Números Racionales

Campos Simplemente Ordenados.

Def. Un sistema algebraico $(K,+,\cdot,0,1)$ se llama un campo, si es un anillo conmutativo con identidad que satisface la siguiente condición:

$$\forall\, a,b\in K,\ b\neq 0,\ \exists\, x\in K \text{ tal que } bx=a$$

Teorema (5.1.2):

Sea $(K,+,\cdot,0,1)$ un anillo conmutativo con identidad. Entonces $(K,+,\cdot,0,1)$ es un campo si y sólo si, $\forall\, b\in K, b\neq 0, \exists\, y\in K$ tal que $by=1$.

Dem:

a) Supongamos que $(K,+,\cdot,0,1)$ es un campo, entonces es anillo conmutativo con identidad y $\forall\, a,b\in K,\ b\neq 0,\ \exists\, x\in K$ tal que:

$$bx=a$$

entonces, en particular, $\forall\, b\in K, b\neq 0$, si $a=1$, $\exists\, y=x\in K$ tal que:

$$by=1$$

b) Supongamos que $(K,+,\cdot,0,1)$ es un anillo conmutativo con identidad tal que $\forall\, b\in K,\ b\neq 0,\ \exists\, y\in K$ tal que:

$$by=1$$

entonces, $\forall\, a\in K$:

$$a(by)=a$$
$$\Rightarrow b(ay)=a$$

y por tanto, $\forall\, a,b\in K, b\neq 0, \exists\, x=ay$ tal que:

$$bx=a.$$

q.e.d.

Teorema (5.1.3)

Todo campo es un dominio entero.

Dem:

Sea $(K,+,\cdot,0,1)$ un campo y sean $a,b\in K$ tales que $a\cdot b=0$. Por probar que $a=0$ o $b=0$. Supongamos que $b\neq 0$, entonces $\exists\, y\in K$ tal que:

$$by=1$$

entonces, como $ab=0$:

$$(ab)y=0\cdot y$$

y por tanto:

$$a(by)=0$$

Luego:

$$a=a\cdot 1=0$$

q.e.d.

Teorema (S.1.9)

Sea $(K,+,\cdot,0,1)$ un campo, y sean $a,b\in K$, $b\neq 0$. Si $x\in K$ es tal que:

$$bx=a$$

entonces x es único.

Dem:

Si $x'\in K$ es tal que:

$$bx'=a$$

entonces:

$$bx'-bx=a-a$$
$$\Rightarrow b\cdot(x'-x)=0$$

como $b\neq 0$, entonces:

$$x'-x=0$$
$$\Rightarrow x'=x$$

q.e.d

obs: Del teorema anterior se sigue que si $b \neq 0$ y $by = 1$, entonces y es único.

Def. Sea $(K, +, \cdot, 0, 1)$ un campo, y sea $b \in K$, $b \neq 0$. Al único $y \in K$ tal que $by = 1$, se le llama inverso multiplicativo de b y se le designa por b^{-1}, así que $bb^{-1} = 1$.

Def: Sea $(K, +, \cdot, 0, 1)$ un campo y sean $a, b \in K$, $b \neq 0$. Definimos:

$$\frac{a}{b}$$

como el único $x \in K$ tal que $bx = a$.

obs: por definición, si $b \neq 0$ y $bx = a$, entonces:

$$x = \frac{a}{b}$$

o sea:

$$b\left(\frac{a}{b}\right) = a$$

En particular, como $bb^{-1} = 1$, entonces:

$$b^{-1} = \frac{1}{b}$$

$b\left(\frac{1}{b}\right) = 1 \iff b^{-1} = \frac{1}{b}$ por unicidad.

Teorema (S.1.7)

Si $(K, +, \cdot, 0, 1)$ es un campo y $a, b, c, d, e \in K$, con $b \neq 0$, $d \neq 0$ y $e \neq 0$, entonces:

i) $1^{-1} = 1$.

ii) $\frac{a}{1} = a$.

iii) $\frac{b}{b} = 1$.

iv) $\frac{a}{b} = a \cdot b^{-1}$.

v) $\frac{a}{b} = 0 \iff a = 0$.

vi) $\frac{a}{b} = \frac{c}{d} \iff ad = bc$.

vii) $\frac{a}{b} = \frac{a \cdot d}{b \cdot d}$.

viii) $\frac{a}{b} + \frac{c}{b} = \frac{a+c}{b}$.

ix) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$.

x) $(bd)^{-1} = b^{-1} \cdot d^{-1}$.

$x_i)\ \frac{a}{b}\cdot\frac{c}{d}=\frac{a\cdot c}{b\cdot d}.$

$x_{ii})\ \frac{a/b}{e/d}=\frac{ad}{be}.$

$x_{iii})\ -\frac{a}{b}=\frac{-a}{b}=\frac{a}{-b}.$

$x_{iv})$ Si $a\neq 0$, $\left(\frac{a}{b}\right)^{-1}=\frac{a^{-1}}{b^{-1}}=\frac{b}{a}.$

$xv)\ (b^{-1})^{-1}=b.$

$xvi)\ \frac{-a}{-b}=\frac{a}{b}.$

Dem:

De (i): Como $1\cdot 1=1$, se sigue de la definición que $1^{-1}=1$.

De (ii): Como $1\neq 0$, entonces existe $x\in K$ tal que:

$$1\cdot x=a$$

donde $x=\frac{a}{1}$. Por tanto:

$$1\cdot\frac{a}{1}=a$$

$$\Rightarrow \frac{a}{1}=a$$

De (iv): Por definición:

$$b\left(\frac{a}{b}\right)=a$$

$$\Rightarrow b^{-1}\cdot b\cdot\left(\frac{a}{b}\right)=b^{-1}\cdot a$$

$$\Rightarrow 1\cdot\left(\frac{a}{b}\right)=a\cdot b^{-1}$$

$$\Rightarrow \frac{a}{b}=a\cdot b^{-1}$$

De (iii): Por (iv):

$$\frac{b}{b}=b\cdot b^{-1}$$

$$=1$$

De (v):

$\Rightarrow)\ \frac{a}{b}=0\Rightarrow ab^{-1}=0\Rightarrow b\cdot(a\cdot b^{-1})=b\cdot 0\Rightarrow 1\cdot a=0\Rightarrow a=0.$

$\Leftarrow)\ a=0\Rightarrow 1\cdot a=0\Rightarrow(b\cdot b^{-1})\cdot a=0\Rightarrow b(a\cdot b^{-1})=0\Rightarrow b\left(\frac{a}{b}\right)=0\Rightarrow\frac{a}{b}=0.$

De (vi):

$\Rightarrow)\ \frac{a}{b}=\frac{c}{d} \Rightarrow a\cdot b^{-1}=c\cdot d^{-1} \Rightarrow (b\cdot d)\cdot(a\cdot b^{-1})=(b\cdot d)\cdot(c\cdot d^{-1}) \Rightarrow a\cdot d=b\cdot c$

$\Leftarrow)\ a\cdot d=b\cdot c \Rightarrow b^{-1}(a\cdot d)=b^{-1}(b\cdot c) \Rightarrow (a\cdot b^{-1})\cdot d=(b^{-1}\cdot b)\cdot c \Rightarrow \left(\frac{a}{b}\right)\cdot d=c$

$\Rightarrow d^{-1}\left(\left(\frac{a}{b}\right)\cdot d\right)=d^{-1}\cdot c \Rightarrow (d\cdot d^{-1})\cdot\left(\frac{a}{b}\right)=c\cdot d^{-1} \Rightarrow \frac{a}{b}=\frac{c}{d}.$

De (x): Tenemos que:

$$\begin{aligned}(b\cdot d)\cdot(b^{-1}\cdot d^{-1}) &= ((b\cdot d)\cdot b^{-1})\cdot d^{-1}\\ &= (b^{-1}\cdot(b\cdot d))\cdot d^{-1}\\ &= ((b^{-1}\cdot b)\cdot d)\cdot d^{-1}\\ &= (b\cdot b^{-1})\cdot(d\cdot d^{-1})\\ &= 1\cdot 1\\ &= 1\end{aligned}$$

y como $(b\cdot d)\cdot(b\cdot d)^{-1}=1$, se sigue que $(b\cdot d)^{-1}=b^{-1}\cdot d^{-1}$.

De (viii):

$$\frac{a}{b}=a\cdot b^{-1}=(a\cdot b^{-1})\cdot 1=(a\cdot b^{-1})\cdot(d\cdot d^{-1})=((a\cdot b^{-1})\cdot d)\cdot d^{-1}=(d\cdot(a\cdot b^{-1}))\cdot d^{-1}=(d\cdot a)\cdot(b^{-1}d^{-1})$$
$$=(a\cdot d)\cdot(b\cdot d)^{-1}=\frac{ad}{bd}.$$

De (viii):

$$\frac{a}{b}+\frac{c}{b}=a\cdot b^{-1}+c\cdot b^{-1}=(a+c)\cdot b^{-1}=\frac{a+c}{b^{-1}}.$$

De (ix):

$$\begin{aligned}\frac{a}{b}+\frac{c}{d} &= \frac{a\cdot d}{b\cdot d}+\frac{c\cdot b}{d\cdot b} && \text{(por viii)}\\ &= \frac{a\cdot d}{b\cdot d}+\frac{b\cdot c}{b\cdot d}\\ &= \frac{ad+bc}{bd} && \text{(por viii)}\end{aligned}$$

De (xi):

$$\begin{aligned}\frac{a}{b}\cdot\frac{c}{d} &= (a\cdot b^{-1})\cdot(c\cdot d^{-1})\\ &= ((a\cdot b^{-1})\cdot c)\cdot d^{-1}\\ &= (c\cdot(a\cdot b^{-1}))\cdot d^{-1}\\ &= (c\cdot a)\cdot(b^{-1}\cdot d^{-1})\end{aligned}$$

$$= (a \cdot c) \cdot (b \cdot d)^{-1}$$
$$= \frac{a \cdot c}{b \cdot d}.$$

De (x_{ii}):

$$\frac{\frac{a}{b}}{\frac{e}{d}} = \frac{\frac{a}{b} \cdot d}{\frac{e}{d} \cdot d} = \frac{\frac{ad}{b}}{e} = \frac{\frac{ad}{b} \cdot b}{eb} = \frac{ad}{eb}$$

De (x_{iii}):

$$-\frac{a}{b} = (-1) \cdot \left(\frac{a}{b}\right)$$
$$= (-1) \cdot (ab^{-1})$$
$$= \left((-1) \cdot a\right) \cdot b^{-1}$$
$$= (-a) \cdot b^{-1}$$
$$= \frac{-a}{b}$$

De (x_{iv}):

Como:

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba}$$
$$= \frac{ab}{ab}$$
$$= 1$$

y $\left(\frac{a}{b}\right) \cdot \left(\frac{a}{b}\right)^{-1} = 1$, entonces, como el inverso es único, $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$, y:

$$\frac{a}{b} \cdot \frac{a^{-1}}{b^{-1}} = \frac{a \cdot a^{-1}}{b \cdot b^{-1}} = \frac{1}{1} = 1$$

$$\Rightarrow \left(\frac{a}{b}\right)^{-1} = \frac{a^{-1}}{b^{-1}} = \frac{b}{a}.$$

De (x_v):

En lo que sigue, P es el conjunto de números naturales o enteros positivos.

Def: Sea $(K,+,\cdot,0,1)$ un campo. Sea $x\in K$, $x\neq 0$ y sea $m\in P$. Definimos x^{-m}, como:

$$x^{-m}=(x^{-1})^m$$

y se define:

$$x^0=1$$

Teorema (5.1.9):

Sea $(K,+,\cdot,0,1)$ un campo. Si $x,y\in K$, $x\neq 0$, $y\neq 0$ y $m,n\in\mathbb{Z}$, entonces:

i) $1^n=1$.

ii) $x^{-m}=(x^{-1})^m$.

iii) $(x\cdot y)^n=x^n\cdot y^n$.

iv) $x^{-m}=(x^m)^{-1}$.

v) $x^{m\cdot n}=(x^m)^n$.

vi) $x^{m+n}=x^m\cdot x^n$

vii) $x^{m-n}=x^m/x^n$.

viii) $(x/y)^n=x^n/y^n$.

Dem:

De (i): Si $n\geq 0$, claro que $1^n=1$. Si $n<0$, sea $K=-n$, entonces $n=-K$, entonces:

$$\begin{aligned}1^n&=1^{-K}\\&=(1^{-1})^K\\&=(1)^K, \text{ pues } 1^{-1}=1.\\&=1\ \square\end{aligned}$$

De (ii):

Si $m\geq 0$, entonces de la definición se sigue que $x^{-m}=(x^{-1})^m$.

Si $m<0$, sea $n=-m$. Entonces $0<n$, y por tanto $0\leq n$. De esta for-

ma:

$$\begin{aligned} x^{-m} &= x^{-(-n)} \\ &= x^{n} \\ &= \left(\left(x^{-1}\right)^{-1}\right)^{n} \\ &= \left(x^{-1}\right)^{-n} \\ &= \left(x^{-1}\right)^{m} \end{aligned}$$

De (iii):

Si $0 \leq n$, entonces por una proposición anterior, $(x \cdot y)^n = x^n \cdot y^n$.

Si $n < 0$, sea $K = -n$, entonces $0 < K$, por lo cual $0 \leq K$. Así:

$$\begin{aligned} (x \cdot y)^n &= (x \cdot y)^{-K} \\ &= \left((x \cdot y)^{-1}\right)^{K} \\ &= \left(x^{-1} \cdot y^{-1}\right)^{K} \\ &= \left(x^{-1}\right)^{K} \cdot \left(y^{-1}\right)^{K} \\ &= x^{-K} \cdot y^{-K} \\ &= x^{n} \cdot y^{n} \end{aligned}$$

De (iv): Veamos que:

$$\begin{aligned} x^m \cdot \left(x^{-1}\right)^m &= \left(x \cdot x^{-1}\right)^m \\ &= 1^m \\ &= 1 \end{aligned}$$

pero $x^m \cdot (x^m)^{-1} = 1$. Por tanto: $(x^m)^{-1} = (x^{-1})^m$. Como $(x^{-1})^m = x^{-m}$, se sigue que:

$$x^{-m} = (x^m)^{-1}$$

De (v):

Si $0 \leq m$ y $0 \leq n$, entonces, por una proposición anterior $x^{m \cdot n} = (x^m)^n$.

Si $m < 0$ y $0 \leq n$, sea $K = -m$, entonces

$$\begin{aligned} x^{m\cdot n} &= x^{(-k)n} \\ &= x^{-(kn)} \\ &= (x^{-1})^{kn} \\ &= (x^{-k})^{n} \\ &= (x^{m})^{n} \end{aligned}$$

Si $0 \leq m$ y $n < 0$, se sigue un caso análogo al anterior.

Si $m < 0$ y $n < 0$, sean $k = -m$ y $l = -n$, entonces $0 < k$ y $0 < l$, por tanto $0 \leq k$ y $0 \leq l$. Entonces:

$$\begin{aligned} x^{mn} &= x^{(-k)\cdot(-l)} \\ &= x^{kl} \\ &= (x^{k})^{l} \\ &= (((x^{k})^{-1})^{-1})^{l} \\ &= (x^{-k})^{-l} \\ &= (x^{m})^{n} \end{aligned}$$

Def. Sea $(K,+,\cdot,0,1)$ un campo. Si $<$ es una relación en K de modo que $(K,+,\cdot,<,0,1)$ es un dominio entero simplemente ordenado, entonces decimos que $(K,+,\cdot,<,0,1)$ es un campo simplemente ordenado.

Teorema (5.1.11)

Sea $(K,+,\cdot,<,0,1)$ un campo simplemente ordenado. Si $a,b,c,d \in K$, con $b\neq 0$ y $d\neq 0$, entonces:

i) $0<\frac{a}{b} \Leftrightarrow 0<ab$

ii) $\frac{a}{b}<\frac{c}{d} \Leftrightarrow (ad)(bd)<(bc)(bd)$

iii) Si $0<bd$, entonces $\frac{a}{b}<\frac{c}{d} \Leftrightarrow ad<bc$.

iv) $0<d<b \Leftrightarrow 0<\frac{1}{b}<\frac{1}{d}$.

Dem:

De (i): dado $b\in K$, $b\neq 0$, como K es dominio entero, entonces:

$$0<b^2$$

y también:

$$0<\left(\frac{1}{b}\right)^2=\frac{1}{b^2}$$

Así que:

$$0<\frac{a}{b} \Rightarrow 0<\left(\frac{a}{b}\right)b^2 \Rightarrow 0<\left[\left(\frac{a}{b}\right)b\right]b \Rightarrow 0<ab$$

Inversamente:

$$0<ab \Rightarrow 0<(ab)\cdot\frac{1}{b^2} \Rightarrow 0<(ab)\frac{1}{b}\cdot\frac{1}{b} \Rightarrow 0<\left[a\left(b\cdot\frac{1}{b}\right)\right]\cdot\frac{1}{b} \Rightarrow 0<a\cdot\frac{1}{b}$$

$$\Rightarrow 0<ab^{-1} \Rightarrow 0<\frac{a}{b}. \quad \square$$

De (ii):

Def. Sea S un conjunto y sea $<$ una relación en S. Decimos que S es densamente ordenado por la relación $<$, y que $(S, <)$ es densamente ordenado, si:

i) $<$ es un orden simple en S, i.e $<$ es tricotómico y transitivo.

ii) $\forall x, y \in S, x < y \Rightarrow \exists z \in S$ tal que $x < z < y$.

Teorema (5.1.13)

Si $(K, +, \cdot, <, 0, 1)$ es un campo simplemente ordenado, entonces K es densamente ordenado por $<$.

Nota: $2 = 2 \cdot 1$

$1 \in D^+$, así:

$2 \in D^+$.

Dem:

Dados $a, b \in K$, basta probar que

$$a < b \Rightarrow a < \frac{a+b}{2} < b$$

Por un lado,

$$a < b \Rightarrow a + a < a + b \Rightarrow 2a < a + b \Rightarrow \frac{1}{2}(2a) < \frac{1}{2}(a+b) \Rightarrow a < \frac{a+b}{2}$$

Por otro lado,

$$a < b \Rightarrow a + b < b + b \Rightarrow a + b < 2b \Rightarrow \frac{1}{2}(a+b) < \frac{1}{2}(2b) \Rightarrow \frac{a+b}{2} < b$$

En resumen:

$$a < b \Rightarrow a < \frac{a+b}{2} < b$$

q.e.d.

Def.

Decimos que un campo $(K', +, \cdot, 0, 1)$ es un subcampo del campo $(K, +, \cdot, 0, 1)$, si es un subsistema de este último. Decimos que:

$$(K', +, \cdot, <, 0, 1)$$

es un subcampo simplemente ordenado de $(K, +, \cdot, <, 0, 1)$, si es un subsistema de este último.

Teorema (5.1.15)

Sea $(K, +, \cdot, <, 0, 1)$ un campo simplemente ordenado. Si $K' \subset K$ es tal que $0, 1 \in K$

Y:

i) $x, y \in K' \Rightarrow x+y \in K'$.

ii) $x, y \in K' \Rightarrow x \cdot y \in K'$.

iii) $x \in K' \Rightarrow -x \in K'$.

iv) $x \in K'$ y $x \neq 0 \Rightarrow x^{-1} \in K'$.

entonces $(K', +, \cdot, <, 0, 1)$ es un subcompo de $(K, +, \cdot, <, 0, 1)$.

Dem:

Observación: La relación de isomorfismo entre sistemas algebraicos, es una relación de equivalencia.

Definición (2.2.2).- Sean

$$(S, F_1, ..., F_k, W_1, ..., W_l, a_1, ..., a_m)$$

y

$$(S', F'_1, ..., F'_k, W'_1, ..., W'_l, a'_1, ..., a'_m)$$

dos sistemas algebraicos del mismo tipo. Decimos que el segundo sistema es un **subsistema** del primero, o que el primero es una **extensión** del segundo, si se satisfacen las siguientes condiciones:

i) $S' \subset S$

ii) $a'_i = a_i, \forall\, i = 1, ..., m.$

iii) $\forall\, i = 1, ..., m.$

$$\begin{aligned} W'_i &= W_i|_{S'} \\ &= \{(x, y) \mid x \in S', y \in S' \text{ y } (x, y) \in W_i\} \end{aligned}$$

iv) Si F_i es, digamos, una operación binaria en S, entonces

$$F'_i(x, y) = F_i(x, y),$$

$\forall\, x, y \in S'$. Es decir, $F'_i = F_i|_{S' \times S'}$, $\forall\, i = 1, ..., m$.

Observación: Cuando $(i), (ii), (iii)$ y (iv) se cumplen, decimos que S' es un subsistema de S, con respecto a operaciones, relaciones y elementos distinguidos.

Ejemplo:

Sean los sistemas $(\mathbb{N}, \cdot, \leq, 1)$ y $(S', \cdot, \prec, 1)$, donde

$$S' = \{2^n \mid n = 0 \text{ o } n \in \mathbb{N}\}$$

$$a \prec b \Longleftrightarrow a|b.$$

Es claro que $(S', \cdot, \prec, 1)$ es un subsistema de $(\mathbb{N}, \cdot, \leq, 1)$. Basta probar que $\prec \;=\; \leq|_{S'}$: Sean $a, b \in S'$,

$$a \prec b \Longleftrightarrow a|b \Longleftrightarrow a \leq b.$$

Teorema (2.2.3).- Sean

$$(S, F_1, ..., F_k, W_1, ..., W_l, a_1, ..., a_m),$$

$$(S', F'_1, ..., F'_k, W'_1, ..., W'_l, a'_1, ..., a'_m)$$

y

$$(S'', F''_1, ..., F''_k, W''_1, ..., W''_l, a''_1, ..., a''_m)$$

sistemas algebraicos del mismo tipo. Si

$$(S, ...) \cong (S', ...)$$

y $(S', ...)$ es un subsistema de $(S'', ...)$, entonces existe un sistema

$$(S^\star, F^\star_1, ..., F^\star_k, W^\star_1, ..., W^\star_l, a^\star_1, ..., a^\star_m)$$

que tiene como subsistema a $(S, ...)$ y tal que

$$(S^\star, ...) \cong (S'', ...).$$

Demostración:

Sea G el isomorfismo entre $(S, ...)$ y $(S', ...)$.

Campo de cocientes.

Teorema (5.2.1)

Sea $(D,+,\cdot,0,1)$ un dominio entero arbitrario. Entonces podemos construir un campo $(Q,+,\cdot,0,1)$ con las siguientes propiedades:

1. $(D,+,\cdot,0,1)$ es un subdominio de $(Q,+,\cdot,0,1)$.
2. Para cada $x\in Q$, existen $a,b\in D$ tales que $x=\frac{a}{b}$.
3. Si $<$ es una relación en D, bajo la cual $(D,+,\cdot,<,0,1)$ es un dominio entero simplemente ordenado, entonces podemos extender la relación $<$ de modo que:

$$(Q,+,\cdot,<,0,1)$$

es un campo simplemente ordenado que contiene como subdominio a:

$$(D,+,\cdot,<,0,1)$$

Dem:

Sea

$$S=\{(a,b)\mid a,b\in D, b\neq 0\}$$
$$=D\times(D-\{0\}).$$

Definimos en S la siguiente relación:

$$(a,b)\sim(c,d)\iff ad=cb.$$

Afirmamos que $\sim$ es relación de equivalencia en S. Obviamente $\sim$ es reflexiva y simétrica.

Veamos que $\sim$ es transitiva: Si

$$(a,b)\sim(c,d) \text{ y } (c,d)\sim(x,y)\Rightarrow ad=cb \text{ y } cy=xd$$

por tanto:

$$ady=cby \quad y \quad bcy=bxd$$

entonces:

$$ady = cby \quad y \quad cby = bxd$$

entonces

$$ady = bxd$$

por ser $d \neq 0$ y D un dominio entero:

$$ay = xb$$

y por tanto:

$$(a,b) \sim (x,y)$$

Denotamos por $[a,b]$ a la clase de equivalencia de $(a,b) \in S$, es decir,

$$[a,b] = C_{\sim}(a,b)$$

Por tanto:

$$[a,b] = \{(x,y) \in S \mid (a,b) \sim (x,y)\}$$

Definimos:

$$R = S_{/\sim}$$
$$= \{[a,b] \mid (a,b) \in S\}$$

Ahora definimos las siguientes operaciones en S: $\forall (a,b),(c,d) \in S$:

$$(a,b) \oplus (c,d) = (a \cdot d + b \cdot c,\ b \cdot d)$$

y

$$(a,b) \odot (c,d) = (a \cdot c,\ b \cdot d)$$

claro que $\oplus$ y $\odot$ son operaciones en S, por definición de pareja ordenada y el hecho de que $+$ y $\cdot$ son operaciones en D:

$$(a,b) \oplus (c,d) = (a \cdot d + b \cdot c,\ b \cdot d)$$
$$= (c \cdot b + d \cdot a,\ d \cdot b)$$
$$= (c,d) \oplus (a,b)$$

y:

$$(a,b) \odot (c,d) = (a \cdot c,\ b \cdot d)$$

$$= (c \cdot a, d \cdot b)$$
$$= (c,d) \odot (a,b)$$

Veamos ahora que $\sim$ es compatible con respecto a las operaciones $\oplus$ y $\odot$, es decir:

A) Si $(a,b) \sim (x,y)$ y $(c,d) \sim (w,z)$, entonces:

i) $(a,b) \oplus (c,d) \sim (x,y) \oplus (w,z)$ y

ii) $(a,b) \odot (c,d) \sim (x,y) \odot (w,z)$.

Para probar A), basta probar que:

B) Si $(a,b) \sim (x,y)$ y $(c,d) \in S$, entonces:

i') $(a,b) \oplus (c,d) \sim (x,y) \oplus (c,d)$ y

ii') $(a,b) \odot (c,d) \sim (x,y) \odot (c,d)$

Pues, si B) es cierto y $(c,d) \sim (w,z)$, entonces:

$$(a,b) \oplus (c,d) \sim (x,y) \oplus (c,d) \sim (c,d) \oplus (x,y) \sim (w,z) \oplus (x,y) \sim (x,y) \oplus (w,z)$$

por tanto:

$$(a,b) \oplus (c,d) \sim (x,y) \oplus (w,z)$$

y análogamente:

$$(a,b) \odot (c,d) \sim (x,y) \odot (c,d) \sim (c,d) \odot (x,y) \sim (w,z) \odot (x,y) \sim (x,y) \odot (w,z)$$

por tanto:

$$(a,b) \odot (c,d) \sim (x,y) \odot (w,z)$$

Ahora, probaremos B):

Supongamos que $(a,b) \sim (x,y)$ y $(c,d) \in S$, es decir, supongamos que $ay = xb$ y $(c,d) \in S$.

i') Deseamos probar que $(a,b) \oplus (c,d) \sim (x,y) \oplus (c,d)$:

$$(a,b) \oplus (c,d) \sim (x,y) \oplus (c,d)$$
$$\Leftrightarrow (ad + bc, bd) \sim (xd + yc, yd)$$

$$\Leftrightarrow (ad+bc)yd = bd(xd+yc)$$
$$\Leftrightarrow (ad+bc)y = (xd+yc)b$$
$$\Leftrightarrow ady+bcy = xdb+ycb$$
$$\Leftrightarrow ady+bcy = xdb+bcy$$
$$\Leftrightarrow ady = xdb$$
$$\Leftrightarrow ay = xb$$
$$\Leftrightarrow (a,b)\sim(x,y) \text{ y } (c,d)\in S.$$

Por tanto, si:

$$(a,b)\sim(x,y) \text{ y } (c,d)\in S$$

entonces

$$(a,b)\oplus(c,d)\sim(x,y)\oplus(c,d)$$

ii) Deseamos probar ahora que $(a,b)\odot(c,d)\sim(x,y)\odot(c,d)$:

$$(a,b)\odot(c,d)\sim(x,y)\odot(c,d)$$
$$\Leftrightarrow (ac,bd)\sim(xc,yd)$$
$$\Leftrightarrow acyd = bdxc$$
$$\Leftrightarrow ay(cd) = xb(cd)$$
$$\Leftrightarrow ayc = xbc$$
$$\Leftarrow ay = xb$$
$$\Leftrightarrow (a,b)\sim(x,y) \text{ y } (c,d)\in S$$

Por tanto, si

$$(a,b)\sim(x,y) \text{ y } (c,d)\in S,$$

entonces

$$(a,b)\odot(c,d)\sim(x,y)\odot(c,d)$$

En resumen, $\sim$ es compatible respecto a las operaciones $\oplus$ y $\odot$. Por tanto $\oplus$ y $\odot$ inducen las operaciones $+$ y $\cdot$ en R, definidas como sigue:

$\forall [a,b],[c,d] \in R$,

$$[a,b]+[c,d] = [(a,b)\oplus(c,d)]$$
$$= [(ad+bc,bd)]$$
$$= [ad+bc,bd]$$

y

$$[a,b]\cdot[c,d] = [(a,b)\odot(c,d)]$$
$$= [ac,bd]$$

Observemos que:

$[a,b]+[c,d]=[a,b] \Leftrightarrow [ad+bc,bd]=[a,b] \Leftrightarrow (ad+bc,bd)\sim(a,b)$

$\Leftrightarrow (ad+bc)b = abd \Leftrightarrow ad+bc = ad \Leftrightarrow bc = 0 \Leftrightarrow c=0.$

Así que, definimos $\bar{0}=[0,d]$, es decir $\bar{0}=[c,d] \Leftrightarrow c=0.$

Por otro lado, si $a\neq 0$:

$[a,d]\odot[c,d] = [a,b] \Leftrightarrow [ac,bd] = [a,b] \Leftrightarrow (ac,bd)\sim(a,b) \Leftrightarrow$

$acb = abd \Leftrightarrow c=d$

Así que, definimos $\bar{1}=[d,d]$, por tanto $\bar{1}=[c,d] \Leftrightarrow c=d.$

Con lo anterior, debe probarse que

$$(R,+,\cdot,\bar{0},\bar{1})$$

es un campo, es decir, que es un anillo conmutativo con identidad, y además que,

$\forall [a,b]\neq[0,b]$,

$$\exists\, x=[c,d]\in R$$

tal que

$$[a,b]\cdot[c,d]=\bar{1}$$

esto último como consecuencia de que, si $[a,b]\neq\bar{0}$, entonces, $a\neq 0$ y $x=[b,a]$ es tal que

$$[a,b]\cdot x = [a,b]\cdot[b,a]$$

$$= [ab, ab]$$
$$= \bar{1}$$

por tanto, $[a,b]^{-1} = [b,a]$.

Se deja como ejercicio probar que $(R, +, \cdot, \bar{0}, \bar{1})$ es un anillo conmutativo con identidad.

Observemos que, dado $[a,b] \in R$,

$$\begin{aligned}[a,b]+[-a,b] &= [ab-ab, b^2] \\ &= [0,b^2] \\ &= \bar{0}\end{aligned}$$

por tanto: $-[a,b]=[-a,b]$.

Veamos ahora que se verifica la condición (1) del teorema. Sea:

$$\bar{R} = \{[a,1] \in R \mid a \in D\}$$

Para cada $a \in D$, definimos:

$$\bar{a} = [a,1]$$

Se deja como ejercicio probar que $\bar{R}$, con las operaciones de R, es un dominio entero (subdominio de R).

Sea $G: D \to \bar{R}$ la regla de asociación definida por: $G(a) = \bar{a}$. Veamos que G es isomorfismo.

a) G es función.

Sean $a, b \in D$, si $a = b$:

$$a = b \Rightarrow a \cdot 1 = b \cdot 1 \Rightarrow (a,1) \sim (b,1) \Rightarrow [a,1] = [b,1] \Rightarrow \bar{a} = \bar{b} \Rightarrow G(a) = G(b)$$

b) G es inyectiva.

Sean $a, b \in D$,

$$G(a) = G(b) \Rightarrow \bar{a} = \bar{b} \Rightarrow [a,1] = [b,1] \Rightarrow (a,1) \sim (b,1) \Rightarrow a \cdot 1 = b \cdot 1 \Rightarrow a = b$$

c) G es suprayectiva.

Si $\bar{a} \in \bar{R}$, entonces $a \in D$ y $G(a) = \bar{a}$.

d) G preserva la suma.

$\forall\, a, b \in D$,

$$\begin{aligned} G(a+b) &= \overline{a+b} \\ &= [a+b, 1] \\ &= [a \cdot 1 + 1 \cdot b, 1 \cdot 1] \\ &= [a,1] \oplus [b,1] \\ &= \bar{a} + \bar{b} \\ &= G(a) + G(b) \end{aligned}$$

e) G preserva la multiplicación:

$\forall\, a, b \in D$,

$$\begin{aligned} G(a \cdot b) &= \overline{a \cdot b} \\ &= [a \cdot b, 1] \\ &= [a \cdot b, 1 \cdot 1] \\ &= [a,1] \cdot [b,1] \\ &= \bar{a} \cdot \bar{b} \\ &= G(a) \cdot G(b) \end{aligned}$$

también:

$G_1(0)=\bar{0}$ y $G_1(1)=\bar{1}$, se sigue que G es un isomorfismo, y por tanto:

$$(D,+,\cdot,0,1)\cong(\bar{R},+,\cdot,\bar{0},\bar{1})$$

Como $(\bar{R},+,\cdot,\bar{0},\bar{1})$ es un subsistema de $(R,+,\cdot,\bar{0},\bar{1})$, entonces por el teorema (2.2.3), existe un sistema $(Q,+,\cdot,0,1)$ que contiene como subsistema a $(D,+,\cdot,0,1)$ y tal que $(Q,+,\cdot,0,1)\cong(R,+,\cdot,\bar{0},\bar{1})$.

Como $(R,+,\cdot,\bar{0},\bar{1})$ es un campo, entonces $(Q,+,\cdot,0,1)$ es un campo que contiene a $(D,+,\cdot,0,1)$ como dominio entero.

Con lo cual se verifica la condición (1) del teorema. Veremos que se satisface (2) del teorema.

Sea $H:Q\to R$ el isomorfismo entre $(Q,+,\cdot,0,1)$ y $(R,+,\cdot,\bar{0},\bar{1})$. Para $x\in R$, $x=[a,b]$, entonces:

$$\begin{aligned}x&=[a,b]\\&=[a,1]\cdot[1,b]\\&=[a,1]\cdot[b,1]^{-1}\\&=\bar{a}\cdot(\bar{b})^{-1}\\&=\frac{\bar{a}}{\bar{b}}\end{aligned}$$

Sea $z\in Q$, entonces existe $w\in R$ tal que $z=H^{-1}(w)$. Como $w=[a,b]$, entonces: $w=\bar{a}\cdot(\bar{b})^{-1}$. Observemos también que si $v\in R$ y $v\neq\bar{0}$, entonces $\exists\, v^{-1}$ tal que $v\cdot v^{-1}=\bar{1}$, entonces:

$$H^{-1}(v\cdot v^{-1})=H^{-1}(\bar{1})$$
$$\Rightarrow H^{-1}(v)\cdot H^{-1}(v^{-1})=1$$

$H^{-1}(v)\neq 0$, entonces:

$$H^{-1}(v^{-1})=(H^{-1}(v))^{-1}$$

Por tanto:

$$z=H^{-1}(w)$$

$$= H^{-1}(\bar{a}\cdot(\bar{b})^{-1})$$
$$= H^{-1}(\bar{a})\cdot H^{-1}((\bar{b})^{-1})$$
$$= H^{-1}(\bar{a})\cdot(H^{-1}(\bar{b}))^{-1}$$
$$= \frac{H^{-1}(\bar{a})}{H^{-1}(\bar{b})}$$

Puesto que $\bar{a},\bar{b}\in\bar{R}$, entonces $H^{-1}(\bar{a}) = G^{-1}(\bar{a}) = a$, y:

$$H^{-1}(\bar{b}) = G^{-1}(\bar{b})$$
$$= b$$
$$\Rightarrow z = \frac{a}{b} \;;\; \frac{a}{1} = a \;\forall a\in D$$

En consecuencia, z se escribe como cociente de dos elementos de D. Finalmente, probaremos que se cumple la propiedad (3) del teorema.

Sea $<$ la relación bajo la cual $(D,+,\cdot,<,0,1)$ es un dominio entero simplemente ordenado Sea:

$$P = \{\tfrac{a}{b}\in Q \mid a,b\in D \text{ y } 0<a\cdot b\}$$

I) Observemos que si $\frac{a}{b}, \frac{c}{d}\in Q$ son tales que

$$\frac{a}{b} = \frac{c}{d},$$

entonces:

$$0<a\cdot b \Leftrightarrow 0< c\cdot d$$

En efecto:

$$\frac{a}{b} = \frac{c}{d} \Leftrightarrow a\cdot b^{-1} = c\cdot d^{-1} \Leftrightarrow ad = bc$$

por tanto

$$(ad)(bc) = b^2c^2$$

y por tanto:

$$(ab)(cd) = b^2c^2$$

Si $0<ab$, entonces $a\neq 0$ y por tanto $c\neq 0$, entonces $0<b^2c^2$, y por tanto $0<c\cdot d$.

Inversamente, si $0<c\cdot d$, entonces $c\neq 0$, y enctonces $0<b^2c^2$, y por tanto $0<a\cdot b$.

II) Observemos ahora que $a\in D^+ \Rightarrow a=\frac{a}{1}\in P$. En efecto:

$$a\in D^+ \Rightarrow 0<a \Rightarrow 0<a\cdot 1 \Rightarrow \frac{a}{1}=a\in P$$

Probaremos ahora que:

a) Si $x,y\in P$, entonces $x+y\in P$ y $x\cdot y\in P$.

b) $\forall\, x\in Q$ se cumple una y solo una de:

i) $x\in P$

ii) $x=0$

iii) $-x\in P$

Prueba de (a): Sean $x,y\in P$, entonces existen $a,b,c,d\in D$ tales que

$$x=\frac{a}{b},\quad y=\frac{c}{d},\quad 0<a\cdot b \text{ y } 0<c\cdot d$$

Como

$$x+y=\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}$$

y

$$(ad+bc)bd=(ab)d^2+a^2(cd)>0$$

debido a que:

$$0<ab,\ 0<d^2,\ 0<b^2 \text{ y } 0<cd,$$

entonces $x+y\in P$.

Puesto que:

$$x\cdot y=\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$$

y

$$(ac)(bd)=(ab)(cd)>0,$$

entonces $x\cdot y\in P$.

Prueba de b): Si $x\in Q$, entonces existen $a,b\in D$, con $b\neq 0$ tales que:

$$x=\frac{a}{b}$$

Como $a,b\in D$, se cumple una y sólo una de:

i') $0<ab$

ii') $ab=0$

iii') $0<-(ab)$

En consecuencia, se cumple una y solo una de:

i) $x\in P$

ii) $x=0$

iii) $-x\in P$

Por el teorema (4.2.4), se sabe que si $P\subset Q$ que cumple a) y b), y definimos la relación $<$ en Q como: $\forall x,y\in Q$:

$$x<y \iff y-x\in P,$$

entonces $(Q,+,\cdot,<,0,1)$ es un dominio entero simplemente ordenado, y en este caso un campo simplemente ordenado, donde:

$$Q^+=\{x\in Q \mid 0<x\}$$
$$=P$$

pues

$$\frac{a}{b}\in Q^+ \iff 0<\frac{a}{b} \iff \frac{a}{b}-0\in P \iff \frac{a}{b}\in P$$

q.e.d.

Teorema (5.2.1) [unicidad]

Sean $(D,+,\cdot,0,1)$ un dominio entero y $(Q,+,\cdot,0,1)$ un campo satisfaciendo (1) y (2) del teorema anterior. Si $(K,\oplus,\odot,0,1)$ es un campo que contiene como subdominio a $(D,+,\cdot,0,1)$ y

$$K'=\{x\in K \mid x=a\cdot b^{-1} \text{ con } a,b\in D \text{ y } b\neq 0\}$$

entonces $(K',\oplus,\odot,0,1)$ es un campo tal que

$$(Q,+,\cdot,0,1)\cong(K',\oplus,\odot,0,1)$$

Particularmente, si $(K,\oplus,\odot,0,1)$ satisface (1) y (2) del teorema anterior, entonces $K=K'$.

Si adicionalmente, $\mathbb{Q}$ y K están bien ordenados por relaciones $<$ y $<$ que coinciden en D, entonces $(\mathbb{Q},+,\cdot,<,0,1) \cong (K,\oplus,\odot,<,0,1)$.

Teorema (5.23)

Existe un campo simplemente ordenado

$$(\mathbb{Q}, +, \cdot, <, 0, 1)$$

tal que

i) $(\mathbb{Z}, +, \cdot, <, 0, 1)$ es un subdominio de $(\mathbb{Q}, +, \cdot, <, 0, 1)$

ii) Para cada $x \in \mathbb{Q}$, $\exists\, a, b \in \mathbb{Z}$, $b \neq 0$ tales que:

$$x = \frac{a}{b}$$

Asimismo, cualquier otro campo que contenga a $(\mathbb{Z}, +, \cdot, <, 0, 1)$, contiene un subcampo isomorfo a $(\mathbb{Q}, +, \cdot, <, 0, 1)$

Dem:

Es consecuencia de los dos teoremas anteriores