Def.)

Pole je množina, řekneme P, spolu s

A) Bin. oper. sčítaní
$P \times P \to P$, $(a,b) \mapsto a+b$

R

B) Bin. oper. násobení
$P \times P \to P$, $(a,b) \mapsto a \cdot b$

C) se dvema vybranými prvky
$0 \neq 1 \in P$

D) zobrazením $P \to P$, $a \to -a$
$-a$ — opačný prvek k a

E) zobrazením $P \setminus \{0\} \to P \setminus \{0\}$,
$a \mapsto a^{-1}$, a^{-1} – převrácená hodnota

přičemž $\forall a,b,c \in P$ platí

1) $a+b = b+a$ – komutat.
2) $(a+b)+c = a+(b+c)$
3) $a+0 = a$
4) $a+(-a) = 0$

komut. grupa $(P,+,0,-a)$

R

5) $a \cdot b = b \cdot a$
6) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
7) $a \cdot 1 = a$

komutat. monoid $(P,\cdot,1)$

8) $a \neq 0 \Rightarrow a^{-1} a = 1$

9) $a \cdot (b+c) = ab + ac \Rightarrow$ distrib.

Pr. $\mathbb{R}$

Pr 2: $(\{0,1\}, +, 0, -, \cdot, 1, ^{-1})$

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

−	
0	1
1	0

$()^{-1}$	
0	—
1	1

→ cvič.

Tvrz. P - pole
Pak pro $\forall a \in P$ platí:

i) $a \cdot 0 = 0$

ii) $a(-1) = -a$

iii) $a \cdot (b-c) = a \cdot b - a \cdot c$

Důkaz iii)

$$a \cdot (b-c) \stackrel{?}{=} a \cdot b - a \cdot c$$

$$a \cdot (b-c) = a \cdot (b + (-c)) \stackrel{(a)}{=}$$

$$= a \cdot b + a(-c) \stackrel{ii}{=} a \cdot b + a \cdot ((-1) \cdot c) =$$

$$\stackrel{(II)(b)}{=} a \cdot b + (-1)(a \cdot c) \stackrel{ii}{=} a \cdot b + (-a \cdot c) =$$

$$= a \cdot b - a \cdot c \quad \square$$

<u>Tvrz.</u> P – pole
$a, b \in P$ splňující $a \cdot b = 0$
Pak $a = 0$ nebo $b = 0$

<u>Tvrz.</u> Je-li P – pole pak
$P^* := P \setminus \{0\}$, je grupa
vzhledem k „·"
$(P^*, \cdot, 1, ^{-1})$

<u>Tvrz.</u> P pole, $a, b \in P$
je-li $b \neq 0$ pak existuje
jediný prvek $\xi \in P$ takový,
že $a\xi + b = 0$
a sice $\xi = \boxed{-b \cdot a^{-1}}$
↳ řešení rovnice
$ax + b = 0$

$\mathbb{Z}_m$
<u>Tvrzení</u> Množ. $\mathbb{Z}_m$, $m > 1$
tvoří pole právě tehdy, když
m je prvočíslo

<u>Def</u> Buď P pole, buď $S \subset P$

Nechť jsou splněny násl. podm.

$0, 1 \in S$, je-li $a, b \in S$ pak

$a + b \in S$, $-a \in S$, $a \cdot b \in S$,

navíc je-li $a \neq 0$ pak $a^{-1} \in S$

Pak S – ~~uzavřená~~ podmnožina

S – je pole

S se nazývá <u>podpole</u>

<u>Def</u> Podpole v poli $\mathbb{C}$ se nazývá <u>číselné pole</u>

Def Okruh je množina R spolu s (platí A – D a hov Pol.) + platí 1 – 7 + 9 – 11

Př Polynómy $P(x)$ ↳ cvič.

$\exists a^{-1}$ a – invertibilní prvek
množ. invertib. prvků se značí R^*
Okruh je pole $\Leftrightarrow$ $R^* = R \setminus \{0\}$

Tvrz. Invertib. prvky okruhu $P(x)$ jsou právě nenulové konst. polyn.

Tvrz. $f, g, h \in P(x)$
1) $(f \cdot g = 0) \Rightarrow (f = 0 \vee g = 0)$
2) $(fg = fh \wedge f \neq 0) \Rightarrow$
$\Rightarrow (g = h)$

Def Buď daná množ. M
Relace $\sim$ na M se nazývá

1) **reflexivní** platí-li $a \sim a$ pro $\forall a \in M$
2) **antisymetrická** platí-li implikace $(a \sim b \wedge b \sim a) \Rightarrow (a = b)$
3) **tranzitivní** platí-li implikace $(a \sim b \wedge b \sim c) \Rightarrow (a \sim c)$

Relace, kt. splňuje 1–3 se nazývá **uspořádání**. Dvojice $(M, \sim)$ – uspoř. množina

Př $(\mathbb{R}, \leq)$, $(\mathbb{R}, \geq)$, $(\mathbb{Z}, \overset{\geq}{\leq})$
$(\mathbb{N}, \overset{\geq}{\leq})$

$(P(M), \subset)$

Buď $\sim$ – uspoř. na množ. M
Buď opačná relace $\sim^{-1}$
je také uspořád.
$\Rightarrow$ **Duální uspoř.**

$\leq \quad \leq^{-1} \; \geq$

Každá podmn. $N \subset M$, kde $(M, \leq)$ je opět uspoř. množ. $(N, \leq_N)$
$\downarrow$
indukované uspoř.

Def • $a, b \in M$ jsou **srovnatelné** platí-li
$a \leq b$ nebo $b \leq a$

• uspoř. množ. M se naz. **řetězec** jsou-li každé 2 prvky $a, b \in M$ srovnatelné

Def Buď $(M, \leq)$ usp. mn.
prvek $x \in M$ se naz.

- **nejmenší**; $x \leq a$ pro $\forall a \in M$
- **největší**; $x \geq a$ — " —
- **maximál.**; neexistuje $a \in M$ takové, že $a > x$
- **minimál.** ...... $a < x$