

Julenød

Lad os først bemærke at ifølge definitionen i opgaven er \mathbb{R}^2 en algebraisk kurve givet som nulpunkterne af nul-polynomiet. Hvis vi tillader denne algebraiske kurve er alle opgaverne trivielle. Vi vælger derfor at betragte \mathbb{R}^2 som et patologisk eksempel på en algebraisk kurve og undlader at betragte dette som en gyldig løsning til opgaverne.

Eksempel 1. *Definer polynomierne:*

$$\begin{aligned} p_1(t) &= t^2 & q_1(t) &= t^3 & f_1(t) &= (p_1(t), q_1(t)) \\ p_2(t) &= t^2 + t & q_2(t) &= t^3 & f_2(t) &= (p_2(t), q_2(t)) \\ p_3(t) &= t^2 + t & q_3(t) &= t^2 & f_3(t) &= (p_3(t), q_3(t)) \\ P_1(x, y) &= x^3 - y^2 \\ P_2(x, y) &= x^3 - 3xy - y^2 - y \\ P_3(x, y) &= x^2 + y^2 - 2xy - y \end{aligned}$$

Da har vi:

$$\begin{aligned} P_1(p_1(t), q_1(t)) &= (t^2)^3 - (t^3)^2 = 0 \\ P_2(p_2(t), q_2(t)) &= (t^2 + t)^3 - 3t^3(t^2 + t) - (t^3)^2 - t^3 = 0 \\ P_3(p_3(t), q_3(t)) &= (t^2 + t)^2 + (t^2)^2 - 2(t^2 + t)t^2 - t^2 = 0 \end{aligned}$$

hvilket viser at billedet af f_i er indeholdt i den algebraiske kurve bestemt af P_i for $i \in \{1, 2, 3\}$.

Graden af polynomier i flere variabler

Lad os først for at kunne tale om specifikke led sige at leddet $ax^i y^j$ har 2-graden (i, j) . Dette er ikke vores foreslag til en grad-funktion, men vi vil benytte denne terminologi i beviserne.

Lad $-\infty$ være et element som ikke er i \mathbb{N}_0 og definer $\mathbb{N}^* = \mathbb{N}_0 \cup \{-\infty\}$. Udvid da addition i \mathbb{N}_0 ved at lade $(-\infty) + x = x + (-\infty) = -\infty$ for alle $x \in \mathbb{N}_0$ og lad $x + y$ være defineret som sædvanlig når $x, y \in \mathbb{N}_0$. 0 er et enhedselement for denne mængde da $0 + x = x + 0 = x$ for $x \in \mathbb{N}^*$ og $0 + (-\infty) = (-\infty) + 0 = -\infty$. Yderligere ser vi at denne addition er associativ og kommutativ. Generelt har et element ikke en invers (kun 0 har en invers). Vi udvider den sædvanlige ordning $<$ af \mathbb{N}_0 til \mathbb{N}^* ved at lade $-\infty < x$ for alle $x \neq -\infty$. Dette er stadig en total ordning.

Når vi tænker på polynomierne i $\mathbb{F}[x]$ eller $\mathbb{F}[x, y]$ falder det os naturligt at give disse mængder additiv og multiplikativ struktur. Disse strukturer opfylder både associativitet og har enheder. Den additive struktur er faktisk en gruppestruktur, men da vi ingen gruppe struktur har på \mathbb{N}^* ser vi bort fra bevarelse af inverser. Den additive og multiplikative struktur er forbundet af distributivitet:

$$p \cdot (q + r) = pq + pr$$

hvor p, q, r er polynomier i enten $\mathbb{F}[x]$ eller $\mathbb{F}[x, y]$. På samme måde ser vi at \mathbb{N}^* kan gives algebraisk struktur. Den naturlige struktur er den additive, men udover den ser vi at vi har en yderligere struktur givet ved at tage maksimum af elementer. Lad os kalde denne struktur max-strukturen på \mathbb{N}^* . Vi har:

1. Identitet: $\max(x, -\infty) = \max(-\infty, x) = x$ for alle $x \in \mathbb{N}^*$ så $-\infty$ er en identitet.
2. Kommutativitet: $\max(x, y) = \max(y, x)$ for alle $x, y \in \mathbb{N}^*$.
3. Associativitet: $\max(x, \max(y, z)) = \max(x, y, z) = \max(\max(x, y), z)$ for alle $x, y, z \in \mathbb{N}^*$.
4. Addition er distributiv over max: $x + \max(y, z) = \max(x + y, x + z)$ for alle $x, y, z \in \mathbb{N}^*$.

Med undtagelse af at elementer ikke generelt har inverser med hensyn til max minder strukturen over \mathbb{N}^* meget om strukturen over $\mathbb{F}[x]$ eller $\mathbb{F}[x, y]$. Det er denne struktur som deg bevarer hvor den additive struktur over $\mathbb{F}[x]$ svarer til max-strukturen over \mathbb{N}^* , og den multiplikative struktur over $\mathbb{F}[x]$ svarer til den additive struktur over \mathbb{N}^* . $\deg : \mathbb{F}[x] \rightarrow \mathbb{N}^*$ er nemlig unikt bestemt af følgende egenskaber:

1. Identiteter bevares: $\deg(0) = -\infty$, $\deg(1) = 0$.
2. Operationer respekteres:

$$\deg(pq) = \deg(p) + \deg(q)$$

og hvis p og q ingen led har tilfælles:

$$\deg(p + q) = \max(\deg(p), \deg(q))$$

for alle polynomier p og q .

3. $\deg(x) = 1$ (garanterer at deg er surjektiv).

Dette giver anledning til følgende generalisering:

Sætning 1. *Lad \mathbb{F} være et vilkårligt legeme. Da eksisterer der en unik funktion $D : \mathbb{F}[x, y] \rightarrow \mathbb{N}^*$ som opfylder:*

1. $D(0) = -\infty$, $D(1) = 0$.
2. For alle $p, q \in \mathbb{F}[x, y]$ har vi:

$$D(pq) = D(p) + D(q)$$

og hvis p og q ingen led har tilfælles:

$$D(p + q) = \max(D(p), D(q))$$

3. $D(x) = D(y) = 1$.

Vi kalder $D(p)$ for graden af p og betegner ofte denne værdi med $\deg(p)$.

Bevis. Vi skal her vise både eksistens og unikhed. Lad os starte med at vise eksistens af en sådan funktion. Lad $p \in \mathbb{F}[x, y]$ være et givent polynomium. p har endelig mange led og de har alle en unik 2-grad. Lad $I(p) \subseteq \mathbb{N}_0^2$ betegne den endelige mængde af 2-grader så $(i, j) \in I(p)$ hvis og kun hvis der eksisterer et

led på formen $\lambda x^i y^j$ med $\lambda \neq 0$ i p . For en 2-grad (i, j) lad $\varphi_p(i, j) \neq 0$ betegne koefficienten for leddet i p med 2-graden (i, j) . Vi har da følgende udtryk for p :

$$p = \sum_{(i,j) \in I(p)} \varphi_p(i, j) x^i y^j$$

Definer da graden af p som:

$$D(p) = \sup \{i + j \mid (i, j) \in I(p)\}$$

Lad os først bekræfte egenskab 1 og 3. Polynomiet 0 har ingen led så $D(0) = \sup(\emptyset)$. Da alle elementer er en øvre grænse for \emptyset og $-\infty$ er det mindste element har vi dermed: $D(0) = -\infty$. Polynomiet 1 har præcis ét led, nemlig leddet med 2-grad $(0, 0)$ og koefficient 1 i $(0, 0)$. Derfor har vi:

$$D(1) = \sup(\{0\}) = 0$$

Vi har nu vist at D opfylder egenskab 1. x har præcis et led; nemlig leddet med 2-grad $(1, 0)$ så vi har $D(x) = \sup(\{1\}) = 1$ og på samme måde har vi $D(y) = 1$. Lad os nu betragte to polynomier $p, q \in \mathbb{F}[x, y]$ givet som før ved:

$$p = \sum_{(i,j) \in I(p)} \varphi_p(i, j) x^i y^j \quad q = \sum_{(i,j) \in I(q)} \varphi_q(i, j) x^i y^j$$

Vi ser dermed at

$$I(pq) = \{(i + i', j + j') \mid (i, j) \in I(p), (i', j') \in I(q)\}$$

så hvis (i, j) er en maksimal 2-grad i p og (i', j') er en maksimal 2-grad i q har vi:

$$D(pq) = i + j + i' + j' = D(p) + D(q)$$

Antag at (i, j) er en maksimal 2-grad i $p + q$ og at p og q ingen led har tilfælles. Da er $\varphi_{p+q}(i, j) \neq 0$ så enten p eller q har også et led med 2-grad (i, j) hvilket viser at $p + q$ aldrig kan have højere grad end både p og q og dets højeste led forekommer også i enten p eller. Dermed har vi:

$$D(p + q) = \max(D(p), D(q))$$

Vi har nu vist eksistensen af en funktion som egenskab 1 – 3.

Vi vil nu vise unikhed. Lad $D : \mathbb{F}[x, y] \rightarrow \mathbb{N}^*$ være som før og lad $D' : \mathbb{F}[x, y] \rightarrow \mathbb{N}^*$ være en vilkårlig funktion som opfylder egenskab 1 – 3. Vi vil vise at $D' = D$. For en skalar $\lambda \in \mathbb{F} - \{0\}$ har vi:

$$0 = D'(1) = D'(\lambda^{-1}\lambda) = D'(\lambda) + D'(\lambda^{-1})$$

$D'(\lambda)$ er altså en additiv invers til $D'(\lambda^{-1})$, men da det eneste element med en additiv invers i \mathbb{N}^* er 0 har vi $D'(\lambda) = 0$. For et led $\lambda x^i y^j$ har vi:

$$D'(\lambda x^i y^j) = D(\lambda) + \underbrace{D(x) + \dots + D(x)}_{i \text{ gange}} + \underbrace{D(y) + \dots + D(y)}_{j \text{ gange}} = i + j = D(\lambda x^i y^j)$$

Vi ser altså at D' og D er ens på enkelte led. Antag nu at der eksisterer et polynomium hvor de er forskellige. Lad $p \in \mathbb{F}[x, y]$ være et sådant polynomium

med et minimalt antal led. Vi har allerede vist tilfældet hvor p har et enkelt eller 0 led så p har flere end 1. Lad $\varphi_p(i, j)x^i y^j$ være et vilkårligt led i p . Da har $p' = p - \varphi_p(i, j)x^i y^j$ et led mindre end p og dermed har vi $D(p') = D(p)$ hvilket giver:

$$\begin{aligned} D'(p) &= D'(p' + \varphi_p(i, j)x^i y^j) = \max(D'(p'), D'(\varphi_p(i, j)x^i y^j)) \\ &= \max(D(p'), D(\varphi_p(i, j)x^i y^j)) = D(p) \end{aligned}$$

hvilket er en modstrid da vi antog at D' og D var forskellige på p så vi må have $D = D'$, men da D' var vilkårlig er sætningen vist. \square

Denne sætning gav os den ønskede definition.

Bevis af eksistens

Sætning 2. *Lad $p, q \in \mathbb{F}[t]$ være polynomier i en variabel af grad $m \in \mathbb{N}_0$ eller mindre. For ethvert positive heltal $k > 2m - 3$ eksisterer der et polynomium $F \in \mathbb{F}[x, y]$ af grad mindre end eller lig k så $F(p(t), q(t)) = 0$ for alle $t \in \mathbb{F}$.*

Bevis. Lad $k > 2m - 3$ være givet. Lad V være vektorrummet over \mathbb{F} bestående af alle polynomier i $\mathbb{F}[t]$ af grad mk eller mindre. $1, t, t^2, \dots, t^{mk}$ er en basis for V så:

$$\dim V = mk + 1$$

Lad

$$L = \{(i, j) \in \mathbb{N}_0^2 \mid i + j \leq k\}$$

Da er $|L| = \frac{(k+2)(k+1)}{2}$ fordi for hvert $i \in \{0, \dots, k\}$ må $j \in \{0, 1, \dots, k - i\}$ så vi har $k - i + 1$ valg for j (det er klart at alle valgene er gyldige). Samlet giver det:

$$|L| = \sum_{i=0}^k (k - i + 1) = \sum_{i=1}^{k+1} i = \frac{(k+2)(k+1)}{2}$$

Hvis $i + j \leq k$ har vi:

$$\deg(p^i q^j) = i \deg(p) + j \deg(q) \leq im + jm \leq km$$

Dermed er $p^i q^j \in V$ hvis $(i, j) \in L$ og vi har dermed en funktion $f : L \rightarrow V$ givet ved

$$f(i, j) = p^i q^j$$

Antag først at f ikke er injektiv. Da eksisterer der to forskellige par $(i, j), (i', j') \in L$ så $f(i, j) = f(i', j')$. Definer da $F \in \mathbb{F}[x, y]$ ved:

$$F(x, y) = x^i y^j - x^{i'} y^{j'}$$

Da har F grad $\deg F = \max(i + j, i' + j') \leq k$ og

$$F(p(t), q(t)) = p(t)^i q(t)^j - p(t)^{i'} q(t)^{j'} = 0$$

hvilket viser sætningen hvis f ikke er injektiv.

Antag nu at f er injektiv. Da har vi

$$\begin{aligned} |f(L)| = |L| &= \frac{(k+2)(k+1)}{2} \\ &= \frac{k^2 + 3k + 2}{2} > \frac{k(2m-3) + 3k + 2}{2} = mk + 1 \end{aligned}$$

Så polynomierne i $f(L)$ må være lineært afhængige. Der må altså eksistere værdier $a_{ij} \in \mathbb{F}$ for $(i, j) \in L$ så:

$$\sum_{(i,j) \in L} a_{ij} p^i q^j = 0$$

og ikke alle a_{ij} er 0. Definer da $F \in \mathbb{F}[x, y]$ ved:

$$F(x, y) = \sum_{(i,j) \in L} a_{ij} x^i y^j$$

Da har alle led i F grad mindre end k så F har grad mindre end k , og vi har:

$$F(p(t), q(t)) = \sum_{(i,j) \in L} a_{ij} p(t)^i q(t)^j = 0$$

hvilket viser sætningen hvis f er injektiv. Sætningen er dermed vist i alle tilfælde. \square

Korollar 1. *Lad p, q være vilkårlige reelle polynomier i en variabel. Da er funktionen $f: \mathbb{R} \rightarrow \mathbb{R}^2$ defineret ved $f(t) = (p(t), q(t))$ indeholdt i en algebraisk kurve forskellig fra \mathbb{R}^2 .*

Bevis. Tag $m = \max(\deg(p), \deg(q))$ i forrige sætning. Da siger sætningen at der eksisterer et polynomium $F \in \mathbb{R}[x, y]$ forskellig fra 0 hvorom det gælder $F \circ f = 0$. Da F er forskellig fra nulpolynomiet har vi ikke $F(\mathbb{R}^2) = \{0\}$ og dermed er den algebraiske kurve bestemt ved F forskellig fra \mathbb{R}^2 og billedet af f er indeholdt i den. \square

Graden af P_{min}

Lad os starte med at fastsætte en nedre grænse.

Sætning 3. *Lad $p(t), q(t)$ være polynomier i $\mathbb{F}[t]$ med $m = \deg(p(t)) \leq n = \deg(q(t))$. Lad $P_{min}(x, y)$ være et polynomium af minimal grad der definerer en algebraisk kurve indeholdende $(p(\mathbb{F}), q(\mathbb{F}))$. Da har vi $\frac{n}{\gcd(m, n)} \leq \deg(P_{min}(x, y))$.*

Bevis. Definer $d = \gcd(m, n)$ og lad $m' = m/d, n' = n/d$. Lad $ax^i y^j$ være et led i P_{min} som maksimerer $ni + mj$. Hvis dette led er det eneste som maksimerer $ni + mj$ da har $ap(t)^i q(t)^j$ og $P_{min}(p(t), q(t))$ samme koefficient for t^{mi+nj} og den er ikke 0 hvilket er en modstrid da $P_{min}(p(t), q(t)) = 0$ per antagelse. Dermed må der eksistere et andet led $bx^{i'} y^{j'}$ i $P_{min}(x, y)$ så $mi + nj = m'i' + n'j'$. Da har vi:

$$m'(i - i') = n'(j' - j)$$

Det giver $m'|n'(j - j')$ og da $\gcd(n', m') = 1$ har vi $m'|j - j'$. j og j' er ikke lig hinanden for da ville $(i, j) = (i', j')$. Antag derfor uden tab på generalitet at

$j > j'$. Da $j \equiv j' \pmod{n}$ eksisterer der et heltal $k > 0$ så $j = j' + n'k$ hvilket medfører:

$$j = j' + n'k \geq n'k \geq n'$$

Dette viser at

$$\deg(P_{\min}(x, y)) \geq \deg(ax^i y^j) = i + j \geq j \geq m' = \frac{m}{\gcd(m, n)}$$

hvilket var hvad skulle vises. \square

Eksempel 2. Vi vil i dette eksempel vise at den nedre grænse opnået i sætning 3 er bedst mulig hvis alt vi kender af graden af $p(t)$ og $q(t)$. Betragt ikke-negative heltal $m \leq n$ og definer deres største fælles divisor $d = \gcd(m, n)$ og lad $m' = m/d$, $n' = n/d$. Lad:

$$p(t) = t^m \quad q(t) = t^n \quad P(x, y) = x^{n'} - y^{m'}$$

Da har vi:

$$\deg(P(x, y)) = n' = \frac{n}{\gcd(m, n)}$$

$$P(p(t), q(t)) = (t^m)^{n'} - (t^n)^{m'} = t^{m'n'd} - t^{m'n'd} = 0$$

så billedet af $f(t) = (p(t), q(t))$ er indeholdt i den algebraiske kurve bestemt af P , og P har minimal grad blandt sådanne polynomier ifølge sætning 3. Dette viser at vi ikke kunne have en højere nedre grænse for da ville dette eksempel give en modstrid.