

1.1 Konečná tělesa

Známým příkladem konečného tělesa je těleso $(\mathbb{Z}_p, +, \cdot)$, kde p je nějaké prvočíslo. Jde o těleso zbytkových tříd modulo p s obvyklým sčítáním a násobením zbytkových tříd. Jako konkrétní příklad uveďme $(\mathbb{Z}_5, +, \cdot)$. Pro jednoduchost označme prvky $\mathbb{Z}_5$ jako $0, 1, 2, 3, 4$ (místo $\bar{0}_5, \dots, \bar{4}_5$). Sčítání a násobení je potom dáno tabulkami:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Tělesa $(\mathbb{Z}_p, +, \cdot)$ jsou tělesa, která mají p prvků. Nejsou však jedinými konečnými tělesy. Dá se ukázat, že všechna konečná tělesa $(T, +, \cdot)$ splňují podmínku

$$|T| = p^n,$$

kde p je prvočíslo a $n \in \mathbb{N}$. Navíc, pro každé prvočíslo p a přirozené číslo n umíme zkonstruovat konečné těleso o p^n prvcích. Ukažme si na konkrétním příkladě.

1.2 Konstrukce tělesa $GF(3^2)$.

Vyjdeme z okruhu polynomů $(\mathbb{Z}_3[x], +, \cdot)$. Prvky $\mathbb{Z}_3[x]$ jsou polynomy jedné neurčité nad $\mathbb{Z}_3$. Jsou to polynomy ve tvaru

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, \text{ kde } a_i \in \mathbb{Z}_3,$$

Pro jednoduchost zápisu budeme dále místo $\bar{a} \bmod 3$ psát pouze a . Jinak řečeno, místo zbytkových tříd budeme psát jejich libovolného reprezentanta. Například, místo $\bar{1} \bmod 3$ můžeme psát jen 1, ale i -2 , nebo 4 $\dots$.

Sčítání a násobení polynomů v $\mathbb{Z}_3[x]$ je definováno „přirozeným způsobem.“ Ilustrujme na příkladech:

$$(x^3 + 2x^2 - x + 2) + (2x^3 + 2x^2 - x - 1) = 3x^3 + 4x^2 - 2x + 1 = x^2 + x + 1,$$

$$(x^3 + 2) \cdot (2x^2 - x) = 2x^5 - x^4 + 4x^2 - 2x = 2x^5 + 2x^4 + x^2 + x.$$

Nyní si vybereme nějaký **ireducibilní polynom** $p(x)$ **druhého stupně** nad $\mathbb{Z}_3$ a faktorizujeme $\mathbb{Z}_3[x]$ podle množiny (ideálu) násobků tohoto polynomu - označme ji $[p(x)]$. To jest, vznikne struktura

$$\mathbb{Z}_3[x]/[p(x)] = \{\mathbf{f}(\mathbf{x}) + [\mathbf{p}(\mathbf{x})] \mid f(x) \in \mathbb{Z}_3[x]\},$$

kde

$$f(x) + [p(x)] = \{f(x) + k \cdot p(x) \mid k \in \mathbb{Z}_3\}.$$

Všimněme si, že

$$(f(x) + [p(x)]) + [p(x)] = \{f(x) + p(x) + k \cdot p(x) \mid k \in \mathbb{Z}_3\} = \{f(x) + k_1 \cdot p(x) \mid k_1 \in \mathbb{Z}_3\} = f(x) + [p(x)]$$

Z toho je zřejmé, že $f(x) + [p(x)]$ a $g(x) + [p(x)]$ jsou tytéž prvky množiny $\mathbb{Z}_3[x]/[p(x)]$ právě když se liší pouze o násobek polynomu $p(x)$ - právě když dávají stejný zbytek po dělení polynomem $p(x)$. Jinak řečeno, třídu rozkladu $f(x) + [p(x)]$ můžeme reprezentovat zbytkem z polynomu $f(x)$ po dělení polynomem $p(x)$. Množinu $\mathbb{Z}_3[x]/[p(x)]$ tedy můžeme chápat jako množinu všech možných zbytků, které můžeme obdržet při dělení polynomů z $\mathbb{Z}_3[x]$ polynomem $p(x)$.

Kolik takových zbytků je? To záleží na stupni polynomu $p(x)$. Vezměme konkrétní příklad:

$$p(x) = x^2 + x + 2.$$

Jedná se o ireducibilní polynom nad $\mathbb{Z}_3$. Při dělení tímto polynomem můžeme obdržet jako zbytek libovolný polynom nad $\mathbb{Z}_3$, jehož stupeň je menší než 2. Jde o polynomy:

$$\left. \begin{array}{l} 0x + 0 \\ 0x + 1 \\ 0x + 2 \\ 1x + 0 \\ 1x + 2 \\ 1x + 3 \\ 2x + 0 \\ 2x + 1 \\ 2x + 2 \end{array} \right\} \Rightarrow \text{počet prvků } \mathbb{Z}_3[x]/[p(x)] \text{ je } 3^2$$

Sčítání a násobení prvků z $\mathbb{Z}_3[x]/[p(x)]$ je opět definováno „přirozeným způsobem“:

$$(f(x) + [p(x)]) + (g(x) + [p(x)]) = (f(x) + g(x)) + [p(x)] \text{ (tři druhy plusů !!! :)})$$

a

$$(f(x) + [p(x)]) \cdot (g(x) + [p(x)]) = (f(x) \cdot g(x)) + [p(x)].$$

Množina $\mathbb{Z}_3[x]/[p(x)]$ s takto definovanými operacemi bude tvořit konečné těleso.

Dá se ukázat, že nezávisí na výběru reprezentantů - místo s prvky $\mathbb{Z}_3[x]/[p(x)]$ (zbytkovými třídami) můžu pracovat s jejich reprezentanty - polynomy nad $\mathbb{Z}_3$ stupně menšího než tři.

Tabulky násobení a sčítání v $\mathbb{Z}_3[x]/[p(x)]$ proto můžeme psát ve tvaru:

$\cdot$	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x + 1$	$x + 2$	$2x$	$2x + 1$	$2x + 2$
2	0	2	1	$2x$	$2x + 2$	$2x + 1$	x	$x + 2$	$x + 1$
x	0	x	$2x$	$2x + 1$	1	$x + 1$	$x + 2$	$2x + 2$	2
x + 1	0	$x + 1$	$2x + 2$	1	$x + 2$	$2x$	2	x	$2x + 1$
x + 2	0	$x + 2$	$2x + 1$	$x + 1$	$2x$	2	$2x + 2$	1	x
2x	0	$2x$	x	$x + 2$	2	$2x + 2$	$2x + 1$	$x + 1$	1
2x + 1	0	$2x + 1$	$x + 2$	$2x + 2$	x	1	$x + 1$	2	$2x$
2x + 2	0	$2x + 2$	$x + 1$	2	$2x + 1$	x	1	$2x$	$x + 2$

$+$	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
0	0	1	2	x	$x + 1$	$x + 2$	$2x$	$2x + 1$	$2x + 2$
1	1	2	0	$x + 1$	$x + 2$	x	$2x + 1$	$2x + 2$	$2x$
2	2	0	1	$x + 2$	x	$x + 1$	$2x + 2$	$2x$	$2x + 1$
x	x	$x + 1$	$x + 2$	$2x$	$2x + 1$	$2x + 2$	0	1	2
x + 1	$x + 1$	$x + 2$	x	$2x + 1$	$2x + 2$	$2x$	1	2	0
x + 2	$x + 2$	x	$x + 1$	$2x + 2$	$2x$	$2x + 1$	2	0	1
2x	$2x$	$2x + 1$	$2x + 2$	0	1	2	x	$x + 1$	$x + 2$
2x + 1	$2x + 1$	$2x + 2$	$2x$	1	2	0	$x + 1$	$x + 2$	x
2x + 2	$2x + 2$	$2x$	$2x + 1$	2	0	1	$x + 2$	x	$x + 1$

Jak bylo řečeno, množinu $\mathbb{Z}_3[x]/[p(x)]$ můžeme chápat jako množinu všech možných zbytků, které můžeme obdržet při dělení polynomů z $\mathbb{Z}_3[x]$ polynomem $p(x)$. Zvolili jsme $p(x) = x^2 + x + 2$. Není to však jediný ireducibilní polynom stupně 2 nad $\mathbb{Z}_3$! Co když zvolíme jiný, například:

$$x^2 + 1 \text{ ?!}$$

Obdržíme jinou strukturu? Zkusme.

Množina zbytků bude jistě stejná - půjde o všechny možné polynomy stupně menšího než dva nad $\mathbb{Z}_3$. Jak bude vypadat jejich tabulka sčítání? Ta se proti

předchozímu případu také nebude lišit – sčítání bude fungovat stejně – nezávisí na volbě polynomu. Tabulky násobení v $\mathbb{Z}_3[x]/[x^2+x+2]$ a $\mathbb{Z}_3[x]/[x^2+1]$ se však lišit budou. Napišme si je pod sebe:

Tabulka násobení v $\mathbb{Z}_3[x]/[x^2+1]$

$\cdot$	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x + 1$	$x + 2$	$2x$	$2x + 1$	$2x + 2$
2	0	2	1	$2x$	$2x + 2$	$2x + 1$	x	$x + 2$	$x + 1$
x	0	x	$2x$	2	$x + 2$	$2x + 2$	1	$x + 1$	$2x + 1$
x + 1	0	$x + 1$	$2x + 2$	$x + 2$	$2x$	1	$2x + 1$	2	x
x + 2	0	$x + 2$	$2x + 1$	$2x + 2$	1	x	$x + 1$	$2x$	2
2x	0	$2x$	x	1	$2x + 1$	$x + 1$	2	$2x + 2$	$x + 2$
2x + 1	0	$2x + 1$	$x + 2$	$x + 1$	2	$2x$	$2x + 2$	x	1
2x + 2	0	$2x + 2$	$x + 1$	$2x + 1$	x	2	$x + 2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/[x^2+x+2]$

$\cdot$	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x + 1$	$x + 2$	$2x$	$2x + 1$	$2x + 2$
2	0	2	1	$2x$	$2x + 2$	$2x + 1$	x	$x + 2$	$x + 1$
x	0	x	$2x$	$2x + 1$	1	$x + 1$	$x + 2$	$2x + 2$	2
x + 1	0	$x + 1$	$2x + 2$	1	$x + 2$	$2x$	2	x	$2x + 1$
x + 2	0	$x + 2$	$2x + 1$	$x + 1$	$2x$	2	$2x + 2$	1	x
2x	0	$2x$	x	$x + 2$	2	$2x + 2$	$2x + 1$	$x + 1$	1
2x + 1	0	$2x + 1$	$x + 2$	$2x + 2$	x	1	$x + 1$	2	$2x$
2x + 2	0	$2x + 2$	$x + 1$	2	$2x + 1$	x	1	$2x$	$x + 2$

Všimněme si, že první tři řádky a také první tři sloupce jsou stejné, jinde se tabulky liší. Ukážeme, že i přesto jde kvalitativně o tytéž struktury.

Přeuspořádejme prvky v tabulce násobení v $\mathbb{Z}_3[x]/[x^2+x+2]$:

Tabulka násobení v $\mathbb{Z}_3[x]/[x^2+1]$

$\cdot$	0	1	2	x	x + 1	x + 2	2x	2x + 1	2x + 2
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x + 1$	$x + 2$	$2x$	$2x + 1$	$2x + 2$
2	0	2	1	$2x$	$2x + 2$	$2x + 1$	x	$x + 2$	$x + 1$
x	0	x	$2x$	2	$x + 2$	$2x + 2$	1	$x + 1$	$2x + 1$
x + 1	0	$x + 1$	$2x + 2$	$x + 2$	$2x$	1	$2x + 1$	2	x
x + 2	0	$x + 2$	$2x + 1$	$2x + 2$	1	x	$x + 1$	$2x$	2
2x	0	$2x$	x	1	$2x + 1$	$x + 1$	2	$2x + 2$	$x + 2$
2x + 1	0	$2x + 1$	$x + 2$	$x + 1$	2	$2x$	$2x + 2$	x	1
2x + 2	0	$2x + 2$	$x + 1$	$2x + 1$	x	2	$x + 2$	1	$2x$

Tabulka násobení v $\mathbb{Z}_3[x]/[x^2+x+2]$

$\cdot$	0	1	2	x + 2	x	x + 1	2x + 1	2x + 2	2x
0	0	0	0	0	0	0	0	0	0
1	0	1	2	$x + 2$	x	$x + 1$	$2x + 1$	$2x + 2$	$2x$
2	0	2	1	$2x + 1$	$2x$	$2x + 2$	$x + 2$	$x + 1$	x
x + 2	0	$x + 2$	$2x + 1$	2	$x + 1$	$2x$	1	x	$2x + 2$
x	0	x	$2x$	$x + 1$	$2x + 1$	1	$2x + 2$	2	$x + 2$
x + 1	0	$x + 1$	$2x + 2$	$2x$	1	$x + 2$	x	$2x + 1$	2
2x + 1	0	$2x + 1$	$x + 2$	1	$2x + 2$	x	2	$2x$	$x + 1$
2x + 2	0	$2x + 2$	$x + 1$	x	2	$2x + 1$	$2x$	$x + 2$	1
2x	0	$2x$	x	$2x + 2$	$x + 2$	2	$x + 1$	1	$2x + 1$

Př. Nalezněte nějaký izomorfismus $(\mathbb{Z}_3[x]/\langle x^2+1 \rangle, +, \cdot)$ na $(\mathbb{Z}_3[x]/\langle x^2+x+2 \rangle, +, \cdot)$

Izomorfismus těles $f: T_1 \rightarrow T_2$ musí splňovat $\forall a, b \in T_1$:

$$1.) \overset{\text{operace na } T_1}{f(a+b)} = \overset{\text{operace na } T_2}{f(a) + f(b)} \Rightarrow \text{Je to izomorfismus grupy } (T_1, +) \text{ na } (T_2, +).$$

$$2.) \overset{\text{operace na } T_1}{f(a \cdot b)} = \overset{\text{operace na } T_2}{f(a) \cdot f(b)} \Rightarrow \text{Je to izomorfismus grupy } (T_1, \cdot) \text{ na } (T_2, \cdot).$$

$$\Rightarrow \boxed{f(0) = 0 \quad \text{a} \quad f(1) = 1}$$

$$f(1) = 1 \Rightarrow f(2) = f(1+1) = f(1) + f(1) = 1+1=2 \Rightarrow f(3) = f(2+1) = f(2) + f(1) = 2+1=3=0$$

Tzn. podtěleso $(\mathbb{Z}_3, +, \cdot)$ se zobrazí (identicky) na sebe.

$$\Rightarrow \boxed{f(ax+b) = f(a)f(x) + f(b) = a \cdot f(x) + b} \Rightarrow \text{Izomorfismus bude jednoznačně určen hodnotou } f(x).$$

$\Rightarrow$ Zvolme například $f(x) = x+2$ a ověřme, že jde o izomorfismus:

$f(x) \notin \{0, 1, 2\}$ jinak by f nebylo injektivní!

$$1.) f(a_1x+b_1) + f(a_2x+b_2) = a_1(x+2)+b_1 + a_2(x+2)+b_2 = (a_1+a_2)(x+2) + (b_1+b_2) = f((a_1+a_2)x + (b_1+b_2))$$

$$2.) f(a_1x+b_1) \cdot f(a_2x+b_2) = [a_1(x+2)+b_1] \cdot [a_2(x+2)+b_2] = a_1a_2(x+2)(x+2) + (a_1b_2+b_1a_2)(x+2) + b_1b_2$$

$$= f(a_1a_2x^2 + (a_1b_2+b_1a_2)x + b_1b_2) = a_1a_2(x+2)(x+2) + (a_1b_2+b_1a_2)(x+2) + b_1b_2$$

$\Rightarrow$ je to homomorfismus

$$3.) \text{Určíme } \text{Ker } f = \{ax+b \in \mathbb{Z}_3[x]/\langle x^2+1 \rangle : f(ax+b) = 0 \text{ v } \mathbb{Z}_3[x]/\langle x^2+x+2 \rangle\}$$

$$f(ax+b) = a(x+2)+b \Leftrightarrow ax+(2a+b) = 0x+0 \Leftrightarrow a=0 \text{ a } b=0 \Rightarrow$$

$$\Rightarrow \text{Ker } f = \{0x+0\} \Rightarrow \text{je injektivní}$$

$$4.) \forall ax+b \in \mathbb{Z}_3[x]/\langle x^2+x+1 \rangle : f(a_0x+b_0) = a_0(x+2)+b_0 = \underset{a}{a_0}x + \underset{b}{b_0-2a_0} \Rightarrow$$

$$(a_0 = a \text{ a } b_0 - 2a = b) \Rightarrow (a_0 = a \text{ a } b_0 = b + 2a)$$

$$\Rightarrow \exists a_0x+b_0 \in \mathbb{Z}_3[x]/\langle x^2+x+1 \rangle : f(a_0x+b_0) = ax+b \Rightarrow \text{je surjektivní}$$

Pr. min Je $\mathbb{Z}[x]/[x^2-1]$ těleso?

Není:
$$\underbrace{(x-1) + [x^2-1]}_{\neq 0 + [x^2-1]} \cdot \underbrace{(x+1) + [x^2-1]}_{\neq 0 + [x^2-1]} = (x-1)(x+1) + [x^2-1] = (x^2-1) + [x^2-1] = 0 + [x^2-1]$$

$\Rightarrow$ součin dvou nenulových prvků je nulový prvek $\Rightarrow$ není to obor integrity $\Rightarrow$ není to těleso

(v tělese platí: $a \cdot b = 0$ / předpokládejme $a, b \neq 0 \Rightarrow \exists a', b' \Rightarrow$
 $a' \cdot a \cdot b = a' \cdot 0$
 $b = 0$ spor!

Pr: Ověřte, zda faktorový okruh $(\mathbb{R}[x]/\langle x^2-1 \rangle, +, \cdot)$ je také oborem integrity, nebo sešesem.

Faktorový okruh $(\mathbb{R}[x]/\langle x^2-1 \rangle, +, \cdot)$ obsahuje "zbytkové třídy modulo x^2-1 ",

$$\text{neboť } \mathbb{R}[x]/\langle x^2-1 \rangle = \{ f(x) + \langle x^2-1 \rangle \mid f(x) \in \mathbb{R}[x] \} = \{ p(x) + \langle x^2-1 \rangle \mid p(x) \in \mathbb{R}[x], \deg p(x) < 2 \}$$

Označení: dohodněme se, že místo $f(x) + \langle x^2-1 \rangle$ budeme psát $\overline{f(x)}$.

Na faktorovém okruhu $(\mathbb{R}[x]/\langle x^2-1 \rangle, +, \cdot)$ sčítáme a násobíme "modulo x^2-1 ".

Příklad:

$$\overline{x+1} + \overline{2x+3} = \overline{3x+4}$$

$$\begin{aligned} \overline{x+1} \cdot \overline{2x+3} &= \overline{(x+1) \cdot (2x+3)} = \overline{2x^2 + 5x + 3} = \\ &= \overline{2x^2 + 5x + 3 - 2(x^2-1)} = \overline{5x+5} \end{aligned}$$

Nulový okruh: $(\mathbb{R}[x]/\langle x^2-1 \rangle, +, \cdot)$ je proto zbytková třída:

$$0 = \overline{0} = \overline{x^2-1} = \overline{2 \cdot (x^2-1)} = \overline{x \cdot (x^2-1)} = \overline{(x+1)(x^2-1)} = \overline{f(x) \cdot (x^2-1)} \quad f(x) \in \mathbb{R}[x]$$

$(\mathbb{R}[x]/\langle x^2-1 \rangle, +, \cdot)$ není oborem integrity, neboť:

$$\overline{(x-1)} \cdot \overline{(x+1)} = \overline{(x^2-1)} = \overline{0}$$

$\neq 0 \quad \neq 0$

Př: Ověřte, zda faktorový okruh $\mathbb{R}[x]/\langle x^2+1 \rangle$ je také oborem integrity, nebo tělesem.

Faktorový okruh $(\mathbb{R}[x]/\langle x^2+1 \rangle, +, \cdot)$ obsahuje „zbytkové třídy modulo x^2+1 “, které sčítáme a násobíme „modulo x^2+1 “. Například:

$$\overline{(3x + \frac{1}{2})} + \overline{(-x + 5)} = \overline{2x + \frac{11}{2}}, \quad \overline{(x-1)} \cdot \overline{(x+1)} = \overline{x^2-1} = \overline{(x^2+1) - (x^2+1)} = \overline{-2}$$

Polynom x^2+1 je ireducibilní - nelze rozložit na součin polynomů jejího stupně je menší než 2 a větší než 0 - tj. na součin dvou lineárních polynomů.

$\Rightarrow (\mathbb{R}[x]/\langle x^2+1 \rangle, +, \cdot)$ je oborem integrity. Zjistíme, zda je tělesem.

Nejprve zjistíme, zda zbytkové třídy ve tvaru $\overline{x+a_0}$, kde $a_0 \in \mathbb{R}$ mají inverzi vzhledem k násobení. $\overline{ax+b} = \overline{x+a_0}^{-1} \Leftrightarrow$ existují $a, b \in \mathbb{R}$:

$$\underbrace{(x+a_0) \cdot (ax+b)}_{\text{výsledek je polynom 2. stupně}} = c \cdot (x^2+1) + 1$$

$\Rightarrow$ hledáme $c \in \mathbb{R}$ (nemusíme $c \in \mathbb{R}[x]$)

(neboť jedničkou v okruhu je $\overline{1} = \overline{1 + c(x^2+1)}$)

$$ax^2 + (a_0a+b)x + a_0b = cx^2 + c+1$$

To nastane $\Leftrightarrow$

$$\left. \begin{array}{l} a=c \\ a_0a+b=0 \\ a_0b=c+1 \end{array} \right\} \Rightarrow \left. \begin{array}{l} a_0a+b=0 \\ a_0b=a+1 \end{array} \right\} \Rightarrow \left. \begin{array}{l} b=-a_0a \\ a_0b=a+1 \end{array} \right\} \Rightarrow a_0(-a_0a) = a+1 \Rightarrow$$

$$\Rightarrow -a_0^2a - a = 1 \Rightarrow a(-a_0^2-1) = 1 \Rightarrow a = \frac{-1}{a_0^2+1} \Rightarrow b = \frac{-a_0}{a_0^2+1} \Rightarrow$$

$$\Rightarrow \overline{X + a_0}^{-1} = \overline{\frac{-1}{a_0^2+1} X + \frac{-a_0}{a_0^2+1}}$$

Musíme ověřit, zda tomu tak skutečně je:

$$\begin{aligned} \overline{(X + a_0) \cdot \left(\frac{-1}{a_0^2+1} X + \frac{-a_0}{a_0^2+1} \right)} &= \overline{\frac{1}{a_0^2+1} (X + a_0)(-X + a_0)} = \overline{\frac{1}{a_0^2+1} (-X^2 + a_0^2)} = \\ &= \overline{\frac{1}{a_0^2+1} (-X^2 + a_0^2) + \frac{1}{a_0^2+1} (X^2 + 1)} = \\ &= \overline{\frac{1}{a_0^2+1} (a_0^2 + 1)} = \overline{1} \end{aligned}$$

Nyní nalezneme prvek inverzní k libovolnému $\overline{a_1 X + a_0} \in \mathbb{R}[X]/\langle X^2+1 \rangle - \{\overline{0}\}$

$$\overline{a_1 X + a_0}^{-1} = \overline{a_1} \cdot \overline{\left(X + \frac{a_0}{a_1} \right)}^{-1} = \overline{\frac{1}{a_1}} \cdot \overline{\left(\frac{-1}{\left(\frac{a_0}{a_1}\right)^2+1} X + \frac{-\frac{a_0}{a_1}}{\left(\frac{a_0}{a_1}\right)^2+1} \right)} = \underline{\underline{\frac{-1}{a_1 \left(\left(\frac{a_0}{a_1}\right)^2+1 \right)} X + \frac{-a_0}{a_1^2 \left(\left(\frac{a_0}{a_1}\right)^2+1 \right)}}}$$

$\Rightarrow (\mathbb{R}[X]/\langle X^2+1 \rangle, +, \cdot)$ je těleso (nekonečné)

Pr. : Dokažte :

Věta 1: Necht' $(R, +, \cdot)$ je obor integrity, $a \in R$, $a \neq 0$.

Polom $\forall n \in \mathbb{N} : a^n \neq 0$

Důkaz 22: Důkaz provedeme indukcí podle n .

1.) $\boxed{n=1}$ $\Rightarrow$ Inverzní věty je splněno, neboť $a^1 = a \neq 0$.

2.) Indukční krok $\Rightarrow$ Předpokládejme, že $a^{n-1} \neq 0$. Dokažeme, že potom také $a^n \neq 0$:

(R_{t1}) je obor integrity $\Rightarrow$

$$a^m = a \cdot a^{m-1} = 0 \Leftrightarrow (a=0, \text{ oder } a^{m-1}=0)$$

ale $a \neq 0$ a také - podle indukčního předpokladu - $a^{m-1} \neq 0 \Rightarrow$

$$a^M = a \cdot a^{M-1} \neq 0$$

Pr: Dokáže:

Věta 2: Necht $(R, +, \cdot)$ je těleso. Potom

$$\forall a \in R - \{0\} : a^{-1} \neq 0$$

Důkaz: $a \in R - \{0\} \Rightarrow$ existuje $((R, +, \cdot)$ je těleso!) $a^{-1} \in R$

Sporem dokážeme, že $\tilde{a}^1 \neq 0$. Předpokládejme proto, že $\tilde{a}^1 = 0$. Pakom:

$$\left. \begin{array}{l} a \cdot \vec{a}^1 = 1 \\ a \cdot \vec{0} = 0 \end{array} \right\} \Rightarrow 1=0 \text{ smor! s nebrivialitou telesa}$$

Důsledek: Podmínku 4.) $\forall a \in R - \{0\} \exists \bar{a}^{-1} \in R : a \cdot \bar{a}^{-1} = \bar{a}^{-1} \cdot a = 1$

z definice tělesa bychom mohli psát ve tvaru:

$$4.) \forall a \in R - \{0\} \exists \bar{a}^{-1} \in R - \{0\} : a \cdot \bar{a}^{-1} = \bar{a}^{-1} \cdot a = 1$$

a jinak by to nerměnilo význam pojmu těleso.

Př.: Dokažte:

Věta 3.: Necht' $(R, +, \cdot)$ je těleso, $a \in R - \{0\}$, $a \neq 0$. Pakom

$$\forall r \in \mathbb{Z} : a^r \neq 0$$

Důkaz:

$$\begin{array}{l} r > 0 \Rightarrow r = m \in \mathbb{N} \Rightarrow \text{z Věty 1. plyne } a^r = a^m \neq 0 \\ \quad \quad \quad \uparrow \\ \quad \quad \quad \text{(tato je splněna, neboť těleso je obor integrity)} \\ r = 0 \Rightarrow a^0 = 1 \neq 0 \text{ (z definice tělesa)} \\ r < 0 \Rightarrow r = -m, \text{ kde } m \in \mathbb{N} \Rightarrow \end{array}$$

$$a^r = \bar{a}^m = (\bar{a}^{-1})^m$$

Věta 2 říká, že $\bar{a}^{-1} \neq 0$ a podle Věty 1. pak $(\bar{a}^{-1})^m \neq 0 \Rightarrow$

$$a^r \neq 0$$

□

Pr: dokažte, že v tělese neexistují vlastní ideály, tzn.
 jestliže I je ideál ve $F \Rightarrow I = \{0\}$, nebo $I = F$

Ideál $(I, +, \cdot)$ je podokruhem okruhu $(F, +, \cdot)$, proto $(I, +)$ je podgrupou grupy $(F, +)$. Proto nula jistě patří do I . Jestliže I obsahuje i nějaký nenulový prvek i , pak k němu existuje inverze (F je těleso). Z definice ideálu pak plyne:

$$\forall x \in F : x \cdot i = i_0 \in I \quad | \cdot i^{-1}$$

$$\lambda = \underbrace{i_0 \cdot i^{-1}}_I \in I$$

To jest, ideál buď obsahuje jen nulu, nebo všechny prvky z F .