Lineární algebra

Kapitola 1 - Základní matematické pojmy

1.1 Relace a funkce

V celém textu budeme používat následující označení pro číselné množiny:

$\mathbb{N}$… množina všech přirozených čísel bez nuly, $\mathbb{N}=\{1, 2, 3, \ldots\}$
$\mathbb{N}_0$… množina všech přirozených čísel s nulou, $\mathbb{N}_0=\{0, 1, 2, 3, \ldots\}$
$\mathbb{Z}$… množina všech celých čísel, $\mathbb{Z}=\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
$\mathbb{Q}$… množina všech racionálních čísel
$\mathbb{R}$… množina všech reálných čísel
$\mathbb{C}$… množina všech komplexních čísel

1.1.1 DEFINICE
Nechť A, B jsou množiny. Kartézský součin $A\times B$ množin A, B je množina všech uspořádaných dvojic (a,b), kde $a\in A$, $b\in B$. Tedy $A\times B=\{(a,b)|a\in A, b\in B\}$. Každá podmnožina množiny $A\times B$ se nazývá (binární) relace z množiny A do množiny B. V případě $A=B$ hovoříme o relaci na množině A.

1.1.2 DEFINICE
Nechť A, B, C jsou množiny, $R\subseteq A\times B$, $S\subseteq B\times C$. Definujeme
(a) Definiční obor $Def\ R$ relace R jako $Def\ R=\{a\in A|$ existuje $b\in B$ tak,že $aRb\}$.
(Zde i v dalším textu píšeme aRb často místo $(a,b)\in R$.)
(b) Obor hodnot $Im\ R$ relace R jako $Im\ R=\{b\in B|$ existuje $a\in A$ tak,že $aRb\}$
(c) inverzní relaci R^{-1} k relaci R jako $R^{-1}=\{(b,a)\in B\times A\,|(a,b)\in R\}$
(d) složení RS relací R a S jako $RS=\{(a,c)\in A\times C|$ existuje $b\in B$ tak, že aRb a $bSc\}$

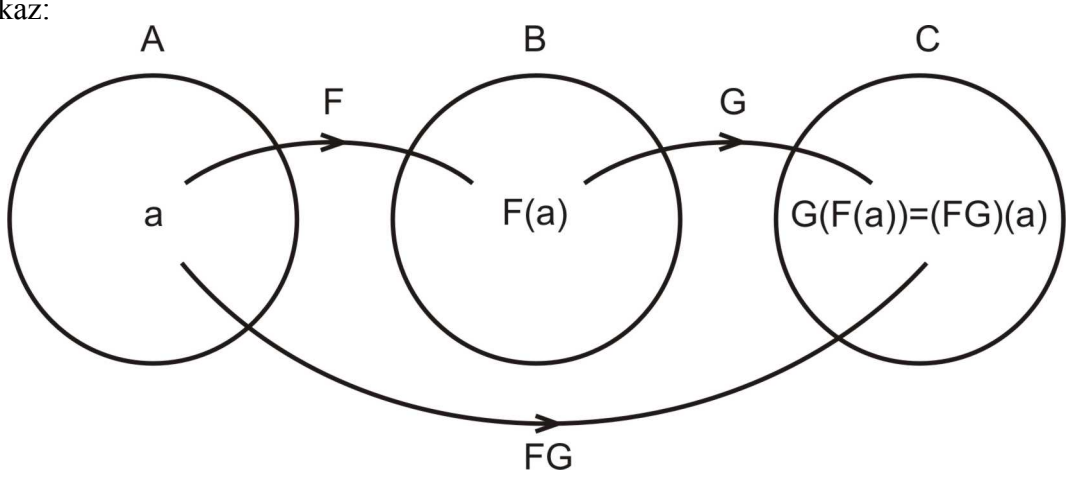
1.1.3 TVRZENÍ
Nechť A, B, C, D jsou množiny, $R\subseteq A\times B$, $S\subseteq B\times C$, $T\subseteq C\times D$. Platí:
(a) $(RS)T=R(ST)$ (skládání relací je asociativní)
(b) $(R^{-1})^{-1}=R$
(c) $(RS)^{-1}=S^{-1}R^{-1}$
Důkaz:
(a) Nechť $a\in A$, $d\in D$. Pak
$a((RS)T)d$ $\Leftrightarrow$ existuje $c\in C: a(RS)c$, cTd
$\Leftrightarrow$ existuje $c\in C$, existuje $b\in B: aRb$, bSc, cTd
$\Leftrightarrow$ existuje $b\in B: aRb$, $b(ST)d$.
$\Leftrightarrow$ $a(R(ST))d$.
Závěr: $(RS)T=R(ST)$.
(b) SAMI
(c) Nechť $c\in C$, $a\in A$. Pak
$c((RS)^{-1})a$ $\Leftrightarrow$ $a(RS)c$ ¨
$\Leftrightarrow$ existuje $b\in B: aRb$, bSc
$\Leftrightarrow$ existuje $b\in B: cS^{-1}b$, $bR^{-1}a$
$\Leftrightarrow$ $c(S^{-1}R^{-1})a$.
Závěr: $(RS)^{-1}=S^{-1}R^{-1}$.

1.1.4 DEFINICE
Nechť A, B jsou množiny, $F\subseteq A\times B$. Relace F se nazývá parciální funkce (částečné zobrazení) z množiny A do množiny B, pokud pro všechna $a\in B$, b_1, $b_2\in B$ platí:

Jestliže $a\,F\,b_1$, $a\,F\,b_2$, pak $b_1=b_2$. $a\,F\,b$ zapisujeme často ve tvaru $F(a)=b$.
Pokud navíc $Def\ F=\mathrm{A}$, pak F nazýváme totální funkce (úplné zobrazení) množiny A do množiny B. Tuto skutečnost vyjadřujeme zápisem $F:\mathrm{A}\to\mathrm{B}$. Místo totální funkce (úplné zobrazení) říkáme někdy pouze funkce (zobrazení).

1.1.5 TVRZENÍ
(a) Složení parciálních funkcí je parciální funkce.
(b) Složení totálních funkcí je totální funkce.
Důkaz:
(a) Nechť A, B, C jsou množiny, $F\subseteq\mathrm{A}\times\mathrm{B}$, $G\subseteq\mathrm{B}\times\mathrm{C}$, F a G jsou parciální funkce.
Nechť $a\in\mathrm{A}$, $c_1, c_2\in\mathrm{C}$, $a(FG)c_1$, $a(FG)c_2$.
chceme: $c_1=c_2$.
$a(FG)c_1\Leftrightarrow$ existuje $b_1\in B:\ a\,F\,b_1$, $b_1\,G\,c_1$.
$a(FG)c_2\Leftrightarrow$ existuje $b_2\in B:\ a\,F\,b_2$, $b_2\,G\,c_2$.
Vidíme, že $a\,F\,b_1$, $a\,F\,b_2$. Jelikož F je parciální funkce, je $b_1=b_2$. Označme $b=b_1=b_2$.
Pak $b\,G\,c_1$, $b\,G\,c_2$. Jelikož G je parciální funkce, je $c_1=c_2$.
(b) Nechť A, B, C jsou množiny, $F:\mathrm{A}\to\mathrm{B}$, $G:\mathrm{B}\to\mathrm{C}$. Dle části (a) již víme, že FG je parciální funkce. Zbývá tedy dokázat, že $Def(FG)=\mathrm{A}$.
$Def(FG)\subseteq\mathrm{A}$: to je zřejmé.
$\mathrm{A}\subseteq Def(FG)$: Nechť $a\in\mathrm{A}$. Víme, že $Def\ F=\mathrm{A}$. Existuje tedy $b\in\mathrm{B}$ tak, že $a\,F\,b$. Víme také, že $Def\ G=\mathrm{B}$. Tudíž $b\in Def\ G$ a existuje $c\in\mathrm{C}$, tak, že $b\,G\,c$. Potom $a(FG)c$, $a\in Def(FG)$.

1.1.6 TVRZENÍ
Nechť $F:\mathrm{A}\to\mathrm{B}$, $G:\mathrm{B}\to\mathrm{C}$, $a\in\mathrm{A}$. Pak $(FG)(a)=G(F(a))$.
Důkaz:



Víme: $(a, F(a))\in F$, $(F(a), G(F(a)))\in G$. Tudíž $(a, G(F(a)))\in FG$ což zapisujeme (dle 1.1.4.) ve tvaru $(FG)(a)=G(F(a))$.

1.1.7 DEFINICE
Nechť $F:\mathrm{A}\to\mathrm{B}$. Funkce F se nazývá
(a) injekce (injektivní, prostá), pokud po všechna a_1, $a_2\in A$ platí:
Jestliže $a_1\neq a_2$, pak $F(a_1)\neq F(a_2)$. (Ekvivalentně: Jestliže $F(a_1)=F(a_2)$, pak $a_1=a_2$.)
(b) surjekce (surjektivní, na), pokud platí:
Pro každé $b\in\mathrm{B}$ existuje $a\in A$ tak, že $F(a)=b$. (Ekvivalentně: $Im\,F=\mathrm{B}$.)
(c) bijekce (bijektivní, vzájemně jednoznačná), pokud je injekce a surjekce současně.

1.1.8 TVRZENÍ

(a) Složení injekcí je injekce.
(b) Složení surjekcí je surjekce.
(c) Složení bijekcí je bijekce.
(d) Inverzní relace k bijekci je bijekce.

Důkaz:

(a) Nechť $F: \mathrm{A} \to \mathrm{B}$, $G: \mathrm{B} \to \mathrm{C}$, F, G jsou injekce. Nechť a_1, $a_2 \in \mathrm{A}$, $(FG)(a_1)=(FG)(a_2)$ .Chceme: $a_1=a_2$. Víme, že $G(F(a_1))=G(F(a_2))$. Jelikož G je injekce, máme $F(a_1)=F(a_2)$. Jelikož F je injekce, máme $a_1=a_2$.

(b) Nechť $F: \mathrm{A} \to \mathrm{B}$, $G: \mathrm{B} \to \mathrm{C}$, F, G jsou surjekce. Nechť $c \in \mathrm{C}$. Hledáme $a \in \mathrm{A}$ tak, aby $(FG)(a)=c$. Jelikož G je surjekce, existuje $b \in \mathrm{B}$ tak, že $G(b)=c$. Jelikož F je surjekce, existuje $a \in \mathrm{A}$ tak, že $F(a)=b$. Pak $(FG)(a)=G(F(a))=G(b)=c$.

(c) Tvrzení ihned plyne z (a) a (b).

(d) Nechť $F: \mathrm{A} \to \mathrm{B}$ je bijekce. Je $F^{-1} \subseteq \mathrm{B} \times \mathrm{A}$. Nejdříve ukážeme, že F^{-1} je parciální funkce: Nechť $b \in \mathrm{B}$, a_1 , $a_2 \in \mathrm{A}$, $b F^{-1} a_1$, $b F^{-1} a_2$. Chceme: $a_1=a_2$. Víme, že $a_1 F b$, $a_2 F b$, tedy $F(a_1)=b$, $F(a_2)=b$, $F(a_1)=F(a_2)$. Protože F je injekce, nutně $a_1=a_2$.

Nyní ukážeme,že $Def\ F^{-1}=\mathrm{B}$.

$Def\ F^{-1} \subseteq \mathrm{B}$: To je zřejmé.

$\mathrm{B} \subseteq Def\ F^{-1}$: Buď $b \in \mathrm{B}$. Protože F je surjekce, existuje $a \in \mathrm{A}$ tak,že $F(a)=b$. Tudíž aFb , $b F^{-1} a$, $b \in Def\ F^{-1}$.

Již jsme dokázali, že $F^{-1}: \mathrm{B} \to \mathrm{A}$. Zbývá dokázat, že F^{-1} je bijekce.

F^{-1} je injekce:

Nechť b_1, $b_2 \in \mathrm{B}$, $F^{-1}(b_1)=F^{-1}(b_2)$. Chceme: $b_1=b_2$. Budiž $a \in \mathrm{A}$, $a=F^{-1}(b_1)=F^{-1}(b_2)$. Takže $b_1 F^{-1} a$, $b_2 F^{-1} a$, aFb_1 , aFb_2 . Jelikož F je funkce, dostáváme $b_1=b_2$.

F^{-1} je surjekce:

Nechť $a \in \mathrm{A}$. Hledáme $b \in \mathrm{B}$ tak, aby $F^{-1}(b)=a$. Hledáme tedy takové $b \in \mathrm{B}$, aby $b F^{-1} a$, čili aFb . Takové b existuje, neboť F je funkce a tudíž $Def\ F=\mathrm{A}$.

1.1.9 DEFINICE

Nechť A je množina. Funkce $id_{\mathrm{A}}: \mathrm{A} \to \mathrm{A}$ definovaná předpisem $id_{\mathrm{A}}(a)=a$ pro všechna $a \in \mathrm{A}$ se nazývá identita (identická funkce) na množině A .

1.1.10 TVRZENÍ

Nechť A , B jsou množiny, $F: \mathrm{A} \to \mathrm{B}$. Platí:

(a) Funkce id_{A} je bijekce
(b) $id_{\mathrm{A}} F = F\, id_{\mathrm{B}} = F$
(c) $FF^{-1}=id_{\mathrm{A}}$, $F^{-1} F = id_{\mathrm{B}}$ (za předpokladu, že F je bijekce.)

Důkaz: SAMI

1.2 Operace na množině

1.2.1 DEFINICE

Nechť A je množina. Zobrazení množiny $\mathrm{A} \times \mathrm{A}$ do množiny A se nazývá (binární) operace na množině A . Je-li $*$ operace na A , pak místo $*((x, y))$ píšeme $x * y$ (pro všechna $x, y \in \mathrm{A}$).

1.2.2 DEFINICE

Nechť $*$ a $\square$ jsou binární operace na množině A .

(a) Říkáme že operace $*$ je asociativní,pokud pro všechna x , y , $z \in \mathrm{A}$ platí:
$x*(y*z)=(x*y)*z$

(b) Říkáme, že operace $*$ je komutativní, pokud pro všechna $x, y \in A$ platí:
$x * y = y * x$
(c) Říkáme, že operace $\square$ je distributivní vzhledem k operaci $*$ pokud pro všechna $x, y, z \in A$ platí:
$x \square (y * z) = (x \square y) * (x \square z)$, $(y * z) \square x = (y \square x) * (z \square x)$.
(d) Nechť $e \in A$. Říkáme, že e je neutrální prvek operace $*$, pokud pro všechna $x \in A$ platí:
$e * x = x$, $x * e = x$.
(e) Nechť $e, x, y \in A$, e je neutrální prvek operace $*$. Říkáme, že prvek y je inverzní (inverze) k prvku x vzhledem k operaci $*$, pokud platí: $x * y = e$, $y * x = e$.

1.2.3 TVRZENÍ
(a) Každá operace má nejvýše jeden neutrální prvek.
(b) Pro každou asociativní operaci s neutrálním prvkem platí:
Ke každému prvku existuje nejvýše jeden prvek inverzní.
Důkaz:
(a) Nechť $*$ je operace na množině A. Nechť e_1, e_2 jsou neutrální prvky operace $*$.
Chceme: $e_1 = e_2$
Počítejme: $e_1 = e_1 * e_2 = e_2$ (první rovnost plyne z toho, že e_2 je neutrální, druhá rovnost plyne z toho, že e_1 je neutrální)
(b) Nechť $*$ je asociativní operace na množině A s neutrálním prvkem e. Nechť $x, y_1, y_2 \in A$, y_1 a y_2 jsou inverze k x. Chceme: $y_1 = y_2$. Počítejme:
$y_1 = y_1 * e = y_1 * (x * y_2) = (y_1 * x) * y_2 = e * y_2 = y_2$.

V případě binárních operací se velmi často používá multiplikativní nebo aditivní symbolika.

Multiplikativní symbolika:
Operace se značí $\cdot$ a nazývá se násobení. Neutrální prvek se značí 1 a nazývá se jednotkový prvek. Inverzní prvek k prvku x se značí x^{-1} nebo $\frac{1}{x}$.

Aditivní symbolika:
Používá se především pro komutativní operace. Operace se značí $+$ a nazývá se sčítání. Neutrální prvek se značí 0 a nazývá se nulový prvek. Inverzní prvek k prvku x se značí $-x$ a nazývá se opačný prvek k prvku x.

1.2.4 DEFINICE
Grupa je množina spolu s binární operací, jež je asociativní, má neutrální prvek a každý prvek má prvek inverzní.

1.2.5 TVRZENÍ
Nechť G je grupa, $x, y \in G$. Platí:
(a) $(x^{-1})^{-1} = x$
(b) $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$
(Použili jsme multiplikativní symboliku.)
Důkaz:
(a) SAMI
(b) Je třeba ukázat, že platí dvě rovnosti: $(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = 1$, $(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = 1$. Počítejme:
$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = x \cdot (y \cdot y^{-1}) \cdot x^{-1} = x \cdot 1 \cdot x^{-1} = x \cdot x^{-1} = 1$,
$(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = y^{-1} \cdot (x \cdot x^{-1}) \cdot y = y^{-1} \cdot 1 \cdot y = y^{-1} \cdot y = 1$.

1.2.6 DEFINICE
Okruh je množina spolu se dvěma binárními operacemi, většinou zvanými sčítání a násobení,

přičemž vzhledem ke sčítání se jedná o komutativní grupu a násobení je distributivní vzhledem ke sčítání. Okruh se nazývá asociativní (komutativní, s jednotkovým prvkem), pokud operace násobení je asociativní (komutativní, má neutrální prvek).

1.2.7 TVRZENÍ

Nechť R je okruh, $x, y \in R$. Platí:

(a) $x \cdot 0 = 0 \cdot x = 0$

(b) $x \cdot (-y) = (-x) \cdot y = -(x \cdot y)$

(c) $(-x) \cdot (-y) = x \cdot y$

Důkaz: $x \cdot 0 = x \cdot (0+0) = x \cdot 0 + x \cdot 0$

$x \cdot 0 + (-x \cdot 0) = (x \cdot 0 + x \cdot 0) + (-x \cdot 0)$

$0 = x \cdot 0 + (x \cdot 0 + (-x \cdot 0))$

$0 = x \cdot 0 + 0$

$0 = x \cdot 0$

Obdobně se dokáže, že $0 \cdot x = 0$.

(b) $x \cdot (-y) + x \cdot y = x \cdot ((-y) + y) = x \cdot 0 = 0$

Vidíme, že $x \cdot (-y)$ je prvek opačný k prvku $x \cdot y$, čili $x \cdot (-y) = -(x \cdot y)$. Obdobně se dokáže, že $(-x) \cdot y = -(x \cdot y)$.

(c) Využijeme již dokázanou část (b): $(-x) \cdot (-y) = -(-(x \cdot y)) = x \cdot y$.

1.2.8 DEFINICE

Obor integrity je asociativní a komutativní okruh, v němž pro každé dva prvky x, y platí: Jestliže $x \cdot y = 0$, pak $x = 0$ nebo $y = 0$.

1.2.9 DEFINICE

Těleso je aspoň dvouprvkový asociativní okruh s jednotkovým prvkem (označme jej 1), v němž pro každý nenulový prvek x existuje prvek y takový, že $x \cdot y = y \cdot x = 1$.

Prvek y se značí x^{-1} nebo $\frac{1}{x}$. Značení je možno zavést, neboť prvek y je určen jednoznačně (nechť $x \cdot z = z \cdot x = 1$; pak $y = y \cdot 1 = y \cdot (x \cdot z) = (y \cdot x) \cdot z = 1 \cdot z = z$).

Je-li v tělese násobení komutativní, pak hovoříme o komutativním tělese. Protože v tomto textu budeme pracovat výhradně s komutativními tělesy, budeme pro stručnost místo názvu komutativní těleso používat pouze slovo těleso.

1.2.10 TVRZENÍ

(a) Každé těleso je obor integrity

(b) Každý aspoň dvouprvkový konečný obor integrity s jednotkovým prvkem je těleso.

Důkaz:

(a) Nechť x, y jsou takové prvky tělesa, že $x \cdot y = 0$. Chceme: $x = 0$ nebo $y = 0$.

Rozlišme dva případy:

(I) $x = 0$

(II) $x \neq 0$

ad (I): Jsme hotovi.

ad (II): $x \cdot y = 0$

$x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0$

$(x^{-1} \cdot x) \cdot y = 0$

$1 \cdot y = 0$

$y = 0$

(b) Nechť obor integrity má n prvků x_1, x_2, …, x_n. Vezměme libovolný prvek x, $x \neq 0$. Hledáme y tak, aby $x \cdot y = 1$ (vztah $y \cdot x = 1$ ihned vyplyne z komutativity násobení). Ukážeme, že prvky $x \cdot x_1$, $x \cdot x_2$, …, $x \cdot x_n$ jsou navzájem různé. Pro důkaz sporem

předpokládejme, že $x\cdot x_i = x\cdot x_j$ pro nějaká i, $j\in\{1,2,3,\ldots,n\}$, $i\neq j$. Pak

$$x\cdot x_i+(-(x\cdot x_j))=x\cdot x_j+(-(x\cdot x_j))$$
$$x\cdot x_i+x\cdot(-x_j)=0$$
$$x\cdot(x_i+(-x_j))=0$$

Protože počítáme v oboru integrity a $x\neq 0$, nutně $x_i+(-x_j)=0$, takže $x_i=x_j$, spor. Víme tedy, že prvky $x\cdot x_1$, $x\cdot x_2$, … , $x\cdot x_n$ jsou navzájem různé. Protože je jich n, jedná se o všechny prvky oboru integrity a tedy $1=x\cdot x_k$ pro nějaké $k\in\{1,2,\ldots,n\}$. Stačí položit $y=x_k$.

Základními příklady těles jsou tělesa $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. *Všechna jsou nekonečná. Později uvedeme nekonečně mnoho příkladů konečných těles.*

1.2.11 DEFINICE

Nechť R je relace na množině A. Relace R se nazývá
reflexivní, pokud pro všechna $x\in\mathrm{A}$ platí xRx
tranzitivní, pokud pro všechna x, y, $z\in\mathrm{A}$ platí: jestliže xRy a yRz, pak xRz.
symetrická, pokud pro všechna x, $y\in\mathrm{A}$ platí: jestliže xRy, pak yRx.
antisymetrická, pokud pro všechna x, $y\in\mathrm{A}$ platí: jestliže xRy a yRx, pak $x=y$.

1.2.12 DEFINICE

Ekvivalence je relace (na nějaké množině), která je současně reflexivní, symetrická a tranzitivní.

1.2.13 DEFINICE

Nechť A je neprázdná množina. Rozklad množiny A je systém množin S splňující:
(a) Jestliže $\mathrm{B}\in S$, pak $\mathrm{B}\neq\emptyset$.
(b) Jestliže B, $\mathrm{C}\in S$, $\mathrm{B}\neq\mathrm{C}$, pak $\mathrm{B}\cap\mathrm{C}=\emptyset$.
(c) $\bigcup_{\mathrm{B}\in S}\mathrm{B}=\mathrm{A}$

Všimněme si, že z podmínky (c) v definici 1.2.13. ihned plyne: jestliže $\mathrm{B}\in S$, pak $\mathrm{B}\subseteq\mathrm{A}$.

1.2.14 TVRZENÍ

Nechť $\sim$ je ekvivalence na neprázdné množině A. Položme pro libovolné $a\in\mathrm{A}$, $\bar{a}=\{x\in\mathrm{A}\,|\,x\sim a\}$.
Nechť $S=\{\bar{a}\,|\,a\in A\}$. Pak S je rozklad množiny A.
Důkaz
(a) Relace $\sim$ je reflexivní. Tudíž $a\sim a$, $a\in\bar{a}$, $\bar{a}\neq 0$.
(b) Nechť a, $b\in\mathrm{A}$, $\bar{a}\neq\bar{b}$. Chceme: $\bar{a}\cap\bar{b}=\emptyset$.
Předpokládejme opak, tj. $\bar{a}\cap\bar{b}\neq\emptyset$. Buď $x\in\bar{a}\cap\bar{b}$. Pak $x\sim a$, $x\sim b$. Ukážeme, že $\bar{a}\subseteq\bar{b}$. Buď $y\in\bar{a}$. Je $y\sim a$. Z $x\sim a$ plyne $a\sim x$, protože relace $\sim$ symetrická. Z $y\sim a$, $a\sim x$ plyne $y\sim x$ ($\sim$ je tranzitivní relace). Z $y\sim x$, $x\sim b$ dostáváme $y\sim b$. Tudíž $y\in\bar{b}$. Obdobně lze ukázat, že $\bar{b}\subseteq\bar{a}$. Takže celkem $\bar{a}=\bar{b}$. to je však spor. Nutně tedy $\bar{a}\cap\bar{b}=\emptyset$.
(c) $\bigcup_{a\in\mathrm{A}}\bar{a}\subseteq\mathrm{A}$: To je jasné, protože $\bar{a}\subseteq\mathrm{A}$. $\mathrm{A}\subseteq\bigcup_{a\in\mathrm{A}}\bar{a}$: Stačí uvědomit, že pro každé $a\in\mathrm{A}$ je $a\in\bar{a}$.
Rozklad S, sestrojený ve tvrzení 1.2.14., se značí $A/\sim$ a nazývá se faktorová množina množiny A podle ekvivalence $\sim$.

1.2.15 TVRZENÍ

Nechť $\sim$ je ekvivalence na neprázdné množině A. Pro libovolné prvky a, $b\in\mathrm{A}$ platí: $\bar{a}=\bar{b}$ právě tehdy, když $a\sim b$.
Důkaz:
(I) Nechť $\bar{a}=\bar{b}$. Jelikož $a\in\bar{a}$, máme $a\in\bar{b}$ a tedy $a\sim b$.

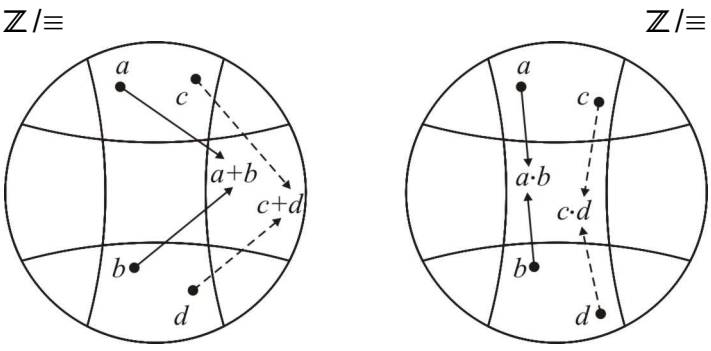
(II) Nechť $a \sim b$.
$\bar{a} \subseteq \bar{b}$: Buď $x \in \bar{a}$. Je $x \sim a$. Protože $\sim$ je tranzitivní, dostáváme $x \sim b$, $x \in \bar{b}$.
$\bar{b} \subseteq \bar{a}$: Obdobně.
Celkem jsme dostali fakt $\bar{a} = \bar{b}$.

1.2.16 DEFINICE
Nechť a, b, m jsou celá čísla, $m > 0$. Říkáme, že a je kongruentní s b modulo m, pokud m dělí $b - a$. Tento vztah zapisujeme $a \equiv b\,(m)$. Bude-li z kontextu jasné, o jaké m se jedná, můžeme psát pouze $a \equiv b$.

1.2.17 TVRZENÍ
$\equiv$ je relace ekvivalence na množině $\mathbb{Z}$.
Důkaz:
(a) $\equiv$ je reflexivní: $m \mid 0 = a - a$, takže $a \equiv a$.
(b) $\equiv$ je symetrická: Nechť $a \equiv b$. Chceme: $b \equiv a$. Víme, že $m \mid b - a$. Existuje tedy $c \in \mathbb{Z}$, $b - a = c \cdot m$. Pak $a - b = (-c) \cdot m$, $m \mid a - b$, $b \equiv a$.
(c) $\equiv$ je tranzitivní: Nechť $a \equiv b$, $b \equiv c$. Chceme: $a \equiv c$. Víme, že $m \mid b - a$, $m \mid c - b$.
Existuje tedy d, $e \in \mathbb{Z}$, $b - a = d \cdot m$, $c - b = e \cdot m$. Pak
$c - a = (c - b) + (b - a) = e \cdot m + d \cdot m = (e + d) \cdot m$, $m \mid c - a$, $a \equiv c$.

Faktorovou množinu $\mathbb{Z} / \equiv$ budeme značit $\mathbb{Z}_m$.

1.2.18 TVRZENÍ
Množina $\mathbb{Z}_m$ má přesně m prvků, totiž $\bar{0}$, $\bar{1}$, …, $\overline{m-1}$.
Důkaz: Je třeba dokázat dvě záležitosti:
(I) $\{\bar{0}, \bar{1}, \ldots, \overline{m-1}\} = \mathbb{Z}_m$
(II) $\bar{0}$, $\bar{1}$, …, $\overline{m-1}$ jsou navzájem různé.
ad (I): $\{\bar{0}, \bar{1}, \ldots, \overline{m-1}\} \subseteq \mathbb{Z}_m$: To je zřejmé.
$\mathbb{Z}_m \subseteq \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$: Nechť $a \in \mathbb{Z}$. Chceme: $a \in \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$. Vydělme číslo a se zbytkem číslem m: $a = q \cdot m + r$ pro jistá q, $r \in \mathbb{Z}$, $0 \le r < m$. Pak ovšem $a - r = q \cdot m$, $m \mid a - r$, $r \equiv a$, $\bar{r} = \bar{a}$, $\bar{a} \in \{\bar{0}, \bar{1}, \ldots, \overline{m-1}\}$
ad (II): Nechť a, $b \in \mathbb{Z}$, $0 \le a < b \le m - 1$. Chceme: $\bar{a} \ne \bar{b}$. Pro důkaz sporem předpokládejme, že $\bar{a} = \bar{b}$. Pak $a \equiv b$, $m \mid b - a$, $b - a = c \cdot m$ pro jisté $c \in \mathbb{Z}$, $c > 0$ (uvědomme si, že $b - a > 0$, $m > 0$). Ovšem $b - a \le (m-1) - 0 = m - 1$ takže $m \le c \cdot m = b - a \le m - 1$, spor.
Na množině $\mathbb{Z}_m$ přirozeným způsobem zavedeme operace sčítání a násobení. Nechť a, $b \in \mathbb{Z}$. Klademe $\bar{a} + \bar{b} = \overline{a+b}$, $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$
Nechť c, $d \in \mathbb{Z}$, $\bar{c} = \bar{a}$, $\bar{d} = \bar{b}$. Aby výše zavedené operace sčítání a násobení v $\mathbb{Z}_m$ byly definovány korektně, musí platit $\overline{a+b} = \overline{c+d}$, $\overline{a \cdot b} = \overline{c \cdot d}$.



1.2.19 TVRZENÍ

Nechť a, b, c, $d\in\mathbb{Z}$. Jestliže $a\equiv c$, $b\equiv d$, pak $a+b\equiv c+d$, $a\cdot b\equiv c\cdot d$.

Důkaz:Nechť $a\equiv c$, $b\equiv d$. Existuje tedy p, $q\in\mathbb{Z}$, $c-a=p\cdot m$, $d-b=q\cdot m$.

$c-a=p\cdot m$

$d-b=q\cdot m$

$(c+d)-(a+b)=(p+q)\cdot m$

Vidíme,že $m|(c+d)-(a+b)$, tedy $a+b\equiv c+d$. Dále,

$c\cdot d-a\cdot b=c\cdot d-c\cdot b+c\cdot b-a\cdot b=c\cdot(d-b)+(c-a)\cdot b=c\cdot q\cdot m+p\cdot m\cdot b=(c\cdot q+p\cdot b)\cdot m$. Čili

$m|c\cdot d-a\cdot b$, $a\cdot b\equiv c\cdot d$.

1.2.20 TVRZENÍ

Nechť na $\mathbb{Z}_m$ definujeme sčítání a násobení takto: $\bar{a}+\bar{b}=\overline{a+b}$, $\bar{a}\cdot\bar{b}=\overline{a\cdot b}$ (a, $b\in\mathbb{Z}$). Pak $\mathbb{Z}_m$ je komutativní asociativní okruh s jednotkovým prvkem $\bar{1}$.

Důkaz: (I) $\mathbb{Z}_m$ s operací $+$ je komutativní grupa s nulovým prvkem $\bar{0}$:

Operace $+$ je asociativní:

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

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

Operace $+$ je komutativní:

$\bar{a}+\bar{b}=\overline{a+b}=\overline{b+a}=\bar{b}+\bar{a}$.

$\bar{0}$ je nulový prvek:

$\bar{a}+\bar{0}=\overline{a+0}=\bar{a}$

Existence opačných prvků:

$\bar{a}+\overline{(-a)}=\overline{a+(-a)}=\bar{0}$

(všimněme si, že $-\bar{a}=\overline{-a}$)

(II) Operace $\cdot$ komutativní, asociativní, $\bar{1}$ je jednotkový prvek: Postupuje se obdobně jako v části (I).

(III) Operace $\cdot$ je distributivní vzhledem k operaci $+$:

$\bar{a}\cdot(\bar{b}+\bar{c})=\bar{a}\cdot\overline{b+c}=\overline{a\cdot(b+c)}=\overline{a\cdot b+a\cdot c}$, $\bar{a}\cdot\bar{b}+\bar{a}\cdot\bar{c}=\overline{a\cdot b}+\overline{a\cdot c}=\overline{a\cdot b+a\cdot c}$.

1.2.21 TVRZENÍ

Nechť m je celé číslo, $m>1$. Platí: $\mathbb{Z}_m$ je těleso právě tehdy, když m je prvočíslo.

Důkaz:

$\Rightarrow$: Nechť d je celé číslo, $d>0$, $d|m$. Chceme: $d=1$ nebo $d=m$.

$m=d\cdot e$ pro nějaké $e\in\mathbb{Z}$, $e>0$.

Zřejmě $0\equiv m(m)$. Takže $\bar{0}=\bar{m}=\overline{d\cdot e}=\bar{d}\cdot\bar{e}$. Protože $\mathbb{Z}_m$ je těleso, je $\mathbb{Z}_m$ obor integrity (viz 1.2.10.) a $\bar{d}=\bar{0}$ nebo $\bar{e}=\bar{0}$.

Nechť $\bar{d}=\bar{0}$. Pak $d\equiv 0(m)$, $m|d$. Protože $d|m$, je $d=m$.

Nechť $\bar{e}=\bar{0}$. Pak $e=m$, $d=1$.

$\Leftarrow$: $\mathbb{Z}_m$ je komutativní asociativní okruh s jednotkovým prvkem (1.2.20). Jelikož $\mathbb{Z}_m$ má m prvků (1.2.18.), je okruh $\mathbb{Z}_m$ aspoň dvouprvkový. S ohledem na 1.2.10. zbývá dokázat: Jestliže $\bar{a}\cdot\bar{b}=\bar{0}$, pak $\bar{a}=\bar{0}$ nebo $\bar{b}=\bar{0}$. Počítejme: $\bar{0}=\bar{a}\cdot\bar{b}=\overline{a\cdot b}$, $0\equiv a\cdot b(m)$, $m|a\cdot b$. Jelikož m je prvočíslo, $m|a$ nebo $m|b$. V případě $m|a$ máme $a\equiv 0(m)$, $\bar{a}=\bar{0}$. V případě $m|b$ máme $\bar{b}=\bar{0}$.

Pro ilustraci uvedeme tabulky operací sčítání a násobení v okruzích $\mathbb{Z}_5$ a $\mathbb{Z}_6$.

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

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

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

$\mathbb{Z}_5$ je těleso (viz 1.2.21.); $\mathbb{Z}_6$ je komutativní asociativní okruh s jednotkovým prvkem $\bar{1}$ (1.2.20.), avšak není to obor integrity, neboť například $\bar{3}\cdot\bar{4}=\bar{0}$.

1.3. Uspořádání

1.3.1 DEFINICE

Uspořádání je relace (na nějaké množině), která je reflexivní, antisymetrická a tranzitivní. Množina, na níž je definováno uspořádání se nazývá uspořádaná. Uspořádání budeme většinou označovat symbolem $\leq$. Je-li $a\leq b$, budeme říkat, že a je menší nebo rovno b. Je-li $a\leq b$ a $a\neq b$, píšeme $a<b$ a říkáme, že a je menší než b. Relace inverzní k $\leq$ a $<$ budeme označovat symboly $\geq$ a $>$. Je-li $a\leq b$ nebo $b\leq a$, pak prvky a, b jsou porovnatelné. Pokud neplatí ani $a\leq b$, ani $b\leq a$, prvky a, b jsou neporovnatelné.

1.3.2 DEFINICE

Nechť A je uspořádaná množina, $x\in A$. Prvek x se nazývá minimální prvek množiny A, pokud neexistuje žádné $y\in A$ splňující podmínku $y<x$. Jinými slovy, pokud pro všechna $y\in A$ platí: jestliže $y\leq x$, pak $y=x$. Obdobně se zavádí pojem maximální prvek množiny A.

1.3.3 DEFINICE

Nechť A je uspořádaná množina, $B\subseteq A$, $x\in A$. Prvek x se nazývá horní hranice (horní odhad, horní mez) podmnožiny B v množině A, pokud pro každé $y\in B$ je $y\leq x$. Podmnožina B se nazývá shora omezená, existuje-li v množině A aspoň jedna horní hranice množiny B. Obdobně se zavádějí pojmy dolní hranice podmnožiny a podmnožina zdola omezená. Je-li podmnožina zdola omezená a současně shora omezená, pak se nazývá omezená.

1.3.4 DEFINICE

Nechť A je uspořádaná množina, $B\subseteq A$. Podmnožina B se nazývá řetězec, pokud pro každá x, $y\in B$ je $x\leq y$ nebo $y\leq x$ (každé dva prvky z B jsou porovnatelné). Řetězec B se nazývá maximální, jestliže neexistuje žádný řetězec $C\subseteq A$ splňující $B\subset C$ (tj. $B\subseteq C$, $B\neq C$).

1.3.5 DEFINICE

Uspořádaná množina, v níž každá neprázdná podmnožina má nejmenší prvek se nazývá dobře uspořádaná množina.

Připomeňme že množina $\mathcal{P}(A)$, která sestává ze všech podmnožin množiny A, tedy $\mathcal{P}(A)=\{X|X\subseteq A\}$, se nazývá potence množiny A.

1.3.6 DEFINICE

Funkce φ, definovaná na množině $\mathcal{P}(A)$, pro kterou platí $(X\in\mathcal{P}(A)\wedge X\neq\emptyset)\Rightarrow\varphi(X)\in X$, se nazývá selektor na množině $\mathcal{P}(A)$.

Je-li množina A konečná, pak lze (aspoň teoreticky) sestrojit selektor na množině $\mathcal{P}(A)$. Nechť například $A=\{a, b, c\}$. Pak $\mathcal{P}(A)=\{\emptyset,\{a\},\{b\},\{c\},\{a, b\},\{a, c\},\{b, c\},\{a, b, c\}\}$

X	$\varphi(X)$
$\emptyset$	Na této hodnotě nezáleží
$\{a\}$	1 možnost: a
$\{b\}$	1 možnost: b
$\{c\}$	1 možnost: c
$\{a, b\}$	2 možnosti: a, b
$\{a, c\}$	2 možnosti: a, c
$\{b, c\}$	2 možnosti: b, c
$\{a, b, c\}$	3 možnosti: a, b, c

Pokud odhlédneme od hodnoty $\varphi(\emptyset)$, existuje celkem $1\cdot1\cdot1\cdot2\cdot2\cdot2\cdot3=24$ selektorů na množině $\mathcal{P}(A)$.
Problém je s existencí selektorů na $\mathcal{P}(A)$, je-li množina A nekonečná. Tento problém obejdeme přijetím následujícího axiomu.

1.3.7 AXIOM VÝBĚRU
Na každé potenční množině existuje selektor.

1.3.8 ZERMELOVA VĚTA
Každou množinu lze dobře uspořádat.

1.3.9 HAUSDORFFOVA VĚTA
Každý řetězec uspořádané množiny je obsažen v některém maximálním řetězci.

1.3.10 VĚTA KURATOWSKÉHO – ZORNOVA
Je-li každý řetězec uspořádané množiny shora omezený, je každý prvek menší nebo roven některému maximálnímu prvku.

1.3.11 TVRZENÍ
Zermelova věta, Hausdorffova věta, a věta Kuratowského - Zornova jsou ekvivalentní s axiomem výběru.
Důkaz:
(I) Z axiomu výběru plyne Zermelova věta.
Viz A. G. KUROŠ, Kapitoly z obecné algebry, Academia, Praha, 1977, strany 23-24.
(II) Z Zermelovy věty plyne Hausdorffova věta.
Viz A. G. KUROŠ, Kapitoly z obecné algebry, Academia, Praha, 1977, strany 24-25.
(III) Z Hausdorffovy věty plyne věta Kuratowského – Zornova.
Nechť M je uspořádaná množina, $a\in M$. Hledáme prvek $b\in M$ splňující dvě podmínky: $(\alpha)\ a\le b$, (β) b je maximální
Uvažme řetězec $A=\{a\}$. Dle Hausdorffovy věty existuje maximální řetězec C takový, že $A\subseteq C$. Každý řetězec uspořádané množiny M je shora omezený. Existuje tedy prvek $b\in M$, jenž je horní hranicí řetězce C. Ukážeme, že b splňuje podmínky (α) a (β)
ad (α): Jelikož b je horní hranicí množiny C, je $x\le b$ pro každé $x\in C$. Ovšem $a\in A\subseteq C$, takže $a\in C$, $a\le b$
ad (β): Předpokládejme, že prvek b maximální není. Existuje tedy $d\in M$, $b<d$. Uvažme množinu $D=C\cup\{d\}$. Množina D je řetězec: Zvolme libovolně x, $y\in D$. Chceme: $x\le y$ nebo $y\le x$.
Rozlišíme 4 případy:
(1) x, $y\in C$
(2) $x\in C$, $y=d$

(3) $y \in C$, $x = d$
(4) $x = y = d$.
ad (1): Jelikož C je řetězec, máme $x \leq y$ nebo $y \leq x$.
ad (2): b je horní hranicí množiny C , takže $x \leq b$. Také $b < d = y$, takže $x \leq y$.
ad (3): Obdobně jak v případě (2) se dokáže, že $y \leq x$.
ad (4): Protože $x = y$, nutně $x \leq y$.
Dále vidíme, že $d \notin \mathrm{C}$. Kdyby totiž platilo $d \in \mathrm{C}$, bylo by $d \leq b$ (b je horní hranicí množiny C) a tedy $b = d$ (víme totiž, že $b \leq d$). To by však byl spor s faktem $b < d$.
Protože $d \notin \mathrm{C}$, je $C \subset \mathrm{D}$. Avšak D je řetězec, spor (předpokládali jsme, že C je maximální řetězec). Nutně tudíž prvek b je maximální.
(IV) Z věty Kuratowského – Zornovy plyne axiom výběru:
Viz A. G. KUROŠ, Kapitoly z obecné algebry, Academia, Praha, 1977, strana 25.

1.3.12 POZNÁMKA
Je snadné dokázat, že z Zermelovy věty plyne axiom výběru. Předpokládejme platnost Zermelovy věty. Ukážeme, že platí axiom výběru. Nechť A je libovolná množina. Je třeba sestrojit selektor φ na množině $\mathcal{P}(\mathrm{A})$. Definujeme funkci φ takto: Nechť $\mathrm{B} \in \mathcal{P}(\mathrm{A})$. Pak

$\varphi(\mathrm{B}) =$
(I) COKOLI pokud $\mathrm{B} = \emptyset$
(II) nejmenší prvek množiny B pokud $\mathrm{B} \neq \emptyset$