$\{[\mathbb{R}]\} = \mathbf{Mod}^{\mathcal{S}}(\mathbf{OF} + \mathbf{AoC})/_{\cong}$

Ref. Um Curso de Cálculo - Guidorizzi

Autor: Xenônio
Discord: xennonio

Sumário

1 Motivação

1.1 Axiomas de Corpo Ordenado (OF)

Para que possamos formalizar os reais, utilizaremos noções e fatos que são usuais na ZFC, em particular, assumindo ela como nossa metateoria, ou trabalhando dentro da ZFC, provaremos que é possível criar um modelo M para os Reais.

Antes de tudo precisamos, portanto, definir o que são os reais. Há uma ideia intuitiva do que de fato é $\mathbb{R}$ como uma reta, mas para formalização completa listamos alguns axiomas que são propriedades básicas que $\mathbb{R}$ satisfaz, conhecidas como axiomas de corpos ordenados (OF).

Seja $\mathcal{S} = \{+, \cdot, \leq, 0, 1\}$ nossa linguagem, então as fórmulas de primeira ordem que constituem OF:

(O1): $\forall x,\ x \leq x$
(O2): $\forall x, y$, se $x \leq y$ e $y \leq x$, então $x = y$
(O3): $\forall x, y, z$, se $x \leq y$ e $y \leq z$, então $x \leq z$
(O4): $\forall x, y,\ x \leq y$ ou $y \leq x$

(O5): $\forall x, y, z$, se $x \leq y$, então $x + z \leq y + z$
(O6): $\forall x, y, z$, se $x \leq y$ e $z \geq 0$, então $x \cdot z \leq y \cdot z$

(A1): $\forall x, y, z\ x + (y + z) = (x + y) + z$
(A2): $\forall x, y\ x + y = y + x$
(A3): $\forall x\ x + 0 = 0 + x = x$
(A4): $\forall x \exists y$ tq $x + y = y + x = 0$

(M1): $\forall x, y, z\ x \cdot (y \cdot z) = (x \cdot y) \cdot z$
(M2): $\forall x, y\ x \cdot y = y \cdot x$
(M3): $\forall x\ x \cdot 1 = 1 \cdot x = x$
(M4): $\forall x \neq 0 \exists y$ tq $x \cdot y = y \cdot x = 1$

(D): $\forall x, y, z\ x \cdot (y + z) = (x \cdot y) + (x \cdot z)$

onde $O = \{$O1, O2, O3, O4$\}$ formam os axiomas de uma ordenação linear, i.e., reflexividade, antisimetria, transitividade e total, respectivamente. Analogamente $A = \{$A1, A2, A3, A4$\}$ e $M = \{$M1, M2, M3, M4$\}$ formam os axiomas de adição e multiplicação, sendo eles associatividade, comutatividade, elemento neutro e existência de inverso. E por último $\{$O5, O6, D$\}$ relacionam ambas as operações com a relação de ordem, e as operações entre si por meio da distributividade.

De fato, temos que, intuitivamente, $(\mathbb{R}, +, \cdot, \leq, 0, 1) \vDash$ OF, entretanto este não é o único modelo para OF, uma vez que, digamos, $(\mathbb{Q}, +, \cdot, \leq, 0, 1) \vDash$ OF também. Em particular, sabemos por Löwenhein-Skolem que nenhuma estrutura infinita pode ser caracterizada até o isomorfismo, então em particular precisamos de algum axioma adicional φ de segunda ordem.

1.2 Definição de $\mathfrak{R}$

Com isso podemos, após construir $\mathfrak{R}$, provar que se $\mathfrak{R}, \mathfrak{A} \vDash \text{OF} + \varphi$, com $\mathfrak{R} = (\mathbb{R}, +, \cdot, \leq, 0, 1)$ e $\mathfrak{A} = (K, \oplus, \odot, \preceq, 0', 1')$, então $\mathfrak{R} \cong \mathfrak{A}$, i.e., existe um isomorfismo $f : \mathbb{R} \to K$ preservando funções, constantes e relações, ou seja, $f(x + y) = f(x) \oplus f(y)$, $f(x \cdot y) = f(x) \odot f(y)$, $f(0) = 0'$, $f(1) = 1'$ e $x \leq y$ sse $f(x) \preceq f(y)$, de fato é possível provar que tal isomorfismo é único.

Feito isso, provamos que um desenvolvimento do cálculo ou de alguma teoria baseada somente nos axiomas OF $+ \varphi$ é justificada e bem definida, uma vez que, assumindo a ZFC como metateoria, provamos que a teoria é de fato consistente, visto que possui um modelo, e este modelo é único até o isomorfismo, logo esetamos trabalhando em uma única estrutura.

Cabe a nós, agora, não só construir um modelo $\mathfrak{R}$, como determinar qual axioma φ podemos utilizar.

Há duas escolhas comuns a tal axioma, em particular o Axioma da Completude (AoC), ou a conjunção do Axioma Dos Intervalos Encaixantes (NIP) com a Propriedade Arquimediana (AP). O primeiro é o seguinte axioma de segunda ordem, que diz:

Para todo $S \subseteq \mathbb{R}$ com $S \neq \emptyset$, se existe M tal que $M \geq x$, $\forall x \in S$, i.e., M é um limitante superior de S, então existe s tal que s é um limitante superior de S e, para todo s' limitante superior de S, temos $s \leq s'$.

Em outras palavras, todo subconjunto S de $\mathbb{R}$ não-vazio e limitado superiormente admite supremo.

Os outros dois, NIP e AP, são também axiomas de segunda ordem, em particular o primeiro diz que:

Se $I_n = [a_n, b_n]$ é uma sequência de intervalos tais que $I_{n+1} \subseteq I_n$ e $|I_n| \to 0$, então existe exatamente um real x tal que $x \in \bigcap_{n \geq 0} I_n$.

Entretanto, tal teorema não é suficiente para caracterizar $\mathbb{R}$ até o isomorfismo, precisamos também da propriedade arquimediana:

Para todo $\varepsilon > 0$, existe $n \in \mathbb{N}$ tal que $\frac{1}{n} < \varepsilon$.

Obs: Podemos também, na presença de AP, tomar outro axioma ao invés de NIP, como por exemplo o Critério de Cauchy (CC), que diz que toda sequência de cauchy é convergente.

Analogamente, se substituirmos AoC pelo Teorema de Bolzano-Weierstrass (BW) ou o Teorema da Convergência Monótona (MCT) teremos uma formalização equivalente dos corpos ordenados completos.

Em particular, até o fim do material, tomaremos $\varphi =$AoC.

1.3 Motivação de Cortes

Richard Dedekind teve a ideia de formalizar os reais por meio de cortes após ser motivado pelo seguinte teorema:

Teorema 1.1. Seja $f : (a, b) \to \mathbb{R}$ crescente

a) Se f for limitada superiormente em (a, b), então

$$\lim_{x \to b^-} f(x) = \sup \underbrace{\{f(x) : x \in (a, b)\}}_{L}$$

b) Se f não for limitada superiormente em (a, b), então

$$\lim_{x \to b^-} f(x) = \infty$$

Prova. a) Como L é não-vazio e limitado superiomente ele admite um supremo s. Assim, para todo $\varepsilon > 0$, temos que existe $y \in \mathrm{Im}(f)$ tal que $s - \varepsilon < y \leq s$, visto que, caso contrário, $s - \varepsilon \geq y$ para todo $y \in \mathrm{Im}(f)$, contradizendo que s é o menor limitante superior. Como $y \in \mathrm{Im}(f)$, existe $x_1 \in (a, b)$ tal que $s - \varepsilon < f(x_1) \leq s$ e, como f é crescente, para todo $x \in (x_1, b)$

$$s - \varepsilon < f(x_1) \leq f(x) \leq s < s + \varepsilon$$

ou seja, $|f(x) - s| < \varepsilon$.

b) Como f é ilimitada, para todo $M > 0$ existe $x_1 \in (a, b)$ tal que $f(x_1) > M$. Como f é crescente, então pra todo $x \in (x_1, b)$, $f(x) > M$, logo f explode. $\dashv$

Tendo motivado, passaremos agora para a definição de $\mathfrak{R}$ e provaremos que tal construção satisfaz todos os axiomas de OF e AoC.

2 Construção de $\mathfrak{R}$

2.1 Cortes de Dedekind à Esquerda

Assumindo a ZFC ou algum fragmento mais fraco suficiente para fazer teoria dos conjunto básicas, assuma que já construímos $(\mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}}, <, 0_{\mathbb{Q}}, 1_{\mathbb{Q}})$.

Definição 2.1. Definimos um corte de Dedekind à esquerda, ou simplismente um corte como $r \subseteq \mathbb{Q}$ tal que:

(R1) r é um subconjunto, não-vazio, próprio de $\mathbb{Q}$, i.e. $\emptyset \neq r \neq \mathbb{Q}$;

(R2) r é "fechado à esquerda", i.e., se $q \in r$ e $p < q$, então $p \in r$;

(R3) r não admite máximo, i.e., para todo $p \in r$, existe $q \in r$ tal que $p < q$.

Um número real é definido como um corte de Dedekind à esquerda e o conjunto $\mathbb{R}$ de todos os cortes é denominado conjunto dos números reais. Obviamente $\mathbb{R}$ existe, visto que a fórmula φ que define um corte através de todas as propriedades (R1), (R2) e (R3) é uma fórmula de primeira ordem e

$$\mathbb{R} := \{x \in \mathcal{P}(\mathbb{Q}) : \varphi(x)\}$$

está bem definido pelo axioma da potência e da especificação.

2.2 Exemplos

Como exemplo, seja $\alpha = \{p \in \mathbb{Q} : p < 2\}$, mostraremos que $\alpha \in \mathbb{R}$

Teorema 2.1. α satisfaz (R1), (R2) e (R3).

Prova. (R1): como $0 < 2$, por definição $0 \in \alpha$, logo $\alpha \neq \emptyset$, ademais 2 não é menor que 2, portanto $2 \notin \alpha$, portanto $\alpha \neq \mathbb{Q}$.

(R2): Se $p < 2$ e $q < p$, pela transitividade de $<$ temos que $q < 2$, i.e., $q \in \alpha$.

(R3) Dado $p \in \alpha$, por definição $p < 2$, provaremos que existe $q \in \alpha$ tal que $p < q$. Seja $q = p + \frac{2-p}{2} = \frac{p+2}{2}$, como $p \in \mathbb{Q}$, então $q \in \mathbb{Q}$. Ademais $q = \frac{p}{2} + 1 < 1 + 1 = 2$, visto que $p < 2$, portanto $q \in \alpha$ e, como $p < 2$, então $0 < 2 - p$, logo $q = p + \frac{2-p}{2} > 2$. $\dashv$

Teorema 2.2. Mostraremos que, dado $r \in \mathbb{Q}$, podemos identificar $r^* := \{p \in \mathbb{Q} : p < r\}$ como r em $\mathbb{R}$, i.e., provaremos que r^* é um real.

Prova. De fato, isso é o primeiro passo para provar que existe uma imersão $\iota : \mathbb{Q} \to \mathbb{R}$ de $\mathbb{Q}$ em $\mathbb{R}$, onde todas as operações definidas em $\mathbb{Q}$ podem ser transportadas para $\mathbb{Q}^* := \iota(\mathbb{Q})$.

(R1) Como $r - 1 \in r^*$, então r^* é não-vazio. Ademais, $r \notin r^*$, portanto $r^* \neq \mathbb{Q}$.

(R2) dados $p, q \in r^*$ com $p \in r^*$ e $q < p$, por definição $p < r$ e, se $q < p$, por transitividade $q < r$, portanto $q \in r^*$.

(R3) Dado $p \in r^*$, defina $q = p + \frac{r-p}{2} = \frac{p+r}{2}$, como $p, r \in \mathbb{Q}$, então $q \in \mathbb{Q}$. Além disso, de $p \in r^*$ concluímos que $p < r$, logo $q = \frac{p}{2} + \frac{r}{2} < \frac{r}{2} + \frac{r}{2} = r$, i.e., $q \in r^*$. Ademais, como $p < r$, então $r - p > 0$, logo $q = p + \frac{r-p}{2} > p$. $\dashv$

Como um exemplo adicional considere

$$r = \mathbb{Q}_{<0} \cup \{p \in \mathbb{Q} : p^2 < 2\}$$

provaremos que $r \in \mathbb{R}$

Prova. Para isso, note que $0 \in r$, logo $r \neq \emptyset$. Analogamente $2 \notin r$, visto que $2 > 0$ e $2^2 > 2$.

Se $p \in r$ e $q < p$, então, se $q < 0$, obviamente $q \in r$, seja portanto $q \geq 0$, logo, como $0 \leq q < p$, então $q^2 < p^2 < 2$, i.e., $q \in r$.

Por último, queremos $q \in r$ tal que $p < q < 2$, para isso, queremos garantir que existe $n \in \mathbb{N}$ positivo tal que $q := p + \frac{1}{n}$ satisfaz $q^2 = \left(p + \frac{1}{n}\right)^2 < 2$, i.e.

$$p^2 + \frac{2p}{n} + \frac{1}{n^2} < 2$$
$$\frac{1}{n}\left(2p + \frac{1}{n}\right) < 2 - p^2$$

como $n > 0$, então queremos

$$\frac{1}{n}\left(2p + \frac{1}{n}\right) < \frac{1}{n}(2p+1) < 2 - p^2$$

ou seja, basta tomarmos

$$n > \frac{2p+1}{2-p^2}$$

que, pela propriedade arquimediana, é garantido existir. $\dashv$

2.3 Relação de Ordem $\leq_{\mathbb{R}}$

Definiremos agora a noção de ordem $\leq_{\mathbb{R}}$ em $\mathbb{R}$:

Definição 2.2. Se $r, s \in \mathbb{R}$, definimos

$$r \leq_{\mathbb{R}} s \text{ sse } r \subseteq s$$

e

$$r <_{\mathbb{R}} s \text{ sse } r \leq_{\mathbb{R}} s \text{ e } r \neq s$$

Com isso, vamos provar que $(\mathbb{R}, \leq_{\mathbb{R}}) \vDash \mathrm{O}$

Teorema 2.3. $(\mathbb{R}, \leq_{\mathbb{R}})$ é uma ordem total, ou linear.

Prova. Precisamos verificar que $(\mathbb{R}, \leq_{\mathbb{R}}) \vDash \{\mathrm{O1}, \mathrm{O2}, \mathrm{O3}, \mathrm{O4}\}$ onde

(O1) reflexivo: $\forall r \in \mathbb{R}(r \leq_{\mathbb{R}} r)$

(O2) anti-simétrico: $\forall r, s \in \mathbb{R}(r \leq_{\mathbb{R}} s \land s \leq_{\mathbb{R}} r \to r = s)$

(O3) transitivo: $\forall r, s, t \in \mathbb{R}(r \leq_{\mathbb{R}} s \land s \leq_{\mathbb{R}} t \to r \leq_{\mathbb{R}} t)$

(O4) linear: $\forall r, s \in \mathbb{R}(r \leq_{\mathbb{R}} s \lor s \leq_{\mathbb{R}} r)$

(O1), (O2) e (O3) seguem diretamente do fato de que $\subseteq$ é uma relação de ordem parcial.

Para demonstrar (O4) sejam $\alpha, \beta \in \mathbb{R}$, temos que $\alpha \subseteq \beta$ ou $\alpha \nsubseteq \beta$, no primeiro caso $\alpha \leq_{\mathbb{R}} \beta$, caso contrário existe $a \in \alpha$ tal que $a \notin \beta$, i.e., $a \geq_{\mathbb{R}} b, \forall b \in \beta$, portanto $b \in \alpha$, i.e., $\beta \subseteq \alpha$. $\dashv$

2.4 Adição $\oplus$ em $\mathbb{R}$

Com o intuito de definir a adição $r \oplus s$ de reais vamos antes garantir que ela faz sentido:

Teorema 2.4. Se $r, s \in \mathbb{R}$, então

$$\gamma := \{p + q : p \in r, q \in s\}$$

é um real.

Prova. Como $r, s \in \mathbb{R}$, então ambos são não-vazios, i.e., existe $p \in r$ e $q \in s$, portanto $p + q \in \gamma$, i.e., $\gamma \neq \emptyset$. Analogamente, como $r, s \neq \mathbb{Q}$, existem $p \notin r$ e $q \notin s$, portanto $p \geq x$, $\forall x \in r$ e $q \geq y$, $\forall y \in s$, portanto $p + q \geq x + y$, $\forall x, y \in \mathbb{Q}$, i.e., $p + q \notin \gamma$, logo $\gamma \neq \mathbb{Q}$.

Se $x \in \gamma$ e $y < x$, por definição existem $p \in r$ e $q \in s$ tais que $x = p + q$, logo $y < x = p + q$, portanto $y - p < q \in s$, como s é um real, então ele é fechado à esquerda, logo $y - p \in s$ e, portanto, $y = (y - p) + p \in \gamma$, visto que $p \in r$ e $y - p \in s$, então γ é fechado à esquerda.

Se $x \in \gamma$, então $x = p + q$ com $p \in r$ e $q \in s$, mas como $r, s \in \mathbb{R}$, então existem $p' \in r$ e $q' \in s$ tal que $p' > p$ e $q' > q$, portanto $p' + q' > p + q$ e $p' + q' \in \gamma$, portanto γ não tem máximo. $\dashv$

Com isso, podemos então definir

Teorema 2.5. Dados $r, s \in \mathbb{R}$, definimos

$$r \oplus s := \{p + q : p \in r, q \in s\}$$

Provaremos que $(\mathbb{R}, \oplus) \vDash A$. Mas, para isso, vamos antes precisar de 2 lemas prévios:

Lema 2.1. Dado $r \in \mathbb{R}$, defina

$$M_r := \{p \in \mathbb{Q} : p \geq x,\ \forall x \in r\}$$

então temos que (para quando $\min(M_r)$ existe)

$$(-r) := \{p \in \mathbb{Q} : -p \in M_r, -p \neq \min(M_r)\}$$

é um número real.

Prova. Como $r \neq \mathbb{Q}$, existe $t \notin r$, i.e., $t > x$, $\forall x \in r$, portanto $t \in M_r$, note que, se $t \in M_r$, $t + 1 \in M_r$. Considere $-t$ e $-(t+1)$, no mínimo um desses é diferente de $\min(M_r)$, digamos t, logo $t \in (-r)$, i.e., $(-r)$ é não-vazio. Temos também que, se $p \in r$, então existe $q \in r$ tq $p < q$, logo $p \notin M_r$, i.e., $-p \notin (-r)$, visto que, caso contrário, $-(-p) = p \in M_r$, então $(-r) \neq \mathbb{Q}$

Seja agora $p \in (-r)$ e $q < p$, como $-p \in M_r$, então $-p > x$, $\forall x \in r$, logo $-q > -p > x$, $\forall x \in r$, i.e., $-q \in M_r$, logo $q \in (-r)$, portanto $(-r)$ é fechado à esquerda.

Seja $p \in (-r)$, i.e., $-p \in M_r$, como $-p \neq \min(M_r)$, então existe $q \in M_r$ tq $q < -p$ (se $q = \min(M_r)$ peguemos a média aritmética entre ambos), assim $-q > p$ e $-q \in (-r)$, logo $(-r)$ não admite máximo. $\dashv$

Lema 2.2. Se $r \in \mathbb{R}$ e $u \in 0^*$, então existem $p \in r$ e $q \in M_r$, $q \neq \min(M_r)$ (se existir) tais que $p - q = u$.

Prova. Como $r \in \mathbb{R}$, existe $s \notin r$. Defina $q_n := un + s$, i.e., uma sequência decrescente partindo de $q_0 = s$. Tomando $\overline{n} := \min\{n \in \mathbb{N} : q_n \in M_r\}$, que está bem definido pelo princípio da boa ordenação. Por definição temos que $q_{\overline{n}} \in M_r$, agora:

Se $q_{\overline{n}+1} \in \alpha$, então tome $p = q_{\overline{n}+1}$ e $q = q_{\overline{n}}$, logo $p - q = u$;

Se $q_{\overline{n}+1} = \min(M_r)$, então tome $p = q_{\overline{n}+1} + \frac{1}{2}u$ e $q = q_{\overline{n}} + \frac{1}{2}u$, logo $p \in r$ e $q \in M_r$, com $p - q = u$. $\dashv$

Teorema 2.6. $(\mathbb{R}, \oplus)$ satisfaz os axiomas de adição.

Prova. (A1): Dados $x, y, z \in \mathbb{R}$, se $p \in x \oplus (y \oplus z)$, então existe $x' \in x$, $a \in y \oplus z$ tal que $p = x' + a$, mas como $a \in y \oplus z$, existem $y' \in y$ e $z' \in z$ tais que $p = x' + (y' + z') = (x' + y') + z'$, i.e., $p \in (x \oplus y) \oplus z$. Portanto $x \oplus (y \oplus z) \subseteq (x \oplus y) \oplus z$, a inclusão contrária é análoga.

(A2): Se $x, y \in \mathbb{R}$ e $p \in x \oplus y$, então existem $a \in x$ e $b \in y$ tais que $p = a + b = b + a$, portanto $p \in y \oplus x$, a inclusão contrária também é análoga.

(A3): Queremos mostrar que $r \oplus 0^* = r$. Note que, se $x \in r \oplus 0^*$, então existe $p \in r$ e $q \in 0^*$ tais que $x = p + q$, por definição $q < 0$, logo $x = p + q < p$, como r é fechado à esquerda, $x \in r$, portanto $r \oplus 0^* \subseteq r$. Analogamente, seja $x \in r$, então existe $p \in r$ tal que $x < p$, visto que r não tem máximo, portanto $x - p < 0$, i.e., $x - p \in 0^*$, logo $x = p + (x - p) \in r \oplus 0^*$.

(A4): Mostraremos que, para $r \in \mathbb{R}$, temos $r \oplus (-r) = 0^*$. Se $x \in r \oplus (-r)$, então existe $p \in r$ e $q \in (-r)$ tq $x = p + q$. Como $q \in (-r)$, então $-q \in M_r$, logo $-q \notin r$, i.e., $-q > x$, $\forall x \in r$, em particular $-q > q$, i.e., $0 > q + p = x$, logo $x \in 0^*$. Para a volta, seja $x \in 0^*$, pela Lema anterior, existem $p \in r$ e $q \in M_r$ com $q \neq \min(M_r)$, se existir, tais que $p - q = x$. Como $q \in M_r$, então $-q \in (-r)$, i.e., $x = p + (-q) \in r \oplus (-r)$, logo $0^* \subseteq r \oplus (-r)$. $\dashv$

Tendo $\leq_{\mathbb{R}}$ e $\oplus$ definidos, provaremos agora O5:

Teorema 2.7. $(\mathbb{R}, \leq_{\mathbb{R}}, \oplus) \vDash$ O5

Prova. Se $p, q, r \in \mathbb{R}$ e $p \leq q$, então se $x = p \oplus r$, temos que existem $a \in p$ e $b \in r$ tais que $x = a + b$, como $a \in p$ e $p \leq q$, então $a \in q$ e, portanto, $x \in q + r$, logo $p + r \leq q + r$. $\dashv$

Teorema 2.8. (Unicidade do Oposto) Se $r \oplus p = 0^*$ e $r \oplus q = 0^*$, então $p = q$.

Prova.

$$p = p \oplus 0^* = p \oplus (r \oplus q) = (p \oplus r) \oplus q = 0^* \oplus q = q$$

$\dashv$

Teorema 2.9. (Unicidade do Elemento Neutro) Se $r \oplus s = r$, para todo $r \in \mathbb{R}$, então $s = 0^*$.

Prova. Como vale para todo $r \in \mathbb{R}$, em particular vale para 0^*, logo

$$0^* \oplus s = s = 0^*$$

$\dashv$

2.5 Multiplicação $\odot$ em $\mathbb{R}$

A fim de definirmos multiplicação em $\mathbb{R}$ precisamos antes garantir que o seguinte número está bem definido:

Teorema 2.10. Sejam $r, s \in \mathbb{R}$ com $r, s >_{\mathbb{R}} 0^*$, então

$$\gamma := \mathbb{Q}_{<0} \cup \{p \cdot q : p, q > 0, p \in r, q \in s\}$$

é um número real

Prova. Vamos antes provar que γ não admite máximo. Se $p \in \gamma$, com $p > 0$, então $p = ab$, para $a \in r$ e $b \in s$ ambos positivos, como $r, s \in \mathbb{R}$, existem $a' \in r$, com $a' > a$ e $b' \in s$, com $b' > b$, portanto $a'b' > ab = p$, com $a'b' \in \gamma$.

Como $\mathbb{Q}_{<0} \subseteq \gamma$ e o primeiro é não-vazio, então $\gamma \neq \emptyset$. Além disso, como $r, s \in \mathbb{R}$ existem $p \notin r$ e $q \notin s$, logo $p > x$, $\forall x \in r$ e $q > x$, $\forall x \in s$, então em particular vale para $x > 0$ em ambos os casos, logo $pq > xy > 0$, para todo $x \in r$, $y \in s$, com $x, y > 0$. Se $pq \in \gamma$, então temos que $pq > x$, $\forall x \in \gamma$, contradizendo que γ não admite máximo, portanto $pq \notin \gamma$, i.e., $\gamma \neq \mathbb{Q}$.

Seja $p \in \gamma$ e $q < p$. Se $p \leq 0$, então $q \in \gamma$, visto que $q < p \leq 0$. Se $p > 0$ e $q \leq 0$, então $q \in \gamma$, visto que, se $q < 0$, $q \in \gamma$, e se $q = 0$, então $p \cdot q = 0 = q \in \gamma$. Seja portanto $p, q > 0$, logo $p = ab$, com $a \in r$, $b \in s$ e $a, b > 0$. Como $q < p = ab$, então $\frac{q}{a} < b \in s$, logo $\frac{q}{a} \in s$ e, portanto $q = \frac{q}{a} \cdot a \in \gamma$. $\dashv$

Definição 2.3. Sejam $r, s \in \mathbb{R}$, defina

$$r \odot s := \begin{cases} \mathbb{Q}_{<0} \cup \{p \cdot q : p \in r, q \in s, p, q > 0\} \text{ se } r, s >_{\mathbb{R}} 0^* \\ 0^* \text{ se } r = 0^* \text{ ou } s = 0^* \\ -((-r) \odot s) \text{ se } r <_{\mathbb{R}} 0^* \text{ e } s >_{\mathbb{R}} 0^* \\ -(r \odot (-s)) \text{ se } r >_{\mathbb{R}} 0^* \text{ e } s <_{\mathbb{R}} 0^* \\ (-r) \odot (-s) \text{ se } r <_{\mathbb{R}} 0^* \text{ e } s <_{\mathbb{R}} 0^* \end{cases}$$

Como exemplo, vamos provar que se $r = \mathbb{Q}_{<0} \cup \{p \in \mathbb{Q} : p^2 < 2\}$, então $r \odot r = 2^*$. Por definição

$$r \odot r = \mathbb{Q}_{<0} \cup \{p \cdot q : p^2, q^2 < 2, p, q > 0\}$$

Se $x \in r \odot r$, se $x \leq 0$, então $x \in 2^*$, assuma portanto que $x > 0$, logo $x = ab$ com $a^2, b^2 < 2$ e $a, b > 0$, logo $x^2 = a^2b^2 < 4$ e, portanto, $x < 2$, ou seja, $x \in 2^*$.

Analogamente, se $x \in 2^*$, então $x^2 < 4$, i.e., $\frac{x^2}{2} < 2$. Queremos encontrar $a \in r$ tal que $\frac{x}{a} \in r$, visto que, se conseguirmos, então $a \cdot \frac{x}{a} = x \in r$. Se $a \in r$, então $a^2 < 2$, com $a > 0$, então em particular basta garantirmos que existe a tal que $\frac{x^2}{2} < a^2 < 2$. Se $\frac{x^2}{2} \leq 1$, obviamente existe $1 < a^2 < 2$ racional. Se $y = \frac{x^2}{2} > 1$, então queremos $n \in \mathbb{N}$ tal que

$$\left(1 + \frac{1}{n}\right)^2 < y, \frac{2}{y}$$

como

$$\left(1 + \frac{1}{n}\right)^2 = 1 + \frac{2}{n} + \frac{1}{n^2} \leq 1 + \frac{3}{n}$$

basta tomar n tal que

$$1 + \frac{3}{n} < \overline{y} := \min\left(y, \frac{2}{y}\right)$$

ou seja

$$n > \frac{3}{\overline{y} - 1}$$

que é garantido existir pela propriedade arquimediana. Seja $(a_i) := \left(1 + \frac{1}{n}\right)^{2i}$. Agora note que, como $a_1 < y, \frac{2}{y}$, então

$$a_2 = \left(1 + \frac{1}{n}\right)^4 = \left(1 + \frac{1}{n}\right)^2 \cdot \left(1 + \frac{1}{n}\right)^2 < y \cdot \frac{2}{y} = 2$$

se $y < a_2 < 2$, então estamos feitos, caso contrário $a_2 < y$ e, como $a_1 < \frac{2}{y}$, então $a_1 \cdot a_2 = a_3 < 2$, repetindo o argumento, é fácil ver por indução que, enquanto $a_n < y$, teremos $a_{n+1} < y$, mas (a_i) é estritamente crescente e, portanto, eventualmente será maior que y, logo algum elemento da sequência está entre 2 e y.

Provamores agora que $(\mathbb{R}, \odot) \vDash M$, mas para isso, antes vamos precisar de um lema prévio, análogo ao utilizado na adição.

Lema 2.3. Sejam $r >_{\mathbb{R}} 0^*$ um número real e $u \in \mathbb{Q}$ com $0 < u < 1$. Então existem $p \in r$, $q \in M_r$, (com $q \neq \min(M_r)$ caso exista) tais que $\frac{p}{q} = u$.

Prova. Como $r \in \mathbb{R}$, em particular existe $s \notin r$, logo $s > x$, $\forall x \in r$. Defina $q_n := su^n$, temos $q_0 = s$ e (q_i) estritamente decrescente, visto que $0 < u < 1$. Assim, o princípio da boa ordenação garante que $\overline{n} := \min\{n \in \mathbb{N} : q_n \in M_r\}$ existe e está bem definido. Por construção de $\overline{n}$, vale então que $q_{\overline{n}} \in M_r$ e:

Se $q_{\overline{n}+1} \in r$, então tome $p = q_{\overline{n}+1}$ e $q = q_{\overline{n}}$, logo $\frac{p}{q} = u$;

Se $q_{\overline{n}+1} = \min(M_r)$, então tome $p = q_{n+1}\sqrt{u}$ e $q = q_{\overline{n}}\sqrt{u}$, logo $p \in r$, $q \in M_r$ e $\frac{p}{q} = u$. $\dashv$

Teorema 2.11. $(\mathbb{R}, \odot)$ Satisfaz os axiomas de multiplicação.

Prova. (M1): Se $x \in (\alpha \odot \beta) \odot \gamma$ e algum deles são 0^*, por definição o produto é 0^* e vale (M1). Se $\alpha, \beta, \gamma >_{\mathbb{R}} 0^*$ e $x \leq 0$, então $x \in \alpha \odot (\beta \odot \gamma)$. Seja então $x > 0$, logo existem $y \in \alpha \odot \beta$ e $c \in \gamma$, com $y, c > 0$, tais que $x = y \cdot c$. Como $y \in \alpha \odot \beta$, então existem $a \in \alpha$ e $b \in \beta$ tais que $y = a \cdot b$, logo $x = (a \cdot b) \cdot c = a \cdot (b \cdot c)$, i.e., $x \in \alpha \odot (\beta \odot \gamma)$. A inclusão contrária é análoga e, os casos onde α, β ou γ são negativos é, pela definição de $\odot$, também análogo, visto que se reduzem ao produto de reais positivos.

(M2): Seja $x \in r \odot s$, se r ou s valem 0^* (M3) é trivialmente verificado, assuma então $r, s >_{\mathbb{R}} 0^*$, se $x \leq 0$, então $x \in s \odot r$. Seja portanto $x > 0$, logo existem $a \in r$ e $b \in s$, com $a, b > 0$ tais que $x = a \cdot b = b \cdot a$, logo $x \in s \odot r$, onde a inclusão contrária é análoga. Obviamente os outros casos para r e s menores que 0^* seguem do caso anterior, visto que, por definição de $\odot$, eles são reduzidos a multiplicação de reais positivos.

(M3): Se $r = 0^*$, então a igualdade é trivialmente verificada. Seja portanto $r >_{\mathbb{R}} 0^*$, se $x \in r \odot 1^*$ e $x \leq 0$, então $x \in r$, seja então $x > 0$, logo existem $a \in r$ e $u \in 1^*$, com $a > 0$ e $0 < u < 1$, tais que $x = a \cdot u < a$, logo $x \in r$.

Se $x \in r$ com $x \leq 0$, então $x \in r \odot 1^*$, seja portanto $x > 0$, logo existe $a \in r$ com $x < a$, i.e., $\frac{x}{a} < 1$, então $\frac{x}{a} \in 1^*$, como $x = a \cdot \frac{x}{a}$, então $x \in r \odot 1^*$.

Se $r <_{\mathbb{R}} 0$, por definição

$$r \odot 1^* = -((-r) \odot 1^*) = -(-r) = r$$

Para ver isso, precisamos primeiro provar que, se $r <_{\mathbb{R}} 0^*$, então $0^* <_{\mathbb{R}} (-r)$:

$$\begin{aligned} r <_{\mathbb{R}} 0^* &\iff r \oplus (-r) <_{\mathbb{R}} 0^* \oplus (-r) && \text{(O5)} \\ &\iff 0^* <_{\mathbb{R}} 0^* \oplus (-r) && \text{(A4)} \\ &\iff 0^* <_{\mathbb{R}} -r && \text{(A3)} \end{aligned}$$

Analogamente, para mostrar que $-(-r) = r$, temos que:

$$\begin{aligned} (-r) \oplus (-(-r)) &= 0^* && \text{(A4)} \\ r \oplus ((-r) \oplus (-(-r))) &= 0^* \oplus r \\ (r \oplus (-r)) \oplus (-(-r)) &= 0^* \oplus r && \text{(A1)} \\ 0^* \oplus (-(-r)) &= 0^* \oplus r && \text{(A4)} \\ -(-r)) &= r && \text{(A3)} \end{aligned}$$

(M4): Se $r > 0^*$, seja

$$s := \mathbb{Q}_{<0} \cup \left\{ p \in \mathbb{Q} : p > 0, \frac{1}{p} \in M_r \text{ e } \frac{1}{p} \neq \min(M_r) \right\}$$

Se $x \in r \odot s$ e $x \leq 0$, então $x \in 1^*$, assuma portanto $x > 0$, logo existem $p \in r$ e $q \in s$ tais que $x = p \cdot q$, com $p, q > 0$. Por definição $\frac{1}{q} \in M_r$, logo $\frac{1}{q} > y$, $\forall y \in r$, em particular $\frac{1}{q} > p$, i.e., $1 > pq = x$, logo $x \in 1^*$ e, portanto, $r \odot s \subseteq 1^*$.

Para o caminho contrário seja $x \in 1^*$, se $x \leq 0$, $x \in r \odot s$, seja portanto $0 < x < 1$, pelo lema anterior existem $p \in r$ e $q \in M_r$, com $q \neq \min(M_r)$ caso existe, tais que $\frac{p}{q} = x$, por definição $\frac{1}{q} \in s$, logo $x = p \cdot \frac{1}{q} \in r \odot s$, logo $1^* \subseteq r \odot s$. $\dashv$

Por fim, podemos provar os teoremas que relacionam ambas as operações e a relação de ordem

Teorema 2.12. $(\mathbb{R}, \oplus, \odot) \vDash \mathrm{D}$.

Prova. Para mostrar que $r \odot (p \oplus q) = (r \odot p) \oplus (r \odot q)$ vamos dividir em alguns casos:

Caso 1. $r, p, q >_{\mathbb{R}} 0^*$. Se $x \in r \odot (p \oplus q)$ e $x \leq 0$, então $x \in (r \odot p) \oplus (r \odot q)$. Seja portanto $x > 0$, logo $x = ay$, para algum $a > 0$ em r e $y > 0$ em $p \oplus q$., logo $y = b + c$, para $b, c > 0$ com $b \in p$ e $c \in q$. Assim, $x = a(b + c) = ab + ac \in (r \odot p) \oplus (r \odot q)$.

Para a inclusão contrário, assuma que $x \in (r \odot p) \oplus (r \odot q)$, se $x \leq 0$, temos $x \in r \odot (p \oplus q)$, seja então $x > 0$, logo existem $u \in r \odot p$ e $v \in r \odot q$ com $u, v > 0$ tais que $x = u + v$. Logo existem $a, a' \in r$, $b \in p$, $c \in q$ com $a, a', b, c > 0$ tais que $x = ab + a'c$. Assumindo WLOG que $a' \leq a$ temos $x = ab + a'c \leq ab + ac = a(b + c) \in r \odot (p \oplus q)$.

Caso 2. $r, p \oplus q >_{\mathbb{R}} 0^*$. Se $p >_{\mathbb{R}} 0^*$, $r \odot (-p) = -(r \odot (-(-p)) = -(r \odot p)$ $(\star)$, portanto

$$\begin{aligned}
r \odot q &= r \odot (q \oplus 0^*) && \text{(A3)}\\
&= r \odot (q \oplus (p \oplus (-p))) && \text{(A4)}\\
&= r \odot ((q \oplus p) \oplus (-p)) && \text{(A1)}\\
&= r \odot ((p \oplus q) \oplus (-p))) && \text{(A2)}\\
&= r \odot (p \oplus q) \oplus (r \odot (-p)) && \text{(Caso 1.)}\\
&= r \odot (p \oplus q) \oplus (-(r \odot p)) && (\star)\\
(r \odot p) \oplus (r \odot q) &= (r \odot (p \oplus q) \oplus (-(r \odot p))) \oplus (r \odot q) &&\\
(r \odot p) \oplus (r \odot q) &= r \odot (p \oplus q) \oplus (-(r \odot p) \oplus (r \odot p)) && \text{(A1)}\\
(r \odot p) \oplus (r \odot q) &= r \odot (p \oplus q) && \text{(A4)}
\end{aligned}$$

Se $q >_{\mathbb{R}} 0^*$ repita o mesmo processo anterior, mas com $r \odot p$ no começo e adicionando $q \oplus (-q)$.

Caso 3. $r >_{\mathbb{R}} 0^*$ e $p \oplus q <_{\mathbb{R}} 0^*$, por definição de $\odot$ temos que $r \odot (p \oplus q) = -(r \odot (-(p \oplus q)))$ $(\star)$. Além disso, temos que $(\dagger)$:

$$\begin{aligned}
(p \oplus q) \oplus (-(p \oplus q)) &= 0^* && \text{(A4)}\\
(-p) \oplus ((p \oplus q) \oplus (-(p \oplus q))) &= (-p) \oplus 0^* &&\\
(-p) \oplus (p \oplus (q \oplus (-(p \oplus q)))) &= (-p) \oplus 0^* && \text{(A1)}\\
((-p) \oplus p) \oplus (q \oplus (-(p \oplus q))) &= (-p) \oplus 0^* && \text{(A1)}\\
0^* \oplus (q \oplus (-(p \oplus q))) &= (-p) \oplus 0^* && \text{(A4)}\\
(-q) \oplus (q \oplus (-(p \oplus q))) &= (-q) \oplus (-p) && \text{(A3)}\\
((-q) \oplus q) \oplus (-(p \oplus q)) &= (-q) \oplus (-p) && \text{(A1)}\\
0^* \oplus (-(q \oplus p)) &= (-q) \oplus (-p) && \text{(A4)}\\
-(q \oplus p) &= (-q) \oplus (-p) && \text{(A3)}
\end{aligned}$$

Portanto, temos finalmente que

$$\begin{aligned} r \odot (p \oplus q) &= -(r \odot (-(p \oplus q))) && (\star) \\ &= -(r \odot ((-q) \oplus (-p))) && (\dagger) \\ &= -((r \odot (-q)) \oplus (r \odot (-p))) && (\text{Caso 2.}) \\ &= (-(r \odot (-q))) \oplus (-(r \odot (-p))) && (\dagger) \\ &= (r \odot q) \oplus (r \odot p) \end{aligned}$$

para justificar a última igualdade, note que, se $p <_{\mathbb{R}} 0^*$, então $-(r \odot p) = -(-(r \odot (-p))) = r \odot (-p)$ e, se $p >_{\mathbb{R}} 0^*$, então $r \odot (-p) = -(r \odot (-(-p))) = -(r \odot p)$, o caso $p = 0^*$ é trivial.

Caso 4. Se $r <_{\mathbb{R}} 0^*$, basta notar que $(p \oplus q) \odot r = -((p \oplus q) \odot (-r))$ onde $-r >_{\mathbb{R}} 0^*$, portanto voltamos aos casos anteriores. O mesmo ocorre quando $r = 0^*$. $\dashv$

E, por último

Teorema 2.13. $(\mathbb{R}, \oplus, \odot, \leq_{\mathbb{R}}) \vDash$ O6.

Prova. Se $r = p$ ou $q = 0$ obviamente vale (O6), seja portanto $r <_{\mathbb{R}} p$ e $q >_{\mathbb{R}} 0^*$, logo existe $p' \in p$ tal que $p > y$, $\forall y \in r$. Assim, vale que que, se $x \in r \odot p$ com $x \leq 0$, então $x \in p \odot q$. Seja, portanto, $x > 0$, logo existem $a \in r$, $b \in p$, com $a, b > 0$ tais que $x = ab < p'b \in p \odot q$. $\dashv$

3 Axioma do Supremo (AoC)

Neste capítulo vamos mostrar que a estrutura construída, agora de forma íntegra, $\mathfrak{R} = (\mathbb{R}, \oplus, \odot, \leq_{\mathbb{R}}, 0^*, 1^*)$ satisfaz de fato todos os axiomas de um corpo ordenado completo. Em particular, para isto, falta somente mostrarmos que $\mathfrak{R} \vDash$ AoC e, para isso, provaremos um lema antes:

Lema 3.1. Seja $\emptyset \neq A \subseteq \mathbb{R}$ limitado superiormente, então

$$\gamma := \bigcup_{\alpha \in A} \alpha$$

é um número real.

Prova. (R1): Como $A \neq \emptyset$, existe $r \in A$ e, como $r \in \mathbb{R}$, $r \neq \emptyset$, logo $\gamma \neq \emptyset$. Como A é limitado superiormente, existe $m \in \mathbb{R}$ tal que $r \leq m$, $\forall r \in A$, em particular, $m \neq \mathbb{Q}$, portanto existe $s \notin m$ e, como $r \leq m$, então $s \notin r$, $\forall r \in A$, logo $s \notin \gamma$, i.e., $\gamma \neq \emptyset$.

(R2): Sejam $p \in \gamma$ e $q < p$, logo existe $r \in A$ tal que $p \in r$, como $r \in \mathbb{R}$, $q \in r$, i.e., $q \in \gamma$.

(R3): Dado $p \in \gamma$, $p \in r$ para algum $r \in A$, como $r \in \mathbb{R}$, existe $p' \in r$ tq $p' > p$, logo $p' \in \gamma$. $\dashv$

Teorema 3.1. (Teorema do Supremo) Se $\emptyset \neq A \subseteq \mathbb{R}$ é limitado superiormente, então A admite supremo.

Prova. Seja $s = \bigcup_{r\in A} r$, pelo lema anterior $s \in \mathbb{R}$, vamos mostrar que $s = \sup(A)$. Por definição de s, dado $r \in A$, temos $r \subseteq s$, i.e., $s \geq_{\mathbb{R}} r$, $\forall r \in A$, portanto s é cota superior de A. Seja s' uma cota superior de A, i.e., $s' \geq_{\mathbb{R}} r$, $\forall r \in A$, logo $r \subseteq s'$, i.e., $s = \bigcup_{r\in A} r \subseteq s'$, portanto $s \leq_{\mathbb{R}} s'$. $\dashv$

Isso termina a prova de que $\mathfrak{R}$ é um modelo pros axiomsa de corpo ordenado completo.

4 Imersão de $\mathbb{Q}$ em $\mathbb{R}$

Da mesma forma que fizemos uma imersão, i.e., provamos que existe uma única função φ injetora, denominada incorporação canônica, que identifica uma estrutura como subestrutura da outra, de $\mathbb{N}$ em $\mathbb{Z} = {}^{\mathbb{N}\times\mathbb{N}}/_{\approx}$ e de $\mathbb{Z}$ em $\mathbb{Q} = {}^{\mathbb{Z}\times\mathbb{Z}}/_{\cong}$, faremos o mesmo para $\mathbb{Q}$ em $\mathbb{R}$.

Em particular, queremos provar que, se $\overline{\mathbb{Q}} := \{r^* : r \in \mathbb{Q}\}$, então $\varphi : \mathbb{Q} \to \overline{\mathbb{Q}}$ definida por $\varphi(r) = r^*$ é um homomorfismo bijetor. Ou seja, φ é bijetora e satisfaz:

i) $\varphi(r + s) = \varphi(r) \oplus \varphi(s)$
ii) $\varphi(r \cdot s) = \varphi(r) \odot \varphi(s)$
iii) $r \leq s \iff \varphi(r) \leq_{\mathbb{R}} \varphi(s)$

Teorema 4.1. $\varphi : \mathbb{Q} \to \overline{\mathbb{Q}}$ é bijetora.

Prova. Seja $r \neq s$, digamos $r < s$, logo $r \in s^*$, mas $r \notin r^*$, i.e., $r^* = \varphi(r) \neq \varphi(s) = s^*$, logo φ é uma função injetora.

Por definição $\mathrm{Im}(\varphi) = \overline{\mathbb{Q}}$, logo φ é sobrejetora. $\dashv$

Vamos aproveitar para provar um resultado direto

Lema 4.1. Para todo $p \in \mathbb{Q}$, temos que

$$-\varphi(p) = \varphi(-p)$$

Prova. $\dashv$

Teorema 4.2. $\varphi : \mathbb{Q} \to \overline{\mathbb{Q}}$ é um homomorfismo.

Prova. i) Se $x \in \varphi(r) \oplus \varphi(s) = r^* \oplus s^* = \{p + q : p \in r, q \in s\}$, então $x = p + q$, com $p < r$ e $q < s$ racionais, logo $x < r + s$, i.e., $x \in (r + s)^* = \varphi(r + s)$. Logo $\varphi(r) \oplus \varphi(s) \subseteq \varphi(r + s)$.

Analogamente, se $x \in \varphi(r + s)$, então $x < r + s$, ou seja, dado quaisquer $p \in r$ e $q \in s$, i.e., $p < r$ e $q < s$, temos que $p + q < r + s$, logo $p + q \in \varphi(r + s)$, portanto $\varphi(r + s) \subseteq \varphi(r) \oplus \varphi(s)$.

ii) Sejam $r, s > 0$, se $x \in \varphi(r) \odot \varphi(s)$ e $x \leq 0$, então $x \in (r \cdot s)^*$, seja portanto $x > 0$, logo $x = p \cdot q$, com $p \in r$, $q \in s$ e $p, q > 0$, assim $p < r$ e $q < s$ e, portanto, $x = pq < rs \in (r \cdot s)^*$. Assuma sem perda de generalidade que $r < 0$, logo Pendente

Assuma agora $r, s < 0$, Pendente

Se $r, s > 0$ e $x \in (r \cdot s)^*$, então, se $x \leq 0$, $x \in r^* \odot s^*$, assuma então $x > 0$, logo $x < r \cdot s$, i.e., $\frac{x}{r} < s$ e, portanto, $x = \frac{x}{r} \cdot r \in r^* \odot s^*$.

Tomando agora Pendente

iii) Se $r \leq s$, então $x < r \Rightarrow x < s$, i.e., $r^* \subseteq s^*$, e vice-versa. $\dashv$

5 Categoricidade de OF + AoC