Algoritmer och komplexitet inom kommutativ algebra & algebraisk geometri

Omparametrisering av kurvor, semigrupper, implicit notation & multiplicitetsföljder

Peter Waher

peterwaher@hotmail.com

https://github.com/PeterWaher/Algebraiska_kurvor

12 november 2015

Outline

Outline

Plana algebraiska kurvor

Plana algebraiska kurvor

Plana algebraiska kurvor

Vad är en plan kurva?

Definition

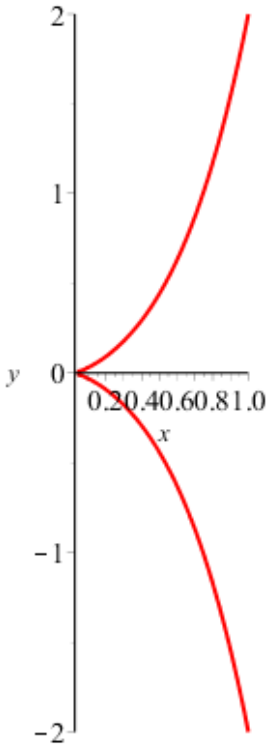
En **plan kurva** C är en delmängd i $\mathbb{C}^2$ sådan att det finns två kontinuerliga funktioner $f : \mathbb{C} \to \mathbb{C}$ och $g : \mathbb{C} \to \mathbb{C}$ sådana att $C = \{(f(t), g(t)) : t \in \mathbb{C}\}$. (f, g) är en **parametrisering** av C. Om C kan parametriseras av två analytiska funktioner f och g kallas C **analytisk**. Om den kan parametriseras av två polynom kallas C för **algebraisk**. Om den kan parametriseras av två formella potensserier kallas C **algebroid**.

Kurvor i det Euklidiska planet

Traditionellt har man ofta studerat plana kurvor i det *Euklidiska planet*. I detta fall är kurvan parametriserad av reellvärda funktioner $f : \mathbb{R} \to \mathbb{R}$ och $g : \mathbb{R} \to \mathbb{R}$.

Exempel

$$C(t) = (t^2, t^3 + t^7)$$



Not: För att förenkla notationen kan vi identifiera kurvan C med en viss parametrisering (f, g), även om parametriseringen inte är unik. Detta görs enklast genom att identifiera kurvan med funktionen $C : \mathbb{C} \to \mathbb{C}^2$, $C(t) = (f(t), g(t))$. Notera dock att kurvan som sådan och en av dess parametriseringar är två olika objekt.

Förenklingar

Förenklingar vi kan göra om vi studerar en plan kurva lokalt:

1. Tillräckligt att studera *algebraiska* kurvor:

Förenklingar

Förenklingar vi kan göra om vi studerar en plan kurva lokalt:

1. Tillräckligt att studera *algebraiska* kurvor:
   1. Analytiska funktioner kan skrivas som formella potensserier kring den punkt vi studerar.

Förenklingar

Förenklingar vi kan göra om vi studerar en plan kurva lokalt:

1. Tillräckligt att studera *algebraiska* kurvor:
   1. Analytiska funktioner kan skrivas som formella potensserier kring den punkt vi studerar.
   2. Formella potensserier kan approximeras av polynom med önskad noggrannhet.

Förenklingar

Förenklingar vi kan göra om vi studerar en plan kurva lokalt:

1. Tillräckligt att studera *algebraiska* kurvor:
   1. Analytiska funktioner kan skrivas som formella potensserier kring den punkt vi studerar.
   2. Formella potensserier kan approximeras av polynom med önskad noggrannhet.
2. Kurvan går genom *origo*: $C(0) = \mathbf{0}$

Reguljära och singulära kurvor

Definition

Om en kurva C har en parametrisering (f, g) sådan att $f'(0) \neq 0$ eller $g'(0) \neq 0$ kallas kurvan **reguljär**. Annars kallas kurvan **singulär**.

Not: Bara för att $f'(0) = 0$ och $g'(0) = 0$ i en parametrisering (f, g) av en kurva C, betyder inte det att kurvan är singulär. Det kan ju finnas en parametrisering av samma kurva där någon av derivatorna är nollskilda. Exempelvis är (t^3, t^3) och (t, t) två olika parametriseringar av samma kurva. I det första exemplet är derivatorna 0 i origo medan de i det andra exemplet båda är nollskilda.

Ordning och grad

Definition

Ordningen av ett polynom eller en potensserie $f(t) = \sum a_i t^i \neq 0$ är det minsta heltalet k sådant att koefficienten a_k är nollskild, och skrivs $\mathbf{o}(f)$. **Graden** for motsvarande polynom är det största heltalet k sådant att koefficienten a_k inte är noll, och skrivs $\deg(f)$.

Varför omparametrisera?

1. För utritande av kurvor spelar parametriseringen inte så stor roll.
2. Vill man beräkna $y(x) = g(f^{-1}(x))$ eller $x(y) = f(g^{-1}(y))$, står man genast inför en mängd problem.

Omparametrisering av kurvor

Sats

Om $C = C(t) = (f(t), g(t))$ *är en komplex analytisk, algebroid eller algebraisk kurva, samt att* $f(0) = g(0) = 0$, *kan kurvan* C *omparametriseras på formen* $C^*(t) = (\pm t^n, g^*(t))$ *eller på formen* $C^*(t) = (f^*(t), \pm t^n)$ *i ett område kring* $t = 0$, *där* $f(t)$ *och* $g(t)$ *är formella potensserier. Dessutom gäller att* $\mathbf{o}(f^*) \geq n$ *eller att* $\mathbf{o}(g^*) \geq n$. *Om* $f(t)$ *och* $g(t)$ *är reellvärda, kan också omparametriseringen göras reellvärd.*

Not: Från *Weierstrass Preparation Theorem* kan man få att en sådan omparametrisering existerar. Dock presenteras inte en metod över hur en sådan omparametrisering kan tas fram.

Översikt bevis

Beviset av satsen går igenom följande steg:

1. Vi skapar en omparametrisering via komposition med $\phi(t)$:

$$C^*(t) = (f^*(t), g^*(t)) = (f(\phi(t)), g(\phi(t)))$$

Översikt bevis

Beviset av satsen går igenom följande steg:

1. Vi skapar en omparametrisering via komposition med $\phi(t)$:

$$C^*(t) = (f^*(t), g^*(t)) = (f(\phi(t)), g(\phi(t)))$$

2. Vi väljer $\phi(t)$ sådan att:

Översikt bevis

Beviset av satsen går igenom följande steg:

1. Vi skapar en omparametrisering via komposition med $\phi(t)$:

$$C^*(t) = (f^*(t), g^*(t)) = (f(\phi(t)), g(\phi(t)))$$

2. Vi väljer $\phi(t)$ sådan att:
   1. Analytisk kring $t = 0$.

Översikt bevis

Beviset av satsen går igenom följande steg:

1. Vi skapar en omparametrisering via komposition med $\phi(t)$:

$$C^*(t) = (f^*(t), g^*(t)) = (f(\phi(t)), g(\phi(t)))$$

2. Vi väljer $\phi(t)$ sådan att:
   1. Analytisk kring $t = 0$.
   2. $\phi(0) = 0$

Översikt bevis

Beviset av satsen går igenom följande steg:

1. Vi skapar en omparametrisering via komposition med $\phi(t)$:

$$C^*(t) = (f^*(t), g^*(t)) = (f(\phi(t)), g(\phi(t)))$$

2. Vi väljer $\phi(t)$ sådan att:
   1. Analytisk kring $t = 0$.
   2. $\phi(0) = 0$
   3. $\mathbf{o}(\phi) = 1 \Longrightarrow \mathbf{o}(f(\phi)) = \mathbf{o}(f) \wedge \mathbf{o}(g(\phi)) = \mathbf{o}(g)$

Översikt bevis

Beviset av satsen går igenom följande steg:

1. Vi skapar en omparametrisering via komposition med $\phi(t)$:

$$C^*(t) = (f^*(t), g^*(t)) = (f(\phi(t)), g(\phi(t)))$$

2. Vi väljer $\phi(t)$ sådan att:
   1. Analytisk kring $t = 0$.
   2. $\phi(0) = 0$
   3. $\mathbf{o}(\phi) = 1 \Longrightarrow \mathbf{o}(f(\phi)) = \mathbf{o}(f) \wedge \mathbf{o}(g(\phi)) = \mathbf{o}(g)$
   4. $\phi(t), f(t), g(t)$ reellvärda $\Longrightarrow$ $C^*(t)$ reellvärd.

Översikt bevis

Beviset av satsen går igenom följande steg:

1. Vi skapar en omparametrisering via komposition med $\phi(t)$:

$$C^*(t) = (f^*(t), g^*(t)) = (f(\phi(t)), g(\phi(t)))$$

2. Vi väljer $\phi(t)$ sådan att:
   1. Analytisk kring $t = 0$.
   2. $\phi(0) = 0$
   3. $\mathbf{o}(\phi) = 1 \Longrightarrow \mathbf{o}(f(\phi)) = \mathbf{o}(f) \wedge \mathbf{o}(g(\phi)) = \mathbf{o}(g)$
   4. $\phi(t), f(t), g(t)$ reellvärda $\Longrightarrow$ $C^*(t)$ reellvärd.
3. Med början i a_1 (som har n lösningar), löses koefficienterna a_i ut ur $\phi(t) = \sum_{k=1}^{\infty} a_k t^k$ för att uppfylla ovanstående.

Översikt bevis

Beviset av satsen går igenom följande steg:

1. Vi skapar en omparametrisering via komposition med $\phi(t)$:

$$C^*(t) = (f^*(t), g^*(t)) = (f(\phi(t)), g(\phi(t)))$$

2. Vi väljer $\phi(t)$ sådan att:
   1. Analytisk kring $t = 0$.
   2. $\phi(0) = 0$
   3. $\mathbf{o}(\phi) = 1 \Longrightarrow \mathbf{o}(f(\phi)) = \mathbf{o}(f) \wedge \mathbf{o}(g(\phi)) = \mathbf{o}(g)$
   4. $\phi(t), f(t), g(t)$ reellvärda $\Longrightarrow$ $C^*(t)$ reellvärd.
3. Med början i a_1 (som har n lösningar), löses koefficienterna a_i ut ur $\phi(t) = \sum_{k=1}^{\infty} a_k t^k$ för att uppfylla ovanstående.
4. Finns precis en lösning i det generella fallet som uppfyller ovanstående, samt satsens, krav.

Reparametrize()

```
Reparametrize := proc(x, y, Variable, t0 , MaxDegree,
    Branch, AllowNegation)
```

1. Algoritm som omparametriserar en algebraisk kurva med given noggrannhet.

Reparametrize()

```
Reparametrize := proc(x, y, Variable, t0 , MaxDegree,
    Branch, AllowNegation)
```

1. Algoritm som omparametriserar en algebraisk kurva med given noggrannhet.
2. Maple-kod finns i `https://github.com/PeterWaher/Algebraiska_kurvor/blob/master/kurvor.mw`

Reparametrize()

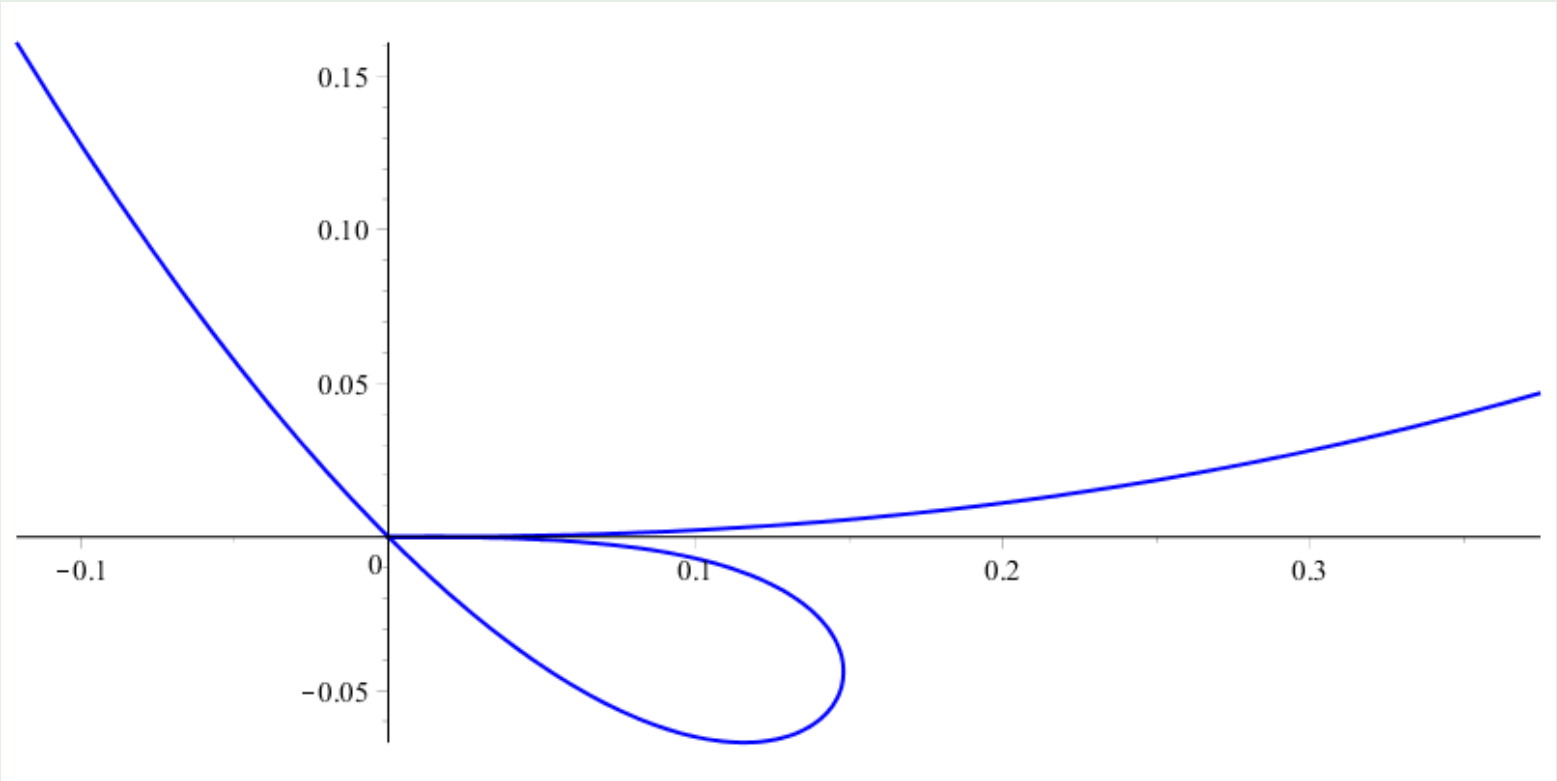
```
Reparametrize := proc(x, y, Variable, t0 , MaxDegree,
    Branch, AllowNegation)
```

1. Algoritm som omparametriserar en algebraisk kurva med given noggrannhet.
2. Maple-kod finns i `https://github.com/PeterWaher/Algebraiska_kurvor/blob/master/kurvor.mw`
3. Text-version finns i `https://github.com/PeterWaher/Algebraiska_kurvor/blob/master/Functions/Reparametrize.txt`

Reparametrize - exempel 1 (1/4)

Exempel

Kurvan $(t^2 + t^3, t^5 + t^6)$ har en singularitet i $t = 0$. Dessutom passerar kurvan genom origo då $t = -1$.



Reparametrize - exempel 1 (2/4)

Exempel

Först ber vi Maple att parametrisera om kurvan kring $t = 0$:

```
> Reparametrize(t^3+t^2,t^6+t^5,t,0,10,0,false);

Elapsed Time: 0.016 s.
```

$$\left[t^2, t^5 - 3/2\, t^6 + \frac{21\, t^7}{8} - 5\, t^8 + \frac{1287\, t^9}{128} - 21\, t^{10}\right]$$

Reparametrize - exempel 1 (3/4)

Exempel

Därefter vill vi ha en omparametrisering kring $t = -1$:

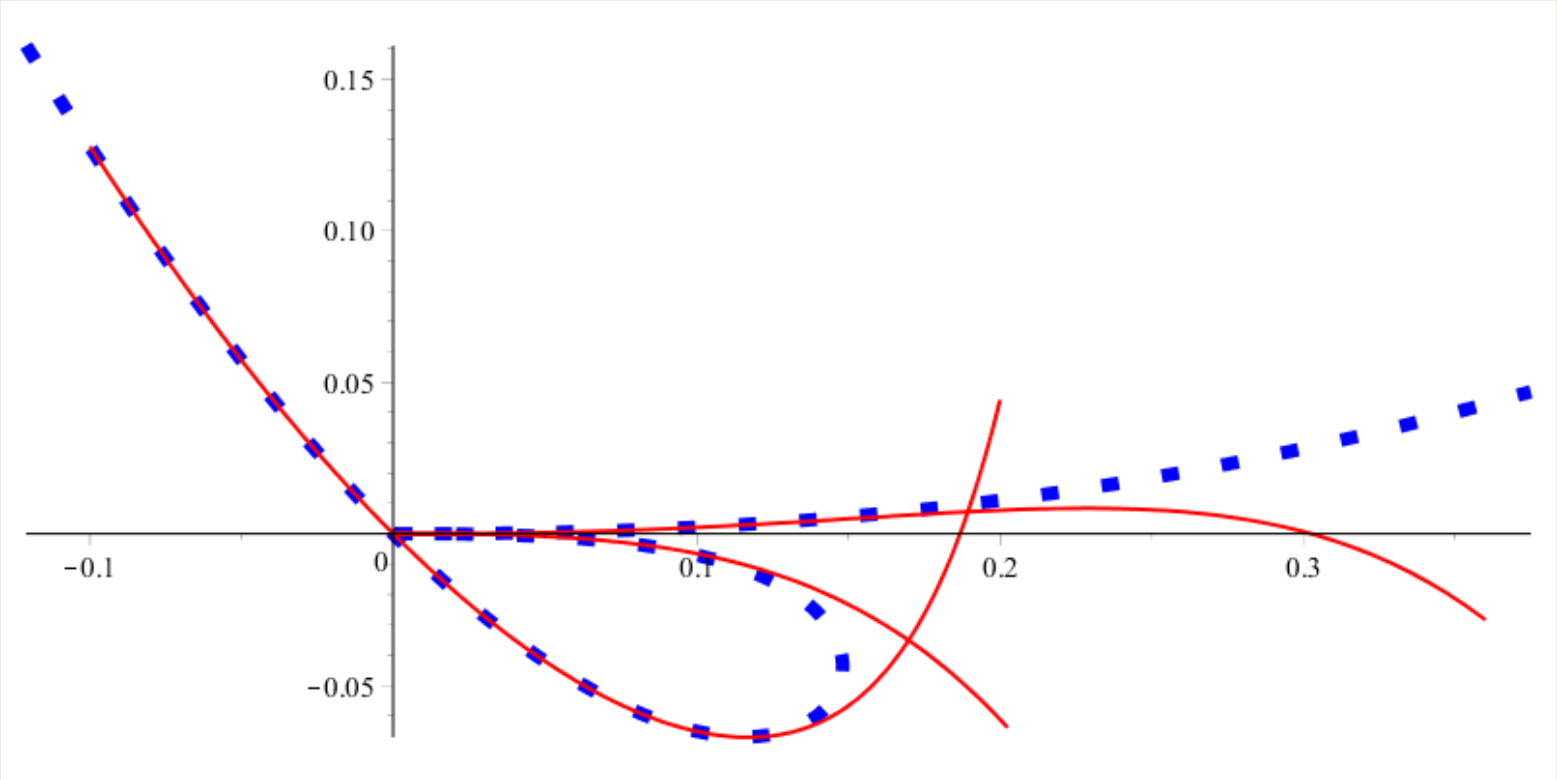
```
> Reparametrize(t^3+t^2, t^6+t^5, t, -1, 10,
    0, false);

Elapsed Time: 0.016 s.
```

$$\left[t, 163438\,t^{10} + 29070\,t^9 + 5304\,t^8 + 1001\,t^7 + 198\,t^6 + 42\,t^5 + \right.$$
$$\left. + 10\,t^4 + 3\,t^3 + 3\,t^2 - t\right]$$

Reparametrize - exempel 1 (4/4)

Exempel

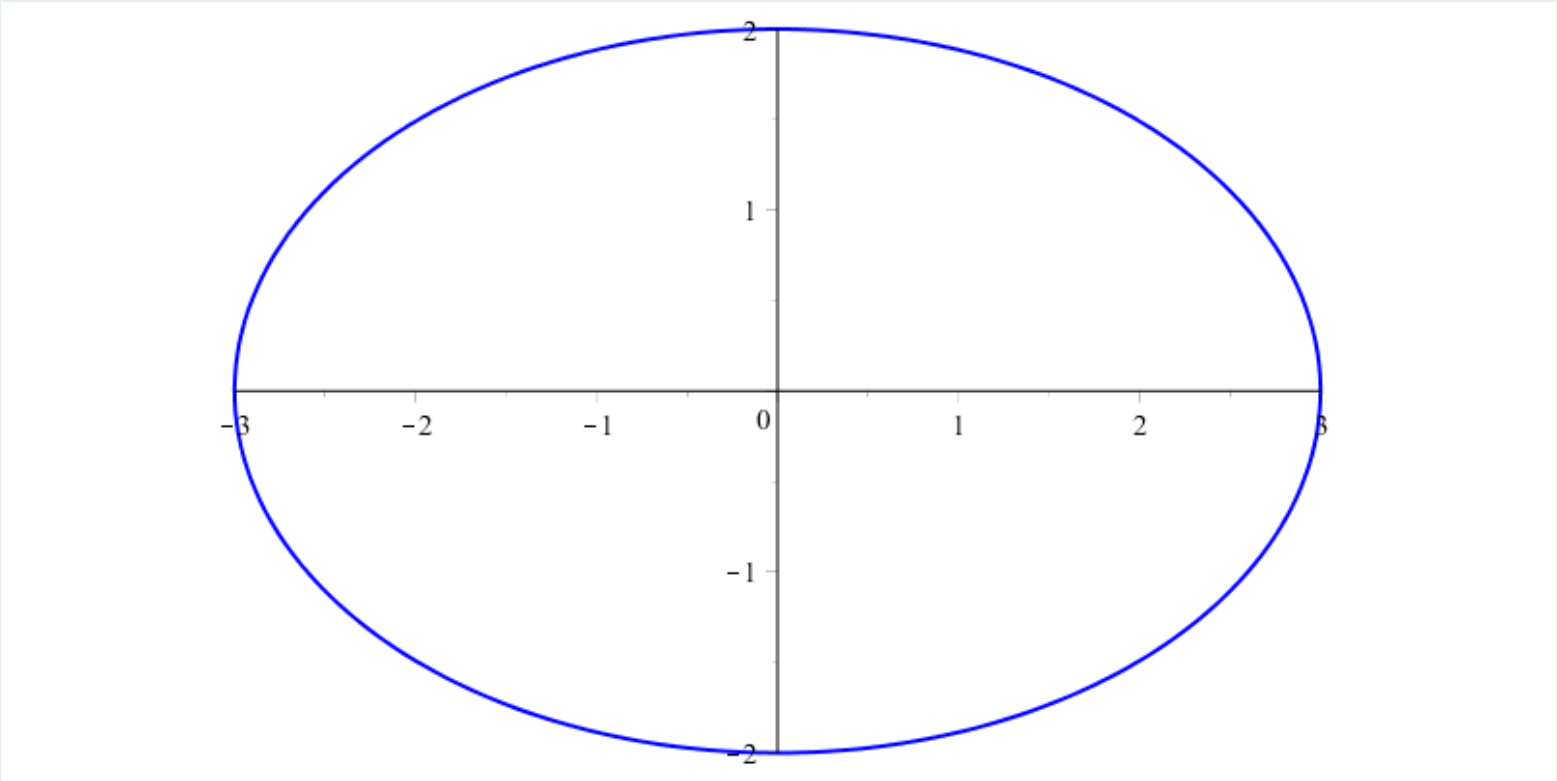
Nedan kurvan $C(t) = (t^2 + t^3, t^5 + t^6)$, med omparametriseringarna kring $t = 0$ och $t = -1$.



Reparametrize - exempel 2 (1/6)

Exempel

Ellipsen $(3\sin(t), 2\cos(t))$ är reguljär, men vi kan parametrisera om kurvan ändå för att illustrera axelbyte.



Reparametrize - exempel 2 (2/6)

Exempel

Första omparametriseringen gör vi kring $t = 0$:

```
> Reparametrize(3*sin(t),2*cos(t),t,0,10,0,false);

Elapsed Time: 0.015 s.
```

$$\left[t, 2 - 1/9\, t^2 - \frac{t^4}{324} - \frac{t^6}{5832} - \frac{5\, t^8}{419904} - \frac{7\, t^{10}}{7558272}\right]$$

Reparametrize - exempel 2 (3/6)

Exempel

Andra omparametriseringen gör vi kring $t = \pi$:

```
> Reparametrize(3*sin(t),2*cos(t),t,Pi,10,0,false);

Elapsed Time: 0.016 s.
```

$$\left[t, -2 + 1/9\, t^2 + \frac{t^4}{324} + \frac{t^6}{5832} + \frac{5\, t^8}{419904} + \frac{7\, t^{10}}{7558272}\right]$$

Reparametrize - exempel 2 (4/6)

Exempel

Tredje omparametriseringen gör vi kring $t = \frac{\pi}{2}$. Notera hur omparametriseringarna skiljer från $t = 0$ och $t = \pi$, jämfört med $t = \pm\frac{\pi}{2}$:

```
> Reparametrize(3*sin(t),2*cos(t),t,(1/2)*Pi,
    10,0,false);

Elapsed Time: 0.016 s.
```

$$\left[3 - 3/8\,t^2 - \frac{3\,t^4}{128} - \frac{3\,t^6}{1024} - \frac{15\,t^8}{32768} - \frac{21\,t^{10}}{262144}, t\right]$$

Reparametrize - exempel 2 (5/6)

Exempel

Fjärde omparametriseringen gör vi kring $t = -\frac{\pi}{2}$:

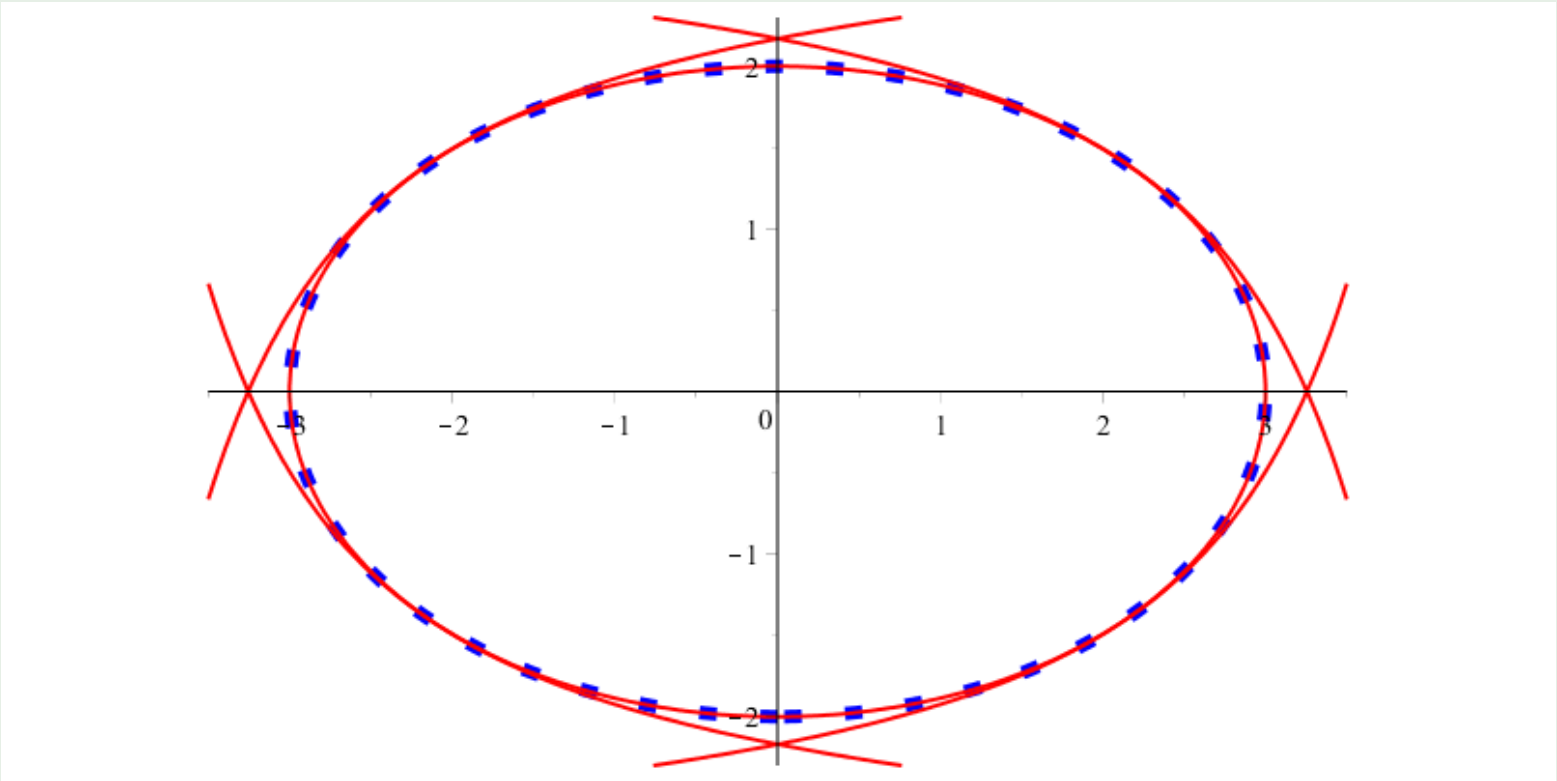
```
> Reparametrize(3*sin(t),2*cos(t),t,-(1/2)*Pi,
    10,0,false);

Elapsed Time: 0.015 s.
```

$$\left[-3 + 3/8\, t^2 + \frac{3\, t^4}{128} + \frac{3\, t^6}{1024} + \frac{15\, t^8}{32768} + \frac{21\, t^{10}}{262144}, t\right]$$

Reparametrize - exempel 2 (6/6)

Exempel

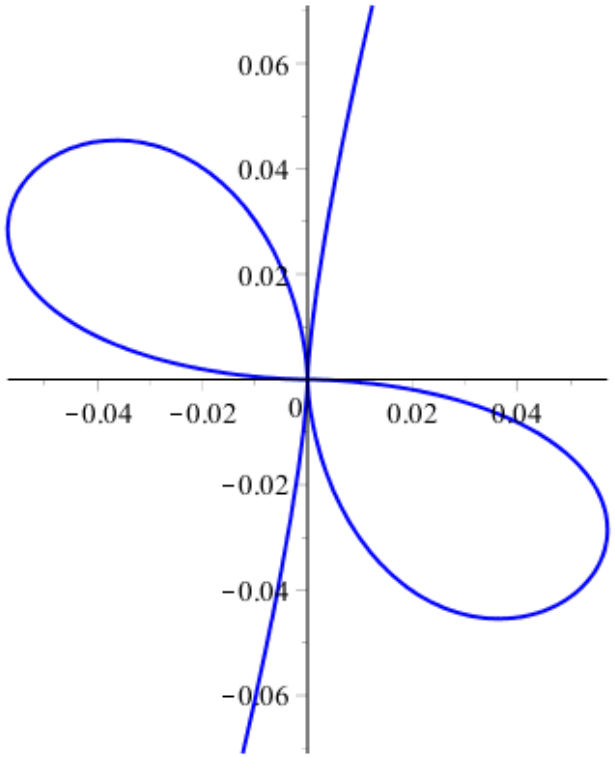
Nedan kurvan $C(t) = (3\sin(t), 2\cos(t))$, med de fyra omparametriseringarna kring $t = 0$, $t = \pi$ och $t = \pm\frac{\pi}{2}$:



Reparametrize - exempel 3 (1/5)

Exempel

Kurvan $\left(t^3(t-1)^3(t+1)^3, t^5(t-1)^2(t+1)^2\right)$ har singulariteter i $t = 0, 1, -1$ av ordningar 2, 1, 1 respektive.



Reparametrize - exempel 3 (2/5)

Exempel

Vi analyserar hur omparametriseringarna uppför sig i dessa tre singulariteter. Första omparametriseringen gör vi kring $t = 0$:

```
> Reparametrize(t^3*(t-1)^3*(t+1)^3,
    t^5*(t-1)^2*(t+1)^2,t,0,15,0, false);

Elapsed Time: 0.031 s.
```

$$\left[t^3, -1428\,t^{15} - 273\,t^{13} - 55\,t^{11} - 12\,t^9 - 3\,t^7 - t^5\right]$$

Reparametrize - exempel 3 (3/5)

Exempel

Därefter kring $t = 1$:

```
> Reparametrize(t^3*(t-1)^3*(t+1)^3,
    t^5*(t-1)^2*(t+1)^2,t,1,15,0,false);

Elapsed Time: 0.063 s.
```

$$\left[1/2\,\sqrt{4}t^3 - 9/4\,t^4 + \frac{207\,\sqrt{4}t^5}{64} - 21\,t^6 + \frac{150183\,\sqrt{4}t^7}{4096} - \frac{137655\,t^8}{512} + \frac{66893079\,\sqrt{4}t^9}{131072} - 3978\,t^{10} + \frac{132735945771\,\sqrt{4}t^{11}}{16777216} - \frac{8385901667\,t^{12}}{131072} + \frac{70379121262905\,\sqrt{4}t^{13}}{536870912} - \frac{4345965\,t^{14}}{4} + \frac{7808782664360745\,\sqrt{4}t^{15}}{34359738368},\ t^2\right]$$

Reparametrize - exempel 3 (4/5)

Exempel

Och sist kring $t = -1$:

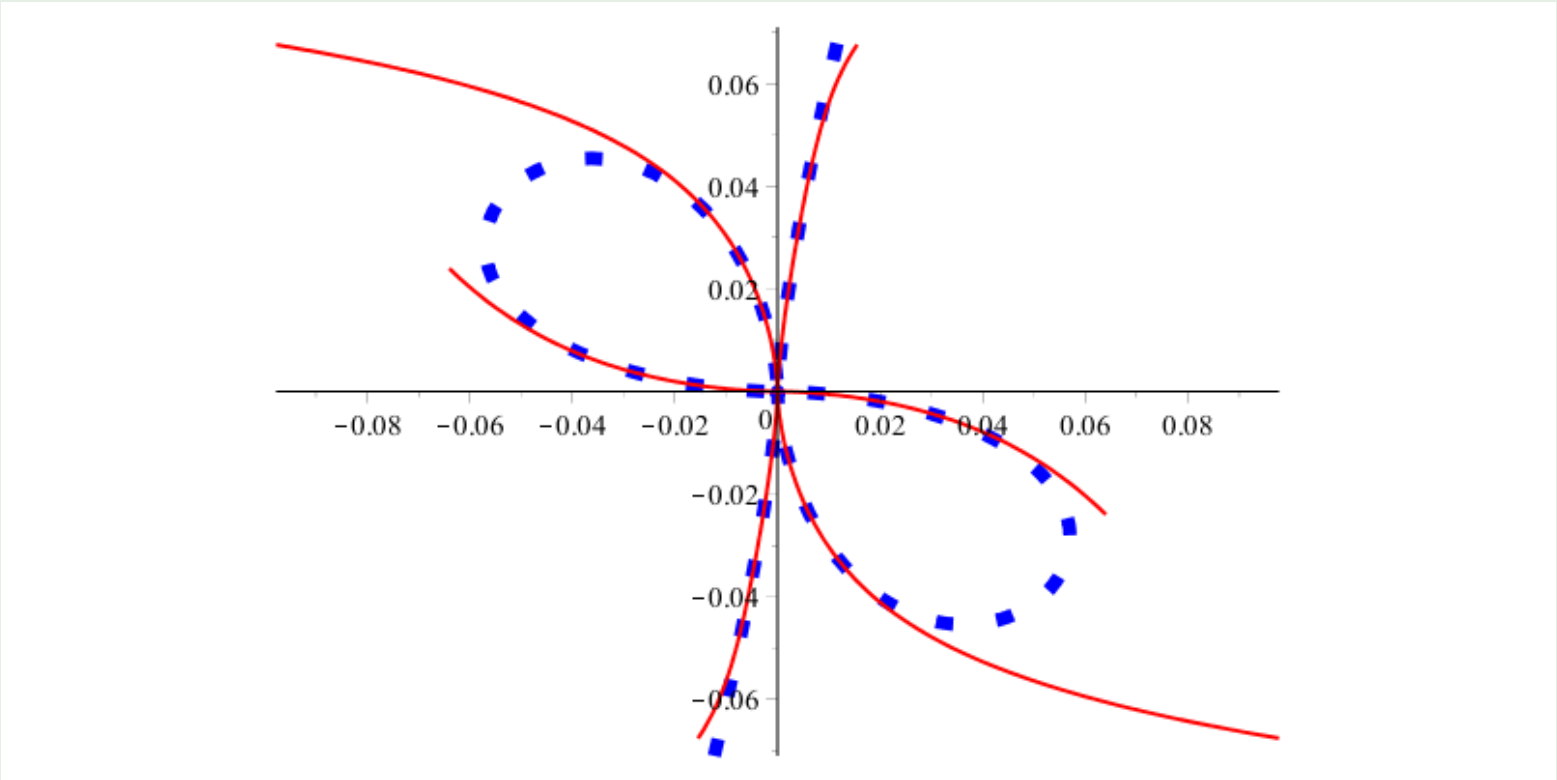
```
> Reparametrize(t^3*(t-1)^3*(t+1)^3,
    t^5*(t-1)^2*(t+1)^2,t,-1,15,0,true);

Elapsed Time: 0.047 s.
```

$$\left[1/2\,\sqrt{4}t^3 + 9/4\,t^4 + \frac{207\,\sqrt{4}t^5}{64} + 21\,t^6 + \frac{150183\,\sqrt{4}t^7}{4096} + \frac{137655\,t^8}{512} + \frac{66893079\,\sqrt{4}t^9}{131072} + 3978\,t^{10} + \frac{132735945771\,\sqrt{4}t^{11}}{16777216} + \frac{8385901667\,t^{12}}{131072} + \frac{70379121262905\,\sqrt{4}t^{13}}{536870912} + \frac{4345965\,t^{14}}{4} + \frac{7808782664360745\,\sqrt{4}t^{15}}{34359738368}, -t^2\right]$$

Reparametrize - exempel 3 (5/5)

Exempel

Ritar vi sedan ut originalparametriseringen av kurvan tillsammans med de tre omparametriseringarna får vi följande intressanta bild:



Semigrupper

Semigrupper

1. Semigrupper
    1. Modulär aritmetik

Semigrupper

Semigrupper

1. Semigrupper
    1. Modulär aritmetik
    2. Semigrupper
    3. Numeriska semigrupper

Semigrupper

1. Semigrupper
   1. Modulär aritmetik
   2. Semigrupper
   3. Numeriska semigrupper
   4. Konduktören

Semigrupper

1. Semigrupper
    1. Modulär aritmetik
    2. Semigrupper
    3. Numeriska semigrupper
    4. Konduktören
    5. $\mathbb{C}[t]$ och dess delringar

Semigrupper

1. Semigrupper
    1. Modulär aritmetik
    2. Semigrupper
    3. Numeriska semigrupper
    4. Konduktören
    5. $\mathbb{C}[t]$ och dess delringar
    6. Semigrupper för $\mathbb{C}[p_1, \ldots, p_n]$

Modulär aritmetik

Definition

Heltalen $m \in \mathbb{Z}^+$ och $n \in \mathbb{Z}^+$ sägs vara **relativt prima** om $m \geq 2$, $n \geq 2$ samt $p \mid m \wedge p \mid n \Longrightarrow p = 1$.

Modulär aritmetik

Definition

Heltalen $m \in \mathbb{Z}^+$ och $n \in \mathbb{Z}^+$ sägs vara **relativt prima** om $m \geq 2$, $n \geq 2$ samt $p \mid m \wedge p \mid n \Longrightarrow p = 1$.

Lemma

Om m och n är relativt prima och $0 < a < m$ *gäller att* $[a \cdot n]_m \neq 0$.

Modulär aritmetik

Definition

Heltalen $m \in \mathbb{Z}^+$ och $n \in \mathbb{Z}^+$ sägs vara **relativt prima** om $m \geq 2$, $n \geq 2$ samt $p \mid m \wedge p \mid n \Longrightarrow p = 1$.

Lemma

Om m och n är relativt prima och $0 < a < m$ *gäller att* $[a \cdot n]_m \neq 0$.

Lemma

Om m och n är relativt prima och $0 < a, b < m$ *gäller:*

$$[a \cdot n]_m = [b \cdot n]_m \Longleftrightarrow a = b$$

Semigrupper

Definition

För en **semigrupp** G, med den implicit definierade binära operatorn $+$ gäller:

$$a \in G \wedge b \in G \Longrightarrow (a + b) \in G$$

$$(a + b) + c = a + (b + c)$$

Generatorer av semigrupp

Definition

En serie tal $n_1, \ldots, n_k$ **genererar** semigruppen G om

$$G = \left\{ \sum_{a_i \neq 0} a_i \cdot n_i : a_i \in \mathbb{N}, \text{ inte alla } a_i = 0 \right\}$$

Detta skrivs även $G = \langle n_1, \ldots, n_k \rangle$.

Not: Notera att med multiplikation med ett positivt heltal inom en semigrupp avses repetitiv användning av additionsoperatorn.

Konduktören för $\langle m, n \rangle$ (m, n relativt prima)

Sats

Om m och n är relativt prima innehåller semigruppen $G = \langle m, n \rangle$ alla tal större än eller lika med $c = (m-1)(n-1)$, men inte talet $c - 1$.

Konduktören för $\langle m, n \rangle$ (m, n relativt prima)

Sats

Om m och n är relativt prima innehåller semigruppen $G = \langle m, n \rangle$ alla tal större än eller lika med $c = (m-1)(n-1)$, men inte talet $c - 1$.

Översikt av bevis:

Konduktören för $\langle m, n \rangle$ (m, n relativt prima)

Sats

Om m och n är relativt prima innehåller semigruppen $G = \langle m, n \rangle$ alla tal större än eller lika med $c = (m-1)(n-1)$, men inte talet $c - 1$.

Översikt av bevis:

1. $\mathbb{Z}_m = \langle [n]_m \rangle$.

Konduktören för $\langle m, n \rangle$ (m, n relativt prima)

Sats

Om m och n är relativt prima innehåller semigruppen $G = \langle m, n \rangle$ alla tal större än eller lika med $c = (m-1)(n-1)$, men inte talet $c - 1$.

Översikt av bevis:

1. $\mathbb{Z}_m = \langle [n]_m \rangle$.
2. Antag att $m < n$.

Konduktören för $\langle m, n \rangle$ (m, n relativt prima)

Sats

Om m och n är relativt prima innehåller semigruppen $G = \langle m, n \rangle$ alla tal större än eller lika med $c = (m-1)(n-1)$, men inte talet $c - 1$.

Översikt av bevis:

1. $\mathbb{Z}_m = \langle [n]_m \rangle$.
2. Antag att $m < n$.
3. Uppdelning av $\mathbb{N}$ i segment om m tal vardera.

Konduktören för $\langle m, n \rangle$ (m, n relativt prima)

Sats

Om m och n är relativt prima innehåller semigruppen $G = \langle m, n \rangle$ alla tal större än eller lika med $c = (m-1)(n-1)$, men inte talet $c - 1$.

Översikt av bevis:

1. $\mathbb{Z}_m = \langle [n]_m \rangle$.
2. Antag att $m < n$.
3. Uppdelning av $\mathbb{N}$ i segment om m tal vardera.
4. Stryk alla tal i $[0]_m$, därefter $[n]_m$, $[2n]_m$, $\ldots$, $[(m-1)n]_m$.

Konduktören för $\langle m, n \rangle$ (m, n relativt prima)

Sats

Om m och n är relativt prima innehåller semigruppen $G = \langle m, n \rangle$ alla tal större än eller lika med $c = (m-1)(n-1)$, men inte talet $c - 1$.

Översikt av bevis:

1. $\mathbb{Z}_m = \langle [n]_m \rangle$.
2. Antag att $m < n$.
3. Uppdelning av $\mathbb{N}$ i segment om m tal vardera.
4. Stryk alla tal i $[0]_m$, därefter $[n]_m$, $[2n]_m$, $\ldots$, $[(m-1)n]_m$.
5. Alla tal större än eller lika med $(m-1)n$ ur $\mathbb{N}$

Konduktören för $\langle m, n \rangle$ (m, n relativt prima)

Sats

Om m och n är relativt prima innehåller semigruppen $G = \langle m, n \rangle$ alla tal större än eller lika med $c = (m-1)(n-1)$, men inte talet $c - 1$.

Översikt av bevis:

1. $\mathbb{Z}_m = \langle [n]_m \rangle$.
2. Antag att $m < n$.
3. Uppdelning av $\mathbb{N}$ i segment om m tal vardera.
4. Stryk alla tal i $[0]_m$, därefter $[n]_m$, $[2n]_m$, $\ldots$, $[(m-1)n]_m$.
5. Alla tal större än eller lika med $(m-1)n$ ur $\mathbb{N}$
6. Det högsta ostrukna talet, är således $(m-1)n - m$.

Numerisk semigrupp

Definition

En **numerisk semigrupp** G är en speciell form av semigrupp, där även följande villkor gäller:

$$\begin{aligned} G &\subseteq \mathbb{N} \\ \|\mathbb{N} \setminus G\| &< \infty \end{aligned}$$

Numerisk semigrupp

Definition

En **numerisk semigrupp** G är en speciell form av semigrupp, där även följande villkor gäller:

$$\begin{aligned} G &\subseteq \mathbb{N} \\ \|\mathbb{N} \setminus G\| &< \infty \end{aligned}$$

Lemma

$G = \langle m, n \rangle$ där m och n är relativt prima, är en numerisk semigrupp.

Konduktör

Definition

I varje numerisk semigrupp G finns det ett tal c_G sådant att följande villkor uppfylls:

$$\begin{array}{rcl} c_G & \in & G \\ n > c_G & \Longrightarrow & n \in G \\ c_G - 1 & \notin & G \end{array}$$

c_G kallas för **konduktören** för G.

Konduktör

Definition

I varje numerisk semigrupp G finns det ett tal c_G sådant att följande villkor uppfylls:

$$\begin{array}{rcl} c_G & \in & G \\ n > c_G & \Longrightarrow & n \in G \\ c_G - 1 & \notin & G \end{array}$$

c_G kallas för **konduktören** för G.

$c = (m-1)(n-1)$ där m och n är relativt prima, är konduktör för den numeriska semigruppen $G = \langle m, n \rangle$.

$\gcd(n_1, \ldots, n_k) = 1$

Sats

Om semigruppen $G = \langle n_1, \ldots, n_k \rangle$ *är numerisk så är den största gemensamma delaren av talen* $\gcd(n_1, \ldots, n_k) = 1$.

$\gcd(n_1, \ldots, n_k) = 1$

Sats

Om semigruppen $G = \langle n_1, \ldots, n_k \rangle$ *är numerisk så är den största gemensamma delaren av talen* $\gcd(n_1, \ldots, n_k) = 1$.

Översikt av trivialt bevis:

$\gcd(n_1, \ldots, n_k) = 1$

Sats

Om semigruppen $G = \langle n_1, \ldots, n_k \rangle$ *är numerisk så är den största gemensamma delaren av talen* $\gcd(n_1, \ldots, n_k) = 1$.

Översikt av trivialt bevis:

1. $\gcd(G) = \gcd(n_1, \ldots, n_k) = d$.

$\gcd(n_1, \ldots, n_k) = 1$

Sats

Om semigruppen $G = \langle n_1, \ldots, n_k \rangle$ *är numerisk så är den största gemensamma delaren av talen* $\gcd(n_1, \ldots, n_k) = 1$.

Översikt av trivialt bevis:

1. $\gcd(G) = \gcd(n_1, \ldots, n_k) = d$.
2. $d > 1 \Longrightarrow \|\mathbb{N} \setminus G\| = \infty$

Minimalt generatorsystem

Sats

För varje numerisk semigrupp G finns ett minimalt generatorsystem $n_1, \ldots, n_k$, sådant att $G = \langle n_1, \ldots, n_k \rangle$. Detta system är unikt för G.

Minimalt generatorsystem

Sats

För varje numerisk semigrupp G finns ett minimalt generatorsystem $n_1, \ldots, n_k$, sådant att $G = \langle n_1, \ldots, n_k \rangle$. Detta system är unikt för G.

Översikt av bevis:

Minimalt generatorsystem

Sats

För varje numerisk semigrupp G finns ett minimalt generatorsystem $n_1, \ldots, n_k$, sådant att $G = \langle n_1, \ldots, n_k \rangle$. Detta system är unikt för G.

Översikt av bevis:

1. Ändlig mängd tal i G som genererar semigruppen.

Minimalt generatorsystem

Sats

För varje numerisk semigrupp G finns ett minimalt generatorsystem $n_1, \ldots, n_k$, sådant att $G = \langle n_1, \ldots, n_k \rangle$. Detta system är unikt för G.

Översikt av bevis:

1. Ändlig mängd tal i G som genererar semigruppen.
2. $\widehat{M}$ mängden av alla ändliga mängder av generatorer.

Minimalt generatorsystem

Sats

För varje numerisk semigrupp G finns ett minimalt generatorsystem $n_1, \ldots, n_k$, sådant att $G = \langle n_1, \ldots, n_k \rangle$. Detta system är unikt för G.

Översikt av bevis:

1. Ändlig mängd tal i G som genererar semigruppen.
2. $\widehat{M}$ mängden av alla ändliga mängder av generatorer.
3. $\widehat{M}' = \{\|M\| : M \in \widehat{M}\}$

Minimalt generatorsystem

Sats

För varje numerisk semigrupp G finns ett minimalt generatorsystem $n_1, \ldots, n_k$, sådant att $G = \langle n_1, \ldots, n_k \rangle$. Detta system är unikt för G.

Översikt av bevis:

1. Ändlig mängd tal i G som genererar semigruppen.
2. $\widehat{M}$ mängden av alla ändliga mängder av generatorer.
3. $\widehat{M}' = \{\|M\| : M \in \widehat{M}\}$
4. $k = \inf \widehat{M}'$ existerar.

Minimalt generatorsystem

Sats

För varje numerisk semigrupp G finns ett minimalt generatorsystem $n_1, \ldots, n_k$, sådant att $G = \langle n_1, \ldots, n_k \rangle$. Detta system är unikt för G.

Översikt av bevis:

1. Ändlig mängd tal i G som genererar semigruppen.
2. $\widehat{M}$ mängden av alla ändliga mängder av generatorer.
3. $\widehat{M}' = \{\|M\| : M \in \widehat{M}\}$
4. $k = \inf \widehat{M}'$ existerar.
5. $\exists M_- \in \widehat{M} : \|M_-\| = k$

Minimalt generatorsystem

Sats

För varje numerisk semigrupp G finns ett minimalt generatorsystem $n_1, \ldots, n_k$, sådant att $G = \langle n_1, \ldots, n_k \rangle$. Detta system är unikt för G.

Översikt av bevis:

1. Ändlig mängd tal i G som genererar semigruppen.
2. $\widehat{M}$ mängden av alla ändliga mängder av generatorer.
3. $\widehat{M}' = \{\|M\| : M \in \widehat{M}\}$
4. $k = \inf \widehat{M}'$ existerar.
5. $\exists M_- \in \widehat{M} : \|M_-\| = k$
6. $N_- \in \widehat{M} \wedge \|N_-\| = k \Longrightarrow N_- = M_-$

$\gcd(\{n_i\}) = 1 \Longrightarrow \langle\{n_i\}\rangle$ numerisk

Sats

Om $n_1, \ldots, n_k$ är heltal sådana att $\gcd(n_1, \ldots, n_k) = 1$ så gäller att $G = \langle n_1, \ldots, n_k \rangle$ är en numerisk semigrupp.

$\gcd(\{n_i\}) = 1 \Longrightarrow \langle\{n_i\}\rangle$ numerisk

Sats

Om $n_1, \ldots, n_k$ är heltal sådana att $\gcd(n_1, \ldots, n_k) = 1$ så gäller att $G = \langle n_1, \ldots, n_k \rangle$ är en numerisk semigrupp.

Översikt av bevis:

1. Anta $n_1 < \ldots < n_k$

$\gcd(\{n_i\}) = 1 \Longrightarrow \langle\{n_i\}\rangle$ numerisk

Sats

Om $n_1, \ldots, n_k$ är heltal sådana att $\gcd(n_1, \ldots, n_k) = 1$ så gäller att $G = \langle n_1, \ldots, n_k \rangle$ är en numerisk semigrupp.

Översikt av bevis:

1. Anta $n_1 < \ldots < n_k$
2. $\left\langle [n_2]_{n_1}, \ldots, [n_k]_{n_1} \right\rangle = \mathbb{Z}_{n_1}$

$\gcd(\{n_i\}) = 1 \Longrightarrow \langle\{n_i\}\rangle$ numerisk

Sats

Om $n_1, \ldots, n_k$ är heltal sådana att $\gcd(n_1, \ldots, n_k) = 1$ så gäller att $G = \langle n_1, \ldots, n_k \rangle$ är en numerisk semigrupp.

Översikt av bevis:

1. Anta $n_1 < \ldots < n_k$
2. $\left\langle [n_2]_{n_1}, \ldots, [n_k]_{n_1} \right\rangle = \mathbb{Z}_{n_1}$
3. $[a_j]_{n_1} \in \mathbb{Z}_{n_1} \Longrightarrow \exists \{b_{i,j}\}, 0 \leq b_{i,j} < n_1 : \sum b_{i,j} \cdot [n_i]_{n_1} = [a_j]_{n_1}$

$\gcd(\{n_i\}) = 1 \Longrightarrow \langle\{n_i\}\rangle$ numerisk

Sats

Om $n_1, \ldots, n_k$ är heltal sådana att $\gcd(n_1, \ldots, n_k) = 1$ så gäller att $G = \langle n_1, \ldots, n_k \rangle$ är en numerisk semigrupp.

Översikt av bevis:

1. Anta $n_1 < \ldots < n_k$
2. $\left\langle [n_2]_{n_1}, \ldots, [n_k]_{n_1} \right\rangle = \mathbb{Z}_{n_1}$
3. $[a_j]_{n_1} \in \mathbb{Z}_{n_1} \Longrightarrow \exists \{b_{i,j}\}, 0 \leq b_{i,j} < n_1 : \sum b_{i,j} \cdot [n_i]_{n_1} = [a_j]_{n_1}$
4. $b_j = \sum_{i=2}^{k} b_{i,j} \cdot n_i \in G, [b_j]_{n_1} = [a_j]_{n_1}$

$\gcd(\{n_i\}) = 1 \Longrightarrow \langle\{n_i\}\rangle$ numerisk

Sats

Om $n_1, \ldots, n_k$ är heltal sådana att $\gcd(n_1, \ldots, n_k) = 1$ så gäller att $G = \langle n_1, \ldots, n_k \rangle$ är en numerisk semigrupp.

Översikt av bevis:

1. Anta $n_1 < \ldots < n_k$
2. $\left\langle [n_2]_{n_1}, \ldots, [n_k]_{n_1} \right\rangle = \mathbb{Z}_{n_1}$
3. $[a_j]_{n_1} \in \mathbb{Z}_{n_1} \Longrightarrow \exists \{b_{i,j}\}, 0 \leq b_{i,j} < n_1 : \sum b_{i,j} \cdot [n_i]_{n_1} = [a_j]_{n_1}$
4. $b_j = \sum_{i=2}^{k} b_{i,j} \cdot n_i \in G, [b_j]_{n_1} = [a_j]_{n_1}$
5. $0 \leq b_j < n_1 \sum_{i=2}^{k} n_i \leq (k-1) n_1 n_k = B$

$\gcd(\{n_i\}) = 1 \Longrightarrow \langle\{n_i\}\rangle$ numerisk

Sats

Om $n_1, \ldots, n_k$ är heltal sådana att $\gcd(n_1, \ldots, n_k) = 1$ så gäller att $G = \langle n_1, \ldots, n_k \rangle$ är en numerisk semigrupp.

Översikt av bevis:

1. Anta $n_1 < \ldots < n_k$
2. $\left\langle [n_2]_{n_1}, \ldots, [n_k]_{n_1} \right\rangle = \mathbb{Z}_{n_1}$
3. $[a_j]_{n_1} \in \mathbb{Z}_{n_1} \Longrightarrow \exists \{b_{i,j}\}, 0 \leq b_{i,j} < n_1 : \sum b_{i,j} \cdot [n_i]_{n_1} = [a_j]_{n_1}$
4. $b_j = \sum_{i=2}^{k} b_{i,j} \cdot n_i \in G, [b_j]_{n_1} = [a_j]_{n_1}$
5. $0 \leq b_j < n_1 \sum_{i=2}^{k} n_i \leq (k-1) n_1 n_k = B$
6. $S_B = \{m \cdot n_1, \ldots, (m+1) \cdot n_1 - 1\} \subset G$, där $m \cdot n_1 \geq B$

FindConductor()

```
FindConductor := proc(Generators)
```

1. Algoritm som beräknar konduktören för en numerisk semigrupp givet dess generatorer.

FindConductor()

```
FindConductor := proc(Generators)
```

1. Algoritm som beräknar konduktören för en numerisk semigrupp givet dess generatorer.
2. Maple-kod finns i `https://github.com/PeterWaher/Algebraiska_kurvor/blob/master/semigrupper.mw`

FindConductor()

```
FindConductor := proc(Generators)
```

1. Algoritm som beräknar konduktören för en numerisk semigrupp givet dess generatorer.
2. Maple-kod finns i `https://github.com/PeterWaher/Algebraiska_kurvor/blob/master/semigrupper.mw`
3. Text-version finns i `https://github.com/PeterWaher/Algebraiska_kurvor/blob/master/Functions/FindConductor.txt`

Generalisering möjlig?

Exempel

Vi beräknar konduktören för
$\langle 2 \cdot 3 \cdot 5, 2 \cdot 3 \cdot 7, 2 \cdot 5 \cdot 7, 3 \cdot 5 \cdot 7 \rangle = \langle 30, 42, 70, 105 \rangle$:

```
> FindConductor([2*3*5,2*3*7,2*5*7,3*5*7]);

Elapsed Time: 0.000 s.
```

$$384$$

Konduktören blir i detta exempel $384 = 2^7 \cdot 3$. Som man kan se i detta exempel verkar det inte finnas någon enkel självklar generalisering av formeln för konduktören av $\langle m, n \rangle$, då m och n är relativt prima ($c = (m-1)(n-1)$).

Stor semigrupp

Exempel

I följande exempel illustreras fördelen med att beräkningen av konduktören genomförs utan att motsvarande semigrupp genereras:

```
> FindConductor([2139,2398,3321]);

Elapsed Time: 8.062 s.
```

$$277188$$

Konduktören för $\langle 2139, 2398, 3321 \rangle$ är alltså 277188, dvs. lite mer än 129 ggr större än den minsta generatorn (2139). Beräkningen av motsvarande semigrupp kommer att ta betydligt mer tid (326.313 s). Utskriften av semigruppen kan också krascha Maple (vilket den gjorde i mitt fall).

FindSemiGroup()

```
FindSemiGroup := proc(Generators)
```

1. Algoritm som genererar semigruppen och dess konduktör, givet dess generatorer.

FindSemiGroup()

```
FindSemiGroup := proc(Generators)
```

1. Algoritm som genererar semigruppen och dess konduktör, givet dess generatorer.
2. Maple-kod finns i `https://github.com/PeterWaher/Algebraiska_kurvor/blob/master/semigrupper.mw`

FindSemiGroup()

```
FindSemiGroup := proc(Generators)
```

1. Algoritm som genererar semigruppen och dess konduktör, givet dess generatorer.
2. Maple-kod finns i `https://github.com/PeterWaher/Algebraiska_kurvor/blob/master/semigrupper.mw`
3. Text-version finns i `https://github.com/PeterWaher/Algebraiska_kurvor/blob/master/Functions/FindSemiGroup.txt`

Enkel semigrupp

Exempel

Det första exemplet beräknar $\langle 15, 10, 6 \rangle$:

```
> FindSemiGroup([15,10,6]);

Elapsed Time: 0.000 s.
```

$$[30, \{6, 10, 12, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30\}]$$

Vi får att konduktören är 30 och att

$$\langle 15, 10, 6 \rangle = \{6, 10, 12, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, \ldots\}$$

där "..." betyder "alla heltal som kommer därefter".

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Exempel

Gäller inte generellt. $x \cdot \mathbb{C}[x, y]$ har inte ett ändligt antal generatorer:

$$xy^2 \notin \mathbb{C}[x, xy]$$

$$xy^3 \notin \mathbb{C}[x, xy, xy^2]$$

$$xy^4 \notin \mathbb{C}[x, xy, xy^2, xy^3]$$

$$\ldots$$

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (1/4)

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (1/4)

1. p_1 bland de polynom i S av lägst grad.

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (1/4)

1. p_1 bland de polynom i S av lägst grad.
2. p_{i+1} väljs bland $S \setminus \mathbb{C}[p_1, \ldots, p_i]$ av lägst grad.

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (1/4)

1. p_1 bland de polynom i S av lägst grad.
2. p_{i+1} väljs bland $S \setminus \mathbb{C}[p_1, \ldots, p_i]$ av lägst grad.
3. $\deg(p_{i+1}) > \deg(p_i)$

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (1/4)

1. p_1 bland de polynom i S av lägst grad.
2. p_{i+1} väljs bland $S \setminus \mathbb{C}[p_1, \ldots, p_i]$ av lägst grad.
3. $\deg(p_{i+1}) > \deg(p_i)$
4. $S_1 = \mathbb{C}[p_1] \subsetneq \ldots \subsetneq S_n = \mathbb{C}[p_1, \ldots, p_n] \subsetneq \ldots \subseteq S \subset \mathbb{C}[t]$

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (1/4)

1. p_1 bland de polynom i S av lägst grad.
2. p_{i+1} väljs bland $S \setminus \mathbb{C}[p_1, \ldots, p_i]$ av lägst grad.
3. $\deg(p_{i+1}) > \deg(p_i)$
4. $S_1 = \mathbb{C}[p_1] \subsetneq \ldots \subsetneq S_n = \mathbb{C}[p_1, \ldots, p_n] \subsetneq \ldots \subseteq S \subset \mathbb{C}[t]$
5. $l_i = \deg(S_i) \Longrightarrow l_1 \subsetneq \ldots \subsetneq l_i \subsetneq \ldots \subseteq \mathbb{N}$

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (2/4)

1. $\bar{I}_i = \{[d]_m : d \in I_i\} \subseteq \mathbb{Z}_m$, där $m = \deg(p_1)$

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (2/4)

1. $\bar{I}_i = \{[d]_m : d \in I_i\} \subseteq \mathbb{Z}_m$, där $m = \deg(p_1)$
2. $\bar{I}_1 \subseteq \ldots \subseteq \bar{I}_i \subseteq \ldots \subseteq \mathbb{Z}_m$

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (2/4)

1. $\bar{I}_i = \{[d]_m : d \in I_i\} \subseteq \mathbb{Z}_m$, där $m = \deg(p_1)$
2. $\bar{I}_1 \subseteq \ldots \subseteq \bar{I}_i \subseteq \ldots \subseteq \mathbb{Z}_m$
3. $\exists N : \bar{I}_i = \bar{I}_N, \forall i \geq N$

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (2/4)

1. $\bar{I}_i = \{[d]_m : d \in I_i\} \subseteq \mathbb{Z}_m$, där $m = \deg(p_1)$
2. $\bar{I}_1 \subseteq \ldots \subseteq \bar{I}_i \subseteq \ldots \subseteq \mathbb{Z}_m$
3. $\exists N : \bar{I}_i = \bar{I}_N, \forall i \geq N$
4. $Q_i = \{q \in \mathbb{C}[p_1, \ldots, p_N] : \deg(q) \equiv i \mod m\}$

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (2/4)

1. $\bar{I}_i = \{[d]_m : d \in I_i\} \subseteq \mathbb{Z}_m$, där $m = \deg(p_1)$
2. $\bar{I}_1 \subseteq \ldots \subseteq \bar{I}_i \subseteq \ldots \subseteq \mathbb{Z}_m$
3. $\exists N : \bar{I}_i = \bar{I}_N, \forall i \geq N$
4. $Q_i = \{q \in \mathbb{C}[p_1, \ldots, p_N] : \deg(q) \equiv i \mod m\}$
5. $\forall [i]_m \in \bar{I}_N, 0 \leq i < m : Q_i \neq \emptyset$

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (3/4)

1. $\deg(Q_i) \subset \mathbb{N} \Longrightarrow \exists d_i = \min(\deg(Q_i))$

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (3/4)

1. $\deg(Q_i) \subset \mathbb{N} \Longrightarrow \exists d_i = \min(\deg(Q_i))$
2. $q_i \in Q_i : \deg(q_i) = d_i \wedge$ ledande koefficient 1.

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (3/4)

1. $\deg(Q_i) \subset \mathbb{N} \Longrightarrow \exists d_i = \min(\deg(Q_i))$
2. $q_i \in Q_i : \deg(q_i) = d_i \wedge$ ledande koefficient 1.
3. $n_i \in \mathbb{N} : \deg(q_i) = i + n_i \cdot m$

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (3/4)

1. $\deg(Q_i) \subset \mathbb{N} \Longrightarrow \exists d_i = \min(\deg(Q_i))$
2. $q_i \in Q_i : \deg(q_i) = d_i \wedge$ ledande koefficient 1.
3. $n_i \in \mathbb{N} : \deg(q_i) = i + n_i \cdot m$
4. Godtyckligt $f \in S$.

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (3/4)

1. $\deg(Q_i) \subset \mathbb{N} \Longrightarrow \exists d_i = \min(\deg(Q_i))$
2. $q_i \in Q_i : \deg(q_i) = d_i \wedge$ ledande koefficient 1.
3. $n_i \in \mathbb{N} : \deg(q_i) = i + n_i \cdot m$
4. Godtyckligt $f \in S$.
5. $\deg(f) \in \bar{I}_N \Longrightarrow \exists [j]_m \in \bar{I}_N, 0 \leq j < m : \deg(f) \equiv j \mod m$

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (4/4)

1. $\exists k \in \mathbb{N} : k \geq n_j \wedge \deg(f) = j + k \cdot m =$
   $j + n_j \cdot m + m \cdot (k - n_j) = \deg(q_j) + \deg(p_1^{k-n_j}) = \deg(q_j \cdot p_1^{k-n_j})$

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (4/4)

1. $\exists k \in \mathbb{N} : k \geq n_j \wedge \deg(f) = j + k \cdot m =$
   $j + n_j \cdot m + m \cdot (k - n_j) = \deg(q_j) + \deg(p_1^{k-n_j}) = \deg(q_j \cdot p_1^{k-n_j})$
2. $f_0 = a_0 \cdot q_j \cdot p_1^{k-n_j} \in \mathbb{C}[p_1, \ldots, p_N] \subset S$

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (4/4)

1. $\exists k \in \mathbb{N} : k \geq n_j \wedge \deg(f) = j + k \cdot m = j + n_j \cdot m + m \cdot (k - n_j) = \deg(q_j) + \deg(p_1^{k-n_j}) = \deg(q_j \cdot p_1^{k-n_j})$
2. $f_0 = a_0 \cdot q_j \cdot p_1^{k-n_j} \in \mathbb{C}[p_1, \ldots, p_N] \subset S$
3. $f - f_0 \in S \wedge \deg(f - f_0) < \deg(f)$

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (4/4)

1. $\exists k \in \mathbb{N} : k \geq n_j \wedge \deg(f) = j + k \cdot m = j + n_j \cdot m + m \cdot (k - n_j) = \deg(q_j) + \deg(p_1^{k-n_j}) = \deg(q_j \cdot p_1^{k-n_j})$
2. $f_0 = a_0 \cdot q_j \cdot p_1^{k-n_j} \in \mathbb{C}[p_1, \ldots, p_N] \subset S$
3. $f - f_0 \in S \wedge \deg(f - f_0) < \deg(f)$
4. $f_0, \ldots, f_l \in \mathbb{C}[p_1, \ldots, p_N]$

Delringar till $\mathbb{C}[t]$

Sats

För varje icketrivial delring $S \subset \mathbb{C}[t]$, sluten under skalär multiplikation, finns ett ändligt antal polynom $p_1, \ldots, p_n \in \mathbb{C}[t]$ som genererar S, dvs. $S = \mathbb{C}[p_1, \ldots, p_n]$.

Översikt motsatsbevis: (4/4)

1. $\exists k \in \mathbb{N} : k \geq n_j \wedge \deg(f) = j + k \cdot m = j + n_j \cdot m + m \cdot (k - n_j) = \deg(q_j) + \deg(p_1^{k-n_j}) = \deg(q_j \cdot p_1^{k-n_j})$
2. $f_0 = a_0 \cdot q_j \cdot p_1^{k-n_j} \in \mathbb{C}[p_1, \ldots, p_N] \subset S$
3. $f - f_0 \in S \wedge \deg(f - f_0) < \deg(f)$
4. $f_0, \ldots, f_l \in \mathbb{C}[p_1, \ldots, p_N]$
5. $\deg(f) > \deg(f - f_0) > \ldots > \deg(f - \sum f_j)$

Semigruppen av ordningar

Betrakta $G_S = \mathbf{o}(S) = \{\mathbf{o}(p), p \in S \wedge p \neq 0\}$, där $S = \mathbb{C}[p_1, \ldots, p_n]$:

Semigruppen av ordningar

Betrakta $G_S = \mathbf{o}(S) = \{\mathbf{o}(p), p \in S \wedge p \neq 0\}$, där $S = \mathbb{C}[p_1, \ldots, p_n]$:

1. G_S är en semigrupp.

Semigruppen av ordningar

Betrakta $G_S = \mathbf{o}(S) = \{\mathbf{o}(p), p \in S \wedge p \neq 0\}$, där $S = \mathbb{C}[p_1, \ldots, p_n]$:

1. G_S är en semigrupp.
2. G_S kan vara större än $\langle \mathbf{o}(p_1), \ldots, \mathbf{o}(p_n) \rangle$

Semigruppen av ordningar

Betrakta $G_S = \mathbf{o}(S) = \{\mathbf{o}(p), p \in S \wedge p \neq 0\}$, där $S = \mathbb{C}[p_1, \ldots, p_n]$:

1. G_S är en semigrupp.
2. G_S kan vara större än $\langle \mathbf{o}(p_1), \ldots, \mathbf{o}(p_n) \rangle$

Exempel

1. $S = \mathbb{C}[t^2, t^4 + t^5]$

Semigruppen av ordningar

Betrakta $G_S = \mathbf{o}(S) = \{\mathbf{o}(p), p \in S \wedge p \neq 0\}$, där $S = \mathbb{C}[p_1, \ldots, p_n]$:

1. G_S är en semigrupp.
2. G_S kan vara större än $\langle \mathbf{o}(p_1), \ldots, \mathbf{o}(p_n) \rangle$

Exempel

1. $S = \mathbb{C}[t^2, t^4 + t^5]$
2. $(t^4 + t^5) - (t^2)^2 = t^5 \in S \Longrightarrow 5 \in G_S$

Semigruppen av ordningar

Betrakta $G_S = \mathbf{o}(S) = \{\mathbf{o}(p), p \in S \wedge p \neq 0\}$, där $S = \mathbb{C}[p_1, \ldots, p_n]$:

1. G_S är en semigrupp.
2. G_S kan vara större än $\langle \mathbf{o}(p_1), \ldots, \mathbf{o}(p_n) \rangle$

Exempel

1. $S = \mathbb{C}[t^2, t^4 + t^5]$
2. $(t^4 + t^5) - (t^2)^2 = t^5 \in S \Longrightarrow 5 \in G_S$
3. $\langle \mathbf{o}(p_1), \mathbf{o}(p_2) \rangle = \langle 2 \rangle \subset \langle 2, 5 \rangle = \{2, 4, 5, 6, \ldots\} = G_S$

Sökning efter polynom

För att beräkna vilka tal som finns i G_S behöver vi systematiskt gå igenom de möjligheter vi har att kombinera nya polynom från generatorerna $\{p_i\}$. Polynom som kan generera polynom av nya ordningar, och som inte är kända sedan tidigare, kan göras på två sätt:

Sökning efter polynom

För att beräkna vilka tal som finns i G_S behöver vi systematiskt gå igenom de möjligheter vi har att kombinera nya polynom från generatorerna $\{p_i\}$. Polynom som kan generera polynom av nya ordningar, och som inte är kända sedan tidigare, kan göras på två sätt:

1. Antingen genom att två kända polynom multipliceras med varandra. I detta fallet blir ordningen av det nya polynomet summan av ordningarna för de individuella polynomen.

Sökning efter polynom

För att beräkna vilka tal som finns i G_S behöver vi systematiskt gå igenom de möjligheter vi har att kombinera nya polynom från generatorerna $\{p_i\}$. Polynom som kan generera polynom av nya ordningar, och som inte är kända sedan tidigare, kan göras på två sätt:

1. Antingen genom att två kända polynom multipliceras med varandra. I detta fallet blir ordningen av det nya polynomet summan av ordningarna för de individuella polynomen.
2. Alternativt kan två kända polynom av samma ordning adderas till varandra, med möjlig föregående skalär multiplicering av det ena, så att termen motsvarande den aktuella ordningen elimineras från svaret. I detta fallet blir ordningen av svaret beroende av de ingående polynomen.

FindSemiGroupFromPolynomialRing()

```
FindSemiGroupFromPolynomialRing := proc(
    PolynomialGenerators,Variable)
```

1. Algoritm som beräknar semigruppen för en delring $\mathbb{C}[p_1, \ldots, p_n] \subset \mathbb{C}[t]$ och returnerar dess generatorer. Den kan också returnera hur generatorerna härletts.

FindSemiGroupFromPolynomialRing()

```
FindSemiGroupFromPolynomialRing := proc(
    PolynomialGenerators,Variable)
```

1. Algoritm som beräknar semigruppen för en delring $\mathbb{C}[p_1, \ldots, p_n] \subset \mathbb{C}[t]$ och returnerar dess generatorer. Den kan också returnera hur generatorerna härletts.
2. Maple-kod finns i `https://github.com/PeterWaher/Algebraiska_kurvor/blob/master/semigrupper.mw`

FindSemiGroupFromPolynomialRing()

```
FindSemiGroupFromPolynomialRing := proc(
    PolynomialGenerators,Variable)
```

1. Algoritm som beräknar semigruppen för en delring $\mathbb{C}[p_1, \ldots, p_n] \subset \mathbb{C}[t]$ och returnerar dess generatorer. Den kan också returnera hur generatorerna härletts.
2. Maple-kod finns i `https://github.com/PeterWaher/Algebraiska_kurvor/blob/master/semigrupper.mw`
3. Text-version finns i `https://github.com/PeterWaher/Algebraiska_kurvor/blob/master/Functions/FindSemiGroupFromPolynomialRing.txt`

Enkelt exempel

Exempel

```
> FindSemiGroupFromPolynomialRing([t^4+t^5,
    t^6+t^7],t,true,true);
```

$$p_1 = t^5 + t^4$$
$$p_2 = t^7 + t^6$$
$$p_1^3 - p_2^2 = t^{15} + 2t^{14} + t^{13}$$

$$[4, 6, 13]$$

```
> FindSemiGroup([4,6,13]);
```

$$[16, \{4, 6, 8, 10, 12, 13, 14, 16\}]$$