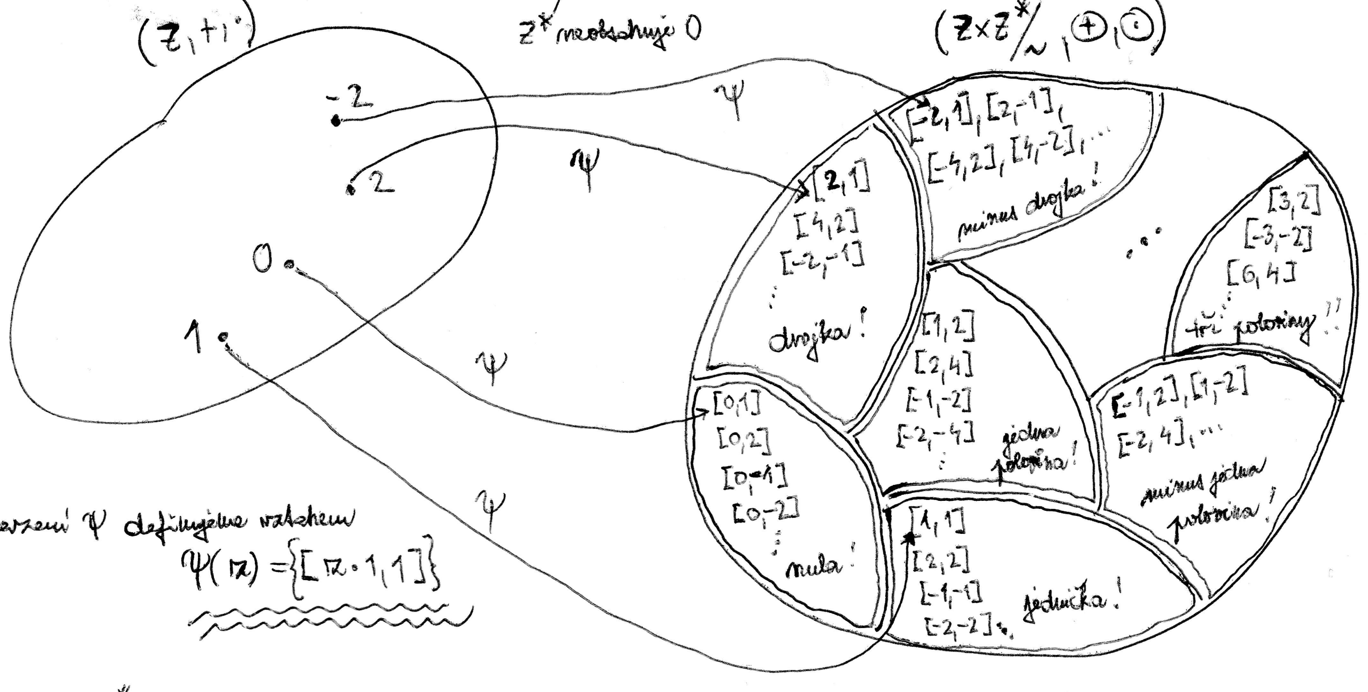
Věta 4: S využitím věty 2 lze komutativní obor integrity $(\mathbb{Z},+,\cdot)$ injektivně vnořit do tělesa (= rozšířit na těleso) $Q := (\mathbb{Z}\times\mathbb{Z}^*/_{\sim}, \oplus, \odot)$

$\mathbb{Z}^*$ neobsahuje 0



zobrazení ψ definujeme vztahem
$$\psi(n) = \{[n\cdot 1, 1]\}$$

a) Na $\mathbb{Z}\times\mathbb{Z}^*$ definujeme relaci ekvivalence $\sim$ takto: $[a,b]\sim[c,d]$, když $a\cdot d = b\cdot c$

staré operace v $(\mathbb{Z},+,\cdot)$

b) vytvoříme faktormnožinu $\mathbb{Z}\times\mathbb{Z}^*/_{\sim}$, jejíž prvky jsou podmnožiny určené danou ekvivalencí

c) na faktormnožině $\mathbb{Z}\times\mathbb{Z}^*/_{\sim}$ definujeme operace $\oplus, \odot$ takto:

$$\{[a,b]\}\oplus\{[c,d]\} := \{[ad+bc,\ b\cdot d]\}$$ (b·d nikdy není rovno 0, protože $b\neq 0$, $d\neq 0$)

staré operace na $(\mathbb{Z},+,\cdot)$

(definici si zapamatujete tak, že operace se chová stejně jako sčítání zlomků převedením na společného jmenovatele: $\frac{a}{b}+\frac{c}{d} = \frac{ad+bc}{b\cdot d}$)

$$\{[a,b]\}\odot\{[c,d]\} := \{[a\cdot c,\ b\cdot d]\}$$ ... chová se podobně jako násobení zlomků $\frac{a}{b}\cdot\frac{c}{d} = \frac{a\cdot c}{b\cdot d}$

staré operace v $(\mathbb{Z},+,\cdot)$

(pro $\{[a,b]\}$ je inverzní vzhledem k $\oplus$ prvek $\{[-a,b]\}$
pro $\{[a,b]\}$ je inverzní vzhledem ke $\odot$ prvek $\{[b,a]\}$)

Pak $(\mathbb{Z}\times\mathbb{Z}^*/_{\sim}, \oplus)$ je komutativní grupa
$(\mathbb{Z}\times\mathbb{Z}^*/_{\sim}, \odot)$ je komutativní grupa
} operace $\oplus, \odot$ splňují distributivní zákon, tj. celkem $(\mathbb{Z}\times\mathbb{Z}^*/_{\sim}, \oplus, \odot)$ je těleso!

d) Zobrazení $\psi: \mathbb{Z}\to\mathbb{Z}\times\mathbb{Z}^*/_{\sim}$ je injektivní homomorfismus, tj. původní výsledky sčítání a násobení celých čísel zůstanou v nové struktuře zachovány.

Tímto způsobem jsme algebraicky přesně jen pomocí celých čísel vytvořili racionální čísla, a dokonce velmi názorně platí, že různé „zlomky" $[3,2], [-3,-2], [6,4]$, atd. jsou jen různými reprezentanty téhož racionálního čísla!!!

Jak už bylo řečeno v předchozí 9, konstrukce $Q \to R$, $R \to C$ už jsou jiného charakteru, protože nevytváří strukturu nového typu (R a C jsou už stále tělesa), pouze obohatí množinu Q o nějaké další prvky.

Konstrukce $Q \to R$

Množina Q se skládá ze racionálních čísel, každé racionální číslo lze vyjádřit nekonečně mnoha zlomky (viz obrázek na předchozí straně), každé racionální číslo lze převést na číslo s desetinným rozvojem ukončeným nebo neukončeným periodickým (viz věta 11 ze základů matematiky). Přidáním iracionálních čísel ze množiny I, jejichž desetinný rozvoj je neperiodický neukončený, dostaneme množinu R reálných čísel.

Abyste měli představu, kolik těch iracionálních čísel vlastně je a jak jsou na reálné ose jejich obrazy rozmístěny, podíváme se na dvě zdánlivě protichůdné věty, a pak na dva způsoby konstrukce $Q \to R$.

Věta 5. Množina Q je stejně mohutná jako množina N.
(možná bych mohl nepřesně říci, že všech zlomků je stejný počet jako přirozených čísel, ale u nekonečných množin neříkáme POČET PRVKŮ, ale MOHUTNOST)

Důkaz: Prvky množiny N lze seřadit do posloupnosti $(1, 2, 3, 4, 5, \dots)$.
Snad mi věříte, že pokud všechny zlomky seřadíme do jedné posloupnosti, bude jich „stejně" jako čísel přirozených. Pojďme tedy na to:

- vezměme všechny zlomky s číslem 1 v čitateli: $\frac{1}{1}, \frac{-1}{1}, \frac{1}{2}, \frac{-1}{2}, \frac{1}{3}, \frac{-1}{3}, \frac{1}{4}, \frac{-1}{4}, \dots$
- vezměme zlomky s číslem 2 v čitateli, ale vynecháme ty, které po zkrácení dávají nějaký zlomek s čitatelem ± 1: $\frac{2}{1}, \frac{-2}{1}, \frac{2}{3}, \frac{-2}{3}, \frac{2}{5}, \frac{-2}{5}, \frac{2}{7}, \frac{-2}{7}, \dots$ ve jmenovateli jsou tedy jen lichá čísla... takových zlomků s čitatelem 2 je stále nekonečně mnoho
- vezměme zlomky s číslem 3 v čitateli, které nelze zkrátit na nějaký zlomek v předchozích dvou posloupnostech: $\frac{3}{1}, \frac{-3}{1}, \frac{3}{2}, \frac{-3}{2}, \frac{3}{4}, \frac{-3}{4}, \frac{3}{5}, \frac{-3}{5}, \dots$
- vezměme všechny další zlomky s číslem 4 v čitateli: $\frac{4}{1}, \frac{-4}{1}, \frac{4}{3}, \frac{-4}{3}, \frac{4}{5}, \frac{-4}{5}, \frac{4}{7}, \frac{-4}{7}, \dots$

⋮

- atd... takové posloupnosti s různými čitateli lze vytvořit do nekonečna.

Všechna různá racionální čísla lze tedy vyjádřit jako nekonečně mnoho posloupností.
Možná byste intuitivně řekli, že nekonečně mnoho posloupností nelze seřadit do jedné posloupnosti. Ale v této věci intuice selhává, je to možné – na následující straně je vyznačen šipkami způsob, jak nekonečně mnoho posloupností lze přeuspořádat a seřadit do jediné

– jako a_1 vezmeme $\frac{1}{1}$

– jako a_2, a_3 vezmeme 1. zlomek ve 2. řadě, 2. zlomek v 1. řadě: $a_2 = \frac{2}{1}$, $a_3 = \frac{-1}{1}$

– jako a_4, a_5, a_6 vezmeme 1. zlomek ve 3. řadě, 2. zlomek ve 2. řadě, 3. zlomek v 1. řadě:
$a_4 = \frac{3}{1}$, $a_5 = \frac{-2}{1}$, $a_6 = \frac{1}{2}$ (I am sorry, používám ZŠ definici posloupnosti jako „řady čísel")

– jako a_7, a_8, a_9, a_{10} vezmeme 1. zlomek ve 4. řadě, 2. zlomek ve 3. řadě, 3. zlomek ve 2. řadě a 4. zlomek v 1. řadě: $a_7 = \frac{4}{1}$, $a_8 = \frac{-3}{1}$, $a_9 = \frac{2}{3}$, $a_{10} = \frac{-1}{2}$

– A TAK DÁLE – tímto postupem se na každý zlomek v daném schématu dostane !!!

$$\begin{array}{ccccccccc}
\frac{1}{1}, & -\frac{1}{1}, & \frac{1}{2}, & -\frac{1}{2}, & \frac{1}{3}, & -\frac{1}{3}, & \frac{1}{4}, & -\frac{1}{4}, & \dots \\
\frac{2}{1}, & -\frac{2}{1}, & \frac{2}{3}, & -\frac{2}{3}, & \frac{2}{5}, & -\frac{2}{5}, & \frac{2}{7}, & -\frac{2}{7}, & \dots \\
\frac{3}{1}, & -\frac{3}{1}, & \frac{3}{2}, & -\frac{3}{2}, & \frac{3}{4}, & -\frac{3}{4}, & \frac{3}{5}, & -\frac{3}{5}, & \dots \\
\frac{4}{1}, & -\frac{4}{1}, & \frac{4}{3}, & -\frac{4}{3}, & \frac{4}{5}, & -\frac{4}{5}, & \frac{4}{7}, & -\frac{4}{7}, & \dots \\
\vdots & & & & & & & &
\end{array}$$

jedna seřazená posloupnost: $\frac{1}{1}, \frac{2}{1}, -\frac{1}{1}, \frac{3}{1}, -\frac{2}{1}, \frac{1}{2}, \frac{4}{1}, -\frac{3}{1}, \frac{2}{3}, -\frac{1}{2}, \dots$

tímto způsobem seřadíme všechna racionální čísla do jedné posloupnosti, důkaz věty 5 je hotov.

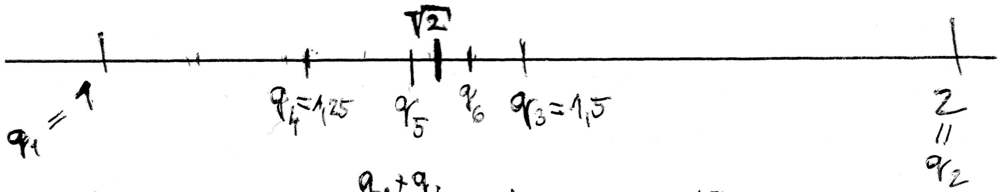
Racionálních čísel tedy z jistého úhlu pohledu „není mnoho" — kdybychom obrazy těchto zlomků trochu „rozhrnuli" od sebe, aby nebyly tak „nahusto" (toto „rozhrnování" by nám mimochodem trvalo nekonečně dlouho), bylo by jich přesně tolik, kolik je čísel přirozených.

<u>Věta 6.</u> Množina $\mathbb{Q}$ je v $\mathbb{R}$ hustá, tj. $\forall r \in \mathbb{R}\ \exists$ posloupnost q_n racionálních čísel, jejíž limita je r ($\lim_{n\to\infty} q_n = r$)

! [(možná vám někdo už říkal, že tento fakt platí pro číslo π... existuje posloupnost zlomků, jejíž limita $= \pi$.)
Tato skutečnost neplatí jen pro π, ale pro jakékoli reálné číslo

<u>Důkaz:</u> Pokud $r \in \mathbb{Q}$, nalézt tuto posloupnost je velmi jednoduché: volíme $q_1 = r, q_2 = r, q_3 = r, \dots$ (Např. pro $r = \frac{3}{5}$ je hledaná posloupnost $(\frac{3}{5}, \frac{3}{5}, \frac{3}{5}, \dots)$). Zajímavější je nalezení posloupnosti pro r iracionální — asi bez újmy na obecnosti (BUNO) zvolme nějaké iracionální r a důkaz provedeme pro ně.

Pro $r = \sqrt{2}$ ... nalezněme posloupnost zlomků $q_1, q_2, q_3, \dots$ s limitou $\sqrt{2}$:
volme $q_1 = 1$, $q_2 = 2$ (tak, aby $q_1 < \sqrt{2}$, $q_2 > \sqrt{2}$).



a) najdeme střed intervalu $q_3 = \frac{q_1 + q_2}{2}$ ... to je racionální číslo, je to součet dvou zlomků dělený dvěma

b) q_3 rozdělí interval $\langle q_1, q_2 \rangle$ na dva intervaly poloviční délky — vezmeme z nich ten, který obsahuje $\sqrt{2}$

$q_4 = \frac{q_1 + q_3}{2}$ c) q_4 rozdělí $\langle q_1, q_3 \rangle$ na dva intervaly poloviční délky — vezmeme z nich $\langle q_4, q_3 \rangle$, protože obsahuje $\sqrt{2}$

$q_5 = \frac{q_4 + q_3}{2}$ d) q_5 rozdělí $\langle q_4, q_3 \rangle$ na dva intervaly poloviční délky — vezmeme z nich $\langle q_5, q_3 \rangle$, protože obsahuje $\sqrt{2}$
$q_5 = 1{,}375$

$q_6 = \frac{q_5 + q_3}{2}$ e) $q_6 = 1{,}4375$ rozdělí $\langle q_5, q_3 \rangle$ na intervaly poloviční délky — vezmeme dále $\langle q_5, q_6 \rangle$, atd.

⋮ tato posloupnost středů intervalů se stále víc blíží k číslu $\sqrt{2}$, důkaz je hotov.

(metoda je stejná jako metoda půlení intervalu ze přednášky 8)

Poznámka: V důkazu věty 6 jsme sestrojili posloupnost čísel $q_n \in Q$, která konverguje, jenže její limita v množině Q neleží!!

Odtud plyne elegantní a asi nejjednodušší popis konstrukce $Q \to R$.

Věta 7 (konstrukce $Q \to R$ jednodušší). Doplníme-li množinu Q o limity všech možných posloupností prvků z Q, které v samotné množině Q neleží, dostaneme množinu R.

(Důkaz: viz věta 6 ... iracionální čísla jsou právě ta čísla, která jsou limitami posloupností zlomků z množiny Q, a přitom nejsou prvky množiny Q)

Věta 8 (konstrukce $Q \to R$ trochu méně názorně)

$\boxed{\text{R je množina řezů (A,B) množiny Q, které jsou 1. druhu nebo 3. druhu}}$

ty odpovídají rac. číslům

ty odpovídají irac. číslům

Důkaz či objasnění:

Nejprve musíme definovat pojem řezu (A,B) lineárně uspořádané množiny M

(tedy M je poset = částečně uspořádaná množina, ve které jsou každé dva prvky srovnatelné = tzv. řetězec).

Řez (A,B) řetězce M je rozklad množiny M na podmnožiny A,B ($A \cap B = \emptyset$, $A \cup B = M$, $A \neq \emptyset$, $B \neq \emptyset$)

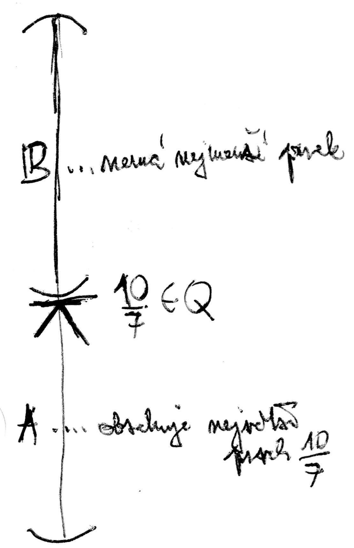
takový, že $\forall a \in A, \forall b \in B: a < b$.

Vzhledem k pojmům nejmenší prvek/největší prvek existují čtyři druhy řezů (vysvětleno na Hasseových diagramech množiny M):

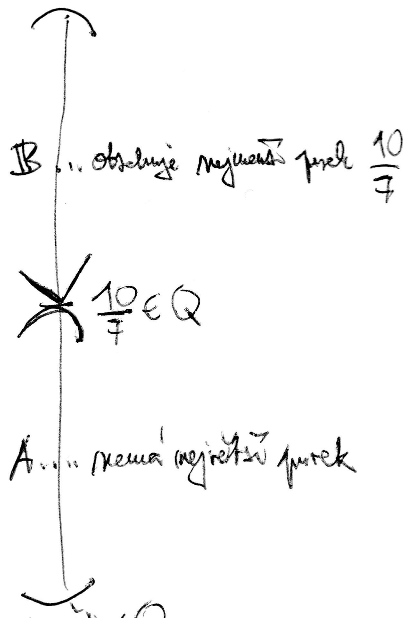
řez 1. druhu:
A obsahuje svůj největší prvek,
B nemá nejmenší prvek

řez 2. druhu:
A nemá největší prvek,
B obsahuje svůj nejmenší prvek

např. $M = Q$:



např. $M = Q$



Racionálních čísel je právě tolik, kolik existuje řezů 1. druhu množiny Q,

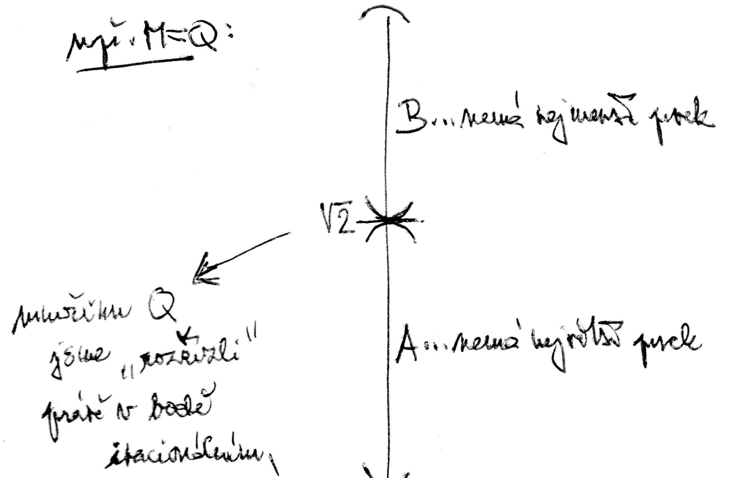
tj. existuje bijekce $Q \to$ řezy Q 1. druhu.

Podobně jsme mohli zlomek $\frac{10}{7}$ umístit namísto do množiny A do množiny B, a tím způsobem vznikne řez 2. druhu. Racionálních čísel je tedy přesně tolik, kolik existuje řezů 2. druhu množiny Q, tj. existuje bijekce $Q \to$ řezy Q 2. druhu.

Podle toho, kam ten „hraniční" zlomek $\frac{10}{7}$ umístíme, vznikne řez 1. druhu nebo řez 2. druhu – můžeme si tedy vybrat, jak budeme racionální čísla (reprezentované zlomky) chápat, zda jako řezy 1. druhu nebo řezy 2. druhu množiny Q.

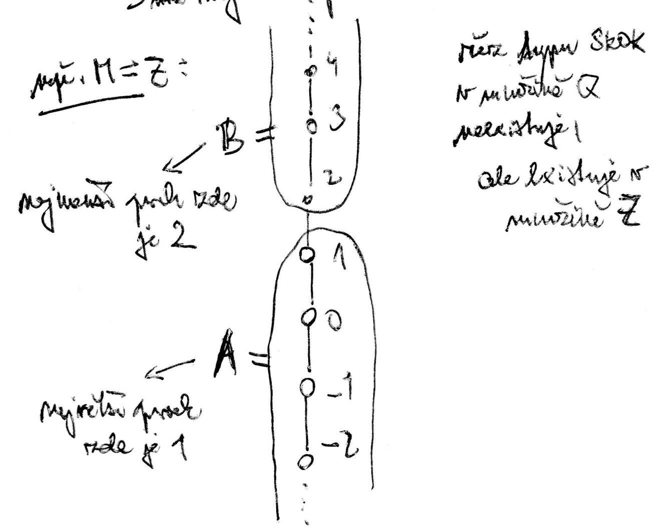
Do tvrzení věty 8 jsme si vybrali rac. čísla reprezentovaná jako řezy množiny Q 1. druhu.

řez 3. druhu neboli MEZERA:
A nemá největší prvek,
B nemá nejmenší prvek



tj. A i B jsou otevřené intervaly

řez 4. druhu neboli SKOK:
A má největší prvek
B má nejmenší prvek



Iracionálních čísel je přesně tolik, kolik existuje MEZER (= řezů 3. druhu) v Q, tj. existuje bijekce $I \to$ mezery v Q. Například mezera na obrázku odpovídá iracionálnímu číslu $\sqrt{2}$

Čili doplníme-li racionální čísla (= řezy 1. druhu) iracionálními čísly (= mezerami v Q = řezy Q 3. druhu), dostaneme $\mathbb{R}$.

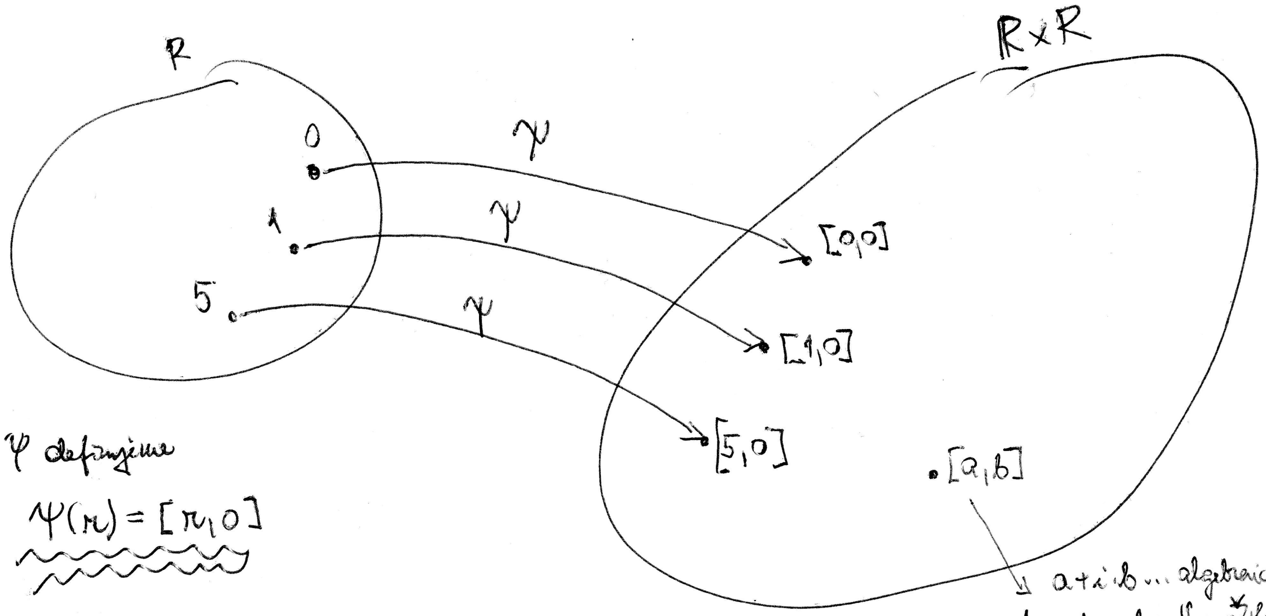
V obrázku mezery $\sqrt{2}$ v Q neexistuje největší prvek množiny A, ani neexistuje nejmenší prvek množiny B – ovšem $\sqrt{2}$ je supremum množiny A, a současně $\sqrt{2}$ je infimum množiny B. Čili místo terminologie řezů lze konstrukci věty 8 formulovat i jinak: pomocí pojmu infimum nebo supremum (můžeme si vybrat, který se nám líbí; protože $\sqrt{2}$ je současně $\inf B$ i $\sup A$, tak nám stačí použít jen jeden pojem – např. infimum ;) :

Doplníme-li množinu Q o infima otevřených intervalů v Q, která neleží v Q, dostaneme $\mathbb{R}$. Konec důkazu či objasnění

Poznámka: Věty 7, 8 popisují tedy tutéž konstrukci $Q \to R$, pouze pomocí jiných pojmů: věta 7 pomocí pojmu limita posloupnosti, věta 8 pomocí pojmu řez/infimum řetězce. Konstrukce pomocí pojmu řez je součástí bakalářské zkoušky ve 3. ročníku.

Věta 9 (konstrukce $R \to C$). Těleso $(R,+,\cdot)$ lze vnořit do tělesa $C := R \times R$, ve kterém má rovnice $x^2+1=0$ řešení.

Důkaz:



Zobrazení ψ definujeme vztahem $\psi(r) = [r,0]$

$a+ib$ ... algebraický tvar komplexního čísla $[a,b]$

1) na $R \times R$ definujeme operace $+$, $\cdot$ takto:

$$[a,b]+[c,d] := [a+c, b+d] \quad \ldots\ldots \quad a+ib+c+id = a+c+i(b+d)$$

$$[a,b]\cdot[c,d] := [ac-bd, ad+bc] \quad \ldots\ldots \quad (a+ib)\cdot(c+id) =$$

$$= ac + \underset{-1}{\underbrace{i^2}}bd + ibc + ida =$$

$$= ac - bd + i(da+bc)$$

Pak struktura $(R \times R, +, \cdot)$ je těleso

(opačný prvek k $[a,b]$ je $[-a,-b]$)

(inverzní prvek k $[a,b]$ (mimo $[0,0]$, ke kterému inverzi NEHLEDÁME)

je $\left[\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right]$:

$$(a+ib)\cdot\frac{1}{(a+ib)} = 1 \quad \ldots \text{ vlastnost inverzního prvku}$$

tohleto je inverzní prvek, upravme jej do tvaru něco $+ i\cdot$(obecně něco jiného):

$$\frac{1}{a+ib} = \frac{1}{a+ib}\cdot\frac{a-ib}{a-ib} = \frac{a-ib}{a^2-i^2b^2} \underset{i^2=-1}{=} \frac{a-ib}{a^2+b^2} = \frac{a}{a^2+b^2} + i\cdot\frac{(-b)}{a^2+b^2}$$

a to je algebraický tvar prvku $\left[\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right]$

2) Platí $[0,1]\cdot[0,1] = [-1,0]$

algebraicky $i^2=-1$, tj. $[0,1]$, algebraicky i, je řešením rovnice $x^2+1=0$.

3) Zobrazení $\psi: R \to R\times R$ je injektivní homomorfismus $R \to R \times R$ vzhledem k definovaným operacím, tj. původní výsledky sčítání a násobení reálných čísel jsou v nové struktuře zachovány