SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Om nolldimensionella ideal och initialideal

av

Ernst Nordström Cederholm

2022 - No M4

Om nolldimensionella ideal och initialideal

Ernst Nordström Cederholm

Självständigt arbete i matematik 30 högskolepoäng, avancerad nivå

Handledare: Samuel Lundqvist

2022

Abstract

It is shown that every zero-dimensional monomial ideal I is the initial ideal of $\mathbf{I}(\Sigma)$, where Σ is the set of multivariate degrees of the monomials outside I. Macaulay may have known this and possibly had a draft towards a proof that precede the concept of the Gröbner basis. Using modern terminology, a universal Gröbner basis to $\mathbf{I}(\Sigma)$ is provided. As a consequence, it is shown that the function that maps finite affine varieties V, to the set of multivariate degrees of the monomials outside the initial ideal of $\mathbf{I}(V)$, stabilizes directly.

Keywords

zero-dimensional ideals, Gröbner basis, initial ideals, finite affine varieties

Tack

Tack Samuel Lundqvist för all hjälp under arbetets gång, med utformandet av frågeställning och bollande av bevisidéer. Samuel är en oerhört trevlig och duktig handledare som alltid varit där när det behövts och samtidigt litat och trott på min förmåga. Bättre än så kan det inte bli!

Innehåll

1 Introduktion och problemformulering

Förståelse för uppsatsen förutsätter grundläggande kunskap om polynomringar och ideal. Första delkapitelet av Kapitel 2 innehåller grundläggande teori inom datoralgebra och kan hoppas över av orienterade läsare inom området. Delkapitel 2.2 redogör för metoder att bestämma nollställemängden för nolldimensionella ideal och är mindre viktigt för uppsatsens huvudresultat men kan eventuellt användas vid framtida forskning, särskilt multiplikationsmatriserna från delkapitel 2.2.2.

Innan problemformuleringen för uppsatsen introduceras redogörs för notation och de konventioner som uppsatsen följer. I direkt anslutning introduceras den nödvändiga teorin som krävs för att förstå problemformuleringen.

1.1 Notation och konventioner

k	godtycklig kropp om inget annat anges
$\mathbb{N}$	naturliga talen inkluderat noll
n	antalet variabler i $k[x_1, x_2, \ldots, x_n]$
α_i	den i:te koordinaten av $\alpha \in k^n$
e_i	$e_i \in k^n$ där $(e_i)_i = 1$ och $(e_i)_j = 0$ om $j \neq i$
x^α	monomet $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ i $k[x_1, x_2, \ldots, x_n]$
0^0	$0^0 \coloneqq 1$
α^β	om $\alpha, \beta \in \mathbb{N}^n$ är $\alpha^\beta \coloneqq \alpha_1^{\beta_1} \cdot \alpha_2^{\beta_2} \cdots \alpha_n^{\beta_n} \in \mathbb{N}$

1.2 Nödvändiga definitioner

Definition 1.1 (Affin varietet)**.** *För polynom $f_1, f_2, \ldots, f_s \in k[x_1, x_2, \ldots, x_n]$ definiera den affina varieteten $\mathbf{V}(f_1, f_2, \ldots, f_s)$ som*

$$\mathbf{V}(f_1, f_2, \ldots, f_s) \coloneqq \{a \in k^n \mid f_i(a) = 0 \, \forall i \in \{1, 2, \ldots, s\}\}.$$

Definition 1.2. *Om $V \subseteq k^n$ är en affin varietet definieras idealet $\mathbf{I}(V)$ som*

$$\mathbf{I}(V) \coloneqq \{f \in k[x_1, x_2, \ldots, x_n] \mid f(a) = 0 \, \forall a \in V\}.$$

Definition 1.3 (Radikalideal)**.** *Låt I vara ett ideal av $k[x_1, x_2, \ldots, x_n]$. Radikalen av I definieras som*

$$\sqrt{I} \coloneqq \{f \in k[x_1, x_2, \ldots, x_n] \mid \exists \alpha \in \mathbb{N} \text{ sådan att } f^\alpha \in I\}.$$

Definition 1.4 (Linjär ordning)**.** *En linjär ordning är en binär relation $>$ på en mängd som uppfyller att för alla element a, b och c i mängden gäller att:*

$$a \geq b \wedge b \geq c \Longrightarrow a \geq c,$$
$$a \geq b \wedge b \geq a \Longleftrightarrow a = b \text{ och}$$
$$a \geq b \vee b \geq a.$$

Definition 1.5 (Monomordning)**.** *En monomordning är en linjär ordning* $>$ *på mängden monomen* $\{x^\alpha \in k[x_1, x_2, \ldots, x_n] \mid \alpha \in \mathbb{N}^n\}$ *som uppfyller att* $x^\alpha \geq 1$ *och om* $x^\alpha > x^\beta$ *för något och* α *och* β *i* $\mathbb{N}^n$ *är* $x^\alpha x^\gamma > x^\beta x^\gamma$ *för alla* $\gamma \in \mathbb{N}^n$*.*

Anmärkning 1.6. *För alla monomordningar är* $x_i^{\alpha+1} > x_i^\alpha$ *för alla* $i \in \{1, 2, \ldots, n\}$ *och* $\alpha \in \mathbb{N}^n$ *eftersom* $x_i > 1$*.*

Definition 1.7 (Lexikografisk ordning)**.** *Definiera relationen* $>_{lex}$ *på mängden monom i* $k[x_1, x_2, \ldots, x_n]$ *sådan att om* $x^\alpha, x^\beta \in k[x_1, x_2, \ldots, x_n]$ *är* $x^\alpha >_{lex} x^\beta$ *om den första nollskilda koordinaten av* $(\alpha - \beta)$ *är positiv.*

Definition 1.8 (Graderad lexikografisk ordning)**.** *Definiera relationen* $>_{Glex}$ *på mängden monom i* $k[x_1, x_2, \ldots, x_n]$ *sådan att om* $x^\alpha, x^\beta \in k[x_1, x_2, \ldots, x_n]$ *är* $x^\alpha >_{Glex} x^\beta$ *om*

$$\sum_{i=1}^{n} \alpha_i > \sum_{i=1}^{n} \beta_i \text{ eller om } \sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i \text{ och } x^\alpha >_{lex} x^\beta.$$

Att både den lexikografiska ordningen och den graderade lexikografiska ordningen faktiskt är monomordningar går att läsa i [1]. Om det är klart från sammanhanget vilken monomordning som menas, eller om monomordningen för sammanhanget inte spelar någon roll, används symbolen $>$ oavsett monomordning.

Definition 1.9 (Multivariat grad)**.** *Låt* $f = \sum_{\alpha \in A} a_\alpha x^\alpha$ *vara ett nollskilt polynom i* $k[x_1, x_2, \ldots, x_n]$ *där* $A \subset \mathbb{N}^n$ *är en ändlig mängd sådan att* $a_\alpha \neq 0$ *för alla* $\alpha \in A$*. Fixera en monomordning på mängden monom i* $k[x_1, x_2, \ldots, x_n]$*. Den multivariata graden av* f *definieras som*

$$grad(f) \coloneqq \max_{\alpha \in A}(x^\alpha)$$

där max tas med avseende på den underliggande monomordningen.

Definition 1.10 (Ledande monom)**.** *Låt* $f = \sum_{\alpha \in A} a_\alpha x^\alpha$ *vara ett nollskilt polynom i* $k[x_1, x_2, \ldots, x_n]$ *där* $A \subset \mathbb{N}^n$ *är en ändlig mängd sådan att* $a_\alpha \neq 0$ *för alla* $\alpha \in A$*. Det ledande monomet av* f *definieras som*

$$LM(f) \coloneqq x^{grad(f)}.$$

Definition 1.11 (Initialideal)**.** *Låt* I *vara ett ideal. Initialidealet av* I *definieras som*

$$\operatorname{in} I \coloneqq \langle LM(f) \mid f \in I \rangle.$$

Definition 1.12 (Nolldimensionellt ideal)**.** *Ett ideal* $I \subseteq k[x_1, x_2, \ldots, x_n]$ *är nolldimensionellt om det för varje* $i \in \{1, 2, \ldots, n\}$ *existerar ett* $\alpha_i \in \mathbb{N}$ *sådan att* $x_i^{\alpha_i} \in \operatorname{in} I$*.*

Definition 1.13 (Nolldimensionell affin varietet)**.** *En affin varietet* $V = \mathbf{V}(I)$ *sägs vara nolldimensionell om* I *är ett nolldimensionellt ideal.*

Definition 1.14 (Gröbnerbas)**.** *Fixera en monomordning. Låt* I *vara ett ideal av* $k[x_1, x_2, \ldots, x_n]$ *och* $G = \{g_1, g_2, \ldots, g_s\}$ *en ändlig uppsättning av polynom tillhörande* I*.* G *sägs vara en Gröbnerbas av* I*, med avseende på den underligande monomordningen, om*

$$\operatorname{in} I = \langle LM(g_1), LM(g_2), \ldots, LM(g_s)\rangle.$$

Sats 1.15 (Existens av Gröbnerbaser)**.** *Låt* I *vara ett ideal av polynomringen* $k[x_1, x_2, \ldots, x_n]$*. För alla monomordningar existerar en Gröbnerbas av* I*.*

Definition 1.16 (Buchbergers algoritm [2])**.** *Buchbergers algoritm är en algoritm som givet ett ideal* I *av* $k[x_1, x_2, \ldots, x_n]$ *och en uppsättning polynom som genererar* I *tar fram en Gröbnerbas av* I*.*

Definition 1.17 (Buchberger-Möller-algoritmen [3])**.** *Buchberger-Möller-algoritmen är en algoritm som givet ett en ändlig uppsättning punkter* $P \subseteq k^n$ *tar fram en Gröbnerbas av idealet* $\mathbf{I}(P)$*.*

1.3 Problemformulering

Låt k vara en kropp och låt $V = \{p_1, ..., p_s\}$ vara en uppsättning av s punkter i k^n. Med hjälp av Buchberger-Möller-algoritmen kan man bestämma en Gröbnerbas av idealet $\mathbf{I}(V)$, vilket i sin tur, enligt Sats 2.10, är en generatormängd för $\mathbf{I}(V)$. Givet Gröbnerbasen är det lätt att ta fram monomen som ligger utanför $\operatorname{in}\mathbf{I}(V)$ med avseende på en fix monomordning. Följdsats 2.27 säger att antalet sådana är exakt s stycken förutsatt att $\mathbf{I}(V)$ är nolldimensionellt, vilket är fallet enligt Sats 2.25. Under antagandet att k innehåller de naturliga talen kan monomen tänkas på som punkter i k^n genom monomens multivariata grad. Sammanlagt fås en avbildning från nolldimensionella affina varieteter till sig själv. Kalla avbildningen för φ. Frågan som studeras i denna uppsats är vad som händer om φ appliceras flera gånger. Svaret ges av Sats 3.10.

Exempel 1.1. *Låt* $V = \{(4, 5, 7, 4, 0), (4, 3, 4, 1, 3), (2, 3, 5, 3, 4)\} \subset \mathbb{Q}^5$*. Det nolldimensionella idealet*

$$I = \mathbf{I}(V) \subset \mathbb{Q}[x_1, x_2, \ldots, x_5]$$

har

$$\begin{aligned} G = \{&x_5^3 - 7x_5^2 + 12x_5, 4x_4 - 3x_5^2 + 13x_5 - 16, 2x_3 - x_5^2 + 5x_5 - 14,\\ &6x_2 - x_5^2 + 7x_5 - 30, 2x_1 + x_5^2 - 3x_5 - 8\}\end{aligned}$$

som en Gröbnerbas med avseende på lexikografisk monomordning där $x_1 > x_2 > \cdots > x_5$. *Initialidealet av* I *genereras således av*

$$x_5^3, x_4, x_3, x_2, x_1$$

och monomen utanför $\operatorname{in} I$ *är* x_5^2, x_5 *och* 1 *med multivariat grader* $(0,0,0,0,2)$, $(0,0,0,0,1), (0,0,0,0,0)$. *Detta ger att*

$$\varphi(V) = \{(0,0,0,0,2), (0,0,0,0,1), (0,0,0,0,0)\},$$

varav en naturlig följdfråga är: vad är $\varphi(\varphi(V))$*?*

1.4 Metod

Arbetet att försöka besvara frågeställningen har varit såväl praktiskt som teoretiskt. Programmeringsspråket Macaulay2 [4] har använts för att implementera funktionen φ från problemformulering för att sedan användas till att generera $\varphi(V)$ utifrån slumpade ändliga delmängder V av $\mathbb{Z}^n$ för olika $n \in \mathbb{N} \setminus \{0\}$. Koden som skapats för att kunna svara på problemformuleringen finns i bilaga A.

I implementeringen av $\varphi(V)$ i Macaulay2 beräknades först idealet $\mathbf{I}(V)$ och en Gröbnerbas av $\varphi(V)$ för att sedan ta fram monomen utanför $\operatorname{in}\mathbf{I}(V)$, i syfte att försöka hitta ett mönster för olika V. Dock insågs i ett tidigt skede att för en fixerad kardinalitet av V och för en bestämd monomordning skulle samma monom utanför $\operatorname{in}\mathbf{I}(V)$ erhållas för olika slumpningar av V. Anledningen kan vara att nolldimensionella radikalideal I som härstammar från slumpade affina varieteter med stor sannolikhet kommer ha en så kallad Shape bas enligt The Shape Lemma [5]. Av denna anledning övergavs idén med att slumpa ändliga delmängder V av $\mathbb{Z}^n$, ty slumpen fångade inte egenskaperna för mer tillrättalagda mängder V. Nästa tillvägagångssätt blev istället att konstruera olika nolldimensionella ideal på ett sådant sätt att olika monom utanför initialidealet erhölls. När φ återupprepades på dessa mängder erhölls resultatet att $\varphi = \varphi^2$. Eftersom $\varphi(V)$ för olika delmängder V av $\mathbb{Z}^n$ alltid såg ut att ha formen som en trappa erhölls idén om trappmängder. Trappmängder definieras i Definition 2.37. Genom generering av olika trappmängder Σ och betraktande av Gröbnerbaser av $\mathbf{I}(\Sigma)$ kunde en sluten formel för en universell Gröbnerbas av $\mathbf{I}(\Sigma)$ anas och senare matematiskt bevisas i Sats 3.1. Resultatet kom i sin tur att användas för att svara på problemformuleringen.

2 Bakgrundsmaterial

Det mesta av teorin i kapitel 2 är kända resultat inom datoralgebra. Boken *Ideals, Varieties, and Algorithms* [1] skriven av David A. Cox, John Little och Donal O'Shea används uteslutande som källa till hela kapitlet med undantag för delkapitlerna 2.2.2 och 2.3. Delkapitel 2.2.2 bygger på artikeln *Gröbner bases and matrix eigenproblems* [6] skriven av Robert Corless. Delkapitel 2.3 innehåller egna definitioner, direkt nödvändiga för att förstå resultaten i kapitel 3.

2.1 Ideal och Gröbnerbaser

Sats 2.1 (Divisionsalgoritm i $k[x_1, x_2, \ldots, x_n]$)**.** *Fixera en monomordning och låt $f_1, f_2, \ldots, f_s$ vara polynom i $k[x_1, x_2, \ldots, x_n]$. Varje polynom $f \in k[x_1, x_2, \ldots, x_n]$ kan skrivas som*

$$f = q_1 f_1 + q_2 f_2 + \cdots + q_s f_s + r,$$

där $q_1, q_2 \ldots, q_s$ samt r tillhör $k[x_1, x_2, \ldots, x_n]$ och antingen är $r = 0$ eller så är r en linjärkombination av monom ej delbara med något av de ledande monomen av polynomen $f_1, f_2, \ldots, f_s$.

Bevis för divisionsalgoritmen kan till exempel läsas i [1].

Definition 2.2 (Reducerad Gröbnerbas)**.** *En Gröbnerbas G för ett polynomideal I sägs vara reducerad om för alla $f \in G$ ligger inget monom av f i $\langle LM(G \setminus \{f\})\rangle$ och koefficienten till det ledande monomet av f är 1.*

Definition 2.3 (Universell Gröbnerbas)**.** *Låt I vara ett ideal av polynomringen $k[x_1, x_2, \ldots, x_n]$ och $G = \{g_1, g_2, \ldots, g_s\}$ en ändlig uppsättning av polynom tillhörande I. G sägs vara en universell Gröbnerbas av I om*

$$\text{in}\, I = \langle LM(g_1), LM(g_2), \ldots, LM(g_s)\rangle$$

för alla monomordningar.

Sats 2.4 (Existens av universella Gröbnerbaser)**.** *Låt I vara ett ideal av $k[x_1, x_2, \ldots, x_n]$. Det existerar en universell Gröbnerbas av I.*

Bevis. Unionen av Gröbnerbaserna för respektive monomordning utgör en universell Gröbnerbas. □

Lemma 2.5. *Låt $I = \langle x^\alpha \mid \alpha \in A \subseteq \mathbb{N}^n\rangle$ vara ett monomideal. Då ligger monomet x^β, $\beta \in \mathbb{N}^n$, i I om och endast om x^α delar x^β för något $\alpha \in A$.*

Bevis av Lemma 2.5 går att läsa i [1].

Sats 2.6. *Låt I vara ett ideal av $k[x_1, x_2, \ldots, x_n]$ med Gröbnerbas $G = \{g_1, g_2 \ldots, g_s\}$. Varje polynom $f \in k[x_1, x_2, \ldots, x_n]$ kan skrivas på formen $f = q+r$ där $q \in I$ och r är ett unikt polynom som antingen är noll eller vars termer ej är delbara med något av elementen $LM(g_1), LM(g_2), \ldots, LM(g_s)$.*

Bevis. Divisionsalgoritmen, Sats 2.1, ger att $f = q_1g_1+q_2g_2 \ldots+q_sg_s+r$ där r antingen är noll eller ingen term av r är delbart med något av elementen $\mathrm{LM}(g_1), \mathrm{LM}(g_2), \ldots, \mathrm{LM}(g_s)$. Antag att det finns en annan representation $f = q_1'g_1 + q_2'g_2 + \ldots + q_s'g_s + r'$ där $r \neq r'$. Då är

$$r - r' = q_1'g_1 + q_2'g_2 + \ldots + q_s'g_s - (q_1g_1 + q_2g_2 + \ldots + q_sg_s) \in I.$$

Alltså är $r - r' \in I$, vilket innebär att

$$\mathrm{LM}(r - r') \in \mathrm{in}\, I = \langle \mathrm{LM}(g_1), \mathrm{LM}(g_2), \ldots, \mathrm{LM}(g_s) \rangle,$$

men detta kan endast vara sant om något av polynomen $\mathrm{LM}(g_1), \mathrm{LM}(g_2), \ldots,$ $\mathrm{LM}(g_s)$ delar $\mathrm{LM}(r - r')$ enligt Lemma 2.5. Eftersom ingen av termerna i varken r eller r' delas av polynomen $\mathrm{LM}(g_1), \mathrm{LM}(g_2), \ldots, \mathrm{LM}(g_s)$ måste $r = r'$. □

Anmärkning 2.7. *Notera att endast resttermen är unik i den mening att om f kan skrivas som två olika utfall av divisionsalgoritmen $f = q + r = q'+r$, där $q = q_1g_1+q_2g_2 \ldots+q_sg_s$ och $q' = q_1'g_1+q_2'g_2+\ldots+q_s'g_s$, behöver q_i inte nödvändigtvis vara lika med q_i' för alla $i \in \{1, 2, \ldots, s\}$. Däremot gäller det alltid att*

$$\sum_{i=1}^{s} a_ig_i = 0,$$

där $a_i = q_i - q_i' \in k[x_1, x_2, \ldots, x_n]$.

Exempel 2.1. *Divideras polynomet $x^2y \in \mathbb{Q}[x, y]$ med Gröbnerbasen $\{x - 1, y - 1\}$ med avsende på graderad lexikografisk ordning erhålls antingen att*

$$x^2y = (xy+y)(x-1)+1\cdot(y-1)+1 \text{ eller } x^2y = x^2(y-1)+(x+1)(x-1)+1,$$

beroende på vilket av polynomen $x-1$ eller $y-1$ divisionsalgrotimen dividerar med först.

Definition 2.8. *Låt f vara ett polynom i polynomringen $k[x_1, x_2, \ldots, x_n]$ och G en Gröbnerbas av ett ideal I. Definiera $\overline{f}^G$ som resten vid division av f med polynom i mängden G.*

Sats 2.9. *Låt I vara ett ideal av $k[x_1, x_2, \ldots, x_n]$ och $G = \{g_1, g_1, \ldots, g_s\}$ en Gröbnerbas av I. Låt f vara ett polynom i $k[x_1, x_2, \ldots, x_n]$. Då är $\overline{f}^G = 0$ om och endast om $f \in I$.*

Bevis. Om $\overline{f}^G = 0$ är $f = q_1g_1+q_2g_2+\ldots+q_ng_n$ varav $f \in I$ ty $\{g_1, g_1, \ldots, g_s\}$ är en delmängd av I. Om $f \in I$ är $f = f + 0$ varav 0 är den unika resten av f vid division av G enligt Sats 2.6. □

Sats 2.10. *Om $\{g_1, g_2, \ldots, g_s\}$ är en Gröbnerbas av ett ideal I är*

$$\langle g_1, g_2, \ldots, g_s\rangle = I.$$

Bevis. Låt f vara ett polynom i I. Eftersom $\{g_1, g_2, \ldots, g_s\} \subseteq I$ kan f skrivas som $f = a_1g_1+a_2g_2+\ldots+a_sg_s+r$ där a_i och r ligger i $k[x_1, x_2, \ldots, x_n]$ och inget av monomen $\mathrm{LM}(g_i)$, för alla $i \in \{1, 2, \ldots, s\}$, delar något av monomen av r enligt Sats 2.1. Men resten $r = f-a_1g_1-a_2g_2-\ldots-a_sg_s \in I$ varav $\mathrm{LM}(r) \in \mathrm{in}\, I = \langle \mathrm{LM}(g_1), \mathrm{LM}(g_2), \ldots, \mathrm{LM}(g_s)\rangle$. Alltså måste $\mathrm{LM}(r) = 0$ enligt Sats 2.9 varav $r = 0$ och $f = a_1g_1+a_2g_2+\ldots+a_sg_s \in \langle g_1, g_2, \ldots, g_s\rangle$. Det följer att $\langle g_1, g_2, \ldots, g_s\rangle = I$. □

Sats 2.11. *Låt I vara ett ideal av $k[x_1, x_2, \ldots, x_n]$ och $\{f_1, f_2, \ldots, f_s\} \subseteq I$. Om antalet monom utanför $\langle LM(f_1), LM(f_2), \ldots, LM(f_s)\rangle$ är lika många som antalet monom utanför* $\mathrm{in}\, I$ *är $\{f_1, f_2, \ldots, f_s\}$ en Gröbnerbas av I för den underliggande monomordningen.*

Bevis. Eftersom $\{f_1, f_2, \ldots, f_s\} \subseteq I$ är $\{\mathrm{LM}(f_1), \mathrm{LM}(f_2), \ldots, \mathrm{LM}(f_s)\} \subseteq \mathrm{in}\, I$ varav $\langle \mathrm{LM}(f_1), \mathrm{LM}(f_2), \ldots, \mathrm{LM}(f_s)\rangle \subseteq \mathrm{in}\, I$. Alltså är alla monom innanför $\langle \mathrm{LM}(f_1), \mathrm{LM}(f_2), \ldots, \mathrm{LM}(f_s)\rangle$ även innanför $\mathrm{in}\, I$ och alla monom utanför $\mathrm{in}\, I$ är utanför $\langle \mathrm{LM}(f_1), \mathrm{LM}(f_2), \ldots, \mathrm{LM}(f_s)\rangle$. Eftersom det är lika många monom utanför idealen följer det att mängden monom utanför idealen är helt överlappande, varav monomen innanför idealen är desamma. Eftersom idealen är monomideal följer att idealen är desamma, ty de genereras av monom. Alltså, eftersom

$$\{f_1, f_2, \ldots, f_s\} \subseteq I \text{ och } \langle \mathrm{LM}(f_1), \mathrm{LM}(f_2), \ldots, \mathrm{LM}(f_s)\rangle = \mathrm{in}\, I$$

är $\{f_1, f_2, \ldots, f_s\}$ en Gröbnerbas av I. □

Sats 2.12. *Om I och J är två ideal av $k[x_1, x_2, \ldots, x_n]$ sådan att $I \subseteq J$ och $\mathrm{in}\, I = \mathrm{in}\, J$, då är $I = J$.*

Bevis. Låt $G = \{g_1, g_2, \ldots, g_s\}$ vara en Gröbnerbas av I. Då är

$$\langle \mathrm{LM}(g_1), \mathrm{LM}(g_2), \ldots, \mathrm{LM}(g_s)\rangle = \mathrm{in}\, I = \mathrm{in}\, J.$$

Men $G \subseteq I \subseteq J$ varav G är en Gröbnerbas av J per definition och $I = J$ enligt Sats 2.10. □

Följdsats 2.13. *Om I är ett ideal sådan att* $\mathrm{in}\, I = \mathrm{in}\sqrt{I}$ *är I radikalt.*

Bevis. Följdsatsen följer av att $I \subseteq \sqrt{J}$ och $\mathrm{in}\, I = \mathrm{in}\sqrt{I}$ varav $I = \sqrt{I}$. □

Definition 2.14 (Kongruent modulo I)**.** *Låt I vara ett ideal av polynomringen $k[x_1, x_2, \ldots, x_n]$ och f samt g två polynom i ringen. Polynomen sägs vara kongruenta modulo I om $f - g \in I$ och skrivs $f \equiv g \bmod I$.*

Definition 2.15. *Låt I vara ett ideal av $k[x_1, x_2, \ldots, x_n]$. Definiera kvotringen av $k[x_1, x_2, \ldots, x_n]$ modulo I som*

$$k[x_1, x_2, \ldots, x_n]/I \coloneqq \{[f] \mid f \in k[x_1, x_2, \ldots, x_n]\},$$

där $[f] = \{g \in k[x_1, x_2, \ldots, x_n] \mid g \equiv f \bmod I\}$ är ekvivalensklassen av f.

Sats 2.16. *Låt I vara ett ideal av $k[x_1, x_2, \ldots, x_n]$. Om $f, g \in k[x_1, x_2, \ldots, x_n]$ representerar samma ekvivalensklass i $k[x_1, x_2, \ldots, x_n]/I$, det vill säga om $[f] = [g]$, är $f(p) = g(p)$ för alla $p \in \mathbf{V}(I)$.*

Bevis. Eftersom

$$[f] = [g] \iff f \equiv g \bmod I \iff f - g \in I$$

och $I \subseteq \mathbf{I}(\mathbf{V}(I))$ gäller det att

$$f - g \in I \implies f - g \in \mathbf{I}(\mathbf{V}(I)) \iff (f - g)(p) = 0 \; \forall p \in \mathbf{V}(I),$$

varav

$$[f] = [g] \implies (f - g)(p) = 0 \; \forall p \in \mathbf{V}(I) \iff f(p) = g(p) \; \forall p \in \mathbf{V}(I).$$

□

Definition 2.17. *Låt I vara ett radikalt ideal av $k[x_1, x_2, \ldots, x_n]$ och $[f]$ en ekvivalensklass i $k[x_1, x_2, \ldots, x_n]/I$. Definiera evalueringen av $[f]$ i punkten $p \in \mathbf{V}(I)$ som $f(p)$.*

Notera att Definitionen 2.17 är väldefinierad enligt Sats 2.16.

Lemma 2.18. *Givet en monomordning på polynomringen $k[x_1, x_2, \ldots, x_n]$ och ett ideal $I \subseteq k[x_1, x_2, \ldots, x_n]$ gäller det att för varje polynom $f \in k[x_1, x_2, \ldots, x_n]$ existerar ett unikt polynom r sådant att $f \equiv r \bmod I$ och $r \notin \operatorname{in} I$ eller $r = 0$.*

Bevis. Välj en Gröbnerbas $G = \{g_1, g_2, \ldots, g_s\}$ av idealet I. Varje polynom $f \in k[x_1, x_2, \ldots, x_n]$ kan enligt Sats 2.6 skrivas som $f = q + r$ där $q \in I$ och $r = \overline{f}^G$ är en unik rest som antingen är noll eller vars termer inte är delbara med något av de ledande monomen till polynomen i G. Antag att $r \neq 0$. Eftersom resten av r vid division med $\{\mathrm{LM}(g_1), \mathrm{LM}(g_1), \ldots, \mathrm{LM}(g_s)\}$ är r följer att $r \notin \operatorname{in} I$ enligt Sats 2.9. □

Lemma 2.19. *Låt f, g vara polynom i $k[x_1, x_2, \ldots, x_n]$ och I ett ideal med Gröbnerbas G. För alla skalärer $c \in k$ är*

$$\overline{f+g}^G = \overline{f}^G + \overline{g}^G \text{ och } \overline{cf}^G = c\overline{f}^G.$$

Bevis. Att $\overline{f+g}^G = \overline{f}^G + \overline{g}^G$ följer av att $f+g$ kan skrivas som $q + \overline{f}^G + \overline{g}^G$ där $q \in I$. Eftersom $\overline{f}^G$ och $\overline{g}^G$ antingen är noll eller ett unikt polynom vars monom ej är delbara med de ledande monomen för polynomen i G, är summan $\overline{f}^G + \overline{g}^G$ antingen noll eller ett polynom vars monomen ej är delbara med de ledande monomen för polynomen i G. Alltså är $\overline{f}^G + \overline{g}^G$ den unika resten av $f+g$ vid division av G enligt Sats 2.6. Med andra ord är $\overline{f}^G + \overline{g}^G = \overline{f+g}^G$.

Att $\overline{cf}^G = c\overline{f}^G$ följer av att om $f = q + r$ där $q \in I$, $c \in k$, och $r = \overline{f}^G$ gäller att $cf = c(q+r) = cq + cr$ där $cq \in I$ och cr är antingen noll eller ett unikt polynom vars monomen ej är delbara med de ledande monomen för polynomen i G. Vilket i sin tur betyder att cr är den unika resten av cf dividerat med G enligt Sats 2.6. Med andra ord är $cr = c\overline{f}^G = \overline{cf}^G$. □

Lemma 2.20. *Funktionen $\psi : k[x_1, x_2, \ldots, x_n]/I \to \text{spann}(x^\alpha \mid x^\alpha \notin \text{in}\, I)$ definierad av $[f] \mapsto \overline{f}^G$ där G är en Gröbnerbas av I är bijektiv.*

Bevis. Först och främst är ψ väldefinierad. Låt g, f vara två polynom i $k[x_1, x_2, \ldots, x_n]/I$ sådan att $[f] = [g]$. Då är $f \equiv g \bmod I$. Men eftersom $f \equiv \overline{f}^G \bmod I$ och $g \equiv \overline{g}^G \bmod I$ är $\overline{f}^G \equiv \overline{g}^G \bmod I$, varav $\overline{f}^G - \overline{g}^G \equiv 0 \bmod I$. Alltså är

$$\psi(\overline{f}^G - \overline{g}^G) = \overline{\overline{f}^G - \overline{g}^G}^G = \overline{\overline{f}^G}^G - \overline{\overline{g}^G}^G = \overline{f}^G - \overline{g}^G = 0,$$

enligt Lemma 2.19, varav $\overline{f}^G = \overline{g}^G$ och $\psi(f) = \psi(g)$.

Låt $r \in \text{spann}(x^\alpha \mid x^\alpha \notin \text{in}\, I)$. Eftersom $r \notin \text{in}\, I$ och G är en Gröbnerbas av I är r inte delbart med något ledande monom av element i G, varav $r = 0 + r$ där $0 \in I$. Alltså är $r = \overline{r}^G$ och då $r \in [r] \in k[x_1, x_2, \ldots, x_n]/I$ är ψ surjektiv.

Låt $[f]$ och $[g]$ vara två element i $k[x_1, x_2, \ldots, x_n]/I$ sådan att $\psi[f] = \psi[g]$ då är $\overline{f}^G = \overline{g}^G =: r$. Detta innebär att $f = q_1 + r$ och $g = q_2 + r$ för något $q_1, q_2 \in I$. Alltså är $f - g = q_1 - q_2 \in I$, varav $[f] = [g]$. □

Sats 2.21. *Kvotringen $k[x_1, x_2, \ldots, x_n]/I$ betraktad som ett vektorrum är isomorf med* $\text{spann}(x^\alpha \mid x^\alpha \notin \text{in}\, I)$. *Dessutom är mängden*

$$\{x^\alpha \mid x^\alpha \notin \text{in}\, I, \alpha \in \mathbb{N}^n\}$$

linjärt oberoende modulo I.

Bevis. Enligt Lemma 2.20 utgör avbildningen $\psi([f]) = \overline{f}^G$ en bijektion mellan $k[x_1, x_2, \ldots, x_n]/I$ och $\text{spann}(x^\alpha \mid x^\alpha \notin \text{in}\, I)$ varav det endast återstår att visa att $\psi([f])$ bevarar vektorrumsoperationerna. Alltså att

$$\psi([f] + [g]) = \overline{f}^G + \overline{g}^G \text{ och } \psi(c[f]) = c\overline{f}^G, \ \forall c \in k.$$

Bevarandet av addition följer av att:

$$\psi([f] + [g]) = \psi([f + g]) = \overline{f + g}^G = \overline{f}^G + \overline{g}^G,$$

enligt Lemma 2.19. Och bevarandet av skalärmultiplikation följer av att

$$\psi(c[f]) = \psi([cf]) = \overline{cf}^G = c\overline{f}^G \ \forall c \in k$$

enligt samma lemma.

Det återstår endast att visa att mängden

$$\{x^\alpha \mid x^\alpha \notin \text{in}\, I, \alpha \in \mathbb{N}^n\}$$

är linjärt oberoende modulo I. Låt A vara en godtycklig ändlig delmängd av $\{x^\alpha \mid x^\alpha \notin \text{in}\, I, \alpha \in \mathbb{N}^n\}$ och antag att

$$\sum_{x^\alpha \in A} c_\alpha x^\alpha \equiv 0 \mod I$$

för skalärer c_α i k sådan åtminstone någon c_α är nollskild. Per definition av kongruens modulo I ligger $\sum_{x^\alpha \in A} c_\alpha x^\alpha$ i $I \subseteq k[x_1, x_2, \ldots, x_n]$ varav $\text{LM}(\sum_{x^\alpha \in A} c_\alpha x^\alpha) \in \text{in}\, I$, vilket är en motsägelse då $\text{LM}(\sum_{x^\alpha \in \Sigma} c_\alpha x^\alpha) \in A$. Alltså är $c_\alpha = 0$ för alla $\alpha \in A$ och A är linjärt oberoende modulo I. □

Sats 2.22. *Låt I vara ett nolldimensionellt ideal av $k[x_1, x_2, \ldots, x_n]$. För varje $i \in \{1, \ldots, n\}$ existerar ett $\beta_i \in \mathbb{N}$ sådan att $x_i^{\beta_i} \in \text{in}\, I$ och*

$$\dim k[x_1, x_2, \ldots, x_n]/I = \dim \text{spann}(x^\alpha \mid x^\alpha \notin \text{in}\, I) \leq \beta_1 \cdot \beta_2 \cdots \beta_n.$$

Dessutom är antalet punkter i $\mathbf{V}(I)$ ändligt.

Bevis. Alla monom $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ där $\alpha_i \geq \beta_i$ för alla $i \in \{1, 2, \ldots, n\}$ ligger i $\text{in}\, I$. Monomen i komplementet av $\text{in}\, I$ uppfyller därför att $0 \leq \alpha_i < \beta_i$ och är alltså inte fler än $\beta_1 \cdot \beta_2 \cdots \beta_n$. Alltså är $\text{spann}(x^\alpha \mid x^\alpha \notin \text{in}\, I)$ ändligtdimensionell varav Sats 2.21 ger att kvotringen $k[x_1, x_2, \ldots, x_n]/I$ är ändligdimensionell. Enligt samma sats är monomen utanför $\text{in}\, I$ linjärt oberoende. Eftersom vektorrumsisomorfier bevarar relationen att vektorer är linjärt oberoende är $\{[x^\alpha] \mid x^\alpha \notin \text{in}\, I\} \subseteq k[x_1, x_2, \ldots, x_n]/I$ linjärt oberoende. Alltså är

$$\dim k[x_1, x_2, \ldots, x_n]/I = \dim \text{spann}(x^\alpha \mid x^\alpha \notin \text{in}\, I),$$

som i sin tur är lika med antalet monom utanför in I vilket är begränsat av $\beta_1 \cdot \beta_2 \cdots \beta_n$.

Det återstår att visa att $\mathbf{V}(I)$ är ändligt. Betrakta de i:te koordinaterna av punkterna i $\mathbf{V}(I)$ samt ekvivalensklasserna $[x_i^j]$ för $j \in \mathbb{N}$. Eftersom $\dim k[x_1, x_2, \ldots, x_n]/I \leq \beta_1 \cdot \beta_2 \cdots \beta_n$ måste uppsättningen ekvivalensklasser $\{[x_i^j] \mid j \in \{1, 2, \ldots, \beta_1 \cdot \beta_2 \cdots \beta_n + 1\}\}$ vara linjärt beroende, vilket per definition innebär att

$$\sum_{j=0}^{\beta_1 \cdot \beta_2 \cdots \beta_n + 1} c_j [x_i^j] = [0],$$

där c_j är skalärer sådan att åtminstone en är nollskild. Det innebär i sin tur att

$$\sum_{j=0}^{\beta_1 \cdot \beta_2 \cdots \beta_n + 1} c_j x_i^j \in I.$$

Eftersom ekvationen

$$\sum_{j=0}^{\beta_1 \cdot \beta_2 \cdots \beta_n + 1} c_j x_i^j = 0$$

har ändligt många lösningar finns det ändligt många distinkta i-koordinater i $\mathbf{V}(I)$. Men då i är ett godtyckligt element i $\{1, 2, \ldots, n\}$ finns endast ändligt många punkter i $\mathbf{V}(I)$. □

Lemma 2.23 (Separatorpolynom)**.** *Givet skilda punkter $p_1, p_2, \ldots, p_s$ i k^n existerar polynom $f_i \in k[x_1, x_2, \ldots, x_n]$ sådant att $f_i(p_t) = 0$ om $i \neq t$ och $f_i(p_t) = 1$ om $i = t$, för alla i och t tillhörandes mängden $\{1, 2, \ldots, s\}$.*

Bevis. Utan att förlora allmängiltighet antag att p_1 och p_2 skiljer sig vid j:te koordinaten och låt a_j respektive b_j vara de j:te koordinaterna för respektive punkt. Polynomet $g_2 = (x_j - b_j)(a_j - b_j)^{-1}$ evalueras till 1 i punkten p_1 och 0 i punkten p_2. Konstruera polynomen $g_3, g_4, \ldots, g_s$ analogt sådant att $g_i(p_1) = 1$ och $g_i(p_t) = 0$ för alla $i \in \{3, 4, \ldots, s\}$ och $t \in \{2, 3, \ldots, s\}$. Polynomet $f_1 = g_2 g_3 \ldots g_s$ har då egenskapen att $f_1(p_1) = 1$ och $f_1(p_t) = 0$ för $t \in \{2, 3, \ldots, s\}$. Analogt kan polynom $f_i \in k[x_1, x_2, \ldots, x_n]$ konstrueras för resterande $i \in \{2, 3, \ldots, s\}$. □

Exempel 2.2. *Betrakta punkterna $p_1 = (1, 1), p_2 = (0, 1), p_3 = (1, 2)$ i $\mathbb{C}^2$. Punkterna p_1 och p_2 skiljer sig i första koordinaten varav polynomet $g_2 = (x_1 - 0)/(1 - 0) = x_1 \in \mathbb{C}[x_1, x_2]$ evalueras till 1 i p_1 och 0 i p_2. På liknande sätt fås att $g_3 = (x_2 - 2)/(1 - 2) = -x_2 + 2$. Sist fås att $f_1 = g_2 g_3 = -x_1 x_2 + 2x_1$ är ett polynom i $\mathbb{C}[x_1, x_2]$ som evalueras till 1 i p_1 men 0 i p_2 och p_3.*

Sats 2.24 (Hilberts Nullstellensatz)**.** *Låt k vara en algebraisk sluten kropp och I ett ideal av $k[x_1, x_2, \ldots, x_n]$. Om $f \in k[x_1, x_2, \ldots, x_n]$ är $f \in \mathbf{I}(\mathbf{V}(I))$ om och endast om $f^\alpha \in I$. Med andra ord:*

$$\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}.$$

Bevis av Hilberts Nullstellensatz går att hitta i exempelvis [1].

Sats 2.25. *Om V är en ändlig affine varietet av k^n är idealet $\mathbf{I}(V)$ av $k[x_1, x_2, \ldots, x_n]$ nolldimensionellt.*

Bevis. Antag att V är tomma mängden. Då är $\mathbf{I}(V) = k[x_1, x_2, \ldots, x_n]$ varav $x_i^0 \in \operatorname{in}\mathbf{I}(V)$ för alla $i \in \{1, 2, \ldots, n\}$. Antag att $V = \{p_1, p_2, \ldots, p_s\}$ för något $s \in \mathbb{N} \setminus \{0\}$. Betrakta polynomen $f_i = (x_i - (p_1)_i)(x_i - (p_2)_i) \cdots (x_i - (p_s)_i)$ för alla $i \in \{1, 2, \ldots, n\}$. Polynomen f_i försvinner per konstruktion på alla punkter i V och ligger därmed i $\mathbf{I}(V)$. Enligt Anmärkning 1.6 är $\operatorname{LM}(f_i) = x_i^s$ och ligger således i $\operatorname{in}\mathbf{I}(V)$ för alla $i \in \{1, 2, \ldots, n\}$ varav $\mathbf{I}(V)$ är nolldimensionellt. □

Sats 2.26. *Låt I vara ett nolldimensionellt ideal av $k[x_1, x_2, \ldots, x_n]$. För alla $i \in \{1, \ldots, n\}$ gäller att $x_i^{\alpha_i} \in \operatorname{in} I$ för något $\alpha_i \in \mathbb{N}$. Antalet punkter i $\mathbf{V}(I)$ är som mest antalet monom utanför $\operatorname{in} I$, vilket i sin tur inte är fler än $\alpha_1 \cdot \alpha_2 \cdots \alpha_n$. Om k dessutom är algebraisk sluten är I radikalt om och endast om*

$$|\mathbf{V}(I)| = \dim k[x_1, x_2, \ldots, x_n]/I = \textit{antalet monom utanför } \operatorname{in} I.$$

Bevis. Enligt Sats 2.22 är $|\mathbf{V}(I)| < \infty$. Skriv $\mathbf{V}(I)$ som $\{p_1, p_2 \ldots, p_s\}$ och konstruera polynomen f_i, $i \in \{1, 2, \ldots, s\}$, som evalueras till 1 i punkten p_i och 0 i de andra, i enlighet med Lemma 2.23. Om $[f_1], [f_2], \ldots, [f_s]$ är linjärt oberoende följer det att $s \leq \dim k[x_1, x_2, \ldots, x_n]/I$. Antag därför att

$$\sum_i^s a_i[f_i] = [\sum_i^s a_i f_i] = [0]$$

för en godtycklig uppsättning skalärer $a_i \in k$. Det innebär att polynomet $g = \sum_i^s a_i f_i \in I$. Alltså för alla $j \in \{1, 2, \ldots, s\}$ är

$$0 = g(p_j) = \sum_i^s a_i f_i(p_j) = 0 + a_j f_j(p_j) = a_j.$$

Av Sats 2.22 följer att $s \leq \alpha_1 \cdot \alpha_2 \cdots \alpha_n$.

Om k dessutom är algebraisk sluten och I radikal utgör $[f_1], [f_2], \ldots, [f_s]$ en bas för $k[x_1, x_2, \ldots, x_n]/I$ vilket kan visas med hjälp av Hilberts Nullstellensatz. Ta en godtycklig ekvivalensklass $[g]$ från $k[x_1, x_2, \ldots, x_n]/I$. Det

återstår att visa att $[g]$ kan skrivas som en linjärkombination av polynomen $[f_1], [f_2], \ldots, [f_s]$. Låt a_i beteckna funktionsvärdet av g evaluerat i punkten $p_i \in \mathbf{V}(I) = \{p_1, p_2, \ldots, p_s\}$. Polynomet $h = g - \sum_i^s a_i f_i$ evalueras till 0 per konstruktion i alla punkter av $\mathbf{V}(I) = \{p_1, p_2, \ldots, p_s\}$ och ligger därmed per definition i idealet $\mathbf{I}(V)$. Av Hilberts Nullstellensatz 2.24 följer att $\mathbf{I}(V) = \mathbf{I}(\mathbf{V}(I)) = \sqrt{I} = I$ ty I är radikal. Alltså $h \in I$ och $[h] = [0]$ varav $[g] = \sum_i^s a_i[f_i]$. Eftersom s är antalet punkter i $\mathbf{V}(I)$ och då $[f_1], [f_2], \ldots, [f_s]$ utgör en bas för $k[x_1, x_2, \ldots, x_n]/I$ är $s = \dim k[x_1, x_2, \ldots, x_n]/I$ antalet monom utanför $\operatorname{in} I$ enligt Sats 2.21 och Sats 2.22.

Det återstår endast att visa att om antalet monom utanför initialidealet av I är lika många som antalet punkter i $\mathbf{V}(I)$ så är I radikalt. Betrakta det radikala idealet $\mathbf{I}(\mathbf{V}(I))$, antalet punkter i $\mathbf{V}(\mathbf{I}(\mathbf{V}(I))) = \mathbf{V}(I)$ är $|\mathbf{V}(I)|$ vilket är antalet monom utanför $\operatorname{in}\mathbf{I}(\mathbf{V}(I))$ (vilket visades tidigare i beviset). Det gäller dessutom att $I \subseteq \mathbf{I}(\mathbf{V}(I))$ varav $\operatorname{in} I \subseteq \operatorname{in}\mathbf{I}(\mathbf{V}(I))$. Eftersom det är lika många monom utanför initialidealen samt att ena initialidealet är inneslutet i det andra följer likheten $\operatorname{in} I = \operatorname{in}\mathbf{I}(\mathbf{V}(I))$ varav $I = \mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$ enligt Sats 2.12. □

Följdsats 2.27. *Om V är en ändlig affine varietet av k^n är antalet monom utanför initialidealet av $\mathbf{I}(V)$ kardinaliteten av V. Det vill säga*

$$|V| = |\{\alpha \mid x^\alpha \notin \operatorname{in}\mathbf{I}(V)\}|.$$

Bevis. Med hjälp av Buchberger-Möller-algoritmen Definition 1.17 kan en Gröbnerbas G av idealet $\mathbf{I}(V)$ tas fram i $k[x_1, x_2, \ldots, x_n]$. På samma sätt kan en Gröbnerbas $\bar{G}$ av idealet $\mathbf{I}(V)$ tas fram i $\bar{k}[x_1, x_2, \ldots, x_n]$, där $\bar{k}$ är den algebraiska tillslutningen av k. Enligt Buchberger-Möller-algoritmen som beskriven i [3] kommer $G = \bar{G}$. Betraktat i ringen $\bar{k}[x_1, x_2, \ldots, x_n]$ är antalet monom utanför initialidealet av $\mathbf{I}(V)$ exakt $|V|$ enligt Sats 2.26. Eftersom det är samma monom utanför initialidealet av $\mathbf{I}(V)$ betrakta i $k[x_1, x_2, \ldots, x_n]$ följer satsen. □

Sats 2.28. *Låt $P = \{p_1, p_2, \ldots, p_s\}$ vara en ändlig uppsättning punkter i k^n och låt $m_1, m_2, \ldots, m_s$ vara monomen utanför $\operatorname{in}\mathbf{I}(P)$. Matrisen*

$$\big(m_j(p_i)\big)_{i,j}$$

har full rang.

Bevis. Antag att matrisen $\big(m_j(p_i)\big)_{i,j}$ inte är inverterbar. Då kan nollvektorn skrivas som en icketrival linjärkombination av kolonnerna:

$$c_1\big(m_1(p_i)\big)_j + c_2\big(m_2(p_i)\big)_j + \ldots + c_s\big(m_s(p_i)\big)_j = 0,$$

där $c_1, c_2, \ldots, c_s$ är skalärer varav åtminstone en är nollskild. Alltså är

$$\sum_{i=1}^{s} c_i m_i(p) = 0 \, \forall p \in P \iff \sum_{i=1}^{s} c_i m_i \in \mathbf{I}(P),$$

varav $\mathrm{LM}(\sum_{i=1}^{s} c_i m_i) \in \mathrm{in}\,\mathbf{I}(P)$. Eftersom $\mathrm{LM}(\sum_{i=1}^{s} c_i m_i) = m_i$ för något $i \in \{1, 2, \ldots, s\}$ fås en motsägelse. □

Definition 2.29 (Vandermondematris)**.** *Låt $1, a_1, a_2, \ldots, a_n$ vara element i k. Matrisen*

$$\begin{pmatrix} 1 & a_1^1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2^1 & a_2^2 & \cdots & a_2^{n-1} \\ 1 & a_3^1 & a_3^2 & \cdots & a_4^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_n^1 & a_n^2 & \cdots & a_n^{n-1} \end{pmatrix}$$

kallas för en Vandermondmatris.

2.2 Bestämning av nollställemängden $\mathbf{V}(I)$ för nolldimensionella ideal I

Detta delkapitel innehåller ingen större relevans för resultaten i kapitel 3, utan inkluderas endast för dess relevans för nolldimensionella ideal i övrigt. Delkapitlet redogör för två olika metoder att lösa system av polynomekvationer förutsatt att lösningsmängden är ändlig. För första metoden, eliminationsteori, har [1] använts som källa. Den andra metoden bygger på teori från artikeln [6].

2.2.1 Eliminationsteori

Definition 2.30 (Elimineringsideal)**.** *Låt I vara ett ideal av $k[x_1, x_2, \ldots, x_n]$. För alla $i \in \{0, 2, \ldots, n-1\}$ definiera det i:te elimineringsidealet av I som*

$$I_i \coloneqq I \cap k[x_{i+1}, x_{i+2}, \ldots, x_n].$$

Sats 2.31. *Låt I vara ett ideal av $k[x_1, x_2, \ldots, x_n]$. För alla $i \in \{0, 1, \ldots, n-1\}$ är det i:te elimineringsidealet I_i ett ideal av $k[x_{i+1}, x_{i+2}, \ldots, x_n]$.*

Bevis. Låt $f, g \in I_i$ då är $f + (-g) \in I_i$ för alla $i \in \{0, 1, \ldots, n-1\}$. Låt $h \in k[x_{i+1}, x_{i+2}, \ldots, x_n] \subseteq k[x_1, x_2, \ldots, x_n]$. För alla $i \in \{0, 1, \ldots, n-1\}$ gäller att om $f \in \mathrm{in}\, I_i$ är $f \in I$ varav $hf \in I$ och $hf \in k[x_{i+1}, x_{i+2}, \ldots, x_n]$ varav $hf \in I_i$. □

Anmärkning 2.32. *Notera att om I är ett nolldimensionellt ideal är även alla elimineringsideal nolldimensionella ty om $x_i^{\alpha_i} \in I$, där $\alpha_i \in \mathbb{N}$, är $x_i^{\alpha_i} \in I_j$ för alla $i \in \{j+1, j+2, \ldots, n-1\}$ och för alla $j \in \{0, 1, \ldots, n-1\}$.*

Lemma 2.33. *Låt I vara ett ideal i $k[x_1, x_2, \ldots, x_n]$. För alla $i \in \{0, 1, \ldots, n-2\}$ är $(I_i)_1 = I_{i+1}$.*

Bevis. Eftersom I_i är ett ideal i $k[x_{i+1}, x_{i+2}, \ldots, x_n]$ är

$$\begin{aligned}(I_i)_1 &= I_i \cap k[x_{i+2}, x_{i+3}, \ldots, x_i] \\ &= (I \cap k[x_{i+1}, x_{i+2}, \ldots, x_n]) \cap k[x_{i+2}, x_{i+3}, \ldots, x_n] \\ &= I \cap k[x_{i+2}, x_{i+3}, \ldots, x_i] \\ &= I_{i+1} \; \forall i \in \{0, 1, \ldots, n-2\}.\end{aligned}$$

□

Sats 2.34. *Antag I är ett ideal av $k[x_1, x_2, \ldots, x_n]$ och G en Gröbnerbas av I med avseende på lexikografisk monomordning gäller för alla $i \in \{1, 2, \ldots, n\}$. Då gäller att $G \cap k[x_{i+1}, x_{i+2}, \ldots, x_i]$ är en Gröbnerbas av I_i med avseende på samma monomordning.*

Ett bevis för Sats 2.34 finns att läsa i [1].

Sats 2.35 (Elimineringssatsen)**.** *Låt k vara en algebraisk sluten kropp och $I = \langle f_1, f_2, \ldots, f_s \rangle$ ett ideal av $k[x_1, x_2, \ldots, x_n]$. Låt I_1 vara det första elimineringsidealet av I. För varje $1 \leq i \leq s$ skriv f_i på formen*

$$f_i = c_i x_i^{\alpha_i} + \text{ termer där graden av } x_i \text{ är mindre än } \alpha_i \in \mathbb{N},$$

där $c_i \in k[x_2, x_3, \ldots, x_n]$. Antag att det finns en partiell lösning $(a_2, a_3 \ldots, a_n)$ i $\mathbf{V}(I_1)$. Om $(a_2, a_3, \ldots, a_n) \notin \mathbf{V}(c_1, c_2, \ldots, c_s)$ existerar ett $a_1 \in k$ sådan att $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$.

Ett bevis för Sats 2.35 finns att läsa i [1].

Följdsats 2.36. *Antag att I är ett nolldimensionellt ideal, k är algebraisk sluten och $G = \{g_1, g_2, \ldots, g_s\}$ är en reducerad Gröbnerbas av I med avseende på lexikografisk monomordning där $x_n < x_{n-1} < \cdots < x_1$. Då existerar ett $g \in G$ sådan att $f \in k[x_n]$.*

Bevis. Låt $G = \{g_1, g_2, \ldots, g_s\}$ vara en reducerad Gröbnerbas av I med avseende på lexikografiska monomordningen där $x_n < x_{n-1} < \cdots < x_1$. Eftersom I är nolldimensionellt ligger x_n^α i $\operatorname{in} I$ för något $\alpha \in \mathbb{N}$ varav $\overline{x_n^\alpha}^G = 0$ enligt Sats 2.9. Låt $\alpha \in \mathbb{N}$ vara minsta talet sådan att $x_n^\alpha \in \operatorname{in} I$. Ett sådant α existerar eftersom I är nolldimensionellt. Av denna anledning måste $\operatorname{LM}(g_i) = x_n^\alpha$ för något $i \in \{1, 2, \ldots, s\}$. Skriv g_i på formen

$$g_i = c_i x_n^\alpha + \text{ termer där graden av } x_n \text{ är mindre än } \alpha \in \mathbb{N}$$

där $c_1 = 1 \in k[x_2, x_3, \ldots, x_n]$, inses att om $(a_2, a_3 \ldots, a_n)$ är en partiell lösning i $\mathbf{V}(I_1)$ existerar ett a_1 sådan att $(a_1, a_2, \ldots, a_n) \in \mathbf{V}(I)$ enligt

Sats 2.35. Notera att $(a_2, a_3 \ldots, a_n) \notin \mathbf{V}(c_1, c_2, \ldots, c_s) = \mathbf{V}(1, c_2, \ldots, c_s) = \mathbf{V}(1) = \emptyset$. Antag att $I_1 = \langle 0 \rangle$ då är $\mathbf{V}(I_1) = k$. Eftersom k är algebraisk sluten och därmed innehåller oändligt många element fås en motsägelse ty då skulle $\mathbf{V}(I)$ innehålla oändligt många punkter vilket motsäger att I är nolldimensionellt enligt Sats 2.22.

Eftersom $I_1 \neq \langle 0 \rangle$ är ett nolldimensionellt ideal av $k[x_2, x_3, \ldots, x_n]$ kan argumentet ovan återupprepas varav första elimineringsidealet av I_1 också är skilt från nollidealet. Av Lemma 2.33 är I_2 första elimineringsidealet av I_1. Ytterligare upprepning av argumentet ger att $I_{n-1} \neq \langle 0 \rangle$. Enligt Sats 2.34 är $G_{n-1} = G \cap k[x_n]$ en Gröbnerbas av I_{n-1}. Observera att $G_{n-i} \neq \emptyset$ varav det existerar ett polynom $g \in G \cap k[x_n]$ varav $g \in G$ och $g \in k[x_n]$. $\square$

Följdsats 2.36 säger att givet en algebraisk sluten kropp k och ett nolldimensionellt ideal I av $k[x_1, x_2, \ldots, x_n]$ går att hitta ett polynom $f \in k[x_n]$. Dessutom kan alla nollställen av f förlängas till punkter i $\mathbf{V}(I)$ enligt Sats 2.35. Sammantaget erhålls ett systematiskt tillvägagångsätt att teoretiskt hitta alla punkter i nollställemängden av I. Ta fram en Gröbnerbas av I med avsende på lexikografisk monomordning, förslagsvis med hjälp av Buchberger-Möller-algoritmen [2]. Eftersom den framtagna Gröbnerbasen innehåller ett polynom i $k[x_n]$ kan rötterna till polynomet enkelt erhållas ifall graden av polynomet är lägre än fem och i vissa fall även annars. När rötterna till polynomet i $k[x_n]$ är framtaget kan variabeln x_n i de andra generatorerna ersättas med den partiella lösningen, varav polynomen som då erhålls i $k[x_1, x_2, \ldots, x_{n-1}]$ genererar ett nytt nolldimensionellt ideal vars nollställemängd är en förlängning av nollställemängden till polynomet i $k[x_n]$, enligt elimineringssatsen Sats 2.35. Proceduren kan återupprepas på det nya idealet i $k[x_1, x_2, \ldots, x_{n-1}]$ och sedan ytterligare gånger tills ett ideal i endast en variabel erhålls och de partiella rötterna har slagits samman till nollställemängden av I.

Dock säger Abel–Ruffinis sats att det inte finns någon sluten formel som endast använder addition, subtraktion, multiplikation, division, upphöjning eller rotutdragning för att hitta rötterna till polynom av grad större eller lika med fem. Vilket kan göra det praktiskt svårt att använda elimineringsmetoden utan att använda sig av approximativa rötter till generatorerna.

Exempel 2.3. *Det nolldimensionella idealet*

$$I = \mathbf{I}(\{(4, 5, 7, 4, 0), (4, 3, 4, 1, 3), (2, 3, 5, 3, 4)\}) \subset \mathbb{Q}[x_1, x_2, \ldots, x_5]$$

har

$$\begin{aligned} G = \{&x_5^3 - 7x_5^2 + 12x_5, 4x_4 - 3x_5^2 + 13x_5 - 16, 2x_3 - x_5^2 + 5x_5 - 14, \\ &6x_2 - x_5^2 + 7x_5 - 30, 2x_1 + x_5^2 - 3x_5 - 8\} \end{aligned}$$

som en Gröbnerbas med avseende på lexikografisk monomordning. Polynomet $x_5^3 - 7x_5^2 + 12x_5 \in I_1 \subset k[x_5]$ *har nollställena* $0, 3, 4$. *Dessa nollställen kan förlängas till punkter i* $\mathbf{V}(I)$. *Ersätts* x_5 *i de andra generatorerna med* $0, 3$ *respektive* 4 *kan resterande koordinater av dessa punkter bestämmas. Till exempel ger den andra generatorn att om* $x_5 = 0$ *måste* $x_4 = 4$. *På detta sätt, genom ersättning av variablerna* x_5 *från de andra generatorerna med nollställena till första generatorn erhålls till slut att*

$$\mathbf{V}(I) = \{(4, 5, 7, 4, 0), (4, 3, 4, 1, 3), (2, 3, 5, 3, 4)\}.$$

2.2.2 Bestämning av $\mathbf{V}(I)$ utifrån multiplikationsmatrisen

Detta kapitel är starkt inspirerat av artikeln [6].

Låt $[f] \in k[x_1, x_2, \ldots, x_n]/I$ där I är ett nolldimensionellt ideal och låt $[t_1], [t_2], \ldots, [t_s]$ vara en bas för $k[x_1, x_2, \ldots, x_n]/I$. Multiplicera varje baselement $[t_i]$ med f fås att

$$[f \cdot t_i] = \sum_{j=1}^{s} a_{i,j}[t_j], \tag{1}$$

för varje $i \in \{1, 2, \ldots, s\}$ där

$$M_f = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,s} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s,1} & a_{s,2} & \cdots & a_{s,s} \end{pmatrix}$$

är multiplikationsmatrisen associerad med f. Hur multiplikationsmatrisen beräknas illustreras genom Exempel 2.4. Multiplikationen av baselementen $[t_1], [t_2], \ldots, [t_s]$ med polynomet $f \in k[x_1, x_2, \ldots, x_n]$ kan på matrisform skrivas som

$$M_f \begin{pmatrix} [t_1] \\ [t_2] \\ \vdots \\ [t_s] \end{pmatrix} = \begin{pmatrix} [f \cdot t_1] \\ [f \cdot t_2] \\ \vdots \\ [f \cdot t_s] \end{pmatrix} = [f] \begin{pmatrix} [t_1] \\ [t_2] \\ \vdots \\ [t_s] \end{pmatrix}.$$

Betrakta nu en punkt $p \in \mathbf{V}(I)$ och evaluera $[t_i]$ och $[f]$ från ekvation (1) i p. Observera att denna evaluering är väldefinerad för p $\in \mathbf{V}(I)$ enligt Sats 2.16. Då gäller det att

$$f(p)t_i(p) = \sum_{j=1}^{s} a_{i,j}t_j(p),$$

ty $ft_i - \sum_{j=1}^{s} a_{i,j}t_j \in I$ och $p \in \mathbf{V}(I)$. Alltså råder även att

$$M_f \begin{pmatrix} t_1(p) \\ t_2(p) \\ \vdots \\ t_s(p) \end{pmatrix} = f(p) \begin{pmatrix} t_1(p) \\ t_2(p) \\ \vdots \\ t_s(p) \end{pmatrix}.$$

Eftersom $(t_1(p), t_2(p), \ldots, t_s(p))^T$ inte beror på f är $(t_1(p), t_2(p), \ldots, t_s(p))^T$ en gemensam egenvektor av matriserna M_f där $f \in k[x_1, x_2, \ldots, x_n]$. Observera att mängden gemensamma egenvektorer $\{(t_1(p), t_2(p), \ldots, t_s(p))^T \mid p \in \mathbf{V}(I)\}$ är linjärt oberoende enligt Sats 2.28. Speciellt intressant är när f är någon av variablerna $x_1, x_2, \ldots, x_n$ eftersom då är $x_i(p)$ ett egenvärde av M_{x_i} med tillhörande egenvektor $(t_1(p), t_2(p), \ldots, t_s(p))^T$. Men $x_i(p)$ är i själva verket den i:te koordinaten av p och eftersom detta gäller för alla $i \in \{1, 2, \ldots, s\}$ och alla $p \in \mathbf{V}(I)$ inses att alla koordinater för punkterna i $\mathbf{V}(I)$ återfinns som egenvärden av matriserna M_{x_i} för $i \in \{1, 2, \ldots, s\}$. Eftersom $(t_1(p), t_2(p), \ldots, t_s(p))^T$ är en gemensam egenvektor av multiplikationsmatriserna för alla $p \in \mathbf{V}(I)$ beräknas den i:te koordinaten av p genom att beräkna egenvärdet för M_{x_i} tillhörande den gemensamma egenvektorn.

För att bestämma $\mathbf{V}(I)$ återstår endast att hitta de gemensamma egenvektorerna för multiplikationsmatriserna M_{x_i} för alla $i \in \{1, 2, \ldots, n\}$. Ifall en multiplikationsmatris M_f för något f har s distinkta egenvärden utgör de motsvarande egenvektorerna gemensamma egenvektorer för samtliga multiplikationsmatriser. Om M_f däremot har samma egenvärde $f(p_1) = f(p_2)$ för två distinkta punkter p_1 och p_2 i $\mathbf{V}(I)$ men linjärt oberoende egenvektorer $(t_1(p_1), t_2(p_1), \ldots, t_s(p_1))^T$ och $(t_1(p_2), t_2(p_2), \ldots, t_s(p_2))^T$ kan det finnas fler egenvektorer av M_f som ej är egenvektorer av de andra multiplikationsmatriserna. Antag att $f(p_1) = f(p_2)$ är egenvärdet av motsvarande egenvektorer $(t_1(p_1), t_2(p_1), \ldots, t_s(p_1))^T$ och $(t_1(p_2), t_2(p_2), \ldots, t_s(p_2))^T$. Då gäller det att

$$M_f\left(c_1 \begin{pmatrix} t_1(p_1) \\ t_2(p_1) \\ \vdots \\ t_s(p_1) \end{pmatrix} + c_2 \begin{pmatrix} t_1(p_2) \\ t_2(p_2) \\ \vdots \\ t_s(p_2) \end{pmatrix}\right) = c_1 M_f \begin{pmatrix} t_1(p_1) \\ t_2(p_1) \\ \vdots \\ t_s(p_1) \end{pmatrix} + c_2 M_f \begin{pmatrix} t_1(p_2) \\ t_2(p_2) \\ \vdots \\ t_s(p_2) \end{pmatrix},$$

vilket i sin tur är lika med

$$c_1 f(p_1) \begin{pmatrix} t_1(p_1) \\ t_2(p_1) \\ \vdots \\ t_s(p_1) \end{pmatrix} + c_2 f(p_2) \begin{pmatrix} t_1(p_2) \\ t_2(p_2) \\ \vdots \\ t_s(p_2) \end{pmatrix} = f(p_1)\left(c_1 \begin{pmatrix} t_1(p_1) \\ t_2(p_1) \\ \vdots \\ t_s(p_1) \end{pmatrix} + c_2 \begin{pmatrix} t_1(p_2) \\ t_2(p_2) \\ \vdots \\ t_s(p_2) \end{pmatrix}\right),$$

för alla skalärer c_1 och c_2 i k. Alltså är linjärkombinationer av vektorerna $(t_1(p_1), t_2(p_1), \ldots, t_s(p_1))^T$ och $(t_1(p_2), t_2(p_2), \ldots, t_s(p_2))^T$ också egenvektorer av M_f med egenvärde $f(p_1)$. Rent praktiskt löses problemet med att hitta de gemensamma egenvektorerna således av att slumpa polynom f tills M_f har s stycken egenvärden. Låt f och g vara polynom med och låt M_f och M_g vara motsvarande multiplikationsmatriser. Beteckna med $a_{i,j}$ elementen på rad i kolumn j för matriserna M_f och beteckna på motsvarande sätt elementen i M_g med $b_{i,j}$. För alla skalärer c_1 och c_2 i k gäller att

$$c_1[f \cdot t_i] + c_2[g \cdot t_i] = c_1 \sum_{j=1}^{s} a_{i,j}[t_j] + c_2 \sum_{j=1}^{s} b_{i,j}[t_j] = \sum_{j=1}^{s} (c_1 a_{i,j} + c_2 b_{i,j})[t_j]$$

och därmed är $c_1 M_f + c_2 M_g = M_{c_1 f + c_2 g}$. Alltså går det lika bra att slumpa olika linjärkombinationer av befintliga multiplikationsmatriser tills en med s stycken egenvärden har funnits. Egenvektorerna för den matrisen utgör gemensamma egenvektorer för alla multiplikationsmatriser varav mängden $\mathbf{V}(I)$ kan bestämmas enligt metoden beskriven i förra stycket.

Exempel 2.4. *Betrakta idealet* $I = \langle y^2 - y, xy - x, x^2 - x \rangle \subseteq k[x_1, x_2, \ldots, x_n]$. *Givet den graderade lexikografiska monomordningen är* $\{y^2 - y, xy - x, x^2 - x\}$ *en Gröbnerbas av* I. *Monomen utanför* $\operatorname{in} I$ *är* $1, x$ *och* y *och* $\{[1], [x], [y]\}$ *utgör en bas för* $k[x_1, x_2, \ldots, x_n]/I$. *Multipliceras basen med* $[x]$ *respektive* $[y]$ *fås att*

$$[x][1] = [x],\ [x][x] = [x],\ [x][y] = [x],$$
$$[y][1] = [y],\ [y][x] = [x],\ [y][y] = [y].$$

Multiplikationsmatriserna ges därmed av

$$M_x = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{pmatrix} \text{ och } M_y = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

För att hitta de gemensamma egenvektorerna av M_x *och* M_y *multipliceras först multiplikationsmatiserna med slumpmässiga skalärer för att sedan adderas till en ny multiplikationsmatris. Låt* M_x *multiplicera med* 3 *och* M_y *med* 5. *Den nya matrisen blir*

$$\begin{pmatrix} 0 & 3 & 5 \\ 0 & 8 & 0 \\ 0 & 3 & 5 \end{pmatrix}$$

och har tre distinkta egenvärden $8, 5$ *och* 0 *med motsvarande egenvektorer* $(1,1,1)^T$, $(1,0,1)^T$, *samt* $(1,0,0)^T$. *Eftersom egenvärdena är distinkta är*

egenvektorerna gemensamma för alla multiplikationsmatriser. Multipliceras M_x med första egenvektorn fås att

$$M_x \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = 1 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Eftersom egenvärdet är 1 finns en punkt p_1 i $\mathbf{V}(I)$ som har 1 som första koordinat. Multipliceras samma egenvetor med M_y fås

$$M_y \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = 1 \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Alltså är även den andra koordinaten 1 varav $p_1 = (1, 1)$. Återupprepas proceduren med nästa egenvektor fås

$$M_x \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = 0 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \text{ och } M_y \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = 1 \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}.$$

Alltså ligger även $p_2 = (0, 1)$ i $\mathbf{V}(I)$. Sist fås även att

$$M_x \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = 0 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \text{ och } M_y \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = 0 \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},$$

varav $p_3 = (0, 0)$ är den sista punkten i $\mathbf{V}(I)$. Sammanfattningsvis har $\mathbf{V}(I) = \{(1, 1), (0, 1), (0, 0)\}$ beräknats utifrån egenvärdena och egenvektorerna av multiplikationsmatriserna.

2.3 Trappmängder

Definition 2.37 (Trappa)**.** *Låt P vara en ändlig delmängd av $\mathbb{N}^n$. Definiera trappan av P som*

$$\Sigma_P \coloneqq \{\alpha \in \mathbb{N}^n \mid \exists\, p \in P \colon 0 \leq \alpha_i \leq p_i \; \forall i \in \{1, 2, \ldots, n\}\}.$$

Ifall det är givet av sammanhangen vad P är skrivs trappan av P endast som Σ.

Anmärkning 2.38. *Låt $\alpha \notin \Sigma$. Notera att om $\beta \in \mathbb{N}^n$ uppfyller att $\beta_i \geq \alpha_i$ för alla $i \in \{1, 2, \ldots, n\}$ är $\beta \notin \Sigma$.*

Sats 2.39. *Låt I vara ett nolldimensionellt ideal. Då är $\Sigma = \{\alpha \mid x^\alpha \notin \operatorname{in} I\}$ en trappa.*

Bevis. Eftersom I är nolldimensionellt är antalet monom utanför initialidealet ändligt. Låt $P = \{\alpha \mid x^\alpha \notin \operatorname{in} I\}$ då är $\Sigma_P = \{\alpha \in \mathbb{N}^n \mid \exists\, p \in P \colon 0 \leq \alpha_i \leq p_i \ \forall i \in \{1, 2, \ldots, n\}\} = \{\alpha \mid x^\alpha \notin \operatorname{in} I\}$. Ty, om $x^\alpha \notin \operatorname{in} I$ är även $x^{\alpha - e_i} \notin \operatorname{in} I$ för alla $i \in \{1, 2, \ldots, n\}$ sådan att $\alpha_i \neq 0$. □

Definition 2.40 (Gränspunktsmängden av en trappa)**.** *Låt P vara en ändlig delmängd av $\mathbb{N}^n$ och Σ_P trappan av P. Definiera gränspunktsmängden av Σ_P som*

$$\partial\Sigma_P \coloneqq \begin{cases} \{\alpha \in \mathbb{N}^n \mid \exists e_i \colon \alpha - e_i \in \Sigma, \alpha \notin \Sigma\} \text{ om } P \neq \emptyset, \\ \{(0, 0, \ldots, 0) \in \mathbb{N}^n\} \text{ om } P = \emptyset. \end{cases}$$

Även här utelämnas index P om mängden förstås av sammanhanget.

Anmärkning 2.41. *Kom ihåg att e_i är vektorn i $\mathbb{N}^n$ där i:te koordinaten är ett och resten noll.*

Lemma 2.42. *För alla $\alpha \in \partial\Sigma$ och för alla $\beta \in \Sigma$ existerar ett $i \in \{1, 2, \ldots, n\}$ sådan att $\alpha_i > \beta_i$.*

Bevis. Om $\Sigma = \emptyset$ är satsen trivialt sann ty då existerar inget $\beta \in \Sigma$. Om $\Sigma \neq \emptyset$ antag att för något $\alpha \in \partial\Sigma$ och för något $\beta \in \Sigma$ är $\alpha_i \leq \beta_i$ för alla $i \in \{1, 2, \ldots, n\}$. Då är $\alpha \in \Sigma$ vilket motsäger att $\alpha \in \partial\Sigma$. □

Lemma 2.43. *För varje punkt $\beta \notin \Sigma$ existerar en punkt $c \in \mathbb{N}^n$ sådan att $\beta - c \notin \Sigma$ och $\beta - c - e_i \in \Sigma$ för alla i sådan att den i:te koordinaten av $\beta - c$ är nollskild.*

Bevis. Om $\Sigma = \emptyset$ och $\beta \notin \Sigma$ existerar $\beta \in \mathbb{N}^n$ och $\beta - \beta = 0$ varav $\beta - \beta - e_i \in \Sigma$ för alla i sådan att den i:te koordinaten av $\beta - \beta$ är nollskild, ty ingen koordinat av $\beta - \beta$ är nollskild.

Om $\Sigma \neq \emptyset$ är negationen av satsen omöjlig. Antag att för någon punkt $\beta \notin \Sigma$ existerar ingen punkt $p \in \mathbb{N}^n$ sådan att $\beta - c \notin \Sigma$ och $\beta - c - e_i \in \Sigma$ för alla i sådan att den i:te koordinaten av $\beta - c$ är nollskild. Eftersom $\beta \notin \Sigma$ och $0 \in \mathbb{N}^n$ måste antingen $\beta - 0 = \beta \in \Sigma$ eller så existerar ett $i_1 \in \{1, 2, \ldots, n\}$ sådan att $\beta - e_{i_1} \notin \Sigma$. Eftersom $\beta \notin \Sigma$ är $\beta - e_{i_1} \notin \Sigma$. Om $\beta - e_i \neq 0$ kan argumentet återupprepas varav det existerar ett $i_2 \in \{1, 2, \ldots, n\}$ sådan att $\beta - e_{i_1} - e_{i_2} \notin \Sigma$. Används argumentet $\beta_1 + \beta_2 + \ldots + \beta_n$ antal gånger fås att det för alla $j \in \{1, 2, \ldots, \beta_1 + \beta_2 + \ldots + \beta_n\}$ existerar ett $i_j \in \{1, 2, \ldots, n\}$ sådan att $0 = \beta - \sum_{j=1}^{\beta_1 + \beta_2 + \ldots + \beta_n} e_{i_j} \notin \Sigma$ varav $\Sigma = \emptyset$, vilket är en motsägelse. □

3 Resultat

Sats 3.1. *Låt P vara en ändlig uppsättning punkter från $\mathbb{N}^n$. Betrakta trappan*

$$\Sigma_P = \{\alpha \in \mathbb{N}^n \mid \exists\, p \in P \colon 0 \leq \alpha_i \leq p_i \ \forall i \in \{1, 2, \ldots, n\}\}.$$

Låt k vara en kropp sådan att $\Sigma_P \subseteq k$. För varje $\alpha \in \partial\Sigma$ konstruera, i $k[x_1, x_2, \ldots, x_n]$, polynomen

$$f_\alpha = f_1 f_2 \cdots f_n \text{ där } f_i = \begin{cases} (x_i - \alpha_i + 1)(x_i - \alpha_i + 2) \cdots x_i \text{ om } \alpha_i \neq 0, \\ 1 \text{ annars.} \end{cases}$$

Betrakta idealet $I = \langle f_\alpha \mid \alpha \in \partial\Sigma \rangle \subset k[x_1, x_2, \ldots, x_n]$. Det gäller att $I = \mathbf{I}(\Sigma)$ samt att $\{f_\alpha \mid \alpha \in \partial\Sigma\}$ utgör en universell Gröbnerbas av I.

Anmärkning 3.2. *Observera att polynomen i Grönerbasen av $\mathbf{I}(\Sigma)$ per konstruktion har en linjär faktorisering. Polynomen uppfyller till och med det starkare villkoret att de irreducibla komponenterna består endast av en variabel av grad* 1.

Att polynomen i Gröbnerbasen har linjär faktorisering är värt att uppmärksamma ty det ofta inte är fallet för Gröbnerbaser i allmänhet. Till exempel har inte Gröbnerbasen i Exempel 1.1 denna egenskap.

Lemma 3.3. *Låt $\alpha \in \partial\Sigma$ då är $LM(f_\alpha) = x^\alpha$ för alla monomordningar.*

Bevis av Lemma 3.3. För alla monomordingar är

$$\mathrm{LM}(f_\alpha) = \mathrm{LM}(f_1 f_2 \cdots f_n) = \mathrm{LM}(f_1)\mathrm{LM}(f_2) \cdots \mathrm{LM}(f_n) = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n},$$

vilket är definitionen av x^α. Att $\mathrm{LM}(f_i) = x_i^{\alpha_i}$ för alla $i \in \{1, 2, \ldots, n\}$ följer av Annmärkning 1.6. □

Lemma 3.4. *Monomet x^β ligger i $\langle LM(f_\alpha) \mid \alpha \in \partial\Sigma \rangle$ om och endast om $\beta \notin \Sigma$.*

Bevis av Lemma 3.4. Om x^β ligger i $\{\mathrm{LM}(f_\alpha) \mid \alpha \in \partial\Sigma\}$ existerar ett $\alpha \in \partial\Sigma$ sådan att $\mathrm{LM}(f_\alpha) = x^\beta$. Men $\mathrm{LM}(f_\alpha) = x^\alpha$ enligt Lemma 3.3. Alltså är $\beta = \alpha \in \partial\Sigma$, varav $\beta \notin \Sigma$. Om x^β inte ligger i $\{\mathrm{LM}(f_\alpha) \mid \alpha \in \partial\Sigma)\}$ men i $\langle \mathrm{LM}(f_\alpha) \mid \alpha \in \partial\Sigma) \rangle$ existerar ett $x^\alpha \in \{\mathrm{LM}(f_\alpha) \mid \alpha \in \partial\Sigma)\}$ sådan att $\beta_i \geq \alpha_i$ för alla $i \in \{1, 2, \ldots, n\}$, men $\alpha \notin \Sigma$ vilket implicerar att $\beta \notin \Sigma$ enligt Anmärkning 2.38.

Låt β vara en godtycklig punkt utanför Σ. Enligt Lemma 2.43 existerar en punkt $c \in \mathbb{N}^n$ sådan att $\beta - c \notin \Sigma$ men $\beta - c - e_i \in \Sigma$ för alla i sådan att den i:te koordinaten av $\beta - c$ är nollskild. Alltså ligger $\beta - c$ i $\partial\Sigma$ per definition av gränspunktsmängden av Σ, varav $x^{\beta - c} \in \langle \mathrm{LM}(f_\alpha) \mid \alpha \in \partial\Sigma \rangle$ och $x^\beta = x^{\beta - c} x^c \in \langle \mathrm{LM}(f_\alpha) \mid \alpha \in \partial\Sigma \rangle$. □

Bevis av Sats 3.1. Att $\Sigma \subseteq \mathbf{V}(I)$ följer av att för alla $\alpha \in \partial\Sigma$ och för alla $\beta \in \Sigma$ existerar ett $i \in \{1, 2, \ldots, n\}$ sådan att f_α innehåller faktorn $(x_i - \beta_i)$. Ty, enligt Lemma 2.42 gäller det att för alla $\alpha \in \partial\Sigma$ och för alla $\beta \in \Sigma$ existerar ett $i \in \{1, 2, \ldots, n\}$ sådan att $\alpha_i > \beta_i$, vilket innebär att

$$f_\alpha = f_1 f_2 \cdots f_n \text{ där } f_i = (x_i - \alpha_i + 1)(x_i - \alpha_i + 2) \cdots (x_i - \beta_i) \cdots x_i.$$

varav $f_\alpha(\beta) = 0$.

För att visa andra inklusionen, antag att $\alpha \notin \Sigma$ varav det återstår att visa att $\alpha \notin \mathbf{V}(I)$. Eftersom $\partial\Sigma \subseteq \mathbb{N}^n \setminus \Sigma$ är α antingen i $\partial\Sigma$ eller inte. Om $\alpha \in \partial\Sigma$ försvinner inte $f_\alpha \in I$ på punkten α ty ingen av de irreducibla komponenterna av f_α förvinner, vilket är ett måste i ett intigritetsområde för att polynomet ska evalueras till noll. Om α inte ligger i $\partial\Sigma$ existerar en punkt $c \in \mathbb{N}^n$ sådan att $\alpha - c$ ligger i $\partial\Sigma$ enligt Lemma 2.43. Av samma argument som tidigare försvinner inte polynomet $f_{\alpha-c}$ på $\alpha - c$ och i förlängningen ej heller på α ty $\alpha_i \geq (\alpha - c)_i$ för alla $i \in \{1, 2, \ldots, n\}$. Alltså är $\alpha \notin \mathbf{V}(I)$.

Antalet monom utanför $\operatorname{in} I$ är $|\Sigma|$ enligt Lemma 3.4. Notera att $\mathbf{I}(\Sigma)$ är nolldimensionellt enligt Sats 2.25. Observera att $\mathbf{V}(I) = \mathbf{V}(\mathbf{I}(\Sigma)) = \Sigma$ och att antalet monom utanför $\operatorname{in}\mathbf{I}(\Sigma)$ är $|\mathbf{V}(\mathbf{I}(\Sigma))| = |\Sigma|$ enligt Följdsats 2.27. Eftersom det är lika många monom utanför $\operatorname{in} I$ och $\operatorname{in}\mathbf{I}(\Sigma)$ samt att $\operatorname{in} I \subseteq \operatorname{in}\mathbf{I}(\Sigma)$ följer det att $\operatorname{in} I = \operatorname{in}\mathbf{I}(\Sigma)$. Idealet $\mathbf{I}(\Sigma)$ innehåller alla polynom i $k[x_1, x_2, \ldots, x_n]$ som försvinner på Σ varav $I \subseteq \mathbf{I}(\Sigma)$ och enligt Sats 2.12 följer att $I = \mathbf{I}(\Sigma)$.

Eftersom $\{f_\alpha \mid \alpha \in \partial\Sigma\} \subset I$ och antalet monom utanför initialidealet av I är lika med antalet monom utanför $\langle \operatorname{LM}(f_\alpha) \mid \alpha \in \partial\Sigma \rangle$, enligt Lemma 3.4, följer det att $\{f_\alpha \mid \alpha \in \partial\Sigma\}$ är en Gröbnerbas av I enligt Sats 2.11. Eftersom

$$\langle \operatorname{LM}(f_\alpha) \mid \alpha \in \partial\Sigma \rangle = \langle x^\alpha \mid \alpha \in \partial\Sigma \rangle$$

för alla monomordningar, enligt Lemma 3.3, är Gröbnerbasen universell. □

Anmärkning 3.5. *Den universiella Gröbnerbasen $\{f_\alpha \mid \alpha \in \partial\Sigma\}$ av $\mathbf{I}(\Sigma)$ är inte nödvändigtvis reducerad. Detta beror på att gränspunktsmängden av en trappa ofta är väldigt stor (ofta större än självaste trappan) varav onödiga generatorer kan komma att läggas till i konstruktionen av idealet.*

Följande exempel visar hur satsen fungerar i praktiken samt bekräftar Anmärkning 3.5.

Exempel 3.1. *Låt $P = \{(2, 1, 0), (1, 0, 2), (0, 2, 1)\} \subset \mathbb{Q}^3$. Då är*

$$\Sigma = \{(0,0,0),(0,0,1),(0,1,0),(1,0,0),(0,0,2),(0,1,1),(0,2,0),\\ (1,0,1),(1,1,0),(2,0,0),(0,2,1),(1,0,2),(2,1,0)\}$$

och

$$\partial\Sigma = \{(1,2,0),(1,1,1),(3,0,0),(2,0,1),(3,1,0),(2,2,0),(2,1,1),(0,1,2),\\ (0,0,3),(2,0,2),(1,1,2),(1,0,3),(0,3,0),(1,2,1),(0,3,1),(0,2,2)\}.$$

För varje punkt α *i* $\partial\Sigma$ *betrakta i* $\mathbb{Q}[x_1,x_2,x_3]$ *polynomen som ges av*

$$f_\alpha = f_1 f_2 \cdots f_n \text{ där } f_i = \begin{cases} (x_i - \alpha_i + 1)(x_i - \alpha_i + 2)\cdots x_i \text{ om } \alpha_i \neq 0, \\ 1 \text{ annars.} \end{cases}$$

De sex första polynomen är:

$$\begin{aligned} f_{(1,2,0)} &= x_1(x_2-1)x_2, \quad f_{(1,1,1)} = x_1x_2x_3, \\ f_{(3,0,0)} &= (x_1-2)(x_1-1)x_1, \quad f_{(2,0,1)} = (x_1-1)x_1x_3, \\ f_{(3,1,0)} &= (x_1-2)(x_1-1)x_1x_2, \quad f_{(2,2,0)} = (x_1-1)x_1(x_2-1)x_2. \end{aligned}$$

Från de sex ovan polynomen framgår att vissa är multipler av varandra:

$$f_{(3,0,0)} = f_{(3,1,0)}x_2 \text{ och } f_{(2,2,0)} = f_{(1,2,0)}(x_1-1).$$

Alltså innehåller $\{f_\alpha \mid \alpha \in \partial\Sigma\}$ *onödigt många generatorer av idealet* $\langle f_\alpha \mid \alpha \in \partial\Sigma\rangle$*. Tas multipler bort fås att*

$$\begin{aligned} \langle f_\alpha \mid \alpha \in \partial\Sigma\rangle &= \langle f_{(3,0,0)}, f_{(2,0,1)}, f_{(1,2,0)}, f_{(1,1,1)}, f_{(0,3,0)}, f_{(0,1,2)}, f_{(0,0,3)}\rangle \\ &= \langle (x_1-2)(x_1-1)x_1, (x_1-1)x_1x_3, x_1(x_2-1)x_2, x_1x_2x_3, \\ &\quad (x_2-2)(x_2-1)x_2, x_2(x_3-1)x_3, (x_3-2)(x_3-1)x_3\rangle. \end{aligned}$$

Genom att betrakta generatorena inses att $\mathbf{V}(\langle f_\alpha \mid \alpha \in \partial\Sigma\rangle) = \Sigma$*. Betrakta initialidealet av* $\mathbf{I}(\Sigma)$ *samt monomidealet* $\langle LM(f_\alpha) \mid \alpha \in \partial\Sigma\rangle$*. Det följer direkt att*

$$\langle LM(f_\alpha) \mid \alpha \in \partial\Sigma\rangle \subseteq \operatorname{in}\mathbf{I}(\Sigma),$$

ty $\mathbf{I}(\Sigma)$ *innehåller alla polynom som försvinner på* Σ*. Oavsett monomordning är*

$$\langle LM(f_\alpha) \mid \alpha \in \partial\Sigma\rangle = \langle x_1^3, x_1x_2^2, x_1x_2x_3, x_1^2x_3, x_2^3, x_2x_3^2, x_3^3\rangle$$

och monomen utanför idealet är:

$$1, x_3, x_2, x_1, x_3^2, x_2x_3, x_2^2, x_1x_3, x_1x_2, x_1^2, x_2^2x_3, x_1x_3^2, x_1^2x_2.$$

Den multivariata graden på monomen utanför motsvarar punkterna i Σ*:*

$$(0,0,0),(0,0,1),(0,1,0),(1,0,0),(0,0,2),(0,1,1),(0,2,0),$$
$$(1,0,1),(1,1,0),(2,0,0),(0,2,1),(1,0,2),(2,1,0).$$

Enligt Sats 2.26 är antalet monom utanför $\operatorname{in}\mathbf{I}(\Sigma)$ *lika många som antalet punkter i* $\mathbf{V}(\mathbf{I}(\Sigma))$ *vilket i sin tur är* $|\Sigma|$*. Men antalet monom utanför* $\langle x_1^3, x_1x_2^2, x_1x_2x_3, x_1^2x_3, x_2^3, x_2x_3^2, x_3^3\rangle$ *är också lika många som antalet monom utanför* $\operatorname{in}\mathbf{I}(\Sigma)$ *varav* $\langle x_1^3, x_1x_2^2, x_1x_2x_3, x_1^2x_3, x_2^3, x_2x_3^2, x_3^3\rangle = \operatorname{in}\mathbf{I}(\mathbf{\Sigma})$ *och*

$$\mathbf{I}(\Sigma) = \langle (x_1-2)(x_1-1)x_1, (x_1-1)x_1x_3, x_1(x_2-1)x_2, x_1x_2x_3,$$
$$(x_2-2)(x_2-1)x_2, x_2(x_3-1)x_3, (x_3-2)(x_3-1)x_3\rangle,$$

enligt Följdsats 2.12.

Sammanfattningsvis följer det att

$$\{(x_1-2)(x_1-1)x_1, (x_1-1)x_1x_3, x_1(x_2-1)x_2, x_1x_2x_3,$$
$$(x_2-2)(x_2-1)x_2, x_2(x_3-1)x_3, (x_3-2)(x_3-1)x_3\},$$

är en universell Gröbnerbas av $\mathbf{I}(\Sigma)$ *och monomen utanför* $\operatorname{in}\mathbf{I}(\Sigma)$ *är de med multivariat grad innanför* Σ*.*

Exempel 3.2. *Betraka Exempel 3.1 men låt polyonomen* f_α *tillhöra ringen* $\mathbb{Z}_3[x_1,x_2,x_3]$ *istället för* $\mathbb{Q}[x_1,x_2,x_3]$*. De ledande monomen av polynomen* f_α *kommer fortfarande vara* x^α *eftersom ledande koefficienten är* 1*. Alltså erhålls samma generatorer av initialidealet* $\langle LM(f_\alpha) \mid \alpha \in \partial\Sigma\rangle$ *varav det fortfarande är* $|\Sigma|$ *monom utanför. Eftersom* Σ *är en delmängd av* $\mathbb{Z}_3[x_1,x_2,x_3]$ *gäller fortfarande likheten* $\mathbf{V}(\langle f_\alpha \mid \alpha \in \partial\Sigma\rangle) = \Sigma$*. Notera att det är* $|\Sigma|$ *monom utanför* $\operatorname{in}\mathbf{I}(\Sigma)$*. Precis som i Exempel 3.1 följer att* $\langle LM(f_\alpha) \mid \alpha \in \partial\Sigma\rangle = \operatorname{in}\mathbf{I}(\mathbf{\Sigma})$ *samt att* $\{f_\alpha \mid \alpha \in \partial\Sigma\}$ *är en universell Gröbnerbas av* $\mathbf{I}(\Sigma) = \langle f_\alpha \mid \alpha \in \partial\Sigma\rangle$*. Monomen utanför* $\operatorname{in}\mathbf{I}(\Sigma)$ *är de med multivariat grad innanför* Σ*.*

Följdsats 3.6. *Låt* Σ *vara en trappa. Då är monomen utanför* $\operatorname{in}\mathbf{I}(\Sigma)$ *de med multivariatgrad i* Σ*.*

Bevis. Låt x^β vara ett monom utanför $\operatorname{in}\mathbf{I}(\Sigma) = \langle \mathrm{LM}(f_\alpha) \mid \alpha \in \partial\Sigma\rangle$. Enligt Lemma 3.4 är $\beta \in \Sigma$. Enligt Sats 2.26 finns $|\Sigma|$ monom utanför $\operatorname{in}\mathbf{I}(\Sigma)$. Alltså är monomen utanför $\operatorname{in}\mathbf{I}(\Sigma)$ de med multivariat grad i Σ. □

Följdsats 3.7. *Varje nolldimensionellt monomideal är initialideal av ett radikalideal som försvinner på punkterna som utgörs av multivariata graden på monomen utanför monomidealet. Mer specifikt: om* I *är ett nolldimensionellt monomideal och* $\Sigma = \{\alpha \mid x^\alpha \notin I\}$ *är* $\operatorname{in}\mathbf{I}(\Sigma) = I$*.*

Bevis. Observera att eftersom I är ett monomideal är $I = \operatorname{in} I$ och enligt Sats 2.39 är Σ en trappa. Enligt Sats 3.1 är $\{f_\alpha \mid \alpha \in \partial\Sigma\}$ en Gröbnerbas av $\mathbf{I}(\Sigma)$. Alltså är

$$\operatorname{in}\mathbf{I}(\Sigma) = \langle \mathrm{LM}(f_\alpha) \mid \alpha \in \partial\Sigma\rangle = \langle x^\alpha \mid \alpha \notin \Sigma\rangle = \langle x^\alpha \mid \alpha \notin \{\alpha \mid x^\alpha \notin I\}\rangle = I$$

eftersom I är ett monomideal. Att $\langle \mathrm{LM}(f_\alpha) \mid \alpha \in \partial\Sigma\rangle = \langle x^\alpha \mid \alpha \notin \Sigma\rangle$ följer av att monomen utanför $\langle x^\alpha \mid \alpha \notin \Sigma\rangle$ är precis de med multivariat grad i Σ, vilket även är fallet för $\langle \mathrm{LM}(f_\alpha) \mid \alpha \in \partial\Sigma\rangle$ enligt Följdsats 3.6. □

Följdsats 3.8. *Låt $\Sigma = \{\alpha_1, \alpha_2, \ldots, \alpha_s\}$ vara en trappa. Matrisen*

$$\left(\alpha_i^{\alpha_j}\right)_{i,j}$$

har full rang.

Bevis. Monomen utanför $\operatorname{in}\mathbf{I}(\Sigma)$ är $x^{\alpha_1}, x^{\alpha_2}, \ldots, x^{\alpha_s}$ enligt Följdsats 3.6. Enligt Sats 2.28 har matrisen

$$\left(x^{\alpha_j}(\alpha_i)\right)_{i,j} = \left(\alpha_i^{\alpha_j}\right)_{i,j}$$

full rang. □

Exempel 3.3. *Låt*

$$\Sigma = \{\{0,0,0\},\{0,1,0\},\{1,0,0\},\{1,1,0\},\{2,0,0\},\{2,1,0\}\}$$

vara en trappa i $\mathbb{N}^n$. Beteckna punkterna i Σ med $\alpha_1, \alpha_2, \ldots, \alpha_6$ på sådant sätt att monomen utanför $\mathbf{I}(\Sigma) \subset k[x_1, x_2, \ldots, x_n]$ är:

$$x^{\alpha_1} = 1, x^{\alpha_2} = x_2, x^{\alpha_3} = x_1, x^{\alpha_4} = x_1x_2, x^{\alpha_5} = x_1^2, x^{\alpha_6} = x_1^2x_2.$$

Då har matrisen $\left(x^{\alpha_j}(\alpha_i)\right)_{i,j} = \left(\alpha_i^{\alpha_j}\right)_{i,j}$ full rang enligt Följdsats 3.8 och ser ut som följer:

$$\begin{pmatrix}
0^00^00^0 & 0^00^10^0 & 0^10^00^0 & 0^10^10^0 & 0^20^00^0 & 0^20^10^0 \\
0^01^00^0 & 0^01^10^0 & 0^11^00^0 & 0^11^10^0 & 0^21^00^0 & 0^21^10^0 \\
1^00^00^0 & 1^00^10^0 & 1^10^00^0 & 1^10^10^0 & 1^20^00^0 & 1^20^10^0 \\
1^01^00^0 & 1^01^10^0 & 1^11^00^0 & 1^11^10^0 & 1^21^00^0 & 1^21^10^0 \\
2^00^00^0 & 2^00^10^0 & 2^10^00^0 & 2^10^10^0 & 2^20^00^0 & 2^20^10^0 \\
2^01^00^0 & 2^01^10^0 & 2^11^00^0 & 2^11^10^0 & 2^21^00^0 & 2^21^10^0
\end{pmatrix} =$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 2^1 & 0 & 2^2 & 0 \\ 1 & 1 & 2^1 & 2^1 & 2^2 & 2^2 \end{pmatrix}.$$

Vandermondematrisen, Definition 2.29, är känd för att ha full rang och en determinant som faktoriseras till

$$\prod_{1 \leq i < j \leq n} (x_j - x_i).$$

Resultatet av Följdsats 3.8 kan användas för ett alternativt bevis av att Vandermondematrisen är inverterarbar i specialfallet då $x_1, x_2, \ldots, x_n$ är distinkta element ur trappan $\{0, 1, \ldots, n-1\}$.

Följdsats 3.9. *Vandermondematrisen av storlek $n \times n$ där $a_1, a_2, \ldots, a_n$ är distinkta element ur trappan $\{0, 1, \ldots, n-1\}$ har full rang.*

Bevis. Betrakta trappan $\Sigma_n = \{0, 1, \ldots, n-1\}$ och beteckna punkterna i trappan med $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ sådan att monomen utanför $\operatorname{in}\mathbf{I}(\Sigma_n) \subset k[x]$ är $x^{\alpha_0} = 1, x^{\alpha_1} = x, \ldots, x^{\alpha_{n-1}} = x^{n-1}$. Då har matrisen

$$\left(x^{\alpha_j}(\alpha_i)\right)_{i,j} = \left(\alpha_i^{\alpha_j}\right)_{i,j} = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 1^1 & 1^2 & \cdots & 1^{n-1} \\ 1 & 2^1 & 2^2 & \cdots & 2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & (n-1)^1 & (n-1)^2 & \cdots & (n-1)^{n-1} \end{pmatrix}$$

full rang enligt Följdsats 3.8. □

Huvudfrågan från problemformuleringen i delkapitel 1.3 går nu att presentera som en sats med tillhörande bevis.

Sats 3.10. *Låt V vara en ändlig delmängd av k^n. Antag att mängden $\{\alpha \mid x^\alpha \notin \operatorname{in}\mathbf{I}(V)\}$ av alla exponenter till monom utanför initialidealet av $\mathbf{I}(V)$ ligger i k^n. Funktionen φ från ändliga delmängder av k^n till ändliga delmängder av k^n definierad av $\varphi : V \mapsto \{\alpha \mid x^\alpha \notin \operatorname{in}\mathbf{I}(V)\}$ uppfyller att*

$$\varphi^2(V) = \varphi(V) = \{\alpha \mid x^\alpha \notin \operatorname{in}\mathbf{I}(V)\}.$$

Bevis. Enligt Sats 2.25 är $\mathbf{I}(V)$ nolldimensionellt varav $\{\alpha \mid x^\alpha \notin \operatorname{in}\mathbf{I}(V)\}$ är en trappa enligt Sats 2.39. Beteckna trappan med Σ. Enligt Sats 3.1 är $\mathbf{I}(\Sigma) = \langle f_\alpha \mid \alpha \in \partial\Sigma\rangle$ där

$$f_\alpha = f_1 f_2 \cdots f_n \text{ och } f_i = \begin{cases} (x_i - \alpha_i + 1)(x_i - \alpha_i + 2)\cdots x_i \text{ om } \alpha_i \neq 0, \\ 1 \text{ annars,} \end{cases}$$

och $\{f_\alpha \mid \alpha \in \partial\Sigma\}$ utgör en universell Gröbnerbas av $\langle f_\alpha \mid \alpha \in \partial\Sigma\rangle$. Alltså är $\langle \operatorname{LM}(f_\alpha) \mid \alpha \in \partial\Sigma\rangle = \operatorname{in}\mathbf{I}(\Sigma)$. Observera att $|\Sigma| = |V|$ eftersom antalet monom utanför $\mathbf{I}(V)$ är $|V|$ enligt Följdsats 2.27, varav $\varphi(\Sigma) = \{\alpha \mid x^\alpha \notin \operatorname{in}\mathbf{I}(\Sigma)\}$ och

$$\varphi(\varphi(V)) = \varphi(\Sigma) = \{\alpha \mid x^\alpha \notin \operatorname{in}\mathbf{I}(\Sigma)\} = \{\alpha \mid x^\alpha \notin \langle \operatorname{LM}(f_\alpha) \mid \alpha \in \partial\Sigma\rangle\} = \Sigma$$

enligt Lemma 3.4.

□

Det är nu möjligt att fortsätta Exempel 1.1 från problemformulering.

Exempel 3.4. *Från Exempel 1.1 där*

$$V = \{(4,5,7,4,0), (4,3,4,1,3), (2,3,5,3,4)\} \subset \mathbb{Q}^5$$

erhölls att

$$\varphi(V) = \{(0,0,0,0,2), (0,0,0,0,1), (0,0,0,0,0)\}$$

och frågan ställdes vad som kan sägas om $\varphi(\varphi(V))$. Av Sats 3.10 besvaras även frågan vad som händer ifall φ skulle upprepas ytterligare. Eftersom $\varphi(V) \subset \mathbb{Q}^5$ fås att

$$\varphi^\alpha(V) = \varphi(V)\ \forall \alpha \in \mathbb{N} \setminus \{0\}$$

enligt återupprepad användning av Sats 3.10.

4 Slutsats och diskussion

Problemformuleringen besvaras av Sats 3.10 och är för matematiken ett nytt resultat. Nämligen att om funktionen φ som skickar ändliga delmängder $V \subset k^n$ till $\{\alpha \mid x^\alpha \notin \operatorname{in}\mathbf{I}(V)\}$ återupprepas gäller det att

$$\varphi^\alpha(V) = \varphi(V)\, \forall \alpha \in \mathbb{N} \setminus \{0\},$$

förutsatt att $\{\alpha \mid x^\alpha \notin \operatorname{in}\mathbf{I}(V)\} \subset k^n$.

En del andra resultat visas på vägen som till exempel Sats 3.1 där en universell Gröbnerbas av $\mathbf{I}(\Sigma)$, där Σ är en trappa, presenteras. I Följdsats 3.7 visas att varje nolldimensionellt monomideal I är initialidealet av det radikala idealet $\mathbf{I}(\Sigma)$, där Σ är trappan genererad av de multivariata graderna av monomen utanför I.

Polynomen i Gröbnerbaserna som konstrueras för $\mathbf{I}(\Sigma)$ i 3.1 har en linjär faktorisering vilket är ovanligt för Gröbnerbaser i allmänhet. Att Gröbnerbasen kan skapas utifrån en sluten formel är anmärkningsvärt och hör också till det ovanliga. Generellt är Gröbnerbaser inte heller universella.

4.1 Relaterade arbeten

Teo Mora uppmärksammade i sin artikel [7] Macaulays resultat från [8]. Enligt Mora hade Macaulay ett tillvängagångsätt att givet en graderad monomordning och ett nolldimensionellt monomideal J, konstruera ett nolldimensionellt ideal I sådan att $\operatorname{in} I = J$. Dessutom presenterade Mora en Gröbnerbas av I med hänvisningar till Macaulays arbete. De radikala idealen konstruerade i Sats 3.1 kan vara ett specialfall av idealen som Mora uppmärksammade beroende på hur artikeln [7] tolkas. Huruvida 3.7 är ett nytt resultat beror också på tolkningen av [7] och [8].

Mer matematiskt beskrev Mora i [7] Macaulays resultat från [8] som: givet graderad lexikografisk monomordning, låt $J = \langle m_1, m_2, \ldots, m_s\rangle$ vara ett nolldimensionellt monomideal av $k[x_1, x_2, \ldots, x_n]$ där $m_l = x_1^{e_{1l}} x_2^{e_{2l}} \cdots x_n^{e_{nl}}$. Eftersom J är nolldimsensionellt existerar för alla $i \in \{1, 2, \ldots, n\}$ ett naturligt tal d_i sådan att $x_i^{d_i} \in J$ och $e_{il} \leq d_i\, \forall l \in \{1, 2, \ldots, s\}$. För alla $i \in \{1, 2, \ldots, n\}$ och för varje $j \in \{1, 2, \ldots, d_i\}$ välj element $a_{ij} \in k$ sådan att för alla i är $a_{ij} \neq a_{ih}$ om $h \neq j$. För alla $l \in \{1, 2, \ldots, s\}$ konstruera polynomen

$$g_l \coloneqq \prod_{i=1}^{n} \prod_{j=0}^{e_{il}-1} (x_i - a_{ij}). \tag{2}$$

Enligt Moras tolkning i [7] av Macaulays resultat från [8] utgör $\{g_1, g_2, \ldots, g_s\}$ en Gröbnerbas av ett nolldimensionellt ideal I sådan att $\operatorname{in} I = J$. Observera

att kravet $a_{ij} \neq a_{ih}$ om $h \neq j$ garanterar att polynomen i Gröbnerbasen har linjär faktorisering. Vad Mora inte uppmärksammar i [7] är att Gröbnerbasen som presenteras är universell, ty

$$\mathrm{LM}(g_l) = \prod_{i=1}^{n} \mathrm{LM}(\prod_{j=0}^{e_{il}-1} (x_i - a_{ij})) = \prod_{i=1}^{n} x_i^{e_{il}}$$

för alla monomordningar enligt Anmärkning 1.6.

Det är oklart huruvida Mora vill att elementen a_{ij} från definitionen av g_l på rad (2) ska vara distinkta eller inte för alla i och j. I fallet då de inte behöver vara distinkta fås att idealen i Sats 3.1 är ett specialfall av de som Mora uppmärksammade. Ett bevis för att idealen i Sats 3.1 är ett specialfall då a_{ij}:na inte behöver vara distinkta ges omgående. Betrakta idealen $\mathbf{I}(\Sigma) = \langle f_\alpha \mid \alpha \in \partial\Sigma \rangle$ för en icke tom trappa Σ där

$$f_\alpha = f_1 f_2 \cdots f_n \text{ och } f_i = \begin{cases} (x_i - \alpha_i + 1)(x_i - \alpha_i + 2) \cdots x_i \text{ om } \alpha_i \neq 0, \\ 1 \text{ annars.} \end{cases}$$

Beteckna punkterna i $\partial\Sigma$ med $\{\alpha_1, \alpha_2, \ldots, \alpha_s\}$, där $s = |\partial\Sigma|$, och det nolldimensionella monom idealet in $\mathbf{I}(\Sigma) = \langle \mathrm{LM}(f_\alpha) \mid \alpha \in \partial\Sigma \rangle$ med

$$\langle \mathrm{LM}(f_{\alpha_1}), \mathrm{LM}(f_{\alpha_2}), \ldots, \mathrm{LM}(f_{\alpha_s}) \rangle$$

där $\mathrm{LM}(f_{\alpha_i}) \in \{\mathrm{LM}(f_\alpha) \mid \alpha \in \partial\Sigma\}$ för alla $i \in \{1, 2, \ldots, s\}$. Eftersom $\mathrm{LM}(f_{\alpha_l}) = x^{\alpha_l}$ för alla $l \in \{1, 2, \ldots, s\}$ enligt Lemma 3.3, är $e_{il} = \alpha_{li}$ den i:te koordinaten av α_l. Låt $a_{ij} = j$ då är $a_{ij} \neq a_{ih}$ om $h \neq j$ för alla $i \in \{1, 2, \ldots, n\}$ och a_{ij}:na är långt ifrån distinkta. Skapa, i enlighet med Moras artikel [7], polynomen

$$g_l \coloneqq \prod_{i=1}^{n} \prod_{j=0}^{e_{il}-1} (x_i - a_{ij}) = \prod_{i=1}^{n} \prod_{j=0}^{\alpha_{li}-1} (x_i - j)$$

för alla $l \in \{1, 2, \ldots, s\}$. Det följer att

$$\begin{aligned} f_{\alpha_l} &= f_1 f_2 \cdots f_n \text{ där } f_i = \begin{cases} (x_i - \alpha_{li} + 1)(x_i - \alpha_{li} + 2) \cdots x_i \text{ om } \alpha_{li} \neq 0, \\ 1 \text{ annars,} \end{cases} \\ &= \prod_{i=1}^{n} \prod_{j=0}^{\alpha_{li}-1} (x_i - j) = g_l \; \forall l \in \{1, 2, \ldots, s\}. \end{aligned}$$

Alltså är den universella Gröbnerbasen $\{f_\alpha \mid \alpha \in \partial\Sigma\}$ av $\mathbf{I}(\Sigma)$ för trappmängder Σ i sådant fall ett specialfall av de Gröbnerbaser presenterade av Moras i [7].

Om a_{ij}:na från rad (2) måste vara distinkta är idealen från Sats 3.1 i huvud sak - per konstruktion - inte specialfall av de som Mora uppmärksammade. Gröbnerbasen för idealen i Sats 3.1 innehåller alltid polynomen

$$(x_i - \max_{p \in \mathbf{V}(\mathbf{I}(\Sigma))}(p_i))(x_i - \max_{p \in \mathbf{V}(\mathbf{I}(\Sigma))}(p_i) + 1) \cdots (x_i + 0) \text{ eller polynomet } 1$$

för varje $i \in \{1, 2, \ldots, n\}$ eftersom $(\max\{(p_i) \mid p \in \mathbf{V}(\mathbf{I}(\Sigma))\} + 1) \cdot e_i$ alltid ligger i $\partial\Sigma$. Därav, om det existerar två punkter p och q i $\mathbf{V}(\mathbf{I}(\Sigma))$ sådana att p och q har varsin nollskild koordinat på skilda positioner, kommer a_{ij}:na inte kunna vara distinkta.

Det får inte förringas att uppmärksammandet av idealen i Sats 3.1 leder till det nya resultatet Sats 3.10. Med hjälp av de universella Gröbnerbaserna för idealen $\mathbf{I}(\Sigma)$, för trappor Σ, går det att besvara frågan från problemformuleringen, vilket är långt ifrån en självklar följd utifrån Gröbnerbaserna som Mora uppmärksammar i [7].

4.2 Förslag på fortsatt forskning

Eftersom Vandermonmatrisen har enkel sluten formel för dess determinant väcks frågan huruvida det finns någon liknande enkel faktorisering för matriserna i Följdsats 3.8. Samma fråga kan också ställas för matriserna som på motsvarande sätt kan skapas av den uppsättning Gröbnerbaser som Mora presenterar i sin artikel [7].

En annan frågeställning är om multiplikationsmatriserna, som presenteras i delkapitel 2.2.2, har särskilda egenskaper för polynomen i idealen $\mathbf{I}(\Sigma)$ där Σ är en trappa. Samma fråga kan ställas för multiplikationsmatriserna för polynomen i uppsättning Gröbnerbaser som Mora presenterar i artikel [7].

Referenser

[1] Cox DA, Little J, O'Shea D. Ideals, varieties, and algorithms - an introduction to computational algebra. 4 uppl. Cham: Springer; 2015

[2] B. Buchberger, Groebner Bases: An Algorithmic Method in Polynomial Ideal Theory, in Multidimensional Systems Theory, ed. by N.K. Bose (D. Reidel Publishing, Dordrecht, 1985), pp. 184–232

[3] Möller, H.M., Buchberger, B. (1982). The construction of multivariate polynomials with preassigned zeros. In: Calmet, J. (eds) Computer Algebra. EUROCAM 1982. Lecture Notes in Computer Science, vol 144. Springer, Berlin, Heidelberg. Hämtad från: `https://doi.org/10.1007/3-540-11607-9_3`

[4] Grayson, Daniel R. and Stillman, Michael E. Macaulay2, a software system for research in algebraic geometry. Hämtad från: `https://math.uiuc.edu/Macaulay2/`

[5] Becker, Eberhard & Marinari, Maria & Mora, Teo & Traverso, Carlo. (1996). The shape of the Shape Lemma

[6] R. Corless. Editor's Corner: Gröbner Bases and Matrix Eigenproblems: 4 december 1996

[7] T. Mora. De Nugis Groebnerialium 2: Applying Macaualay's Trick in order to easily write a Groebner basis, J. AAECC., 13 (2003) 437–446

[8] Macaulay FS. The theory of modular systems. sida 548. Hämtad från: `https://www.math.unl.edu/~bharbourne1/ReginaWorkshop/ReginaAccessOnly/MacAulay1927.pdf`

A Kod

Denna bilaga innehåller den Macaulay2 kod som skapats för att kunna svara på problemformulering.

```
-- Funktionen enpunktsideal tar en punkt p och en
-- polynomring R och ger idealet I(p).

enpunktsideal = (p,R) -> (I = ideal((gens R)#0 - p#0);
    IList = {}; IList = append(IList,I);
    for i from 1 to (length p-1) do (
        IList = append(IList,(gens R)#i - p#i));
    return ideal(IList))

-- Funktionen flerpunktsideal tar en uppsättning
-- punkter P och en polynomring R och ger idealet I(P).

flerpunktsideal = (P,R) -> (IList = {};
    for i from 0 to length P-1 do (
        IList = append(IList,enpunktsideal(P#i,R)));
    return intersect(IList));

-- Funktionen phi tar en uppsättning punkter P
-- och en polynomring R och ger mängden multivariata
-- grader av monomen utanför initialidealet av I(P).
-- Denna funktion phi är alltså samma som phi från
-- problemformuleringen.

phi = (P,R) -> (I = flerpunktsideal(P,R);
    punkter = {};
    normalMängd = flatten entries basis (R/I);
    for i from 0 to length normalMängd -1 do (
        punkter = append(punkter,
            flatten exponents normalMängd#i));
    return punkter);

-- Funktionen phiiterator tar en extra parameter n
-- och applicerar phi n gånger.

phiiterator = (p,R,n) -> (punkter = p;
    for i from 1 to n do punkter = phi(p,R);
    return punkter);

-- Funktionen enpunktstrappa
```

```
enpunktstrappa = (lista) -> (ut = {}; nylista = {};
    if length lista != 1 then (
        for i from 1 to length lista -1 do (
            nylista = append(nylista, lista#i)
        );
        if length nylista > 0 then (
            A = enpunktstrappa(nylista)) else (
            for j in 0..lista#0 do (
                ut = append(ut,{j})); return ut
            );
        for element in 0..lista#0 do (
            for tal in A do (
                tal = prepend(element, tal);
                ut = append(ut,tal)
                )
            )
        ) else (trappDel = {};
        for j in 0..lista#0 do (
            trappDel = append(trappDel,{j}));
        return trappDel);
    for element in ut do (
        if length element == length A#0 then (
            ut = delete(element,ut)));
    return ut
    );

-- Funktionen trappa tar en uppsättning punkter och
-- ger trappan som genereras av de punkterna.

trappa = (punkter) -> (trappListan = {};
    for p in punkter do (
        trappListan = join(trappListan,
            enpunktstrappa(p)));
     return unique trappListan);

-- Funktionen slumppunkter slumpar punkter
-- utifrån valda parametrar.

slumppunkter = (antalVariabler,
    antalpunkter,maxKoefficient) -> (punkter = {};
     for i from 1 to antalpunkter do
        (punkt = {}; for j from 1 to antalVariabler do
            (punkt = append(punkt,
```

```
                    random maxKoefficient));
        punkter = append(punkter, punkt));
    return unique punkter
    );

-- Funktionen slumptrappa slumpar trappmängder
-- utifrån valda parametrar.

slumptrappa = (antalVariabler,antalLedandeMonom,
    maxKoefficient) -> (
    return trappa(slumppunkter(antalVariabler,
            antalLedandeMonom,maxKoefficient))
    );

-- Fixera en monomordning och antalet punkter i V.
-- Som nämndes i delkapitel Metod erhålls då med
-- stor sannolikhet samma monom utanför idealet I(V),
-- för slumpade affina varieteter.
-- Detta kan ha att göra med The Shape Lemma.
-- Nedan ses att samma monom utanför I(V) erhålls
-- redan när koordinaterna i V begränsas till 100
-- för Glex ordningen.

antalPunkter = 5;
antalVariabler = 3;
monomOrdning = GLex;
maxKoefficient = 100;

R = QQ[x_1..x_antalVariabler,
    MonomialOrder => monomOrdning]

for i from 1 to 10 do (
    sigma = slumppunkter(antalVariabler,
        antalPunkter,maxKoefficient);
    print(flatten entries basis (
            R / flerpunktsideal(sigma,R)))
)

antalPunkter = 7;
monomOrdning = GLex;
maxKoefficient = 100;

for i from 1 to 10 do (
    sigma = slumppunkter(antalVariabler,
```

```
        antalPunkter,maxKoefficient);
    print(flatten entries basis (
            R / flerpunktsideal(sigma,R)))
)

-- Nedan ses att samma monom utanför I(V) erhålls
-- redan när koordinaterna i V begränsas till 2000
-- för Glex ordnignen.

antalPunkter = 5;
monomOrdning = Lex;
maxKoefficient = 2000;

R = QQ[x_1..x_antalVariabler,
    MonomialOrder => monomOrdning]

for i from 1 to 10 do (
    sigma = slumppunkter(antalVariabler,
        antalPunkter,maxKoefficient);
    print(flatten entries basis (
            R / flerpunktsideal(sigma,R)))
)

antalPunkter = 7;
monomOrdning = Lex;
R = QQ[x_1..x_antalVariabler,
    MonomialOrder => monomOrdning]

for i from 1 to 10 do (
    sigma = slumppunkter(antalVariabler,
        antalPunkter,maxKoefficient);
    print(flatten entries basis (
            R / flerpunktsideal(sigma,R)))
)


-- Funktion problemformuleringstest testar om
-- problemformuleringen håller för slumpade ändliga
-- affina varieteter.

problemformuleringstest = (antalExemple,
    antalVariabler,antalPunkter,
    maxKoefficient, monomOrdning) -> (
    for i from 0 to antalExemple-1 do (
```

```
        Sigma= slumppunkter(antalVariabler,
            antalPunkter,maxKoefficient);
    print (
        phiiterator(Sigma,R,2) == (
            phiiterator(Sigma,R,1)
            )
        )
    )
)

--Välj parametrar för att testa huruvida
--phi^2(Sigma)=phi^2(Sigma) där Sigma är en trappa.
--För varje exempel slumpas nya trappor

antalExempel = 5;
antalVariabler = 3;
antalPunkter = 2;
maxKoefficient = 100;
monomOrdning = GLex;

R = QQ[x_1..x_antalVariabler,
    MonomialOrder => monomOrdning]
problemformuleringstest(antalExempel,
    antalVariabler,antalPunkter,
    maxKoefficient, monomOrdning)


-- Funktion problemformuleringstestTrappa testar
-- huruvida problemformuleringen håller för slumpade
-- trappor utifrån valda parametrar.

problemformuleringstestTrappa = (antalExempel,
    antalVariabler,antalPunkter,
    maxKoefficient, monomOrdning) -> (
    for i from 0 to antalExempel-1 do
    (Sigma= slumptrappa(antalVariabler,
            antalPunkter,maxKoefficient);
    print (phiiterator(Sigma,R,2) == (
            phiiterator(Sigma,R,1)
            )
        )
    )
)
```

```
-- Tips: sätt låga värden på parametrarna ty
-- trappor blir snabbt väldigt stora.

maxKoefficient = 7;
problemformuleringstestTrappa(antalExempel,
    antalVariabler,antalPunkter,
    maxKoefficient, monomOrdning)

-- För att se hur en trappa ser ut
-- använd funktionen slumpTrappaPrint.
-- Tips: sätt låga värden på parametrarna.

slumptrappaPrint = (antalVariabler,
    antalVariabler,maxKoefficient) -> (
    P = slumppunkter(antalVariabler,
        antalVariabler, maxKoefficient);
    print P;
    return trappa(P))


maxKoefficient = 4;
slumptrappaPrint(antalVariabler,
    antalVariabler,maxKoefficient)


-- Funktion hittaMönsterTrappa användes för att
-- hitta mönster i generatorerna för I(Sigma),
-- för slumpade trappmängder Sigma.
-- hittaMönster slumpar en trappa Sigma
-- utifrån givna parametrar och returnerar
-- trappstegen (punkterna som genererar Sigma) samt
-- generatorerna till I(Sigma) i faktoriserad form.
-- Ett mönster börjar anas men är inte helt tydligt.

antalExempel = 3;
maxKoefficient = 7;

hittaMönsterTrappa = (antalExempel,
    antalVariabler,antalpunkter,
    maxKoefficient, monomOrdning) -> (
    for i from 0 to antalExempel-1 do (
        punkter = slumptrappaPrint(
            antalVariabler,antalpunkter,
            maxKoefficient);
```

```
        print (
            apply (
                (flatten entries (
                        gens flerpunktsideal(
                            punkter, R))),
                factor)
            )
    )
)

hittaMönsterTrappa(antalExempel,
    antalVariabler,antalPunkter,
    maxKoefficient, monomOrdning)

-- Eftersom trappan som genereras av punkterna
-- (6,3) och (3,3) är samma som trappan som
-- genereras av endast (6,3) inses att den kan vara
-- bra att rensa bort punkter som leder till dubbletter.
-- Detta görs med funktionen taBortOnödigaPunkter.

taBortOnödigaPunkter = (punkter,R) -> (
    dåligaPunkter = {}; for i in punkter do (
        for j in punkter do (
            if ((i != j) and ((R_i % R_j)==0)) then (
                dåligaPunkter = append(dåligaPunkter,R_j)
                )
            )
        );
    dåligaPunkter = unique(dåligaPunkter);
    for i in dåligaPunkter do (
        punkter=delete((exponents i)#0,punkter));
    return punkter
    )

-- Funktionen hittaMönsterTrappaEndastNödvändigaPunkter
-- fungerar på samma sätt som hittaMönsterTrappa
-- men rensar först punkter som leder till dubbletter.

hittaMönsterTrappaEndastNödvändigaPunkter = (antalExempel,
    antalVariabler,antalPunkter,
    maxKoefficient, monomOrdning,R) -> (
    for i from 0 to antalExempel-1 do (
        punkter = slumppunkter(antalVariabler,
            antalPunkter, maxKoefficient);
```

```
        nödvändigaPunkter = (
            taBortOnödigaPunkter(punkter, R));
        print nödvändigaPunkter;
        Sigma = trappa(nödvändigaPunkter);
        print (
            apply (
                (flatten entries (
                        gens flerpunktsideal(Sigma,R))),
                factor)
            )
    )
)

hittaMönsterTrappaEndastNödvändigaPunkter(antalExempel,
    antalVariabler,antalPunkter,
    maxKoefficient, monomOrdning,R)

-- Ett mönster är fortfarande inte helt tydligt.
-- Låt se om gränspunktsmängden för en
-- trappa Simga har tydligare koppling med
-- generatorerna till I(Sigma).

-- relavantaGränspunkter är en funktion som tar
-- fram gränspunktsmängden av trappan Sigma,
-- för att sedan ta bort de punkter i
-- gränspunktsmängden som är överflödiga för att
-- definiera I(Sigma). Den tar bort gränspunkter
-- som är större eller lika med en annan gränspunkt
-- i alla koordinater.

relvantaGränspunkter = (Sigma) -> (
    relevantaTrappsteg = {};
    for i in Sigma do (
        sanningsvärden = {};
        for n from 1 to length gens R do (
            sanningsvärden = append(sanningsvärden,
                false)
            );
        int = 0;
        for j in Sigma do (
            for k in gens R do (
                if (R_i*k == R_j) then (
                    sanningsvärden= replace(int,
                        true,sanningsvärden);
```

```
                    int = int + 1)
                else int = int + 1);
            int = 0
            );
        for l from 0 to length gens R - 1 do (
            if not sanningsvärden#l then (
                relevantaTrappsteg=append(
                    relevantaTrappsteg,
                    R_i*(gens R)#l))
            )
        );
    for i in relevantaTrappsteg do (
        for j in relevantaTrappsteg do (
            if (i % j == 0) and i != j then (
                relevantaTrappsteg = delete(i,
                    relevantaTrappsteg)
            )
        )
    );
    return relevantaTrappsteg)

-- För att kontrollera att dessa verkligen
-- är de relevanta punkterna jämförs de med
-- monomen utanför initialidealet av I(Sigma)
-- genom nedanstående två forloopar.

slumpPunkter = slumppunkter(antalVariabler,
    antalPunkter,maxKoefficient);
punkter = taBortOnödigaPunkter(slumpPunkter,R);
Sigma = trappa(punkter);

for i in sort flatten (
    entries gens flerpunktsideal(Sigma,R)
    ) do print (leadTerm(i))

for i in unique relvantaGränspunkter(Sigma) do print i

-- En koppling mellan dessa gränspunktsmängder
-- och Gröbnerbasen för I(Sigma) märks när
-- polynomen i Gröbnerbasen faktoriseras.

apply ((flatten entries gens flerpunktsideal(Sigma,R)),
    factor)
```

— *Exakt hur sambandet ser ut beskrivs i*
— *kapitel Resultat.*