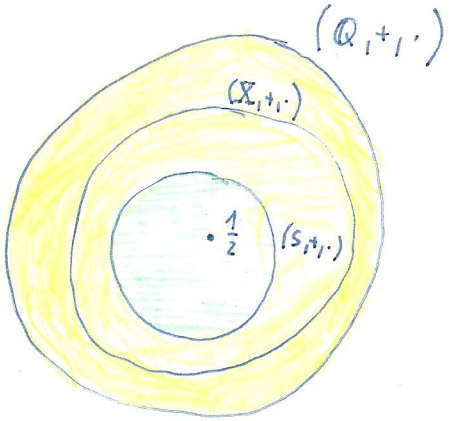
Př: $(\mathbb{Q},+,\cdot)$ je okruh. Nalezněte nejmenší podokruh (označme jej $(S,+,\cdot)$) obsahující prvek $\frac{1}{2}$. Tzn. jestliže $\frac{1}{2} \in X \subseteq S$, $(X,+,\cdot)$ je podokruh okruhu $(\mathbb{Q},+,\cdot)$, potom $S = X$. Určete S.



$\frac{1}{2} \in S$ a $(S,+,\cdot)$ je podokruh, potom S jistě musí obsahovat:

$$-\frac{1}{2} \; ; \; 0$$

protože $(S,+)$ je grupa. a protože $(S,+)$ je uzavřená vzhledem ke sčítání

$$\forall m \in \mathbb{N}_0 : \left.\begin{array}{l} \frac{1}{2}+\frac{1}{2}+\ldots+\frac{1}{2} = m\cdot\frac{1}{2} \in S \\ -\frac{1}{2}+(-\frac{1}{2})+\ldots+(-\frac{1}{2}) = m\cdot(-\frac{1}{2}) = -m\cdot\frac{1}{2} \in S \end{array}\right\} \Rightarrow \forall z \in \mathbb{Z} : z\cdot\frac{1}{2} \in S$$

(m-krát)

$(S,\cdot)$ je pologrupa $\Rightarrow$ S je množina uzavřená vzhledem k „násobení" $\Rightarrow$

$$\forall m \in \mathbb{N} : \underbrace{z}_{\in S}\cdot\underbrace{\frac{1}{2}}_{\in S}\cdot\underbrace{\frac{1}{2}}_{\in S}\cdot\ldots\cdot\underbrace{\frac{1}{2}}_{\in S} = z\cdot\left(\frac{1}{2}\right)^m \in S \qquad (m\text{-krát})$$

$\Rightarrow$ $X = \{ z\cdot(\frac{1}{2})^m \mid z \in \mathbb{Z}, m \in \mathbb{N} \} \subseteq S$. Ukážeme, že $(X,+,\cdot)$ je podokruh $(\mathbb{Q},+,\cdot)$.

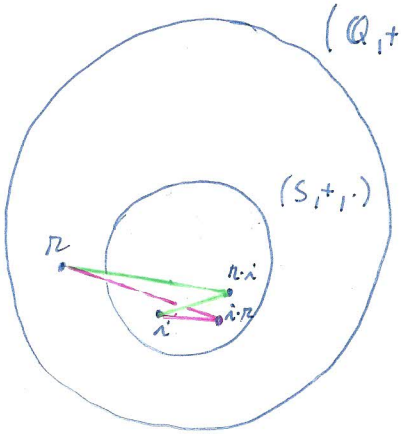
$$\forall\, z_1\left(\tfrac{1}{2}\right)^{m_1}, z_2\left(\tfrac{1}{2}\right)^{m_2} \in X : 1.)\; z_1\left(\tfrac{1}{2}\right)^{m_1} - z_2\left(\tfrac{1}{2}\right)^{m_2} = \frac{z_1 2^{m_2} - z_2 2^{m_1}}{2^{m_1+m_2}} = z\cdot\left(\tfrac{1}{2}\right)^{m_1+m_2} \in X$$

$$2.)\; z_1\left(\tfrac{1}{2}\right)^{m_1}\cdot z_2\left(\tfrac{1}{2}\right)^{m_2} = \left(\tfrac{1}{2}\right)^{m_1+m_2}\cdot \underbrace{z_1\cdot z_2}_{\in\mathbb{Z}} \in X$$

$\Rightarrow$ $(X,+,\cdot)$ je podokruh $\Rightarrow$ $S = X = \{ z\left(\frac{1}{2}\right)^m \mid z \in \mathbb{Z}, m \in \mathbb{N} \}$

□

Př: $(S,+,\cdot)$, kde $S=\{z\left(\frac{1}{2}\right)^m \mid z\in\mathbb{Z},\ m\in\mathbb{N}\}$ je podokruh okruhu $(\mathbb{Q},+,\cdot)$. Ověřte, zda $(S,+,\cdot)$ je ideál v $(\mathbb{Q},+,\cdot)$.



$(S,+,\cdot)$ je podokruh v $(\mathbb{Q},+,\cdot)$ $\Rightarrow$

stačí ověřit: $\forall r\in\mathbb{Q}\ \forall i\in S: (r\cdot i\in S)\wedge(i\cdot r\in S)$

$\forall r\in\mathbb{Q}\ \forall i=z\cdot\left(\frac{1}{2}\right)^m\in S:$

$$r\cdot i = i\cdot r = \underbrace{r}_{\in\mathbb{Q}}\cdot z\cdot\left(\frac{1}{2}\right)^m \quad (z\in\mathbb{Z})$$

r nemusí náležet do $\mathbb{Z}$!!!

např: $\underbrace{\frac{2}{3}}_{\in\mathbb{Q}}\cdot\underbrace{5\left(\frac{1}{2}\right)^3}_{\in S} = \underbrace{\frac{10}{3}}_{\notin\mathbb{Z}}\left(\frac{1}{2}\right)^3 \notin S$

$\Rightarrow$ $(S,+,\cdot)$ není ideál v $(\mathbb{Q},+,\cdot)$

Věta: Nechť $(R, +, \cdot)$ je obor integrity; $a, b, c \in R$, $a \neq 0$. Potom platí:

1.) $b \cdot a = c \cdot a \Rightarrow b = c$

2.) $a \cdot b = a \cdot c \Rightarrow b = c$

Důkaz: 1.)

$$ab = ac$$

$$ab - ac = 0$$

$$a(b-c) = 0 \quad / \ (R,+,\cdot) \text{ je obor integrity} \Rightarrow \begin{cases} a = 0 \\ \text{nebo} \\ b - c = 0 \end{cases}$$

ale $a \neq 0 \Rightarrow$

$$b - c = 0$$

$$b = c$$

2.) $ba = ca$

$$ba - ca = 0$$

$$(b-c)a = 0 \quad / \ a \neq 0, (R,+,\cdot) \text{ je obor integrity} \Rightarrow$$

$$(b-c) = 0$$

$$b = c$$

□

Věta: Jestliže $(R,+,\cdot)$ je konečný obor integrity, pak $(R,+,\cdot)$ je těleso.

Důkaz: Definice oboru integrity a tělesa se liší pouze v bodu 4.). Cílem je tedy dokázat platnost implikace:

① $|R| < \infty$

② $\forall a,b \in R : a \cdot b = 0 \Rightarrow (a = 0 \vee b = 0)$

$\Rightarrow \forall a \in R - \{0\}\ \exists \bar{a}^1 \in R : a \cdot \bar{a}^1 = \bar{a}^1 \cdot a = 1.$

Uvažujme libovolné $a \in R - \{0\}$ a množinu $A = \{a^n \mid n \in \mathbb{N}\}$.
Protože $A \subseteq R$ a $|R| < \infty$ musí existovat $i > j$ takové, že

$$a^i = a^j$$

$$a^{i-1} \cdot a = a^{j-1} \cdot a$$

(V oboru integrity můžeme krátit pokud $a \neq 0$, a to je.)

$$a^{i-1} = a^{j-1}$$

$$\vdots$$

$$a^{i-j} = 1$$

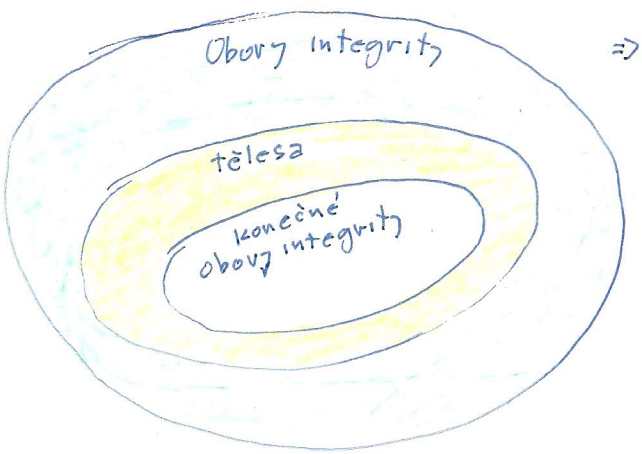
I.) $i - j = 1 \Rightarrow a^{i-j} = a = 1 \Rightarrow \bar{a}^1$ existuje a $\bar{a}^1 = 1$

II.) $i - j > 1 \Rightarrow a^{i-j-1} \cdot a = a \cdot a^{i-j-1} = a^{i-j} = 1$

$\Rightarrow a^{i-j-1} = \bar{a}^1$ (neboť $i - j > 1$)

$i-j-1 \in \mathbb{N}$

$a^{i-j-1} \in A \subseteq R$



□

Věta: Nechť p je prvočíslo. $\mathbb{Z}_p = \mathbb{Z}/_{p\mathbb{Z}}$. Označme: $\forall a \in \mathbb{Z}$: $\bar{a} = a + p\mathbb{Z}$,

$\oplus : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$, kde $\forall \bar{a}, \bar{b} \in \mathbb{Z}_p$: $\bar{a} \oplus \bar{b} = \overline{a+b}$

$\odot : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p$, kde $\forall \bar{a}, \bar{b} \in \mathbb{Z}_p$: $\bar{a} \odot \bar{b} = \overline{a \cdot b}$

Potom $(\mathbb{Z}_p, \oplus, \odot)$ je těleso.

Poznámka: To znamená, že okruh zbytkových tříd modulo p, kde p je prvočíslo je vždy těleso.

Důkaz: $(\mathbb{Z}_p, \oplus, \odot)$ je faktorovým okruhem okruhu $(\mathbb{Z}, +, \cdot)$ podle ideálu $p\mathbb{Z}$. Je to tedy okruh a zbývá dokázat platnost podmínek 1.) až 4.) z definice tělesa a nebo (a to uděláme), že jde o konečný obor integrity.

1.) existence jedničky v $\mathbb{Z}_p$

$$\forall \bar{a} \in \mathbb{Z}_p : \quad \bar{a} \cdot \bar{1} = \bar{1} \cdot \bar{a} = \bar{a} \quad \Rightarrow \quad 1 = \bar{1}$$

2.) netriviálnost:

$$1 = \bar{1} \neq \bar{0} = 0$$

3.) komutativita:

$$\forall a, b \in \mathbb{Z}: \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b} = \overline{b \cdot a} = \bar{b} \cdot \bar{a}$$

4.) neexistují nenulové dělitelé nuly:

$$\forall \bar{a}, \bar{b} \in \mathbb{Z}_p : \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b} = \bar{0} \quad \Rightarrow \quad a \cdot b = k \cdot p \quad \text{a protože } p$$

$\Leftarrow$

je prvočíslo $\Rightarrow (p \mid a \ \vee \ p \mid b) \Rightarrow$
$(a = k_1 \cdot p \ \vee \ b = k_2 \cdot p) \Rightarrow (\bar{a} = \bar{0} \ \vee \ \bar{b} = \bar{0})$

5.) konečnost:

$$\mathbb{Z}_p = \{\bar{0}, \bar{1}, \dots, \overline{p-1}\} \quad \Rightarrow \quad \mathbb{Z}_p \text{ je konečná množina}$$

□

Příklad: $(R, +, \cdot)$, kde R je množina reálných funkcí reálné proměnné jejichž definičním oborem je $\mathbb{R}$ a operace $+$ a $\cdot$ jsou dány předpisy

$$+ : \quad \forall x \in R : \quad (f+g)(x) = f(x) + g(x)$$

$$\cdot : \quad \forall x \in R : \quad (f \cdot g)(x) = f(x) \cdot g(x)$$

je okruh. Uvažujme množinu polynomických funkcí

$$\mathbb{R}[x] = \{ f : \mathbb{R} \to \mathbb{R} \mid f(x) = a_n x^n + \dots + a_1 x + a_0 ; \; a_n, \dots, a_0 \in \mathbb{R}, \; n \in \mathbb{N}_0 \}$$

Definičním oborem každé polynomické funkce (a ty existují) je $\mathbb{R}$. Navíc rozdíl i součin dvou polynomických funkcí je zase polynomická funkce $\Rightarrow$ $(\mathbb{R}[x], +, \cdot)$ je podokruhem $(R, +, \cdot)$. $\Rightarrow$

$$(\mathbb{R}[x], +, \cdot) \text{ je okruh}$$

$(\mathbb{R}[x], +, \cdot)$ budeme nazývat okruhem polynomických funkcí nad $\mathbb{R}$

Lema: Nechť $p(x) \in \mathbb{R}[x]$. Označme $\langle p(x) \rangle = \{ f(x) \cdot p(x) \mid f(x) \in \mathbb{R}[x] \}$.
Potom $(\langle p(x) \rangle, +, \cdot)$ je ideál v okruhu $(\mathbb{R}[x], +, \cdot)$

Důkaz: $\langle p(x) \rangle \subseteq \mathbb{R}[x]$ a $\langle p(x) \rangle \neq \emptyset$ neboť $1 \cdot p(x) \in \langle p(x) \rangle$. Navíc

1.) $\forall a(x), b(x) \in \langle p(x) \rangle$: $\left.\begin{array}{l} a(x) = f(x)\,p(x) \\ b(x) = g(x)\,p(x) \end{array}\right\} \Rightarrow a(x) - b(x) = \underbrace{(f(x) - g(x))}_{\in \mathbb{R}[x]}\, p(x) \in \langle p(x) \rangle$

2.) $\forall r(x) \in \mathbb{R}[x] \;\; \forall i(x) = f(x)\,p(x) \in \langle p(x) \rangle$: $r(x) \cdot i(x) = i(x)\, r(x) = (r(x) f(x)) \cdot p(x) \in \langle p(x) \rangle$

□

Př: Ověřte, zda okruh polynomů nad $\mathbb{R}$, tj. $(\mathbb{R}[x], +, \cdot)$ je oborem integrity, nebo tělesem.

1.) Ukážeme, že $(\mathbb{R}[x], +, \cdot)$ je obor integrity.

Nulou v $\mathbb{R}[x]$ je nulový polynom $o(x) = 0$

Nechť $a(x), b(x) \in \mathbb{R}[x] - \{o(x)\}$, potom:

$a(x) = a_m x^m + \dots + a_1 x + a_0$, kde $a_m \neq 0$

$b(x) = b_m x^m + \dots + b_1 x + b_0$, kde $a_m \neq 0$

$$\Rightarrow a(x) \cdot b(x) = \underbrace{a_m \cdot b_m}_{\neq 0} x^{m+m} + (a_{m-1} b_m + a_m b_{m-1}) x^{m+m-1} + \dots + a_0 b_0$$

protože $(\mathbb{R}, +, \cdot)$ je obor integrity

$$\Downarrow$$

$$a(x)\, b(x) \neq o(x)$$

$\Rightarrow (\mathbb{R}[x], +, \cdot)$ je obor integrity.

Poznámka: Výše uvedené uvažení lze zobecnit (důkaz analogický):

Okruh polynomů nad oborem integrity je obor integrity.

2.) Ukážeme, že $(\mathbb{R}[x], +, \cdot)$ není těleso.

Dokážeme, že polynom x nemá prvek inverzní vzhledem k násobení.

$\forall f(x) \in \mathbb{R}[x] - \{\sigma(x)\}$: $f(x) \cdot x =$ polynom stupně $\geq 1 \Rightarrow f(x) \cdot x \neq 1$

$\forall$ případě $f(x) = \sigma(x)$: $f(x) \cdot x = \sigma(x) \cdot x = \sigma(x) \neq 1$

$\Rightarrow$ x^{-1} neexistuje $\Rightarrow$ $(\mathbb{R}[x], +, \cdot)$ není těleso.

Příklad: Prozkoumejte faktorový okruh $\mathbb{R}[x]/\langle x^2-1\rangle$.

$$\mathbb{R}[x]/\langle x^2-1\rangle = \{ f(x) + \langle x^2-1\rangle \mid f(x) \in \mathbb{R}[x] \}$$

libovolný polynom $f(x)$ můžeme podělit polynomem x^2-1 se zbytkem.

Např: $(x^3-2x^2+x-1) : (x^2-1) = x-2$ ($= f(x)$)

$-(x^3-x)$

$-2x^2+2x-1$

$-(-2x^2+2)$

$2x-3$ $= r(x)$ ... zbytek po dělení x^2-1 $\Rightarrow st(r(x)) < 2$

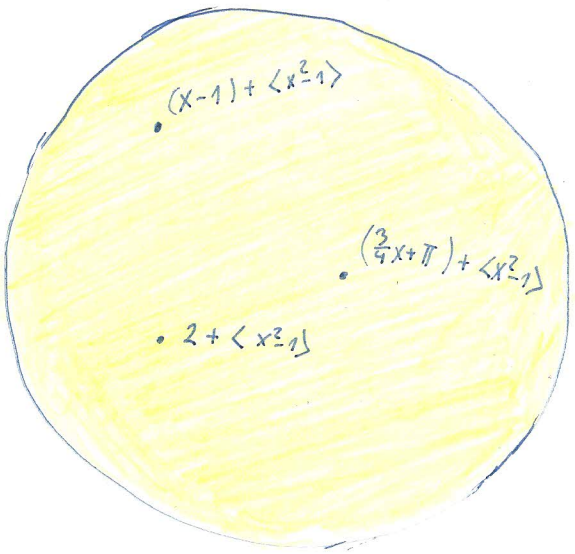
$\Rightarrow$ $x^3-2x^2+x-1 = (x-2)(x^2-1) + (2x-3)$

$\Rightarrow$ $\underbrace{(x^3-2x^2+x-1)}_{f(x)} + \langle x^2-1\rangle = (2x-3) + \underbrace{(x-2)(x^2-1)}_{\in \langle x^2-1\rangle} + \langle x^2-1\rangle = \underbrace{(2x-3)}_{r(x)} + \langle x^2-1\rangle$

Obecně: $f(x) + \langle x^2-1\rangle = r(x) + q(x)(x^2-1) + \langle x^2-1\rangle = r(x) + \langle x^2-1\rangle \Rightarrow$

$$\mathbb{R}[x]/\langle x^2-1\rangle = \{ r(x) + \langle x^2-1\rangle \mid r(x) \in \mathbb{R}[x],\ st(r(x)) \in \{0,1\} \} \Rightarrow$$

$$\boxed{\mathbb{R}[x]/\langle x^2-1\rangle = \{(ax+b) + \langle x^2-1\rangle \mid a,b \in \mathbb{R}\}}$$



např: $\underbrace{((x-1)+\langle x^2-1\rangle)}_{\neq 0+\langle x^2-1\rangle} \cdot \underbrace{((x+1)+\langle x^2-1\rangle)}_{\neq 0+\langle x^2-1\rangle} =$

$= (x-1)(x+1) + \langle x^2-1\rangle =$

$= (x^2-1) + \langle x^2-1\rangle =$

$= \underbrace{0+\langle x^2-1\rangle}_{\text{nulový prvek v okruhu } \mathbb{R}[x]/\langle x^2-1\rangle}$

($\Rightarrow$ existují zde netriviální dělitelé nuly)

např.: $((2x+1)+\langle x^2-1\rangle)\cdot(x+\langle x^2-1\rangle) =$

$= (2x^2+x) + \langle x^2-1\rangle = (2x^2+x) - 2(x^2-1) =$

$= \underline{\underline{(x+2)+\langle x^2-1\rangle}}$

Př.: Ověřte, zda $(S,+,\cdot)$, kde $S=\{q\cdot\frac{1}{2} \mid q\in\mathbb{Q}\}$ je ideál v $(\mathbb{Q},+,\cdot)$. Pokud ano, určete $\mathbb{Q}/S$

Musíme ověřit, zda

1.) $\forall a,b\in S: a-b\in S$:

$$a,b\in S \Rightarrow \left.\begin{array}{l} a=\frac{1}{2}q_1 \\ b=\frac{1}{2}q_2 \end{array}\right\} \Rightarrow \quad a-b=\frac{1}{2}\underbrace{(q_1-q_2)}_{\in\mathbb{Q}}=\frac{1}{2}q\in S$$

2.) $\forall a\in\mathbb{Q}\ \forall b\in S: a\cdot b\in S$:

$$b\in S \Rightarrow b=\frac{1}{2}q \text{, kde } q\in\mathbb{Q} \Rightarrow a\cdot b=a\cdot\frac{1}{2}q=\frac{1}{2}\underbrace{q^*}_{=a\cdot q\in\mathbb{Q}}\in S$$

$\Rightarrow$ $(S,+,\cdot)$ je ideál v $(\mathbb{Q},+,\cdot)$

$$\mathbb{Q}/S=\{q+S \mid q\in\mathbb{Q}\}=\{\{q+\tfrac{1}{2}q \mid q\in\mathbb{Q}\} \mid q\in\mathbb{Q}\}$$

Platí:

$$g_1+S=g_2+S \iff g_1-g_2\in S \iff \exists q\in\mathbb{Q}: g_1-g_2=\frac{1}{2}\cdot q$$

ale $g_1-g_2\in\mathbb{Q} \Rightarrow g_1-g_2=s\in\mathbb{Q} \Rightarrow$

$\Rightarrow \quad s=\frac{1}{2}q \Rightarrow q=2s \Rightarrow$ takové q existuje vždy!

$\Rightarrow \forall g_1,g_2\in\mathbb{Q}: g_1+S=g_2+S \Rightarrow \mathbb{Q}/S=\{\{0+\mathbb{Q}\}\}$

a opravdu $S=\{q\cdot\frac{1}{2} \mid q\in\mathbb{Q}\}=\mathbb{Q}$ (obsahuje libovolné rac. číslo q^* stačí zvolit $q=2q^*$)

$\Rightarrow$ $\mathbb{Q}/S=\{\mathbb{Q}\}$