10. přednáška, 29. 11. 2022

6.5. Faktorové grupy

Definice 6.5.1. *Relace* na množině X je podmnožina kartézského součinu $X \times X$.

Je-li ρ relace, místo $(x, y) \in \rho$ často píšeme $x \,\rho\, y$.

Definice 6.5.2. Relace ρ na množině X je *relace ekvivalence*, jestliže je

(1) reflexivní, tj. $x \,\rho\, x$ pro každé $x \in X$,
(2) symetrická, tj. $x \,\rho\, y$ implikuje $y \,\rho\, x$,
(3) tranzitivní, tj. $x \,\rho\, y$, $y \,\rho\, z$ implikuje $x \,\rho\, z$.

Buďte $\equiv$ relace ekvivalence na množině X a $x \in X$. Množina všech prvků ekvivalentních prvku x je *třída ekvivalence* příslušná x a označujeme ji $[x]_\equiv$ nebo jen $[x]$, je-li zřejmé, o jakou relaci ekvivalence se jedná, tedy

$$[x]_\equiv = \{y \in X \mid x \equiv y\},$$

a množina všech tříd ekvivalence je *faktorová množina* a označujeme ji $\tilde{X}_\equiv$ nebo jen $\tilde{X}$, tedy

$$\tilde{X}_\equiv = \{[x]_\equiv \mid x \in X\}.$$

Poznamenejme, že $\tilde{X}$ je rozklad množiny X, čili množiny $[x]$ jsou neprázdné, po dvou disjunktní a jejich sjednocení je X.

Definice 6.5.3. Buďte X množina s binární operací $*$ a $\equiv$ relace ekvivalence na množině X. Relace $\equiv$ je *kongruence* na X s $*$, jestliže platí implikace (*podmínka kompatibility*)

$$\text{jestliže } x_1 \equiv x_2 \text{ a } y_1 \equiv y_2, \text{ pak } x_1 * y_1 \equiv x_2 * y_2, \tag{4}$$

nebo ekvivalentně zapsáno

$$\text{jestliže } [x_1] = [x_2] \text{ a } [y_1] = [y_2], \text{ pak } [x_1 * y_1] = [x_2 * y_2].$$

Tvrzení 6.5.1. *Buďte $\equiv$ kongruence na množině s asociativní binární operací a x, y invertibilní prvky. Pak platí implikace*

$$\textit{jestliže } x \equiv y, \textit{ pak } x^{-1} \equiv y^{-1}$$

nebo ekvivalentně zapsáno

$$\textit{jestliže } [x] = [y], \textit{ pak } [x^{-1}] = [y^{-1}].$$

Důkaz. Nechť $x \equiv y$. Jelikož $x^{-1} \equiv x^{-1}$ a $y^{-1} \equiv y^{-1}$, z podmínky kompatibility dostaneme $x * x^{-1} \equiv y * x^{-1}$, tedy $e \equiv y * x^{-1}$, a $y^{-1} * e \equiv y^{-1} * y * x^{-1}$, tedy $y^{-1} \equiv x^{-1}$. □

Příklad. (1) Mějme grupu $(\mathbb{Z}, +, 0, -)$ a relaci $\equiv$ na $\mathbb{Z}$ danou předpisem: $x \equiv y$ právě tehdy, když x, y jsou obě sudá nebo obě lichá, tedy $\tilde{\mathbb{Z}} = \{[0], [1]\}$. Potom $\equiv$ je kongruence, protože součet jakýchkoliv sudých čísel je sudé číslo, součet jakýchkoliv lichých čísel je sudé číslo a součet jakéhokoliv sudého čísla a jakéhokoliv lichého čísla je liché číslo.

(2) Mějme grupu $(\mathbb{Z}, +, 0, -)$ a relaci $\equiv$ na $\mathbb{Z}$ danou předpisem: $x \equiv y$ právě tehdy, když x, y jsou obě záporná nebo obě kladná nebo obě nulová, tedy $\tilde{\mathbb{Z}} = \{[-1], [0], [1]\}$. Potom $\equiv$ je relace ekvivalence, platí implikace

$$\text{jestliže } x \equiv y, \text{ pak } -x \equiv -y,$$

ale existují $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ taková, že $x_1 \equiv x_2$ a $y_1 \equiv y_2$, ale $x_1 + y_1 \not\equiv x_2 + y_2$. Čili $\equiv$ nesplňuje podmínku kompatibility a není to tedy kongruence na $\mathbb{Z}$. ■

Máme-li kongruenci a třídy $[x], [y]$, pak díky podmínce kompatibility třída $[x * y]$ je jednoznačně určena třídami $[x], [y]$, čili nezávisí na konkrétním výběru jejich prvků x, y (*reprezentantů*). Na množině $\tilde{X}$ tedy můžeme zavést binární operaci $\tilde{*}$ předpisem

$$[x]\tilde{*}[y] = [x * y]. \tag{5}$$

Příklad. Mějme grupu $(\mathbb{Z}, +, 0, -)$ a kongruenci $\equiv$ danou předpisem: $x \equiv y$ právě tehdy, když x, y jsou obě sudá nebo obě lichá, tedy $\tilde{\mathbb{Z}} = \{[0], [1]\}$.

Na $\tilde{\mathbb{Z}}$ máme binární operaci $\tilde{+}$ definovanou předpisem (5), tedy $[x]\tilde{+}[y] = [x + y]$. Takže

$$\begin{aligned}
&[0]\tilde{+}[0] = [0 + 0] = [2 + 6] = [8 + (-14)] = [0],\\
&[0]\tilde{+}[1] = [0 + 1] = [2 + 7] = [(-6) + 11] = [1],\\
&[1]\tilde{+}[0] = [1 + 0] = [7 + 6] = [17 + (-2)] = [1],\\
&[1]\tilde{+}[1] = [1 + 1] = [3 + 13] = [(-7) + 5] = [0].
\end{aligned}$$

■

Tvrzení 6.5.2. *Mějme kongruenci na množině X s binární operací $*$. Buď $\tilde{*}$ binární operace na $\tilde{X}$ definovaná předpisem (5). Potom*

(i) je-li $*$ asociativní, pak $\tilde{*}$ je asociativní;
(ii) je-li e neutrální prvek $*$, pak $[e]$ je neutrální prvek $\tilde{*}$;
(iii) je-li x^{-1} inverze k x vzhledem k $*$, pak $[x^{-1}]$ je inverze k $[x]$ vzhledem k $\tilde{*}$;
(iv) je-li $*$ komutativní, pak $\tilde{*}$ je komutativní.

Důkaz. (i) Jestliže $*$ je asociativní, potom pro libovolné třídy $[x], [y], [z] \in \tilde{X}$ platí

$$\begin{aligned}
[x]\tilde{*}([y]\tilde{*}[z]) &= [x]\tilde{*}[y * z] =\\
&= [x * (y * z)] =\\
&= [(x * y) * z] =\\
&= [x * y]\tilde{*}[z] =\\
&= ([x]\tilde{*}[y])\tilde{*}[z],
\end{aligned}$$

takže $\tilde{*}$ je asociativní.

(ii) Jestliže e je neutrální prvek oparace $*$, potom pro libovolnou třídu $[x] \in \tilde{X}$ platí

$$\begin{aligned}
&[x]\tilde{*}[e] = [x * e] = [x],\\
&[e]\tilde{*}[x] = [e * x] = [x],
\end{aligned}$$

takže $[e]$ je neutrální prvek operace $\tilde{*}$.

(iii) Jestliže x^{-1} je inverzní prvek k x vzhledem k $*$, pak

$$\begin{aligned}
&[x]\tilde{*}[x^{-1}] = [x * x^{-1}] = [e],\\
&[x^{-1}]\tilde{*}[x] = [x^{-1} * x] = [e],
\end{aligned}$$

takže $[x^{-1}]$ je inverzní prvek k $[x]$ vzhledem k operaci $\tilde{*}$.

(iv) Z (5) je zřejmé, že je-li $*$ komutativní, pak i $\tilde{*}$ je komutativní. □

Důsledek. *Pro každou (komutativní) grupu a každou kongruenci na této grupě příslušná faktorová množina s operací definovanou předpisem (5) je (komutativní) grupa.*

Důkaz. Tvrzení je jednoduchým důsledkem předchozího Tvrzení. □

Jelikož každý prvek množiny s asociativní operací má nejvýše jeden inverzní prvek, viz Tvrzení 6.1.2 nebo Tvrzení 6.5.1, třída $[x^{-1}]$ je v takovém případě jednoznačně určena třídou $[x]$, čili nezávisí na konkrétním výběru jejího prvku x, a proto je korektní ji označovat $[x]^{-1}$.

Definice 6.5.4. Faktorová množina s operací definovanou předpisem (5) z předchozího Důsledku je *faktorová grupa*.

Příklad. Mějme grupu $(\mathbb{Z}, +, 0, -)$ a kongruenci danou předpisem: $x \equiv y$ právě tehdy, když x, y jsou obě sudá nebo obě lichá, tedy $\tilde{\mathbb{Z}} = \{[0], [1]\}$.

Na $\tilde{\mathbb{Z}}$ máme asociativní binární operaci $\tilde{+}$: $[x]\tilde{+}[y] = [x + y]$, neutrální prvek operace $\tilde{+}$ je $[0]$ a opačný prvek $-[x]$ k prvku $[x]$ je $[-x]$, čili $-[0] = [0]$, $-[1] = [-1] = [1]$. ■

6.6. Zbytkové třídy

Mějme aditivní grupu $(\mathbb{Z}, +, 0, -)$ a buď m libovolné přirozené (kladné celé) číslo. Definujme relaci $\equiv_m$ na $\mathbb{Z}$ předpisem:

$$x \equiv_m y \text{ právě tehdy, když } x - y \text{ je celočíselný násobek čísla } m$$

(čili $m \mid (x - y)$ a existuje tedy $k \in \mathbb{Z}$ takové, že $x - y = km$ a $x = y + km$).

Potom $\equiv_m$ je relace ekvivalence (cvičení), příslušné třídy ekvivalence $[i]_{\equiv_m}$ se značí $[i]_m$ a

$$\begin{aligned}
&\vdots\\
[-2]_m &= \{-2 + km \mid k \in \mathbb{Z}\} = \{\ldots, -2 - 2m, -2 - m, -2, -2 + m, -2 + 2m, \ldots\},\\
[-1]_m &= \{-1 + km \mid k \in \mathbb{Z}\} = \{\ldots, -1 - 2m, -1 - m, -1, -1 + m, -1 + 2m, \ldots\},\\
[0]_m &= \{km \mid k \in \mathbb{Z}\} = \{\ldots, -2m, -m, 0, m, 2m, \ldots\},\\
[1]_m &= \{1 + km \mid k \in \mathbb{Z}\} = \{\ldots, 1 - 2m, 1 - m, 1, 1 + m, 1 + 2m, \ldots\},\\
[2]_m &= \{2 + km \mid k \in \mathbb{Z}\} = \{\ldots, 2 - 2m, 2 - m, 2, 2 + m, 2 + 2m, \ldots\},\\
&\vdots\\
[i]_m &= \{i + km \mid k \in \mathbb{Z}\} = \{\ldots, i - 2m, i - m, i, i + m, i + 2m, \ldots\},\\
&\vdots
\end{aligned}$$

Pro $i \in \{0, \ldots, m-1\}$ třída ekvivalence $[i]_m$ obsahuje právě ta celá čísla z, po jejichž celočíselném dělení číslem m číslo i je zbytek. Třídám $[i]_m$, kde $i \in \{0, \ldots, m-1\}$, se proto říká *zbytkové třídy*. Při dělení číslem m všechny možné zbytky jsou právě $0, 1, \ldots, m-1$, takže každé celé číslo leží v právě jedné ze zbytkových tříd $[0]_m, [1]_m, \ldots, [m-1]_m$. Příslušná faktorová množina $\tilde{\mathbb{Z}}_{\equiv_m}$ se značí $\mathbb{Z}_m$, tedy

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}.$$

Ověříme, zda $\equiv_m$ je kongruence na $\mathbb{Z}$, čili podmínku kompatibility (4). Předpokládejme, že $[x_1]_m = [x_2]_m$ a $[y_1]_m = [y_2]_m$. To znamená, že $x_2 \in [x_1]_m$ a $y_2 \in [y_1]_m$, čili $x_2 = x_1 + km$, $y_2 = y_1 + lm$ pro vhodná $k, l \in \mathbb{Z}$. Potom $x_2 + y_2 = x_1 + km + y_1 + lm = x_1 + y_1 + (k + l)m \in [x_1 + y_1]_m$, a tedy $[x_1 + y_1]_m = [x_2 + y_2]_m$.

Na množině $\mathbb{Z}_m$ tedy máme binární operaci $+$ (značí se obvykle stejně jako původní operace) podle (5)

$$[x]_m + [y]_m = [x + y]_m$$

a příslušná faktorová grupa $(\mathbb{Z}_m, +, [0]_m, -)$ je komutativní *aditivní grupa zbytkových tříd modulo* m.

Na množině $\mathbb{Z}$ uvažujme operaci $\cdot$, která je asociativní a má neutrální prvek 1. Ověříme podmínku kompatibility (4) pro operaci $\cdot$.

Předpokládejme, že $[x_1]_m = [x_2]_m$ a $[y_1]_m = [y_2]_m$. To znamená, že $x_2 = x_1 + km$, $y_2 = y_1 + lm$ pro vhodná $k, l \in \mathbb{Z}$. Potom $x_2 \cdot y_2 = (x_1 + km) \cdot (y_1 + lm) = x_1 y_1 + (ky_1 + lx_1 + klm)m \in [x_1 y_1]_m$, a tedy $[x_1 y_1]_m = [x_2 y_2]_m$.

Na $\mathbb{Z}_m$ tedy máme i binární operaci $\cdot$ podle (5)

$$[x]_m \cdot [y]_m = [x \cdot y]_m.$$

Podle Tvrzení 6.5.2 operace $\cdot$ na množině $\mathbb{Z}_m$ je komutativní, asociativní a má neutrální prvek $[1]_m$. Faktorová množina $\mathbb{Z}_m$ s operací $\cdot$ a neutrálním prvkem $[1]_m$ je komutativní *multiplikativní monoid zbytkových tříd modulo m* (*monoid* je množina s asociativní binární operací a neutrálním prvkem). Otázka existence inverzí vzhledem k operaci $\cdot$ není tak jednoduchá jako v případě operace $+$.

Tvrzení 6.6.1. *Prvek $[x]_m \in \mathbb{Z}_m$ má inverzi vzhledem k operaci $\cdot$ právě tehdy, když x a m jsou nesoudělná, tedy jejich největší společný dělitel $D(x, m)$ je 1.*

Důkaz. Předpokládejme, že $[y]_m$ je inverze k $[x]_m$, tedy $[x]_m \cdot [y]_m = [xy]_m = [1]_m$. Takže $xy + km = 1$ pro vhodné $k \in \mathbb{Z}$ a každý společný dělitel čísel x a m je dělitel i čísla 1. Proto $D(x, m) = 1$.

Předpokládejme, že $D(x, m) = 1$. Podle Bézoutovy věty existují čísla $y, k \in \mathbb{Z}$ taková, že $D(x, m) = yx + km$. V našem případě $1 = xy + km$, takže $[1]_m = [xy]_m = [x]_m \cdot [y]_m$ a $[y]_m$ je inverze k $[x]_m$. □

Příklad. Nechť $m = 5$. Následující tabulka naznačuje rozložení množiny všech celých čísel do pěti tříd:

$[0]_5$				-5						0						5				
$[1]_5$						-4						1						6		
$[2]_5$	$\cdots$						-3						2						7				$\cdots$
$[3]_5$									-2						3						8		
$[4]_5$											-1						4						9

Aditivní grupa $\mathbb{Z}_5$ resp. multiplikativní monoid $\mathbb{Z}_5$ mají tabulky

$+$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$
$[2]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$
$[3]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$

resp.

$\cdot$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$
$[1]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[0]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[0]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[0]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

■

7. Okruhy a pole

Definice 7.0.1. Množina P se dvěmi binárními operacemi $+$ a $\cdot$ je *okruh*, jestliže

(1) $+$ a $\cdot$ jsou asociativní a komutativní operace,
(2) $+$ má neutrální prvek, značíme ho 0,
(3) $\cdot$ má neutrální prvek různý od 0, značíme ho 1,
(4) ke každému prvku x existuje inverzní prvek vzhledem k operaci $+$,
(5) pro libovolné $x, y, z \in P$ platí $x \cdot (y + z) = x \cdot y + x \cdot z$.

Pokud navíc

(6) ke každému prvku $x \neq 0$ existuje inverzní prvek vzhledem k operaci $\cdot$,

množina P s operacemi $+$ a $\cdot$ je *pole*.

Inverzní prvek k x vzhledem k operaci $+$ se nazývá *opačný* k x a značí se $-x$. Inverzní prvek k x vzhledem k operaci $\cdot$ se značí x^{-1}.

Podmínka (5) v předchozí definici je *distributivní zákon*.

Příklad. (1) Množiny $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ s operacemi sčítání a násobení jsou pole.

(2) Množina $\mathbb{Z}$ s operacemi sčítání a násobení je okruh, ale není pole.

(3) Množina $\mathbb{N}_0$ s operacemi sčítání a násobení není okruh.

(4) Množina $P[x]$ s operacemi sčítání a násobení polynomů je okruh, ale není pole.

(5) Množina $\mathcal{M}_n(P)$ s operacemi sčítání a násobení matic není okruh.

(6) Nechť $P = \{0, 1\}$ a binární operace $+$ a $\cdot$ na P jsou takové, že

$+$	0	1
0	0	1
1	1	0

a

$\cdot$	0	1
0	0	0
1	0	1

Neutrální prvek operace $+$ je 0 a inverzní (opačné) prvky jsou $-0 = 0$ a $-1 = 1$. Neutrální prvek operace $\cdot$ je 1 a inverzní prvek k 1 je 1 ($1^{-1} = 1$), inverzní prvek k 0 neexistuje. Množina $\{0, 1\}$ s těmito operacemi je pole.

(7) Nechť $P = \{0, 1, 2, 3\}$ a binární operace $+$ a $\cdot$ na P jsou takové, že

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

a

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Potom neutrální prvek operace $+$ je 0, neutrální prvek operace $\cdot$ je 1 a

$$\begin{array}{ll} -0 = 0 & 0^{-1} \text{ neexistuje} \\ -1 = 3 & 1^{-1} = 1 \\ -2 = 2 & 2^{-1} \text{ neexistuje} \\ -3 = 1 & 3^{-1} = 3 \end{array}$$

a

Množina $\{0, 1, 2, 3\}$ s těmito operacemi je okruh, ale není pole. ■

Tvrzení 7.0.1. *Buď P okruh. Pak pro libovolné prvky $x, y, z \in P$ platí*

(i) $x \cdot 0 = 0$;
(ii) $x \cdot (-1) = -x$;
(iii) $x \cdot (y - z) = x \cdot y - x \cdot z$.

Důkaz. (i) Platí

$$\begin{aligned} x \cdot 0 &= x \cdot (0 + 0) = \\ &= x \cdot 0 + x \cdot 0 \end{aligned}$$

a po přičtení $-(x \cdot 0)$ k oběma stranám rovnosti dostaneme $0 = x \cdot 0$.

(ii) Platí

$$0 = x \cdot 0 = x \cdot (1 + (-1)) = x \cdot 1 + x \cdot (-1) = \\ = x + x \cdot (-1)$$

a po přičtení $-x$ k oběma stranám rovnosti dostaneme $-x = x \cdot (-1)$.

(iii) Cvičení. □

Cvičení. Dokažte, že v každém okruhu platí:

(1) $(-1) \cdot (-1) = 1$,

(2) $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$. ▷

Tvrzení 7.0.2. *Buď P pole a buďte $x, y, z \in P$.*

(1) $x \cdot y = 0$ právě tehdy, když $x = 0$ nebo $y = 0$.

(2) Jestliže $x \cdot y = x \cdot z$ a $x \neq 0$, pak $y = z$.

Důkaz. (1) Jestliže $x = 0$ nebo $y = 0$, pak podle Tvrzení 7.0.1(i) také $x \cdot y = 0$.

Nechť $x \cdot y = 0$. Předpokládejme, že jeden z prvků x, y je nenulový, například $x \neq 0$. Potom s využitím Tvrzení 7.0.1(i) dostaneme

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

(2)

$xy = xz$	k oběma stranám přičteme $-xz$
$xy - xz = 0$	použijeme (iii) z předchozího tvrzení
$x(y - z) = 0$	použijeme první část tvrzení a $x \neq 0$
$y - z = 0$	k oběma stranám přičteme z
$y = z$	

□

Příklad. (1) V příkladu (7) máme okruh, v němž $2 \cdot 2 = 0$ a $2 \cdot 1 = 2 \cdot 3$. To ukazuje, že předchozí tvrzení neplatí pro okruhy.

(2) Pro okruh $P[x]$ ale předchozí tvrzení platí, viz kapitolu o polynomech. ■

Obdobně jako v kapitole 6 P^* označuje množinu $P \setminus \{0\}$.

Je-li P okruh, pak P s operací $+$ je komutativní grupa. Pro pole máme navíc následující tvrzení.

Tvrzení 7.0.3. *Je-li P pole, pak P^* s operací $\cdot$ je komutativní grupa.*

Důkaz. Buďte $x, y \in P^*$, tedy $x \neq 0$ a $y \neq 0$. Podle Tvrzení 7.0.2(i) $x \cdot y \neq 0$, tedy $x \cdot y \in P^*$, a množina P^* je uzavřená vzhledem k operaci $\cdot$. Zbytek tvrzení plyne z toho, že operace $\cdot$ je asociativní a komutativní, $1 \in P^*$ je neutrální prvek, každý nenulový prvek je invertibilní a příslušné inverze jsou nenulové. □

Tvrzení 7.0.4. *Množina $\mathbb{Z}_m$ zbytkových tříd je pole právě tehdy, když m je prvočíslo.*

Důkaz. Číslo 1 není prvočíslo a $\mathbb{Z}_1$ není pole (cvičení). Buď $m > 1$. Podle kapitol 6.5 a 6.6 $\mathbb{Z}_m$ splňuje podmínky (1)–(4) z definice okruhu a pole. Ověření, že platí distributivní zákon (5), ponecháme jako cvičení. Zbývá ukázat, že ke každému prvku $[x]_m \neq [0]_m$ existuje inverzní prvek vzhledem k operaci $\cdot$ právě tehdy, když m je prvočíslo.

Předpokládejme, že ke každému prvku $[x]_m \neq [0]_m$ existuje inverze. Podle Tvrzení 6.6.1 každé takové x je nesoudělné s m, tedy m je prvočíslo.

Na druhou stranu, je-li m prvočíslo, pak každé $x \in \mathbb{Z}$ takové, že $[x]_m \neq [0]_m$, je nesoudělné s m. Opět podle Tvrzení 6.6.1 $[x]_m$ má inverzi.

Jiný důkaz tohoto tvrzení lze nalézt v [Marvan, 3. Pole]. □

Takže, například, $\mathbb{Z}_4$ není pole. Čtyřprvkové pole ale existuje.

Příklad. Nechť $X = \{0, 1, a, b\}$ a binární operace + a · na X jsou takové, že

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

a

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Množina X s těmito operacemi + a · je pole. ■

Poznámka. Pro libovolné přirozené číslo n existuje n-prvkové pole právě tehdy, když n je mocnina prvočísla, čili $n = p^k$, kde p je prvočíslo a k je přirozené číslo.

Stejně jako máme podgrupy grup (a podstruktury dalších algebraických struktur), existují podokruhy okruhů a podpole polí. Zmíníme jen podpole.

Definice 7.0.2. Buď P pole. Buď $Q \subset P$ podmnožina taková, že

(1) $0, 1 \in Q$;
(2) je-li $x, y \in Q$, pak $x + y \in Q$ a $xy \in Q$;
(3) je-li $x \in Q$, pak $-x \in Q$;
(4) je-li $x \in Q$, $x \neq 0$, pak $x^{-1} \in Q$.

Potom Q je *podpole* pole P.

Aby podmnožina pole byla podpole, musí obsahovat neutrální prvky obou binárních operací, musí být uzavřená vzhledem k oběma binárním operacím a musí být uzavřená vzhledem k inverzím vzhledem k oběma binárním operacím.

Každé podpole je pole.

Příklad. (1) Pole $\mathbb{Q}$ je podpole polí $\mathbb{R}$ a $\mathbb{C}$. Pole $\mathbb{R}$ je podpole pole $\mathbb{C}$.

(2) $\mathbb{Z}$ není podpole pole $\mathbb{Q}$, neboť neobsahuje inverzi k 2 vzhledem k operaci ·.

(3) Množina $\{0, 1\}$ není podpole pole $\mathbb{Q}$ (a samozřejmě ani $\mathbb{R}$ a $\mathbb{C}$), protože $1 + 1 = 2 \notin \{0, 1\}$. Ačkoliv, jak už víme, na množině $\{0, 1\}$ lze definovat operace sčítání a násobení tak, že to je pole. ■

Definice 7.0.3. Podpole pole $\mathbb{C}$ je *číselné pole*.