. Pak f musí být surjekce.

(7) **(a)$\Longrightarrow$(b)**. Nechť h není surjekce. Pak existuje $a\in A$ tak, že $h(x)\neq a$ pro každé $x\in A$. Jelikož h je injekce, je $h(x)=h(y)\Longleftrightarrow x=y$. Díky konečnosti A musí existovat dva různé prvky, které se zobrazí na týž prvek, spor.

(b)$\Longrightarrow$(c) podobně jako předchozí implikace.

(c)$\Longrightarrow$(a) zřejmé. Je-li $\mathbb{Z}$ množina celých čísel (je nekonečná), pak je-li $h:\mathbb{Z}\longrightarrow\mathbb{Z}$, $h(x)=2x$, pak tvrzení věty neplatí.

(8) Je-li $a\in h(A\cap B)$, pak $a=h(y), y\in A\cap B$. Pak $a\in h(A)\cap h(B)$. Stačí zvolit $A\cap B=\emptyset$, $h(A)=h(B)\neq\emptyset$.

(10) Je jich $2^4=16$.

(11) Je-li $h:A\longrightarrow B$ surjekce, pak pro každé $b\in B$ existuje $a\in A$ tak, že $h(a)=b$. Stačí položit pro tento prvek b: $g(b)=a$.

(12) Podobně jako (11).

(13) Např. $h(x)=x$ pro $x<0$, $h(0)=h(1)=0$, $h(x)=x-1$ pro $x>1$.

(14) Jestliže pro každé $i,j\in I$ platí $x\in A_i\cap A_j\Longrightarrow f_i(x)=f_j(x)$.

(15) Jestliže $x\in A\cap B$, pak $h_{A\cap B}(x)=1$, $h_A(x)=h_B(x)=1$.
Jestliže $x\notin A\cap B$, pak $h_{A\cap B}(x)=0$, $h_A(x)=0$ nebo $h_B(x)=0$.
Jestliže $x\in A\cup B$, pak $h_{A\cup B}(x)=1$, $h_A(x)=1$ nebo $h_B(x)=1$.
Jestliže $x\notin A\cup B$, pak $h_{A\cup B}(x)=0$, $h_A(x)=h_B(x)=0$.

(16) Je-li $f(X)=b$ pro $X\subseteq A$ a $b\in B$, vybereme libovolně $a\in X$ a

položíme $h(b)=a$. Pro ostatní prvky z $B\setminus f(A)$ (t.j. ty, které nejsou obrazem žádného prvku $a\in A$) definujeme zobrazení h libovolně.

(17) $(f\circ g)\circ(f\circ g)=f\circ(g\circ f)\circ g=f\circ(f\circ g)\circ g=(f\circ f)\circ(g\circ g)=f\circ g$.

(18) Je-li A alespoň dvouprvková, t.j. $A\supseteq\{a_1,a_2\}$, pak $pr_2(\langle a_1,b\rangle)=pr_2(\langle a_2,b\rangle)$, přičemž $\langle a_1,b\rangle\neq\langle a_2,b\rangle$, není tedy pr_2 bijekce.

3. EKVIVALENCE

Relace R na množině $A\neq\emptyset$ se nazývá <u>ekvivalence</u>, je-li reflexivní, symetrická a tranzitivní. Je-li R ekvivalence na A a $x\in A$, označme $[x]_R=\{y\in A;\langle x,y\rangle\in R\}$. Tuto množinu $[x]_R$ nazveme <u>třída</u> ekvivalence R (obsahující prvek x). Zřejmě $[x]_R=[y]_R$ právě když $\langle x,y\rangle\in R$. Množinu všech tříd ekvivalence R na A nazýváme <u>faktorová množina dle ekvivalence R</u> a označujeme A/R.

Je-li $h:A\longrightarrow B$ zobrazení, pak relace E_h daná předpisem

$$\langle x,y\rangle\in E_h \iff h(x)=h(y)$$

je zřejmě ekvivalence, tzv. <u>ekvivalence indukovaná zobrazením h</u>.

Je-li E ekvivalence na množině A, pak zobrazení $h_E:A\longrightarrow A/E$ dané předpisem

$$h_E(x)=[x]_E$$

je tzv. kanonické neboli <u>přirozené zobrazení</u> (indukované ekvivalencí E). Zřejmě h_E je surjekce.

Je-li A množina, $\{B_\gamma;\gamma\in\Gamma\}$ systém neprázdných podmnožin v A, pak $\{B_\gamma;\gamma\in\Gamma\}$ se nazývá <u>rozklad</u> množiny A, jestliže

(i) $\cup\{B_\gamma;\gamma\in\Gamma\}=A$

(ii) jsou-li $\gamma,\delta\in\Gamma$, $\gamma\neq\delta$, pak $B_\gamma\cap B_\delta=\emptyset$.

Je-li $\pi=\{B_\gamma;\gamma\in\Gamma\}$ rozklad množiny A, pak relace E_π daná předpisem $\langle x,y\rangle\in E_\pi$ právě tehdy, když existuje $\delta\in\Gamma$ tak, že $x,y\in B_\delta$, je ekvivalence na A, tzv. <u>ekvivalence indukovaná rozkladem π</u>.

Je-li E ekvivalence na A, pak množina všech po dvou různých tříd této ekvivalence, t.j. A/E je rozklad, tzv. <u>rozklad indukovaný ekvivalencí E</u>.

Příklady:

(1) Určete všechny rozklady na

(a) dvouprvkové množině

(b) tříprvkové množině

(c) čtyřprvkové množině.

(2) Počet všech rozkladů (a tedy i ekvivalencí) na n+1-prvkové množině je

$$p_{n+1}=\sum_{k=1}^{n}\binom{n}{k}p_k\ ,\ \text{kde } p_1=1.$$

Tedy $p_1=1$, $p_2=2$, $p_3=5$, $p_4=15$, $p_5=52$, $p_6=203$, atd. Dokažte!

(3) Nechť $\mathbb{C}$ je množina všech komplexních čísel. Definujme relace R,S na $\mathbb{C}$ takto:

$\langle x+iy,x'+iy'\rangle\in R \iff |x+iy|=|x'+iy'|$,

$\langle x+iy,x'+iy'\rangle\in S \iff \arg(x+iy)=\arg(x'+iy')$,

přičemž klademe arg 0=0. Rozhodněte, zda některá z relací R,S je ekvivalence na $\mathbb{C}$; vyznačte třídy rozkladu!

(4) Ukažte příklad dvou ekvivalencí R,S na A takových, že $R\cup S$ není ekvivalence.

(5) Ukažte příklad ekvivalencí R,S na A takových, že $R\circ S$ není ekvivalence na A.

(6) Nechť R,S jsou ekvivalence na $A\neq\emptyset$. Dokažte, že následující podmínky jsou ekvivalentní:

(a) $R\circ S=S\circ R$

(b) $R\circ S\subseteq S\circ R$.

(7) Nechť $f:A\longrightarrow B$ je zobrazení, E_f je ekvivalence indukovaná zobrazením f. Nechť E je ekvivalence na A. Nechť g je relace mezi A/E a B daná předpisem

$$\langle [a]_E,b\rangle\in g \iff b=f(a).$$

Dokažte, že g je zobrazení $A/E\longrightarrow B$, právě když $E\subseteq E_f$.

(8) Nechť $A=\{a,b,c,d,e,f\}$ a nechť ekvivalence E na A je indukovaná rozkladem

$$\{\{a,b,c\},\{d,e\},\{f\}\}.$$

Určete množinu B a zobrazení $h:A\longrightarrow B$ tak, aby $E=E_h$.

(9) Nechť A,B,C jsou množiny, $f:A\longrightarrow B, g:A\longrightarrow C$ zobrazení, f je surjekce. Dokažte:

(a) existuje zobrazení $h:B\longrightarrow C$ tak, že $f\circ h=g$, právě když $E_f\subseteq E_g$; pak h je jednoznačně určené.

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[dr, "g"'] & B \arrow[d, dotted, "h"] \\ & C \end{tikzcd}$$

(b) h je surjekce, právě když g je surjekce

(c) h je injekce, právě když $E_f=E_g$.

(10) Nechť R,S jsou ekvivalence na množině A. Dokažte, že $R\cup S$ je ekvivalence na A, právě když $R\cup S=R\circ S$.

(11) Nechť E je ekvivalence na množině A. Pro $X\subseteq A$ položme

$$[X]_E=\{a\in A;\langle a,x\rangle\in E \text{ pro některé } x\in X\}.$$

Dokažte: **(a)** $[X]_E\cup[Y]_E=[X\cup Y]_E$

(b) $[X]_E\cap[Y]_E\supseteq[X\cap Y]_E$,

přičemž rovnost platí, právě když $[X]_E=X$ a $[Y]_E=Y$.

(12) Nechť R,S jsou ekvivalence na množině A. Položme $R\vee S=R\cup(R\circ S)\cup(R\circ S\circ R)\cup(R\circ S\circ R\circ S)\cup\ldots$. Dokažte, že $R\vee S$ je ekvivalence na A, přičemž $R\subseteq R\vee S$, $S\subseteq R\vee S$.

(13) Nechť $M\neq\emptyset$, S je ekvivalence na M a nechť T je taková tranzitivní relace na M, že $S\subseteq T$. Definujme relaci T/S na faktorové množině M/S takto:

$$\langle[a]_S,[b]_S\rangle\in T/S \Leftrightarrow \langle a,b\rangle\in T.$$

Dokažte, že je-li T ekvivalence, pak je i T/S ekvivalence na M/S a platí: existuje bijekce

$$(M/S)/(T/S)\longrightarrow M/T.$$

(14) Nechť $K\subseteq M$ a S je ekvivalence na M.

Položme $K^S=\{x\in M;\langle x,y\rangle\in S$ pro některé $y\in K\}$. Pak $S\cap K^2$ je ekvivalence na K a existuje bijekce $K/S\cap K^2$ na K^S/S. Dokažte!

(15) Nechť $\mathbb{N}$ je množina přirozených čísel, $m\in\mathbb{N}$, $m>1$. Zaveďme

relaci Θ_m na $\mathbb{N}$ takto: $\langle x,y\rangle\in\Theta_m \Leftrightarrow m$ dělí $(x-y)$.
Dokažte, že Θ_m je ekvivalence na $\mathbb{N}$ a určete třídy této ekvivalence. Určete počet tříd a počty prvků v jednotlivých třídách.

Návody k řešení:

(1)(a) Nechť $A=\{a,b\}$, pak existují právě dva rozklady množiny A, a to: $\pi_1=\{\{a\},\{b\}\}$;
$\pi_2=\{\{a,b\}\}$.

(b) existuje 5 rozkladů množiny $A=\{a,b,c\}$, a to
$\pi_1=\{\{a\},\{b\},\{c\}\}$;
$\pi_2=\{\{a\},\{b,c\}\}$; $\pi_3=\{\{a,b\},\{c\}\}$; $\pi_4=\{\{a,c\},\{b\}\}$;
$\pi_5=\{\{a,b,c\}\}$.

(c) existuje 15 rozkladů množiny $A=\{a,b,c,d\}$.

(3) Obě relace jsou ekvivalence na $\mathbb{C}$. Třídy relace R jsou soustředné kružnice se středem v bodě 0, třídy relace S jsou polopřímky, procházející bodem 0 ale neobsahující tento bod pokud polopřímka není totožná s kladnou částí reálné osy.

(5) Zvolme např. $A=\{a,b,c\}$, nechť:

R má rozklad $\{\{a,b\},\{c\}\}$,

S má rozklad $\{\{a\},\{b,c\}\}$.

Pak $\langle a,b\rangle\in R, \langle b,c\rangle\in S$, tedy $\langle a,c\rangle\in R\circ S$. Avšak neexistuje $x\in A$ tak, aby $\langle c,x\rangle\in R$ a $\langle x,a\rangle\in S$, tedy $\langle c,a\rangle\notin R\circ S$, t.j. $R\circ S$ není symetrická, t.j. není ekvivalence.

(6) Zřejmě (a)$\Longrightarrow$(b), stačí tedy dokázat (b)$\Longrightarrow$(a): Nechť $R\circ S\subseteq S\circ R$. Z monotonie inverzní relace obdržíme $(R\circ S)^{-1}\subseteq(S\circ R)^{-1}$, a tedy

$$S\circ R=S^{-1}\circ R^{-1}=(R\circ S)^{-1}\subseteq(S\circ R)^{-1}=R^{-1}\circ S^{-1}=R\circ S,$$

(neboť pro ekvivalence platí $R^{-1}=R$, $S^{-1}=S$), t.j. $S\circ R\subseteq R\circ S$. Dohromady, $S\circ R=R\circ S$, t.j. platí (a).

(8) Zvolme např. $B=\{x,y,z\}$. Prvky patří do téže třídy v E_h, mají-li stejný obraz v zobrazení h, t.j. musí platit

$$h(a)=h(b)=h(c),$$

tedy např. $h(a)=h(b)=h(c)=x$, analogicky $h(d)=h(e)=y, h(f)=z$. Zřejmě E_h má třídy $\{a,b,c\},\{d,e\},\{f\}$, tedy $E_h=E$.

(9) (a) Nechť $E_f \subseteq E_g$. Jestliže $b \in B$, pak existuje $a_b \in A$ tak, že $f(a_b)=b$, neboť f je surjekce. Definujme h takto: $h(b)=g(a_b)$. Zřejmě platí $f \circ h(a)=g(a)$ pro každé $a \in A$. Obráceně, jestliže existuje $h: B \longrightarrow C$ tak, že $f \circ h=g$, pak z $\langle a_1,a_2\rangle \in E_f$ plyne $g(a_1)=h(f(a_1))=h(f(a_2))=g(a_2)$, t.j. $\langle a_1,a_2\rangle \in E_g$, odtud $E_f \subseteq E_g$. Jednoznačnost h je zřejmá.

(b) Je-li g surjektivní a $f \circ g=g$, pak musí být i h surjektivní. Je-li h surjektivní, pak z předpokladu, že f je surjektivní, plyne i surjektivita $f \circ g$, tedy i $g=f \circ h$ je surjektivní.

(c) Je-li h injekce, pak $E_{f \circ h}=E_f$. Ale $g=f \circ h$, tedy $E_g=E_{f \circ h}=E_f$. Obráceně, nechť $E_f=E_g$, t.j. $E_f=E_{f \circ h}$. Jestliže h není injekce, pak existují $a_1,a_2 \in A$ tak, že $f(a_1) \neq f(a_2)$ ale $f \circ h(a_1)=f \circ h(a_2)$, t.j. $g(a_1)=g(a_2)$, tedy $\langle a_1,a_2\rangle \in E_g=E_f$, t.j. $f(a_1)=f(a_2)$, spor. Tedy h je injekce.

(10) (a) Nechť $R \cup S$ je ekvivalence. Nechť $\langle x,y\rangle \in R \circ S$. Pak existuje $z \in A$ tak, že $\langle x,z\rangle \in R$ a $\langle z,y\rangle \in S$. Tedy $\langle x,z\rangle \in R \cup S$ a $\langle z,y\rangle \in R \cup S$, odtud $\langle x,y\rangle \in R \cup S$, tedy $R \circ S \subseteq R \cup S$. Dle příkladu 6 platí obrácená inkluze, tedy $R \circ S=R \cup S$.

(b) Nechť platí $R \circ S=R \cup S$. Relace $R \cup S$ je zřejmě reflexivní a symetrická. Jelikož $R \cup S$ je symetrická, je i $R \circ S$ symetrická, tedy $(R \circ S)=(R \circ S)^{-1}=S^{-1} \circ R^{-1}=S \circ R$.

Dokážeme tranzitivitu:

$(R \cup S) \circ (R \cup S)=(R \circ S) \circ (R \circ S)=R \circ (S \circ R) \circ S=R \circ R \circ S \circ S \subseteq R \circ S=R \cup S$.

Tedy $R \cup S$ (viz. příklad 2(c)) je tranzitivní, t.j. $R \cup S$ je ekvivalence.

(12) Jelikož R,S jsou reflexivní, t.j. $\omega \subseteq R$, $\omega \subseteq S$, zřejmě i $\omega \subseteq R \cup S$, t.j. $R \cup S$ je reflexivní. Nechť $\langle x,y\rangle \in R \cup S$. Pak existuje $n \in \mathbb{N}$ tak, že $\langle x,y\rangle \in R \circ S \circ \ldots \circ R \circ S$ (n činitelů).

Pak existují prvky $c_1,c_2,\ldots,c_{n-1} \in A$ tak, že $\langle x,c_1\rangle \in R$,

$\langle c_1,c_2\rangle\in S,\dots,\langle c_{n-1},y\rangle\in S$. Jelikož R,S jsou symetrické, plyne odtud $\langle y,c_{n-1}\rangle\in S$, $\langle c_{n-1},c_{n-2}\rangle\in R,\dots,\langle c_2,c_1\rangle\in S,\langle c_1,x\rangle\in R$, t.j. $\langle y,x\rangle\in \underbrace{S\circ R\circ\dots\circ S\circ R}_{n}\subseteq R\circ \underbrace{S\circ R\circ\dots\circ S\circ R}_{n}$, tedy $\langle y,x\rangle\in R\vee S$, t.j. $R\vee S$ je symetrická.

Dokážeme tranzitivitu: Nechť $\langle x,y\rangle\in R\vee S$, $\langle y,z\rangle\in R\vee S$. Pak existují $n,m\in\mathbb{N}$ tak, že:

$\langle x,y\rangle\in R\circ S\circ\dots\circ R\circ S$ (n činitelů)

$\langle y,z\rangle\in R\circ S\circ\dots\circ R\circ S$ (m činitelů), a tedy:

$\langle x,z\rangle\in R\circ S\circ\dots\circ R\circ S\circ R\circ S\circ\dots\circ R\circ S$ ($m+n$ činitelů),

tedy opět $\langle x,z\rangle\in R\vee S$, t.j. $R\vee S$ je i tranzitivní, tedy $R\vee S$ je ekvivalence. Zřejmě $R\subseteq R\vee S$, také $S\subseteq R\circ S\subseteq R\vee S$.

(13) Nejprve je třeba ukázat, že T/S je dobře definovaná, t.j. že nezávisí na výběru reprezentantů:

je-li $[a]_s=[a']_s$, $[b]_s=[b']_s$, pak $\langle a,a'\rangle\in S$, $\langle b,b'\rangle\in S$, tedy $\langle a,a'\rangle,\langle b,b'\rangle\in T$. Je-li $\langle [a]_s,[b]_s\rangle\in T/S$, pak $\langle a,b\rangle\in T$ a díky tranzitivitě relace T platí $\langle a',a\rangle\in T$, $\langle a,b\rangle\in T$, $\langle b,b'\rangle\in T$, t.j. $\langle a',b'\rangle\in T$, tedy $\langle [a']_s,[b']_s\rangle\in T/S$.

Bijekce mezi množinami $(M/S)/(T/S)$ a M/T je dána takto:

$$\left[[a]_S\right]_{T/S}\longrightarrow [a]_T.$$

(14) Definujme f: $K\longrightarrow K^S/S$ takto:

$f(x)=K_x=\{y\in M:\ \langle y,x\rangle\in S\}$; f je zřejmě surjekce a platí:

$f(x)=f(y)\iff\langle x,y\rangle\in S\iff\langle x,y\rangle\in S\cap(K\times K)$.

Použijte větu o surjektivním zobrazení.

(15) Zbytkové třídy mod m, počet prvků ve třídách je nekonečný, počet tříd je m.

4. USPOŘÁDÁNÍ

Relace R na množině A se nazývá kvaziuspořádání, je-li reflexivní a tranzitivní.

Relace R na A je uspořádání, je-li reflexivní, antisymetrická a tranzitivní.

Je-li R uspořádání na A, pak tuto relaci obvykle označujeme symbolem $\leq$ a místo $\langle x,y\rangle\in\leq$ zapisujeme $x\leq y$. Inverzní relace k relaci $\leq$ je opět uspořádání; tuto relaci označujeme $\geq$.

Prvek $a\in A$ se nazývá největší (nejmenší) vzhledem k $\leq$, jestliže pro každé $x\in A$ platí $x\leq a$ (resp. $a\leq x$). Prvek $b\in A$ je maximální (resp. minimální), jestliže neexistuje $y\in A$ tak, že $b\leq y$, $b\neq y$ (resp. $y\leq b$, $b\neq y$).

Zobrazení $f:A\longrightarrow B$ (kde $\leq_1$ resp. $\leq_2$ je uspořádání na A resp. na B) se nazývá izotonní (nebo také monotonní), jestliže $x\leq_1 y \Longrightarrow f(x)\leq_2 f(y)$. Zobrazení f se nazývá izomorfismus uspořádaných množin, neboli o-izomorfismus, je-li bijektivní, izotonní a f^{-1} je rovněž izotonní.

Uspořádaná množina A se nazývá řetězec, jestliže pro každé $a,b\in A$ platí $a\leq b$ nebo $b\leq a$.

Uspořádaná množina se nazývá antiřetězec, jestliže pro každé $a,b\in A$ platí $a\leq b \Longrightarrow a=b$.

Nechť $\leq$ je uspořádání na $A\neq\emptyset$. Množina A se nazývá (shora) usměrněná, jestliže pro každé $a,b\in A$ existuje $c\in A$ tak, že $a\leq c, b\leq c$ (c je tzv. horní závora a,b).

Příklady:

(1) Nechť A je neprázdná množina; označme symbolem $Exp\ A$ množinu všech podmnožin množiny A. Dokažte, že množinová inkluze $\subseteq$ je uspořádání na A.

(2) Nechť $\leq$ je uspořádání na A. Dokažte, že $\leq^{-1}$ je rovněž uspořádání na A.

(3) Dokažte, že je-li $\leq$ uspořádání na A, pak v A existuje nejvýše jeden největší prvek a nejvýše jeden nejmenší prvek.

(4) Dejte příklad množiny s relací uspořádání $\leq$, která:

(a) nemá ani největší ani nejmenší prvek

(b) má největší ale nemá nejmenší prvek

(c) má nejmenší ale nemá největší prvek

(d) má největší i nejmenší prvek.

(5) Dokažte, že relace ω_A je uspořádání na A, ale ι_A není uspořádání na A pro $|A| \geq 2$.

(6) Dokažte, že má-li A vzhledem k $\leq$ největší prvek, je tento prvek maximální; má-li A nejmenší prvek, je tento prvek minimální.

(7) Zobrazte diagramem příklad množiny s uspořádáním, která má:

(a) více než jeden maximální prvek a prvek nejmenší

(b) více než jeden prvek minimální a prvek největší

(c) více prvků maximálních a více prvků minimálních; dokažte, že v tomto případě nemá ani nejmenší ani největší prvek.

(8) Jaké je uspořádání na alespoň dvouprvkové množině, kde každý prvek je současně minimální a současně maximální?

(9) Nakreslete diagramy všech uspořádaných množin

(a) dvouprvkových

(b) tříprvkových

(c) čtyřprvkových.

Ukažte, které z nich jsou usměrněné.

(10) Na množině přirozených čísel $\mathbb{N}$ zaveďme relaci dělitelnosti:

$$x|y \Leftrightarrow x \text{ dělí } y.$$

Ukažte, že tato relace je uspořádání na $\mathbb{N}$. Má $\mathbb{N}$ vzhledem k tomuto uspořádání největší resp. nejmenší prvek?

(11) Nakreslete diagram uspořádané množiny vzhledem k relaci dělitelnosti (příklad 10)

(a) všech dělitelů čísla 15

(b) všech dělitelů čísla 24

(c) všech dělitelů čísla 30

(d) všech dělitelů čísla 64.

(12) Nechť $\mathbb{Z}$ je množina čísel celých. Na kartézském součinu $\mathbb{K}=\mathbb{Z}\times\mathbb{Z}\times\ldots\times\mathbb{Z}$ (n-krát) zaveďme relaci R takto:

$\langle\langle x_1,\ldots,x_n\rangle,\langle y_1,\ldots,y_n\rangle\rangle\in R \Leftrightarrow$ existuje $k\in\mathbb{N}, 0\le k\le n$ tak, že platí

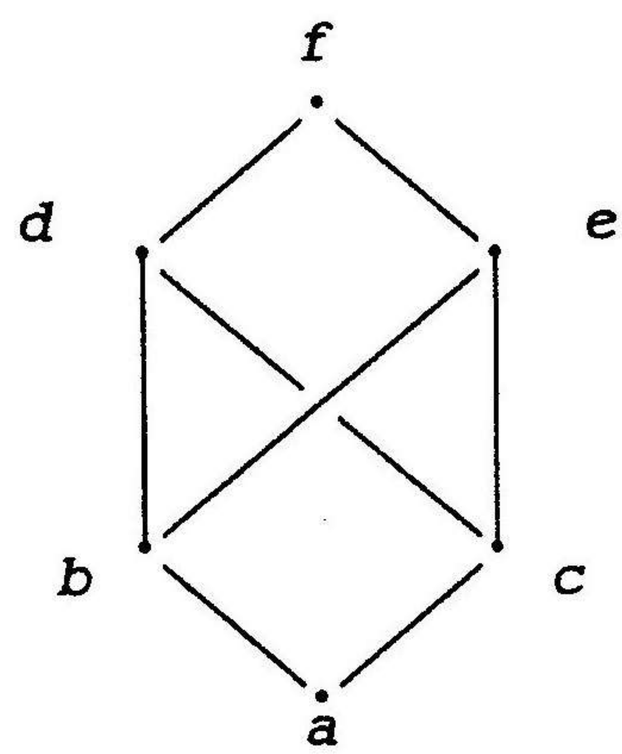
(i) pro $i\le k$ platí $x_i=y_i$

(ii) $x_{k+1}<y_{k+1}$.

Je relace R uspořádání na $\mathbb{K}$? Jestliže ano, nakreslete diagram uspořádání R následující podmnožiny $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}$:

$\{\langle 1,-2,5\rangle,\langle 1,3,3\rangle,\langle 1,3,-1\rangle,\langle 2,2,0\rangle,\langle -1,-2,0\rangle\}$.

(13) Nechť A je množina, jejíž uspořádání je dáno diagramem



Nechť E je ekvivalence na A určená rozkladem:

$\{\{a\},\{b,d\},\{c,e\},\{f\}\}$.

Definujme na množině A/E relace R,S takto:

$\langle[x]_E,[y]_E\rangle\in R \Leftrightarrow$ existují $z\in[x]_E$, $v\in[y]_E$ tak, že $z\le v$,

$\langle[x]_E,[y]_E\rangle\in S \Leftrightarrow$ pro každé $z\in[x]_E, v\in[y]_E$ platí $z\le v$.

Která z relací R,S je uspořádání na A/E?

(14) Každá uspořádaná množina $(A,\leq)$ je o-izomorfní některé podmnožině množiny $(ExpA;\subseteq)$. Dokažte!

(15) Je-li Q relace kvaziuspořádání na množině $A\neq\emptyset$, pak $E_Q=Q\cap Q^{-1}$ je ekvivalence (dokažte!), a relace Q/E_Q na faktorové množině A/E_Q definovaná předpisem
$\langle [a]_{E_Q},[b]_{E_Q}\rangle\in Q/E_Q \Leftrightarrow \langle a,b\rangle\in Q$, je uspořádání. Dokažte!

(16) Na množině $\mathbb{Z}$ všech celých čísel položme $\langle a,b\rangle\in Q \Leftrightarrow$ a dělí b. Dokažte, že Q je kvaziuspořádání, určete E_Q, $\mathbb{Z}/E_Q$ a uspořádání Q/E_Q.

(17) Nechť Q je ekvivalence na $A\neq\emptyset$. Pak zřejmě Q je kvaziuspořádání. Tedy pro ekvivalenci Q určete $E_Q, A/E_Q, Q/E_Q$!

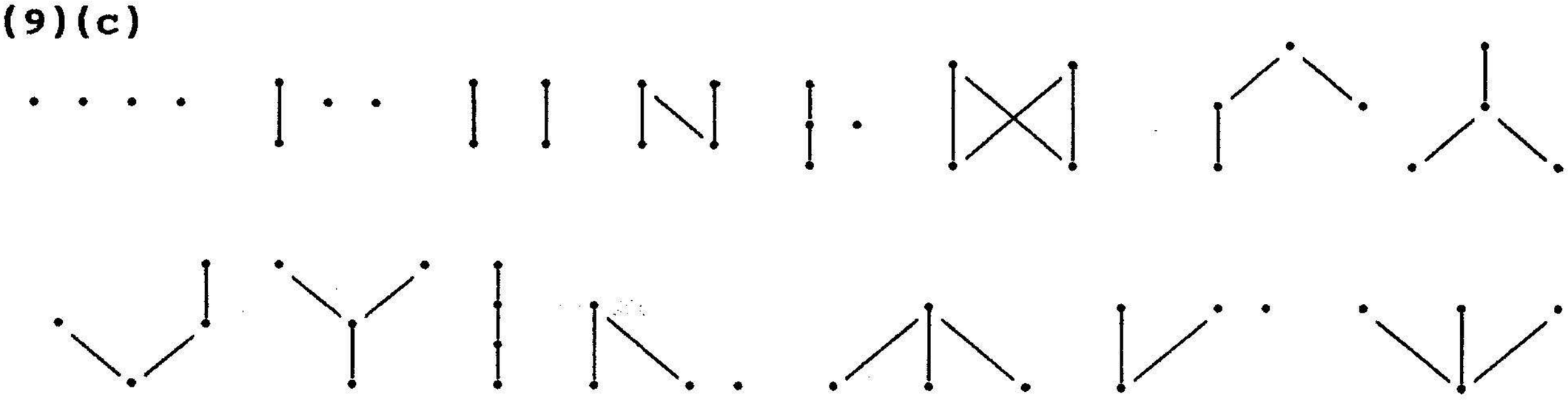
(18) Každé uspořádání na $A\neq\emptyset$ je kvaziuspořádání. Je-li tedy $\leq$ uspořádání na A, určete $E_{\leq}$, $A/E_{\leq}$, $\leq/E_{\leq}$.

<u>Návody k řešení</u>:

(2) Buď R uspořádání, t.j. $\omega_A\subseteq R$, $R\cap R^{-1}\subseteq\omega_A$, $R\circ R\subseteq R$. Stačí ukázat, že totéž platí pro R^{-1}:
$\omega_A=\omega_A^{-1}\subseteq R^{-1}$, $R^{-1}\cap R=R^{-1}\cap(R^{-1})^{-1}\subseteq\omega_A$, $R^{-1}\circ R^{-1}=(R\circ R)^{-1}\subseteq R^{-1}$.

(8) antiřetězec

(9)(c)



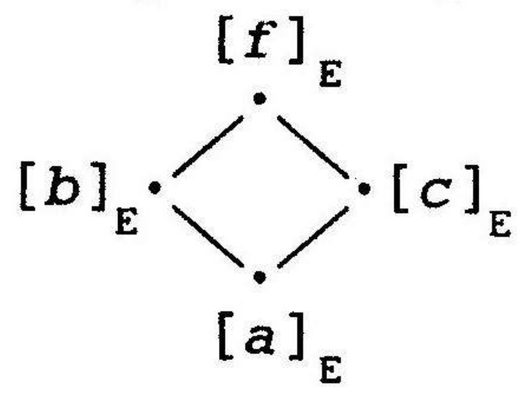
(11) Ukažte, že $\sup(a,b)=NSN(a,b)$, $\inf(a,b)=NSD(a,b)$ (viz. kapitola o svazech).

(12) Je to stejné uspořádání jako ve slovníku (lexikální);

příklad: $(2,2,0)$, $(1,3,3)$, $(1,3,-1)$, $(1,-2,5)$, $(-1,-2,0)$ je to řetězec.

(13) R není uspořádání : $\langle [b]_E, [c]_E \rangle \in R, \langle [c]_E, [b]_E \rangle \in R$, $[b]_E \neq [c]_E$.

S je uspořádání:



(14) Uvažujte zobrazení $f: A \longrightarrow \mathrm{Exp}A$ takto:
$f(a)=L(a)=\{x \in A: x \leq a\}$. Exp$A$ uspořádejte inkluzí a ukažte, že zobrazení f je prosté a izotonní.

(15) $Q \supseteq \omega_A, Q \circ Q \subseteq Q$. Pak $Q^{-1} \supseteq \omega_A^{-1} = \omega_A$, $Q^{-1} \circ Q^{-1} \subseteq Q^{-1}$, $Q \cap Q^{-1} \supseteq \omega_A$, t.j. $E_Q = Q \cap Q^{-1}$ je reflexivní.
E_Q je tranzitivní, neboť $(Q \cap Q^{-1}) \circ (Q \cap Q^{-1}) \subseteq Q \cap Q^{-1}$, $Q \cap Q^{-1}$ je zřejmě symetrická, tedy E_Q je ekvivalence.
Je třeba ukázat, že Q/E_Q je dobře definovaná:
je-li $[a]_{E_Q} = [a']_{E_Q}, [b]_{E_Q} = [b']_{E_Q}$, pak $\langle a, a' \rangle \in E_Q, \langle b, b' \rangle \in E_Q$.
Je-li $\langle [a]_{E_Q}, [b]_{E_Q} \rangle \in Q/E_Q$, pak $\langle a, b \rangle \in Q, \langle b, b' \rangle \in Q, \langle a', a \rangle \in Q$,
Q je tranzitivní, tedy $\langle a', b' \rangle \in Q$.
Reflexivita relace Q/E_Q je zřejmá,
$\langle a, b \rangle \in Q$ a $\langle b, a \rangle \rangle \in Q \Longrightarrow \langle a, b \rangle \in Q \cap Q^{-1} = E_Q$, odtud dostaneme antisymetrii relace Q/E_Q, tranzitivita relace Q/E_Q vyplývá z tranzitivity Q.

(16) Využijte (15).

(17) $Q = Q^{-1}$, tedy $E_Q = Q$, $A/E_Q = A/Q$, t.j. uspořádání $Q/E_Q = \omega$, t.j. antiřetězec.

(18) $Q \cap Q^{-1} \subseteq \omega_A$, je tedy nutně $E_\leq = \omega_A$, $A/E_\leq = A/\omega_A \cong A$, $\leq/_{E_\leq} = \omega_{E_\leq}$.

5. UZÁVĚROVÉ SYSTÉMY

Nechť A je neprázdná množina, $\mathcal{M}$ některý systém jejích podmnožin, t.j. $\mathcal{M} \subseteq Exp A$. Nazveme $\mathcal{M}$ uzávěrový systém na A, je-li uzavřen vzhledem k libovolným průnikům, t.j. pro každý systém $\{A_\gamma; \gamma \in \Gamma\} \subseteq \mathcal{M}$ platí $\cap\{A_\gamma; \gamma \in \Gamma\} \in \mathcal{M}$.

Speciálně, je-li $\mathcal{M}$ uzávěrový systém na A, pak $A \in \mathcal{M}$, neboť A je průnik prázdného podsystému množin z $\mathcal{M}$ (t.j. $\Gamma = \emptyset$).

Systém $\mathcal{N}$ se nazývá usměrněný, jestliže pro každé $B, C \in \mathcal{N}$ existuje $D \in \mathcal{N}$ tak, že $B \subseteq D$, $C \subseteq D$.

Uzávěrový systém $\mathcal{M}$ na množině A se nazývá algebraický, jestliže pro každý usměrněný podsystém $\mathcal{N} \subseteq \mathcal{M}$ platí $\cup \mathcal{N} \in \mathcal{M}$.

Je-li $\mathcal{M}$ uzávěrový systém na množině A, a je-li $X \subseteq A$, označme

$$[X] = \cap\{B \in \mathcal{M}; X \subseteq B\}$$

tzv. uzávěr množiny X v $\mathcal{M}$. Tedy $[X]$ je nejmenší (vzhledem k $\subseteq$) člen uzávěrového systému $\mathcal{M}$ obsahující množinu X.

Je-li $\mathcal{M}$ algebraický uzávěrový systém, pak platí

$$[X] = \cup\{[Y];\ Y \subseteq X,\ Y \text{ konečná}\}.$$

Příklady:

(1) Nechť $A \neq \emptyset$. Dokažte, že $Exp A$ je uzávěrový systém na A. Je to největší uzávěrový systém na A.
Dokažte, že $\{A\}$ je uzávěrový systém na A. Je to nejmenší uzávěrový systém na A.

(2) Nechť A je nekonečná množina, nechť $\mathcal{Y}$ je systém všech konečných podmnožin v A. Tvoří $\mathcal{Y}$ uzávěrový systém na A?

(3) Nechť $A = \{a, b, c\}$, položme $B_0 = \emptyset$, $B_1 = \{a\}$, $B_2 = \{b\}$, $B_3 = \{c\}$, $B_4 = \{a, b\}$, $B_5 = A$.

(a) Je $\{B_0, B_1, B_2, B_3, B_4, B_5\}$ uzávěrový systém na A?

(b) Je $\{B_1, B_4, B_5\}$ uzávěrový systém na A?

(c) Je $\{B_1, B_2, B_5\}$ uzávěrový systém na A?

(d) Je $\{B_0, B_1, B_2, B_3\}$ uzávěrový systém na A?

4) Nechť $A=(0,1)$ je otevřený interval na reálné ose. Ukažte, že systém všech otevřených intervalů $\{(0,r); 0 \le r \le 1\}$ je uzávěrový systém (pokládáme $\emptyset=(0,0)$) na A.

5) Buď I množina všech intervalů na reálné ose, přičemž předpokládejme $(-\infty,\infty) \in I$, $\emptyset \in I$ a $\langle a,a\rangle=\{a\} \in I$.

Které z následujících systémů tvoří uzávěrové systémy na I?:

(a) všechny intervaly z I

(b) všechny intervaly konečné délky

(c) všechny otevřené intervaly ($\emptyset$ je otevřený interval, $\{a\}$ je uzavřený interval)

(d) všechny zleva otevřené a zprava uzavřené intervaly

(e) všechny intervaly obsahující 0

(f) všechny intevaly obsahující 1.

6) Nechť $A \neq \emptyset$. Dokažte, že

(a) Množina všech reflexivních relací na A tvoří uzávěrový systém (na množině $A \times A$). Určete uzávěr prázdné relace!

(b) Ukažte, že v předchozím uzávěrovém systému reflexivních relací je uzávěr relace R roven $[R]=R \cup \omega_A$.

(c) Ukažte, že množina všech symetrických relací tvoří uzávěrový systém na $A \times A$. Dokažte, že v tomto systému je $[R]=R \cup R^{-1}$.

(d) Ukažte, že množina všech tranzitivních relací na A tvoří uzávěrový systém na $A \times A$. V tomto uzávěrovém systému platí

$$[R]=R \cup (R \circ R) \cup (R \circ R \circ R) \cup \ldots .$$

Označme $R^t=[R]$ a nazveme <u>tranzitivní uzávěr</u> relace R.

(e) Dokažte, že množina všech ekvivalencí na A tvoří uzávěrový systém na $A \times A$. Dokažte, že v tomto systému platí

$$[R]=(R \cup R^{-1} \cup \omega)^t.$$

Je-li $R=\{\langle a,b\rangle\}$, jaký je uzávěr $[R]$ (t.j. nejmenší ekvivalence na A obsahující dvojici $\langle a,b\rangle$)?

(7) Ukažte, že množina všech relací uspořádání na A netvoří uzávěrový systém na $A \times A$.

(8) Nechť $\le$ je uspořádání na $A \neq \emptyset$. Dokažte, že množina všech

uspořádání $R \subseteq \leq$ tvoří uzávěrový systém na množině $\leq$ (zřejmě ω je nejmenší a $\leq$ je největší prvek tohoto uzávěrového systému)

(9) Nechť $\leq$ je uspořádání na $A \neq \emptyset$. Označme pro $B \subseteq A$ symbolem $L(B)=\{x \in A;\ x \leq b$ pro každé $b \in B\}$, $U(B)=\{x \in A;\ b \leq x$ pro každé $b \in B\}$. Položme $L(\emptyset)=A=U(\emptyset)$.

(a) Dokažte, že $\{L(B); B \subseteq A\}$ tvoří uzávěrový systém, kde $[X]=L(U(X))$;

(b) Dokažte, že $\{U(B); B \subseteq A\}$ tvoří uzávěrový systém, v němž $[X]=U(L(X))$.

(10) Nechť $(G,\cdot)$ je grupoid. Dokažte, že množina všech jeho podgrupoidů spolu s $\emptyset$ tvoří uzávěrový systém. Označme $[X]$ uzávěr podmnožiny $X \subseteq G$. Zaveďme relaci Q takto:

$$\langle A,B \rangle \in Q \iff [A]=[B].$$

Dokažte, že Q je kvaziuspořádání na $ExpG$.

Zadejte příklad grupoidu $(G,\cdot)$ takový, aby

(a) Q nebylo uspořádání

(b) Q bylo uspořádání.

(11) Je-li $\mathcal{M}$ uzávěrový systém na $A \neq \emptyset$, pak relace R na $ExpA$ daná předpisem

$$\langle C,D \rangle \in R \iff [C]=[D]$$

je kvaziuspořádání na $ExpA$. Ukažte příklady, kdy R není uspořádání, a kdy R je uspořádání.

(12) Nechť $(G,\cdot)$ je grupoid, $a,b \in G$.

(a) Tvoří množina všech podgrupoidů obsahujících prvek a uzávěrový systém v G?

(b) Tvoří množina všech podgrupoidů neobsahujících b spolu s $\emptyset$ uzávěrový systém v G?

(c) Množina podgrupoidů neobsahujících b spolu s $\emptyset$ a G?

(13) Dokažte, že množina všech podgrup dané grupy tvoří uzávěrový systém.

(14) Dokažte, že množina všech normálních podgrup tvoří uzávěrový systém.

Návody k řešení:

1) Je-li $\mathcal{N} \subseteq Exp A$, pak $\cap \mathcal{N}$ je opět podmnožina v A, t.j. $\cap \mathcal{N} \in Exp A$, tedy $Exp A$ je uzávěrový systém. Jelikož dle definice je pro uzávěrový systém $\mathcal{M}$ na A také $\mathcal{M} \subseteq Exp A$, je $Exp A$ největší uzávěrový systém na A.
Dále, průnik neprázdného podsystému systému $\{A\}$ roven A, ale průnik prázdného systému podmnožin A je také roven A, tedy $\{A\}$ je uzávěrový systém .
Jelikož pro každý uzávěrový systém $\mathcal{M}$ na A platí $A \in \mathcal{M}$, t.j. $\{A\} \subseteq \mathcal{M}$, je $\{A\}$ nejmenší uzávěrový systém na A.

2) Netvoří, neboť $A \notin \mathcal{Y}$ (A je nekonečná).
Avšak $\mathcal{Y} \cup \{A\}$ již uzávěrový systém tvoří.

3) **(a)** ano, **(b)** ano, **(c)** ne, **(d)** ne.

5) **(a)** ano
(b) ne, interval $(-\infty,\infty)$ není konečné délky
(c) ne, interval $\bigcap_{n \in \mathbb{N}} \{(a-\frac{1}{n}, a+\frac{1}{n})\} = \{a\}$ není otevřený
(d) ne, $(-\infty,\infty)$ nesplňuje
(e) ano
(f) ano

6) Uzávěr prázdné relace je ω_A.

7) $A \times A$ není uspořádání na A.

9) **(a)** Platí:

$$\cap\{L(B_\alpha); \alpha \in \Gamma\} = L(\cup\{B_\alpha; \alpha \in \Gamma\}), \quad L(\emptyset) = A.$$

Zřejmě $L(U(X)) \supseteq X$ (ověřte!).
Buď $Z \subseteq A$ taková že $L(Z) \supseteq X$. Pak $U(L(Z)) \subseteq U(X)$ (ukažte!) a $L(Z) = L(U(L(Z))) \supseteq L(U(X))$, tedy $L(U(X))$ je nejmenší množina ze systému obsahující X. Ukažte, že $L(U(L(Z))) = L(Z)$.
(b) podobně jako (a).

10) **(a)** Zvolme $G = (\mathbb{Z}, +)$; pak $[1] = [-1] = \mathbb{Z}$.
(b) Např. jednoprvkový grupoid nebo grupoid, v němž

výsledek operace je roven vždy pevně zvolenému prvku.

(11) Zvolíme-li zadání z příkladu 9(a), pak pro množinu A platí:

$LU(\{a,b\})=LU(\{a,c\})=LU(\{b,c\})=LU(A)=A.$

Zvolíme-li A dle obrázku:

pak $LU(\{a,b\})=LU(b)=L(b)$.

Tedy A nesmí obsahovat řetězec ani antiřetězec s alespoň třemi prvky. Je-li tedy Q uspořádání, pak nutně A je jednoprvková.

(12)(a) ano

(b) ne

(c) ano.

6. GRUPOIDY

Nechť $A\neq\emptyset$. Zobrazení $f:A\times A\longrightarrow A$ se nazývá <u>binární operace množině A</u>. Místo $f(a,b)$ budeme binární operaci na A často značovat jen symbolem $\cdot$, t.j. $a\cdot b$, někdy také $a\circ b$ nebo $a+b$.

<u>Grupoidem</u> nazveme dvojici $(A,\cdot)$, kde $\cdot$ je binární operace množině A.

Je-li $\mathcal{G}=(A,\cdot)$ grupoid a $\emptyset\neq B\subseteq A$, pak B nazveme <u>podgrupoidem</u> grupoidu $\mathcal{G}$, jestliže pro každé $a,b\in B$ platí $a\cdot b\in B$; podgrupoid B budeme také označovat $(B,\cdot)$, neboť je sám grupoidem.

Jsou-li $(A,\cdot),(B,\circ)$ dva grupoidy, pak na kartézském součinu $A\times B$ lze zavést binární operaci $\odot$ takto: $\langle a,b\rangle,\langle c,d\rangle\in A\times B$, pak

$$\langle a,b\rangle\odot\langle c,d\rangle=\langle a\cdot c,b\circ d\rangle.$$

Dvojici $(A\times B,\odot)$, která je zřejmě grupoid, nazveme <u>direktní součin grupoidů</u> $(A,\cdot),(B,\circ)$ a označíme $(A,\cdot)\times(B,\circ)$; je-li zřejmé, jak jsou operace $\cdot,\circ$ definovány, řekneme stručně, že $A\times B$ je direktní součin grupoidů A,B.

Zobrazení $h:A\longrightarrow B$ je <u>homomorfismus</u> grupoidu $(A,\cdot)$ do $(B,\circ)$, jestliže pro každé $a,b\in A$ platí

$$h(a\cdot b)=h(a)\circ h(b).$$

Je-li homomorfismus h bijektivní, nazývá se <u>izomorfismus</u>.

Nechť $(A,\cdot)$ je grupoid, E je ekvivalence na množině A. Nazveme <u>kongruence</u> grupoidu $(A,\cdot)$, jestliže pro každé $\langle a,b\rangle,\langle c,d\rangle\in E$ platí také

$$\langle a\cdot c,b\cdot d\rangle\in E,$$

což nazýváme tzv. <u>substituční podmínkou</u>.

Grupoid $(G,\cdot)$ je <u>komutativní</u>, jestliže pro každé $a,b\in G$ platí:

$$a\cdot b=b\cdot a;$$

je <u>idempotentní</u>, jestliže pro každé $a\in G$ platí $a\cdot a=a$.

Prvek e (resp. n) grupoidu G se nazývá <u>jednotka</u> (resp. <u>nula</u>), jestliže pro každé $a\in G$ platí $a\cdot e=e\cdot a=a$ (resp. $a\cdot n=n\cdot a=n$).

Nechť $\mathbb{N}$ resp. $\mathbb{Z}$ označuje množinu přirozených resp. celých čísel.

Příklady:

(1)(a) Ukažte, že $(\mathbb{N},\cdot)$ resp. $(\mathbb{N},+)$ jsou grupoidy.

(b) Ukažte, že $(\mathbb{N},-)$ není grupoid, ale $(\mathbb{Z},-)$ je grupoid. Má $(\mathbb{Z},-)$ nulu resp. jednotku?

(c) Ukažte, že $(\mathbb{Z},+),(\mathbb{R},+),(\mathbb{Q},+),(\mathbb{C},+)$ resp. $(\mathbb{Z},\cdot),(\mathbb{R},\cdot),(\mathbb{Q},\cdot),(\mathbb{C},\cdot)$ jsou grupoidy (kde $\mathbb{Z}$ resp. $\mathbb{Q}$ resp. $\mathbb{R}$ resp. $\mathbb{C}$ označuje množinu všech čísel celých resp. racionálních resp. reálných resp. komplexních, $\cdot$ je násobení a $+$ je sčítání čísel). Který z těchto grupoidů je podgrupoidem dalšího z nich?

(d) Ukažte, že na množině $\mathbb{Z}$ je binární operací $\max(a,b)$; je grupoid $(\mathbb{Z};\max)$ komutativní resp. idempotentní? Má tento grupoid nulu resp. jednotku? Analogicky popište grupoid $(\mathbb{Z},\min)$, kde operace je $\min(a,b)$.

(2) Nechť $A\neq\emptyset$. Jaké vlastnosti mají grupoidy $(ExpA;\cap),(ExpA,\cup)$?

(3) Nechť B je podgrupoid grupoidu $(A,\cdot)$ a nechť C je podgrupoidem grupoidu B. Dokažte, že také C je podgrupoidem grupoidu $(A,\cdot)$.

(4) Dokažte, že množina všech komplexních jednotek tvoří podgrupoid multiplikativního grupoidu $(\mathbb{C},\cdot)$ všech komplexních čísel. Má tento podgrupoid jednotku?

(5) Každý idempotentní grupoid, který má nejvýše dva prvky, je asociativní. Dokažte!

(6) Ukažte příklad grupoidu, ve kterém průnik podgrupoidů může být $\emptyset$.

(7) Určete všechny možné dvouprvkové grupoidy. Které z nich jsou

(a) komutativní

(b) asociativní

(c) idempotentní

(d) mají nulu

(e) mají jednotku

(f) mají nulu i jednotku?

(8) Nechť $(G,\cdot)$ je grupoid, ve kterém platí $x\cdot y=y$ pro každé x,y (resp. $x\cdot y=x$). Tento grupoid se nazývá grupoidem <u>pravých n</u>

(resp. levých nul). Dokažte:

(a) tento grupoid je idempotentní a asociativní;

(b) každá podmnožina $\emptyset \neq A \subseteq G$ je podgrupoid grupoidu $(G,\cdot)$;

(c) každá ekvivalence na G je kongruence na $(G,\cdot)$.

9) Nechť $(A,\cdot)$ resp. $(B,\cdot)$ je grupoid levých resp. pravých nul (viz příklad **(8)**). Jak je definována operace na direktním součinu $(A,\cdot)\times(B,\cdot)$?

10) Nechť grupoid $(G,\cdot)$ má nulu 0 a jednotku 1. Ukažte, že direktní součin $(G,\cdot)\times(G,\cdot)$ má alespoň 4 idempotentní prvky.

11) Nechť $(\mathbb{N},+)$ je grupoid všech přirozených čísel vzhledem ke sčítání. Dokažte, že množina $\{1\}$ generuje $(\mathbb{N},+)$. Určete podgrupoid generovaný množinou:

(a) $\{2,3\}$

(b) $\{3,4\}$.

12) Je grupoid $(\mathbb{Z},-)$ generovaný některou z následujících množin?

(a) $\{-1\}$

(b) $\{1\}$.

13) Nechť $(G,\cdot)$ je n-prvkový grupoid, jehož tabulka je

	a_1	a_2	.	.	.	.	a_n
a_1	a_1	a_1	.	.	.	.	a_1
a_2	a_1	a_1	.	.	.	.	a_1
.	.	.					.
.	.	.					.
.	.	.					.
a_n	a_1	a_1	.	.	.	.	a_1

Dokažte, že každá ekvivalence na G je kongruence $(G,\cdot)$. Určete všechny podgrupoidy grupoidu G!

14) Dokažte, že homomorfní obraz idempotentního prvku je idempotentní prvek.

15) Nechť $(\mathbb{R},\cdot)$ je multiplikativní grupoid všech reálných čísel. Dokažte, že zobrazení $h:\mathbb{R}\longrightarrow\mathbb{R}$ dané předpisem $h(x)=|x|$ je homomorfismus $(\mathbb{R},\cdot)$ do $(\mathbb{R},\cdot)$.

16) Nechť $(\mathbb{R}_+,\cdot)$ je multiplikativní grupoid všech kladných

reálných čísel. Dokažte, že zobrazení $h:\mathbb{R}_+\longrightarrow\mathbb{R}$, dané předpisem $h(x)=\log x$, je surjektivní homomorfismus grupoidu $(\mathbb{R}_+,\cdot)$ na grupoid $(\mathbb{R},+)$. Dokažte, že h je izomorfismus.

(17) Nechť $(\mathbb{C},\cdot)$ je multiplikativní grupoid všech komplexních čísel. Dokažte, že zobrazení $h:\mathbb{C}\longrightarrow\mathbb{R}$, dané předpisem $h(x)=|x|$, je surjektivní homomorfismus $(\mathbb{C}\setminus\{0\},\cdot)$ na $(\mathbb{R}_+,\cdot)$.

(18) Nechť $(\mathbb{C},+)$ je aditivní grupoid všech komplexních čísel. Dokažte, že zobrazení $h:\mathbb{C}\longrightarrow\mathbb{R}$, dané předpisem $h(a+ib)=a$, je surjektivní homomorfismus $(\mathbb{C},+)$ na $(\mathbb{R},+)$.

(19) Nechť Θ je ekvivalence na $\mathbb{N}$ daná rozkladem $\{1\},\{2\},\{3\},\{4,5,6,\dots\}$. Dokažte, že Θ je kongruence na $(\mathbb{N},+)$ a určete faktorový grupoid $(\mathbb{N},+)/\Theta$.

(a) Kolik má $(\mathbb{N},+)/\Theta$ prvků?

(b) Určete všechny podgrupoidy $(\mathbb{N},+)/\Theta$.

(20) Nechť Θ je na $\mathbb{N}$ definovaná stejně jako v příkladu **(19)**. Ukažte, že Θ je kongruence na $(\mathbb{N},\cdot)$ a určete $(\mathbb{N},\cdot)/\Theta$.

(21) Nechť $\mathbb{N}$ je množina přirozených čísel a $\circ$ je binární operace na $\mathbb{N}$ daná předpisem $n\circ m=n^m$. Nechť S resp. L je množina všech kladných sudých, resp. lichých čísel. Ukažte, že množiny S,L tvoří rozklad $\mathbb{N}$ a příslušná ekvivalence je kongruencí na $(\mathbb{N},\circ)$. Určete faktorový grupoid grupoidu $(\mathbb{N},\circ)$ dle této ekvivalence!

Návody k řešení, výsledky:

(1)(b) $(\mathbb{N},-)$ není grupoid, neboť pro $a,b\in\mathbb{N}, a<b$ totiž $a-b\notin\mathbb{N}$. Grupoid $(\mathbb{Z},-)$ nemá nulu ani jednotku (platí pro každé $a\in\mathbb{Z}$ $a-0=a$, avšak $0-a\neq a$ pro $a\neq 0$).

(d) Operace max i operace min jsou komutativní a idempotentní. Grupoidy $(\mathbb{Z},\max)$, $(\mathbb{Z},\min)$ nemají nulu ani jednotku.

(2) Oba grupoidy jsou komutativní a idempotentní. Nulou grupoidu $(Exp\,A;\cap)$ je $\emptyset$, jednotkou je A. Nulou grupoidu $(Exp\,A;\cup)$ je A, jednotkou je $\emptyset$.

(4) Komplexní jednotkou je komplexní číslo $z=a+ib$ takové, že

$|z|=1$. Jsou-li z,v dvě komplexní jednotky, pak $|z\cdot v|=|z|\cdot|v|=1\cdot 1=1$, je tedy $z\cdot v$ opět komplexní jednotka, tedy tyto prvky tvoří podgrupoid $(\mathbb{C},\cdot)$. Zřejmě číslo 1 je jednotkou tohoto podgrupoidu.

Je-li $(G,\cdot)$ jednoprvkový, je důkaz triviální. Nechť tedy $G=\{a,b\}$. Jelikož je idempotentní, je jeho tabulka

	a	b
a	a	x
b	y	b

kde $x,y\in\{a,b\}$. Vyzkoušejte všechny 4 možnosti!

Např. v idempotentním, aspoň dvouprvkovém grupoidu platí: $a^2=a$, $b^2=b$, $\{a\},\{b\}$ jsou podgrupoidy, $\{a\}\cap\{b\}=\emptyset$.

Jsou to grupoidy:

(a)

	a	b
a	a	a
b	a	a

(b)

	a	b
a	a	a
b	a	b

(c)

	a	b
a	a	b
b	a	a

(d)

	a	b
a	b	a
b	a	a

(e)

	a	b
a	a	a
b	b	a

(f)

	a	b
a	a	a
b	b	b

(g)

	a	b
a	b	b
b	a	a

(h)

	a	b
a	b	a
b	a	b

(i)

	a	b
a	a	b
b	a	b

(j)

	a	b
a	b	a
b	b	a

Z nich jsou idempotentní:(b), (f), (i)
komutativní:(a),(b),(d),(h)
mají nulu: (a),(b)
mají jednotku: (h),(b).

) Zřejmě $\langle a,b\rangle\circ\langle c,d\rangle=\langle a,d\rangle$.

) Jsou to prvky $\langle 0,0\rangle,\langle 0,1\rangle,\langle 1,0\rangle,\langle 1,1\rangle$.

1) Jelikož pro každé $n\in\mathbb{N}$ platí $n=(\ldots(1+1)+1)+\ldots)+1$ (n sčítanců), tedy $\{1\}$ generuje $(\mathbb{N},+)$.

(a) $\{2,3\}$ generuje podgrupoid $(A,+)$, kde

$$A=\{2,3,4,5,\ldots\}=\mathbb{N}\setminus\{1\}$$

(b) $\{3,4\}$ generuje $(B,+)$, kde $B=\mathbb{N}\setminus\{1,2,5\}$.

(12)(a) Ano, **(b)** Ano.

(13) Každá podmnožina G obsahující prvek a_1 je podgrupoidem grupoidu $(G,\cdot)$.

(19) Faktorový grupoid:

	{1}	{2}	{3}	{4,5,...}
{1}	{2}	{3}	{4,5,...}	{4,5,...}
{2}	{3}	{4,5,...}	{4,5,...}	{4,5,...}
{3}	{4,5,...}	{4,5,...}	{4,5,...}	{4,5,...}
{4,5,...}	{4,5,...}	{4,5,...}	{4,5,...}	{4,5,...}

(a) 4

(b) Jsou 2, a to celý faktorový grupoid $(\mathbb{N},+)/\Theta$ a jednoprvkový {4,5...}.

(20) Faktorový grupoid:

	{1}	{2}	{3}	{4,5,...}
{1}	{1}	{2}	{3}	{4,5,...}
{2}	{2}	{4,5,...}	{4,5,...}	{4,5,...}
{3}	{3}	{4,5,...}	{4,5,...}	{4,5,...}
{4,5,..}	{4,5,...}	{4,5,...}	{4,5,...}	{4,5,...}

(21) Faktorový grupoid:

$\circ$	S	L
S	S	S
L	L	L

7. POLOGRUPY

Grupoid $\mathcal{G}=(A,\cdot)$ se nazývá <u>pologrupa</u>, platí-li pro jeho prvky sociativní zákon, t.j. pro každé $a,b,c\in A$ platí $a\cdot(b\cdot c)=(a\cdot b)\cdot c$.

Nechť $(A,\cdot)$ je pologrupa. Prvek $a\in A$ se nazývá <u>idempotentní</u>, platí-li $a\cdot a=a$. Prvek $b\in A$ se nazývá <u>levá</u> (resp. <u>pravá</u>) <u>nula</u>, platí-li $b\cdot a=b$ (resp. $a\cdot b=b$) pro každé $a\in A$. Pologrupa $(A,\cdot)$ se nazývá <u>pologrupa levých nul</u> (resp. <u>pologrupa pravých nul</u>), je-li každý její prvek levou (resp. pravou) nulou.

Pologrupa $(A,\cdot)$ se nazývá <u>pologrupa s krácením zprava</u> (<u>zleva</u>), platí-li pro každé $a,b,c\in A$

$$a\cdot c=b\cdot c \Longrightarrow a=b$$

(resp. $c\cdot a=c\cdot b \Longrightarrow a=b$).

$(A,\cdot)$ se nazývá <u>pologrupa s krácením</u>, je-li pologrupou s krácením zleva i zprava.

<u>Příklady</u>:

(1) Množina všech binárních relací na množině A tvoří pologrupu vzhledem k relačnímu součinu. Dokažte!

(2) Množina všech zobrazení množiny $A\neq\emptyset$ do sebe tvoří pologrupu (vzhledem ke skládání zobrazení). Dokažte!

(3) Nechť $\mathbb{R}$ je množina všech reálných čísel. Dokažte, že $(\mathbb{R},\max)$ a $(\mathbb{R},\min)$ jsou pologrupy.

(4) Nechť $(G,\cdot)$ je grupoid. Množina všech homomorfismů $(G,\cdot)$ do $(G,\cdot)$ tvoří pologrupu. Množina všech surjektivních (injektivních) homomorfismů $(G,\cdot)$ na (do) $(G,\cdot)$ tvoří pologrupu. Množina všech izomorfismů $(G,\cdot)$ na $(G,\cdot)$ tvoří pologrupu (je to dokonce grupa). Dokažte!

(5) Nechť $A\neq\emptyset$. Pak $(Exp A,\cap),(Exp A,\cup)$ jsou komutativní a idempotentní pologrupy. Dokažte!

(6) Je $(\mathbb{R},-)$ (operace odčítání reálných čísel) pologrupa?

(7) Nechť $(A,\cdot)$ je pologrupa, $(B,\cdot)$ grupoid. Dokažte:

(a) každý podgrupoid grupoidu $(A,\cdot)$ je pologrupa;

(b) direktní součin $(A,\cdot)\times(A,\cdot)$ je pologrupa;

(c) je-li h homomorfismus $(A,\cdot)$ do $(B,\cdot)$, pak $h(A)$ je podgrupoid v $(B,\cdot)$, který je pologrupou.

Zadejte příklad pologrupy $(A,\cdot)$, grupoidu $(B,\cdot)$ a zobrazení $h: A \longrightarrow B$ tak, aby h byl homomorfismus, avšak $(B,\cdot)$ nebyla pologrupa.

(8) Nechť $(G,\cdot)$ je grupoid, $g \in G$. Definujme $g^1=g$, $g^n=g\cdot g^{n-1}$ pro $n \geq 2$.

(a) Dokažte, že množina $\{g, g^2, g^3, \ldots\}$ tvoří podgrupoid $(G,\cdot)$, který je pologrupou.

(b) Je-li množina $\{g, g^2, g^3, \ldots\}$ konečná, pak obsahuje cyklickou grupu.

(9) Nechť $\mathbb{Z}$ je množina všech celých čísel, n pevně určené přirozené číslo. Položme pro $x, y \in \mathbb{Z}$

$$\langle x, y\rangle \in \Theta_n$$

jestliže n dělí $x-y$.

Říkáme, že relace Θ_n je <u>kongruence modulo n</u>, často zapisujeme $x \equiv y \pmod{n}$.

(a) Dokažte, že Θ_n je ekvivalence na $\mathbb{Z}$,

(b) Dokažte, že Θ_n je kongruence na $(\mathbb{Z},+)$,

(c) Dokažte, že Θ_n je kongruence na $(\mathbb{Z},\cdot)$,

(d) Pro $n=6$ určete $(\mathbb{Z},\cdot)/\Theta_6$.

Faktorovou pologrupu $(\mathbb{Z},+)/\Theta_n$ resp $(\mathbb{Z},\cdot)/\Theta_n$ budeme označovat $(\mathbb{Z}_n,+), (\mathbb{Z}_n,\cdot)$, a nazývat <u>aditivní</u> resp. <u>multiplikativní pologrupa zbytkových tříd mod n</u>.

(e) Určete všechny podpologrupy v $(\mathbb{Z}_6,\cdot)$,

(f) Určete všechny idempotentní prvky v $(\mathbb{Z}_6,\cdot)$,

(g) Určete podpologrupu pologrupy $(\mathbb{Z}_6,\cdot)$ generovanou množinou $\{\bar{2}\}, \{\bar{3}\}, \{\bar{4}\}, \{\bar{5}\}$,

(h) Dokažte, že ekvivalence E, daná na $\mathbb{Z}_6$ rozkladem $\{\bar{0}, \bar{2}, \bar{3}, \bar{4}\}$, $\{\bar{1}, \bar{5}\}$, je kongruence na $(\mathbb{Z}_6,\cdot)$ a určete faktorovou pologrupu $(\mathbb{Z}_6,\cdot)/E$.

(10) Analogicky zkoumejte podpologrupy a kongruence na $(\mathbb{Z}_3,\cdot)$, $(\mathbb{Z}_4,\cdot)$, $(\mathbb{Z}_3,+)$, $(\mathbb{Z}_4,+)$, $(\mathbb{Z}_6,+)$.

(11) Nechť $(S,\cdot)$ je pologrupa, $\emptyset \neq A \subseteq S$. Dokažte, že podpologrupa pologrupy $(S,\cdot)$ generovaná množinou A je množinou všech prvků tvaru $x=a_1\cdot\ldots\cdot a_n$, kde $n \in \mathbb{N}$ a $a_i \in A$.

(12) Nechť $X \neq \emptyset$, nechť $\lambda \notin X$. Zaveďme operaci zřetězení (neboli

konkatenace) takto: pro $x_1, x_2 \in X$ položme $x_1 \cdot x_2 = x_1 x_2$ (píšeme prostě symboly za sebe), dále položme pro $x \in X$:

$$x \cdot \lambda = x, \quad \lambda \cdot x = x.$$

Pak $(X \cup \{\lambda\}, \cdot)$ je pologrupa s jednotkou λ, tedy monoid. Je to tzv. volný monoid generovaný množinou X. Jeho prvky jsou všechny konečné posloupnosti symbolů z X, t.j. tvaru $x_1 x_2 \ldots x_n$. Množina prvků z X se nazývá abeceda, prvky volného monoidu se nazývají slova nad abecedou X, symbol λ se nazývá prázdné slovo. Každý faktorový monoid volného monoidu se nazývá syntaktický monoid. Používá se v teorii formálních jazyků.

) Nechť $(S, \cdot)$ je pologrupa, a nechť F je množina všech zobrazení $S \longrightarrow S$. Pro každé $a \in S$ definujme $f_a \in F$ předpisem

$$f_a(x) = x \cdot a$$

(tzv. translace). Zřejmě $(F, \circ)$ je pologrupa vzhledem k skládání zobrazení. Dokažte, že zobrazení $\varphi: S \longrightarrow F$, dané předpisem

$$\varphi(a) = f_a,$$

je homomorfismus pologrupy $(S, \cdot)$ do $(F, \circ)$.

) Dokažte, že pologrupa levých (pravých) nul je skutečně pologrupou.

) Nechť $(S, \cdot)$ je pologrupa, a nechť S nemá jednotku. Nechť 1 je nějaký prvek , $1 \notin S$. Definujme: $s \cdot 1 = 1 \cdot s = s$ pro každé $s \in S$. Pak $(S \cup \{1\}, \cdot)$ je zřejmě opět pologrupou; označme ji S^1. Dokažte:

a) 1 je jednotka v S^1,

b) Je-li S pologrupa s krácením, je i S^1 pologrupa s krácením,

c) Je-li S pologrupa levých nul, $|S| > 1$, pak S je pologrupa s krácením zprava ale S^1 již tuto vlastnost nemá.

) Nechť $(S, \cdot)$ je pologrupa splňující $a \cdot b = c \cdot d \Longrightarrow a = c$ nebo $b = d$. Pak $(S, \cdot)$ je pologrupa levých nul nebo pologrupa pravých nul. Dokažte!

) Je-li množina všech pravých (resp. levých) nul pologrupy $(S, \cdot)$ neprázdná, je podpologrupou. Dokažte!

) Nechť $(F, \cdot)$ je pologrupa všech zobrazení $X \longrightarrow X$. Předpokládejme $|X| > 1$. Dokažte, že pravé nuly jsou právě všechna konstantní zobrazení (t.j. zobrazení splňující $f(x) = a$ pro každé $x \in X$, kde a je pevně zvolený prvek z X).

(19) Nechť $(F,\cdot)$ je pologrupa z příkladu **(18)**. Je-li $h\in F$ idempotent (t.j. $h\cdot h(x)=h(x)$), pak restrikce h na podmnožinu $h(X)=\{h(x);x\in X\}$ je identické zobrazení. Dokažte! Formulujte a dokažte obrácené tvrzení!

(20) Nechť $(S,\cdot)$ je pologrupa. Položme pro pevně zvolené $a\in S$ $A=\{x;\ a\cdot x\cdot a=a\}$. Je-li $A\neq\emptyset$, pak $A\cdot a=\{y\cdot a;\ y\in A\}$ je podpologrupa pologrupy $(S,\cdot)$, která je pologrupou levých nul. Dokažte!

<u>Návody k řešení:</u>

(6) Není.

(7)(c): Např.

B:

$\cdot$	a	b	c
a	a	c	c
b	b	c	b
c	c	b	a

Pak $a\cdot a=a$, t.j. a je idempotent. Avšak $(B,\cdot)$ není pologrupa, neboť $a\cdot(b\cdot c)=a\cdot b=c\neq a=c\cdot c=(a\cdot b)\cdot c$.

Nechť $(A,\cdot)$ je libovolná pologrupa a $h:A\longrightarrow B$ je dáno předpisem $h(x)=a$ pro každé $x\in A$. Pak h je homomorfismus (ověřte!), $h(A)=\{a\}$ je pologrupa v $(B,\cdot)$.

(8)(b) Je-li $H=\{g,g^2,g^3,\dots\}$ konečná, pak existují $m,k\in\mathbb{N}$ takové, že $m>k$ a $g^m=g^k$. Nechť m,k jsou nejmenší přirozená čísla této vlastnosti. Pak $r=m-k$ je opět přirozené číslo. Množina prvků

$$H=\{g^k,g^{k+1},\dots,g^{k+r-1}\}$$

tvoří cyklickou grupu. Jednotkou je prvek g^t, kde $t=s\cdot r$ přičemž s je nejmenší přirozené číslo takové, že $s\cdot r\in\{k,k+1,\dots,k+r-1\}$, (pak $g^x\cdot g^t=g^{x+t}=g^{x+s\cdot r}=g^x$). Inverzní prvek k prvku g^x je prvek g^{t-x} pro $t-x>0$, pro $t-x<0$ je to prvek g^{t+r-x}.

(d) Označme $\overline{k}$ třídu $\mathbb{Z}$ dle Θ_n, obsahující číslo k.

$(\mathbb{Z}_6,+)$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$(\mathbb{Z}_6,\cdot)$:

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

(e) podpologrupy jsou
$\{\overline{0}\},\{\overline{1}\},\{\overline{3}\},\{\overline{4}\},\{\overline{0},\overline{1}\},\{\overline{0},\overline{3}\},\{0,4\},\{\overline{1},\overline{5}\},\{\overline{1},\overline{4}\},\{\overline{1},\overline{3}\},\{\overline{2},\overline{4}\},$
$\{\overline{0},\overline{2},\overline{4}\},\{\overline{1},\overline{2},\overline{4}\},\{\overline{0},\overline{1},\overline{3}\},\{\overline{0},\overline{1},\overline{4}\},\{\overline{1},\overline{3},\overline{5}\},\{\overline{0},\overline{1},\overline{5}\},$
$\{\overline{0},\overline{2},\overline{3},\overline{4}\},\{\overline{1},\overline{2},\overline{4},\overline{5}\},\{\overline{0},\overline{1},\overline{2},\overline{4}\},\{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\},(\mathbb{Z}_6,\cdot)$.

(f) $\overline{0},\overline{1},\overline{3},\overline{4}$

(g) $\{\overline{2}\}$ generuje $\{\overline{2},\overline{4}\}$
$\{\overline{3}\}$ " $\{\overline{3}\}$
$\{\overline{4}\}$ " $\{\overline{4}\}$
$\{\overline{5}\}$ " $\{\overline{1},\overline{5}\}$

(h) $(\mathbb{Z}_6,\cdot)/E$ je

	$\{\overline{0},\overline{2},\overline{3},\overline{4}\}$	$\{\overline{1},\overline{5}\}$
$\{\overline{0},\overline{2},\overline{3},\overline{4}\}$	$\{\overline{0},\overline{2},\overline{3},\overline{4}\}$	$\{\overline{0},\overline{2},\overline{3},\overline{4}\}$
$\{\overline{1},\overline{5}\}$	$\{\overline{0},\overline{2},\overline{3},\overline{4}\}$	$\{\overline{1},\overline{5}\}$

(i) Označme $[A]$ podpologrupu $(S,\cdot)$ generovanou množinou A. Zřejmě $A\subseteq[A]$ (volbou $n=1, x=a_1\in A$, tedy $x\in[A]\Longrightarrow A\subseteq[A]$). Jestliže $x,y\in[A]$, pak $x=a_1\cdot\ldots\cdot a_n$, $y=a'_1\cdot\ldots\cdot a'_m$, tedy

$x\cdot y=(a_1\cdot\ldots\cdot a_n)\cdot(a'_1\cdot\ldots\cdot a'_m)=a^*_1\cdot\ldots\cdot a^*_k$, kde $k=n+m\in\mathbb{N}$

a $a^*_i=a_i$ pro $i=1,\ldots,n$, $a^*_j=a'_{j-n}$ pro $j=n+1,\ldots,n+m$.

Opět $x\cdot y$ je předepsaného tvaru, t.j. $x\cdot y\in[A]$, tedy $[A]$ je grupoid. Ověření asociativního zákona v $[A]$ je jednoduché,

tedy $[A]$ je podpologrupa obsahující A. Je-li B podpologrupa obsahující A a $x=a_1\cdot\ldots\cdot a_n$ pro $a_i\in A$, zřejmě $x\in B$, tedy $[A]\subseteq B$, t.j. $[A]$ je nejmenší podpologrupa této vlastnosti (je tedy průnikem všech podpologrup obsahujících A), t.j. $[A]$ je generovaná množinou A.

(13) Nejprve ukážeme: pro $a,b\in S$ je

$f_a\circ f_b(x)=f_b(f_a(x))=f_b(x\cdot a)=(x\cdot a)\cdot b=x\cdot(a\cdot b)$,

tedy $f_a\circ f_b=f_{ab}$. Odtud je již zřejmé

$$\varphi(a\cdot b)=f_{ab}=f_a\circ f_b=\varphi(a)\circ\varphi(b).$$

(15)(b) Je-li $a\cdot x=a\cdot y$, pak pro $a,x,y\neq 1$ platí $x=y$, neboť S je pologrupa s krácením. Je-li $a=1$, pak $x=y$.

Předpokládejme sporem, že existují $a\neq 1$, $x=1, y\neq 1$ tak, že $a=a\cdot x=a\cdot y$. Pak $a\cdot y=a\cdot y\cdot y$, odkud $y=y\cdot y$. Je-li $b\in S$ libovolný prvek, pak $b\cdot y=b\cdot y\cdot y$. odkud $b=b\cdot y$. Podobně se dokáže $b=y\cdot b$, tedy y by byla jednotka v S, spor.

(c) Pro každé $z\in S$, $x\in S$ platí: $z\cdot x=z$. Je-li $z_1\cdot x=z_2\cdot x$, pak $z_1=z_2$. Dále: $1\cdot x=x=x\cdot x$, $x\neq 1$, tedy S^1 tuto vlastnost nemá.

(16) Nechť S není pologrupa pravých nul ani levých nul. Pak existují $a,b,c,d\in S$:

$a\cdot b\neq a$, $c\cdot d\neq d$ (a není levá nula, d není pravá nula).

Pak $(a\cdot b)\cdot(c\cdot d)=a\cdot(b\cdot c\cdot d)$.

Ale $a\cdot b\neq a$, tedy $c\cdot d=b\cdot(c\cdot d)$, $d\neq c\cdot d$, tedy $b=c$. Pak $a\cdot(b\cdot d)=(a\cdot b)\cdot d$, tedy $a\neq a\cdot b$, $b\cdot d=c\cdot d=d$, spor.

(17) Jsou-li a,b levé nuly, pak $a\cdot z=a$, $b\cdot z=b$ pro každé $z\in G$; $(a\cdot b)\cdot z=a\cdot(b\cdot z)=a\cdot b$ pro každé $z\in G$.

(18) Nechť f je konstantní zobrazení takové, že $f(x)=a$ pro každé $x\in X$. Pak $(g\cdot f)(x)=f(g(x))=a=f(x)$, tedy f je pravá nula.

Není-li f konstantní, pak existují $x_1,x_2,a,b\in X$:

$$f(x_1)=a,\ f(x_2)=b,\ a\neq b.$$

Volíme-li g tak, aby $g(x_1)=x_2$, $g(x_2)=x_1$, pak $f(g(x_1))=b\neq f(x_1)$, t.j. f není pravá nula.

(19) Pro každé $x\in h(X)$ je $x=h(y)$ pro $y\in X$, tedy $h(x)=h(h(y))=h(y)=x$. Je-li restrikce h na $h(X)$ identické zobrazení, pak h je zřejmě idempotentní.

(20) Nechť $z,v\in A\cdot a$, t.j. $z=y\cdot a$, $v=x\cdot a$ pro některé $x,y\in A$ (tedy $a\cdot x\cdot a=a$, $a\cdot y\cdot a=a$). Pak $z\cdot v=y\cdot a\cdot x\cdot a=y\cdot(a\cdot x\cdot a)=y\cdot a=z$.

Tedy pro $A\neq\emptyset$ je $A\cdot a$ vskutku pologrupa levých nul.

8. GRUPY

Pologrupa $(G,\cdot)$ se nazývá grupa, jestliže pro každé dva prvky $a,b\in G$ existují prvky $x,y\in G$ tak, že platí

$$a\cdot x=b \quad , \quad y\cdot a=b.$$

Je dokázat, že v každé grupě $(G,\cdot)$ existuje jednotka, označme ji e a pro každý prvek $a\in G$ existuje prvek $b\in G$ tak, že

$$a\cdot b=b\cdot a=e$$

Pro prvek b nazveme inverzní k prvku a, označme jej a^{-1}.

Na grupu lze také pohlížet jako na čtveřici

$$(G,\cdot,^{-1},e),$$

kde $G\neq\emptyset$ je množina, $\cdot$ je binární operace, $^{-1}$ je unární operace a e je nulární operace, přičemž platí pro každé $x,y,z\in G$ identity:

$$x\cdot(y\cdot z)=(x\cdot y)\cdot z$$

$$x\cdot e=e\cdot x=x$$

$$x\cdot x^{-1}=x^{-1}\cdot x=e.$$

Grupa $(G,\cdot)$ se nazývá abelovská, je-li operace $\cdot$ komutativní, tj. pro každé $x,y\in G$ platí

$$x\cdot y=y\cdot x.$$

Zapisujeme-li binární grupovou operaci symbolem $\cdot$, pak tomuto zápisu říkáme multiplikativní. V multiplikativní notaci často symbol operace vynecháváme, a místo $x\cdot y$ píšeme jen stručně xy.

Zapisujeme-li binární operaci grupy symbolem $+$, pak tomuto zápisu říkáme aditivní. V aditivní notaci označujeme jednotku grupy $(G,+)$ symbolem 0 a prvek inverzní k prvku $a\in G$ symbolem $-a$; říkáme, že $-a$ je prvek opačný k prvku a.

Příklady:

(1) Nechť $\mathbb{N}$ resp. $\mathbb{Z}$ resp. $\mathbb{R}$ resp. $\mathbb{C}$ označuje množinu všech čísel přirozených resp. celých resp. reálných resp. komplexních.

(a) Dokažte, že $(\mathbb{Z},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ jsou grupy.

(b) Dokažte, že ani $(\mathbb{N},+)$ ani $(\mathbb{N},\cdot)$ netvoří grupu.

(c) Dokažte, že $(\mathbb{Z},\cdot)$ není grupa, ani $(\mathbb{Z}-\{0\};\cdot)$ není grupa.

(d) Dokažte, že $(\mathbb{R}\setminus\{0\},\cdot)$, $(\mathbb{C}\setminus\{0\},\cdot)$ tvoří grupy.

(2) Dokažte, že množina všech bijekcí množiny $M\neq\emptyset$ na sebe tvoří

grupu.

(3) Dokažte, že množina všech translací (t.j. posunutí) v rovině tvoří grupu.

(4) Dokažte, že množina všech rotací (o témže středu otáčení) v rovině tvoří grupu.

(5) Dokažte, že množina všech zákrytových pohybů:

(a) rovnostranného trojúhelníka
(b) čtverce
(c) obdélníka
(d) krychle
(e) kvádru
(f) kruhu

tvoří grupu. Které z nich jsou nekonečné? Pro konečné určete jejich řády a Cayleyho tabulky.

(6) Dokažte, že je-li $(G,\cdot)$ grupa a $a,b\in G$, pak $(a\cdot b)^{-1}=b^{-1}\cdot a^{-1}$.

(7) Dokažte, že množina všech regulárních matic $n\times n$ nad tělesem reálných čísel tvoří grupu. Určete její jednotku a prvek inverzní k dané matici. Je tato grupa abelovská? Tvoří množina všech matic $n\times n$ nad $\mathbb{R}$ grupu?

(8) Nechť $M\neq\emptyset$ je množina. Označme symbolem A' komplement podmnožiny $A\subseteq M$ v množině M, t.j. $A'=M\setminus A$. Pro $A\subseteq M$, $B\subseteq M$ položme

$$A\oplus B=(A\cap B')\cup(A'\cap B).$$

Dokažte, že $(ExpA;\oplus)$ je grupa, určete její jednotku a prvek inverzní k $A\subseteq M$.

(9) Nechť $(G,\cdot)$ je grupa. Na G definujme binární operaci $\circ$ takto:

$$x\circ y=x\cdot x\cdot y\cdot y.$$

Ověřte, zda je $(G,\circ)$ pologrupa a ukažte, že $(G,\circ)$ je grupou právě tehdy, je-li G jednoprvková.

(10) Nechť $(G,\cdot)$ je konečná grupa. Dokažte, že v Cayleyho tabulce grupy $(G,\cdot)$ se každý prvek objeví právě jedenkrát v každém řádku a v každém sloupci. Tato vlastnost však ještě necharakterizuje grupu! Např. grupoid, daný tabulkou

$\cdot$	a	b	c	d	e
a	e	d	b	c	a
b	c	e	d	a	b
c	d	a	e	b	c
d	b	c	a	e	d
e	a	b	c	d	e

má výše uvedenou vlastnost (dokonce e je jeho jednotka a pro každý prvek existuje prvek inverzní), avšak není grupou. Proč?

) Nechť $\mathbb{Q}$ je množina všech čísel racionálních. Dokažte, že množina D všech čísel tvaru $a+b\sqrt{2}$ tvoří grupu vzhledem ke sčítání.

Dokažte, že množina $D\setminus\{0\}$ tvoří také grupu vzhledem k násobení (určete jednotku a prvek inverzní k prvku $a+b\sqrt{2}$)!

) Nechť $\mathbb{C}$ je množina všech čísel komplexních, nechť $f_i:\mathbb{C}\longrightarrow\mathbb{C}$ $(i=1,2,\ldots,6)$ jsou zobrazení daná předpisem:

$$f_1(v)=v \qquad f_4(v)=\frac{1-2v}{2}$$

$$f_2(v)=\frac{1}{2}-\frac{1}{2(1-2v)} \qquad f_5(v)=\frac{1}{2}-\frac{1}{4v}$$

$$f_3(v)=\frac{1}{4v} \qquad f_6(v)=\frac{1}{2(1-2v)}.$$

Dokažte, že $\{f_1,f_2,f_3,f_4,f_5,f_6\}$ tvoří grupu vzhledem k operaci skládání zobrazení.

) Nechť $(G,\cdot)$ je grupa. Definujme operaci $*$ na G předpisem: $a*b=b\cdot a$. Dokažte, že $(G,*)$ je opět grupa, a to izomorfní s $(G,\cdot)$. Určete tento izomorfismus!

) Určete všechny neizomorfní grupy řádu

(a) 2

(b) 3

(c) 4.

) Je-li grupa lichého (sudého) řádu, je počet prvků, které jsou samy k sobě inverzní, lichý (sudý). Dokažte!

) Nechť $(G,\cdot)$ je grupa, nechť $p\in G$. Zaveďme na G operaci $*$ takto:

$$x*y=x\cdot p^{-1}\cdot y.$$

Dokažte, že $(G,*)$ je opět grupa.

(17) Nechť $(G,\cdot)$ je tzv. <u>involutorní grupa</u>, t.j. pro každé $g\in G$ platí $g\cdot g=e$. Dokažte, že $(G,\cdot)$ je abelovská.

(18) Nechť $(G,\cdot)$ je grupa. Položme

$$\mathrm{Int}G=\{\varphi_a : G\longrightarrow G;\ \varphi_a(x)=a^{-1}\cdot x\cdot a\}.$$

Dokažte, že IntG je grupou (vzhledem ke skládání zobrazení). Je to tzv. <u>grupa vnitřních automorfismů grupy</u> $(G,\cdot)$.

(19) Nechť p je některé prvočíslo. Dokažte, že množina $Q_p=\{\frac{m}{p^n};\ m,n\in\mathbb{Z}\}$ tvoří grupu vzhledem ke sčítání! Je to tzv. <u>grupa p-adických čísel</u>. Ukažte, že pro $p\neq q$ je $Q_p\not\cong Q_q$.

(20) Nechť $\cdot$ označuje maticové násobení, $\mathbb{R}$ je množina reálných čísel. Dokažte, že množina všech matic ve tvaru $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$ pro $a^2+b^2\neq 0$ tvoří vzhledem k násobení matic grupu.

(21) Označme $(\mathbb{Q},+)$ grupu všech racionálních čísel vzhledem ke sčítání. Dokažte, že množina $\{\frac{1}{n};\ n\in\mathbb{N}\}$ generuje $(\mathbb{Q},+)$, a že $(\mathbb{Q},+)$ nemá konečný počet generátorů.

(22) Dokažte, že množina všech matic $n\mathrm{x}n$ nad reálnými čísly, jejichž determinant je roven 1, tvoří grupu (vzhledem k maticovému násobení).

(23) Nechť G je množina všech reálných čísel z polouzavřeného intervalu $\langle 0,1)$. Definujme na G operaci:

$$r_1\cdot r_2=\begin{cases} r_1+r_2 & \text{pro } r_1+r_2<1 \\ r_1+r_2-1 & \text{pro } r_1+r_2\geq 1. \end{cases}$$

Dokažte, že $(G,\cdot)$ je grupa.

(24) Nechť A je množina všech reálných čísel větších než 1. Definujme $a*b=a\cdot b-a-b+2$.
Dokažte, že $(A;*)$ je grupa.

<u>**Návody k řešení**</u>:

(3) Každá translace v rovině je popsána transformačními vztahy

$$T_1:\quad \begin{aligned} x'&=x+b_1 \\ y'&=y+b_2 \end{aligned},$$

kde $[x,y]$ jsou souřadnice vzoru, $[x',y']$ souřadnice obrazu a $[b_1,b_2]$ souřadnice vektoru posunutí. Je-li translace T_2 dána vztahy $x'=x+b_1'$

$y'=y+b'_2$, pak

$T_1 \circ T_2$ je dáno vztahy $x'=x+b_1+b'_1$

$y'=y+b_2+b'_2$, je tedy translací.

Translace T^*: $x'=x-b_1$

$y'=y-b_2$ je inverzní k translaci T_1.

Identické zobrazení je zřejmě jednotkou této grupy.

8) Nekonečná grupa je (f). Řády konečných grup jsou:
(a) 6, **(b)** 8, **(c)** 4, **(d)** 48.

9) Jednotkou je $\emptyset$, neboť $A \oplus \emptyset = \emptyset \oplus A = A$, inverzní prvek k A je opět prvek A, neboť $A \oplus A = \emptyset$.

10) Zřejmě operace $\circ$ není obecně asociativní, neboť platí
$x \cdot (y \cdot z) = x \cdot (y \cdot y \cdot z \cdot z) = x \cdot x \cdot y \cdot y \cdot z \cdot z \cdot y \cdot y \cdot z \cdot z$,
$(x \cdot y) \circ z = (x \cdot x \cdot y \cdot y) \circ z = x \cdot x \cdot y \cdot y \cdot x \cdot x \cdot y \cdot y \cdot z \cdot z$.
$(G, \circ)$ navíc nemusí mít jednotku: je-li např. $f \in G$ jednotkou v G, pak $x = x \circ f = x \cdot x \cdot f \cdot f$, což může platit pouze v případě $f=e$ (e jednotka $(G, \cdot)$) a $x \cdot x = x$. V grupě $(G, \cdot)$ však $x \cdot x = x$ platí jen pro $x=e$.

11) Uvedený grupoid není asociativní. Platí však, že má-li $(G, \cdot)$ splňující uvedenou vlastnost nejvýše 4 prvky, pak je grupou!

11) $(a+b\sqrt{2})+(c+d\sqrt{2})=(a+c)+(b+d)\sqrt{2}$, jednotkou je 0,

$-(a+b\sqrt{2})=(-a)+(-b)\sqrt{2}$,

$$(a+b\sqrt{2})^{-1}=\left(\frac{a}{a^2-2b^2}\right)+\left(\frac{-b}{a^2-2b^2}\right)\sqrt{2} \quad \text{pro } a \neq 0 \neq b.$$

12) Tabulka této grupy je:

	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

Přesvědčte se!

(13) Zobrazení $f: a \longrightarrow a^{-1}$ je hledaný izomorfismus.

(14)(a) Jediná, a to

	e	a
e	e	a
a	a	e

(b) jediná, a to

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

(c) jsou dvě, a to

	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

(15) Nechť G je grupa řádu k, nechť l je počet prvků, které jsou inverzní samy k sobě. Pak musí být počet prvků, které nejsou inverzní samy k sobě, vždy sudý (proč?), a tedy $k-l$ je vždy sudé číslo.
Je-li tedy k liché, musí být l liché,
k sudé, musí být l sudé.

(16) Jednotkou $(G,*)$ je prvek p, prvek inverzní k prvku x je prvek $px^{-1}p$.

(17) Nechť $a,b\in G$. Zřejmě $a\cdot a=e$, $b\cdot b=e$ implikují $a^{-1}=a$, $b^{-1}=b$. Jelikož také $(a\cdot b)\cdot(a\cdot b)=e$, platí $(a\cdot b)^{-1}=a\cdot b$. Avšak v grupě platí $(a\cdot b)^{-1}=b^{-1}\cdot a^{-1}$ (viz příklad (6)), a tedy $a\cdot b=a^{-1}\cdot b^{-1}=(b\cdot a)^{-1}=b\cdot a$.

(18) $\varphi_a(x)\circ\varphi_b(x)=\varphi_b(\varphi_a(x))=\varphi_b(a^{-1}xa)=b^{-1}a^{-1}xab=(ab)^{-1}xab=\varphi_{ab}(x)$.
Jednotkou je identické zobrazení $\varphi_e(x)=x$, inverzní prvky: $(\varphi_a(x))^{-1}=\varphi_{a^{-1}}(x)$.
Ukažte dále, že každé ze zobrazení $\varphi_a(x)$ je izomorfismus G na G!

(19) $\dfrac{m}{p^n}+\dfrac{m'}{p^{n'}}=\dfrac{m}{p^n}+\dfrac{m'\cdot p^{n-n'}}{p^n}=\dfrac{m+m'\cdot p^{n-n'}}{p^n}$ pro $n\geq n'$,
t.j. $n-n'\geq 0$; tedy $m+m'p^{n-n}\in\mathbb{Z}$. Jednotkou je 0, inverzní prvek k prvku $\dfrac{m}{p^n}$ je $\dfrac{-m}{p^n}$.
Dokažte, že kbyby ϕ byl izomorfismus Q_p a Q_q, pak pro libovolné $k\in\mathbb{N}$ platí:

$$\phi(\frac{1}{p^k}) = p^{k-1}\phi(\frac{1}{p}).$$

Je-li $\phi(\frac{1}{p}) = \frac{m}{q^n}$, pak $p^{k-1}|m$ pro libovolné $k\in\mathbb{N}$, takové celé číslo m však neexistuje. Platí tedy $Q_p \not\cong Q_q$ pro $p\neq q$.

Že množina $\{\frac{1}{n};\ n\in\mathbb{N}\}$ generuje $\mathbb{Q}$ je zřejmé. Kdyby množina $\left\{\frac{p_1}{q_1},\dots,\frac{p_n}{q_n}\right\}$ byla konečná množina generátorů, pak by $\mathbb{Q}$ byla generována prvkem $\left\{\frac{1}{q_1\cdots q_n}\right\}$, byla by tedy cyklická. Ukažte, že to není možné.

Užijte vlastnosti pro násobení determinantů čtvercových matic: $\det(A\cdot B)=\det A\cdot\det B$.

Jednotkou je 0, ověřte asociativitu. Dále,

$r_1^{-1}=1-r_1$, neboť $r_1+r_1^{-1}=r_1+1-r_1=1\geq 1$, tedy

$r_1\cdot r_1^{-1}=r_1^{-1}\cdot r_1=r_1+1-r_1-1=0.$

Nejprve je třeba ukázat, že pro $a,b>1$ platí

$a\cdot b-a-b+2>1$, t.j. $a\cdot b-a-b+1>0$.

Stačí si uvědomit, že $a-1>0$, $b-1>0$, tedy

$(a-1)\cdot(b-1)>0$, tedy $a\cdot b-a-b+1>0$.

Jednotka:

$a*e=a\cdot e-a-e+2=a$ pro všechna $a\in A$; zvolme $a=0$; pak $0*e=-e+2=0$, $\underline{e=2}$. Skutečně platí, $a*2=2*a=2a-a-2+2=a$.

Platí $a^{-1}=\frac{a}{a-1}>1$. Skutečně,

$$a*a^{-1}=a\cdot\frac{a}{a-1}-a-\frac{a}{a-1}+2=\frac{a^2-a^2+a-a+2(a-1)}{a-1}=2.$$

Jiné a rychlejší řešení: Zřejmě $(A,*)$ je grupoid.

Definujme zobrazení $h:A\longrightarrow R_+\setminus\{0\}$, tak, že $h(a)=a-1$. Je zřejmé, že h je bijekce (dokažte!) a že h je homomorfismus:

$h(a*b) = h(ab-a-b+2)=ab-a-b+1$

$h(a)\cdot h(b)=(a-1)(b-1)=ab-a-b+1.$

Je tedy h izomorfismus a $(A,*)$ musí být grupa.

9. PODGRUPY, ROZKLADY

Nechť $(G,\cdot)$ je grupa. Neprázdnou podmnožinu $A\subseteq G$ nazveme <u>podgrupa</u> grupy $(G,\cdot)$, je-li A sama grupou vzhledem k operaci $\cdot$ grupy $(G,\cdot)$, t.j. je-li $(A,\cdot)$ grupa.

Je-li A podgrupa grupy $(G,\cdot)$, pak $e\in A$ a pro každé $a\in A$ také $a^{-1}\in A$. Také naopak, je-li $\emptyset\neq A\subseteq G$ taková, že $e\in A$, pro každé $a,b\in A$ také $a^{-1}\in A$ a $a\cdot b\in A$, pak A je podgrupou grupy $(G,\cdot)$.

Také platí, že $A\subseteq G$, $A\neq\emptyset$ je podgrupa grupy $(G,\cdot)$, jestliže pro každé $a,b\in A$ je $a\cdot b^{-1}\in A$.

Podgrupa H grupy $(G,\cdot)$ se nazývá <u>normální</u>, jestliže pro každé $h\in H$ a pro každé $g\in G$ platí

$$g^{-1}\cdot h\cdot g\in H.$$

Označme $a\cdot H=\{a\cdot h;h\in H\}$ tzv. <u>levou třídu</u> prvku a dle podgrupy H. Podgrupa H je normální právě když $a\cdot H=H\cdot a=\{h\cdot a;h\in H\}$ pro každé $a\in G$.

Je-li H podgrupa grupy $(G,\cdot)$, pak pro každé $a\in G$ je $|H|=|aH|$ a dále množina všech po dvou různých levých tříd tvoří rozklad množiny G, t.j. indukuje na G ekvivalenci E:

$$\langle x,y\rangle\in E \iff x\cdot H=y\cdot H.$$

Tato ekvivalence je <u>kongruence</u> na grupě $(G,\cdot)$, právě když H je normální podgrupa. Kongruence E se pak nazývá <u>indukovaná normální podgrupou H</u>.

<u>Příklady</u>:

(1) Které grupy mají vlastnost, že každý jejich podgrupoid, obsahující jednotku, je podgrupou?

(2) Určete všechny podgrupy grupy zákrytových pohybů rovnostranného trojúhelníka. Určete, které z nich jsou normální.

(3) Určete všechny podgrupy grupy $(\mathbb{Z},+)$.

Určete všechny faktorové grupy grupy $(\mathbb{Z},+)$.

Ukažte, že každá grupa $(G,\cdot)$ je izomorfní normální podgrupě některé grupy.

Nechť $(G,\cdot)$ je grupa, e její jednotka. Dokažte, že $G/G \cong \{e\}$, $G/\{e\}\cong G$.

Nechť $(G,\cdot)$ je abelovská grupa. Dokažte, že množina $\{x\in G;\ x=x^{-1}\}$ tvoří podgrupu této grupy.

Nechť $(G,\cdot)$ je grupa, $\emptyset\neq A\subseteq G$. Dokažte, že množina

$$\{p\in G;\ p\cdot A=A\cdot p\}$$

tvoří podgrupu grupy $(G,\cdot)$.

Nechť $(G,\cdot)$ je abelovská grupa, $n\in\mathbb{N}$. Dokažte, že množina

$$\{a\in G;\ a^n=e\}$$

je podgrupa grupy $(G,\cdot)$.

Nechť $(G,\cdot)$ je grupa, Θ_1,Θ_2 jsou dvě kongruence na $(G,\cdot)$. Dokažte, že také $\Theta_1\circ\Theta_2$ (relační součin) je kongruence na $(G,\cdot)$.

(11) Nechť $(G,\cdot)$ je grupa. Dokažte, že množina

$Z(G)=\{x\in G;\ a\cdot x=x\cdot a$ pro každé $a\in G\}$ je normální podgrupa v $(G,\cdot)$. Podgrupa $Z(G)$ se nazývá tzv. <u>centrum grupy</u> $(G,\cdot)$.

(12) Nechť $(G,\cdot)$ je grupa. Dokažte, že podgrupa $K(G)$ grupy $(G,\cdot)$ generovaná množinou $\{x^{-1}\cdot y^{-1}\cdot x\cdot y;\ x,y\in G\}$ je normální podgrupa v $(G,\cdot)$. Tato podgrupa se nazývá tzv. <u>komutant</u> grupy $(G,\cdot)$. Dokažte, že $K(G)$ je podgrupou každé normální podgrupy grupy $(G,\cdot)$, a že $G/K(G)$ je již abelovská.

(13) Dokažte, že jsou-li A,B (stačí alespoň jedna z nich) normální podgrupy grupy $(G,\cdot)$, pak také $A\cdot B=\{a\cdot b;\ a\in A, b\in B\}$ je normální podgrupa grupy $(G,\cdot)$.

(14) Nechť A,B jsou podgrupy v $(G,\cdot)$. Dokažte, že $A\cdot B$ je podgrupa v $(G,\cdot)$, právě když platí $A\cdot B=B\cdot A$.

(15) Označme f_{ab} množinu zobrazení $\mathbb{R}\longrightarrow\mathbb{R}$ daných předpisem $f_{ab}(x)=ax+b$ pro každé $a,b\in\mathbb{R}$.

Označme G množinu všech f_{ab}, pro které $a,b\in\mathbb{R}$, $a\neq 0$. Dokažte, že $(G,\cdot)$ je grupa ($\cdot$ je skládání zobrazení) a dokažte, že $N=\{f_{ab};a=1\}$ je normální podgrupa ale $H=\{f_{ab};b=0\}$ nemusí být normální podgrupa. Určete G/N.

(16) Ověřte, zda podgrupa H je normální podgrupou grupy G:

(a) $G=(\mathbb{R}\times\mathbb{R},+)$, $H=\{\langle x,y\rangle;x+2y=0\}$

(b) $G=(\mathbb{R}\times\mathbb{R},+)$, $H=\{\langle x,3x\rangle;x\in\mathbb{R}\}$

(c) $G=(\mathbb{C},+)$, $H=\mathbb{R}$

(d) $G=(\mathbb{C}\setminus\{0\},\cdot)$, $H=\mathbb{R}\setminus\{0\}$

(e) $G=(\mathbb{Z},+)$, $H=\{4\cdot k;k\in\mathbb{Z}\}$

(f) $G=(\mathbb{Z}_4\times\mathbb{Z}_6,+)$, H je generovaná množinou $\{\langle\overline{2},\overline{2}\rangle\}$

(g) $G=(\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z},+)$, $H=\{\langle n,m,0\rangle;n,m\in\mathbb{Z}\}$

(h) $G=(\{c\in\mathbb{C};c^{12}=1\},\cdot)$, $H=\{c\in\mathbb{C};c^2=1\}$.

(17) Ověřte, že H je normální podgrupa v G a určete G/H:

(a) $G=(\mathbb{C}\setminus\{0\},\cdot)$, $H=\{c\in\mathbb{C};|c|=1\}$

(b) $G=(\mathbb{C}\setminus\{0\},\cdot)$, $H=(\mathbb{R}_+,\cdot)$ (kladná reálná čísla)

(c) $G=(\mathbb{R}\setminus\{0\},\cdot)$, $H=(\{-1,1\},\cdot)$

(d) $G=(\mathbb{R},+)$, $H=(\mathbb{Z},+)$

(e) $G=(\mathbb{C},+)$, $H=(\mathbb{R},+)$

(f) $G=(\mathbb{Z},+)\times(\mathbb{Z},+)$, $H=\{\langle 2k,3h\rangle;k,h\in\mathbb{Z}\}$

(g) $G=(\mathbb{R}\times\mathbb{R},+)$, $H=\{\langle x,2x\rangle;x\in\mathbb{R}\}$.

(18) Je-li A normální podgrupa v G, B normální v G, pak $A\cdot B$ je normální podgrupa v G. Dokažte!

(19) Ukažte, že může být A normální podgrupa v B, B normální v C, ale A není normální v C.

(20) Ukažte, že je-li $G=A\times B$, pak $G/A\cong B$.

(21) Najděte všechny levé (pravé) třídy rozkladu grupy G dle podgrupy H, je-li:

(a) $G=(\mathbb{Z},+)$, $H=\{5k;h\in\mathbb{Z}\}$

(b) G je grupa zákrytových pohybů obdélníka, H={identita+ jedna osová souměrnost

(c) G je grupa zákrytových pohybů rovnostranného trojúhelníka H={identita + jedna osová souměrnost}

(d) G je grupa regulárních matic řádu n nad $\mathbb{R}$, H je grupa skalárních matic (jsou tvaru $d \cdot E$, $d \in \mathbb{R} \setminus \{0\}$, E jednotková matice).

(e) G je grupa regulárních matic řádu n nad $\mathbb{R}$, H je grupa diagonálních matic regulárních ($a_{ij}=0$ pro $i \neq j$).

2) Ukažte, že je-li řád grupy G roven součinu dvou různých prvočísel, pak pro libovolné podgrupy H_1, H_2 splňující $G \neq H_1 \neq H_2 \neq G$ platí $H_1 \cap H_2 = \{e\}$.

Body k řešení:

1) Jsou to tzv. involutorní grupy, t.j. grupy, ve kterých pro každý prvek x platí $x \cdot x = e$.

2) Prvky grupy zákrytových pohybů rovnostranného trojúhelníka jsou $id, o_1, o_2, o_3, r_1, r_2$, kde o_i je otočení kolem i-té osy, r_1 je rotace o 120^0, r_2 rotace o 240^0.

Podgrupy $\{id, o_1\}, \{id, o_2\}, \{id, o_3\}$ nejsou normální,

podgrupy $\{id, r_1, r_2\}, \{id\}, \{id, o_1, o_2, o_3, r_1, r_2\}$ jsou normální.

3) Zřejmě $\{0\}$ a $\mathbb{Z}$ jsou podgrupy grupy $(\mathbb{Z},+)$. Nechť $\{0\} \neq H \neq \mathbb{Z}$ je podgrupa grupy $(\mathbb{Z},+)$. Pak $1 \notin H$ (jinak by $H=\mathbb{Z}$), a protože $H \neq \{0\}$, existuje $h \in H$ takové, že $1 \neq h > 0$. Zvolme za k nejmenší přirozené číslo různé od 1, které patří do H. Ukážeme, že H je generovaná množinou $\{k\}$. Jestliže $m \in H$, pak $m = q \cdot k + r$ kde $q, r \in \mathbb{Z}$ a platí $0 \leq r < k$. Jelikož $m \in H$, $k \in H$, pak také $q \cdot k = k + k + \ldots + k$ (q-krát) patří do H, a tedy také $r = m - q \cdot k \in H$. Avšak $r < k$. Jelikož k je nejmenší přirozené číslo z H, je tedy $r=0$. Neboli $m = q \cdot k$, t.j. $m = k + \ldots + k$ (q-krát). Tedy každé $m \in H$ lze vygenerovat pomocí k, t.j. $\{k\}$ generuje H. Tedy každá podgrupa grupy $(\mathbb{Z},+)$ je množinou všech násobků některého čísla $k \in \mathbb{Z}$ (pro $\{0\}$ je $k=0$, pro $\mathbb{Z}$ je $k=1$).

(4) Jak jsme dokázali v (3), je každá podgrupa H grupy $(\mathbb{Z},+)$ množinou $H = \{a \cdot k; a \in \mathbb{Z}\}$. Jelikož $(\mathbb{Z},+)$ je abelovská, je každá její podgrupa normální. Pak

$$(\mathbb{Z},+)/\{a\cdot k; a\in\mathbb{Z}\}=(\mathbb{Z}_k,+)$$

t.j. grupa všech zbytkových tříd mod k pro $k\neq 0$, $k\neq 1$; pro $k=0$ je $(\mathbb{Z},+)/\{0\}\cong(\mathbb{Z},+)$, pro $k=1$ je $(\mathbb{Z},+)/(\mathbb{Z},+)\cong\{0\}$.

(5) Zvolme libovolnou grupu $(H,\cdot)$. Pak grupa $(G,\cdot)$ je zřejmě izomorfní podgrupě

$$(G,\cdot)\times(\{e\},\cdot)$$

direktního součinu $(G,\cdot)\times(H,\cdot)$ (kde e je jednotka $(H,\cdot)$), avšak tato podgrupa je v tomto direktním součinu normální (je indukovaná faktorovou kongruencí).

(7) Stačí si uvědomit, že pro $x\neq e$ platí $x=x^{-1}$, právě když x je řádu 2. Ukažte, že prvky řádu 2 spolu s jednotkou tvoří podgrupu.

(8) Nejprve ukažme, že $N_A=\{p\in G; pA=Ap\}$ je podgrupa: jestliže $p,q\in N_A$, pak $(pq)(A)=p(qA)=p(Aq)=(pA)q=(Ap)q=A(pq)$, dále $p^{-1}(Ap)=p^{-1}(pA)=(p^{-1}p)A=A$, tedy $(p^{-1}A)p=A$, $(p^{-1}A)p\cdot p^{-1}=A\cdot p^{-1}=(p^{-1}A)(p\cdot p^{-1})=p^{-1}A=Ap^{-1}$. Zřejmě e je jednotka a p^{-1} je inverzní k prvku p.

(9) Je-li $a^n=b^n=e$, pak $(a\cdot b)^n=a^n\cdot b^n=e\cdot e=e$, neboť G je abelovská. Podobně platí $(a^{-1})^n=(a^n)^{-1}=e^{-1}=e$.

(10) Víme, že $\Theta_1\circ\Theta_2$ je kongruence právě když $\Theta_1\circ\Theta_2=\Theta_2\circ\Theta_1$ (to je podmínka pro to, aby $\Theta_1\circ\Theta_2$ byla ekvivalence, substituční podmínka je zřejmá). Ověříme tedy tuto rovnost. Nechť $\langle x,y\rangle\in\Theta_1\circ\Theta_2$. Pak existuje $z\in G$ tak, že $\langle x,z\rangle\in\Theta_1$ a $\langle z,y\rangle\in\Theta_2$. Ze substituční podmínky plyne

$$\langle x,x\cdot z^{-1}\cdot y\rangle=\langle x\cdot z^{-1}\cdot z,x\cdot z^{-1}\cdot y\rangle\in\Theta_2$$
$$\langle x\cdot z^{-1}\cdot y,y\rangle=\langle x\cdot z^{-1}\cdot y,z\cdot z^{-1}\cdot y\rangle\in\Theta_1,$$

tedy $\langle x,y\rangle\in\Theta_2\cdot\Theta_1$, t.j. $\Theta_1\cdot\Theta_2\subseteq\Theta_2\cdot\Theta_1$. Analogicky se dokáže obrácená inkluze, tedy

$$\Theta_1\circ\Theta_2=\Theta_2\circ\Theta_1$$

pro každé dvě kongruence na $(G,\cdot)$, a tedy $\Theta_1\circ\Theta_2$ je kongruence na $(G,\cdot)$.

(11) Ukažme nejprve, že $Z(G)$ je podgrupa: jestliže $x,y\in Z(G)$, $a\in$

libovolný prvek, pak $(xy)a=x(ya)=x(ay)=(xa)y=a(xy)$,
$x^{-1}ax=x^{-1}xa=a$, tedy $x^{-1}ax\cdot x^{-1}=ax^{-1}, x^{-1}a=ax^{-1}$.
Buď $x\in Z(G)$, $y\in G, a\in G$. Ukažme, že $y^{-1}xy\in Z(G)$:
$(y^{-1}xy)a=y^{-1}\cdot x(ya)=y^{-1}\cdot ya\cdot x=a\cdot x=a\cdot x\cdot y^{-1}\cdot y=a\cdot y^{-1}x\cdot y=a(y^{-1}xy)$.

) Označme M množinu prvků tvaru $g^{-1}h^{-1}gh$, $g,h\in G$. Pro libovolné $x\in G$ platí:

$x^{-1}g^{-1}h^{-1}ghx=x^{-1}g^{-1}xx^{-1}h^{-1}xx^{-1}gxx^{-1}hx=$

$=(x^{-1}gx)^{-1}\cdot(x^{-1}hx)^{-1}\cdot(x^{-1}gx)\cdot(x^{-1}hx)\in M$, je tedy $K(G)$ normální podgrupa. Ukažme, že grupa $G/K(G)$ je abelovská:

$(g^{-1}K(G))(h^{-1}K(G))(hK(G))=(g^{-1}h^{-1}gh)K(G)=K(G)$, odkud
$(gK(G))(hK(G))=(hK(G))(gK(G))$, je tedy $G/K(G)$ abelovská.
Ukažme, že pokud N je normální podgrupa obsahující $K(G)$, pak G/N je abelovská:
definujme zobrazení $f:G/K(G)\longrightarrow G/N$ předpisem $f(gK(G))=g\cdot N$.
Platí, že jestliže $g\cdot K(G)=g_1K(G)$, pak $g^{-1}g_1\in K(G)\subseteq N$, tedy $gN=g_1N$ a f je zobrazení. Ukažte, že f je surjektivní homomorfismus. Je tedy G/N homomorfní obraz $G/K(G)$ která je abelovská, tedy G/N je abelovská.

13) Ukažme nejprve, že $A\cdot B$ je podgrupa:
Buďte $a_1\cdot b_1$, $a_2\cdot b_2\in A\cdot B$. Zřejmě $b_1\cdot a_2\in b_1\cdot A=A\cdot b_1$, tedy
$b_1a_2=a'_2\cdot b_1$ pro nějaký prvek $a'_2\in A$. Pak
$(a_1\cdot b_1)(a_2\cdot b_2)=a_1\cdot(b_1\cdot a_2)\cdot b_2=a_1\cdot(a'_2\cdot b_1)\cdot b_2=(a_1\cdot a'_2)(b_1\cdot b_2)\in A\cdot B$.

$(a_1\cdot b_1)^{-1}=b_1^{-1}a_1^{-1}\in b_1\cdot A=A\cdot b_1$, tedy $b_1^{-1}\cdot a_1^{-1}=a_1'^{-1}\cdot b_1\in A\cdot B$ pro

nějaké $a_1'^{-1}$, tedy $A\cdot B$ je podgrupa. Ukažme, že $A\cdot B$ je normální:
pro $x\in G$ platí:
$x\cdot(A\cdot B)=(x\cdot A)\cdot B=(A\cdot x)\cdot B=A\cdot(x\cdot B)=A\cdot(B\cdot x)=(A\cdot B)\cdot x$.

14) Nechť $A\cdot B=B\cdot A$. Pak
$(a_1\cdot b_1)\cdot(a_2\cdot b_2)=a_1\cdot(b_1\cdot a_2)\cdot b_2$, $b_1a_2\in B\cdot A=A\cdot B$, tedy $b_1\cdot a_2=a'_2\cdot b'_1$
pro nějaké $a'_2\in A$, $b'_1\in B$.
Tedy $a_1\cdot(b_1\cdot a_2)\cdot b_2=a_1\cdot(a'_2\cdot b'_1)\cdot b_2=(a_1\cdot a'_2)\cdot(b'_1\cdot b_2)\in A\cdot B$.

Podobně $(a_1 \cdot b_1)^{-1} = b_1^{-1} \cdot a_1^{-1} = a_1'^{-1} \cdot b_1'^{-1} \in A \cdot B$.
Naopak, je-li $A \cdot B$ podgrupa, pak pro každé $a_1, a_2 \in A$, $b_1, b_2 \in B$ existují $a_3 \in A$, $b_3 \in B$ tak, že $(a_1 \cdot b_1) \cdot (a_2 \cdot b_2) = a_3 \cdot b_3$, tedy

$b_1 \cdot a_2 = a_1^{-1} a_3 \cdot b_3 \cdot b_2^{-1} \in A \cdot B$.

Tedy $B \cdot A \subseteq A \cdot B$. Podobně se ukáže $A \cdot B \subseteq B \cdot A$.

(15) $f_{a,b}(x) \circ f_{c,d}(x) = f_{c,d}(f_{a,b}(x)) = c(f_{a,b}(x)) + d = c(ax+b) + d =$

$= cax + cb + d = f_{ca,cb+d}$; je-li $a, c \neq 0$, pak $a \cdot c \neq 0$;

Ukažte, že $f_{1,0}(x) = x$ je jednotkový prvek;

$(f_{a,b}(x))^{-1} = f_{\frac{1}{a}, -\frac{b}{a}}(x)$.

Ukažte sami, že N je podgrupa. Dokážeme, že N je normální: Buď $f_{a,b}(x)$ libovolný prvek, $f_{1,c}$ libovolný prvek z N. Pak

$$f_{a,b}^{-1} \circ f_{1,c} \circ f_{a,b} = f_{\frac{1}{a}, -\frac{b}{a}} \circ f_{1,c} \circ f_{a,b} =$$

$$f_{\frac{1}{a}, -\frac{b}{a}+c} \circ f_{a,b} = f_{1,-b+ac+b} = f_{1,ac} \in N.$$

Ukažme, že H nemusí být normální: buď $f_{c,0} \in H$ libovolný; pak

$$f_{a,b}^{-1} \circ f_{c,0} \circ f_{a,b} = f_{\frac{1}{a}, -\frac{b}{a}} \circ f_{c,0} \circ f_{a,b} =$$

$$= f_{\frac{c}{a}, -\frac{cb}{a}} \circ f_{a,b} = f_{c,-cb+b},$$

$-cb+b$ nemusí být 0, tedy H nemusí být normální.

Zřejmě $f_{x,y} \circ N = \{f_{x,z};\ z \in \mathbb{R}\}$

Uvažujme zobrazení $F: (\{f_{a,b}\}, \circ) \longrightarrow (\mathbb{R} \setminus \{0\}, \cdot)$ takto:

$$F(f_{a,b}) = a .$$

Ukažte, že F je surjektivní homomorfismus, Ker $F = N$, ted

$(\{f_{a,b}\}, \circ)/N \cong (\mathbb{R} \setminus \{0\}, \cdot)$.

(16)(a) Ano, $(\mathbb{R} \times \mathbb{R}, +)$ je abelovská

(b) Ano, $(\mathbb{R}\times\mathbb{R},+)$ je abelovská

(c) Ano, $(\mathbb{C},+)$ je abelovská

(d) Ano

(e) Ano

(f) Ano

(g) Ano

(h) Ano

(a) Soustředné kružnice o středu v počátku.

(c) Uvažujte zobrazení $\varphi:(\mathbb{R}\setminus\{0\},\cdot)\longrightarrow(\mathbb{R}^+,\cdot)$ tak, že

$$\varphi: a\longrightarrow|a|.$$

Ukažte, že φ je surjektivní homomorfismus a že Ker $\varphi=H$. Pak $G/H\cong(\mathbb{R}_+,\cdot)$.

(d) Třídy jsou množiny $\{r+z; z\in\mathbb{Z}\}$ pro každé $r\in\mathbb{R}$.

(e) Ukažte, že $K=\{c\in\mathbb{C};\ c=a-\bar{a}$ pro nějaké $a\in\mathbb{C}\}$ je vzhledem ke sčítání podgrupa:

$(a-\bar{a})+(b-\bar{b})=(a+b)-\overline{a+b}$

$-(a-\bar{a})=-a+\bar{a}=(-a)+\overline{(-a)}$.

Uvažujte zobrazení φ: $\mathbb{C}\longrightarrow K$ tak, že

$$\varphi(c)=c-\bar{c}.$$

Ukažte, že φ je surjektivní homomorfismus a že Ker $\varphi=H$, tedy $G/H\cong K$.

) Že je podgrupa $A\cdot B$ normální, plyne z příkladu **(13)**.

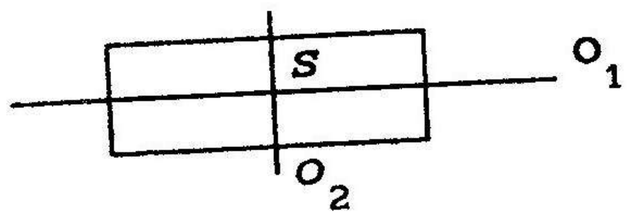
) Kleinova čtyřgrupa K_4 je normální v S_4 (viz. příklad **(6)**, §12).

$K=\left(\left\{\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\mathrm{id}\right\},\cdot\right)$ je normální v K_4 (K_4 je abelovská), ale K není normální v S_4:

$$\begin{pmatrix}2&3&1&4\\1&2&3&4\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}\notin K.$$

) Uvažujte zobrazení $\varphi:G\longrightarrow B$ takové, že $\varphi(\langle a,b\rangle)=b$. Pak φ je surjektivní homomorfismus. Ukažte, že Ker $\varphi\cong A$, tedy $G/\mathrm{Ker}\varphi\cong G/A\cong B$.

)(a) $a\cdot H=\{5ah;\ h\in\mathbb{Z}\}=H\cdot a=\{5ah;\ h\in\mathbb{Z}\}$.

(b) 

$G=\{o_1, o_2, s, id\}$
$H=\{o_1, id\}$

$id\cdot H=H=\{o_1, id\}$
$o_1\cdot H=\{o_1, o_1\cdot o_1\}=\{o_1, id\}=H$
$o_2\cdot H=\{o_2, o_2\cdot o_1\}=(s, o_2\}$
$s\cdot H=\{s, s\cdot o_1\}=\{s, o_2\}$
$G/H=\{\{o_1, id\}, \{s, o_2\}\}$ $\quad G/H=G/H.$

(d) $A\cdot H=A\cdot\{d\cdot E; d\in\mathbb{R}\setminus\{0\}\}=\{A\cdot d\cdot E\}=\{d\cdot A; d\in\mathbb{R}\setminus\{0\}\}=H\cdot A.$

(e) Ukažme, že existuje regulární matice A taková, že $A\cdot H\neq H\cdot A$.

Nechť $A=\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$. Zřejmě $\begin{pmatrix} 1 & -2 \\ 1 & 2 \end{pmatrix}=\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\cdot\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}\in A\cdot H$,

Kdyby $\begin{pmatrix} 1 & -2 \\ 1 & 2 \end{pmatrix}\in H\cdot A$, pak existují $d_1, d_2\in\mathbb{R}$ takové, že

$$\begin{pmatrix} d_1 & 0 \\ 0 & d_2 \end{pmatrix}\cdot\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}=\begin{pmatrix} 1 & -2 \\ 1 & 2 \end{pmatrix}=\begin{pmatrix} d_1 & -d_1 \\ d_2 & d_2 \end{pmatrix},$$

tedy $d_1=1$, $d_1=2$, spor.

(22) Je-li grupa G řádu $p\cdot q$, kde p, q jsou prvočísla, pak G má nejvýše dvě různé netriviální podgrupy: H_1 řádu p a H_2 řádu q. Jejich průnik je různý od H_1 i H_2, tedy může být pouze $\{e\}$.

10. HOMOMORFISMY GRUP

Nechť $(G,\cdot),(H,\cdot)$ jsou grupy. Zobrazení $h:G\longrightarrow H$ je homomorfismem těchto grup, jestliže pro každé $a,b\in G$ platí

$$h(a\cdot b)=h(a)\cdot h(b).$$

Dále lze dokázat, že pro každý homomorfismus h grupy $(G,\cdot)$ do grupy $(H,\cdot)$ platí

$$h(e)=e',$$

kde e resp. e' je jednotkou v $(G,\cdot)$ resp. v $(H,\cdot)$, a že pro každé a platí

$$h(a^{-1})=(h(a))^{-1}.$$

Jádrem homomorfismu h nazveme množinu

$$Ker\ h=\{a\in G;\ h(a)=e'\}.$$

Snadno se dokáže, že $Ker\ h$ je normální podgrupa grupy $(G,\cdot)$.

Je-li $h:(G,\cdot)\longrightarrow(H,\cdot)$ homomorfismus, pak ekvivalence Θ_h indukovaná homomorfismem h je kongruencí na $(G,\cdot)$, a je to právě kongruence indukovaná normální podgrupou $Ker\ h$.

Obráceně, je-li Θ kongruence na grupě $(G,\cdot)$, pak kanonické zobrazení $(G,\cdot)$ na $(G/\Theta,\cdot)$ (dané předpisem $h_\Theta(a)=[a]_\Theta$) je homomorfismus a jeho jádro $Ker\ h_\Theta$ je normální podgrupa, přičemž $Ker\ h_\Theta=\{a\in G;\ \langle a,e\rangle\in\Theta\}$.

Homomorfismus $h:(G,\cdot)\longrightarrow(H,\cdot)$ se nazývá izomorfismus, je-li bijektivní.

Příklady:

(1) Nechť $(\mathbb{R}_+,\cdot)$ je multiplikativní grupa všech kladných reálných čísel. Dokažte, že zobrazení $h(x)=2^x$ je surjektivní homomorfismus grupy $(\mathbb{R},+)$ na grupu $(\mathbb{R}_+,\cdot)$.

(2) Nechť $(G,\cdot)$ je grupa. Dokažte, že zobrazení $h(x)=x^{-1}$ je izomorfismus $(G,\cdot)$ na $(G,\cdot)$, právě když $(G,\cdot)$ je abelovská.

(3) Nechť $(\mathbb{C},+)$ je aditivní grupa všech komplexních čísel. Rozhodněte, která ze zobrazení $f:\mathbb{C}\longrightarrow\mathbb{C}$ jsou homomorfismy $(\mathbb{C},+)$ do $(\mathbb{C},+)$:

(a) $f(z)=\bar{z}$

(b) $f(z)=z+1$

(c) $f(r(\cos\varphi+i\sin\varphi))=r\left[\cos(\varphi+\frac{\pi}{2})+i(\sin(\varphi+\frac{\pi}{2})\right]$

(d) $f(r(\cos\varphi+i\sin\varphi))=r^2(\cos\varphi+i\sin\varphi)$.

(4) Nechť $(G,\cdot)=(\mathbb{Z},+)\times(\mathbb{Z},+)$. Rozhodněte, která ze zobrazení $f:G\longrightarrow G$ jsou izomorfismy $(G,+)$ na $(G,+)$:

(a) $f(\langle m,n\rangle)=\langle m+n;-n\rangle$ (b) $f(\langle m,n\rangle)=\langle 2m,n\rangle$

(c) $f(\langle m,n\rangle)=\langle 2n+2m,m+2n\rangle$ (d) $f(\langle m,n\rangle)=\langle m+1,n\rangle$.

(5) Najděte všechny izomorfismy grupy $(G,+)=(\mathbb{Z},+)\times(\mathbb{Z},+)$ na $(G,+)$.

(6) Nechť $\mathbb{R}_0=\mathbb{R}\setminus\{0\}$. Dokažte, že zobrazení $f(x)=\mathrm{sgn}(x)$ je homomorfismus grupy $(\mathbb{R}_0,\cdot)$ do grupy $(\{1,-1\},\cdot)$. Co je jádrem tohoto homomorfismu?

(7) Určete, která ze zobrazení jsou homomorfismy a určete jejich jádra:

(a) $f:(\mathbb{Z},+)\longrightarrow(\mathbb{R},+)$, $f(n)=2n+1$

(b) $f:(\mathbb{Q}\setminus\{0\},\cdot)\longrightarrow(\mathbb{R},+)$, $f(x)=\log|x|$

(c) $f:(\mathbb{Z},+)\longrightarrow(\mathbb{C}\setminus\{0\},\cdot)$, $f(n)=i^n$

(d) $f:(\mathbb{R}\times\mathbb{R}\times\mathbb{R},+)\longrightarrow(\mathbb{R}\times\mathbb{R},+)$, $f(\langle a,b,c\rangle)=\langle a-b,b+2c\rangle$

(e) $f:(\mathbb{R},+)\longrightarrow(\mathbb{R}\setminus\{0\},\cdot)$, $f(a)=|a|$

(f) $f:(\mathbb{R},+)\longrightarrow(\mathbb{R}\setminus\{0\},\cdot)$, $f(a)=2^a$

(g) $f:(\mathbb{C}\setminus\{0\},\cdot)\longrightarrow(\mathbb{C}\setminus\{0\},\cdot)$, $f(c)=\frac{c}{|c|}$

(h) $f:(M_n,+)\longrightarrow(\mathbb{R},+)$, $f([a_{ij}])=a_{11}$, kde M_n je množina všech matic $n\times n$ nad $\mathbb{R}$.

(8) Najděte izomorfismus grup $(\mathbb{R},+)$ a $(\mathbb{R}_+,\cdot)$.

(9) Nechť $\mathbb{Q}_+$ je množina všech kladných racionálních čísel. Dokažte, že grupy $(\mathbb{Q},+)$ a $(\mathbb{Q}_+,\cdot)$ nejsou izomorfní!

(10) Pro danou grupu G ověřte, že H je její normální podgrupa a najděte grupu H' a surjektivní homomorfismus φ G na H' tak, aby $Ker\ \varphi=H$, tedy $G/H\cong H'$:

(a) $G=(\mathbb{C}\setminus\{0\},\cdot)$, $H=\{c\in\mathbb{C};|c|=1\}$

(b) $G=(\mathbb{C}\setminus\{0\},\cdot)$, $H=(\mathbb{R}^+,\cdot)$

(c) $G=(\mathbb{R}\setminus\{0\},\cdot)$, $H=(\{-1,1\},\cdot)$

$G=(\mathbb{R},+)$, $H=(\mathbb{Z},+)$

$G=(\mathbb{C},+)$, $H=(\mathbb{R},+)$

$G=(\mathbb{Z},+)\times(\mathbb{Z},+)$, $H=\{\langle 2k,3h\rangle; k,h\in\mathbb{Z}\}$

$G=(\mathbb{R}\times\mathbb{R},+)$, $H=\{\langle x,2x\rangle; x\in\mathbb{R}\}$.

Buďte $\mathbb{Q}_p$ grupa p-adických čísel (viz př.19,kap. 11) a C_{p^∞} nazicyklická grupa typu p^∞ (viz. př. 17, kap.11), ε_{p^n} primitivní p^n-tá odmocnina z 1, t.j. ε_n je kořen rovnice $x^{p^n}=1$ takový, že nejmenší přirozene číslo m vlastnosti $\varepsilon_n^m=1$ je p^n. Ukažte, že zobrazení

$\varphi:\mathbb{Q}_p\longrightarrow C_{p^\infty}$ takové, že $\frac{m}{p^n}\longrightarrow\varepsilon_n^m$, je homomorfismus $\mathbb{Q}_p$ na C_{p^∞}. Ukažte, že $Ker\ \varphi=\mathbb{Z}$ a tedy $\mathbb{Q}_p/\mathbb{Z}\cong C_{p^\infty}$.

2) Ukažte, že zobrazení $\varphi:S_n\longrightarrow(\{\pm1\},\cdot)$ takové, že každé permutaci přiřadí její znaménko, je homomorfismus. Ukažte, že $Ker\ \varphi=A_n$, tedy $S_n/A_n\cong\mathbb{Z}_2$.

3) Ukažte, že zobrazení $\varphi:(\mathbb{R}\setminus\{0\},\cdot)\longrightarrow(\{\pm1\},\cdot)$, přiřazující každému prvku jeho znaménko, je homomorfismus. Ukažte, že $Ker\ \varphi=\mathbb{R}_+$, a tedy $(\mathbb{R}\setminus\{0\},\cdot)/(\mathbb{R}_+,\cdot)\cong\mathbb{Z}_2$.

4) Ukažte, že zobrazení přiřazující každé regulární matici její determinant, je homomorfismus grupy všech regulárních matic stupně n na grupu $(\mathbb{R}\setminus\{0\},\cdot)$.

5) Uvažujte grupu $Int\ G$ z příkladu 18, kap. 8. Uvažujte zobrazení $\psi:G\longrightarrow Int\ G$ takové, že $\psi(a)=\varphi_a$, kde $\varphi_a(x)=a^{-1}\cdot x\cdot a$. Ukažte, že ψ je surjektivní homomorfismus G na $Int\ G$ s jádrem $Ker\ \psi=Z(G)$ (viz příklad 11, kap. 9). Je tedy $G/Z(G)\cong Int\ G$.

16) Najděte všechny izomorfismy cyklické grupy řádu n do sebe. Jaké jsou všechny izomorfismy $(\mathbb{Z},+)$ na $(\mathbb{Z},+)$?

17) Najděte všechny izomorfismy Kleinovy čtyřgrupy do sebe.

18) Najděte všechny izomorfismy grupy $(\mathbb{Q},+)$ do sebe.

(19) Jsou následující zobrazení $(\mathbb{Z},+)\longrightarrow(\mathbb{Z},+)$ homomorfismy?

(a) $f(n)=3n$

(b) $f(n)=5n+1$

(c) $f(n)=h\cdot n,\ h\in\mathbb{Z}$

(d) $f(n)=n^2$

(e) $f(n)=1$

(f) $f(n)=0$.

(20) Rozhodněte, zda existuje surjektivní homomorfismus:

(a) $(\mathbb{Z},+)$ na $(\mathbb{Q},+)$

(b) $(\mathbb{Q},+)$ na $(\mathbb{Z},+)$

(c) $(\mathbb{Q},+)$ na $(\mathbb{Q}\setminus\{0\},\cdot)$.

(21) Rozhodněte, zda existuje surjektivní homomorfismus grupy zákrytových pohybů rovnostranného trojúhelníka na

(a) grupu řádu 2

(b) grupu řádu 3.

(22) Nechť G je grupa, zobrazení $d:G\longrightarrow G\times G$ takové, že $d(g)=\langle g,g\rangle$. Ukažte, že G je abelovská, právě když $d(G)$ je normální podgrupa v $G\times G$.

(23) Nechť G je grupa, m zobrazení $G\times G\longrightarrow G$ takové, že $m(\langle g_1,g_2\rangle)=g_1\cdot g_2$. Ukažte, že G je abelovská, právě když m je homomorfismus.

Návody k řešení:

(1) Zřejmě $h(x+y)=2^{x+y}=2^x\cdot 2^y=h(x)\cdot h(y)$. Dále, pro každé $b\in\mathbb{R}_+$ existuje $a\in\mathbb{R}$ tak, že $h(a)=b$, totiž $a=\log_2 b$.

(2) Je-li G abelovská, pak

$$h(x\cdot y)=(x\cdot y)^{-1}=y^{-1}\cdot x^{-1}=x^{-1}\cdot y^{-1}=h(x)\cdot h(y).$$

Není-li G abelovská, pak existují $x,y\in G$ tak, že $x\cdot y\neq y\cdot x$. Pa $h(x\cdot y)\neq h(x)\cdot h(y)$, tedy h není homomorfismus.

(3)(a) ANO $f(a+b)=\overline{a+b}=\overline{(a_1+a_2i)+(b_1+b_2i)}=(a_1+b_1)-(a_2+b_2)i=\overline{a}+\overline{b}$.

(b) NE $f(a+b)=a+b+1$

$f(a)+f(b)=a+1+b+1=a+b+2$.

(c) ANO

Uvažte, že uvedené zobrazení je otočení kolem počátku o 90°.

Ukažte, že úhel mezi z a $f(z)$ je 90°.

NE, např. pro $a=1$, $b=2i$, je $|f(a+b)|=5$, $|f(a)+f(b)|=\sqrt{17}$, tedy $f(a+b)\neq f(a)+f(b)$.

f je bijekce (ověřte!),

$f(\langle m_1,n_1\rangle+\langle m_2,n_2\rangle)=f(\langle m_1+m_2,n_1+n_2\rangle)=\langle m_1+m_2+n_1+n_2,-n_1-n_2\rangle$

$f(\langle m_1,n_1\rangle)+f(\langle m_2,n_2\rangle)=\langle m_1+n_1,-n_1\rangle+\langle m_2+n_2,-n_2\rangle=$

$\langle m_1+n_1+m_2+n_2,-n_1-n_2\rangle$, je tedy f izomorfismus.

ANO (c) ANO

NE: $f(\langle m_1,n_1\rangle+\langle m_2,n_2\rangle)=f\langle m_1+m_2+1,n_1+n_2\rangle$

$f(\langle m_1,n_1\rangle)+f(\langle m_2,n_2\rangle)=\langle m_1+m_2+2,n_1+n_2\rangle$.

Jsou to zobrazení

$$f(\langle m,n\rangle)=\begin{bmatrix} a & b \\ c & d \end{bmatrix}\cdot\begin{pmatrix} m \\ n \end{pmatrix}$$

pro která $\begin{vmatrix} a & b \\ c & d \end{vmatrix}\neq 0$.

Jádrem je množina $\mathbb{R}^+$.

a) $f(x+y)=2(x+y)+1=2x+2y+1$.

$f(x)+f(y)=2x+1+2y+1=2x+2y+2$, není to homomorfismus.

b) ANO, je to dokonce izomorfismus, neboť $Ker\ f=\{1\}$.

c) $f(x+y)=i^{x+y}=i^x\cdot i^y=f(x)\cdot f(y)$, $Ker\ f=\{4k;k\in\mathbb{Z}\}$.

d) ANO

$f(\langle a,b,c\rangle+\langle a',b',c'\rangle)=\langle a+a'-b-b',b+b'+2c+2c'\rangle$

$f(\langle a,b,c\rangle)+f(\langle a',b',c'\rangle)=\langle a-b,b+2c\rangle+\langle a'-b',b'+2c'\rangle=$

$\langle a+a'-b-b',b+b'+2c+2c'\rangle$

$Ker\ f=\{\langle a,b,c\rangle;\ a:b:c=2:2:-1\}$.

e) NE

$f(a+b)=|a+b|$, $f(a)\cdot f(b)=|a|\cdot|b|$.

f) ANO: $f(x+y)=2^{x+y}=2^x\cdot 2^y=f(x)\cdot f(y)$, $Ker\ f=\{0\}$.

g) ANO: $f(c_1\cdot c_2)=\dfrac{c_1\cdot c_2}{|c_1\cdot c_2|}=\dfrac{c_1\cdot c_2}{|c_1|\cdot|c_2|}=\dfrac{c_1}{|c_1|}\cdot\dfrac{c_2}{|c_2|}=f(c_1)\cdot f(c_2)$

$Ker\ f=\{c\in\mathbb{C};\ c=|c|\}=\mathbb{R}^+$.

h) ANO: $f([a_{ij}]+[b_{ij}])=a_{11}+b_{11}=f([a_{ij}])+f([b_{ij}])$,

$$Ker\ f=\{[a_{ij}];\ a_{11}=0\}.$$

(8) Například $\varphi:(\mathbb{R},+)\longrightarrow(\mathbb{R}^+,\cdot)$, $\varphi(x)=2^x$.

(9) Buď h nějaký izomorfismus $\mathbb{Q}\longrightarrow\mathbb{Q}^+$. Nechť $f(a)=2\in\mathbb{Q}^+$, nechť $f(\frac{a}{2})=c\in\mathbb{Q}^+$. Pak $2=f(a)=f(\frac{a}{2}+\frac{a}{2})=f(\frac{a}{2})\cdot f(\frac{a}{2})=c^2$, tedy $c^2=2$, $c\in\mathbb{Q}_+$, to je spor.

(10) Podívejte se na řešení úlohy č.17 z kap.9.

(11) $\varphi\left(\frac{m}{p^n}+\frac{m'}{p^{n'}}\right)=\varphi\left(\frac{m+m'p^{n-n'}}{p^n}\right)=\varepsilon_n^{m+m'p^{n-n'}}$, $n\geq n'$.

$\varphi(\frac{m}{p^n})\cdot\varphi(\frac{m}{p^{n'}})=\varepsilon_n^m\cdot\varepsilon_{n'}^{m'}$.

Musíme ukázat, že $\varepsilon_n^m\cdot\varepsilon_{n'}^{m'}=\varepsilon_n^m\cdot\varepsilon_n^{m'p^{n-n'}}$, tedy $\varepsilon_{n'}^{m'}=\varepsilon_n^{m'p^{n-n'}}$.

Zřejmě $(\varepsilon_{n'})^{p^{n'}}=1$, je tedy $\varepsilon_{n'}=\varepsilon_n^{p^{n-n'}}$, tedy

$\varepsilon_{n'}^{m'}=\varepsilon_n^{m'\cdot p^{n-n'}}$, což jsme měli dokázat.

Je zřejmé, že φ je surjekce, neboť ε_n jsou generátory cyklických podgrup v C_{p^∞}.

Je-li $n=0$, $m\in\mathbb{Z}$, pak $\varphi(\frac{m}{p^n})=\varphi(m)=1$, tedy $Ker\ \varphi\supseteq\mathbb{Z}$. Ukažte, že $Ker\ \varphi\subseteq\mathbb{Z}$.

(12) Ukažte, že znaménko součinu dvou permutací je rovno součinu znamének. Jádro tvoří permutace znaménka +1, tedy sudé permutace, t.j. A_n.

(13) Jako příklad (12).

(15) $\psi(a\cdot b)=\varphi_{ab}(x)$

$\varphi_{ab}(x)=(ab)^{-1}xab=b^{-1}a^{-1}xab$

$\varphi_a(x)\circ\varphi_b(x)=\varphi_b(\varphi_a(x))=\varphi_b(a^{-1}xa)=b^{-1}a^{-1}xab$, tedy $\varphi_{ab}=\varphi_a\circ\varphi_b$.

Je zřejmé že ψ je surjekce.

$\varphi_a(x)\in Ker\ \psi\Longleftrightarrow\varphi_a(x)=id$, tedy pro všechna $x\in G$: $a^{-1}\cdot x\cdot a=x$, t.j. $xa=ax$, tedy $a\in Z(G)$. Je tedy $Ker\ \psi=Z(G)$, $G/Z(G)\cong Int\ G$.

Buď G cyklická grupa řádu n, nechť a je generátor G. Je-li f izomorfismus G do G, pak

$f(a)=a^k$, $f(a^2)=a^{2k}, \ldots,$ $f(a^j)=a^{jk}$, t.j. obrazy prvků z G jsou mocniny prvku a^k. Musí tedy a^k být generátor G.

Je tedy izomorfismů tolik, kolik má G generátorů, t.j. číslo $\varphi(n)$ (počet čísel menších než n nesoudělných s n). Nekonečná cyklická grupa $(\mathbb{Z},+)$ má pouze dva izomorfismy do sebe: buď $1\longrightarrow 1$, pak je to identita, nebo $1\longrightarrow -1$, pak je to zobrazení $f(x)=-x$.

Uvažujme model zákrytových pohybů s prvky o_1, o_2, s, id. Zřejmě $o_1\circ o_1=o_2\circ o_2=s\circ s=id$, každý z prvků o_1, o_2, s je roven součinu zbylých dvou. Je-li tedy f izomorfismus na sebe, pak $f(id)=id$; ukažme, že na prvcích o_1, o_2, s může být f libovolná bijekce: označme $\{o_1, o_2, s\}=\{s_1, s_2, s_3\}$. Pak pro každou bijekci f platí:

pro $i\neq j$: $f(s_i\circ s_j)=f(s_k)=f(s_i)\circ f(s_j)$

pro $i=j$: $f(s_i\circ s_i)=f(id)=id=f(s_i)\circ f(s_i)$.

Je tedy množina všech izomorfismů do sebe izomorfní s grupou S_3.

18) Ukažte, že pro libovolné $q\in\mathbb{Q}$, $q\neq 0$, je zobrazení $f: x\longrightarrow qx$ izomorfismus do sebe.

Ukážeme, že jiné izomorfismy nejsou.

Je-li $f(1)=q$, pak pro libovolné $n\in\mathbb{N}$ platí

$$f(\underbrace{\frac{1}{n}+\frac{1}{n}+\ldots+\frac{1}{n}}_{n\text{-krát}})=nf(\frac{1}{n})=f(1)=q,$$

tedy $f(\frac{1}{n})=\frac{q}{n}$. Pak pro libovolné $m\in\mathbb{Z}$ platí

$f(\frac{m}{n})=mf(\frac{1}{n})=\frac{mq}{n}$, tedy $f(x)=qx$ pro každé $x\in\mathbb{Q}$.

19) (a), (c), (f) ANO

(b), (d), (e) NE

(20)(a) NE, kdyby $f:(\mathbb{Z},+)\longrightarrow(\mathbb{Q},+)$ byl surjektivní homomorfismus, pak $f(1)=\frac{m}{n}\neq 0$ (jinak by $f(x)=0$ pro každé $x\in\mathbb{Z}$).
Pak pro každé $k\in\mathbb{Z}$ je $f(k)=\frac{km}{n}$. Číslo $\frac{m}{2n}$ by nebylo obrazem žádného celého čísla.

(b) NE, kdyby $f:(\mathbb{Q},+)\longrightarrow(\mathbb{Z},+)$ byl surjektivní homomorfismus, pak pro nějaké $\frac{m}{n}\in\mathbb{Q}$ je $f(\frac{m}{n})=1$. Pak prvek $f(\frac{m}{2n})$ splňuje v $\mathbb{Z}$ rovnici $x+x=1$, spor.

(c) NE, kdyby $f:(\mathbb{Q},+)\longrightarrow(\mathbb{Q},\cdot)$ byl surjektivní homomorfismus, pak pro nějaké $\frac{m}{n}\in\mathbb{Q}$ je $f(\frac{m}{n})=2$. Pak prvek $f(\frac{m}{2n})$ splňuje v $(\mathbb{Q},\cdot)$ rovnici $x\cdot x=2$, spor.

(21)(a) ANO, buďte o_1,o_2,o_3 osové souměrnosti, r_1,r_2 rotace. Pak zobrazení $f:(\{o_1,o_2,o_3,r_1,r_2,id\},\circ)\longrightarrow(\{0,1\},+)$ takové, že
$f(id)=f(r_1)=f(r_2)=0$,
$f(o_1)=f(o_2)=f(o_3)=1$,
je surjektivní homomorfismus.

(b) NE, kdyby takový homomorfismus f existoval, bylo by jádro $Ker\ f$ normální podgrupou řádu 2, ale tu grupa zákrytových pohybů rovnostranného trojúhelníka nemá.

(22) Nechť G je abelovská. Buď $\langle g,g\rangle$ lib. prvek z $d(G)$, $\langle x,y\rangle$ libovolný prvek z $G\times G$. Pak $\langle x,y\rangle^{-1}\cdot\langle g,g\rangle\cdot\langle x,y\rangle=$
$=\langle x^{-1},y^{-1}\rangle\cdot\langle g,g\rangle\cdot\langle x,y\rangle=\langle x^{-1}gx,y^{-1}gy\rangle=\langle xx^{-1}g,y^{-1}yg\rangle=\langle g,g\rangle$, je tedy $d(G)$ normální podgrupa v $G\times G$.
Naopak, je-li $d(G)$ normální v $G\times G$, pak pro každé $x,y,g\in G$ existuje $g'\in G$ tak, že $x^{-1}gx=g'$, $y^{-1}gy=g'$, tedy $x^{-1}gx=y^{-1}gy$.
Zvolíme-li $g=y$, pak $x^{-1}yx=y$, tedy $xy=yx$ a G je abelovská.

(23) Nechť G je abelovská. Pak $m(\langle g_1,g'_1,g_2,g'_2\rangle)=g_1g'_1g_2g'_2=$
$=g_1g_2g'_1\ g'_2=m(\langle g_1,g_2\rangle)\ m(\langle g'_1,g'_2\rangle)$.
Naopak, je-li m homomorfismus, pak pro každé $g_1,g_2,g'_1,g'_2\in G$ platí $g_1g'_1g_2g'_2=g_1g_2g'_1g'_2$. Zvolíme-li $g_1=g'_2=e$, pak $g'_1g_2=g_2g'_1$, tedy G abelovská.

11. CYKLICKÉ GRUPY

Nechť $(G,\cdot)$ je grupa, $a\in G$. Množina všech mocnin $C(a)=\{a^n; n\in\mathbb{Z}\}$ je podgrupou grupy $(G,\cdot)$, tzv. <u>cyklická podgrupa grupy</u> $(G,\cdot)$ generovaná prvkem a.

Je-li dále b některý symbol, lze tvořit formální mocniny $\{\ldots,b^{-2},b^{-1},b^0,b,b^2,\ldots\}$.

Zavedeme-li operaci $\circ$ takto:

$$b^k\circ b^h=b^{k+h} \quad \text{pro } k,h\in\mathbb{Z},$$

je zřejmě množina všech formálních mocnin vzhledem k této operaci tvoří grupu, b^0 je její jednotka a prvek b^{-k} je inverzní k prvku b^k. Tato grupa se nazývá <u>cyklická grupa generovaná prvkem b</u>.

Je-li $(G,\cdot)$ cyklická grupa generovaná prvkem b a pro každé $m\in\mathbb{Z}$, $k\neq m$ je $b^k\neq b^m$, pak $(G,\cdot)$ je <u>nekonečná cyklická grupa</u>. Každá nekonečná cyklická grupa je izomorfní grupě $(\mathbb{Z},+)$, přičemž, je-li její generátor b, je tento izomorfismus dán vztahem

$$h(b^k)=k.$$

Speciálně, každé dvě nekonečné cyklické grupy jsou izomorfní.

Je-li $(G,\cdot)$ cyklická grupa generovaná prvkem b a existují-li $m\in\mathbb{Z}$, $k\neq m$ tak, že $b^k=b^m$, pak existuje nejmenší přirozené číslo n takové, že $b^n=b^0$, a tedy $(G,\cdot)$ je zřejmě konečná, a má řád n.

Každá konečná cyklická grupa řádu n je izomorfní grupě všech zbytkových tříd mod n, t.j. grupě $(\mathbb{Z}_n,+)$.

Je-li $(G,\cdot)$ grupa, $a\in G$, pak <u>řádem prvku a</u> rozumíme řád cyklické podgrupy $C(a)$.

<u>Příklady:</u>

(1) Dokažte, že homomorfní obraz cyklické grupy je cyklická grupa.

(2) Určete řády všech prvků grupy

	a_1	a_2	a_3	a_4	a_5	a_6
a_1	a_1	a_2	a_3	a_4	a_5	a_6
a_2	a_2	a_1	a_5	a_6	a_3	a_4
a_3	a_3	a_6	a_1	a_5	a_4	a_2
a_4	a_4	a_5	a_6	a_1	a_2	a_3
a_5	a_5	a_4	a_2	a_3	a_6	a_1
a_6	a_6	a_3	a_4	a_2	a_1	a_5

(3) Dokažte, že každá cyklická grupa je abelovská.

(4) Dokažte, že direktní součin cyklických grup je abelovská grupa. Je tato grupa cyklická?

(5) Určete řády prvků následující grupy a rozhodněte, zda je cyklická:

	1	a	ab	ab^2	b	b^2
1	1	a	ab	ab^2	b	b^2
a	a	1	b	b^2	ab	ab^2
ab	ab	b^2	1	b	ab^2	a
ab^2	ab^2	b	b^2	1	a	ab
b	b	ab^2	a	ab	b^2	1
b^2	b^2	ab	ab^2	a	1	b

(6) Nechť $(G,\cdot)$ je grupa řádu n. Dokažte, že $(G,\cdot)$ je cyklická, právě když v $(G,\cdot)$ existuje prvek řádu n.

(7) Dokažte, že pro každé $n\in\mathbb{N}$ existuje cyklická grupa řádu n.

(8) Nechť $C(g)$ je cyklická grupa řádu n, kde $n=m\cdot k$ $(m>1,\ k>1)$. Pak $C(g^m)$ je její podgrupa (jakého řádu?) a je normální(proč? Určete faktorovou grupu $C(g)/C(g^m)$. Je tato faktorová grup cyklická?

(9) Nechť r,s jsou nesoudělná přirozená čísla, $n=r\cdot s$. Pa cyklická grupa řádu n je izomorfní s $C_r\times C_s$, kde

resp. C_s je cyklická grupa řádu r resp. s.

(9) Dokažte, že direktní součin $\mathbb{Z}_2 \times \mathbb{Z}_2$ není izomorfní grupě $\mathbb{Z}_4$. Dokažte, že $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, určete tento izomorfismus!

(11) Určete všechny možné generátory grupy $\mathbb{Z}_6$.

(12) Ukažte, že každý prvek různý od jednotky je generátorem grupy $\mathbb{Z}_5$.

(13) Dokažte, že generátor grupy $(\mathbb{Z},+)$ může být pouze 1 nebo -1.

(14) Nechť $\mathbb{Z}_n$ je grupa zbytkových tříd mod n. Určete, které její prvky jsou její generátory.

(15) Dokažte, že v libovolné grupě mají prvky $a \cdot b$, $b \cdot a$ stejný řád.

(16) Dokažte, že v každé grupě mají prvky $a \cdot b \cdot c$, $b \cdot c \cdot a$, $c \cdot a \cdot b$ stejný řád.

(17) Označme C_{p^∞} množinu všech kořenů všech binomických rovnic $x^{p^n}-1=0$ (p je dané prvočíslo, $n=1,2,\ldots$) v $\mathbb{C}$. Dokažte, že C_{p^∞} (operace násobení) tvoří grupu. Tato grupa se nazývá tzv. kvazicyklická grupa typu p^∞.

(18) Najděte nekonečnou grupu, jejíž každý prvek je konečného řádu, a tedy každá její vlastní podgrupa je konečná.

(19) Určete všechny grupy řádu 6.

(20) Ukažte, že je-li v grupě G právě jeden prvek a řádu 2, pak $x \cdot a = a \cdot x$ pro každý prvek $x \in G$.

(21) Ukažte, že v cyklické grupě řádu n existuje jediná podgrupa řádu r pro každé $r|n$.

(22) Ukažte, že konečná grupa má právě tři různé podgrupy, právě když její řád je roven p^2, p je prvočíslo.

Návody k řešení:

(2) Prvek a_1 je jednotkou, je tedy řádu 1.
Prvek a_2 je řádu 2, generuje podgrupu $\{a_1, a_2\}$.

Prvek a_3 je řádu 2, generuje podgrupu $\{a_1, a_3\}$.
Prvek a_4 je řádu 2, generuje podgrupu $\{a_1, a_4\}$.
Prvky a_5, a_6 jsou řádu 3, každý z nich generuje podgrupu $\{a_1, a_5, a_6\}$.

(4) Jsou-li A, B cyklické grupy, $G=A\times B$, $x=\langle a_1, b_1\rangle$, $y=\langle a_2, b_2\rangle$, pak $x\cdot y=\langle a_1\cdot a_2, b_1\cdot b_2\rangle=\langle a_2\cdot a_1, b_2\cdot b_1\rangle=y\cdot x$, tedy G je abelovská. Tato grupa je cyklická, je-li alespoň jedna z grup A, B jednoprvková, nebo je-li každý prvek grupy A a každý prvek grupy B, různý od jednotky jejím generátorem (např. jsou-li A, B prvočíselného řádu).

(5) Prvek 1 je řádu 1

a	2
b	3
b^2	3
ab	2
ab^2	2

Grupa tedy není cyklická, nemá jediný generátor. Je však generovaná množinou $\{a, b\}$. Přesvědčte se!

(6) Existuje-li v $(G,\cdot)$ prvek g řádu n, pak g generuje n-prvkovou podgrupu grupy $(G,\cdot)$, ale $|G|=n$, tedy g je generátor G, tedy $(G,\cdot)=C(g)$. Obráceně, je-li $(G,\cdot)$ cyklická a g je její generátor, pak g je řádu n.

(7) Totiž $(\mathbb{Z}_n, +)$ (grupa zbytkových tříd mod n).

(8) Řád $C(g^m)$ je k, je normální, neboť $C(g)$ je abelovská. Dále, $C(g)/C(g^m)\cong C(g^k)$, je to tedy cyklická grupa řádu k.

(9) Stačí ukázat, že pro $n=r\cdot s$, r, s nesoudělné, $\mathbb{Z}_n\cong\mathbb{Z}_r\times\mathbb{Z}_s$, tedy že $\mathbb{Z}_r\times\mathbb{Z}_s$ je cyklická grupa. Ukážeme, že $(\bar{1}_r, \bar{1}_s)$ generuje $\mathbb{Z}_r\times\mathbb{Z}_s$. Buďte $\bar{m}\in\mathbb{Z}_r$, $\bar{n}\in\mathbb{Z}_s$ libovolné. Stačí ukázat existenci $k\in\mathbb{Z}$ tak, že

$\bar{k}\cdot\bar{1}=\bar{m}$ v $\mathbb{Z}_r$ a $\overline{k\cdot 1}=\bar{n}$ v $\mathbb{Z}_s$, tedy $k=m+xr$ pro nějaké $x\in\mathbb{Z}$, $k=n+ys$ pro nějaké $y\in\mathbb{Z}$,

tedy $m-n=ys-xr$ pro nějaké $x, y\in\mathbb{Z}$.

Taková x,y však vždy existují, neboť největší společný dělitel r,s je roven 1 (existují $x',y'\in\mathbb{Z}$ tak, že $x'r+y's=\mathrm{NSD}(r,s)$, vynásobením číslem $m-n$ dostaneme požadované prvky x,y).

9) $\mathbb{Z}_2\times\mathbb{Z}_2$ je izomorfní Kleinově čtyřprvkové grupě, která není izomorfní grupě $\mathbb{Z}_4$.

11) $\{\bar{1}\}$, $\{\bar{5}\}$, $\{\bar{2},\bar{3}\}$.

12) Vyjděte z toho, že $\mathbb{Z}_5$ je prvočíselného řádu, tedy je cyklická.

13) Číslo 1 není celým násobkem žádného celého čísla různého od ± 1.

14) Jsou to právě prvky $\bar{m}$, $m<n$, m nesoudělné s n.

15) Buďte $a,b\in G$ libovolné, nechť $a\cdot b$ má řád n. Ukažme nejprve, že $(b\cdot a)^n=e$:

$(b\cdot a)^n=b\cdot(a\cdot b)^{n-1}\cdot a$,

$(a\cdot b)^n=e$, tedy $(a\cdot b)^{n-1}=b^{-1}\cdot a^{-1}$, tedy po dosazení

$(b\cdot a)^n=b\cdot b^{-1}\cdot a^{-1}\cdot a=e$.

Zbývá ukázat, že n je nejmenší přirozené číslo této vlastnosti. Kdyby tomu tak nebylo, pak by existovalo $n'\in\mathbb{N}$, $n'<n$, $(b\cdot a)^{n'}=e$. Stejným postupem bychom odvodili, že pak $(a\cdot b)^{n'}=e$, tj. spor s řádem prvku $a\cdot b$. Mají tedy $a\cdot b$ a $b\cdot a$ stejný řád.

16) Podle (15) mají prvky $a\cdot(b\cdot c)$ a $(b\cdot c)\cdot a$ stejný řád a také prvky $b\cdot(c\cdot a)$ a $(c\cdot a)\cdot b$ mají stejný řád, tedy všechny tři mají stejný řád.

18) Je to například grupa C_{p^∞} z příkladu (17).

19) Obsahuje-li tato grupa prvek řádu 6, je cyklická. Neobsahuje-li prvek řádu 6, musí obsahovat prvky řádů 2 a 3. Je-li $a^2=e$ (tj. a je řádu 2) a $b^3=e$ (tj. b je řádu 3), pak tato grupa je rovna grupě z příkladu (5). Jiné grupy řádu 6 už zřejmě neexistují, tedy tato grupa je izomorfní s S_3.

(20) Kdyby existoval prvek $x \in G$ tak, že $x \cdot a \neq a \cdot x$, pak $x^{-1} \cdot a \cdot x \neq a$, a přitom $(x^{-1}ax)^2 = x^{-1}aax = x^{-1}ex = e$, což je spor.

(21) Je-li $n = r \cdot s$, pak je-li a generátor grupy G, je prvek a^s generátor cyklické podgrupy řádu r.

Buď a^m, $m \in \mathbb{N}$, generátor cyklické podgrupy řádu r v G. Pak je $(a^m)^r = a^{m \cdot r} = e$. Jelikož a je generátor grupy G řádu n, platí $n | m \cdot r$, odkud $s \cdot r | m \cdot r$, tedy $m = s \cdot k$ pro nějaké $k \in \mathbb{N}$. Pak ovšem máme $C(a^s) \subseteq C(a^m)$ a jelikož tyto grupy jsou stejných řádů, platí $C(a^s) = C(a^m)$. Cyklická podgrupa řádu r je v G tedy jediná.

(22) Je-li grupa G řádu p^2, p prvočíslo, má právě jednu podgrupu řádu p. Má tedy celkem tři podgrupy (dvě nevlastní).

Je-li řád grupy prvočíslo, má právě dvě podgrupy. Je-li řád n grupy G číslo složené, které není kvadrátem prvočísla, pak existují alespoň dvě různá prvočísla p_1, p_2 taková, že $p_1, p_2 | n$. Pak ale má alespoň jednu podgrupu řádu p_1 i p_2, má tedy alespoň čtyři podgrupy.

12. PERMUTAČNÍ GRUPY

Nechť $\{1,2,\ldots,n\}$ je n-prvková množina. Množinu všech permutací n-prvkové množiny nazveme <u>symetrická grupa n prvků</u> a označíme ji S_n. Zřejmě S_n má řád $n!$. Její podgrupu všech sudých permutací označíme A_n a nazveme <u>alternující grupa n prvků</u>. Zřejmě řád A_n je $\frac{n!}{2}$. Každou podgrupu grupy S_n nazveme <u>permutační grupa</u>. Dle Cayleyovy věty je každá grupa řádu n izomorfní některé permutační grupě, která je podgrupou grupy S_n.

<u>Příklady</u>:

(1) Určete faktorovou grupu S_n/A_n.

(2) Určete všechny podgrupy S_3. Které z nich jsou normální? Utvořte faktorovou grupu S_3/H podle nalezené normální podgrupy H.

(3) Určete permutační grupu, izomorfní Kleinově čtyřprvkové grupě.

(4) Najděte 4 různé podgrupy symetrické grupy S_4, které jsou izomorfní s S_3.

(5) Nechť $\pi \in S_n$, a nechť

$$\pi = p_1 \cdot p_2 \cdot \ldots \cdot p_r,$$

kde p_i jsou nezávislé cykly. Dokažte, že řád prvku π v grupě S_n je roven nejmenšímu společnému násobku délek cyklů $p_1, p_2, \ldots, p_r$.

(6) Dokažte, že Kleinova grupa K je normální podgrupou v S_4 (přesněji její izomorfní reprezentace-příklad (3)), a určete S_4/K.

(7) Najděte třídy navzájem konjugovaných prvků v S_3, S_4.

(8) Ukažte, že každá grupa S_n má pouze jedinou podgrupu indexu 2.

(9) Ukažte, že je-li s cyklus délky n, t transpozice, pak $t \circ s \circ t^{-1} = t \circ s \circ t$ je cyklus délky n.

(10) Najděte v S_n dva prvky konjugované, které nejsou konjugované v A_n.

Návody k řešení:

(1) S_n/A_n je izomorfní dvouprvkové (a tedy cyklické) grupě.

(2) S_3 má 3 podgrupy řádu 2, žádná z nich není normální, a grupu A_3, která je normální. S_3/A_3-viz. příklad (1).

(3) Kleinova grupa má 4 prvky, budeme tedy dle Cayleyovy věty hledat její reprezentaci mezi permutacemi na čtyřprvkové množině. Označme e identickou permutaci, a dále, nechť jsou permutace a,b,c určeny transpozicemi:
$a=(12)(34)$, $b=(13)(24)$, $c=(14)(23)$.
Pak si ověřte, že $\{e,a,b,c\}$ je Kleinova grupa.

(5) Ukažte, že řád každého cyklu je roven jeho délce. Jelikož cykly jsou nezávislé, je řád prvku roven nejmenšímu společnému násobku řádů cyklů.

(6) Buď $x=\begin{pmatrix} 1 & 2 & 3 & 4 \\ h_1 & h_2 & h_3 & h_4 \end{pmatrix}$ libovolná permutace z S_4.

Pak $x^{-1}=\begin{pmatrix} 1 & 2 & 3 & 4 \\ h_1 & h_2 & h_3 & h_4 \end{pmatrix}^{-1} = \begin{pmatrix} h_1 & h_2 & h_3 & h_4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ (ověřte!). Buď nyní $a=(13)(24)$. Pak platí:

$$x^{-1} \circ a \circ x = \begin{pmatrix} h_1 & h_2 & h_3 & h_4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ h_1 & h_2 & h_3 & h_4 \end{pmatrix} =$$

$=(h_1 h_3) \circ (h_2 h_4) \in K$.

Podobně dokažte, že pro všechny zbývající prvky $a \in K$ platí $x^{-1} \circ a \circ x \in K$. Ukažte, že $S_4/K \cong S_3$.

7) S_3: $\{id\}$, $\{(12),(13),(23)\}$, $\{(123),(132)\}$

S_4: $\{id\}$, třída obsahující šest transpozic (ab),
třída obsahující osm cyklů (abc),
třída obsahující tři permutace tvaru $(ab)\circ(cd)$
třída obsahující šest cyklů $(abcd)$.

8) A_n je podgrupa indexu 2. Kdyby G byla podgrupa S_n indexu 2, $G\neq A_n$, pak $G\cap A_n$ by byla normální podgrupa v S_n (dokažte!), a i vlastní normální podgrupou v A_n. Pro $n>5$ je A_n jednoduchá. Rozeberte případy pro $n\leq 4$.

9) Nejprve je třeba si uvědomit, že $(ab)^{-1}=(ab)$.
Uvažujme tři případy:

1) cyklus a transpozice jsou nezávislé. Pak $(a_1a_2)\circ(a_3a_4\ldots)\circ(a_1a_2)=(a_3a_4a_5\ldots)$, neboť skládání je komutativní.

2) cyklus a transpozice mají jeden společný prvek. Pak $(a_1a_2)\circ(a_1a_3a_4\ldots)(a_1a_2)=(a_2a_3a_4\ldots)$.

3) cyklus a transpozice mají dva společné prvky. Pak $(a_ia_j)\circ(a_1a_2\ldots a_j\ldots a_i\ldots)\circ(a_ia_j)=(a_1a_2\ldots a_i\ldots a_j\ldots)=$ cyklus vzniklý záměnou z původního prvků a_i, a_j.

(10) Zvolme například $n=5$, $s=(12345)$, $t=(13245)$.
Prvek s je konjugovaný s t, neboť $s=(23)\circ t\circ(23)$.
Kdyby s a t byly konjugované v A_5, pak $s=n\circ t\circ n^{-1}$, kde $n\in A_n$.
Označíme-li $w=n\circ(23)$, pak $s=w\circ s\circ w^{-1}$. Rozložíme-li w na součin transpozic, je jich lichý počet (neboť n je sudá permutace). Díky předchozímu příkladu prvek konjugovaný s prvkem s pomocí transpozice je cyklus vzniklý z prvku s záměnou dvou prvků. Avšak výraz $w\circ s\circ w^{-1}$ vznikne lichým počtem transpozic (neboť počet transpozic ve w je lichý), což je spor.

13. VNOŘENÍ POLOGRUP DO GRUP

Injektivní homomorfismus h pologrupy $(S,\cdot)$ do pologrupy $(G,\cdot)$ nazveme <u>vnoření</u>. Je-li navíc $(G,\cdot)$ grupa, řekneme, že h je <u>vnoření pologrupy</u> $(S,\cdot)$ <u>do grupy</u> $(G,\cdot)$.

Je-li $(S,\cdot)$ komutativní pologrupa s krácením, pak existuje grupa $(G,\cdot)$ a vnoření h pologrupy $(S,\cdot)$ do $(G,\cdot)$. V tomto případě lze položit

$$(G,\cdot)\cong((S,\cdot)\times(S,\cdot))/\theta,$$

$$\text{kde } \langle\langle a,b\rangle,\langle c,d\rangle\rangle\in\theta \iff a\cdot d=b\cdot c.$$

<u>Příklady</u>:

(1) Je-li pologrupa $(S,\cdot)$ konečná, pak je to pologrupa s krácením, právě když v každém řádku a každém sloupci je každý prvek nejvýše (a tedy právě) jedenkrát. Dokažte!

(2) Ukažte, že pologrupy $(\mathbb{N},+)$ a $(\mathbb{N},\cdot)$ jsou pologrupy s krácením.

(3) Dokažte, že pologrupu $(\mathbb{N},+)$ lze vnořit do $(\mathbb{Z},+)$, přičemž toto vnoření je identické zobrazení a tato grupa je nejmenší grupou této vlastnosti.

(4) Ukažte, že nejmenší grupa $(G,+)$, do které by bylo možno vnořit $(\mathbb{N},+)$, je izomorfní s $(\mathbb{Z},+)$.

(5) Ukažte, že zobrazení $f(x)=3x$ je vnoření pologrupy $(\mathbb{N},+)$ do grupy všech násobků trojky, t.j. $\{3\cdot k;\ k\in\mathbb{Z}\}$.

(6) Ukažte konstrukci, jak lze vnořit $(\mathbb{N},\cdot)$ do grupy $(\mathbb{Q}_+,\cdot)$ všech kladných racionálních čísel.

(7) Dokažte, že vnoření $(\mathbb{N},\cdot)$ do $(\mathbb{Q}_+,\cdot)$ lze realizovat homomorfismem $f(k)=\frac{k}{1}$, t.j. identickým zobrazením.

II. ČÁST : OKRUHY, TĚLESA, POLYNOMY, KOŘENY POLYNOMŮ

14. OKRUHY, OBORY INTEGRITY, TĚLESA

Nechť $A \neq \emptyset$ je množina, $+, \cdot$ jsou binární operace na A. Trojici $(A,+,\cdot)$ nazveme okruh , jestliže $(A,+)$ je abelovská grupa, $(A,\cdot)$ je pologrupa a operace $+, \cdot$ jsou spolu vázány distributivními zákony :

$$a\cdot(b+c) = a\cdot b + a\cdot c$$
$$(b+c)\cdot a = b\cdot a + c\cdot a$$

pro každé $a,b,c\in A$. Operaci $\cdot$ často nevyznačujeme, místo $a\cdot b$ píšeme jen ab. Okruh R nazveme komutativní, jestliže $ab = ba$ pro každé $a,b \in A$. Okruh R nazveme unitární, má-li pologrupa $(A,\cdot)$ jednotku ; tuto jednotku označíme 1 a nazveme jednotka okruhu R. Jednotku tzv. aditivní grupy $(A,+)$ okruhu R označíme 0 a nazveme nula okruhu R.

Nechť $R=(A,+,\cdot)$ je okruh, $\emptyset\neq B\subseteq A$. Nazveme B podokruh okruhu R, je-li $(B,+,\cdot)$ opět okruhem, přičemž operace $+, \cdot$ jsou tytéž jako v R, tentokrát ale pouze pro prvky z B.

Jsou-li $R_i=(A_i,+,\cdot)$, $(i\in I)$, okruhy, pak na kartézském součinu množin A_i lze zavést operace „po souřadnicích". Kartézský součin $\Pi\{A_i; i\in I\}$ spolu s takto zavedenými operacemi nazýváme direktní součin okruhů R_i a označujeme symbolem $\Pi\{R_i; i\in I\}$. Speciálně, je-li I konečná množina, např. $I=\{1,2,\ldots,n\}$, pak tento direktní součin zapisujeme $R_1\times R_2\times\ldots\times R_n$. Je-li pro každé $i=1,2,\ldots,n$ $R_1=R_2=\ldots=R_n=R$, pak místo $R_1\times R_2\times\ldots\times R_n$ zapisujeme stručně R^n.

Nechť $R=(A,+,\cdot)$ je okruh , $a,b\in A$, $a\neq 0\neq b$. Prvky a,b nazveme dělitelé nuly, jestliže $a\cdot b=0$. Okruh R je bez dělitelů nuly, jestliže pro každé $a,b\in A$ s vlastností $a\cdot b=0$ platí buď $a=0$ nebo $b=0$.

Komutativní unitární okruh bez dělitelů nuly se nazývá obor integrity.

Jestliže v okruhu $R=(A,+,\cdot)$ tvoří množina všech nenulových prvků grupu vzhledem k násobení, t.j. $(A\setminus\{0\},\cdot)$ je grupa, pak se R nazývá těleso. Podtělesem nazýváme takový podokruh tělesa, který je sám tělesem.

V celé II. části budeme symboly $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ označovat množinu všech čísel přirozených resp. celých resp. racionálních resp. reálných resp. komplexních. Symbolem $\mathbb{Z}_n$ označíme množinu všech zbytkových tříd *mod n*.

<u>Příklady :</u>

(1) Dokažte, že $(\mathbb{Z},+,\cdot),(\mathbb{R},+,\cdot),(\mathbb{Q},+,\cdot),(\mathbb{C},+,\cdot)$ jsou okruhy. $(\mathbb{N},+,\cdot)$ není okruh.

Dokažte, že $(\mathbb{Z}_n,+,\cdot)$, kde $+$ resp. $\cdot$ jsou operace sčítání resp. násobení *mod n*, jsou okruhy pro každé $n\in\mathbb{N}$; tyto okruhy nazýváme <u>okruhy zbytkových tříd</u> *mod n*. V dalších příkladech budeme tyto okruhy označovat stručně $\mathbb{Z}_n$.

(2) Které z následujících trojic jsou okruhy ? :

(a) $(\{a+b\sqrt{2};\ a,b\in\mathbb{Z}\},+,\cdot)$

(b) $(\{\frac{a}{2^k}\ ;\ a\in\mathbb{Z},\ k\in\mathbb{Z},k\geq 0\},+,\cdot)$

(c) $(\{a+b\sqrt[3]{2}\ ;\ a,b\in\mathbb{Z}\},+,\cdot)$.

(3) Dokažte, že množina všech čtvercových matic typu $n\times n$ nad $\mathbb{Z}$ (resp. nad $\mathbb{Q}$, resp. nad $\mathbb{R}$, resp. nad $\mathbb{C}$) tvoří okruh vzhledem k maticovému sčítání a maticovému násobení.

(4) Buď F množina všech funkcí splňující danou (níže) podmínku a definovaných na intervalu $\langle 0,1\rangle$. Nechť $+,\cdot$ je sčítání resp. násobení funkcí. Které z nich tvoří okruh ?:

(a) F jsou ohraničené funkce

(b) F jsou funkce splňující $f(\frac{1}{2})=0$

(c) F jsou funkce splňující $f(0)=f(1)$

(d) F jsou polynomy.

(5) Nechť G je množina všech funkcí na $\langle 0,1\rangle$, $+$ je sčítání funkcí, pro $f,g\in G$ položme za $f\circ g$ složenou funkci. Dokažte, že $(G,+,\circ)$ není okruh.

(6) Existuje okruh $(M,+,\cdot)$ a prvek $a\in M$ tak, že $M\setminus\{a\}$ je jeho podokruh ?

(7) Nechť $k\in\mathbb{N}$ a nechť $Z(k)=\{\ \frac{m}{n};\ n\in\mathbb{Z}\setminus\{0\}, m\in\mathbb{Z}$ a k nedělí $m\ \}$. Pro která k je $(Z(k),+,\cdot)$ okruh ?

(8) Najděte okruh S a jeho podokruh P tak, že P nemá dělitele nuly, ale S má dělitele nuly, přičemž $P\neq\emptyset$.

(9) Nechť P je podokruh okruhu S, $a\in P$ a nechť a je dělitel nuly v S. Plyne odtud, že a je dělitel nuly v P ?

(10) Které z následujících okruhů mají dělitele nuly ? :

(a) okruh ohraničených funkcí na $\langle 0,1\rangle$

(b) okruh matic $\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix};\ a,b\in\mathbb{R}\right\}$

(operace maticové sčítání a maticové násobení)

(c) Okruh matic $\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix}\ ;\ a,b\in\mathbb{R}\ \right\}$

(d) Direktní součin $(D,+,\cdot)\times(D,+,\cdot)$, kde $(D,+,\cdot)$ je obor integrity.

(11) Nechť F_Q je množina všech cauchyovských posloupností (a_k) $(k=0,1,\ldots)$, kde $a_k\in\mathbb{Q}$ pro každé $k=0,1,\ldots$. Definujeme

$$(a_k)+(b_k)=(a_k+b_k)$$
$$(a_k)\cdot(b_k)=(a_k\cdot b_k).$$

Dokažte, že $(F_Q,+,\cdot)$ je okruh.

(12) V okruhu $\mathbb{Z}_{10}$ označme $D_1=\{\bar{0},\bar{5}\}, D_2=\{\bar{0},\bar{2},\bar{4},\bar{6},\bar{8}\}$. Dokažte, že D_1, D_2 jsou podokruhy $\mathbb{Z}_{10}$, které jsou obory integrity. Dále dokažte, že každý prvek $a\in\mathbb{Z}_{10}$ lze psát ve tvaru $a=a_1+a_2$, kde $a_1\in D_1, a_2\in D_2$.

(13) Je $(\{a,b,c,d\},+,\cdot)$ okruh pro

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

·	a	b	c	d
a	a	a	a	a
b	a	b	a	b
c	a	c	a	c
d	a	d	a	d

?

(14) Ukažte, že $(\{a,b\},+,\cdot)$, kde

+	a	b
a	a	b
b	b	a

·	a	b
a	a	a
b	a	b

je okruh. Je tento okruh těleso?

(15) Dokažte, že v každém okruhu platí:

$$0\cdot a=a\cdot 0 \quad ; \quad -(-a)=a \quad ; \quad a\cdot(-b)=(-a)\cdot b=-(ab).$$

(16) Na množině $M=\{\langle a,b,c,d\rangle;\ a,b,c,d\in\mathbb{Q}\}$ definujeme operace

$$\langle a,b,c,d\rangle+\langle e,f,g,h\rangle=\langle a+e,b+f,c+g,d+h\rangle$$

$$\langle a,b,c,d\rangle\cdot\langle e,f,g,h\rangle=\langle a\cdot e+b\cdot g,a\cdot f+b\cdot h,c\cdot e+d\cdot g,c\cdot f+d\cdot h\rangle.$$

Dokažte, že $(M,+,\cdot)$ je okruh.

(17) Dokažte, že $P=\{\langle a,b,-b,-a\rangle;\ a,b\in\mathbb{Q}\}$ je komutativní podokruh okruhu $(M,+,\cdot)$ z příkladu (16).

(18) Nechť $+,\cdot$ jsou aritmetické operace celých čísel. Dokažte, že vzhledem k těmto operacím

(a) $\{2k;\ k\in\mathbb{Z}\}$ je okruh

(b) $\{2k+1;\ k\in\mathbb{Z}\}$ není okruh.

(19) Položme $a\oplus b=a+b+1$, $a\odot b=a+b+ab$. Dokažte, že $(\mathbb{R},\oplus,\odot)$ je okruh.

(20) Dokažte, že $S=\{\langle a,b,-b,a\rangle;\ a,b\in\mathbb{Q}\}$ je podokruh okruhu $(M,+,\cdot)$ z příkladu (16). Je tento okruh tělesem?

(21) Doplňte tabulku tak, aby $(\{a,b,c,d\},+,\cdot)$ byl okruh:

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

·	a	b	c	d
a	a	a	a	a
b	a	b	·	·
c	a	·	·	c
d	a	b	c	·

(22) Ukažte, že $(P,+,\cdot)$ pro $P=\{\langle a,b,-b,a\rangle;\ a,b\in\mathbb{R}\}$, kde

$$\langle a,b,-b,a\rangle+\langle c,d,-d,c\rangle=\langle a+c,b+d,-b-d,a+c\rangle$$

$$\langle a,b,-b,a\rangle\cdot\langle c,d,-d,c\rangle=\langle ac-bd,ad+bc,-ad-bc,ac-bd\rangle,$$

je těleso. Toto těleso je izomorfní s tělesem komplex. čísel $\mathbb{C}$.

(23) Ukažte, že v okruhu $\mathbb{Z}_{15}$ jsou $S=\{\overline{0},\overline{5},\overline{10}\}$ a $T=\{\overline{0},\overline{3},\overline{6},\overline{9},\overline{12}\}$ podokruhy. $\mathbb{Z}_{15}$ není těleso, ale S,T jsou tělesa. Dokažte!

(24) Na množině $\mathbb{R}\times\mathbb{Z}$ definujeme operace $\oplus,\odot$ takto:

$$\langle a,r\rangle\oplus\langle b,s\rangle=\langle a+b,r+s\rangle$$

$$\langle a,r\rangle\odot\langle b,s\rangle=\langle ab+rb+sa,rs\rangle.$$

(a) Dokažte, že $(\mathbb{R}\times\mathbb{Z},\oplus,\odot)$ je okruh;

(b) Ukažte, že $\langle 0,0\rangle$ je nula a $\langle 0,1\rangle$ je jednotka tohoto okruhu.

(25) Nechť a je prvek okruhu $(P,+,\cdot)$. Dokažte, že prvky $1,a,a^2,\ldots$ tvoří aritmetickou posloupnost právě tehdy, když $(a-1)^2=0$.

(26) Na množině $\mathbb{Q}\times\mathbb{Q}$ definujeme $\langle a,b\rangle\oplus\langle c,d\rangle=\langle a+c,b+d\rangle$
$\langle a,b\rangle\odot\langle c,d\rangle=\langle ac+2bd,ad+ba\rangle$.

Je $(\mathbb{Q}\times\mathbb{Q},\oplus,\odot)$ těleso?

(27) Které z následujících množin čísel tvoří těleso vzhledem k aritmetickým operacím $+,\cdot$?

(a) $\{a+b\sqrt{3};\ a,b\in\mathbb{Q}\}$
(b) $\{a+b\sqrt[3]{3};\ a,b\in\mathbb{Q}\}$
(c) $\{a+b\sqrt[3]{3}+c\sqrt[3]{9};\ a,b,c\in\mathbb{Q}\}$
(d) $\{a+b\sqrt{2};\ a,b\in\mathbb{Q}\}$
(e) $\{a\in\mathbb{Q};\ a>0\}$
(f) $\{a\in\mathbb{Q};\ a<0\}$
(g) $\{a\in\mathbb{Q};\ a\leq 0\}$
(h) $\{a+b;\ a,b\in\mathbb{Q}\}$
(i) $\{a+bi;\ a,b\in\mathbb{R},b\geq 0\}$ (i je imaginární jednotka)
(j) $\{a+bi\sqrt{2};\ a,b\in\mathbb{Q}\}$.

(28) Které je nejmenší těleso T obsahující $\mathbb{Q}$ a prvek $c\notin\mathbb{Q}$?:

(a) pro $c=\sqrt{3}$
(b) pro $c=\sqrt[3]{2}$
(c) pro $c=1+\sqrt{2}$.

(29) Dokažte, že každý konečný obor integrity je tělesem.

(30) Nechť $A\neq\emptyset$, na Exp A definujme operace

$$X+Y=(X\setminus Y)\cup(Y\setminus X)\ ,\quad X\cdot Y=X\cap Y.$$

Dokažte, že (Exp $A,+,\cdot$) je okruh. Co je nulou tohoto okruhu? Má tento okruh dělitele nuly?

(31) Ukažte, že množina $\{0,1\}\times\{0,1\}$, ve které je sčítání definované *mod* 2 po souřadnicích a násobení je definované předpisem

$$\langle x,y\rangle\cdot\langle u,v\rangle=\langle xu+yv,xv+yu+yv\rangle,$$

tvoří čtyřprvkové těleso.

(32) Nechť $\mathbb{R}$ je množina všech reálných čísel, definujme na $\mathbb{R}\times\mathbb{R}$ operace $\oplus,\odot$ takto :

(a) $\langle a,b\rangle\oplus\langle c,d\rangle=\langle ac,bc+d\rangle$, $\langle a,b\rangle\odot\langle c,d\rangle=\langle ac,bd\rangle$

(b) $\langle a,b\rangle\oplus\langle c,d\rangle=\langle a+c,b+d\rangle$, $\langle a,b\rangle\odot\langle c,d\rangle=\langle ac+bc,ad+bd\rangle$

(c) $\langle a,b\rangle\oplus\langle c,d\rangle=\langle ad+bc,bd\rangle$, $\langle a,b\rangle\odot\langle c,d\rangle=\langle ac,bd\rangle$.

Je v některém z těchto případů $(\mathbb{R}\times\mathbb{R},\oplus,\odot)$ okruh?

(33) Dokažte, že v každém okruhu platí:

$$(a+b)\cdot(c+d)=ac+bc+ad+bd,$$
$$-(abc)=(-a)\cdot(-b)\cdot(-c).$$

(34) Dokažte, že v komutativním okruhu platí:

$$(a+b)^2= a^2+2\times ab+b^2.$$

(35) Nechť $R=(A,+,\cdot)$ je okruh, $Z(A)=\{c\in A;\ cx=xc$ pro každé $x\in A\}$. Dokažte, že $Z(A)$ je podokruh okruhu R (tento podokruh se nazývá <u>centrum</u> okruhu R).

(36) Nechť $(T,+,\cdot)$ je těleso, $\alpha,\beta\in T$, $\alpha\neq\beta$. Definujme operace $\oplus,\odot$ na množině T takto:

$$a\oplus b = a+b-\alpha$$
$$a\odot b = \frac{(a-\alpha)\cdot(b-\beta)}{\beta-\alpha} + \alpha.$$

Je $(T,\oplus,\odot)$ těleso? Kdy je toto těleso komutativní?

(37) Uvažujme množinu $\bar{Q}=\{\langle z_1,z_2,-\bar{z}_2,\bar{z}_1\rangle;\ z_1,z_2\in\mathbb{C}\}$ s operacemi

$$\langle z_1,z_2,-\bar{z}_2,\bar{z}_1\rangle\oplus\langle z'_1,z'_2,-\bar{z}'_2,\bar{z}'_1\rangle=\langle z_1+z'_1,z_2+z'_2,-\bar{z}_2-\bar{z}'_2,\bar{z}_1+\bar{z}'_1\rangle ,$$

$$\langle z_1,z_2,-\bar{z}_2,\bar{z}_1\rangle\odot\langle z'_1,z'_2,-\bar{z}'_2,\bar{z}'_1\rangle=$$
$$=\langle z_1z'_1+z_2z'_2,z_1z'_2+z_2\bar{z}'_1,-\bar{z}_2z'_1-\bar{z}_1\bar{z}'_2,\bar{z}_2\bar{z}'_2+\bar{z}_1\bar{z}'_1\rangle.$$

Ukažte, že je to nekomutativní okruh s jednotkou $\langle 1,0,0,1\rangle$, kde k prvku $\langle z_1,z_2,-\bar{z}_2,\bar{z}_1\rangle$ je inverzní $\langle\frac{\bar{z}_1}{\Delta},-\frac{z_2}{\Delta},\frac{\bar{z}_2}{\Delta},\frac{z_1}{\Delta}\rangle$, kde $\Delta=|z_1|^2+|z_2|^2$.

<u>Návody k řešení :</u>

(2) (a),(b) Ano

(c) Ne, neboť $(a+b\sqrt[3]{2})\cdot(c+d\sqrt[3]{2})=ac+(bc+ad)\sqrt[3]{2}+bd\sqrt[3]{4}$ obecně nepatří do této množiny.

(4) (a) Ano, ukažte, že součet a součin ohraničených funkcí je ohraničená funkce.

(b) Ano, stačí ověřit uzavřenost operací a existenci inverzního prvku pro sčítání:

nechť $f,g\in F$; pak $f(\frac{1}{2})+g(\frac{1}{2})=0+0=0=(f+g)(\frac{1}{2})$,

$f(\frac{1}{2})\cdot g(\frac{1}{2})=0\cdot 0=0=(f\cdot g)(\frac{1}{2})$,

$(-f)(\frac{1}{2})=-f(\frac{1}{2})=-0=0$.

(c) Ano, jsou-li $f,g\in F$, pak

$(f+g)(0)=f(0)+g(0)=f(1)+g(1)=(f+g)(1)$;

analogicky pro součin.

(d) Ano.

(5) Položme $f(x)=x^2$, $g(x)=h(x)\equiv 1$, $x\in\langle 0,1\rangle$.

Pak $(g+h)\circ f=f(g+h)\equiv f(2)=4$,

$g\circ f+h\circ f=f(1)+f(1)=2$, neplatí distributivní zákon.

(6) Ano, např. $M=\mathbb{Z}_2$, $a=1$.

(7) k musí být prvočíslo:

$\frac{m}{n}+\frac{m'}{n'}=\frac{mn'+m'n}{n\cdot n'}$; je-li k prvočíslo, pak $k|n\cdot n'\Rightarrow k|n$ nebo $k|n'$ (proč?); je-li k složené, pak implikace nemusí platit a + nemusí být operace na $Z(k)$.

(8) Stačí vzít např. $S=(\mathbb{Z},+,\cdot)\times(\mathbb{Z},+,\cdot)$, $P=(\mathbb{Z},+,\cdot)\times(\{0\},+,\cdot)$.

(9) Ne. Stačí uvažovat $P=(\{\bar{0},\bar{3}\},+,\cdot)$, $a=\bar{3}$, $S=(\mathbb{Z}_6,+,\cdot)$.

(10) (a) Ano, např. $f(x)=sgn(x)$, $g(x)=sgn(-x)$, atd. Každá funkce, která se anuluje v aspoň jednom bodě a není nulová, je dělitel nuly.

(b) Ano, jsou to právě matice $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$.

(c) Ne, neboť $a^2+b^2=0$, právě když $a=b=0$.

(d) Ano, je-li 1 jednotka v D, pak $(1,0),(0,1)$ jsou dělitelé nuly.

(11) Využijte definice cauchyovské posloupnosti a známých postupů z teorie posloupností.

(12) V okruhu D_1 by mohl být dělitelem nuly pouze prvek $\bar{5}$, ale $\bar{5}\cdot\bar{5}=\bar{5}$, tedy $\bar{5}$ není dělitel nuly. Podobně prověřte pro D_2.

(13) Ano, ověřte všechny axiomy!

(14) Okruh je tělesem.

(15) $a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0$, tedy $-(a\cdot 0)+a\cdot 0=-(a\cdot 0)+a\cdot 0+a\cdot 0$, t.j. $a\cdot 0=0$.
Dále, $a\cdot(-b)+a\cdot b=a\cdot(-b+b)=a\cdot 0=0$, tedy $a\cdot(-b)=-(ab)$, podobně pro zbylé případy.

(18) **(b)** Neplatí uzavřenost vzhledem ke sčítání.

(19) Je-li $(\mathbb{R},+,\cdot)$ těleso reálných čísel, ukažte, že zobrazení $f:(\mathbb{R},+,\cdot)\longrightarrow(\mathbb{R},\oplus,\odot)$ takové, že $f(a)=a-1$, je izomorfismus. Je tedy $(\mathbb{R},\oplus,\odot)$ dokonce těleso.

(21) $c\cdot b=(b+d)\cdot b=b\cdot b+d\cdot b=b+b=a$
$c\cdot c=c\cdot(b+d)=c\cdot b+c\cdot d=a+c=c$
$d\cdot d=d\cdot(c+b)=d\cdot c+d\cdot b=c+b=d$
$b\cdot c=(c+d)\cdot c=c\cdot c+d\cdot c=c+c=a$
$b\cdot d=b\cdot(b+c)=b\cdot b+b\cdot c=b+a=b$.

(22) Ukažte, že zobrazení $f:(\mathbb{C},+,\cdot)\longrightarrow(P,+,\cdot)$: $f(\langle a,b\rangle)=\langle a,b,-b,a\rangle$, je izomorfismus těles.

(23) Ověřte axiomy pro podokruhy, ukažte, že $S\cong\mathbb{Z}_3$, $T\cong\mathbb{Z}_5$.

(24) Ověřte axiomy okruhu, $\langle a,r\rangle\odot\langle 0,1\rangle=\langle a\cdot 0+r\cdot 0+1\cdot a,r\cdot 1\rangle=\langle a,r\rangle$.

(25) Tvoří-li prvky $1,a,a^2,a^3,\ldots$ aritmetickou posloupnost, pak $a-1=a^2-a=a^3-a^2=\ldots$, tedy $a-1=a\cdot(a-1)$, odkud máme $a\cdot(a-1)-(a-1)=0$, tedy $(a-1)\cdot(a-1)=0$, t.j. $(a-1)^2=0$.
Naopak, je-li $(a-1)^2=0$, pak pro každé $n\in\mathbb{N}$ platí:

$a^{n+1}-a^n=a^n(a-1)=a(a-1)\cdot a^{n-1}=a^{n-1}\cdot(a-1)=a^{n-2}\cdot a\cdot(a-1)=\ldots=a-1.$

(26) Ověřte distributivní zákony; jednotkou je $\langle 1,0\rangle$, k prvku $\langle a,b\rangle\neq\langle 0,0\rangle$ je inverzní $\langle\frac{1+2b}{a},-b\rangle$. Snadno se ověří, že tento okruh je těleso.

(27) **(a)** Ano, je to nejmenší těleso obsahující $\mathbb{Q}$ a číslo $\sqrt{3}$.

(b) Ne, neplatí uzavřenost vzhledem k násobení :
$(a+b\sqrt[3]{3})\cdot(c+d\sqrt[3]{3})=ac+(bc+da)\sqrt[3]{3}+bd\sqrt[3]{9}$,
nemusí být obecně z dané množiny.

(c) Ano, je to nejmenší těleso obsahující $\sqrt[3]{3}$ a těleso $\mathbb{Q}$.

(d) Ano, je to nejmenší těleso obsahující $\mathbb{Q}$ a číslo $\sqrt{2}$.

(e) Ne, neobsahuje nulu.

(f) Ne, totéž jako (e).

(g) Ne, neplatí například uzavřenost vzhledem k násobení.

(h) Ano, je to těleso $\mathbb{Q}$.

(i) Ne, vzhledem ke sčítání není grupa.

(j) Ano, je to nejmenší těleso obsahující $\mathbb{Q}$ a $\sqrt{-2}$.

(28) **(a)** Nejmenší číselné těleso je $\mathbb{Q}$, ovšem $\sqrt{3}\notin\mathbb{Q}$. Každé těleso, obsahující $\mathbb{Q}$ a $\sqrt{3}$, musí obsahovat prvky $b\sqrt{3}$ a také $a+b\sqrt{3}$, $a,b\in\mathbb{Q}$. Stačí ukázat, že tato množina spolu s operacemi $+$ a $\cdot$ již tvoří těleso.

(b) $T=\{a+b\sqrt[3]{2}+d\sqrt[3]{4};\ a,b,d\in\mathbb{Q}\}$

(c) $T=\{a+b\sqrt{2};\ a,b\in\mathbb{Q}\}$.

(29) Buďte $a_1,\ldots,a_n$ všechny nenulové prvky oboru integrity (stručně OI).
Buď a_i libovolný prvek této množiny. Ukažme, že množina $a_i\cdot a_1,a_i\cdot a_2,\ldots,a_i\cdot a_n$ je množina všech nenulových prvků OI : kdyby existovaly indexy j,j' tak, že $a_i\cdot a_j=a_i\cdot a_{j'}$, pak $a_i\cdot(a_j-a_{j'})=0$, $a_i\neq 0$ (proč?) a jelikož v OI neexistují dělitelé nuly, je nutně $a_j=a_{j'}$. Jsou-li tedy a_i,a_j libovolné nenulové prvky, pak vždy existuje prvek $a_{i'}$ tak, že $a_i\cdot a_{i'}=a_j$ (proč?), tedy tento OI je těleso.

(30) Nulou je $\emptyset$, každý prvek X různý od $\emptyset$ a množiny A je dělitel nuly, neboť $X\cap(A\setminus X)=\emptyset$.

(31) Jednotkou je $\langle 1,0\rangle$, nulou $\langle 0,0\rangle$. Inverzní prvky jsou
$\langle 1,0\rangle^{-1}=\langle 1,0\rangle$, $\langle 0,1\rangle^{-1}=\langle 1,1\rangle$, $\langle 1,1\rangle^{-1}=\langle 0,1\rangle$.

(32) (a) Ne, operace + není komutativní; ověřte, že $\langle 1,0\rangle$ je nulou.

(c) Ne, nulou je $\langle 0,1\rangle$, ale k prvku $\langle 0,0\rangle$ neexistuje prvek opačný.

(33) Užijte distributivního zákona. Ukažte, že $(-a)\cdot b=-(ab)=a\cdot(-b)$.
Pak ukažte, že $(-a)\cdot(-b)=-(a\cdot(-b))=-(-ab)=ab$.
Pak $(-a)\cdot(-b)\cdot(-c)=ab\cdot(-c)=a\cdot(-(bc))=-(abc)$.

(34) $(a+b)^2=(a+b)\cdot(a+b)=a\cdot a+a\cdot b+b\cdot a+b\cdot b=a^2+a\cdot b+b\cdot a+b^2=a^2+2ab+b^2$.

(35) Jsou-li $a,b\in Z(A)$, pak pro libovolný prvek $x\in A$ platí :
$(a-b)\cdot x=a\cdot x-b\cdot x=x\cdot a-x\cdot b=x\cdot(a-b)$, tedy $a-b\in Z(A)$, t.j.
$(Z(A),+)$ je abelovská grupa.
Dále $(a\cdot b)\cdot x=a\cdot(b\cdot x)=a\cdot(x\cdot b)=(a\cdot x)\cdot b=(x\cdot a)\cdot b=x\cdot(a\cdot b)$, tedy $a\cdot b\in Z(A)$. Dohromady je $Z(A)$ podokruh.

(36) Nulou je prvek α, opačný prvek k a je prvek $2\alpha-a$. Ověřte asociativitu násobení a distributivní zákony.

15. PRVOIDEÁLY A MAXIMÁLNÍ IDEÁLY DĚLITELNOST

Nechť $R=(A,+,\cdot)$ je okruh, $\emptyset\neq I\subseteq A$. Množinu I nazveme <u>ideál</u> okruhu R, je-li podokruhem R a jestliže pro každé $a\in A$ a pro každé $i\in I$ platí $a\cdot i\in I$, $i\cdot a\in I$. Množina všech ideálů na okruhu R tvoří uzávěrový systém. Tedy, je-li $M\subseteq A$, pak existuje <u>ideál generovaný množinou</u> M. Je to nejmenší ideál okruhu R obsahující M; označme jej $I(M)$. Je-li $M=\emptyset$, zřejmě $I(\emptyset)=\{0\}$, kde 0 je nulou okruhu R. Zřejmě A a $\{0\}$ jsou ideály okruhu, nazývají se tzv. <u>nevlastní ideály</u>. Ideál I okruhu R, který není nevlastní, se nazývá <u>vlastní</u>. Snadno se dokáže, že

$$I(M)=\{\sum_{i=1}^{n} r_i m_i s_i;\ r_i,s_i\in A,\ m_i\in M,\ n\in\mathbb{N}\}.$$

Ideál I okruhu R je <u>maximální</u>, jestliže pro každý ideál J takový, že $I\subseteq J\subseteq A$, platí buď $I=J$ nebo $J=A$.

Ideál I okruhu R je <u>prvoideál</u>, jestliže pro každé $a,b\in A$ platí: $a\cdot b\in I \Rightarrow a\in I$ nebo $b\in I$.

Je-li I ideál okruhu R, tvoří množina všech levých tříd, tj. $\{a+I;a\in A\}$ tzv. <u>faktorový okruh dle ideálu I;</u> označujeme jej R/I. V R/I jsou operace $\oplus,\odot$ definovány takto:

$$(a+I)\oplus(b+I)=(a+b)+I$$
$$(a+I)\odot(b+I)=ab+I.$$

Nechť $R=(A,+,\cdot)$ je unitární komutativní okruh, $a,b\in A$. Řekneme, že a <u>dělí</u> b (neboli prvek b je <u>dělitelný</u> prvkem a), symbolicky $a|b$, jestliže existuje $q\in A$ tak, že $b=a\cdot q$. Jestliže není pravda, že a dělí b, říkáme, že a <u>nedělí</u> b a zapisujeme $a\nmid b$.

Jestliže $a|b$ a také $b|a$, říkáme, že prvky a,b jsou <u>asociovány</u>, což zapisujeme $a\|b$. Prvek $j\in A$ asociovaný s jednotkou $1\in R$ se nazývá <u>jednotka dělení</u>.

Nechť $a_1,\dots,a_n\in A$. Prvek $d\in A$ je <u>největší společný dělitel</u> prvků $a_1,\dots,a_n$ (zkratkou NSD), jestliže $d|a_i$ pro $i=1,\dots,n$, a pro každé $t\in A$ takové, že $t|a_i$ $(i=1,\dots,n)$ platí $t|d$. Prvek $s\in A$ je <u>nejmenší společný násobek</u> (zkratkou NSN) prvků $a_1,\dots,a_n$, jestliže $a_i|s$ pro $i=1,\dots,n$ a pro každé $r\in A$ takové, že $a_i|r$ $(i=1,\dots,n)$

platí $s|r$. Největšího společného dělitele prvků a,b budeme značit buď NSD(a,b) nebo jen (a,b), nejmenší společný násobek buď NSN(a,b) nebo jen $[a,b]$.

Prvek $b\in A$ je v okruhu $R=(A,+,\cdot)$ <u>ireducibilní</u>, jestliže z vlastnosti $b=x\cdot y$ plyne, že $x\|b$ a $y\|1$ nebo naopak.

Prvek $p\in A$ je <u>prvočinitel</u>, jestliže z vlastnosti $p|ab$ pro některé $a,b\in A$ plyne buď $p|a$ nebo $p|b$.

Řekneme, že okruh $R=(A,+,\cdot)$ splňuje podmínku EIR (<u>existence rozkladu na ireducibilní prvky</u>), jestliže pro každé $b\in A$ existují ireducibilní prvky $p_1,\dots,p_n\in A$ tak, že $b=p_1\cdot\ldots\cdot p_n$.

Okruh $R=(A,+,\cdot)$ splňuje podmínku JIR (<u>jednoznačnosti ireducibilních rozkladů</u>), jestliže p_i,q_i jsou ireducibilní prvky v R a platí-li $p_1\cdot\ldots\cdot p_n=q_1\cdot\ldots\cdot q_m$, pak $m=n$ a při vhodném očíslování prvků $q_1,\dots,q_m$ je $p_i\|q_i$ $(i=1,\dots,n)$.

Okruh R je <u>Gaussův</u>, jestliže splňuje podmínky EIR a JIR.

Okruh R splňuje podmínku KŘVD (<u>konečnosti řetězců vlastních dělitelů</u>), jestliže $a_1,a_2,\dots$ je posloupnost prvků z R taková, že $a_{i+1}|a_i$ $(i=1,2,\dots)$, pak existuje $n_0\in\mathbb{N}$ tak, že pro $i\geq n_0$ platí $a_i\|a_{i+1}$.

Nechť $R=(A,+,\cdot)$ je komutativní unitární okruh bez dělitelů nuly, tj. obor integrity. Nechť n je zobrazení $A\setminus\{0\}$ do množiny nezáporných celých čísel. Řekneme, že n je <u>eukleidovská funkce</u>, jestliže platí: $a|b \Rightarrow n(a)\leq n(b)$. Okruh R je <u>eukleidovský</u>, jestliže na něm existuje eukleidovská funkce, a pro každé $a,b\in A$, $b\neq 0$, existují $q,r\in A$ tak, že

$$a=bq+r, \text{ přičemž } r=0 \text{ nebo } n(r)<n(b).$$

Každý eukleidovský okruh je Gaussův.

Nechť $R=(A,+,\cdot)$ je okruh, nechť $d\notin A$. Označme $R[d]$ nejmenší okruh, obsahující prvek d a podokruh R.

<u>Příklady</u>:

(1) Ukažte, že unitární okruh je tělesem právě když má pouze nevlastní levé (pravé) ideály.

(2) Nechť I,J jsou ideály okruhu R. Dokažte, že také

$$I+J=\{a+b;\ a\in I, b\in J\} \text{ a}$$

$$I\cdot J=\{\textstyle\sum a_i\cdot b_i;\ a_i\in I, b_i\in J\}$$

jsou ideály okruhu R. Dále dokažte $I\cdot J\subseteq I\cap J\subseteq I\subseteq I+J$.
Ukažte příklad, kdy tyto inkluze jsou ostré (tj. neplatí =).

(3) Dokažte, že jsou-li T,S tělesa, pak okruh $T\times S$ má právě 4 ideály.

(4) Nechť R je okruh všech ohraničených funkcí jedné reálné proměnné na intervalu $\langle a,b\rangle$ (pro $a\neq b$).
Nechť $X\subseteq\langle a,b\rangle$, $X\neq\emptyset$. Dokažte, že množina $I=\{f\in R;\ f(x)=0\ \forall x\in X\}$ tvoří ideál v R.

(5) Dokažte, že ideál I generovaný množinou $\{p\}$ v okruhu $(\mathbb{Z},+,.)$ je maximální, právě když p je prvočíslo.

(6) Nechť P je okruh všech spojitých funkcí na intervalu $\langle a,b\rangle$, $a\neq b$, a nechť $c\in\langle a,b\rangle$. Dokažte, že množina $I=\{f\in P;\ f(c)=0\}$ tvoří maximální ideál v P. Nechť $d\in\langle a,b\rangle$, $c<d$. Dokažte, že množina $J=\{f\in P;\ f(x)=0\ \forall x\in\langle c,d\rangle\}$ je ideál v P, který není maximální.

(7) Nechť P je konečný okruh, I ideál v P. Dokažte, že I je prvoideál, právě když I je maximální ideál.

(8) Sestrojte faktorový okruh $\mathbb{Z}_6/I$ kde $I=\{\bar{0},\bar{2},\bar{4}\}$.

(9) Nechť F_Q je okruh všech cauchyovských posloupností nad racionálními čísly, (viz. příklad (11) v kap 14.). Dokažte, že množina $I=\{(a_k)\in F_Q;\ \lim_{k\to\infty} a_k=0\}$ je maximální ideál v F_Q.

(10) Dokažte, že v okruhu $\mathbb{Z}[i]$ jsou množiny $A=\{2g;\ g\in\mathbb{Z}[i]\}$, $F=\{(1+i)g;\ g\in\mathbb{Z}[i]\}$, $B=\{5g;\ g\in\mathbb{Z}[i]\}$ ideály, a že faktorové okruhy $\mathbb{Z}[i]/A$, $\mathbb{Z}[i]/B$ nejsou obory integrity, ale $\mathbb{Z}[i]/F$ je těleso izomorfní se $\mathbb{Z}_2$.

(11) Nechť R je komutativní okruh, $p\in R$. Dokažte, že $I=\{px;\ x\in R\}$ je ideál v R.

(12) Nechť I,J jsou ideály okruhu R. Ukažte, že $I\cup J$ nemusí být ideál.

(13) Dokažte, že v oboru integrity $\mathbb{Z}[\sqrt{17}]$ je

(a) prvek $9-2\sqrt{17}$ ireducibilní

(b) prvek $15+7\sqrt{17}$ reducibilní

(c) prvky $33+8\sqrt{17}$, $33-8\sqrt{17}$, $-33+8\sqrt{17}$, $-33-8\sqrt{17}$ jsou jednotky dělení

(d) $\mathbb{Z}[\sqrt{17}]$ nesplňuje JIR.

(14) Ukažte, že $\mathbb{Z}[i]$ je eukleidovský obor integrity, přičemž $n(a+bi)=a^2+b^2$ je eukleidovská funkce.

(15) Nechť p je prvočíslo. Pak platí, že buď p je prvočinitel v $\mathbb{Z}[i]$ nebo $p=a^2+b^2$, kde $a+bi$, $a-bi$ jsou prvočinitelé v $\mathbb{Z}[i]$. Dokažte!

(16) Nechť p je prvočíslo. Pak p je prvočinitel v $\mathbb{Z}[i]$, právě když $p\equiv 3 \pmod 4$. Dokažte!

(17) Dokažte následující tvrzení :

(a) Je-li p prvočíslo a $p\equiv 1 \pmod 4$, pak existují $a,b\in\mathbb{Z}$ tak, že $p=a^2+b^2$.

(b) existuje nekonečně mnoho prvočísel p takových, že

(i) $p\equiv 1 \pmod 4$

(ii) $p\equiv 3 \pmod 4$.

(c) Nechť $a,b\in\mathbb{Z}$, $(a,b)=1$ (t.j. jsou nesoudělné). Nechť p je liché prvočíslo takové, že $p|a^2+b^2$. Pak $p\equiv 1 \pmod 4$.

(18) Dokažte, že v okruhu $(\mathbb{Z},+,\cdot)$ je rovnice $ax+by=c$ řešitelná, právě když $(a,b)|c$.

(19) Dokažte, že v okruhu $(\mathbb{Z},+,\cdot)$ platí:

(a) $(u,v)=1 \Rightarrow (u+v,u-v)=1$ nebo 2,

(b) $(a,a+k)|k$,

(c) jestliže $(u,v)=1$, $u|a$, $v|a \Rightarrow uv|a$

(d) $(a+b,[a,b])=(a,b)$

(e) jestliže $x^2+y^2=z^2$, $(x,y)=(x,z)=(y,z)=1$, pak existují $u,v\in\mathbb{Z}$ tak, že $x=2uv$, $y=v^2-u^2$, $z=v^2+u^2$.

(20) Ukažte, že pro $\alpha = \frac{-1+i\sqrt{3}}{2}$ je $\mathbb{Z}[\alpha]$ eukleidovský obor

integrity, přičemž eukleidovská funkce je $n(a+b\alpha)=a^2-ab+b^2$. Jednotky dělení tohoto okruhu jsou 1, -1, α, $-\alpha$, α^2, $-\alpha^2$.

(21) Ukažte, že $\mathbb{Z}[\sqrt{-2}]$ je eukleidovský obor integrity, ve kterém $n(a+b\sqrt{-2})=a^2+2b^2$ a jehož jednotky dělení jsou 1, -1.

(22) Najděte všechny jednotky dělení v $\mathbb{Z}[\sqrt{2}]$.

(23) V okruhu $(\mathbb{Z},+,\cdot)$ dokažte:

(a) $6|a^3+11a$,

(b) $4a+3$ není mocninou žádného čísla ze $\mathbb{Z}$ pro žádné $a\in\mathbb{Z}$,

(c) Jestliže $2\nmid a$, $3\nmid a$, pak $24|a^2-1$.

(24) Ukažte, že v okruhu $\mathbb{Z}[\sqrt{-5}]$ je prvek 3 ireducibilní, ale není prvočinitel.

(25) Určete největší společný dělitel:

(a) v $\mathbb{Z}$ pro (600,-252)
(1100,441)
(-2520,3300)

(b) v $\mathbb{Z}[i]$ pro $(32,\ 2+i)$
$(50,\ 11+3i)$
$(4+i,\ 3+i)$

(26) Nechť R je eukleidovský obor integrity, $n\geq 2$, $a_1,\dots,a_n\in R$, $b\neq 0$, $b\in R$. Je-li a_i nesoudělné s b pro $i=1,\dots,n$, pak prvek $p=a_1a_2\dots a_n$ je nesoudělný s b. Dokažte!

(27) Nechť R je eukleidovský obor integrity, p ireducibilní prvek v R. Pak $p|a_1a_2\dots a_n$, právě když $p|a_i$ pro některé $i\in\{1,\dots,n\}$. Dokažte!

(28) Nechť $a,b\in\mathbb{Z}$. Ověřte, že NSD prvků a,b v $\mathbb{Z}[i]$ je roven NSD prvků a,b v $\mathbb{Z}$.

(29) Ukažte, že NSD prvků 4, $2+2i\sqrt{3}$ v okruhu $\mathbb{Z}[\sqrt{-3}]$ neexistuje.

PŘÍKLADY OKRUHŮ NA EIR, JIR, KŘVD A NEEXISTENCI TĚCHTO VLASTNOSTÍ.

(30) Definujme v okruhu $\mathbb{Z}[\sqrt{d}]$, kde $d\in\mathbb{Z}$ a d není kvadrát přirozeného čísla, tzv. normu dělení n: $n(a+b\sqrt{d}) = a^2-b^2d$. Ukažte, že platí:

(i) pro $\alpha,\beta\in\mathbb{Z}[\sqrt{d}]$: $n(\alpha\cdot\beta) = n(\alpha)\cdot n(\beta)$,

(ii) α je jednotka dělení, právě když $n(\alpha)=\pm 1$,

(iii) $\alpha|\beta \Rightarrow n(\alpha)|n(\beta)$.

(31) Buď F množina všech polynomů jedné neurčité s koeficienty ze $\mathbb{Z}$. Uvažujme zobrazení $f:F \longrightarrow \mathbb{Z}$ takové, že $f(p) = p(0)$. Ukažte, že $Ker\ f = \{p\in F;\ p(0)=0\}$ je ideál v F, který je prvoideál, ale není maximální.

(32) Ukažte, že okruh $\mathbb{Z}\times\mathbb{Z}\times\mathbb{Z}\times$ ... (nekonečně spočetně mnohokrát) je okruh, který není oborem integrity. Ukažte, že nesplňuje podmínku KŘVD. Splňuje EIR ?

(33) Ukažte, že obory integrity $\mathbb{Z}[\sqrt{d}]$ z příkladu (30) splňují podmínku KŘVD, ale nesplňují obecně JIR.

(34) Nechť I je obor integrity, $a,b,c,d\in I$. Dokažte, že platí:

(a) je-li $a\|b$, $c\|d$, pak $ac\|bd$, ale obecně neplatí, že $a+c\|b+d$,

(b) je-li $a\neq 0$, pak je-li $a\|b$, $ac\|bd$, pak $c\|d$.

(35) Nechť $x\in\mathbb{R}$, $x\geq 2$. Označme $\pi(x)$ počet prvočísel menších nebo rovných x. Ukažte, že $\pi(x)\geq\ln(\ln x)$ (tj. prvočísel je nekonečně mnoho).

(36) Buď $a>1$, $a,m,n\in\mathbb{N}$, $n>m$. Pak $NSD(a^{2^m}+1,\ a^{2^n}+1)$ je buď 1 nebo 2, přičemž druhý případ nastane pro a sudé. Dokažte!

(37) Najděte všechny prvky nerozložitelné v okruzích:

(a) $P_1 = \{\frac{n}{m} \in \mathbb{Q};\ m$ liché$\}$,

(b) $P_2 = \{\frac{n}{m} \in \mathbb{Q};\ 2|m$ a $3|m\}$,

(c) $P_3 = \{\frac{f(x)}{g(x)} \in \mathbb{Q}[x];\ g(0)\neq 0\}$,

(d) $P_4 = \{\frac{f(x)}{g(x)} \in \mathbb{Q}[x];\ g(0)\cdot g(1)\neq 0\}$.

Návody k řešení:

(1) Nechť T je těleso, I ideál v T, $a\in I$, $a\neq 0$. Je-li $b\in T$, $b\neq 0$, b libovolný prvek, pak existuje jediný prvek $x\in T$ tak, že $a\cdot x=b$ (proč?). Pak ale $a\cdot x=b\in I$ (proč?), tedy $I=T$. Naopak, nechť má unitární okruh R bez dělitelů nuly pouze nevlastní ideály. Pak označme $I=\{x\in R;\ a\cdot x=x\cdot a=0\}$, kde $a\in R$, $a\neq 0$. Pro $x,y\in I$ je $(x-y)\cdot a = xa-ya = 0$, $(z\cdot x)\cdot a = z\cdot(x\cdot a) = 0$, a I je levý ideál v R. Zřejmě $1\notin I$, tedy $I=\{0\}$. Dále, množina $Ra = \{r\cdot a;\ r\in R\}$ je levý ideál v R, $0\neq a=1\cdot a\in Ra$, tedy $Ra = R$. Je-li $b\in R$ libovolný prvek, pak existuje $x\in R$ tak, že $x\cdot a = b$, je tedy R těleso.

(2) Nechť $x,y\in I+J$, tedy $x = a+b$, $y = a'+b'$ pro $a,a'\in I$, $b,b'\in J$. Pak $x-y = a+b-b'-a' = (a-a')+(b-b')$, $a-a'\in I$, $b-b'\in J$ (proč?), tedy $x-y\in I+J$. Je-li $z\in R$, pak $z\cdot x = z(a+b) = za+zb$, $za\in I$, $zb\in J$ (proč?), t.j. $z\cdot x\in I+J$, $x\cdot z = (a+b)\cdot z = az+bz\in I+J$, tedy $I+J$ je ideál.
Jsou-li $x,y\in I\cdot J$, pak $x = \sum_i a_i b_i$, $y = \sum_j a_j b_j$, tedy $x-y =$
$= \sum_i a_i b_i + \sum_j (-a_j)\cdot b_j \in I\cdot J$. Podobně $x\cdot z = \sum_i a_i (b_i\cdot z)\in I\cdot J$, tedy $I\cdot J$ je ideál.

(3) Ideály jsou $I_1 = \{\langle t,0\rangle;\ t\in T\}$, $I_2 = \{\langle 0,s\rangle;\ s\in S\}$, $I_3 = \{\langle 0,0\rangle\}$ a $I_4 = T\times S$.

(4) Jsou-li $f,g\in I$, pak
$(f-g)(x) = f(x)-g(x) = 0-0 = 0$ pro každé $x\in X$,
$(f\cdot m)(x) = f(x)\cdot m(x) = 0\cdot m(x) = 0$ pro každé $m\in R$ a $x\in X$.

(5) Nechť $I_p = \{k\cdot p;\ k\in\mathbb{Z}\}$. Nechť $a\notin I_p$.
Buď I ideál generovaný množinou $I_p\cup\{a\}$. Pak čísla p,a jsou nesoudělná (proč?) a tedy existují celá čísla x,y tak, že

$px+ay = 1$ (proč?). Ovšem $px+ay \in I$ (proč?) a tedy $1 \in I$, tedy $I=\mathbb{Z}$.

Naopak, je-li s složené číslo, $s= m\cdot n$, $m,n \neq \pm 1$, $m,n \neq \pm s$, pak $\{k\cdot n;\ k\in\mathbb{Z}\} \supset \{k\cdot s;\ k\in\mathbb{Z}\}$, tedy ideál I_s není maximální.

(6) Ukažme, že I je ideál:

Nechť $f,g\in I$. Pak $(f-g)(c) = f(c)-g(c) = 0-0 = 0$; pro $m\in P$ platí $(f\cdot m)(c) = f(c)\cdot m(c) = 0\cdot m(c) = 0$, neboť spojitá funkce na uzavřeném intervalu je ohraničená. Buď $\psi\in P$, $\psi\notin I$, tj. $\psi(c)\neq 0$.

Buď J^* ideál generovaný množinou $\{\psi\}\cup I$.

Buď f funkce definovaná takto: $f(x) = \psi(x)-\psi(c)$. Zřejmě $f\in J^*$, neboť $f(c) = \psi(c)-\psi(c) = 0$, tedy $f\in I$. Pak ale $-f+\psi\in J^*$ (proč?), tedy $(-f+\psi)(x) = -\psi(x)+\psi(c)+\psi(x) = \psi(c)$, tedy $-f+\psi$ je konstantní funkce s hodnotou $\psi(c)\neq 0$. Pak ale funkce $j(x)\equiv 1\in J^*$ (proč?), tedy $J^*=P$ a I je maximální ideál v P.

Z těchto úvah bezprostředně plyne, že ideál J není maximální.

(7) Je-li P konečný, pak faktorový okruh dle libovolného ideálu je konečný. Podle cvičení (1) je každý konečný obor integrity těleso. Je-li tedy ideál I prvoideál, musí být maximální.

(8) Označme $J = \{\overline{1},\overline{3},\overline{5}\}$. Pak $\mathbb{Z}_6/I$ je dvojprvkový okruh $(\{I,J\},+,\cdot)$, kde

+	I	J
I	I	J
J	J	I

$\cdot$	I	J
I	I	I
J	I	J

a je izomorfní s tělesem $\mathbb{Z}_2$.

(9) Jelikož $\mathbb{R}$ je úplný metrický prostor, každá cauchyovská posloupnost v $\mathbb{Q}$ má limitu v $\mathbb{R}$. Uvažujme zobrazení

$$f\colon F_Q \longrightarrow \mathbb{R} \text{ takové, že } f(\{p_n\}) = \lim_{n\to\infty} p_n .$$

Ukažte, že f je surjektivní homomorfismus jehož jádrem je právě ideál I. Podle věty o homomorfismu je tedy $F_Q/I \cong \mathbb{R}$.

(10) Obor integrity $\mathbb{Z}[i]$ je eukleidovský. Zde platí, že ideál generovaný prvkem x je maximální, právě když x je

ireducibilní (dokažte!). Prvky 2, 5 jsou rozložitelné, $2=(1-i)(1+i)$, $5=(2-i)(2+i)$. Prvek $(1+i)$ je ireducibilní (dokažte!), tedy $\mathbb{Z}[i]/F$ je těleso. Má právě dvě třídy, a to F a $\mathbb{Z}[i]\setminus F$. Je-li $[1-i]$ třída určená prvkem $(1-i)$ v $\mathbb{Z}[i]/A$, pak $[1-i]$ je v $\mathbb{Z}[i]/A$ dělitel nuly:

$$[1-i]\odot[1+i]=[(1-i)(1+i)]=[2]=I=[0].$$

Podobně třída $[2+i]$ je v $\mathbb{Z}[i]/B$ dělitel nuly.

(12) Jsou-li $a\in I$, $b\in J$, pak $a+b$ nemusí patřit ani do I ani do J: v příkladu (3) $I_1\cup I_2$ není ideál: $\langle t,0\rangle\in I_1$, $\langle 0,s\rangle\in I_2$, $\langle t,0\rangle+\langle 0,s\rangle=\langle t,s\rangle\notin I_1\cup I_2$.

(13) **(a)** Dle příkladu (30) je pro $\alpha\in\mathbb{Z}[\sqrt{17}]$ $n(\alpha)=n(a+b\sqrt{17})=a^2-17b^2$. Pak $n(9-2\sqrt{17})=81-68=13$. Kdyby $\beta|(9-2\sqrt{17})$, pak $n(\beta)|n(9-2\sqrt{17})$, tedy $n(\beta)|13$. Pak jedině $n(\beta)=\pm1,\pm13$. V případě $n(\beta)=\pm1$ by β byla jednotka, v druhém případě $\beta\|(9-2\sqrt{17})$.

(b) $15+7\sqrt{17} = (6-\sqrt{17})(11+3\sqrt{17})$

(d) $8 = 2\cdot2\cdot2 = 2\cdot(8+2\sqrt{17})(-8+2\sqrt{17}) = (5+\sqrt{17})(5-\sqrt{17})$.

(14) Buďte $n(a+bi)\geq n(c+di)$. Označme $\frac{a+bi}{c+di}=x+yi$, kde $x,y\in\mathbb{Q}$. Zvolme $q_1,q_2\in\mathbb{Z}$ tak, aby $|q_1-x|\leq\frac{1}{2}$, $|q_2-y|\leq\frac{1}{2}$. (Ukažte, že je to vždy možné!). Nechť $(a+bi)=(c+di)(q_1+q_2i)+(r_1+r_2i)$. Ukažme, že $n(r_1+r_2i)<n(c+di)$:

$$r_1+r_2i=(a+bi)-(c+di)(q_1+q_2i)=(c+di)(x+yi)-(c+di)(q_1+q_2i)=$$
$$=(c+di)((x-q_1)+(y-q_2)i).$$

Pak $\sqrt{n(r_1+r_2i)}=|r_1+r_2i|=\sqrt{r_1{}^2+r_2{}^2}=|(c+di)((x-q_1)+(y-q_2)i)|=$

$=\sqrt{(c^2+d^2)}\cdot\sqrt{(x-q_1)^2+(y-q_2)^2}\leq\sqrt{c^2+d^2}\cdot\sqrt{\frac{1}{4}+\frac{1}{4}}=\sqrt{\frac{1}{2}(c^2+d^2)}$, tedy

$$n(r_1+r_2i)\leq\frac{c^2+d^2}{2}<c^2+d^2=n(c+di).$$

(15) $\mathbb{Z}[i]$ je Gaussův, tedy $p=q_1\cdot q_2\cdot\ldots\cdot q_k$, kde $q_1,q_2,\ldots q_k$ jsou ireducibilní v $\mathbb{Z}[i]$. Pak $n(p)=p^2=n(q_1\cdot q_2\cdot\ldots\cdot q_k)=$ $n(q_1)\cdot\ldots\cdot n(q)$, tedy nutně $k\leq2$. Je-li $k=1$, pak $p=q_1$ a p je ireducibilní. Je-li $k=2$, pak $p=q_1\cdot q_2$, $n(q_1)=n(q_2)=p$. Je-li $q_1=a+bi$, pak $n(q_1)=a^2+b^2=p=(a-bi)(a+bi)$, tedy díky jednoznačnosti rozkladu $a-bi=q_2$.

(16) Nechť $p\equiv 3 \pmod 4$. Není-li p prvočinitel, pak dle cvičení (15) platí
$p=a^2+b^2$, $a,b\in\mathbb{Z}$. Přitom pro $a\equiv 0 \pmod 4$ je $a^2\equiv 0 \pmod 4$, pro $a\equiv 1 \pmod 4$ je $a^2\equiv 1 \pmod 4$, pro $a\equiv 2 \pmod 4$ je $a^2\equiv 0 \pmod 4$, pro $a\equiv 3 \pmod 4$ je $a^2\equiv 1 \pmod 4$.
Tedy $p=a^2+b^2\equiv 0,1,2 \pmod 4$, spor. Tedy p je prvočinitel.

Nechť $p\equiv 1 \pmod 4$. Pak $\prod_{i=\frac{p+1}{2}}^{p-1} i = \prod_{i=1}^{\frac{1}{2}(p-1)} (p-i)$. Položme $x=(\frac{p-1}{2})!$.

Protože $p\equiv 1 \pmod 4$, je $\frac{p-1}{2}$ sudé, tedy $x=\prod_{i=1}^{\frac{1}{2}(p-1)} (-i)$. Protože

$p-i\equiv -i \pmod p$, je $x\equiv \prod_{i=1}^{\frac{1}{2}(p-1)} (p-i) = \prod_{i=\frac{p+1}{2}}^{p-1} i$, tedy

$x^2\equiv (p-1)! \pmod p$.
Dle Wilsonovy věty $(p-1)! \equiv -1 \pmod p$, tedy $x^2\equiv -1 \pmod p$, odtud $k=x^2+1=(x+i)(x-i)$. Nechť p je prvočinitel. Pak buď $p|(x-i)$ nebo $p|(x+i)$. Pak $p(a+bi)=x+i$ nebo $p(a+bi)=x-i$, tedy $pa=x$, $pb=\pm 1$, což není možné. Tedy p není prvočinitel.

(17) **(a)** Podle cvičení (16) není p prvočinitel a tedy dle (15) je $p=a^2+b^2$, $a,b\in\mathbb{Z}$.
(b) (i) Nechť prvočísel p tvaru $p\equiv 3 \pmod 4$ je pouze konečně mnoho, např. $p_1,\dots,p_k$. Označme $u=4\cdot p_1\cdot p_2\cdot\ldots\cdot p_k-1$. Zřejmě $u\equiv 3 \pmod 4$. Nechť $u=q_1\cdot\ldots\cdot q_m$ je rozklad čísla u. Kdyby $\forall i\in\{1,\dots,n\}$ bylo $q_i\equiv 1 \pmod 4$, pak $u\equiv 1 \pmod 4$, což není možné. Existuje tedy $p|u$ tak, že $p\equiv 3 \pmod 4$. Kdyby $p=p_j$ pro některé $j\in\{1,\dots,k\}$, pak by $u=4px-1$, tedy $u\equiv -1 \pmod p$, což je spor s $p|u$. Tedy $p\neq p_j$, přitom $p\equiv 3 \pmod 4$, spor.
(ii) Nechť $p_1,\dots,p_k$ jsou všechna prvočísla, $p_i\equiv 1 \pmod 4$. Nechť $n=p_1^2p_2^2\dots p_k^2+4$. Nechť p je prvočíslo, $p|n$. Pak

$p|(p_1p_2\dots p_k)^2+2^2$. Dle (c) je $p\equiv 1 \pmod 4$. Kdyby $p=p_i$ pro některé i, pak by z $p|n$ plynulo $p|4$, tedy p by nebylo liché prvočíslo, spor.
(c) Kdyby $p|a$, pak z $p|a^2+b^2$ plyne $p|b^2$, $p|b$, což je spor s $(a,b)=1$. Dle Fermatovy věty $a^{p-1}\equiv 1 \pmod p$. Dále,
$b^2\equiv -a^2 \pmod p$, neboť $p|a^2+b^2$. Pak

$(a^{p-2}b)^2=(a^{p-2})^2b^2\equiv(a^{p-2})^2(-a^2)=-(a^{p-1})^2 \equiv -1 \pmod p$,
tedy prvek $a^{p-2}b$ je řádu 4 v multiplikativní grupě $\mathbb{Z}_p$.
Protože ta má řád $p-1$, je $4|p-1$, tedy $p\equiv 1 \pmod 4$.

(18) Nechť $d=(a,b)$. Pak $a=dx_1$, $b=dy_1$, pro některé $x_1,y_1\in\mathbb{Z}$, a tedy $ax+by=dx_1x+dy_1y=d(x_1x+y_1y)=c$, tedy $d|c$.
Naopak, jestliže $d|c$, pak existují $x_1,y_1\in\mathbb{Z}$ tak, že $ax_1+by_1=d$ (proč?). Jestliže $c=du$, pak $aux_1+buy_1=c$, tedy rovnice je řešitelná .

(19) **(a)** Jestliže $(u,v)=1$, pak existují $x,y\in\mathbb{Z}$ tak, že $ux+vy=1$ (proč?). Pak $(u+v)(x+y)+(u-v)(x-y)=2$ (ověřte!), a tedy dle (18) platí $(u+v,u-v)|2$.
(b) $a(k+a-1)+(a+k)(1-a)=k$, tedy $(a,a+k)|k$.
(c) $(u,v)=1 \Rightarrow ux+vy=1$ pro nějaké $x,y\in\mathbb{Z}$, $u|a$, $v|a$. Pak $a=ku=ku^2x+kyuv=aux+kyuv$, $a=lv=lxuv+lyv^2=lxuv+avy$.
Sečtením dostaneme: $2a=uv(ky+lx)+a(ux+vy)=uv(ky+lx)+a$. Odtud $a=uv(ky+lx)$, tedy $u\cdot v|a$.
(d) Nechť $a=p_1^{\alpha_1}\cdots p_n^{\alpha_n}$, $b=p_1^{\beta_1}\cdots p_n^{\beta_n}$. Pak
$a+b=p_1^{\min(\alpha_1,\beta_1)}\cdot p_2^{\min(\alpha_2,\beta_2)}\cdots p_n^{\min(\alpha_n,\beta_n)}\cdot x$, kde $x\in\mathbb{Z}$, $p_i\nmid x$ (ověřte!) a $[a,b]=p_1^{\max(\alpha_1,\beta_1)}\cdot\ldots\cdot p_n^{\max(\alpha_n,\beta_n)}$. Odtud je vidět, že $NSD(a,b)=p_1^{\min(\alpha_1,\beta_1)}\cdot\ldots\cdot p_n^{\min(\alpha_n,\beta_n)}|\ a+b,[a,b]$.
Kdyby prvek $NSD(a,b)$ byl vlastní dělitel $d=NSD(a+b,[a,b])$, pak by muselo existovat p_i, $i\in\{1,\ldots,n\}$ tak, že $p_i|x$ (proč?), a to by byl spor s volbou čísla x. Je tedy $NSD(a+b,[a,b])=NSD(a,b)$.
(e) x,y nemohou být zároveň lichá: pak by $2|z^2$, tedy $4|z^2$, ale čtverec lichého čísla dá při dělení čtyřmi zbytek 1. Tedy $x=2l$, pak $4l^2=z^2-y^2=(z-y)(z+y)$. Je tedy $z+y=2j$, $z-y=2k$, pro některé $k,j\in\mathbb{Z}$, odkud $z=j+k$, $y=j-k$ a tedy $l^2=jk$. Dále, $(j,k)=1$ (jinak $(y,z)\neq 1$). Musí být $j=u^2$, $k=v^2$, $l=u.v$, kde $u\geq v$, $(u,v)=1$. Pak $x=2uv$, $y=u^2-v^2$, $z=u^2+v^2$.

(20) Ukažte, že pro $\alpha,\beta\in\mathbb{Z}[\alpha]$ platí $n(\alpha\cdot\beta)=n(\alpha)\cdot n(\beta)$.
Jednotky jsou takové prvky, že $n(\alpha)=\pm 1$ (dokažte!).
Pak pro $\alpha=a+b\alpha$ je $n(\alpha)=a^2-ab+b^2=1$, tedy

$$\left(a-\frac{b}{2}\right)^2-\frac{b^2}{4}+b^2=1,\ \text{tedy}\ \left(a-\frac{b}{2}\right)^2+\frac{3}{4}b^2=1,\ \text{odkud}$$

$\left(a-\frac{b}{2}\right)^2+3\left(\frac{b}{2}\right)^2=1$, tedy $(2a-b)^2+3b^2=4$. Pak nutně $|b|\le 1$.

Je-li $b=0$, pak $2a-b=\pm 2$, tedy $a=\pm 1$,

$b=1$, pak $2a-b=\pm 1$, $a=1$ nebo $a=0$,

$b=-1$, pak $2a-b=\pm 1$, $a=0$ nebo $a=1$.

Eukleidovská vlastnost funkce n se dokáže podobně jako ve (14).

Jsou-li $a+b\alpha$, $c+d\alpha\in\mathbb{Z}[\alpha]$, pak existují $x,y\in\mathbb{Q}[\alpha]$ (proč ?) tak, že $\frac{a+b\alpha}{c+d\alpha}=x+y\alpha$. Zvolíme q_1,q_2 tak, aby $|q_1-x|\le\frac{1}{2}$, $|q_2-y|\le\frac{1}{2}$.

Pak $r_1+r_2\alpha=(c+d\alpha)\cdot((x-q_1)+(y-q_2)\alpha)$.

Zřejmě $n(r_1+r_2\alpha)=\left(r_1-\frac{r_2}{2}\right)^2+r_2^2\cdot\frac{3}{4}=r_1^2-r_1r_2+r_2^2$.

Pak $n(r_1+r_2\alpha)=n(c+d\alpha)\cdot\left[(x-q_1)^2+(y-q_2)^2-(x-q_1)(y-q_2)\right]$.

Zřejmě $|x-q_1|\cdot|y-q_2|\le\frac{1}{2}\cdot\frac{1}{2}=\frac{1}{4}$, tedy

$(x-q_1)^2+(y-q_2)^2-(x-q_1)(y-q_2)\le\frac{1}{4}+\frac{1}{4}+\frac{1}{4}=\frac{3}{4}$, odkud máme

$$n(r_1+r_2\alpha)\le n(c+d\alpha)\cdot\frac{3}{4}<n(c+d\alpha).$$

(21) Postupujte obdobně jako v příkladech (14) a (20), jednotky dělení jsou prvky s normou 1.

(22) Dle příkladu (30) mají všechny jednotky normu rovnou ± 1, tedy $n(a+b\sqrt{2})=a^2-2b^2=\pm 1$.

Tato rovnice má v $\mathbb{Z}\times\mathbb{Z}$ nekonečně mnoho řesení, jsou to právě všechna čísla $\pm(1+\sqrt{2})^n$, $\pm(-1+\sqrt{2})^n$, $n\in\mathbb{N}$.

(23) **(a)** Jestliže

$a\equiv 0 \pmod 6$,	pak $a^3\equiv 0 \pmod 6$,	$11a\equiv 0 \pmod 6$,	$a^3+11a\equiv 0 \pmod 6$,
$a\equiv 1 \pmod 6$,	$a^3\equiv 1 \pmod 6$,	$11a\equiv 5 \pmod 6$,	$a^3+11a\equiv 6\equiv 0 \pmod 6$,
$a\equiv 2 \pmod 6$,	$a^3\equiv 2 \pmod 6$,	$11a\equiv 4 \pmod 6$,	$a^3+11a\equiv 6\equiv 0 \pmod 6$,
$a\equiv 3 \pmod 6$,	$a^3\equiv 3 \pmod 6$,	$11a\equiv 3 \pmod 6$,	$a^3+11a\equiv 6\equiv 0 \pmod 6$,
$a\equiv 4 \pmod 6$,	$a^3\equiv 4 \pmod 6$,	$11a\equiv 2 \pmod 6$,	$a^3+11a\equiv 6\equiv 0 \pmod 6$,
$a\equiv 5 \pmod 6$,	$a^3\equiv 5 \pmod 6$,	$11a\equiv 1 \pmod 6$,	$a^3+11a\equiv 0 \pmod 6$.

(b) Je-li

$a\equiv 0 \pmod 4$,	pak $4a+3\equiv 3 \pmod 4$	a	$a^2\equiv 0 \pmod 4$,
$a\equiv 1 \pmod 4$,	$4a+3\equiv 3 \pmod 4$		$a^2\equiv 1 \pmod 4$,
$a\equiv 2 \pmod 4$,	$4a+3\equiv 3 \pmod 4$		$a^2\equiv 0 \pmod 4$,
$a\equiv 3 \pmod 4$,	$4a+3\equiv 3 \pmod 4$		$a^2\equiv 1 \pmod 4$,

tedy $4a+3$ nemůže být druhou mocninou přirozeného čísla.

(c) Máme tyto možnosti:

$a\equiv 0 \pmod{24}$ ...nemůže nastat, neboť pak by $24|a$

$a\equiv 1 \pmod{24}$ ...pak $a^2-1\equiv 0 \pmod{24}$

$a\equiv 2 \pmod{24}$ ...nemůže nastat, pak by $2|a$

$a\equiv 3 \pmod{24}$ ... -''- $3|a$

$a\equiv 4 \pmod{24}$ ... -''- $4|a$

$a\equiv 5 \pmod{24}$ ... $a^2-1\equiv 0 \pmod{24}$

⋮

Prověřte všechny zbývající možnosti.

(24) Podle (30) má prvek 3 normu $n(3)=3^2+5.0^2=9$.
Kdyby existoval prvek $\alpha|3$, pak by $n(\alpha)|n(3)=9$, tedy buď

$n(\alpha)=1$ ... α by byla jednotka,

$n(\alpha)=3$ ... takový prvek neexistuje,

$n(\alpha)=9$ ... pak by $\alpha\in\{\pm 3, \pm 2\pm i\sqrt{5}\}$, ale $\pm 3\|3$, $\pm 2\pm i\sqrt{5}\nmid 3$.

Dále $9=3\cdot 3=(2-i\sqrt{5})(2+i\sqrt{5})$, tedy $3|(2-i\sqrt{5})(2+i\sqrt{5})$,
ale $3\nmid(2-i\sqrt{5})$ ani $3\nmid(2+i\sqrt{5})$.

(25) (b) $n(4+i)=17$, $n(3+i)=10$.

$$\frac{4+i}{3+i} = \frac{(4+i)(3-i)}{10} = \frac{13}{10} - \frac{i}{10} = x+yi.$$

Zvolme $q_1=1$, $q_2=0$. Pak $r_1+r_2i=(4+i)-(3+i)(1+0.i)=1$, tedy $n(r_1+r_2i)=1<n(3+i)=10$. Je tedy $(4+i)=(3+i)(1+0\cdot i)+1$. Dále $3+i=(3+i).1+0$, tedy $(4+i, 3+i)=1$.

(26) $(a_i,b)=1$, tedy existují $x_i, y_i\in\mathbb{R}$ tak, že $a_ix_i+by_i=1$ (proč?).
Pak $a_ix_i=1-by_i$. Vynásobme všechny takovéto rovnice:

$$a_1\cdot a_2\cdot \ldots \cdot a_n\cdot \underbrace{x_1\cdot \ldots \cdot x_n}_{x}=(1-by_1)(1-by_2)\ldots(1-by_n).$$

Pak pravá strana má tvar $1+bk$, kde $k\in\mathbb{R}$ (ověřte !), a tedy

$a_1\cdot \ldots \cdot a_n\cdot x - bk = 1$, tj. $(a_1,\ldots,a_n,b)=1$ (proč ?).

(27) V eukleidovském oboru integrity je ireducibilní prvek p prvočinitel. Je-li tedy $p|a_1\cdot a_2$, pak $p|a_1$ nebo $p|a_2$.
Indukcí dokažte pro každé $n\in\mathbb{N}$.

(28) Nechť $p,q\in\mathbb{Z}$. Pokud p,q jsou ireducibilní v $\mathbb{Z}[i]$, pak v obou případech $NSD(p,q)=1$. Kdyby existoval prvek (který není jednotka dělení) $(a+bi)$, $b\neq 0$ tak, že $(a+bi)|p,q$, pak by muselo platit $(a-bi)|p,q$ (proč ?), a tedy $(a^2+b^2)|p,q$. Musí

tedy být největší společný dělitel p,q v $\mathbb{Z}[i]$ celé číslo.

(29) Zřejmě $4=(1+i\sqrt{3})(1-i\sqrt{3})$, $2+2i\sqrt{3}=2(1+i\sqrt{3})$. Je tedy $2|4$, $2|(2+2i\sqrt{3})$, $(1+i\sqrt{3})|4$, $(1+i\sqrt{3})|(2+2i\sqrt{3})$. Dále, $n(2)=4$ je vlastní dělitel $n(4)=16$ a $n(2+2i\sqrt{3})=16$, $n(1+i\sqrt{3})=4$ je vlastní dělitel $n(4)=16$ a $n(2+2i\sqrt{3})=16$. Navíc 2, $1+i\sqrt{3}$ nejsou jednotky dělení (proč?), a tedy jsou to vlastní dělitelé. Je zřejmé že $2\nmid(1+i\sqrt{3})$ ani $(1+i\sqrt{3})\nmid 2$, tedy $2\nparallel(1+i\sqrt{3})$. Kdyby existoval další prvek α takový, že $\alpha|4$, $\alpha|(2+2i\sqrt{3})$ a $2,1+i\sqrt{3}|\alpha$, pak by $n(\alpha)=4$ nebo $n(\alpha)=16$. V prvním případě $\alpha\in\{\pm2,\pm1\pm i\sqrt{3}\}$, ve druhém $\alpha\in\{\pm4,\pm2\pm2i\sqrt{3}\}$.
V prvním případě $\pm2\parallel2$, $1+i\sqrt{3},-1-i\sqrt{3}\parallel1+i\sqrt{3}$, $-1+i\sqrt{3},1-i\sqrt{3}$ nejsou dělitelné $1+i\sqrt{3}$. Ve druhém $\pm4\parallel4$, $2+2i\sqrt{3}$, $-2-2i\sqrt{3}\parallel2+2i\sqrt{3}$, $2-2i\sqrt{3}$, $-2+2i\sqrt{3}$ nejsou dělitelné $2+2i\sqrt{3}$.

(30) (i) $n[(a+b\sqrt{d})(c+e\sqrt{d})]= n[(ac+bed)+(ae+bc)\sqrt{d}]=$
$=(ac+bed)^2-(ae+bc)^2d=a^2c^2+2abcde+b^2e^2d^2-a^2e^2d-2abcde-b^2c^2d=$
$=a^2c^2+b^2e^2d^2-a^2e^2d-b^2c^2d.$
$n(a+b\sqrt{d})\cdot n(c+e\sqrt{d})=(a^2-b^2d)(c^2-e^2d)=a^2c^2-a^2e^2d-b^2c^2d+b^2e^2d^2.$
(ii) je-li α jednotka, pak $\alpha|1$, tedy dle (i) $n(\alpha)|n(1)=1$, tedy $n(\alpha)=\pm1$. Nechť $\alpha=a+b\sqrt{d}$ je takový prvek, že $n(\alpha)=\pm1$. Pak $n(\alpha)=(a+b\sqrt{d})(a-b\sqrt{d})=\pm1$, $a+b\sqrt{d}|\pm1$ a α je jednotka dělení.
(iii) plyne z (i).

(31) Nechť $p,q\in$ *Ker f*. Pak $(p-q)(0)=p(0)-q(0)=0-0=0$, tedy $p-q\in$*Ker f*. Jeli $m\in F$, pak $(p\cdot m)(0)=p(0)\cdot m(0)=0\cdot m(0)=0$, je tedy *Ker f* ideál.
Nechť existují $p,q\in F$ takové, že $p\cdot q\in$ *Ker f*, tedy $(p\cdot q)(0)=0$. Pak $p(a)\cdot q(0)=0$, tedy buď $p(0)=0$, nebo $q(0)=0$, je tedy *Ker f* prvoideál.
Označíme-li $I=\{p\in F;$ absolutní člen p je sudé číslo$\}$, pak I je ideál (ověřte !) a přitom *Ker f*$\subset I$. Není tedy *Ker f* maximální ideál. Ukažte, že $F/$*Ker f*$\cong\mathbb{Z}$.

(32) Každý prvek , který má na nekonečně mnoha místech prvky různé od 1, má nekonečný retězec vlastních dělitelů, např. prvek $\langle1,2,1,2...\rangle$ má řetězec vlastních dělitelů $\langle1,1,1,2,1,2,..\rangle$, $\langle1,1,1,1,1,2,1,2..\rangle$,...atd.
Okruh nesplňuje EIR.

(33) Ukázali jsme v příkladu (30), že pro $\alpha,\beta\in\mathbb{Z}[\sqrt{d}]$ platí $\alpha|\beta \Rightarrow n(\alpha)|n(\beta)$. Zde se dělitelnost převede na dělitelnost v $\mathbb{Z}$, kde platí KŘVD. Například $\mathbb{Z}[\sqrt{-5}]$ nesplňuje podmínku JIR.

(35) Nechť p_n označuje n-té prvočíslo. Ukažte, že

$p_{n+1} \le p_1 \cdot \ldots \cdot p_n + 1$. Zřejmě platí $p_1 < 2^{2^1}$, $p_2 < 2^{2^2}$.

Indukcí dle n dokažte, že $p_n < 2^{2^n}$. Pak musí platit

$\pi(2^{2^n}) \ge n$. Pro každé $x \ge 2$ existuje $n\in\mathbb{N}$ tak, že

$e^{e^{n-1}} \le x \le e^{e^n}$ (dokažte!). Ukažte, že pro $n \ge 4$ platí $e^{n-1} > 2^n$.

Odtud pak máme

$$\pi(x) \ge \pi(e^{e^{n-1}}) \ge \pi(e^{2^n}) \ge \pi(2^{2^n}) \ge n \ge \ln(\ln x).$$

(36) Buď p prvočíslo, $p|a^{2^m}+1$.

Pak $a^{2^m} \equiv -1 \pmod p$, tedy

$$a^{2^n}-1 = a^{2^{n-m}\cdot 2^m}-1 = (a^{2^m})^{2^{n-m}}-1 \equiv (-1)^{2^{n-m}}-1 \equiv 1-1=0 \pmod p.$$

Platí tedy $p|a^{2^n}-1$. Pokud $p\ne 2$, pak $p\nmid a^{2^n}+1$ (proč?), a tedy tvrzení platí.

(37) (a) Pouze prvek 2. Všechny jednotky jsou právě prvky $\frac{c}{d}$, kde c,d jsou lichá čísla.

(b) Prvky 2 a 3. Zapište si prvek n ve tvaru

$$n = 2^x \cdot 3^y \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}, \quad p_1,\ldots,p_k \ne 2,3.$$

Jednotky jsou prvky $\frac{c}{d}$, kde $2\nmid c$ a $3\nmid c$.

(c) Pouze prvek x. Jednotky jsou prvky $\frac{f(x)}{g(x)}$, kde $f(0)\ne 0$.

(d) Prvky $x, x-1$. Jednotky jsou prvky $\frac{f(x)}{g(x)}$, kde $f(0)\cdot f(1)\ne 0$.

16. HLAVNÍ IDEÁLY

Ideál I okruhu $R=(A,+,\cdot)$ se nazývá <u>hlavní</u>, jestliže existuje prvek $a\in A$ tak, že I je generován množinou $\{a\}$, t.j. I je generován jediným generátorem a. Tuto skutečnost vyjadřujeme označením $I=I(a)$. Okruh R je <u>okruhem hlavních ideálů</u>, jestliže každý ideál okruhu R je hlavní. V okruhu hlavních ideálů platí

$$a|b \text{ právě když } I(b)\subseteq I(a).$$

<u>Příklady</u>:

(1) Nechť J,I jsou ideály oboru integrity hlavních ideálů. Pak $J=I$ právě když $J=I(a)$, $I=I(b)$ kde $a\|b$. Dokažte!

(2) Nechť $R=(A,+,\cdot)$ je unitární komutativní okruh, $a\in A$. Dokažte, že $I(a)=\{a\cdot x;\ x\in A\}$.

(3) Nechť $T_1,\dots,T_n$ jsou tělesa, $R=T_1\times\dots\times T_n$. Pak R je okruh hlavních ideálů. Dokažte!

(4) Dokažte, že $(\mathbb{Z},+,\cdot)$ je obor integrity hlavních ideálů.

(5) Ukažte, že ideál $I(2+i)$ v okruhu $\mathbb{Z}[i]$ je maximální.

(6) Sestrojte faktorový okruh

$$\mathbb{Z}[i]/I, \text{ kde } I=I(2+i),$$
$$\mathbb{Z}[\sqrt{2}]/I, \text{ kde } I=I(3+\sqrt{2}).$$

(7) Určete všechny hlavní ideály v okruzích $\mathbb{Z}_4$, $\mathbb{Z}_6$, $\mathbb{Z}_{10}$.

(8) Jsou všechny okruhy $\mathbb{Z}_n$ okruhy hlavních ideálů?

(9) Nechť R je euklidovský obor integrity, $a_1,\dots,a_n\in R$, nechť I je ideál generovaný množinou $\{a_1,\dots,a_n\}$. Dokažte, že pak I je hlavní ideál.

(10) Dokažte, že v okruhu $\mathbb{Z}[\sqrt{5}]$ ideál generovaný množinou $\{2,1-\sqrt{5}\}$ není hlavní.

(11) V okruhu $(\mathbb{Z},+,\cdot)$ je ideál $I(p)$ maximální, právě když p je prvočíslo. V tomto případě je $I(p)$ také prvoideál, a naopak. Dokažte!

Návody k řešení:

(1) Jestliže $I(a)=I(b)$, pak $a\in I(b)=\{k\cdot b;\ k\in R\}$, tedy $a=k\cdot b$ pro nějaké $k\in R$, odkud $b|a$. Podobně $a|b$, tedy $a\|b$.

(2) Stačí ukázat, že množina $\{a\cdot x;\ x\in A\}$ je ideál.

(3) Nechť $n=2$. Jediné ideály v $T_1\times T_2$ jsou:
$I_1=\{\langle 0,0\rangle\}$, $I_2=\{\langle t_1,0\rangle;\ t_1\in T_1\}$, $I_3=\{\langle 0,t_2\rangle;\ t_2\in T_2\}$, $I_4=T_1\times T_2$.
Ideál I_2 je generován prvkem $\langle 1,0\rangle$, I_3 prvkem $\langle 0,1\rangle$. Dokažte indukcí pro libovolné $n\in\mathbb{N}$.

(5) Jelikož $\mathbb{Z}[i]$ je eukleidovský obor integrity, stačí ukázat, že $2+i$ je ireducibilní prvek. Dle příkladu (30) kap.15 je $n(2+i)=2^2+1^2=5$, tedy $2+i$ je ireducibilní.

(6) I je dle (5) maximální, tedy $\mathbb{Z}[i]/I$ je těleso. Užijme složené zobrazení $f:\mathbb{Z}\longrightarrow\mathbb{Z}[i]\longrightarrow\mathbb{Z}[i]/I$, kde $f(a)=[a]_I$. Snadno se ukáže, že f je surjektivní homomorfismus, Ker $f=\{z\in\mathbb{Z};z\in I(2+i)\}$. Zřejmě $5=(2+i)(2-i)\in$Ker f, přitom Ker $f=I(5)$. Podle věty o homomorfismu platí $\mathbb{Z}[i]/I(2+i)\cong\mathbb{Z}/I(5)=\mathbb{Z}_5$.
Podobně $\mathbb{Z}[\sqrt{2}]$ je eukleidovský obor integrity. Prvek $3+\sqrt{2}$ je ireducibilní, jeho norma $n(3+\sqrt{2})=7$.
Podobně zobrazení $f:\mathbb{Z}\longrightarrow\mathbb{Z}[\sqrt{2}]\longrightarrow\mathbb{Z}[\sqrt{2}]/I$, kde $f(a)=[a]_I$, je surjektivní hommorfismus, jeho jádro Ker $f=I(7)$ (dokažte!), a tedy $\mathbb{Z}[\sqrt{2}]/I(3+\sqrt{2})\cong\mathbb{Z}_7$.

(7) V $\mathbb{Z}_4$ jsou to ideály $\{\overline{0}\}=I(\overline{0})$, $\mathbb{Z}_4=I(\overline{3})=I(\overline{1})$, $\{\overline{2},\overline{0}\}=I(\overline{2})$;
v $\mathbb{Z}_6$ pak $\{\overline{0}\}$, $\mathbb{Z}_6$, $\{\overline{2},\overline{4},\overline{0}\}=I(\overline{2})$, $\{\overline{3},\overline{0}\}=I(\overline{3})$;
v $\mathbb{Z}_{10}$ pak $\{\overline{0}\}$, $\mathbb{Z}_{10}$, $\{\overline{2},\overline{4},\overline{6},\overline{8},\overline{0}\}=I(\overline{2})=I(\overline{4})$, $\{\overline{5},\overline{0}\}=I(\overline{5})$.

(9) Zřejmě I je generován NSD$(a_1,\dots,a_n)=b$, t.j. $I=I(b)$.

(10) Předpokládejme naopak, že ideál $I(2,1-\sqrt{5})=I(a+b\sqrt{5})$ je hlavní. Ukažme nejprve, že $I(2,1-\sqrt{5})$ je vlastní ideál.

Například $2+\sqrt{5}\notin I(2,1-\sqrt{5})$, neboť pak by musely existovat prvky $a+b\sqrt{5}$, $c+d\sqrt{5}$ tak, že $2+\sqrt{5} = 2(a+b\sqrt{5})+(1-\sqrt{5})(c+d\sqrt{5})$.
Pak ale $2a+c-5d=2$, $2b-c+d=1$, pak $c-5d$ je sudé, tedy buď
(i) c a d jsou sudá, pak i $2b-c+d$ je sudé, což je spor,
(ii) c a d jsou lichá, pak $2b-c+d$ je sudé, což je spor.
Je tedy I vlastní ideál.
Pak není $a+b\sqrt{5}$ jednotka dělení (proč?), t.j. $a^2-5b^2\neq\pm1$.
Musí existovat $c,d\in\mathbb{Z}$ tak, že $(a+b\sqrt{5})(c+d\sqrt{5})=2$, tedy
$n(a+b\sqrt{5})\cdot n(c+d\sqrt{5})=(a^2-5b^2)(c^2-5d^2)=n(2)=4$.
Ukažme, že $a^2-5b^2\neq\pm2$ pro každé $a,b\in\mathbb{Z}$. Zřejmě pro
$a \equiv 0 \pmod 5$ je $a^2\equiv 0 \bmod 5$, $5a^2\equiv 0 \pmod 5$
$a \equiv 1 \pmod 5$ je $a^2\equiv 1 \pmod 5$
$a \equiv 2 \pmod 5$ je $a^2\equiv 4 \pmod 5$
$a \equiv 3 \pmod 5$ je $a^2\equiv 4 \pmod 5$
$a \equiv 4 \pmod 5$ je $a^2\equiv 1 \pmod 5$,
tedy $a^2\not\equiv 2,3 \pmod 5$, t.j. $a^2-5b^2\not\equiv\pm2 \pmod 5$.
Odtud $c^2-5d^2=\pm1$, je tedy $c+5d$ jednotka dělení.
Platí $2|a+b\sqrt{5}$ a $a+b\sqrt{5}|1-\sqrt{5}$, neboli $2|1-\sqrt{5}$, což není možné.

(11) Není-li p prvočíslo, pak $p=r\cdot s$, $r,s\neq\pm1,\pm p$.
Pak $I(p) \subset I(s)$, $I(p) \subset I(r)$.
$\mathbb{Z}$ je obor integrity hlavních ideálů, tedy prvoideály a maximální ideály splývají.

17. HOMOMORFISMY OKRUHŮ, CHARAKTERISTIKA

Nechť $(R,+,\cdot)$, $(S,+,\cdot)$ jsou okruhy a $h:R\to S$ zobrazení. Nazveme h homomorfismus okruhů, jestliže pro každé $a,b\in R$ platí

$$h(a+b)=h(a)+h(b),\ h(a\cdot b)=h(a)\cdot h(b).$$

Jelikož $(R,+)$ je abelovská grupa, plyne odtud, že homomorfismus okruhů je speciálně také homomorfismem příslušných abelovských grup, a tedy

$$h(0_R)=0_S\ ,\quad h(-a)=-h(a),$$

kde 0_R resp. 0_S je nulou okruhu R resp. S. Bijektivní homomorfismus se nazývá izomorfismus. Existuje-li izomorfismus okruhu R na okruh S, říkáme, že R,S jsou izomorfní, což zapisujeme symbolem $R\cong S$.

Je-li h homomorfismus okruhu R na okruh S, pak úplný vzor nuly 0_S, t.j. $h^{-1}(0_S)$, se nazývá jádro homomorfismu h, značí se $Ker\ h$. Zřejmě $Ker\ h$ je ideálem v okruhu R a dle Věty o homomorfismu platí: je-li h surjektivní homomorfismus okruhu R na S, pak $R/Ker\ h\cong S$.

Nechť a je prvek okruhu $(R,+,\cdot)$. Výraz $a+a+\ldots+a$ (n sčítanců) nazýváme přirozený násobek prvku a a označujeme symbolem $n\times a$. Řekneme, že prvek $a\in R$ je řádu k, je-li k nejmenší přirozené číslo, pro které $k\times a=0$. Zřejmě prvek 0 je řádu 1 a žádný jiný prvek okruhu není řádu 1. Je-li $(R,+,\cdot)$ obor integrity, pak všechny nenulové prvky mají stejný řád, tedy jejich řád je roven řádu jednotky. Charakteristikou okruhu R (resp. tělesa) nazýváme nejmenší přirozené číslo p takové, že pro každé $a\neq 0$ platí $p\times a=0$, symbolicky zapisujeme $char\ R=p$. Jestliže takové přirozené číslo neexistuje, pak říkáme, že R je charakteristiky 0, což zapisujeme $char\ R=0$.

Speciálně, každé číselné těleso (např. $\mathbb{Q},\mathbb{R},\mathbb{C}$) a každý číselný obor integrity (např. $\mathbb{Z}$, $\mathbb{Z}[i]$) jsou charakteristiky 0. Každé konečné těleso a každý konečný obor integrity mají konečnou nenulovou charakteristiku. Je-li p prvočíslo, pak těleso $\mathbb{Z}_p$ (zbytkových tříd $mod\ p$) je charakteristiky p. Platí také, že každé těleso charakteristiky p má p^n prvků (pro některé $n\in\mathbb{N}$).

Je-li T těleso, pak nejmenší těleso obsažené v T se nazývá

prvotěleso. Je-li *char* $T=0$, pak T obsahuje prvotěleso izomorfní s $\mathbb{Q}$, t.j. těleso racionálních čísel $\mathbb{Q}$ je nejmenší těleso charakteristiky 0 (až na izomorfismus). Je-li *char* $T=p$ (p prvočíslo), pak T obsahuje prvotěleso izomorfní se $\mathbb{Z}_p$, t.j. těleso zbytkových tříd *mod* p je (až na izomorfismus) nejmenší těleso charakteristiky p (jestliže p není prvočíslo, pak $\mathbb{Z}_p$ obsahuje dělitele 0, a tudíž není ani oborem integrity, ani tělesem).

Příklady:

(1) Uvažujme okruh M všech čtveřic $\langle a,b,c,d\rangle$, kde $a,b,c,d\in\mathbb{Q}$, s operacemi

$$\langle a,b,c,d\rangle+\langle e,f,g,h\rangle=\langle a+e,b+f,c+g,d+h\rangle$$

$$\langle a,b,c,d\rangle\cdot\langle e,f,g,h\rangle=\langle ac+bg,af+bh,ce+dg,cf+dh\rangle.$$

Ukažte, že $M_1=\{\langle a,0,c,d\rangle;\ a,c,d\in\mathbb{Q}\}$ a

$$M_2=\{\langle a,0,0,d\rangle;\ a,d\in\mathbb{Q}\}$$

jsou podokruhy okruhu M a zobrazení $h:M_1\longrightarrow M_2$ dané předpisem $h(\langle x,0,y,w\rangle)=\langle x,0,0,w\rangle$ je homomorfismus. Určete *Ker h* a $M_1/Ker\ h$.

(2) Jsou okruhy P, P' izomorfní ?

P:

+	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

·	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

P':

+	p	q	r	s
p	r	s	p	q
q	s	r	q	p
r	p	q	r	s
s	q	p	s	r

·	p	q	r	s
p	s	p	r	q
q	p	q	r	s
r	r	r	r	r
s	q	r	r	p

(3) Ukažte, že $P=\{\langle a,b,-b,a\rangle;\ a,b\in\mathbb{Z}\}$ je podokruh okruhu M z příkladu (1). Je zobrazení $h:\langle a,b,-b,a\rangle\longrightarrow a$ homomorfismus P do $(\mathbb{Z},+,\cdot)$?

(4) Ukažte, že zobrazení $h:\mathbb{Z}[\sqrt{3}]\longrightarrow\mathbb{Z}[\sqrt{3}]$, dané předpisem $h(a+b\sqrt{3})=a-b\sqrt{3}$, je izomorfismus.

(5) Ukažte, že zobrazení $h:\mathbb{C}\longrightarrow\mathbb{C}$ (těleso komplexních čísel), dané předpisem $h(a+bi)=a-bi$, je izomorfismus.

(6) Ukažte, že těleso M matic $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$, kde $a,b\in\mathbb{Q}$, je izomorfní s $\mathbb{Q}[\sqrt{2}]$.

(7) Ukažte, že neexistuje surjektivní homomorfismus oboru integrity $\mathbb{Z}[\sqrt{2}]$ na $\mathbb{Z}[\sqrt{3}]$.

(8) Ukažte, že jediný izomorfismus okruhu $P=\mathbb{Z}_2\times\mathbb{Z}_4$ na sebe je identické zobrazení.

(9) Ukažte, že těleso komplexních čísel $\mathbb{C}$ je izomorfní s tělesem matic M: $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, kde $a,b\in\mathbb{R}$.

(10) Dokažte, že následující dvojice okruhů jsou izomorfní:

(a) $\mathbb{Q}[\sqrt{2}]\cong\mathbb{Q}[-\sqrt{2}]$

(b) $\mathbb{Z}_2\times\mathbb{Z}_3\cong\mathbb{Z}_6$

(c) $\mathbb{Q}(\sqrt[3]{2})\cong\mathbb{Q}(\frac{-1+\sqrt{3}i}{2}\cdot\sqrt[3]{2})$.

(11) Nechť P_1,P_2 jsou okruhy, $h:P_1\longrightarrow P_2$ homomorfismus.

(a) Je-li I prvoideál v P_2, je $h^{-1}(I)$ prvoideál v P_1 ?

(b) Je-li h surjektivní a J je maximální ideál v P_2, dokažte, že $h^{-1}(J)$ je maximální ideál v P_1.

(c) Je-li h surjektiví a I je maximální ideál v P_1. Je $h(I)$ maximální ideál v P_2?

(12) Nechť T je těleso charakteristiky p. Pak pro každé $a,b\in T$ a pro libovolné $k\in\mathbb{N}$ platí

$$(a+b)^{p^k} = a^{p^k}+b^{p^k}.$$

Dokažte!

(13) Určete charakteristiky okruhů $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_6$, $\mathbb{Z}_8$.

(14) Nechť R je okruh charakteristiky 2, $a,b\in R$. Jestliže $a\cdot b=b\cdot a$, pak $(a+b)^2= a^2+b^2=(a-b)^2$. Dokažte!

(15) Najděte charakteristiku tělesa T , ve kterém platí

$$(1+1+1+1)^2=(1+1)^5.$$

(16) Dokažte, že je-li *char* $T=p$, p prvočíslo, pak pro $a,b\in T$ platí

$$a^p=b^p \Rightarrow a=b.$$

(17) Dokažte, že v každém okruhu R tvoří množina všech prvků konečného řádu podokruh okruhu R.

(18) Ukažte příklad okruhu charakteristiky 0, kde každý prvek je konečného řádu.

(19) Nechť R je obor integrity, *char* $R=p$. Nechť $R^p=\{a^p;\ a\in R\}$. Dokažte:

(a) R^p je podokruh okruhu R,

(b) zobrazení $h:\ a \longrightarrow a^p$ je izomorfismus R na R^p,

(c) je-li R konečný, pak $R=R^p$.

(20) Malá Fermatova věta: Nechť $a\in\mathbb{Z}$, $n\in\mathbb{N}$ a platí $(a,n)=1$. Označme $\varphi(n)$ počet všech přirozených čísel menších než n a nesoudělných s n. Pak v $\mathbb{Z}_n$ platí:

$$\overline{a^{\varphi(n)}}=\overline{1} \quad (\text{neboli } a^{\varphi(n)}\equiv 1 \ (mod\ n)).$$

(21) Speciální případ příkladu (20) : Je-li p prvočíslo, $a\in\mathbb{Z}_p$, $a\neq 0$, pak $a^{p-1}\equiv 1$ $(mod\ p)$.

(22) Nechť $p>2$ je prvočíslo, $a\in\mathbb{Z}_p$. Pak $a^2=\overline{1}$ právě když $a=\overline{1}$ nebo $a=\overline{p-1}$. Dokažte!

(23) Wilsonova věta: Nechť p je prvočíslo. Pak v $\mathbb{Z}_p$ platí:

$$\overline{(p-1)!}+\overline{1}=0.$$

Dokažte!

<u>**Návody k řešení:**</u>

(1) *Ker* $h=\{\langle 0,0,y,0\rangle; y\in\mathbb{Q}\}$, h je zřejmě surjektivní, tedy dle věty o homomorfismu platí $M_1/Ker\ h\cong M_2$.

(2) Ano, P,P' jsou izomorfní, izomorfismem je zobrazení

$$a \longrightarrow r,\ b \longrightarrow q,\ c \longrightarrow s,\ d \longrightarrow p.$$

(3) $h(\langle a,b,-b,a\rangle+\langle a',b',-b',a'\rangle)= h(\langle a+a',b+b',-b-b',a+a'\rangle)=a+a'=$
$=h(\langle a,b,-b,a\rangle)+h(\langle a',b',-b',a'\rangle)$.
Dále, $h(\langle a,b,-b,a\rangle\cdot\langle a',b',-b',a'\rangle)=$
$=h(\langle aa'-bb',ab'+ba',-ba'-ab',-bb'+aa'\rangle)= aa'-bb'$,
$h(\langle a,b,-b,a\rangle)\cdot h(\langle a',b'-b',a'\rangle)= aa'$, tedy h není homomorfismus.

(6) Ukažte, že zobrazení $f:\mathbb{Q}[\sqrt{2}]\longrightarrow M$, kde $f(a+b\sqrt{2})=\begin{pmatrix} a & b \\ 2b & a\end{pmatrix}$, je hledaný izomorfismus.

(7) Předpokládejme, že h je takový surjektivní homomorfismus. Zřejmě $h(1)=1$. Pak $h(\sqrt{2})=a+b\sqrt{3}$ pro některé $a,b\in\mathbb{Z}$, avšak $(h(\sqrt{2}))^2=h(\sqrt{2})\cdot h(\sqrt{2})=h(\sqrt{2}\cdot\sqrt{2})=h(2)=h(1+1)=h(1)+h(1)=1+1=2$.
Tedy $(a+b\sqrt{3})^2=2$, avšak taková celá čísla a,b neexistují.

(8) Ukažte nejprve, že množina $\{\langle\bar{1},\bar{1}\rangle,\langle\bar{1},\bar{0}\rangle\}$ generuje P. Je-li h izomorfismus P na P, pak $h(\langle\bar{1},\bar{1}\rangle)=\langle\bar{1},\bar{1}\rangle$, neboť $\langle\bar{1},\bar{1}\rangle$ je jednotka v P, $h(\langle\bar{1},\bar{0}\rangle)=\langle\bar{1},\bar{0}\rangle$, neboť $\langle\bar{1},\bar{0}\rangle$ je jediný prvek různý od nuly, splňující $x+x=\bar{0}$, $x\cdot x=x$. Jelikož $\langle\bar{1},\bar{1}\rangle$, $\langle\bar{1},\bar{0}\rangle$ jsou generátory P a zobrazují se na sebe, pak také

$$h(\langle a,b\rangle)=\langle a,b\rangle \text{ pro každé } \langle a,b\rangle\in P.$$

(9) Ukažte, že zobrazení h: $\mathbb{C}\to M$ takové, že $h(z)=h(a+bi)=\begin{pmatrix} a & b \\ -b & a\end{pmatrix}$, je izomorfismus.

(10) (a) Ukažte, že zobrazení f: $\mathbb{Q}[\sqrt{2}]\longrightarrow \mathbb{Q}[-\sqrt{2}]$ takové, že $h(a+b\sqrt{2})=a-b\sqrt{2}$, je izomorfismus těles.

(b) Ukažte, že zobrazení h: $\mathbb{Z}_6\longrightarrow \mathbb{Z}_2\times\mathbb{Z}_3$ dané předpisem:

$\bar{0}\to\langle\bar{0},\bar{0}\rangle$, $\bar{1}\to\langle\bar{1},\bar{1}\rangle$, $\bar{2}\to\langle\bar{0},\bar{2}\rangle$, $\bar{3}\to\langle\bar{1},\bar{0}\rangle$, $\bar{4}\to\langle\bar{0},\bar{1}\rangle$, $\bar{5}\to\langle\bar{1},\bar{2}\rangle$,

je hledaný izomorfismus.

(c) Ověřte, že $\mathbb{Q}(\sqrt[3]{2})=\{a+b\cdot\sqrt[3]{2}+c\cdot\sqrt[3]{4};\ a,b,c\in\mathbb{Q}\}$;
dále, číslo $\xi=\frac{-1+\sqrt{3}i}{2}$ je třetí odmocnina z 1, tedy $\xi^3=1$.
Pak $\mathbb{Q}(\xi\cdot\sqrt[3]{2})=\{a+b\cdot\xi\cdot\sqrt[3]{2}+c\cdot\xi^2\cdot\sqrt[3]{4}\ ;\ a,b,c\in\mathbb{Q}\}$.
Ověřte, že zobrazení $h:\mathbb{Q}(\sqrt[3]{2})\longrightarrow \mathbb{Q}(\xi\cdot\sqrt[3]{2})$ dané předpisem:

$$h(a+b\cdot\sqrt[3]{2}+c\cdot\sqrt[3]{4})=a+b\cdot\xi\cdot\sqrt[3]{2}+c\cdot\xi^2\cdot\sqrt[3]{4},$$

je izomorfismus těchto těles.

(11) (a) Nechť $a,b\in h^{-1}(I)$, tedy $h(a\cdot b)\in I$, $h(a)\cdot h(b)\in I$. Jelikož I

je prvoideál, je buď $h(a)\in I$ nebo $h(b)\in I$, tedy buď $a\in h^{-1}(I)$ nebo $b\in h^{-1}(I)$.

(b) Nechť I' je ideál obsahující $h^{-1}(J)$ a prvek $a\notin h^{-1}(J)$. Pak $h(a)\notin J$, tedy ideál I, obsahující J a prvek $h(a)$, je roven P_2 (proč?).
Ukažme, že $h^{-1}(I)=I'$. Nechť $z\in I$, tedy
$z=\Sigma(r_i\cdot j_i\cdot s_i)+r\cdot h(a)\cdot s$, kde $j_i\in J$. Jelikož h je surjekce, existují $j_i'\in P_1$ tak, že $h(j_i')=j_i$, neboli
$j_i'=h^{-1}(j_i)\in h^{-1}(J)$. Pak
$h^{-1}(z)=h^{-1}((\Sigma(r_i\cdot j_i\cdot s_i)+r\cdot h(a)\cdot s)=$
$\Sigma(h^{-1}(r_i)\cdot h^{-1}(j_i)\cdot h^{-1}(s_i))+h^{-1}(r)\cdot a\cdot h^{-1}(s)$,
kde $h^{-1}(j_i)\in h^{-1}(J)$. Tedy $h^{-1}(z)\in I'$ (proč?), tudíž
$h^{-1}(I)\subseteq I'$. Obrácená inkluze je zřejmá, tedy $I'=h^{-1}(I)=P_1$, a tedy $h^{-1}(J)$ je maximální ideál.

(c) Nechť $b\in P_2$, $b\notin h(I)$. Jelikož h je surjekce, je $b=h(a)$ pro nějaký prvek $a\in P_1$. Zřejmě $a\notin I$, neboť pak by $b=h(a)\in h(I)$. Ideál I' generovaný ideálem I a prvkem a je roven P_1 (proč?), tedy každý prvek $x\in P_1$ se dá vyjádřit ve tvaru:
$x=\Sigma\ (r_k\cdot i_k\cdot s_k)+r\cdot a\cdot s$. Pak
$h(x)=\Sigma\ \ (h(r_k)\cdot h(i_k)\cdot h(s_k))+h(r)\cdot h(a)\cdot h(s)$, tedy $h(x)$ padne do ideálu generovaného $h(I)$ a prvkem b. Jelikož h je surjekce a x libovolný prvek, je ideál generovaný $h(I)$ a b roven P_2. Je tedy $h(I)$ maximální ideál.

(12) Nechť $k=1$. Pak

$$(a+b)^p=a^p+p\times(a^{p-1}b)+\binom{p}{2}\times(a^{p-2}\ b^2)+\ldots+\binom{p}{p}\times b^p\ =\ a^p+b^p.$$

Dále indukcí dle k:

$$(a+b)^{p^{k+1}}=((a+b)^{p^k})^p=(a^{p^k}+b^{p^k})^p=a^{p^{k+1}}+b^{p^{k+1}}.$$

(14) $(a+b)^2=\ (a+b)\cdot(a+b)\ =\ a^2+ab+ba+b^2=\ a^2+b^2;$
$(a-b)^2=\ (a-b)\cdot(a-b)\ =\ a^2-ab-ba+b^2=\ a^2+b^2.$

(15) $(1+1+1+1+1)^2=\ (5\times1)\cdot(5\times1)\ =\ 25\times1,$
$(1+1)^5=\ (2\times1)^5=\ 2^5\times1\ =\ 32\times1.$
Tedy musí v T platit: $25\times1\ =\ 32\times1$, t.j. $(32-25)\times1=0$, t.j. $7\times1=0$. Odtud char $T=7$.

(16) Jestliže $a^p=b^p$, pak $(a-b)^p = a^p-b^p = 0$, neboť char $T=p$.
Odtud $a-b=0$, t.j. $a=b$.

(18) Např. $R= \Pi\{\mathbb{Z}_n;\ n\in\mathbb{N}_1\}$, kde $\mathbb{N}_1=\{2,3,4,\dots\}$.

(19) **(a)** Nechť $a,b\in R^p$. Pak $a^p-b^p=(a-b)^p$ (dokažte!) a
$a^p\cdot b^p=(a\cdot b)^p$.

(b) Je-li $a^p=b^p$, pak $a^p-b^p=0$. Jelikož R neobsahuje dělitele nuly, je $a-b=0$, tedy $a=b$. Surjekce zobrazení h je zřejmá, pro $a,b\in R$ platí:
$h(a+b)=(a+b)^p=a^p+b^p=h(a)+h(b)$ (proč?),
$h(ab)=(ab)^p=a^p\cdot b^p=h(a)\cdot h(b)$.

(c) Vždy $R\supseteq R^p$. Dle (b) je h bijekce mezi konečnými množinami a tedy $R=R^p$.

(20) Dokažte toto tvrzení: prvek $\bar{a}\in\mathbb{Z}_n$ je v $\mathbb{Z}_n$ nedělitel nuly právě když $(a,n)=1$.
Buďte tedy $\bar{a}_1,\dots,\bar{a}_{\phi(n)}$ všichni nedělitelé nuly v $\mathbb{Z}_n$.
Ukažte, že pak množina $\{\bar{a}\cdot\bar{a}_1,\dots,\bar{a}\cdot\bar{a}_{\phi(n)}\}$ je opět množina všech nedělitelů nuly, tedy

$$\bar{a}_1\cdot\bar{a}_2\cdot\dots\cdot\bar{a}_{\phi(n)} = \bar{a}\cdot\bar{a}_1\cdot\dots\cdot\bar{a}\cdot\bar{a}_{\phi(n)}\ ,\ \text{tedy}\ \bar{1}=(\bar{a})^{\phi(n)}.$$

(22) Je-li $(\bar{a})^2=\bar{1}$, pak $(\bar{a}-\bar{1})\cdot(\bar{a}+\bar{1})=\bar{0}$. Jelikož $\mathbb{Z}_p$ je těleso, je buď $\bar{a}=\bar{1}$ nebo $\bar{a}=-\bar{1}=\overline{p-1}$.

(23) Buďte $\bar{1},\bar{2},\dots,\overline{p-1}$ všechny prvky ze $\mathbb{Z}_p$. Jelikož $\mathbb{Z}_p$ je těleso a podle cvičení (22) jsou k sobě invertibilní pouze prvky $\bar{1},\overline{p-1}$, je $\bar{2}\cdot\bar{3}\cdot\dots\cdot\overline{p-2}=\bar{1}$ (proč ?),
tedy $\bar{1}\cdot\bar{2}\cdot\bar{3}\cdot\dots\cdot\overline{p-2}\cdot\overline{p-1}= \overline{p-1} = \overline{-1}$,
tedy $\overline{(p-1)!}=\overline{-1}$, $\overline{(p-1)!+1}=\bar{0}$.

18. VNOŘENÍ OBORU INTEGRITY DO TĚLESA

Nechť $(R,+,\cdot)$, $(S,+,\cdot)$ jsou okruhy, $h:R\to S$ homomorfismus okruhů. Je-li h injektivní, nazývá se <u>vnoření</u> . Je-li h vnoření okruhu R do S, pak $h(R)$ je podokruh okruhu S izomorfní s R.

Je-li D obor integrity, pak vždy existuje těleso T a homomorfismus $h:D\to T$ tak, že h je vnoření. Nejmenší těleso T s touto vlastností se nazývá <u>podílové těleso</u> k oboru integrity D a označuje se $Q(D)$. Tedy $Q(D)$ je takové těleso, že existuje vnoření $h:D\to Q(D)$ a pro každé těleso T a vnoření $g:D\to T$ existuje vnoření $k:Q(D)\to T$, viz. obr.:

$$\begin{tikzcd} D \arrow[rr, "h"] \arrow[dr, "g"'] & & Q(D) \arrow[dl, dotted, "k"] \\ & T & \end{tikzcd}$$

Dá se dokázat, že lze (až na izomorfismus) položit $Q(D)=D\times(D\setminus\{0\})/\Theta$, kde Θ je kongruence daná předpisem

$$\langle\langle a,b\rangle,\langle c,d\rangle\rangle\in\Theta \iff ad = bc.$$

Na $D\times(D\setminus\{0\})$ jsou operace $\oplus,\odot$ dané předpisem :

$$\langle a,b\rangle\oplus\langle c,d\rangle = \langle ad+bc,bd\rangle$$

$$\langle a,b\rangle\odot\langle c,d\rangle = \langle ac,bd\rangle.$$

<u>Příklady</u>:

(1) Dokažte, že podílové těleso k oboru integrity $(\mathbb{Z},+,\cdot)$ je (až na izomorfismus) právě těleso racionálních čísel $\mathbb{Q}$.

(2) Dokažte, že podílové těleso k $\mathbb{Z}[i]$ je $\mathbb{Q}[i]$.

(3) Dokažte, že nejmenší obor integrity obsahující $\mathbb{Z}$ a číslo $\frac{1}{2}$ je $R=\{\frac{n}{2^k}\ ;\ k\in\mathbb{N},\ n\in\mathbb{Z}\}$. Sestrojte podílové těleso k R.

(4) Ukažte, že je-li T těleso, pak podílové těleso k T je izomorfní s T.

(5) Sestrojte podílové těleso $Q(D)$ k oboru integrity D regulárních matic $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$, $a,b\in\mathbb{Z}$. Je $Q(D)$ izomorfní s tělesem

regulárních matic $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$, kde $a,b\in\mathbb{Q}$?

(6) Sestrojte podílové těleso k $\mathbb{Z}[\sqrt{2}]$.

(7) Sestrojte podílové těleso k $\mathbb{Z}[\sqrt[3]{2}]$.

(8) Nechť D je obor integrity , char $D=0$, e jeho jednotka. Dokažte, že množina $R=\{n\times e;\ n\in\mathbb{Z}\}$ je rovněž obor integrity, který je podoborem integrity oboru D.

(9) Je-li D obor integrity, pak okruh polynomů jedné neurčité $D[x]$ je rovněž obor integrity. Určete podílové těleso k $D[x]$.

Návody k řešení :

(2) Ukažte, že zobrazení $\varphi : Q(\mathbb{Z}[i])\to \mathbb{Q}[i]$ takové, že $\varphi(\langle a+bi,c+di\rangle) = \dfrac{a+bi}{c+di}$, $(c+di\neq 0)$, je hledaný izomorfismus.

(3) Je to $\mathbb{Q}$.

(4) Nechť $Q(T)$ je podílové těleso k T. Ukažte, že zobrazení $\varphi : Q(T) \to T$ takové, že $\varphi(\langle a,b\rangle) = a\cdot b^{-1}$ $(b\neq 0)$, je hledaný izomorfismus.

(5) Tyto regulární matice skutečně tvoří obor integrity, neboť (z regularity) neobsahují dělitele nuly, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ je jednotka;
ověřte, že násobení je komutativní. Podílové těleso je izomorfní s tělesem všech regulárních matic tvaru $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$, kde ale již $a,b\in\mathbb{Q}$. Izomorfismus je dán zobrazením

$$\varphi(\langle A,B\rangle) = A\cdot B^{-1}.$$

(6) Je to $\mathbb{Q}[\sqrt{2}]$. (Přesvědčte se, že je to vskutku těleso !)

(7) Je to $\mathbb{Q}[\sqrt[3]{2}]$.

(9) Je to těleso všech racionálních funkcí lomených (s koeficienty z D).

19. OKRUHY POLYNOMŮ JEDNÉ NEURČITÉ

Nechť R je okruh, nechť $x \notin R$. Okruhem polynomů jedné neurčité nad R rozumíme množinu všech formálních výrazů

$\sum_{i=0}^{n} a_i x^i$, kde $a_i \in R$, s operacemi $+, \cdot$ definovanými takto :

$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i = \sum_{i=0}^{k} (a_i + b_i) x^i$, kde $k = \max(m,n)$, přičemž klademe $a_i = 0$ pro $n < i \leq k$, $b_i = 0$ pro $m < i \leq k$,

$\left(\sum_{i=0}^{n} a_i x^i \right) \cdot \left(\sum_{i=0}^{m} b_i x^i \right) = \sum_{i=0}^{n+m} c_i x^i$, kde pro každé $k = 0, 1, .., n+m$ klademe $c_k = \sum_{i=0}^{k} a_i b_{k-i}$, neboli $c_k = \sum_{i+j=k} a_i b_j$.

Je-li R unitární, klademe $x^0 = 1$. Zpravidla vyšetřujeme polynomy jedné neurčité nad oborem integrity. Je-li R obor integrity, pak $R[x]$ je rovněž obor integrity. Je-li R Gaussův, je i $R[x]$ Gaussův. Je-li R těleso, je $R[x]$ Eukleidův obor integrity, kde eukleidovská funkce je stupeň polynomu. Přitom stupněm polynomu $f(x) = \sum_{i=0}^{n} a_i x^i$ nazýváme číslo n, je-li $a_n \neq 0$.

Polynom $f(x)$ se nazývá normovaný, je-li $a_n = 1$.

Polynom $f(x)$ je primitivní, je-li $NSD(a_0, a_1, .., a_n) = 1$.

Polynom stupně 3 se nazývá kubický,

polynom stupně 2 se nazývá kvadratický,

polynom stupně 1 se nazývá lineární,

polynom stupně 0 se nazývá konstantní.

Polynom $f(x) \equiv 0$ se nazývá nulový. Nulový polynom nemá stupeň.

Polynom $f(x)$ nad R je ireducibilní, jestliže neexistují polynomy $h(x), g(x) \in R[x]$ tak, že $f(x) = g(x) \cdot h(x)$, přičemž jsou stupně alespoň prvního.

Je-li $f(x) = \sum_{i=0}^{n} a_i x^i$ polynom nad R a jestliže $b \in R$, pak hodnotou polynomu $f(x)$ v bodě b nazýváme prvek $a_0 + a_1 b + \ldots + a_n b^n = \sum_{i=0}^{n} a_i b^i$.

Příklady:

(1) Určete součet a součin polynomů

(a) $4 + x + 2x^2$, $1 + 2x + 3x^2$ v $\mathbb{Z}_5[x]$

(b) $1 + 5x + 2x^2$, $7 + 2x + 3x^2 + 4x^3$ v $\mathbb{Z}_8[x]$

(c) $2 + 2x + x^3$, $1 + x + x^2 + x^4$ v $\mathbb{Z}_3[x]$.

(2) Dokažte, že pro žádný obor integrity D není $D[x]$ tělesem.

(3) Určete největšího společného dělitele polynomů

(a) $x^5 + x^4 - x^3 - 3x + 2$, $x^3 + 2x^2 - x - 2$ nad $\mathbb{Q}$

(b) $3x^4 - 6x^3 + 12x^2 + 8x - 6$, $x^3 - 3x^2 + 6x - 3$ nad $\mathbb{Q}$

(c) $x^5 - 3ix^3 - 2ix^2 - 6$, $x^2 - 2i$ nad $\mathbb{C}$

(d) $x^5 + 3x^3 + x^2 + 2x + 2$, $x^4 + 3x^3 + 3x^2 + x + 2$ nad $\mathbb{Z}_5$

(e) $x^5 + x^3 + x$, $x^4 + 2x^3 + 2x$ nad $\mathbb{Z}_3$.

(4) Určete všechny polynomy tvaru $3x^2 + cx + 4$ ireducibilní nad $\mathbb{Z}_5$.

(5) Rozložte na součin polynomů tyto polynomy nad

(i) $\mathbb{Q}$, (ii) $\mathbb{R}$, (iii) $\mathbb{C}$:

(a) $x^4 - 1$

(b) $x^4 - 4x^2 - x + 2$

(c) $6x^4 + 5x^3 + 4x^2 - 2x - 1$

(d) $4x^5 + 4x^4 - 13x^3 - 11x^2 + 10x + 6$.

(6) Rozložte na součin polynomů tyto polynomy :

(a) $x^2 + 1$ nad $\mathbb{Z}_5$

(b) $x^2 + x + 1$ nad $\mathbb{Z}_3$

(c) $2x^2 + 2x + 1$ nad $\mathbb{Z}_5$

(d) $3x^3 + 4x^2 + 3$ nad $\mathbb{Z}_5$.

(7) Dokažte, že v $\mathbb{R}[x]$ ($\mathbb{R}$ je těleso čísel reálných), jsou ireducibilními tyto polynomy :

(a) $x^2 + 1$

(b) $x^4 + 1$

(c) $x^6 + x^3 + 1$

(d) $x^p - px + 2p - 1$, kde p je prvočíslo.

(8) Ukažte, že polynom $f(x)=x^m-p$ je ireducibilní nad $\mathbb{Z}[x]$, kde $m\in\mathbb{Z}$ a p je prvočíslo.

(9) Najděte všechna řešení rovnice $x^m=1$ v $\mathbb{Z}_p$, p prvočíslo.

(10) Nechť R je obor integrity. V oboru integrity $R[x]$ definujeme: $W=\{f(x)\in R[x];\ f(0)=f(1)=0\}$. Dokažte, že

(a) W je podokruh $R[x]$

(b) W je generovaný množinou $\{x(x-1), x^2(x-1)\}$.

(11) Nechť K je těleso. Které z následujících množin jsou podokruhy resp. ideály v $K[x]$?:

(a) $\{f(x)\in K[x];\ f(0)=0\}$

(b) $\{f(x)\in K[x];\ f'(0)=0\}$

(c) $\{f(x)\in K[x];\ f''(0)=0\}$.

(12) Určete v okruhu $\mathbb{Z}[x]$ hlavní ideál, generovaný prvkem $x-1$, a dokažte, že $\mathbb{Z}[x]/I(x-1)\cong\mathbb{Z}$.

(13) Dokažte, že pro zadané okruhy R,S je $h\colon R\longrightarrow S$ homomorfismus okruhů; určete $Ker\ h$:

(a) $R=\mathbb{Q}[x]$, $S=\mathbb{R}$, $h\colon f(x)\to f(\sqrt{2})$

(b) $R=R[x]$, $S=\mathbb{R}$, $h\colon f(x)\to f(\sqrt{2})$.

(14) Nechť F je těleso, $f(x)\in F[x]$, $f(x)$ je ireducibilní nad $F[x]$. Nechť $I(f(x))$ je hlavní ideál generovaný prvkem $f(x)$ v $F[x]$. Dokažte, že $F[x]/I(f(x))$ je těleso.

(15) Analogicky jako v příkladu (14) dokažte, že $\mathbb{R}[x]/I(x^2+1)\cong\mathbb{C}$, kde $\mathbb{R}$ je těleso čísel reálných a $\mathbb{C}$ je těleso čísel komplexních.

(16) Určete největšího společného dělitele $d(x)$ polynomů $f(x)=6x^5+7x^4-5x^3-2x^2-x+1$, $g(x)=6x^4-5x^3-19x^2-13x-5$ nad $\mathbb{Q}[x]$ a určete polynomy $s(x),t(x)\in\mathbb{Q}[x]$ tak, aby platilo

$$d(x)=s(x)\cdot f(x)+t(x)\cdot g(x).$$

(17) Dokažte, že x^2-3 je ireducibilní polynom v $\mathbb{Q}[x]$ a platí

$$\mathbb{Q}[x]/I(x^2-3)\cong\mathbb{Q}[\sqrt{3}].$$

(18) Nechť P je okruh, který má dělitele nuly, nechť $f(x)\in P[x]$.

Pak, je-li $f(x)$ dělitel nuly v $P[x]$, existuje $a \in P$, $a \neq 0$ tak, že $a \cdot f(x)=0$. Dokažte!

(19) Dokažte, že P nemá dělitele nuly, právě když $P[x]$ nemá dělitele nuly.

(20) Které z následujících množin tvoří podokruh okruhu $\mathbb{Z}[x]$:

(a) polynomy $f(x)$ takové, že $5 | f(5)$

(b) polynomy $f(x)=\sum_{i=0}^{n} a_i x^i$ takové, že $7 | a_0$

(c) součet koeficientů $f(x)$ je roven 0

(d) koeficient při x je roven 0

(e) $1+(x^2+1)\cdot g(x)$, kde $g(x) \in \mathbb{Z}[x]$

(f) $2f(x)+(x^2+1)\cdot g(x)$, kde $f(x), g(x) \in \mathbb{Z}[x]$

(g) $xf(x)+(x^2+1)\cdot g(x)$, kde $f(x), g(x) \in \mathbb{Z}[x]$.

(21) Najděte všechny polynomy jedné neurčité nad $\mathbb{Z}_2[x]$ a $\mathbb{Z}_3[x]$, které jsou stupně nejvýše 5.

(22) Ukažte, že v $\mathbb{Z}_2[x]$ platí:

$$(x+\overline{1})^2=x^2+\overline{1}\ ,\quad (x+\overline{1})^4=x^4+\overline{1}.$$

(23) Ukažte, že pro polynomy $f(x)=x^2+x+\overline{2}$, $g(x)=x^3+x^2+\overline{2}$ v $\mathbb{Z}_3[x]$ platí $f(a)=g(a)$ pro každé $a \in \mathbb{Z}_3$.

(24) Nechť p je prvočíslo. Pak polynom $f(x)=x^{p-1}+x^{p-2}+\ldots+x+1$, (tzv. polynom dělení kruhu), je ireducibilní nad $\mathbb{Z}[x]$. Dokažte!

<u>Návody k řešení:</u>

(4) Jsou to polynomy $3x^2+4$, $3x^2+x+4$, $3x^2+4x+4$.

(6) **(a)** $(x+2)(x+3)$

(d) $(x+2)^2\cdot(3x+2)$

(b),(c) jsou nerozložitelné.

(7) **(a),(b)**- binomické polynomy, najděte kořeny!

(d) funkce nabývá minima pro $x=1$, $p(1)=p>0$.

(8) Dle Eisensteinova kriteria ireducibility, $p\nmid 1$, $p|0$, $p^2\nmid p$.

(10) Zřejmě W je generován prvky $x^n(x-1)$, avšak pro $n\geq 3$ je $x^n(x-1)=x(x-1)\cdot x^{n-2}(x-1)+x^{n-1}(x-1)$, tedy je generován jen prvky $x(x-1)$ a $x^2(x-1)$.

(11) **(a)** Je to ideál.

(b) Je-li $f(x)=a_n x^n+\ldots+a_1 x+a_0$, pak

$$f'=(n\times a_n)x^{n-1}+\ldots+(2\times a_2)x+a_1.$$

Je tedy $f'(0)=0$ právě když $a_1=0$. Je-li $g'(0)=0$, kde $g=b_n x^n+\ldots+b_1 x+b_0$, pak $(f-g)'(0)=0$.

Dále $f\cdot g=a_0b_0+(a_0b_1+b_0a_1)x+\ldots$, je tedy $(f\cdot g)'(0)=0$ právě když $a_0b_1+b_0a_1=0$. Tudíž jde o podokruh. Nemusí to být ideál.

(c) $f''(0)=0$ právě když $2\times a_2=0$. Je-li $f''(0)=g''(0)$, pak $(f-g)''(0)=0$ právě když $2\times(a_2-b_2)=0$, tedy $a_2-b_2+a_2-b_2=0$. Dále, $(f\cdot g)''(0)$ právě když

$2\times(a_1b_1+a_2b_0+a_0b_2)=0$, t.j. $2\times(a_1b_1+a_0b_2)=0$.

Odtud je zřejmé, že množina už nemusí být ideál.

(12) Je zřejmé, že $I(x-1)=\{f\in\mathbb{Z}[x];\ f(1)=0\}$. Uvažujte zobrazení ϕ: $\mathbb{Z}[x]\longrightarrow\mathbb{Z}$ takové, že $\varphi(f)=f(1)$. Ukažte, že ϕ je surjektivní homomorfismus, $Ker\ \varphi=I(x-1)$, tedy $\mathbb{Z}[x]/I(x-1)\cong\mathbb{Z}$.

(13) **(a)** $Ker\ h=\{f\in\mathbb{Q}[x];\ f(\sqrt{2})=0\}$.

(b) Podobně jako (a).

(14) Ukažme, že $I(f(x))$ je maximální ideál. Nechť $g(x)\notin I(f(x))$; pak $(f(x),g(x))=1$, neboť f je ireducibilní. Pak existují polynomy $v(x)$, $u(x)$ takové, že $f(x)\cdot v(x)+g(x)\cdot u(x)=1$ (proč?), tedy $1\in I(f(x),g(x))$, tj. $I(f(x),g(x))=F[x]$. Je tedy faktorový okruh tělesem.

(15) Polynom x^2+1 je ireducibilní nad $\mathbb{R}[x]$. Uvažujme zobrazení φ: $\mathbb{R}[x]\to\mathbb{C}$ takové, že $\varphi(f)=f(i)$. Ukažte, že φ je surjektivní homomorfismus s jádrem $I(x^2+1)$.

(16) $d(x)=x^2+\frac{2}{3}x+\frac{1}{3}$ a platí $d(x)=-\frac{1}{279}(8x-23)f(x)+\frac{1}{32}(8x^2-7x-14)g(x)$.

(17) Ukažte, že x^3-3 nemá racionální kořeny. Uvažujte zobrazení $\varphi\colon \mathbb{Q}[x]\to\mathbb{Q}[\sqrt{3}]$ takové, že $\varphi(f)=f(\sqrt{3})$. Ukažte, že jádro $Ker\ \varphi=I(x^2-3)$.

(24) Platí totiž

$$f(x+1)=\frac{(x+1)^p-1}{(x+1)-1}=x^{p-1}+\binom{p}{1}x^{p-2}+\ldots+\binom{p}{p-2}x+\binom{p}{p-1},$$

všechny koeficienty $f(x+1)$ s vyjímkou nejvyššího jsou dělitelné p (neboť $\binom{p}{k}=\frac{p(p-1)\ldots(p-k+1)}{k!}$), ale $\binom{p}{p-1}=p$, tedy absolutní člen není dělitelný p^2, tedy dle Eisensteinova kriteria ireducibility je $f(x+1)$ ireducibilní, a tedy i $f(x)$ je ireducibilní.

20. POLYNOMY VÍCE NEURČITÝCH, SYMETRICKÉ POLYNOMY

Nechť R je okruh a $x_1,\dots,x_n$ (pro $n\geq 1$) jsou takové symboly, že $x_i\notin R$ $(i=1,\dots,n)$. Indukcí definujeme

$$R[x_1,\dots,x_k]=R[x_1,\dots,x_{k-1}][x_k]$$

pro $k=1,\dots,n$, přičemž pro $k=1$ klademe $R[x_1,\dots,x_{k-1}]=R$. Zřejmě tedy $R[x_1]$ je okruh polynomů jedné neurčité nad R. Pak $R[x_1,\dots,x_n]$ nazveme <u>okruh polynomů n neurčitých nad R</u>.

Z definice vyplývá, že každý polynom n neurčitých nad R lze jednoznačně psát ve tvaru

$$f(x_1,\dots,x_n) = \sum_{i_1=0}^{k_1}\sum_{i_2=0}^{k_2}\dots\sum_{i_n=0}^{k_n} a_{i_1 i_2\dots i_n}\, x_1^{i_1}x_2^{i_2}\dots x_n^{i_n},$$

kde $k_1,\dots,k_n$ jsou celá nezáporná čísla.

Analogicky jako pro polynomy jedné neurčité platí:

R je obor integrity, právě když $R[x_1,\dots x_n]$ je obor integrity,
R je obor integrity s jednoznačným rozkladem, právě když $R[x_1,\dots x_n]$ je obor integrity s jednoznačným rozkladem.

Polynom $f(x_1,\dots,x_n)\in R[x_1,\dots x_n]$ nazveme <u>symetrický</u>, jestliže $f(x_1,\dots,x_n)=f(x_{\pi(1)},\dots,x_{\pi(n)})$ pro každou permutaci π množiny $\{1,\dots,n\}$.

Je-li $f(x_1,\dots,x_n)\in R[x_1,\dots x_n]$, označme symbolem $\sum f(x_1,\dots,x_n)$ polynom n neurčitých, který vznikne jako součet všech polynomů $f(x_{\pi(1)},\dots,x_{\pi(n)})$, kde se sčítá přes všechny permutace $\pi\in S_n$. Zřejmě $\sum f(x_1,\dots,x_n)$ je vždy symetrický polynom. Je-li

$$f(x_1,\dots,x_n) = \sum_{i_1=0}^{k_1}\sum_{i_2=0}^{k_2}\dots\sum_{i_n=0}^{k_n} a_{i_1 i_2\dots i_n}\, x_1^{i_1}x_2^{i_2}\dots x_n^{i_n},$$

pak číslo $i_1+i_2+\dots+i_n$ nazveme <u>stupněm</u> členu

$a_{i_1 i_2\dots i_n}x_1^{i_1}x_2^{i_2}\dots x_n^{i_n}$, n-tici $\langle i_1,i_2,\dots,i_n\rangle$ nazveme <u>výškou</u> tohoto členu.

Symetrický polynom $f(x_1,\dots,x_n)$ nazveme <u>homogenní</u> (neboli <u>forma</u>), mají-li všechny členy stejný stupeň. Každý symetrický polynom je zřejmě součtem homogenních polynomů.

Symetrické polynomy n neurčitých tvaru $\sigma_k = \sum x_1 x_2 \ldots x_k$ se nazývají <u>elementární symetrické formy n neurčitých</u>.

Zřejmě tedy

$$\sigma_1 = \sum x_1 = x_1 + x_2 + \ldots + x_n$$
$$\sigma_2 = \sum x_1 x_2 = x_1 x_2 + x_1 x_3 + \ldots + x_{n-1} x_n$$
$$\cdot$$
$$\cdot$$
$$\sigma_n = \sum x_1 x_2 \ldots x_n = x_1 x_2 \ldots x_n .$$

Hlavní věta o symetrických polynomech tvrdí, že každý symetrický polynom nad $\mathbb{R}$ lze jednoznačně vyjádřit jakožto polynom v elementárních symetrických formách $\sigma_1, \sigma_2, \ldots, \sigma_n$.

<u>Příklady</u>:

(1) Ukažte, že zobrazení $h: P \longrightarrow S$ je homomorfismus a určete Ker h:
$P = \mathbb{R}[x,y]$, $S = \mathbb{R}[x]$, $h(f(x,y)) = f(x,x)$.

(2) Nechť K je těleso. Které z následujících množin polynomů tvoří ideál v $K[x,y]$?:

(a) polynomy s absolutním členem rovným 0;

(b) polynomy stupně ≥ 2 s absolutním členem rovným 0;

(c) polynomy splňující $f(x,y) = f(x,-y)$, přičemž předpokládejme, že *char* $K \neq 2$;

(d) symetrické polynomy;

(e) polynomy $(x-1) \cdot f(x,y) + 4 \cdot g(x,y)$, kde $f(x,y), g(x,y) \in K[x,y]$.

(3) Ukažte, že ideál v okruhu $K[x,y]$, kde K je těleso, generovaný množinou $\{x,y\}$, není hlavní.

(4) Nechť K je těleso. Je množina

$$M = \{f(x,y) \in K[x,y];\ f(0,0) = 0,\ \frac{\partial f(x,y)}{\partial x}(0,0) = 0\}$$

ideálem v $K[x,y]$?

(5) Určete všechny homomorfismy okruhu $\mathbb{Q}[x,y]/I(x^2+y^2-1)$ do $\mathbb{Q}$.

(6) Napište obecný tvar formy druhého a třetího stupně o třech

neurčitých.

(7) Napište všechny vzájemně různé polynomy, které vzniknou permutacemi neurčitých v polynomech

(a) $x_1^3+x_2^3-2x_1x_2+x_3$

(b) $x_1-x_1x_2+x_2$.

(8) Napište symetrický polynom v $\mathbb{Z}[x_1,x_2,x_3]$, jehož vedoucí člen je $3x_1^2x_2^2x_3$.

(9) Napište symetrickou formu v neurčitých x_1,x_2,x_3,x_4, která má jeden člen roven $x_2^2x_3^3$, a jejíž každý člen obsahuje právě dvě neurčité.

(10) Uveďte příklad symetrického polynomu, jehož vedoucí člen nemá největší stupeň.

(11) Doplňte následující polynomy vhodnými členy tak, aby vznikly symetrické polynomy; tyto lexikálně uspořádejte:

(a) $2x_1^2x_2-3x_2x_3+\ldots$ (vzhledem k x_1,x_2,x_3)

(b) $x_1x_2^2+x_2^3+x_1x_2x_3+\ldots$ (- " -)

(c) $x_1^3+x_1^2+x_1+\ldots$ (vzhledem k x_1,x_2)

(d) $x_1^3x_2^2x_3+\ldots$ (vzhledem k x_1,x_2,x_3)

(e) $x_1^2x_2^2+2x_1x_2x_3+3x_1^3+\ldots$ (vzhledem k x_1,x_2,x_3,x_4).

(12) Napište obecný tvar symetrického polynomu **(a)** druhého, **(b)** třetího stupně o 3 neurčitých.

(13) Napište obecný tvar symetrické formy **(a)** třetího stupně o 4 neurčitých, **(b)** čtvrtého stupně o 3 neurčitých.

(14) Vyjádřete pomocí elementárních symetrických forem:

(a) $x_1^2x_2+x_1x_2^2$

(b) $x_1^2x_2+x_1^2x_3+x_1x_2^2+x_1x_3^2+x_2^2x_3+x_2x_3^2$

(c) $x_1^3+x_2^3+x_3^3-3x_1x_2x_3$

(d) $(x_1+x_2)(x_1+x_3)(x_2+x_3)$

(e) $(x_1^2+x_2^2)(x_1^2+x_3^2)(x_2^2+x_3^2)$

(f) $(x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2$

(g) $(x_1x_2+x_3x_4)(x_1x_3+x_2x_4)(x_1x_4+x_2x_3)$.

(15) Vyjádřete pomocí elementárních symetrických forem:

(a) $\sum x_1^2$ (b) $\sum x_1^2x_2$ (c) $\sum x_1^3$

(d) $\sum x_1^2x_2x_3$ (e) $\sum x_1^2x_2^2$ (f) $\sum x_1^3x_2$.

(16) Vyjádřete pomocí elementárních symetrických forem:

(a) $\sum x_1^2x_2^2$ (b) $\sum x_1^3x_2$ (c) $\sum x_1^4$

(d) $\sum x_1^2x_2^2x_3$ (e) $\sum x_1^3x_2x_3$ (f) $\sum x_1^3x_2^2$

(g) $\sum x_1^4x_2$ (h) $\sum x_1^5$ (i) $\sum x_1^2x_2^2x_3x_4$

(j) $\sum x_1^2x_2^2x_3^2$.

Návody k řešení :

(1) $h(f+g) = (f+g)(x,x) = f(x,x)+g(x,x) = h(f)+h(g)$,
$h(f\cdot g) = (f\cdot g)(x,x) = f(x,x)\cdot g(x,x) = h(f)\cdot h(g)$,
$Ker\ h = \{f(x,y)\in P;\ f(x,x)=0$ pro každé $x\in P\}$.

(2) (a) ANO

(b) NE, polynom 0 není stupně ≥ 2.

(c) NE. Nechť $f(x,y) = f(x,-y)$, $g(x,y) = g(x,-y)$. Pak
$(f-g)(x,y)=f(x,y)-g(x,y)=f(x,-y)-g(x,-y)=(f-g)(x,-y)$,
$(f\cdot m)(x,y) = f(x,y)\cdot m(x,y) = f(x,-y)\cdot m(x,y)$;
např. pro $f(x,y) = y^2$, $m(x,y) = y$, je $f\cdot m = y^3$,
obecně $(f\cdot m)(x,y)\neq(f\cdot m)(x,-y)$.

(d) NE, např. pro $f(x,y)=x+y+z$, $g(x,y)=x$, je
$f\cdot g=x^2+xy+xz$, ten ale není symetrický.

(e) ANO, je to ideál generovaný polynomy $x-1$ a 4.

(3) Předpokládejme, že ideál generovaný množinou $\{x,y\}$ je hlavní. Nechť $a(x,y)$ je generátor daného ideálu. Pak $x,y\in I(a(x,y))$, tedy $x = a(x,y)\cdot f(x,y)$ pro nějaký polynom f. Pak $a(x,y)$ nesmí záviset na y. Podobně $y \in I(a(x,y))$, tedy $a(x,y)$ nezávisí na x, je tedy $a(x,y)$ konstanta. Pak ovšem $I(a(x,y)) = K[x,y]$. Ale např. polynom konstantní nelze pouze pomocí x a y nagenerovat.

(4) Jsou-li $f,g \in M$, pak $(f-g)(0,0) = f(0,0)-g(0,0) = 0$,

$\frac{\partial(f-g)(0,0)}{\partial x} = \frac{\partial f}{\partial x}(0,0) - \frac{\partial g}{\partial x}(0,0) = 0.$

Nechť $m \in K[x,y]$. Pak $(f\cdot m)(0,0) = f(0,0)\cdot m(0,0) = 0$,

$\frac{\partial(m\cdot f)}{\partial x}(0,0) = m\cdot\frac{\partial f}{\partial x}(0,0)+f\cdot\frac{\partial m}{\partial x}(0,0) = m(0,0)\cdot 0 +$

$+ f(0,0)\cdot\frac{\partial m}{\partial x}(0,0) = 0$, tedy M je ideál.

(5) Označme p přirozený homomorfismus okruhu $\mathbb{Q}[x,y]$ na faktorový okruh $\mathbb{Q}[x,y]/I(x^2+y^2-1)$ (kde $I(x^2+y^2-1)$ je hlavní ideál v $\mathbb{Q}[x,y]$ generovaný prvkem x^2+y^2-1). Nechť

g: $\mathbb{Q}[x,y]/I(x^2+y^2-1) \longrightarrow \mathbb{Q}$ je homomorfismus. Pak složené zobrazení $p\circ g$ je homomorfismus $\mathbb{Q}[x,y]$ do $\mathbb{Q}$, pro který

$$f(x,y) \longrightarrow f(u,v) \text{ pro } u=p\circ g(x),\ v=p\circ g(y)\in\mathbb{Q}.$$

Avšak $g([x^2+y^2-1]_I)=0$, tedy také $(p\circ g)(x^2+y^2-1)=0$, t.j. $u^2+v^2-1=0$. Zřejmě lze racionální čísla u,v vyjádřit ve tvaru $u=\frac{a}{c}$, $v=\frac{b}{c}$, kde $a,b,c\in\mathbb{Z}$, tedy $a^2+b^2=c^2$. Odtud zobrazení

g: $f(x,y) \longrightarrow f\left(\frac{a}{c}, \frac{b}{c}\right)$, kde $a^2+b^2=c^2$, $a,b,c\in\mathbb{Z}$, je hledaný homomorfismus.

(6) druhého stupně:

$a_1x_1^2+ a_2x_2^2+ a_3x_3^2+ a_4x_1x_2+ a_5x_1x_3+ a_6x_2x_3$

třetího stupně:

$a_1x_1^3+a_2x_2^3+a_3x_3^3+a_4x_1^2x_2+a_5x_1^2x_3+a_6x_1x_2^2+a_7x_2^2x_3+a_8x_1x_3^2+$

$+a_9x_2x_3^2+a_{10}x_1x_2x_3.$

(7) (a) $x_1^3+x_2^3-2x_1x_2+x_3$; $x_1^3+x_3^3-2x_1x_3+x_2$; $x_2^3+x_3^3-2x_2x_3+x_1$.

(b) Tento polynom je symetrický.

(8) Je to polynom $3x_1^2x_2^2x_3+3x_1^2x_2x_3^2+3x_1x_2^2x_3^2$.

(9) $x_1^3x_2^2+x_1^3x_3^2+x_1^3x_4^2+x_1^2x_2^3+x_1^2x_3^3+x_1^2x_4^3+x_2^3x_3^2+x_2^3x_4^2+x_2^2x_3^3+x_2^2x_4^3+$

$+x_3^3x_4^2+x_3^2x_4^3.$

(10) Např. $x_1^2-x_1x_2x_3+x_2^2+x_3^2.$

(11) (a) $2x_1^2x_2+ 2x_1^2x_3+ 2x_1x_2^2- 3x_1x_2+ 2x_1x_3^3- 3x_1x_3+ 2x_2^2x_3+$
$+ 2x_2x_3^2- 3x_2x_3$

(b) $x_1^3+ x_1^2x_2+ x_1^2x_3+ x_1x_2^2+ x_1x_2x_3+ x_1x_3^2+ x_2^3+ x_2^2x_3+ x_2x_3^2+ x_3^3$

(c) $x_1^3+ x_1^2+ x_1+ x_2^3+ x_2^2+ x_2$

(d) $x_1^3x_2^2x_3+ x_1^3x_2x_3^2+ x_1^2x_2^3x_3+ x_1^2x_2x_3^3+ x_1x_2^3x_3^2+ x_1x_2^2x_3^3$

(e) $3x_1^3+ x_1^2x_2^2+ x_1^2x_3^2+ x_1^2x_4^2+ 2x_1x_2x_3+ 2x_1x_2x_4+ 2x_1x_3x_4+ 3x_2^3+$
$+x_2^2x_3^2+ x_2^2x_4^2+ 2x_2x_3x_4+ 3x_3^3+ x_3^2x_4^2+ 3x_4^3.$

(12) (a) $a(x_1^2+ x_2^2+ x_3^2)+ b(x_1x_2+ x_1x_3+ x_2x_3)+ c(x_1+ x_2+ x_3)+ d,$

(b) $a(x_1^3+ x_2^3+ x_3^3)+ b(x_1^2x_2+ x_1x_2^2+ x_1^2x_3+ x_1x_3^2+ x_2^2x_3+ x_2x_3^2)+$
$+cx_1x_2x_3+ d(x_1^2+ x_2^2+ x_3^2)+ e(x_1x_2+ x_1x_3+ x_2x_3)+$
$+f(x_1+ x_2+ x_3)+ g.$

(13) (a) $a(x_1^3+ x_2^3+ x_3^3+ x_4^3)+ b(x_1^2x_2+ x_1x_2^2+ x_1^2x_3+ x_1x_3^2+ x_1^2x_4+ x_1x_4^2+$
$+x_2^2x_3+ x_2x_3^2+ x_2^2x_4+ x_2x_4^2+ x_3^2x_4+ x_3x_4^2)+$
$+c(x_1x_2x_3+ x_1x_2x_4+ x_1x_3x_4+ x_2x_3x_4),$

(b) $a(x_1^4+ x_2^4+ x_3^4)+ b(x_1^3x_2+ x_1x_2^3+ x_1^3x_3+ x_1x_3^3+ x_2^3x_3+ x_2x_3^3)+$
$+c(x_1^2x_2^2+ x_1^2x_3^2+ x_2^2x_3^2)+ d(x_1^2x_2x_3+ x_1x_2^2x_3+ x_1x_2x_3^2).$

(14) (a) $\sigma_1\sigma_2$ (b) $\sigma_1\sigma_2-3\ \sigma_3$ (c) $\sigma_1^3-3\ \sigma_1\sigma_2$

(d) $\sigma_1\sigma_2-\ \sigma_3$

(e) $\sigma_1^2\sigma_2^2-\ 2\ \sigma_1^3\sigma_3-\ 2\ \sigma_2^3+\ 4\ \sigma_1\sigma_2\sigma_3-\ \sigma_3^2$

(f) $\sigma_1^2\sigma_2^2 - 4\,\sigma_1^3\sigma_3 - 4\,\sigma_2^3 + 18\,\sigma_1\sigma_2\sigma_3 - 27\,\sigma_3^2$

(g) $\sigma_1^2\sigma_4 + \sigma_3^2 - 4\,\sigma_2\sigma_4$.

Poznámka. Jako vzor uvedeme řešení cvičení (e). Budiž dána symetrická forma $P(x_1,x_2,x_3) = (x_1^2+x_2^2)(x_1^2+x_3^2)(x_2^2+x_3^2)$. Její vedoucí člen je $x_1^4x_2^2$. Při lexikálním uspořádání by za sebou následovaly symetrické formy šestého stupně tří neurčitých x_1,x_2,x_3, přičemž vedoucí členy by byly $x_1^4x_2^2$; $x_1^4x_2x_3$; $x_1^3x_2^3$; $x_1^3x_2^2x_3$; $x_1^2x_2^2x_3^2$. Jim u neurčitých odpovídají výšky: (4,2,0); (4,1,1); (3,3,0); (3,2,1); (2,2,2); těm pak zase v příslušných součinech mocnin elementárních symetrických forem odpovídají mocnitelé 4-2,2-0; 4-1,1-1,1-0; 3-3,3-0; 3-2,2-1,1-0; 2-2,2-2,2-0; tj. 2,0; 3,0,1; 0,3; 1,1,1; 0,0,2. Bude tedy

$$P(x_1,x_2,x_3) = \sigma_1^2\sigma_2^2 + A\,\sigma_1^3\sigma_3 + B\,\sigma_2^3 + C\,\sigma_1\sigma_2\sigma_3 + D\,\sigma_3^2\ ,$$

kde A,B,C,D jsou číselné koeficienty. Určíme je tím, že si zvolíme čtyři jednoduché pomocné rovnice, jež sestavíme z vhodně volených kořenů x_1,x_2,x_3 ; pak určíme číselné hodnoty jim odpovídajících elementárních symetrických forem i hodnotu symetrické formy $P(x_1,x_2,x_3)$. Pomocí těchto hodnot obdržíme čtyři lineární rovnice pro koeficienty A,B,C,D. Vše zapíšeme do tabulky.

Kořeny x_1	x_2	x_3	*Rovnice*	σ_1	σ_2	σ_3	P
1	1	0	$(x-1)^2 = 0$ *čili* $x^2-2x+1 = 0$	2	1	0	2
2	-1	-1	$(x-2)(x+1)^2 = 0$ *čili* $x^3 -3x-2 = 0$	0	-3	2	50
1	-2	-2	$(x-1)(x+2)^2 = 0$ *čili* $x^3+3x^2 -4 = 0$	-3	0	4	200
1	-1	-1	$(x^2-1)(x+1) = 0$ *čili* $x^3+x^2-x-1 = 0$	-1	-1	-1	8

$$2 = 4 + B$$
$$50 = -27B + 4D$$
$$200 = -108A + 16D$$
$$8 = 1 - A - B + C + D$$

Odtud postupně určíme: $B = -2$, $D = -1$, $A = -2$, $C = 4$. Je tedy

$$P(x_1, x_2, x_3) = \sigma_1^2\sigma_2^2 - 2\,\sigma_1^3\sigma_3 - 2\,\sigma_2^3 + 4\,\sigma_1\sigma_2\sigma_3 - \sigma_3^2.$$

(15) (a) $\sigma_1^2 - 2\,\sigma_2$ (b) $\sigma_1\sigma_2 - 3\,\sigma_3$

(c) $\sigma_1^3 - 3\,\sigma_1\sigma_2 + 3\,\sigma_3$ (d) $\sigma_1\sigma_3 - 4\,\sigma_4$

(e) $\sigma_2^2 - 2\,\sigma_1\sigma_3 + 2\,\sigma_4$ (f) $\sigma_1^2\sigma_2 - \sigma_1\sigma_3 - 2\,\sigma_2^2 + 4\,\sigma_4$.

(16) (a) $\sigma_2^2 - 2\,\sigma_1\sigma_3 + 2\,\sigma_4$

(b) $\sigma_1^2\sigma_2 - \sigma_1\sigma_3 - 2\,\sigma_2^2 + 4\,\sigma_4$

(c) $\sigma_1^4 - 4\,\sigma_1^2\sigma_2 + 2\,\sigma_2^2 + 4\,\sigma_1\sigma_3 - 4\,\sigma_4$

(d) $\sigma_2\sigma_3 - 3\,\sigma_1\sigma_4 + 5\,\sigma_5$

(e) $\sigma_1^2\sigma_3 - 2\,\sigma_2\sigma_3 - \sigma_1\sigma_4 + 5\,\sigma_5$

(f) $\sigma_1\sigma_2^2 - 2\,\sigma_1^2\sigma_3 - \sigma_2\sigma_3 + 5\,\sigma_1\sigma_4 - 5\,\sigma_5$

(g) $\sigma_1^3\sigma_2 - 3\,\sigma_1\sigma_2^2 - \sigma_1^2\sigma_3 + 5\,\sigma_2\sigma_3 + \sigma_1\sigma_4 - 5\,\sigma_5$

(h) $\sigma_1^5 - 5\,\sigma_1^3\sigma_2 + 5\,\sigma_1\sigma_2^2 + 5\,\sigma_1^2\sigma_3 - 5\,\sigma_2\sigma_3 - 5\,\sigma_1\sigma_4 + 5\,\sigma_5$

(i) $\sigma_2\sigma_4 - 4\,\sigma_1\sigma_5 + 9\,\sigma_6$

(j) $\sigma_3^2 - 2\,\sigma_2\sigma_4 + 2\,\sigma_1\sigma_5 - 2\,\sigma_6$.

21. KOŘENY POLYNOMŮ

Nechť $f(x)$ je polynom nad tělesem P, nechť K je nadtěleso tělesa P. Prvek $\alpha \in K$ se nazývá kořen polynomu $f(x)$, jestliže po dosazení prvku α za x obdržíme rovnost $f(\alpha)=0$. Je-li $f(x)$ polynom nad tělesem P, pak nejmenší nadtěleso tělesa P, do kterého patří všechny kořeny polynomu $f(x)$, se nazývá kořenové těleso polynomu $f(x)$.

Těleso P se nazývá algebraicky uzavřené, jestliže každý polynom $f(x)$ stupně alespoň prvního nad tělesem P má v tělese P alespoň jeden kořen (a tedy všechny své kořeny).

Uveďme nejdůležitější věty o kořenech polynomů.

(1) Prvek $\alpha \in K$, kde K je nadtěleso tělesa P, je kořenem polynomu $f(x)$ nad P, je-li polynom $f(x)$ v $K[x]$ dělitelný lineárním polynomem $x-\alpha$, t.j. v $K[x]$ platí $f(x)=(x-\alpha)\cdot g(x)$.
Polynom $x-\alpha$ nazýváme kořenový činitel polynomu $f(x)$.
Tento výsledek je důsledkem věty Bézoutovy.

(2) Věta Viètova: Nechť $f(x) = \sum_{i=0}^{n} a_i x^i$ je normovaný polynom n-tého stupně nad tělesem komplexních čísel (t.j. $a_n=1$), nechť $\alpha_1,\dots,\alpha_n$ jsou jeho kořeny. Pak platí

$$a_{n-1} = -(\alpha_1+\alpha_2+\dots+\alpha_n) = -\sigma_1$$

$$a_{n-2} = \alpha_1\alpha_2+\alpha_1\alpha_3+\dots+\alpha_{n-1}\alpha_n = \sigma_2$$

$$\vdots$$

$$a_0 = (-1)^n \alpha_1\alpha_2\dots\alpha_n = \sigma_n,$$

tedy koeficient a_{n-k} je roven elementární symetrické formě σ_k v proměnných $\alpha_1,\dots,\alpha_n$ se znaménkem $(-1)^k$.

(3) Tzv. základní věta algebry: Těleso komplexních čísel $\mathbb{C}$ je algebraicky uzavřené, neboli každý polynom $f(x)$ stupně aspoň prvního nad $\mathbb{C}$ má v $\mathbb{C}$ aspoň jeden kořen, neboli každý

polynom $f(x)$ nad $\mathbb{C}$ stupně aspoň prvního má v $\mathbb{C}$ všechny své kořeny, jejichž počet se rovná stupni $f(x)$, uvažujeme-li každý i s jeho násobností.

(4) Má-li polynom $f(x)\in\mathbb{R}[x]$ komplexní kořen $a+bi$, pak má i kořen $a-bi$.

Je-li $f(x)$ polynom nad tělesem T a $b\in T$, pak hodnotu $f(b)$ určujeme pomocí tzv. <u>Hornerova schematu</u>: je-li $f(x)=\sum_{i=0}^{n} a_i x^i$, pak do 1.řádku schematu napíšeme koeficienty $a_n, a_{n-1}, \ldots, a_1, a_0$ (včetně těch, které jsou =0), do druhého řádku pak pod prvek a_{n-1} píšeme výsledek součinu $a_n \cdot b$, do 3.řádku pod a_n opíšeme a_n, pod a_{n-1} (z 1.řádku) napíšeme součet $a_{n-1}+a_n \cdot b$. Analogicky pod a_{n-i}-tý prvek (v 1.ř.) píšeme ve druhém řádku součin $a_{n-i}+a_{n-i+1} \cdot b$. Takto pokračujeme, až pod a_0 ve 3.řádku je hodnota $f(b)$.

např. pro $f(x)=5x^4-7x^3+x-3$ a $b=2$ dostáváme

5	-7	0	1	-3
	$5\cdot 2=10$	6	12	26
	$10-7=3$	6	13	$23=f(2)$

(5) Prvek $\alpha\in K$ se nazývá algebraický nad P kde $P\subseteq K$, je-li α kořenem některého polynomu $f(x)\in P[x]$.

<u>Příklady</u>:

(1) Určete kořenové těleso polynomu $x^3-3\in\mathbb{Q}[x]$.

(2) Určete kořeny polynomů

(a) x^2+1 nad $\mathbb{Z}_5$

(b) x^2+x+1 nad $\mathbb{Z}_3$

(c) $3x^3+4x^2+3$ nad $\mathbb{Z}_5$.

(3) Nechť $a,b,c\in\mathbb{Z}$, $\sqrt{c}\notin\mathbb{Z}$. Je-li $a+b\sqrt{c}$ kořenem polynomu $f(x)$ nad $\mathbb{Z}[x]$, pak je také $a-b\sqrt{c}$ kořenem $f(x)$. Dokažte!

(4) Určete polynomy nejnižšího stupně nad $\mathbb{Z}[x]$, které mají kořeny

(a) $\sqrt{3}$, 2

(b) i, 3

(c) 1, $2+3\sqrt{5}$

(d) $-1+i$, $2-3i$

(e) dvojnásobný kořen $1+i$.

(5) Ukažte, že nejnižší stupeň polynomu, jehož kořen je $\sqrt{3}+2i$, je nad $\mathbb{Q}$ stupně 4, ale nad $\mathbb{R}$ stupně 2.

(6) Zadejte polynom nejnižšího stupně nad $\mathbb{Q}$, který má kořen $\sqrt{i}$.

(7) Najděte zbývající kořeny polynomu $f(x)=x^4+4x^2+8x-4$, je-li jeden jeho kořen $1+i$.

(8) Najděte polynom čtvrtého stupně nad $\mathbb{R}$ s koeficientem $a_4=1$, který má dvojnásobný kořen $2+i$.

(9) Určete čísla a,b,c tak, aby byla kořeny polynomu

$$f(x)=x^3+ax^2+bx+c.$$

(10) Ukažte, že je-li komplexní číslo $a+bi$ algebraický prvek nad $\mathbb{Q}$, pak je také $a-bi$ algebraický prvek nad $\mathbb{Q}$.

(11) Ukažte, že je-li $z=a+bi$ algebraický prvek nad $\mathbb{Q}$, pak jsou algebraické i prvky $\frac{1}{2}(z+\bar{z})$, $\frac{i}{2}(\bar{z}-z)$, a naopak.

(12) Dokažte, že pro racionální číslo q jsou čísla $\sin q\pi$, $\cos q\pi$ algebraická nad $\mathbb{Q}$.

(13) Najděte rozkladová tělesa polynomů

(a) x^2-2 (c) x^4-2 (e) x^4+x^2+1.

(b) x^3-2 (d) x^4+2

(14) Ukažte, že rozkladové těleso polynomu $x^2+\bar{1}\in\mathbb{Z}_3[x]$ je devítiprvkové (char = 3) a má prvky $\bar{0}$, $\bar{1}$, $\bar{2}$, a, $a+\bar{1}$, $a+\bar{2}$, $a+a$, $a+a+\bar{2}$, $a+a+\bar{1}$, kde $a^2=\bar{2}$.

(15) Nechť je dán polynom $f(x)=x^3+3x+6$ nad $\mathbb{Q}$. Určete polynom $g(y)=y^3+b_1y^2+b_2y+b_3$, jehož kořeny jsou druhými mocninami kořenů polynomu $f(x)$ (aniž řešíte rovnici $f(x)=0$).

(16) Výšky v_a, v_b, v_c trojúhelníka jsou kořeny polynomu $f(x)=x^3-47x^2+720x-3600$. Vypočtěte poloměr ρ kružnice vepsané

tomuto trojúhelníku.

(17) Určete součet druhých mocnin kořenů polynomu $x^3+3x-3=0$.

(18) (a) Nechť $\alpha_1,,\alpha_2, \alpha_3$ jsou kořeny polynomu x^3-x^2-4x+1. Určete $\sum \alpha_1^3\alpha_2$.

(b) Nechť $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ jsou kořeny polynomu $x^4+x^3-2x^2-3x+1$. Určete $\sum \alpha_1^3\alpha_2\alpha_3$.

(19) Dokažte, že součet třetích mocnin kořenů polynomu $x^n+a_{n-2}x^{n-2}+\ldots+a_0$, kde a_{n-3} je číslo celé, je vždy dělitelný číslem 3.

(20) Polynom $x^n+a_{n-2}x^{n-2}+a_{n-4}x^{n-4}+\ldots$ nad $\mathbb{R}[x]$ nemůže mít všechny kořeny reálné kladné ani reálné záporné. Dokažte!

(21) Jaký je tvar polynomu, který má alespoň jeden kořen roven 0?

(22) Za jaké podmínky je polynom

(a) x^3+px+q dělitelný polynomem x^2+mx-1

(b) x^4+px^2+q dělitelný polynomem x^2+mx+1?

(23) Vypočtěte $f(a)$ pro

(a) $f(x)=x^4-3x^3+6x^2-10x+16, \quad a=4$

(b) $f(x)=x^5+(1+2i)x^4-(1+3i)x^2+7, \quad a=-2-i$

(c) $f(x)=x^2-2x+3, \quad a=2,31$

(d) $f(x)=2x^3-3x^2+2x-5, \quad a=3,99$.

(24) Dokažte, že $(x-7)$ je kořenový činitel polynomu $2x^5-17x^4+23x^3-18x^2+29x-7$,
$(x-2)$ je kořenový činitel polynomu $x^5-x^4-13x^3+13x^2+36x-36$.

(25) Jestliže víte, že $f(x)=x^5-5x^3+4x$ má kořeny $\alpha_1=0$, $\alpha_2=1$, $\alpha_3=2$, vypočítejte zbývající kořeny α_4, α_5.

(26) Určete kořeny polynomu $x^4-3x^3+6x^2-3x+5$, jestliže víte, že jeden kořen je $\alpha_1=i$.

(27) Ověřte Hornerovým schematem, že polynom x^5-5x^3+4x má kořeny

$-2,-1,0,1,2$.

(28) Sestavte polynom čtvrtého stupně, který má kořeny $5,2,-3,-4$.

(29) Sestavte obecný tvar polynomů 5. stupně, které mají čtyři kořeny $-1,0,1/3,3$ a pátý kořen a.

(30) Sestrojte polynom pátého stupně, který má trojnásobný kořen 2 a dvojnásobný kořen 3.

(31) Ověřte, že polynom $x^4-5x^3+6x^2+4x-8$ má trojnásobný kořen 2, a určete čtvrtý kořen.

(32) Polynom $x^6-7x^5+22x^4-40x^3+44x^2-28x+8$ má dvojnásobný kořen $1+i$. Určete ostatní kořeny.

(33) Pomocí Hornerova schematu vyjádřete $f(x)$ pomocí mocnin $x-a$, je-li dáno

(a) $f(x)=3x^3+2x^2+1, \quad a=2$

(b) $f(x)=x^4+2x^3-3x^2-4x+1, \quad a=-1$

(c) $f(x)=x^5, \quad a=1$

(d) $f(x)=x^4-8x^3+24x^2-50x+90, \quad a=2$.

(34) Nechť má kvadratický polynom $x^2+a_1x+a_0$ kořeny α_1,α_2. Určete polynom $y^2+b_1y+b_0$, který má kořeny $\alpha_1-\beta,\alpha_2-\beta$, aniž kořeny α_1,α_2 určujete.

<u>Návody k řešení :</u>

(1) Je to $\mathbb{Q}[\sqrt[3]{3}]$. Jeho prvky jsou tvaru $a+b\sqrt[3]{3}+c\sqrt[3]{9}$, kde $a,b,c\in\mathbb{Q}$.

(2) **(a)** jsou to $\overline{2},\overline{3}$ **(b)** je to $\overline{1}$

(c) Polynom se dá rozložit na součin $(x+2)^2(3x+2)$, tedy jeho kořeny v $\mathbb{Z}_5$ jsou $\overline{1}$ a dvojnásobný kořen $\overline{3}$.

(4) **(a)** $(x-\sqrt{3})(x+\sqrt{3})(x-2)$

(b) $(x-i)(x+i)(x-3)$

(c) $(x-1)(x-2-3\sqrt{5})(x-2+3\sqrt{5})$

(d) $(x+1-i)(x+1+i)(x-2+3i)(x-2-3i)$

(e) $(x-1-i)^2(x-1+i)^2$.

(9) Musí platit: $c=-abc$, $ab+bc+ac=b$, $a+b+c=-a$.

(a) je-li $c=0$, pak $ab=b$, $2a+b=0$.

(i) je-li $b=0$, pak $a=0$, tedy $a=b=c=0$.

(ii) je=li $b\neq 0$, pak $a=1$, $b=-2$.

(b) je-li $c\neq 0$, pak $ab=-1$, $bc+ac=b+1$, $2a+b+c=0$, tedy $c=-2a-b$; dosazením do druhé rovnice dostaneme soustavu

$$ab=-1,\ -(2a+b)(a+b)=b+1, \text{ odkud}$$

$2a^2+3ab+b^2=-b-1$ a tedy $2a^2-3+b^2=-b-1$. Pak

$$2a^2=-b^2-b+2 \quad |\cdot b^2$$

$$2(ab)^2=-b^4-b^3+2b^2$$

$$b^4+b^3-2b^2+2=0.$$

Najděte řešení této rovnice.

(11) Je-li z algebraický, pak i $\bar{z}$ je algebraický, neboť je kořenem polynomu s komplexně sdruženými koeficienty k polynomu pro prvek z.

Jelikož i je také algebraický, jsou $\frac{1}{2}(z+\bar{z}), \frac{i}{2}(z+\bar{z})$ algebraické.

(12) Je-li q racionální, pak $q=m/n$ pro $m,n\in\mathbb{Z}$, a pak je číslo $\cos(m\pi/n)+i\sin(m\pi/n)$ řešením binomické rovnice $x^{2n}-1=0$. Odtud již plyne tvrzení (viz. příklad (11)).

(13) **(a)** $\mathbb{Q}[\sqrt{2}]$

(b) Polynom x^3-2 je ireducibilní nad $\mathbb{Q}$, je tedy ideál $I(x^3-2)$ maximální a faktorový okruh $\mathbb{Q}[x]/I(x^3-2)$ je rozkladové těleso polynomu x^3-2. Je to těleso $\mathbb{Q}[\varepsilon\sqrt[3]{2}]$, kde ε je primitivní třetí odmocnina z 1.

(c) Polynom x^4-2 má kořeny: $\sqrt[4]{2}, \sqrt[4]{2}i, -\sqrt[4]{2}, -\sqrt[4]{2}i$. Je tedy jeho rozkladové těleso $\mathbb{Q}[\sqrt[4]{2}, i]$.

(15) $g(y)=y^3+10y^2+25y-36$.

(16) $$\rho=\frac{P}{s}=\frac{2P}{a+b+c}=\frac{2P}{\frac{2P}{v_a}+\frac{2P}{v_b}+\frac{2P}{v_c}}=\frac{v_a v_b v_c}{v_a v_b+v_a v_c+v_b v_c}=\frac{3600}{72}=5.$$

(17) Jsou-li kořeny $\alpha_1,\alpha_2,\alpha_3$, pak symetrický polynom $\alpha_1^2+\alpha_2^2+\alpha_3^2$ (v

proměnných $\alpha_1,\alpha_2,\alpha_3$) vyjádříme pomocí elementárních symetrických forem v $\alpha_1,\alpha_2,\alpha_3$, což jsou (až na znaménko) koeficienty daného polynomu. Výsledek je 4.

(18) **(a)** -35 **(b)** 16.

(19) Pro normovaný polynom n-tého stupně platí $\sum_{i=1}^{n}\alpha_i^3=\sigma_1^3-3\sigma_1\sigma_2+3\sigma_3=-a_{n-1}^3+3a_{n-1}a_{n-2}-3a_{n-3}$. Jelikož v našem případě je $a_{n-1}=0$, dostaneme $\sum_{i=1}^{n}\alpha_i^3=-3a_{n-3}$.

(20) Platí $\sum_{i=0}^{n}\alpha_i^3=\sigma_1^3-3\sigma_1\sigma_3+3\sigma_3=-a_{n-1}^3+3a_{n-1}a_{n-2}-3a_{n-3}$.

V našem případě je $a_{n-1}=a_{n-3}=0$, a tedy $A=\sum_{i=1}\alpha_i^3=0$. Kdyby byly všechny kořeny kladné, bylo by $A>0$. Kdyby byly všechny kořeny záporné, bylo by $A<0$, tedy ani v jednom případě by neplatilo $A=0$.

(21) Absolutní člen je roven 0.

(22) **(a)** $p=-q^2-1$, $m=q$.
(b) buď $q=p-1$, $m=0$ nebo $q=1$, $m=\pm\sqrt{2-p}$.

(23) **(a)** 136, **(b)** $-(1+44i)$, **(c)** 3,7161, **(d)** 82,262098.

(24) Pomocí Hornerova schematu.

(25) Použitím Hornerova schematu redukujeme až na kvadratickou rovnici, která má kořeny $\alpha_4=-1$, $\alpha_5=-2$.

(26) Má-li polynom s reálnými koeficienty kořen i, pak má také kořen $-i$, a tedy polynom je dělitelný polynomem $(x^2+1)=(x+i)(x-i)$. Odtud určíme zbývající kořeny $\alpha_{3,4}=\frac{1}{2}(3\pm\sqrt{11})$.

(29) Pomocí kořenových činitelů dostaneme
$f(x)=(2x^4-5x^3-4x^2+3x)(x-a)=25x^5-(2a+5)x^4+(5a-4)x^3+(4a+3)x^2-3ax$.

(30) $x^5-12x^4+57x^3-134x^2+156x-72$.

(31) $\alpha_4 = -1$, $f(x)=(x-2)^3(x+1)$.

(32) Kořeny jsou $1+i, 1-i$, oba dvojnásobné, dále pak 1, 2.

(33) (a) $3(x-2)^3+20(x-2)^2+44(x-2)+53$

(b) $(x+1)^4-3(x+1)^3-3(x+1)^2+4(x+1)+1$

(c) $(x-1)^5+5(x-1)^4+10(x-1)^3+10(x-1)^2+5(x-1)+1$

(d) $(x-2)^4-18(x-2)+38$.

22. SPOLEČNÉ KOŘENY POLYNOMŮ, NÁSOBNÉ KOŘENY POLYNOMŮ

Polynomy $f(x),g(x)\in R[x]$ mají <u>společný kořen</u> α, jsou-li dělitelné kořenovým činitelem $(x-\alpha)$. Tedy $f(x),g(x)$ mají společný kořen, je-li jejich NSD stupně aspoň prvního.

Polynom $f(x)$ má <u>k-násobný kořen α</u>, je-li dělitelný polynomem $(x-\alpha)^k$, ale není dělitelný polynomem $(x-\alpha)^{k+1}$. Má-li $f(x)$ k-násobný kořen α $(k>1)$, pak jeho derivace $f'(x)$ má $(k-1)$-násobný kořen α (pro polynomy nad číselnými tělesy), neboť $f(x)=(x-\alpha)^k g(x)$, a tedy

$$f'(x)=k(x-\alpha)^{k-1}g(x)+(x-\alpha)^k g(x).$$

Jsou-li $f(x)=\sum_{i=0}^{n} a_i x^i$, $g(x)=\sum_{i=0}^{m} b_i x^i$, pak <u>resultantem</u> polynomů $f(x),g(x)$ nazýváme hodnotu detrminantu

$$R(f(x),g(x))=\begin{vmatrix} a_n & a_{n-1} & \dots & a_1 & a_0 & & & \\ & a_n & a_{n-1} & \dots & a_1 & a_0 & & \\ & & \dots & \dots & \dots & \dots & \dots & \\ & & & a_n & a_{n-1} & \dots & a_1 & a_0 \\ b_m & b_{m-1} & \dots & b_1 & b_0 & & & \\ & b_m & b_{m-1} & \dots & b_1 & b_0 & & \\ & & \dots & \dots & \dots & \dots & \dots & \\ & & & b_m & b_{m-1} & \dots & b_1 & b_0 \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m\text{-krát} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n\text{-krát} \end{matrix}$$

Polynomy $f(x)$, $g(x)$ mají společný kořen, právě když $R(f(x),g(x))=0$.

<u>Diskriminantem</u> $D(f(x))$ polynomu $f(x)$ nazýváme resultant $f(x)$ s jeho derivací opatřený znaménkem a dělený koeficientem a_n , tj.:

$$D(f(x))=(-1)^{\frac{n(n-1)}{2}}\cdot\frac{1}{a_n}\cdot R(f(x),f'(x)).$$

Polynom $f(x)$ má násobný kořen právě když $D(f(x))=0$.

<u>Příklady</u>:

(1) Vypočítejte resultant polynomů $f(x)=x^2+px+q$, $g(x)=x-a$.

(2) Vypočítejte resultant $f(x)$, $g(x)$ pro:

(a) $f(x)=x^3-3x^2+2x+1$, $g(x)=2x^2-x-1$

(b) $f(x)=2x^3-3x^2+2x+1$, $g(x)=x^2+x+3$

(c) $f(x)=x^2-5x+6$, $g(x)=x^3+2x^2-4x-12$

(d) $f(x)=x^2-x+1$, $g(x)=x^4-2x^3-3x+4$

(e) $f(x)=2x^3-3x^2-x+2$, $g(x)=x^4-2x^3-3x+4$

(f) $f(x)=x^3-x^2+5x-2$, $g(x)=x^5-2x^3+x^2-x+5$

(g) $f(x)=x^3-7x+6$, $g(x)=x^2+x-6$.

(3) Pro kterou hodnotu λ mají polynomy $f(x),g(x)$ společný kořen:

(a) $f(x)=x^2+\lambda x+2$, $g(x)=x^3-\lambda x+2$

(b) $f(x)=x^2+\lambda^2-2$, $g(x)=x^3-2\lambda x+\lambda^3$.

(4) Určete, zda polynom x^3-2x^2+4 má násobný kořen.

(5) Zjistěte, zda polynom $x^4+5x^3+6x^2-4x-8$ má k-násobný kořen a určete k. Určete tento kořen a kořeny zbývající.

(6) V polynomu x^3-5x^2+3x+a určete a tak, aby polynom měl dvojnásobný kořen. Určete tento kořen i zbývající kořeny.

(7) Dokažte, že pro $a\neq 0$ polynom x^n+a nemá vícenásobný kořen.

(8) Určete (výpočtem NSD), zda polynomy

$$9x^5-12x^4+22x^3-15x^2-4x+4 \text{ a } 45x^4-48x^3+66x^2-30x-4$$

mají společný kořen.

(9) Dokažte, že polynom x^5+ax+b má vícenásobný kořen, právě když

$$\left(\frac{a}{5}\right)^5+\left(\frac{b}{4}\right)^4=0.$$

(10) Nechť T je těleso charakteristiky p, nechť $k\in\mathbb{N}$ přičemž $p\nmid k$. Ukažte, že pak $f(x)\in T[x]$ má k-násobný kořen α, právě když je α $(k-1)$-násobným kořenem derivace $f'(x)$.

(11) Určete diskriminant polynomu:

(a) ax^2+bx+c

(b) x^3+px+q.

Návody k řešení :

(1) a^2+pa+q.

(2) (a) -7 (b) 243 (c) 0 (d) 19
(e) 0 (f) 31923 (g) 0.

(3) (a) $\lambda_1 = -1$, $\lambda_2 = 3$.

(b) $\lambda_1 = 1$, $\lambda_{2,3} = \frac{1}{2}\left(-3+\sqrt{2}\pm i\sqrt{4\sqrt{2}-2}\right)$,

$\lambda_{4,5} = \frac{1}{2}\left(-3-\sqrt{2}\pm i\sqrt{4\sqrt{2}+2}\right)$.

(4) Nemá.

(5) Má 3-násobný kořen, je roven -2. Zbývající kořen je roven 1.

(6) $a = 9$ nebo $a = -\frac{13}{27}$.
Pro $a = 9$ je $x_{1,2} = 3$, $x_3 = -1$,
pro $a = -\frac{13}{27}$ je $x_{1,2} = \frac{1}{3}$, $x_3 = \frac{13}{3}$.

(7) Zřejmě x^n+a není soudělný se svou derivací nx^{n-1} pro $a\neq 0$.

(8) Společný dělitel je $(3x-2)^2$, tedy polynomy mají společný dvojnásobný kořen $\frac{2}{3}$.

(9) Zřejmě $f'(x) = 5x^4+a$. Hledejme NSD(f,f'):

$$(5x^5 + 5ax + 5b) : (5x^4 + a) = x$$
$$4ax + 5b$$

Nyní polynom $5x^4+a$ vynásobíme 4^4a^4:

$$(5\cdot 4^4a^4x^4+4^4a^4):(4ax+5b)=5\cdot 4^3a^3x^3-5^2\cdot 4^2ba^2x^2+5^3b^2 4ax-5^4b^3$$
$$-5^2\cdot 4^3ba^3x^3 \quad +4^4a^5$$
$$+5^3\cdot 4^2b^2a^2x^2+4^4a^5$$
$$-5^4b^3\cdot 4ax \quad +4^4a^5$$
$$5^5b^4 \quad +4^4a^5.$$

Polynomy jsou soudělné právě když $5^5b^4+4^4a^5=0$, tedy $(\frac{b}{4})^4+(\frac{a}{5})^5=0$.

(10) Nechť $f(x) = a_0+ a_1x+...+ a_nx^n$.
Pak $f'(x) = a_1+ (2\times a_2)x+...+ (n\times a_n)x^{n-1}$.
Je-li α k-násobný kořen f, pak $f=(x-\alpha)^k\cdot g$, kde $g(\alpha)\neq 0$,
$f'=(k\times(x-\alpha)^{k-1})g+ (x-\alpha)^k\cdot g'=(x-\alpha)^{k-1}(k\times g(x)+(x-\alpha)g'(x))$.
Je tedy α alespoň $(k-1)$-násobný kořen derivace. Stačí ukázat, že α není kořen $h=k\times g(x)+(x-\alpha)g'(x)$. Platí $h(\alpha)=k\times g(\alpha)$, dle předpokladu je $g(\alpha)\neq 0$, $f\nmid h$, tedy $k\times g(\alpha)\neq 0$.

(11) (a)

$$R(f,f')=\begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix}=\begin{vmatrix} a & b & c \\ 0 & -b & -2c \\ 0 & 2a & b \end{vmatrix}=a\cdot(-b^2+4ac),$$

tedy $D(f)=-b^2+4ac$.

(b)

$$R(f,f')=\begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 3 & 0 & p & 0 & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{vmatrix}=\begin{vmatrix} 1 & 0 & p & q & 0 \\ 0 & 1 & 0 & p & q \\ 0 & 0 & -2p & -3q & 0 \\ 0 & 3 & 0 & p & 0 \\ 0 & 0 & 3 & 0 & p \end{vmatrix}=$$

$$=\begin{vmatrix} 1 & 0 & p & q \\ 0 & -2p & -3q & 0 \\ 3 & 0 & p & 0 \end{vmatrix}=\begin{vmatrix} 1 & 0 & p & q \\ 0 & -2p & -3q & 0 \\ 0 & 0 & -2p & -3q \end{vmatrix}=\begin{vmatrix} -2p & -3q & 0 \\ 0 & -2p & -3q \\ 3 & 0 & p \end{vmatrix}=$$

$$=(-2p)(-2p^2)+3(9q^2)= 27q^2+4p^3=4\cdot 27\cdot((\tfrac{q}{2})^2+(\tfrac{p}{3})^3),$$ tedy

$$D(f)= -4\cdot 27\cdot((\tfrac{q}{2})^2+(\tfrac{p}{3})^3).$$

23. ŘEŠENÍ ALGEBRAICKÝCH ROVNIC.

Algebraickou rovnicí nazýváme výraz $f(x)=0$, kde $f(x)$ je polynom nad některým tělesem. Kořeny polynomu $f(x)$ nazýváme řešení nebo též kořeny rovnice $f(x)=0$. Zde se budeme zabývat pouze rovnicemi nad číselnými tělesy.

Rovnice $f(x)=0$ se nazývá lineární resp. kvadratická resp. kubická resp. n-tého stupně, je-li polynom $f(x)$ stupně 1 resp. 2 resp. 3 resp. n. Rovnice $f(x)=0$ se nazývá binomická n-tého stupně, je-li $f(x)=x^n-a$. Rovnice $f(x)=0$ se nazývá kladně reciproká, je-li $a_n=a_0$, $a_{n-1}=a_1,\dots,a_{n-i}=a_i$ pro každé $i=0,\dots,n$. Rovnice $f(x)=0$ je záporně reciproká, je-li $a_{n-i}=-a_i$ pro každé $i=0,\dots,n$ (je-li sudého stupně, t.j. $n=2m$, pak $a_m=-a_m=0$).

Nechť $x^n-a=0$ je binomická rovnice, a komplexní číslo. Označme $\gamma_1,\dots,\gamma_n$ všechny n-té odmocniny z 1 (leží v Gaussově komplexní rovině ve vrcholech pravidelného n-úhelníka se středem v 0, jehož jeden vrchol je 1). Pak je-li $\alpha=\sqrt[n]{a}$ jeden kořen této rovnice, pak všechny její kořeny jsou $\alpha_1=\alpha\cdot\gamma_1,\dots,\alpha_n=\alpha\cdot\gamma_n$.

Hodnotu $\sqrt[n]{a}$ pro komplexní číslo $a=|a|\cdot(\cos\varphi+i\sin\varphi)$ určíme pomocí Moivreova vzorce

$$\sqrt[n]{a} = \sqrt[n]{|a|}\left(\cos\frac{\varphi+2k\pi}{n} + i\cdot\sin\frac{\varphi+2k\pi}{n}\right),$$

$k=0,1,\dots,n-1$.

Kvadratickou rovnici $ax^2+bx+c=0$, $a\neq0$, nad tělesem čísel komplexních lze snadno vyřešit doplněním levé strany na úplný čtverec a výpočtem druhé odmocniny. Takto odvodíme vzorec pro její kořeny v tělese čísel komplexních : $x_{1,2}=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$, přičemž odmocninu z komplexního čísla $z=a+bi$ lze určit pomocí vzorce

$$\sqrt{a+bi} = \pm\frac{\sqrt{2}}{2}\left(\sqrt{\sqrt{a^2+b^2}+a} + i\cdot\varepsilon\cdot\sqrt{\sqrt{a^2+b^2}-a}\right),$$ kde

$\varepsilon=\operatorname{sgn} b$.

Na kvadratickou a binomickou rovnici lze převést algebraickou rovnici $x^{2n}+ax^n+b=0$, a to substitucí $x^n=y$. Řešíme pak rovnici

$y^2+ay+b=0$, a posléze pro určené hodnoty $y_{1,2}$ řešíme binomické rovnice $x^n-y_1=0$, $x^n-y_2=0$.

Obecnou kubickou rovnici zpravidla nejprve normujeme na tvar

$$x^3+a_2x^2+a_1x+a_0=0,$$

a poté substitucí $x = y - \frac{a_2}{3}$ převedeme na tzv. <u>redukovaný tvar</u>

$$x^3+px+q=0. \qquad (*)$$

Pak vypočítáme

$$x_1= \sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},$$

$$x_2= \varepsilon \sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}} + \varepsilon^2 \sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},$$

$$x_3= \varepsilon^2 \sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}} + \varepsilon \sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}},$$

kde $\varepsilon= \frac{-1+i\sqrt{3}}{2}$. Tyto vztahy se nazývají Cardanovy vzorce, hodnoty x_1, x_2, x_3 jsou řešeními redukované kubické rovnice (*).

Má-li redukovaná kubická rovnice všechny tři kořeny reálné a $D_3= -4p^3-27q^2>0$, pak $\frac{p^2}{27} + \frac{q^2}{4} <0$, lze z goniometrické rovnice

$$\cos t = -\frac{q}{2}\sqrt{-\frac{27}{p^3}}$$

vypočítat t (hledáme řešení pro $0<t<\pi$). Pak řešení rovnice (*) lze určit v tzv. <u>goniometrickém tvaru</u>:

$$x_1 = 2\sqrt{\frac{-p}{3}} \cdot \cos\frac{t}{3},$$

$$x_2 = 2\sqrt{\frac{-p}{3}} \cdot \cos\frac{t+2\pi}{3},$$

$$x_3 = 2\sqrt{\frac{-p}{3}} \cdot \cos\frac{t+4\pi}{3}.$$

Rovnici 4. stupně nejprve normujeme na tvar $x^4+a_3x^3+a_2x^2+a_1x+a_0=0$, a pomocí substituce $x = y - \frac{a_3}{4}$ převedeme na redukovaný tvar

$$x^4 + px^2 + qx + r = 0. \qquad (**)$$

Řešíme tzv. <u>kubickou resolventu</u> , t.j. rovnici

$$y^3+\frac{p}{2}y^2+\left(\frac{p^2}{16}-\frac{r}{4}\right)y-\frac{q^2}{64}=0$$

(např. pomocí Cardanových vzorců). Označme y_1, y_2, y_3 její řešení. Řešeními redukované rovnice 4. stupně (**) jsou pak

$$x_1 = \sqrt{y_1}+\sqrt{y_2}+\sqrt{y_3}$$
$$x_2 = \sqrt{y_1}-\sqrt{y_2}-\sqrt{y_3}$$
$$x_3 = -\sqrt{y_1}+\sqrt{y_2}-\sqrt{y_3}$$
$$x_4 = -\sqrt{y_1}-\sqrt{y_2}+\sqrt{y_3}.$$

Obecný vzorec pro rovnice n-tého stupně pro $n\geq 5$ nemůže existovat, což je důsledkem Galoisovy teorie.

Při řešení reciprokých rovnic využíváme následující tvrzení:

(A) Každá kladně reciproká rovnice lichého stupně a každá záporně reciproká rovnice sudého stupně má kořen -1.

(B) Každá záporně reciproká rovnice má kořen 1.

(C) Je-li $f(x)=0$ kladně reciproká rovnice stupně $2k$, pak substitucí $y=x+\frac{1}{x}$ lze snížit stupeň na k.

Dosazujeme $y = x+\frac{1}{x}$

$$y^2-2 = x^2+\frac{1}{x^2}$$
$$y^3-3y = x^3+\frac{1}{x^3}$$
$$y^4-4y^2+2 = x^4+\frac{1}{x^4}$$
$$y^5-5y^3+5y = x^5+\frac{1}{x^5}, \text{ atd.}$$

Dostaneme rovnici $g(y)=0$ stupně k. Hodnoty kořenů původní rovnice pak z kořenů y rovnice $g(y)=0$ určíme ze vztahu $y=x+\frac{1}{x}$, t.j. řešením kvadratické rovnice $x^2-xy+1=0$.

Je-li $f(x)=0$ rovnice nad tělesem čísel racionálních $\mathbb{Q}$, lze ji násobením NSN jmenovatelů koeficientů převést na rovnici s celočíselnými koeficienty. Pak platí tvrzení:

(D) Má-li algebraická rovnice $f(x) = \sum_{i=0}^{n} a_i x^i = 0$ celočíselné koeficienty, pak je-li racionální číslo $\frac{r}{s}$ kořenem této rovnice, pak platí $r|a_0$, $s|a_n$.

Je-li tedy $f(x)=0$ rovnice s celočíselnými koeficienty, lze

snadno určit, která racionální čísla mohou být jejími řešeními a pomocí Hornerova schematu lze snadno ověřit, zda některé z nich skutečně kořeny jsou.

Příklady:

(1) Řešte kvadratické rovnice:

(a) $x^2-(2+i)x+(-1+7i)=0$

(b) $x^2-(3-2i)x+(5-5i)=0$,

(c) $(2+i)x^2-(5-i)x+(2-2i)=0$,

(d) $x^2-(3+2i)x+5+i=0$,

(e) $x^2-(2+2i)x-1+2i=0$,

(f) $x^2-(4+2i)x+6+8i=0$,

(g) $x^2-(1-3i)x+2+6i=0$,

(h) $x^2-8x+13-4i=0$,

(i) $x^2-4ix+3+24i=0$,

(j) $x^2-(6-4i)x+5-12i=0$.

(2) Pomocí derivace dokažte, že nutná a postačující podmínka pro existenci dvojnásobného kořene redukované kubické rovnice $x^3+px+q=0$ je $\left(\frac{q}{2}\right)^2+\left(\frac{p}{3}\right)^3=0$.

(3) Pro které λ má rovnice $x^3-3x+\lambda=0$ tři reálné kořeny ?

(4) Sestavte kvadratickou rovnici, která má kořeny:

(a) $x_1=1+2i$, $x_2=3-2i$

(b) $x_1=2+i$, $x_2=-i$.

(5) Určete kořeny rovnice $(1+i)x^2+(1+3i)x-8+6i=0$ v algebraickém tvaru.

(6) Řešte rovnici:

(a) $x^4-30x^2+289=0$

(b) $x^4-3x^2+4=0$.

(7) Odvoďte vzorec pro řešení rovnice

$$x^4+px^2+q=0$$

s reálnými koeficienty pro případ $\left(\frac{p}{2}\right)^2-q<0$.

(8) Pro které $a \neq 0$ má rovnice $x^n - Ax^{n-1} + a = 0$ $(n \geq 2)$, $A \neq 0$, dvojnásobný kořen ? Určete tento kořen!

(9) Řešte rovnici $x^5 + 3x^4 - 2x^3 - 6x^2 + 5x - 1 = 0$.

(10) Řešte rovnici $x^6 - 6x^4 - 4x^3 + 9x^2 + 12x + 4 = 0$.

(11) Dokažte, že rovnice $x^3 + px + 2 = 0$ má všechny kořeny reálné právě když $p \leq -3$.

(12) Řešte kubické rovnice:

(a) $x^3 + 6x + 7 = 0$ -1
(b) $x^3 - 9x + 28 = 0$ -4
(c) $x^3 + 3x - 14 = 0$ 2
(d) $x^3 + 24x - 56 = 0$ 2
(e) $x^3 - 6x - 9 = 0$ 3
(f) $x^3 + 36x + 208 = 0$ -4
(g) $x^3 + 3x^2 + 48x + 144 = 0$ -3
(h) $x^3 + 3x^2 + 9x - 13 = 0$ 1
(i) $x^3 - 9x^2 + 21x - 13 = 0$ 1
(j) $4x^3 - 12x^2 - x + 3 = 0$ 3
(k) $x^3 - 8x^2 + 72 = 0$ 6 4
(l) $3x^3 - 9x^2 + 4 = 0$
(m) $x^3 - 3x^2 + 3 = 0$
(n) $x^3 + 3x^2 - 1 = 0$
(o) $x^3 - 3x^2 - x + 2 = 0$
(p) $x^3 + x^2 - 2x - 1 = 0$.

(13) Vypočtěte délky hran kvádru, je-li součet délek hran 36, povrch 52, objem 24.

(14) Řešte rovnice 4. stupně (pokuste se určit jeden nebo dva racionální kořeny):

(a) $x^4 + 2x^3 + 4x^2 - 7 = 0$ 1
(b) $x^4 + 6x^3 + 16x^2 \mp 11 = 0$
(c) $x^4 - 2x^3 + 4x^2 + 2x - 5 = 0$ 1

(d) $x^4 - 40x^3 + 39 = 0$

(e) $x^4 - 2x^3 + 4x^2 - 13x + 10 = 0$

(f) $x^4 - 6x^3 + 10x^2 - 2x - 3 = 0$

(g) $x^4 - 2x^3 + 2x^2 + 4x - 8 = 0.$

(15) Řešte rovnice 4. stupně:

(a) $x^4 - 3x^2 - 12x + 40 = 0$

(b) $x^4 + 11x^2 + 10x + 50 = 0$

(c) $x^4 - 2x^3 + 4x^2 - 2x + 3 = 0$

(d) $x^4 + 2x^3 + 8x^2 + 2x + 7 = 0$

(e) $x^4 - x^3 - x^2 + 2x - 2 = 0$

(f) $x^4 + 2x^3 + 2x^2 + 10x + 25 = 0$

(g) $x^4 - 4x^3 + 5x^2 - 2x - 6 = 0$

(h) $x^4 - \frac{3}{2}x^2 + x - \frac{3}{16} = 0.$

(16) Řešte reciproké rovnice:

(a) $x^4 + 1 = 0$

(b) $x^6 + 3x^4 + 3x^2 + 1 = 0$

(c) $6x^6 - 35x^5 + 56x^4 - 56x^3 + 35x - 6 = 0$

(d) $x^7 - 2x^6 - x^4 - x^3 - 2x + 1 = 0$

(e) $x^8 - 10x^7 + 39x^6 - 80x^5 + 100x^4 - 80x^3 + 39x^2 - 10x + 1 = 0$

(f) $x^8 - x^7 + 20x^6 - 19x^5 + 38x^4 - 19x^3 + 20x^2 - x + 1 = 0$

(g) $x^{10} - 6x^9 + 12x^8 - 8x^7 - x^6 + x^4 + 8x^3 - 12x^2 + 6x - 1 = 0.$

(17) Řešte binomické rovnice:

(a) $x^2 - 1 = 0$

(b) $x^3 - 1 = 0$

(c) $x^4 - 1 = 0$

(d) $x^6 - 1 = 0$

(e) $x^8 - 1 = 0$

(f) $x^{12} - 1 = 0$

(g) $x^{24} - 1 = 0.$

(18) Určete racionální kořeny rovnic:

(a) $10x^6 - 13x^5 - 8x^4 + 9x^3 - 53x^2 + 12x + 6 = 0$

(b) $x^4 + x^3 - 3x^2 + 7x - 6 = 0$

(c) $4x^4 - 2x^2 + x - 6 = 0$

(d) $15x^6 + 2x^5 + 29x^4 + 49x^3 - 11x^2 - 5x + 1 = 0$

(e) $6x^5 + 5x^4 + 6x^3 + 4x^2 - 17x + 6 = 0$

(f) $5x^4 - 3x^3 + 7x^2 - x - 3 = 0.$

(19) Dokažte, že rovnice

$$1 + x + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!} = 0$$

nemá násobné kořeny.

(20) Nalezněte racionální kořen rovnice

$$x^3 - 5x^2 + 9x - 9 = 0$$

a tuto rovnici vyřešte.

(21) Rovnice $x^4 + 7x^3 + 12x^2 - 4x - 16 = 0$ má vícenásobný kořen. Určete tento kořen a řešte rovnici.

(22) Řešte binomickou rovnici:

(a) $x^4 - (2 + 2i) = 0$

(b) $x^3 - i = 0$

(c) $x^4 - 16 = 0$

(d) $x^5 - 32 = 0.$

(23) Řešte goniometricky rovnice:

(a) $x^3 - 3x + 1 = 0$

(b) $x^3 - 5x + 3 = 0$

(c) $x^3 - 9x - 7 = 0$

(d) $x^3 - 3x - 1 = 0$

(e) $x^3 - 11x + 5 = 0$

(f) $x^3 - 28x + 48 = 0.$

(24) Určete $a, b \in \mathbb{R}$ tak, aby rovnice

$x^3 + ax^2 + bx - 15 = 0$ měla kořen $2+i$.

(25) Najděte NSD polynomů

$$x^4 + 3x^3 + 5x^2 + 3x + 4, \quad x^4 + 2x^3 + 4x^2 + 2x + 3.$$

(26) Zjistěte, zda mají společný kořen polynomy

$$8x^3 + 6x + 1 \text{ a } -4x^3 - x^2 + 12x + 3.$$

Výsledky řešení :

(1) (a) $3-i$, $-1+2i$

(b) $2+i$, $1-3i$

(c) $1-i$, $\frac{2}{5}(2-i)$

(d) $2+3i$, $1-i$

(e) $2+i$, i

(f) $3-i$, $1+3i$

(g) $2-4i$, $-1+i$

(h) $6+i$, $2-i$

(i) $3-2i$, $3+6i$

(j) $3-2i$, dvojnásobný.

(3) Pro $-2 < \lambda < 2$.

(4) (a) $x^2 - 4x + 7 + 4i = 0$

(b) $x^2 + 2x + 1 + 2i = 0$.

(5) $x_1 = 1-2i$, $x_2 = 3+i$.

(6) (a) $\pm(4\pm i)$

(b) $\pm(\sqrt{7}\pm i)$.

(7) $x_{1,2,3,4} = \pm\frac{1}{2}(\sqrt{2\sqrt{q}-p} \pm \sqrt{2\sqrt{q}+p})$.

(8) $a = \frac{A^n}{n^n}(n-1)^{n-1}$, $x = \frac{n-1}{n}\cdot A$.

(9) Snadno ověříme, že rovnice má racionální kořen 1, dělením derivací polynomu $f(x)$ zjistíme, že má násobné kořeny

$$x_{2,3} = -1+\sqrt{2}, \quad x_{4,5} = -1-\sqrt{2}.$$

(10) Dělením derivací polynomu zjistíme, že rovnice má dvojnásobný kořen 2 a čtyřnásobný kořen -1.

(11) Pro $(\frac{q}{2})^2+(\frac{p}{3})^3 \le 0$, t.j. $\frac{p^3}{27} \le -1$, odkud $p^3 \le -27$, t.j. $p \le -3$.

(12) (a) $-1;\ \frac{1}{2}(1\pm 3i\sqrt{3})$

(b) $-4;\ 2\pm i\sqrt{3}$

(c) $2;\ -1\pm i\sqrt{6}$

(d) $2;\ -1\pm 3i\sqrt{3}$

(e) $3;\ \frac{1}{2}(-3\pm i\sqrt{3})$

(f) $-4;\ 2\pm 4i\sqrt{3}$

(g) $-3;\ \pm 4i\sqrt{3}$

(h) $1;\ -2\pm 3i$

(i) $1;\ 4\pm\sqrt{3}$

(j) $3;\ \pm\ \frac{1}{2}$

(k) $6;\ 1\pm\sqrt{13}$

(l) 2,834..; 0,77392..; -0,6079..

(m) 2,53208; 1,34730; -0,87938

(n) 0,53209..; -0,65270..; -2,87939..

(o) 3,1149..; 0,7459..; -0.8608..

(p) 1,2469796..; -0,4450419..; -1,8019377...

(13) Délky hran jsou 2, 3, 4.

(14) (a) $0;\ 1;\ \frac{1}{2}(-3\pm i\sqrt{19})$

(b) $0;\ -1;\ \frac{1}{2}(-5\pm i\sqrt{19})$

(c) $\pm 1;\ 1\pm 2i$

(d) $1;\ 3;\ -2+3i$

(e) $1;\ 2;\ \frac{1}{2}(-5\pm i\sqrt{19})$

(f) $1;\ 3;\ 1\pm\sqrt{2}$

(g) $\pm 2;\ 1\pm i\sqrt{3}$

(15) (a) $2\pm i;\ -2\pm 2i$

(b) $1\pm 3i;\ -1\pm 2i$

(c) $\pm i;\ -1\pm i\sqrt{2}$

(d) $\pm i;\ -1\pm i\sqrt{6}$

(e) $\pm\sqrt{2};\ \frac{1}{2}(1\pm i\sqrt{3})$

(f) $1\pm 2i;\ -2\pm i$

(g) $1\pm\sqrt{3};\ 3\pm\sqrt{5}$

(h) $\frac{1}{2}$ (trojnásobný kořen); $-\frac{3}{2}$.

(16) (a) $\pm\frac{1}{2}\sqrt{2}\cdot(1+i)$; $\pm\frac{1}{2}\sqrt{2}\cdot(1-i)$

(c) ± 1; 3; $\frac{1}{3}$; 2; $\frac{1}{2}$

(d) -1; $\frac{1}{2}(1\pm i\sqrt{3})$; $\frac{1}{2}(1+\sqrt{3}\pm i\sqrt[4]{12})$; $\frac{1}{2}(1-\sqrt{3}\pm i\sqrt[4]{12})$

(e) 1; 1; $\frac{1}{2}(1\pm i\sqrt{3})$; $\frac{1}{2}(3\pm\sqrt{3})$; $2\pm\sqrt{3}$

(f) $\pm i$; $\frac{1}{2}(1\pm i\sqrt{3})$; $(2\pm\sqrt{3})i$; $(-2\pm\sqrt{5})i$

(g) pětinásobný kořen 1; -1; $\frac{1}{2}(3\pm\sqrt{5})$; $\frac{1}{2}(-1\pm i\sqrt{3})$

(17) (a) ± 1 (b) 1; $\frac{1}{2}(-1\pm i\sqrt{3})$ (c) ± 1; $\pm i$

(d) ± 1; $\frac{1}{2}(1\pm i\sqrt{3})$; $-\frac{1}{2}(1\pm i\sqrt{3})$

(f) ± 1; $\pm i$; $\frac{1}{2}(1\pm i\sqrt{3})$; $-\frac{1}{2}(1\pm i\sqrt{3})$; $\frac{1}{2}(\sqrt{3}\pm i)$; $-\frac{1}{2}(\sqrt{3}\pm i)$.

(18) (a) 2; $-\frac{3}{2}$; $-\frac{1}{5}$

(19) Je-li $f(x)= 1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^n}{n!}$, pak

$$f'(x)= 1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots + \frac{x^{n-1}}{(n-1)!}.$$

Je tedy $(f-f')(x)= \frac{x^n}{n!}$. Je-li $d=\mathrm{NSD}(f,f')$, pak $d|f-f'$, tedy polynom d je až na koeficient polynom x^k pro některé $k\leq n$. To je ovšem možné jen pro $k=0$, neboť 0 není kořen ani $f(x)$ ani $f'(x)$.

(24) $a=17$, $b=-77$.

(25) x^2+1

(26) Mají společný kořen $-\frac{1}{5}$.

III. Č Á S T

1. USPOŘÁDANÉ MNOŽINY, POLOSVAZY

Dvojice $(A,\leq)$ je uspořádaná množina, je-li $A\neq\emptyset$ a $\leq$ je relace uspořádání na A. Je-li $(A,\leq)$ uspořádaná množina, $X\neq A$, pak má-li množina $U(X)$ všech horních závor množiny X nejmenší prvek, nazývá se tento prvek supremum množiny X a označuje se $\sup X$; duálně, má-li množina $L(X)$ všech dolních závor množiny X největší prvek, nazývá se tento prvek infimum množiny X a označuje se $\inf X$.

Grupoid $(A,\circ)$ se nazývá polosvaz, je-li operace $\circ$ komutativní, asociativní a idempotentní. Je-li $(A,\circ)$ polosvaz, pak relace $\leq$ definovaná předpisem:

$$a\leq b \Leftrightarrow a\circ b=a$$

je uspořádání na A a v uspořádané množině $(A,\leq)$ mají každé dva prvky a,b infimum, přičemž platí $\inf(a,b)=a\circ b$. V tomto případě označujeme $a\wedge b=\inf(a,b)=a\circ b$ a říkáme, že $(A,\wedge)$ je průsekový polosvaz.

Duálně, je-li $(A,\circ)$ polosvaz, je relace $\leq$ definovaná předpisem

$$a\leq b \Leftrightarrow a\circ b=b$$

uspořádání na A a v $(A,\leq)$ mají každé dva prvky a,b supremum, přičemž platí $\sup(a,b)=a\circ b$. V tomto případě označíme $a\vee b=\sup(a,b)=a\circ b$ a říkáme, že $(A,\vee)$ je spojový polosvaz.

Má-li $(A,\leq)$ nejmenší prvek, označíme jej symbolem 0 a nazveme nula uspořádané množiny $(A,\leq)$. Má-li $(A,\leq)$ největší prvek, označíme jej symbolem 1 a nazveme jednička $(A,\leq)$.

Jestliže $a,b\in A$, $a\leq b$, pak označíme

$$[a,b] = \{x\in A;\ a\leq x\leq b\}$$

a nazveme interval uspořádané množiny $(A,\leq)$.

Jestliže $a,b\in A$, $a\leq b$ a z podmínky $a\leq x\leq b$ plyne $a=x$ nebo $b=x$, říkáme, že prvek b pokrývá prvek a, což označíme $b\succ a$.

Příklady:

(1) Nechť $(P,\leq)$ je uspořádaná množina, $A\subseteq B\subseteq P$. Dokažte, že existují-li $\sup A$, $\sup B$, pak

$$\sup A\leq \sup B,$$

existují-li $\inf A$, $\inf B$, pak

$$\inf A\leq \inf B.$$

Ukažte příklad, kdy $A\subseteq B$ ale

(i) $\sup A=\sup B$, $\inf A=\inf B$

(ii) $\sup A<\sup B$, $\inf A<\inf B$.

(2) Nechť $(A,\leq)$ je uspořádaná množina, $\emptyset\neq B\subseteq A$. Dokažte, že je ekvivalentní:

(i) u je nejmenší prvek v B;

(ii) $u\in B$ a $u=\inf B$.

(3) Nechť $(A,\leq)$ je upořádaná množina, $C\subseteq B\subseteq A$. Dokažte, že jestliže $\inf B\in C$, pak $\inf C=\inf B$. Analogické tvrzení vyslovte a dokažte pro supremum.

(4) Nechť $(A,\leq)$ je upořádaná množina, $a_1,a_2,\ldots,a_n\in A$. Dokažte, že jestliže platí

$$a_1\leq a_2\leq\ldots\leq a_n\leq a_1,$$

pak $a_1=a_2=\ldots=a_n$.

(5) Nechť $(A,\leq)$ je uspořádaná množina, $\emptyset\neq B\subseteq A$. Položme $\leq_B=(B\times B)\cap\leq$. Dokažte, že $\leq_B$ je uspořádání na B.

(6) Dokažte, že existuje-li v uspořádáné množině $(A,\leq)$ pro $a,b\in A$ $\inf(a,b)$, pak existuje i $\sup(a,\inf(a,b))$ a platí

$$a=\sup(a,\inf(a,b)).$$

(7) Na příkladě tříprvkových uspoř. množin ukažte, že může existovat bijektivní izotonní zobrazení, k němuž inverzní zobrazení není izotonní. Lze takový příklad zkonstruovat i pro dvouprvkové uspořádané množiny?

(8) Nechť $(A,\leq)$ je <u>konečná</u> s 0 a 1. Dokažte, že je-li A $\vee$-polosvazem (t.j. pro každé $a,b\in A$ existuje $\sup(a,b)$), pak A je rovněž $\wedge$-polosvazem, t.j. pro každé $a,b\in A$ existuje také $\inf(a,b)$ (a také obráceně, v každé <u>konečné</u> uspoř. množině

existence $inf(a,b)$ pro každé $a,b \in A$ implikuje existenci $sup(a,b)$).

(9) Nechť grupoidy $(A,\cdot)$, $(B,\cdot)$ jsou polosvazy. Dokažte, že i direktní součin $(A,\cdot)\times(B,\cdot)$ je polosvaz.

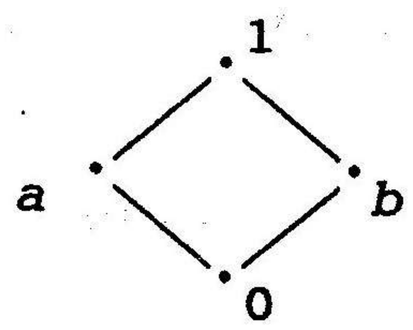
(10) Ukažte příklad (konečné) uspořádané množiny, která je $\vee$-polosvazem, ale není $\wedge$-polosvazem.

(11) Je-li $(A,\vee)$ konečný $\vee$-polosvaz, pak v $(A,\leq)$ existuje 1. Je-li $(A,\wedge)$ konečný $\wedge$-polosvaz, pak v $(A,\leq)$ existuje 0. Dokažte!

<u>Návody k řešení</u>:

(1) $supA$ je nejmenší prvek té vlastnosti, že $a \leq supA$ pro každé $a \in A$. Jelikož $supB \geq a$ pro každé $a \in A$, je $supA \leq supB$.

(i)



Zvolme $A=\{a,b\}$, $B=\{a,b,0\}$. Pak $A \subseteq B$ a $supA=supB=1$, $infA=infB=0$.

(3) $infB$ je největší prvek z A takový, že $infB \leq b$ pro každé $b \in B$. Jelikož $C \subseteq B$, je $infB \leq c$ pro každé $c \in C$. Nyní $infB \in C$, tedy $infB$ je nejmenší prvek v C a $infB=infC$.

(4) Užijte antisymetrie uspořádání.

(5) Ukažte, že restikce relace $\leq$ na podmnožinu B je reflexivní, antisymetrická, tranzitivní.

(6) Je zřejmé, že $a \leq a$, $a \geq inf(a,b)$. Je-li $z \geq a$, $z \geq inf(a,b)$, pak $z \geq a$, je tedy $a=sup(a,inf(a,b))$.

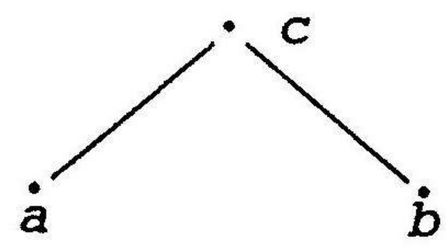
(7) Nechť $(A,\cdot),(B,\cdot)$ jsou $\vee$-polosvazy. Buďte $\langle x,y\rangle$, $\langle x',y'\rangle \in A\times B$. Ukažte, že existuje jejich supremum v $A\times B$ a že je rovno $\langle x\cdot x',y\cdot y'\rangle$.

(7) Ano, stačí vzít $(A,\leq)$: $\underset{a}{\bullet}$ $\underset{b}{\bullet}$ (antiřetězec),

$(B,\leq)$: $\begin{array}{l} \bullet f(b) \\ \bullet f(a) \end{array}$ (řetězec), kde $f: a \longrightarrow f(a)$, $b \longrightarrow f(b)$.

(8) Nechť $(A,\leq)$ je $\vee$-polosvaz s nulou 0. Buďte $a,b \in A$, $L(a,b)$ množina dolních hranic pro prvky a,b. Je vždy $0 \in L(a,b)$, tedy $L(a,b) \neq \emptyset$. Jestliže $x,y \in L(a,b)$, pak také $x \vee y \in L(a,b)$(proč?); označme tedy $z = \vee\{x; x \in L(a,b)\}$. Toto spojení existuje, neboť A je konečná a přitom $z \in L(a,b)$. Je tedy prvek z největší v $L(a,b)$, tedy $z = inf(L(a,b))$.

(10) Například množina:



(11) Nechť $A = \{a_1, a_2, \ldots, a_n\}$. Stačí položit $1 = a_1 \vee a_2 \vee \ldots \vee a_n$ v prvním a $0 = a_1 \wedge a_2 \wedge \ldots \wedge a_n$ ve druhém případě.

2. SVAZY

Uspořádaná množina $(A;\leq)$ je <u>svaz</u>, jestliže pro každé $a,b\in A$ existuje $sup(a,b)$ a $inf(a,b)$, t.j. je-li současně $\vee$-polosvazem i $\wedge$-polosvazem. Tyto (indukované) operace $\vee$ a $\wedge$ pak splňují:

(i)	idempotenci:	$a\vee a=a$	$a\wedge a=a$
(ii)	komutativitu	$a\vee b=b\vee a$	$a\wedge b=b\wedge a$
(iii)	asociativitu	$a\vee(b\vee c)=(a\vee b)\vee c$	$a\wedge(b\wedge c)=(a\wedge b)\wedge c$
(iv)	absorpci	$a\vee(a\wedge b)=a$	$a\wedge(a\vee b)=a$.

Je-li A množina se dvěma binárními operacemi (označenými např. $\vee,\wedge$), pak $(A;\vee,\wedge)$ je svazem, jestliže splňuje (i), (ii), (iii), (iv), přičemž (i) je důsledkem (ii), (iii), (iv).

Je-li $(A,\leq)$ svaz a 0 resp. 1 je nulou resp. jedničkou v $(A,\leq)$, pak se 0 resp. 1 nazývá <u>nula svazu</u> resp <u>jednička svazu</u> $(A,\leq)$.

Má-li svaz 0, pak prvek $a\in A$ takový, že $a\succ 0$, se nazývá <u>atom.</u>

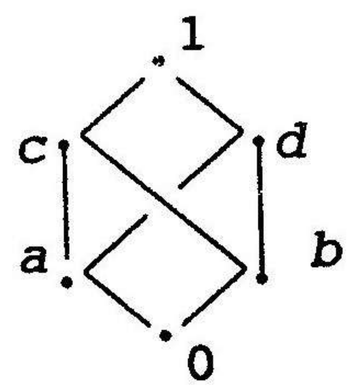
Nechť $(A;\vee,\wedge)$, $(B;\vee,\wedge)$ jsou dva svazy. Zobrazení $h:A\longrightarrow B$ je <u>homomorfismus</u> svazu $(A;\vee,\wedge)$ do $(B;\vee,\wedge)$, jestliže $h(a\vee b)=h(a)\vee h(b)$, $h(a\wedge b)=h(a)\wedge h(b)$ pro každé $a,b\in A$. Zřejmě každý homomorfismus je izotonní zobrazení. Je-li homomorfismus svazu $(A;\vee,\wedge)$ do svazu $(B;\vee,\wedge)$ bijekce, nazývá se <u>izomorfismus</u>.

Bude-li u svazu $(A,\vee,\wedge)$ zřejmé, jak jsou definovány operace $\vee$, $\wedge$, budeme z důvodu stručnosti označovat svaz jen jeho nosičem, t.j. místo svaz $(A;\vee,\wedge)$ píšeme jen svaz A.

<u>Příklady</u>:

(1) Nakreslete diagramy všech uspořádaných dvouprvkových, trojprvkových, čtyřprvkových a pětiprvkových množin, které jsou svazy.

(2) Ukažte, že uspořádaná množina



není svaz. Proč?

(3) Dokažte, že systém všech podmnožin neprázdné množiny A tvoří svaz vzhledem k uspořádání $\subseteq$. Co je *sup*, *inf*? Nakreslete tento svaz pro 2,3,4-prvkovou množinu A.

(4) Dokažte, že množina všech přirozených čísel, které jsou dělitelé přirozeného čísla n, tvoří svaz vzhledem k relaci dělitelnosti. Co je v tomto svazu *sup*, *inf*?

(5) Ukažte, že množina všech celých resp. racionálních resp. reálných čísel tvoří svaz vzhledem k obvyklému uspořádání dle velikosti. Co je $sup(a,b)$, $inf(a,b)$? Mají tyto svazy 0 resp. 1?

(6) Nechť $\mathbb{N}$ je množina všech přirozených čísel, uspořádaná relací dělitelnosti, t.j.

$$a \leq b \Leftrightarrow a|b.$$

Je $(\mathbb{N},|)$ svaz? Má největší a nejmenší prvek?

(7) Nechť $\mathbb{N}_0=\mathbb{N}\cup\{0\}$. Je $(\mathbb{N}_0,|)$ svaz? Má největší a nejmenší prvek?

(8) Nakreslete diagramy všech neizomorfních šestiprvkových svazů.

(9) Dokažte, že pro každé dva prvky svazu L platí:

(i) Jestliže $x\|y$, pak $x\wedge y<x$, $x\wedge y<y$;

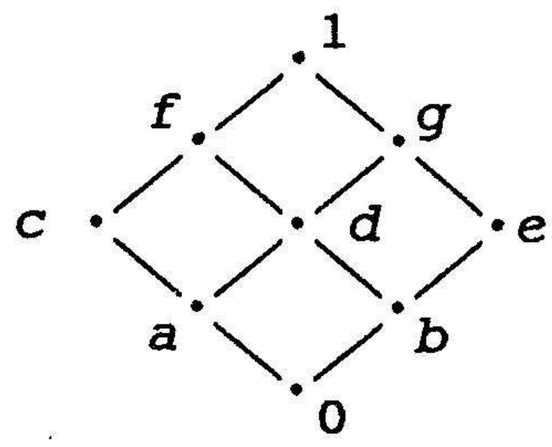
(ii) Jestliže $x\wedge y<x$, pak $y<x\vee y$.

(10) Nechť $L(a,b)$ je množina všech funkcí jedné reálné proměnné na intervalu (a,b). Definujme pro $f,g\in L(a,b)$ relaci $f\leq g \Leftrightarrow f(x)\leq g(x)$ pro každé $x\in(a,b)$. Dokažte, že $(L(a,b),\leq)$ je svaz. Určete $\vee,\wedge$.

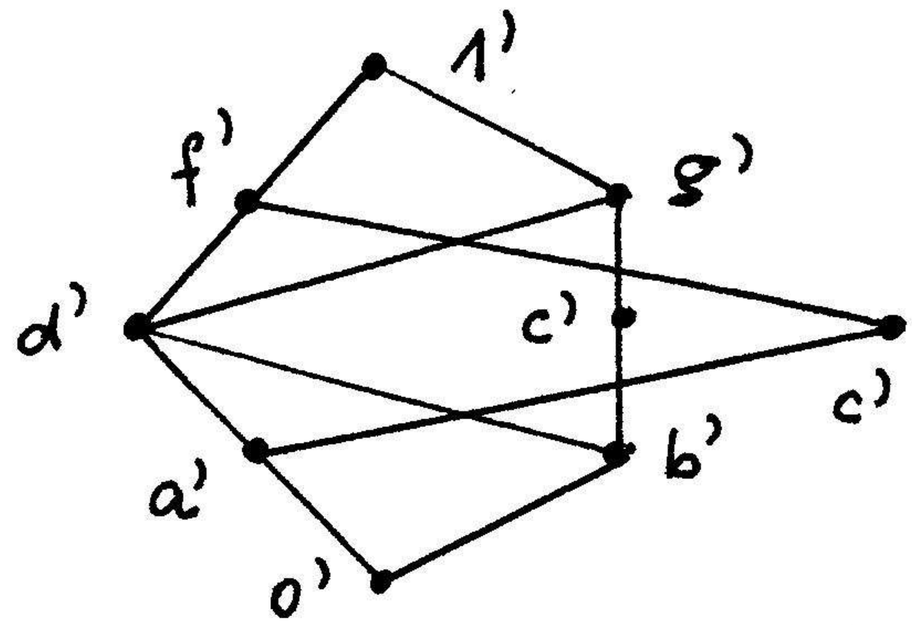
(11) Dokažte, že v každém svazu $(L;\vee,\wedge)$ je ekvivalentní:

$$a\wedge b=a \Leftrightarrow a\vee b=b.$$

(12) Ukažte, že následující svazy L_1, L_2 jsou izomorfní.



L_1



L_2

(13) Množina všech binárních relací na množině $A \neq \emptyset$ tvoří svaz vzhledem k $\subseteq$. Dokažte. Kolik prvků má svaz všech binárních relací na dvojprvkové množině A ?

(14) Najděte svaz $(L;\vee,\wedge)$ a jeho neprázdnou podmnožinu $H \subseteq L$ takovou, že H je opět svazem vzhledem k indukovanému uspořádání (svazu $(L;\vee,\wedge)$), ale není podsvazem svazu $(L;\vee,\wedge)$.

(15) Dokažte, že podsvaz svazu $(L;\vee,\wedge)$ generovaný dvojprvkovou podmnožinou $A \subseteq L$ je buď dvojprvkový nebo čtyřprvkový.

(16) Nechť $(L_1;\vee,\wedge)$, $(L_2;\vee,\wedge)$ jsou svazy a $f: L_1 \longrightarrow L_2$ je bijekce. Dokažte, že f je izomorfismus právě když f je izotonní a f^{-1} je rovněž izotonní. Na příkladu ukažte, že jen požadavek izotonnosti f nestačí k tomu, aby f byl izomorfismus svazů.

(17) Nechť h je surjektivní homomorfismus svazu L_1 na L_2. Dokažte, že má-li L_1 nulu 0 (resp. jedničku 1), pak $h(0)$ resp. $h(1)$ je nula resp. jednička svazu L_2.

(18) Je-li svaz L řetězec, pak každé izotonní zobrazení L do libovolného svazu L' je homomorfismus. Dokažte!

(19) Nechť L je svaz, $a,b \in L$. Dokažte, že zobrazení $h: L \longrightarrow L$ dané předpisem

$$h(x)=((a\wedge b)\vee x)\wedge(a\vee b)$$

je izotonní zobrazení svazu L na interval $[a\wedge b, a\vee b]$ svazu L.

(20) Nechť A je n-prvková množina, $n \geq 1$. Kolik atomů má svaz $(Exp A;\subseteq)$? Určete tyto atomy!

(21) Nechť L je svaz, $a,b \in L$. Dokažte, že zobrazení $h_b: x \longrightarrow x\wedge b$ zobrazuje interval $[a, a\vee b]$ do intervalu $[a\wedge b, b]$, a že

zobrazení $g_a: x \longrightarrow x \vee a$ zobrazuje $[a \wedge b, b]$ do $[a, a \vee b]$. Dokažte, že platí

$$h_b \circ g_a \circ h_b = h_b \ , \ g_a \circ h_b \circ g_a = g_a .$$

(22) Ukažte, že pro libovolné prvky a, b, c svazu L platí: jestliže

$$c \succ a, \ c \succ b, \ a \neq b, \text{ pak } c = a \vee b.$$

(23) Dokažte, že průnik dvou intervalů svazu L je buď $\emptyset$ nebo opět interval svazu L.

(24) Nechť $h: L \longrightarrow L'$ je homomorfismus svazů, $x, y \in L$ a $y \succ x$. Platí pak, že buď $h(x) = h(y)$ nebo $h(y) \succ h(x)$?

(25) Nechť L je svaz. Dokažte, že pro každé $a, b, c, d \in L$ platí:

(i) $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$;

(ii) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$;

(iii) $a \vee (b \wedge c) \leq (a \vee b) \wedge c$, kde $a \leq c$;

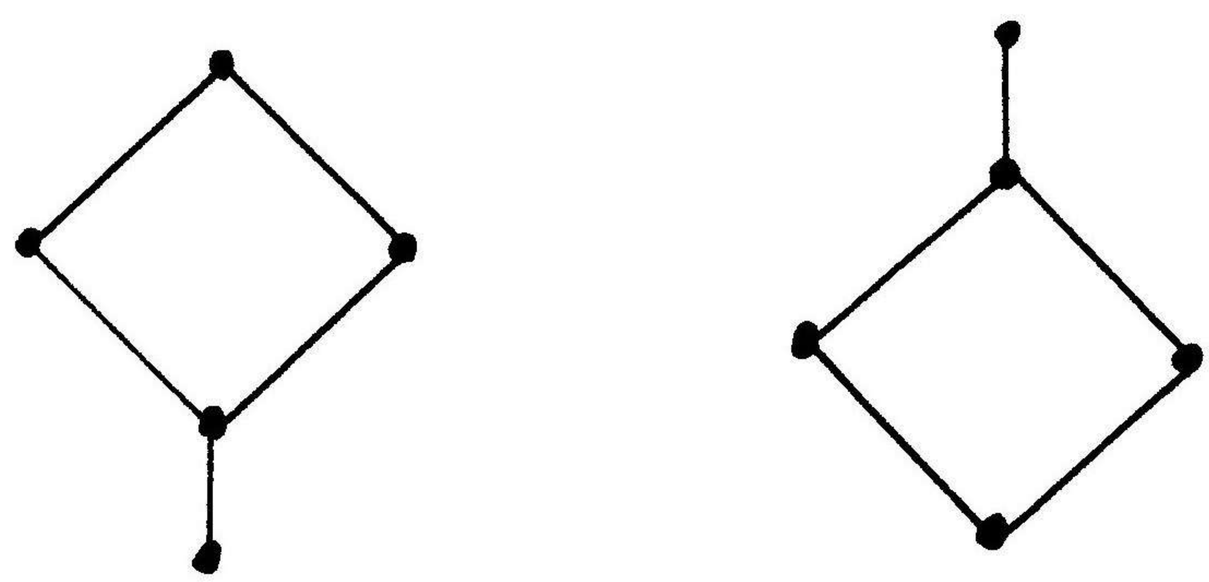
(iv) $(a \wedge c) \vee (b \wedge d) \leq (a \vee b) \wedge (c \vee d)$;

(v) $(a \wedge b) \vee (b \wedge c) \vee (c \wedge a) \leq (a \vee b) \wedge (b \vee c) \wedge (c \vee a)$.

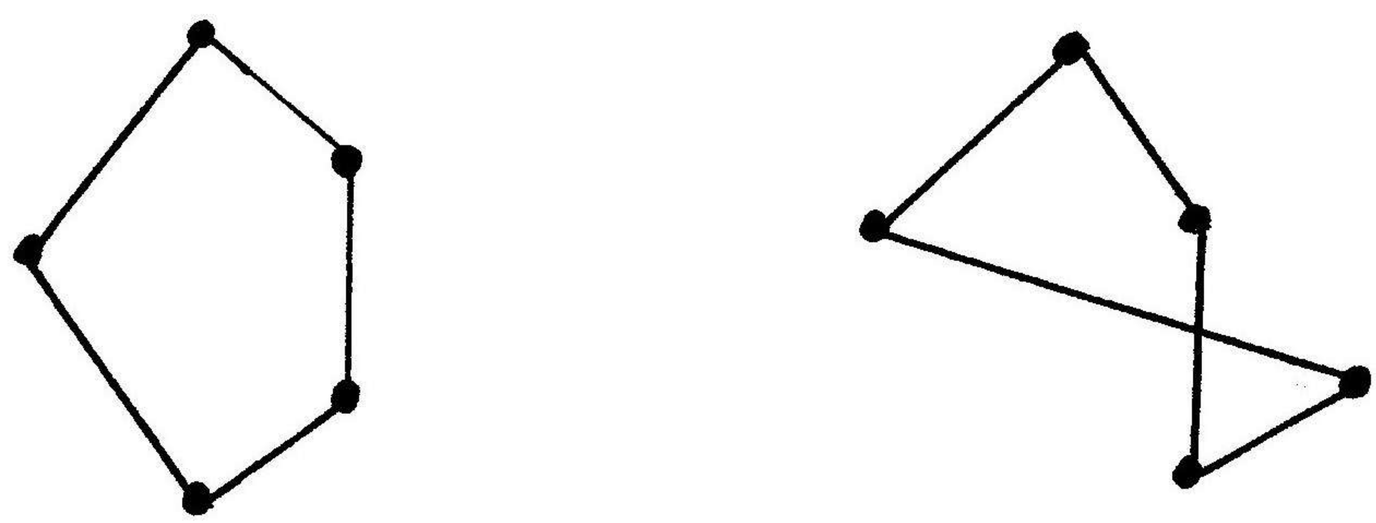
(26) Ve kterém svazu je každá podmnožina podsvaz?

(27) Rozhodněte, zda následující dvojice svazů jsou izomorfní:

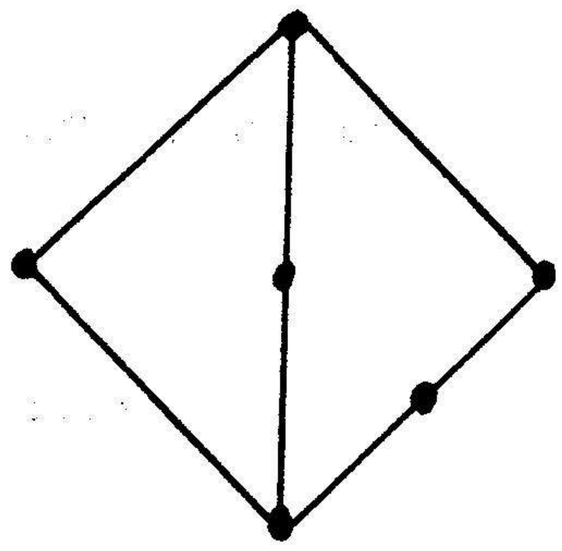
(a)

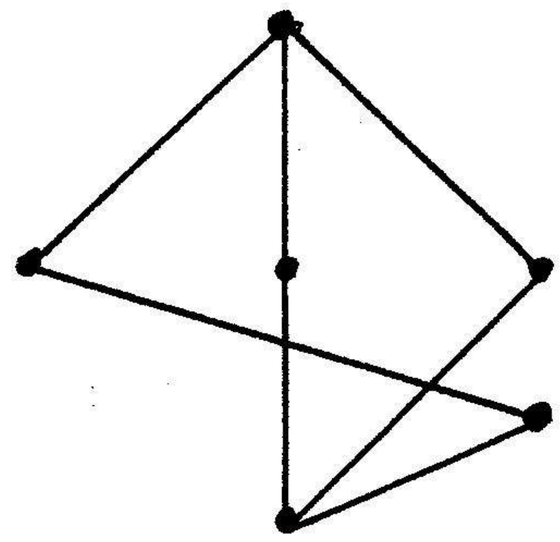


(b)

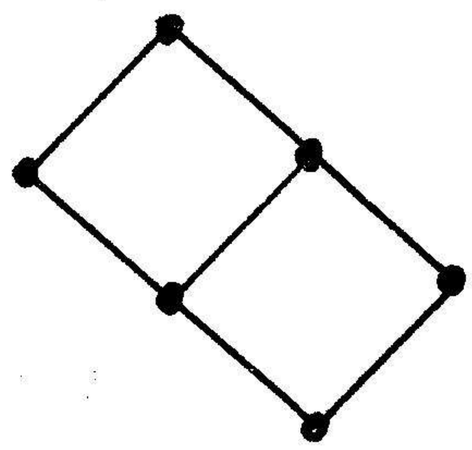


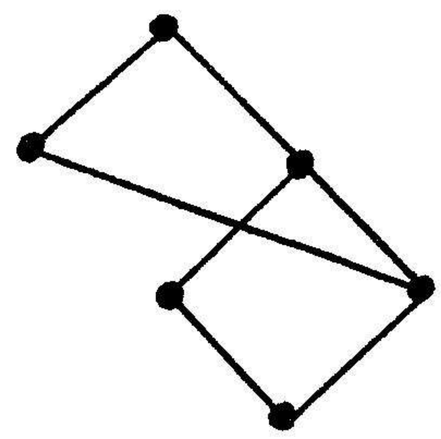
(c)



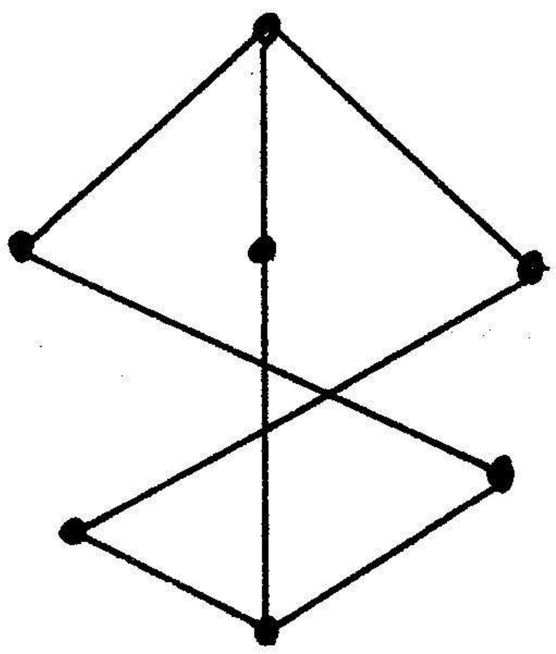


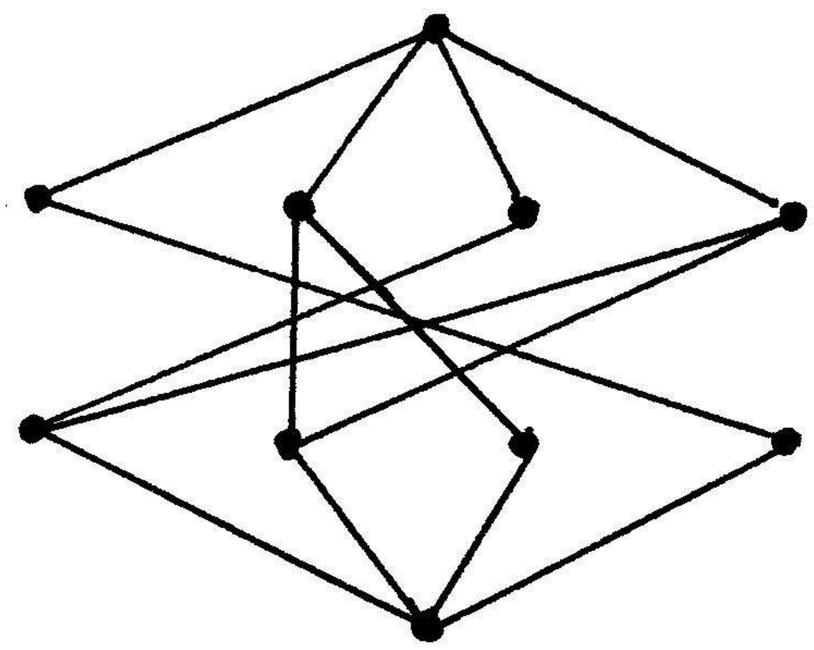
(d)





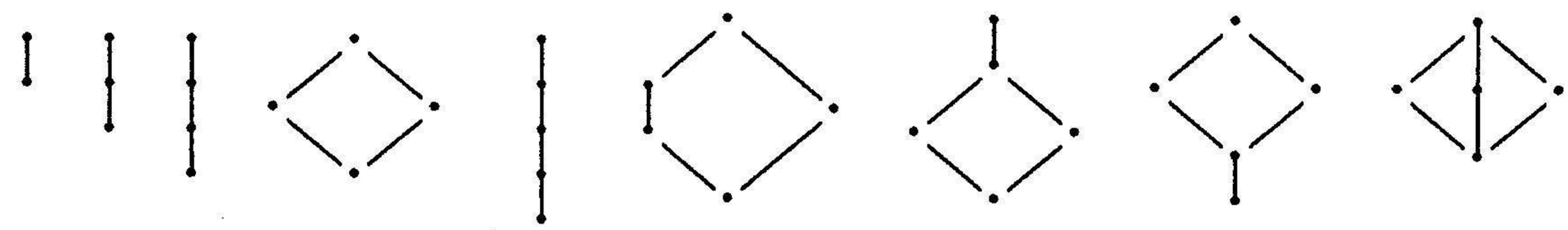
(28) Zjednodušte Hasseovy diagramy svazů:





Návody k řešení:

(1)



(2) $sup(a,b)$ neexistuje, $inf(c,d)$ neexistuje.

(3) infimum je průnik, supremum je sjednocení.

(4) Ukažte, že $sup(a,b)$=NSN(a,b), $inf(a,b)$=NSD(a,b).

(5) Uvědomte si, že zde jsou každé dva prvky srovnatelné. Žádný ze svazů nemá 0 a 1.

(6) Ukažte, že $(\mathbb{N},|)$ je svaz, kde $sup(a,b)=NSN(a,b)$,
$inf(a,b)=NSD(a,b)$.
Nejmenší prvek je 1, největší prvek svaz nemá.

(7) Užijte cvičení (6). Svaz $(\mathbb{N}_0,|)$ má největší prvek 0.

(9)(i) Kdyby $x\wedge y=x$, pak $x\leq y$, což je spor s $x\|y$. Podobně $x\wedge y=y$ implikuje $y\leq x$.

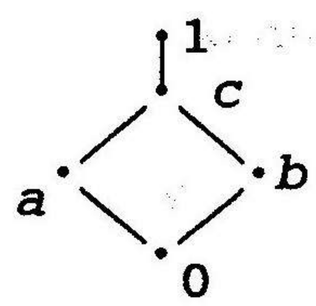
(10) Ukažte nejprve, že $\leq$ je uspořádání na $L(a,b)$. Ukažte dále, že $f\vee g=h$, kde $h(x)=f(x)$, jestliže $f(x)\geq g(x)$, $h(x)=g(x)$, je-li $f(x)\leq g(x)$. Ukažte podobné tvrzení pro infimum.

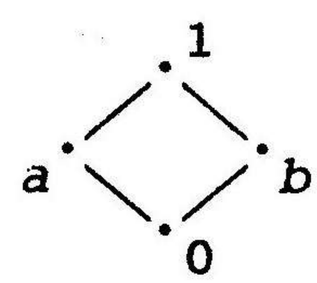
(11) Je-li $a\wedge b=a$, pak dle definice $a\leq b$, tedy $a\vee b=b$. Obrácené tvrzení se dokáže podobně.

(12) Ukažte, že zobrazení $x\mapsto x'$ pro každé $x\in\{0,1\ a,b,c,d,e,f,g\}$ je izomorfismus.

(13) Ukažte, že jsou-li $R,S\subseteq A^2$, pak $inf(R,S)=R\cap S$, $sup(R,S)=R\cup S$. Na n-prvkové množině je tolik relací, kolik je podmnožin v A^2, tedy 2^{n^2}. Pro $n=2$ existuje $2^4=16$ relací.

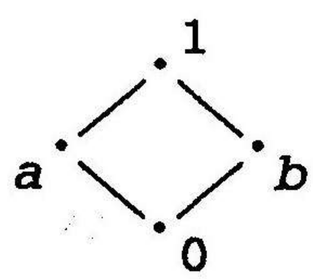
(14) Například:

L: 

H: 

(15) Jsou-li prvky a,b srovnatelné, např. $a\leq b$, pak podsvaz generovaný prvky a,b je roven $\{a,b\}$. Jsou-li $a\|b$, pak obsahuje prvky $a\wedge b\neq a,b$, $a\vee b\neq a,b$.

(16) Například zobrazení f:

L_1: 

$\xrightarrow{f}$ L_2: $f(1)$, $f(a)$, $f(b)$, $f(0)$

L_1, L_2 nejsou izomorfní.

f není isomorfismus, neboť f^{-1} není izotonní.

(17) Pro každý prvek $x \in L_1$ platí: $x \wedge 0 = 0$.
Jelikož h je homomorfismus, platí $h(x \wedge 0) = h(x) \wedge h(0) = h(x)$.
Jelikož h je surjekce, je $h(0)$ nejmenší prvek v L_2.
Podobně se důkaz provede pro prvek 1.

(18) Nechť $a, b \in L$, $a \leq b$. Pak
$h(a \vee b) = h(b)$. Jelikož h je izotonní, je $h(a) \leq h(b)$, tedy $h(a) \vee h(b) = h(b)$. Podobně proveďte pro průsek.

(19) Ukažme nejprve, že $h(x) \in [a \wedge b, a \vee b]$.
Platí $((a \wedge b) \vee x)) \wedge (a \vee b) \leq a \vee b$ (proč?), $(a \wedge b) \vee x \geq a \wedge b$, $a \vee b \geq a \wedge b$, tedy $((a \wedge b) \vee x) \wedge (a \vee b) \geq a \wedge b$.
Je-li $x \leq y$, pak $x \vee (a \wedge b) \leq y \vee (a \wedge b)$, tedy

$$(x \vee (a \wedge b)) \wedge (a \vee b) \leq (y \vee (a \wedge b)) \wedge (a \vee b), \text{ t.j.}$$

$$h(x) \leq h(y).$$

(20) Ukažte, že jsou to právě všechny jednoprvkové množiny, je jich právě n.

(21) Ukažme nejprve, že $h_b(x) \in [a \wedge b, b]$:
Je jasné, že $x \wedge b \leq b$. Je-li $x \in [a, a \vee b]$, pak $x \geq a$, tedy $x \wedge b \geq a \wedge b$.
Ukažte podobně pro g_a.
Dokažme nyní, že $h_b \circ g_a \circ h_b = h_b$.
Dle předpokladu $x \in [a, a \vee b]$. Obecně platí $a \vee (b \wedge x) \geq b \wedge x$, tedy

$$b \wedge (a \vee (b \wedge x)) \geq b \wedge (b \wedge x) = b \wedge x.$$

Dále, $b \wedge x \leq x$, $a \vee (b \wedge x) \leq a \vee x = x$, tedy

$b \wedge (a \vee (b \wedge x)) \leq b \wedge x$, dohromady $b \wedge (a \vee (b \wedge x)) = b \wedge x$, což bylo dokázat.

(22) Jestliže $c \succ a$, $c \succ b$, $a \neq b$, pak $c > a$, $c > b$, tedy $c \geq a \vee b$.
Kdyby $c > a \vee b$, pak c nekryje prvek a, spor. Je tedy $c = a \vee b$.

(23) Nechť $M = [a, b] \cap [c, d]$, $M \neq \emptyset$.
Nechť $a \leq x \leq b$, $c \leq x \leq d$. Pak $a \leq a \vee c \leq x \leq b$, $c \leq a \vee c \leq x \leq d$, tedy $a \vee c \in [a, b] \cap [c, d]$.
Dále $b \wedge d \leq b, d$; $b \wedge d \geq x \geq c, a$, tedy $b \wedge d \in [a, b] \cap [c, d]$.
Zřejmě $x \geq a \vee c$, $x \leq b \wedge d$, tedy $a \vee c$ je nejmenší prvek a $b \wedge d$ je

největší prvek z $[a,b]\cap[c,d]$, t.j. $[a,b]\cap[c,d]=[a\vee c, b\wedge d]$.

(24) Ne:

$$\begin{tikzcd} b \arrow[r, "h"] \arrow[d, dash] & h(b) \arrow[d, dash] \\ & c \\ a \arrow[r, "h"] & h(a) \end{tikzcd}$$

(25)(i) Platí $a\geq a\wedge b, a\wedge c$,

$b\vee c\geq a\wedge b$, $a\wedge c$, tedy $a\wedge(b\vee c)\geq(a\wedge b)\vee(a\vee c)$.

(ii) Platí $a\leq a\vee b, a\vee c$

$b\vee c\leq a\vee b, a\vee c$, tedy $a\vee(b\wedge c)\leq(a\vee b)\wedge(a\vee c)$.

(iii) Platí $a\leq a\vee b, c$

$b\wedge c\leq a\vee b, c$, tedy $a\vee(b\wedge c)\leq(a\vee b)\wedge c$.

(iv) Platí $a\wedge c\leq a\vee b, c\vee d$

$b\wedge d\leq a\vee b, c\vee d$, tedy $(a\wedge c)\vee(b\wedge d)\leq(a\vee b)\wedge(c\vee d)$.

(v) Platí $a\wedge b, b\wedge c, c\wedge a\leq a\vee b, b\vee c, a\vee c$, tedy

$(a\wedge b)\vee(a\wedge c)\vee(b\wedge c)\leq(a\vee b)\wedge(a\vee c)\wedge(b\vee c)$.

(26) V řetězci.

3. ÚPLNÉ SVAZY

Uspořádaná množina $(A,\leq)$ je <u>úplný svaz</u>, jestliže pro každou podmnožinu $X\subseteq A$ existuje $\sup X$ a $\inf X$. Specielně, každý úplný svaz je svazem, který má nulu, neboť $0=\inf A$, a jedničku, neboť $1=\sup A$.

Příklady:

(1) Dokažte, že pro $A\neq\emptyset$ je $(Exp A,\subseteq)$ úplný svaz.

(2) Nechť $\mathbb{N}$ je množina všech přirozených čísel, symbol $|$ označuje relaci dělitelnosti. Je $(\mathbb{N},|)$ úplný svaz? Položme $\mathbb{N}_0=\mathbb{N}\cup\{0\}$. Je $(\mathbb{N}_0,|)$ úplný svaz?

(3) Dokažte, že množina všech ekvivalencí na množině $A\neq\emptyset$ tvoří úplný svaz vzhledem k $\subseteq$.

(4) Nechť $(G,\cdot)$ je grupoid. Dokažte, že množina všech

(a) kongruencí na $(G,\cdot)$;

(b) všech podgupoidů spolu s $\emptyset$,

tvoří úplné svazy (vzhledem k $\subseteq$).

(5) Dokažte, že množina všech podgrup dané grupy tvoří úplný svaz vzhledem k $\subseteq$.

(6) Dokažte, že množina všech normálních podgrup grupy $(G,\cdot)$ tvoří úplný svaz. Pro normální podgrupy N,H grupy $(G,\cdot)$ určete $N\wedge H$, $N\vee H$ v tomto svazu!

(7) Dokažte, že podsvaz úplného svazu nemusí být úplný.

(8) Nechť Φ je třída některých zobrazení množiny $\emptyset\neq I$ do I. Ukažte, že podmnožiny $X\subseteq I$ takové, že $\varphi(X)\subseteq X$ pro každé $\varphi\in\Phi$, tvoří úplný svaz (uspořádání je obvyklé uspořádání zobrazení).

(9) Ukažte, že konvexní podmnožiny X libovolné uspořádané množiny $(A,\leq)$ tvoří spolu s $\emptyset$ vzhledem k inkluzi úplný svaz.
(Množina $X\subseteq A$ je konvexní, platí-li : $a\leq x\leq b$, $a,b\in X \Rightarrow x\in X$).

(10) Ukažte, že úplný svaz všech ideálů okruhu $(\mathbb{Z},+,\cdot)$ je izomorfní svazu celých nezáporných čísel uspořádaných

relací dělitelnosti.

(11) Nechť P je uspořádaná množina, v níž existuje $\inf H$ pro každou množinu $H \subseteq P$. Pak P je úplný svaz. Dokažte!

Návody k řešení:

(2) $(\mathbb{N}, |)$ není úplný svaz, neboť nemá největší prvek. $(\mathbb{N}_0, |)$ je úplný svaz, $\sup \mathbb{N}_0 = 0$.

(3) Je-li $\{E_\alpha;\ \alpha \in I\}$, systém ekvivalencí na A, pak $\cap\{E_\alpha;\ \alpha \in I\}$ je ekvivalence (dokažte!) a množina $A \times A$ je ekvivalence na A. Ekvivalence na A tvoří tedy uzávěrový systém na množině $A \times A$. Je tedy svaz ekvivalencí úplný.

(4)(a) Je-li $\{C_\alpha; \alpha \in \Lambda\}$ systém kongruencí na G, pak $\cap\{C_\alpha; \alpha \in \Lambda\}$ je kongruence na G (dokažte!). Kongruence tedy tvoří na $G \times G$ uzávěrový systém a svaz kongruencí je úplný.

(b) Je-li $\{G_\alpha; \alpha \in \Lambda\}$ systém podgrupoidů spolu s $\emptyset$, pak $\cap\{G_\alpha; \alpha \in \Lambda\}$ je buď $\emptyset$ nebo podgrupoid (dokažte!) a G je podgrupoid v G. Podgrupoidy tedy tvoří uzávěrový systém na množině G a svaz podgrupoidů je úplný.

(5) Použijte a modifikujte cvičení (4).

(6) $N \wedge H = N \cap H$, $N \vee H = N \cdot H = \{n \cdot h;\ n \in N,\ h \in H\}$.

(7) Např. podsvaz $(\mathbb{N}, |)$ úplného svazu $(\mathbb{N}_0, |)$ (z příkladu (2)) není úplný.

(8) Nechť $\varphi_\alpha \in \Phi$, $\alpha \in K$, K indexová množina. Nechť $\varphi_\alpha(X_\beta) \subseteq X_\beta$ pro každé $\alpha \in K$, $\beta \in K'$, K' indexová množina.
Pak pro pevné α platí:

$$\varphi_\alpha(\cap\{X_\beta;\ \beta \in K'\}) \subseteq \cap\{\varphi_\alpha(X_\beta);\ \beta \in K'\} \subseteq \cap\{X_\beta;\ \beta \in K'\},$$

tedy třída Φ je uzavřena na libovolné průniky. Dále, $\varphi_\alpha(I) \subseteq I$ pro každé $\alpha \in K$, tedy uvažované množiny tvoří úplný svaz.

(9) Ukažte, že libovolný průnik konvexních podmnožin je buď konvexní podmnožina nebo $\emptyset$.

(10) V okruhu $(\mathbb{Z}, +, \cdot)$ je každý ideál hlavní. Přiřadíme-li každému

$n \in \mathbb{N}_0$ ideál generovaný n, dostaneme izomorfismus svazů.

(11) Nechť $H \subseteq P$, K množina všech horních závor množiny H. Nechť $a = infK$. Je-li $h \in H$, pak $h \leq k$ pro každé $k \in K$, tedy $h \leq a$, $a \in K$. Tedy a je nejmenší prvek v K, t.j. $a = supH$. Jelikož každá množina $H \subseteq P$ má také supremum $supH$, je P úplný svaz.

4. MODULÁRNÍ, DISTRIBUTIVNÍ A KOMPLEMENTÁRNÍ SVAZY.

Svaz $(L;\vee,\wedge)$ se nazývá <u>modulární</u>, jestliže pro každé $a,b,c\in L$ platí

$$a\leq c \Longrightarrow a\vee(b\wedge c)=(a\vee b)\wedge c.$$

Svaz L je <u>distributivní</u>, jestliže pro každé $a,b,c\in L$ platí

$$a\vee(b\wedge c)=(a\vee b)\wedge(a\vee c).$$

Svaz L s 0 a 1 je <u>komplementární</u>, jestliže pro každý prvek $a\in L$ existuje prvek $b\in L$ tak, že

$$a\vee b=1 \ , \ a\wedge b=0;$$

prvek b se nazývá <u>komplement</u> prvku a. Jestiže v komplementárním svazu L má každý prvek jediný komplement, pak se L nazývá <u>jednoznačně komplementární</u>.

Je-li ve svazu L každý interval $[a,b]$ (pro $a\leq b$) komplementární podsvaz, pak se L nazývá <u>relativně komplementární</u>. Prvek $y\in[a,b]$ je <u>relativní komplement</u> prvku $x\in[a,b]$ v intervalu $[a,b]$, jestliže

$$x\wedge y=a \ , \ x\vee y=b.$$

<u>Příklady</u>:

(1) Nechť L je distributivní svaz. Nechť $o,j\notin L$, a nechť $L^*=L\cup\{o,j\}$, kde v množině L^* platí:

(i) $x\leq y$ pro $x,y\in L \Longrightarrow x\leq y$ také na L^*

(ii) $o\leq x\leq j$ pro každé $x\in L$.

Dokažte, že L^* je opět distributivní svaz s nulou o a jedničkou j. Platí obdobné tvrzení i pro modulární svaz?

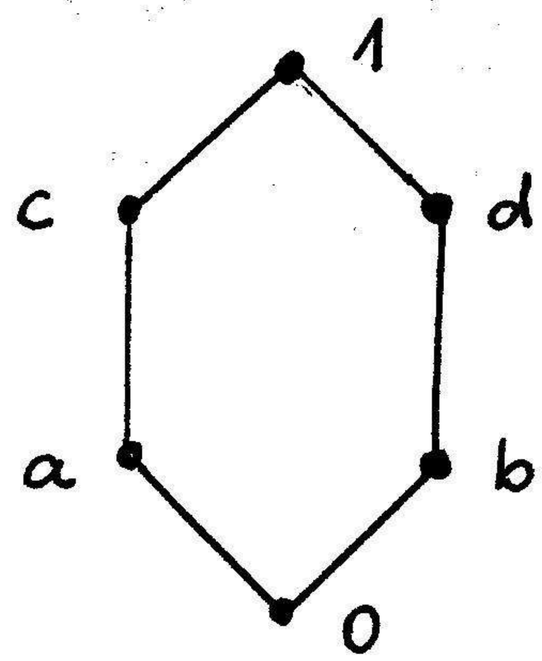
(2) Ukažte, že modulární zákon je samoduální.

(3) Ukažte, že je-li svaz L modulární, pak pro každé $a,b\in L$ platí:

(i) $a\succ a\wedge b,\ b\succ a\wedge b \Longrightarrow a\vee b\succ a,\ a\vee b\succ b;$

(ii) $a\vee b\succ a,\ a\vee b\succ b \Longrightarrow a\succ a\wedge b,\ b\succ a\wedge b.$

(4) Ukažte, že svaz

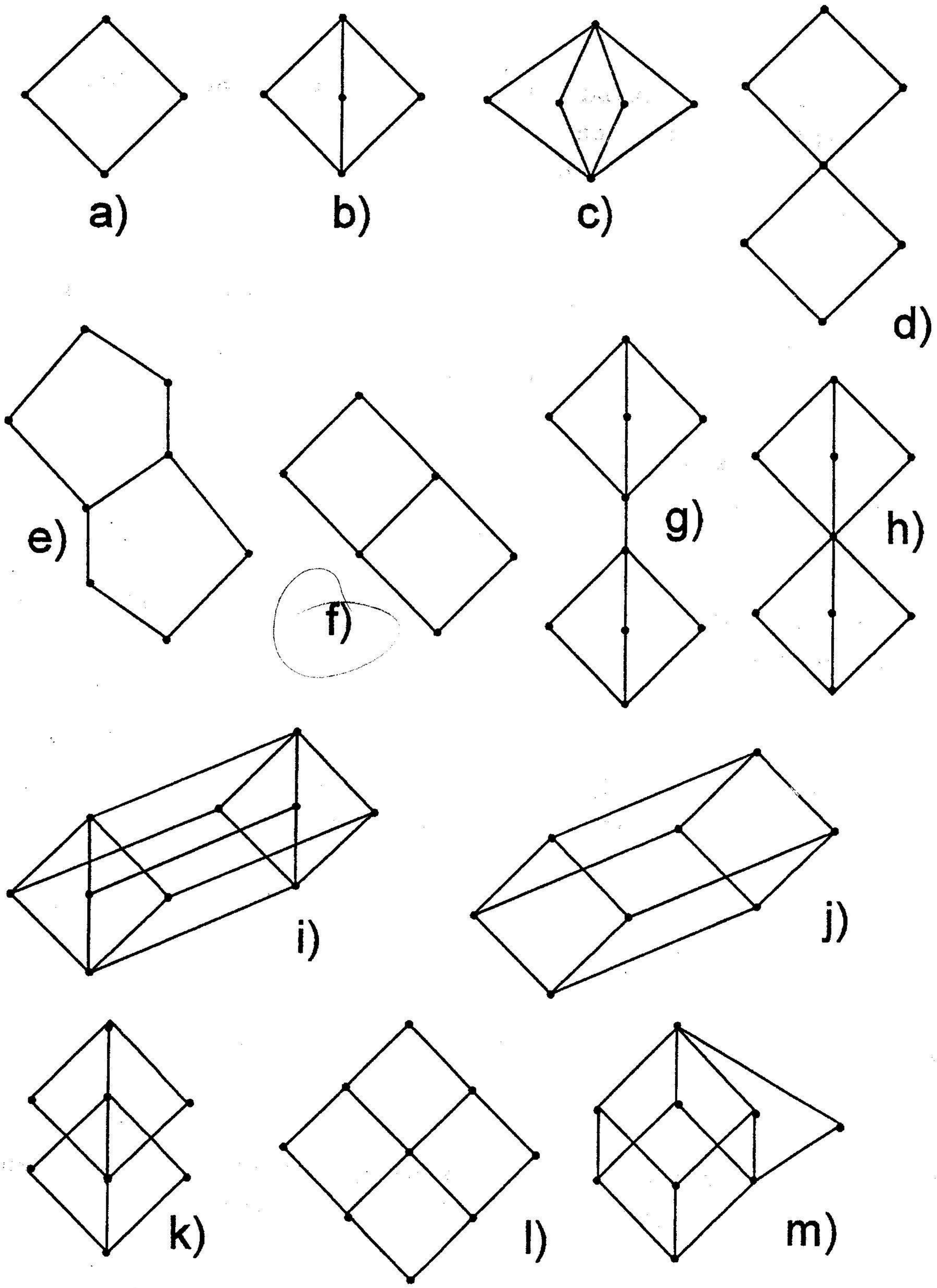


není modulární.

(5) Dokažte, že každý řetězec je distributivní svaz. Kdy je řetězec úplný svaz?

(6) Dokažte, že v distributivním svazu L platí pro každé $n \in \mathbb{N}$ a $b, a_1, \ldots, a_n \in L$ identity:
$b \wedge (a_1 \vee \ldots \vee a_n) = (b \wedge a_1) \vee \ldots \vee (b \wedge a_n)$,
$b \vee (a_1 \wedge \ldots \wedge a_n) = (b \vee a_1) \wedge \ldots \wedge (b \vee a_n)$.

(7) Které z následujících svazů jsou modulární, které jsou distributivní?


a)
b)
c)
d)
e)
f)
g)
h)
i)
j)
k)
l)
m)

(8) Nechť L je distributivní svaz, $a,b\in L$, $a\leq b$. Dokažte, že zobrazení $h:L\longrightarrow[a,b]$ dané předpisem

$$h(x)=(a\vee x)\wedge b,$$

je homomorfismus svazu L na podsvaz $[a,b]$.

(9) Dokažte, že svaz L je distributivní právě když pro každé $x,y,z\in L$ platí

$$(x\vee y)\wedge z\leq x\vee(y\wedge z).$$

(10) Dokažte, že L je distributivní svaz právě když pro každé $a,b,c\in L$ platí

$$(a\vee c=b\vee c,\ a\wedge c=b\wedge c)\implies a=b.$$

(11) Dokažte, že L je distributivní svaz právě když pro každé $a,b,c\in L$ platí

$$(a\wedge b)\vee(b\wedge c)\vee(c\wedge a)=(a\vee b)\wedge(b\vee c)\wedge(c\vee a).$$

(12) Ukažte, že každý podsvaz a každý homomorfní obraz distributivního svazu je opět distributivní svaz.

(13) Dokažte, že direktní součin distributivních svazů je distributivní svaz.

(14) Dokažte, že každý svaz s méně než pěti prvky je distributivní.

(15) Dokažte, že svaz L je modulární, právě když splňuje identitu

$$(x\vee(y\wedge z))\wedge(y\vee z)=(x\wedge(y\vee z))\vee(y\wedge z).$$

(16) Dokažte, že množina všech podprostorů vektorového prostoru V nad tělesem T tvoří modulární svaz.

(17) Nechť $\mathbb{N}$ ja množina všech přirozených čísel, symbol $|$ označuje relaci dělitelnosti, $\mathbb{N}_0=\mathbb{N}\cup\{0\}$. Ukažte, že svaz $(\mathbb{N}_0,|)$ (neboli $(\mathbb{N}_0,NSN,NSD)$) je distributivní svaz. Co je nulou a jedničkou v tomto svazu?

(18) Je svaz N_5 komplementární? Je N_5 relativně komplementární?

(19) Může být řetězec komplementární svaz?

(20) Je svaz $(ExpA;\subseteq)$ pro $A\neq\emptyset$ komplementární? Co je komplementem množiny $X\subseteq A$?

(21) Najděte nemodulární svaz, ve kterém prvky mající komplement netvoří podsvaz.

(22) Dejte příklad relativně komplementárního svazu, který není distributivní a má právě n prvků ($n\geq 5$).

(23) Dejte příklad modulárního svazu, ve kterém má každý prvek $x\neq 0$, $x\neq 1$ právě n komplementů.

(24) Ukažte, že v relativně komplementárním svazu konečné délky (t.j. každý jeho řetězec je konečný), je každý prvek spojením atomů.

(25) Ukažte, že v modulárním komplementárním svazu konečné délky je každý prvek spojením atomů.

(26) Dokažte, že svaz L je modulární právě tehdy, když pro každé $a,b,c\in L$ platí:
jestliže $a\leq b$, $a\vee c=b\vee c$, $a\wedge c=b\wedge c$, pak $a=b$.

(27) Buď I interval reálných čísel. Nechť D je systém rozkladů množiny I na konečný počet konečných podintervalů. Množinu D uspořádáme relací $\leq$ takto: $D_1, D_2 \in D$, pak $D_1 \leq D_2$ je-li rozklad D_1 částí rozkladu D_2. Ukažte, že $(D, \leq)$ je distributivní svaz.

(28) Ukažte, že modularita svazu L je ekvivalentní podmínce: je-li $x<z$, pak $x \vee (y \wedge z) \geq (x \vee y) \wedge z$.

(29) Ukažte, že svaz délky nejvýše 2 je modulární.

(30) Podle příkladu (16) tvoří podprostory n-rozměrného vektorového prostoru uspořádané inkluzí modulární svaz. Sestrojte tento svaz pro vektorový prostor dimenze 2 nad $\mathbb{Z}_2$ a ukažte, že je to svaz M_3.

(31) Ukažte, že libovolný svaz L je podsvaz komplementárního svazu obsahujícího o nejvýše tři prvky více. Je-li L konečný svaz, stačí přidat pouze jediný prvek.

(32) Ukažte, že v ohraničeném distributivním svazu má každý prvek nejvýše jeden komplement.

(33) V ohraničeném svazu L nechť x je relativní komplement prvku a v $[b,c]$, y je relativní komplement prvku c v $[x,1]$, z je relativní komplement prvku b v $[0,x]$, t je relativní komplement prvku x v $[z,y]$. Ukažte, že t je komplement prvku a.

(34) Nechť R je unitární okruh. Ukažte, že svaz ideálů okruhu R tvoří modulární svaz.

Návody k řešení:

(1) Jsou-li $a, b \in L^*$, pak

$o\wedge(a\vee b)=a\vee b=(o\wedge a)\vee(o\wedge b)$

$a\wedge(o\vee b)=a\wedge b=(a\wedge o)\vee(a\wedge b)$

$a\wedge(b\vee o)=a\wedge b=(a\wedge b)\vee(a\wedge o)$.

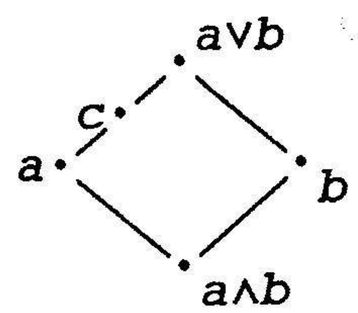
Podobně ukažte pro prvek j.

(2) Nechť pro $a\leq c$ platí $a\vee(b\wedge c)=(a\vee b)\wedge c$.

Zaměníme-li v této rovnosti prvky a,c, pak je

$$a\wedge(b\vee c)=c\vee(a\wedge b) \text{ pro } a\geq c.$$

(3)(i) Nechť $a\succ a\wedge b$, $b\succ a\wedge b$ ale $a\vee b$ nekryje a. Pak nastane situace na diagramu:



Pak $b\vee a\leq b\vee c\leq b\vee a$, tedy $b\vee c=b\vee a$,

$b\wedge c\geq a\wedge b$, ale jelikož $a,b\succ a\wedge b$, musí být $b\wedge c=a\wedge b$.

Pak prvky $\{a,b,a\wedge b,c,a\vee b\}$ tvoří pentagon N_5 a L není modulární.

(4) Obsahuje podsvaz $\{a,c,b,0,1\}$ izomorfní s N_5.

(5) Řetězec je úplný svaz právě tehdy, má-li nejmenší a největší prvek a jestliže každá jeho podmnožina má supremum.

Např. řetězec racionálních čísel s 0 a 1 není úplný svaz).

Dokážeme distributivitu řetězce:

Nechť $a,b,c\in L$, a např. nechť $b\leq c$. Pak

$a\vee(b\wedge c)=a\vee b=(a\vee b)\wedge(a\vee c)$, neboť $a\vee b\leq a\vee c$.

(6) Užijte matematické indukce.

(7) Distributivní jsou **(a),(d),(f),(j),(l)**.

Modulární jsou všechny distributivní a dále: **(b),(c),(g),(h),(i),(k)**.

(8) Ukažte nejprve, že $h(x)\in[a,b]$. Pak

$\underline{h(x\vee y)}=(a\vee x\vee y)\wedge b=((a\vee x)\vee(a\vee y))\wedge b=((a\vee x)\wedge b)\vee((a\vee y)\wedge b)=\underline{h(x)\vee h(y)}$

$\underline{h(x\wedge y)}=(a\vee(x\wedge y))\wedge b=((a\vee x)\wedge(a\vee y))\wedge b=((a\vee x)\wedge b)\wedge((a\vee y)\wedge b)=$

$=\underline{h(x)\wedge h(y)}$.

(9) Nechť platí podmínka tvrzení. Položme $x=a$, $y=b$, $z=a\vee c$. Pak $(a\vee b)\wedge(a\vee c)=a\vee(a\vee(b\wedge c))=a\vee(b\wedge c)$, tedy $(a\vee b)\wedge(a\vee c)=a\vee(b\wedge c)$.
Je-li L distributivní, pak splňuje podmínku tvrzení!

(10) Existují-li $a,b,c\in L$ tak, že $a\vee c=b\vee c$, $a\wedge c=b\wedge c$, $a\neq b$, pak $\{a,b,c,a\wedge c,a\vee c\}$ tvoří buď svaz M_3 nebo N_5.

(11) Je-li L distributivní, pak
$(a\wedge b)\vee(b\wedge c)\vee(a\wedge c)=(a\wedge(b\vee c))\vee(b\wedge c)=(a\vee(b\wedge c))\wedge(b\vee c)=$
$=(a\vee b)\wedge(a\vee c)\wedge(b\vee c)$.
Splňuje-li L podmínku tvrzení, pak položme $c^*=a\wedge c$. Dostaneme
$(a\wedge b)\vee(b\wedge c^*)\vee(a\wedge c^*)=(a\wedge b)\vee(b\wedge a\wedge c)\vee(a\wedge a\wedge c)=(a\wedge b)\vee(a\wedge b\wedge c)\vee c^*=$
$=\underline{(a\wedge b)\vee c^*}$;
$(a\vee b)\wedge(a\vee c^*)\wedge(b\vee c^*)=(a\vee b)\wedge(a\vee(a\wedge c))\wedge(b\vee(a\wedge c))=$
$=(a\vee b)\wedge a\wedge(b\vee(a\wedge c))=a\wedge(b\vee(a\wedge c))=\underline{a\wedge(b\vee c^*)}$, tedy L je distributivní.

(12) Buď S podsvaz distributivního svazu L, $a,b,c\in S$, označme operace v S symboly $\vee_s$, $\wedge_s$. Pak
$a\vee_s(b\vee_s c)=a\vee(b\vee c)$, neboť S je podsvaz. Platí
$a\vee(b\vee c)=(a\vee b)\wedge(a\vee c)$, neboť svaz L je distributivní; dále
$(a\vee b)\wedge(a\vee c)=(a\vee_s b)\wedge_s(a\vee_s c)$, neboť S je podsvaz, tedy S je distributivní svaz.
Je-li $h(L)$ homomorfní obraz L, pak platí
$h(a)\vee(h(b)\wedge h(c))=h(a)\vee h(b\wedge c)=h(a\vee(b\wedge c))=h((a\vee b)\wedge(a\vee c))=$
$=h(a\vee b)\wedge h(a\vee c)=(h(a)\vee h(b))\wedge(h(a)\vee h(c))$, tedy homomorfní obraz distributivního svazu je distributivní svaz.

(13) Buďte K,L distributivní svazy, $\langle k_1,l_1\rangle,\langle k_2,l_2\rangle,\langle k_3,l_3\rangle\in K\times L$.

Pak $\langle k_1,l_1\rangle\vee(\langle k_2,l_2\rangle\wedge\langle k_3,l_3\rangle)=\langle k_1,l_1\rangle\vee\langle k_2\wedge k_3,l_2\wedge l_3\rangle=$
$=\langle k_1\vee(k_2\wedge k_3),l_1\vee(l_2\wedge l_3)\rangle=\langle(k_1\vee k_2)\wedge(k_1\vee k_3),(l_1\vee l_2)\wedge(l_1\vee l_3)\rangle=$
$=\langle k_1\vee k_2,l_1\vee l_2\rangle\wedge\langle k_1\vee k_3,l_1\vee l_3\rangle=(\langle k_1,l_1\rangle\vee\langle k_2,l_2\rangle)\wedge(\langle k_1,l_1\rangle\vee\langle k_3,l_3\rangle)$.

(14) Najděte všechny nejvýše čtyřprvkové svazy.

(15) Je-li L modulární, pak $a\leq c \Longrightarrow a\vee(b\wedge c)=(a\vee b)\wedge c$.

Jelikož $a \le c$, je $a=a \wedge c$, $c=a \vee c$. Po dosazení dostaneme:
$(a \wedge c) \vee (b \wedge (a \vee c)) = ((a \wedge c) \vee b) \wedge (a \vee c)$.
Opačně, platí-li předchozí identita, pro $a \le c$ dostaneme modulární zákon.

(16) Jelikož průnik podprostorů je podprostor (dokažte!) a celý prostor je podprostor, tvoří podprostory uspořádané inkluzí svaz. Infimum podprostorů je rovno průniku, spojení podprostorů T_1, T_2 je rovno: $T_1 \vee T_2 = \{\underline{a}+\underline{b};\ \underline{a} \in T_1, \underline{b} \in T_2\}$ (dokažte!).
Dokažme, že tento svaz je modulární:
Nechť T_1, T_2, T_3 jsou libovolné podprostory, $T_1 \subseteq T_3$. Pak stačí ukázat, že $T_1 \vee (T_2 \wedge T_3) \supseteq (T_1 \vee T_2) \wedge T_3$ (proč?).
Buď $\underline{a} \in (T_1 \vee T_2) \wedge T_3$, tedy $\underline{a} \in T_3$, $\underline{a} = \underline{a}_1 + \underline{a}_2$, pro $\underline{a}_1 \in T_1$, $\underline{a}_2 \in T_2$.
Jelikož $T_1 \subseteq T_3$, je $\underline{a}_1 \in T_3$. Pak $a_2 = \underline{a} - \underline{a}_1 \in T_3$, tedy $\underline{a}_2 \in T_2 \wedge T_3$, tedy $\underline{a} \in T_1 \vee (T_2 \wedge T_3)$.

(17) Nulou ve svazu je 1, jedničkou je 0; nechť $a, b, c \in \mathbb{N}_0$. Pak

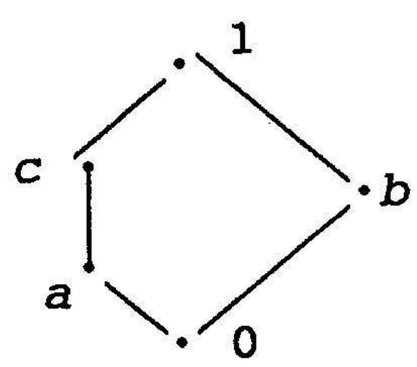
$$a = p_1^{\alpha_1} \dots p_n^{\alpha_n},\ b = p_1^{\beta_1} \dots p_n^{\beta_n},\ c = p_1^{\kappa_1} \dots p_n^{\kappa_n} \text{ a platí}$$

$$NSN(a, NSD(b,c)) = NSN(a, p_1^{\min(\beta_1,\kappa_1)} \cdot \dots \cdot p_n^{\min(\beta_n,\kappa_n)}) =$$

$$= p_1^{\max(\alpha_1, \min(\beta_1,\kappa_1))} \cdot \dots \cdot p_n^{\max(\alpha_n, \min(\beta_n,\kappa_n))}.$$

Ukažte, že $\max(\alpha_i, \min(\beta_i, \kappa_i)) = \min(\max(\alpha_i, \beta_i), \max(\alpha_i, \kappa_i))$.

(18)

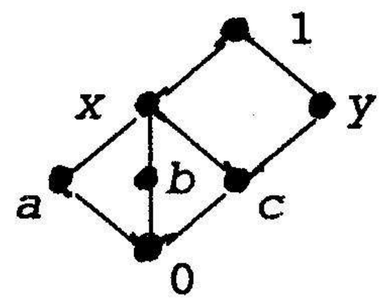


N_5 je komplementární, $0'=1, 1'=0, b'=c, a'=b=c'$.
N_5 není relativně komplemenární:
prvek a nemá v intervalu $[0,c]$ komplement.

(19) ANO, je-li dvouprvkový nebo jednoprvkový.

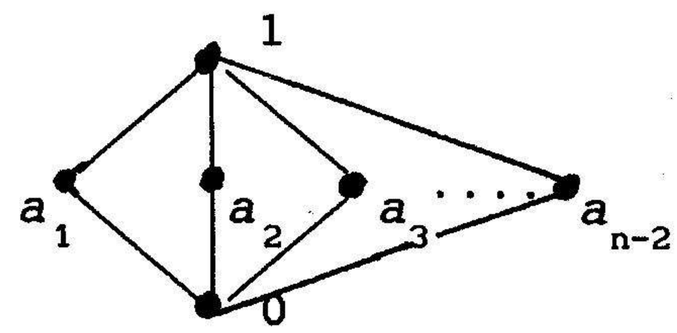
(20) ANO, komplementy jsou doplňky, t.j. komplement $X \subseteq A$ je $X \setminus A$.

(21) Např:



Prvky $a, b, y, 0, 1$ mají komplement, ale netvoří podsvaz tohoto svazu.

(22) Například:

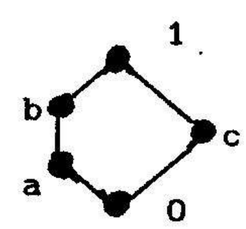


(23) Analogicky jako v (22).

(24) Je-li $a>0$, pak buď a je atom, nebo $a>b>0$ pro nějaké $b\in L$. Nechť c je relativní komplement prvku b v $[0,a]$. Indukcí dle délky intervalu $[0,a]$ se dokáže, že prvky b i c jsou spojením konečného počtu atomů. To pak platí i pro prvek a, neboť $a=b\vee c$.

(25) Každý modulární komplementární svaz je relativně komplementární (ukažte!). Využijte předchozího cvičení.

(26) Je-li L modulární, $a\leq b$, $a\vee c=b\vee c$, $a\wedge c=b\wedge c$, pak platí $a=a\vee(a\wedge c)=a\vee(b\wedge c)=(a\vee c)\wedge b=(b\vee c)\wedge b=b$.
Platí-li tvrzení věty a L není modulární, pak L obsahuje podsvaz izomorfní s N_5:



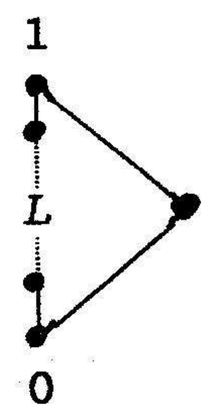
Pak $a\leq b$, $a\vee c=b\vee c$, $a\wedge c=b\wedge c$, ale $a\neq b$, spor.

(27) Nechť X resp. Y jsou dělící body dělení D_1 resp. D_2. Pak body $X\cup Y$ resp. $X\cap Y$ jsou dělící body dělení $D_1\cap D_2=D_1\wedge D_2$ resp. $D_1\vee D_2$ (dokažte!). Zbytek tvrzení je zřejmý.

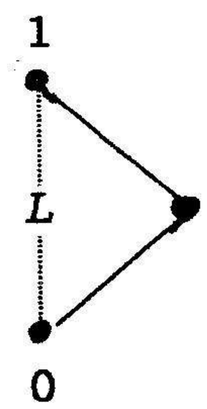
(28) Je-li L modulární, pak $x<z \Longrightarrow x\vee(y\wedge z)=(x\vee y)\wedge z$, tedy podmínka věty platí. Naopak, platí-li podmínka věty, pak $x<z$ implikuje $x\vee(y\wedge z)\geq(x\vee y)\wedge z$. Obrácená nerovnost platí triviálně, je tedy L modulární.

(30) Je-li $\{\underline{x},\underline{y}\}$ báze uvažovaného prostoru, pak jedinými netriviálními podprostory jsou $[\underline{x}]$, $[\underline{y}]$, $[\underline{x}+\underline{y}]$. Dokažte, že tyto podprostory jsou navzájem různé!

(31) Uvažujte svazy



, je-li L konečný, pak



.

(32) Vyšetřujte platnost či neplatnost distributivního zákona.

(33) Předpoklady tvrzení lze přepsat do vztahů

$$x \vee a = c \quad y \vee c = 1 \quad z \vee b = x \quad t \vee x = y$$

$$x \wedge a = b \quad y \wedge c = x \quad z \wedge b = 0 \quad t \wedge x = z.$$

Zřejmě $z \leq t \leq y$, $b \leq a \leq c$. Odtud pak

$t \wedge a \leq y \wedge c = x$, tedy $t \wedge a = t \wedge a \wedge a \leq x \wedge a = b$, t.j. $t \wedge a \leq b$. Podobně

$t \wedge a = t \wedge t \wedge a \leq t \wedge x = z$, t.j. $t \wedge a \leq z$. Dohromady $t \wedge a \leq b \wedge z = 0$, t.j. $t \wedge a = 0$.

Dokažte podobně, že $t \vee a = 1$.

5. KONGRUENCE A IDEÁLY NA SVAZECH.

Nechť $L=(A;\vee,\wedge)$ je svaz. Ekvivalence Θ na množině A se nazývá <u>kongruence svazu</u> L, má-li substituční podmínku vzhledem k operacím $\vee$ a $\wedge$, t.j. jestliže pro každé čtyři prvky $a,b,c,d\in A$ platí: jestiže $\langle a,b\rangle\in\Theta$ a $\langle c,d\rangle\in\Theta$, pak $\langle a\vee c,b\vee d\rangle\in\Theta$ a $\langle a\wedge c,b\wedge d\rangle\in\Theta$. Má-li svaz L nejmenší prvek 0, pak se množina $[0]_\Theta=\{a\in A;\ \langle a,0\rangle\in\Theta\}$ nazývá jádro kongruence Θ.

Nechť $L=(A;\vee,\wedge)$ je svaz, $\emptyset\neq I\subseteq A$; nazveme I <u>ideál svazu</u> L, jestliže pro každé dva prvky $a,b\in I$ a pro každý prvek $x\in A$ platí: $a\vee b\in I$, $a\wedge x\in I$.

Má-li svaz L nejmenší prvek 0, a je-li Θ kongruence svazu L, pak je $[0]_\Theta$ ideál svazu L.

Je-li svaz L distributivní s 0, pak je každý ideál svazu L jádrem aspoň jedné kongruence; obráceně, má-li svaz L s 0 tuto vlastnost, je distributivní.

Je-li svaz L s 0 relativně komplementární, pak je každý jeho ideál jádrem nejvýše jedné kongruence.

Ve svazu L s 0 jsou ekvivalentní tyto podmínky:

(i) každý ideál je jádrem právě jedné kongruence na L;

(ii) L je relativně komplementární distributivní svaz.

Je-li $L=(A;\vee,\wedge)$ svaz a $x\in A$, pak $I(x)=\{y\in A;\ y\leq x\}$ je ideálem svazu L. Tento ideál se nazývá <u>hlavní</u> (generovaný prvkem x). Jsou-li a,b prvky z A, pak nejmenší kongruence svazu L, obsahující dvojici $\langle a,b\rangle$ (t.j. průnik všech kongruencí svazu L, obsahujících $\langle a,b\rangle$) se nazývá <u>hlavní kongruence</u> (generovaná dvojicí $\langle a,b\rangle$).

Množina všech kongruencí na svazu L tvoří úplný svaz, označujeme jej Con$L$. Zřejmě ω je nejmenší a $\iota=L\times L$ největší prvek v Con$L$. Svaz Con$L$ je algebraický.

Množina $J(L)$ všech ideálů svazu L (spolu s $\emptyset$, pokud L nemá 0) tvoří úplný svaz. Jeho největší prvek je L, nejmenší prvek je $\{0\}$, pokud L má 0, nebo $\emptyset$, pokud L nulu nemá. $J(L)$ je algebraický svaz.

Svaz $J(L)$ je distributivní (modulární), právě když L je

distributivní (modulární).

Svaz Con$L$ je distributivní pro každý svaz L.

Příklady:

(1) Dokažte, že ve svazu jsou třídy kongruencí konvexní podsvazy.

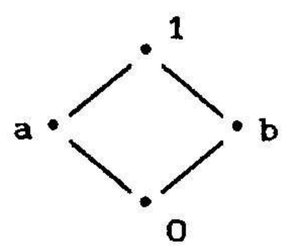
(2) Dokažte, že každý svaz je možno vnořit do svazu jeho ideálů.

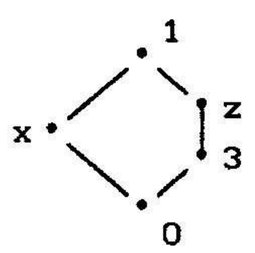
(3) Dokažte, že svaz ideálů distributivního svazu je distributivní.

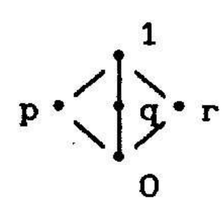
(4) Buď L distributivní svaz, $a \in L$. Nechť h: $L \longrightarrow I(a) \times D(a)$ je zobrazení dané předpisem $h(x) = \langle x \wedge a, x \vee a \rangle$.

Ukažte, že h je svazové vnoření a h je izomorfismus právě když prvek a má komplement v L.

(5) Určete všechny kongruence ve svazech:

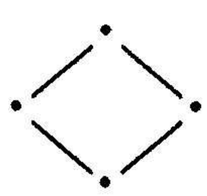
(a) 

(b) 

(c) 

(d)

(6) Nakreslete diagram direktního součinu $L_1 \times L_2$, kde L_2 je dvouprvkový svaz: $L_2 = \begin{smallmatrix} 1 \\ 0 \end{smallmatrix}$ a L_1 je :

(a) N_5 (b)  (c) M_3

(7) Na příkladu tříprvkového řetězce ukažte příklad ideálu,který je jádrem dvou konguencí.

(8) Na příkladu svazu N_5 ukažte příklad ideálu, který není

jádrem žádné kongruence.

(9) Je-li L_2 dvouprvkový svaz, určete svazy $L_2 \times L_2$, $L_2 \times L_2 \times L_2$, $L_2 \times L_2 \times L_2 \times L_2$. Ukažte všechny ideály a všechny kongruence.

(10) Nechť I je ideál distributivního svazu L. Definujme relaci R na L takto:

$$\langle x,y\rangle \in R \Leftrightarrow (\forall\ a \in L \text{ platí } (x \wedge a \in I) \Leftrightarrow (y \wedge a \in I)).$$

Dokažte, že R je kongruence na L a I je jádro této kongruence.

(11) Nechť A je nekonečná množina, nechť J je množina všech konečných podmnožin množiny A. Dokažte, že J je ideál svazu $(\mathrm{Exp}A, \subseteq)$. Tento ideál není hlavní.

(12) Určete svaz všech ekvivalencí na dvouprvkové a tříprvkové množině.

(13) Ukažte, že podmnožina $I \neq \emptyset$ svazu L je ideál právě když pro každé $a,b \in I$ platí: $a \vee b \in I \Leftrightarrow a \in I$ a $b \in I$.

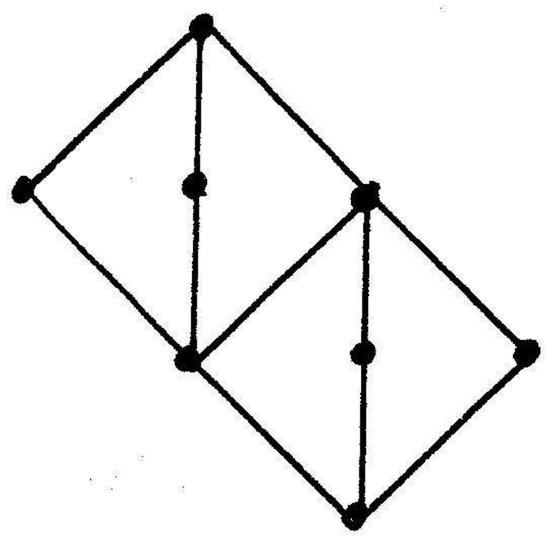
(14) Nechť θ je kongruence svazu L. Dokažte, že

$$\langle a,b\rangle \in \theta \Leftrightarrow \langle a \wedge b, a \vee b\rangle \in \theta.$$

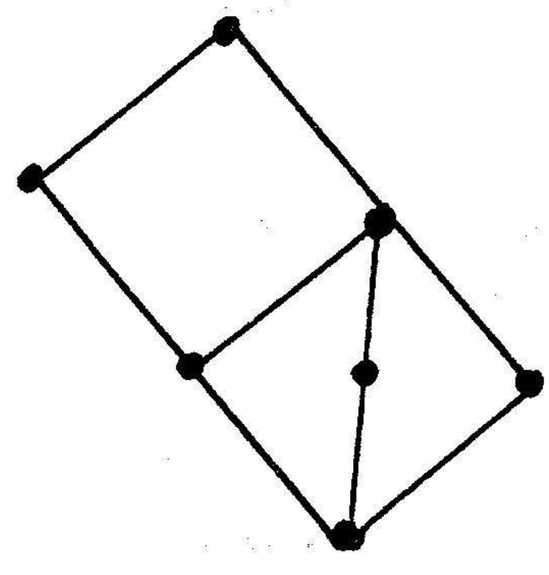
(15) Nechť L je distributivní svaz, J jeho ideál. Nechť R je relace na L daná předpisem $\langle x,y\rangle \in R \Leftrightarrow$ existuje $v \in J$ tak, že $x \vee v = y \vee v$. Dokažte, že má-li L nulu, pak R je kongruence na L jejíž jádro je J.

(16) Určete všechny kongruence svazů:

(a)



(b)



(17) Nakreslete svazy ideálů těchto svazů:

(a) N_5 (b) M_3.

(18) Nechť L je distributivní svaz, $a,b \in L$. Dokažte, že množina $J(a,b)=\{x \in L;\ a \wedge x = b \wedge x\}$, je ideál svazu L.

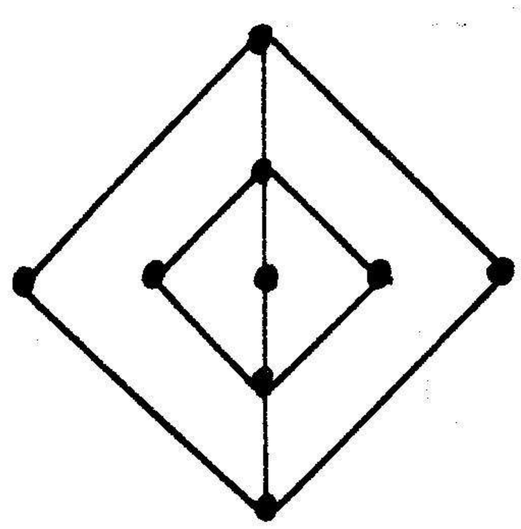
(19) Dokažte, že je-li svaz L konečný, pak je izomorfní svazu $J(L)$.

(20) Nechť L,K jsou svazy, $h: L \longrightarrow K$ surjektivní homomorfismus. Dokažte, že:

(i) je-li J ideál v L, je $h(J)$ ideál v K;

(ii) je-li I ideál v K, je $h^{-1}(I)$ ideál v L.

(21) Určete všechny kongruence svazu:



Zobecněním tohoto příkladu dokažte, že každý konečný řetězec je izomorfní svazu všech kongruencí některého konečného svazu.

(22) Ukažte, že je-li každé izotonní zobrazení svazu L do L homomorfismem, pak L je řetězec.

(23) Ukažte, že je-li L svaz konečné délky, $f: L \longrightarrow L$ svazový

homomorfismus $a \in L$, pak $f^{-1}(a)$ je interval v L, (tj. konvexní podsvaz).

(24) Ukažte, že svaz L je řetězec právě když každý ideál v L je prvoideál.

(25) Ukažte, že zobrazení $f: S \longrightarrow [S]$ přiřazující každé podmnožině S grupy G podgrupu $[S]$ kterou generuje, je $\vee$-homomorfismus svazu $(G, \leq)$ na svaz všech podgrup grupy G.

(26) Ukažte, že libovolný distributivní svaz s $n>2$ prvky má vždy dvě kongruence $\theta_1 \neq \omega \neq \theta_2$ takové, že $\theta_1 \cap \theta_2 = \omega$.

(27) Ukažte, že I je ideál svazu L právě když existuje $\vee$-homomorfismus φ svazu L na dvouprvkový řetězec $\{0,1\}$ takový, že $I = \varphi^{-1}(0)$.

(28) Nechť I, J jsou ideály ve svazu L. Dokažte, že

$$I \vee J = \{t \in L;\ t \leq i \vee j \text{ pro nějaké } i \in I, j \in J\}.$$

(29) Ukažte, že I je ideál svazu L právě když pro libovolné dva ideály I, J v L platí: (spojení ve svazu ideálů)

$$I \vee J = \{i \vee j;\ i \in I, j \in J\}.$$

(30) Ukažte, že v distibutivním svazu L s 0 a 1 direktní rozklady $L = L_1 \times L_2$ jsou ve vzájemně jednoznačném vztahu s prvky z L, majícími komplementy.

(31) Nechť L je distibutivní svaz, $x, y, a, b \in L$, $a \leq b$, $x \leq y$. Ukažte, že jestliže $x \wedge a = y \wedge a$, $x \vee b = y \vee b$, pak existují $p, q \in L$ takové, že $x = (a \vee p) \wedge q$, $y = (b \wedge p) \vee q$.

(32) Nechť L je svaz, $a \in L$. Ukažte ekvivalenci následujících podmínek:

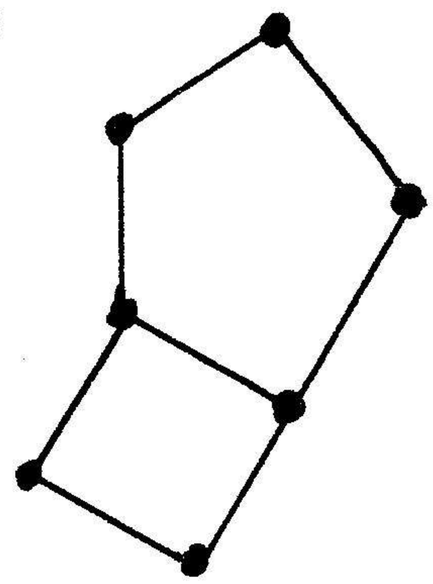
(i) pro každé $x, y \in L$ platí: $a \vee (x \wedge y) = (a \vee x) \wedge (a \vee y)$;

(ii) zobrazení $\varphi: L \longrightarrow D(a)$, $x \longrightarrow x \vee a$, je homomorfismus;

(iii) relace θ_a : $\langle x, y \rangle \in \theta_a \Leftrightarrow a \vee x = a \vee y$, je kongruence.

(33) Buď L svaz, D množina prvků z L splňující podmínku (i) ze cvičení (32). Ukažte, že D je uzavřena na suprema.

(34) Nechť L je svaz na obrázku:



Ukažte, že ideál $I(a)$ je jádrem některé kongruence na L a že prvek a splňuje podmínku (*i*) cvičení (32).

(35) Nechť prvek a svazu L splňuje podmínky cvičení (32). Dokažte, že faktorový svaz $L/\theta_a \cong D(a)$, kde $D(a)=\{x\in L;\ x\geq a\}$.

(36) Ukažte, že v modulárním komplementárním svazu je ekvivalentní pro libovolnou kongruenci θ:

(i) $\langle x,y\rangle\in\theta$;

(ii) $\langle x\wedge y, x\vee y\rangle\in\theta$;

(iii) $\langle (x\wedge y)'\wedge(x\vee y), 0\rangle\in\theta$ pro nějaký komplement prvku $x\wedge y$;

(iv) $\langle (x\wedge y)'\wedge(x\vee y), 0\rangle\in\theta$ pro libovolný komplement prvku $x\wedge y$.

(37) Ukažte, že svaz ideálů Booleovy algebry nemusí být booleovský.

(38) Ukažte, že I je ideál svazu L, právě když I je podsvaz a pro každé $a\in L$, $i\in I$ platí $a\wedge i\in I$.

(39) Nechť K,L jsou dva svazy, $\theta\in Con\ L$, $\vartheta\in Con\ K$. Definujme relaci $\vartheta\times\theta$ na $K\times L$ takto:
$\langle\langle a,b\rangle,\langle c,d\rangle\rangle \in \vartheta\times\theta$ právě když $\langle a,c\rangle\in\vartheta$ a $\langle b,d\rangle\in\theta$. Ukažte, že $\vartheta\times\theta\in Con\ (K\times L)$.

(40) Ukažte, že modulární zákon a distributivní zákon jsou samoduální.

(41) Ukažte, že je-li svaz L distributivní, pak platí pro každé $n\in\mathbb{N}$, $b,a_1,\dots,a_n\in L$:

$b\wedge(a_1\vee a_2\vee\dots\vee a_n) = (b\wedge a_1)\vee(b\wedge a_2)\vee\dots\vee(b\wedge a_n)$

$b\vee(a_1\wedge a_2\wedge\dots\wedge a_n) = (b\vee a_1)\wedge(b\vee a_2)\wedge\dots\wedge(b\vee a_n)$.

(42) Nechť L je úplný svaz, nechť L je distributivní. Ukažte, že ve cvičení (41) není možné vzít obecně libovolný (tj. nekonečný) počet prvků tak, aby rovnost platila.

Návody k řešení:

(1) Nechť $[a]_\theta$ je třída určená prvkem a. Jsou-li $x,y\in[a]_\theta$, $x\le z\le y$, pak $\langle x,y\rangle\in\theta$ (proč?), pak $\langle x\wedge z,y\wedge z\rangle\in\theta$, tedy $\langle x,z\rangle\in\theta$, $z\in[a]_\theta$ (proč?). Je tedy $[a]_\theta$ konvexní podmnožina.
Jelikož $\langle x,a\rangle$, $\langle y,a\rangle\in\theta$, platí $\langle x\vee y,a\vee a\rangle = \langle x\vee y,a\rangle\in\theta$, tedy $x\vee y\in[a]_\theta$. Podobně ukažte, že $x\wedge y\in[a]_\theta$.

(2) Průnik ideálů je buď $\emptyset$ nebo ideál (ukažte!) a celý svaz L je ideál, tedy ideály tvoří svaz vzhledem k inkluzi. Ukažme, že jsou-li $I(a),I(b)$ hlavní ideály, pak ve svazu ideálů platí: $I(a)\wedge I(b) = I(a\wedge b)$, $I(a)\vee I(b) = I(a\vee b)$. Pak je zobrazení $a\longrightarrow I(a)$ homomorfismus. Ukažte, že je-li $I(a)=I(b)$, pak $a=b$.

(3) Nechť L je distributivní, I,J,K ideály z $Id(L)$.
Ukažme nejprve, že $I\vee J = \{i\vee j;\ i\in I, j\in J\}$.
Zřejmě $I\vee J = \{x;\ x\le i\vee j;\ i\in I, j\in J\}$. Je-li $x\le i\vee j$, pak $\underline{x} = x\wedge(i\vee j) = \underline{(x\wedge i)\vee(x\wedge j)}$, ale $x\wedge i\in I$, $x\wedge j\in J$ (proč?), tedy $x = i'\vee j'$, $i'\in I, j'\in J$. Pro důkaz distributivnosti stačí ukázat $I\vee(J\cap K) \supseteq (I\vee J)\cap(I\vee K)$. Je-li $x\in(I\vee J)\cap(I\vee K)$, pak $x=i\vee j, x=i'\vee k'$, kde $i,i'\in I$, $j\in J$, $k'\in K$. Pak $x = (i\vee j)\wedge(i'\vee k') = (i\wedge i')\vee(i\wedge k')\vee$ $\vee(j\wedge i')\vee(j\wedge k')$, ovšem $i\wedge i', i\wedge k', j\wedge i'\in I$ (proč?), $j'=j\wedge k'\in J\cap K$ (proč?), tedy $i''=(i\wedge i')\vee(i\wedge k')\vee(j\wedge i')\in I$ (proč?) a $x = i''\vee j'$, tedy $x\in I\vee(J\cap K)$. Je tedy $Id(L)$ distributivní.

(4) Ukažme, že h je injekce. Je-li $h_a(x) = h_a(y)$, pak $x\wedge a = y\wedge a$, $x\vee a = y\vee a$. Kdyby $x\neq y$, pak prvky $x,y,a,x\wedge y,x\vee y$ tvoří svaz M_3 (ukažte!) a L by nebyl disributivní.
Dále, h je homomorfismus:
$h_a(x\wedge y) = \langle x\wedge y\wedge a,(x\wedge y)\vee a\rangle = \langle(x\wedge a)\wedge(y\wedge a),(x\vee a)\wedge(y\vee a)\rangle =$
$= \langle x\wedge a,x\vee a\rangle \wedge \langle y\wedge a,y\vee a\rangle = h_a(x)\wedge h_a(y)$. Podobně proveďte pro $h_a(x\vee y)$.

Nechť prvek a má kompelement a'. Buď $\langle x,y\rangle \in I(a)\times D(a)$, $x\leq a$, $y\geq a$. Ukážeme, že h_a je surjekce, tj. existuje $b\in L$ tak, že $h_a(b) = \langle x,y\rangle$. Je-li $b = (x\vee a')\wedge y$, pak $b\wedge a = a\wedge y\wedge(x\vee a') =$
$= a\wedge(x\vee a') = (a\wedge x)\vee(a\wedge a') = a\wedge x = x$, $b\vee a = ((x\vee a')\wedge y)\vee a =$
$= (a\vee y)\wedge(a\vee(x\vee a')) = y\wedge 1 = y$. Je tedy h surjekce a tedy h je izomorfismus.

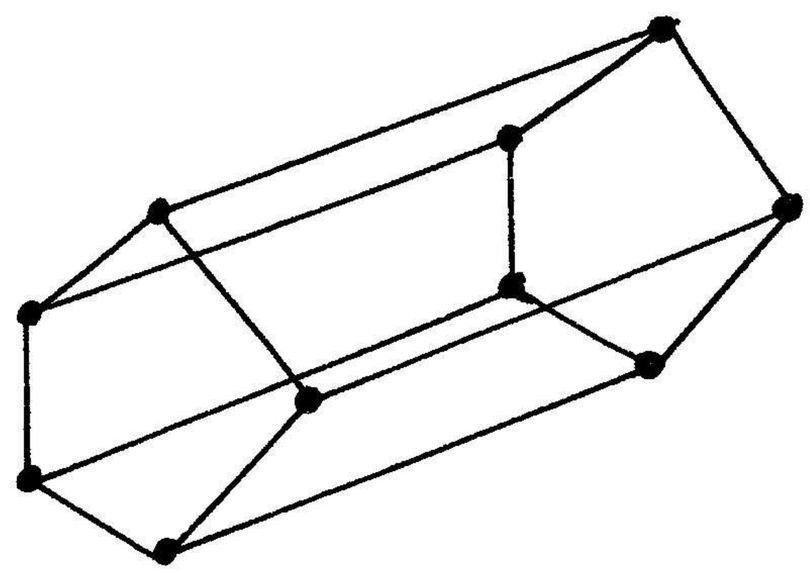
(5) (a) jsou to ω, ι, $\theta(0,a)$, $\theta(0,b)$;

(b) ω, ι, $\theta(0,x)$, $\theta(0,y) = \theta(0,z)$, $\theta(y,z)$;

(c) ω, ι;

(d) ω, ι, $\theta(0,r)$, $\theta(0,s)$, $\theta(r,s)$, $\theta(r,1)$, $\theta(s,1)$.

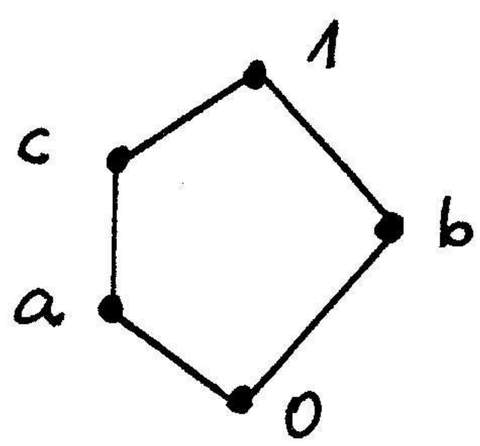
(6) (a)



(7)

$\{0\}$ je jádrem kongruencí: $\theta_1 = \omega_A \cup \{\langle a,1\rangle,\langle 1,a\rangle\}$; $\theta_2 = \omega_A$.

(8)



Ideál $\{a,0\}$ není jádrem žádné kongruence. Kdyby existovala kongruence θ tak, že $[0]_\theta = \{a,0\}$, pak $\langle a,0\rangle\in\theta$, $\langle b,b\rangle\in\theta$, tedy $\langle a\vee b, 0\vee b\rangle\in\theta$, $\langle 1,b\rangle\in\theta$. Dále $\langle c,c\rangle\in\theta$, tedy $\langle c\wedge 1, b\wedge c\rangle = \langle c,0\rangle\in\theta$, tedy $c\in[0]_\theta$, spor.

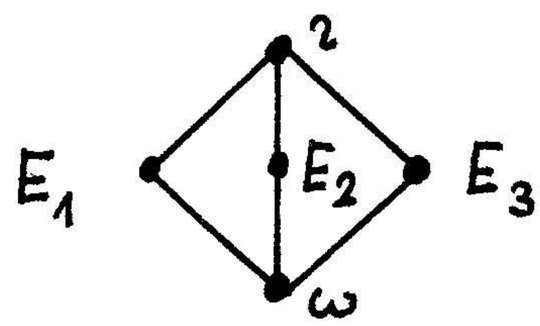
(9) $I_2 \times I_2$ je čtyřprvkový svaz,
$I_2 \times I_2 \times I_2$ je osmiprvkový booleovský svaz,
$I_2 \times I_2 \times I_2 \times I_2$ je šestnáctiprvkový booleovský svaz.
Všechny ideály jsou hlavní, kongruence vzájemně jednoznačně souvisejí s ideály. Je-li I iodeál, pak θ_I je kongruence daná předpisem: $\langle a,b\rangle \in \theta_I \Leftrightarrow$ existuje $v \in I$: $a \vee v = b \vee v$.

(10) Reflexivita, symetrie a tranzitivita relace R jsou zřejmé. Je-li $\langle a,b\rangle \in R$, $\langle x,y\rangle \in R$, pak $z \wedge a \in I \Leftrightarrow z \wedge b \in I$, $z \wedge x \in I \Leftrightarrow z \wedge y \in I$ pro každé $z \in L$. Nechť $a \wedge x \wedge z \in I$. Pak $x \wedge (a \wedge z) \in I \Leftrightarrow y \wedge (a \wedge z) \in I$, $a \wedge (y \wedge z) \in I \Leftrightarrow b \wedge y \wedge z \in I$, tedy $x \wedge a \wedge z \in I \Leftrightarrow b \wedge y \wedge z \in I$, tj. $\langle a \wedge x, b \wedge y\rangle \in R$. Dále $(a \vee x) \wedge z \in I \Leftrightarrow (a \wedge z) \vee (x \wedge z) \in I \Leftrightarrow a \wedge z, x \wedge z \in I \Leftrightarrow b \wedge z, y \wedge z \in I \Leftrightarrow (b \wedge z) \vee (y \wedge z) \in I \Leftrightarrow (b \vee y) \wedge z \in I$, tedy $\langle a \vee x, b \vee y\rangle \in R$.

(11) Nechť $A \in J$, tedy A je konečná. Je-li $B \subseteq A$, pak B je konečná, tedy $B \in J$. Jsou-li A, B konečné, pak i $A \cup B$ je konečná. Kdyby byl J hlavní ideál, musela by existovat konečná množina X tak, že každá konečná množina je její podmnožinou. Taková ale neexistuje.

(12) Na dvouprvkové množině je to

Na tříprvkové $\{a,b,c\}$ je to svaz



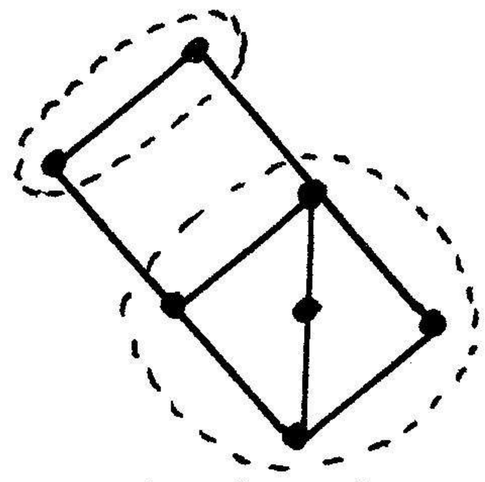
kde E_1 má třídy $\{a\},\{b,c\}$, E_2: $\{a,b\},\{c\}$, E_3: $\{a,c\},\{b\}$.

(13) Nechť I je ideál. Je-li $a \vee b \in I$, pak $a,b \leq a \vee b$, tedy $a,b \in I$. Jsou-li $a,b \in I$, pak $a \vee b \in I$. Naopak, nechť $a \vee b \in I \Leftrightarrow a,b \in I$. Je-li $a \leq b$, $b \in I$, pak $a \vee b = b \in I$, tedy $a,b \in I$. Jsou-li $a,b \in I$, pak $a \vee b \in I$ a I je ideál.

(14) Nechť $\langle a,b\rangle \in \theta$. Pak $\langle a \wedge b, b \wedge b\rangle = \langle a \wedge b, b\rangle \in \theta$,
$\langle a \vee b, b \vee b\rangle = \langle a \vee b, b\rangle \in \theta$, tedy $\langle a \wedge b, a \vee b\rangle \in \theta$.
Nechť $\langle a \wedge b, a \vee b\rangle \in \theta$. Pak $\langle a \vee (a \wedge b), a \vee a \vee b\rangle = \langle a, a \vee b\rangle \in \theta$,
$\langle b \vee (a \wedge b), b \vee a \vee b\rangle = \langle b, a \vee b\rangle \in \theta$,
tedy $\langle a,b\rangle \in \theta$.

(15) Je zřejmé, že R je reflexivní a symetrická relace. Je-li $\langle x,y\rangle\in R$, $\langle y,z\rangle\in R$, pak $x\vee v=y\vee v$, $y\vee v'=z\vee v'$, $v,v'\in J$. Pak $x\vee(v\vee v')=y\vee v\vee v'=z\vee(v\vee v')$, ale $v\vee v'\in J$. Je tedy $\langle x,z\rangle\in R$.
Nechť $\langle x,y\rangle$, $\langle a,b\rangle\in R$. Pak $x\vee v=y\vee v$, $a\vee v'=b\vee v'$, $v,v'\in J$ a dále $x\vee a\vee(v\vee v')=y\vee b\vee(v\vee v')$, ale $v\vee v'\in J$, tedy $\langle x\vee a,y\vee b\rangle\in\theta$.
Dále $(x\vee v)\wedge(a\vee v')=(y\vee v)\wedge(b\vee v')$, $(x\wedge a)\vee(x\wedge v')\vee(a\wedge v)\vee(v\wedge v')=$
$=(y\wedge b)\vee(y\wedge v')\vee(v\wedge b)\vee(v\wedge v')$.
Pak
$(x\wedge a)\vee(x\wedge v')\vee(v\wedge v')\vee(a\wedge v)\vee(v\wedge v')=(x\wedge a)\vee(v'\wedge(x\vee v))\vee(v\wedge(a\vee v'))$.
Avšak $v'\wedge(x\vee v)\in I$, $v\wedge(a\vee v')\in I$(proč?).
Označíme-li $z=(v'\wedge(x\vee v))\vee(v\wedge(a\vee v'))$, pak
$z=(v'\wedge(y\vee v))\vee(v\wedge(b\vee v'))=(y\wedge v')\vee(v\wedge v')\vee(v\wedge b)$, tedy
$(x\wedge a)\vee z=(y\wedge b)\vee z$, tedy $\langle x\wedge a,y\wedge b\rangle\in R$.
Dále $a\in[0]_R \Leftrightarrow$ existuje $v\in J$ takový, že $a\vee v=0\vee v=v$, tedy $a\leq v$.
Je tedy $[0]_R=J$.

(16) (a) ω, ι;
(b) ω, ι a kongruence určená rozkladem:



(17) (a), (b)...všechny ideály jsou hlavní. Jsou tedy svazy ideálů s nimi izomorfní.

(18) Nechť $x\in J(a,b)$, $y\leq x$. Pak $x\wedge a=x\wedge b$, $y=x\wedge y$. Dále $y\wedge a=x\wedge y\wedge a=(x\wedge a)\wedge y=(x\wedge b)\wedge y=y\wedge b$ a $y\in J(a,b)$. Jsou-li $x,y\in J(a,b)$, pak $x\wedge a=x\wedge b$, $y\wedge a=y\wedge b$, tedy $(x\vee y)\wedge a=(x\wedge a)\vee(y\wedge a)=$
$=(x\wedge b)\vee(y\wedge b)=b\wedge(x\vee y)$, tedy $x\vee a\in J(a,b)$.

(19) Je-li L konečný, pak každý ideál je hlavní.

(20) (i) Nechť $h(a)\in h(J)$, $h\in K$, $k\leq h(a)$. Pak existuje $b\in L$ takový, že $k=h(b)$ (proč?) a tedy $h(b)\leq h(a)$, $h(b)\wedge h(a)=h(b)=h(a\wedge b)$.
Jelikož $a\in J$, je $a\wedge b\in J$ (proč?) a $h(b)\in h(J)$.
Jsou-li $h(a)$, $h(b)\in h(J)$, pak $h(a)\vee h(b)=h(a\vee b)$, ovšem $a\vee b\in J$ (proč?), tedy $h(a\vee b)\in h(J)$.
(ii) Nechť $a\in h^{-1}(I)$, tedy $a=h^{-1}(i)$. Nechť $b\in L$, $b\leq a$. Pak $b=h^{-1}(z)$, $z\in K$, tedy $h^{-1}(z)\leq h^{-1}(i)$, h je homomorfismus,

tedy $h(h^{-1}(z))\leq h(h^{-1}(i))$, $z\leq i$, $z\in I$ (proč?) a tedy $b=h^{-1}(z)\in h^{-1}(I)$.
Jsou-li $a=h^{-1}(i_1)$, $b=h^{-1}(i_2)$, $i_1,i_2\in I$, pak $h(a)=i_1$, $h(b)=i_2$, $h(a)\vee h(b)=h(a\vee b)=i_1\vee i_2\in I$ (proč?), tedy $a\vee b\in h^{-1}(I)$.

(21) Je to tříprvkový řetězec $\omega < \theta < \iota$, kde θ je kongruence, jejíž třídou je $\{x,y,z,p,q\}$ a ostatní třídy jsou jednoprvkové. Vložíme-li tento svaz do M_3 místo "prostředního" prvku, dostaneme svaz S, jehož $Con\ S$ je čtyřprvkový řetězec, atd.

(22) Nechť L není řetězec. Pak v L existují nesrovnatelné prvky a, b. Izotonní zobrazení f takové, že $f(a\vee b)\neq f(a)$ a $f(a)=f(b)$, není homomorfismem: $f(a\vee b)=f(a)\vee f(b)=f(a)$, což je spor.

(23) Nechť $f(x)=f(y)=a$, $x\leq z\leq y$. Pak f je izotonní, tedy $f(x)\leq f(z)\leq f(y)$, $f(z)=a$.
Dále $f(x\vee y)=f(x)\vee f(y)=a\vee a=a$,
$f(x\wedge y)=f(x)\wedge f(y)=a\wedge a=a$,
tedy $x\vee y$, $x\wedge y\in f^{-1}(a)$. Jelikož L je konečné délky, musí být $f^{-1}(a)$ konečné délky, tedy interval konečné délky.

(24) Je-li L řetězec, a je-li I ideál, a, $b\in L$, $a\wedge b\in I$, pak buď $a\in I$ nebo $b\in I$ (proč?).
Není-li L řetězec, existují v L nesrovnatelné prvky $a\|b$. Pak hlavní ideál I generovaný prvkem $a\wedge b$ není prvoideál, neboť $a\wedge b\in I$, ale $a\notin I, b\notin I$.

(25) Buďte $S_1,S_2\subseteq G$. Stačí ukázat, že podgrupa generovaná $S_1\cup S_2$ je rovna spojení podgrup $[S_1]\cup[S_2]$. Tak je ovšem přesně definováno spojení podgrup.

(26) Jelikož $n>2$, existuje $a\in L$, $a\neq 0$, 1, pokud L má 0 a 1.
Ověřte, že zobrazení f_1: $L\longrightarrow L$: $x\longmapsto x\wedge a$,
f_2: $L\longrightarrow L$: $x\longmapsto x\vee a$,
jsou homomorfismy a relace $\theta_1=\{\langle x,y\rangle: f_1(x)=f_1(y)\}$,
$\theta_2=\{\langle x,y\rangle: f_2(x)=f_2(y)\}$
jsou kongruence. Ověřte, že $\theta_1\cap\theta_2=\omega$, navíc $\theta_1,\theta_2\neq\omega$, neboť pro

libovolný prvek $b>a$ platí $\langle a,b\rangle\in\theta_1$, pro libovolný $b<a$ platí $\langle a,b\rangle\in\theta_2$.

(27) Nechť I je ideál. Definujme φ takto: $\varphi(x)=0$ pro $x\in I$, jinak $\varphi(x)=1$. Ukažte, že φ je v-homomorfismus. Obráceně, nechť φ je v-homomorfismus, $I=\varphi^{-1}(0)$. Pak pro a, $b\in I$ je $\varphi(a)=\varphi(b)=0$, tedy $\varphi(a\vee b)=\varphi(a)\vee\varphi(b)=0\vee 0=0$, tedy $a\vee b\in I$. Je-li $a\in I$, $x\leq a$, pak $\varphi(x)\leq\varphi(a)=0$ (proč?) a tedy $\varphi(x)=0$, $x\in I$.

(28) Ukažme, že $M=\{t\in L;\ t\leq i\vee j$ pro nějaké $i\in I, j\in J\}$, je ideál. Jestliže $t_1,t_2\in M$,pak

$$t_1\leq i_1\vee j_1,\quad t_2\leq i_2\vee j_2,\quad i_1,i_2\in I,\quad j_1,j_2\in J\ .$$

Pak $t_1\vee t_2\leq(i_1\vee i_2)\vee(j_1\vee j_2)$, ale $i_1\vee i_2\in I$, $j_1,j_2\in J$ (proč?) a tedy

$$t_1\vee t_2\in M\ .$$

Jestliže $t\leq t_1$, $t_1\in M$, pak $t\leq t_1\leq i\vee j$, tedy $t\in M$. Je tedy M ideál. Ukažte, že $I,J\subseteq M$. Je-li M' ideál takový, že $M'\supseteq I,J$, pak $i,j\in M'$, tedy $i\vee j\in M'$ a tedy $t\leq i\vee j\in M'$. Je tedy M nejmenší ideál obsahující ideály I a J.

(29) Nechť L je distributivní. Pak pro $t\in I\cup J$ platí $t\leq i\vee j$ pro nějaké $i\in I$, $j\in J$ dle cv.(28). Pak $t=t\wedge(i\vee j)=(t\wedge i)\vee(t\wedge j)$, $t\wedge i\in I$, $t\wedge j\in J$ (proč?). Nechť L není distributivní. Pak obsahuje podsvaz.

Nechť $I=L(b),J=L(c)$. Platí $a\leq b\vee c$, tedy $a\in I\cup J$. Kdyby $a=i\vee j$, $i\in I$, $j\in J$, pak $j\leq a$, $j\leq c$ (proč?), tedy $j\leq a\wedge c<b$, tedy $j\in I$ a potom $a=i\vee j\in I$, což neplatí.

(30) Podle cvičení (4). Má-li $a\in L$ komplement, pak $L\cong I(a)\times D(a)$. Naopak, nechť $L\cong L_1\times L_2$. Jelikož L má 0 a 1, pak mají L_1 i L_2 nejmenší a největší prvky $0_{L_1},1_{L_1},0_{L_1},1_{L_2}$ (dokažte!). Pak prvek $\langle 1_{L_1},0_{L_2}\rangle\in L$ má komplement (proč?). Ztotožníme-li L_1 s množinou $\{\langle x_1,0_{L_2}\rangle;x_1\in L_1\}$ a množinu L_2 s množinou $\{\langle 1_{L_1},x_2\rangle;x_2\in L\}$,pak pro libovolný prvek $\langle x_1,x_2\rangle\in L$ platí:

$$\langle x_1,x_2\rangle\wedge\langle 1_{L_1},0_{L_2}\rangle=\langle x_1,0_{L_2}\rangle\ ,$$
$$\langle x_1,x_2\rangle\vee\langle 1_{L_1},0_{L_2}\rangle=\langle 1_{L_1},x_2\rangle.$$

Má tedy prvek $\langle 1_{L_1},0_{L_2}\rangle$ stejnou vlastnost jako prvek a v první části důkazu.

(31) Platí $x=x\vee(x\wedge a)=x\vee(y\wedge a)=(x\vee y)\wedge(x\wedge a)=y\wedge(x\vee a)$.
Položme $x=p$, $y=q$. Pak $y=(b\wedge x)\vee y=(b\wedge p)\vee q$.

(32)(i)⇒(ii)
ϕ je vždy v-homomorfismus, neboť $\phi(x\vee z)=x\vee y\vee a=(x\vee a)\vee(z\vee a)=$ $=\phi(x)\vee\phi(y)$. Dále $\phi(x)\wedge\phi(y)=(a\vee x)\wedge(a\vee y)=a\vee(x\wedge y)$, neboť a splňuje (i) a tedy $\phi(x)\wedge\phi(y)=\phi(x\wedge y)$. Je tedy ϕ homomorfismus.
(ii)⇒(iii)
Relace θ_a je jádrem homomorfismu ϕ z podmínky (ii).
(iii)⇒(i)
Jelikož $x\vee a=(x\vee a)\vee a$, je $\langle x,a\vee x\rangle\in\theta_a$. Analogicky, $\langle y,a\vee y\rangle\in\theta_a$. Pak $\langle x\wedge y,(a\wedge x)\vee(a\wedge y)\rangle\in\theta_a$, neboť θ_a je kongruence. Odtud díky definici θ_a máme $a\vee(x\wedge y)=a\vee((a\wedge x)\vee(a\wedge y))=(a\vee x)\wedge(a\vee y)$.

(33) Nechť $a,b\in D$. Pak

$$(a\vee b)\vee(x\wedge y)=a\vee[b\vee(x\wedge y)]=a\vee[(b\vee x)\wedge(b\vee y)]=(a\vee b\vee x)\wedge(a\vee b\vee y)=$$
$$=[(a\vee b)\vee x]\wedge[(a\vee b)\vee y],\text{ tedy } a\vee b\in D.$$

(34) $a\vee(x\wedge y)=a\vee b=c\neq x=(a\vee x)\wedge(a\vee y)=x\wedge 1$.
Množina $I(a)=\{a,0\}$ je jádrem kongruence s třídami
$$\{a,0\},\{b,c,x,y,1\}.$$

(35) Podle cvičení (32) je θ_a jádrem surjektivního homomorfismu ϕ svazu L na svaz $D(a)$. Podle věty o homomorfismu tedy $L/\theta_a\cong D(a)$.

(36)(i)⇒(ii) je cvičení (14).
(ii)⇒(iii) je-li $\langle(x\wedge y),(x\vee y)\rangle\in\theta$, pak $\langle(x\wedge y)',(x\wedge y)'\rangle\in\theta$ a tedy $\langle(x\wedge y)\wedge(x\wedge y)',(x\wedge y)'\wedge(x\vee y)\rangle=\langle 0,(x\wedge y)'\wedge(x\vee y)\rangle\in\theta$.
(iii)⇒(iv) zřejmé.
(iv)⇒(ii) Je-li $\langle 0,(x\wedge y)'\wedge(x\vee y)\rangle\in\theta$, pak $\langle(x\wedge y),(x\wedge y)\rangle\in\theta$, tedy $\langle(x\wedge y)\vee 0,(x\wedge y)\vee[(x\wedge y)'\wedge(x\vee y)]\rangle\in\theta$,
ovšem $(x\wedge y)\vee 0=x\wedge y$, $x\wedge y\leq x\vee y$, použitím modularity máme
$(x\wedge y)\vee[(x\wedge y)'\wedge(x\vee y)]=[(x\wedge y)\vee(x\wedge y)']\wedge(x\vee y)=1\wedge(x\vee y)=x\vee y$.
Tedy $\langle x\wedge y,x\vee y\rangle\in\theta$.

(37) Buď S nekonečná množina, svaz L nechť je $(ExpS,\subseteq)$. Ideál I nechť je ideál konečných podmnožin v S. Ukážeme, že I nemá v $Id(Exp(S))$ komplement. Kdyby ano, pak existuje ideál J takový, že $I\cap J=\emptyset$, tj. pro každé $X\in I, Y\in J$ je $X\cap Y=\emptyset$ (proč?). Nechť $Y\in J$. Pak pro libovolné $p\in S$ platí $\{p\}\in I$, $\{p\}\cap Y=\emptyset$, $p\notin Y$, tedy $Y=\emptyset$ a tedy $J=\emptyset$.

Pak ale $I \vee J = I \vee \emptyset = I \neq Exp(S)$, tedy J není komplement I a $(Id(Exp(S)), \leq)$ není booleovský svaz.

(38) Je-li I ideál, pak zřejmě I je podsvaz (proč?) a pro každé $a \in L, i \in I$ platí $a \wedge i \in I$.
Naopak, jestliže $x, y \in I$, pak $x \vee y \in I$, neboť I je podsvaz.
Je-li $x \in I$, $y \leq x$, pak $y = y \wedge x \in I$.

(39) Ověříme pouze substituční podmínku:
Nechť $\langle\langle a,b\rangle,\langle c,d\rangle\rangle$, $\langle\langle a',b'\rangle,\langle c',d'\rangle\rangle \in \psi \times \theta$; pak

$$\langle a,c\rangle, \langle a',c'\rangle \in \psi, \quad \langle b,d\rangle, \langle b',d'\rangle \in \theta, \text{ tedy}$$
$$\langle a \vee a', c \vee c'\rangle \in \psi, \quad \langle b \vee b', d \vee d'\rangle \in \theta, \text{ tj.}$$
$$\langle\langle a \vee a', b \vee b'\rangle, \langle c \vee c', d \vee d'\rangle\rangle \in \psi \times \theta.$$

(41) Dokažte indukcí dle n.

(42) Uvažujme svaz $(\mathbb{N}_0, |)$. Tento svaz je distributivní (viz. cvičení (2), §3). Zde $inf = NSD$, $sup = NSN$. Nechť a_n jsou všechna lichá čísla, $b=2$. Pak $sup\{a_n\}=0$ (proč?), $x \wedge a_n = NSD(2, a_n) = 1$ (proč?), tedy

$$x \wedge (a_1 \vee \ldots \vee a_n \vee \ldots) = x \wedge 0 = x = 2 \text{ (proč?)},$$
$$(x \wedge a_1) \vee (x \wedge a_2) \vee \ldots \vee (x \wedge a_n) \vee \ldots = 1 \vee 1 \vee \ldots \vee 1 \vee \ldots = 1 \text{ (proč?), ale } 2 \neq 1.$$

6. BOOLEOVY ALGEBRY

Svaz L se nazývá <u>booleovský</u>, je-li distributivní a komplementární (t.j. jednoznačně komplementární). Vzhledem k jednoznačné komplementaci budeme symbolem a' označovat komplement prvku $a \in L$.

<u>Booleovou</u> <u>algebrou</u> nazveme šestici $(A;\wedge,\vee,',0,1)$ takovou, že $(A;\wedge,\vee)$ je booleovský svaz s nulou 0 a jednotkou 1, a' je komplement prvku $a \in A$. Podmnožinu $\emptyset \neq B \subseteq A$ nazveme <u>podalgebra</u> Booleovy algebry $(A;\wedge,\vee,',0,1)$, jestliže $0 \in B, 1 \in B, (B;\wedge,\vee)$ je podsvaz svazu $(A;\wedge,\vee)$ a pro každé $a \in B$ také $a' \in B$. Ekvivalence θ na A je <u>kongruence</u> této Booleovy algebry, je-li θ kongruencí svazu $(A;\wedge,\vee)$ a dále splňuje $\langle a,b\rangle \in \theta \Rightarrow \langle a',b'\rangle \in \theta$. Nechť A,B jsou dvě Booleovy algebry, $h: A \to B$ zobrazení. h je <u>homomorfismus</u> těchto Booleových algeber, je-li homomorfismem příslušných svazů, a platí-li dále

$$h(0)=0 \ , \ h(1)=1 \ , \ h(a')=h(a)'$$

pro každé $a \in A$.

Podmnožina I Booleovy algebry $(A;\wedge,\vee,',0,1)$ je jejím <u>ideálem</u>, je-li ideálem svazu $(A;\wedge,\vee)$.

Okruh $(R;+,\cdot)$ je <u>booleovský</u>, je-li unitární a idempotentní, t.j. $a \cdot a = a$ pro každé $a \in R$.

Nechť $(A;\wedge,\vee,',0,1)$ je Booleova algebra. Pro $a,b \in A$ definujeme

$$a \oplus b = (a \wedge b') \vee (a' \wedge b) \ , \ a \cdot b = a \wedge b \ .$$

Pak $(A;\oplus,\cdot)$ booleovský okruh, jehož jednotkou je 1.

Je-li $(R;+,\cdot)$ booleovský okruh s jednotkou 1, položme pro $a,b \in R$:

$$a \vee b = a+b+ab \ , \ a \wedge b = a \cdot b \ , \ a' = 1+a \ .$$

Pak $(R;\wedge,\vee,',0,1)$ je Booleova algebra.

Nechť $(A;\wedge,\vee,',0,1)$ je Booleova algebra. <u>Booleovským</u> <u>termem</u> neboli <u>booleovským</u> <u>polynomem</u> nazveme:

(i) každý prvek $x \in A$;

(ii) jsou-li p,q booleovské termy, pak rovněž $p \vee q$, $p \wedge q$, p' jsou booleovské termy;

(iii) všechny booleovské termy vznikly užitím konečného počtu kroků (i),(ii).

Příklady:

(1) Buď $A \neq \emptyset$. Dokažte, že $(\mathrm{Exp}\ A, \subseteq)$ je Booleova algebra.

(2) Dokažte, že každý interval v booleovském svazu je booleovský svaz.

(3) Dokažte, že každý interval v booleovském svazu je relativně komplementární svaz.

(4) Je každý podsvaz booleovského svazu booleovský?

(5) Dokažte, že v booleovském svazu platí:

$$a \leq b \text{ právě když } a \wedge b' = 0.$$

(6) Sestrojte svazy všech podmnožin dvoprvkové a tříprvkové množiny. Ukažte, že jsou oba booleovské.

(7) Dokažte, že svaz kongruencí konečného řetězce je booleovský.

(8) Ukažte, že v každém konečném booleovském svazu L platí: $|Con\ L| = |L|$.

(9) Ukažte, že pro dva různé atomy p, q jednoznačně komplementárního atomického svazu platí $p \leq q'$.

(10) Dokažte, že množina všech prvků distributivního svazu L majících komplement tvoří v L booleovský podsvaz.

(11) Buď L Booleova agebra. Ukažte, že pro operace + a $\cdot$ na L definované předpisy:

$a+b=(a \wedge b') \vee (a' \wedge b)$, $a \cdot b = a \wedge b$,

je $(L, +, \cdot)$ booleovský okruh.

(12) Dokažte, že každý booleovský okruh je komutativním okruhem charakteristiky 2.

(13) Ukažte, že množina všech symetrických relací tvoří v množině všech relací uspořádané inkluzí booleovský podsvaz.

(14) Určete svazové diagramy Booleovy algebry s n prvky, kde:

(a) $n=2$, **(b)** $n=4$, **(c)** $n=8$, **(d)** $n=16$.

Určete všechny ideály a všechny kongruence těchto Booleových algeber.

(15) Nechť L je booleovský svaz, J jeho ideál. Dokažte, že relace R na L daná předpisem:

$$\langle x,y\rangle \in R \iff (x'\wedge y)\vee(x\wedge y')\in J$$

je kongruence na L a J je její jádro.

(16) Ukažte, že v konečném booleovském svazu je ideál I maximální právě když je roven hlavnímu ideálu $I(a)$ pro prvek $1\succ a$.

(17) Dokažte, že je-li L distributivní svaz s 0 a 1 konečné délky a prvek 1 je spojením atomů, je L booleovský.

(18) Dokažte, že v booleovském svazu konečné délky je každý prvek spojením atomů.

Nechť $p(x_1,x_2,\dots,x_n)$ je booleovský term n proměnných.

<u>Elementární disjunkcí</u> nazveme term:

$$x_1\vee x_2\vee\dots\vee x_n \ , \text{ kde } x_i=x_i \text{ nebo } x_i=x_i'.$$

Analogicky <u>elementání konjunkcí</u> nazveme term:

$$x_1\wedge x_2\wedge\dots\wedge x_n \ , \text{ kde } x_i=x_i \text{ nebo } x_i=x_i'.$$

Term $p_1\wedge p_2\wedge \dots \wedge p_k$ nazveme <u>normální konjunktní forma</u>, je-li p_j elementární disjunkcí pro každé $j=1,..,k$.

Term $q_1\vee q_2\vee \dots \vee q_k$ nazveme <u>normální disjunktní forma</u>, je-li q_j elementární konjunkcí pro každé $j=1,..,k$.

Každý booleovský term lze převést na normální konjunktní a normální disjunktní formu.

(19) Následující booleovské termy převeďte na normální konjunktní a normální disjunktní formy:

(i) $p(x_1,\dots,x_n)=x_1$, $q(x_1,\dots,x_n)=0$, $r(x_1,\dots,x_n)=1$

(ii) $x\vee(y\wedge z)$

(iii) $[(x_1'\vee x_2)\wedge x_3]'\wedge x_2'$

(iv) $[(x_2 \wedge x_3)' \vee x_4]' \wedge (x_2' \vee x_1')$

(v) $[(x_1 \wedge x_2 \wedge x_3')' \vee (x_1' \wedge x_3)' \vee x_2]'$

(vi) $[(x_2 \vee x_3') \wedge (x_3 \wedge x_1')]' \vee (x_1' \wedge x_3')$

(vii) $(x_1 \wedge x_2' \wedge x_3') \vee [(x_1 \vee x_2) \wedge (x_1 \vee x_3)']'$

(viii) $[(x_1 \wedge x_2) \vee (x_2' \wedge x_3)]' \wedge (x_1' \wedge x_2)$

(ix) $[x_1 \wedge x_2 \wedge (x_3 \vee x_4')]' \wedge (x_1 \vee x_4) \wedge x_2$

(x) $[(x_1 \vee x_2) \wedge (x_1' \wedge x_3)] \vee (x_1' \wedge x_3')$

(xi) $[(x_1 \vee x_2) \wedge x_3']' \wedge (x_1' \wedge x_3)$

(xii) $[(x_1 \vee x_2') \wedge (x_3' \vee x_1) \wedge (x_2 \wedge x_1')]' \wedge x_3$

(xiii) $[[x_1 \wedge (x_3 \vee x_2' \vee x_1)']' \vee x_4']'$

(xiv) $[x_1' \vee (x_2 \wedge x_3' \wedge x_4)' \vee (x_1 \wedge x_3)]'$

(xv) $[[x_2' \wedge (x_3' \wedge x_1)' \wedge (x_4 \vee x_1)]' \wedge x_2]'$.

(20) Ukažte, že každý booleovský term lze vyjádřit pomocí jediné operace:

$$a \mid b \overset{\text{def}}{=} a' \wedge b'.$$

(21) Jak vypadají svazy kongruencí na n-prvkové Booleově algebře?

(22) Buď M nekonečná množina. Buď L systém podmožin X množiny M takových, že buď X nebo X' jsou konečné. Ukažte, že $(L, \cap, \cup)$ je Booleova algebra.

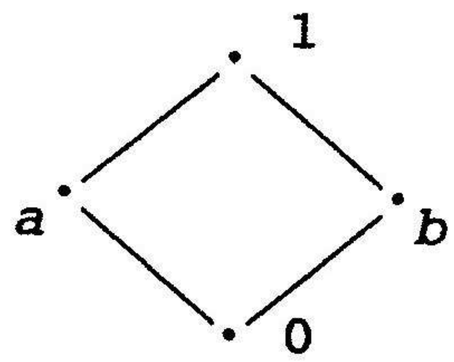
(23) Ukažte, že v Booleově algebře platí $b \leq c$, právě když $a \wedge c = 0$ imlikuje $a \wedge b = 0$.

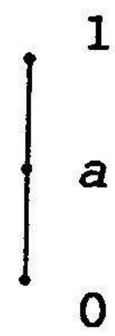
Návody k řešení:

(1) Průsek je roven průniku, spojení je rovno sjednocení, komplement je roven doplňku. Dokažte distributivní zákon pro množiny.

(2) Každý interval v Booleově algebře je podsvaz (dokažte) a tedy distributivní svaz. Každý booleovský svaz je relativně komplementární (dokažte), a tedy každý interval je komplementární.

(3) Použijte (2).

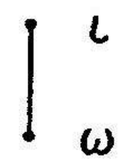
(4) Např. L: 

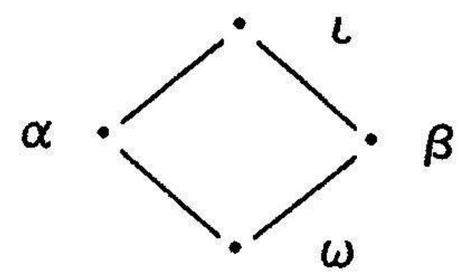
, S: 

, ale S není podalgebra Booleovy algebry.

(5) Je-li $a \le b$, pak $a = a \wedge b$ a tedy $a \wedge b' = a \wedge b \wedge b' = a \wedge 0 = 0$.
Je-li $a \wedge b' = 0$, pak $a = a \wedge (b \vee b') = (a \wedge b) \vee (a \wedge b') = (a \wedge b) \vee 0 = a \wedge b$, tedy $a \le b$.

(7) Buď $a_1 < a_2 < \ldots < a_n$ řetězec délky n.

Je-li $n=2$, pak svaz kongruencí je tvaru 

$n=3$, pak svaz kongruencí je tvaru 

, kde

$\alpha = \omega \cup \{\langle a,1\rangle, \langle 1,a\rangle\}$, $\beta = \omega \cup \{\langle a,0\rangle, \langle 0,a\rangle\}$ $(0 < a < 1)$.
Ukážeme, že je-li P_n řetězec délky n, pak $Con\ P_n \simeq 2^n$.

Důkaz provedeme indukcí dle n. Nechť tvrzení platí pro řetězec délky n $(a_1 < a_2 < \ldots < a_n)$.
Bez újmy na obecnosti lze předpokládat, že a_{n+1} je největší prvek řetězce. Je-li θ libovolná kongruence na řetězci $\{a_1, \ldots, a_n\}$, pak mohou pro prvek a_{n+1} nastat dvě možnosti :
Buď a_{n+1} je v relaci pouze sám se sebou nebo $a_{n+1} \in [a_n]_\theta$ (uvědomte si, že třídy kongruence jsou konvexní podmnožiny). Tedy každé kongruenci θ lze přiřadit právě dvě kongruence na svazu $\{a_1, \ldots, a_n\}$. Je tedy $Con\ P^n \simeq Con\ P^{n-1} \times \mathbf{2} = \mathbf{2}^{n-1} \times 2 = \mathbf{2}^n$.

(8) Ukažte, že v konečném svazu je každý ideál hlavní.
Ideály vzájemně jednoznačně souvisejí s kongruencemi.

(9) Kdyby $p \le q'$, pak $p \wedge q' < p$ a tedy $p \wedge q' = 0$(proč?). Položme $x = p \wedge q'$. Platí $x > q'$(proč?). Není-li $x \ge q$, pak $x \wedge q < q$ a tedy $x \wedge q = 0$. Ale $x \vee q \ge q' \vee q = 1$, tedy $x = q'$(proč?) a to je spor s $x > q'$. Je tedy $x \ge q$. Pak $x \ge q \vee q' = 1$, $x = 1$, $p \vee q' = 1$, tedy $p' = q'$(proč?) a tedy $p = q$,

spor.

(10) Nechť prvky $a,b\in L$ mají komplementy a',b'.
Ukážeme, že $a\wedge b$ má komplement $a'\vee b'$:
$a\wedge b\wedge(a'\vee b')=(a\wedge b\wedge a')\vee(a\wedge b\wedge b')=0\vee 0=0$,
$(a\wedge b)\vee(a'\vee b')=(a'\vee b'\vee a)\wedge(a'\vee b'\vee b)=1\wedge 1=1$.
Prvek $a\vee b$ má komplement $a'\wedge b'$:
$(a\vee b)\wedge(a'\wedge b')=(a'\wedge b'\wedge a)\vee(a'\wedge b'\wedge b)=0\vee 0=0$,
$(a\vee b)\vee(a'\wedge b')=(a\vee b\vee a')\wedge(a\vee b\vee b')=1\wedge 1=1$.
Je tedy B podsvaz. Zřejmě je B distributivní (proč ?) a komplementární, tedy Booleův.

(11) $(x\wedge y')\vee(x'\wedge y)=(x\vee x')\wedge(x\vee y)\wedge(y'\vee x')\wedge(y'\vee y)=(x\vee y)\wedge(x'\vee y')$,

(12) Z rovností
$x+y=(x+y)^2=x^2+xy+yx+y^2=x+xy+yx+y$ dostaneme
$xy+yx=0$. Pro $x=y$ odtud plyne $x^2+x^2=x+x=0$, t.j. R je charakteristiky 0. Dále platí $xy+xy=0$, tedy $xy=-xy=-yx$, t.j. $xy=yx$.

(13) Průsek relací je průnik, spojení je rovno sjednocení, doplněk relace R je roven $A^2\setminus R$. Průnik symetrických relací je symetrická relace (dokažte!), sjednocení symetrických relací R,S je symetrická relace: $(R\cup S)^{-1}=R^{-1}\cup S^{-1}=R\cup S$. Je tedy množina symetrických relací podsvaz a ten je distributivní (proč?). Stačí ukázat, že doplněk symetrické relace R je symetrická relace: $(A^2\setminus R)^{-1}=A^2\setminus R$.

(14) Všechny ideály jsou hlavní, kongruence jsou jednoznačně určeny ideály.

(15) Reflexivita: $\langle x,x\rangle\in R\Leftrightarrow(x'\wedge x)\vee(x\wedge x')=0\vee 0=0\in J$; symetrie je zřejmá; tranzitivita: Stačí si uvědomit, že $(x'\wedge y)\vee(x\wedge y')=$ $=x\oplus y$ je tzv. symetrická diference, splňující zřejmě asociativitu a vlastnosti $x\oplus 0=0\oplus x=x$, $x\oplus x=0$. Pak, nechť $\langle x,y\rangle\in R$ a $\langle y,z\rangle\in R$, t.j. $x\oplus y\in J$ a $y\oplus z\in J$, a tedy také $(x\oplus y)\oplus(y\oplus z)\in J$. Avšak $(x\oplus y)\oplus(y\oplus z)=x\oplus(y\oplus y)\oplus z=x\oplus 0\oplus z=x\oplus z$, t.j. $x\oplus z\in J$, nebo-li $\langle x,z\rangle\in J$.

(16) Každý ideál tvaru $I(a)$, kde $1 \succ a$, je maximální, neboť jinak by musel být obsažen v ideálu $I(b)$, tedy $a \leq b$, spor. Je-li $I(b)$ libovolný ideál, $b \leq c$ pro nějaký prvek $1 \succ c$, pak $I(b) \subseteq I(c)$.

(17) Jsou-li $a_1, \ldots, a_n$ atomy svazu a $1 = a_1 \vee \ldots \vee a_n$, pak pro $a \in L$ platí: $a = a \wedge 1 = (a \wedge a_1) \vee \ldots \vee (a \wedge a_n)$. Je-li $a_i \leq a$, pak $a_i \wedge a = a_i$, jinak $a_i = \wedge a = 0$. Je tedy prvek a spojením atomů, které leží v uspořádaní pod ním. Nechť jsou to atomy $a_1, \ldots, a_j$, $j \leq n$.

Uvažujme prvek $a' = a_{j+1} \vee \ldots \vee a_n$. Pak:

$a \vee a' = a_1 \vee \ldots \vee a_j \vee a_{j+1} \vee \ldots \vee a_n = 1$; $a \wedge a' = (a_1 \vee \ldots \vee a_j) \wedge (a_{j+1} \ldots \vee a_n) =$
$= (a_1 \wedge a_{j+1}) \vee \ldots \vee (a_1 \wedge a_n) \vee \ldots \vee (a_j \wedge a_n) = 0 \vee \ldots \vee 0 = 0$.

Je tedy a' komplementem prvku a.

(18) Užijte příklad (25), § 4.

(19) Reflexivita a symetrie relace R jsou zřejmé.

Dále, $\langle x,y \rangle \in R \Leftrightarrow x' \wedge y,\ x \wedge y' \in J$ (dokažte!).

Je-li tedy $\langle x,y \rangle \in R$, $\langle y,z \rangle \in R$, pak

$x \wedge y'$, $y \wedge x'$, $y' \wedge z$, $z' \wedge y \in J$ a tedy

$x \wedge z' = x \wedge z' \wedge (y \vee y') = (x \wedge z' \wedge y) \vee (x \wedge z' \wedge y') \in J$ (proč?),

$x' \wedge z = x' \wedge z \wedge (y \vee y') = (x' \wedge z \wedge y) \vee (x' \wedge z \wedge y') \in J$ (proč?)

a tedy $\langle x,z \rangle \in R$.

Nechť $\langle x,y \rangle$, $\langle a,b \rangle \in R$, tedy $x' \wedge y$, $x \wedge y'$, $a' \wedge b$, $a \wedge b' \in J$.

Pak $(x \wedge a) \wedge (y \wedge b)' = x \wedge a \wedge (y' \vee b') = (x \wedge a \wedge y') \vee (x \wedge a \wedge b') \in J$ (proč?),

$(x \wedge a)' \wedge (y \wedge b) = (x' \vee a') \wedge (y \wedge b) = (x' \wedge y \wedge b) \vee (a' \wedge y \wedge b) \in J$ (proč?),

tedy $\langle x \wedge a, y \wedge b \rangle \in R$.

Dokažte podobně, že $\langle x \vee a, y \vee b \rangle \in R$.

Dále $x \in [0]R \Leftrightarrow x' \wedge 0',\ x \wedge 0' \in J$, tedy $x \in J$.

(20) Ukažte, že $a' = a|a$, $a \vee b = (a|b)|(a|b)$, $a \wedge b = (a|a)|(b|b)$.

(21) Kongruence jsou ve vzájemně jednoznačné korespondenci s ideály a ty jsou na konečné algebře hlavní. Tedy svazy kongruencí jsou izomorfní s původními svazy.

(22) Uvažujme tři případy pro množiny $X, Y \in L$:

1) X, Y konečné; pak $X \wedge Y$, $X \vee Y$ jsou konečné a tedy prvky L,

2) X', Y' konečné; pak $(X \vee Y)' = M \setminus (X \vee Y) = (M \setminus X) \wedge (M \setminus Y) = X' \wedge Y'$ je konečná, tedy $(X \vee Y)'$ je konečná, tedy $X \vee Y \in L$.
Dále, $(X \wedge Y)' = X' \vee Y'$ je konečná, tedy $X \wedge Y \in L$,

3) X je konečná, Y nekonečná; pak $X \wedge Y$ je konečná, $(X \vee Y)' = X' \wedge Y'$ je konečná, neboť Y' je konečná.

(23) Je-li $b \leq c$ a $a \wedge c = 0$, pak $a \wedge b \leq a \wedge c = 0$, tedy $a \wedge b = 0$.
Naopak, platí $c \wedge c' = 0$, tedy $b \wedge c' = 0$. Dále $(b \wedge c')' = b' \vee c = 0' = 1$;
$b = b \wedge 1 = b \wedge (b' \vee c) = (b \wedge b') \vee (b \wedge c) = 0 \vee (b \wedge c) = b \wedge c$, tedy $b \leq c$.

O B S A H

I. ČÁST

1. Relace....4
2. Zobrazení....9
3. Ekvivalence....15
4. Uspořádání....21
5. Uzávěrové systémy....26
6. Grupoidy....31
7. Pologrupy....37
8. Grupy....43
9. Podgrupy, rozklady....50
10. Homomorfismy grup....59
11. Cyklické grupy....67
12. Permutační grupy....73
13. Vnoření pologrup do grup....76

II. ČÁST

14. Okruhy, obory integrity, tělesa....77
15. Prvoideály a maximální ideály, dělitelnost....87
16. Hlavní ideály....102
17. Homomorfismy okruhů, charakteristika....105
18. Vnoření oboru integrity do tělesa....112
19. Okruhy polynomů jedné neurčité....114
20. Polynomy více neurčitých, symetrické polynomy....120
21. Kořeny polynomů....128
22. Společné kořeny polynomů, násobné kořeny polynomů....136
23. Řešení algebraických rovnic....140

III. ČÁST

1. Uspořádané množiny, polosvazy....150
2. Svazy....154
3. Úplné svazy....162
4. Modulární, distributivní a komplementární svazy....165
5. Kongruence a ideály na svazech....176
6. Booleovy algebry....190