Pavel Horák

ZÁKLADY MATEMATIKY

UČEBNÍ TEXT

Podzimní semestr 2006

Ú V O D

Tento učební text je určen pro předmět M1125 Základy matematiky, který je povinným předmětem v bakalářském studijním programu Matematika, studijních oborech Matematika se zaměřením na vzdělávání a Matematika pro víceoborové studium na přírodovědecké fakultě Masarykovy Univerzity v Brně. Jedná se o úvodní jednosemestrální kurz, který je doporučen absolvovat v 1. semestru studia.

Předmět Základy matematiky je ve výše uvedených studijních oborech úvodním matematickým kurzem, jehož cílem je zopakovat a rozšířit středoškolskou látku z matematiky a následně probrat některá další témata, zejména algebraického charakteru. Dalším cílem kurzu je pokud možno "srovnat" matematické znalosti studentů, kteří přicházejí z různých středních škol, mnohdy s různou úrovní a intenzitou výuky matematiky. Z tohoto důvodu je výklad orientován spíše na studenty s chatrnějšími matematickými znalostmi. Ovšem i u těchto studentů se předpokládá, že vlastní pílí svoje případné nedostatky ve středoškolských znalostech matematiky zacelí. Přehled středoškolského učiva z matematiky je možno nalézt například v publikaci "Odmaturuj z matematiky", autorů P. Čermáka a P. Červinkové, kterou vydalo nakladatelství Didaktis (druhé, opravené vydání v roce 2003). Tuto nebo podobnou knížku by si měli pořídit všichni studenti, kteří cítí, že v jejich středoškolských matematických znalostech jsou mezery.

Učební text předpokládá pouze elementární znalosti základních matematických pojmů a jejich vlastností, vyučovaných na každé střední škole. V textu je užívána běžná symbolika známá ze střední školy. Nově zaváděná označení jsou v textu vždy řádně vysvětlena. Vzhledem k tomu, že pro mnohé čtenáře může být tento text prvním matematickým textem, kterým se budou opravdu vážně zabývat, je výklad veden co možná nejpodrobnější a nejelementárnější formou. Téměř všechna tvrzení jsou podrobně dokazována s cílem, aby si čtenář dobře osvojil základní matematické postupy a dovednosti, které bude následně během dalšího studia mnohokrát používat. Konec důkazu je v textu opticky označen symbolem ■, umístěným na konci řádku.

Pro označování základních číselných množin jsou v textu použity následující standardní symboly:

$\mathbb{N}$ ... množina všech přirozených čísel

$\mathbb{Z}$ ... množina všech celých čísel

$\mathbb{Q}$ ... množina všech racionálních čísel

$\mathbb{R}$ ... množina všech reálných čísel

$\mathbb{C}$ ... množina všech komplexních čísel.

I. OPAKOVÁNÍ A DOPLNĚNÍ STŘEDOŠKOLSKÉ LÁTKY

1. Základní logické pojmy.

V matematice se zabýváme studiem vlastností různých objektů a vztahů mezi nimi. K označování matematických objektů užíváme různých symbolů. Některé z nich mají pevný význam a nazýváme je **konstanty** (například symboly 1, π, $\sqrt{2}$, atd.). Jiné symboly takový přesně stanovený význam nemají, ale můžeme za ně konstanty vhodným způsobem dosazovat a nazýváme je **proměnné**. U proměnných musí být vždy vymezeny ty objekty, které je možno za proměnné dosazovat (například *"přirozené číslo x"*, *"přímka p"*, atd.).

Výrok je sdělení, o němž má smysl říci, že je pravdivé nebo nepravdivé. Hovoříme pak o pravdivém výroku nebo nepravdivém výroku. Například sdělení *"Praha má více než tisíc obyvatel"* je pravdivým výrokem, zatímco sdělení *"Číslo sedm je sudé"* je nepravdivým výrokem. Může se také stát, že dané sdělení je výrokem, o němž však momentálně neumíme rozhodnout, zdali pravdivým či nepravdivým. Takovým je například výrok *"Mimo naši sluneční soustavu žijí myslící bytosti"*.

Každému výroku V se přiřazuje jeho **pravdivostní hodnota** $p(V)$ takto: je-li výrok V pravdivý, klademe $p(V) = 1$ a je-li výrok V nepravdivý, klademe $p(V) = 0$

Logické spojky nám umožňují z jednotlivých výroků tvořit další výroky. Nejběžněji se používají následující logické spojky, které mají své ustálené názvy i označení, jak je uvedeno v následující tabulce (kde A, B značí libovolné výroky).

Název logické spojky	Označení	Slovní vyjádření
negace	$\neg A$	není pravda, že A
konjunkce	$A \wedge B$	A a (současně) B
disjunkce	$A \vee B$	A nebo B
implikace	$A \Rightarrow B$	jestliže A, pak B
ekvivalence	$A \Leftrightarrow B$	A právě když B.

Každou z uvedených logických spojek popíšeme nyní tak, že uvedeme, jaké pravdivostní hodnoty přiřazujeme výroku, utvořenému s její pomocí (v závislosti na pravdivostních hodnotách výchozích výroků A, B). Vznikne tak tzv. **tabulka pravdivostních hodnot**, která má pro negaci dva řádky a pro ostatní uvedené logické spojky čtyři řádky.

$p(A)$	$p(\neg A)$
1	0
0	1

$p(A)$	$p(B)$	$p(A \wedge B)$	$p(A \vee B)$	$p(A \Rightarrow B)$	$p(A \Leftrightarrow B)$
1	1	1	1	1	1
1	0	0	1	0	0
0	1	0	1	1	0
0	0	0	0	1	1

Rozeberme si nyní podrobněji jednotlivé logické spojky.

Negace libovolného výroku A se dá bez problémů správně vytvořit obratem *"není pravda, že A"*. Tato formulace bývá však často jazykově poněkud kostrbatá, a proto se snažíme i v matematice tvořit negace bez užití tohoto obratu. Například místo *"není pravda, že číslo 7 je dělitelné třemi"* řekneme raději *"číslo 7 není dělitelné třemi"*.

Konjunkce výroků působí obvykle nejméně potíží. Z tabulky vidíme, že výrok $A \wedge B$ je pravdivý jedině v případě, že oba výroky A, B jsou pravdivé.

Disjunkce $A \vee B$ je pravdivá, je-li pravdivý alespoň jeden z výroků A, B (to jest jeden, druhý nebo oba dva). Zde tedy při použití spojky *"nebo"* dochází někdy k odchylce od běžné hovorové řeči, v níž se spojka *"nebo"* velmi často používá ve smyslu vylučovacím (*"Budu doma nebo ve škole"*).

Implikace $A \Rightarrow B$ je nepravdivá pouze v případě, když výrok A je pravdivý a výrok B je nepravdivý. Ve všech ostatních případech je implikace pravdivá. Je nutné si zejména dobře uvědomit, že implikace $A \Rightarrow B$ je vždy pravdivá v případě, když výrok A je nepravdivý (a to bez ohledu na pravdivostní hodnotu výroku B).

Je-li implikace $A \Rightarrow B$ pravdivá, pak říkáme též, že A je **dostatečná podmínka** pro B a dále říkáme, že B je **nutná podmínka** pro A.

Ekvivalence $A \Leftrightarrow B$ je pravdivá právě v případě, že oba výroky A, B mají stejnou pravdivostní hodnotu, tzn. jsou oba současně pravdivé nebo současně nepravdivé. Výroky A, B se pak též nazývají **ekvivalentní výroky**.

$\star \qquad \star \qquad \star$

V matematických úvahách můžeme tedy daný výrok nahradit jiným výrokem, který je s ním ekvivalentní. Velmi často se jedná o negaci konjunkce dvou výroků a negaci disjunkce dvou výroků, pro které platí:

$$(\neg(A \wedge B)) \qquad \text{je ekvivalentní s} \qquad ((\neg A) \vee (\neg B))$$

$$(\neg(A \vee B)) \qquad \text{je ekvivalentní s} \qquad ((\neg A) \wedge (\neg B)).$$

O tom, že dané výroky jsou skutečně ekvivalentní, se můžeme přesvědčit pomocí tabulky pravdivostních hodnot těchto výroků. Utvořme takovou tabulku pro první z uvedených vztahů.

$p(A)$	$p(B)$	$p(A \wedge B)$	$p(\neg(A \wedge B))$	$p(\neg A)$	$p(\neg B))$	$p(\neg A \vee \neg B)$
1	1	1	**0**	0	0	**0**
1	0	0	**1**	0	1	**1**
0	1	0	**1**	1	0	**1**
0	0	0	**1**	1	1	**1**

Pro druhý vztah se odpovídající tabulka pravdivostních hodnot vytvoří analogicky (udělejte si sami!).

Podobným způsobem lze ukázat, že ekvivalenci dvou výroků je možno vyjádřit pomocí konjunkce obou implikací těchto výroků, tzn.

$$(A \Leftrightarrow B) \qquad \text{je ekvivalentní s} \qquad ((A \Rightarrow B) \wedge (B \Rightarrow A))$$

což je možno opět ověřit pomocí příslušné tabulky pravdivostních hodnot.

Další důležitý vztah, který budeme v dalším velmi často využívat se týká implikací. Platí totiž:

$$(A \Rightarrow B) \qquad \text{je ekvivalentní s} \qquad ((\neg B) \Rightarrow (\neg A))$$

tzn. implikace $A \Rightarrow B$ je z logického hlediska totéž co implikace $\neg B \Rightarrow \neg A$. Pravdivost tohoto tvrzení okamžitě vyplývá z níže uvedené tabulky. Poznamenejme ještě, že implikaci $\neg B \Rightarrow \neg A$ se říká **obměna implikace** $A \Rightarrow B$.

$p(A)$	$p(B)$	$p(A \Rightarrow B)$	$p(\neg B)$	$p(\neg A))$	$p(\neg B \Rightarrow \neg A)$
1	1	**1**	0	0	**1**
1	0	**0**	1	0	**0**
0	1	**1**	0	1	**1**
0	0	**1**	1	1	**1**

Podobným způsobem se dá odvodit ekvivalentnost celé řady výroků složených ze tří výroků A, B, C. Pro ilustraci uveďme dvě dvojice ekvivalentních výroků, s nimiž se při logických úvahách poměrně často setkáváme. Platí:

$$((A \wedge (B \vee C))) \qquad \text{je ekvivalentní s} \qquad ((A \wedge B) \vee (A \wedge C)))$$

$$((A \vee (B \wedge C))) \qquad \text{je ekvivalentní s} \qquad ((A \vee B) \wedge (A \vee C))) \,.$$

Ekvivalentnost uvedených dvojic výroků se dokáže stejným způsobem, jako dříve, tzn. pomocí tabulky pravdivostních hodnot, která v tomto případě bude mít osm řádků. Sestavíme tuto tabulku tentokrát pro druhou dvojici výroků. Pro první dvojici se sestaví analogicky (proveďte si sami!).

$p(A)$	$p(B)$	$p(C)$	$p(B \wedge C)$	$p(A \vee (B \wedge C))$	$p(A \vee B)$	$p(A \vee C)$	$p((A \vee B) \wedge (A \vee C))$
1	1	1	1	**1**	1	1	**1**
1	1	0	0	**1**	1	1	**1**
1	0	1	0	**1**	1	1	**1**
1	0	0	0	**1**	1	1	**1**
0	1	1	1	**1**	1	1	**1**
0	1	0	0	**0**	1	0	**0**
0	0	1	0	**0**	0	1	**0**
0	0	0	0	**0**	0	0	**0**

$\star \qquad \star \qquad \star$

Všimněme si, že sdělení obsahující nějakou proměnnou, například *"celé číslo x je větší než 5"*, není výrokem. Z tohoto sdělení se stane výrok (ať už pravdivý, či nepravdivý) teprve tehdy, až za proměnnou x dosadíme nějakou konstantu z příslušné

množiny, z níž můžeme konstanty volit, v našem případě tedy nějaké konkrétní celé číslo. Přitom je zřejmé, že takovéto sdělení může obsahovat případně i více proměnných, například: *"reálné číslo x je menší než reálné číslo y"* obsahuje dvě proměnné x, y.

Sdělení obsahující proměnné, z něhož se stane výrok teprve po dosazení (přípustných) konstant za příslušné proměnné, se nazývá **výroková funkce**.

Z výrokové funkce můžeme tedy utvořit výrok tím, že za všechny proměnné dosadíme (přípustné) konstanty. Další možností, jak z výrokové funkce utvoříme výrok je tzv. **kvantifikace proměnných**. Ta spočívá v tom, že nějakým způsobem udáme počet objektů, pro něž z výrokové funkce obdržíme výrok. Ta část výroku, v níž je tento počet udáván, se nazývá **kvantifikátor**. Příkladem kvantifikátorů jsou obraty: *"každý", "nejvýše jeden", "alespoň jeden", "právě jeden", "právě čtyři", "nekonečně mnoho", "konečně mnoho"*, atd.

Konkrétně, z výše uvedené výrokové funkce *"celé číslo x je větší než 5"* je možno například utvořit následující kvantifikované výroky:

"alespoň jedno celé číslo je větší než 5"	(pravdivý výrok)
"nejvýše jedno celé číslo je větší než 5"	(nepravdivý výrok)
"každé celé číslo je větší než 5"	(nepravdivý výrok).

Poznamenejme ještě, že některé kvantifikátory můžeme vyjádřit několika různými slovními obraty se stejným významem. Například místo *"alespoň jeden"* můžeme stejně dobře říci *"existuje"* či *"jeden nebo více"*. Podobně místo *"nejvýše jeden"* můžeme říci *"žádný nebo jeden"*. V každém případě si při použití jakéhokoliv kvantifikátoru musíme vždy velmi dobře rozmyslet přesný význam toho, co říkáme.

Nejčastěji používané kvantifikátory mají svá označení. Kvantifikátor *"každý"* se též nazývá **obecný kvantifikátor** a označuje symbolem $\forall$. Podobně, kvantifikátor *"existuje"* se nazývá **existenční kvantifikátor** a označuje symbolem $\exists$.

V matematických úvahách je třeba velmi často provádět negace kvantifikovaných výroků. Obvykle nepoužíváme matematicky "bezpečného", ale gramaticky nepěkného obratu *"není pravda, že ..."*. Ukažme si nyní schematicky princip tvoření negací výroků s obecnými a existenčními kvantifikátory, což jsou případy, s nimiž se v praxi nejčastěji setkáváme:

výrok s obecným kvantifikátorem:	*"pro každý prvek z oboru U platí V"*
negace tohoto výroku:	*"existuje prvek z oboru U, pro který neplatí V"*
výrok s existenčním kvantifikátorem:	*"existuje prvek z oboru U, pro který platí V"*
negace tohoto výroku:	*"pro každý prvek z oboru U neplatí V"*

přičemž v posledním případě je samozřejmě vhodné slovo *"každý"* nahradit gramaticky správnějším slovem *"žádný"*. K tomu ještě poznamenejme, že při tvoření kvantifikovaných výroků a jejich negací můžeme samozřejmě užít i jiných gramatických obratů, které však musí zachovávat daný smysl. Ukažme si to na následujícím příkladu.

Kvantifikovaný výrok: *"každé nové auto je červené"* můžeme přeformulovat například do tvaru *"všechna nová auta jsou červená"*. Negací tohoto kvantifikovaného

výroku pak bude výrok *"existuje nové auto, které není červené"*, který můžeme případně přeformulovat do tvaru *"alespoň jedno nové auto není červené"*.

⋆ ⋆ ⋆

Na závěr této kapitoly si ještě stručně všimneme struktury matematických tvrzení a jejich důkazů. Této problematice je nutné důkladně porozumět a při dalším studiu tohoto textu se k ní stále vracet.

Matematická tvrzení, kterým se také říká "věty", mají nejčastěji tvar implikace výroků nebo ekvivalence výroků. Rozeberme si oba případy a ukažme, jak se taková tvrzení obvykle dokazují.

Matematická věta tvaru implikace má tvar $P \Rightarrow T$, přičemž výrok P se nazývá předpokladem této věty a výrok T se nazývá tvrzením věty. K důkazu matematických vět tvaru implikace $P \Rightarrow T$ je možno použít různých důkazových metod. Nejčastější jsou:

a) **důkaz přímý**, který spočívá v tom, že z platnosti výroku P (předpokladu) řadou platných implikací odvodíme platnost výroku T (tvrzení). Jinak řečeno, hledáme výroky $A_1, A_2, \ldots, A_n$ tak, že platí:

$$P \Rightarrow A_1 \quad \wedge \quad A_1 \Rightarrow A_2 \quad \wedge \quad \ldots \quad \wedge \quad A_{n-1} \Rightarrow A_n \quad \wedge \quad A_n \Rightarrow T.$$

b) **důkaz nepřímý** spočívá v přímém důkazu tvrzení $\neg T \Rightarrow \neg P$. Zde tedy využíváme již dokázaného faktu, že implikace $P \Rightarrow T$ a její obměna $\neg T \Rightarrow \neg P$ jsou ekvivalentní výroky. Při důkazu touto metodou tedy předpokládáme, že je pravdivý výrok $\neg T$ a řadou platných implikací dokážeme platnost výroku $\neg P$. Jinak řečeno, z negace tvrzení dokážeme (řadou platných implikací) negaci předpokladu.

   Určitou modifikací nepřímého důkazu je tzv. **důkaz sporem**, kdy předpokládáme, že platí předpoklad P a neplatí tvrzení T. Následně potom řadou platných implikací odvodíme spor. Přitom sporem rozumíme situaci, kdy nějaký výrok a jeho negace mají být současně pravdivé – je zřejmé, že tato situace nemůže nastat.

Matematická věta tvaru ekvivalence má tvar $A \Leftrightarrow B$ a dokazuje se většinou tak, že dokážeme jednak platnost implikace $A \Rightarrow B$ a dále pak platnost implikace $B \Rightarrow A$, a to metodami popsanými výše. Uvědomme si, že správnost této úvahy vyplývá z dříve dokázaného faktu, že ekvivalence $A \Leftrightarrow B$ je logicky ekvivalentní s konjunkcí implikací $(A \Rightarrow B) \ \wedge \ (B \Rightarrow A)$.

Poměrně často se můžeme setkat s tvrzeními, která je možno považovat za jisté zobecnění matematických vět typu ekvivalence. Jedná se o věty tvaru

"Jestliže platí výrok P, potom výroky $A_1, A_2, \ldots, A_n$ jsou ekvivalentní".

K tomu nejprve poznamenejme, že pojem ekvivalentních výroků, který jsme zavedli pro dva výroky, můžeme rozšířit na libovolný konečný počet výroků $A_1, A_2, \ldots, A_n$ takto: řekneme, že výroky $A_1, A_2, \ldots, A_n$ jsou ekvivalentní, jestliže platí $A_i \Leftrightarrow A_j$ pro každé $i, j = 1, \ldots, n$.

Větu tohoto tvaru většinou nedokazujeme ověřováním všech ekvivalencí $A_i \Leftrightarrow A_j$ pro každé $i \neq j$ (kterých je celkem $n \cdot (n-1)$), ale obvykle postupujeme tak, že dokážeme platnost pouze n implikací tvaru:

$$A_1 \Rightarrow A_2 \ , \ A_2 \Rightarrow A_3 \ , \ \ldots \ , \ A_{n-1} \Rightarrow A_n \ , \ A_n \Rightarrow A_1.$$

Je jednoduché ukázat, že odsud již plyne ekvivalentnost všech výroků $A_1, A_2, \ldots, A_n$. Poznamenejme ještě, že zvolené pořadí výroků v uvedených implikacích není závazné. Bylo by také možné dokazovat libovolných n implikací $A_i \Rightarrow A_j$ $(i \neq j)$, v nichž se každý z výroků $A_1, A_2, \ldots, A_n$ objeví právě jednou jako předpoklad a právě jednou jako tvrzení a to tak, že je-li daný výrok v jedné implikaci tvrzením, pak je v následující implikaci předpokladem. Nepřesně, ale názorně řečeno je pouze nutné, aby se nám "kruh implikací uzavřel".

Zvláštním typem důkazu matematické věty je **důkaz matematickou indukcí**. Touto metodou není možné dokazovat jakoukoliv matematickou větu, nýbrž jenom ty věty, které tvrdí, že za daných předpokladů platí výrok $V(n)$, a to pro všechna celá čísla $n \geq n_0$, kde n_0 je nějaké pevně dané celé číslo. Nejčastěji je $n_0 = 1$.

Důkaz takové věty matematickou indukcí pak probíhá ve dvou krocích, následujícím způsobem: za daných předpokladů

α) dokážeme platnost výroku $V(n_0)$

β) předpokládáme, že výrok $V(n)$ platí pro $n = n_0, n_0 + 1, \ldots, k$ a za tohoto předpokladu dokážeme platnost výroku $V(k+1)$. Věta je pak dokázána.

Přepoklad vyslovený v β) se nazývá **indukční předpoklad**. Poznamenejme, že ve většině důkazů matematickou indukcí se z indukčního předpokladu využije pouze to, že platí $V(k)$ a z platnosti $V(k)$ se pak již odvodí požadovaná platnost $V(k+1)$. Mohlo by se tedy zdát, že stačí indukční předpoklad "redukovat" na předpoklad platnosti $V(k)$. V dalším se však setkáme s matematickými větami, které se budou dokazovat matematickou indukcí, přičemž taková "redukce" indukčního předpokladu nebude možná.

2. Základní množinové pojmy.

Pojem množiny je základním pojmem celé matematiky. Přitom pod pojmem **množina** budeme rozumět libovolně, jednoznačně vymezený souhrn nějakých objektů, které budeme nazývat **prvky množiny**. Pro názornost budeme množiny obvykle označovat velkými latinskými písmeny a prvky množin pak malými latinskými písmeny.

Základní a přitom vlastně jedinou vlastností množin je, že mají prvky. Skutečnost, že objekt x je prvkem množiny A (tzn. x patří do A) budeme zapisovat: $x \in A$. Skutečnost, že objekt x není prvkem množiny A (tzn. x nepatří do A) pak budeme zapisovat: $x \notin A$.

Množina je jednoznačně určená svými prvky. Proto dvě množiny, nezávisle na způsobu jejich zadání, považujeme za stejné, právě když mají stejné prvky. Tato vlastnost množin se nazývá **extenzionalita**. Můžeme tedy psát:

$$A = B \quad \Leftrightarrow \quad (\forall x)\,(x \in A \;\Leftrightarrow\; x \in B).$$

Existuje množina, která se vyznačuje tím, že nemá žádné prvky. Nazývá se **prázdná množina** a označuje se symbolem $\emptyset$.

Množina se nazývá **konečná**, jestliže je možné ji zadat vyjmenováním všech jejích prvků. Je-li A konečná množina a $a_1, a_2, \ldots, a_n$ jsou všechny její prvky, pak píšeme

$$A \;=\; \{a_1, a_2,\; \ldots\; , a_n\}.$$

Z extenzionality vyplývá, že nezáleží na pořadí v jakém vyjmenováváme, resp. zapisujeme prvky množiny A. Mohlo by se však stát, že uvedená množina A má méně než n prvků; v takovém případě se některé z prvků $a_1, a_2, \ldots, a_n$ opakují. Obvykle pak v zápise množiny A opakující se prvky až na jeden vynecháváme. Například tedy: $\{x, y\} = \{y, x\}$ a pokud je $x = y$, potom $\{x, y\} = \{x\} = \{y\}$.

Kromě konečných množin se v matematice můžeme velmi často setkat i s neprázdnou množinou, kterou není možné zadat vyjmenováním všech jejích jednotlivých prvků. Taková množina se nazývá **nekonečná**. Nekonečné množiny obvykle zadáváme nějakou jejich charakteristickou vlastností. Jestliže $P(x)$ je nějaká vlastnost, pak píšeme

$$X \;=\; \{\, x \;\mid\; P(x)\,\},$$

čímž myslíme, že pro libovolné x platí: $x \in X$ právě tehdy, když x splňuje $P(x)$. Například vlastností *"x je sudé celé číslo"* je určena množina všech celých sudých čísel. Poznamenejme, že z rovnosti $X = \{\, x \;\mid\; P(x)\,\}$ nemusí automaticky vyplývat, že množina X je nekonečná – stejně dobře může být konečná nebo dokonce prázdná. Například množina

$$X = \{\, x \;\mid\; x \in \mathbb{Z} \;\wedge\; x^2 - 1 = 0\,\}$$

je dvouprvková množina sestávající z čísel 1 a -1 , tzn. $X = \{1, -1\}$, zatímco množina

$$X = \{\, x \;\mid\; x \in \mathbb{Z} \;\wedge\; x^2 + 1 = 0\,\}$$

je prázdnou množinou.

Na tomto místě je nutné upozornit na to, že výše uvedené vymezení pojmu množiny není vlastně přesnou definicí a vede k rozporům, protože jsou "souhrny", které za množiny považovat nemůžeme. Nejjednoduší příklad takové "zakázané množiny" byl nalezen zhruba před sto lety. Je to souhrn $\mathcal{M} = \{ X \mid X \notin X \}$ všech množin X, které neobsahují sebe jako prvek. Pokud by $\mathcal{M}$ byla množina, pak si můžeme položit otázku, zda $\mathcal{M} \in \mathcal{M}$ či nikoliv. Jestliže však $\mathcal{M} \in \mathcal{M}$, pak podle definice je $\mathcal{M} \notin \mathcal{M}$, což je spor. Jestliže by bylo $\mathcal{M} \notin \mathcal{M}$, pak podle definice dostáváme $\mathcal{M} \in \mathcal{M}$, což je opět spor. Řešení problémů spojených s definicí pojmu množiny podává speciální matematická disciplína, axiomatická teorie množin, kterou se však v tomto textu nebudeme zabývat. Budeme pracovat v tzv. naivní teorii množin, která je vybudována na základě výše uvedeného nepřesného vymezení pojmu množiny, přičemž však naše úvahy budou z hlediska teorie množin legální.

Říkáme, že množina A je **podmnožina** množiny B a píšeme $A \subseteq B$, jestliže libovolný prvek množiny A je zároveň prvkem množiny B. Vztah $\subseteq$ se nazývá **množinová inkluze**. Jestliže $A \subseteq B$ a $A \neq B$, pak říkáme, že A je **vlastní podmnožina** množiny B a píšeme $A \subset B$.

Máme-li dokázat, že $A \subseteq B$ pak postupujeme tak, že vezmeme libovolný prvek $x \in A$ a dokážeme, že $x \in B$. Jestliže množina A není podmnožinou množiny B, pak budeme psát $A \not\subseteq B$. Chceme-li dokázat, že $A \not\subseteq B$, pak (podle předchozích úvah o negacích kvantifikovaných výroků) dokazujeme, že existuje prvek x takový, že $x \in A$ a zároveň $x \notin B$, a to nejlépe tak, že tento prvek konkrétně nalezneme.

Pro libovolné množiny A, B, C zřejmě platí:

$$A \subseteq A\,,\ \emptyset \subseteq A\,,\ (A \subseteq B\ \wedge\ B \subseteq C)\ \Rightarrow\ A \subseteq C\,,\ A = B\ \Leftrightarrow\ (A \subseteq B\ \wedge\ B \subseteq A).$$

Důležitý je zejména poslední z výše uvedených vztahů, pomocí kterého obvykle dokazujeme rovnost dvou množin A, B. Důkaz vedeme tak, že dokážeme nejdříve inkluzi $A \subseteq B$ a potom inkluzi $B \subseteq A$.

Jsou-li A, B množiny, pak můžeme utvořit další množiny

$$\begin{aligned} A \cup B &= \{ x \mid x \in A \ \vee\ x \in B \} \\ A \cap B &= \{ x \mid x \in A \ \wedge\ x \in B \} \\ A - B &= \{ x \mid x \in A \ \wedge\ x \notin B \} \end{aligned}$$

které postupně nazýváme **sjednocení**, **průnik** a **rozdíl množin** A a B.

Poznamenejme ještě, že při různých množinových úvahách je třeba vyjádřit nejenom skutečnost, daný prvek ve sjednocení, průniku nebo rozdílu množin leží, ale často také skutečnost, že v nich neleží. V takových případech zřejmě platí:

$$\begin{aligned} x \notin A \cup B &\quad \text{právě když} \quad x \notin A \ \wedge\ x \notin B \\ x \notin A \cap B &\quad \text{právě když} \quad x \notin A \ \vee\ x \notin B \\ x \notin A - B &\quad \text{právě když} \quad x \notin A \ \vee\ x \in B\ . \end{aligned}$$

Pro sjednocení, průnik a rozdíl množin platí celá řada tvrzení, z nichž si některé uvedeme v následující větě.

Věta 2.1.
Nechť A, B, C jsou libovolné množiny. Pak platí:

1. $A \cup B = B \cup A$
2. $A \cap B = B \cap A$
3. $(A \cup B) \cup C = A \cup (B \cup C)$
4. $(A \cap B) \cap C = A \cap (B \cap C)$
5. $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
6. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
7. $A - (B \cup C) = (A - B) \cap (A - C)$
8. $A - (B \cap C) = (A - B) \cup (A - C)$

Důkaz.
Důkaz všech uvedených tvrzení se provádí stejným způsobem, a to dokazováním příslušných množinových inkluzí. Pro ilustraci dokážeme například vztah 8:

"$\subseteq$": $x \in A - (B \cap C) \;\Rightarrow\; x \in A \wedge x \notin (B \cap C) \;\Rightarrow\; x \in A \wedge (x \notin B \vee x \notin C) \;\Rightarrow$
$\Rightarrow\; (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C) \;\Rightarrow\; x \in (A - B) \vee x \in (A - C) \;\Rightarrow$
$\Rightarrow\; x \in (A - B) \cup (A - C)\,.$

"$\supseteq$": $x \in (A - B) \cup (A - C) \;\Rightarrow\; x \in (A - B) \vee x \in (A - C) \;\Rightarrow$
$\Rightarrow\; (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C) \;\Rightarrow\; x \in A \wedge (x \notin B \vee x \notin C) \Rightarrow$
$\Rightarrow\; x \in A \wedge x \notin (B \cap C) \;\Rightarrow\; x \in A - (B \cap C)\,.$ ■

Pokud si pozorně prohlédneme předchozí důkaz, zjistíme, že jeho druhá část je pouze "obrácením" části první. Bylo by tedy možné provést důkaz "najednou" tak, že bychom napsali pouze jeho první část a všechny symboly $\Rightarrow$ pro implikace bychom nahradili symboly $\Leftrightarrow$ pro ekvivalence. Tento postup však nelze aplikovat vždycky, a proto zejména začátečník by měl množinovou rovnost napoprve vždy dokazovat pomocí důkazu dvou množinových inkluzí.

Pojem sjednocení a průniku dvou množin je možné zobecnit. Je-li $I \neq \emptyset$ libovolná (tzv. indexová) množina a A_i je množina pro každé $i \in I$, pak

sjednocení množin A_i je množina $\displaystyle\bigcup_{i \in I} A_i = \{\, x \mid \exists\, i_0 \in I : x \in A_{i_0} \}$

průnik množin A_i je množina $\displaystyle\bigcap_{i \in I} A_i = \{\, x \mid \forall\, i \in I : x \in A_i \,\}.$

Uvědomme si, že předchozí definice zahrnují sjednocení a průnik jak dvou množin, tak libovolného konečného počtu množin a případně i nekonečného počtu množin. To, který z těchto případů nastane, záleží zřejmě na indexové množině I.

V případě, že I je konečná množina, například $I = \{1, 2, \ldots n\}$, píšeme též

$$A_1 \cup A_2 \cup \cdots \cup A_n\,, \qquad \text{resp.} \qquad A_1 \cap A_2 \cap \cdots \cap A_n\,.$$

V případě, že je $I = \mathbb{N}$, píšeme též $\displaystyle\bigcup_{i=1}^{\infty} A_i$, resp. $\displaystyle\bigcap_{i=1}^{\infty} A_i$. Přitom je nutné zdůraznit, že poslední dva zápisy samozřejmě není možné použít univerzálně pro jakoukoliv nekonečnou indexovou množinu I.

V matematice se poměrně často setkáváme s množinami, jejichž prvky jsou zase množiny. Pro takovou množinu budeme používat názvu **systém množin**.

Příklad 2.1.
Nechť A je libovolná množina. Pak všechny podmnožiny množiny A tvoří systém množin, který budeme nazývat **systém všech podmnožin množiny** A a označovat symbolem 2^A. Konkrétně, například pro $A = \{x, y, z\}$ je

$$2^A \;=\; \{\,\emptyset\,, \{x\}\,, \{y\}\,, \{z\}\,, \{x, y\}\,, \{x, z\}\,, \{y, z\}\,, \{x, y, z\}\,\}\,.$$

Podobně například pro $A = \emptyset$ je $2^\emptyset = \{\emptyset\}$, tzn. $2^\emptyset$ je jednoprvkovou množinou, jejímž jediným prvkem je prázdná množina.

Obecněji, je-li množina A konečná, o n prvcích, potom množina 2^A je jistě také konečná a lze ukázat, že má 2^n prvků. Tento fakt do jisté míry zdůvodňuje použité označení 2^A pro systém všech podmnožin množiny A. Na druhé straně, je-li množina A nekonečná, pak je množina 2^A samozřejmě také nekonečná.

Na závěr tohoto paragrafu si ještě zavedeme pojem kartézského součinu dvou množin. K tomu budeme potřebovat pojem **uspořádaná dvojice prvků**. Pro naše účely postačí intuitivní představa, že ke každým dvěma prvkům x, y lze přiřadit nový prvek (x, y), nazývaný uspořádanou dvojicí tak, že dvě uspořádané dvojice (x, y) a (r, s) jsou si rovny, právě když $x = r$ a $y = s$. V uspořádané dvojici (x, y) tedy záleží na pořadí prvků x, y, přičemž prvek x se nazývá **první složka** a prvek y se nazývá **druhá složka** uspořádané dvojice (x, y).

Analogickým způsobem lze pro libovolné $n \geq 2$ zavést pojem **uspořádaná $n-$tice prvků**, kterou označujeme symbolem $(a_1, a_2, \ldots a_n)$. Přitom klademe

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n) \;\text{ právě když }\; a_1 = b_1 \wedge a_2 = b_2 \wedge \ldots \wedge a_n = b_n\,,$$

tzn. dvě uspořádané $n-$tice prvků se rovnají právě když se rovnají jejich odpovídající si složky.

Jestliže A, B jsou libovolné množiny, pak množina

$$A \times B \;=\; \{\,(x, y) \mid x \in A\,,\; y \in B\,\}$$

se nazývá **kartézský součin množin** A, B (v tomto pořadí).

Z předchozí definice je zřejmé, že v kartézském součinu záleží na pořadí množin, tzn. množiny $A \times B$ a $B \times A$ jsou obecně různé. Je-li například $A = \{a\}$ a $B = \{x, y\}$, pak je:

$$A \times B \;=\; \{(a, x), (a, y)\} \qquad \text{a} \qquad B \times A \;=\; \{(x, a), (y, a)\}\,,$$

a tedy $A \times B \;\neq\; B \times A$.

Dále je zřejmé, že je-li některá z množin A, B prázdná, tzn. $A = \emptyset$ nebo $B = \emptyset$, pak i jejich kartézský součin je prázdná množina, tzn. $A \times B = \emptyset$.

Analogickým způsobem zavádíme pro libovolné $n \geq 2$ kartézský součin množin $A_1, A_2, \ldots, A_n$, jako množinu

$$A_1 \times A_2 \times \ldots \times A_n \;=\; \{\,(a_1, a_2, \ldots, a_n) \mid a_i \in A_i\,,\; i = 1, 2, \ldots, n\,\}\,.$$

Je-li $A_1 = A_2 = \ \ldots \ = A_n = A$, pak příslušný kartézský součin označujeme symbolem A^n a nazýváme jej $n-$tá **kartézská mocnina množiny** A. Například tedy kartézská mocnina

$$\mathbb{R}^3 \ = \ \{(x,y,z) \mid x,y,z \in \mathbb{R} \text{ libovolné}\}$$

je množinou všech uspořádaných trojic reálných čísel.

Pro sjednocení, průnik, rozdíl a kartézský součin množin opět platí celá řada tvrzení. Některé z nich uvedeme v následující větě.

Věta 2.2.
Nechť A, B, C jsou libovolné množiny. Pak platí:

1. $A \times (B \cup C) \ = \ (A \times B) \cup (A \times C)$
2. $(A \cup B) \times C \ = \ (A \times C) \cup (B \times C)$
3. $A \times (B \cap C) \ = \ (A \times B) \cap (A \times C)$
4. $(A \cap B) \times C \ = \ (A \times C) \cap (B \times C)$
5. $A \times (B - C) \ = \ (A \times B) - (A \times C)$
6. $(A - B) \times C \ = \ (A \times C) - (B \times C)$

Důkaz.
Důkaz všech uvedených tvrzení se opět provede technickým rozepsáním příslušných množinových inkluzí. Pro ilustraci dokažme například vztah 5:

"$\subseteq$": $(x,y) \in A \times (B-C) \ \Rightarrow \ x \in A \wedge y \in (B-C) \ \Rightarrow \ x \in A \wedge (y \in B \wedge y \notin C) \ \Rightarrow$
$\Rightarrow \ (x,y) \in (A \times B) \ \wedge \ (x,y) \notin (A \times C) \ \Rightarrow \ (x,y) \in (A \times B) - (A \times C)$.

"$\supseteq$": $(x,y) \in (A \times B) - (A \times C) \ \Rightarrow \ (x,y) \in (A \times B) \wedge (x,y) \notin (A \times C) \ \Rightarrow$
$\Rightarrow \ (x \in A \wedge y \in B) \ \wedge \ (x \notin A \vee y \notin C) \ \Rightarrow \ (x \in A \wedge y \in B \wedge x \notin A) \ \vee$
$\vee \ (x \in A \wedge y \in B \wedge y \notin C) \ \Rightarrow \ x \in A \wedge (y \in B \wedge y \notin C) \ \Rightarrow$
$\Rightarrow \ x \in A \ \wedge \ y \in (B - C) \ \Rightarrow \ (x,y) \in A \times (B - C)$. ■

Poznamenejme, že v některých množinových rovnostech uvedených ve větách 2.1. a 2.2. je možné sjednocení a průnik dvou množin nahradit "obecným" sjednocením a průnikem množin, jak je vidět z následující věty.

Věta 2.3.
Nechť I je neprázdná indexová množina a nechť A, B_i jsou množiny, pro každé $i \in I$. Pak platí:

1. $A \cap \bigcup\limits_{i \in I} B_i \ = \ \bigcup\limits_{i \in I} (A \cap B_i)$
2. $A \cup \bigcap\limits_{i \in I} B_i \ = \ \bigcap\limits_{i \in I} (A \cup B_i)$
3. $A \ - \bigcup\limits_{i \in I} B_i \ = \ \bigcap\limits_{i \in I} (A - B_i)$
4. $A \ - \bigcap\limits_{i \in I} B_i \ = \ \bigcup\limits_{i \in I} (A - B_i)$
5. $A \times \bigcup\limits_{i \in I} B_i \ = \ \bigcup\limits_{i \in I} (A \times B_i)$
6. $A \times \bigcap\limits_{i \in I} B_i \ = \ \bigcap\limits_{i \in I} (A \times B_i)$.

Důkaz.
Důkaz všech uvedených tvrzení se, stejně jako v předchozích větách, provede technickým rozepsáním příslušných množinových inkluzí. Pro ilustraci tentokrát dokažme například vztah 1:

"$\subseteq$": $x \in A \cap \bigcup\limits_{i\in I} B_i \;\Rightarrow\; x \in A \;\wedge\; x \in \bigcup\limits_{i\in I} B_i \;\Rightarrow\; x \in A \;\wedge\; \exists\, i_0 \in I \;:\; x \in B_{i_0} \;\Rightarrow$

$\Rightarrow\; \exists\, i_0 \in I : x \in A \cap B_{i_0} \;\Rightarrow\; x \in \bigcup\limits_{i\in I} (A \cap B_i)\,.$

"$\supseteq$": $x \in \bigcup\limits_{i\in I} (A \cap B_i) \;\Rightarrow\; \exists\, i_0 \in I : x \in A \cap B_{i_0} \;\Rightarrow\; x \in A \;\wedge\; \exists\, i_0 \in I \;:\; x \in B_{i_0} \;\Rightarrow$

$\Rightarrow\; x \in A \;\wedge\; x \in \bigcup\limits_{i\in I} B_i \;\Rightarrow\; x \in A \cap \bigcup\limits_{i\in I} B_i\,.$ ■

Závěrem našich úvodních úvah o množinách je nutné varovat před představou, že všechny jednoduché množinové vztahy, které "pěkně vypadají" musí vždy také platit. Například rovnost: $A - (B - C) = (A - B) - C$ obecně neplatí. To, že uvedená rovnost neplatí, dokazujeme tak, že uvedeme jeden konkrétní příklad množin A, B, C, které tuto rovnost nesplňují. V našem případě je to celkem jednoduché: stačí vzít například dva různé prvky a, b a utvořit množiny $A = \{a\}\,,\; B = \{b\}\,,\; C = \{a\}$. Při této volbě je pak $A - (B - C) = \{a\}$, zatímco $(A - B) - C = \emptyset$, což dokazuje, že uvedená rovnost skutečně neplatí.

To, že neplatí rovnost daných množin samozřejmě nemusí nutně znamenat, že neplatí ani jedna z obou inkluzí. Uvědomme si, že

$$A = B \quad \Leftrightarrow \quad (\, A \subseteq B \;\wedge\; B \subseteq A\,)$$

což tedy znamená, že

$$A \neq B \quad \Leftrightarrow \quad (\, A \not\subseteq B \;\vee\; B \not\subseteq A\,)\,.$$

Například v přechozí úvaze jsme uvedením konkrétního protipříkladu dokázali, že neplatí množinová inkluze $A-(B-C) \subseteq (A-B)-C$, a tedy neplatí příslušná množinová rovnost. Pokud jde o opačnou inkluzi, tj. $A-(B-C) \supseteq (A-B)-C$, tak ta v uvedeném případě platí (dokažte si sami rozepsáním).

3. Základní číselné obory.

Pojem čísla je základním matematickým pojmem, s nímž se setkáváme již od předškolního věku. Na základní a střední škole se čísla a operace s nimi zavádějí víceméně intuitivně a žáci postupně poznávají jejich důležité vlastnosti. V této kapitole zavedeme označení, resp. popis základních číselných oborů a podrobněji se zmíníme pouze o vlastnostech komplexních čísel.

Čísla přirozená
označujeme symbolem $\mathbb{N}$, přičemž $\mathbb{N} = \{1, 2, 3, \ \dots\}$. Poznamenejme, že někdy se mezi přirozená čísla zahrnuje i číslo nula. Jde o věc dohody, my v tomto textu nulu do přirozených čísel zahrnovat nebudeme.

Čísla celá
označujeme symbolem $\mathbb{Z}$, přičemž $\mathbb{Z} = \{\dots \ -3, -2, -1, 0, 1, 2, 3, \ \dots\}$. Základními vlastnostmi celých čísel se budeme podrobněji zabývat v následující kapitole.

Čísla racionální
označujeme symbolem $\mathbb{Q}$. Jedná se o čísla, která lze vyjádřit ve tvaru zlomku, kde čitatel i jmenovatel jsou celá čísla, přičemž jmenovatel je různý od nuly. Připomeňme, že každé racionální číslo má nekonečně mnoho možných vyjádření uvedeného tvaru, např.

$$\frac{2}{3}\,, \quad \frac{-2}{-3}\,, \quad \frac{4}{6}\,, \quad \frac{-4}{-6}\,, \quad \frac{6}{9}\,, \quad \frac{-6}{-9}\,, \quad \dots \quad \text{atd.}$$

Použijeme-li pro racionální číslo zápis, kde se ve jmenovateli vyskytuje nejmenší kladné číslo, pak říkáme, že jsme dané číslo vyjádřili v **základním tvaru**. Takové vyjádření je pro každé racionální číslo zřejmě jediné. V předchozím příkladu je to zápis $\frac{2}{3}$.

Čísla reálná
označujeme symbolem $\mathbb{R}$. Množina $\mathbb{R}$ reálných čísel se skládá ze dvou disjunktních podmnožin, z nichž jedna je tvořena čísly racionálními a druhá čísly iracionálními. Přitom iracionální čísla nelze vyjádřit jako podíl celých čísel, jsou to například čísla

$$\sqrt{2}\,, \quad \sqrt{5}\,, \quad \pi\,, \quad \log 6\,, \quad \sin\tfrac{1}{3}\pi\,, \quad \text{atd.}$$

Množina $\mathbb{R}$ má jednu důležitou vlastnost: existuje vzájemně jednoznačné přiřazení všech reálných čísel a všech bodů libovolné přímky. Jinak řečeno, každému reálnému číslu lze přiřadit jediný bod zvolené přímky a také obráceně, každému bodu této přímky odpovídá jediné reálné číslo. Podrobným studiem vlastností reálných čísel se zabývá základní kurz matematické analýzy.

Jak již bylo řečeno, uvedené číselné obory jsme popsali pouze intuitivně. K jejich přesné konstrukci a přesnému odvození základních vlastností je potřeba matematických znalostí, které přesahují rámec středoškolské matematiky. Touto problematikou se bude později zabývat kurz teoretické aritmetiky. Nicméně, všechny základní vlastnosti čísel uváděné na střední škole samozřejmě platí a my je budeme i nadále používat.

Víme tedy, že ve všech uvedených číselných oborech je možno čísla sčítat a násobit, přičemž jak sčítání tak násobení jsou komutativní, asociativní a platí distributivní zákon. Navíc v $\mathbb{Z}$, $\mathbb{Q}$ a $\mathbb{R}$ ke každému číslu existuje číslo opačné, zatímco v oboru přirozených čísel $\mathbb{N}$ tomu tak není. Dále, v oborech $\mathbb{Q}$ a $\mathbb{R}$ ke každému nenulovému číslu existuje číslo převrácené, zatímco v $\mathbb{N}$ a v $\mathbb{Z}$ tomu tak není. Konečně, čísla všech uvedených číselných množin je možno uspořádat "podle velikosti" (tzn. zavést symboly pro nerovnosti $\leq$, $<$, atd.). Pro počítání s nerovnostmi pak platí celá řada známých početních pravidel.

Čísla komplexní
označujeme symbolem $\mathbb{C}$. Na rozdíl od předchozích číselných oborů nejsou komplexní čísla mírou žádné reálné veličiny a nelze je tedy získat jako výsledek fyzikálních či jiných měření. Komplexní čísla vznikla postupným zobecňováním pojmu čísla v souvislosti s potřebou řešit úlohy, jejichž řešení v předchozích číselných oborech neexistuje. Příkladem takové úlohy je třeba hledání řešení jednoduché kvadratické rovnice

$$x^2 + 1 = 0\,.$$

V žádném z předchozích číselných oborů řešení této rovnice evidentně neexistuje, protože tam pro každé číslo x platí, že $x^2 \geq 0$, což znamená, že je vždy $x^2 + 1 \neq 0$. V oboru komplexních čísel však existuje řešení nejenom této kvadratické rovnice, ale dá se ukázat, že existuje řešení jakékoliv kvadratické rovnice a dokonce, že existuje řešení všech podobných rovnic libovolných stupňů.

Definice.
Komplexní čísla $\mathbb{C}$ zavádíme jako množinu všech uspořádaných dvojic reálných čísel, tzn. $\mathbb{C} = \mathbb{R} \times \mathbb{R}$. Sčítání a násobení komplexních čísel definujeme takto: pro libovolné $(a, b), (c, d) \in \mathbb{C}$ položíme

$$\begin{aligned}(a, b) + (c, d) &= (a + c\ ,\ b + d)\\ (a, b) \cdot (c, d) &= (ac - bd\ ,\ ad + bc)\,.\end{aligned}$$

Úmluva.
Všimněme si, že pro komplexní čísla tvaru $(t, 0)$ platí:

$$(a, 0) + (c, 0) = (a + c\ ,\ 0) \qquad \text{a} \qquad (a, 0) \cdot (c, 0) = (ac\ ,\ 0)\,,$$

což znamená, že komplexní čísla tohoto tvaru se sčítají a násobí stejným způsobem jako čísla reálná. Můžeme tedy každé komplexní číslo tvaru $(t, 0)$ ztotožnit s reálným číslem t. Označíme-li navíc komplexní číslo $(0, 1)$ symbolem i, je pak možné každé komplexní číslo $z = (a, b)$ zapsat ve tvaru:

$$z = (a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0) \cdot (0, 1) = a + bi$$

Definice.
Vyjádření komplexního čísla $z = (a, b)$ ve tvaru $z = a + bi$ se nazývá **algebraický tvar komplexního čísla** z. Přitom reálné číslo a se nazývá **reálná část** komplexního čísla z, reálné číslo b se nazývá **imaginární část** komplexního čísla z a číslo $i = (0, 1)$ se nazývá **imaginární jednotka**.

Z předchozích definic bezprostředně vyplývá několik důležitých poznatků:

1. pro imaginární jednotku i platí:

$$i^2 \;=\; (0,1)\cdot(0,1) \;=\; (-1,0) \;=\; -1\,.$$

   Vidíme tedy, že výše zmiňovaná kvadratická rovnice tvaru $x^2+1=0$ má v oboru komplexních čísel řešení a tímto řešením je například komplexní číslo i. Pro úplnost jenom poznamenejme, že tato rovnice má celkem dvě řešení, tím druhým je komplexní číslo $-i=(0,-1)$.

2. dvě komplexní čísla v algebraickém tvaru se rovnají právě když se rovnají jejich reálné části a jejich imaginární části.

3. sčítání a násobení dvou komplexních čísel v algebraickém tvaru se provádí stejným způsobem, jako sčítání a násobení dvojčlenů (s využitím toho, že $i^2=-1$). Nemusíme si tedy nazpaměť pamatovat definice pro sčítání a násobení komplexních čísel uvedené v předchozí definici.

4. komplexní čísla je možno graficky znázorňovat, a sice jako body v tzv. Gaussově rovině. Jedná se o rovinu s kartézským souřadnicovým systémem s osami x ("reálná osa") a y ("imaginární osa"), v níž je každé komplexní číslo $z=(a,b)=a+bi$ znázorněno jako bod o souřadnicích $[a,b]$. Přitom zde platí podobný vztah jako platil mezi reálnými čísly a body na přímce. V tomto případě je tedy každému komplexnímu číslu uvedeným způsobem přiřazen právě jeden bod Gaussovy roviny a naopak, každému bodu Gausssovy roviny odpovídá jediné komplexní číslo.

Jednoduchými technickými výpočty se lehce ověří, že sčítání a násobení komplexních čísel splňuje stejná základní pravidla, které platí pro racionální čísla a reálná čísla. Konkrétně - sčítání a násobení komplexních čísel je komutativní, asociativní a platí distributivní zákon. Roli nuly hraje komplexní číslo $(0,0)$, které ztotožňujeme s reálným číslem 0 a roli jedničky hraje komplexní číslo $(1,0)$, které zotožňujeme s reálným číslem 1. Dále, ke komplexnímu číslu $z=(a,b)=a+bi$ existuje číslo opačné, kterým je komplexní číslo $-z=(-a,-b)=-a-bi$ a konečně platí, že k nenulovému komplexnímu číslu z existuje číslo převrácené $\frac{1}{z}$. Můžeme tedy provádět dělení čísla $a+bi$ nenulovým číslem $c+di$. Přitom se používá standardní "trik", kdy čitatele i jmenovatele rozšíříme číslem $c-di$, jak je vidět z následujícího příkladu.

Příklad 3.1.
Napište v algebraickém tvaru komplexní číslo $\dfrac{4+i}{2-3i}$.

Řešení:

$$\frac{4+i}{2-3i} \;=\; \frac{4+i}{2-3i}\cdot\frac{2+3i}{2+3i} \;=\; \frac{8+12i+2i+3i^2}{2^2-(3i)^2} \;=\; \frac{5+14i}{13} \;=\; \frac{5}{13}+\frac{14}{13}\,i\,.$$

Poznámka.
Na rozdíl od čísel reálných nelze komplexní čísla uspořádat "podle velikosti". Pro komplexní čísla nelze zavést vztah nerovnosti tak, aby splňoval všechny základní vlastnosti a početní pravidla, které má v případě čísel reálných. Komplexní čísla tedy například

nelze rozlišit na "kladná" a "záporná" (tj. větší nebo menší než nula) a do množiny komplexních čísel nelze přenést žádné partie z oboru čísel reálných, v nichž se vyskytují pojmy "větší" nebo "menší" (tzn. například partii o nerovnicích).

Je-li dáno komplexní číslo $z = a + bi$, pak komplexní číslo $a - bi$ se nazývá **číslo komplexně sdružené** k číslu z a označuje se symbolem $\overline{z}$. Přitom platí, že součin komplexních čísel z a $\overline{z}$ je číslo reálné, které je dokonce nezáporné. Skutečně:

$$z \cdot \overline{z} \;=\; (a+bi)\cdot(a-bi) \;=\; a^2 + b^2 \;\geq\; 0\,.$$

Podobným způsobem se rozepsáním dokáže, že pro libovolná komplexní čísla u, v platí:

$$\overline{u+v} \;=\; \overline{u} + \overline{v} \qquad\qquad \overline{u\cdot v} \;=\; \overline{u}\cdot\overline{v} \qquad\qquad \overline{\left(\frac{u}{v}\right)} \;=\; \frac{\overline{u}}{\overline{v}}\,.$$

Pro ilustraci dokažme například druhý z uvedených vztahů, ostatní se dokáží podobně. Je-li tedy $u = a + bi$, $v = c + di$, potom je

$$\overline{u\cdot v} \;=\; \overline{(a+bi)\cdot(c+di)} \;=\; \overline{(ac-bd)+(ad+bc)i} \;=\; (ac-bd)-(ad+bc)i$$

$$\overline{u}\cdot\overline{v} = (a-bi)\cdot(c-di) = (ac-bd)+(-ad-bc)i = (ac-bd)-(ad+bc)i$$

což znamená, že dokazovaný vztah platí.

Další pojem, který známe z předchozích číselných oborů a který lze zavést pro komplexní čísla je pojem absolutní hodnoty. Je-li tedy $z = (a, b) = a + bi$ libovolné komplexní číslo, pak **absolutní hodnota komplexního čísla** z se označuje $|\,z\,|$ a definuje se takto:

$$|\,z\,| \;=\; \sqrt{a^2+b^2}\,.$$

Z této definice ihned vidíme, že geometrický význam absolutní hodnoty z komplexního čísla je stejný, jako je tomu u reálných čísel. V obou případech totiž absolutní hodnota udává vzdálenost obrazu daného čísla od počátku soustavy souřadnic. Pro počítání s absolutními hodnotami z komplexních čísel platí podobná základní pravidla jako u čísel reálných, tzn. pro libovolná komplexní čísla u, v je:

$$|\,u\cdot v\,| \;=\; |\,u\,|\cdot|\,v\,| \qquad\qquad \text{a je-li } v\neq 0\text{, pak} \quad \left|\,\frac{u}{v}\,\right| \;=\; \frac{|\,u\,|}{|\,v\,|}\,.$$

Oba vztahy můžeme dokázat bezprostředním rozepsáním podle definice absolutní hodnoty. Je-li tedy $u = a + bi$, $v = c + di$, potom je $u \cdot v = (ac - bd) + (ad + bc)i$, odkud dostáváme

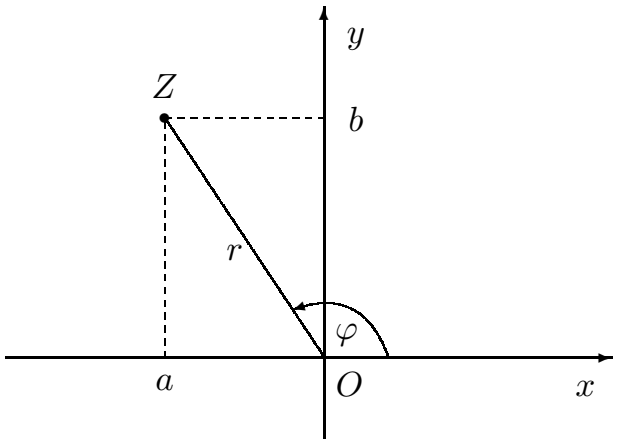
$$|\,u\cdot v\,| = \sqrt{(ac-bd)^2+(ad+bc)^2} = \sqrt{a^2c^2+b^2d^2+a^2d^2+b^2c^2}$$

$$|\,u\,|\cdot|\,v\,| = \sqrt{(a^2+b^2)}\cdot\sqrt{(c^2+d^2)} = \sqrt{a^2c^2+a^2d^2+b^2c^2+b^2d^2}$$

odkud plyne první z obou vztahů. Druhý vztah se dokáže analogicky.

Komplexní čísla jsme doposud zapisovali pouze v algebraickém tvaru. Nyní si ukážeme jiný způsob jejich zápisu. Jeho princip spočívá v tom, že bod $Z \neq O$ v Gaussově

rovině můžeme jednoznačně určit pomocí jeho vzdálenosti r od počátku souřadné soustavy O a velikosti orientovaného úhlu φ jehož počáteční rameno je kladná poloosa x a koncové rameno je polopřímka OZ (viz obrázek). Je zřejmé, že v případě $Z = O$, tzn. pro komplexní číslo $z = 0$, uvedené vyjádření není možné.



Reálné číslo φ určující velikost daného orientovaného úhlu se nazývá **argument komplexního čísla** z a označuje se symbolem $\arg z$.

Ze známých vlastností orientovaného úhlu plyne, že má-li komplexní číslo $z \neq 0$ argument φ, pak má též argument $\varphi + k \cdot 2\pi$, kde k je libovolné celé číslo. Jinými slovy řečeno, argument nenulového komplexního čísla není určen jednoznačně, nýbrž je určen "až na celočíselný násobek 2π".

Z předchozího obrázku je dále vidět, že platí:

$$r = \sqrt{a^2 + b^2} \qquad , \qquad \sin\varphi = \frac{b}{r} \qquad , \qquad \cos\varphi = \frac{a}{r} \ .$$

Znamená to, že pro číslo r nemusíme zavádět zvláštní pojmenování, protože je rovno absolutní hodnotě daného komplexního čísla, tzn. $r = |\,z\,|$. Pro komplexní číslo $z \neq 0$ tedy dostáváme:

$$z \ = \ a + bi \ = \ r\cos\varphi + (r\sin\varphi)\,i \ = \ |\,z\,|\,(\cos\varphi + i\sin\varphi) \ .$$

Definice.
Zápis nenulového komplexního čísla ve tvaru $z = |\,z\,|\,(\cos\varphi + i\sin\varphi)$ se nazývá **goniometrický tvar komplexního čísla** z.

Uvědomme si, že dvě komplexní čísla vyjádřená v goniometrickém tvaru se rovnají právě když se rovnají jejich absolutní hodnoty a jejich argumenty se liší o $k{\cdot}2\pi$, kde $k \in \mathbb{Z}$ (popřípadě se argumenty mohou přímo rovnat, je-li $k = 0$).

Jednou z výhod zápisu komplexních čísel v goniometrickém tvaru je to, že se lehce spočítá jejich součin a podíl. Přímým rozepsáním, s využitím součtových vzorců pro sinus a kosinus, se dá ukázat, že pro daná nenulová komplexní čísla z_1, z_2, kde

$$z_1 = |\,z_1\,|\,(\cos\varphi_1 + i\sin\varphi_1) \qquad , \qquad z_2 = |\,z_2\,|\,(\cos\varphi_2 + i\sin\varphi_2)$$

platí

$$z_1 \cdot z_2 \;=\; |\,z_1\,|\cdot|\,z_2\,|\,(\cos(\varphi_1+\varphi_2)\;+\;i\,\sin(\varphi_1+\varphi_2))$$

$$\frac{z_1}{z_2} \;=\; \frac{|\,z_1\,|}{|\,z_2\,|}\,(\cos(\varphi_1-\varphi_2)\;+\;i\,\sin(\varphi_1-\varphi_2))\;.$$

Předchozí vztah pro součin dvou komplexních čísel v goniometrickém tvaru je možné zobecnit na součin libovolného konečného počtu komplexních čísel (důkaz se vede matematickou indukcí). Podobně se postupuje v případě, když umocňujeme komplexní číslo v goniometrickém tvaru na přirozený exponent.

Věta 3.1.
Nechť $z = |\,z\,|\,(\cos\varphi + i\sin\varphi) \in \mathbb{C}$. *Pak pro libovolné* $n \in \mathbb{N}$ *platí:*

$$z^n = |\,z\,|^n\;(\,\cos n\varphi\;+\;i\,\sin n\varphi\,)\,.$$

Důkaz.
Tvrzení dokážeme matematickou indukcí vzhledem k n.

α) pro $n = 1$ tvrzení evidentně platí

β) předpokládáme, že tvrzení platí pro 1, ... , $n-1$ ($n \geq 2$). Dokážeme nyní dané tvrzení pro n. Použijeme-li postupně definici mocniny, indukční předpoklad a součtové vzorce pro kosinus a sinus, dostáváme:

$$z^n = z\cdot z^{n-1} = |\,z\,|\;(\cos\varphi + i\sin\varphi)\cdot|\,z\,|^{n-1}\;(\cos(n-1)\varphi + i\sin(n-1)\varphi) =$$

$$= |z|^n\big[\cos\varphi\cos(n-1)\varphi - \sin\varphi\sin(n-1)\varphi + i(\cos\varphi\sin(n-1)\varphi + \sin\varphi\cos(n-1)\varphi)\big] =$$

$$= |\,z\,|^n\;(\,\cos n\varphi\;+\;i\,\sin n\varphi\,)\;\;. \qquad \blacksquare$$

Dosadíme-li do předchozí věty $|\,z\,| = 1$, dostaneme tvrzení, které odvodil francouzský matematik Abraham de Moivre (1667 - 1754) již počátkem 18. století.

Důsledek (Moivreova věta).
Pro každé přirozené číslo n *a libovolné reálné číslo* φ *platí:*

$$(\,\cos\varphi\;+\;i\,\sin\varphi\,)^{\,n} \;=\; (\,\cos n\varphi\;+\;i\,\sin n\varphi\,)\,.$$

Na závěr této kapitoly se ještě budeme zabývat řešením speciálního typu rovnic v oboru komplexních čísel, a to tak zvaných binomických rovnic. Přitom **binomická rovnice** je rovnice tvaru

$$x^{\,n} \;-\; a \;=\; 0$$

kde a je dané komplexní číslo, x je neznámá a $n > 1$ je přirozené číslo. Řešit takovou rovnici znamená najít všechna komplexní čísla, která jí vyhovují. Tato komplexní čísla budeme také nazývat (komplexní) n**−té odmocniny z komplexního čísla** a.

Při řešení binomických rovnic budeme vždy předpokládat, že $a \neq 0$, protože pro $a = 0$, má tato rovnice zřejmě jediné řešení, a to $x = 0$. Tento předpoklad nám

také umožní vyjádřit číslo a v goniometrickém tvaru. Řešení binomických rovnic jsou popsána v následujícím tvrzení.

Věta 3.2.
Binomická rovnice

$$x^n - a = 0,$$

kde $a = |a|(\cos\alpha + i\sin\alpha)$, *má v oboru komplexních čísel právě* n *různých řešení, a to*

$$x_k = \sqrt[n]{|a|}\left(\cos\frac{\alpha+2k\pi}{n} + i\sin\frac{\alpha+2k\pi}{n}\right), \qquad pro\ k = 0,1,2,\ \ldots\ ,n-1.$$

Důkaz.
K tomu, abychom tuto větu dokázali, je třeba ukázat tři věci, a to, že:

1. číslo x_k dané rovnici vyhovuje – to však ihned dostaneme dosazením čísla x_k do dané rovnice a umocněním podle věty 3.1.
2. čísla $x_0, x_1, \ldots, x_{n-1}$ jsou navzájem různá – to bezprostředně vyplývá z vyjádření komplexního čísla v goniometrickém tvaru a z vlastností funkcí kosinus a sinus.
3. žádná další řešení dané binomické rovnice neexistují.
   Je-li tedy $z = |z|(\cos\varphi + i\sin\varphi)$ řešením dané rovnice, potom po dosazení z za x do dané rovnice a úpravě dostaneme:

$$|z|^n(\cos n\varphi + i\sin n\varphi) = |a|(\cos\alpha + i\sin\alpha).$$

   Z rovnosti dvou čísel v goniometrickém tvaru však plyne, že

$$|z|^n = |a| \qquad \wedge \qquad n\varphi = \alpha + t\cdot 2\pi, \ \text{kde}\ t\in\mathbb{Z},$$

   odkud ihned vyplývá, že z je rovno některému z čísel $x_0, x_1, \ldots, x_{n-1}$. ■

Pokud bychom si všechna řešení binomické rovnice $x^n - a = 0$ chtěli nakreslit v Gaussově rovině, pak zjistíme, že čísla $x_0, x_1, \ldots, x_{n-1}$ leží ve vrcholech pravidelného n-úhelníku vepsaného do kružnice se středem v počátku a poloměrem $\sqrt[n]{|a|}$.

Příklad 3.2.
Nalezněte všechny páté odmocniny z komplexního čísla $c = \dfrac{2i\cdot(\sqrt{3}-i)^{10}}{(1+i\sqrt{3})^8\cdot(-1+i)^6}$.

Řešení.
Hledané řešení označíme z. Spočítáme zvlášť jeho absolutní hodnotu a jeho argument (s využitím početních pravidel, která jsme uvedli dříve). Tedy:

$$|z| = \sqrt[5]{\frac{|2i|\cdot|\sqrt{3}-i|^{10}}{|1+i\sqrt{3}|^8\cdot|-1+i|^6}} = \sqrt[5]{\frac{2\cdot 2^{10}}{2^8\cdot(\sqrt{2})^6}} = 1$$

$$\arg z \;=\; \tfrac{1}{5}\left(\arg(2i) + 10\arg(\sqrt{3}-i) \;-\; [\,8\arg(1+i\sqrt{3}) + 6\arg(-1+i)\,] \;+\; k\cdot 2\pi\right) \;=$$
$$=\; \tfrac{1}{5}\left(\tfrac{\pi}{2} \;+\; 10\cdot\tfrac{11}{6}\pi \;-\; 8\cdot\tfrac{\pi}{3} \;-\; 6\cdot\tfrac{3}{4}\pi \;+\; k\cdot 2\pi\right) \;=\; \tfrac{7}{3}\pi \;+\; k\cdot\tfrac{2}{5}\pi\;.$$

Hledanými pátými odmocninami z c je pak následujících pět komplexních čísel (místo argumentu $\frac{7}{3}\pi$ můžeme vzít hodnotu $\frac{7}{3}\pi - 2\pi = \frac{\pi}{3}$ z intervalu $\langle 0, 2\pi)\,)$:

$$z_k \;=\; \cos(\,\tfrac{\pi}{3} + k\cdot\tfrac{2}{5}\pi\,) \;+\; i\,\sin(\,\tfrac{\pi}{3} + k\cdot\tfrac{2}{5}\pi\,) \qquad \text{pro } k = 0,1,2,3,4\,.$$

Velmi důležitým zvláštním případem binomické rovnice je rovnice

$$x^n \;-\; 1 \;=\; 0\,.$$

Řešení této rovnice budeme nazývat **n-té odmocniny z jedné**. Vzhledem k tomu, že číslo 1 (chápané jako komplexní číslo) má argument $\alpha = 0$ a jeho absolutní hodnota je rovna jedné, dostáváme dosazením do vzorce pro řešení binomické rovnice, že pro n-té odmocniny z jedné platí:

$$x_k \;=\; \cos\frac{2k\pi}{n} \;+\; i\,\sin\frac{2k\pi}{n}\;, \qquad\qquad k = 0,1,2,\;\ldots\;,n{-}1\,.$$

Vidíme tedy, že n-tých odmocnin z jedné (v oboru komplexních čísel) je právě n a jejich obrazy, nakreslené v Gaussově rovině, leží ve vrcholech pravidelného n-úhelníku vepsaného do jednotkové kružnice se středem v počátku, přičemž jeden z vrcholů leží v bodě 1 na reálné ose. Nakreslete si sami obrázek znázorňující například všech osm osmých odmocnin z jedné.

Na závěr našich úvah o binomických rovnicích uveďme dvě důležité vlastnosti n-tých odmocnin z jedné, které budeme později využívat.

Věta 3.3.
Pro n – té odmocniny z jedné platí:

1. *součin dvou n-tých odmocnin z jedné je opět n-tá odmocnina z jedné*
2. *převrácená hodnota n-té odmocniny z jedné je opět n-tá odmocnina z jedné.*

Důkaz.
Nechť x_r, x_s jsou libovolné n-té odmocniny z jedné. Potom je: $x_r^n = 1$ a $x_s^n = 1$.

Nyní vezměme číslo $x_r{\cdot}x_s$ a číslo $\dfrac{1}{x_r}$ a umocněme je na n – tou. Dostaneme:

$$(x_r{\cdot}x_s)^n \;=\; x_r^n\cdot x_s^n \;=\; 1 \qquad\qquad \text{a} \qquad\qquad \left(\frac{1}{x_r}\right)^n \;=\; \frac{1^n}{x_r^n} \;=\; 1\,,$$

odkud plyne, že čísla $x_r{\cdot}x_s$ a $\dfrac{1}{x_r}$ jsou řešeními binomické rovnice $x^n - 1 = 0$. Jinak řečeno, obě čísla jsou n-tými odmocninami z jedné. ■

4. Základní vlastnosti celých čísel.

Na střední škole byla odvozena nebo jenom uvedena řada vlastností celých čísel a pravidel pro počítání s nimi. V této kapitole zopakujeme a doplníme zejména základní vlastnosti celých čísel, které souvisejí s dělitelností.

Definice.
Nechť a, b jsou celá čísla. Říkáme, že a **dělí** b a píšeme $a \mid b$, jestliže

$$\text{existuje celé číslo } \ z \ \text{ tak, že platí } \ b = a \cdot z\,.$$

V opačném případě říkáme, že a **nedělí** b a píšeme $a \nmid b$.

Je nutné vždy přesně vědět, co znamená výše uvedený slovní obrat "v opačném případě". Jinak řečeno, je nutné správně utvořit negaci výroku s existenčním kvantifikátorem. Tedy a nedělí b, znamená, že pro každé celé číslo z platí, že $b \neq a \cdot z$.

Dále je nutné si uvědomit, že zvláštní roli při dělitelnosti celých čísel hraje číslo nula. Přímo z definice dělitelnosti v oboru celých čísel totiž plyne, že

$$\begin{aligned} &a \mid 0 \ \text{ pro každé } \ a \in \mathbb{Z} && \text{tzn. každé celé číslo dělí nulu} \\ &0 \mid b \ \text{ právě když } \ b = 0 && \text{tzn. nula dělí pouze nulu.} \end{aligned}$$

Všimněme si dále, že každé celé číslo b je vždy dělitelné čísly 1, -1, b, $-b$. Tato čísla se nazývají **nevlastní dělitelé** čísla b. Všichni ostatní dělitelé čísla b (pokud existují) se nazývají **vlastní dělitelé** čísla b. S vlastními a nevlastními děliteli přirozených čísel souvisí následující dva pojmy.

Definice.
Celé číslo p se nazývá **prvočíslo**, jestliže $p > 1$ a p má pouze nevlastní dělitele. Podobně, celé číslo s se nazývá **složené číslo** jestliže $s > 1$ a s má i vlastní dělitele.

Některé základní vlastnosti celých čísel, které se týkají dělitelnosti, popisuje následující věta.

Věta 4.1.

Nechť a, b, c jsou libovolná celá čísla. Pak platí:

1. $a \mid a$
2. $a \mid b \ \wedge \ b \mid c \ \Rightarrow \ a \mid c$
3. $a \mid b \ \wedge \ a \mid c \ \Rightarrow \ a \mid (b \cdot x + c \cdot y) \ \ \textit{pro každé } x, y \in \mathbb{Z}$
4. $a \mid b \ \wedge \ b \mid a \ \Leftrightarrow \ b = \pm a\,.$

Důkaz.

1. tvrzení je zřejmé, neboť lze napsat $a = a \cdot 1$, což znamená, že $a \mid a$.
2. nechť $a \mid b \ \wedge \ b \mid c$. Pak existují celá čísla z_1, z_2 tak, že: $b = a \cdot z_1 \ \wedge \ c = b \cdot z_2$. Po dosazení dostáváme $c = a \cdot (z_1 \cdot z_2)$, neboli $a \mid c$.

3. nechť $a \mid b \ \wedge \ a \mid c$. Pak existují celá čísla z_1, z_2 tak, že: $b = a \cdot z_1 \ \wedge \ c = a \cdot z_2$. Tedy: $b \cdot x + c \cdot y = a \cdot (z_1 \cdot x \ + \ z_2 \cdot y)$, odkud plyne, že $a \mid (b \cdot x \ + \ c \cdot y)$.

4. *Důkaz implikace "⇒".*
Nechť $a \mid b \ \wedge \ b \mid a$. Potom existují $z_1, z_2 \in \mathbb{Z}$ tak, že $b = z_1\, a \ \wedge \ a = z_2\, b$. Po dosazení dostáváme

$$b \ = \ z_1\, z_2\, b\,.$$

Nyní, pokud je $b = 0$, pak musí být $a = 0$ (proč?) a tvrzení platí. Nechť tedy $b \neq 0$. Potom můžeme číslem b vykrátit a dostáváme $1 \ = \ z_1 \cdot z_2$. Tato rovnice je však v oboru celých čísel splněna pouze pro $z_1 = z_2 = 1$ nebo pro $z_1 = z_2 = -1$. Platí tedy, že $b \ = \ \pm\, a$.

Důkaz implikace "⇐".
$b = \pm a \quad \Rightarrow \quad b = a \cdot (\pm 1) \ \wedge \ a = b \cdot (\pm 1) \quad \Rightarrow \quad a \mid b \ \wedge \ b \mid a.$ ■

Jedním ze základních algoritmů, který se učí žáci již na základní škole, je algoritmus pro dělení dvou přirozených čísel. Uvědomme si, že výsledkem výpočtu je vlastně nalezení dalších dvou čísel, tzv. částečného podílu a zbytku. Celou situaci lze zformulovat v oboru celých čísel pomocí následující věty.

Věta 4.2. (Věta o dělení se zbytkem celých čísel)

Nechť a, b jsou celá čísla, taková, že $b \neq 0$. Potom existují celá čísla q, r, splňující vztah:

(1) $$a \ = \ b \cdot q \ + \ r \qquad \wedge \qquad 0 \leq r \ < \ |\, b \,|\,,$$

přičemž toto vyjádření je jednoznačné.

Důkaz.
Důkaz věty provedeme ve dvou krocích. V prvním kroku dokážeme, že uvedené vyjádření existuje a ve druhém kroku pak ukážeme, že čísla q, r splňující vztah (1) jsou určena jednoznačně.

1. *Důkaz existence vyjádření* (1).
Uvažme množinu celých čísel

$$M \ = \ \{\, x \cdot |\, b \,| \ \mid \ x \in \mathbb{Z} \ \wedge \ x \cdot |\, b \,| \leq \ a \,\}.$$

Množina M je zřejmě neprázdná a existuje v ní největší prvek, který si označíme $x_0 \cdot |\, b \,|$ (rozmyslete si podrobně, že tomu tak skutečně je). Potom platí:

(2) $$a \ = \ x_0 \cdot |\, b \,| \ + \ r \qquad \text{kde } \ r \geq 0$$

a dále zřejmě je $(x_0 + 1) \cdot |\, b \,| \ > \ a$, neboli $x_0 \cdot |\, b \,| + |\, b \,| \ > \ a$, odkud po úpravě dostáváme, že $a - x_0 \cdot |\, b \,| \ < \ |\, b \,|$ a po dosazení za a ze (2) vychází

(3) $$r \ < \ |\, b \,|$$

Nyní už jenom stačí pouze provést označení

$$q \ = \ \begin{cases} \ \ x_0\,, & \text{je-li } \ b > 0 \\ -x_0\,, & \text{je-li } \ b < 0 \end{cases}$$

a při tomto označení dostáváme ze (2) a (3) okamžitě hledaný vztah (1).

2. *Důkaz jednoznačnosti vyjádření* (1) .
Budeme předpokládat, že existují dvě dvojice celých čísel, splňující vztah (1) a dokážeme, že se odpovídající si čísla rovnají. Nechť tedy q, q', r, r' jsou celá čísla, splňující vztah (1), tzn.:

$$a \;=\; b\cdot q \,+\, r\,, \quad 0 \,\leq\, r \,<\mid b \mid \qquad \wedge \qquad a \;=\; b\cdot q' \,+\, r'\,, \quad 0 \,\leq\, r' \,<\mid b \mid .$$

Pak odečtením obou rovnic obdržíme $b\cdot(q-q') \;=\; r'-r$, odkud přechodem k absolutním hodnotám dostáváme:

$$\mid b\cdot(q-q') \mid \;=\mid b \mid \;\cdot\mid q-q' \mid \;=\mid r'-r \mid .$$

Dále, z předpokladů o číslech r a r' plyne, že musí být $\mid r'-r \mid \,<\mid b \mid$.

Nyní – pokud by bylo $q \neq q'$, dostáváme $\mid r'-r \mid =\mid b \mid \;\cdot\mid q-q' \mid \geq \mid b \mid$, což je spor. Musí tedy být $q = q'$, odkud pak ihned plyne, že $r = r'$. To však znamená, že vyjádření (1) je jednoznačné. ■

Číslo q z vyjádření (1) se nazývá (neúplný) **podíl** po dělení čísla a číslem b. Číslo r z vyjádření (1) se nazývá **zbytek** po dělení čísla a číslem b. Mimo jiné tedy vidíme, že zbytek r po dělení čísla a číslem b je definován jednoznačně a nabývá vždy právě jedné z hodnot $0\,,\,1\,,\,\ldots\,,\,\mid b\mid -1$.

Nyní zavedeme v oboru celých čísel $\mathbb{Z}$ pojem největšího společného dělitele dvou celých čísel a popíšeme jeho základní vlastnosti.

Definice.
Nechť a, b jsou celá čísla. Celé číslo d se nazývá **největší společný dělitel** čísel a, b, jestliže platí:

1. $d \mid a \;\;\wedge\;\; d \mid b$
2. jestliže $k \mid a \wedge k \mid b$ pro nějaké $k \in \mathbb{Z}$, potom také $k \mid d$.

Věta 4.3.
Nechť a, b jsou libovolná celá čísla. Pak platí:

1. *existuje největší společný dělitel čísel a, b*
2. *jestliže d je největším společným dělitelem čísel a, b , pak $\{d, -d\}$ je množinou všech největších společných dělitelů čísel a, b*
3. *jestliže d je největším společným dělitelem čísel a, b , pak existují celá čísla u, v tak, že platí*

$$a\cdot u \;+\; b\cdot v \;=\; d\,.$$

Důkaz.

1. pro $a = 0\,,\; b = 0$ existuje největší společný dělitel, a sice číslo 0 (ověřte si sami, že tomu tak skutečně je). Nechť tedy $a \neq 0$ nebo $b \neq 0$. Uvažme množinu čísel

$$M \;=\; \{\, a\cdot x \,+\, b\cdot y \;\mid\; x, y \in \mathbb{Z} \text{ libovolné}\}$$

a označme $d = a \cdot x_0 + b \cdot y_0$ nejmenší kladné číslo patřící do M (rozmyslete si, že takové číslo určitě existuje). Nyní ukážeme, že d je hledaným největším společným dělitelem čísel a, b (ověřením obou částí definice). Tedy:

1. podle věty o dělení celých čísel existují $q, r \in \mathbb{Z}$ tak, že

   $$a = d \cdot q + r \qquad \text{kde} \quad 0 \leq r < d$$

   (zde $|\, d \,| = d$ protože d je podle předpokladu kladné). Pak

   $r = a - d \cdot q = a - (a \cdot x_0 + b \cdot y_0) \cdot q = a \cdot (1 - x_0 \cdot q) + b \cdot (-y_0 \cdot q) \in M.$

   Poněvadž však $0 \leq r < d$ a d je nejmenším kladným číslem patřícím do M, musí být $r = 0$. To ale znamená, že $a = d \cdot q$, a tedy $d \mid a$.
   Podobným způsobem se ukáže, že také $d \mid b$.

2. jestliže $k \mid a$, $k \mid b$, pak podle věty 4. 1. 3. platí, že $k \mid (a \cdot x_0 + b \cdot y_0) = d$.

Dokázali jsme tak, že d je největším společným dělitelem čísel a, b.

2. nechť d je daný největší společný dělitel čísel a, b a nechť f je libovolný největší společný dělitel a, b. Potom:

   $f \mid a \ \wedge \ f \mid b$, odkud plyne (protože d je největší společný dělitel a, b), že $f \mid d$,

   $d \mid a \ \wedge \ d \mid b$, odkud plyne (protože f je největší společný dělitel a, b), že $d \mid f$.

   Tedy $f \mid d \ \wedge \ d \mid f$, tzn. podle věty 4. 1. 4 dostáváme, že $f = \pm d$.

3. z důkazu 1. části věty plyne, že existují $x_0, y_0 \in \mathbb{Z}$ tak, že $a \cdot x_0 + b \cdot y_0$ je největším společným dělitelem čísel a, b. Vzhledem k 2. části věty však libovolného největšího společného dělitele čísel a, b můžeme vyjádřit ve tvaru $a \cdot (\pm x_0) + b \cdot (\pm y_0)$, odkud po vhodném označení dostáváme žádané tvrzení. ■

Z předchozí věty plyne, že pro $a = b = 0$ existuje jediný jejich největší společný dělitel, a sice číslo 0. V všech ostatních případech (tzn. pro $a \neq 0 \vee b \neq 0$) existují vždy dva největší společní dělitelé čísel a, b, lišící se znaménkem. Dále poznamenejme, že třetí část věty pouze zaručuje existenci celých čísel u, v, splňujících uvedený vztah. Dá se ukázat, že takových dvojic čísel u, v existuje nekonečně mnoho.

Poznámka - dělitelnost v oboru přirozených čísel.
Na střední škole se pojem dělitelnosti obvykle probírá v oboru přirozených čísel. Samotný pojem dělitelnosti lze bez problémů přeformulovat pro přirozená čísla zřejmým způsobem: pro přirozená čísla a, b řekneme, že a dělí b, jestliže existuje přirozené číslo u tak, že $b = a \cdot u$. Základní vlastnosti dělitelnosti, které jsme uvedli ve větě 3. 1. platí i pro dělitelnost v oboru přirozených čísel. Rovněž pojem největšího společného dělitele je možné zavést pro přirozená čísla stejným způsobem, jako jsme to učinili pro čísla celá. Poznamenejme, že v tomto případě je možno druhou podmínku v definici největšího společného dělitele dvou přirozených čísel, tzn. podmínku

" jestliže $k \mid a$, $k \mid b$ pro nějaké $k \in \mathbb{N}$, potom také $k \mid d$ "

nahradit ekvivalentní podmínkou

" d je největší ze všech přirozených čísel k splňujících: $k \mid a$, $k \mid b$ ".

Největší společný dělitel čísel a, b v oboru přirozených čísel existuje jediný.

Definice.
Řekneme, že dvě **celá čísla** a, b **jsou nesoudělná**, jestliže číslo 1 je jejich největším společným dělitelem.

Následující věta ukáže některé jednoduché vlastnosti nesoudělných čísel. Všimněte si, že se při jejich důkazu podstatným způsobem využívá 3. část předchozí věty.

Věta 4.4.
Nechť $a, b, c, a_1, \ldots, a_n$ jsou celá čísla. Pak platí:

1. $a\,, b$ *jsou nesoudělná* $\wedge$ $a\,, c$ *jsou nesoudělná* $\Rightarrow$ $a\,, b \cdot c$ *jsou nesoudělná*
2. $a \mid b \cdot c \ \wedge\ a\,, b$ *jsou nesoudělná* $\Rightarrow\ a \mid c$
3. p *je prvočíslo* $\wedge\ p \mid a_1 \cdot \ldots \cdot a_n \ \Rightarrow\ p \mid a_i$ *pro nějaké* $i = 1, 2, \ldots, n\,.$

Důkaz.

1. Nechť $a\,, b$ jsou nesoudělná a a, c jsou nesoudělná. Podle věty 4.3.3 existují celá čísla u, v, x, y tak, že platí:
$$a \cdot u + b \cdot v \ = \ 1 \qquad \wedge \qquad a \cdot x + c \cdot y \ = \ 1\,.$$
Vynásobením obou rovností dostáváme:
$$a \cdot (uax + ucy + bvx) \ + \ bc \cdot (vy) \ = \ 1 \qquad (4)$$
Nyní dokážeme, že 1 je největším společným dělitelem čísel $a\,,\ b \cdot c\,.$
   1. zřejmě platí, že $1 \mid a \ \wedge\ 1 \mid bc$
   2. jestliže $k \mid a \ \wedge\ k \mid bc$, potom ze (4), užitím věty 4.1.3 dostáváme, že
$$k \mid [\, a \cdot (uax + ucy + bvx) \ + \ bc \cdot (vy)\,] \ \Rightarrow \ k \mid 1\,.$$
   Dokázali jsme tak, že čísla $a\,, b \cdot c$ jsou nesoudělná.
2. Nechť $a \mid b \cdot c \ \wedge\ a\,, b$ jsou nesoudělná. Pak podle věty 4.3.3 existují celá čísla u, v tak, že $a \cdot u + b \cdot v \ = \ 1\,.$ Po vynásobení této rovnice číslem c dostáváme:
$$acu + bcv \ = \ c\,,$$
   odkud podle věty 4.1.3 (poněvadž $a \mid a \ \wedge\ a \mid bc$) plyne, že $a \mid c\,.$
3. Tvrzení budeme dokazovat matematickou indukcí vzhledem k $n\,.$
   $\alpha)$ pro $n = 1$ tvrzení evidentně platí
   $\beta)$ předpokládáme, že tvrzení platí pro $1, \ldots, n{-}1$ $(n \geq 2)\,.$ Nechť nyní p je prvočíslo $\wedge\ p \mid a_1 \cdot \ldots \cdot a_n$, tzn.
$$p \mid (a_1 \cdot \ldots \cdot a_{n-1}) \cdot a_n\ .$$
   Jestliže $p \mid a_n$, pak dostáváme požadované tvrzení. Nechť tedy p nedělí $a_n\,.$ Potom jsou čísla $p\,, a_n$ nesoudělná (proč ?) a podle 2. části této věty platí, že
$$p \mid (a_1 \cdot \ldots \cdot a_{n-1})\,.$$
   Podle indukčního předpokladu pak $p \mid a_i$ pro nějaké $i = 1, 2, \ldots, n{-}1\,.$ ■

Věta 4. 5.
Každé celé číslo $a > 1$ lze rozložit na součin prvočísel, a to jednoznačně, až na jejich pořadí

Důkaz.
Nejprve budeme dokazovat existenci požadovaného rozkladu a pak jeho jednoznačnost.

1. *Důkaz existence rozkladu.*
Důkaz povedeme sporem. Předpokládejme, že existují celá čísla větší než jedna, která nelze rozložit na součin prvočísel a nejmenší z těchto čísel označme u. Pak ale u není prvočíslo, tzn. u musí mít vlastního dělitele b, a tedy: $u = b \cdot c$, kde $1 < b < u$, $1 < c < u$. Ale čísla b, c lze rozložit na součin prvočísel (jinak spor s definicí čísla u), a tedy $u = b \cdot c$ lze pak také rozložit na součin prvočísel, což je spor.

2. *Důkaz jednoznačnosti rozkladu (až na pořadí činitelů).*
Nechť

$$a = p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_k \tag{5}$$

jsou dva rozklady čísla $a > 1$ na součin prvočísel. Požadovanou jednoznačnost vyjádření (až na pořadí činitelů) nyní dokážeme matematickou indukcí vzhledem k n.

α) pro $n = 1$ je a prvočíslem, tzn. musí být také $k = 1$ a následně pak $p_1 = q_1$.

β) předpokládejme, že pro všechna celá čísla větší než jedna, mající rozklad na součin méně než n prvočísel, je tento rozklad jednoznačný (až na pořadí činitelů).
Vezměme celé číslo $a > 1$, pro které platí (5). Potom $p_n \mid a = q_1 \cdot \ldots \cdot q_k$. Ale p_n je prvočíslo, tzn. musí platit $p_n \mid q_i$ pro nějaké $i = 1, \ldots, k$. Poněvadž p_n i q_i jsou prvočísla, musí být $p_n = q_i$, takže po zkrácení číslem $p_n = q_i$ ve (4) a následném užití indukčního předpokladu dostáváme žádanou jednoznačnost. ■

Věta 4. 6.
Prvočísel je nekonečně mnoho.

Důkaz.
Budeme postupovat sporem. Předpokládejme, že existuje pouze konečně mnoho prvočísel a označme je například $p_1, p_2, \ldots, p_n$. Nyní utvořme číslo

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1.$$

Číslo a lze podle předchozí věty rozložit na součin jistého počtu prvočísel, tzn. jinak řečeno, číslo a je určitě dělitelné alespoň jedním prvočíslem. Existuje tedy prvočíslo p_i (kde $i = 1, 2, \ldots, n$) tak, že $p_i \mid a$. Kromě toho také $p_i \mid p_1 \cdot p_2 \cdot \ldots \cdot p_n$ (proč ?). Potom užitím věty 4. 1. 3. dostáváme:

$$p_i \mid (a - p_1 \cdot p_2 \cdot \ldots \cdot p_n) = 1$$

tzn. $p_i \mid 1$, což je spor, protože děliteli čísla 1 jsou zřejmě pouze ± 1, zatímco prvočíslo je podle definice vždy větší než 1. ■

Na závěr našich úvah o celých číslech uvedeme ještě jeden pojem, který budeme ve zbývající části tohoto textu často využívat.

Definice.
Nechť m je pevné přirozené číslo a nechť a, b jsou celá čísla. Jestliže platí, že $m \mid (b-a)$, pak řekneme, že **čísla** a, b **jsou kongruentní podle modulu** m a píšeme $a \equiv b \pmod{m}$.

Podmínku kongruentnosti dvou celých čísel podle modulu m je možné vyjádřit dalšími dvěma způsoby, ekvivalentními s předchozí definicí.

Věta 4.7.
Nechť m je pevné přirozené číslo a nechť a, b jsou celá čísla. Pak následující výroky jsou ekvivalentní:

1. $a \equiv b \pmod{m}$
2. *čísla a, b dávají po dělení číslem m stejný zbytek*
3. *čísla a, b se liší o celočíselný násobek čísla m*

Důkaz.
Důkaz provedeme ve třech krocích, postupným dokázáním následujících implikací:

Důkaz implikace "$1 \Rightarrow 2$".
Nechť platí 1 a nechť $a = m \cdot q_1 + r_1$, resp. $b = m \cdot q_2 + r_2$, přičemž $0 \leq r_1, r_2 < m$. Odečtením obou rovnic dostaneme:

$$r_2 - r_1 = (b - a) + m \cdot (q_1 - q_2).$$

Podle 1 je $m \mid (b-a)$ a triviálně platí $m \mid m$, a tedy podle V. 4. 1. 3. je pak $m \mid (r_2 - r_1)$, což znamená, že existuje celé číslo z, tak že

$$r_2 - r_1 = m \cdot z. \tag{5}$$

Zřejmě však je $-m < (r_2 - r_1) < m$ (proč ?), a tedy jediná hodnota z, která splňuje vztah (5) je číslo nula. Je tedy $r_2 - r_1 = m \cdot 0 = 0$, neboli $r_2 = r_1$. Platí tedy 2.

Důkaz implikace "$2 \Rightarrow 3$".
Nechť platí 2, tzn. čísla a, b dávají po dělení číslem m stejný zbytek. Můžeme tedy psát

$$a = m \cdot q_1 + r, \qquad b = m \cdot q_2 + r \qquad (\text{přičemž } 0 \leq r < m).$$

Po odečtení obou rovnic dostáváme $b - a = m \cdot (q_2 - q_1)$, což znamená, že

$$b = a + m \cdot (q_2 - q_1), \qquad \text{kde } (q_2 - q_1) \in \mathbb{Z}.$$

Tedy čísla a, b se liší o celočíselný násobek čísla m, čímž jsme dokázali 3.

Důkaz implikace "$3 \Rightarrow 1$".
Nechť platí 3, tzn. existuje celé číslo z tak, že $b = a + z \cdot m$. Pak ale $b - a = z \cdot m$, neboli $m \mid (b - a)$. Podle definice je tedy $a \equiv b \pmod{m}$, což znamená, že jsme dokázali platnost 1. ■

Kongruence mají celou řadu zajímavých vlastností a pro počítání s nimi platí celá řada pravidel. Některé ze základních vlastností kongruencí nyní uvedeme.

Věta 4.8.
Nechť m je pevné přirozené číslo a nechť a, b, c jsou celá čísla. Pak platí:

1. $a \equiv a \pmod{m}$
2. $a \equiv b \pmod{m} \quad \Rightarrow \quad b \equiv a \pmod{m}$
3. $a \equiv b \pmod{m} \ \wedge \ b \equiv c \pmod{m} \quad \Rightarrow \quad a \equiv c \pmod{m}$

Důkaz.
Vztahy 1. a 2. okamžitě plynou například z 2. části předchozí věty.

Důkaz vztahu 3.
Nechť $a \equiv b \pmod{m} \ \wedge \ b \equiv c \pmod{m}$. Pak $m \mid (b-a) \ \wedge \ m \mid (c-b)$ odkud užitím věty 4.1.3 dostáváme, že

$$m \mid \ (1 \cdot (c-b) + 1 \cdot (b-a)) \quad \Rightarrow \quad m \mid (c-a),$$

což znamená, že $a \equiv c \pmod{m}$. Platí tedy vztah 3. ■

Věta 4.9.
Nechť $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$. Pak platí:

1. $a + c \equiv b + d \pmod{m}$
2. $a - c \equiv b - d \pmod{m}$
3. $a \cdot c \equiv b \cdot d \pmod{m}$
4. $a^n \equiv b^n \pmod{m}$, *pro libovolné přirozené* n.

Důkaz.
Dokážeme například vztah 3.
Podle předpokladů a podle věty 4.7 (část 3), existují celá čísla z_1, z_2 tak, že $a = b + z_1 m$, $c = d + z_2 m$. Dosazením a výpočtem dostáváme:

$$a \cdot c \ = \ (b + z_1 m) \cdot (d + z_2 m) \ = \ (b \cdot d) + (b z_2 + z_1 d + z_1 z_2 m) \cdot m$$

odkud vidíme (opět užitím věty 4.7, část 3), že platí vztah 3.

Vztahy 1. a 2. se dokáží analogicky a vztah 4. se dokáže ze vztahu 3. užitím matematické indukce (proveďte si sami). ■

Z předchozí věty mimo jiné vyplývá, že se kongruence chovají vzhledem ke sčítání, odčítání a násobení kongruencí (podle stejného modulu m) podobně jako rovnice. Navíc pro kongruence platí další pravidla, která používáme u rovnic. Například, k oběma stranám kongruence je možno přičíst nebo odečíst libovolné celé číslo, resp. obě strany kongruence můžeme vynásobit libovolným celým číslem (to vyplývá ihned z předchozí věty a z faktu, že každé celé číslo je vždy kongruentní samo se sebou).

Pozor – v kongruencích nelze obecně provádět "krácení"! Například je:

$$3 \cdot 6 \ \equiv \ 7 \cdot 6 \pmod{8}, \quad \text{ale přitom neplatí, že} \quad 3 \ \equiv \ 7 \pmod{8}.$$

Následující věta však ukáže, že v kongruencích je možné provádět "krácení" číslem, které je nesoudělné s modulem.

Věta 4.10.
Nechť m je pevné přirozené číslo a nechť a, b, c jsou celá čísla. Pak platí:

$$a \cdot c \equiv b \cdot c \pmod{m} \ \wedge \ c, m \text{ jsou nesoudělná} \implies a \equiv b \pmod{m}.$$

Důkaz.
$a \cdot c \equiv b \cdot c \pmod{m} \implies m \mid (bc - ac) \implies m \mid (b-a) \cdot c$. Ale protože m, c jsou nesoudělná, musí (podle věty 4.4.2) platit, že $m \mid (b-a)$, což tedy znamená, že $a \equiv b \pmod{m}$. ■

5. Zobrazení.

Pojem zobrazení patří k základním pojmům celé matematiky. S tímto pojmem je možné se setkat již na střední škole.

Definice.
Nechť A, B jsou libovolné množiny. Předpis f, který každému prvku množiny A přiřazuje právě jeden prvek množiny B, se nazývá **zobrazení množiny** A **do množiny** B. Píšeme pak $f : A \longrightarrow B$.

Uvedená definice je sice názorná a pro naše účely dostačující, ale z hlediska teorie množin není zcela přesná, protože obsahuje předem nedefinovaný pojem "předpis". Přesnou definici zobrazení uvedeme později, v kapitole o relacích.

Jestliže $f : A \longrightarrow B$ je zobrazení, pak množina A se nazývá **definiční obor** a množina B se nazývá **obor hodnot** tohoto zobrazení. Skutečnost, že prvku $a \in A$ je přiřazen prvek $b \in B$, budeme vyjadřovat zápisem:

$$f(a) \;=\; b\,.$$

Jestliže je $f(a) \;=\; b$, pak budeme říkat, že prvek b je **obraz prvku** a, resp. budeme říkat, že prvek a je **vzor prvku** b.

Dvě zobrazení $f : A \longrightarrow B$, $g : C \longrightarrow D$ se rovnají (což budeme stručně vyjadřovat zápisem $f = g$), jestliže:

$$A = C \quad \wedge \quad B = D \quad \wedge \quad f(x) = g(x) \text{ pro každé } x \in A$$

tzn. jestliže se rovnají jejich definiční obory, obory hodnot a příslušné předpisy. V opačném případě (tzn. není-li splněna alespoň jedna z předchozích tří podmínek) se obě zobrazení nerovnají, což budeme stručně zapisovat ve tvaru $f \neq g$.

Vidíme, že k zadání zobrazení je nutno zadat definiční obor, obor hodnot a příslušný předpis. Na příkladech nyní ukážeme, jak je při tom možno postupovat.

Příklad 5. 1.
Definujme zobrazení $f : A \longrightarrow B$ takto:

1. $A = \{a, b, c, d\}$, $B = \{r, s, t, u, v\}$ a položíme:

$$f(a) = u\,, \quad f(b) = r\,, \quad f(c) = v\,, \quad f(d) = t.$$

2. $A = \mathbb{Z}$, $B = \mathbb{N}$ a položíme:

$$f(x) \;=\; \begin{cases} 2x + 1 & \text{pro } x \geq 0 \\ -2x & \text{pro } x < 0 \end{cases}$$

3. $A = \mathbb{R}$, $B = \mathbb{R}$ a položíme: $f(x) = \sin x$ pro každé $x \in \mathbb{R}$

4. $A = \mathbb{R}$, $B = \langle -1, 1 \rangle$ a položíme: $f(x) = \sin x$ pro každé $x \in \mathbb{R}$.

Všimněte si toho, že poslední dvě zobrazení mají stejný předpis (a sice $f(x) = \sin x$), ale přesto se nerovnají!! Mají totiž různé obory hodnot – jednou je oborem hodnot množina $B = \mathbb{R}$ a podruhé je oborem hodnot množina $B = \langle -1, 1 \rangle$.

Poznámka.

1. Definice zobrazení nevylučuje situaci, že některá z množin A, B je prázdnou množinou. Rozeberme si tento případ podrobněji.
   Je-li A prázdná množina a B je libovolná množina, pak existuje jediné zobrazení $\emptyset \longrightarrow B$, které se nazývá **prázdné zobrazení** (rozmyslete si, jak je v tomto případě splněna definice zobrazení!).
   Je-li A neprázdná množina a B je prázdná množina, potom neexistuje žádné zobrazení $A \longrightarrow \emptyset$.

2. Je-li A libovolná neprázdná množina, pak zobrazení $id_A : A \longrightarrow A$ definované předpisem: $id_A(x) = x$, pro každé $x \in A$ se nazývá **identické zobrazení** (nebo též identita) na množině A.

3. Je-li $A \subseteq \mathbb{R}, B \subseteq \mathbb{R}$, pak zobrazení $f : A \longrightarrow B$ se obvykle nazývá (reálná) **funkce** (jedné reálné proměnné). Tato zobrazení se podrobně studují v matematické analýze.

4. Zobrazení mohou také vystupovat v roli prvků množin. Důležitým příkladem je **množina všech zobrazení** $A \longrightarrow B$, kterou označujeme symbolem B^A.
   Ilustrujme si tento pojem na příkladu množin $A = \{a, b, c\}$ a $B = \{x, y\}$. Lehce zjistíme, že existuje právě 8 různých zobrazení $A \longrightarrow B$ (nakreslete si sami příslušné obrázky!). Množina B^A má tedy 8 (tzn. 2^3) prvků.
   Obecně lze pro konečné množiny ukázat, že má-li množina A n prvků a množina B má s prvků, potom existuje právě s^n různých zobrazení $A \longrightarrow B$, neboli množina B^A má s^n prvků. Tato úvaha do jisté míry vysvětluje, proč je pro označení množiny všech zobrazení $A \longrightarrow B$ použit symbol B^A (a nikoliv třeba symbol A^B).

Zobrazení mohou mít různé další vlastnosti. Nejzákladnější a zároveň nejdůležitější vlastnosti zobrazení jsou popsány v následující definici.

Definice.
Zobrazení $f : A \longrightarrow B$ se nazývá

- **injektivní zobrazení** (nebo též **prosté zobrazení**), jestliže každý prvek z množiny B má při zobrazení f nejvýše jeden vzor.
- **surjektivní zobrazení** (nebo též **zobrazení na**), jestliže každý prvek z množiny B má při zobrazení f alespoň jeden vzor.
- **bijektivní zobrazení**, jestliže každý prvek z množiny B má při zobrazení f právě jeden vzor.

O každém z výše definovaných pojmů je nutno mít zcela jasnou a názornou představu. Vyjádříme-li předchozí definici pouze jinými slovy (rozmyslete si podrobně sami, že obsahově jde skutečně o totéž), pak můžeme také říci, že:

- zobrazení $f : A \longrightarrow B$ je injektivní právě když se každé dva různé prvky množiny A zobrazí vždy na dva různé prvky množiny B
- zobrazení $f : A \longrightarrow B$ je surjektivní, právě když se na každý prvek množiny B vždy zobrazí nějaký prvek množiny A.
- zobrazení $f : A \longrightarrow B$ je bijektivní právě když je současně injektivní a surjektivní.

V praxi je velmi často potřeba technicky dokázat, že zadané zobrazení má, případně nemá některou z výše uvedených vlastností. Obvykle postupujeme následujícím způsobem: dokazujeme-li, že zobrazení $f : A \longrightarrow B$

- **je injektivní**, pak předpokládáme, že pro prvky $x, y \in A$ platí $f(x) = f(y)$ a následně dokážeme, že $x = y$.
  Můžeme také dokazovat implikaci: $x \neq y \Rightarrow f(x) \neq f(y)$ (rozmyslete si, proč jsou oba postupy ekvivalentní). Technicky jednodušší bývá obvykle způsob první.
- **není injektivní**, pak nalezneme dva konkrétní různé prvky z množiny A, které se zobrazí na stejný prvek v množině B.
- **je surjektivní**, pak vezmeme libovolný (obecný) prvek $y \in B$ a najdeme k němu vzor, tzn. najdeme prvek $a \in A$, pro který platí: $f(a) = y$.
- **není surjektivní**, pak nalezneme v množině B takový konkrétní prvek, který nemá při zobrazení f žádný vzor.

Budeme-li u jednotlivých zobrazení z příkladu 5.1. zjišťovat, zda jsou injektivní, resp. surjektivní, resp. bijektivní, pak celkem jednoduše zjistíme (proveďte si ověření podrobně sami!), že

- zobrazení z příkladu 5.1.1. je injektivní a není surjektivní,
- zobrazení zobrazení z příkladu 5.1.2. je injektivní i surjektivní, tzn. je bijektivní,
- zobrazení zobrazení z příkladu 5.1.3. není injektivní a není surjektivní
- zobrazení zobrazení z příkladu 5.1.4. není injektivní a je surjektivní.

Definice.
Nechť $f : A \longrightarrow B$ je bijektivní zobrazení. Definujme zobrazení $f^{-1} : B \longrightarrow A$ takto: pro každé $y \in B$ položíme

$$f^{-1}(y) \;=\; a\;,$$

kde a je ten prvek z množiny A, který je vzorem prvku y při původním zobrazení f (tzn. je $f(a) = y$). Zobrazení f^{-1} se potom nazývá **inverzní zobrazení k zobrazení** f.

Je třeba si uvědomit, že f^{-1} je skutečně zobrazením, což vyplývá z toho, že původní zobrazení f je bijektivní (tento předpoklad nelze z definice vypustit!!), a tedy prvek a, o kterém se v definici hovoří, opravdu existuje, a to jediný.

Jestliže je zobrazení $f : A \longrightarrow B$ bijektivním zobrazením, pak přímo z definice inverzního zobrazení ihned plyne, že $f^{-1} : B \longrightarrow A$ je také bijektivním zobrazením, a navíc zřejmě platí, že:

$$(f^{-1})^{-1} \;=\; f\,.$$

Příklad 5. 2.
Zobrazení $f : \mathbb{Z} \longrightarrow \mathbb{N}$ z příkladu 5. 1. 2 je, jak víme, bijektivní. Existuje tedy k němu zobrazení inverzní $f^{-1} : \mathbb{N} \longrightarrow \mathbb{Z}$. Lehce se zjistí, že:

$$f^{-1}(x) \;=\; \begin{cases} \frac{x-1}{2} & \text{pro každé liché } x \in \mathbb{N} \\ -\frac{x}{2} & \text{pro každé sudé } x \in \mathbb{N}. \end{cases}$$

Definice.
Nechť $f : A \longrightarrow B$, $g : B \longrightarrow C$ jsou zobrazení. Potom zobrazení $(g \circ f) : A \longrightarrow C$ definované předpisem

$$(g \circ f)(x) = g\,(\,f(x)\,) \qquad \text{pro každé } x \in A$$

se nazývá **složené zobrazení** (ze zobrazení f a g, v tomto pořadí).

Z definice je vidět, že složené zobrazení je možno definovat pouze v případě, že obor hodnot prvního zobrazení je roven definičnímu oboru druhého zobrazení. Poznamenejme ještě, že symbol $g \circ f$ čteme buď "g kolečko f" nebo "g po f". U zápisu složeného zobrazení $g \circ f$ si ještě všimněme toho, že i když se nejprve provádí zobrazení f a potom zobrazení g, je zaveden zápis "v obráceném pořadí". Nutí nás k tomu vžitá konvence, podle které se argument x píše napravo od symbolu zobrazení f. Poznamenejme, že někteří autoři dávají při označování složeného zobrazení přednost "skutečnému pořadí" obou zobrazení a místo $g \circ f$ píší $f \circ g$. Kvůli tomu pak opouštějí zmiňovanou konvenci a místo $f(x)$ píší $(x)f$, popřípadě xf.

Jestliže $f : A \longrightarrow B$ je zobrazení, pak přímo z definice složeného zobrazení ihned plyne, že

$$f \circ id_A = f \qquad \wedge \qquad id_B \circ f = f\,.$$

Je-li zobrazení $f : A \longrightarrow B$ navíc bijektivní, pak (jak víme) existuje inverzní zobrazení $f^{-1} : B \longrightarrow A$ a zřejmě platí

$$f^{-1} \circ f = id_A \qquad \wedge \qquad f \circ f^{-1} = id_B.$$

Další základní vlastnosti složených zobrazení shrneme v následujících větách.

Věta 5. 1.
Nechť $f : A \longrightarrow B$, $g : B \longrightarrow C$, $h : C \longrightarrow D$ jsou zobrazení. Pak platí:

$$h \circ (\,g \circ f\,) \;=\; (\,h \circ g\,) \circ f\,.$$

Důkaz.
Zřejmě je $h \circ (g \circ f) : A \longrightarrow D$, $(h \circ g) \circ f : A \longrightarrow D$, a tedy definiční obory a obory hodnot obou zobrazení jsou si rovny. K dokázání věty zbývá dokázat rovnost příslušných předpisů. Nechť tedy je $x \in A$ libovolný. Pak je:

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

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

tedy oba předpisy jsou stejné a věta platí. ■

Věta 5. 2.
Nechť $f : A \longrightarrow B$ a $g : B \longrightarrow C$ jsou zobrazení. Pak platí:

1. *f, g jsou injektivní zobrazení* $\Rightarrow$ *$g \circ f$ je injektivní zobrazení*
2. *f, g jsou surjektivní zobrazení* $\Rightarrow$ *$g \circ f$ je surjektivní zobrazení*
3. *$g \circ f$ je injektivní zobrazení* $\Rightarrow$ *f je injektivní zobrazení*
4. *$g \circ f$ je surjektivní zobrazení* $\Rightarrow$ *g je surjektivní zobrazení.*

Důkaz.
Jednotlivá tvrzení dokážeme tak, jak bylo popsáno v komentáři k definici injektivního a surjektivního zobrazení.

1. předpokládáme, že f, g jsou injektivní zobrazení a dokazujeme, že $(g \circ f)$ je injektivní zobrazení. Nechť tedy pro prvky $x, y \in A$ platí:
$$(g \circ f)(x) = (g \circ f)(y)\,.$$
Užitím definice složeného zobrazení dostáváme $g(f(x)) = g(f(y))$. Protože však g je injektivní, dostáváme $f(x) = f(y)$, odkud (protože f je injektivní) dostáváme, že $x = y$. Dokázali jsme tak, že zobrazení $(g \circ f)$ je injektivní.

2. Předpokládáme, že f, g jsou surjektivní zobrazení a dokazujeme, že $g \circ f$ je surjektivní zobrazení. Nechť tedy $z \in C$ je libovolný prvek.
Protože g je surjektivní, existuje prvek $y \in B$ tak, že $g(y) = z$. Ale také f je surjektivní, tzn. k prvku $y \in B$ existuje prvek $x \in A$ tak, že $f(x) = y$.
Dohromady pak:
$$z = g(y) = g(f(x)) = (g \circ f)(x)\,,$$
což znamená, že prvek x je vzorem prvku z při zobrazení $(g \circ f)$. Dokázali jsme tak, že zobrazení $g \circ f$ je surjektivní.

3. Předpokládáme, že $(g \circ f)$ je injektivní zobrazení a dokazujeme, že f je injektivní zobrazení. Nechť tedy pro prvky $x, y \in A$ platí:
$$f(x) \;=\; f(y).$$
Potom je jistě také $g(f(x)) = g(f(y))$, neboli $(g \circ f)(x) = (g \circ f)(y)$. Protože však je $(g \circ f)$ injektivní, dostáváme odtud, že $x = y$. Dokázali jsme tak, že zobrazení f je injektivní.

4. Přepokládáme, že $(g \circ f)$ je surjektivní zobrazení a dokazujeme, že g je surjektivní zobrazení. Nechť tedy $z \in C$ je libovolný prvek.
Protože $(g \circ f)$ je surjektivní, musí existovat prvek $x \in A$ takový, že
$$(g \circ f)(x) = z\,, \text{ neboli } \; g(f(x)) = z.$$
To však znamená, že prvek $f(x)$ je hledaným vzorem prvku z při zobrazení g. Dokázali jsme tak, že zobrazení g je surjektivní. ■

Věta 5. 3.
Nechť $f : A \longrightarrow B\,,\ g : B \longrightarrow A$ jsou zobrazení. Pak platí:
$$g \circ f = id_A \ \wedge\ f \circ g = id_B \quad \Leftrightarrow \quad f, g \text{ jsou bijektivní } \wedge\ g = f^{-1}\,.$$

Důkaz.
Implikace "$\Leftarrow$" zřejmě platí. Dokážeme tedy pouze implikaci opačnou.

Důkaz implikace "$\Rightarrow$".
Vzhledem k tomu, že identické zobrazení je bijektivní, tzn. je injektivní i surjektivní, tak z předchozí věty (část 3 a 4) ihned plyne, že f i g jsou bijektivní zobrazení.

Dále, zřejmě je $g : B \longrightarrow A\,,\ \ f^{-1} : B \longrightarrow A$. Zbývá tedy dokázat rovnost příslušných předpisů. Nechť tedy $y \in B$ libovolný. Ale f je bijektivní, tzn. existuje jediný prvek

$x \in A$ s vlastností $f(x) = y$. Pak ale

$$f^{-1}(y) \;=\; x \;=\; id_A(x) \;=\; (g \circ f)(x) \;=\; g(f(x)) \;=\; g(y)\,.$$

Dokázali jsme tedy, že $g = f^{-1}$. ■

Poznamenejme, že v předchozí větě k tomu, aby $g = f^{-1}$ nestačí platnost pouze jedné z uvedených rovností $g \circ f = id_A$ nebo $f \circ g = id_B$, jak by se snad na první pohled mohlo zdát. Ukažme si to na následujícím příkladu.

Příklad 5. 3.
Nechť $f : \mathbb{N} \longrightarrow \mathbb{N}$, resp. $g : \mathbb{N} \longrightarrow \mathbb{N}$ jsou zobrazení, definovaná takto:

$$f(x) = x + 1 \quad \text{pro } \forall\, x \in \mathbb{N} \qquad \text{resp.} \qquad g(x) = \begin{cases} 1 & \text{pro } \; x = 1 \\ x - 1 & \text{pro } \; x \geq 2 \end{cases}$$

(zkuste si nejprve obě zobrazení schematicky nakreslit!). Zřejmě platí:

$$g \circ f \;=\; id_{\mathbb{N}}$$

protože $(g \circ f)(x) = g(f(x)) = g(x + 1) = (x + 1) - 1 = x$.

Přitom však zobrazení f není surjektivní (neboť číslo 1 nemá při zobrazení f žádný vzor) a zobrazení g není injektivní (neboť $g(1) = g(2)$). Vidíme tedy, že k zobrazením f, g inverzní zobrazení vůbec neexistují.

Na závěr kapitoly o zobrazeních uvedeme některé základní úvahy týkající se porovnávání množin, zejména nekonečných. Půjde především o to, abychom se oprostili od představy, kterou si nevědomky přinášíme již ze základní školy, a sice, že počet prvků množiny je číslo. Provedeme přitom nejjednodušší klasifikaci nekonečných množin na množiny spočetné a nespočetné. Navíc uvidíme, že není možné automaticky přenášet všechny vžité (a správné!) představy o konečných množinách na množiny nekonečné.

Definice.
Nechť A, B jsou množiny. Jestliže existuje bijektivní zobrazení $f : A \longrightarrow B$, pak říkáme, že **množiny** A, B **jsou ekvivalentní** nebo též, že **množiny** A, B **mají stejnou mohutnost** a píšeme $A \sim B$.

Věta 5.4.
Nechť A, B, C jsou libovolné množiny. Pak platí:

1. $A \sim A$
2. $A \sim B \implies B \sim A$
3. $A \sim B \;\wedge\; B \sim C \implies A \sim C$

Důkaz.

1. Identické zobrazení $id_A : A \longrightarrow A$ je vždy bijektivní, tzn. vždy platí $A \sim A$.
2. Nechť $A \sim B$, tzn. existuje bijektivní zobrazení $f : A \longrightarrow B$. Potom však existuje inverzní zobrazení $f^{-1} : B \longrightarrow A$, které je také bijektivní, a tedy $B \sim A$.

3. Nechť $A \sim B \wedge B \sim C$, tzn. existují bijektivní zobrazení $f : A \longrightarrow B$ a $g : B \longrightarrow C$. Potom podle věty 5.2 (část 1 a 2) je složené zobrazení $(g \circ f) : A \longrightarrow C$ také bijektivní, což znamená, že je $A \sim C$.

Příklad 5.4.

1. Dvě konečné množiny mají stejnou mohutnost, právě když mají stejný počet prvků.

2. Množiny $\mathbb{N}$ a $\mathbb{Z}$ mají stejnou mohutnost.
   To dokážeme tak, že sestrojíme nějaké bijektivní zobrazení mezi těmito dvěma množinami. Například zobrazení z příkladu 5.1.2, tzn.

$$f : \mathbb{Z} \longrightarrow \mathbb{N} \qquad \text{definované předpisem} \qquad f(x) \;=\; \begin{cases} 2x+1 & \text{pro } \; x \geq 0 \\ -2x & \text{pro } \; x < 0 \end{cases}$$

   je bijektivní.

3. Množiny $\mathbb{Z}$ a $\mathbb{Q}$ mají stejnou mohutnost.
   Stručně popíšeme princip, jak se sestrojí bijektivní zobrazení mezi množinami $\mathbb{Q}$ a $\mathbb{Z}$. Toto zobrazení budeme konstruovat postupně. Nejprve zobrazíme bijektivně kladná racionální čísla na kladná celá čísla takto: napíšeme kladná racionální čísla, vyjádřená v základním tvaru, do řádků tak, že do 1. řádku napíšeme postupně všechna racionální čísla s čitatelem 1 (a vzrůstajícími jmenovateli), do 2. řádku podobně všechna racionální čísla s čitatelem 2, atd. Vznikne "tabulka" tvaru

$$\begin{array}{cccccc} \frac{1}{1} & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} & \cdots \\ \frac{2}{1} & \frac{2}{3} & \frac{2}{5} & \frac{2}{7} & \cdots \\ \frac{3}{1} & \frac{3}{2} & \frac{3}{4} & \frac{3}{5} & \cdots \end{array}$$

   Vypíšeme-li nyní její prvky po diagonálách, tzn.

$$\tfrac{1}{1}\ ,\ \tfrac{1}{2}\ ,\ \tfrac{2}{1}\ ,\ \tfrac{1}{3}\ ,\ \tfrac{2}{3}\ ,\ \tfrac{3}{1}\ ,\ \tfrac{1}{4}\ ,\ \tfrac{2}{5}\ ,\ \cdots\ ,$$

   seřadíme tím kladná racionální čísla do posloupnosti a dostaneme hledanou bijekci kladných racionálních čísel na kladná celá čísla. Podobným způsobem zobrazíme bijektivně záporná racionální čísla na záporná celá čísla a konečně, nulu zobrazíme na nulu.
   Dohromady pak dostáváme bijektivní zobrazení množiny $\mathbb{Q}$ na množinu $\mathbb{Z}$.

4. Nechť (a, b) je libovolný pevný otevřený interval na reálné ose. Pak platí:
   (a, b) a (c, d) mají stejnou mohutnost pro jakýkoliv otevřený interval (c, d);
   (a, b) a $\mathbb{R}^+$ mají stejnou mohutnost (kde $\mathbb{R}^+$ značí množinu kladných reálných čísel);
   (a, b) a $\mathbb{R}$ mají stejnou mohutnost.

   Tato tvrzení dokážeme uvedením příslušných bijektivních zobrazení. Dokažte si sami, že následující zobrazení jsou skutečně bijektivní.

$$f : (a, b) \longrightarrow (c, d) \qquad \text{kde} \quad f(x) = c + \frac{d-c}{b-a} \cdot (x - a)$$

$$f : (a,b) \longrightarrow \mathbb{R}^+ \qquad \text{kde} \quad f(x) = \frac{x-a}{b-x}$$

$$f : (a,b) \longrightarrow \mathbb{R} \qquad \text{kde} \quad f(x) = \begin{cases} \dfrac{x-p}{x-a} & \text{pro } a < x \leq p \\ \dfrac{x-p}{b-x} & \text{pro } p \leq x < b \end{cases}$$

přičemž p je libovolné pevné reálné číslo takové, že $a < p < b$.

5. Nechť (a,b) je libovolný pevný otevřený interval na reálné ose. Pak platí, že intervaly (a,b), $\langle a,b)$, $(a,b\rangle$, $\langle a,b\rangle$ mají stejnou mohutnost.

   Vzhledem k 4. bude zřejmě stačit, když sestrojíme bijekci mezi $(0,1\rangle$ a $(0,1)$. Ale zobrazení:

   $$f : (0,1\rangle \longrightarrow (0,1) \qquad \text{definované} \qquad f(x) \;=\; \begin{cases} \frac{1}{x+1} & \text{pro } \; x = 1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots \\ x & \text{jinak} \end{cases}$$

   je bijektivní (nakreslete si sami schematický obrázek a dokažte).

   Zbývající bijekce mezi intervaly $\langle 0,1)$ a $(0,1)$, resp mezi intervaly $\langle 0,1\rangle$ a $(0,1)$ se sestrojí podobným způsobem.

6. Množiny $\mathbb{N}$ a $\mathbb{R}$ **nemají** stejnou mohutnost.
   Vzhledem ke 4. stačí dokázat, že reálný interval $(0,1)$ a množina $\mathbb{N}$ nemají stejnou mohutnost. Budeme postupovat sporem. Předpokládáme tedy, že interval $(0,1)$ a množina $\mathbb{N}$ mají stejnou mohutnost, tzn. prvky intervalu $(0,1)$ je možné seřadit do posloupnosti. Tedy:

   $$(0,1) \;=\; \{a_1, a_2, a_3, \ldots, a_n, \ldots\}\,.$$

   Každé číslo a_i má přitom dekadický zápis

   $$a_i \;=\; \sum_{k=1}^{\infty} a_{ik} \cdot 10^{-k} \;=\; 0\,,\, a_{i1}\, a_{i2}\, a_{i3}\, \ldots$$

   Pokud má číslo a_i dva různé dekadické zápisy, pak vybereme nekonečný zápis, tj. takový, že pro nekonečně mnoho k je $a_{ik} \neq 0$. V této souvislosti připomeňme, že dekadický zápis reálného čísla je jednoznačný, až na jednu výjimku, a sice nekonečný periodický zápis s periodou obsahující samé devítky představuje totéž racionální číslo, jako konečný dekadický zápis, který dostaneme z předchozího tak, že vynecháme periodu $\overline{9}$ a zvětšíme předchozí cifru o jedničku. Například tedy 0,2499999... a 0,25 jsou dva zápisy téhož (racionálního) čísla.

   Čísla a_i vyjádřená dekadicky zapíšeme do následující tabulky:

   $$\begin{array}{lcl} a_1 & = & 0\;,\; a_{11}\;\; a_{12}\;\; a_{13}\;\; \ldots\;\; a_{1n}\;\; \ldots \\ a_2 & = & 0\;,\; a_{21}\;\; a_{22}\;\; a_{23}\;\; \ldots\;\; a_{2n}\;\; \ldots \\ \vdots & & \\ a_n & = & 0\;,\; a_{n1}\;\; a_{n2}\;\; a_{n3}\;\; \ldots\;\; a_{nn}\;\; \ldots \\ \vdots & & \end{array}$$

Nyní sestrojíme číslo b, mající dekadický zápis $b = 0, b_1\, b_2\, b_3 \ldots b_n \ldots$ takto: položíme

$$b_k = \begin{cases} 1 & \text{je-li } a_{kk} \neq 1 \\ 2 & \text{je-li } a_{kk} = 1 \end{cases} \qquad \text{pro } k = 1, 2, 3, \ldots .$$

Potom číslo b patří do intervalu $(0, 1)$, což znamená, že je rovno některému z čísel $a_1, a_2, a_3, \ldots, a_n, \ldots$, například $b = a_s$. Musí tedy (mimo jiné) být $a_{ss} = b_s$. Ale číslo b bylo sestrojené tak, že pro každé k je $b_k \neq a_{kk}$ a specielně tedy také $b_s \neq a_{ss}$. Dostáváme tak hledaný spor.

K předchozímu důkazu provedenému v příkladu 5.4.6. poznamenejme, že jeho základní myšlenku objevil německý matematik Georg Cantor (1845 - 1918) koncem 19. století. Uvedená metoda se proto také nazývá "Cantorova diagonální metoda".

Definice.
Množina, která má stejnou mohutnost jako množina $\mathbb{N}$ všech přirozených čísel, se nazývá **spočetná množina**. Nekonečná množina, která není spočetná, se nazývá **nespočetná množina**.

Věta 5.5.
1. *Množiny* $\mathbb{N}$, $\mathbb{Z}$ *a* $\mathbb{Q}$ *jsou spočetné množiny.*
2. *Libovolný reálný interval a množiny* $\mathbb{R}^+$ *a* $\mathbb{R}$ *jsou nespočetné množiny.*

Důkaz.
Obě tvrzení ihned vyplývají z úvah, které jsme provedli v předchozím příkladu. ■

Věta 5.6.
Množiny A *a* 2^A *nikdy nemají stejnou mohutnost.*

Důkaz.
Důkaz provedeme sporem. Předpokládejme tedy, že množiny A a 2^A mají stejnou mohutnost, tzn. existuje bijektivní zobrazení $f : A \longrightarrow 2^A$. Označme pak

$$Y = \{a \in A \mid a \notin f(a)\}.$$

Vidíme, že Y je podmnožina v A, tzn. jinak řečeno, $Y \in 2^A$. Protože však f je bijekce, musí existovat (dokonce jediný) prvek $u \in A$ tak, že $f(u) = Y$. Pro prvek u však mohou nastat dvě možnosti:

1. $u \in Y$, odkud plyne, že $u \notin f(u) = Y$, což je spor
2. $u \notin Y$, odkud plyne, že $u \in f(u) = Y$, což je opět spor.

Dohromady tedy dostáváme spor, což znamená, že věta platí. ■

Důsledek.
Jestliže množina A *je spočetná, potom množina* 2^A *je nespočetná.*

Důkaz.
Nechť A je spočetná množina. Pak A je nekonečná množina a 2^A je tedy také nekonečná množina. Z věty 5.6 pak ihned plyne, že 2^A je nespočetná množina. ■

Poznámka.
Podrobnějšími úvahami o mohutnosti množin (a nejen o ní) se bude později zabývat speciální kurz z teorie množin. Jenom pro ilustraci uveďme bez důkazu několik zajímavých tvrzení o konečných, spočetných a nespočetných množinách. Například platí, že:

1. Množina A je konečná, právě když každá její vlastní podmnožina má jinou mohutnost než A.
2. Je-li I konečná nebo spočetná indexová množina a pro každé $i \in I$ je A_i konečná nebo spočetná množina, potom $\bigcup_{i \in I} A_i$ je konečná nebo spočetná množina.
3. Kartézský součin konečného počtu spočetných množin je spočetná množina.
4. Je-li A nespočetná množina a $A \subseteq B$, pak B je také nespočetná množina.

Z předchozí poznámky mimo jiné bezprostředně vyplývají důležité poznatky o iracionálních a komplexních číslech, které uvedeme v následující větě.

Věta 5.7.
Množina všech iracionálních čísel a množina všech komplexních čísel jsou nespočetné množiny.

Důkaz.
Označme symbolem $\mathbb{I}$ množinu všech iracionálních čísel. Pak zřejmě

$$\mathbb{R} = \mathbb{Q} \cup \mathbb{I}\,.$$

Množina racionálních čísel $\mathbb{Q}$ je spočetná a pokud by množina $\mathbb{I}$ byla konečná nebo spočetná, potom by podle 2. části předchozí poznámky musela být množina $\mathbb{Q} \cup \mathbb{I} = \mathbb{R}$ spočetná, což však není. Množina $\mathbb{I}$ je tedy nespočetná.

Dále, množina $A = \{(r, 0) \mid r \in \mathbb{R}\}$ má zřejmě stejnou mohutnost jako množina $\mathbb{R}$ (proč?), tzn. je nespočetná. Protože je $A \subseteq \mathbb{C}$, pak podle 4. části předchozí poznámky je množina všech komplexních čísel $\mathbb{C}$ nepočetná. ■

6. Relace.

Definice.
Nechť A, B jsou množiny. Pak libovolná podmnožina ϱ kartézského součinu $A \times B$ se nazývá **relace mezi množinami** A a B. Je-li $(x, y) \in \varrho$, pak říkáme, že prvek x je v relaci ϱ s prvkem y. Naopak, jestliže $(x, y) \notin \varrho$, pak říkáme, že prvek x není v relaci ϱ s prvkem y.

Z definice je především vidět, že v ní záleží na pořadí množin A, B. Jinak řečeno, relace mezi množinami A, B je něco jiného, než relace mezi množinami B, A. Dále, je zřejmé, že relace mezi množinami je opět množina. Je třeba si pouze zvyknout na to, že se v tomto případě k označení množiny obvykle používá malé řecké písmeno. Jakékoliv úvahy o relacích jsou tedy úvahami o množinách. Například při důkazu rovnosti dvou relací mezi množinami postupujeme stejně jako při důkazu jakékoliv jiné rovnosti dvou množin, tzn. obvykle pomocí důkazu dvou množinových inkluzí.

Definovat relaci ϱ mezi množinami A, B znamená popsat jistou podmnožinu množiny $A \times B$, tzn. v podstatě jakýmkoliv korektním způsobem jednoznačně určit všechny uspořádané dvojice z $A \times B$, které patří do ϱ. Následuje několik příkladů relací mezi množinami.

Příklad 6. 1.

1. Nechť $A = \{a, b, c, d\}$, $B = \{x, y, z\}$. Pak

$$\varrho \;=\; \{(a, y), (c, y), (c, z)\}$$

   je relací mezi množinami A, B.

2. Nechť $A = \mathbb{N}$, $B = \mathbb{N}$. Pak

$$\varrho = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid y - x \text{ je kladné číslo}\}$$

   je relací mezi množinami A, B. Je zřejmé, že v tomto případě je číslo x v relaci ϱ s číslem y právě tehdy, když x je menší než y (při běžném uspořádání čísel podle velikosti).

3. Nechť A, B jsou libovolné množiny. Uvedeme dva speciální případy relací mezi množinami A, B:

   a) prázdná množina je zřejmě podmnožinou $A \times B$, a tedy $\varrho = \emptyset$ je relací mezi množinami A, B, kterou budeme nazývat **prázdná relace** mezi A, B. Je to tedy taková relace, kdy žádný prvek z A není v relaci s žádným prvkem z B.

   b) druhým speciálním případem podmnožiny $A \times B$ je množina $A \times B$ samotná. Tedy $\varrho = A \times B$ je také relací mezi množinami A, B, kterou budeme nazývat **univerzální relace** mezi A, B. Je to taková relace, kdy každý prvek z množiny A je v relaci s každým prvkem z množiny B.

Připomeňme, že definice relace mezi množinami A, B nevylučuje případ, že některá z množin A, B je prázdná. Je-li $A = \emptyset$ nebo $B = \emptyset$, pak je zřejmě $A \times B = \emptyset$, odkud plyne, že jedinou možnou relací mezi množinami A, B je v tomto případě prázdná relace.

Poznámka.
Pojem zobrazení, který jsme dříve zavedli ne zcela přesným způsobem, by bylo možné nyní naprosto korektně a přesně definovat pomocí relací takto:

Nechť A, B jsou množiny a nechť f je relace mezi množinami A, B, splňující podmínku:

ke každému $x \in A$ existuje jediné $y \in B$ tak, že $(x, y) \in f$.

Pak uspořádanou trojici (A, B, f) nazýváme zobrazením množiny A do množiny B.

Vidíme, že v této definici není použit problematický pojem "předpis", a proto není například nutné zvlášť popisovat rovnost dvou zobrazení. Na druhé straně, úvahy o zobrazeních v této podobě by byly formálně komplikované a nepřehledné. Proto nadále budeme pracovat s pojmem zobrazení tak, jak byl původně zaveden.

Definice.
Nechť ϱ je relace mezi množinami A, B a nechť σ je relace mezi množinami B, C. Pak relace

$$\sigma \circ \varrho \;=\; \{(x, y) \in A \times C \mid \exists\, b \in B \text{ tak, že } (x, b) \in \varrho \wedge (b, y) \in \sigma\}$$

se nazývá **složená relace** z relací ϱ a σ (v tomto pořadí).

Symbol $\sigma \circ \varrho$ pro složenou relaci čteme buď "σ kolečko ϱ" nebo "σ po ϱ". Ilustrujme si skládání relací na jednoduchém konkrétním příkladu.

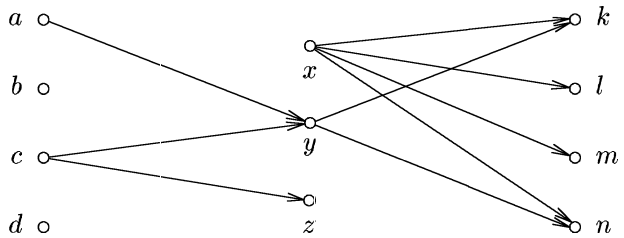
Příklad 6. 2.
Nechť $A = \{a, b, c, d\}$, $B = \{x, y, z\}$, $C = \{k, l, m, n\}$ a nechť je dána relace ϱ mezi množinami A, B a relace σ mezi množinami B, C takto:

$$\varrho = \{(a, y), (c, y), (c, z)\} \qquad \sigma = \{(x, k), (x, l), (x, m), (x, n), (y, k), (y, n)\}\,.$$

Potom z definice složené relace ihned plyne, že $\sigma \circ \varrho \;=\; \{(a, k), (a, n), (c, k), (c, n)\}$.

Poznámka.
Pro větší názornost si můžeme relace mezi množinami znázorňovat graficky, zejména jsou-li množiny konečné. Je-li například ϱ relací mezi množinami A, B , pak si znázorníme prvky obou množin jako body v rovině a bod $r \in A$ spojíme orientovanou šipkou s bodem $s \in B$ právě tehdy, když $(r, s) \in \varrho$. Výsledný obrázek budeme nazývat **graf relace** ϱ .

Pro relace ϱ, σ z předchozího příkladu tak dostáváme následující grafy:



Pomocí grafů si můžeme schematicky znázornit i další pojmy, jako například skládání

relací. Je zřejmé, že při relaci $\sigma \circ \varrho$ vede orientovaná šipka z bodu $r \in A$ do bodu $t \in C$, právě když tuto šipku lze "složit" ze šipky patřící do grafu relace ϱ, začínající v bodu r, a šipky patřící do grafu relace σ, končící v bodu t, přičemž obě šipky mají společný bod v množině B.

Věta 6.1.
Nechť ϱ je relace mezi množinami A, B, σ je relace mezi množinami B, C, a τ je relace mezi množinami C, D. Pak platí:

$$\tau \circ (\sigma \circ \varrho) \;=\; (\tau \circ \sigma) \circ \varrho \,.$$

Důkaz.
Je zřejmé, že $\tau \circ (\sigma \circ \varrho)$ i $(\tau \circ \sigma) \circ \varrho$ jsou relace mezi množinami A, D. Jejich rovnost dokazujeme jako množinovou rovnost.

"$\subseteq$" nechť $(x, y) \in \tau \circ (\sigma \circ \varrho)$ libovolné. Pak podle definice složené relace existuje $c \in C$ tak, že $(x, c) \in \sigma \circ \varrho \;\wedge\; (c, y) \in \tau$. Dále existuje $b \in B$ tak, že $(x, b) \in \varrho \wedge (b, c) \in \sigma$. Nyní opět užitím definice složené relace dostáváme, že $(b, y) \in \tau \circ \sigma$ a následně pak $(x, y) \in (\tau \circ \sigma) \circ \varrho$. Dohromady tak dostáváme, že $\tau \circ (\sigma \circ \varrho) \subseteq (\tau \circ \sigma) \circ \varrho$.

"$\supseteq$" inkluze $(\tau \circ \sigma) \circ \varrho \subseteq \tau \circ (\sigma \circ \varrho)$ se dokáže analogickým způsobem. ■

Definice.
Nechť ϱ je libovolná relace mezi množinami A, B. Potom relace ϱ^{-1} mezi množinami B, A, definovaná vztahem:

$$\varrho^{-1} \;=\; \{(u, v) \in B \times A \mid (v, u) \in \varrho\}$$

se nazývá **inverzní relace k relaci** ϱ.

Z definice inverzní relace okamžitě vyplývá, že $(u, v) \in \varrho^{-1}$ právě tehdy, když je $(v, u) \in \varrho$. Znázorníme-li si relaci ϱ grafem, pak zřejmě graf relace ϱ^{-1} získáme tak, že vezmeme původní graf relace ϱ a v něm pouze změníme orientaci všech šipek.

Věta 6.2.
Nechť ϱ je relace mezi množinami A, B a σ je relace mezi množinami B, C. Potom platí:

1. $(\varrho^{-1})^{-1} \;=\; \varrho$
2. $(\sigma \circ \varrho)^{-1} \;=\; \varrho^{-1} \circ \sigma^{-1}$.

Důkaz.
1. dokazovaná rovnost okamžitě vyplývá z definice inverzní relace.
2. zřejmě $(\sigma \circ \varrho)^{-1}$ i $\varrho^{-1} \circ \sigma^{-1}$ jsou relace mezi množinami C, A. Jejich rovnost tedy dokazujeme jako množinovou rovnost.

"$\subseteq$" nechť $(u, v) \in (\sigma \circ \varrho)^{-1}$. Podle definice inverzní relace je pak $(v, u) \in \sigma \circ \varrho$ a dále, podle definice složené relace existuje $b \in B$ tak, že $(v, b) \in \varrho \;\wedge\; (b, u) \in \sigma$. Potom však $(b, v) \in \varrho^{-1} \;\wedge\; (u, b) \in \sigma^{-1}$, odkud pak podle definice složené relace dostáváme $(u, v) \in \varrho^{-1} \circ \sigma^{-1}$. Dohromady tedy: $(\sigma \circ \varrho)^{-1} \subseteq \varrho^{-1} \circ \sigma^{-1}$.

"$\supseteq$" inkluze $\varrho^{-1} \circ \sigma^{-1} \subseteq (\sigma \circ \varrho)^{-1}$ se dokáže analogickým způsobem. ■

Na závěr této kapitoly se budeme nyní zabývat speciálním, ale v praxi se často vyskytujícím typem relace mezi množinami A, B, a sice případem, kdy $A = B \neq \emptyset$.

Definice.
Nechť M je neprázdná množina. Pak libovolná podmnožina ϱ kartézského součinu $M \times M$ se nazývá **relace na množině** M. Množinu M spolu s relací ϱ budeme označovat symbolem (M, ϱ) a budeme říkat, že (M, ϱ) je množina s relací.
Pro $x, y \in M$ budeme místo $(x, y) \in \varrho$ psát obvykle $x \varrho y$, resp. místo $(x, y) \notin \varrho$ budeme psát $x \overline{\varrho} y$.

Příklad 6. 3.

1. Nechť $M = \{a, b, c, d\}$ a nechť například $\varrho = \{(a, b), (b, a), (b, b), (b, c)\}$. Potom ϱ je relace na množině M.
2. Nechť M je libovolná neprázdná množina. Pak
   a) prázdná relace $\varrho = \emptyset$ je relací na množině M.
   b) univerzální relace $\varrho = M \times M$ je relací na množině M.
   c) množina $\{(x, x) \mid x \in M \text{ libovolné}\}$ je relací na množině M, kterou nazýváme **relace rovnosti** a označujeme symbolem ι (řecké písmeno jota).
3. Nechť $M = 2^A$, kde A je libovolná množina. Potom množina
   $$\{(X, Y) \mid X, Y \in 2^A \wedge X \subseteq Y\}$$
   je relací na množině 2^A, kterou nazýváme **relace inkluze** a obvykle ji označujeme symbolem $\subseteq$.
4. Nechť $M = \mathbb{N}$ je množina všech přirozených čísel. Pak množina
   $$\{(a, b) \mid a, b \in \mathbb{N} \wedge a \text{ dělí } b\}$$
   je relací na množině $\mathbb{N}$, kterou nazýváme **relace dělitelnosti** (na množině přirozených čísel) a obvykle ji označujeme symbolem $|$. Zdůrazněme, že dělitelnost je v tomto případě chápána jako dělitelnost v oboru přirozených čísel, tzn. obrat "a dělí b" znamená: "existuje $x \in \mathbb{N}$ tak, že platí $b = a \cdot x$".
5. Nechť $M = \mathbb{Z}$ je množina všech celých čísel a nechť m je pevné přirozené číslo. Pak množina
   $$\{(a, b) \mid a, b \in \mathbb{Z} \wedge a \equiv b \pmod{m}\}$$
   je relací na množině všech celých čísel $\mathbb{Z}$, kterou nazýváme **relace kongruence podle modulu** m.

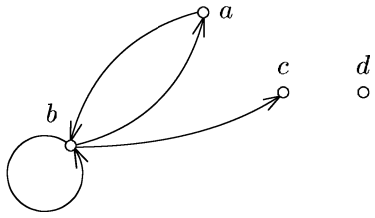
Poznámka.
Schematické znázorňování relací na množině (zejména, je-li množina konečná) můžeme provést obrázkem, podobně jako u relací mezi množinami. Jestliže je tedy (M, ϱ) množina s relací, pak prvky množiny M znázorníme jako body v rovině a z bodu x

nakreslíme orientovanou šipku do bodu y právě tehdy, když $x \varrho y$. Přitom je samozřejmě možné, že šipka začíná a končí ve stejném bodu. Taková šipka se nazývá smyčka. Vzniklý obrázek budeme nazývat **uzlový graf relace** ϱ.

Relaci ϱ na konečné množině M je možné také vyjádřit pomocí tabulky, kterou sestrojíme následujícím způsobem: do záhlaví řádků a sloupců vypíšeme prvky množiny M, a to ve stejném pořadí. Do průsečíku řádku označeného x a sloupce označeného y pak napíšeme jedničku, je-li $x \varrho y$, resp. napíšeme nulu, je-li $x \overline{\varrho} y$.

Oba způsoby vyjádření relací si ukažme na relaci z příkladu 6. 3. 1., tzn. je-li

$$M = \{a, b, c, d\} \qquad \text{a} \qquad \varrho = \{(a, b), (b, a), (b, b), (b, c)\}.$$



	a	b	c	d
a	0	1	0	0
b	1	1	1	0
c	0	0	0	0
d	0	0	0	0

Později uvidíme, že některé speciální typy relací na množině je výhodné znázorňovat i jiným způsobem. Nyní si však nejprve popíšeme základní vlastnosti relací na množině.

Definice.
Nechť (M, ϱ) je množina s relací. Řekneme, že relace ϱ je

1. **reflexivní**, jestliže: $x \in M$ libovolný $\Rightarrow$ $x \varrho x$
2. **symetrická**, jestliže: $x, y \in M \ \wedge \ x \varrho y \ \Rightarrow \ y \varrho x$
3. **antisymetrická**, jestliže: $x, y \in M \ \wedge \ x \varrho y \ \wedge \ y \varrho x \ \Rightarrow \ x = y$
4. **tranzitivní**, jestliže: $x, y, z \in M \ \wedge \ x \varrho y \ \wedge \ y \varrho z \ \Rightarrow \ x \varrho z$
5. **úplná**, jestliže: $x, y \in M$ libovolné $\Rightarrow \ x \varrho y \ \vee \ y \varrho x$.

Poznámka.
Předchozí definice bude hrát v úvahách o relacích na množině zásadní roli, a proto je nutné ji dobře pochopit a bezpečně zvládnout. Ukažme si ještě, jak se poznají výše definované vlastnosti relací (kromě tranzitivity, kde je situace složitější) z uzlového grafu (viz a)) a z tabulky relace (viz b)):

reflexivnost: a) každý bod je opatřen smyčkou
b) v hlavní diagonále tabulky jsou samé jedničky

symetrie: a) mezi dvěma různými body jsou buď dvě šipky nebo žádná šipka
b) tabulka je symetrická podle hlavní diagonály

antisymetrie: a) mezi dvěma různými body je buď jedna nebo žádná šipka
b) dvě různá políčka symetrická podle hlavní diagonály obsahují nejvýše jednu jedničku

úplnost: a) každý bod je opatřen smyčkou a každé dva různé body jsou spojeny (alespoň jednou) šipkou
b) v hlavní diagonále jsou samé jedničky a dvě různá políčka symetrická podle hlavní diagonály obsahují alespoň jednu jedničku

Jinou charakterizaci základních typů relací na množině uvádí následující věta.

Věta 6. 3.
Nechť (M, ϱ) *je množina s relací. Pak platí:*

1. *relace* ϱ *je reflexivní* $\Leftrightarrow \quad \iota \subseteq \varrho$ *(kde* ι *značí relaci rovnosti na* M*)*
2. *relace* ϱ *je symetrická* $\Leftrightarrow \quad \varrho \subseteq \varrho^{-1}$
3. *relace* ϱ *je antisymetrická* $\Leftrightarrow \quad \varrho \cap \varrho^{-1} \subseteq \iota$
4. *relace* ϱ *je tranzitivní* $\Leftrightarrow \quad \varrho \circ \varrho \subseteq \varrho$
5. *relace* ϱ *je úplná* $\Leftrightarrow \quad \varrho \cup \varrho^{-1} = M \times M$.

Důkaz.
1. tvrzení zřejmě platí.
2. *Důkaz implikace* "$\Rightarrow$".
Nechť ϱ je symetrická relace na M. Dokážeme, že $\varrho \subseteq \varrho^{-1}$. Nechť $(x, y) \in \varrho$ libovolné, tzn. $x \varrho y$. Podle předpokladu je ale $y \varrho x$, neboli $(y, x) \in \varrho$ odkud dostáváme $(x, y) \in \varrho^{-1}$. Platí tedy: $\varrho \subseteq \varrho^{-1}$.

   Důkaz implikace "$\Leftarrow$".
Předpokládejme, že $\varrho \subseteq \varrho^{-1}$. Nechť $x \varrho y$, tzn. $(x, y) \in \varrho$. Podle předpokladu je ale $(x, y) \in \varrho^{-1}$, neboli $(y, x) \in \varrho$. Tedy $y \varrho x$ a relace ϱ je symetrická.
3. *Důkaz implikace* "$\Rightarrow$".
Nechť ϱ je antisymetrická relace na M a nechť $(x, y) \in \varrho \cap \varrho^{-1}$ libovolné, tzn. platí $x \varrho y \ \wedge \ y \varrho x$. Ale ϱ je antisymetrická, a tedy $x = y$, neboli $(x, y) \in \iota$. Dostáváme tak, že $\varrho \cap \varrho^{-1} \subseteq \iota$.

   Důkaz implikace "$\Leftarrow$".
Nechť $\varrho \cap \varrho^{-1} \subseteq \iota$ a nechť je $x \varrho y \wedge y \varrho x$. To ale znamená, že $(x, y) \in \varrho \cap \varrho^{-1}$, a podle předpokladu je tedy $(x, y) \in \iota$, neboli $x = y$. Dokázali jsme tedy, že relace ϱ je antisymetrická.
4. *Důkaz implikace* "$\Rightarrow$".
Nechť relace ϱ je tranzitivní a nechť $(x, y) \in \varrho \circ \varrho$ libovolné. Pak podle definice složené relace existuje prvek $u \in M$ tak, že $x \varrho u \wedge u \varrho y$. Z tranzitivnosti relace ϱ pak plyne, že $x \varrho y$, neboli $(x, y) \in \varrho$. Dokázali jsme tak, že $\varrho \circ \varrho \subseteq \varrho$.

   Důkaz implikace "$\Leftarrow$".
Nechť $\varrho \circ \varrho \subseteq \varrho$ a nechť $x \varrho y \wedge y \varrho z$, což znamená, že $(x, y) \in \varrho \wedge (y, z) \in \varrho$. Potom podle definice složené relace je $(x, z) \in \varrho \circ \varrho \subseteq \varrho$, tzn. $x \varrho z$. Tedy relace ϱ je tranzitivní.

5. *Důkaz implikace "⇒".*
Nechť ϱ je úplná relace. Vzhledem k tomu, že jistě platí: $\varrho \cup \varrho^{-1} \subseteq M \times M$, stačí dokázat pouze opačnou inkluzi. Nechť tedy $(x, y) \in M \times M$. Z toho, že relace ϱ je úplná vyplývá, že $x \varrho y \vee y \varrho x$, tzn. $(x, y) \in \varrho \vee (y, x) \in \varrho$. Je tedy $(x, y) \in \varrho \vee (x, y) \in \varrho^{-1}$, což znamená, že $(x, y) \in \varrho \cup \varrho^{-1}$. Dokázali jsme tedy, že $\varrho \cup \varrho^{-1} = M \times M$.

Důkaz implikace "⇐".
Nechť $\varrho \cup \varrho^{-1} = M \times M$. Nechť $x, y \in M$ jsou libovolné prvky. Potom zřejmě $(x, y) \in M \times M = \varrho \cup \varrho^{-1}$, odkud plyne, že $(x, y) \in \varrho \vee (x, y) \in \varrho^{-1}$, a tedy $x \varrho y \vee y \varrho x$. Tím jsme dokázali, že relace ϱ je úplná. ■

K uvedeným vlastnostem relací na množině ještě poznamenejme, že symetričnost a antisymetričnost se navzájem nevylučují (například relace rovnosti na M je zároveň symetrická i antisymetrická). Dále je ještě dobré si uvědomit, že úplná relace musí být vždy reflexivní.

Následující tabulka nám přehledně uvádí, které z výše zavedených vlastností mají či nemají relace z příkladu 6. 3. Je velmi užitečné si každou jednotlivou odpověď podrobně samostatně ověřit. Číslování relací je stejné jako v příkladu 6. 3.

	1	2 a	2b	2 c	3	4	5
reflexivní	ne	ne	ano	ano	ano	ano	ano
symetrická	ne	ano	ano	ano	(∗∗)	ne	ano
antisymetrická	ne	ano	(∗)	ano	ano	ano	ne
tranzitivní	ne	ano	ano	ano	ano	ano	ano
úplná	ne	ne	ano	(∗)	(∗∗∗)	ne	ne

V některých případech závisí uvedené vlastnosti relací na počtu prvků množiny M:
(∗) ano, je-li M jednoprvková množina, jinak ne
(∗∗) ano, je-li A prázdná množina, jinak ne
(∗∗∗) ano, je-li A prázdná nebo jednoprvková množina, jinak ne.

Relace na množině M, tak jak byla v této kapitole definována, se také někdy nazývá "binární relace". Tento pojem je možno zřejmým způsobem zobecnit na pojem tzv. "$n-$ární relace na množině M", která je pak definována jako libovolná podmnožina kartézského součinu $M^n = M \times M \times \ldots \times M$ ($n-$krát), pro libovolné pevné přirozené číslo n. Ve speciálních případech dostáváme:

pro $n = 1$ tzv. unární relaci (což je vlastně libovolná podmnožina množiny M),

pro $n = 2$ tzv. binární relaci, s níž jsme pracovali výše,

pro $n = 3$ tzv. ternární relaci, což je libovolná podmnožina $M \times M \times M$, atd.

7. Uspořádané množiny.

V této a v následující kapitole budeme podrobněji studovat relace na množině, které splňují současně několik z dříve definovaných vlastností relací.

Definice.
Nechť (M, ϱ) je množina s relací, přičemž relace ϱ je reflexivní, antisymetrická a tranzitivní. Pak relace ϱ se nazývá **uspořádání** a (M, ϱ) se nazývá **uspořádaná množina**.
Je-li navíc relace ϱ úplná, pak se ϱ nazývá **lineární uspořádání** a (M, ϱ) se nazývá **lineárně uspořádaná množina** nebo krátce řetězec.

Příklad 7.1.

1. Relace inkluze $\subseteq$ na množině 2^A (tzn. na množině všech podmnožin množiny A) je relací uspořádání.
   Přitom $(2^A, \subseteq)$ je lineárně uspořádaná množina, právě když množina A je prázdná nebo jednoprvková (tzn. právě když množina 2^A má jeden nebo dva prvky).

2. Relace dělitelnosti $|$ na množině všech přirozených čísel $\mathbb{N}$ je relací uspořádání. Přitom $(\mathbb{N}, |)$ není lineárně uspořádaná množina.
   V této souvislosti poznamenejme, že relace dělitelnosti na množině všech celých čísel $\mathbb{Z}$ **není** relací uspořádání, a to proto, že není antisymetrická.

3. Relace uspořádání čísel podle velikosti $\leq$ na množině $\mathbb{N}$ je relací lineárního uspořádání, a tedy $(\mathbb{N}, \leq)$ je lineárně uspořádaná množina.

   Přitom relací "uspořádání čísel podle velikosti" rozumíme relaci $\leq$ definovanou způsobem známým ze střední školy, tzn.

   $$x \leq y \qquad \text{právě když} \qquad y - x \text{ je nezáporné číslo.}$$

   Podobně, relace uspořádání čísel podle velikosti $\leq$ je relací lineárního uspořádání na množině všech celých čísel $\mathbb{Z}$, racionálních čísel $\mathbb{Q}$ a reálných čísel $\mathbb{R}$. Dostáváme tak lineárně uspořádané množiny $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$ a $(\mathbb{R}, \leq)$.

Úmluva.
Libovolnou relaci uspořádání budeme v dalším při obecných úvahách označovat symbolem $\leq$ ("menší nebo rovno") místo symbolu ϱ nebo jiných řeckých písmen. Jedná se o vžitou konvenci vzniklou z toho, že klasickým příkladem relace uspořádání je uspořádání čísel podle velikosti, označované standardně symbolem $\leq$. V této souvislosti je však nutno zdůraznit, že v obecné rovině nebude mít symbol $\leq$ nic společného s uspořádáním čísel podle velikosti. Je-li $\leq$ libovolná relace uspořádání, pak zavedeme další úmluvu, a sice:

$$\text{místo konjunkce} \quad x \leq y \ \wedge \ x \neq y \qquad \text{budeme stručně psát} \qquad x < y$$

a číst "x je menší než y". Modelem pro toto označení je opět stejný symbol používaný na střední škole pro porovnávání čísel podle velikosti, přičemž v našem případě nebude mít zavedený symbol $<$ s čísly opět obecně nic společného. Výhodou tohoto označení je především to, že jediným symbolem označuje konjunkci dvou podmínek.

Poznámka.
Uspořádanou množinu $(M, \leq)$ můžeme (zejména, je-li množina M konečná) znázorňovat graficky. Postupujeme přitom následujícím způsobem:

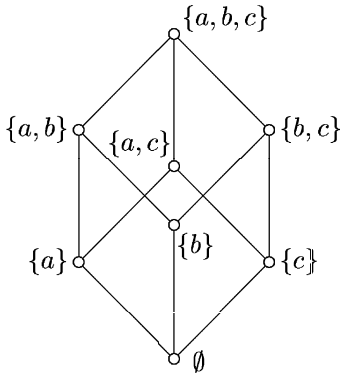
1. prvky množiny M znázorníme jako body v rovině
2. je-li $x < y$ pak bod x nakreslíme níže než bod y
3. dva body x, y spojíme úsečkou právě tehdy, když $x < y$ a neexistuje žádný bod "mezi nimi", tzn. neexistuje $k \in M$ tak, že $x < k \ \wedge \ k < y$.

Výsledný graf se pak nazývá **hasseovský diagram** uspořádané množiny $(M, \leq)$. Je ihned vidět, že se vlastně jedná o zjednodušený uzlový graf relace $\leq$ (jsou vynechány smyčky, které by měly být u každého bodu, dále je vynechána orientace šipek, která je nahrazena umístěním bodu "níže" či "výše" a konečně jsou vynechány "zbytečné" šipky, jejichž existence plyne z tranzitivnosti relace $\leq$).

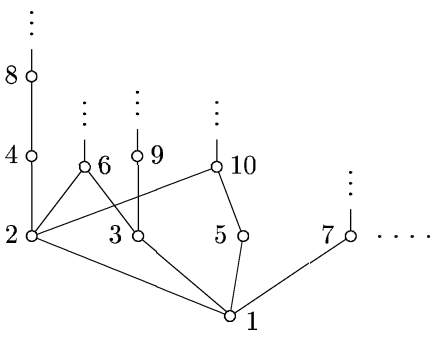
Pro úplnost poznamenejme, že uvedená konstrukce nedefinuje jednoznačně "tvar" hasseovského diagramu. Jednu a tutéž uspořádanou množinu je často možné znázornit hasseovskými diagramy různých tvarů tak, že na první pohled nemusí být vůbec zřejmé, že jde o diagramy téže uspořádané množiny. Na druhé straně, známe-li hasseovský diagram uspořádané množiny, pak z něj lze relaci $\leq$ jednoznačně zpětně zrekonstruovat. Vidíme tedy, že je možné zadávat uspořádanou množinu pomocí jejího hasseovského diagramu.

Příklad 7. 2.

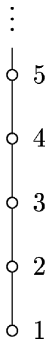
1. Nechť $A = \{a, b, c\}$; potom je $2^A = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$ a hasseovský diagram uspořádané množiny $(2^A, \subseteq)$ je znázorněn na obrázku a).
2. Část hasseovského diagramu uspořádané množiny $(\mathbb{N}, |)$ z příkladu 7. 1. 2 je znázorněna na obrázku b). Zde si uvědomme, že obrázek vlastně nezachycuje správně celou situaci, protože z každého čísla x ve skutečnosti vychází nekonečně mnoho úseček, vedoucích do čísel $x \cdot p$, kde p je libovolné prvočíslo, přičemž prvočísel je, jak víme, nekonečně mnoho.
3. Část hasseovského diagramu uspořádané množiny $(\mathbb{N}, \leq)$ z příkladu 7. 1. 3 (tzn. symbol $\leq$ v tomto případě značí uspořádání přirozených čísel podle velikosti) je znázorněna na obrázku c).



a)



b)



c)

Je jasné, že u nekonečných uspořádaných množin nelze jejich hasseovský diagram nikdy nakreslit celý. Vzniklý obrázek je pak jen více či méně názornou orientační pomůckou a někdy ani nemá smysl se snažit jej nakreslit, jako třeba u uspořádané množiny $(\,2^{\mathbb{R}}, \subseteq\,)$.

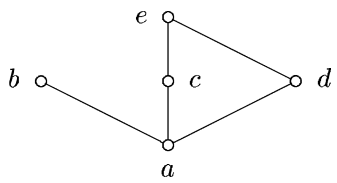
V uspořádaných množinách se mohou vyskytovat jisté "význačné" prvky, které si nyní popíšeme v následující definici.

Definice.
Nechť $(M, \leq)$ je uspořádaná množina. Prvek $a \in M$ se nazývá
nejmenší, jestliže pro každé $x \in M$ platí: $a \leq x$
největší, jestliže pro každé $x \in M$ platí: $x \leq a$
minimální, jestliže neexistuje prvek $x \in M$ s vlastností: $x < a$
maximální, jestliže neexistuje prvek $x \in M$ s vlastností: $a < x$.

Dále, dva prvky $u, v \in M$ se nazývají **srovnatelné**, jestliže platí, že $u \leq v$ nebo $v \leq u$. V opačném případě se prvky u, v nazývají **nesrovnatelné**.

Příklad 7. 3.

1. Nechť uspořádaná množina $(M, \leq)$ je zadána následujícím hasseovským diagramem:



   Potom: nejmenším prvkem této uspořádané množiny je prvek a, největší prvek zde neexistuje, minimálním prvkem je prvek a a maximálními prvky jsou prvky b, e. Dále, nesrovnatelnými prvky jsou dvojice prvků b, c, resp. b, d, resp. b, e, resp. c, d. Všechny ostatní dvojice prvků jsou srovnatelné prvky.

2. U uspořádaných množin z příkladu 7. 2. platí:

   1. nejmenším a zároveň jediným minimálním prvkem je $\emptyset$. Největším a zároveň jediným maximálním prvkem je $\{a, b, c\}$.

   2. nejmenším a zároveň jediným minimálním prvkem je číslo 1, největší ani maximální prvek zde neexistuje – rozmyslete si podrobně, proč tomu tak je.
      Zároveň si zkuste rozmyslet, jak by se situace změnila v případě, že bychom k množině $\mathbb{N}$ přidali číslo nula a relací by byla relace dělitelnosti na této množině všech nezáporných celých čísel.

   3. nejmenším a zároveň jediným minimálním prvkem je číslo 1, největší ani maximální prvek zde neexistuje.

Poznámka.
Ověřujeme-li o nějakém prvku $a \in M$, že je minimálním prvkem uspořádané množiny $(M, \leq)$, pak je obvykle technicky nejvýhodnější postupovat tak, že dokazujeme implikaci:

$$x \in M \quad \wedge \quad x \leq a \qquad \Rightarrow \qquad x = a\,.$$

Podobně, ověřujeme-li, že prvek a je maximálním prvkem uspořádané množiny $(M, \leq)$, pak obvykle dokazujeme implikaci:

$$x \in M \quad \wedge \quad a \leq x \qquad \Rightarrow \qquad x = a\,.$$

Z předchozích příkladů je vidět, že nejmenší, největší, minimální a maximální prvek v uspořádané množině existovat může, ale nemusí. Navíc, minimálních nebo maximálních prvků může v uspořádané množině existovat případně i více. Co všechno v této souvislosti platí, ukazuje následující věta.

Věta 7. 1.
Nechť $(M, \leq)$ je uspořádaná množina. Pak platí:

1. *v uspořádané množině $(M, \leq)$ existuje nejvýše jeden nejmenší prvek a nejvýše jeden největší prvek.*
2. *je-li $a \in M$ nejmenším prvkem, pak je také minimálním prvkem a žádné další minimální prvky v uspořádané množině $(M, \leq)$ neexistují.*
   Podobně, je-li $a \in M$ největším prvkem, pak je také maximálním prvkem a žádné další maximální prvky v uspořádané množině $(M, \leq)$ neexistují.

Důkaz.
Tvrzení věty dokážeme vždy pro nejmenší / minimální prvek. Zbytek obou tvrzení pro největší / maximální prvky se dokáže analogicky.

1. dokazujeme, že v $(M, \leq)$ existuje nejvýše jeden nejmenší prvek. Budeme přitom postupovat tak, že budeme předpokládat existenci dvou nejmenších prvků a dokážeme, že se tyto prvky rovnají.
   Nechť tedy a, b jsou nejmenší prvky v $(M, \leq)$. Potom je $a \leq b$ (protože a je nejmenším prvkem) a zároveň je $b \leq a$ (protože b je nejmenším prvkem). Z antisymetrie relace $\leq$ pak ihned dostáváme, že $a = b$.
2. nechť $a \in M$ je nejmenší prvek. Postupem popsaným v předchozí poznámce dokážeme, že a je minimálním prvkem.
   Nechť tedy $x \in M \ \wedge \ x \leq a$. Ale a je podle předpokladu nejmenší prvek, tzn. musí platit $a \leq x$. Z antisymetrie relace $\leq$ pak dostáváme, že $x = a$. Tedy a je minimální prvek.
   Zbývá dokázat, že žádné další minimální prvky různé od a už v $(M, \leq)$ neexistují. Nechť tedy $y \in M$ je libovolný minimální prvek.
   Prvek a je podle předpokladu nejmenším prvkem, tzn. musí platit, že $a \leq y$, odkud již plyne (vzhledem k tomu, že y je minimální prvek), že $y = a$. ■

Poznámka.
Upozorněme ještě jednou na typickou úvahu použitou v 1. části důkazu předchozí věty, kde jsme dokazovali, že nejmenší prvek v uspořádané množině existuje nejvýše jeden. Jestliže v matematice dokazujeme, že něčeho existuje nejvýše jeden exemplář, pak obvykle postupujeme tak, že předpokládáme existenci dvou exemplářů a následně o nich dokážeme, že se sobě rovnají.

Věta 7. 2.
Uspořádaná množina $(M, \leq)$ je lineárně uspořádaná právě když jsou každé dva prvky množiny M srovnatelné.

Důkaz.
Tvrzení plyne ihned z definice lineárně uspořádané množiny a z definice srovnatelných prvků. ■

Věta 7. 3.
Nechť $(M, \leq)$ je lineárně uspořádaná množina. Potom platí:

1. *prvek $a \in M$ je minimální, právě když je nejmenší*
2. *prvek $a \in M$ je maximální, právě když je největší.*

Důkaz.
Tvrzení dokážeme pro minimální a nejmenší prvek. Pro maximální a největší prvek se důkaz provede analogicky.

Důkaz implikace "$\Rightarrow$".
Nechť a je minimální prvek a nechť $x \in M$ je libovolný prvek. Podle předpokladu je $(M, \leq)$ lineárně uspořádaná množina, tzn. musí být $a \leq x$ nebo $x \leq a$. Ale z $x \leq a$ plyne, že $x = a$ (protože prvek a je minimální), neboli $a \leq x$. Vždy tedy platí $a \leq x$, což znamená, že prvek a je nejmenším prvkem.

Důkaz implikace "$\Leftarrow$".
Tato implikace ihned plyne z 2. části věty 7.1. ■

Na závěr kapitoly o uspořádaných množinách zavedeme nejprve pro libovolnou uspořádanou množinu pojmy suprema a infima nějaké její podmnožiny a následně pak rozebereme jejich základní vlastnosti. Uvedené pojmy najdou uplatnění v dalších matematických disciplinách.

Definice.
Nechť $(M, \leq)$ je uspořádaná množina, nechť A je libovolná podmnožina v M a nechť $c \in M$. Prvek c se nazývá

- **dolní závora množiny** A, jestliže pro libovolné $x \in A$ platí $c \leq x$
- **horní závora množiny** A, jestliže pro libovolné $x \in A$ platí $x \leq c$
- **infimum množiny** A (v množině M), jestliže c je největší dolní závora množiny A; píšeme pak $c = \inf_M A$ nebo jenom stručně $c = \inf A$
- **supremum množiny** A (v množině M), jestliže c je nejmenší horní závora množiny A; píšeme pak $c = \sup_M A$ nebo jenom stručně $c = \sup A$.

Poznámka.
Obrat "c je největší dolní závora množiny A", použitý v definici infima, lze přesněji vyjádřit slovním obratem "c je největším prvkem uspořádané množiny všech dolních závor množiny A". Dokazujeme-li tedy, že $c = \inf A$ pak musíme dokázat dvě věci:

α) c je dolní závora množiny A

β) je-li m dolní závora množiny A, pak je $m \leq c$.

Samotná definice infima obecně nezaručuje jeho existenci. Může se totiž stát, že množina dolních závor množiny A je prázdná nebo je sice neprázdná, ale nemá největší prvek. V takovém případě pak infimum A neexistuje. Na druhé straně, pokud infimum A existuje, pak musí být jediné (což ihned vyplývá z věty 7.1.1.), přičemž toto infimum může nebo také nemusí být prvkem množiny A.

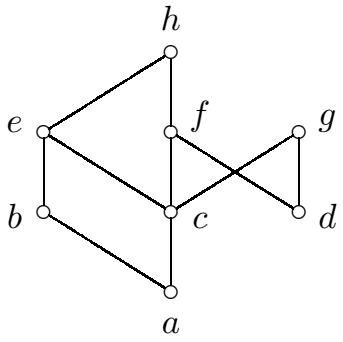
Analogické úvahy platí pro supremum množiny A v uspořádané množině $(M, \leq)$, tzn. supremum A může anebo nemusí existovat a pokud existuje, pak je jediné, přičemž může anebo nemusí v A ležet.

Připomeňme ještě, že definice infima a suprema množiny A nevylučuje situaci, že množina A je prázdná. Potom:

- infimum prázdné množiny existuje právě když uspořádaná množina $(M, \leq)$ má největší prvek c a v takovém případě je $\inf \emptyset = c$.
- podobně, $\sup \emptyset$ je rovno nejmenšímu prvku uspořádané množiny $(M, \leq)$, pokud tento nejmenší prvek existuje, jinak $\sup \emptyset$ neexistuje.

Příklad 7.4.

1. Nechť $M = \{a, b, c, d, e, f, g, h\}$ a uspořádaná množina $(M, \leq)$ je zadána hasseovským diagramem



   Ukažme si, jak vypadají infima a suprema některých podmnožin množiny M.

   - je-li $A = \{a, b, c\}$, potom $\inf A = a$ a $\sup A = e$
   - je-li $A = \{e, f, g\}$, potom $\inf A = c$ a $\sup A$ neexistuje (protože množina horních závor A je prázdná)
   - je-li $A = \{d, e\}$, potom $\inf A$ neexistuje (protože množina dolních závor A je prázdná) a $\sup A = h$
   - je-li $A = \{c, d\}$, potom $\inf A$ neexistuje (protože množina dolních závor A je prázdná) a $\sup A$ také neexistuje (protože množina horních závor A, tj. množina $\{f, g, h\}$ nemá nejmenší prvek).

2. Uvažme uspořádanou množinu $(\mathbb{N}, |)$, tzn. množinu všech přirozených čísel s relací dělitelnosti. Potom například platí:
   - každá dvouprvková podmnožina $\{a, b\}$ má infimum, kterým je největší společný dělitel čísel a, b

– každá dvouprvková podmnožina $\{a, b\}$ má supremum, kterým je nejmenší společný násobek čísel a, b

– je-li A libovolná nekonečná podmnožina v $\mathbb{N}$ pak její supremum neexistuje (množina horních závor A je v tomto případě prázdná).

3. Uvažme uspořádanou množinu $(\mathbb{R}, \leq)$, tzn. množinu všech reálných čísel s relací uspořádání čísel podle velikosti. Potom například pro intervaly $(0,1)$ a $\langle 0,1\rangle$ platí:

$$\inf(0,1) = 0\,, \quad \sup(0,1) = 1\,, \quad \inf\langle 0,1\rangle = 0\,, \quad \sup\langle 0,1\rangle = 1\,.$$

4. Uvažme uspořádanou množinu $(2^A, \subseteq)$. Nechť $\mathcal{B}$ je neprázdná podmnožina množiny 2^A (tzn. prvky množiny $\mathcal{B}$ jsou jisté podmnožiny množiny A), potom je zřejmě

$$\inf \mathcal{B} = \bigcap_{X \in \mathcal{B}} X\,, \quad \sup \mathcal{B} = \bigcup_{X \in \mathcal{B}} X\,.$$

Vidíme tedy, že v tomto případě je infimem množinový průnik a supremem je množinové sjednocení všech množin patřících do $\mathcal{B}$.

Vzájemný vztah mezi existencí infim a suprem libovolných podmnožin dané uspořádané množiny $(M, \leq)$ popisuje následující věta. Poznamenejme ještě, že předpoklad "libovolná podmnožina má infimum" vynucuje existenci nejmenšího a největšího prvku v $(M, \leq)$ (nejmenším prvkem je $\inf M$ a největším prvkem je $\inf \emptyset$). Podobně, předpoklad "libovolná podmnožina má supremum" rovněž vynucuje existenci nejmenšího prvku (kterým je $\sup \emptyset$) a největšího prvku (kterým je $\sup M$).

Věta 7.4.
Nechť $(M, \leq)$ je uspořádaná množina. Pak následující výroky jsou ekvivalentní:

1. *libovolná podmnožina množiny M má infimum*
2. *libovolná podmnožina množiny M má supremum.*

Důkaz.

Důkaz implikace "$1 \Longrightarrow 2$".

Nechť A je libovolná podmnožina v M. Označme H množinu všech horních závor množiny A (v M). Podle předpokladu existuje infimum množiny H, které označíme c. Nyní budeme dokazovat, že c je hledané supremum množiny A.

$\alpha)$ nechť $a \in A$ je libovolný prvek.
Je-li $H = \emptyset$, pak c je největší prvek M, a tedy $a \leq c$. Je-li $H \neq \emptyset$ a $h \in H$, pak musí být $a \leq h$ (proč?). To však znamená, že prvek a je dolní závorou množiny H. Ale c je infimem množiny H a proto musí být $a \leq c$.
Dokázali jsme tedy, že c je horní závora množiny A.

$\beta)$ nechť y je libovolná horní závora množiny A.
Jinými slovy řečeno, $y \in H$. Prvek c je však infimem množiny H, a tedy musí být $c \leq y$. Dokázali jsme tak, že c je nejmenší horní závora množiny A.

Dohromady platí, že $c = \sup A$, tzn. libovolná podmnožina v M má supremum.

Důkaz implikace "$2 \Longrightarrow 1$".
Provede se analogickým způsobem, jako předchozí část důkazu. ■

Definice.
Nechť $(M, \leq)$ je uspořádaná množina.

Jestliže každá dvouprvková podmnožina množiny M má infimum i supremum, pak se $(M, \leq)$ nazývá **svaz**.

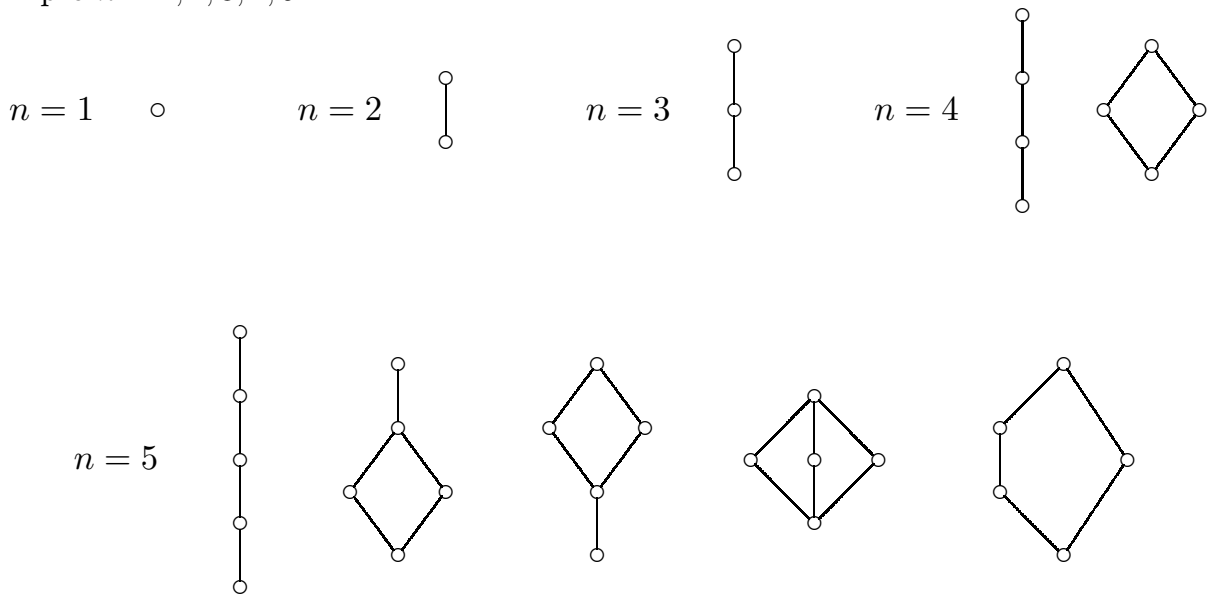
Jestliže každá podmnožina množiny M má infimum i supremum, pak se $(M, \leq)$ nazývá **úplný svaz**.

Poznámka.
Z předchozí definice bezprostředně vyplývá několik skutečností, které je dobré si uvědomit. Například:

1. Je-li $(M, \leq)$ svaz, potom také každá konečná neprázdná podmnožina v M má infimum a supremum (dokáže se matematickou indukcí). V případě, že množina M je konečná (a neprázdná), tedy pojmy svaz a úplný svaz splývají.
2. Je-li $(M, \leq)$ úplný svaz, potom je také svaz. Opačná implikace samozřejmě neplatí, jak ukážeme dále na příkladech.
3. Každý úplný svaz $(M, \leq)$ má nejmenší a největší prvek, kterým je $\inf M$ a $\sup M$.

Příklad 7.5.

1. Každá lineárně uspořádaná množina je svaz.
   Specielně tedy $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$, kde $\leq$ značí uspořádání čísel podle velikosti, jsou svazy. Žádný z nich však není úplným svazem.
2. Uspořádaná množina $(\mathbb{N}, |\,)$ je svaz, který není úplným svazem, což vyplývá z příkladu 7.4.2.
3. Nechť A je libovolná množina. Pak uspořádaná množina $(2^A, \subseteq)$ je úplný svaz, což vyplývá z příkladu 7.4.4.
4. Následující obrázek udává hasseovské diagramy všech konečných n-prvkových svazů pro $n = 1, 2, 3, 4, 5$.



8. Ekvivalence a rozklady.

Definice.
Nechť (M, ϱ) je množina s relací, přičemž relace ϱ je reflexivní, symetrická a tranzitivní. Pak se relace ϱ nazývá **ekvivalence** (na množině M).

Pro označování relace ekvivalence budeme místo řeckých písmen obvykle používat symbol $\sim$ (čti "vlnovka").

Příklad 8. 1.

1. Nechť M je libovolná neprázdná množina. Pak nejjednoduššími příklady relací ekvivalence na množině M jsou
   a) relace rovnosti ι
   b) univerzální relace $M \times M$,

   které jsme zavedli v kapitole o relacích (viz příklad 6. 3. 2 c a 6. 3. 2 b), kde jsme také uvedli, že každá z těchto relací je reflexivní, symetrická a tranzitivní.
2. Relace kongruence podle modulu m je relací ekvivalence na množině $\mathbb{Z}$ všech celých čísel. Tuto relaci jsme zavedli v příkladu 6. 3. 5. Věta 4. 8. pak ukazuje, že relace kongruence podle modulu m je reflexivní, symetrická a tranzitivní, tzn. je to skutečně relace ekvivalence na $\mathbb{Z}$.
3. Nechť $f : A \longrightarrow B$ je zobrazení. Na množině A nyní definujeme relaci $\sim$ takto:

   $$\text{pro } x, y \in A \text{ položíme: } x \sim y \text{ právě když } f(x) = f(y).$$

   Je ihned vidět, že $\sim$ je relace na A, která je reflexivní, symetrická a tranzitivní (sami si podrobně rozmyslete!). Tedy $\sim$ je relací ekvivalence na množině A.

Poznámka.
Na dané neprázdné množině M lze zřejmě definovat celou řadu různých relací ekvivalence. Označme si symbolem $\mathcal{E}(M)$ množinu všech relací ekvivalence na množině M. Uvědomíme-li si, že relace ekvivalence na M je vlastně jistá podmnožina kartézského součinu $M \times M$ a relace množinové inkluze je vždy reflexivní, antisymetrická a tranzitivní, potom je zřejmé, že $(\mathcal{E}(M), \subseteq)$ je uspořádaná množina. Uvážíme-li dále, že relace rovnosti ι a univerzální relace $M \times M$ jsou relacemi ekvivalence na množině M (viz příklad 8. 1. 1.), pak je již jednoduché ukázat, že relace rovnosti je nejmenším prvkem uspořádané množiny $(\mathcal{E}(M), \subseteq)$ a univerzální relace je největším prvkem uspořádané množiny $(\mathcal{E}(M), \subseteq)$.

Definice.
Nechť M je libovolná neprázdná množina. Pak systém $\mathcal{R}$ neprázdných podmnožin množiny M, splňujících podmínky:

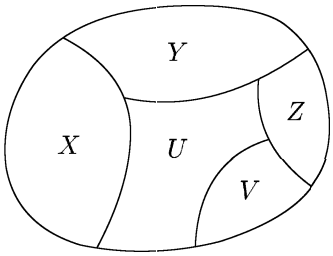
1. libovolné dvě různé množiny ze systému $\mathcal{R}$ jsou disjunktní
2. sjednocení všech množin ze systému $\mathcal{R}$ je rovno celé množině M,

se nazývá **rozklad na množině** M. Prvky systému $\mathcal{R}$ se nazývají **třídy rozkladu** $\mathcal{R}$.

Podmínky, které jsme v předchozí definici vyjádřili slovně, lze pomocí matematické symboliky zapsat následovně:

1. $X, Y \in \mathcal{R} \ \wedge \ X \neq Y \quad \Rightarrow \quad X \cap Y = \emptyset$
2. $\bigcup X \, (X \in \mathcal{R}) \, = \, M$

Rozklad na množině si můžeme ilustrovat náčrtkem podobného tvaru, jaký je uveden na následujícím obrázku. Na něm je znázorněn rozklad $\mathcal{R}$ na množině M, takový, že $\mathcal{R} = \{U, V, X, Y, Z\}$. Rozklad $\mathcal{R}$ má tedy v tomto případě 5 tříd rozkladu, kterými jsou množiny U, V, X, Y, Z. Uvedený obrázek je samozřejmě pouze orientační a nepřesný (mělo by například být řečeno, kam patří hranice jednotlivých množin). Je zřejmé, že počet tříd rozkladu nemusí být konečný tak jako na obrázku, ale může být i nekonečný. V každém případě však musí být $\mathcal{R} \neq \emptyset$.



Poznámka.
Dokazujeme-li, že systém množin $\mathcal{R}$ je rozkladem na množině M, pak z definice rozkladu plyne, že je nutné ověřit následující tři podmínky:

1. každá množina z $\mathcal{R}$ je **neprázdnou** podmnožinou v M.
2. dvě **různé** množiny z $\mathcal{R}$ jsou disjunktní. Tuto podmínku je obvykle technicky nejvýhodnější dokazovat tak, že:

   $$\text{předpokládáme} \quad X, Y \in \mathcal{R} \ \wedge \ X \cap Y \neq \emptyset \quad \text{a} \quad \text{dokážeme, že} \quad X = Y \, .$$

3. sjednocení všech množin z $\mathcal{R}$ je rovno celé množině M. Zde technicky dokazujeme pouze inkluzi $M \ \subseteq \ \bigcup X \, (X \in \mathcal{R})$, protože opačná inkluze je zřejmě vždycky splněna.

Příklad 8. 2.

1. Nechť M je libovolná neprázdná množina. Pak nejjednoduššími příklady rozkladů na množině M jsou následující dva rozklady:

   a) $\mathcal{R} = \{\{x\} \mid \text{pro každé } x \in M\}$, což je rozklad, který má tolik tříd, kolik prvků má množina M, přičemž každá jeho třída obsahuje vždy právě jeden prvek

   b) $\mathcal{R} = \{M\}$, což je rozklad, který má jedinou třídu, a to množinu M.

2. Nechť $M = \mathbb{Z}$. Pak například množiny

   $$\{x \in \mathbb{Z} \mid x \leq -2\}, \ \{-1, 0\}, \ \{x \in \mathbb{Z} \mid x \, \text{je sudé, kladné}\}, \ \{x \in \mathbb{Z} \mid x \, \text{je liché, kladné}\}$$

   tvoří rozklad na množině $\mathbb{Z}$ všech celých čísel. Tento rozklad má 4 třídy, z nichž tři třídy mají nekonečně mnoho prvků a jedna třída má konečně mnoho prvků.

3. Nechť $M = \mathbb{R}$. Pro libovolné celé číslo k označme symbolem I_k reálný interval $\langle k\,,\, k+1)$, tzn.:

$$I_k = \{x \in \mathbb{R} \mid k \leq x < k+1\}\,.$$

Potom $\mathcal{R} = \{I_k \mid k \in \mathbb{Z}\}$ je rozklad na množině $\mathbb{R}$ všech reálných čísel, který má nekonečně mnoho tříd a každá jeho třída má nekonečně mnoho prvků.

Nyní sestrojíme ještě jeden důležitý rozklad na množině $\mathbb{Z}$ všech celých čísel. K tomu ale nejprve zavedeme následující pojem.

Definice.
Nechť m je pevné přirozené číslo. Označme:

(1) $\quad C_i = \{\, x \in \mathbb{Z} \mid x$ dává po dělení číslem m zbytek $i\,\}$, pro $i = 0, 1, \ldots, m-1$

Pak množina C_i se nazývá **zbytková třída** podle modulu m. Symbolem $\mathbb{Z}_m$ se označí **množina všech zbytkových tříd podle modulu** m, tzn. $\mathbb{Z}_m = \{C_0, C_1, \ldots, C_{m-1}\}$.

Poznámka.
Někdy bude technicky výhodnější přeformulovat definici zbytkové třídy C_i do ekvivalentního tvaru:

(2) $\qquad C_i = \{\, x \in \mathbb{Z} \mid x \equiv i \,(\mathrm{mod}\ m)\,\}\,, \qquad$ pro $i = 0, 1, \ldots, m-1\,.$

Ekvivalentnost vyjádření (1) a (2) okamžitě plyne z věty 4. 7., uvědomíme-li si zřejmý fakt, že číslo i, kde $0 \leq i \leq m-1$, dává po dělení číslem m zbytek i.

Z věty o dělení se zbytkem celých čísel plyne, že zbytkových tříd podle modulu m musí být opravdu právě m (neboť zbytek po dělení každého celého čísla číslem m musí podle této věty nabývat právě jedné z hodnot $0, 1, \ldots, m-1$). Dále, každá zbytková třída podle modulu m obsahuje zřejmě nekonečně mnoho celých čísel, lišících se o nějaký celočíselný násobek modulu m. Pokusíme-li se schematicky zapsat jednotlivé zbytkové třídy podle modulu m, dostaneme:

$$\begin{aligned}
C_0 &= \{\ldots, \quad -2m \quad, \quad -m \quad, \quad 0 \quad, \quad m \quad, \quad 2m \quad, \quad \ldots\} \\
C_1 &= \{\ldots, \ -2m+1\,, \ -m+1\,, \quad 1 \quad, \quad m+1\,, \ 2m+1\,, \quad \ldots\} \\
C_2 &= \{\ldots, \ -2m+2\,, \ -m+2\,, \quad 2 \quad, \quad m+2\,, \ 2m+2\,, \quad \ldots\} \\
&\ \ \vdots \\
C_{m-1} &= \{\ldots, \quad -m-1\,, \quad -1 \quad, \ m-1\,, \ 2m-1\,, \ 3m-1\,, \ \ldots\}
\end{aligned}$$

V této souvislosti je ještě třeba důrazně upozornit na to, že není možné navzájem porovnávat množiny zbytkových tříd podle různých modulů. Není tedy například možné říci, že $\mathbb{Z}_3 \subseteq \mathbb{Z}_4$, i když zavedené označení

$$\mathbb{Z}_3 = \{C_0, C_1, C_2\} \qquad\qquad \mathbb{Z}_4 = \{C_0, C_1, C_2, C_3\}$$

by k tomu na první pohled mohlo svádět. Srovnáme-li však např. zbytkovou třídu

$$C_0 \in \mathbb{Z}_3\,, \quad \text{tzn.:} \qquad C_0 = \{\ldots, -6\,, -3\,, 0\,, 3\,, 6\,, \ldots\}$$

a zbytkovou třídu

$$C_0 \in \mathbb{Z}_4\,, \quad \text{tzn.:} \qquad C_0 = \{\ldots\,, -8\,, -4\,, 0\,, 4\,, 8\,, \ldots\}$$

pak ihned vidíme, že se jedná o dvě naprosto rozdílné množiny. Přesněji řečeno, každá zbytková třída se vždy váže k jedinému, pevně danému modulu m, což by se správně mělo projevit i v použitém označení. Například místo C_i bychom psali třeba $(C_i)_m$. Z důvodu stručnosti vyjadřování však i nadále zůstaneme u původně zavedeného označení.

Věta 8.1.
Nechť m je pevné přirozené číslo. Pak množina $\mathbb{Z}_m$ všech zbytkových tříd podle modulu m tvoří rozklad na množině $\mathbb{Z}$ všech celých čísel.

Důkaz.
Uvažme množinu zbytkových tříd $\mathbb{Z}_m = \{C_0, C_1, \ldots, C_{m-1}\}$. Podle návodu uvedeného v poznámce za definicí rozkladu dokážeme, že $\mathbb{Z}_m$ je rozklad na $\mathbb{Z}$.

1. každá ze zbytkových tříd C_i je zřejmě neprázdnou podmnožinou v $\mathbb{Z}$.
2. nechť $C_i, C_j \in \mathbb{Z}$ a $C_i \cap C_j \neq \emptyset$. Potom existuje číslo $x \in C_i \cap C_j$, což znamená, že x dává po dělení číslem m zbytek i a současně také zbytek j. Ale z věty o dělení celých čísel se zbytkem víme, že zbytek po dělení je určen jednoznačně, tzn. $i = j$, odkud dostáváme, že $C_i = C_j$.
3. zřejmě platí, že sjednocení $C_0 \cup C_1 \cup \cdots \cup C_{m-1} = \mathbb{Z}$. ■

Ve zbývající části této kapitoly se budeme zabývat vzájemnými vztahy mezi relacemi ekvivalence na dané množině a rozklady na téže množině. Ukážeme, že mezi oběma pojmy je velmi úzká souvislost.

Věta 8.2.
Nechť $\sim$ je relace ekvivalence na množině M. Pro každé $a \in M$ položme:

$$X_a = \{x \in M \mid x \sim a\}.$$

Potom systém množin:

$$\{\, X \mid \textit{existuje } a \in M \textit{ tak, že } X = X_a\} \tag{3}$$

je rozklad na množině M, který budeme označovat symbolem $M/\!\sim$.

Důkaz.
Z toho, že $a \in X_a$ bezprostředně vyplývá, že systém množin (3) sestává z neprázdných podmnožin množiny M a že platí $\bigcup X_a (a \in M) = M$. Zbývá tedy dokázat pouze vlastnost 1. z definice rozkladu.

Nechť tedy X_a, X_b jsou množiny ze systému (3) takové, že $X_a \cap X_b \neq \emptyset$, tzn. existuje prvek $z \in X_a \cap X_b$. Nyní dokážeme, že $X_a = X_b$.

"$\subseteq$": nechť $x \in X_a$ libovolné, tzn. platí, že $x \sim a$. Dále, z toho, že $z \in X_a \cap X_b$ plyne, že $z \sim a \wedge z \sim b$. Je tedy $x \sim a \wedge a \sim z \wedge z \sim b$, odkud vzhledem k tranzitivnosti relace $\sim$ dostáváme, že $x \sim b$, neboli $x \in X_b$. Tím jsme dokázali, že $X_a \subseteq X_b$.

"$\supseteq$": tato inkluze se dokáže analogicky. ■

Definice.
Nechť $\sim$ je relace ekvivalence na množině M. Pak rozklad $M/\sim$ budeme nazývat **rozklad příslušný ekvivalenci** $\sim$.

Poznámka.
Připomeňme, že zápis (3) budeme chápat v obvyklém množinovém smyslu tak, jak bylo vysvětleno v kapitole o základních množinových pojmech, tzn. ve (3) budou vypsány pouze různé množiny. Jinak řečeno, jestliže pro $a, b \in M$ je $X_a = X_b$, pak v zápisu (3) bude z množin X_a, X_b zapsána pouze jedna. Vidíme tedy, že o skutečném počtu různých tříd rozkladu $M/\sim$ se jenom ze samotného zápisu (3) nedá nic říci.

Příklad 8. 3.
Ukažme si, jak vypadají rozklady příslušné ekvivalencím, které jsme uváděli v příkladu 8. 1.

1. Nechť M je libovolná neprázdná množina. Pak
   a) rozklad příslušný relaci rovnosti ι je zřejmě tvaru $\{\{x\} \mid x \in M\}$, tzn. jedná se o rozklad množiny M na jednoprvkové třídy
   b) rozklad příslušný univerzální relaci $M \times M$ je tvaru $\{M\}$, tzn. je to rozklad množiny M, který má jedinou třídu, a sice celou množinu M.
2. Nechť $M = \mathbb{Z}$ a nechť relací ekvivalence je relace $\equiv$ kongruence podle modulu m. Pak rozklad příslušný této ekvivalenci je roven rozkladu množiny $\mathbb{Z}$ na zbytkové třídy podle modulu m (což plyne z definice zbytkových tříd podle modulu m). Jinak zapsáno, je tedy: $\mathbb{Z}/\equiv = \{C_0, C_1, \ldots, C_{m-1}\}$.
3. Nechť $f : A \longrightarrow B$ je zobrazení a nechť $\sim$ je relace ekvivalence na množině A, definovaná v příkladu 8. 1. 3. (tzn.: $x \sim y \Leftrightarrow f(x) = f(y)$). Potom rozkladem příslušným této relaci ekvivalence je rozklad na množině A, jehož třídy jsou tvořeny vždy právě těmi prvky z A, které se při zobrazení f zobrazí na stejný prvek množiny B. Je tedy:
$$A/\sim \; = \; \{ X \mid X \subseteq A \; \wedge \; \exists\, b_0 \in B : x \in X \Leftrightarrow f(x) = b_0 \}.$$
   Rozklad $A/\sim$ budeme také nazývat **rozklad příslušný zobrazení** f.

Věta 8. 3.
Nechť $\mathcal{R}$ je rozklad na množině M. Pro prvky $a, b \in M$ položme:
$$a \sim_{\mathcal{R}} b \;\; \textit{právě když existuje třída} \;\; X \in \mathcal{R} \;\; \textit{tak, že} \;\; a, b \in X \;\; .$$
Pak relace $\sim_{\mathcal{R}}$ je relací ekvivalence na množině M.

Důkaz.
Relace $\sim_{\mathcal{R}}$ je zřejmě reflexivní a symetrická. Zbývá tedy dokázat, že relace $\sim_{\mathcal{R}}$ je tranzitivní.
Nechť tedy pro prvky $a, b, c \in M$ platí: $a \sim_{\mathcal{R}} b \;\wedge\; b \sim_{\mathcal{R}} c$. Podle definice relace $\sim_{\mathcal{R}}$ existují třídy X, Y rozkladu $\mathcal{R}$ takové, že $a, b \in X \;\wedge\; b, c \in Y$. Tedy $b \in X \cap Y$, což znamená, že $X \cap Y \neq \emptyset$, a podle definice rozkladu musí být $X = Y$. Potom však $a, c \in X$, a tedy $a \sim_{\mathcal{R}} c$. Dokázali jsme tak, že relace $\sim_{\mathcal{R}}$ je tranzitivní. ■

Definice.
Nechť $\mathcal{R}$ je rozklad na množině M. Potom relace $\sim_{\mathcal{R}}$ se nazývá **ekvivalence příslušná rozkladu** $\mathcal{R}$.

Příklad 8. 4.
Ukažme si, jak vypadají ekvivalence příslušné některým rozkladům, které jsme uvedli dříve.

1. Nechť M je libovolná neprázdná množina a nechť $\mathcal{R}$ je rozklad na M tvaru:
   a) $\mathcal{R} = \{\{x\} \mid x \in M\}$, tzn. jedná se o rozklad množiny M na jednoprvkové třídy. Potom ekvivalence příslušná tomuto rozkladu je zřejmě relace rovnosti ι.
   b) $\mathcal{R} = \{M\}$, tzn. jedná se o rozklad na množině M, sestávající z jediné třídy. Pak relací ekvivalence, příslušné tomuto rozkladu je zřejmě univerzální relace.
2. Nechť $M = \mathbb{Z}$ a nechť $\mathcal{R}$ je rozklad množiny $\mathbb{Z}$ na zbytkové třídy podle modulu m, tzn. $\mathcal{R} = \mathbb{Z}_m = \{C_0, C_1, \ldots, C_{m-1}\}$.
   Pak relací ekvivalence příslušné tomuto rozkladu je relace kongruence podle modulu m, neboť platí:
   $$a \sim_{\mathcal{R}} b \quad \Leftrightarrow \quad a, b \in C_i \text{ pro nějaké } i = 0, 1, \ldots, m-1 \quad \Leftrightarrow \quad a \equiv b\,(mod\ m).$$

Poznámka.
Uvědomme si, že rozklad příslušný ekvivalenci $\sim$ je pouze jedním z mnoha rozkladů, které je možno na množině M vytvořit a jeho definice evidentně závisí na dané relaci $\sim$. Tak například rozklad na množině $\mathbb{Z}$, příslušný relaci kongruence podle modulu m je právě rozklad $\mathbb{Z}_m$ a žádný jiný. Podobně je tomu s relací ekvivalence příslušné rozkladu $\mathcal{R}$, která je definována v závislosti na tomto rozkladu.

Na závěr této kapitoly ukážeme, že mezi ekvivalencemi na množině M a rozklady na množině M existuje velice úzká souvislost. Přesněji řečeno, vyjdeme-li od jisté ekvivalence na množině M, utvoříme rozklad příslušný této ekvivalenci a následně utvoříme ekvivalenci příslušnou předchozímu rozkladu, pak skončíme u původní ekvivalence, od níž jsme vyšli. Podobně, máme-li nějaký rozklad na množině M, utvoříme ekvivalenci příslušnou tomuto rozkladu a nakonec sestrojíme rozklad příslušný poslední ekvivalenci, tak dostaneme původní rozklad na M. Můžeme tedy říci, že se tímto způsobem ekvivalence a rozklady vzájemně určují. Přesně popisuje tuto situaci následující věta.

Věta 8. 4.
Nechť M je libovolná neprázdná množina. Pak platí:

1. *je-li $\sim$ ekvivalence na množině M, potom $\sim_{M/\sim} = \sim$*
2. *je-li $\mathcal{R}$ rozklad na množině M, potom $M/\sim_{\mathcal{R}} = \mathcal{R}$*

Důkaz.
Dokazovaná tvrzení jsou v obou případech množinové rovnosti a budeme je tedy také jako množinové rovnosti dokazovat.

1. dokazovaná rovnost je rovností dvou relací na množině M, tzn. budeme dokazovat rovnost dvou podmnožin kartézského součinu $M \times M$.

"$\subseteq$": nechť $(a,b) \in \sim_{M/\sim}$, tzn. $a \sim_{M/\sim} b$. Pak existuje třída rozkladu $M/\sim$, která obsahuje prvky a, b. Nechť tedy $a, b \in X_u$. Potom podle definice třídy X_u je $a \sim u \ \wedge \ b \sim u$, odkud plyne (užitím symetričnosti a tranzitivnosti relace $\sim$), že $a \sim b$. Dostáváme tak, že $(a,b) \in \sim$.

"$\supseteq$": nechť $(a,b) \in \sim$, tzn. $a \sim b$. Pak zřejmě je $a \in X_a \ \wedge \ b \in X_a$, kde X_a je jedna ze tříd rozkladu $M/\sim$. To ale znamená, že je $a \sim_{M/\sim} b$. Dostáváme tak, že $(a,b) \in \sim_{M/\sim}$.

2. dokazovaná rovnost je rovností dvou rozkladů na množině M, tzn. budeme dokazovat rovnost dvou systémů podmnožin množiny M.

"$\subseteq$": nechť $X \in M/\sim_{\mathcal{R}}$, tzn. X je třída rozkladu $M/\sim_{\mathcal{R}}$. Pak existuje prvek $a \in M$ tak, že $X = X_a = \{x \in M \mid x \sim_{\mathcal{R}} a\}$. Ale poslední množina je právě jedna ze tříd rozkladu $\mathcal{R}$, což znamená, že $X \in \mathcal{R}$.

"$\supseteq$": nechť $X \in \mathcal{R}$, tzn. X je třída rozkladu $\mathcal{R}$. Nechť dále a je libovolný pevný prvek z X. Pak ale $X = \{x \in M \mid x \sim_{\mathcal{R}} a\} = X_a \in M/\sim_{\mathcal{R}}$. Dokázali jsme tedy, že $X \in M/\sim_{\mathcal{R}}$. ■

II. ZÁKLADNÍ ALGEBRAICKÉ STRUKTURY

1. Algebraické struktury s jednou operací.

V této kapitole se budeme zabývat jistými speciálními typy zobrazení, které se nazývají operace. Pojem operace vznikl zobecněním pojmů běžně známých ze střední školy, jako jsou například násobení přirozených čísel nebo sčítání celých čísel, atd. Vidíme, že v těchto případech je vždy libovolné uspořádané dvojici čísel z jisté množiny přiřazeno jediné, přesně určené číslo z téže množiny.

Definice.
Nechť G je neprázdná množina. Pak libovolné zobrazení $G \times G \longrightarrow G$ se nazývá **operace na množině** G. Je-li při tomto zobrazení uspořádané dvojici $(a, b) \in G \times G$ přiřazen prvek $c \in G$, pak budeme obvykle psát

$$a \cdot b = c$$

a budeme hovořit o operaci $\cdot$ (čti "tečka"). Množina G spolu s operací $\cdot$ se nazývá **grupoid** a označuje se symbolem $(G, \cdot)$.

Poznámka.
1. Pro označování operace na množině G (což je vlastně jisté zobrazení) se ukazuje jako nepraktické používat písmena a symboliku zavedenou v kapitole o zobrazeních. Vhodnější je používat speciálních symbolů. Nejčastěji to budou:
   - symbol $\cdot$ (tzv. multiplikativní symbolika), který budeme číst "krát" a budeme hovořit o operaci "násobení". Je-li $a \cdot b = c$, pak prvek c budeme nazývat součinem prvků a, b (v tomto pořadí).
   - symbol $+$ (tzv. aditivní symbolika), který budme číst "plus" a budeme hovořit o operaci "sčítání". Je-li $a + b = c$, pak prvek c budeme nazývat součtem prvků a, b (v tomto pořadí).

   Poznamenejme, že výše zavedené symboly $\cdot$ nebo $+$ obecně nemají nic společného s násobením nebo sčítáním čísel. Dodejme ještě, že pro označování operací na množině budeme podle potřeby používat i jiné symboly, například $\circ$, $*$ atd.
2. Z předchozí definice plyne, že grupoid $(G, \cdot)$ je uspořádaná dvojice, sestávající z množiny G (která se též nazývá nosná množina grupoidu) a z operace $\cdot$ na množině G. Rovnost dvou grupoidů znamená tedy rovnost nosných množin a současně rovnost příslušných operací.

Pojem operace na množině G tak, jak byl výše definován, je možné ještě dále zobecnit na pojem tzv. "n-ární operace" na množině G, pro libovolné přirozené n, což je libovolné zobrazení $G \times G \times \cdots \times G$ (n–krát) $\longrightarrow G$. Je to tedy předpis, který každé uspořádané n-tici prvků z G přiřazuje jediný prvek z G. Příkladem n-ární operace na množině reálných čísel $\mathbb{R}$ může být třeba operace $\max(x_1, x_2, \ldots, x_n)$, která každé uspořádané n-tici reálných čísel přiřazuje to číslo, které je z nich maximální. Pro $n = 1$,

resp. $n = 2$, resp. $n = 3$ se pak užívá názvů unární operace, resp. binární operace, resp. ternární operace.

Příklad 1. 1.

1. Uvažme množinu $\mathbb{Z}$ všech celých čísel. Pak obyčejné násobení čísel $\cdot$ je zřejmě operací na množině $\mathbb{Z}$. Tedy $(\mathbb{Z}, \cdot)$ je grupoid.

   Podobně dostáváme grupoidy $(\mathbb{Z}, +)$, resp. $(\mathbb{Z}, -)$, kde $+$, resp. $-$ značí obyčejné sčítání, resp. obyčejné odčítání celých čísel. Je jasné, že se jedná o různé grupoidy, i když nosná množina je ve všech třech případech stejná.

2. Vezmeme-li množinu $\mathbb{N}$ všech přirozených čísel, pak obyčejné odčítání čísel není operací na $\mathbb{N}$, protože například pro přirozená čísla $2, 3$ je $2 - 3 \notin \mathbb{N}$, tzn. nejedná se o zobrazení $\mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$.

   Dále například obyčejné dělení čísel není operací na množině $\mathbb{R}$ všech reálných čísel (rozmyslete si proč).

3. Nechť A je libovolná množina. Pak sjednocení, průnik a rozdíl dvou podmnožin množiny A je opět (jednoznačně určená) podmnožina v A. Tedy sjednocení, průnik a rozdíl množin jsou operace na množině 2^A (tj. na systému všech podmnožin množiny A). Dostáváme tak grupoidy $(2^A, \cup)$, resp. $(2^A, \cap)$, resp. $(2^A, -)$.

4. Nechť A je libovolná neprázdná množina. Symbolem A^A, jak víme, označujeme systém všech zobrazení množiny A do množiny A (tzn. roli prvků množiny A^A tedy hrají zobrazení $A \longrightarrow A$).
   Pro $f, g \in A^A$ je zřejmě složené zobrazení $g \circ f$ opět zobrazením $A \longrightarrow A$, tzn. jinak řečeno $g \circ f \in A^A$. Skládání zobrazení je tedy operací na množině A^A a $(A^A, \circ)$ je pak grupoid.

Operace na množině G je zobrazení $G \times G \longrightarrow G$, tzn. je to vlastně jistý předpis, který každé uspořádané dvojici prvků z G přiřadí jediný prvek z G. Tento předpis je možno zadávat různými způsoby, jak jsme ukázali v kapitole o zobrazeních. Pokud je však množina G konečná a má malý počet prvků, pak je výhodné zadávat operaci na G pomocí tabulky, sestrojené následujícím způsobem: do svislého i vodorovného záhlaví tabulky napíšeme prvky množiny G, a to ve stejném pořadí. Výsledek operace pro uspořádanou dvojici $(a, b) \in G$ pak zapíšeme do toho políčka tabulky, které se nachází v řádku označeném "a" a ve sloupci nadepsaném "b". Použití tabulky při definování operace ukazuje následující příklad.

Příklad 1. 2.
Na množině $G = \{a, b, c, d\}$ definujeme operaci $\cdot$ tabulkou:

	a	b	c	d
a	b	a	b	c
b	a	b	c	d
c	b	c	a	c
d	a	d	a	d

Potom $(G, \cdot)$ je grupoid, přičemž například platí: $a \cdot d = c$, $d \cdot a = a$, atd.

Definice.
Nechť $(G, \cdot)$ je grupoid. Jestliže platí:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \text{pro každé } a, b, c \in G \qquad \text{(asociativní zákon)}$$

pak operace $\cdot$ se nazývá **asociativní operace** a grupoid $(G, \cdot)$ se nazývá asociativní grupoid neboli **pologrupa**.

Definice.
Nechť $(G, \cdot)$ je grupoid. Jestliže platí:

$$a \cdot b = b \cdot a \quad \text{pro každé } a, b \in G \qquad \text{(komutativní zákon)}$$

pak operace $\cdot$ se nazývá **komutativní operace** a grupoid $(G, \cdot)$ se nazývá **komutativní grupoid**.

Příklad 1. 3.
Ověřujeme-li u grupoidů z příkladů 1.1 a 1.2 platnost asociativního a komutativního zákona (proveďte si podrobně sami), pak zjistíme, že:

a) grupoidy $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}, +)$, $(2^A, \cup)$, $(2^A, \cap)$ jsou asociativní i komutativní

b) grupoid $(\mathbb{Z}, -)$ a grupoid $(G, \cdot)$ z příkladu 1.2 není asociativní a není komutativní

c) grupoid $(2^A, -)$ je asociativní i komutativní v případě, že $A = \emptyset$; je-li množina A neprázdná, pak grupoid $(2^A, -)$ není asociativní a není komutativní

d) grupoid $(A^A, \circ)$ je vždy asociativní; komutativní je tento grupoid pouze v případě, že množina A je jednoprvková, jinak komutativní není.

Připomeňme ještě jednou, že při důkazu toho, že nějaké tvrzení obecně neplatí obvykle postupujeme tak, že ukážeme jednu konkrétní situaci, v níž toto tvrzení není splněno. Například chceme-li dokázat, že grupoid $(G, \cdot)$ z příkladu 1.2 není asociativní, pak najdeme konkrétní tři prvky, které platnost asociativního zákona porušují. V tomto případě například stačí vzít prvky $a, d, c \in G$ a spočítat příslušné součiny, tzn.

$$a \cdot (d \cdot c) = b \qquad \text{a} \qquad (a \cdot d) \cdot c = a\,.$$

Na hledání výše zmiňovaného protipříkladu neexistuje žádná univerzální "rada". Je třeba pouze postupovat systematicky a všímat si pozorně toho, jak je tabulka vytvořena. V našem případě je třeba zřejmé, že v hledaném protipříkladu se nemůže vyskytovat prvek b (proč?).

Z definice pologrupy vyplývá, že v ní součin tří prvků (v daném pořadí) nezáleží na jejich uzávorkování, které u tří prvků lze provést právě uvedenými dvěma způsoby. Následující věta ukáže, že totéž platí v pologrupě i pro libovolný konečný počet n prvků, kde je počet možných uzávorkování samozřejmě mnohem větší.

Věta 1. 1.
Nechť $(G, \cdot)$ je pologrupa a $a_1, a_2, \ldots, a_n \in G$. Pak součin prvků $a_1, a_2, \ldots, a_n$ (v tomto pořadí) nezáleží na jejich uzávorkování.

Důkaz.
Tvrzení dokážeme matematickou indukcí vzhledem k n.

$\alpha)$ pro $n = 1$ tvrzení zřejmě platí (prvek a_1 chápeme jako "jednočlenný součin")

$\beta)$ předpokládáme, že tvrzení platí pro $1, \ldots, n-1$ $(n \geq 2)$, tzn. předpokládáme, že součin libovolných k prvků vybraných z prvků $a_1, \ldots, a_n$ (v tomto pořadí), kde $1 \leq k \leq n-1$ nezáleží na jejich uzávorkování. Hodnotu tohoto součinu budeme označovat pomocí hranatých závorek.
Nyní mějme dán součin prvků $a_1, \ldots, a_n$ při libovolném uzávorkování. Hodnotu tohoto součinu označme u. Pak (uvážíme-li "poslední" závorky) je $u = b \cdot c$, kde b je součin prvků $a_1, \ldots, a_r$ a c je součin prvků $a_{r+1}, \ldots, a_n$ $(1 \leq r \leq n-1)$. Potom:
- pro $r = 1$ je $u = [a_1] \cdot [a_2, \ldots, a_n]$
- pro $2 \leq r \leq n-1$ je (použijeme-li postupně indukční předpoklad, asociativní zákon a opět indukční předpoklad):

$$u = [a_1, \ldots, a_r] \cdot [a_{r+1}, \ldots, a_n] = (\,[a_1] \cdot [a_2, \ldots, a_r]\,) \cdot [a_{r+1}, \ldots, a_n] =$$
$$= [a_1] \cdot (\,[a_2, \ldots, a_r] \cdot [a_{r+1}, \ldots, a_n]\,) = [a_1] \cdot [a_2, \ldots, a_n]\,.$$

Tedy součin prvků $a_1, \ldots, a_n$ má při každém uzávorkování stejnou hodnotu. ■

Definice.
Nechť $(G, \cdot)$ je grupoid. Prvek $e \in G$ se nazývá **neutrální prvek** grupoidu $(G, \cdot)$, jestliže platí:

$$(1) \qquad a \cdot e = a \quad \wedge \quad e \cdot a = a \qquad \text{pro každý prvek } a \in G\,.$$

Předchozí definice především nezaručuje existenci neutrálního prvku v grupoidu a v případě, že neutrální prvek v grupoidu existuje, pak neříká nic o případném počtu neutrálních prvků v tomto grupoidu. Odpověď na tyto otázky nám dává následující věta.

Věta 1. 2.
V grupoidu existuje nejvýše jeden neutrální prvek.

Důkaz.
Budeme předpokládat, že v grupoidu existují dva neutrální prvky a dokážeme, že se rovnají. Nechť tedy $(G, \cdot)$ je grupoid a nechť $e, e' \in G$ jsou neutrální prvky tohoto grupoidu. Pak platí: $e \cdot e' = e'$ (protože e je neutrálním prvkem grupoidu) a současně také platí: $e \cdot e' = e$ (protože e' je neutrálním prvkem grupoidu). Dostáváme tedy, že $e = e'$. ■

Z předchozí věty plyne, že grupoid buďto nemá žádný neutrální prvek nebo má jeden neutrální prvek. Máme-li v daném grupoidu nalézt neutrální prvek, pak v jednoduchých případech postupujeme tak, že neutrální prvek "uhodneme" a ověřením definice (1) následně ukážeme, že se skutečně o neutrální prvek jedná. Ve složitějších případech, musíme neutrální prvek ze vztahů (1) vypočítat.

Příklad 1. 4.
Vyšetřujeme-li existenci neutrálního prvku u grupoidů z příkladu 1.1 a příkladu 1.2 (proveďte si podrobně sami), pak zjistíme, že:

a) grupoid $(\mathbb{Z}, \cdot)$ má neutrální prvek 1; grupoid $(\mathbb{Z}, +)$ má neutrální prvek 0 a grupoid $(\mathbb{Z}, -)$ nemá neutrální prvek

b) grupoid $(2^A, \cup)$ má neutrální prvek, kterým je $\emptyset$; grupoid $(2^A, \cap)$ má neutrální prvek, kterým je množina A a grupoid $(2^A, -)$ má neutrální prvek $\emptyset$ v případě, že $A = \emptyset$, jinak neutrální prvek nemá

c) grupoid $(A^A, \circ)$ má neutrální prvek, kterým je identické zobrazení id_A

d) grupoid $(G, \cdot)$ z příkladu 1.2 má neutrální prvek b.
Všimněme si toho, že u grupoidů zadaných tabulkou se neutrální prvek nalezne velmi jednoduše tak, že u tohoto prvku se v příslušném řádku opakuje vodorovné záhlaví tabulky a v příslušném sloupci se opakuje svislé záhlaví tabulky.

Úmluva.
V dalším textu budeme místo termínu "neutrální prvek grupoidu $(G, \cdot)$" (tzn. při multiplikativní symbolice) používat častěji termín "**jednička grupoidu** $(G, \cdot)$" a tento prvek budeme (stejně jako doposud) označovat symbolem e.

Pokud budeme používat aditivní symboliku (tzn. operaci budeme označovat symbolem $+$), pak místo termínu "neutrální prvek grupoidu $(G, +)$" budeme používat termín "**nula grupoidu** $(G, +)$" a tento prvek budeme označovat symbolem o.

Rozlišování obou pojmů budeme potřebovat později v situaci, kdy na dané množině budou najednou definovány dvě operace. Použitá terminologie je přitom motivována situací, kdy při obyčejném násobení čísel hraje roli neutrálního prvku číslo 1 a při obyčejném sčítání čísel hraje roli neutrálního prvku číslo nula.

Definice.
Nechť $(G, \cdot)$ je grupoid s jedničkou e a nechť $a \in G$ je pevný prvek. Nechť $x \in G$ je prvek, pro který platí:

$$a \cdot x = e \qquad \wedge \qquad x \cdot a = e\,.$$

Pak prvek x se nazývá **inverzní prvek k prvku** a.

Na tomto místě zdůrazněme zásadní rozdíl mezi oběma právě zavedenými pojmy. Zatímco pojem neutrálního prvku se týká celého grupiodu a je tedy v pořádku říci "e je neutrálním prvkem daného grupoidu", pojem inverzního prvku se vždy váže k nějakému konkrétnímu prvku. Je tedy nutné trvat na formulaci "x je inverzní prvek **k prvku** a" a není možné používat formulace typu: "x je inverzní prvek" nebo "x je inverzní prvek grupoidu" nebo "grupoid má inverzní prvek", apod.

Úmluva.
Pokud budeme používat aditivní symboliku (tzn. operaci budeme označovat $+$), pak místo termínu "inverzní prvek k prvku a" budeme používat termín "**opačný prvek k prvku** a". Opačným prvkem k prvku a v grupoidu $(G, +)$ s nulou o je tedy takový prvek $x \in G$, pro který platí:

$$a + x = o \qquad \wedge \qquad x + a = o\,.$$

Poznamenejme, že z předchozí definice nevyplývá, že v grupoidu s jedničkou k danému prvku a musí existovat prvek inverzní, ani to, že inverzní prvek k prvku a musí

existovat jediný. Může se totiž stát, že v grupoidu s jedničkou k danému prvku

- neexistuje žádný inverzní prvek (například v grupoidu $(\mathbb{Z}, \cdot)$ k číslu 2 neexistuje inverzní prvek)
- existuje jediný inverzní prvek (například v grupoidu $(\mathbb{Z}, \cdot)$ k číslu -1 existuje jediný inverzní prvek, kterým je zřejmě číslo -1)
- existuje více inverzních prvků (například v grupoidu z příkladu 1.2 k prvku a existují dva inverzní prvky, a sice prvky $a\,,\, c$) .

Bude-li však daný grupoid pologrupou (tzn. operace bude asociativní), pak poslední možnost nemůže nenastat, což vyplývá z následující věty.

Věta 1. 3.
V pologrupě s jedničkou ke každému prvku existuje nejvýše jeden prvek inverzní.

Důkaz.
Nechť $(G, \cdot)$ je pologrupa s jedničkou e a nechť a je libovolný prvek z G. Důkaz povedeme tak, že budeme předpokládat existenci dvou inverzních prvků k prvku a a dokážeme o nich, že se rovnají. Nechť tedy x, y jsou inverzní prvky k prvku a , tzn. podle předchozí definice platí :

$$a \cdot x = e \quad \wedge \quad x \cdot a = e \qquad \wedge \qquad a \cdot y = e \quad \wedge \quad y \cdot a = e\,.$$

Pomocí těchto vztahů, užitím asociativity operace $\cdot$ a definice jedničky, pak dostáváme :

$$x \,=\, x \cdot e \,=\, x \cdot (a \cdot y) \,=\, (x \cdot a) \cdot y \,=\, e \cdot y \,=\, y \qquad \blacksquare$$

Označení.
Z předchozí věty plyne, že když v pologrupě k prvku a existuje prvek inverzní, pak je jediný. V takovém případě budeme tento jediný inverzní prvek k prvku a označovat symbolem a^{-1} (při multiplikativní symbolice) nebo symbolem $-a$ (při aditivní symbolice).

Věta 1. 4.
Nechť $(G, \cdot)$ je pologrupa s jedničkou e . Nechť $a, b \in G$ jsou prvky, k nimž v $(G, \cdot)$ existují inverzní prvky a^{-1}, b^{-1}. Pak platí :

1. $e^{-1} \,=\, e$
2. $(a^{-1})^{-1} \,=\, a$
3. $(a \cdot b)^{-1} \,=\, b^{-1} \cdot a^{-1}$.

Důkaz.
1. a 2. část věty plynou okamžitě z definice inverzního prvku k prvku e a definice inverzního prvku k prvku a^{-1} (rozepište si sami příslušné definice).

3. tvrzení říká, že inverzním prvkem k prvku $a \cdot b$ má být prvek $(b^{-1} \cdot a^{-1})$. Ověříme tedy pro tento prvek definici inverzního prvku k prvku $a \cdot b$. Tedy:

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) \,=\, a \cdot (b \cdot b^{-1}) \cdot a^{-1} \,=\, a \cdot e \cdot a^{-1} \,=\, a \cdot a^{-1} \,=\, e$$

$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) \,=\, b^{-1} \cdot (a^{-1} \cdot a) \cdot b \,=\, b^{-1} \cdot e \cdot b \,=\, b^{-1} \cdot b \,=\, e$$

a dostáváme tak, že prvek $(b^{-1} \cdot a^{-1})$ je opravdu inverzním prvkem k prvku $a \cdot b$. $\blacksquare$

Zkusíme-li se zamyslet nad známými příklady pologrup, pak zjistíme, že bude zřejmě užitečné požadovat, aby daná pologrupa měla neutrální prvek a navíc, aby v ní ke každému prvku existoval prvek inverzní. Tato úvaha nás vede k následující definici.

Definice.
Nechť $(G, \cdot)$ je pologrupa s jedničkou, ve které ke každému prvku existuje prvek inverzní. Potom se $(G, \cdot)$ nazývá **grupa**.
Je-li operace $\cdot$ navíc komutativní, pak se grupa $(G, \cdot)$ nazývá **komutativní grupa** (nebo též abelovská grupa).

Příklad 1. 5.

1. Značí-li $+$ obyčejné sčítání čísel, pak $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, jsou komutativní grupy.

2. Značí-li $\cdot$ obyčejné násobení čísel, pak $(\mathbb{Q}-\{0\}, \cdot)$, $(\mathbb{R}-\{0\}, \cdot)$, $(\mathbb{C}-\{0\}, \cdot)$, $(\mathbb{R}^+, \cdot)$ (kde $\mathbb{R}^+$ je množina všech kladných reálných čísel) jsou komutativní grupy.

3. Nechť $G = \{ x \in \mathbb{C} \mid |x| = 1 \}$, tzn. G je množina všech komplexních čísel ležících na jednotkové kružnici a nechť $\cdot$ značí násobení komplexních čísel. Pak $(G, \cdot)$ je komutativní grupa (která má zřejmě nekonečně mnoho prvků).

4. Nechť n je pevné přirozené číslo a nechť G_n značí množinu všech $n-$tých odmocnin z jedné v oboru komplexních čísel, tak jak jsme o nich hovořili v kapitole o komplexních číslech. Tedy:
$$G_n = \{ z \in \mathbb{C} \mid z^n = 1 \}.$$
Nechť $\cdot$ značí násobení komplexních čísel. Pak $(G_n, \cdot)$ je komutativní grupa, která má n prvků (tento fakt plyne z vět 3.2. a 3.3. o komplexních číslech z 1. části textu).

   Vidíme, že uvedeným způsobem je možno sestrojit komutativní grupu, která má libovolný, předem daný konečný počet prvků.

5. Nechť $n \in \mathbb{N}$. Na množině $\mathbb{R}^n$ všech uspořádaných $n-$tic reálných čísel definujeme operaci $+$ takto: pro libovolné $(a_1, \ldots, a_n), (b_1, \ldots, b_n) \in \mathbb{R}^n$ položme
$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$
kde symboly $+$ na pravé straně značí obyčejné sčítání čísel (stručně též říkáme, že "sčítání je definováno po složkách"). Potom $(\mathbb{R}^n, +)$ je komutativní grupa.

   Rozepsáním se lehce ukáže, že neutrálním prvkem (nulou) této grupy je uspořádaná $n-$tice $(0, 0, \ldots, 0)$, a dále, že opačným prvkem k prvku $(a_1, a_2, \ldots, a_n)$ je uspořádaná $n-$tice $(-a_1, -a_2, \ldots, -a_n)$.

6. Nechť $A = \{a, b, c\}$ a nechť G značí množinu všech bijektivních zobrazení množiny A na množinu A (kterých je celkem 6 – nakreslete si je!). Nechť dále $\circ$ značí skládání zobrazení. Potom $(G, \circ)$ je grupa, která není komutativní.

   To, že $(G, \circ)$ je grupa, bezprostředně vyplývá ze základních vlastností zobrazení (rozmyslete si podrobně sami – užijte přitom příslušná tvrzení a úvahy z kapitoly 5., z první části tohoto textu).

Ukažme, že tato grupa není komutativní. Vezměme například zobrazení $f, g \in G$, definovaná:

$$f(a) = b,\ f(b) = c,\ f(c) = a \qquad \text{a} \qquad g(a) = c,\ g(b) = b,\ g(c) = a$$

Potom dostáváme: $(f \circ g)(a) = f(c) = a$, a $(g \circ f)(a) = g(b) = b$, odkud již ihned plyne, že $f \circ g \neq g \circ f$, a tedy operace $\circ$ není komutativní.

Poslední příklad je důležitým příkladem nekomutativní grupy. Je vidět, že stejným způsobem je možno sestrojit sestrojit další nekomutativní grupy:

- vezmeme-li za výchozí množinu libovolnou konečnou množinu G o n prvcích ($n \geq 3$), potom je počet bijekcí G na G roven číslu n faktoriál a dostáváme nekomutativní grupu o $n!$ prvcích (roli prvků hrají bijekce G na G, operací je skládání zobrazení).
- vezmeme-li za výchozí množinu G nějakou nekonečnou množinu, pak bijekcí G na G je nekonečně mnoho a dostáváme tak nekonečnou nekomutativní grupu, kde opět roli prvků hrají bijekce G na G a operací je skládání zobrazení.

Další důležitý příklad komutativní grupy, která má konečný počet prvků, ukáže následující věta. Předtím však na množině $\mathbb{Z}_m$ zbytkových tříd podle modulu m definujeme operaci, kterou nazveme "sčítání zbytkových tříd".

Definice.
Nechť $\mathbb{Z}_m = \{C_0, C_1, \ldots, C_{m-1}\}$ je množina všech zbytkových tříd podle modulu m. Na množině $\mathbb{Z}_m$ definujeme operaci **sčítání zbytkových tříd podle modulu** m takto: pro $C_i, C_j \in \mathbb{Z}_m$ položíme:

(2) $$C_i + C_j = C_r, \qquad \text{kde } r \text{ je zbytek po dělení čísla } (i+j) \text{ číslem } m.$$

Poznámka.
Připomeňme, že symbol + je ve vztahu (2) použit dvakrát, a to vždy v jiném významu; jednou jako symbol pro právě definovanou operaci na množině $\mathbb{Z}_m$ a podruhé pro obyčejné sčítání čísel.

Dále poznamenejme, že definici sčítání zbytkových tříd, která byla ve (2) popsána slovně, je možné přepsat pomocí věty o dělení se zbytkem celých čísel následovně:

(3) $$C_i + C_j = C_r, \qquad \text{kde } \ i + j = z \cdot m + r \quad \wedge \quad 0 \leq r < m$$

kde z je vhodné celé číslo.

Věta 1. 5.
Nechť $\mathbb{Z}_m = \{C_0, C_1, \ldots, C_{m-1}\}$ je množina zbytkových tříd podle modulu m a nechť $+$ je operace sčítání zbytkových tříd podle modulu m. Potom $(\mathbb{Z}_m, +)$ je komutativní grupa.

Důkaz.

1. z definice sčítání zbytkových tříd ihned plyne, že $(\mathbb{Z}_m, +)$ je grupoid, který je navíc zřejmě komutativní.
2. dokážeme, že operace + je asociativní. Nechť tedy $C_i, C_j, C_k \in \mathbb{Z}_m$ jsou libovolné zbytkové třídy podle modulu m. Označme nejprve:

$$C_i + C_j = C_r \qquad \text{a} \qquad (C_i + C_j) + C_k = C_s\,.$$

Při tomto označení pak (podle (3)) platí:

$$i + j = z_1 m + r \quad \wedge \quad 0 \le r < m \qquad \text{a} \qquad r + k = z_2 m + s \quad \wedge \quad 0 \le s < m\,,$$

odkud $r = i + j - z_1 m$ a po dosazení: $i + j - z_1 m + k = z_2 m + s$. Tedy:

$$i + j + k = (z_1 + z_2) \cdot m + s \qquad \wedge \qquad 0 \le s < m\,. \tag{4}$$

Podobně označme:

$$C_j + C_k = C_t \qquad \text{a} \qquad C_i + (C_j + C_k) = C_u\,.$$

Při tomto označení pak (opět podle (3)) platí:

$$j + k = z_3 m + t \quad \wedge \quad 0 \le t < m \qquad \text{a} \qquad i + t = z_4 m + u \quad \wedge \quad 0 \le u < m\,,$$

odkud po stejné úpravě a dosazení jako výše dostáváme:

$$i + j + k = (z_3 + z_4) \cdot m + u \qquad \wedge \qquad 0 \le u < m\,. \tag{5}$$

Ale vztahy (4) a (5) říkají, že číslo $(i+j+k)$ dává po dělení číslem m jednou zbytek s a podruhé zbytek u. Podle věty o dělení celých čísel je však zbytek určen jednoznačně, a tedy musí být $s = u$, neboli $C_s = C_u$, což však znamená, že

$$(C_i + C_j) + C_k = C_i + (C_j + C_k)\,.$$

3. neutrálním prvkem (nulou) v $(\mathbb{Z}_m, +)$ je zřejmě zbytková třída C_0, neboť z definice sčítání zbytkových tříd ihned plyne, že pro libovolné $C_i \in \mathbb{Z}_m$ je: $C_i + C_0 = C_i$.
4. zbývá dokázat, že ke každému prvku $C_i \in \mathbb{Z}_m$ existuje prvek opačný. Ale:
   - je-li $C_i = C_0$, pak opačným prvkem k C_0 je zřejmě prvek C_0
   - je-li $C_i \neq C_0$, pak opačným prvkem k C_i je prvek C_{m-i}, neboť $C_{m-i} \in \mathbb{Z}_m$ a platí (rozmyslete si, proč): $C_i + C_{m-i} = C_0$. ■

Úmluva.
Abychom zjednodušili a zkrátili zápis při práci se zbytkovými třídami, zavedeme úmluvu, že podle potřeby budeme při označování zbytkových tříd používat místo symbolu C_i pouze symbol i. V souvislosti s tím je však nutné mít neustále na paměti, že symbol i potom neznamená číslo, ale je to jenom jiný zápis pro příslušnou zbytkovou třídu a je tedy nutné se symbolem i zacházet jako se zbytkovou třídou a nikoliv jako s číslem.

Pracujeme-li s grupou zbytkových tříd $(\mathbb{Z}_m, +)$ pro nějaké konkrétní (ne příliš velké) m, potom bývá užitečné si setrojit tabulku operace $+$. Například pro modul $m = 6$ dostáváme následující tabulku.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

V praxi se často setkáváme s případem, že máme dánu nějakou pologrupu a máme o ní dokázat, že je grupou. Nalezení jedničky je většinou jednoduché. Technicky složitější bývá důkaz toho, že ke každému prvku existuje prvek inverzní. Následující věta ukáže, že v takovém případě (bez ohledu na to, zda je zadaná operace komutativní či nekomutativní) stačí ověřovat pouze "polovinu" příslušné definice.

Věta 1.6. *Nechť $(G,\cdot)$ je pologrupa s jedničkou e. Pak následující výroky jsou ekvivalentní:*

1. *ke každému prvku $a \in G$ existuje prvek inverzní*
2. *ke každému prvku $a \in G$ existuje prvek $x \in G$ tak, že $x \cdot a = e$*
3. *ke každému prvku $a \in G$ existuje prvek $x \in G$ tak, že $a \cdot x = e$*

Důkaz.
Je okamžitě vidět, že implikace "$1 \Rightarrow 2$" a implikace "$1 \Rightarrow 3$" zřejmě platí.

Důkaz implikace "$2 \Rightarrow 1$" .
Nechť $a \in G$ je libovolný prvek. Pak podle 2 existuje prvek $x \in G$ tak, že $x \cdot a = e$ a následně, opět podle 2, k prvku x existuje prvek z tak, že $z \cdot x = e$. Potom po dosazení a úpravě dostáváme:

$$a \cdot x \;=\; e \cdot (a \cdot x) \;=\; (z \cdot x) \cdot (a \cdot x) \;=\; z \cdot (x \cdot a) \cdot x \;=\; z \cdot e \cdot x \;=\; z \cdot x \;=\; e\,.$$

Tedy prvek x je inverzním prvkem k prvku a, což znamená, že platí 1.

Důkaz implikace "$3 \Rightarrow 1$" se provede analogicky. ■

Definice.
Nechť $(G,\cdot)$ je grupoid. Potom:

1. řekneme, že v grupoidu $(G,\cdot)$ platí **zákony o dělení**, jestliže pro každé $a, b \in G$ platí:
$$\exists\, x \in G \text{ tak, že } a \cdot x = b \qquad \wedge \qquad \exists\, y \in G \text{ tak, že } y \cdot a = b$$
2. řekneme, že v grupoidu $(G,\cdot)$ platí **zákony o krácení**, jestliže pro každé $a, b, c \in G$ platí:
$$c \cdot a = c \cdot b \;\Rightarrow\; a = b \qquad \wedge \qquad a \cdot c = b \cdot c \;\Rightarrow\; a = b\,.$$

Následující věta ukáže, že v definici grupy je možné požadavek existence jedničky a existence inverzního prvku ke každému prvku nahradit požadavkem platnosti zákonů o dělení.

Věta 1.7.
Nechť $(G,\cdot)$ je pologrupa. Pak platí: $(G,\cdot)$ je grupa $\Leftrightarrow$ v $(G,\cdot)$ platí zákony o dělení.

Důkaz.
Důkaz implikace "$\Rightarrow$" .
Nechť $(G,\cdot)$ je grupa a nechť $a, b \in G$ jsou libovolné prvky. Jestliže položíme: $x = a^{-1} \cdot b$ a $y = b \cdot a^{-1}$ (uvědomme si, že z definice grupy plyne existence prvku a^{-1}), potom dostáváme: $a \cdot x = a \cdot (a^{-1} \cdot b) = b$ a dále $y \cdot a = (b \cdot a^{-1}) \cdot a = b$. Dokázali jsme tedy, že v $(G,\cdot)$ platí zákony o dělení.

Důkaz implikace "$\Leftarrow$".
Nechť v pologrupě $(G, \cdot)$ platí zákony o dělení. Důkaz toho, že $(G, \cdot)$ je grupou rozdělíme na dvě části.

1. Dokážeme, že v $(G, \cdot)$ existuje jednička.
   Nechť $a, b \in G$ jsou libovolné prvky. Pak z platnosti zákonů o dělení plyne, že existují prvky $x, y, e, e' \in G$ takové, že platí:
   $$a \cdot x = b \quad \wedge \quad y \cdot a = b \qquad \wedge \qquad a \cdot e = a \quad \wedge \quad e' \cdot a = a$$
   Nyní postupným dosazováním z těchto vztahů dostáváme:
   $$b \cdot e = (y \cdot a) \cdot e = y \cdot (a \cdot e) = y \cdot a = b \tag{6}$$
   $$e' \cdot b = e' \cdot (a \cdot x) = (e' \cdot a) \cdot x = a \cdot x = b\,. \tag{7}$$
   Ale prvek b byl libovolný, tzn. ze (6) pro $b = e'$ dostáváme $e' \cdot e = e'$ a podobně ze (7) pro $b = e$ dostáváme $e' \cdot e = e$.
   Je tedy $e' = e$ a po dosazení e za e' do (7) pak ze (6) a (7) plyne, že prvek e je jedničkou v $(G, \cdot)$.
2. Dokážeme, že v $(G, \cdot)$ ke každému prvku existuje prvek inverzní.
   Nechť $a \in G$ je libovolný prvek. Z platnosti zákonů o dělení plyne, že existují prvky $x, y \in G$ tak, že platí: $a \cdot x = e \quad \wedge \quad y \cdot a = e$. Nyní už jenom stačí dokázat, že $y = x$. Ale:
   $$y = y \cdot e = y \cdot (a \cdot x) = (y \cdot a) \cdot x = e \cdot x = x\,.$$
   Dokázali jsme tedy, že prvek x je hledaným inverzním prvkem k prvku a.
   Dohromady potom z 1. a 2. dostáváme, že $(G, \cdot)$ je grupa. ■

Věta 1. 8.
Nechť $(G, \cdot)$ je grupa. Pak v $(G, \cdot)$ platí zákony o krácení.

Důkaz.
Nechť $(G, \cdot)$ je grupa a nechť $a, b, c \in G$ jsou prvky, pro které platí: $c \cdot a = c \cdot b$. Vynásobíme-li tuto rovnost zleva prvkem c^{-1} (který musí existovat, protože $(G, \cdot)$ je grupa), dostáváme: $c^{-1} \cdot (c \cdot a) = c^{-1} \cdot (c \cdot b)$, odkud po přezávorkování a výpočtu dostáváme, že $a = b$.
Analogickým způsobem se dokáže implikace $a \cdot c = b \cdot c \quad \Rightarrow \quad a = b$. ■

Poznámka.
Poznamenejme, že předchozí větu nelze obrátit (v tom smyslu, že z platnosti zákonů o krácení obecně neplyne, že grupoid nebo pologrupa je grupou). Například v pologrupě $(\mathbb{N}, \cdot)$ platí zákony o krácení, ale přitom $(\mathbb{N}, \cdot)$ není grupou.

Na závěr kapitoly nyní zavedeme pojem celočíselné mocniny prvku v grupě a odvodíme pro něj základní početní pravidla. Uvidíme, že pravidla pro počítání s celočíselnými mocninami prvků v grupě jsou analogická podobným pravidlům pro počítání s čísly, známými ze střední školy.

Definice.
Nechť $(G, \cdot)$ je grupa, jejíž jedničkou je e, nechť $a \in G$ a nechť $r \in \mathbb{Z}$. Pak **celočíselná mocnina prvku** a je definována takto:

$$a^r = \begin{cases} \underbrace{a \cdot a \cdot \ldots \cdot a}_{r\text{-krát}} & \text{je-li } r \text{ celé kladné číslo} \\ e & \text{je-li } r = 0 \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{(-r)\text{-krát}} & \text{je-li } r \text{ celé záporné číslo} \end{cases}$$

Věta 1. 9.
Nechť $(G, \cdot)$ je grupa a nechť r, s jsou libovolná celá čísla. Pak pro libovolný prvek $a \in G$ platí:

1. $a^r \cdot a^s = a^{r+s}$
2. $(a^r)^s = a^{r \cdot s}$.

Důkaz.
Důkaz obou tvrzení provedeme najednou a rozdělíme jej na tři části, podle možných hodnot r, s. Nechť tedy $a \in G$ je libovolný prvek.

I. pro $r > 0 \wedge s > 0$ nebo $r = 0 \wedge s$ libovolné celé nebo $s = 0 \wedge r$ libovolné celé plynou obě tvrzení přímo z předchozí definice celočíselné mocniny prvku a.

II. nechť je $r < 0 \wedge s < 0$. Potom:

$$a^r \cdot a^s = (\underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{(-r)\text{-krát}}) \cdot (\underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{(-s)\text{-krát}}) = \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{(-r-s)\text{-krát}} = a^{r+s}$$

což je první z dokazovaných vztahů.

Dokážeme druhý vztah. Z definice celočíselné mocniny prvku a z věty 1.4.3 plyne (užitím matematické indukce), že pro libovolné přirozené k je $a^{-k} = (a^{-1})^k = (a^k)^{-1}$. Využitím tohoto faktu a věty 1.4.2 pak dostáváme:

$$(a^r)^s = ((a^{-r})^{-1})^s = (((a^{-r})^{-1})^{-s})^{-1} = (((a^{-r})^{-s})^{-1})^{-1} = (a^{-r})^{-s}.$$

Ale $-r > 0 \wedge -s > 0$, tzn. podle I. je: $(a^{-r})^{-s} = a^{(-r)(-s)} = a^{r \cdot s}$. Dohromady tak pro tento případ dostáváme, že $(a^r)^s = a^{r \cdot s}$.

III. případ $r < 0 \wedge s > 0$ a případ $r > 0 \wedge s < 0$ se dokazují analogickými úvahami jako v předchozích částech důkazu. Poznamenejme, že důkaz této části věty je poměrně rozsáhlý a technicky nepříjemný. ■

Poznámka.
Používáme-li aditivního zápisu operace, tzn. máme-li grupu $(G, +)$, jejímž neutrálním prvkem je o, pak místo názvu "celočíselná mocnina prvku a" budeme používat název **celočíselný násobek prvku** a, který je tedy definován následujícím způsobem:

$$r \cdot a \;=\; \begin{cases} \underbrace{a + a + \cdots + a}_{r\text{-krát}} & \text{je-li } \; r \text{ celé kladné číslo} \\ o & \text{je-li } \; r = 0 \\ \underbrace{(-a) + (-a) + \cdots + (-a)}_{(-r)\text{-krát}} & \text{je-li } \; r \text{ celé záporné číslo} \end{cases}$$

V tomto případě má potom předchozí věta formálně jiný tvar, a sice:

Nechť $(G, +)$ je grupa a nechť $r, s \in \mathbb{Z}$. Pak pro libovolný prvek $a \in G$ platí:

1. $(r \cdot a) + (s \cdot a) \;=\; (r + s) \cdot a$
2. $s \cdot (r \cdot a) \;=\; (s \cdot r) \cdot a$.

Zde je potřeba dávat obzvláštní pozor na použité symboly, přesněji řečeno na to, že jeden symbol může být použit ve dvou významech. Například, ve vztahu 1. znamená symbol $+$ na levé straně operaci v dané grupě, zatímco symbol $+$ na pravé straně znamená obyčejné sčítání celých čísel. Podobně, ve vztahu 2. je symbol $\cdot$ použit čtyřikrát, přičemž třikrát značí celočíselný násobek prvků z G a jedenkrát obyčejné násobení čísel.

2. Podstruktury algebraických struktur s jednou operací.

Definice.
Nechť $(G, \cdot)$ je grupoid a nechť H je neprázdná podmnožina množiny G. Pak řekneme, že podmnožina H je **uzavřená vzhledem k operaci** $\cdot$, jestliže platí:

$$a, b \in H \text{ libovolné } \Rightarrow \quad a \cdot b \in H .$$

Poznámka.
Je-li dán grupoid $(G, \cdot)$ a podmnožina $H \subseteq G$ je uzavřená vzhledem k operaci $\cdot$, pak můžeme na množině H přirozeným způsobem definovat operaci, označme ji třeba $*$, takto:

$$\text{pro libovolné } x, y \in H \text{ položíme } x * y = x \cdot y .$$

Tímto způsobem dostáváme grupoid $(H, *)$. Z praktických důvodů zaveďme úmluvu, že operaci $*$ na množině H budeme všude v dalším vždy značit stejným symbolem jako původní operaci na množině G. Máme tedy grupoid $(H, \cdot)$, pro který zavedeme následující pojmenování.

Definice.
Nechť $(G, \cdot)$ je grupoid a nechť neprázdná podmnožina $H \subseteq G$ je uzavřená vzhledem k operaci $\cdot$. Pak grupoid $(H, \cdot)$ se nazývá **podgrupoid grupoidu** $(G, \cdot)$.

Věta 2. 1.
Nechť $(H, \cdot)$ je podgrupoid grupoidu $(G, \cdot)$. Pak platí:

1. *$(G, \cdot)$ je asociativní $\Rightarrow$ $(H, \cdot)$ je asociativní*
2. *$(G, \cdot)$ je komutativní $\Rightarrow$ $(H, \cdot)$ je komutativní*
3. *prvek e je jedničkou v $(G, \cdot)$ $\wedge$ $e \in H$ $\Rightarrow$ e je jedničkou v $(H, \cdot)$.*

Důkaz.
Všechna tři tvrzení plynou okamžitě z příslušných definic. ■

Poznamenejme, že žádnou z implikací v předchozí větě nelze obrátit. Například v grupoidu $(G, \cdot)$ z příkladu 1. 2. je $(\{d\}, \cdot)$ podgrupoidem, který je asociativní, je komutativní a má jedničku d, zatímco celý grupoid $(G, \cdot)$ není asociativní, není komutativní a prvek d není jeho jedničkou.

Definice.
Nechť $(G, \cdot)$ je grupa a nechť $(H, \cdot)$ je podgrupoid v $(G, \cdot)$, který je sám grupou. Potom $(H, \cdot)$ se nazývá **podgrupa grupy** $(G, \cdot)$.

Věta 2. 2.
Nechť $(H, \cdot)$ je podgrupa grupy $(G, \cdot)$. Pak platí:

1. *jednička podgrupy $(H, \cdot)$ je totožná s jedničkou grupy $(G, \cdot)$*
2. *je-li $a \in H$, pak inverzní prvek k prvku a v podgrupě $(H, \cdot)$ je totožný s inverzním prvkem k prvku a v grupě $(G, \cdot)$.*

Důkaz.

1. nechť e_H značí jedničku v $(H, \cdot)$ a e_G značí jedničku v $(G, \cdot)$. Pak platí:

$$e_H \cdot e_H = e_H \qquad \text{(protože } e_H \text{ je jedničkou v } (H, \cdot)\text{)}$$

$$e_G \cdot e_H = e_H \qquad \text{(protože } e_G \text{ je jedničkou v } (G, \cdot)\text{)}.$$

   Je tedy $e_H \cdot e_H = e_G \cdot e_H$, odkud užitím zákona o krácení (který v grupě platí) dostáváme, že $e_H = e_G$.

2. nechť $a \in H$ libovolný a nechť x značí inverzní prvek k prvku a v podgrupě $(H, \cdot)$, resp. y značí inverzní prvek k prvku a v grupě $(G, \cdot)$. Potom je:

$$a \cdot x = e_H = e_G \qquad \wedge \qquad a \cdot y = e_G$$

   odkud plyne, že $a \cdot x = a \cdot y$ a užitím zákonů o krácení dostáváme, že $x = y$. ■

Poznámka.
Vzhledem k 2. části předchozí věty nemusíme rozlišovat inverzní prvek k prvku $a \in H$ v podgrupě a v celé grupě. V obou případech budeme proto inverzní prvek k prvku a označovat symbolem a^{-1}.

V praxi se budeme často setkávat s úlohou rozhodnout o tom, zda daný podgrupiod je podgrupou dané grupy či nikoliv. Je vidět, že pokud bychom postupovali přesně podle definice podgrupy, dělali bychom řadu zbytečných kroků (například ověřování toho, že v podgrupoidu platí asociativní zákon). Proto nyní uvedeme větu, která tento postup zjednoduší.

Věta 2. 3.
Nechť $(G, \cdot)$ je grupa a nechť H je neprázdná podmnožina v G. Potom následující výroky jsou ekvivalentní:

1. $(H, \cdot)$ *je podgrupa grupy* $(G, \cdot)$
2. *pro* $a, b \in H$ *libovolné platí:* $a \cdot b \in H \quad \wedge \quad a^{-1} \in H$
3. *pro* $a, b \in H$ *libovolné platí:* $a \cdot b^{-1} \in H$
4. *pro* $a, b \in H$ *libovolné platí:* $a^{-1} \cdot b \in H$

Důkaz.
Tvrzení budeme dokazovat obvyklým způsobem, tzn. dokážeme postupně čtyři implikace.

Důkaz implikace "$1 \Rightarrow 2$*".*
Platnost této implikace plyne bezprostředně z definice podgrupy.

Důkaz implikace "$2 \Rightarrow 3$*".*
Nechť platí 2. a nechť $a, b \in H$. Potom (podle 2.) je $b^{-1} \in H$ a následně opětovným užitím 2. dostáváme, že $a \cdot b^{-1} \in H$. Dokázali jsme tak platnost 3.

Důkaz implikace "$3 \Rightarrow 4$*".*
Nechť platí 3. a nechť $a, b \in H$. Podle 3. je: $a \cdot a^{-1} = e \in H$. Tedy $e, a, b \in H$ a

použitím 3. dostaneme:

$$e \cdot a^{-1} = a^{-1} \in H \qquad \text{a} \qquad e \cdot b^{-1} = b^{-1} \in H\,.$$

Je tedy $a^{-1}, b^{-1} \in H$, odkud opět podle 3. dostáváme: $a^{-1} \cdot (b^{-1})^{-1} = a^{-1} \cdot b \in H$, což znamená, že platí 4.

Důkaz implikace "$4 \Rightarrow 1$*".*
Nechť platí 4. a nechť $a, b \in H$. Podle 4. je: $a^{-1} \cdot a = e \in H$. Tedy $a, e \in H$ a podle 4. je: $a^{-1} \cdot e = a^{-1} \in H$. Je tedy $a^{-1}, b \in H$, odkud opět podle 4. dostáváme:

$$(a^{-1})^{-1} \cdot b = a \cdot b \in H\,,$$

čímž jsme dokázali, že $(H, \cdot)$ je podgrupoid v $(G, \cdot)$, který je podle věty 2.1.1 asociativní. Ale výše bylo dokázáno, že $e \in H$ a pro libovolné $a \in H$ je $a^{-1} \in H$. To znamená, že $(H, \cdot)$ je grupa, neboli $(H, \cdot)$ je podgrupa grupy $(G, \cdot)$ a platí 1. ■

Poznámka.
Jak bylo řečeno dříve, předchozí větu používáme k praktickému ověřování toho, zda je $(H, \cdot)$ podgrupou grupy $(G, \cdot)$. Obvykle postupujeme tak, že použijeme část 2., tzn. dokazujeme, že:

1. $H \subseteq G \quad \wedge \quad H \neq \emptyset$
2. $a, b \in H$ libovolné $\quad \Rightarrow \quad a \cdot b \in H$
3. $a \in H$ libovolné $\quad \Rightarrow \quad a^{-1} \in H$.

Příklad 2. 1.
Uvedeme několik užitečných příkladů podgrup v grupách.

1. Každá grupa $(G, \cdot)$ má vždy dvě podgrupy, a sice podgrupu $(\{e\}, \cdot)$ a podgrupu $(G, \cdot)$. Tyto podgrupy se nazývají **nevlastní podgrupy** grupy $(G, \cdot)$. Ostatní podgrupy (pokud existují) se potom nazývají **vlastní podgrupy** grupy $(G, \cdot)$.
2. V grupě $(\mathbb{C}, +)$ všech komplexních čísel, s operací obyčejného sčítání čísel jsou podgrupami například $(\mathbb{R}, +)$ nebo $(\mathbb{Q}, +)$ nebo $(\mathbb{Z}, +)$.
3. V grupě $(\mathbb{R} - \{0\}, \cdot)$ všech nenulových reálných čísel, s operací obyčejného násobení čísel jsou podgrupami například $(\mathbb{Q} - \{0\}, \cdot)$ nebo $(\mathbb{R}^+, \cdot)$, kde $\mathbb{R}^+$ značí množinu všech kladných reálných čísel.
4. V grupě $(\mathbb{C} - \{0\}, \cdot)$ všech nenulových komplexních čísel, s operací obyčejného násobení čísel jsou podgrupami například
   - podgrupa $(\mathbb{R} - \{0\}, \cdot)$;
   - podgrupa $(G, \cdot)$, kde $G = \{\, z \in \mathbb{C} \mid |z| = 1 \,\}$ (tzn. G je množina všech komplexních čísel, která leží na jednotkové kružnici) ;
   - podgrupa $(G_n, \cdot)$, kde n je pevné přirozené číslo a $G_n = \{\, z \in \mathbb{C} \mid z^n = 1 \,\}$ (tzn. G_n je množina všech n-tých odmocnin z 1).

   Z tohoto příkladu vidíme, že v grupě, která má nekonečný počet prvků mohou existovat podgrupy, které mají jak nekonečný, tak i konečný počet prvků.

Poznamenejme, že v grupách $(\mathbb{C}, +)$, resp. $(\mathbb{R} - \{0\}, \cdot)$, resp. $(\mathbb{C} - \{0\}, \cdot)$ existuje mnohem více podgrup, než které jsme v předchozích příkladech uvedli. Jinými slovy řečeno, uvedené příklady zdaleka nevyčerpávají všechny podgrupy v uvedených grupách. Na druhé straně je možné podat poměrně jednoduchý popis všech podgrup v grupě $(\mathbb{Z}, +)$, který si dále uvedeme. Nejprve však zavedeme jedno označení.

Označení.
Nechť k značí libovolné celé nezáporné číslo. Pak symbolem $k \cdot \mathbb{Z}$ budeme označovat množinu všech celočíselných násobků čísla k, tzn.

$$k \cdot \mathbb{Z} \;=\; \{\, k \cdot z \mid z \in \mathbb{Z} \text{ libovolné} \,\}.$$

Následující věta nyní ukáže, že všechny podgrupy v grupě $(\mathbb{Z}, +)$ jsou právě podgrupy $(k \cdot \mathbb{Z}, +)$, kde k je libovolné celé nezáporné číslo.

Věta 2. 4.
$(H, +)$ *je podgrupou grupy* $(\mathbb{Z}, +) \quad \Leftrightarrow \quad$ *existuje celé nezáporné číslo* k *tak, že* $H = k \cdot \mathbb{Z}$.

Důkaz.
Dokážeme postupně obě implikace.

Důkaz implikace "$\Rightarrow$".
Nechť $(H, +)$ je libovolná podgrupa grupy $(\mathbb{Z}, +)$. Jestliže množina H neobsahuje žádné přirozené číslo, pak musí být $H = \{0\}$ (proč?), což znamená, že $H = 0 \cdot \mathbb{Z}$ a množina H je požadovaného tvaru.

Nechť tedy množina H obsahuje alespoň jedno přirozené číslo. Potom nejmenší přirozené číslo, které náleží do množiny H, označme k (rozmyslete si, že toto číslo skutečně existuje!). Nyní dokážeme, že $H = k \cdot \mathbb{Z}$.

"$\subseteq$" nechť $x \in H$ libovolné. Pak podle věty o dělení celých čísel se zbytkem existují čísla $q, r \in \mathbb{Z}$ tak, že

$$x \;=\; q \cdot k + r \qquad \wedge \qquad 0 \le r < k\,.$$

Ale $k \in H$, tzn. potom také $-q \cdot k \in H$ (pozor - zde je nutno symbol $\cdot$ chápat ve smyslu celočíselného násobku prvku v grupě, tzn. ve smyslu "opakovaného sčítání"). Kromě toho je $x \in H$, odkud dostáváme, že: $x + (-q \cdot k) \;=\; r \in H$. Pak ale musí být $r = 0$ (jinak dostáváme spor s volbou čísla k), a tedy $x \;=\; q \cdot k \in k \cdot \mathbb{Z}$.

"$\supseteq$" nechť $x \in k \cdot \mathbb{Z}$ libovolné. Pak existuje $s \in \mathbb{Z}$ tak, že $x \;=\; k \cdot s$. Ale $k \in H$, a tedy také $s \cdot k \;=\; x \in H$. (pozor - zde opět symbol $\cdot$ chápeme ve smyslu celočíselného násobku prvku v grupě, tzn. ve smyslu "opakovaného sčítání").

Důkaz implikace "$\Leftarrow$".
Nechť $H = k \cdot \mathbb{Z}$, kde k je pevné celé nezáporné číslo. Užitím věty 2.3.2 dokážeme, že $(k \cdot \mathbb{Z}, +)$ je podgrupou grupy $(\mathbb{Z}, +)$. Tedy:

1. zřejmě je $\quad k \cdot \mathbb{Z} \subseteq \mathbb{Z} \quad \wedge \quad k \cdot \mathbb{Z} \neq \emptyset$

2. $a, b \in k \cdot \mathbb{Z} \;\Rightarrow\; \exists\, x, y \in \mathbb{Z} :\; a = k \cdot x\,,\; b = k \cdot y \;\Rightarrow\; a + b = k \cdot (x + y) \in k \cdot \mathbb{Z}$

3. $a \in k \cdot \mathbb{Z} \;\Rightarrow\; \exists\, x \in \mathbb{Z} :\; a = k \cdot x \;\Rightarrow\; -a = k \cdot (-x) \in k \cdot \mathbb{Z}$. ■

Vidíme tedy, že v grupě $(\mathbb{Z}, +)$ existuje nekonečně mnoho podgrup, které musí být výše popsaného tvaru. Specielně, podgrupami grupy $(\mathbb{Z}, +)$ jsou například: $0 \cdot \mathbb{Z} = \{0\}$, $1 \cdot \mathbb{Z} = \mathbb{Z}$, $2 \cdot \mathbb{Z}$ (což je množina všech celých sudých čísel), $3 \cdot \mathbb{Z}$ (což je množina všech celočíselných násobků čísla 3), atd.

Podobným způsobem, jako jsme popsali všechny podgrupy v grupě celých čísel $(\mathbb{Z}, +)$, se dají charakterizovat všechny podgrupy v grupě zbytkových tříd $(\mathbb{Z}_m, +)$. Podrobný důkaz nebudeme v tomto případě provádět, ale pouze si všechny podgrupy popíšeme. Přitom platí:

1. podgrup v grupě $(\mathbb{Z}_m, +)$ je tolik, kolik je přirozených dělitelů čísla m.
2. je-li k přirozeným dělitelem čísla m, potom jemu odpovídající podgrupou je podgrupa

$$(\{C_0\,,\ C_k\,,\ C_{2k}\,,\ \ldots\ ,\ C_{m-k}\}\,,+)\,.$$

   Všimněme si, jak je podgrupa odpovídající děliteli k zkonstruována. Patří do ní vždy zbytková třída C_0 a následně další zbytkové třídy, které dostaneme tak, že k indexu předchozí zbytkové třídy přičítáme číslo k, a to provádíme tak dlouho, "dokud to jde".

Příklad 2.2.

1. Je-li m prvočíslo, potom má grupa $(\mathbb{Z}_m, +)$ pouze nevlastní podgrupy, tzn. podgrupy

$$(\mathbb{Z}_m, +) \qquad \text{a} \qquad (\{C_0\}, +)\,,$$

   které odpovídají postupně dělitelům 1 a m daného modulu m.

2. Vypišme všechny podgrupy v grupě $(\mathbb{Z}_6, +)$.

   Číslo 6 má čtyři přirozené dělitele, a sice $1, 2, 3, 6$, a grupa $(\mathbb{Z}_6, +)$ má tedy právě následující čtyři podgrupy:

   $(\{C_0, C_1, C_2, C_3, C_4, C_5\}\,,+) \;=\; (\mathbb{Z}_6\,,+)\,,$

   $(\{C_0, C_2, C_4\}\,,+)\,,$

   $(\{C_0, C_3\}\,,+)\,,$

   $(\{C_0\}\,,+)\,.$

3. Algebraické struktury se dvěma operacemi.

V tomto paragrafu se budeme zabývat algebraickými strukturami se dvěma operacemi, tzn. množinami, na kterých jsou definovány dvě operace. Přitom pro jednu operaci budeme používat aditivní symboliku a pro druhou operaci multiplikativní symboliku. Uvidíme, že zaváděné pojmy budou opět do jisté míry zobecňovat vlastnosti běžných algebraických struktur se dvěma operacemi, se kterými se pracuje na střední škole, tj. celých čísel, resp. racionálních čísel nebo reálných čísel s operacemi obyčejného sčítání a násobení čísel.

Definice.
Nechť R je množina se dvěma operacemi $+$ a $\cdot$ taková, že platí:

1. $(R, +)$ je komutativní grupa
2. $(R, \cdot)$ je pologrupa
3. platí distributivní zákony, tzn. pro každé $a, b, c \in R$ platí:

$$a \cdot (b + c) \;=\; a \cdot b \;+\; a \cdot c \qquad \wedge \qquad (a + b) \cdot c \;=\; a \cdot c \;+\; b \cdot c$$

Pak množina R s operacemi $+$ a $\cdot$ se nazývá **okruh** a označuje se $(R, +, \cdot)$.

Jestliže navíc

- operace $\cdot$ je komutativní, potom se okruh $(R, +, \cdot)$ nazývá **komutativní okruh**
- pologrupa $(R, \cdot)$ má neutrální prvek (jedničku), potom se okruh $(R, +, \cdot)$ nazývá **okruh s jedničkou**.

Poznámka.

1. Operaci $+$ v okruhu $(R, +, \cdot)$ budeme nazývat sčítání. Neutrální prvek grupy $(R, +)$ budeme nazývat **nula okruhu** $(R, +, \cdot)$ a označovat symbolem 0. Opačný prvek k prvku a budeme označovat symbolem $-a$. Místo zápisu $a + (-b)$ budeme používat stručnější zápis: $a - b$.
2. Operaci $\cdot$ v okruhu $(R, +, \cdot)$ budeme nazývat násobení. Neutrální prvek pologrupy $(R, \cdot)$ budeme (jak je vidět z definice) nazývat **jednička okruhu** $(R, +, \cdot)$ a označovat symbolem 1. Tento symbol pochopitelně nemá obecně nic společného s číslem 1.
3. Pokud se v některém výrazu objeví obě operace bez uzávorkování (jako například na pravých stranách distributivních zákonů), pak budeme vždy předpokládat, že násobení "má přednost" před sčítáním, tzn. budeme dodržovat stejnou úmluvu, jaká se na střední škole zavádí pro obyčejné násobení a sčítání čísel.

Příklad 3. 1.

1. Značí–li $+$, resp. $\cdot$ obyčejné sčítání, resp. obyčejné násobení čísel, pak $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ a $(\mathbb{C}, +, \cdot)$ jsou okruhy.

   Dalšími okruhy jsou pak například:

   $(\mathbb{Z}[\sqrt{2}], +, \cdot)$, kde $\mathbb{Z}[\sqrt{2}] \;=\; \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$

   $(\mathbb{Q}(\sqrt{2}), +, \cdot)$, kde $\mathbb{Q}(\sqrt{2}) \;=\; \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

2. Na množině $\mathbb{R} \times \mathbb{R}$ definujme operace $+$ a $\cdot$ takto: pro libovolné $(a,b),(c,d) \in \mathbb{R} \times \mathbb{R}$ položme

$$(a,b) + (c,d) = (a+c\,,\, b+d) \qquad \text{a} \qquad (a,b) \cdot (c,d) = (a \cdot c\,,\, b \cdot d)$$

kde symboly $+$ a $\cdot$ na pravých stranách značí obyčejné sčítání a násobení čísel. Potom $(\mathbb{R} \times \mathbb{R}\,, +\,, \cdot\,)$ je okruh.

3. Je-li R jednoprvková množina, například $R = \{x\}$, pak je zřejmě možno definovat na množině R operaci pouze jedním způsobem. Položíme-li nyní:

$$x + x = x \qquad \text{a} \qquad x \cdot x = x$$

potom $(R\,, +\,, \cdot\,)$ je okruh, který budeme nazývat **triviální okruh**. Triviální okruh je jakýmsi "nepřirozeným" příkladem okruhu, ve kterém obě operace splývají, a proto jej často budeme z našich úvah vylučovat.

4. Všechny doposud uvedené příklady okruhů byly komutativní okruhy. Jednoduchý příklad nekomutativního okruhu bude uveden v kurzu lineární algebry, v souvislosti se studiem matic.

Další důležitý příklad okruhu je možno sestrojit na množině $\mathbb{Z}_m$ zbytkových tříd podle modulu m. Připomeňme, že na množině $\mathbb{Z}_m = \{C_0\,, C_1\,, \ldots\,, C_{m-1}\}$ jsme již dříve definovali operaci sčítání $+$ takto: pro $C_i, C_j \in \mathbb{Z}_m$ jsme položili

$$C_i + C_j = C_r\,, \qquad \text{kde } r \text{ je zbytek po dělení čísla } i+j \text{ číslem } m\,.$$

Analogickým způsobem nyní definujeme na množině $\mathbb{Z}_m$ operaci násobení zbytkových tříd.

Definice.
Na množině $\mathbb{Z}_m$ všech zbytkových tříd podle modulu m definujeme operaci **násobení zbytkových tříd** podle modulu m (kterou označíme symbolem $\cdot$) takto: pro $C_i, C_j \in \mathbb{Z}_m$ položíme:

$$C_i \cdot C_j = C_s\,, \qquad \text{kde } s \text{ je zbytek po dělení čísla } i \cdot j \text{ číslem } m\,.$$

Poznamenejme, že definici násobení zbytkových tříd podle modulu m je možné (rozepsáním věty o dělení se zbytkem celých čísel) formálně přepsat do tvaru:

$$C_i \cdot C_j = C_s\,, \qquad \text{kde } i \cdot j = z \cdot m + s \quad \wedge \quad 0 \leq s < m\,,$$

kde z značí celé číslo.

Věta 3. 1.
Nechť $\mathbb{Z}_m = \{C_0\,, C_1\,, \ldots\,, C_{m-1}\}$ je množina zbytkových tříd podle modulu m. Pak $(\mathbb{Z}_m\,, +\,, \cdot\,)$ je okruh. Tento okruh je komutativním okruhem s jedničkou.

Důkaz.
Operace násobení zbytkových tříd je zřejmě komutativní. Budeme tedy pouze ověřovat definici okruhu a existenci jedničky.

1. $(\mathbb{Z}_m\,, +\,)$ je komutativní grupa (podle věty 1. 5).

2. $(\mathbb{Z}_m\,, \cdot\,)$ je zřejmě grupoid. Analogickým způsobem jako ve větě 1. 5 se dokáže, že operace $\cdot$ je asociativní, tzn. $(\mathbb{Z}_m\,, \cdot\,)$ je pologrupa.

3. Dokážeme platnost distributivních zákonů.
   Vzhledem k tomu, že operace násobení zbytkových tříd je komutativní, stačí dokázat pouze jeden z obou distributivních zákonů. Nechť tedy $C_i, C_j, C_k \in \mathbb{Z}_m$ a budeme dokazovat vztah:

$$(C_i + C_j) \cdot C_k = C_i \cdot C_k + C_j \cdot C_k .$$

   Označme nejprve

$$C_i + C_j = C_r \qquad \text{a} \qquad (C_i + C_j) \cdot C_k = C_s .$$

   Při tomto označení pak platí:

$$i + j = z_1 \cdot m + r \ \wedge \ 0 \leq r < m \quad \text{a} \quad r \cdot k = z_2 \cdot m + s \ \wedge \ 0 \leq s < m$$

   odkud $r = i + j - z_1 \cdot m$ a po dosazení: $(i + j - z_1 \cdot m) \cdot k = z_2 \cdot m + s$, tzn.

(1) $$i \cdot k + j \cdot k = (z_1 \cdot k + z_2) \cdot m + s \qquad \wedge \qquad 0 \leq s < m .$$

   Podobně označme:

$$C_i \cdot C_k = C_u \quad , \quad C_j \cdot C_k = C_v \qquad \text{a} \qquad C_i \cdot C_k + C_j \cdot C_k = C_t .$$

   Při tomto označení platí:

$$i \cdot k = z_3 \cdot m + u \quad , \quad j \cdot k = z_4 \cdot m + v \quad , \quad u + v = z_5 \cdot m + t$$

   kde $0 \leq u, v, t < m$. Nyní po úpravě a dosazení, podobně jako předtím, dostáváme:

(2) $$i \cdot k + j \cdot k = (z_3 + z_4 + z_5) \cdot m + t \qquad \wedge \qquad 0 \leq t < m .$$

   Ale z (1) a (2) užitím věty o dělení se zbytkem (zbytek je určen jednoznačně!) dostáváme, že $s = t$, a tedy i $C_s = C_t$, což jsme chtěli dokázat.

   Dokázali jsme tedy, že $(\mathbb{Z}_m, +, \cdot)$ je okruh.

4. Z definice násobení zbytkových tříd ihned plyne, že zbytková třída C_1 je neutrálním prvkem v $(\mathbb{Z}_m, \cdot)$, tzn. C_1 je jedničkou okruhu $(\mathbb{Z}_m, +, \cdot)$.

   Tedy $(\mathbb{Z}_m, +, \cdot)$ je komutativní okruh s jedničkou. ■

Pracujeme-li s okruhy zbytkových tříd podle konkrétního (ne příliš velkého) modulu, m, bývá užitečné si sestrojit tabulky pro operace sčítání zbytkových tříd a násobení zbytkových tříd. Uvedeme nyní tyto tabulky pro sčítání a násobení zbytkových tříd podle modulu $m = 6$ a modulu $m = 7$. Na základě dříve zavedené úmluvy budeme používat zjednodušeného zápisu zbytkových tříd, tzn. místo C_i budeme psát pouze i.

Tabulky operací okruhu zbytkových tříd $(\mathbb{Z}_6, +, \cdot)$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Tabulky operací okruhu zbytkových tříd $(\mathbb{Z}_7, +, \cdot)$:

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\cdot$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

V následujících dvou větách si odvodíme základní pravidla, která platí pro "počítání" v okruhu. Uvidíme, že jsou podobná pravidlům pro počítání s čísly.

Věta 3. 2.
Nechť $(R, +, \cdot)$ je okruh, $a, b, c \in R$ jsou libovolné prvky. Pak platí:

1. $a \cdot (b - c) = a \cdot b - a \cdot c \quad \wedge \quad (b - c) \cdot a = b \cdot a - c \cdot a$
2. $a \cdot 0 = 0 \cdot a = 0$
3. $a \cdot (-b) = (-a) \cdot b = -(a \cdot b)$
4. $(-a) \cdot (-b) = a \cdot b$

Důkaz.

1. $a \cdot (b-c) = a \cdot (b-c) + a \cdot c - a \cdot c = a \cdot [\,(b + (-c)) + c\,] - a \cdot c = a \cdot [\,b + (-c + c)\,] - a \cdot c = a \cdot [\,b + 0\,] - a \cdot c = a \cdot b - a \cdot c$.

   Zbývající část se dokáže analogicky.

2. Platí: $a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 = a \cdot 0 + 0$, odkud použitím zákonů o krácení (v grupě $(R, +)$) dostáváme, že $a \cdot 0 = 0$. Analogickým způsobem se ukáže, že $0 \cdot a = 0$.

3. Užitím 1. a 2. dostáváme:

$$a \cdot (-b) = a \cdot (0 - b) = a \cdot 0 - (a \cdot b) = 0 - (a \cdot b) = -(a \cdot b)$$

   Podobným způsobem se ukáže, že také $(-a) \cdot b = -(a \cdot b)$.

4. Užitím 3. dostáváme:

$$(-a) \cdot (-b) = -((-a) \cdot b) = -(-(a \cdot b)) = a \cdot b. \qquad \blacksquare$$

Věta 3. 3.
Nechť $(R, +, \cdot)$ je okruh, $a, b, a_i, b_j \in R$ a nechť $z \in \mathbb{Z}$. Pak platí:

1. $a \cdot (a_1 + a_2 + \cdots + a_n) = a \cdot a_1 + a \cdot a_2 + \cdots + a \cdot a_n$
2. $(a_1 + a_2 + \cdots + a_n) \cdot a = a_1 \cdot a + a_2 \cdot a + \cdots + a_n \cdot a$
3. $(a_1 + \cdots + a_n) \cdot (b_1 + \cdots + b_k) = a_1 \cdot b_1 + \cdots + a_1 \cdot b_k + \cdots + a_n \cdot b_1 + \cdots + a_n \cdot b_k$
4. $z \cdot (a \cdot b) = (z \cdot a) \cdot b = a \cdot (z \cdot b)$.

Důkaz.
Všechna tvrzení se dokáží pomocí matematické indukce (proveďte si sami). U tvrzení 4. je nutné upozornit na to, že symbol $\cdot$ je zde použit ve dvou významech – jednou pro celočíselný násobek prvku v grupě $(R\,,+\,)$ a podruhé pro operaci násobení v okruhu. ■

Označení.
Pro zjednodušení označování součtu n prvků v okruhu $(R\,,+\,,\cdot\,)$ budeme místo zápisu $a_1+\cdots+a_n$ podle potřeby také používat sumační symboliku, tzn. zápis $\sum\limits_{i=1}^{n} a_i\,.$

První tři tvrzení předchozí věty nám udávají základní početní pravidla pro počítání se sumačními symboly v okruhu. Přepíšeme-li je do sumační symboliky, dostáváme postupně následující tři rovnosti:

$$a\cdot(\sum_{i=1}^{n} a_i)=\sum_{i=1}^{n}(a\cdot a_i)\quad,\quad(\sum_{i=1}^{n} a_i)\cdot a=\sum_{i=1}^{n}(a_i\cdot a)\quad,\quad(\sum_{i=1}^{n} a_i)\cdot(\sum_{j=1}^{k} b_j)=\sum_{i=1}^{n}\sum_{j=1}^{k}(a_i\cdot b_j)\,.$$

Definice.
Nechť $(R\,,+\,,\cdot\,)$ je okruh. Nechť pro prvky $a,b\in R$ platí:

$$a\neq 0\quad\wedge\quad b\neq 0\quad\wedge\quad a\cdot b=0\,.$$

Potom se prvky a,b nazývají **dělitelé nuly** v okruhu $(R\,,+\,,\cdot\,)$.

Příklad 3. 2.

1. Ve všech okruzích, kde prvky jsou čísla a operacemi jsou obyčejné sčítání čísel a obyčejné násobení čísel dělitelé nuly neexistují. Tedy například všechny okruhy uvedené v příkladu 3. 1. 1 jsou okruhy bez dělitelů nuly.

2. Okruh $(\mathbb{R}\times\mathbb{R}\,,+\,,\cdot\,)$ z příkladu 3. 1. 2 má dělitele nuly. Nulou tohoto okruhu je zřejmě uspořádaná dvojice $(0,0)$, přičemž například

   $$(1,0)\neq(0,0)\quad\wedge\quad(0,1)\neq(0,0)\quad\wedge\quad(1,0)\cdot(0,1)=(0,0)\,,$$

   což znamená, že prvky $(1,0)$ a $(0,1)$ jsou dělitelé nuly v tomto okruhu.

3. Okruh zbytkových tříd $(\mathbb{Z}_6\,,+\,,\cdot\,)$ má dělitele nuly. Jsou jimi například zbytkové třídy C_2 a C_3, protože zřejmě nulou tohoto okruhu je zbytková třída C_0 a platí:

   $$C_2\neq C_0\qquad\wedge\qquad C_3\neq C_0\qquad\wedge\qquad C_2\cdot C_3=C_0\,.$$

   Okruh zbytkových tříd $(\mathbb{Z}_7\,,+\,,\cdot\,)$ dělitele nuly nemá. Tento fakt okamžitě vyplývá z tabulky operace násobení zbytkových tříd podle modulu 7, uvedené dříve. Z ní je ihned vidět, že pro $C_i\neq C_0\wedge C_j\neq C_0$ je vždy $C_i\cdot C_j\neq C_0\,.$

Poznámka.
V praxi je potřeba často dokazovat, že daný okruh **nemá** dělitele nuly. Znamená to dokázat implikaci:

$$(\,a\neq 0\quad\wedge\quad b\neq 0\,)\quad\Rightarrow\quad a\cdot b\neq 0$$

Většinou bývá v tomto případě jednodušší dokazovat obměnu předchozí implikace, tzn. implikaci

$$a \cdot b = 0 \quad \Rightarrow \quad (\, a = 0 \quad \vee \quad b = 0\,) .$$

Technicky bude potom obvykle nejvýhodnější postupovat tak, že budeme dokazovat například implikaci

$$(\, a \cdot b = 0 \quad \wedge \quad a \neq 0\,) \quad \Rightarrow \quad b = 0 .$$

Definice.
Okruh $(R\,, +\,, \cdot\,)$, který je netriviální, je komutativní, má jedničku a nemá dělitele nuly se nazývá **obor integrity**.

Příklad 3. 3.

1. Klasickým příkladem oboru integrity je okruh celých čísel $(\mathbb{Z}\,, +\,, \cdot\,)$.

   Dalšími příklady oborů integrity jsou pak okruhy $(\mathbb{Q}\,, +\,, \cdot\,)$, $(\mathbb{R}\,, +\,, \cdot\,)$, $(\mathbb{C}\,, +\,, \cdot\,)$, $(\mathbb{Z}[\sqrt{2}]\,, +\,, \cdot\,)$, $(\mathbb{Q}(\sqrt{2})\,, +\,, \cdot\,)$ uvedené v příkladu 3. 1. 1 .

2. Okruh $(\mathbb{R}\times\mathbb{R}\,, +\,, \cdot\,)$ z příkladu 3. 1. 2 není oborem integrity, protože má dělitele nuly (jak jsme ukázali v předchozím příkladu).

3. Okruh $(\mathbb{Z}_m\,, +\,, \cdot\,)$ zbytkových tříd podle modulu m je pro $m \geq 2$ vždy netriviálním, komutativním okruhem s jedničkou. Tento okruh tedy je (resp. není) oborem integrity podle toho, zda nemá (resp. má) dělitele nuly. Z předchozího příkladu tedy vyplývá, okruh $(\mathbb{Z}_7\,, +\,, \cdot\,)$ je oborem integrity, zatímco okruh $(\mathbb{Z}_6\,, +\,, \cdot\,)$ oborem integrity není.

Z předchozího příkladu vidíme, že některé okruhy zbytkových tříd jsou obory integrity, zatímco jiné naopak obory integrity nejsou. Přesně tuto situaci rozebírá následující věta.

Věta 3. 4.
Okruh $(\mathbb{Z}_m\,, +\,, \cdot\,)$ zbytkových tříd podle modulu m je oborem integrity $\Leftrightarrow$ modul m je prvočíslo.

Důkaz.
Připomeňme, že celé číslo je prvočíslem, jestliže je větší než 1 a má pouze nevlastní dělitele.

Důkaz implikace "$\Rightarrow$" .
Nechť okruh $(\mathbb{Z}_m\,, +\,, \cdot\,)$ je oborem integrity. Pak je netriviálním okruhem a tedy musí být $m > 1$.
Zbývá dokázat, že m má pouze nevlastní dělitele. Budeme postupovat sporem. Předpokládejme, že m má nějakého vlastního dělitele. Potom má také kladného vlastního dělitele (proč ?), kterého označíme r . Platí tedy :

$$1 < r < m \quad \text{a existuje } \; s \in \mathbb{Z}\,, \text{ tak že: } \; r \cdot s = m .$$

Potom však musí být $1 < s < m$, a tedy $C_r, C_s \in \mathbb{Z}_m$, přičemž $C_r \neq C_0$, $C_s \neq C_0$ a $C_r \cdot C_s = C_0$. To však znamená, že C_r, C_s jsou dělitelé nuly v $(\mathbb{Z}_m\,, +\,, \cdot\,)$, což je spor s předpokladem, že $(\mathbb{Z}_m\,, +\,, \cdot\,)$ je obor integrity. Tedy m nemá žádné vlastní dělitele a dokázali jsme tak, že m je prvočíslo.

Důkaz implikace "$\Leftarrow$" .
Nechť m je prvočíslo. Potom $m > 1$, což znamená, že okruh $(\mathbb{Z}_m\,, +\,, \cdot\,)$ je netriviální. Dále víme, že okruh zbytkových tříd je vždy komutativní a má jedničku. Zbývá tedy dokázat, že $(\mathbb{Z}_m\,, +\,, \cdot\,)$ nemá dělitele nuly.

Nechť tedy $C_r, C_s \in \mathbb{Z}_m$ jsou zbytkové třídy takové, že $C_r \cdot C_s = C_0 \;\wedge\; C_r \neq C_0$. Pak z definice násobení zbytkových tříd plyne (rozmyslete si proč), že

$$m \mid r \cdot s \quad \wedge \quad m \nmid r\,.$$

Protože však m je prvočíslo, pak (podle věty 4.4.3 z kapitoly I.) musí m dělit s, což znamená, že $C_s = C_0$. Dokázali jsme tak, že okruh $(\mathbb{Z}_m\,, +\,, \cdot\,)$ nemá dělitele nuly.

Tedy okruh $(\mathbb{Z}_m\,, +\,, \cdot\,)$ je oborem integrity. ■

Věta 3. 5.
Nechť $(R\,, +\,, \cdot\,)$ je okruh a nechť $a, b, c \in R$. Pak následující výroky jsou ekvivalentní.

1. okruh $(R\,, +\,, \cdot\,)$ nemá dělitele nuly
2. $a \cdot b = a \cdot c \;\wedge\; a \neq 0 \quad \Rightarrow \quad b = c$
3. $b \cdot a = c \cdot a \;\wedge\; a \neq 0 \quad \Rightarrow \quad b = c$

Důkaz
Tvrzení dokážeme obvyklým způsobem, tzn. budeme postupně dokazovat tři implikace.

Důkaz implikace "1. $\Rightarrow$ 2." .
Nechť platí výrok 1. a nechť $a \cdot b = a \cdot c \;\wedge\; a \neq 0$. Potom $a \cdot b - a \cdot c = 0$, tzn. $a \cdot (b - c) = 0$. Protože $a \neq 0$ a okruh nemá dělitele nuly, musí být $b - c = 0$, a tedy $b = c$.

Důkaz implikace "2. $\Rightarrow$ 3." .
Nechť platí výrok 2. a nechť $b \cdot a = c \cdot a \;\wedge\; a \neq 0$. Potom $(b - c) \cdot a = 0$. Podle věty 3.2.2 je součin libovolného prvku s nulou okruhu roven nule okruhu, a tedy specielně musí být $(b - c) \cdot 0 = 0$. Dostáváme tedy

$$(b - c) \cdot a \;=\; 0 \;=\; (b - c) \cdot 0\,.$$

Pokud by bylo $(b - c) \neq 0$, pak bychom užitím 2. dostali $a = 0$, což by byl spor s předpokladem, že $a \neq 0$. Musí tedy být $(b - c) = 0$, odkud již plyne, že $b = c$.

Důkaz implikace "3 $\Rightarrow$ 1" .
Nechť platí výrok 3. Dále postupujeme sporem, tzn. předpokládáme, že okruh $(R\,, +\,, \cdot\,)$ má dělitele nuly. Potom existují prvky $x, y \in R$ takové, že $x \neq 0$, $y \neq 0$ a $x \cdot y = 0$. Podle věty 3.2.2 je součin nuly okruhu s libovolným prvkem roven nule, tzn. platí také $0 \cdot y = 0$. Dostáváme tedy

$$x \cdot y \;=\; 0 \;=\; 0 \cdot y$$

odkud užitím 3. plyne, že $x = 0$, což je spor. Dokázali jsme tak, že okruh $(R\,, +\,, \cdot\,)$ nemá dělitele nuly. ■

Podmínky 2. a 3. z předchozí věty se nazývají **omezené zákony o krácení** (levý a pravý). Slovo "omezené" naznačuje, že nemůžeme krátit všemi prvky z R (v našem případě nelze krátit nulou okruhu).

Na závěr našich úvah o algebraických strukturách se dvěma operacemi se budeme zabývat dalším speciálním případem okruhu, s nímž se budeme často setkávat.

Definice.
Nechť $(R, +, \cdot)$ je komutativní okruh s vlastností, že množina jeho nenulových prvků s operací násobení je grupa. Pak $(R, +, \cdot)$ se nazývá **těleso**.

Následující větu můžeme s výhodou použít při praktickém ověřování toho, zda konkrétní okruh je či není tělesem.

Věta 3. 6.
Nechť $(R, +, \cdot)$ je netriviální, komutativní okruh s jedničkou. Pak $(R, +, \cdot)$ je těleso právě když ke každému nenulovému prvku z R existuje prvek inverzní.

Důkaz.
Důkaz implikace "$\Rightarrow$".
Platnost této implikace okamžitě vyplývá z definice tělesa.

Důkaz implikace "$\Leftarrow$".
Podle předpokladu je okruh $(R, +, \cdot)$ komutativní. Budeme tedy dokazovat, že množina všech nenulových prvků z R s operací násobení, tj. $(R - \{0\}, \cdot)$, je grupou.

Nejprve dokažme, že $(R - \{0\}, \cdot)$ je grupoid, tzn. jinak řečeno, že v okruhu $(R, +, \cdot)$ neexistují dělitelé nuly. Nechť tedy pro prvky $x, y \in R$ platí:

$$x \cdot y \;=\; 0 \;\wedge\; x \neq 0\,.$$

Podle předpokladu však k prvku x existuje prvek inverzní x^{-1}, tzn. po úpravě je

$$x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 \quad \Rightarrow \quad (x^{-1} \cdot x) \cdot y = 0 \quad \Rightarrow \quad y = 0\,.$$

Tedy $(R - \{0\}, \cdot)$ je grupoid a z ostatních předpokladů již bezprostředně plyne, že $(R - \{0\}, \cdot)$ je grupa. Dokázali jsme tak, že $(R, +, \cdot)$ je těleso. ■

Příklad 3. 4.

1. Okruhy $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ jsou tělesa.
2. Na množině $\mathbb{Q} \times \mathbb{Q}$ definujme operace $+$ a $\cdot$ takto:
$$(a, b) + (c, d) \;=\; (a + c\,,\, b + d) \quad , \quad (a, b) \cdot (c, d) \;=\; (ac - 3bd\,,\, ad + bc)\,.$$
Potom $(\mathbb{Q} \times \mathbb{Q}, +, \cdot)$ je těleso (dokažte si sami, rozepsáním definice tělesa).
3. Okruh $(\mathbb{Z}_m, +, \cdot)$ zbytkových tříd podle modulu m je tělesem právě když modul m je prvočíslem (plyne z věty 3. 4, a věty 3.8).
4. Okruhy $(\mathbb{Z}, +, \cdot)$ a $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ (viz příklad 3. 1. 1) nejsou tělesa. Podobně, okruh $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ z příkladu 3. 1. 2 není tělesem a dále též triviální okruh není tělesem.

V tomto paragrafu jsme zavedli tři základní algebraické struktury se dvěma operacemi: okruh, obor integrity a těleso. Víme již, že obor integrity je vždy okruhem, ale okruh nemusí vždy být oborem integrity. Nyní si všimneme, jaký je vzájemný vztah mezi obory integrity a tělesy.

Věta 3. 7.
Každé těleso je oborem integrity.

Důkaz.
Nechť $(R, +, \cdot)$ je těleso. Potom:

1. $(R, +, \cdot)$ je netriviální okruh.
   V opačném případě by by totiž množina jeho nenulových prvků $R - \{0\}$ byla prázdná a tedy $(R - \{0\}, \cdot)$ by nebyla grupou.
2. $(R, +, \cdot)$ je komutativní okruh, což plyne přímo z definice tělesa.
3. $(R, +, \cdot)$ je okruhem s jedničkou.
   Jedničkou tělesa bude jednička e grupy $(R - \{0\}, \cdot)$, protože pro každý nenulový prvek $y \in R$ pak je $y \cdot e = e \cdot y = y$ a pro nulu platí $0 \cdot e = e \cdot 0 = 0$ (podle věty 3. 2. 2). Dohromady tedy je $x \cdot e = e \cdot x = x$ pro $\forall x \in R$.
4. $(R, +, \cdot)$ nemá dělitele nuly.
   Množina nenulových prvků tělesa je vzhledem k operaci násobení grupou, tzn. je také grupoidem, a tedy součin dvou nenulových prvků je opět nenulovým prvkem.

Dohromady tak dostáváme, že $(R, +, \cdot)$ je oborem integrity. ■

Předchozí větu není možné obrátit, tzn. obor integrity nemusí být obecně tělesem. Například okruh celých čísel $(\mathbb{Z}, +, \cdot)$ je oborem integrity, který není tělesem (protože například k číslu 2 zde neexistuje inverzní prvek). Je-li však množina R konečná, potom obrácení předchozí věty možné je, jak vyplývá z následující věty. Znamená to tedy, že pro konečné množiny pojmy obor integrity a těleso splývají.

Věta 3. 8.
Každý konečný obor integrity je tělesem.

Důkaz.
Nechť $(R, +, \cdot)$ je konečný obor integrity a nechť množina R sestává z n prvků $(n \geq 2)$. Podle předpokladu je $(R, +, \cdot)$ netriviální, komutativní okruh s jedničkou, tzn. podle věty 3.6 stačí dokázat, že k libovolnému nenulovému prvku z R existuje prvek inverzní. Nechť tedy $a \in R - \{0\}$. Uvažme množinu

$$M \;=\; \{\, a \cdot x \mid x \in R - \{0\} \text{ libovolný} \,\},$$

která je podmnožinou množiny $R - \{0\}$ (protože daný obor integrity nemá dělitele nuly). Množina M je konečná a má stejný počet prvků jako množina $R - \{0\}$, protože podle věty 3.5.2 (použijeme obměnu implikace) pro $x_1, x_2 \in R - \{0\}$ platí:

$$x_1 \neq x_2 \quad \Rightarrow \quad a \cdot x_1 \neq a \cdot x_2 \,.$$

Musí tedy být $M = R - \{0\}$, což ale znamená, že určitě existuje prvek $x_0 \in R - \{0\}$ takový, že $a \cdot x_0 = 1$. Prvek x_0 je potom hledaným inverzním prvkem k prvku a. ■

S pojmem tělesa se bude pracovat i v jiných matematických disciplínách. Pokud chceme situaci co nejvíce zjednodušit (při zachování většiny podstatných vlastností), omezujeme se často na tělesa, jejichž prvky budou čísla a operacemi budou obyčejné sčítání a násobení čísel. Nyní taková tělesa zavedeme a ukážeme některé jejich příklady a základní vlastnosti.

Definice.
Nechť $(T\,,+\,,\cdot\,)$ je těleso takové, že $T \subseteq \mathbb{C}$ a $+$, resp. $\cdot$ značí obyčejné sčítání, resp. obyčejné násobení čísel. Pak $(T\,,+\,,\cdot\,)$ se nazývá **číselné těleso**.

Praktické ověřování toho, zda je $(T\,,+\,,\cdot\,)$ číselným tělesem provádíme pomocí následující věty. K ní předem poznamenejme, že ve smyslu dříve zavedených úmluv bude $a-b$ znamenat obyčejný rozdíl čísel a, b a podobně $\frac{a}{b}$ bude značit obyčejný podíl čísel a, b (kde $b \neq 0$).

Věta 3. 9.
Nechť T je alespoň dvouprvková podmnožina množiny $\mathbb{C}$ všech komplexních čísel a $+$, resp. $\cdot$ značí obyčejné sčítání, resp. obyčejné násobení čísel. Potom $(T\,,+\,,\cdot\,)$ je číselným tělesem právě když platí:

1. $a, b \in T \;\Rightarrow\; a-b \in T$
2. $a, b \in T \;\wedge\; b \neq 0 \;\Rightarrow\; \frac{a}{b} \in T$.

Důkaz.
Tvrzení věty ihned plyne z definice tělesa, z věty 2.3. a ze známých vlastností platných pro počítání s čísly. ■

Příklad 3. 5.

1. $(\mathbb{Q}\,,+\,,\cdot\,)$, $(\mathbb{R}\,,+\,,\cdot\,)$, $(\mathbb{C}\,,+\,,\cdot\,)$ jsou zřejmě číselnými tělesy.
2. $(\mathbb{Q}(\sqrt{2}\,)\,,+\,,\cdot\,)$ je číselné těleso.

   Připomeňme, že $\mathbb{Q}(\sqrt{2}\,) = \{a+b\cdot\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Pro ilustraci ověřme (s využitím předchozí věty), že se skutečně jedná o číselné těleso.

   Množina $\mathbb{Q}(\sqrt{2}\,)$ je nekonečná, tzn. je tedy alespoň dvouprvková.

   Nechť $a+b\sqrt{2}\,,\, c+d\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, tzn. $a, b, c, d \in \mathbb{Q}$. Potom:

   1. $(a+b\sqrt{2})-(c+d\sqrt{2}) = (a-c)+(b-d)\sqrt{2} \;\in\; \mathbb{Q}(\sqrt{2})$,
   2. nechť navíc $c+d\sqrt{2} \neq 0$. Potom též $c-d\sqrt{2} \neq 0$ (proč?) a platí:

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} \;=\; \frac{a+b\sqrt{2}}{c+d\sqrt{2}}\cdot\frac{c-d\sqrt{2}}{c-d\sqrt{2}} \;=\; \frac{ac-2bd}{c^2-2d^2}+\frac{bc-ad}{c^2-2d^2}\cdot\sqrt{2} \;\in\; \mathbb{Q}(\sqrt{2})\,,$$

   Tedy podle věty 3. 9 je $(\mathbb{Q}(\sqrt{2}\,)\,,+\,,\cdot\,)$ číselným tělesem.

3. Při stejném označení lze podobným způsobem dokázat, že například $(\mathbb{Q}(\sqrt{p}\,)\,,+\,,\cdot\,)$, kde p je libovolné prvočíslo, je číselné těleso.

4. Označme $\mathbb{Q}(i) \;=\; \{a+bi \mid a, b \in \mathbb{Q}\}$. Potom $(\mathbb{Q}(i)\,,+\,,\cdot\,)$ je číselné těleso, což se ukáže obdobným výpočtem jako ve 2. části tohoto příkladu.

Z předchozích příkladů především vidíme, že číselných těles je nekonečně mnoho a dále, že se neomezují pouze na reálnou osu. K příkladům 3.5.3 a 3.5.4 poznamenejme,

že se jedná o speciální příklady obecnějšího tvrzení, podle kterého jsou číselnými tělesy všechny množiny tvaru

$$\mathbb{Q}(\sqrt{d}\,) \;=\; \{\, a + b \cdot \sqrt{d} \;\mid\; a, b \in \mathbb{Q} \,\}$$

(s operacemi obyčejného sčítání a obyčejného násobení čísel), přičemž d je libovolné celé číslo, takové, že $d \neq 0, 1$ a d není dělitelné druhou mocninou přirozeného čísla většího než 1. Odmocninu přitom chápeme jako libovolnou z obou druhých odmocnin z čísla d v oboru komplexních čísel (tzn. libovolné z obou řešení rovnice $x^2 = d$ v $\mathbb{C}$).

Rozebereme-li předchozí příklady číselných těles, pak zjistíme, že všechna uvedená číselná tělesa vždy obsahovala všechna racionální čísla. Skutečnost, že tomu tak musí být vždycky, ukazuje následující věta.

Věta 3. 10.
Nechť $(T\,, +\,, \cdot\,)$ je libovolné číselné těleso. Potom množina T obsahuje množinu $\mathbb{Q}$ všech racionálních čísel.

Důkaz.
Z definice tělesa plyne, že musí existovat nenulový prvek $a \in T$. Potom ale platí, že $\frac{a}{a} = 1 \in T$, tzn. množina T obsahuje číslo 1. Sečteme-li jedničku se sebou samou libovolný konečný počet-krát, pak výsledek opět musí ležet v T, a tedy T obsahuje množinu všech přirozených čísel.

Dále: $a - a = 0 \in T$ a pro libovolné přirozené číslo $x \in T$ musí být i $0 - x = -x \in T$. Tedy množina T obsahuje nulu a všechna záporná čísla. Dohromady pak $T \supseteq \mathbb{Z}$.

Konečně, v T leží i podíl libovolných dvou celých čísel (s nenulovým jmenovatelem), tzn. v T leží každé racionální číslo. Dostáváme tak, že $T \supseteq \mathbb{Q}$. ■

4. Homomorfizmy algebraických struktur.

V tomto paragrafu se budeme zabývat studiem vzájemných vztahů mezi algebraickými strukturami se stejným počtem operací. K tomu účelu budeme používat zobrazení mezi těmito algebraickými strukturami, která budou "zachovávat operace" a na základě toho potom ve větší či menší míře "přenášet danou strukturu".

Úmluva.
Při označování algebraických struktur jsme doposud vždy kromě symbolu nosné množiny důsledně vypisovali i symbol operace či operací. Zaveďme nyní úmluvu, že z důvodů stručnosti zápisu budeme symboly operací podle potřeby vynechávat, a to zejména tam, kde nebude nebezpečí nedorozumění a z kontextu bude jasné, o jakou operaci, resp. operace se jedná.

Budeme tedy místo obratu "grupoid $(G, \cdot)$" říkat stručně "grupoid G" nebo místo "těleso $(\mathbb{Q}, +, \cdot)$" budeme říkat "těleso $\mathbb{Q}$", atd. Při tom budeme mít na paměti, že se nejedná pouze o množiny, ale jedná se o množiny s operacemi.

Definice.
Nechť $(G, \cdot)$ a $(H, *)$ jsou grupoidy a nechť $\varphi : G \longrightarrow H$ je zobrazení takové, že

(1) $$\varphi(a \cdot b) = \varphi(a) * \varphi(b) \qquad \text{pro každé } a, b \in G$$

Pak φ se nazývá **homomorfizmus** grupoidu G do grupoidu H.

Je-li zobrazení φ navíc injektivní, pak se nazývá **vnoření**, resp. je-li zobrazení φ navíc bijektivní, pak se nazývá **izomorfizmus**.

Poznámka.

1. Jsou-li grupoidy G, H z předchozí definice navíc pologrupami, resp. grupami, atd., potom hovoříme o homomorfizmu pologrup, resp. grup, atd. Totéž platí i pro vnoření a izomorfizmus.
2. Existuje-li vnoření $\varphi : G \longrightarrow H$, pak také říkáme, že grupoid (pologrupu, grupu) G **lze vnořit** do grupoidu (pologrupy, grupy) H.
3. V předchozí definici homomorfizmu je jasné, že operace $\cdot$ a $*$ jsou obecně různé, což plyne již z použitého označení. Pro jednoduchost zápisu budeme v dalším obě operace označovat obvykle stejným symbolem, většinou symbolem $\cdot$. Při tom nebude moci dojít k nedorozumění, protože ze souvislostí a ze samotného zápisu bude vždy patrné, o kterou z obou operací se jedná.

Příklad 4. 1.

1. Nechť G je libovolný grupoid. Pak identické zobrazení $id_G : G \longrightarrow G$ je vždy homomorfizmus, který je navíc vždy izomorfizmem.
2. Nechť G je libovolný grupoid a nechť H je grupoid s neutrálním prvkem e. Potom zobrazení
$$\varphi : G \longrightarrow H, \text{ definované: } \varphi(x) = e \text{ pro každé } x \in G$$

je homomorfizmus. Tento homomorfizmus je vnořením, právě když množina G je jednoprvková, resp. je izomorfizmem, právě když množiny G, H jsou jednoprvkové.

3. Uvažme grupu celých čísel $(\mathbb{Z}, +)$ a grupu $(\mathbb{Z}_m, +)$ zbytkových tříd podle modulu m. Pak zobrazení $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$, definované pro každé $a \in \mathbb{Z}$ vztahem:

$$\varphi(a) = C_r\,, \qquad \text{kde } r \text{ je zbytek po dělení čísla } a \text{ číslem } m$$

je homomorfizmus (dokažte si sami rozepsáním, pomocí věty o dělení se zbytkem celých čísel). Tento homomorfizmus není vnoření a není izomorfizmus.

4. Uvažme pologrupu $(\mathbb{N}, +)$ a grupu $(\mathbb{Z} \times \mathbb{Z}, +)$, kde operací je "sčítání po složkách", tzn. $(a, b) + (c, d) = (a + c\,,\ b + d)$. Definujme nyní zobrazení

$$\varphi : \mathbb{N} \longrightarrow \mathbb{Z} \times \mathbb{Z} \qquad \text{vztahem:} \quad \varphi(x) = (x, 0)\,, \ \text{ pro } \forall\, x \in \mathbb{N}\,.$$

Potom φ je vnoření (ověřte si sami příslušným rozepsáním).

5. Nechť $\mathbb{R}^+$ značí množinu všech kladných reálných čísel. Uvažme grupy $(\mathbb{R}^+, \cdot)$ a $(\mathbb{R}, +)$ a definujme zobrazení

$$\varphi : \mathbb{R}^+ \longrightarrow \mathbb{R} \qquad \text{vztahem:} \quad \varphi(x) = \ln x\,, \ \text{ pro } \forall\, x \in \mathbb{R}^+\,.$$

Potom φ je bijekce (proč?) a pro každé $a, b \in \mathbb{R}^+$ platí:

$$\varphi(a \cdot b) = \ln(a \cdot b) = \ln a + \ln b = \varphi(a) + \varphi(b)\,.$$

Dohromady tedy dostáváme, že φ je izomorfizmus.

6. Uvažme grupu $(\mathbb{Z}_3, +)$ zbytkových tříd podle modulu 3 a dále grupu $(G, \cdot)$ všech třetích odmocnin z jedné v oboru komplexních čísel, tzn.

$$\mathbb{Z}_3 = \{\, C_0, C_1, C_2 \,\}\,, \qquad G = \{\, x_0, x_1, x_2 \,\}\,,$$

kde $x_k = \cos\frac{2k\pi}{3} + i \sin\frac{2k\pi}{3}$ pro $k = 0, 1, 2$ a tabulky operací mají tvar:

$+$	C_0	C_1	C_2
C_0	C_0	C_1	C_2
C_1	C_1	C_2	C_0
C_2	C_2	C_0	C_1

$\cdot$	z_0	z_1	z_2
x_0	x_0	x_1	x_2
x_1	x_1	x_2	x_0
x_2	x_2	x_0	x_1

Definujme zobrazení

$$\varphi : \mathbb{Z}_3 \longrightarrow G \qquad \text{vztahem:} \quad \varphi(C_i) = x_i\,, \ \text{ pro } i = 0, 1, 2\,.$$

Potom φ je izomorfizmus (což je v podstatě ihned vidět z obou tabulek operací).

Věta 4.1.
Nechť G, H, K jsou grupoidy, nechť $\varphi : G \longrightarrow H$ a $\psi : H \longrightarrow K$ jsou homomorfizmy. Potom platí:

1. složení homomorfizmů $\psi \circ \varphi$ je opět homomorfizmus
2. je-li φ izomorfizmus, pak inverzní zobrazení φ^{-1} je také izomorfizmus.

Důkaz.

1. Zřejmě $\psi \circ \varphi : G \longrightarrow K$. Nechť $a, b \in G$ libovolné. Potom:

$$(\psi \circ \varphi)(a \cdot b) = \psi(\varphi(a \cdot b)) = \psi(\varphi(a)) \cdot \psi(\varphi(b)) = (\psi \circ \varphi)(a) \cdot (\psi \circ \varphi)(b)$$

   což znamená, že $\psi \circ \varphi$ je homomorfizmus.

2. Nechť $\varphi : G \longrightarrow H$ je izomorfizmus. Pak φ je bijektivní zobrazení, a tedy existuje inverzní zobrazení $\varphi^{-1} : H \longrightarrow G$, které je také bijektivní. Zbývá dokázat, že φ^{-1} je homomorfizmus.

   Nechť tedy $u, v \in H$ libovolné. Potom (protože φ je bijektivní) existují prvky $a, b \in G$ tak, že $\varphi(a) = u$, $\varphi(b) = v$. To však znamená, že je

$$\varphi^{-1}(u) \;=\; a \qquad \wedge \qquad \varphi^{-1}(v) \;=\; b\,.$$

   Dostáváme tak: $u \cdot v = \varphi(a) \cdot \varphi(b) = \varphi(a \cdot b)$, což znamená, že

$$\varphi^{-1}(u \cdot v) \;=\; a \cdot b \;=\; \varphi^{-1}(u) \cdot \varphi^{-1}(v)\,.$$

   Dokázali jsme tedy, že φ^{-1} je izomorfizmus. ■

Označení.
Je-li $f : A \longrightarrow B$ zobrazení množiny A do množiny B, a X je libovolná podmnožina množiny A, pak symbolem $f(X)$ budeme označovat množinu obrazů všech prvků z X při zobrazení f, tzn.

$$f(X) \;=\; \{\, f(u) \mid u \in X \,\}$$

Věta 4. 2.
Nechť G, H jsou grupoidy a $\varphi : G \longrightarrow H$ je homomorfizmus. Pak platí:

1. *$\varphi(G)$ je podgrupoidem grupoidu H*
2. *G je komutativní $\Rightarrow$ $\varphi(G)$ je komutativní*
3. *G je asociativní $\Rightarrow$ $\varphi(G)$ je asociativní.*

Důkaz.
Nechť $(G, \cdot)$ a $(H, \cdot)$ jsou uvažované grupoidy. Nechť $u, v \in \varphi(G)$ jsou libovolné prvky. Pak existují prvky $a, b \in G$ tak, že

$$\varphi(a) \;=\; u \qquad \text{a} \qquad \varphi(b) \;=\; v\,.$$

Nyní dokážeme jednotlivá tvrzení.

1. Množina $\varphi(G)$ je zřejmě neprázdná a zbývá tedy dokázat, že množina $\varphi(G)$ je uzavřená vzhledem k operaci $\cdot$ (v množině H). Ale:

$$u \cdot v \;=\; \varphi(a) \cdot \varphi(b) \;=\; \varphi(a \cdot b)\,, \quad \text{a tedy} \quad u \cdot v \in \varphi(G)\,.$$

2. Nechť G je komutativní grupoid. Potom

$$u \cdot v \;=\; \varphi(a) \cdot \varphi(b) \;=\; \varphi(a \cdot b) \;=\; \varphi(b \cdot a) \;=\; \varphi(b) \cdot \varphi(a) \;=\; v \cdot u$$

   což znamená, že grupoid $\varphi(G)$ je komutativní.

3. Dokáže se analogicky jako 2. ■

V dalším se nyní budeme zabývat homomorfizmy grup. Připomeňme naši dřívější úmluvu, že neutrální prvek grupy G budeme nazývat jedničkou této grupy a označovat symbolem e_G. Analogicky, jedničku grupy H označujeme e_H.

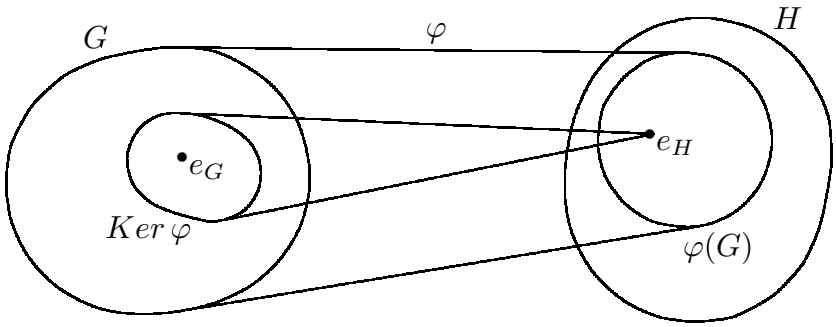
Definice.
Nechť G, H jsou grupy a $\varphi : G \longrightarrow H$ je homomorfizmus. Pak množinu

$$Ker\,\varphi \;=\; \{\, x \in G \mid \varphi\,(x) \;=\; e_H \}$$

nazýváme **jádro homomorfizmu** φ.

Jádro homomorfizmu grup je tedy množina prvků z G, které se při tomto homomorfizmu zobrazí na jedničku grupy H. Poznamenejme, že označení $Ker\,\varphi$ je běžně používanou zkratkou, pocházející z anglického "kernel" = jádro. Množina $\varphi(G)$ se také někdy nazývá **obraz homomorfizmu**.

Jádro homomorfizmu $Ker\,\varphi$ a obraz homomorfizmu $\varphi(G)$ je možno schematicky znázornit následujícím obrázkem.



Věta 4. 3.
Nechť G, H jsou grupy a $\varphi : G \longrightarrow H$ je homomorfizmus. Pak platí:

1. $\varphi\,(e_G) \;=\; e_H$
2. $\varphi\,(a^{-1}) \;=\; \varphi\,(a)^{\,-1}$ *pro každé* $a \in G$
3. *jádro* $Ker\,\varphi$ *je podgrupa grupy* G
4. *obraz* $\varphi(G)$ *je podgrupa grupy* H.

Důkaz.
Nechť $\varphi : G \longrightarrow H$ je grupový homomorfizmus.

1. Pro jedničku e_G grupy G a jedničku e_H grupy H platí:

$$\varphi\,(e_G) \cdot \varphi\,(e_G) \;=\; \varphi\,(e_G \cdot e_G) \;=\; \varphi\,(e_G) \;=\; \varphi\,(e_G) \cdot e_H$$

   odkud užitím zákona o krácení (který v grupě platí) dostáváme, že $\varphi\,(e_G) \;=\; e_H$.

2. Pro libovolný prvek $a \in G$ platí:

$$\varphi\,(a) \cdot \varphi\,(a^{-1}) = \varphi\,(a \cdot a^{-1}) = \varphi\,(e_G) = e_H$$
$$\varphi\,(a^{-1}) \cdot \varphi\,(a) = \varphi\,(a^{-1} \cdot a) = \varphi\,(e_G) = e_H$$

   odkud plyne, že prvek $\varphi\,(a^{-1})$ je inverzním prvkem k prvku $\varphi\,(a)$.

3. Podle 1. části této věty je $e_G \in Ker\,\varphi$, a tedy $Ker\,\varphi$ je neprázdná množina. Nechť dále $a, b \in Ker\,\varphi$. Dokážeme, že prvek $a \cdot b^{-1} \in Ker\,\varphi$. Ale

$$\varphi(a \cdot b^{-1}) \;=\; \varphi(a) \cdot \varphi(b^{-1}) \;=\; \varphi(a) \cdot \varphi(b)^{-1} \;=\; e_H \cdot e_H^{-1} \;=\; e_H$$

což znamená, že $a \cdot b^{-1} \in Ker\,\varphi$, a tedy podle věty 2.3 dostáváme, že $Ker\,\varphi$ je podgrupou grupy G.

4. Množina $\varphi(G)$ je zřejmě neprázdná. Dále nechť $u, v \in \varphi(G)$. Ale podle 2. části této věty je $v^{-1} \in \varphi(G)$ a podle věty 4.2.1 je potom $u \cdot v^{-1} \in \varphi(G)$, odkud opět použitím věty 2.3 dostáváme, že $\varphi(G)$ je podgrupou grupy H. ■

Pomocí jádra grupového homomorfizmu můžeme jednoduchým způsobem charakterizovat injektivnost tohoto homomorfizmu, jak ukazuje následující věta.

Věta 4.4.
Nechť G, H jsou grupy a $\varphi : G \longrightarrow H$ je homomorfizmus. Pak platí: zobrazení φ je injektivní $\Leftrightarrow$ $Ker\,\varphi = \{e_G\}$

Důkaz.
Tvrzení budeme dokazovat obvyklým způsobem, ve dvou krocích.

Důkaz implikace "$\Rightarrow$".
Nechť φ je injektivní zobrazení. Budeme dokazovat, že $Ker\,\varphi = \{e_G\}$. Jedná se o možinovou rovnost, tzn. dokážeme obě množinové inkluze.

"$\subseteq$": Nechť $x \in Ker\,\varphi$. Potom $\varphi(x) = e_H = \varphi(e_G)$. Ale zobrazení φ je injektivní, tzn. $x = e_G$, neboli $x \in \{e_G\}$.

"$\supseteq$": Tato inkluze zřejmě platí, protože (podle věty 4.3.1) je $\varphi(e_G) = e_H$, což znamená, že $e_G \in Ker\,\varphi$.

Důkaz implikace "$\Leftarrow$".
Předpokládáme, že $Ker\,\varphi = \{e_G\}$ a dokážeme, že φ je injektivní. Ale

$$\varphi(x) = \varphi(y) \;\Rightarrow\; \varphi(x) \cdot \varphi(y)^{-1} = e_H \;\Rightarrow\; \varphi(x \cdot y^{-1}) = e_H \;\Rightarrow\; x \cdot y^{-1} \in Ker\,\varphi,$$

což však podle předpokladu znamená, že $x \cdot y^{-1} = e_G$, neboli $x = y$. Dokázali jsme tedy, že zobrazení φ je injektivní. ■

Definice.
Řekneme, že grupoidy (resp. pologrupy, resp. grupy) G, H **jsou izomorfní**, jestliže existuje izomorfizmus $\varphi : G \longrightarrow H$. Píšeme pak $G \cong H$.

Poznámka.
Předchozí definice je zformulována korektně, neboť z věty 4.1.2 plyne, že je-li $G \cong H$, potom je také $H \cong G$ a můžeme tedy říkat, že G, H (bez ohledu na pořadí) jsou izomorfní. Připomeňme ještě, že zřejmě platí $G \cong G$ a dále také platí:

$$G \cong H \;\wedge\; H \cong K \;\Rightarrow\; G \cong K$$

(rozmyslete si podrobně proč!).

Z našich dosavadních úvah a tvrzení vyplývá, že izomorfní grupoidy (resp. pologrupy, resp. grupy) se mezi sebou z algebraického hlediska vůbec neliší. Pomineme-li totiž konkrétní smysl prvků a konkrétní smysl operací, pak vidíme, že dvě izomorfní algebraické struktury mají naprosto stejné všechny vlastnosti, které je možno zformulovat pomocí operace na dané množině, tj. například komutativnost, asociativnost, existence neutrálního prvku, atd. Pěkně je to vidět třeba v příkladu 4. 1. 6 , kde obě grupy jsou konečné, mají stejný počet prvků a tabulky operací jsou "stejné". Z algebraického hlediska je potom nepodstatné, že v jednom případě se jedná o zbytkové třídy a jejich sčítání a ve druhém případě se jedná o jistá komplexní čísla a jejich násobení. Z těchto důvodů je v matematice obvyklé v případě potřeby izomorfní algebraické struktury ztotožňovat. To znamená, že každý prvek jedné struktury se potom považuje za totožný s tím prvkem druhé struktury, který je jeho obrazem při daném izomorfizmu a navíc se nečiní rozdíl mezi operacemi v obou strukturách.

Do jisté míry podobná situace nastává též u vnoření. Máme-li vnoření (tzn. injektivní homomorfizmus) $\varphi : G \longrightarrow H$, pak zřejmě zobrazení φ můžeme chápat jako bijektivní homomorfizmus G na $\varphi(G)$. Tedy G a $\varphi(G)$ jsou izomorfní a můžeme je podle naší předchozí úmluvy ztotožnit. Na základě tohoto ztotožnění můžeme potom strukturu G chápat jako podstrukturu struktury H . Konkrétně, například pologrupa $(\mathbb{N}\,,+)$ a grupa $(\mathbb{Z}\times\mathbb{Z}\,,+)$ z příkladu 4. 1. 4 jsou evidentně disjunktní, ovšem existence vnoření $\varphi : \mathbb{N} \longrightarrow \mathbb{Z}\times\mathbb{Z}$ popsaného v příkladu 4. 1. 4 nám umožňuje považovat pologrupu $(\mathbb{N}\,,+)$ za podpologrupu grupy $(\mathbb{Z}\times\mathbb{Z}\,,+)$, přičemž ztotožníme prvek $x \in \mathbb{N}$ s jeho obrazem $\varphi\,(x) = (x, 0) \in \mathbb{Z}\times\mathbb{Z}$.

Pro algebraické struktury se dvěma operacemi je možno zavést pojem homomorfizmu podobným způsobem jako u algebraických struktur s jednou operací. Jeho vlastnosti budou, jak lze očekávat, podobné vlastnostem homomorfizmů algebraických struktur s jednou operací. Velmi stručně se o některých z nich nyní zmíníme.

Definice.
Nechť $(R\,,+\,,\cdot\,)$, $(S\,,+\,,\cdot\,)$ jsou okruhy a $\varphi : R \longrightarrow S$ je zobrazení takové, že pro libovolné prvky $a, b \in R$ platí:

$$\varphi\,(a+b) \;=\; \varphi\,(a) \,+\, \varphi\,(b) \qquad\qquad \wedge \qquad\qquad \varphi\,(a\cdot b) \;=\; \varphi\,(a)\,\cdot\,\varphi\,(b)\,.$$

Potom se φ nazývá **homomorfizmus** (okruhu R do okruhu S) .

Je-li φ navíc injektivní, pak se nazývá **vnoření** , resp. je-li φ navíc bijektivní, pak se nazývá **izomorfizmus**.

Příklad 4. 2.

1. Nechť R je libovolný okruh. Pak identické zobrazení $id_R : R \longrightarrow R$ je izomorfizmus okruhu R na sebe.
2. Vezměme okruh celých čísel $(\mathbb{Z}\,,+\,,\cdot\,)$ a okruh $(\mathbb{Z}_m\,,+\,,\cdot\,)$ zbytkových tříd podle modulu m. Pak zobrazení $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$ definované pro každé $a \in \mathbb{Z}$ vztahem

   $$\varphi\,(a) \;=\; C_r\;, \qquad \text{kde } r \text{ je zbytek po dělení čísla } a \text{ číslem } m$$

   je homomorfizmus, který není ani vnořením ani izomorfizmem.

Dokažme, že tomu tak opravdu je. Především je zřejmé, že zobrazení φ není injektivní ani bijektivní. Dále, z příkladu 4. 1. 3 plyne, že

$$\varphi\,(a+b) \;=\; \varphi\,(a) + \varphi\,(b) \qquad \text{pro } \forall\, a, b \in \mathbb{Z}\,.$$

Zbývá nám tedy dokázat, že platí:

$$\varphi\,(a \cdot b) \;=\; \varphi\,(a) \cdot \varphi\,(b) \qquad \text{pro } \forall\; a, b \in \mathbb{Z}\,.$$

Označme: $\varphi\,(a) \,=\, C_i\,,\;\; \varphi\,(b) \,=\, C_j\,.$ Potom existují celá čísla z_1, z_2 tak, že platí

$$a \,=\, z_1 m + i\,,\;\; \text{kde } 0 \leq i < m \qquad \wedge \qquad b \,=\, z_2 m + j\,,\;\; \text{kde } 0 \leq j < m\,.$$

Po vynásobení čísel a, b a následné úpravě dostáváme:

$$a \cdot b \;=\; (z_1 m + i) \cdot (z_2 m + j) \;=\; (z_1 z_2 m + z_1 j + i z_2) \cdot m \,+\, i \cdot j$$

odkud plyne, že $a \cdot b \equiv i \cdot j \,(\mathrm{mod}\; m)$, což znamená, že čísla $a \cdot b$ a $i \cdot j$ dávají po dělení číslem m stejný zbytek, který označíme například k. Potom z definice zobrazení φ a z definice násobení zbytkových tříd plyne, že

$$\varphi\,(a \cdot b) \;=\; C_k \;=\; C_i \cdot C_j \;=\; \varphi\,(a) \cdot \varphi\,(b)$$

což je požadovaný vztah.

Definice.
Nechť R, S jsou okruhy a $\varphi : R \longrightarrow S$ je homomorfizmus. Potom množina

$$Ker\,\varphi \;=\; \{\, x \in R \;\mid\; \varphi\,(x) = 0_S \,\}$$

se nazývá **jádro homomorfizmu** φ.

Základní vlastnosti okruhových homomorfizmů budou analogické odpovídajícím základním vlastnostem homomorfizmů algebraických struktur s jednou operací, jak vyplývá z následujících vět.

Věta 4. 5.
Nechť R, S, T jsou okruhy, nechť $\varphi : R \longrightarrow S$ a $\psi : S \longrightarrow T$ jsou homomorfizmy těchto okruhů. Potom platí:

1. *složení homomorfizmů $\psi \circ \varphi$ je opět homomorfizmus*
2. *je-li φ izomorfizmus (okruhů), pak inverzní zobrazení φ^{-1} je také izomorfizmus.*

Důkaz.
Důkaz tvrzení se provede analogicky jako důkaz obdobné věty pro grupoidy, tzn. jako důkaz věty 4. 1. ■

Věta 4. 6.
Nechť R, S jsou okruhy a $\varphi : R \longrightarrow S$ je homomorfizmus. Pak platí:

1. $\varphi\,(0_R) \,=\, 0_S$
2. $\varphi\,(-a) \,=\, -\,\varphi\,(a)$ *pro každé* $a \in R$
3. *zobrazení φ je injektivní* $\;\Leftrightarrow\;$ $Ker\,\varphi \;=\; \{\, 0_R \,\}$.

Důkaz.
Uvědomíme-li si, že $(R\,, +\,)$ a $(S\,, +\,)$ jsou grupy, pak je zřejmé, že 1. a 2. platí (jedná se vlastně o 1. a 2. část věty 4. 3, přeformulované do aditivní symboliky).

Tvrzení 3. okamžitě plyne z věty 4.4., vzhledem k tomu, že okruhový homomorfizmus je současně homomorfizmem příslušných aditivních grup, tzn. grup $(R\,,+\,)$ a $(S\,,+\,)$. ■

Jestliže existuje izomorfizmus φ okruhů R, S, pak (podobně jako u algebraických struktur s jednou operací) se okruhy R a S z algebraického hlediska neliší a můžeme je podle potřeby ztotožňovat. V takovém případě se tedy všechny nám známé okruhové vlastnosti přenášejí, tzn. například R je oborem integrity právě když je S oborem integrity nebo R je tělesem právě když je S tělesem, atd.

Podobně, jsou – li R, S okruhy a $\varphi : R \longrightarrow S$ je vnoření, pak můžeme podle potřeby ztotožnit okruh R s jeho obrazem $\varphi(R)$.

O B S A H