Línuleg rakningarvensl með fastastuðlum

Inngangur

Markmiðið hér er að sýna hvernig nota má margliður til þess að leysa línuleg rakningarvensl með fastastuðla. Við munum hér gera ráð fyrir að allar tölur sem notaðar eru séu rauntölur en lengra komnir lesendur mega að setja aðrar „tölur“ í stað rauntalna. Við táknum mengi raunmargliða í breytunni x með $\mathbb{R}[x]$ og megi rautöluruna með vísmengið $\mathbb{N}(=\{0,1,2,\ldots\})$ með $\mathbb{R}^{\mathbb{N}}$. Við táknum margliður oft eins og $p(x)$ og runur yfirleitt með $(a_n)_{n\in\mathbb{N}}$. Sé $p(x)$ margliða og $n\in\mathbb{N}$ þá táknum við stuðul p við x^n með p_n. Við táknum stig margliðu $p(x)$ með $\deg(p)$, tökum sérstaklega fram að stig núllmargliðunnar er $-\infty$.

Algebra margliða

Gerum ráð fyrir að $a\in\mathbb{R}$ og $p(x),q(x)\in\mathbb{R}[x]$ séu margliður þá er $(p+q)(x)=p(x)+q(x)=\sum\limits_{n\in\mathbb{N}}(p_n+q_n)x^n$ og $(a\cdot p)(x)=a\cdot p(x)=\sum\limits_{n\in\mathbb{N}}(a\cdot p_n)x^n$. Einnig þá er $(p\cdot q)(x)=p(x)\cdot q(x)=\sum\limits_{n\in\mathbb{N}}(p(x)\cdot q(x))=\sum\limits_{n\in\mathbb{N}}\left(\sum\limits_{m=0}^{n}p_m\cdot q_{n-m}\right)x^m$. Lesandi er boðið að sannprófa eftirfarandi eiginleika:

Gerum ráð fyrir að $a,b\in\mathbb{R}$ og $p(x),q(x),r(x)\in\mathbb{R}[x]$. Þá gildir:

1. $(p+(q+r))(x)=((p+q)+r)(x)$.
2. $(p+q)(x)=(q+p)(x)$.
3. Til er margliða 0 þannig að $p(x)+0=0+p(x)=p(x)$ fyrir allar margliður $p(x)$. (Hún er ótvíræð og er kölluð núllmargliðan).
4. Fyrir sérhverja margliðu $p(x)$ þá er til margliða $q(x)$ þannig að $(p+q)(x)=(q+p)(x)=0$. (Hún er ótvíræð og er táknuð $(-p)(x)$).
5. $(p\cdot(q\cdot r))(x)=((p\cdot q)\cdot r)(x)$.
6. $(p\cdot q)(x)=(q\cdot p)(x)$.
7. Til er margliða 1 þannig að $1\cdot p(x)=p(x)\cdot 1=p(x)$ fyrir allar margliður $p(x)$. (Hún er ótvíræð og er fasta margliða 1).
8. $(p\cdot(q+r))(x)=((p\cdot q)+(p\cdot r))(x)$ og $((p+q)\cdot r)(x)=((p\cdot r)+(q\cdot r))(x)$.
9. $(1\cdot p)(x)=p(x)$.
10. $(a\cdot(p+q))(x)=((a\cdot p)+(a\cdot q))(x)$.
11. $((a+b)\cdot p)(x)=((a\cdot p)+(b\cdot p))(x)$.
12. $(a\cdot(b\cdot p))(x)=((a\cdot b)\cdot p)(x)$.
13. $((a\cdot p)\cdot q)(x)=(a\cdot(p\cdot q))(x)=(p\cdot(a\cdot q))(x)$.

Þar sem þessi skilyrði gilda þá er formlega sagt að $\mathbb{R}[x]$ sé $\mathbb{R}$- algebra.

Lesandi ætti að geta sannað að ef $a \in \mathbb{R}$ og $p(x), q(x) \in \mathbb{R}[x]$ þá er $\deg((a \cdot p)(x)) \begin{cases} \deg(p) & \text{ef } a \neq 0 \\ 0 & \text{ef } a = 0 \end{cases}$, $\deg((p \cdot q)(x)) = \deg(p(x)) + \deg(q(x))$ (þar sem $(-\infty) + n = n + (-\infty) = -\infty$ fyrir öll $n \in \mathbb{N}$ og $(-\infty) + (-\infty) = -\infty$), $\deg((p+q)(x)) \leqslant \max(\deg(p), \deg(q))$ og $\deg((p-q)(x)) \leqslant \max(\deg(p), \deg(q))$. Þar af leiðir að ef $p(x), q(x) \in \mathbb{R}[x] \backslash \{0\}$ að $\deg((p \cdot q)(x)) = \deg(p(x)) + \deg(q(x)) \geqslant 0 + 0 = 0$ svo $(p \cdot q)(x) \neq 0$. Það er $\mathbb{R}[x]$ hefur enga núlldeila.

Setning 2.1 (Setning um margliðudeilingu)**.** *Gerum ráð fyrir að $p(x), q(x) \in \mathbb{R}[x]$ og $q(x) \neq 0$. Þá eru til (ótvíræðar) margliður $d(x), r(x)$ þannig að $r(x) = 0$ eða $\deg(r(x)) < \deg(q(x))$ og $p(x) = d(x) \cdot q(x) + r(x)$.*

Sönnun. Gerum ráð fyrir að $q(x) \in \mathbb{R}[x] \backslash \{0\}$ sé gefin. Við sönnum með þrepun yfir $\deg(p(x)) \in \mathbb{N}$ að til séu $d(x), r(x) \in \mathbb{R}[x]$ þannig að $p(x) = d(x) \cdot q(x) + r(x)$.

1. Gerum ráð fyrir að $p(x) = 0$. Þá er $p(x) = d(x) \cdot q(x) + r(x)$ þar sem $d(x) = 0$ og $r(x) = p(x) = 0$.

   Gerum ráð fyrir að $p(x) \in \mathbb{R}[x]$ og $\deg(p) = 0$. Þá er $p(x) = p_0 \in \mathbb{R} \backslash \{0\}$.

   (a) Gerum ráð fyrir að $\deg(q(x)) = 0$. Þá er $q(x) = q_0 \in \mathbb{R} \backslash \{0\}$. Þá er $p(x) = p_0 = \frac{p_0}{q_0} \cdot q_0 + 0 = d(x) \cdot q(x) + r(x)$ þar sem $d(x) = \frac{p_0}{q_0}$ og $r(x) = 0$.

   (b) Gerum ráð fyrir að $\deg(q(x)) > 0$. Þá er $p(x) = 0 \cdot q(x) + p(x) = d(x) \cdot q(x) + r(x)$ þar sem $d(x) = 0$, $r(x) = p(x)$ og $\deg(r(x)) = \deg(p(x)) = 0 < \deg(q(x))$.

   Í báðum tilvikum þá má finna $d(x), r(x) \in \mathbb{R}[x]$ þannig að $r(x) = 0$ eða $\deg(r(x)) < \deg(q(x))$.

2. Gerum ráð fyrir að $n \in \mathbb{N}$ og $p(x) \in \mathbb{R}[x]$ þannig að $\deg(p(x)) = n$. Setjum sem svo að þá megi finna $d(x), r(x) \in \mathbb{R}[x]$ þannig að $p(x) = d(x) \cdot q(x) + r(x)$ þar sem $r(x) = 0$ eða $\deg(r(x)) < \deg(q(x))$.

   Gerum nú ráð fyrir að $p(x) \in \mathbb{R}[x]$ og $\deg(p(x)) = n + 1$. Þá getur tvennt gerst:

   (a) Gerum ráð fyrir að $\deg(p(x)) < \deg(q(x))$. Þá er $p(x) = 0 \cdot q(x) + p(x) = d(x) \cdot q(x) + r(x)$ þar sem $d(x) = 0$, $r(x) = p(x)$ og $\deg(r(x)) = \deg(p(x)) < \deg(q(x))$.

   (b) Gerum ráð fyrir að $\deg(p(x)) \geqslant \deg(q(x))$. Gerum ráð fyrir að $m = \deg(q)$. Látum $p_1(x) = p(x) - \frac{p_{n+1}}{q_m} x^{n+1-m} q(x)$. Nú er $\deg(p) = n+1$ og $\deg\left(\frac{p_{n+1}}{q_m} x^{n+1-m} q(x)\right) 0 \deg(x^{n+1-m}) + \deg(q(x) = (n+1-m) + m = n+1$. Þar af leiðir að $\deg(p_1(x)) \leqslant \max\left(\deg(p(x), \deg\left(\frac{p_{n+1}}{q_m} x^{n+1-m} q(x)\right)\right) = \max(n+1, n+1) = n+1$. Nú er $p_{1,n+1} = p_{n+1} - \left(\frac{p_{n+1}}{q_m} x^{n+1-m} q(x)\right)_{n+1} = p_{n+1} - \frac{p_{n+1}}{q_m} \cdot q_m = 0$. Þar af leiðir að $\deg(p_1) < n+1$ það er $\deg(p_1) \leqslant n$.

   Af þrepunarforsendu þá eru til margliður $d_1(x), r(x)$ þannig að $r_1(x) = 0$ eða $\deg(r_1(x)) < \deg(q(x))$ og $p_1(x) = d_1(x) \cdot q(x) + r(x)$. Látum $q(x) = \frac{p_{n+1}}{q_m} x^{n+1-m} + q_1(x)$. Þá fæst:

$$\begin{aligned} p(x) &= \frac{p_{n+1}}{q_m} x^{n+1-m} \cdot q(x) + p_1(x) \\ &= \frac{p_{n+1}}{q_m} x^{n+1-m} \cdot q(x) + (d_1(x) \cdot q(x) + r(x)) \\ &= \left(\frac{p_{n+1}}{q_m} x^{n+1-m} + d_1(x)\right) \cdot q(x) + r(x) \\ &= d(x) \cdot q(x) + r(x) \end{aligned}$$

   Í báðum tilvikum fæst að til eru margliður $d(x), r(x)$ þannig að $r(x) = 0$ eða $\deg(r(x)) < \deg(q(x))$ og $p(x) = d(x) \cdot q(x) + r(x)$.

Með þrepun fæst að fyrir allar margliður $p(x)$ þá eru til margliður $d(x), r(x)$ þannig að $r(x) = 0$ eða $\deg(r(x)) < \deg(q(x))$.

Gerum nú ráð fyrir að $d(x), d_1(x), r(x), r_1(x)$ séu margliður þannig að $r(x) = 0$ eða $\deg(r(x)) < \deg(q(x))$, $r_1(x) = 0$ eða $\deg(r_1(x)) < \deg(q(x))$, $p(x) = d(x) \cdot q(x) + r(x)$ og $p(x) = d_1(x) \cdot q(x) + r_1(x)$. Þá fæst:

$$(d(x) - d_1(x)) \cdot q(x) = d(x) \cdot q(x) - d_1(x) \cdot q(x) = r_1(x) - r(x)$$

Sér í lagi þá er $\deg((d(x) - d_1(x)) \cdot q(x)) = \deg(r_1(x) - r(x))$.

Nú er $\deg((d(x) - d_1(x)) \cdot q(x)) = \deg(d(x) - d_1(x)) + \deg(q(x))$ svo $\deg((d(x) - d_1(x)) \cdot q(x)) \geqslant \deg(q(x))$ ef $d(x) - d_1(x) \neq 0$. Svo er $\deg(r_1(x) - r(x)) \leqslant \max(\deg(r_1(x)), \deg(r(x))) < \max(\deg(q), \deg(q)) = \deg(q)$. Þar af leiðir að ef $d(x) - d_1(x) \neq 0$ þá er $\deg((d(x) - d_1(x)) \cdot q(x)) \geqslant \deg(q(x)) > \deg(r_1(x) - r(x))$ sem er mótsögn. Við ályktum að $d(x) - d_1(x) = 0$ og því $r_1(x) - r(x) = (d(x) - d_1(x)) \cdot q(x) = 0$. Það er $d(x) = d_1(x)$ og $r(x) = r_1(x)$. Þetta sýnir að $d(x)$ og $r(x)$ eru ótvírætt ákvörðuð. □

Gerum ráð fyrir að $p(x), q(x) \in \mathbb{R}[x]$. Við segjum að $q(x)$ gangi upp í margliðu $p(x)$ ef til er $d(x) \in \mathbb{R}[x]$ þannig að $p(x) = d(x) \cdot q(x)$. Ef $q(x)$ gengur upp í margliðu $p(x)$ þá ritum við $q(x) \mid p(x)$.

Við höfum eftirfarandi setningu sem lesandi má spreyta sig á að sanna:

Setning 2.2. *Gerum ráð fyrir að $a, b \in \mathbb{R}$ og $p(x), q(x), r(x) \in \mathbb{R}[x]$. Þá gildir:*

1. $p(x) \mid p(x)$.
2. *Ef $p(x) \neq 0$ og $p(x) \mid q(x)$ þá er $q(x) = 0$ eða $\deg(p(x)) \leqslant \deg(q(x))$.*
3. *Ef $p(x) \mid q(x)$ og $q(x) \mid r(x)$ þá $p(x) \mid r(x)$.*
4. *Ef $p(x) \mid q(x)$ og $q(x) \mid p(x)$ þá er til $a \in \mathbb{R}\backslash\{0\}$ þannig að $q(x) = a \cdot p(x)$.*
5. *Ef $p(x) \mid q(x)$ og $p(x) \mid r(x)$ þá $p(x) \mid (q + r)(x)$.*
6. *Ef $p(x) \mid q(x)$ þá $p(x) \mid (a \cdot q)(x)$.*
7. *Ef $p(x) \mid q(x)$ þá $(a \cdot p)(x) \mid (a \cdot q)(x)$ og $(r \cdot p)(x) \mid (r \cdot q)(x)$.*
8. *$1 \mid p(x)$ fyrir allar margliður $p(x) \in \mathbb{R}[x]$.*
9. *Ef $p(x) \mid 1$ þá er $\deg(p(x)) = 0$, það er $p(x) = a$ fyrir $a \in \mathbb{R}\backslash\{0\}$.*
10. *$p(x) \mid 0$ fyrir allar margliður $p(x) \in \mathbb{R}[x]$.*
11. *Ef $0 \mid p(x)$ þá er $p(x) = 0$.*
12. *Ef $p(x) \mid q(x)$ og $q(x) \mid p(x)$ þá er til $a \in \mathbb{R}\backslash\{0\}$ þannig að $q(x) = (a \cdot p)(x)$.*
13. *Ef $p(x), q(x) \in \mathbb{R}[x]$ og $q(x) \neq 0$ þá er til ótvírætt margliða $r(x) \in \mathbb{R}[x]$ þannig að $\deg(r(x)) < \deg(q(x))$ og $q(x) \mid (p - r)(x)$.*

Sönnun. Sönnun er eftirlátin lesanda. □

Gerum ráð fyrir að $p(x), q(x) \in \mathbb{R}[x]$. Við setjum að $d(x) \in \mathbb{R}[x]$ sé stærsti samdeilir $p(x)$ og $q(x)$ ef $d(x) \mid p(x)$, $d(x) \mid q(x)$ og ef $d_1(x) \in \mathbb{R}[x]$ þannig að $d_1(x) \mid p(x)$, $d_1(x) \mid q(x)$ þá $d_1(x) \mid d(x)$.

Hjálparsetning 2.1. *Gerum ráð fyrir að $p(x), q(x), d(x), d_1(x) \in \mathbb{R}[x]$ og $d(x)$ og $d_1(x)$ séu stærstu samdeilar $p(x)$ og $q(x)$. Þá er til $a \in \mathbb{R}\backslash\{0\}$ þannig að $d_1(x) = (a \cdot d)(x)$.*

Eins er $(a \cdot d)(x)$ stærsti samdeilir $p(x)$ og $q(x)$ ef $a \in \mathbb{R}\backslash\{0\}$ og $d(x)$ er stærsti samdeilir $p(x)$ og $q(x)$.

Sönnun. Gerum ráð fyrir að $p(x), q(x), d(x), d_1(x) \in \mathbb{R}[x]$ og $d(x)$ og $d_1(x)$ séu stærstu samdeilar $p(x)$ og $q(x)$. Þá $d(x) \mid d_1(x)$ og $d_1(x) \mid d(x)$ svo til er $a \in \mathbb{R}\backslash\{0\}$ þannig að $d_1(x) = (a \cdot d)(x)$.

Gerum nú ráð fyrir að $d(x)$ sé stærsti samdeilir $p(x)$ og $q(x)$ og $a \in \mathbb{R}\backslash\{0\}$. Setjum $d_1(x) = (a \cdot d)(x)$. Þá er $(a^{-1} \cdot d_1)(x) = (a^{-1} \cdot (a \cdot d))(x) = ((a^{-1} \cdot a) \cdot d)(x) = (1 \cdot d)(x) = d(x)$. Þetta sýnir að $d(x) | d_1(x)$ og $d_1(x) \mid d(x)$.

Þar sem $d_1(x) \mid d(x)$, $d(x) \mid p(x)$ og $d(x) \mid q(x)$ þá $d_1(x) \mid p(x)$ og $d_1(x) \mid q(x)$. Gerum nú ráð fyrir að $c(x) \in \mathbb{R}[x]$ og $c(x) \mid p(x)$ og $c(x) \mid q(x)$. Þar sem $d(x)$ er stærsti samdeilir $p(x)$ og $q(x)$ þá $c(x) \mid d(x)$. Þar sem $d(x) \mid d_1(x)$ þá $c(x) \mid d_1(x)$. Það þýðir að $d_1(x)$ er stærsti samdeilir $p(x)$ og $q(x)$. □

Við sjáum því að ef $p(x), q(x) \in \mathbb{R}$ þá er 0 stærsti samdeilir $p(x)$ og $q(x)$ eða til er stöðluð (forystustuðullin er 1) margliða $d(x)$ sem er stærsti samdeilir $p(x)$ og $q(x)$.

Við höfum reyndar ekki sannað tilvist stærsta samdeilis margliða. Við bætum nú úr því.

Hjálparsetning 2.2. *Gerum ráð fyrir að $I \subseteq \mathbb{R}[x]$ þannig að $0 \in I$, $(p+q)(x) \in I$ ef $p(x), q(x) \in I$ og $(a \cdot p(x)) \in I$ ef $a \in \mathbb{R}$ og $p(x) \in I$. Þá er til $d(x) \in \mathbb{R}[x]$ þannig að $I = d(x) \cdot \mathbb{R}[x] \coloneqq \{d(x) \cdot s(x) \mid s(x) \in \mathbb{R}[x]\}$.*

Sönnun. Gerum ráð fyrir að $I \subseteq \mathbb{R}[x]$ þannig að $0 \in I$, $(p+q)(x) \in I$ ef $p(x), q(x) \in I$ og $(a \cdot p(x)) \in I$ ef $a \in \mathbb{R}$ og $p(x) \in I$. Skiptum í tvö tilvik:

1. Gerum ráð fyrir að $I = \{0\}$. Þá er $I\{0\} = \{0 \cdot s(x) \mid s(x) \in \mathbb{R}[x]\} = 0 \cdot \mathbb{R}[x]$.

2. Gerum ráð fyrir að $I \neq \{0\}$. Þar sem $0 \in I$ þá er $I\backslash\{0\} \neq \varnothing$. Þá er $\deg[I\backslash\{0\}] \subseteq \mathbb{N}$ og $\deg[I\backslash\{0\}] \neq \varnothing$. Því hefur $\deg[I\backslash\{0\}]$ minnsta stak. Gerum ráð fyrir að $d(x) \in I\backslash\{0\}$ þannig að $\deg(d(x)) = \min(\deg[I\backslash\{0\}])$. Sér í lagi þá er $d(x) \neq 0$.

   Setjum sem svo að $p(x) \in I$. Af hjálparsetningu 2.1 leiðir að til eru margliður $q(x), r(x)$ þannig að $\deg(r(x)) < \deg(d(x))$ og $p(x) = q(x) \cdot d(x) + r(x)$. Þar sem $d(x) \in I$ þá er $((-q) \cdot d)(x) \in I$. Þar sem $p(x)$ og $((-q) \cdot d)(x) \in I$ þá er $r(x) = (p + ((-q) \cdot d))(x) \in I$. Ef $r(x) \neq 0$ þá er $r \in I\backslash\{0\}$ en þá er $\deg(r(x)) < \deg(d(x)) = \min(\deg[I\backslash\{0\}])$ sem er mótsögn við það að $\deg(r(x)) \in \deg[I\backslash\{0\}]$. Við ályktum því að $r(x) = 0$. Það er $p(x) = q(x) \cdot d(x) = d(x) \cdot q(x) \in d(x) \cdot \mathbb{R}[x]$.

Í báðum tilvikum þá fæst að til er $d(x) \in \mathbb{R}[x]$ þannig að $I = d(x) \cdot \mathbb{R}[x]$. □

Setning 2.3. *Gerum ráð fyrir að $p(x), q(x) \in \mathbb{R}[x]$. Þá hafa $p(x)$ og $q(x)$ stærsta samdeili $d(x) \in \mathbb{R}[x]$ og finna má margliður $a(x), b(x) \in \mathbb{R}[x]$ þannig að $d(x) = a(x) \cdot p(x) + b(x) \cdot q(x)$.*

Sönnun. Gerum ráð fyrir að $p(x), q(x) \in \mathbb{R}[x]$. Látum $I = p(x) \cdot \mathbb{R}[x] + q(x) \cdot \mathbb{R}[x] = \{a(x) \cdot p(x) + b(x) \cdot q(x) \mid a(x), b(x) \in \mathbb{R}[x]\}$. Athugum nú:

1. $0 = 0 \cdot p(x) + 0 \cdot q(x) \in I$.

2. Gerum ráð fyrir að $c_1(x), c_2(x) \in I$. Þá eru til $a_1(x), a_2(x), b_1(x), b_2(x) \in \mathbb{R}[x]$ þannig að $c_1(x) = a_1(x) \cdot p(x) + b_1(x) \cdot q(x)$ og $c_2(x) = a_2(x) \cdot p(x) + b_2(x) \cdot q(x)$. Þá fæst:

$$\begin{aligned} c_1(x) + c_2(x) &= (a_1(x) \cdot p(x) + b_1(x) \cdot q(x)) + (a_2(x) \cdot p(x) + b_2(x) \cdot q(x)) \\ &= (a_1(x) + a_2(x)) \cdot p(x) + (b_1(x) + b_2(x)) \cdot q(x) \in I \end{aligned}$$

3. Gerum ráð fyrir að $s \in \mathbb{R}$ og $c(x) \in I$. Þá eru til $a(x), b(x) \in \mathbb{R}[x]$ þannig að $c(x) = a(x) \cdot p(x) + b(x) \cdot q(x)$. Þá er

$$s \cdot c(x) = s \cdot (a(x) \cdot p(x) + b(x) \cdot q(x)) = (s \cdot a(x)) \cdot p(x) + (s \cdot b(x)) \cdot q(x) \in I$$

Af hjálparsetningu 2.2 leiðir að til er $d(x) \in \mathbb{R}[x]$ þannig að $I = d(x) \cdot \mathbb{R}[x]$. Þar sem $d(x) = d(x) \cdot 1 \in d(x) \cdot \mathbb{R}[x] = I$ þá er ljóst að $d(x) \in I$. Því má finna $a(x), b(x) \in \mathbb{R}[x]$ þannig að $d(x) = a(x) \cdot p(x) + b(x) \cdot q(x)$. Eins er $p(x) = p(x) \cdot 1 + q(x) \cdot 0 \in I$ og $q(x) = p(x) \cdot 0 + q(x) \cdot 1 \in I$.

Skiptum í tilvik:

1. Gerum ráð fyrir að $d(x) = 0$. Þá er $I = d(x) \cdot \mathbb{R}[x] = 0 \cdot \mathbb{R}[x] = \{0\}$. Þar sem $p(x), q(x) \in I$ þá er $p(x) = q(x) = 0$ og því ljóst að $d(x) \mid p(x)$ og $d(x) \mid q(x)$.

2. Gerum ráð fyrir að $d(x) \neq 0$. Af setningu 2.1 leiðir að til eru margliður $q(x), r(x) \in \mathbb{R}[x]$ þannig að $\deg(r(x)) < \deg(d(x))$ og $p(x) = q(x) \cdot d(x) + r(x)$. Þar sem $d(x) \in I$ þá er $(-q)(x) \cdot d(x) \in I$. Þar sem $p(x) \in I$ þá er $r(x) = p(x) + (-q)(x) \cdot d(x) \in I = d(x) \cdot \mathbb{R}[x]$. Því er til $s(x) \in \mathbb{R}[x]$ þannig að $r(x) = d(x) \cdot s(x)$. Ef $s(x) \neq 0$ þá er $\deg(d(x)) \leqslant \deg(d(x)) + \deg(s(x)) = \deg(d(x) \cdot s(x)) = \deg(r(x)) < \deg(d(x))$ en það er mótsögn. Við ályktum að $s(x) = 0$ og því $r(x) = d(x) \cdot s(x) = d(x) \cdot 0 = 0$. Þar af leiðir að $p(x) = q(x) \cdot d(x)$, það er $d(x) \mid p(x)$.

   Með sama hætti sést að $d(x) \mid q(x)$.

Í báðum tilvikum fæst að $d(x) \mid p(x)$ og $d(x) \mid q(x)$.

Gerum nú ráð fyrir að $c(x) \in \mathbb{R}[x]$ þannig að $c(x) \mid p(x)$ og $c(x) \mid q(x)$. Af setningu 2.2 leiðir að $c(x) \mid a(x) \cdot p(x) + b(x) \cdot q(x) = d(x)$. Þetta sýnir að $d(x)$ er stærsti samdeilir $p(x)$ og $q(x)$. □

Við höfum því sannað að stærsti samdeilir $d(x)$ tveggja margliða $p(x), q(x)$ er alltaf til og finna má margliður $a(x), b(x) \in \mathbb{R}[x]$ þannig að $d(x) = a(x) \cdot p(x) + b(x) \cdot q(x)$. Lesandi getur spreytt sig á því að finna reiknirit til þess að finna slíkar margliður $a(x), b(x), d(x)$ fyrir gefnar margliður $p(x), q(x)$.

Ef $p(x), q(x) \in \mathbb{R}[x]$ þá segjum við að $p(x)$ og $q(x)$ séu ósamþátta ef ef 1 er stærsti samdeilir þeirra. Við sönnum nú mikilvægar hjálparsetningar:

Hjálparsetning 2.3. *Gerum ráð fyrir að $p(x), q(x), r(x) \in \mathbb{R}[x]$. Þá gildir:*

1. *Gerum ráð fyrir að $d(x) \in \mathbb{R}[x]$ sé stærsti samdeilir $p(x)$ og $q(x)$. Þá eru til ósamþátta margliður $p_1(x), q_1(x)$ þannig að $p(x) = p_1(x) \cdot d(x)$ og $q(x) = q_1(x) \cdot d(x)$.*

2. *Gerum ráð fyrir að $p(x)$ og $q(x)$ séu ósamþátta og $r(x) \in \mathbb{R}[x]$ þannig að $p(x) \mid q(x) \cdot r(x)$. Þá $p(x) \mid r(x)$.*

3. *Gerum ráð fyrir að $p(x)$ og $q(x)$ séu ósamþátta og $p(x)$ og $r(x)$ séu ósamþátta, þá eru $p(x)$ og $q(x) \cdot r(x)$ ósamþátta.*

4. *Gerum ráð fyrir að $p(x), q(x), r(x) \in \mathbb{R}[x]$, $p(x)$ og $q(x)$ séu ósamþátta, $p(x) \mid r(x)$ og $q(x) \mid r(x)$. Þá $p(x) \cdot q(x) \mid r(x)$.*

Sönnun. Gerum ráð fyrir að $p(x), q(x) \in \mathbb{R}[x]$. Fáum nú:

1. Gerum ráð fyrir að $d(x) \in \mathbb{R}[x]$ sé stærsti samdeilir $p(x)$ og $q(x)$. Skiptum í tvö tilvik:

   (a) Gerum ráð fyrir að $d(x) = 0$. Þar sem $0 = d(x) \mid p(x)$ og $0 = d(x) \mid q(x)$ þá leiðir af setingu 2.2 að $p(x) = q(x) = 0$. Þá er $p(x) = 0 = 1 \cdot 0 = p_1(x) \cdot d(x)$ þar sem $d_1(x) = 1$. Eins er $q(x) = q_1(x) \cdot d(x)$ þar sem $q_1(x) = 1$. Nú $1 \mid p_1(x)$, $1 \mid q_1(x)$ og ef $c(x) \mid p(x) = 1$, $c(x) \mid q(x) = 1$ þá leiðir af setningu 2.2 að $c(x) = c_0$ þar sem $c_0 \in \mathbb{R} \backslash \{0\}$. Þá er $1 = {c_0}^{-1} \cdot c(x)$ svo $c(x) \mid 1$. Það er 1 er stærsti samdeilir $p_1(x)$ og $q_1(x)$.

   (b) Gerum ráð fyrir að $d(x) \neq 0$. Þar sem $d(x)$ er stærsti samdeilir $p(x)$ og $q(x)$ þá $d(x) \mid p(x)$ og $d(x) \mid q(x)$. Það er til eru $p_1(x), q_1(x) \in \mathbb{R}[x]$ þannig að $p(x) = p_1(x) \cdot d(x)$ og $q(x) = q_1(x) \cdot d(x)$. Gerum ráð fyrir að $c(x)$ sé stærsti samdeilir $p_1(x)$ og $q_1(x)$. Þá $c(x) \mid p_1(x)$ og $c(x) \mid q_1(x)$. Af setningu 2.2 leiðir að $c(x) \cdot d(x) \mid p_1(x) \cdot d(x) = p(x)$ og $c(x) \cdot d(x) \mid q_1(x) \cdot d(x) = q(x)$. Þar sem $d(x)$ er stærsti samdeilir $p(x)$ og $q(x)$ þá fæst að $c(x) \cdot d(x) \mid d(x)$. Það er, til er $s(x) \in \mathbb{R}[x]$ þannig að $d(x) = s(x) \cdot c(x) \cdot d(x)$. Með öðrum orðum $(1 - s(x) \cdot c(x)) \cdot d(x) = 0$. Þar sem $d(x) \neq 0$ þá er $1 - s(x) \cdot c(x) = 0$. Það er $1 = s(x) \cdot c(x)$ en það þýðir $c(x) \mid 1$.

   Ljóst er að $1 \mid p_1(x)$ og $1 \mid q_1(x)$. Gerum ráð fyrir að $t(x) \in \mathbb{R}[x]$ þannig að $t(x) \mid p_1(x)$ og $t(x) \mid q_1(x)$. Þar sem $c(x)$ er stærsti samdeilir $p_1(x)$ og $q_1(x)$ þá $t(x) \mid c(x)$. Þar sem $c(x) \mid 1$ þá $t(x) \mid 1$. Þetta sýnir að 1 er stærsti samdeilir $p_1(x)$ og $q_1(x)$.

Í báðum tilvikum þá má finna ósamþátta $p_1(x), q_1(x) \in \mathbb{R}[x]$ þannig að $p(x) = p_1(x) \cdot d(x)$ og $q(x) = q_1(x) \cdot d(x)$.

2. Gerum ráð fyrir að $p(x), q(x) \in \mathbb{R}[x]$ séu ósamþátta og $r(x) \in \mathbb{R}[x]$ þannig að $p(x) \mid q(x) \cdot r(x)$.

   Þar sem $p(x)$ og $q(x)$ eru ósamþátta þá er 1 stærsti samdeilir þeirra og af setningu 2.3 leiðir að til eru $a(x), b(x) \in \mathbb{R}[x]$ þannig að $1 = a(x) \cdot p(x) + b(x) \cdot q(x)$. Þar sem $p(x) \mid p(x)$ þá $p(x) \mid a(x) \cdot r(x) \cdot p(x)$ og þar sem $p(x) \mid q(x) \cdot r(x)$ þá $p(x) \mid r(x) \cdot b(x) \cdot q(x)$. Því fæst:

$$\begin{aligned} p(x) &\mid a(x) \cdot r(x) \cdot p(x) + r(x) \cdot b(x) \cdot q(x) \\ &= r(x) \cdot (a(x) \cdot p(x) + b(x) \cdot q(x)) \\ &= r(x) \cdot 1 \\ &= r(x) \end{aligned}$$

   Það er $p(x) \mid r(x)$.

3. Gerum ráð fyrir að $p(x)$ og $q(x)$ séu ósamþátta og $p(x)$ og $r(x)$ séu ósamþátta. Ljóst er að $1 \mid p(x)$ og $1 \mid q(x) \cdot r(x)$.

   Gerum ráð fyrir að $c(x) \in \mathbb{R}[x]$ þannig að $c(x) \mid p(x)$ og $c(x) \mid q(x) \cdot r(x)$. Þar sem $c(x) \mid q(x) \cdot r(x)$ þá er til $a(x) \in \mathbb{R}[x]$ þannig að $a(x) \cdot c(x) = q(x) \cdot r(x)$. Þá $q(x) \cdot r(x) = a(x) \cdot c(x) \mid a(x) \cdot p(x)$. Þar sem $p(x)$ og $q(x)$ eru ósamþátta og $q(x) \mid a(x) \cdot q(x)$ þá fæst af síðasta lið að $q(x) \mid a(x)$. Því er til $b(x) \in \mathbb{R}[x]$ þannig að $a(x) = b(x) \cdot q(x)$. Því fæst að $q(x) \cdot r(x) = a(x) \cdot c(x) = b(x) \cdot q(x) \cdot c(x)$. Það er $q(x) \cdot (r(x) - b(x) \cdot c(x)) = 0$. Þá er $q(x) = 0$ eða $r(x) - b(x) \cdot c(x) = 0$.

   (a) Gerum ráð fyrir að $q(x) = 0$. Þá er $p(x)$ og 0 ósamþátta og þar sem $q(x) \cdot r(x) = 0$ þá eru $p(x)$ og $q(x) \cdot r(x)$ ósamþátta, sér í lagi þá $r(x) \mid 1$.

   (b) Gerum ráð fyrir að $r(x) - b(x) \cdot c(x) \neq 0$, það er $r(x) = b(x) \cdot c(x)$. Því $c(x) \mid r(x)$ en þar sem $c(x) \mid p(x)$ og $p(x)$ og $r(x)$ eru ósamþátta þá $c(x) \mid 1$.

   Í báðum tilvikum fæst að $c(x) \mid 1$.

   Þetta sýnir að 1 er stærsti samdeilir $p(x)$ og $q(x) \cdot r(x)$. Það er $p(x)$ og $q(x) \cdot r(x)$ eru ósamþátta.

4. Gerum ráð fyrir að $p(x), q(x), r(x) \in \mathbb{R}[x]$, $p(x)$ og $q(x)$ séu ósamþátta, $p(x) \mid r(x)$ og $q(x) \mid r(x)$. Þar sem $p(x) \mid r(x)$ þá er til $s(x) \in \mathbb{R}[x]$ þannig að $r(x) = s(x) \cdot p(x)$. Nú $q(x) \mid r(x) = s(x) \cdot p(x)$. Þar sem $q(x)$ og $p(x)$ eru ósamþátta þá leiðir af fyrri lið að $q(x) \mid s(x)$. Því er til $t(x) \in \mathbb{R}[x]$ þannig að $s(x) = t(x) \cdot q(x)$.

   Við höfum því $r(x) = s(x) \cdot p(x) = t(x) \cdot q(x) \cdot p(x) 0 t(x) \cdot p(x) \cdot q(x)$. Það er $p(x) \cdot q(x) \mid r(x)$.

□

Gerum ráð fyrir að $p(x) \in \mathbb{R}[x]$ og $\deg(p(x)) > 0$. Sagt er að $p(x)$ sé óþáttanleg ef fyrir margliður $s(x), t(x) \in \mathbb{R}[x]$ þannig að $p(x) = s(x) \cdot t(x)$ þá er $\deg(s(x)) = 0$ eða $\deg(t(x)) = 0$. Ljóst er að allar fyrsta stig margliður $p(x)$ eru óþáttanlegar þar sem ef $s(x), t(x) \in \mathbb{R}[x]$, $\deg(s(x)), \deg(t(x)) > 0$ þá er $\deg(s(x) \cdot t(x)) \geqslant \deg(s(x)) + \deg(t(x)) \geqslant 1 + 1 = 2 > \deg(p(x))$.

Gerum ráð fyrir að $p(x) \in \mathbb{R}[x]$ og $\deg(p(x)) > 0$. Við segjum að $p(x)$ sé frummargliða ef fyrir allar margliður $a(x), b(x)$ þannig að $p(x) \mid a(x) \cdot b(x)$ þá $p(x) \mid a(x)$ eða $p(x) \mid b(x)$. Það kemur í ljóst að óþáttanlegar margliður eru nákvæmlega frummargliðurnar.

Hjálparsetning 2.4. *Gerum ráð fyrir að $p(x) \in \mathbb{R}[x]$. Þá er $p(x)$ óþáttanleg ef og aðeins ef $p(x)$ er frummargliða.*

Sönnun. Gerum ráð fyrir að $p(x) \in \mathbb{R}[x]$.

1. Gerum ráð fyrir að $p(x)$ sé frummargliða. Þá er $\deg(p(x)) > 0$. Gerum ráð fyrir að $p(x) = s(x) \cdot t(x)$ þar sem $s(x), t(x) \in \mathbb{R}[x]$. Þá $s(x) \mid p(x)$ og $t(x) \mid p(x)$. Þar sem $p(x) \mid p(x) = s(x) \cdot t(x)$ og þar sem $p(x)$ er frumargliða þá deilir $p(x)$ annari af $s(x)$ og $t(x)$.

   (a) Gerum ráð fyrir að $p(x) \mid s(x)$. Þar sem $p(x) \mid s(x)$ og $s(x) \mid p(x)$ þá leiðir af setningu 2.2 að til er $a \in \mathbb{R}\backslash\{0\}$ þannig að $p(x) = a \cdot s(x)$. Því fæst:

   $$0 = p(x) - p(x) = t(x) \cdot s(x) - a \cdot s(x) = (t(x) - a) \cdot s(x)$$

   Þá er $t(x) - a = 0$ eða $s(x) = 0$. Ef $s(x) = 0$ þá er $p(x) = s(x) \cdot t(x) = 0$ sem er í mótsögn við forsenduna að $p(x) \neq 0$. Við ályktum að $t(x) - a = 0$, það er $t(x) = a$.

   (b) Eins fæst að ef $p(x) \mid t(x)$ að til sé $a \in \mathbb{R}\backslash\{0\}$ þannig að $s(x) = a$.

   Þetta sýnir $p(x)$ er óþáttanleg.

2. Gerum ráð fyrir að $p(x)$ sé óþáttanleg. Þá er $\deg(p(x)) > 0$. Setjum sem svo að $q(x), r(x) \in \mathbb{R}[x]$ þannig að $p(x) \mid q(x) \cdot r(x)$. Gerum ráð fyrir að $p(x) \nmid q(x)$.

   Látum $d(x)$ vera stærsta samdeili $p(x)$ og $q(x)$. Þar sem $d(x) \mid p(x)$ þá er til $s(x) \in \mathbb{R}[x]$ þannig að $p(x) = s(x) \cdot d(x)$. Þar sem $p(x)$ er óþáttanleg þá er $\deg(d(x)) = 0$ eða $\deg(s(x)) = 0$.

   Ef $\deg(s(x)) = 0$ þá er $s(x) = s_0$ þar sem $s_0 \in \mathbb{R}\backslash\{0\}$. Þetta sýnir að $d(x) = {s_0}^{-1} \cdot s_0 \cdot d(x) = {s_0}^{-1} \cdot p(x)$, það er $p(x) \mid d(x)$. Þar sem $d(x) \mid q(x)$ þá $p(x) \mid q(x)$ í mótsögn við forsendu. Við ályktum að $\deg(s(x)) \neq 0$ og því $\deg(d(x)) = 0$.

   Þetta sýnir að $p(x)$ og $q(x)$ eru ósamþátta. Þar sem $p(x)$ og $q(x)$ eru ósamþátta og $p(x) \mid q(x) \cdot r(x)$ þá leiðir af hjálparsetningu 2.3 að $p(x) \mid r(x)$.

   Við höfum því sýnt að ef $p(x) \mid s(x) \cdot r(x)$ fyrir margliður $q(x), r(x) \in \mathbb{R}[x]$ þá $p(x) \mid q(x)$ eða $p(x) \mid r(x)$, það er $p(x)$ er frummargliða.

□

Við getum nú sannað setningu um frumþáttun margliða:

Setning 2.4. *Gerum ráð fyrir að $p(x) \in \mathbb{R}[x]\backslash\{0\}$. Þá er til $m \in \mathbb{N}$ og frummargliður $q_1(x), q_2(x), \ldots, q_m(x)$ þannig og fasti $a \in \mathbb{R}\backslash\{0\}$ að*

$$p(x) = a \cdot q_1(x) \cdot q_2(x) \cdots q_m(x)$$

Sönnun. Gerum ráð fyrir að til sé margliða $p(x) \in \mathbb{R}[x]\backslash\{0\}$ sem ekki má skrifa sem margfeldi óþáttanlegra margliða og fasta. Þá er til margliða $p(x) \in \mathbb{R}[x]\backslash\{0\}$ af lægsta stigi sem ekki má skrifa sem margfeldi af óþáttanlegum margliðum.

Ef $\deg(p(x)) = 0$ þá er $p(x) = a$, þar sem $a \in \mathbb{R}\backslash\{0\}$ og því er $p(x) = a$ leið til þess að skrifa $p(x)$ sem margfeldi af (engum) óþáttanlegum margliðum og fasta. Ef $\deg(p(x)) > 0$ og $p(x)$ er óþáttanleg þá er $p(x) = 1 \cdot p(x)$ leið til þess að skrifa $p(x)$ sem margfeldi af óþáttanlegum margliðum og fasta.

Gerum næst ráð fyrir að $\deg(p(x)) > 0$ og $p(x)$ sé ekki óþáttanleg. Þá eru til margliður $s(x), t(x) \in \mathbb{R}[x]\backslash\{0\}$ þannig að $0 < \deg(s(x)), \deg(t(x)) < \deg(p(x))$. Þar sem $\deg(s(x)) < \deg(p(x))$ og $\deg(t(x)) < \deg(p(x))$ þá má finna $m, n \in \mathbb{N}$, óþáttanlegar margliður $q_1(x), q_2(x), \ldots, q_m(x)$, $r_1(x), r_2(x), \ldots, r_n(x)$ ásamt föstum $a, b \in \mathbb{R}\backslash\{0\}$ þannig að $s(x) = a \cdot q_1(x) \cdot q_2(x) \cdots q_m(x)$ og $t(x) = b \cdot r_1(x) \cdot r_2(x) \cdots r_n(x)$. Því er:

$$p(x) = s(x) \cdot t(x) = (a \cdot b) \cdot q_1(x) \cdot q_2(x) \cdots q_m(x) \cdot r_1(x) \cdot r_2(x) \cdots r_n(x)$$

Í öllum tilvikum fæst að rita má $p(x)$ sem margfeldi af fasta og óþáttanlegum margliðum en það er í mótsögn við forsendu. Við ályktum að forsendan að til sé margliða $p(x) \in \mathbb{R}[x]\backslash\{0\}$ sem ekki má skrifa sem margfeldi fasta og óþáttanlegra margliða sé röng.

Fyrir sérhverja margliðu $p(x) \in \mathbb{R}[x]\backslash\{0\}$ þá má finna $m \in \mathbb{N}$, fasta $a \in \mathbb{R}\backslash\{0\}$ og óþáttanlegar (og því einnig frummargliður samkvæmt hjálparsetning 2.4) margliður $q_1(x), q_2(x), \ldots, q_m(x)$ þannig að

$$p(x) = a \cdot q_1(x) \cdot q_2(x) \cdots q_m(x)$$

□

Gerum ráð fyrir að $p(x), q(x), d(x) \in \mathbb{R}[x]$. Við segjum að $p(x)$ sé samleifa $q(x)$ mát (e. modulus) $d(x)$ ef $d(x) \mid (q(x) - p(x))$. Ef $p(x)$ og $q(x)$ eru samleifa mát $d(x)$ þá ritum við $p(x) \equiv q(x) \mod d(x)$. Við höfum eftirfarandi:

Setning 2.5. *Eftirfarandi gildir:*

1. *Ef* $p(x), d(x) \in \mathbb{R}[x]$ *þá* $p(x) \equiv p(x) \mod d(x)$.
2. *Ef* $p(x), q(x), d(x) \in \mathbb{R}[x]$ *og* $p(x) \equiv q(x) \mod d(x)$ *þá* $q(x) \equiv p(x) \mod d(x)$.
3. *Ef* $p(x), q(x), r(x), d(x) \in \mathbb{R}[x]$, $p(x) \equiv q(x) \mod d(x)$ *og* $q(x) \equiv r(x) \mod d(x)$ *þá* $p(x) \equiv r(x) \mod d(x)$.
4. $p(x) \equiv 0 \mod p(x)$.
5. *Ef* $a \in \mathbb{R}$, $p(x), q(x), d(x) \in \mathbb{R}[x]$ *og* $p(x) \equiv q(x) \mod d(x)$ *þá* $a \cdot p(x) \equiv a \cdot q(x) \mod d(x)$.
6. *Ef* $p(x), q(x), r(x), s(x), d(x) \in \mathbb{R}[x]$, $p(x) \equiv r(x) \mod d(x)$ *og* $q(x) \equiv s(x) \mod d(x)$ *þá* $p(x) + q(x) \equiv r(x) + s(x) \mod d(x)$.
7. *Ef* $p(x), q(x), r(x), s(x), d(x) \in \mathbb{R}[x]$, $p(x) \equiv r(x) \mod d(x)$ *og* $q(x) \equiv s(x) \mod d(x)$ *þá* $p(x) \cdot q(x) \equiv r(x) \cdot s(x) \mod d(x)$.
8. *Ef* $p(x), q(x), d_1(x), d_2(x) \in \mathbb{R}[x]$, $p(x) \equiv q(x) \mod d_1(x)$ *og* $d_2(x) \mid d_1(x)$ *þá* $p(x) \equiv q(x) \mod d_2(x)$.
9. *Ef* $p(x), d(x) \in \mathbb{R}[x]$ *þá er til* $q(x) \in \mathbb{R}[x]$ *þannig að* $p(x) \cdot q(x) \equiv c(x) \mod d(x)$ *þar sem* $c(x)$ *er stærsti samdeilir* $p(x)$ *og* $d(x)$.
10. *Ef* $p(x), q(x) \in \mathbb{R}[x]$ *þá er* $p(x) \equiv q(x) \mod 0$ *ef og aðeins ef* $p(x) = q(x)$.
11. *Ef* $p(x), q(x) \in \mathbb{R}[x]$ *þá er* $p(x) \equiv q(x) \mod 1$.
12. *Ef* $p(x), d(x) \in \mathbb{R}[x]$ *og* $d(x) \neq 0$ *þá er til ótvírætt* $r(x) \in \mathbb{R}[x]$ *þannig að* $r(x) = 0$ *eða* $\deg(r(x)) < \deg(d(x))$ *og* $p(x) \equiv r(x) \mod d(x)$.
13. *Ef* $p(x) \in \mathbb{R}[x]$ *og* $a \in \mathbb{R}$ *þá er* $p(x) \equiv p(a) \mod (x - a)$.

Sönnun. Sönnun er eftirlátin lesanda. □

Eftirfarandi setning er mikilvæg

Setning 2.6. *Gerum ráð fyrir að* $p(x), q(x), a(x), b(x) \in \mathbb{R}[x]$ *og* $p(x)$ *og* $q(x)$ *séu ósamþátta. Þá er til* $c(x) \in \mathbb{R}[x]$ *þannig að:*

$$c(x) \equiv a(x) \mod p(x) \qquad \text{og} \qquad c(x) \equiv b(x) \mod q(x)$$

Sönnun. Gerum ráð fyrir að $p(x), q(x), a(x), b(x) \in \mathbb{R}[x]$ og $p(x)$ og $q(x)$ séu ósamþátta. Af hjálparsetningu 2.5 leiðir að til eru $s(x), t(x) \in \mathbb{R}[x]$ þannig að $s(x) \cdot p(x) \equiv 1 \mod q(x)$ og $t(x) \cdot q(x) \equiv 1 \mod p(x)$. Látum $c(x) = b(x) \cdot s(x) \cdot p(x) + a(x) \cdot t(x) \cdot q(x)$.

Með því að beita setningu 2.5 þá fæst

$$c(x) = b(x) \cdot s(x) \cdot p(x) + a(x) \cdot t(x) \cdot q(x) \equiv b(x) \cdot s(x) \cdot 0 + a(x) \cdot 1 \equiv a(x) \mod p(x)$$

og

$$c(x) = b(x) \cdot s(x) \cdot p(x) + a(x) \cdot t(x) \cdot q(x) \equiv b(x) \cdot 1 + a(x) \cdot t(x) \cdot 0 \equiv b(x) \mod q(x)$$

□

Lesanda ætti að vera ljóst af sönnunni hér að ofan hvernig fyrir gefin $a(x), b(x), p(x), q(x) \in \mathbb{R}[x]$ þannig að $p(x)$ og $q(x)$ séu ósammþátta þá megi finna $c(x) \in \mathbb{R}[x]$ þannig að $c(x) \equiv a(x) \mod p(x)$ og $c(x) \equiv b(x) \mod q(x)$.

Gerum ráð fyrir að $m \in \mathbb{N}$ og $a \in \mathbb{R}$. Af setningu 2.5 leiðir að $x^m \equiv a^m \mod (x-a)$. Hvernig reiknum við afang deilingar x^m með $(x-a)^n$ þar sem $m, n \in \mathbb{N}$ og $a \in \mathbb{R}$? Við gerum ráð fyrir að lesandi kannist við tvíliðusetninguna en hún segir að ef $m \in \mathbb{N}$ þá er:

$$(x+y)^m = \sum_{n \in \mathbb{N}} \binom{m}{n} x^n y^{m-n}$$

Þar sem $\binom{m}{n} = 0$ ef $m < n$.

Gerum ráð fyrir að $m, n \in \mathbb{N}$ og $a \in \mathbb{R}$. Þá fæst:

$$\begin{aligned}
x^m &= ((x-a)+a)^m \\
&= \sum_{k \in \mathbb{N}} \binom{m}{k} a^{m-k} (x-a)^k \\
&= \left(\sum_{k=n}^{\infty} \binom{m}{k} a^{m-k} (x-a)^{k-n} \right) \cdot (x-a)^n + \left(\sum_{k=0}^{n-1} \binom{m}{k} a^{m-k} (x-a)^k \right) \\
&\equiv \left(\sum_{k=n}^{\infty} \binom{m}{k} a^{m-k} (x-a)^{k-n} \right) \cdot 0 + \left(\sum_{k=0}^{n-1} \binom{m}{k} a^{m-k} (x+(-a))^k \right) \\
&\equiv \sum_{k=0}^{n-1} \binom{m}{k} \left(\sum_{i=0}^{k} \binom{k}{i} (-a)^{k-i} x^i \right) \\
&= \sum_{i=0}^{n-1} \left(\sum_{k=i}^{n-1} \binom{k}{i} (-a)^{k-i} \right) x^i \mod (x-a)^n
\end{aligned}$$

Örlítil línuleg algebra

Við getum litið á $\mathbb{R}[x]$ og $\mathbb{R}^{\mathbb{N}}$ sem vigurrúm yfir $\mathbb{R}$ sem mun hjálpa við framsetningu í framhaldinu.

Skilgreining 3.1. Gerum ráð fyrir að X sé mengi og $+$ og $\cdot$ sé varpanir $+ : X \times X \to X$, $\cdot : \mathbb{R} \times X \to X$ sem fullnægja eftirafarandi skilyrðum:

1. Ef $\vec{u}, \vec{v}, \vec{w} \in X$. Þá er $\vec{u} + (\vec{v} + \vec{w}) = (\vec{u} + \vec{v}) + \vec{w}$.
2. Til er $\vec{0} \in X$ þannig að $\vec{u} + \vec{0} = \vec{0} + \vec{u} = \vec{u}$ fyrir öll $\vec{u} \in X$. (Slíkt $\vec{0}$ er ótvírætt ákarðað af þessum skilyrðum).
3. Fyrir sérhvert $\vec{u} \in X$ þá er til $-\vec{u} \in X$ þannig að $\vec{u} + (-\vec{u}) = (-\vec{u}) + \vec{u} = \vec{0}$. (Fyrir sérhvert $\vec{u} \in X$ þá er það $-\vec{u}$ ótvírætt ákvarðað af þessum skilyrðum).
4. Ef $\vec{u}, \vec{v} \in X$. það er $\vec{u} + \vec{v} = \vec{v} + \vec{u}$.
5. Ef $\vec{u} \in X$ þá er $1 \cdot \vec{u} = \vec{u}$.
6. Ef $a, b \in \mathbb{R}$ og $\vec{u} \in X$ þá er $(a+b) \cdot \vec{u} = (a \cdot \vec{u}) + (b \cdot \vec{u})$.
7. Ef $a \in \mathbb{R}$ og $\vec{u}, \vec{v} \in X$ þá er $a \cdot (\vec{u} + \vec{v}) = (a \cdot \vec{u}) + (a \cdot \vec{v})$.
8. Ef $a, b \in \mathbb{R}$ og $\vec{u} \in X$ þá er $a \cdot (b \cdot \vec{u}) = (a \cdot b) \cdot \vec{u}$.

Þá kallast X (ásamt $+$ og $\cdot$) $\mathbb{R}$- vigurrúm. Stökin í X kallasta vigrar.

Við höfum þegar gert grein fyrir að $\mathbb{R}[x]$ sé $\mathbb{R}$-vigurrúm (reyndar líka $\mathbb{R}$-algebra líka). Einnig má líta á $\mathbb{R}$ sem $\mathbb{R}$-vigurrúm með venjulegu samlagninunni og venjulegu margföldueninni. Fyrir $\mathbb{R}^{\mathbb{N}}$ þá getum við skilgreint $+$ þannig að ef $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ þá er $(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}}$. Við getum skilgreint $\cdot$ fyrir $\mathbb{R}\cdot\mathbb{R}^{\mathbb{N}}$ þannig að ef $c\in\mathbb{R}$ og $(a_n)_{n\in\mathbb{N}}$ þá er $c\cdot(a_n)_{n\in\mathbb{N}} = (c\cdot a_n)_{n\in\mathbb{N}}$. Lesandi ætti að sannfæra sjálfan sig að með þessu þá er $\mathbb{R}^{\mathbb{N}}$ orðið að $\mathbb{R}$-vigurrúmi.

Við höfum mikin áhuga á þeim vörpunum milli vigurrúma sem varðveita samlagninguna og margföldunina. Þær kallast línulegar varpanir.

Skilgreining 3.2. Gerum ráð fyrir að X og Y séu vigurrúm yfir $\mathbb{R}$. Vörpun $L : X \to Y$ kallast línuleg vörpun (eða $\mathbb{R}$-línuleg) ef:

1. Fyrir öll $\vec{u}, \vec{v} \in X$ þá er $L(\vec{u}+\vec{v}) = L(\vec{u}) + L(\vec{v})$.
2. Fyrir öll $a\in\mathbb{R}$ og öll $\vec{u}\in X$ þá er $L(a\cdot\vec{u}) = a\cdot L(\vec{u})$.

Lesandi getur sannfært sig um að ef X er $\mathbb{R}$ vigurrúm að $\mathrm{id}_X : X \to X$ sé $\mathbb{R}$-línuleg. Ef X, Y, Z eru $\mathbb{R}$-vigurrúm, $L_1 : X \to Y$ og $L_2 : Y \to Z$ eru línulega varpanir þá er $L_2 \circ L_1 : X \to Z$ línuleg vörpun. Einnig gildir að ef X, Y eru $\mathbb{R}$-vigurrúm og $L : X \to Y$ er andhverfanleg vörpum það andhverfan $L^{-1} : Y \to X$ sé einnig línuleg.

Gerum ráð fyrir að X, Y séu $\mathbb{R}$-vigurrúm og $L : X \to Y$ sé sé $\mathbb{R}$-línuleg vörpun. Ef $m\in\mathbb{N}$, $a_1, a_2, \ldots, a_m \in \mathbb{R}$ og $\vec{u}_1, \vec{u}_2, \ldots, \vec{u}_n \in X$ þá má auðveldlega sanna með þrepun að:

$$L\left(\sum_{n=1}^{m} a_n\cdot\vec{u}_n\right) = \sum_{n=1}^{m} a_n\cdot L(\vec{u}_n)$$

Gerum ráð fyrir að X, Y, Z séu $\mathbb{R}$-vigurrúm. Vörpun $L : X\times Y \to Z$ kallast $\mathbb{R}$-tvílínuleg ef fyrirsérhvert $\vec{y}\in Y$ og sérhvert $\vec{x}\in X$ þá eru varpanirnar $X\to Z$, $\vec{u}\mapsto L(\vec{u},\vec{y})$ og $Y\to Z$, $\vec{u}\mapsto L(\vec{x},\vec{u})$ $\mathbb{R}$-línulegar. Það er vörpun er $\mathbb{R}$-tvílínuleg ef hún er $\mathbb{R}$-línuleg í hvorri breytu fyrir sig.

Þekkt dæmi um tvílínulega vörpun er margföldunin á $\mathbb{R}$, einnig er innfeldi og krossfeldi tvílínulegar varpanir.

Við höfum sérstakan áhuga á vörpuninn $L : \mathbb{R}[x]\times\mathbb{R}^{\mathbb{N}} \to \mathbb{R}$, $(p(x), (a_n)_{n\in\mathbb{N}}) \mapsto \sum\limits_{n\in\mathbb{N}} p_n\cdot a_n$. Þessi vörpun er vel skilgreind þar sem $p_n \neq 0$ fyrir endanlega mörg $n\in\mathbb{N}$. Lesandi getur auðveldlega sannfært sig um að L sé tvílínuleg vörpun.

Einnig er auðvelt að sjá að ef $m\in\mathbb{N}$, $p(x)\in\mathbb{R}[x]$ og $(a_n)_{n\in\mathbb{N}}\in\mathbb{R}^{\mathbb{N}}$ að:

$$\begin{aligned}
L(x^m\cdot p(x), (a_n)_{n\in\mathbb{N}}) &= \sum_{n\in\mathbb{N}} (x^m p(x))_n \cdot a_n \\
&= \sum_{n=m}^{\infty} (x^m p(x))_n \cdot a_n \\
&= \sum_{n=m}^{\infty} p_{n-m}\cdot a_n \\
&= \sum_{n\in\mathbb{N}} p_n \cdot a_{n+m} \\
&= L(p(x), (a_{n+m})_{n\in\mathbb{N}})
\end{aligned}$$

Örlítið um línuleg rakningarvensl

Gerum ráð fyrir að $m\in\mathbb{N}$ og $c_0, c_1, \ldots, c_{m-1}\in\mathbb{R}$ séu fastar. Skilyrðið $a_{n+m} = \sum\limits_{k=0}^{m-1} c_k\cdot a_{n+k}$ fyrir öll $n\in\mathbb{N}$ fyrir runu $(a_n)_{n\in\mathbb{N}}$ kallast línuleg rakningarvensl. Við hyggjumst rannsaka þau með hjálp vörpuninnar $L : \mathbb{R}[x]\times\mathbb{R}^{\mathbb{N}} \to \mathbb{R}, (p(x), (a_n)_{n\in\mathbb{N}}) \mapsto \sum\limits_{n\in\mathbb{N}} p_n\cdot a_n$.

Gerum ráð fyrir að $m \in \mathbb{N}$ og $c_0, c_1, \ldots, c_{m-1} \in \mathbb{R}$. Margliðan $p(x) = x^m + \sum_{k=0}^{m-1}(-c_k)x^k \in \mathbb{R}[x]$ kallast kennimargliða rakningarvenslanna. Við sjáum að fyrir $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ þá er jafngilt að $(a_n)_{n\in\mathbb{N}}$ fullnægi rakningarvenslunum $a_{n+m} = \sum_{k=0}^{m-1} c_k \cdot a_{n+k}$ fyrir öll $n \in \mathbb{N}$ og að $\sum_{k\in\mathbb{N}} p_k a_{n+k} = 0$ fyrir öll $n \in \mathbb{N}$.

Athugum að fyrir $n \in \mathbb{N}$ þá er

$$(x^n \cdot p(x), (a_k)_{k\in\mathbb{N}}) = L(p(x), (a_{k+n})_{n\in\mathbb{N}}) = \sum_{k\in\mathbb{N}} p_k \cdot a_{k+n}$$

Þetta sýnir að það er jafngilt að $(a_n)_{n\in\mathbb{N}}$ fullnægi rakningarvenslunum og að $L(x^n \cdot p(x), (a_k)_{k\in\mathbb{N}}) = 0$ fyrir öll $n \in \mathbb{N}$.

Gerum ráð fyrir að $L(x^n \cdot p(x), (a_k)_{k\in\mathbb{N}}) = 0$ fyrir öll $n \in \mathbb{N}$. Gerum ráð fyrir að $q(x) \in \mathbb{R}[x]$. Þá fæst:

$$\begin{aligned} L(q(x) \cdot p(x), (a_n)_{n\in\mathbb{N}}) &= L\left(\sum_{k\in\mathbb{N}} q_k x^k \cdot p(x), (a_n)_{n\in\mathbb{N}}\right) \\ &= \sum_{k\in\mathbb{N}} q_k \cdot L(x^k \cdot p(x), (a_n)_{n\in\mathbb{N}}) \\ &= \sum_{k\in\mathbb{N}} q_k \cdot 0 \\ &= 0 \end{aligned}$$

Öfugt ef $L(q(x) \cdot p(x), (a_n)_{n\in\mathbb{N}}) = 0$ fyrir öll $q(x) \in \mathbb{R}[x]$ þá er $L(x^n \cdot p(x), (a_k)_{k\in\mathbb{N}}) = 0$ fyrir öll $n \in \mathbb{N}$ þar sem $x^n \in \mathbb{R}[x]$ fyrir öll $n \in \mathbb{N}$.

Við sjáum því að það er jafngilt að $(a_n)_{n\in\mathbb{N}}$ fullnægi rakningarvenslunum og að $L(q(x) \cdot p(x), (a_n)_{n\in\mathbb{N}}) = 0$ fyrir öll $q(x) \in \mathbb{R}[x]$. Með öðrum orðum þá fullnægir $(a_n)_{n\in\mathbb{N}}$ rakningarvenslunum ef og aðeins ef $L(q(x), (a_n)_{n\in\mathbb{N}}) = 0$ fyrir allar margliður $q(x) \in \mathbb{R}[x]$ þannig að $p(x) \mid q(x)$.

Gerum héðan í frá ráð fyrir að $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ sem fullnægir línulegu rakningarvenslunum. Gerum nú ráð fyrir að $s(x), t(x) \in \mathbb{R}[x]$ og $s(x) \equiv t(x) \mod p(x)$. Þá $p(x) \mid (t(x) - s(x))$. Þá fæst:

$$L(t(x), (a_n)_{n\in\mathbb{N}}) - L(s(x), (a_n)_{n\in\mathbb{N}}) = L(t(x) - s(x), (a_n)_{n\in\mathbb{N}}) = 0$$

Það er $L(s(x), (a_n)_{n\in\mathbb{N}}) = L(t(x), (a_n)_{n\in\mathbb{N}})$.

Þar sem fyrir sérhverja margliðu $q(x) \in \mathbb{R}[x]$ þá má finna ótvíræða margliðu $r(x)$, $q(x) \equiv r(x) \mod p(x)$ þannig að $\deg(r(x)) < \deg(p(x))$ þá getum við reiknað $L(q(x), (a_n)_{n\in\mathbb{N}})$ með því að finna fyrst afganginn $r(x)$ úr deilingu $q(x)$ með $p(x)$ og reikna síðan $L(r(x), (a_n)_{n\in\mathbb{N}}) = \sum_{n=0}^{\deg(r)} r_n \cdot a_n$ sem er endanleg summa með í mesta lagi $\deg(p)$ liði þar sem $\deg(r) < \deg(p)$.

Athugum að þessi aðferð gerir okkur kleift að ákvarða a_m fyrir öll $m \in \mathbb{N}$ þar sem $a_m = L(x^m, (a_n)_{n\in\mathbb{N}})$.

Nokkur rakningarvensl

Gerum ráð fyrir að $r \in \mathbb{R}$ og $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ fullnægi rakningarvenslunum $a_{n+1} = ra_n$ fyrir öll $n \in \mathbb{N}$. Kennimargliðan er $x - r$. Fyrir $m \in \mathbb{N}$ þá er $x^m \equiv r^m \mod (x - r)$ svo

$$a_m = L(x^m, (a_n)_{n\in\mathbb{N}}) = L(r^m, (a_n)_{n\in\mathbb{N}}) = r^m \cdot a_0$$

Ljóst er að frjálst val er á a_0 og að runan $(a_n)_{n\in\mathbb{N}}$ ákvarðast af a_0.

Gerum nú ráð fyrir að $r \in \mathbb{R}$, $k \in \mathbb{N}$ og að $(a_n)_{n\in\mathbb{N}}$ fullnægi línulegum rakningarvenslum með kennimargliðuna $(x - r)^k$. Fyrir $m \in \mathbb{N}$ þá er $x^m \equiv \sum_{i=0}^{k-1}\left(\sum_{n=i}^{k-1}\binom{n}{i}(-r)^{n-i}\right)x^i \mod (x - r)^k$ og þar af leiðir

$$a_m = L(x^m, (a_n)_{n\in\mathbb{N}}) = L\left(\sum_{i=0}^{k-1}\left(\sum_{n=i}^{k-1}\binom{n}{i}(-r)^{n-i}\right)x^i, (a_n)_{n\in\mathbb{N}}\right) = \sum_{i=0}^{k-1}\left(\sum_{n=i}^{k-1}\binom{n}{i}(-r)^{n-i}\right)a_i$$

Látum $t_{i,m}(n) = \sum_{n=i}^{k-1} \binom{n}{i}(-r)^{n-i}$. Það er ekki erfitt að sjá að rita má $t_{i,m}(n) = r^m \cdot p_i(n)$ þar sem $p_i(x) \in \mathbb{R}[x]$ er margliða þannig að $\deg p_i \leqslant k-1-i$. Við getum því ritað:

$$a_m = \sum_{i=0}^{k-1} r^m p_i(n) a_i = r^m \sum_{i=0}^{k-1} p_i(n) \cdot a_i$$

Ljóst er að $a_0, a_1, \ldots, a_{k-1}$ má velja frjálst og runan $(a_n)_{n\in\mathbb{N}}$ ákvarðast af a_0.

Gerum nú ráð fyrir að $p(x), q(x) \in \mathbb{R}[x]$, $p(x)$ og $q(x)$ séu ósamþátta og $(a_n)_{n\in\mathbb{N}}$ sé runa sem fullnægir línulegum rakningarvenslum með kennimarglið $p(x)\cdot q(x)$. Gerum ráð fyrir að $m \in \mathbb{N}$, $x^m \equiv a(x) \mod p(x)$ og $x^m \equiv b(x) \mod q(x)$. Þar sem $p(x)$ og $q(x)$ eru ósamþátta þá getum við fundið $s(x), t(x) \in \mathbb{R}[x]$ þannig að $s(x)\cdot p(x) + t(x)\cdot q(x) = 1$.

Segjum $c(x) = b(x)\cdot s(x)\cdot p(x) + a(x)\cdot t(x)\cdot q(x)$ eins og í sönnuninn á setningu 2.6. Þá fæst að $c(x) \equiv a(x) \equiv x^m \mod p(x)$ og $c(x) \equiv b(x) \equiv x^m \mod q(x)$. Það er $p(x) \mid (x^m - c(x))$ og $q(x) \mid (x^m - c(x))$. Af hjálparsetningu 2.3 leiðir að $p(x)\cdot q(x) \mid (x^m - c(x))$. Það er $c(x) \equiv x^m \mod (p(x)\cdot q(x))$.

Við sjáum að við getum því reiknað $x^m \mod p(x)\cdot q(x)$ með því að reikna $x^m \mod p(x)$ og $x^m \mod q(x)$. Sýnum hvernig þetta er gert með því að reikna lokaða formúlu fyrir fibonacci tölurnar:

Fibonacci tölurnar $(\mathrm{fib}_n)_{n\in\mathbb{N}}$ er skilgreindar þannig að $\mathrm{fib}_0 = 0$, $\mathrm{fib}_1 = 1$ og $\mathrm{fib}_{n+2} = \mathrm{fib}\, n + 1 + \mathrm{fib}_n$ fyrir öll $n \in \mathbb{N}$. Kennimargliða þessara rakningarvensla er $p(x) = x^2 - x - 1$. Við þáttum $p(x) = (x - r_1)(x - r_2)$ þar sem $r_1 = \frac{1+\sqrt{5}}{2}$ og $r_2 = \frac{1-\sqrt{5}}{2}$.

Við fáum að $1 = \frac{-\sqrt{5}}{5}(x - r_1) + \frac{\sqrt{5}}{5}(x - r_2)$. Ef $m \in \mathbb{N}$ þá er $x^m \equiv {r_1}^m \mod (x - r_1)$ og $x^m \equiv {r_2}^m \mod (x - r_2)$. Því fæst:

$$\begin{aligned} x^m &\equiv \frac{-\sqrt{5}}{5}\cdot {r_2}^m (x - r_1) + \frac{\sqrt{5}}{5}\cdot {r_1}^m (x - r_2) \\ &= \frac{\sqrt{5}\cdot {r_1}^m - \sqrt{5}\cdot {r_2}^m}{5} x + \frac{\sqrt{5}\cdot r_1 \cdot {r_2}^m - \sqrt{5}\cdot r_2 \cdot {r_1}^m}{5} \mod (x^2 - x - 1) \end{aligned}$$

Við álytum að fyrir sérhvert $m \in \mathbb{N}$ þá er

$$\begin{aligned} \mathrm{fib}_m &= L(x^m, (\mathrm{fib}_n)_{n\in\mathbb{N}}) \\ &= L\left(\frac{\sqrt{5}\cdot {r_1}^m - \sqrt{5}\cdot {r_2}^m}{5} x + \frac{\sqrt{5}\cdot r_1 \cdot {r_2}^m - \sqrt{5}\cdot r_2 \cdot {r_1}^m}{5}, (\mathrm{fib}_n)_{n\in\mathbb{N}}\right) \\ &= \frac{\sqrt{5}\cdot {r_1}^m - \sqrt{5}\cdot {r_2}^m}{5}\cdot \mathrm{fib}_1 + \frac{\sqrt{5}\cdot r_1 \cdot {r_2}^m - \sqrt{5}\cdot r_2 \cdot {r_1}^m}{5}\cdot \mathrm{fib}_0 \\ &= \frac{\sqrt{5}\cdot {r_1}^m - \sqrt{5}\cdot {r_2}^m}{5}\cdot 1 + \frac{\sqrt{5}\cdot r_1 \cdot {r_2}^m - \sqrt{5}\cdot r_2 \cdot {r_1}^m}{5}\cdot 0 \\ &= \frac{\sqrt{5}\cdot \left(\frac{1+\sqrt{5}}{2}\right)^m - \sqrt{5}\cdot \left(\frac{1-\sqrt{5}}{2}\right)^m}{5} \end{aligned}$$

Lesanda ætti nú að vera ljóst hvernig finna má formúlu fyrir runu $(a_n)_{n\in\mathbb{N}}$ sem fullnægir línulegum rakningarvenslum með kennimargliður $p(x) = \prod_{i=1}^{k}(x - r_i)^{e_i}$ þar sem $r_i \in \mathbb{R}$ eru ólíkar rauntölur og $e_i \in \mathbb{N}$ fyrir öll $i \in \mathbb{N}$.

Gerum aftur ráð fyrir að $p(x) \in \mathbb{R}[x]$ sé kennimargliða fyrir rakningarvensl af stigi $m \in \mathbb{N}$. Þá er $p_m = 1$. Fyrir öll $n \in \mathbb{N}$ þá má finna (ótvíræða) margliðu $r_n(x) \in \mathbb{N}$, $\deg(r_n(x)) < \deg(p(x)) = m$ þannig að $x^n \equiv r_n(x)$

mod $p(x)$. Þá fæst:

$$\begin{aligned}
0 &= x^n \cdot 0 \\
&\equiv x^n \cdot p(x) \\
&\equiv \sum_{i=0}^{m} p_i x^{n+i} \\
&\equiv \sum_{i=0}^{m} p_i r_{n+i}(x) \\
&= \sum_{i=0}^{m} p_i \left(\sum_{j=0}^{m-1} r_{n+i,j} x^j \right) \\
&= \sum_{j=0}^{m-1} \left(\sum_{i=0}^{m} p_i r_{n+i,j} \right) x^j \\
&= \sum_{j=0}^{m-1} L(p(x), (r_{i+n,j})_{i\in\mathbb{N}}) x^j \\
&= \sum_{j=0}^{m-1} L(x^n \cdot p(x), (r_{i,j})_{i\in\mathbb{N}}) x^j
\end{aligned}$$

Nú er $\deg\left(\sum_{j=0}^{m-1} L(x^n \cdot p(x), (r_{i,j})_{i\in\mathbb{N}})x^j\right) \leqslant m-1 < m = \deg(p)$ og þar sem $0 \equiv \sum_{j=0}^{m-1} L(x^n \cdot p(x), (r_{i,j})_{i\in\mathbb{N}})x^j$ þá fæst að $\sum_{j=0}^{m-1} L(x^n \cdot p(x), (r_{i,j})_{i\in\mathbb{N}})x^j = 0$. Sér í lagi þá fæst að $L(x^n \cdot p(x), (r_{i,j})_{i\in\mathbb{N}}) = 0$ fyrir öll $i \in \{0, 1, \ldots, m-1\}$ og öll $n \in \mathbb{N}$. Við sjáum sér í lagi að $(r_{i,j})_{i\in\mathbb{N}}$ fullnægir rakningarvenslunum með kennimargliðuna $p(x)$ fyrir öll $j \in \{0, 1, \ldots, m-1\}$.

Nú er

$$\begin{aligned}
r_{n+1}(x) &\equiv x^{n+1} \\
&= x^n \cdot x \\
&\equiv r_n(x) \cdot x \\
&\equiv r_n(x) \cdot x - r_{n,m-1} p(x) \\
&= \left(\sum_{i=1}^{m} r_{n,i-1} x^{n+i} \right) - \left(\sum_{i=0}^{m} p_m x^{n+i} \right) \\
&= \sum_{i=0}^{m-1} (r_{n,i-1} - r_{n,m-1} \cdot p_i) x^i \mod p(x)
\end{aligned}$$

þar sem við lítum sem svo að $r_{n,-1} = 0$. Þar sem $\deg(r_{n+1}(x)) \leqslant m-1 < m = \deg(p(x))$, $\deg\left(\sum_{i=0}^{m-1} (r_{n,i-1} - r_{n,m-1} \cdot p_i)x^i\right) \leqslant m-1 < m = \deg(p)$ og $r_{n+1}(x) \equiv \sum_{i=0}^{m-1} (r_{n,i-1} - r_{n,m-1} \cdot p_i)x^i \mod p(x)$ þá fæst að $r_{n+1}(x) = \sum_{i=0}^{m-1} (r_{n,i-1} - r_{n,m-1} \cdot p_i)x^i$. Sér í lagi þá er $r_{n+1,i} = r_{n,i-1} - r_{n,m-1} \cdot p_i$ fyrir öll $i \in \{0, 1, \ldots, m-1\}$.

Við fáum að $r_{n,m-1} = 0$ ef $n \in \{0, 1, \ldots, m-1\}$ og $r_{m-1,m-1} = 1$. Svo fullnægir $(r_{n,m-1})_{n\in\mathbb{N}}$ rakningarvenslunum með kennimargliðu $p(x)$ svo við getum notað rakningarvenslin. Gerum ráð fyrir að við höfum ákvarðað $(r_{n,k})_{n\in\mathbb{N}}$ og $(r_{n,m-1})_{n\in\mathbb{N}}$ hafi verið ákörðuð fyrir $k \in \{1, 2, \ldots, m-1\}$. Þá er $r_{n,k-1} = r_{n+1,k+1} + r_{n,m-1} \cdot p_{k+1}$ fyrir öll $n \in \mathbb{N}$.

Skoðum þetta nú með tilliti til Fibonnacci rununnar $(\mathrm{fib}_n)_{n\in\mathbb{N}}$. Kennimargliðan er $p(x) = x^2 - x - 1$. Gerum ráð fyrir að $m \in \mathbb{N}$. Þá er

$$\mathrm{fib}_m = L(x^m, (\mathrm{fib}_n)_{n\in\mathbb{N}}) = L(r_m(x), (\mathrm{fib}_n)_{n\in\mathbb{N}}) = r_{m,1} \cdot \mathrm{fib}_1 + r_{m,0} \cdot \mathrm{fib}_0 = r_{m,1} \cdot 1 + r_{m,0} \cdot 0 = r_{m,1}$$

Þá fæst að $r_{n,0} = r_{n+1,1} + r_{n,1} \cdot p_1 = \mathrm{fib}_{n+1} + \mathrm{fib}_n \cdot(-1) = \mathrm{fib}_{n+1} - \mathrm{fib}_n$. Ljóst er að $r_{0,0} = 1$ og ef $n > 0$ þá er $\mathrm{fib}_{n+1} - \mathrm{fib}_n = \mathrm{fib}_n + \mathrm{fib}_{n-1} - \mathrm{fib}_n = \mathrm{fib}_{n-1}$, það er $r_{n,0} = \mathrm{fib}_{n-1}$ ef $n > 0$.

Gerum nú ráð fyrir að $n \in \mathbb{N}$ og $n > 0$. Þá er

$$\begin{aligned}
\mathrm{fib}_{2n}\, x + \mathrm{fib}_{2n-1} &= r_{2n}(x) \\
&\equiv x^{2n} \\
&= (x^n)^2 \\
&\equiv r_n(x)^2 \\
&= (\mathrm{fib}_n\, x + \mathrm{fib}_{n-1})^2 \\
&\equiv (\mathrm{fib}_n\, x + \mathrm{fib}_{n-1})^2 - {\mathrm{fib}_n}^2(x^2 - x - 1) \\
&= ({\mathrm{fib}_n}^2 x^2 + 2 \cdot \mathrm{fib}_n \cdot \mathrm{fib}_{n-1}\, x + {\mathrm{fib}_{n-1}}^2) - ({\mathrm{fib}_n}^2 x^2 - {\mathrm{fib}_n}^2 x - {\mathrm{fib}_n}^2) \\
&= (2 \cdot \mathrm{fib}_n \cdot \mathrm{fib}_{n-1} + {\mathrm{fib}_n}^2)x + ({\mathrm{fib}_n}^2 + {\mathrm{fib}_{n-1}}^2) \\
&= \mathrm{fib}_n \cdot((\mathrm{fib}_n + \mathrm{fib}_{n-1}) + \mathrm{fib}_{n-1})x + ({\mathrm{fib}_n}^2 + {\mathrm{fib}_{n-1}}^2) \\
&= \mathrm{fib}_n \cdot(\mathrm{fib}_{n+1} + \mathrm{fib}_{n-1})x + \mathrm{fib}_{n-1})x + ({\mathrm{fib}_n}^2 + {\mathrm{fib}_{n-1}}^2) \mod (x^2 - x - 1)
\end{aligned}$$

Þar sem báðar margliðurnar eru af stigi $\leqslant 1 < 2 = \deg(x^2 - x - 1)$ þá fæst að $\mathrm{fib}_{2n}\, x + \mathrm{fib}_{2n-1} = \mathrm{fib}_n \cdot(\mathrm{fib}_{n+1} + \mathrm{fib}_{n-1})x + \mathrm{fib}_{n-1})x + ({\mathrm{fib}_n}^2 + {\mathrm{fib}_{n-1}}^2) \mod (x^2 - x - 1)$. Sér í lagi fáum við að $\mathrm{fib}_{2n} = \mathrm{fib}_n \cdot(\mathrm{fib}_{n+1} + \mathrm{fib}_{n-1})$ og $\mathrm{fib}_{2n-1} = ({\mathrm{fib}_n}^2 + {\mathrm{fib}_{n-1}}^2)$.

Minnumst aðeins á runur sem eru lotubundar. Runa $(a_n)_{n\in\mathbb{N}}$ er sögð lotubundin með lotu $t \in \mathbb{N}\backslash\{0\}$ ef $a_{n+t} = a_n$ fyrir öll $n \in \mathbb{N}$. Jafngilt er að segja að $(a_n)_{n\in\mathbb{N}}$ sé lotubundin með lotu t ef $L(q(x)(x^t - 1), (a_n)_{n\in\mathbb{N}}) = 0$ fyrir öll $q(x) \in \mathbb{R}[x]$.

Gerum ráð fyrir að $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ fullnægi línulegum rakningarvenslum með kennimarliðu $p(x) \in \mathbb{R}[x]$. Þá er $L(q(x), (a_n)_{n\in\mathbb{N}}) = 0$ fyrir öll $q(x) \in \mathbb{R}[x]$ þannig að $p(x) \mid q(x)$. Gerum ráð fyrir að $p(x) \mid x^t - 1$ þar sem $t \in \mathbb{N}\backslash\{0\}$. Gerum ráð fyrir að $x^t - 1 \mid q(x) \in \mathbb{R}[x]$. Þá $p(x) \mid q(x)$ og því $L(q(x), (a_n)_{n\in\mathbb{N}}) = 0$. Þetta sýnir að $(a_n)_{n\in\mathbb{N}}$ er lotubunin með lotu $t \in \mathbb{N}$.

Sem dæmi má nefna að $x^6 - 1 = (x^2 + x + 1) \cdot (x - 1) \cdot (x^2 - x + 1) \cdot (x + 1)$ svo runa $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ sem fullnægir línulegu rakningarvenslunum $a_{n+2} = a_{n+1} - a_n$ hefur því kennimargliðu $p(x) = x^2 - x + 1$ sem gengur upp í $x^6 - 1$. Því fæst sjálfkrafa að $(a_n)_{n\in\mathbb{N}}$ verður lotubunin með lotu 6.

Öfugt getur lesandi sannað að ef $p(x) \in \mathbb{R}[x]$ er kennimargliða fyrir línuleg rakningarvensl, $t \in \mathbb{N}\backslash\{0\}$ og allar runur $(a_n)_{n\in\mathbb{N}}$ sem fullnægja línulegu rakningarvenslunum hafa lotu t þá verður $p(x) \mid x^t - 1$ að gilda.

Hlurðir fyrir margliður

Gerum ráð fyrir að $p(x), q(x) \in \mathbb{R}[x]$ og $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$. Látum $(b_n)_{n\in\mathbb{N}} = (L(x^n \cdot q(x), (a_k)_{k\in\mathbb{N}}))_{n\in\mathbb{N}}$. Þá fæst:

$$\begin{aligned}
L(p(x), (b_n)_{n\in\mathbb{N}}) &= L\left(p(x), (L(x^n \cdot q(x), (a_k)_{k\in\mathbb{N}}))\right) \\
&= L\left(p(x), \left(\sum_{k\in\mathbb{N}} (x^n \cdot q(x))_k \cdot a_k\right)_n\right) \\
&= L\left(p(x), \left(\sum_{k=n}^{\infty} q_{k-n} \cdot a_k\right)_n\right) \\
&= L\left(p(x), \left(\sum_{k\in\mathbb{N}} q_k \cdot a_{k+n}\right)_n\right) \\
&= \sum_{k\in\mathbb{N}} q_k \cdot L(p(x), (a_{n+k})_{n\in\mathbb{N}}) \\
&= \sum_{k\in\mathbb{N}} q_k \cdot L(x^k \cdot p(x), (a_n)_{n\in\mathbb{N}}) \\
&= L\left(\sum_{k\in\mathbb{N}} q_k x^k \cdot p(x), (a_n)_{n\in\mathbb{N}}\right) \\
&= L\left(\left(\sum_{k\in\mathbb{N}} q_k x^k\right) \cdot p(x), (a_n)_{n\in\mathbb{N}}\right) \\
&= L(q(x) \cdot p(x), (a_n)_{n\in\mathbb{N}}) \\
&= L(p(x) \cdot q(x), (a_n)_{n\in\mathbb{N}})
\end{aligned}$$

Skilgreinum vörpun $\Delta : \mathbb{R}^{\mathbb{N}} \to \mathbb{R}^{\mathbb{N}}$, $(a_n)_{n\in\mathbb{N}} \mapsto (a_{n+1} - a_n)_{n\in\mathbb{N}}$. Lesandi getur auðveldlega sanfært sig um Δ er línuleg og $\Delta((a_n)_{n\in\mathbb{N}}) = (L(x^n \cdot (x-1), (a_k)_{k\in\mathbb{N}})_{n\in\mathbb{N}}$. Skilgreinum einnig vörpunina $\Sigma : \mathbb{R}^{\mathbb{N}} \to \mathbb{R}^{\mathbb{N}}$, $(a_n)_{n\in\mathbb{N}} \mapsto \left(\sum_{m=0}^{n-1} a_m\right)_{n\in\mathbb{N}}$. Auðvelt er að sjá að ef $(a_n)_{n\in\mathbb{N}}$ að

$$\begin{aligned}
(\Delta \circ \Sigma)((a_n)_{n\in\mathbb{N}}) &= \Delta\left(\left(\sum_{m=0}^{n-1} a_m\right)_{n\in\mathbb{N}}\right) \\
&= \left(\left(\sum_{m=0}^{k-1} a_m\right)_{k=n+1} - \left(\sum_{m=0}^{k-1} a_m\right)_{k=n}\right)_{n\in\mathbb{N}} \\
&= \left(\left(\sum_{m=0}^{n} a_m\right) - \left(\sum_{m=0}^{n-1} a_m\right)\right)_{n\in\mathbb{N}} \\
&= (a_n)_{n\in\mathbb{N}}
\end{aligned}$$

Þetta sýnir að $\Delta \circ \Sigma = \mathrm{id}_{\mathbb{R}^{\mathbb{N}}}$. Ef $p(x) \in \mathbb{R}[x]$ og $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ þá fæst:

$$L\left((x-1) \cdot p(x), \Sigma((a_n)_{n\in\mathbb{N}})\right) = L\left(p(x), \Delta\left(\Sigma((a_n)_{n\in\mathbb{N}})\right)\right) = L(p(x), (a_n)_{n\in\mathbb{N}})$$

Ef $(a_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ er runa sem fullnægir rakningarvenslum með kenninargliðu $p(x) \in \mathbb{R}[x]$ þá er $L(q(x) \cdot p(x), (a_n)_{n\in\mathbb{N}}) = 0$ fyrir öll $q(x) \in \mathbb{R}[x]$. Því fæst

$$\begin{aligned}
L\left(q(x) \cdot (x-1) \cdot p(x), \Sigma((a_n)_{n\in\mathbb{N}})\right) &= L\left((x-1) \cdot q(x) \cdot p(x), \Sigma((a_n)_{n\in\mathbb{N}})\right) \\
&= L(q(x) \cdot p(x), (a_n)_{n\in\mathbb{N}}) \\
&= 0
\end{aligned}$$

fyrir öll $q(x) \in \mathbb{R}[x]$. Þetta sýnir að $\Sigma((a_n)_{n\in\mathbb{N}})$ fullnægir línulegum rakningarvenslum með kennimargliðu $(x-1)\cdot p(x)$.

Gerum ráð fyrir að $s(x) \in \mathbb{R}[x]$ og $m \in \mathbb{N}$, $m \geqslant \deg(s(x))$. Látum $(a_n)_{n\in\mathbb{N}} = (s(n))_{n\in\mathbb{N}}$. Þá fæst:

$$\begin{aligned}
\Delta((a_n)_{n\in\mathbb{N}}) &= \Delta((s(n))_{n\in\mathbb{N}}) \\
&= (s(n+1) - s(n))_{n+1} \\
&= \left(\left(\sum_{k=0}^{m} s_k(n+1)^k\right) - \left(\sum_{k=0}^{m} s_k n^k\right)\right)_{n\in\mathbb{N}} \\
&= \left(\left(\sum_{k=0}^{m} s_k \left(\sum_{i=0}^{k} \binom{k}{i} n^i\right)\right) - \left(\sum_{k=0}^{m} s_k n^k\right)\right)_{n\in\mathbb{N}} \\
&= \left(\left(\sum_{k=0}^{m} \left(\sum_{i=k}^{m} \binom{i}{k} s_i\right) n^k\right) - \left(\sum_{k=0}^{m} s_k n^k\right)\right)_{n\in\mathbb{N}} \\
&= \left(\sum_{k=0}^{m} \left(\left(\sum_{i=k}^{m} \binom{i}{k} s_i\right) - s_k\right) n^k\right)_{n\in\mathbb{N}} \\
&= \left(\left(\sum_{k=0}^{m-1} \left(\sum_{i=k}^{m} \binom{i}{k} s_i\right) - s_k\right) n^k\right)_{n\in\mathbb{N}} \\
&= (t(n))_{n\in\mathbb{N}}
\end{aligned}$$

Þar sem $t(x) = \left(\sum_{k=0}^{m-1} \left(\sum_{i=k}^{m} \binom{i}{k} s_i\right) - s_k\right) x^k \in \mathbb{R}[x]$ og $\deg(t(x)) < m$. Þetta sýnir að $\Delta((s(n))_{n\in\mathbb{N}}) = (t(n))_{n\in\mathbb{N}}$ þar sem $\deg(t(n)) \leqslant \deg(s(n)) - 1$.

Með öðrum orum þá höfum við sannað að ef $s(x) \in \mathbb{R}[x]$ þá er

$$(L(x^n \cdot (x-1), (s(k))_{k\in\mathbb{N}}))_{n\in\mathbb{N}} = (L(x^n, \Delta((s(k))_{k\in\mathbb{N}})))_{n\in\mathbb{N}} = (L(x^k, (t(n))_{k\in\mathbb{N}}))_{n\in\mathbb{N}}$$

þar sem $t(x) \in \mathbb{R}[x]$ og $\deg(t(x)) \leqslant \deg(s(x)) - 1$.

Með þrepun á $k \in \mathbb{N}$ fæst því að ef $s(x) \in \mathbb{R}[x]$ að

$$(L(x^n \cdot (x-1)^k, (s(m))_{m\in\mathbb{N}}))_{n\in\mathbb{N}} = (L(x^n, (t(m))_{m\in\mathbb{N}}))_{n\in\mathbb{N}}$$

Þar sem $t(x) \in \mathbb{R}[x]$ og $deg(t(x)) \leqslant \deg(s(x)) - k$. Sér í lagi fæst að ef $k > \deg(s(x))$ að $\deg(t(x)) < 0$ það er $t(x) = 0$. Við fáum því að ef $k \in \mathbb{N}$, $s(x) \in \mathbb{R}[x]$, $k > \deg(s(x))$ að

$$L(x^n \cdot (x-1)^k, (s(m))_{m\in\mathbb{N}}) = L((x-1)^k, (0)_{m\in\mathbb{N}}) = 0$$

fyrir öll $n \in \mathbb{N}$. Þetta sýnir að $(s(n))_{n\in\mathbb{N}}$ fullnægir línulegum rakningarvenslum með kennimargliðuna $(x-1)^k$ þar sem $k > \deg(s(x))$.

Gerum nú ráð fyrir að $s(x) \in \mathbb{R}[x]$ og $\deg(s(x)) = m \in \mathbb{N}$. Þá er $L(q(x)\cdot(x-1)^{m+1}, (s(n))_{n\in\mathbb{N}}) = 0$ fyrir öll $q(x) \in\in \mathbb{R}[x]$. Fyrir öll $q(x) \in \mathbb{R}[x]$ fæst því:

$$\begin{aligned}
L\left(q(x)\cdot(x-1)^{m+2}, \Sigma((s(n))_{n\in\mathbb{N}})\right) &= L\left((x-1)\cdot q(x)\cdot(x-1)^{m+1}, \Sigma((s(n))_{n\in\mathbb{N}})\right) \\
&= L(q(x)\cdot(x-1)^{m+1}, (s(n)_{n\in\mathbb{N}})) \\
&= 0
\end{aligned}$$

Það er $\left(\sum_{k=0}^{n-1} s(k)\right)_{n\in\mathbb{N}} = \Sigma((s(n))_{n\in\mathbb{N}})$ fullnægir raknigarvenslum með kennimargliðu $(x-1)^{m+2}$. Ef $n \in \mathbb{N}$ þá er

$$x^n \equiv \sum_{i=0}^{m+1} \left(\sum_{k=i}^{m+1} \binom{k}{i} (-1)^{k-i}\right) x^i \mod (x-1)^{m+2}$$

Við fáum því:

$$\begin{aligned}\sum_{k=0}^{n-1} s(k) &= L\left(x^n, \Sigma((s(k))_{k\in\mathbb{N}})\right)\\ &= L\left(\sum_{i=0}^{m+1}\left(\sum_{k=i}^{m+1}\binom{k}{i}(-1)^{k-i}\right)x^i, \Sigma((s(k))_{k\in\mathbb{N}})\right)\\ &= \sum_{i=0}^{m+1}\left(\sum_{k=i}^{m+1}\binom{k}{i}(-1)^{k-i}\right)\cdot\left(\sum_{j=0}^{i-1} s(j)\right)\\ &= t(n)\end{aligned}$$

Þar sem $t(n) \in \mathbb{R}[x]$, $\deg(t(x)) \leqslant m+1 = \deg(s(x))+1$.

Sér í lagi þá sést að $\sum_{k=0}^{n-1} s(k) = t(n)$ þar sem $t(x) \in \mathbb{R}[x]$ og $\deg(s(x))+1 \geqslant \deg(t(x))$.

Algebra línulegra rakningavensla

Gerum ráð fyrir að $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ séu runur sem fullnægi línulegum rakningarvenslum með kennimargliður $p(x), q(x) \in \mathbb{R}[x]$, í þessari röð. Hvað getum við sagt um runurnar $(a_n + b_n)_{n\in\mathbb{N}}$ og $(a_n \cdot b_n)_{n\in\mathbb{N}}$? Eru þær líka gefnar með línulegum rakningarvenslum og getum við þá fundið þau? Svarið við þessu er já eins og nú verður sýnt.

Byjum á því að sanna að summa runa sem gefnar eru með rakningarvenslum séu gefin með rakingarvenslum. Gerum ráð fyrir að $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ séu runur sem fullnægja rakningarvenslum með kennimargliður $p(x), q(x) \in \mathbb{R}[x]$, í þessari röð. Látum $r(x) \in \mathbb{R}[x]$ vera þá stöðluð margliðu sem er minnsta samfeldi $p(x)$ og $q(x)$ (hún er $\frac{p(x)\cdot q(x)}{d(x)}$ þar sem $d(x)$ er sú staðala margliða sem er stærsti samdeilir $p(x)$ og $q(x)$). Fyrir öll $s(x) \in \mathbb{R}[x]$ fæst nú:

$$\begin{aligned}L(s(x)\cdot r(x), (a_n+b_n)_{n\in\mathbb{N}}) &= L(s(x)\cdot r(x), (a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}})\\ &= L(s(x)\cdot r(x), (a_n)_{n\in\mathbb{N}}) + L(s(x)\cdot r(x), (b_n)_{n\in\mathbb{N}})\\ &= 0+0\\ &= 0\end{aligned}$$

þar sem $p(x) \mid s(x)\cdot r(x)$ og $q(x) \mid s(x)\cdot r(x)$. Þetta sýnir að $(a_n+b_n)_{n\in\mathbb{N}}$ fullnægir rakningarvenslum með kennimargliðu $r(x)$.

Snúnara er að sýna að margfeldi runa sem fullnægja línulegum rakningarvenslum fullnægi línulegum rakningarvenslum.

Rétt eins og $\mathbb{R}[x]$ er mengi allra $\mathbb{R}$-margliða í breytinni x þá er $\mathbb{R}[x,y]$ mengi allra $\mathbb{R}$-margliða í breytunum x og y. Lesandi getur auðveldlega sannfært sig að við höfum samlagningu, margföldun með fasta og margfeldi margliða og með þessu þá verður $\mathbb{R}[x,y]$ að $\mathbb{R}$-vigurrúmi. Ef $p(x,y) \in \mathbb{R}[x,y]$ þá táknum við stuðul $p(x,y)$ við $x^m y^n$ með $p_{m,n}$.

Látum $\mathbb{R}^{\mathbb{N}^2}$ vera mengi allar „runa“ með vísamengið $\mathbb{N}^2 = \mathbb{N}\times\mathbb{N}$. Við táknum stak í $\mathbb{R}^{\mathbb{N}^2}$ með $(a_{m,n})_{(m,n)\in\mathbb{N}^2}$. Við höfum margföldun með fasta, $c\cdot(a_{m,n})_{(m,n)\in\mathbb{N}^2} = (c\cdot a_{m,n})_{(m,n)\in\mathbb{N}^2}$ og samlagningu runa $(a_{m,n})_{(m,n)\in\mathbb{N}^2} + (b_{m,n})_{(m,n)\in\mathbb{N}^2} = (a_{m,n}+b_{m,n})_{(m,n)\in\mathbb{N}^2}$. Með þessu má auðveldlega sjá að $\mathbb{R}^{\mathbb{N}^2}$ er $\mathbb{R}$-vigurrúm.

Rétt eins og við skilgreindum tvílínuleguvörunin $L : \mathbb{R}[x]\times\mathbb{R}^{\mathbb{N}} \to \mathbb{R}$ þá getum við skilgreint vörpun $K : \mathbb{R}[x,y]\times\mathbb{R}^{\mathbb{N}^2} \to \mathbb{R}$, $(p(x,y), (a_{m.n})_{(m,n)\in\mathbb{N}^2}) \mapsto \sum_{(m,n)\in\mathbb{N}^2} p_{m,n}\cdot a_{m,n}$. Þar sem aðeins endanlega mörg $p_{m,n} \neq 0$ þá er ljóst að þetta er er vel skilgreind vörpun. Lesandi getur auðveldlega sannfært sig um að K er tvílínuleg. Ef $s,t \in \mathbb{N}$, $p(x,y) \in \mathbb{R}[x,y]$ og $(a_{n,m})_{(m,n)\in\mathbb{N}^2}$ þá fæst auðveldlega að $K(x^s y^t \cdot p(x,y), (a_{m,n})_{(m,n)\in\mathbb{N}^2}) = K(p(x,y), (a_{m+s,n+t})_{(m,n)\in\mathbb{N}^2})$.

Gerum ráð fyrir að $I \subseteq \mathbb{R}[x,y]$ þannig að $0 \in I$, $p(x,y) + q(x+y) \in I$ ef $p(x,y), q(x,y) \in I$ og $r(x,y) \cdot p(x,y) \in I$ ef $r(x,y) \in \mathbb{R}[x,y]$ og $p(x,y) \in I$. Þá kallast I íðal í $\mathbb{R}[x,y]$.

Gerum ráð fyrir að $I \subseteq \mathbb{R}[x,y]$ sé íðal í $\mathbb{R}[x,y]$. Ef $p(x,y), q(x,y) \in \mathbb{R}[x,y]$ og $q(x,y) - p(x,y) \in I$ þá segjum við að $p(x,y)$ og $q(x,y)$ séu samleifa mát (modulo) I. Við ritum þá $p(x,y) \equiv q(x,y) \mod I$. Eftirfarndi hjálparsetningu má sanna á sama hátt og setningu 2.5:

Hjálparsetning 7.1. *Gerum ráð fyrir að $I \subseteq \mathbb{R}[x,y]$ sé íðal. Þá gildir:*

1. *Ef $p(x,y) \in \mathbb{R}[x,y]$ þá er $p(x,y) \equiv 0 \mod I$ ef og aðeins ef $p(x,y) \in I$.*
2. *Ef $p(x,y) \in \mathbb{R}[x,y]$ þá er $p(x,y) \equiv p(x,y) \mod I$.*
3. *Ef $p(x,y), q(x,y) \in \mathbb{R}[x,y]$ og $p(x,y) \equiv q(x,y) \mod I$ þá er $q(x,y) \equiv p(x,y) \mod I$.*
4. *Ef $p(x,y), q(x,y), r(x,y) \in \mathbb{R}[x,y]$, $p(x,y) \equiv q(x,y) \mod I$ og $q(x,y) \equiv r(x,y) \mod I$ þá er $p(x,y) \equiv r(x,y) \mod I$.*
5. *Ef $c \in \mathbb{R}$, $p(x,y), q(x,y) \in \mathbb{R}[x,y]$ og $p(x,y) \equiv q(x,y) \mod I$ þá er $c \cdot p(x,y) \equiv c \cdot q(x,y) \mod I$.*
6. *Ef $p(x,y), q(x,y), r(x,y), s(x,y) \in \mathbb{R}[x,y]$, $p(x,y) \equiv r(x,y) \mod I$ og $q(x,y) \equiv s(x,y) \mod I$ þá er $p(x,y) + q(x,y) \equiv r(x,y) + s(x,y) \mod I$.*
7. *Ef $p(x,y), q(x,y), r(x,y), s(x,y) \in \mathbb{R}[x,y]$, $p(x,y) \equiv r(x,y) \mod I$ og $q(x,y) \equiv s(x,y) \mod I$ þá er $p(x,y) \cdot q(x,y) \equiv r(x,y) \cdot s(x,y) \mod I$.*

Sönnun. Sönnun eftirlátin lesanda. □

Fyrir íðal $I \subseteq \mathbb{R}[x,y]$ og $p(x,y)$ þá látum við $[p(x,y)]_I = \{q(x,y) \in \mathbb{R}[x,y] \mid q(x,y) \equiv p(x,y) \mod I\}$. Ljóst er að $p(x,y) \in [p(x,y)]_I$ og $q(x,y) \in [p(x,y)]_I$ ef og aðeins ef $[p(x,y)]_I = [q(x,y)]_I$. Látum $\mathbb{R}[x,y]/I = \{[p(x,y)]_I \mid p(x,y) \in \mathbb{R}[x,y]\}$.

Við viljum skilgreina samlagningu, margföldun og margföldun með rauntölu á $\mathbb{R}[x,y]/I$.

Gerum ráð fyrir að $a \in \mathbb{R}[x,y]/I$. Þá er til $p(x,y) \in \mathbb{R}[x,y]$ þannig að $a = [p(x,y)]_I$. Fyrir $c \in \mathbb{R}$ þá látum við $c \cdot a = [c \cdot p(x,y)]_I$. Ljóst er að það $p(x,y) \in \mathbb{R}[x,y]$ þannig að $a = [p(x,y)]_I$ hefur ekki áhrif á niðurstöðuna $c \cdot a$ þar sem ef $p(x,y), q(x,y) \in \mathbb{R}[x,y]$ og $[p(x,y)]_I = a = [q(x,y)]_I$ þá er $p(x,y) \equiv q(x,y) \mod I$ og af hjálparsetningu 7.1 leiðir að $c \cdot p(x,y) \equiv c \cdot q(x,y) \mod I$, það er $[c \cdot p(x,y)]_I = [c \cdot q(x,y)]_I$.

Gerum ráð fyrir að $a, b \in \mathbb{R}[x,y]/I$. Þá má finna $p(x,y), q(x,y) \in \mathbb{R}[x,y]$ þannig að $a = [p(x,y)]_I$ og $b = [q(x,y)]_I$. Þá látum við $a + b = [p(x,y) + q(x,y)]_I$ og $a \cdot b = [p(x,y) \cdot q(x,y)]_I$. Með því að skoða hjálparsetningu 7.1 sést að $a + b$ og $a \cdot b$ er óháð valin á $p(x,y), q(x,y) \in \mathbb{R}[x,y]$ þannig að $a = [p(x,y)]_I$ og $b = [q(x,y)]_I$.

Við höfum nú:

Setning 7.1. *Gerum ráð fyrir að $I \subseteq \mathbb{R}[x,y]$ sé íðal. Þá gildir:*

1. *Ef $a, b, c \in \mathbb{R}[x,y]/I$ þá er $a + (b + c) = (a + b) + c$ og $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.*
2. *Ef $a, b \in \mathbb{R}[x,y]/I$ þá er $a + b = b + a$ og $a \cdot b = b \cdot a$.*
3. *Ef $a \in \mathbb{R}[x,y]/I$ þá er $a + [0]_I = [0]_I + a = a$ og $a \cdot [1]_I = [1]_I \cdot a = a$. Það er $0 \coloneqq [0]_I$ og $1 \coloneqq [1]_I$ eru samlagningarhlutleysa og margföldunarhlutleysa fyrir $\mathbb{R}[x,y]/I$.*
4. *Ef $a \in \mathbb{R}[x,y]/I$ og $a = [p(x,y)]_I$ þar sem $p(x,y) \in \mathbb{R}[x,y]$ og $b = [-p(x,y)]_I$ þá er $a + b = b + a = 0$. Það er $-a = [-p(x,y)]_I$.*
5. *$a, b, c \in \mathbb{R}[x,y]/I$ þá er $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ og $(a + b) \cdot c)(a \cdot c) + (b \cdot c)$.*
6. *Ef $a \in \mathbb{R}[x,y]/I$ og $1 \in \mathbb{R}$ þá er $1 \cdot a = a$.*
7. *Ef $r \in \mathbb{R}$ og $a, b \in \mathbb{R}[x,y]/I$ þá er $r \cdot (a + b) = (r \cdot a) + (r \cdot b)$.*

8. *Ef* $r, s \in \mathbb{R}$ *og* $a \in \mathbb{R}[x,y]/I$ *þá er* $(r+s)\cdot a = (r\cdot a) + (s\cdot a)$.

9. *Ef* $r, s \in \mathbb{R}$ *og* $a \in \mathbb{R}[x,y]/I$ *þá er* $(r\cdot s)\cdot a = r\cdot(s\cdot a)$.

Þetta þýðir sér í lagi að $\mathbb{R}[x,y]/I$ *er línulegt rúm yfir* $\mathbb{R}$. *Náttúrlega ofanvarpið* $\mathrm{pr}_I : \mathbb{R}[x,y] \to \mathbb{R}[x,y]/I$, $p(x,y) \mapsto [p(x,y)]_I$ *er línuleg vörpun. Enn fremur gildir að* $\mathrm{pr}_I(p(x,y)\cdot q(x,y)) = \mathrm{pr}_I(p(x,y))\cdot \mathrm{pr}_I(q(x,y))$.

Sönnun. Sönnun er eftirlátin lesanda. □

Gerum ráð fyrir að $p(x), q(x) \in \mathbb{R}[x]$. Látum $I = p(x)\cdot\mathbb{R}[x,y] + q(y)\cdot\mathbb{R}[x,y] = \{p(x)\cdot r(x,y) + q(y)\cdot s(x,y) \mid r(x,y), s(x,y) \in \mathbb{R}[x,y]\}$. Auðvelt er að sjá að $I \subseteq \mathbb{R}[x,y]$ er íðal. Sýna má að fyrir sérhvert $s(x,y) \in \mathbb{R}[x,y]$ þá er til (ótvírætt) $r(x,y) \in \mathbb{R}[x,y]$ þannig að $r(x,y) = \sum_{\substack{(m,n)\in \\ [[0,\deg(p(x))-1]] \\ \times[[0,\deg(q(x))-1]]}} r_{m,n}x^m y^n$ og $s(x,y) \equiv r(x,y) \mod I$ þar sem $[[0,s]] = \{0,1,\ldots,s\}$ þar sem $s \in \mathbb{N}$. Þar af leiðir að $B = \{[x^m y^n]_I \mid (m,n) \in [[0,\deg(p(x))-1]] \times [[0,\deg(q(x))-1]]\}$ spannar $\mathbb{R}[x,y]/I$ og B er línulega óháð (yfir $\mathbb{R}$). Þar af leiðir er B grunnur fyrir $\mathbb{R}[x,y]/I$. Þar sem B hefur $m\cdot n$ stök þá er ljóst að $\mathbb{R}[x,y]/I$ er $m\cdot n$ vítt vigurrúm yfir $\mathbb{R}$.

Gerum nú ráð fyrir að $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ fullnægi línulegum rakningarvenslum með kenni margliður $p(x), q(x) \in \mathbb{R}[x]$, í þessari röð. Látum $I = p(x)\cdot\mathbb{R}[x,y] + q(y)\cdot\mathbb{R}[x,y]$ eins og áður. Gerum ráð fyrir að $m_0, n_0 \in \mathbb{N}$. Þá fæst:

$$\begin{aligned}
K(x^{m_0}y^{n_0}\cdot p(x), (a_m\cdot b_n)_{(m,n)\in\mathbb{N}^2}) &= K(p(x), (a_{m+m_0}\cdot b_{n+n_0})_{(m,n)\in\mathbb{N}^2}) \\
&= \sum_{m\in\mathbb{N}} p_m \cdot a_{m+m_0}\cdot b_{n+n_0} \\
&= \left(\sum_{m\in\mathbb{N}} p_m\cdot a_{m+m_0}\right)\cdot b_{n_0} \\
&= L(p(x), (a_{m+m_0})_{m\in\mathbb{N}})\cdot b_{n_0} \\
&= L(x^{m_0}\cdot p(x), (a_m)_{m\in\mathbb{N}})\cdot b_{n_0} \\
&= 0\cdot b_{n_0} \\
&= 0
\end{aligned}$$

Þar sem K er tvílínuleg þá fæst að $K(s(x,y)\cdot p(x), (a_m\cdot b_n)_{(m,n)\in\mathbb{N}^2}) = 0$ fyrir öll $s(x,y) \in \mathbb{R}[x,y]$.

Eins má sanna að $K(t(x,y)\cdot q(y), (a_m\cdot b_n)_{(m,n)\in\mathbb{N}^2}) = 0$ fyrir öll $t(x,y) \in \mathbb{R}[x,y]$.

Gerum nú ráð fyrir að $r(x,y) \in I$. Þá eru til $s(x,y), t(x,y) \in \mathbb{R}[x,y]$ þannig að $r(x,y) = s(x,y)\cdot p(x) + t(x,y)\cdot q(y)$. Þá fæst:

$$\begin{aligned}
K(r(x,y), (a_m\cdot b_n)_{(m,n)\in\mathbb{N}^2}) &= K(s(x,y)\cdot p(x) + t(x,y)\cdot q(y), (a_m\cdot b_n)_{(m,n)\in\mathbb{N}^2}) \\
&= K(s(x,y)\cdot p(x), (a_m\cdot b_n)_{(m,n)\in\mathbb{N}^2}) + K(t(x,y)\cdot q(y), (a_m\cdot b_n)_{(m,n)\in\mathbb{N}^2}) \\
&= 0 + 0 \\
&= 0
\end{aligned}$$

Það er $K(r(x,y), (a_m\cdot b_n)_{(m,n)\in\mathbb{N}^2}) = 0$ fyrir öll $r(x,y) \in I$. Við ályktum að ef $c(x,y), d(x,y) \in \mathbb{R}[x,y]$ og $c(x,y) \equiv d(x,y) \mod I$ þá er $K(c(x,y), (a_m\cdot b_n)_{(m,n)\in\mathbb{N}^2}) = K(d(x,y), (a_m\cdot b_n)_{(m,n)\in\mathbb{N}^2})$.

Við getum því skilgreint vörpun $J : \mathbb{R}[x,y]/I \to \mathbb{R}$, $[p(x,y)]_I \mapsto K(p(x,y), (a_m\cdot b_n)_{(m,n)\in\mathbb{N}^2})$. Þessi vörpun er vel skilgreind þar sem $K(p(x,y), (a_m\cdot b_n)_{(m,n)\in\mathbb{N}^2})$ tekur sama gildi fyrir öll $p(x,y) \in [p(x,y)]_I$. Ljóst er að J er línuleg vörpun.

Látum $z = [xy]_\in K[x,y]/I$. Nú eru $1, z, z^2, \ldots$ öll í $K[x,y]/I$ og þar sem $K[x,y]/I$ er endanlega vítt sem vigurrúm yfir $\mathbb{R}$ þá er til $k \in \mathbb{N}$ þannig að $\{1, z, z^2, \ldots, z^k\}$ séu háð. Við megum gera ráð fyrir að $k \in \mathbb{N}$

sé minnsta talan þannig að $1, z, z^2, \ldots, z^k$ séu línulega háð. Þá eru til $(c_0, c_1, \ldots, c_k) \in \mathbb{R}^{k+1} \backslash \{\vec{0}\}$ þannig að $\sum_{i=0}^{k} c_i z^i = 0$.

Setjum sem svo að $c_k = 0$. Þá er $(c_0, c_1, \ldots, c_{k-1}) \in \mathbb{R}^k \backslash \{\vec{0}\}$ og $0 = \sum_{i=0}^{k} c_i \cdot z^i = \sum_{i=0}^{k-1} c_i \cdot z^i$ en það þýðir að $1, z, z^2, \ldots, z^{k-1}$ séu línulega háð. Þar sem $k-1 < k$ og k er minnsta talan þannig að $1, z, z^2, \ldots, z^k$ séu línulega háð þá er þetta mótsögn. Við ályktum að $c_k \neq 0$. Með því að skipta c_i út fyrir $\frac{c_i}{c_k}$ þá má gera ráð fyrir að $c_k = 1$. Látum $r(X) = \sum_{i=0}^{k} c_i X^i$. Þá er $r(X) \in \mathbb{R}[X]$ stöðluð margliða og $r(z) = 0 \in \mathbb{R}[x, y]/I$.

Gerum ráð fyrir að $s(X) \in \mathbb{R}[X]$. Þá er $s(xy) \in K[x, y]$. Nú fæst:

$$\begin{aligned} L(s(X) \cdot r(X), (a_n \cdot b_n)_{n\in\mathbb{N}}) &= K(s(xy) \cdot r(xy), (a_m \cdot b_n)_{(m,n)\in\mathbb{N}^2}) \\ &= J(s(z) \cdot r(z)) \\ &= J(s(z) \cdot 0) \\ &= J(0) \\ &= 0 \end{aligned}$$

Þetta sýnir að $(a_n \cdot b_n)_{n\in\mathbb{N}}$ fullnægir línulegum rakningarvenslum með kennimargliðuna $r(X) \in \mathbb{R}[X]$.

Við sjáum t.d. strax að þar sem Fibonacci tölurnar $(\mathrm{fib}_n)_{n\in\mathbb{N}}$ fullnægja línulegum rakningarvenslum með kennimargliðuna $p(x) = x^2 - x - 1$ þá fullnægir $(\mathrm{fib}_n{}^2)_{n\in\mathbb{N}}$ línulegum rakningarvenslum. Lesanda má spreyta sig á því að finna þau.