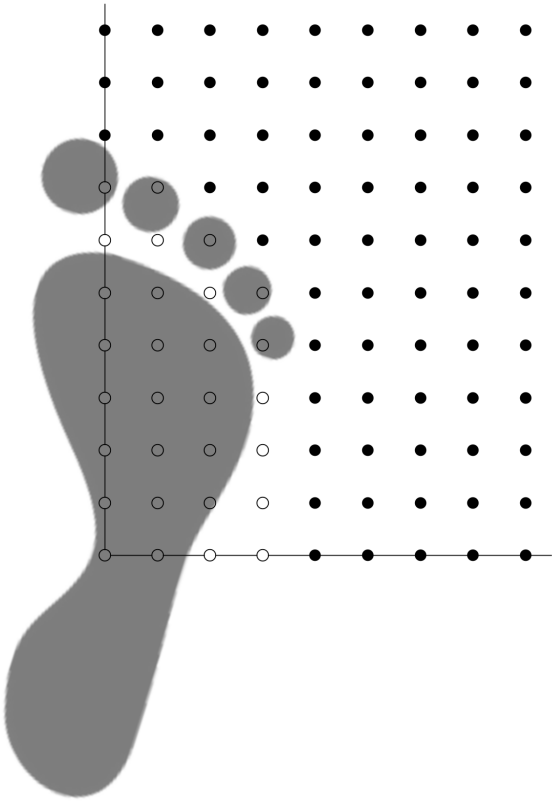
BODIL KRONGAARD KRISTENSEN

# GRÖBNERBASER
## OG EKSISTENS AF
# ORDENSFUNKTIONER

VEJLEDER: DIEGO RUANO



SPECIALEAFHANDLING I MATEMATIK

INSTITUT FOR MATEMATISKE FAG
AALBORG UNIVERSITET
JANUAR 2010

**Institut for Matematiske Fag**
Fredrik Bajers Vej 7G
9220 Aalborg Øst
Telefon 99 40 88 04
Fax 98 15 81 29
http://www.math.aau.dk

**Titel:**

Gröbnerbaser og eksistens af ordensfunktioner

**Projektperiode:**

MAT6 - efterårssemesteret 2009

**Skrevet af:**

Bodil Krongaard Kristensen

**Vejleder:**

Diego Ruano

**Oplagstal:** 7

**Antal sider:** 85

**Synopsis:**

Formålet med dette speciale er at forstå og forklare artiklen *On the existence of order functions* af Ruud Pellikaan, herunder Gröbnerbasisteori og evalueringskoder. Hovedresultatet er et bevis for eksistensen af ordensfunktioner. Dette medfører at der kan findes en grænse for minimumsafstanden og en dekodningsalgoritme.
For at bevise eksistensen af ordensfunktioner benyttes Gröbnerbaserteori. Dette inkluderer bl.a. Dicksons lemma, Hilberts basissætning, Buchbergers kriterium og Buchbergers algoritme. Derudover beskrives ordensfunktioner og ordensgrænsen i forbindelse med evalueringskoder. Algebraisk geometrikoder forklares kort, og til sidst vises hovedsætningen om eksistens af ordensfunktioner.
Som anvendelse og illustration af hovedresultateterne vil forskellige evalueringskoder også blive behandlet i projektet, bl.a. Reed Solomon og Reed Muller koder.

# English Summary

In coding theory one of the main goals is to develop good error-correcting codes for communication through noisy channels. The error-correcting codes are linear codes with the parameters $n, k, d$, where $n$ is the length, $k$ the dimension and $d$ the minimum distance of the code. By good codes we mean codes with good parameters, which is a high dimension, to make the communication fast, and a high minimum distance to correct more errors. Another important factor, is to have a fast decoding algorithm.

Some important codes are the Algebraic Geometry codes, which are codes with good parameters and decoding algorithms. But these results require the existence of an order function, which is difficult to prove with the algebraic geometry.

The objective of this thesis is to understand and explain article (Pellikaan, 2001) by Ruud Pellikaan. The main result in this article is a proof of the existence of order functions, which gives an order bound on the evaluation codes. Most of the article is based on algebraic geometry, but the main result are proved using Gröbner bases, and shows that it is much easier to check for an orderfunction, when using Gröbner bases.

Therefore an important part of this thesis will deal with Gröbner bases, which is also an interesting topic in its own right. Gröbner bases have many applications, both in coding theory and in other topics, and it is an important tool in working with ideals and polynomials.

In the first chapter of the thesis some basic concepts is introduced. Linear codes is described and then some basic algebra is defined, including rings, fields, ideals and the polynomial rings $\mathbb{F}[x_1, \ldots, x_n]$ and $\mathbb{F}[x_1, \ldots, x_n]/I$ which is used throughout the thesis. An affine variety is a geometric object, and it is shown that there is a connection between ideals and varieties. In fact it can be shown that a

variety $V$ is irreducible if and only if the ideal of the variety $I(V)$ is prime.

To show whether a polynomial is in an ideal or not, we need to do divisions, and therefore the division algorithm in $n$ variables is included. To use this algorithm, it is necessary to have an ordering on the monomials in $\mathbb{F}[x_1, \ldots, x_n]$, so the monomial ordering $<$ is defined, and lexicografic order, graded lexicografic order and weigted lexicografic order are examples of this. The division algorithm do not give a uniquely determined remainder, when the order of the division polynomials are changed, unless a Gröbner basis is used. A basis $\{g_1, \ldots, g_t\}$ is a Gröbner basis for an ideal $I$ if $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. Chapter 2 is devoted to the theory of Gröbner basis. This includes Dickson's lemma and The Hilbert basis theorem, that every ideal has a finite generating set. It will also be shown that every ideal has a Gröbner basis, and then Buchbergers algorithm can be used to construct such a basis.

Chapter 3 is about the evaluation codes and some results concerning this topic. First the quotientring $\mathbb{F}[x_1, \ldots, x_n]/I$ is described and we define the footprint $\Delta(I) = \{\mathbf{x}^\alpha \mid \mathbf{x}^\alpha \notin \langle \text{LT}(I) \rangle\}$, which gives a basis of $\mathbb{F}[x_1, \ldots, x_n]/I$. We show that the number of points in $V(I)$ is at most the dimension of $\mathbb{F}[x_1, \ldots, x_n]/I$, which is the number of monomials in $\Delta(I)$. This gives information on the length of an evaluation codes.

To prove the order bound for evaluation codes, we use the concept of an order function $\rho$, that satisfy five conditions. This gives a basis of $R$ that is a well-behaving sequence. With the concepts of syndromes and the order function it is possible to show the order bound for evaluation codes.

The end result is the existence of an order function on $R$, which is proved for $R = \mathbb{F}[x_1, \ldots, x_n]/I$, when the following is satisfied: (1) That every monomial in the footprint has mutually different weighted degree, and (2) that every polynomial in the Gröbner basis has exactly two monomoials of highest weighted degree. When these properties are satisfied, we now know that there is an order function, which gives us the order bound and the Majority Voting Decoding algorithm for free.

# Forord

Dette er et speciale indenfor hovedretningen Diskret Matematik ved Institut for Matematiske Fag, Aalborg Universitet. Specialet er udarbejdet i perioden 1.sep.2009 - 11.jan.2010. Målet med specialet er at forstå og forklare artikel (Pellikaan, 2001) og herunder at forstå og forklare Gröbnerbasisteori og evalueringskoder. Der forudsættes et basalt kendskab til abstrakt algebra, lineær algebra og kodningsteori.

I rapporten er vektorer noteret med fed, som $\mathbf{x}$. Vigtige begreber står i kursiv første gang de nævnes og/eller når de defineres. Litteraturhenvisninger angives som (Forfatter(e), udgivelsesår, evt. placering i kilden) og litteraturliste findes bagerst i rapporten. I starten af hvert afsnit anføres hvilke kilder afsnittet er baseret på. Ved nogle sætninger er beviset udeladt. Her vil i stedet være henvisninger til kilder, hvor et bevis kan findes. Henvisninger i parentes som (1.2) henviser til et ligningsnummer, mens sætninger mv. henvises til vha. "Sætning 1.2".

Til nogle eksempler er brugt programmet Singular. For mere information om programmet henvises til http://www.singular.uni-kl.de. I nogle af eksemplerne vil Singular-koden være inkluderet.

Til slut vil jeg gerne takke min vejleder Diego Ruano for et stort engagement og faglig vejledning gennem hele processen. Jeg vil også gerne takke min forlovede Jonas for stor tålmodighed og støtte.

Bodil Krongaard Kristensen
Aalborg den 11/1 2010

# INDHOLD

# Indledning

Kodningsteori er et af de nyere forskningsområder inden for matematikken, og mange væsentlige resultater er opnået inden for det seneste årti. I dette speciale vil jeg beskæftige mig med *Gröbnerbaser*, som er et nyere forskningsfelt med anvendelser inden for mange forskellige områder. Mit hovedfokus vil være på deres anvendelser inden for kodningsteorien, med udgangspunkt i G.R.Pellikaans resultater i (Pellikaan, 2001).

Kodningsteori handler bl.a. om kommunikation over støjfyldte kanaler, hvor udfordringen er at kunne kode informationen, sådan at eventuelle fejl der sker mellem afsender og modtager kan rettes. Dette illustreres med følgende model, hvor en meddelelse afsendes som en vektor, hvorefter den kodes og sendes gennem en støjfyldt kanal, inden den dekodes og når frem til modtageren. Igennem kanalen kan der være opstået fejl på vektoren, og målet med dekodningen er nu, ud fra den modtagne vektor, at rekonstruere den afsendte meddelelse.


For at vurdere om en kode er god, er der flere parametre man kan se på. En *lineær kode* defineres ud fra dens længde $n$, dimension $k$ og *minimumsafstanden* $d$. Længden af en kode er længden af kodeordene, mens dimensionen svarer til længden af den meddelelse der bliver kodet. Dimensionen bestemmer antallet af kodeord i koden.

For at opnå en effektiv kommunikation over kanalen ønsker vi at kunne sende så meget information som muligt på mindst mulig plads. Dette kræver at dimen-

sionen af koden er så stor som muligt, dvs. jo større dimension, jo bedre kode. Når der sendes over støjfyldte kanaler, er der, udover en hurtig kommunikation, også et ønske om at kunne rette mange fejl. Minimumsafstanden for en kode er den korteste afstand mellem to ord i koden og det kan vises, at antallet af fejl, som en kode kan rette, afhænger af minimumsafstanden. Jo større minimumsafstand, jo flere fejl kan koden rette. Opgaven er derfor at finde koder, som både har en høj dimension og en stor minimumsafstand. Det kan dog være svært at finde koder, hvor begge parametre er gode, og derudover kan det være svært at udregne minimumsafstanden for en kode. Derfor findes i stedet øvre og nedre grænser for minimumsafstanden, hvorefter det kan vises at forskellige familier af koder opfylder nogle af grænserne.

Når meddelelsen ender hos modtageren skal den dekodes igen for at få den oprindelige meddelelse. Så et andet vigtigt aspekt for en god kode er, om der findes en god, dvs. hurtig, *dekodningsalgoritme*. Dette kan dog være mindst lige så svært at finde som selve koderne, og det er derfor også et vigtigt forskningsområde.

En bestemt type koder er *algebraisk geometrikoder (AG-koder)*. Denne type koder er vigtige fordi de har meget gode parametre. Det er vist at man kan konstruere koder som opfylder Tsfasman-Vladut-Zink grænsen (se fx. (Høholdt et al., 1998, thm 2.81)) som i visse tilfælde er bedre end Gilbert-Varshamov grænsen. Derudover findes der også gode dekodningsalgoritmer for nogle af AG-koderne, kaldet one-point codes, hvilket gør dem særligt interessante. Teorien bag den algebraiske geometri er dog rimelig avanceret og derfor er den nok mere forskningsmæssig interessant, end den er praktisk anvendelig. Da det har vist sig at Gröbnerbasisteori giver en meget simplere og smartere tilgang til emnet, så vil jeg i dette speciale kun kort introducere algebraisk geometri.

En særlig form for AG-koder er dog mere anvendelige, nemlig *one-point codes*, som svarer til *evalueringskoder*. Disse koder har flere fordele. De er lette at arbejde med, der er en grænse for minimumsafstanden, *ordensgrænsen*, og der er gode dekodningsalgoritmer, herunder majority voting-algoritmen. Blandt evalueringskoderne findes også mange velkendte familier af koder, som f.eks. *Reed Solomon-koder*, der anvendes bl.a. i cd-afspillere.

Alle de gode resultater kræver dog at der eksisterer en *ordensfunktion* på området, som vist i bl.a. (Høholdt et al., 1998). Til at vise dette benyttes Gröbnerbaser, som en stor del af specialet handler om. Udover deres betydning for ordensfunktioner, er Gröbnerbaser også interessante i sig selv, da de kan anvendes inden for mange andre dele af kodningsteorien og andre områder, som f.eks. løsning af polynomiumsligninger. Derfor vil jeg i specialet gå i dybden med Gröbnerbasisteorien og også nå omkring flere emner, end hvad der er nødvendigt for at forstå resultaterne omkring eksistens af ordensfunktioner.

Udover at behandle Gröbnerbasisteori er formålet med specialet at forstå og forklare artiklen (Pellikaan, 2001). Hovedresultatet i artiklen er et bevis for eksistensen af ordensfunktioner for bestemte polynomiumsringe. Starten af artiklen bygger på algebraisk geometri, men pointen er blandt andet at vise, at dette emne

er meget simplere at arbejde med, når der i stedet benyttes Gröbnerbaser. Herved bliver flere sætninger meget lettere at bevise, og artiklens hovedresultat er vist ved hjælp af Gröbnerbaser.

Som anvendelse og illustration af hovedresultateterne vil forskellige evalueringskoder også blive behandlet i projektet. Eksistensen af en ordensfunktion har nemlig nogle interessante anvendelser i forbindelse med evalueringskoder. Det gør det bl.a. muligt at bestemme en grænse for minimumsafstanden for koderne og giver mulighed for nogle gode dekodningsalgoritmer. Hovedresultatet fra (Pellikaan, 2001) medfører, at givet en polynomiumsalgebra $R$, så er det nok at udregne en Gröbnerbasis og tjekke de to betingelser i sætningen. Derved opnås eksistensen af en ordensfunktion på $R$, hvilket uden videre arbejde giver os både ordensgrænsen for minimumsafstanden og en dekodningsalgoritme, kaldet Majority Voting Decoding Algorithm.

Specialet er opbygget sådan at det første kapitel omhandler det mest grundlæggende teori, hvor lineære koder beskrives, sammen med de vigtigste begreber fra algebraen, som polynomiumsringe, idealer og varieteter.

Kapitel to handler om Gröbnerbaser, hvor Dicksons lemma og Hilberts basissætning vises, hvorefter Gröbnerbaser introduceres, efterfulgt af Buchbergers kriterium og Buchbergers algoritme, der benyttes til at finde en Gröbnerbasis.

Det tredje kapitel handler om ordensfunktioner og deres anvendelse i forbindelse med evalueringskoder. Først defineres en ordensfunktion og derefter beskrives evalueringskoder og ordensgrænsen for evalueringskoder vises vha. ordensfunktioner. Algebraisk geometrikoder forklares kort, og sidst i kapitlet vises hovedsætningen om eksistens af ordensfunktioner.

KAPITEL

# 1

# Grundlæggende teori

## 1.1 Lineære koder

Dette afsnit er skrevet på baggrund af (Justesen og Høholdt, 2004, Afsnit 1.1-1.2) og (Huffman og Pless, 2003, Afsnit 1.2-1.4) og afsnittet vil indeholde en kort introduktion til lineære koder.

Lad $\mathbb{F}_q$ være et endeligt legeme. En kode $\mathcal{C}$ over $\mathbb{F}_q$ er en delmængde af $\mathbb{F}_q^n$. Vektorerne i $\mathcal{C}$ kaldes kodeord og har alle længden $n$. I dette projekt arbejdes udelukkende med lineære koder, som defineres på følgende måde:

**Definition 1.1.** Koden $\mathcal{C}$ kaldes en lineær $(n, k)$-kode, hvis den er et $k$-dimensionelt underrum af $\mathbb{F}_q^n$. □

Antallet af ord i koden er alle linearkombinationer, der kan skabes ud fra en basis. Da $\dim \mathcal{C} = k$ og $\mathcal{C}$ er et underrum, kan der altså vælges en basis $\mathbf{g}_1, \mathbf{g}_2, \ldots, \mathbf{g}_k$, så alle kodeord kan skrives på formen $\lambda_1\mathbf{g}_1 + \lambda_2\mathbf{g}_2 + \cdots + \lambda_k\mathbf{g}_k$, hvor $\lambda_1, \ldots, \lambda_k \in \mathbb{F}_q$. Da der er $q$ elementer i $\mathbb{F}_q$, bliver antallet af ord i koden derved $|\mathcal{C}| = q^k$.

En lineær kode er ofte givet ved en *generatormatrix*, som er en $k \times n$ matrix $G$, hvis rækkevektorer danner en basis for $\mathcal{C}$. Når en besked kodes, så sker det ved at beskeden, i form af en vektor $\mathbf{u}$ af længde $k$, multipliceres med generatormatricen $G$, hvilket giver kodeordet $\mathbf{c} = \mathbf{u}G$.

**Eksempel 1.2.** Et oplagt eksempel til at illustrere idéen med de lineære koder

er en (7,4)-Hammingkode. En generatormatrix for (7,4)-koden kan skrives

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Rækkerne i $G$ er basis for koden, og i alt er der, når vi bruger binære koder, $2^4 = 16$ forskellige kodeord af længden 7.

For at kode vektoren $\mathbf{u} = (u_1, u_2, u_3, u_4)$ ganges den på $G$ fra venstre:

$$\begin{aligned} \mathbf{u} \mapsto \mathbf{u}G =& (u_1, u_2, u_3, u_4) \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \\ =& (u_1, u_2, u_3, u_4, u_2 + u_3 + u_4, u_1 + u_3 + u_4, u_1 + u_2 + u_4). \end{aligned}$$ □

Da $\mathcal{C}$ er et underrum til et vektorrum, så har $\mathcal{C}$ også et nulrum med dimensionen $\dim \ker \mathcal{C} = n - k$. Dette nulrum er i sig selv et underrum af $\mathbb{F}_q^n$ og benyttes til at danne en *paritetscheckmatrix* $H$, som er en $(n-k) \times n$ matrix. Dette giver en ny definition på koden $\mathcal{C}$ :

$$\mathcal{C} = \{\mathbf{x} \in \mathbb{F}_q^n \mid H\mathbf{x}^T = 0.\}$$

Da rækkerne i $H$ er lineært uafhængige, så er $H$ en generatormatrix for en $(n, n-k)$ kode, som benævnes $\mathcal{C}^\perp$:

$$\mathcal{C}^\perp = \{\mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{x} \cdot \mathbf{c} = 0 \, \forall \, \mathbf{c} \in \mathcal{C}\}.$$

### 1.1.1 Vægt og afstand

En vigtig egenskab for en kode er minimumsafstanden mellem kodeord.

**Definition 1.3.** *Hammingafstanden* $d(\mathbf{x}, \mathbf{y})$ mellem to kodeord $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n$ er lig med antallet af koordinater, hvor $\mathbf{x}$ og $\mathbf{y}$ er forskellige. □

*Minimumsafstanden* $\mathrm{d}(\mathcal{C})$ for en kode $\mathcal{C}$ er den mindste afstand mellem to kodeord i koden, og dette er en vigtig egenskab i forbindelse med fejlretning. Det kan vises, at jo større minimumsafstand, jo flere fejl kan koden rette. Derfor ønskes altid den størst mulige minimumsafstand for en kode. Hammingvægten $w(\mathbf{x})$ for et $\mathbf{x} \in \mathbb{F}_q^n$ er antallet af koordinater forskellig fra nul, og det kan vises, at $d(\mathbf{x}, \mathbf{y}) = w(\mathbf{x} - \mathbf{y})$. Dermed er minimumsafstanden det samme som minimumsvægten for en kode.

En kode $\mathcal{C}$ kaldes *t-fejlkorrigerende*, hvis den altid kan rette mindst $t$ fejl. Det kan vises, at en kode $\mathcal{C}$ er $t$-fejlkorrigerende hvis og kun hvis $t < \frac{d}{2}$, hvor $d$ er minimumsafstanden for $\mathcal{C}$.

Når en kodet besked sendes over en støjfyldt kanal, kan eventuelle fejl ses som en tilføjelse af en fejlvektor $\mathbf{e}$ til kodeordet $\mathbf{c}$. Dette resulterer i en modtaget vektor $\mathbf{r} = \mathbf{c} + \mathbf{e}$. Når fejlretningen udføres kan man benytte *syndromdekodning*, hvor syndromet $\mathbf{s}$ udregnes som $\mathbf{s} = H\mathbf{r}^T$. Dette betyder at

$$\mathbf{s} = H\mathbf{r}^T = H(\mathbf{c} + \mathbf{e})^T = H\mathbf{e}^T,$$

så hvis der ingen fejl er sket og $\mathbf{e} = 0$, så er $s = 0$.

## 1.2 Algebra og polynomier

I dette afsnit behandles den grundlæggende algebra, som benyttes i resten af specialet. Jeg vil herunder definere ringe, legemer, idealer og polynomiumsringe.

### 1.2.1 Ringe, legemer og integritetsområder

Dette afsnit er skrevet på baggrund af (Greuel og Pfister, 2002, kap. 1), (Lauritzen, 2003, kap. 3) og (Huffman og Pless, 2003, kap. 3). Først defineres hvad man forstår ved en ring.

**Definition 1.4.** En ring $(A, +, \cdot)$ er en mængde $A$ med operationerne addition: $A \times A \to A$, $(a, b) \mapsto a + b$ og multiplikation: $A \times A \to A$, $(a, b) \mapsto a \cdot b = ab$, hvorom der gælder følgende:

- addition og multiplikation er associativ, dvs. $(a + b) + c = a + (b + c)$ og $(ab)c = a(bc)$, for alle $a, b, c \in A$
- addition er kommutativ, dvs. $a + b = b + a$, for alle $a, b \in A$
- den distributive lov gælder, dvs. $a(b + c) = ab + ac$, for alle $a, b, c \in A$
- der eksisterer et neutralt element mht. addition, $0 \in A$, og et neutralt element mht. multiplikation, $1 \in A$
- for alle $a \in A$ findes der et inverst element mht addition, $-a \in A$.

En ring $A$ kaldes kommutativ, hvis der endvidere gælder, at $ab = ba$, for alle $a, b \in A$. □

Nogle ringe har særlige egenskaber, som vil vise sig nyttige, nemlig legemer og integritetsområder. De vil blive beskrevet her, sammen med definitioner af inverse elementer og nuldivisorer.

**Definition 1.5.** Et element $a \in A$ har et inverst element mht multiplikation, hvis der findes et $b \in A$ så $ab = 1$. Da er $b = a^{-1}$. Lad $A^*$ være mængden af elementer i $A$, som har et inverst element mht. multiplikation. Et element $a \in A\backslash\{0\}$ kaldes for en nuldivisor, hvis der eksisterer et $b \in A\backslash\{0\}$, så $ab = 0$ eller $ba = 0$. På baggrund af dette defineres følgende:

- En ring $A$ er et *legeme*, hvis alle ikke-nul elementer i $A$ har et inverst element mht. multiplikation, altså hvis $A^* = A\backslash\{0\}$.
- En ring $A \neq \{0\}$ uden nuldivisorer kaldes et *integritetsområde*. □

Nogle almindelige eksempler på legemer er de rationelle tal $\mathbb{Q}$, de reelle tal $\mathbb{R}$ og de komplekse tal $\mathbb{C}$, som alle har inverse til alle deres elementer. Mængden af hele tal $\mathbb{Z}$ er en ring, men ikke et legeme, da $\mathbb{Z}^* = \{-1, 1\}$.

Et legeme kaldes endeligt når det består af et endeligt antal elementer. Antallet af elementer i $F$ kaldes ordenen af $\mathbb{F}$, og hvis $F$ har orden $q$, skrives det som $\mathbb{F}_q$. Hvis $p$ er et primtal, så er $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et endeligt legeme, da alle elementer har en invers. Dette er ikke sandt når $p$ ikke er et primtal.

**Eksempel 1.6.** Se på mængden $\mathbb{Z}/4\mathbb{Z}$. Så er både 1 og 3 deres egen inverse, da $1 \cdot 1 \equiv 1 \pmod 4$ og $3 \cdot 3 \equiv 9 \equiv 1 \pmod 4$. Derimod har 2 ingen invers, da $2 \cdot 1 \equiv 2 \pmod 4$, $2 \cdot 2 \equiv 0 \pmod 4$ og $2 \cdot 3 \equiv 6 \equiv 2 \pmod 4$. Altså er $\mathbb{Z}/4\mathbb{Z}$ ikke noget legeme. □

*Karakteristikken* af et endeligt legeme er det tal $p$, så $1 + 1 + \cdots + 1$ $p$ gange er lig med nul. Karakteristikken er altid et primtal. En mængde af $p$ forskellige elementer $\{0, 1, \ldots, p-1\}$ i $\mathbb{F}_q$ er isomorf med $F_p$, dvs. at et endeligt legeme med $p$ elementer altid kan betragtes som mængden $\mathbb{Z}/p\mathbb{Z}$. På samme måde er alle legemer med $q$ elementer isomorf med $\mathbb{F}_q$. Legemet $\mathbb{F}_q$ indeholder altså $\mathbb{F}_p$ som dellegeme, dvs. $\mathbb{F}_q$ er et vektorrum over $\mathbb{F}_p$ af dimension $m$, hvor $q = p^m$.

I resten af rapporten benyttes hovedsageligt det endelige legeme $\mathbb{F}_q$, hvor $q = p^m$ er en primtalspotens. Senere i rapporten vil det blive vist, hvordan et sådant legeme kan konstrueres. Dette kræver dog først et indblik i polynomiumsringe og idealer.

### 1.2.2 Idealer

Dette afsnit er skrevet med udgangspunkt i (Greuel og Pfister, 2002) og (Lauritzen, 2003). Afsnittet indledes med en generel definition af idealer, hvorefter følger afsnit om kvotientringe og idealer i polynomiumsringe.

**Definition 1.7.** Lad $A$ være en kommutativ ring. Så er $I \subseteq A$ et *ideal*, hvis følgende gælder

1. $0 \in I$
2. $a + b \in I$ når $a, b \in I$
3. for ethvert $\lambda \in A$ og $a \in I$, så er $\lambda a \in I$ □

Et ideal $I$ har en generatormængde, så hvis $a \in A$, så er

$$I = \langle a \rangle = \{\lambda a \mid \lambda \in A\}$$

et ideal, genereret af $a$. En generatormængde kan også bestå af flere elementer

$$\langle r_1, \ldots, r_n \rangle = \{\lambda_1 r_1 + \cdots + \lambda_n r_n \mid \lambda_1, \ldots, \lambda_n \in A.\} \tag{1.1}$$

Idealet i (1.1) er endeligt genereret, da generatormængden består af endeligt mange elementer. Et ideal kan også være genereret af en uendelig mængde på følgende måde, hvor $M \subseteq A$

$$\langle r \mid r \in M \rangle = \{a_1 r_1 + \cdots + a_n r_n \mid n \in N,\, a_1, \ldots, a_n \in A,\, r_1, \ldots, r_n \in M.\}$$

Et ideal, som kun er genereret af ét element kaldes et *hovedideal*. Der gælder, at $I = A \Leftrightarrow I = \langle 1 \rangle$, da $\langle 1 \rangle = \{a \cdot 1 \mid a \in A\} = A$.

### 1.2.3 Kvotientringe

Dette afsnit er skrevet med udgangspunkt i (Lauritzen, 2003). Lad $I$ være et ideal i $A$, $I \subseteq A$. Så er $A/I = \{[x] \mid x \in A\}$ en mængde bestående af sideklasserne $[x] = x + I$, hvorom der gælder, at $[x] = [y] \Leftrightarrow x - y \in I$. Det kan vises, at $A/I$ er en ring, hvor addition og multiplikation defineres til

$$[x] + [y] = [x + y] \text{ og } [x][y] = [xy].$$

Ringen $A/I$ kaldes en *kvotientring* og har som neutrale elementer [0] og [1]. Der gælder, at

$$[x] = 0 \Leftrightarrow x \in I.$$

Ofte arbejder man ikke kun med ringe, men med afbildninger mellem ringe. En ringhomomorfi er en særlig afbildning.

**Definition 1.8.** En *ringhomomorfi* er en afbildning $\varphi : A \to B$ mellem to ringe, som opfylder

$$\varphi(a + b) = \varphi(a) + \varphi(b) \text{ og } \varphi(ab) = \varphi(a)\varphi(b) \tag{1.2}$$

for $a, b \in A$ og

$$\varphi(1) = 1. \tag{1.3}$$

$B$ kaldes da en $A$-algebra.

Hvis der gælder (1.2) og at $\varphi$ er en bijektion, så kaldes afbildningen for en ringisomorfi. To ringe $A$ og $B$ er isomorfe, hvis der er en isomorfi i mellem dem, $\varphi : A \to B$. Dette skrives $A \simeq B$. □

I dette speciale benyttes kun ringhomomorfier mellem ringe hvor $A \subset B$ nemlig fra et legeme $\mathbb{F}$ ind i ringen $R = \mathbb{F}[x_1, \ldots, x_n]$ eller $R = \mathbb{F}[x_1, \ldots, x_n]/I$, hvor $\mathbb{F}$ er en delring af $R$. De to krav 1.2 og 1.3 gælder da stadig og $R$ kaldes en $\mathbb{F}$-algebra.

### 1.2.4 Polynomiumsringe

Dette afsnit er skrevet på baggrund af (Greuel og Pfister, 2002) og (Cox et al., 2007, kap.1). Her introduceres terminologien omkring polynomier og hvad der forstås ved en polynomiumsring.

**Definition 1.9.** Et *monomium* i $n$ variable $x_1, \ldots, x_n$ er et produkt på formen

$$\mathbf{x}^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n},$$

hvor $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$. □

Den totale grad af $\mathbf{x}^\alpha$ er $|\alpha| = \alpha_1 + \cdots + \alpha_n$. Når $\alpha = (0, \ldots, 0)$ så er $\mathbf{x}^\alpha = 1$. Der gælder at $\mathbf{x}^\alpha \mid \mathbf{x}^\beta$ hvis og kun hvis $\alpha_i \leq \beta_i$ for alle $i$, og dermed er $\mathbf{x}^\beta = \mathbf{x}^\gamma \mathbf{x}^\alpha$ for $\gamma = \beta - \alpha \in \mathbb{N}^n$.

**Eksempel 1.10.** Givet de to monomier $\mathbf{x}^\alpha = x_1^2 x_2$ og $\mathbf{x}^\beta = x_1^2 x_2^5 x_3^3$. Så er $\alpha = (2,1,0)$ med $|\alpha| = 2+1 = 3$ og $\beta = (2,5,3)$ med $|\beta| = 10$. Så gælder at $\mathbf{x}^\alpha \mid \mathbf{x}^\beta$ fordi $2 \leq 2$, $1 \leq 5$ og $0 \leq 3$, dvs. $\alpha_i \mid \beta_i$ for alle $i$. Dermed er $\gamma = \beta - \alpha = (2,5,3) - (2,1,0) = (0,4,3)$, sådan at $\mathbf{x}^\beta = \mathbf{x}^\gamma \mathbf{x}^\alpha$. □

**Definition 1.11.** Et *polynomium*, over en ring $A$, er en endelig linearkombination af monomier med koefficienter i $A$ på formen

$$f = \sum_{\alpha \in \mathbb{N}^n} a_\alpha \mathbf{x}^\alpha = \sum_{\alpha \in \mathbb{N}^n} a_{\alpha_1,\ldots,\alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n},\ a_\alpha \in A.$$

□

I polynomiet $f$ kaldes $a_\alpha$ for koefficient til monomiet $\mathbf{x}^\alpha$ og $a_\alpha \mathbf{x}^\alpha$ kaldes for et led i $f$, når $a_\alpha \neq 0$. Graden af $f$ betegnes $\deg(f) := \max\{|\alpha| \mid a_\alpha \neq 0\}$. Der gælder pr. definition, at $\deg(f) = -\infty$ for $f = 0$.

**Eksempel 1.12.** Lad $f = 2x^4y^2 + xy^2 + 6x$ være et polynomium over $A = \mathbb{R}$. Der er 3 led i $f$ bestående af monomierne: $x^4y^2$, $xy^2$ og $x$ med koefficienterne $a_{(4,2)} = 2$, $a_{(1,2)} = 1$ og $a_{(1,0)} = 6$, hvor $a_{(i,j)} = 0$ for resten. Graden af $f$ er $\deg(f) = \max\{6,3,1\} = 6$. □

**Definition 1.13.** En *polynomiumsring* $A[x_1, \ldots, x_n]$ er mængden af alle polynomier i $n$ variable med koefficienter i $A$, med den sædvanlige addition og multiplikation:

$$\sum_\alpha a_\alpha \mathbf{x}^\alpha + \sum_\alpha b_\alpha \mathbf{x}^\alpha := \sum_\alpha (a_\alpha + b_\alpha)\, \mathbf{x}^\alpha$$

$$\left(\sum_\alpha a_\alpha \mathbf{x}^\alpha\right) \cdot \left(\sum_\beta b_\beta \mathbf{x}^\beta\right) := \sum_\gamma \left(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta\right) \mathbf{x}^\gamma.$$

□

Polynomiumsringen er en kommutativ ring, hvor det neutrale element mht. multiplikation er $1 = x_1^0 \cdots x_n^0$, så $1 \in A$. Elementerne i $A \subset A[x_1, \ldots, x_n]$ kaldes konstante polynomier, og $\deg(f) \leq 0$ for $f \in A$.

### 1.2.5 Idealer i polynomiumsringe

Dette afsnit er skrevet på baggrund af (Cox et al., 2007, afsnit 1.4). Se på den kommutative ring $\mathbb{F}[x_1, \ldots, x_n]$. Et ideal over en polynomiumsring er defineret som i 1.7.

**Definition 1.14.** En delmængde $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ er et ideal hvis

1. $0 \in I$
2. $f + g \in I$ når $f, g \in I$
3. for ethvert $f \in I$ og $h \in \mathbb{F}[x_1, \ldots, x_n]$, så er $hf \in I$. □

Ofte benyttes idealer genereret af endeligt mange polynomier, dette giver god mening, som næste proposition viser.

**Proposition 1.15.** Lad $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$ og sæt

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \mid h_i \in \mathbb{F}[x_1, \ldots, x_n] \right\}.$$

Så er $\langle f_1, \ldots, f_s \rangle$ et ideal. □

**Bevis.** Det ses let, at $0 \in \langle f_1, \ldots, f_s \rangle$, da $\sum 0 \cdot f_i = 0$. At også $f + g$ og $hf$ er i mængden, ses af følgende. Lad $f = \sum_{i=1}^{s} p_i f_i$, $g = \sum_{i=1}^{s} q_i f_i$ og $h \in \mathbb{F}[x_1, \ldots, x_n]$. Da fås

$$f + g = \sum_{i=1}^{s} (p_i + q_i) f_i \in \langle f_1, \ldots, f_s \rangle \,, \text{, da } (p_i + q_i) \in \mathbb{F}[x_1, \ldots, x_n]$$

$$hf = \sum_{i=1}^{s} (hp_i) f_i \in \langle f_1, \ldots, f_s \rangle \text{ , da } (hp_i) \in \mathbb{F}[x_1, \ldots, x_n].$$

Dermed er $\langle f_1, \ldots, f_s \rangle$ et ideal ifølge definitionen. ■

**Eksempel 1.16.** Lad $I = \langle xy, x - 1 \rangle \subseteq \mathbb{F}[x, y]$ være et ideal. Vi ser nu på to vilkårlige polynomier i idealet for at illustrere nogle af egenskaberne for idealer. Lad $f = 2 \cdot f_1 + f_2 = 2xy + x - 1 \in I$ og lad $g = y^2 \cdot f_2 = xy^2 - y^2 \in I$. Så er $f + g = xy^2 + 2xy - y^2 + x - 1 = 2 \cdot f_1 + (y^2 + 1) \cdot f_2 \in I$, da 2, $y^2 + 1 \in \mathbb{F}[x, y]$.□

Et ideal $I$ er endeligt genereret, hvis der eksisterer $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$ så $I = \langle f_1, \ldots, f_s \rangle$. Da kaldes $f_1, \ldots, f_s$ for en basis for $I$. Faktisk kan det vises, at ethvert ideal over $\mathbb{F}[x_1, \ldots, x_n]$ er endeligt genereret, dette er Hilberts basissætning, som vil blive behandlet i et senere afsnit.

Et givet ideal kan have mange forskellige baser, som alle genererer den samme mængde. Senere vil vi se, at en bestemt type basis, nemlig Gröbnerbasis, er særlig velegnet at arbejde med.

En anden særlig egenskab for idealer er, at de fungerer som underrum. Faktisk svarer definitionen af et ideal til definitionen af et underrum. Begge er lukket under addition og multiplikation med hhv. skalarer og polynomier. Begge er udspændt af en basis. I underrummets tilfælde består denne af vektorer, mens idealet er udspændt af polynomier. Ved dette forstås, at mængderne består af linearkombinationer af basiselementerne, med koefficienter som er hhv. skalarer og polynomier.

### 1.2.6 Konstruktion af endelige legemer

I afsnit 1.2.1 blev vist, at det endelige legeme $\mathbb{F}_p$, hvor $p$ er et primtal, svarer til $\mathbb{Z}/p\mathbb{Z}$. Med kendskab til endelige legemer, polynomiumsringe og idealer, er det nu muligt at konstruere det endelige legeme $\mathbb{F}_{p^m}$. Dette konstrueres over en polynomiumsring $\mathbb{F}_p[x]$. Det er en kommutativ ring, dvs. som et endeligt legeme uden multiplikative inverse. For at konstruere et endeligt legeme med karakteristik $p$, benyttes et *irreducibelt* polynomium $f \in \mathbb{F}_p[x]$. At et polynomium er irreducibelt over $\mathbb{F}_p$ betyder, at det ikke kan faktoriseres i et produkt af to polynomier af lavere grad i $\mathbb{F}_p[x]$. Konstruktionen ses i følgende proposition, som medtages uden bevis.

**Proposition 1.17.** Lad $f(x)$ være et irreducibelt polynomium af grad $m$ i $\mathbb{F}_p[x]$, hvor $p$ er et primtal. så er $\mathbb{F}_p[x]/\langle f(x)\rangle$ et endeligt legeme med $p^m$ elementer. □

**Eksempel 1.18.** Lad $f(x) = x^2 + x + 1$. Den har ingen rødder i $\mathbb{F}_2$ og kan derfor ikke faktoriseres. Så $f$ er irreducibel over $\mathbb{F}_2$. Så er $m = 2, p = 2$ og $\mathbb{F}_4 = \mathbb{F}_2[x]/\langle x^2 + x + 1\rangle$. Elementerne i $\mathbb{F}_4$ er sideklasserne:

$$0 + \langle f(x)\rangle$$
$$1 + \langle f(x)\rangle$$
$$x + \langle f(x)\rangle$$
$$x + 1 + \langle f(x)\rangle$$

svarende til vektorerne $(0,0), (0,1), (1,0)$ og $(1,1)$. □

Proposition 1.17 medfører, at $\mathbb{F}_q = \mathbb{F}_p[x]/\langle f(x)\rangle$ kan dannes ved at udvide $\mathbb{F}_p$ med en rod $\alpha$ til $f(x)$. Så er $f(\alpha) = \alpha^2 + \alpha + 1 = 0$. Da $\alpha$ er et primitivt element i $\mathbb{F}_4$, kan elementerne i $\mathbb{F}_4$ også skrives som $\mathbb{F}_4 = \{0, \alpha^0, \alpha^1, \alpha^2\}$, hvor $\alpha^2 = \alpha + 1 + \langle f(\alpha)\rangle$.

Addition i $\mathbb{F}_4$ fås ved at addere polynomier eller vektorer, mens multiplikation opnås på en simpel måde, ved at multiplicere $\alpha$-potenserne, hvilket svarer til at addere eksponenterne.

## 1.3 Varieteter

I dette afsnit, som er skrevet på baggrund af (Cox et al., 2007, afsnit 1.2) defineres først det affine rum og der ses på polynomier betragtet som funktioner. Derefter

beskrives affine varieteter og sammenhængen mellem varieteter og idealer.

**Definition 1.19.** Givet et legeme $\mathbb{F}$ og et tal $n \in \mathbb{N}$, så defineres det $n$-dimensionale affine rum over $\mathbb{F}$ til at være mængden

$$\mathbb{F}^n = \{(a_1, \ldots, a_n) \mid a_1, \ldots, a_n \in \mathbb{F}\}. \qquad \square$$

For eksempel er $\mathbb{F} = \mathbb{R}$ et legeme og $\mathbb{R}^n$ er det sædvanlige $n$-dimensionale rum. $\mathbb{F}$ kan også være et endeligt legeme, fx. $\mathbb{F}_2$.

Polynomier er indtil nu blevet defineret som rent algebraiske objekter, men et polynomium kan også ses som en funktion. Hvis $f = \sum_\alpha a_\alpha \mathbf{x}^\alpha \in \mathbb{F}[x_1, \ldots, x_n]$ er et polynomium, så giver det en funktion

$$f : \mathbb{F}^n \to \mathbb{F},$$

hvor $\mathbf{a} \in \mathbb{F}^n$ giver $f(\mathbf{a}) = \sum_\alpha a_\alpha \mathbf{a}^\alpha \in \mathbb{F}$, da alle $f$'s koefficienter også er i $\mathbb{F}$. Det bemærkes, at $f = 0$ dermed kan betyde to ting. At alle koefficienter i $f$ er nul, dvs. at $a_\alpha = 0 \, \forall \alpha$, eller at $f(\mathbf{a}) = 0 \, \forall \mathbf{a} \in \mathbb{F}$. Hvis $\mathbb{F}$ er endelig, så kan de to versioner være forskellige. Som eksempel på dette ses på det endelige legeme $\mathbb{F}_2$, med elementerne 0 og 1. Lad $f = x^2 - x \in \mathbb{F}_2[x]$. Så har $f$ koefficienter forskellige fra nul, men $f(0) = 0$ og $f(1) = 0$, hvilket medfører, at $f(a) = 0$ for alle $a \in \mathbb{F}_2$.

### 1.3.1 Affine Varieteter

**Definition 1.20.** Lad $\mathbb{F}$ være et legeme og lad $f_1, \ldots, f_s$ være polynomier i $\mathbb{F}[x_1, \ldots, x_n]$. Så er

$$V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in \mathbb{F}^n \mid f_i(a_1, \ldots, a_n) = 0 \text{ for } i = 1, \ldots, s\}.$$

Da kaldes $V(f_1, \ldots, f_s)$ for den *affine varietet* defineret af $f_1, \ldots, f_s$. $\square$

En varietet er altså en mængde af punkter, som giver nul for alle de definerende funktioner. Dvs. punkter som opfylder ligningerne

$$f_1(\mathbf{x}) = 0, \; f_2(\mathbf{x}) = 0, \ldots, f_s(\mathbf{x}) = 0,$$

som kaldes de definerende ligninger for $V(f_1, \ldots, f_s)$.

Dette vises med et par eksempler.

**Eksempel 1.21.** Lad $V(xy) = \{(a_1, a_2) \in \mathbb{R}^2 \mid a_1 a_2 = 0\}$, altså mængden af punkter $(x, y)$, som opfylder $xy = 0$, dvs. at enten $x$ eller $y$ er nul. Dermed er varieteten $V(x, y)$ lig med $x$- og $y$-aksen. $\square$

**Eksempel 1.22.** Lad $V(x^2+y^2-1)$. Så er varieteten alle de punkter som opfylder

$$f(x) = 0 \Rightarrow x^2 + y^2 - 1 = 0 \Rightarrow x^2 + y^2 = 1,$$

hvoraf det ses, at varieten er en cirkel med centrum i origo og radius 1. $\square$

Affine varieteter er geomtriske objekter, der kan optræde som punkter, kurver og flader, og en varietet kan også være den tomme mængde, hvis ingen punkter i legemet opfylder alle definitionsligningerne.

En særlig egenskab ved varieteter er, at både skærings- og foreningsmængden af to varieteter selv er varieteter.

**Lemma 1.23.** Hvis $V, W \subseteq \mathbb{F}^n$ er affine varieteter, så er også $V \cup W$ og $V \cap W$ affine varieteter. □

**Bevis.** Lad $V = V(f_1, \ldots, f_s)$ og $W = V(g_1, \ldots, g_t)$. Påstanden er nu, at

$$V \cap W = V(f_1, \ldots, f_s, g_1, \ldots, g_t) \tag{1.4}$$
$$V \cup W = V(f_i g_j \mid 1 \leq i \leq s,\, 1 \leq j \leq t), \tag{1.5}$$

for så er begge mængder selv varieteter.

Ligheden i (1.4) er triviel, da skæringsmængden af $V$ og $W$ er lig med alle nulpunkter for de definerende funktioner til både $V$ og $W$.

For at vise (1.5) antages først, at $\mathbf{a} \in V$. Så er $f(\mathbf{a}) = 0 \, \forall i$ og dermed er også $f_i(\mathbf{a}) g_j(\mathbf{a}) = 0 \, \forall i$. Heraf ses, at $V \subseteq V(f_i g_j)$, og de samme argumenter viser at $W \subseteq V(f_i g_j)$. Dermed gælder der også for foreningsmængden, at $v \cup W \subseteq V(f_i g_j)$. For at vise den modsatte inklusion antages, at $\mathbf{a} \in V(f_i g_j)$. Hvis $\mathbf{a} \in V$ så er inklusionen vist. Ellers må $\mathbf{a} \notin V$, hvilket medfører, at $f_{i_0}(\mathbf{a}) \neq 0$ for et $i_0$. Men $f_i g_j(\mathbf{a}) = 0$ for alle $i$, dvs. også for $i_0$, så $f_{i_0} g_j(\mathbf{a}) = 0$ for alle $j$. Da $f_{i_0}(\mathbf{a}) \neq 0$, så må $g_j(\mathbf{a}) = 0$ for alle $j$, hvilket medfører, at $\mathbf{a} \in W$, og dermed $V(f_i g_j) \subseteq V \cup W$, og ligheden er vist. ■

**Eksempel 1.24.** Se på de to varieteter $V(x), V(y) \subseteq \mathbb{R}^2$, som svarer til hhv. $x$- og $y$-aksen. Lemmaet giver os, at

$$V(x) \cup V(y) = V(x \cdot y).$$

Denne varietet fandt vi i eksempel 1.21 til at være foreningen af $x$- og $y$-aksen, altså foreningsmængden af de to varieteter. Skæringsmængden er

$$V(x) \cap V(y) = V(x, y),$$

dvs. alle punkter som opfylder, at $x = 0 \wedge y = 0$, dvs. $V(x, y) = (0, 0)$, hvilket passer med at origo er skæringen mellem akserne. □

### 1.3.2 Idealer og Varieteter

Dette afsnit er skrevet på baggrund af (Cox et al., 2007, afsnit 1.4). Varieteter giver aneldning til en særlig slags ideal, nemlig et ideal som består af alle de polynomier som er nul på varieteten.

**Definition 1.25.** Lad $V \subseteq \mathbb{F}^n$ være en affin varietet. Så er

$$I(V) = \{f \in \mathbb{F}[x_1, \ldots, x_n] \mid f(\mathbf{a}) = 0 \text{ for alle } \mathbf{a} \in V\}.$$ □

Næste lemma viser, at $I(V)$, som defineret ovenfor, rent faktisk er et ideal.

**Lemma 1.26.** Hvis $V \subseteq \mathbb{F}^n$ er en affin varietet, så er $I(V) \subseteq \mathbb{F}[x_1, \ldots, x_n]$ et ideal. □

**Bevis.** Det ses let, at $0 \in I(V)$, da nulpolynomiet er nul på hele $\mathbb{F}^n$ og dermed også på $V$. Lad $f, g \in I(V)$, $h \in \mathbb{F}[x_1, \ldots, x_n]$ og $\mathbf{a} \in V$. Så er $f(\mathbf{a}) + g(\mathbf{a}) = 0 + 0 = 0$ og $h(\mathbf{a}) \cdot f(\mathbf{a}) = h(\mathbf{a}) \cdot 0 = 0$. Dermed er $f + g \in I(V)$ og $h \cdot f \ \in I(V)$, hvilket medfører, at $I(V)$ er et ideal. ■

Givet en mængde af polynomier $f_1, \ldots, f_s$, så kan disse både generere et ideal og definere en varietet. I dette afsnit har vi set, hvordan et ideal kan genereres af en varietet, hvilket giver følgende sammenhæng:

$$\begin{array}{ccccc} \text{polynomier} & & \text{varietet} & & \text{ideal} \\ f_1, \ldots, f_s & \to & V(f_1, \ldots, f_s) & \to & I(V(f_1, \ldots, f_s)). \end{array}$$

Det er nu interessant at se på om der mon gælder, at $I(V(f_1, \ldots, f_s)) = \langle f_1, \ldots, f_s \rangle$. Som det ses af følgende lemma er dette dog ikke altid tilfældet.

**Lemma 1.27.** Hvis $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$, så er $\langle f_1, \ldots, f_s \rangle \subseteq I(V(f_1, \ldots, f_s))$, men der gælder ikke altid lighed. □

For radikale idealer gælder der lighedstegn i lemmaet, dvs. at $I(V(I)) = \sqrt{I}$, hvor $\sqrt{I}$ er et radikalt ideal. Et *radikalt ideal*, er et ideal hvorom der gælder

$$f^m \in I \text{ for } m \in \mathbb{N} \Rightarrow f \in I. \tag{1.6}$$

Se (Cox et al., 2007, afsnit 4.2) for mere om radikale idealer og korrespondancen mellem idealer og varieteter.

### 1.3.3 Irreducible varieteter og primidealer

Dette afsnit er skrevet med udgangspunkt i (Cox et al., 2007, afsnit 4.5) og omhandler sammenhængen mellem irreducible varieteter og primidealer.

**Definition 1.28.** En affin varietet $V \subseteq \mathbb{F}^n$ er *irreducibel* hvis der gælder at, hvis $V = V_1 \cup V_2$ hvor $V_1, V_2$ er affine varieteter, så er enten $V_1 = V$ eller $V_2 = V$. □

En affin varietet er altså irreducibel når den ikke er forening af to "mindre" varieteter.

**Eksempel 1.29.** Se på varieteten $V(xz, yz) \subset \mathbb{R}^3$. Dette er foreningen af $xy$-planet og $z$-aksen, og kan skrives som $V(xz, yz) = V(x, y) \cup V(z)$, og er derfor ikke irreducibel. Det samme resultat opnås for varieteten $V(xy)$ i eksempel 1.21, da dette er foreningen af $x$-aksen og $y$-aksen, $V(xy) = V(x) \cup V(y)$. Til gengæld er varieterne $V(x), V(y), V(x, y)$ irreducible. □

Generelt gælder der, at punkter, linjer og planer altid er irreducible varieteter, hvilket virker meget intuitivt, da man kan sige at de er mere "fundamentale" end andre geometriske objekter. Men ellers kan det være svært at bevise, hvornår en varietet er irreducibel. Løsningen på dette problem kan være at benytte sammenhængen mellem varieteter og idealer, da det er lettere at regne med idealer.

**Definition 1.30.** Lad $f, g \in \mathbb{F}[x_1, \ldots, x_n]$. Et ideal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ er et *primideal* hvis der gælder, at

$$f \cdot g \in I \Rightarrow f \in I \vee g \in I. \qquad \square$$

Af følgende sætning ses, at vi hermed har fundet et ideal som svarer til en irreducibel varietet.

**Sætning 1.31.**
Lad $V \subseteq \mathbb{F}^n$ være en affin varietet. Så er $V$ irreducibel hvis og kun hvis $I(V)$ er et primideal.

**Bevis.** Her vises blot den ene vej. Beviset for den anden vej kan findes i (Cox et al., 2007, kap. 4.5). Antag, at $V$ er irreducibel og lad $f \cdot g \in I(V)$. Det skal nu vises, at $I(V)$ er et primideal, dvs. at $f \in I$ eller $g \in I$. Lad

$$V_1 = V \cap V(f) \text{ og } V_2 = V \cap V(g).$$

Da $fg \in I(V)$, så er $f(\mathbf{a})g(\mathbf{a}) = 0$ for alle $\mathbf{a} \in V$, dvs. at $f(\mathbf{a}) = 0 \vee g(\mathbf{a}) = 0$ for alle $\mathbf{a} \in V$. Heraf ses, at for alle $\mathbf{a} \in V$ så er enten $\mathbf{a} \in V(f)$ eller $\mathbf{a} \in V(g)$. Dermed er $V = (V \cap V(f)) \cup (V \cap V(g)) = V_1 \cup V_2$.

Da $V$ er irreducibel, så er enten $V_1 = V$ eller $V_2 = V$. Antag uden tab af generalitet at $V = V_1 = V \cap V(f)$, så er $f(\mathbf{a}) = 0 \forall \mathbf{a} \in V$, dvs. at $f \in I(V)$, hvormed det er vist, at $I(V)$ er et primideal. ■

**Proposition 1.32.** Lad $V \subseteq \mathbb{F}^n$ være en affin varietet. Så kan $V$ skrives som en endelig forening

$$V = V_1 \cup \cdots \cup V_m,$$

hvor alle $V_i$'erne er irreducible varieteter. $\square$

Beviset for denne sætning benytter "Descending Chain Condition", der medfører at $V_1 \supset V_2 \supset V_3 \supset \cdots$ i $\mathbb{F}^n$ stabiliserer sig, så $V_N = V_{N+1} = \cdots$. Bevis for dette og for proposition 1.32 findes i (Cox et al., 2007, afsnit 4.6).

## 1.4 Monomiumsordning

Dette afsnit er skrevet med udgangspunkt i (Cox et al., 2007, kap. 2.2) og (Høholdt et al., 1998, kap. 3.1). I de tidligere afsnit er monomier og polynomier blevet introduceret. Dette afsnit handler om forskellige måder at rangordne monomier på, så det er muligt at arrangere leddene i et polynomium i voksende eller aftagende rækkefølge.

For en *monomiumsordning* $<$ ønsker vi, at der skal gælde følgende: For det første skal det være en total ordning, dvs. en ordning, hvor der for ethvert par af monomier $\mathbf{x}^\alpha$ og $\mathbf{x}^\beta$ gælder præcist én af følgende:

$$\mathbf{x}^\alpha < \mathbf{x}^\beta,\ \mathbf{x}^\alpha = \mathbf{x}^\beta \text{ eller } \mathbf{x}^\alpha > \mathbf{x}^\beta.$$

Da vil det altid være muligt at arrangere leddene i et polynomium i voksende eller aftagende rækkefølge.

Vi ønsker også at kunne addere og multiplicere med polynomier uden at ændre på den indbyrdes rækkefølge af leddene. Addition giver ingen problemer, men ved multiplikation er det et nødvendigt krav, at multiplikation med et monomium ikke ændrer på rækkefølgen. Hvis $\mathbf{x}^\alpha < \mathbf{x}^\beta$ og $\mathbf{x}^\gamma$ er et vilkårligt monomium, skal altså gælde at $\mathbf{x}^\alpha\mathbf{x}^\gamma < \mathbf{x}^\beta\mathbf{x}^\gamma$. Der er en en-til-en korrespondance mellem monomierne i $\mathbb{F}[x_1, \ldots, x_n]$ og $\mathbb{N}^n$, da en ordning af monomierne svarer til en ordning af eksponenterne, hvor multiplikation bliver til addition. Betingelsen kan derfor omskrives til:

- hvis $\alpha < \beta$ og $\gamma \in \mathbb{N}_0^n$ så er $\alpha + \gamma < \beta + \gamma$.

Derudover skal monomiumsordningen være en *velordning* på $\mathbb{N}_0^n$, hvilket betyder at enhver ikke-tom delmængde af $\mathbb{N}_0^n$ har et mindste element under $<$. Disse tre krav er samlet i følgende definition.

**Definition 1.33.** En monomiumsordning på $\mathbb{F}[x_1, \ldots, x_n]$, er en relation $<$ på $\mathbb{N}_0^n$ eller en relation på mængden af monomier med eksponenten i $\mathbb{N}_0^n$, som opfylder følgende tre betingelser:

1. At $<$ er en total ordning på mængden af monomier $\mathbf{x}^\alpha$, hvor $\alpha \in \mathbb{N}_0^n$
2. Hvis $\mathbf{x}^\alpha < \mathbf{x}^\beta$ og $\mathbf{x}^\gamma$ er et monomium, så er $\mathbf{x}^\alpha\mathbf{x}^\gamma < \mathbf{x}^\beta\mathbf{x}^\gamma$
3. Der gælder, at $<$ er en velordning. □

I næste lemma fås en anden definition af velordning, som ofte kan være lettere at vise. For bevis henvises til (Cox et al., 2007, afsnit 2.2, lemma 2).

**Lemma 1.34.** En ordensrelation $<$ på $\mathbb{N}_0^n$ er en velordning, hvis og kun hvis enhver strengt aftagende følge i $\mathbb{N}_0^n$ er endelig. □

**Eksempel 1.35.** Et polynomium i én variabel er let at ordne, ved blot at se på graden af leddene, fx. $x^4+3x^2+7x$. Ordning mht. graden på $\mathbb{F}[x]$ opfylder nemlig definition 1.33, når gradordningen $<_{\text{deg}}$ defineres på følgende måde: $x^a <_{\text{deg}} x^b \Leftrightarrow a < b$. Det er altså nok at se på eksponenterne, og gradordningen er da en total ordning, da $<$ er en total ordning på $\mathbb{N}$. Punkt to er også opfyldt, da $a < b \Leftrightarrow a + c < b + c$, for $c \in \mathbb{N}$, og $<_{\text{deg}}$ er veldefineret fordi $<$ er veldefineret på $\mathbb{N}$.

Ved polynomier over flere variable er der derimod ikke én bestemt måde at ordne leddene på. Den naturlige ordning (natural position order), hvor der ses på de enkelte variable hver for sig, dvs.

$$(a, b) < (c, d) \Leftrightarrow a < c \text{ og } b < d,$$

giver intet resultat, hvis $a < c$ men $b > d$. Det er heller ikke muligt at ordne leddene ved blot at se på den totale grad, da flere monomier kan have samme grad uden at være ens, fx. $x^2y^3$ og $x^4y$. Ved kun at ordne efter total grad, fås altså ikke en total ordning, da ingen af de to monomier er størst og de heller ikke er lig med hinanden. Det vil her være nødvendigt også at rangordne variablene, så fx $x$ er større end $y$. □

### 1.4.1 Eksempler på monomiumsordninger

**Leksikografisk Orden** Den første ordning kaldes leksikografisk ordning (eller lex-orden), fordi den sorterer efter samme princip, som et leksikon, der sorterer efter bogstaver. Leksikografisk orden sorterer efter variablene, så $x_1 > x_2 > \cdots > x_n$, så et monomium med variablen $x_1$ altid vil være større end et monomium kun med $x_2$, uafhængigt af graden af variablene.

**Definition 1.36.** Lad $\alpha, \beta \in \mathbb{N}_0^n$. Så gælder, at $<_L$ er en leksikografisk orden med $x_1 > \cdots > x_n$, når

$$\mathbf{x}^\alpha <_L \mathbf{x}^\beta \text{ hvis og kun hvis } \alpha_1 = \beta_1, \ldots, \alpha_{l-1} = \beta_{l-1}$$
$$\text{og } \alpha_l < \beta_l \text{ for et } l,\ 1 < l < n.$$ □

**Sætning 1.37.**
Lex-ordningen er en monomiumsordning.

**Bevis.** For at være en monomiumsordning skal lex-ordningen opfylde de tre betingelser i definition 1.33.

1. At det er en total ordning ses af definitionen og at den sædvanlige ordning på $\mathbb{N}_0$ er en total ordning.

2. Hvis $\mathbf{x}^\alpha <_L \mathbf{x}^\beta$ så medfører definitionen på lex-orden, at det mest venstrestillede element i $\alpha - \beta$ er negativt. Men $\mathbf{x}^\alpha\mathbf{x}^\gamma = \mathbf{x}^{\alpha+\gamma}$ og $\mathbf{x}^\beta\mathbf{x}^\gamma = \mathbf{x}^{\beta+\gamma}$. Så er

$(\alpha+\gamma)-(\beta+\gamma)=\alpha-\beta$, dvs. det mest venstrestillede element er også her negativt, så $\mathbf{x}^{\alpha+\gamma} <_L \mathbf{x}^{\beta+\gamma}$.

3. For at være en velordning, skal enhver strengt aftagende følge i $\mathbb{N}_0^n$ være endelig. Dette vises ved modstrid, og det antages at der findes en uendelig strengt aftagende følge

$$\alpha(1) >_L \alpha(2) >_L \alpha(3) >_L \cdots$$

af elementer i $\mathbb{N}_0^n$. Først ses på første koordinat i hvert punkt $\alpha(i)$ i følgen. Pr. definition af lex-orden danner disse en aftagende følge af ikke-negative heltal, som stabiliserer sig, da $<$ er en velordning på $\mathbb{N}_0^n$. Altså findes et $k$, så første koordinat er ens i alle $\alpha(i)$ med $i \geq k$. For $\alpha(i)$ med $i \geq k$ ses nu på 2. koordinat, og disse danner igen en aftagende følge, som pga. velordningen på $\mathbb{N}_0^n$ stabiliseres. På samme måde kan fortsættes med et nyt $k$ og næste koordinat, og det ses at der må findes et $k$, så alle koordinater er ens i $\alpha(k), \alpha(k+1), \cdots$. Dette giver en modstrid, og derfor må lex-ordningen være en velordning. ■

Når der arbejdes med to eller tre variable benyttes $x, y, z$ i stedet for $x_1, x_2, x_3$ og hvor intet andet er nævnt er $x > y > z$. Lex-ordningen tager ingen hensyn til total grad, dvs. $x^2 >_L y^3z^7$. Til udregninger vil det dog ofte være lettere at benytte total grad, som de følgende to ordninger er eksempler på.

**Graderet Leksikografisk Orden** Denne metode sorterer først efter den totale grad af monomierne, og i tilfælde af lighed benyttes lex-orden.

**Definition 1.38.** For graderet leksikografisk orden $<_{GL}$ gælder, at

$$\mathbf{x}^\alpha <_{GL} \mathbf{x}^\beta$$

hvis og kun hvis der gælder én af følgende to muligheder:

$$\deg(\mathbf{x}^\alpha) < \deg(\mathbf{x}^\beta) \text{ eller } \deg(\mathbf{x}^\alpha) = \deg(\mathbf{x}^\beta) \text{ og } \mathbf{x}^\alpha <_L \mathbf{x}^\beta. \qquad \square$$

Graderet leksikografisk orden kaldes herefter glex-orden.

**Sætning 1.39.**
Glex-orden er en monomiumsordning.

**Bevis.** 1. $<_{GL}$ er en total ordning, da der ordnes efter hhv. total grad, som svarer til den totale ordning $<$ på $\mathbb{N}$, og lex-ordning som også er en total ordning.

2. Hvis $\mathbf{x}^\alpha <_{GL} \mathbf{x}^\beta$, så er der to muligheder. Enten er $\deg(\mathbf{x}^\alpha) < \deg(\mathbf{x}^\beta)$, hvilket medfører at

$$\begin{aligned} |\alpha| &< |\beta| \\ |\alpha| + |\gamma| &< |\beta| + |\gamma| \\ |\alpha + \gamma| &< |\beta + \gamma| \\ \deg(\mathbf{x}^{\alpha+\gamma}) &< \deg(\mathbf{x}^{\beta+\gamma}) \end{aligned}$$

hvorved $\mathbf{x}^\alpha\mathbf{x}^\gamma <_{GL} \mathbf{x}^\beta\mathbf{x}^\gamma$ og punkt 2 er opfyldt.

Den anden mulighed er, at $\deg(\mathbf{x}^\alpha) = \deg(\mathbf{x}^\beta)$, dvs. at $|\alpha| = |\beta|$, og $\mathbf{x}^\alpha <_L \mathbf{x}^\beta$. Da $<_L$ er monomiumsordning, så betyder det, at $\mathbf{x}^\alpha\mathbf{x}^\gamma <_L \mathbf{x}^\beta\mathbf{x}^\gamma$, og da $|\alpha| = |\beta| \Rightarrow |\alpha + \gamma| = |\beta + \gamma|$, så giver definitionen af glex-orden at punkt 2 er opfyldt.

3. Se på den aftagende følge $\alpha(1) > \alpha(2) > \cdots$. Så er $|\alpha(1)| > |\alpha(2)| > \cdots$, og pga. velordningen på $\mathbb{N}_0^n$ så stabiliserer følgen sig. Herefter ordnes efter lex-orden som også er velordning, hvilket betyder at enhver monomiumsfølge $\mathbf{x}^{\alpha(1)} >_{GL} \mathbf{x}^{\alpha(2)} >_{GL} \cdots$ er endelig. ■

**Graded Reverse Lex Orden** Den sidste metode som nævnes her er graded reverse lex orden (herefter GRL-orden). Den er mindre intuitiv, men har vist sig at være den mest effektive til udregninger på computer.

**Definition 1.40.** GRL-ordningen $<_{GRL}$ er defineret ved, at

$$\mathbf{x}^\alpha <_{GRL} \mathbf{x}^\beta$$

hvis og kun hvis der gælder én af følgende:

$$\begin{aligned} &\deg(\mathbf{x}^\alpha) < \deg(\mathbf{x}^\beta) \text{ eller} \\ &\deg(\mathbf{x}^\alpha) = \deg(\mathbf{x}^\beta) \text{ og } \alpha_n = \beta_n, \ldots, \alpha_{l+1} = \beta_{l+1} \\ &\qquad \text{og } \alpha_l > \beta_l \text{ for et } l,\ 1 < l < n. \end{aligned}$$

□

GRL-ordningen sorterer altså først efter total grad ligesom glex-ordningen, men ved lighed benyttes nu en omvendt udgave af lex ordning, hvor der ses på de sidste indgange i $\alpha$ og $\beta$ i stedet for de første.

**Sætning 1.41.**
GRL-ordningen er en monomiumsordning.

**Bevis.** Punkt 1 og 2 i definition 1.33 ses ved samme fremgangsmåde som i glex-ordning. Punkt 3 opnås igen ved at betragte en aftagende følge, hvis numeriske

værdier stabiliseres, dvs. der findes et $k$ så $|\alpha(i)| = |\alpha(i+1)|$ for $i \geq k$. Herefter ses som ved lex-orden på et koordinat i $\alpha(i)$ ad gangen for $i \geq k$. Det mest højrestillede først. Disse koordinater danner en voksende følge, men da den totale grad i monomierne er konstant for $i \geq k$, så må den voksende følge være endelig. På samme måde fortsættes med resten af koordinaterne og det ses at følgen $\alpha(1) >_{GRL} \alpha(2) >_{GRL} \cdots$ er endelig. ■

De to sidste ordninger, der sorterer efter total grad, er begge ordninger, som er isomorfe med $\mathbb{N}$ med den sædvanlige ordning. Monomierne vil nemlig kunne skrives op i rækkefølge, så det er muligt at nummerere hvert enkelt led, som i følgende eksempel, hvor $<$ er glex-ordning og $n = 3$:

$$1 < z < y < x < z^2 < yz < y^2 < xz < xy < x^2 < z^3 < \cdots$$

Sorteringen kan være lettere at gennemføre ved at se på eksponenterne som n-tupler:

$$\begin{aligned}(0,0,0) < (0,0,1) < (0,1,0) < (1,0,0) < (0,0,2) < (0,1,1) < (0,2,0)\\ < (1,0,1) < (1,1,0) < (2,0,0) < (0,0,3) < \cdots\end{aligned}$$

**Vægtet Graderet Leksikografisk Orden** Et alternativ til glex-orden, er at give variablene vægte, så det f.eks. er muligt at vægte $x$ højere end $y$. På denne måde er det muligt at få glex-ordningen til at ligne en almindelig leksikografisk orden, hvis blot vægtene er høje nok. Dette er anvendeligt, da glex-ordningen er isomorf med den sædvanlige ordning på $\mathbb{N}_0$, i modsætning til den leksikografiske orden.

Lad $\mathbf{w} = (w_1, \ldots, w_n)$ være en samling af vægte. Så defineres den vægtede grad af monomiet $\mathbf{x}^\alpha$, som

$$\operatorname{wdeg}(\mathbf{x}^\alpha) = \operatorname{wdeg}(\alpha) = \sum_{i=1}^{n} \alpha_i w_i,$$

og den vægtede grad af et polynomium $f = \sum \lambda_\alpha^\alpha$ defineres som

$$\operatorname{wdeg}(f) = \max\{\operatorname{wdeg}(\mathbf{x}^\alpha) \mid \lambda_\alpha \neq 0\}.$$

**Definition 1.42.** For vægtet graderet leksikografisk orden $<_w$ gælder, at

$$\mathbf{x}^\alpha <_w \mathbf{x}^\beta$$

hvis og kun hvis

$$\operatorname{wdeg}(\mathbf{x}^\alpha) < \operatorname{wdeg}(\mathbf{x}^\beta) \text{ eller } \operatorname{wdeg}(\mathbf{x}^\alpha) = \operatorname{wdeg}(\mathbf{x}^\beta) \text{ og } \mathbf{x}^\alpha <_L \mathbf{x}^\beta.$$

Dette er en monomiumsordning som er isomorf med $\mathbb{N}$, hvilket vi senere skal benytte. □

For at give en større forståelse for de forskellige monomiumsordninger medtages her et konkret eksempel.

**Eksempel 1.43.** Lad $f = x^2y^3z + x^3 + xy^5$. Ved benyttelse af lex-orden fås rækkefølgen:

$$x^3 >_L x^2y^3z >_L xy^5,$$

hvilket i eksponenterne svarer til $(3,0,0) >_L (2,3,1) >_L (1,5,0)$. Her har det kun været nødvendigt at se på første koordinat i eksponenterne. Hvis $f$ i stedet ordnes efter glex-ordningen, ser man først på graden af monomierne. Da $\deg(x^2y^3z) = \deg(xy^5) > \deg(x^3)$, og $(2,3,1) >_{GL} (1,5,0)$, fås rækkefølgen:

$$x^2y^3z >_{GL} xy^5 >_{GL} x^3.$$

Til sidst ses på GRL-orden, som er den mest kryptiske af de tre. Igen ses først på de to monomier af samme grad, $\deg(x^2y^3z) = \deg(xy^5)$. De sidste koordinater sammenlignes, og da $xy^5$ har den laveste grad af $z$ ordnes dette monomium som størst, dvs. $(1,5,0) >_{GRL} (2,3,1)$, hvilket giver GRL-rækkefølgen:

$$xy^5 >_{GRL} x^2y^3z >_{GRL} x^3.$$

Hermed ses det hvor meget den valgte monomiumsordning kan ændre på rækkefølgen af monomierne i et polynomium, og med vægtet graderet ordning er der netop mulighed for at konstruere vægtene så man kan få en ordning, som man vil have den. □

### 1.4.2 Terminologi

I arbejdet med polynomier benyttes her følgende terminologi:

Lad $f = \sum_a a_\alpha \mathbf{x}^\alpha$ være et ikke-nul polynomium i $\mathbb{F}[x_1, \ldots, x_n]$ og lad $<$ være en monomiumsordning på $\mathbb{F}[x_1, \ldots, x_n]$.

**Multigraden af** $f$ er det $\alpha \in \mathbb{N}_0^n$ der hører til det største led i forhold til den valgte monomiumsordning, altså

$$\text{multideg}(f) = \max\{\alpha \in \mathbb{N}_0^n \mid a_\alpha \neq 0\}$$

**Førende koefficient til** $f$ er koefficienten til det største led, altså

$$\text{LC}(f) = a_{\text{multideg}(f)}$$

**Førende monomium til** $f$ er det største monomium i polynomiet, nemlig

$$\text{LM}(f) = \mathbf{x}^{\text{multideg}(f)}$$

**Førende led** [1] er det største led, hvor både koefficient og monomium er med,

$$\mathrm{LT}(f) = \mathrm{LC}(f) \cdot \mathrm{LM}(f).$$

Som vist i eksempel 1.43, har den valgte monomiumsordning betydning for rækkefølgen af monomierne og dermed også for, hvad der er det førende led. I det næste eksempel vises, hvordan termerne bruges.

**Eksempel 1.44.** Lad $f = 2x^2y + 5y^4 + xy + 1$, med glex-ordningen på $\mathbb{F}[x, y]$. Da fås følgende:

$$\begin{aligned}
&\mathrm{multideg}(f) = \max\{(2,1),(0,4),(1,1),(0,0)\} = (0,4),\\
&\textsc{lc}(f) = a_{(0,4)} = 5,\\
&\textsc{lm}(f) = \mathbf{x}^{(0,4)} = y^4,\\
&\textsc{lt}(f) = 5y^4.
\end{aligned}$$

Benyttes i stedet lex-ordning fås $\textsc{lt}(f) = 2x^2y$, så igen ses det at valget af monomiumsordning er vigtigt. □

Om multigraden gælder der følgende lemma.

**Lemma 1.45.** Lad $f, g \in \mathbb{F}[x_1, \ldots, x_n]$ være ikke-nul polynomier. Så gælder følgende

1. $\mathrm{multideg}(fg) = \mathrm{multideg}(f) + \mathrm{multideg}(g)$.
2. Hvis $f + g \neq 0$, så er $\mathrm{multideg}(f + g) \leq \max(\mathrm{multideg}(f), \mathrm{multideg}(g))$. Hvis $\mathrm{multideg}(f) \neq \mathrm{multideg}(g)$, så gælder der lighedstegn. □

**Bevis.** Beviset opdeles i mindre dele. Først vises, at $\textsc{lt}(m \cdot f) = m \cdot \textsc{lt}(f)$. Lad $f = \sum_{i=1}^{n} a_i \mathbf{x}^{\alpha_i}$ med $\textsc{lt}(f) = a_1 \mathbf{x}^{\alpha_1}$. Så gælder

$$m \cdot f = m \cdot (a_1 \mathbf{x}^{\alpha_1} + \sum_{i=2}^{n} a_i \mathbf{x}^{\alpha_i}) = m \cdot a_1 \mathbf{x}^{\alpha_1} + \sum_{i=2}^{n} m \cdot a_i \mathbf{x}^{\alpha_i}. \tag{1.7}$$

Så er $\mathbf{x}^{\alpha_1} > \mathbf{x}^{\alpha_i}$ for $i > 1$, og da $>$ er en monomiumsordning, så medfører det, at

$$m \cdot a_1 \mathbf{x}^{\alpha_1} > m \cdot a_i \mathbf{x}^{\alpha_i} \text{ for } i > 1. \tag{1.8}$$

Det ses af (1.7) og (1.8) at

$$\textsc{lt}(m \cdot f) = \textsc{lt}(m \cdot a_1 \mathbf{x}^{\alpha_1} + \sum_{i} m \cdot a_i \mathbf{x}^{\alpha_i}) = m \cdot a_1 \mathbf{x}^{\alpha_1} = m \cdot \textsc{lt}(f).$$

[1] Forkortelserne kommer af de engelske udtryk som er hhv. leading coefficient, leading monomial og leading term.

Herefter vises, at $\text{LT}(f \cdot g) = \text{LT}(f) \cdot \text{LT}(g)$. Ved at benytte resultatet fra før, og at $\mathbf{x}^{\alpha_i}$ og $\text{LT}(g)$ er monomier ses, at

$$\begin{aligned}\text{LT}(f \cdot g) &= \text{LT}\left(\sum_{i=1}^{n} g \cdot a_i \mathbf{x}^{\alpha_i}\right) = \text{LT}\left(\sum_{i=1}^{n} \text{LT}(g) \cdot a_i \mathbf{x}^{\alpha_i}\right) \\ &= \text{LT}(\text{LT}(g) \cdot f) = \text{LT}(g) \cdot \text{LT}(f).\end{aligned}$$

Der gælder, at multideg$(f \cdot g)$ er det $\alpha$ så $\text{LM}(f \cdot g) = \mathbf{x}^{\alpha}$. Lad $\text{LM}(f) = \mathbf{x}^{\alpha}$ og $\text{LM}(g) = \mathbf{x}^{\beta}$, så er multideg$(f) = \alpha$ og multideg$(g) = \beta$. Fra før ved vi, at $\text{LM}(f \cdot g) = \text{LM}(f) \cdot \text{LM}(g) = \mathbf{x}^{\alpha} \cdot \mathbf{x}^{\beta} = \mathbf{x}^{\alpha+\beta}$. Dvs. at multideg$(f \cdot g) =$ multideg$(f) +$ multideg$(g)$.

Mht. multideg$(f + g)$, så kan multigraden højest blive multigraden af $f$ eller $g$, da polynomiet $f + g$ består af alle leddene fra de to polynomier, så leddet med det største $\alpha$ må findes blandt leddene i enten $f$ eller $g$. Den eneste måde multigraden kan blive mindre på, er hvis multideg$(f) =$ multideg$(g)$, hvilket giver mulighed for at leddene med størst multigrad går ud med hinanden. Heraf ses, at multideg$(f + g) \leq \max(\text{multideg}(f), \text{multideg}(g))$. ■

## 1.5 Polynomiumsdivision i flere variable

For at bestemme om et polynomium $f$ er i et givet ideal, ses på om det kan skrives som en kombination af idealets generatorer. I én variabel er dette problem simpelt, da ethvert ideal i $\mathbb{F}[x]$ er et hovedideal[2], dvs. genereret af ét element. Så er $f$ i idealet, hvis og kun hvis $f$ er deleligt med generatorpolynomiet. I flere variable bliver dette problem mere kompliceret at løse. Først ønsker vi at definere en divisionsalgoritme i $\mathbb{F}[x_1, \ldots, x_n]$, som gør det muligt at dividere $f \in \mathbb{F}[x_1, \ldots, x_n]$ med polynomierne $f_1, \ldots, f_s \in \mathbb{F}[x_1, \ldots, x_n]$. I én variabel medfører divisionsalgoritmen at ethvert polynomium $f$ kan skrives på formen $f = q \cdot g + r$, hvor $r = 0$ eller $\deg(r) < \deg(g)$. Så er $r$ resten ved division af $f$ med $g$. Dette kan generaliseres til flere variable, så $f$ kan skrives på formen $f = a_1 f_1 + \cdots + a_s f_s + r$, hvor $r$ er resten ved division af $f$ med polynomierne $a_1, \ldots, a_s$. Som i én variabel, hvor $r$ har lavere grad end $g$, så er resten i flere variable på en form, så det ikke er muligt at reducere yderligere.

[2]Se (Cox et al., 2007, cor.4) for bevis.

### 1.5.1 Divisionsalgoritmen

**Sætning 1.46.**
Vælg en monomiumsordning på $\mathbb{N}_0^n$ og lad $F = (f_1, \ldots, f_s)$, hvor $f_i \in \mathbb{F}[x_1, \ldots, x_n]$ for $i = 1, \ldots, s$. Så kan ethvert $f \in \mathbb{F}[x_1, \ldots, x_n]$ skrives på formen

$$f = a_1 f_1 + \cdots + a_s f_s + r, \tag{1.9}$$

hvor $a_i, r \in \mathbb{F}[x_1, \ldots, x_n]$. Polynomiet $r$ kaldes for resten af $f$ ved division med $F$. Der gælder, at enten er $r = 0$ eller også er $r$ en $\mathbb{F}$-linearkombination af monomier, hvoraf ingen er delelige med nogen af $\text{LT}(f_1), \ldots, \text{LT}(f_s)$. Endvidere gælder, at hvis $a_i f_i \neq 0$ så er multideg$(f) \geq$ multideg$(a_i f_i)$.

Beviset vil ikke blive gennemgået i detaljer her, blot nævnes strategien i beviset. For at vise sætningen defineres en divisionsalgoritme, som ved input af $F$ og et polynomium $f$, giver koefficienter og rest, så $f$ kan skrives på formen i (1.9). Herefter kan det vises, at divisionsalgoritmen opfylder sætningen.

**Divisionsalgoritmen i $\mathbb{F}[x_1, \ldots, x_n]$**

Input: polynomier $(f_1, \ldots, f_s)$ til division og et polynomium $f$
Output: koefficienterne $a_1, \ldots, a_s$ og resten $r$

Sæt $a_1 := 0, \ldots, a_s := 0, r := 0$ og $p := f$
WHILE $p \neq 0$ DO
    $i := 1$
    division:=false
    WHILE $i \leq s$ AND division=false DO
        IF $\text{LT}(f_i) \mid \text{LT}(p)$ THEN
            $a_i := a_i + \text{LT}(p)/\text{LT}(f_i)$
            $p := p - (\text{LT}(p)/\text{LT}(f_i))f_i$
            division:=true
        ELSE $i := i + 1$
    IF division=false THEN
        $r := r + \text{LT}(p)$
        $p := p - \text{LT}(p)$

Hvad der sker i de forskellige trin af algoritmen er følgende: I WHILE-DO løkken tjekkes for hvert monomium i $f$ om det er deleligt med en af $\text{LT}(f_i)$. Polynomiet $p$ benyttes til at holde styr på hvor meget af $f$ som stadig mangler

at blive skrevet på formen $f = a_1 f_a + \cdots + a_s f_s + r$. Hvis der ikke gælder, at $\text{LT}(f_i) \mid \text{LT}(p)$ for nogen $f_i$, så tilføjes monomiet $\text{LT}(p)$ til resten. Algoritmen slutter når $p = 0$.

For at bevise sætning 1.46 skal det vises, at divisionsalgoritmen slutter efter et endeligt antal trin og at outputtet opfylder sætningen. Strategien er følgende:

- Vis, at $f = a_1 f_1 + \cdots + a_s f_s + r + p$ holder i alle trin i algoritmen. Da vil (1.9) være opfyldt når $p = 0$ og algoritmen slutter. Betingelsen er klart opfyldt ved algoritmens start, hvor $a_1 = 0, \ldots, a_s = 0$ og $f = p$. Det kan vises, at ligheden også holder ved både divisionstrin og rest-trin, hvorved (1.9) er opfyldt til sidst.

- Kravene til $r$ er opfyldt, da led kun tilføjes til resten, hvis det ikke har nogen af $\text{LT}(f_i)$ som divisorer.

- At algoritmen er endelig, ses af at $\text{multideg}(p)$ er aftagende i alle trin. Da $<$ er en velordning, ifølge 1.34, så må $p = 0$ indtræffe efter et endeligt antal trin.

- Til sidst må vises, at $\text{multideg}(f) \geq \text{multideg}(a_i f_i)$, hvilket ikke nævnes nærmere her.

For flere detaljer henvises til beviset i (Cox et al., 2007, kap. 2.3).

Bemærk, at rækkefølgen af divisionspolynomierne $f_1, \ldots, f_s$ er vigtig for entydigheden af resten. Hvis der ændres på rækkefølgen af polynomierne, kan både koefficienterne $a_i$ og resten $r$ blive ændret.

**Eksempel 1.47.** Lad $f = xy^2 + xy + x + y^3 \in \mathbb{F}[x, y]$, $F = (xy - 1, y^2 + 1)$. Ved benyttelse af lex-orden kommer det til at foregå på følgende måde, når $f$ divideres med $F$:

Første trin: Her er $p := f$, $a_1 = 0, a_2 = 0$, og $\text{LT}(p) = \text{LT}(f) = xy^2$. Først ses på om $\text{LT}(f_1) \mid \text{LT}(p)$? Da det er tilfældet fås vha. algoritmen

$$a_1 := a_1 + \frac{\text{LT}(p)}{\text{LT}(f_1)} = 0 + \frac{xy^2}{xy} = y$$
$$p := p - y \cdot (xy - 1) = xy + x + y^3 + y.$$

Andet trin: Nu er $\text{LT}(p) = xy$ og igen har vi at $\text{LT}(f_1) \mid \text{LT}(p)$, så

$$a_1 := a_1 + \frac{\text{LT}(p)}{\text{LT}(f_1)} = y + \frac{xy}{xy} = y + 1$$
$$p := p - 1 \cdot (xy - 1) = x + y^3 + y + 1.$$

Tredje trin: Her er $\text{LT}(p) = x$ og hverken $\text{LT}(f_1)$ eller $\text{LT}(f_2)$ går op i $x$, som derfor bliver tilføjet til resten,

$$r := r + \text{LT}(p) = x \text{ og } p := p - \text{LT}(p) = y^3 + y + 1.$$

Der fortsættes på samme måde, indtil $p = 0$, hvilket giver følgende udregninger:

$$\begin{array}{ll} xy^2 + xy + x + y^3 & a_1 : y + 1 \\ \underline{xy^2 - y\qquad\qquad\quad} & a_2 : y \\ \qquad xy + x + y^3 + y & rest : x + 1 \\ \qquad \underline{xy - 1\qquad\qquad} & \\ \qquad\qquad x + y^3 + y + 1 & \\ \qquad\qquad \underline{y^3 + y\quad} & \\ \qquad\qquad\qquad 1 & \end{array}$$

Resultatet af divisionen bliver altså

$$a_1 = y + 1,\ a_2 = y,\ \text{og}\ r = x + 1,$$

hvormed det ses, at

$$f = (y + 1)(xy - 1) + y \cdot (y^2 + 1) + x + 1.$$

Hvis divisionen foretages med den modsatte rækkefølge af polynomierne $f_1$ og $f_2$, dvs. med $F = (y^2 + 1, xy - 1)$, fås udregningerne:

$$\begin{aligned} f &:= xy^2 + xy + x + y^3, p := f, a_1 = 0, a_2 = 0, \text{LT}(p) = xy^2 \\ a_1 &:= x \text{ og } p := xy + y^3 \\ a_2 &:= 1 \text{ og } p := y^3 + 1 \\ a_1 &:= x + y \text{ og } p := -y + 1 \\ r &:= -y + 1 \end{aligned}$$

Dette viser, at $f$ også kan skrives som

$$f = (x + y)(y^2 + 1) + (xy - 1) + (-y + 1),$$

hvoraf det ses, at hverken resten $r$ eller polynomierne $a_1$ og $a_2$ er entydigt bestemte. Senere skal vi se, at med et bestemt valg af divisions-polynomier $f_1, \ldots, f_n$ er det muligt at få en entydigt bestemt rest, som er uafhængig af rækkefølgen af divisionen. Dette er en af de vigtigste sætninger i Gröbnerbasisteorien. □

KAPITEL

# 2

# Gröbnerbaser

Dette kapitel handler om Gröbnerbaser. Teorien er skrevet med udgangspunkt i (Cox et al., 2007, kap. 2). En Gröbnerbasis for et polynomiumsideal er en basis med særligt gode egenskaber. Med en sådan basis bliver det muligt at besvare spørgsmål som tidligere var umulige at løse.

Dette kapitel vil tage udgangspunkt i to problemer, som man ofte vil støde på ved det praktiske arbejde med polynomiumsidealerne.

1. *Ideal description problem*: Dette er spørgsmålet om hvorvidt alle polynomiumsidealer har en endelig genererende mængde.

2. *Ideal membership problem*: Givet et ideal $I$ og et polynomium $f$, hvordan afgør man så om $f \in I$?

Det første af problemerne er blevet bevist før Gröbnerbasisteorien blev udviklet, men den nye teori giver et simplere bevis. Det andet problem var derimod umuligt at løse tidligere, så det er her at Gröbnerbasisteorien virkelig kommer til sin ret.

Udover disse to problemstillinger kan teorien i de følgende afsnit også anvendes til at løse polynomiumsligninger eller bestemme hvilke punkter som ligger i en affin varietet, da disse problemer kan opstilles som polynomiumsidealer. Derudover er Gröbnerbaser vigtige i forbindelse med ordensfunktioner, som vi senere skal se.

## 2.1 Dicksons Lemma

I dette afsnit ses på monomiumsidealer. Det er idealer som kun er genereret af monomier, hvilket gør dem simplere at arbejde med end polynomiumsidealer, fx. i

forbindelse med division. I dette afsnit vil vi se, at problem 1 fra indledningen også er lettere at løse for monomiumsidealer. Dette resultat opnås i Dicksons Lemma, der går ud på at alle monomiumsidealer er endeligt genereret.

**Definition 2.1.** Et ideal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ er et *monomiumsideal*, hvis der findes en mængde $A \subseteq \mathbb{N}_0^n$, så $I$ består af alle polynomier som er endelige summer på formen $\sum_{\alpha \in A} h_\alpha \mathbf{x}^\alpha$, $h_\alpha \in \mathbb{F}[x_1, \ldots, x_n]$. Da er

$$I = \langle \mathbf{x}^\alpha \mid \alpha \in A \rangle .$$ □

Idealet er altså genereret af monomier. Senere introduceres en særlig slags monomiumsideal genereret af førende led, hvilket kommer til at spille en stor rolle ved udviklingen af Gröbnerbasis-teorien.

**Lemma 2.2.** Lad $I = \langle \mathbf{x}^\alpha \mid \alpha \in A \rangle$ være et monomiumsideal. Så gælder der om et monomium $\mathbf{x}^\beta$, at $\mathbf{x}^\beta \in I \Leftrightarrow \mathbf{x}^\alpha \mid \mathbf{x}^\beta$ for et $\alpha \in A$. □

**Bevis.** Hvis $\mathbf{x}^\alpha \mid \mathbf{x}^\beta$ for et $\alpha \in A$, så er $\mathbf{x}^\beta = \mathbf{x}^\gamma \mathbf{x}^\alpha \in I$ pr. definition af $I$. Omvendt antages at $\mathbf{x}^\beta \in I$. Så er

$$\mathbf{x}^\beta = \sum_{i=1}^{s} h_i \mathbf{x}^{\alpha(i)},\ h_i \in \mathbb{F}[x_1, \ldots, x_n],\ \alpha(i) \in A.$$

Ved at skrive de enkelte led i $\mathbf{x}^\beta$ ud, fås en sum af monomier, hvor hvert af leddene er deleligt med et $\mathbf{x}^{\alpha(i)}$, hvor $\alpha(i) \in A$:

$$\begin{aligned} \mathbf{x}^\beta &= h_1 \mathbf{x}^{\alpha(1)} + \cdots + h_s \mathbf{x}^{\alpha(s)} \\ &= \sum_j M_{1_j} \mathbf{x}^{\alpha(1)} + \cdots + \sum_j M_{s_j} \mathbf{x}^{\alpha(s)} \\ &= \sum_{i,j} \mathbf{x}^{\alpha(i)+m_j}. \end{aligned}$$

I hvert led på højresiden af lighedstegnet går altså mindst ét $\alpha(i) \in A$ op i leddet. Da $\mathbf{x}^\beta$ er et monomium, må $\sum_{i,j} \mathbf{x}^{\alpha(i)+m_j}$.også være et monomium. Altså findes der et $\alpha(i) \in A$, så $\mathbf{x}^{\alpha(i)} \mid \mathbf{x}^\beta$. ■

Lemmaet medfører nogle interessante geometriske perspektiver. Der gælder om to monomier $\mathbf{x}^\alpha$ og $\mathbf{x}^\beta$, at

$$\mathbf{x}^\alpha \mid \mathbf{x}^\beta \Leftrightarrow \mathbf{x}^\beta = \mathbf{x}^\alpha \mathbf{x}^\gamma \Leftrightarrow \beta = \alpha + \gamma.$$

Altså har alle monomier som er delelige med $\mathbf{x}^\alpha$ eksponenter i mængden

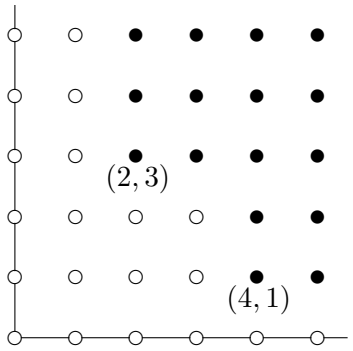
$$\alpha + \mathbb{N}_0^n = \{\alpha + \gamma \mid \gamma \in \mathbb{N}_0^n\}.$$

Da alle monomier i monomiumsidealet er multiplum af et $\mathbf{x}^\alpha$, hvor $\alpha \in A$, jvf. lemma 2.2, så kan alle idealets monomier opskrives som

$$(\alpha_1 + \mathbb{N}_0^n) \cup (\alpha_2 + \mathbb{N}_0^n) \cup \cdots \cup (\alpha_s + \mathbb{N}_0^n),\ \text{for } \alpha_1, \ldots, \alpha_s \in A.$$

Dette muliggør en geometrisk fortolkning af idealet, som i følgende eksempel.

**Eksempel 2.3.** Lad $I = \langle \mathbf{x}^{\alpha_1}, \mathbf{x}^{\alpha_2} \rangle$. Så består idealet af alle linearkombinationer af monomier med eksponenter i $(\alpha_1 + \mathbb{N}_0^n) \cup (\alpha_2 + \mathbb{N}_0^n)$. Når $n = 2$ er dette muligt at indtegne i et koordinatsystem, som det er gjort på figuren, hvor $\alpha_1 = (4,1)$ og $\alpha_2 = (2,3)$, og $((4,1) + \mathbb{N}_0^2) \cup ((2,3) + \mathbb{N}_0^2)$ svarer til de sorte punkter på figuren.□




**Lemma 2.4.** Lad $I$ være et monomiumsideal, og lad $f \in \mathbb{F}[x_1, \ldots, x_n]$. Da er følgende ækvivalent:

1. $f \in I$
2. ethvert led i $f$ er i $I$
3. $f$ er en k-linearkombination af monomierne i $I$. □

Bevis for lemmaet kan findes i (Cox et al., 2007, afsnit 2.4). Som følge af lemma 2.4 ses det, at for alle $f \in I$ så er $f$ en linearkombination af monomierne i $I$, dvs. at monomiumsidealet er entydigt bestemt af dets monomier, så to idealer er ens hvis og kun hvis de indeholder de samme monomier.

Hovedsætningen i dette afsnit er Dicksons Lemma, der løser description problemet fra indledningen, i tilfældet hvor idealet er et monomiumsideal.

**Sætning 2.5 (Dicksons Lemma).**
Lad $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ være et monomiumsideal. Så har $I$ en endelig basis.

**Bevis.** Sætningen vises ved induktion over $n$, antallet af variable. For $n = 1$ er $I = \langle x^\alpha \mid \alpha \in A \rangle$, hvor $A \subseteq \mathbb{N}_0$. Lad $\beta = \min\{\alpha \mid \alpha \in A\}$. Så er $\beta \leq \alpha$, dvs. $x^\beta \mid x^\alpha$ for alle $\alpha \in A$. Det ses nu af lemma 2.2, at $I = \langle x^\beta \rangle$.

For $n > 1$ er induktionsantagelsen, at ethvert monomiumsideal i $n-1$ variable er endeligt genereret. Strategien i beviset for $n$ variable, er at se på et ideal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$, og så lave en projektion af $I$ på $\mathbb{F}[x_1, \ldots, x_{n-1}]$, hvorved induktionsantagelsen kan bruges.

Lad $I \subseteq \mathbb{F}[x_1, \ldots, x_{n-1}, y]$ være et ideal i $n$ variable. Så kan elementerne i $I$ skrives på formen $\mathbf{x}^\alpha y^m$, hvor $\alpha = (\alpha_1, \ldots, \alpha_{n-1}) \in \mathbb{N}_0^{n-1}$ og $m \in \mathbb{N}_0$. Nu er idéen så, at projicere $I$ ned på $\mathbb{F}[x_1, \ldots, x_{n-1}]$, for at skabe nogle nye idealer, som er endeligt genereret pga. induktionsantagelsen, og som kan bruges til at konstruere en endelig basis for $I$.

Lad $J \subseteq \mathbb{F}[x_1, \ldots, x_{n-1}]$ være genereret af alle de monomier $\mathbf{x}^\alpha$, så $\mathbf{x}^\alpha y^m \in I$ for et $m \geq 0$. Pga. induktionsantagelsen er $J$ endeligt genereret, dvs. $J = \left\langle \mathbf{x}^{\alpha(1)}, \ldots, \mathbf{x}^{\alpha(s)} \right\rangle$.

For hvert $i$, hvor $1 \leq i \leq s$, så er altså $\mathbf{x}^{\alpha(i)} y^{m_i} \in I$ for et $m_i \geq 0$. Lad $m = \max\{m_1, \ldots, m_s\}$. Så gælder for alle generatorer $\mathbf{x}^{\alpha(i)}$ for $J$, at $\mathbf{x}^{\alpha(i)} y^m \in I$, fordi

$$m \geq m_i \Rightarrow y^{m_i} \mid y^m \Rightarrow \mathbf{x}^{\alpha(i)} y^{m_i} \mid \mathbf{x}^{\alpha(i)} y^m,$$

så vha. lemma 2.2 ses, at $\mathbf{x}^{\alpha(i)} y^m \in I$.

For hvert $k$, hvor $0 \leq k \leq m-1$, konstrueres nu idealet

$$J_k \subseteq \mathbb{F}[x_1, \ldots, x_{n-1}], \quad J_k = \left\langle \mathbf{x}^\beta \mid \mathbf{x}^\beta y^k \in I \right\rangle.$$

Pr. induktion har $J_k$ en endelig genererende mængde $\{\mathbf{x}^{\alpha_k(1)}, \ldots, \mathbf{x}^{\alpha_k(s_k)}\}$.

Påstanden er nu at $I$ er genereret af følgende monomier:

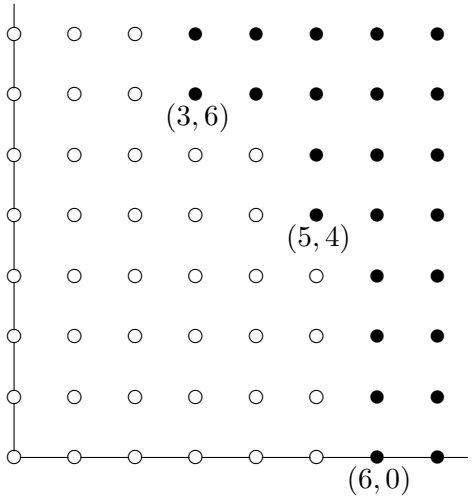
$$\begin{aligned}
\text{fra } J\text{: } & \mathbf{x}^{\alpha(1)} y^m, \ldots, \mathbf{x}^{\alpha(s)} y^m \\
\text{fra } J_0\text{: } & \mathbf{x}^{\alpha_0(1)}, \ldots, \mathbf{x}^{\alpha_0(s_0)} \\
& \vdots \\
\text{fra } J_k\text{: } & \mathbf{x}^{\alpha_k(1)} y^k, \ldots, \mathbf{x}^{\alpha_k(s_k)} y^k \\
& \vdots \\
\text{fra } J_{m-1}\text{: } & \mathbf{x}^{\alpha_{m-1}(1)} y^{m-1}, \ldots, \mathbf{x}^{\alpha_{m-1}(s_{m-1})} y^{m-1}
\end{aligned} \tag{2.1}$$

Denne mængde genererer $I$, fordi hvert monomium i $I$ er deleligt med én af generatorerne, hvilket ses af følgende argument.

Lad $\mathbf{x}^\alpha y^p \in I$ være et vilkårligt monomium i $I$. Hvis $p \geq m$ så $\mathbf{x}^\alpha y^m \mid \mathbf{x}^\alpha y^p$ og dermed er $\mathbf{x}^\alpha \in J$ pga. konstruktionen af $J$. Dette medfører at $\mathbf{x}^{\alpha(i)} \mid \mathbf{x}^\alpha$ for et $\alpha(i)$, og derfor fås, at $\mathbf{x}^{\alpha(i)} y^m \mid \mathbf{x}^\alpha y^p$, altså at monomiet er deleligt med et af de genererende monomier.

Hvis i stedet $p \leq m-1$, så gælder der at $\mathbf{x}^{\alpha_p(j)} y^p \mid \mathbf{x}^\alpha y^p$ pga. konstruktionen af $J_p$. Fra lemma 2.2 ses, at monomierne i (2.1) danner samme monomier som $I$, og som følge af lemma 2.4 er de dermed ens. Altså er $I$ endeligt genereret. ■

**Eksempel 2.6.** Lad $I$ være idealet udspændt af monomierne $\mathbf{x}^\alpha$, hvor $\alpha$ befinder sig blandt de sorte punkter på figuren.




Ifølge Dicksons Lemma, sætning 2.5 har $I$ en endelig basis, som vi kan konstruere ved at benytte samme fremgangsmåde som i beviset for sætningen. På figuren ses, at $J$ er genereret af monomierne $x^3, x^4, x^5, \ldots$, så $J = \langle x^3 \rangle \subset \mathbb{F}[x]$. Da $x^3y^6 \in I$, så er $m = 6$. Dette giver altså idealerne

$$\begin{aligned} J &= \langle x^3 \rangle \\ J_0 = J_1 = J_2 = J_3 &= \langle x^6 \rangle \\ J_4 = J_5 &= \langle x^5 \rangle , \end{aligned}$$

som danner $I = \langle x^3y^6, x^6, x^6y, x^6y^2, x^6y^3, x^5y^4, x^5y^5 \rangle$. Dette giver det samme ideal, som $I = \langle x^3y^6, x^6, x^5y^4 \rangle$, som er den mindst mulige basis for $I$. □

## 2.2 Hilberts basissætning

I det foregående afsnit blev description problemet besvaret for monomiumsidealer. I dette afsnit findes den komplette løsning på problemet i Hilberts basissætning, hvor det vises, at alle idealer har en endelig basis. For at nå dertil, ses først på et bestemt monomiumsideal, der består af de førende led fra et ideal. I dette afsnit antages det, at en bestemt monomiumsordning er valgt, hvorved de førende led vil være entydigt bestemt.

**Definition 2.7.** Lad $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ være et ideal. For en valgt monomiumsordning defineres følgende:

1. $\text{LT}(I)$ er mængden af førende led for polynomier i $I$. Dvs.

$$\text{LT}(I) = \{\text{LT}(f) \mid f \in I\}.$$

2. $\langle \text{LT}(I) \rangle$ er idealet genereret af elementer i $\text{LT}(I)$.

Dette kaldes *idealet af førende led.* □

Idealet af førende led, som defineret i 2.7, er ikke det samme som idealet genereret af de førende led for generatorpolynomierne. Dvs. $\langle \text{LT}(I) \rangle \neq \langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle$. Derimod gælder der altid, at $\text{LT}(f_i) \in \text{LT}(I) \subseteq \langle \text{LT}(I) \rangle$, så derfor er

$$\langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle \subseteq \langle \text{LT}(I) \rangle .$$

Dette ses i det følgende eksempel.

**Eksempel 2.8.** Lad $I = \langle f_1, f_2 \rangle \subset \mathbb{F}[x, y, z]$, med $f_1 = x^2y - z$ og $f_2 = xy - 1$. Ved lex-orden med $x > y > z$ ses, at $\langle \text{LT}(f_1), \text{LT}(f_2) \rangle = \langle x^2y, xy \rangle$. Lad nu

$$f = y \cdot f_1 - (xy + 1) \cdot f_2 = x^2y^2 - yz - x^2y^2 + 1 = 1 - yz.$$

Da $f \in I$, så er $\text{LT}(f) \in \langle \text{LT}(I) \rangle$, men

$$\text{LT}(f) = -yz \notin \langle x^2y, xy \rangle = \langle \text{LT}(f_1), \text{LT}(f_2) \rangle .$$ □

Selvom de to idealer ikke altid er lig med hinanden, så vises det i den følgende sætning, at der for ethvert ideal $I$ altid findes et endeligt antal polynomier i $I$, så deres førende led danner samme ideal som $\langle \text{LT}(I) \rangle$. En egenskab, som vil vise sig meget nyttig.

**Proposition 2.9.** Lad $I$ være et ideal. Så gælder følgende:

1. $\langle \text{LT}(I) \rangle$ er et monomiumsideal.

2. Der eksisterer $g_1, \ldots, g_t \in I$ så $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. □

For bevis henvises til (Cox et al., 2007, prop.3, afsnit 2.5). Fra proposition 2.9 ved vi nu, at idealet af førende led er et monomiumsideal, og derfor kan Dicksons lemma bruges til at vise Hilberts basissætning.

**Sætning 2.10 (Hilberts Basissætning).**
Ethvert ideal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ har en endelig generatormængde. Dvs.

$$I = \langle g_1, \ldots, g_t \rangle$$

for $g_1, \ldots, g_t \in I$.

**Bevis.** Hvis $I = \{0\}$, så er generatormængden $\{0\}$ og dermed endelig. Alternativt har vi fra 2.9, at der findes polynomier $g_1, \ldots, g_t \in I$ så $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. Vi vil nu vise, at $g_1, \ldots, g_t$ er generatormængde for $I$.

Det ses klart, at $\langle g_1, \ldots, g_t \rangle \subseteq I$, da $g_1, \ldots, g_t \in I$, så det er blot nødvendigt at vise den modsatte inklusion. Lad $f \in I$. Nu divideres med $g_1, \ldots, g_t$, vha. divisionsalgoritmen i flere variable, sætning 1.46. Hermed fås, at $f$ kan skrives på formen

$$f = a_1 g_1 + a_2 g_2 + \cdots + a_t g_t + r,$$

hvor ingen led i $r$ er delelig med nogle af monomierne $\text{LT}(g_1), \ldots, \text{LT}(g_t)$.

For at vise at $r = 0$, antages modsætningsvist, at $r \neq 0$. Så er $r = f - a_1 g_1 + \cdots + a_t g_t \in I$. Men da $r \in I$, så er $\text{LT}(r) \in \langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. Fra lemma 2.2 fås, at $\text{LT}(r)$ er delelig med et $\text{LT}(g_i)$, hvilket er i modstrid med at $r$ er divisionsresten. Altså må $r = 0$, hvilket medfører at $f$ er en linearkombination af $g_1, \ldots, g_t$, så $I \subseteq \langle g_1, \ldots, g_t \rangle$. ■

### 2.2.1 Varieteter defineret af idealer

Som konsekvens af Hilberts basissætning kan ethvert ideal være definerende mængde for en varietet.

**Definition 2.11.** Lad $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ være et ideal. Så er

$$V(I) = \{\mathbf{a} \in \mathbb{F}^n \mid f(\mathbf{a}) = 0 \text{ for alle } f \in I\}.$$ □

Fra Hilberts basissætning vides, at ethvert ideal har en endelig genererende mængde. På baggrund af dette vises, at en affin varietet genereret af et ideal også selv kan genereres af en endelig mængde.

**Proposition 2.12.** Lad $V(I)$ være en affin varietet. Hvis $I = \langle f_1, \ldots, f_s \rangle$ så er $V(I) = V(f_1, \ldots, f_s)$. □

**Bevis.** Hilberts basissætning giver, at $I = \langle f_1, \ldots, f_s \rangle$ er en endelig generatormængde. Det skal nu vises, at $V(I) = V(f_1, \ldots, f_s)$. Først antages, at $\mathbf{a} \in V(I)$. Så er $f(\mathbf{a}) = 0 \forall f \in I$ og specielt er $f_i(\mathbf{a}) = 0$ for $i = 1, \ldots, s$, hvormed $\mathbf{a} \in V(f_1, \ldots, f_s)$, dvs $V \subseteq V(f_1, \ldots, f_s)$.

For at vise den modsatte inklusion antages, at $\mathbf{a} \in V(f_1, \ldots, f_s)$. Så er $f_i(\mathbf{a}) = 0$ for $i = 1, \ldots, s$. Lad $f \in I$. Så er $f = \sum_{i=1}^{s} h_i f_i$ for et $h \in \mathbb{F}[x_1, \ldots, x_n]$. Så er

$$f(\mathbf{a}) = \sum_{i=1}^{s} h_i(\mathbf{a}) f_i(\mathbf{a}) = \sum_{i=1}^{s} h_i(\mathbf{a}) \cdot 0 = 0.$$

Altså er $\mathbf{a} \in V(I)$ og $V(f_1, \ldots, f_s) \subseteq V(I)$, hvormed ligheden er vist. ■

Heraf ses, at varieteter er bestemt af idealer.

## 2.3 Groebnerbaser

I dette afsnit behandles Gröbnerbasis, som er en idealbasis med særligt gode egenskaber. Det vil blive vist, at en sådan basis eksisterer for alle idealer, og sidst i afsnittet præsenteres nogle af de mest interessante egenskaber ved en Gröbnerbasis. Det antages, at en fast monomiumsordning er valgt.

I Hilberts basissætning, sætning 2.10, vises at $g_1, \ldots, g_t$ er generatormængde, dvs. basis, for $I$, når der gælder, at $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. Denne egenskab er vigtig og benyttes derfor til følgende definition.

**Definition 2.13.** Lad $I$ være et ideal. En endelig mængde $\{g_1, \ldots, g_t\} \subset I$ kaldes en *Gröbnerbasis*, hvis der gælder, at

$$\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle . \qquad \square$$

En følge af sætning 2.10 er, at ethvert ideal har en Gröbnerbasis.

**Korollar 2.14.** Ethvert ideal forskelligt fra $\{0\}$ har en Gröbnerbasis, som er en endelig basis for idealet. $\square$

**Bevis.** Lad $I$ være et ikke-nul ideal. Så findes der ifølge proposition 2.9 en endelig mængde $g_1, \ldots, g_t \in I$ så $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. I beviset for sætning 2.10 ses, at $I = \langle g_1, \ldots, g_t \rangle$, så dette er en Gröbnerbasis for $I$. ■

I eksempel 2.8 fandt vi frem til, at $\langle \text{LT}(I) \rangle \neq \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$, så ifølge definition 2.13 danner $\{f_1, f_2\}$ ikke en Gröbnerbasis. Men ethvert ideal har en endelig Gröbnerbasis ifølge korollaret, og et af de store resultater indenfor Gröbnerbasisteorien, som vil blive nævnt senere, er Buchbergers Algoritme, der kan benyttes til at finde en sådan basis.

### 2.3.1 Egenskaber

Ved division i flere variable afhænger resultatet både af den valgte monomiumsordning og af rækkefølgen af de polynomier, der divideres med. Dette kan være problematisk i det praktiske arbejde med polynomiumsidealer, fx. ved spørgsmålet om hvorvidt et polynomium er i et givet ideal $I$, nemlig Membership problemet som nævnt i starten af kapitlet. Polynomiet er i $I$, hvis det kan skrives som en linearkombination af generatorpolynomierne for $I$, men desværre giver divisionsalgoritmen ikke et entydigt resultatet, som kan afgøre dette. I det følgende vil vi dog vise, at det er muligt, når en Gröbnerbasis benyttes som basis for $I$, og netop derfor er denne basis så anvendelig. Først vises at restleddet ved division med en Gröbnerbasis er entydigt bestemt.

**Proposition 2.15.** Lad $G = \{g_1, \ldots, g_t\}$ være en Gröbnerbasis for idealet $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ og lad $f \in \mathbb{F}[x_1, \ldots, x_n]$. Ved division af $f$ med $G$ opnås en rest $r \in \mathbb{F}[x_1, \ldots, x_n]$, hvorom der gælder

(i) Der findes et $g \in I$, så $f = g + r$

(ii) Intet led i $r$ er deleligt med en af $\text{LT}(g_1), \ldots, \text{LT}(g_t)$

(iii) Restleddet $r$ er entydigt bestemt og uafhængigt af rækkefølgen af $g_1, \ldots, g_t$ ved divisionen. □

**Bevis.** Divisionsalgoritmen giver ifølge sætning 1.46 at $f = a_1 g_1 + \cdots + a_t g_t + r$, hvor $r$ opfylder (ii), og ved at lade $g = a_1 g_1 + \cdots + a_t g_t \in I$, så er også (i) opfyldt. Entydigheden ses ved modsætningsvist at antage, at $f = g + r = g' + r'$. Så er $r - r' = g' - g \in I$, da $g, g' \in I$. Hvis $r \neq r'$, så må $\text{LT}(r - r') \in \langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$, hvilket ifølge lemma 2.2 medfører, at $\text{LT}(r - r')$ er delelig med én af $\text{LT}(g_1), \ldots, \text{LT}(g_t)$. Men dette er en modstrid, da det førende monomium i $r - r'$ er et monomium i $r$ eller $r'$, som begge opfylder (ii), dvs. ingen led i $r$ eller $r'$ er delelige med noget $\text{LT}(g_i)$. Derfor må $r = r'$ og restleddet er entydigt bestemt. ■

I beviset for 2.15 benyttes $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$, til at vise, at restleddet er entydigt bestemt. Entydigheden er altså en konsekvens af den særlige egenskab for Gröbnerbaser. Rækkefølgen af polynomierne ved divisionen ændrer ikke på restleddet, men til gengæld afhænger $a_i$'erne i $f = a_1 g_1 + \cdots + a_t g_t + r$ af, i hvilken rækkefølge divisionen foretages, som det følgende eksempel vil vise.

**Eksempel 2.16.** Lad $g_1 = x + z$ og $g_2 = y - z$. Så er $G = \{g_1, g_2\}$ en Gröbnerbasis, når monomierne ordnes efter lex-orden på $\mathbb{F}_3[x, y, z]$. Dette tjekkes i Singular med kommandoen

```
> ring r = 3,(x,y,z),lp;
> poly g1 = x+z;
> poly g2= y-z;
> ideal I = g1,g2;
> std(I);
_[1]=y-z
_[2]=x+z
```

Se nu på polynomiet $g = xy$. Ved division med $g_1, g_2$ fås

$$g = y \cdot (x + z) + (-z) \cdot (y - z) - z^2 = y g_1 - z g_2 + r,$$

og ved division i den modsatte rækkefølge, med $f_2, f_1$ fås

$$g = x \cdot (y - z) + z \cdot (x + z) - z^2 = x g_2 + z g_1 + r.$$

Det ses her, at resten $r = -z^2$ ikke er delelig med $\text{LT}(g_1) = x$ eller $\text{LT}(g_2) = y$, som følge af (ii) i proposition 2.15, og der gælder, at restleddet er uafhængigt af divisionsrækkefølgen, da $r = -z^2$ i begge udregninger, hvilket passer med (iii). Til gengæld er koefficienterne til $g_1$ og $g_2$ er forskellige. Rækkefølgen af elementerne i basen er altså vigtig for, hvilke koefficienter der opnås ved divisionen. □

Entydigheden af restleddet gør det nu muligt at bestemme, hvornår et polynomium er i et ideal.

**Korollar 2.17.** Lad $G = \{g_1, \ldots, g_t\}$ være en Gröbnerbasis for idealet $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ og lad $f \in \mathbb{F}[x_1, \ldots, x_n]$. Så er $f \in I$ hvis og kun hvis restleddet ved division af $f$ med $G$ er nul. □

**Bevis.** Ved division med $G$ fås fra 2.15, at $f = g+r$, hvor $g \in I$, så hvis restleddet er nul, så er $f = g \in I$. Omvendt, hvis $f \in I$, så opfylder $f = f + 0$ betingelserne i 2.15, og restleddet er dermed nul. ■

**Eksempel 2.18.** Lad $I = \langle x + z, y - z \rangle \subseteq \mathbb{F}_3[x, y, z]$. I eksempel 2.16 så vi, at restleddet, ved division af $g = xy$ med Gröbnerbasen, var $r = -z^2 \neq 0$, ved brug af lex-orden. Ifølge korollaret medfører det, at $g \notin I$. Lad $f = xy^2 + y^3 + x^2 + xz$. Er $f \in I$?. Reduce-kommandoen i Singular giver ved brug af lex-orden resultatet

```
ring r = 3,(x,y,z),lp;
ideal I = x+z,y-z;
poly f= xy2+y3+x2+xz;
reduce(f,std(I));
0
```

Så $\overline{f}^G = 0$, hvilket medfører at $f \in I$ ifølge korollar 2.17. Når $f$ er ordnet efter lex-orden, så er $\text{LT}(f) = x^2$, men hvis vi ændrer monomiumsordningen til glex-orden, så ændres også leddenes rækkefølge, og $\text{LT}(f) = xy^2$. Korollar 2.17 er dog uafhængig af den valgte monomiumsordning, og restleddet giver da også nul, når vi reducerer $f$ med glex-orden:

```
ring r = 3,(x,y,z),Dp;
ideal I = x+z,y-z;
poly f= xy2+y3+x2+xz;
reduce(f,std(I));
0
```

## 2.4 Buchbergers sætninger

I dette afsnit beskrives Buchbergers kriterium og Buchbergers algoritme.

### 2.4.1 Buchbergers kriterium

Vi har set, at Membership problemet er muligt at løse, så længe vi kender en Gröbnerbasis for idealet. Men hvordan bestemmes så, om en givet basis er en Gröbnerbasis? For at svare på dette, ser vi først på, hvad der skal til for at en

basis ikke er en Gröbnerbasis. Da må der gælde, at $\langle \text{LT}(I) \rangle \neq \langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle$, hvor $f_1, \ldots, f_s$ danner en basis for $I$. Der findes altså et $f \in I$, hvor

$$\text{LT}(f) \notin \langle \text{LT}(f_1), \ldots, \text{LT}(f_s) \rangle .$$

Men da $f$ er en linearkombination af $f_1, \ldots, f_s$, så er den eneste måde hvorpå det kan ske, hvis nogle af de førende led går ud med hinanden. Dette problem ses i det følgende eksempel.

**Eksempel 2.19.** Lad $I = \langle f_1, f_2 \rangle \subseteq \mathbb{R}[x, y, z]$, hvor $f_1 = xy^2 + yz$ og $f_2 = x^2 - z$, og benyt den leksikografiske ordning. Lad nu

$$f = xf_1 - y^2 f_2 = x(xy^2 + yz) - y^2(x^2 - z) = xyz + y^2 z$$

Så er $f \in I$ og $xyz = \text{LT}(f) \in \text{LT}(I)$. Men $xyz$ er hverken deleligt med $\text{LT}(f_1) = xy^2$ eller $\text{LT}(f_2) = x^2$, så $\text{LT}(f) \notin \langle \text{LT}(f_1), \text{LT}(f_2) \rangle$.

Problemet skyldes her, at $f_1$ og $f_2$ multipliceres med monomier som gør, at de fremkomne polynomier $xf_1$ og $-y^2 f_2$ har førende led der går ud med hinanden, her $x^2y^2$ og $-x^2y^2$. □

Dette princip udforskes nærmere i den følgende definition.

**Definition 2.20.** Lad $f, g \in \mathbb{F}[x_1, \ldots, x_n]$ være ikke-nul polynomier. Så defineres *mindste fælles multiplum* og *S-polynomier* som følger:

- Lad multideg$(f) = \alpha$ og multideg$(g) = \beta$, og lad $\gamma = (\gamma_1, \ldots, \gamma_n)$, hvor $\gamma_i = \max(\alpha_i, \beta_i)$. Da er

  $$\mathbf{x}^\gamma = \text{LCM}(\text{LM}(f), \text{LM}(g))$$

  og $\mathbf{x}^\gamma$ kaldes for mindste fælles multiplum af $\text{LM}(f)$ og $\text{LM}(g)$.

- S-polynomiet for $f$ og $g$ er

  $$S(f, g) = \frac{\mathbf{x}^\gamma}{\text{LT}(f)} \cdot f - \frac{\mathbf{x}^\gamma}{\text{LT}(g)} \cdot g \tag{2.2}$$

□

I definitionen ses, at S-polynomiet netop dannes ved at gange polynomierne med det mindste fælles multiplum divideret med den førende koefficient, hvilket resulterer i at de fremkomne polynomier begge får mindste fælles multiplum som førende led.

**Eksempel 2.21.** Fra eksempel 2.19 haves, at $f = xy^2 + yz$ og $g = x^2 - z$. Da er $\gamma = (2, 2)$ og

$$\begin{aligned} S(f, g) &= \frac{x^2y^2}{xy^2} \cdot f - \frac{x^2y^2}{x^2} \cdot g \\ &= x \cdot f - y^2 \cdot g \\ &= xyz + y^2 z, \end{aligned}$$

hvorved vi får samme polynomium som i eksempel 2.19. □

S-polynomier er simpelthen konstrueret til at få de førende led til at gå ud med hinanden, og faktisk kan det vises, at S-polynomierne er de eneste polynomier med denne egenskab, hvilket ses af følgende lemma, som medtages uden bevis. For bevis, se (Cox et al., 2007).

**Lemma 2.22.** Givet en sum $\sum_{i=1}^{s} c_i f_i$, hvor $c_i \in \mathbb{F}$ og multideg$(f_i) = \delta \in \mathbb{N}_0^n$ for alle $i$. Hvis multideg$(\sum_{i=1}^{s} c_i f_i) < \delta$, så er $\sum_{i=1}^{s} c_i f_i$ en linearkombination med koefficienter i $\mathbb{F}$ af S-polynomierne $S(f_j, f_k)$ for $1 \leq j, k \leq s$. Endvidere er alle multideg$(S(f_j, f_k)) < \delta$. □

Det ses af (2.2), at $S$ er en linearkombination af $f$ og $g$, dvs. $S \in \langle f, g \rangle$. Så når $f$ og $g$ er generatorer for $I$, så er $S \in I$. Disse egenskaber benyttes i beviset for Buchbergers Kriterium, der viser hvornår en basis for et ideal er en Gröbnerbasis.

**Sætning 2.23 (Buchbergers Kriterium).**
Lad $I$ være et polynomiumsideal. Lad $G = \{g_1, \ldots, g_t\}$ være en basis for $I$. Så er $G$ en Gröbnerbasis for $I$ hvis og kun hvis der gælder for alle par $i \neq j$, at resten ved division af $S(g_i, g_j)$ med $G$ er nul.

**Bevis.** Hvis $G$ er en Gröbnerbasis for $I$, så er $S(g_i, g_j) \in I$ og resten ved division med $G$ er nul ifølge korollar 2.17. Den modsatte vej kræver længere udregninger. Her skitseres beviset blot, mens de nærmere detaljer kan findes i (Cox et al., 2007, kap.2.6).

Lad $f \in I$. Det skal nu vises, at hvis alle S-polynomierne giver resten nul ved division med $G$, så er $\text{LT}(f) \in \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. Så er nemlig $\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$ og $G$ er en Gröbnerbasis.

Når $f \in I$ og $I = \langle g_1, \ldots, g_t \rangle$, så kan $f$ skrives på formen

$$f = \sum_{i=1}^{t} h_i g_i,\ h_i \in \mathbb{F}[x_1, \ldots, x_n].$$

Fra lemma 1.45 fås, at

$$\text{multideg}(f) \leq \max(\text{multideg}(h_i g_i)). \tag{2.3}$$

Der er nu to muligheder. Hvis der gælder lighedstegn i (2.3), så er multideg$(f) =$ multideg$(h_i g_i)$ for et $i$, og dermed er $\text{LT}(f)$ deleligt med et $\text{LT}(g_i)$. Heraf ses via lemma 2.2, at $\text{LT}(f) \in \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$, som var det ønskede resultat.

Hvis derimod der gælder skarp ulighed i (2.3), så må det betyde at nogle af de førende led i summen går ud med hinanden. Da $f = \sum_{i=1}^{t} h_i g_i$ kan forekomme på mange måder med forskellige kombinationer af polynomier, så vælges det udtryk der giver den *mindste* værdi af max(multideg$(h_i g_i)$). Lad $\delta =$ max(multideg$(h_i g_i)$)

og lad $m(i) = \text{multideg}(h_i g_i)$. Idéen i beviset er nu at benytte lemma 2.22 og se, at $f$ kan skrives som en sum af S-polynomier med multigrad mindre end $\delta$. Disse kan, pga. antagelsen med at alle restleddene er nul ved division med $G$, skrives som summer af $g_i$'erne, og ved nogle snedige omskrivninger er det muligt at nå frem til

$$f = \sum_i \tilde{h}_i g_i + \sum_{m(i)=\delta} (h_i - \text{LT}(h_i))g_i + \sum_{m(i)<\delta} h_i g_i,$$

hvor $\text{multideg}(\tilde{h}_i g_i) < \delta$. Her fås altså et udtryk for $f$ som polynomiumskombination af $g_i$'erne, hvor alle leddene har multigrad mindre end $\delta$. Dette er i modstrid med at $\delta$ er valgt som den mindste værdi af $\max(\text{multideg}(h_i g_i))$. Det må betyde at der gælder lighedstegn i (2.3), og sætningen er vist. ■

Fremover benyttes notationen $\overline{f}^F$ for resten ved division af polynomiet $f$ med den ordnede mængde $F = (f_1, \ldots, f_s)$. Hvis $F$ er en Gröbnerbasis følger det af 2.15, at rækkefølgen i $F$ er uden betydning, så $F$ kan anses som mængden $\{f_1, \ldots, f_s\}$.

**Eksempel 2.24.** Lad $I = \langle x^2y - 1, xy^2 - x \rangle$. Er $G = \{x^2y - 1, xy^2 - x\}$ en Gröbnerbasis for $I$ med lex-orden? For at undersøge dette udregnes S-polynomiet, hvor $\gamma = (2, 2, 0)$

$$S(x^2y - 1, xy^2 - x) = y(x^2y - 1) - x(xy^2 - x) = x^2 - y.$$

Ved at dividere med $G$ fås resten $\overline{S(x^2y - 1, xy^2 - x)}^G = x^2 - y$, altså er $G$ ikke en Gröbnerbasis. Bemærk også, at

$$LT(x^2 - y) = x^2 \notin \langle x^2y, xy^2 \rangle = \langle \text{LT}(x^2y - 1), \text{LT}(xy^2 - x) \rangle,$$

hvorved det også ses at $G$ ikke kan være en Gröbnerbasis. □

I eksemplet var den givne basis for $I$ ikke en Gröbnerbasis. I dette tilfælde ønsker vi at finde en Gröbnerbasis, for at kunne regne videre med idealet. Buchbergers Kriterium kan kun tjekke om en givet basis er en Gröbnerbasis, men beviset er ikke-konstruktivt, så det kan ikke bruges til at finde en sådan basis. I næste afsnit bliver Buchbergers kriterium anvendt til at finde en algoritme, der kan konstruere en Gröbnerbasis for et givet ideal.

### 2.4.2 Buchbergers Algoritme

I dette afsnit udvikles en metode til at konstruere en Gröbnerbasis for et givet ideal. Metoden er algoritmisk og princippet bag udnytter Buchbergers kriterium for Gröbnerbaser. Ifølge kriteriet, sætning 2.23, gælder der for en basis $G$, at $\overline{S(g_i, g_j)}^G = 0$ for alle $g_i, g_j \in G$ hvis og kun hvis $G$ er en Gröbnerbasis. Givet en basis for idealet $I$, så tjekkes alle resterne $\overline{S(f_i, f_j)}^G$, og når et restpolynomium

er forskellig fra nul tilføjes det til basen. På den måde sikres at restleddet ved division af $S(g_i, g_j)$ med den nye basis er nul. På denne måde fortsættes med at tilføje restpolynomier til basen, indtil alle resterne er nul, hvilket betyder at den konstruerede basis er en Gröbnerbasis. Dette er fremgangsmåden i Buchbergers Algoritme. I beviset benyttes følgende notation: Lad $G = \{g_1, \ldots, g_t\}$. Så er

$$\langle G \rangle = \langle g_1, \ldots, g_t \rangle \tag{2.4}$$

$$\langle \mathrm{LT}(G) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_t) \rangle \,. \tag{2.5}$$

Beviset benytter også sætningen *The Ascending Chain Condition* (voksende kæde betingelse). For bevis henvises til (Cox et al., 2007, kap.2.5).

**Lemma 2.25 (Ascending Chain Condition).** Lad $I_1 \subset I_2 \subset I_3 \subset \cdots$ være en voksende kæde af idealer i $\mathbb{F}[x_1, \ldots, x_n]$. Så eksisterer der et $N \geq 1$ sådan at

$$I_N = I_{N+1} = I_{N+2} = \cdots \,. \qquad \square$$

Sætningen betyder altså at enhver voksende kæde af idealer vil stabilisere sig efter et endeligt antal trin. Dette er en nødvendig betingelse for at vise den følgende sætning.

**Sætning 2.26 (Buchbergers Algoritme).**
Lad $I = \langle f_1, \ldots, f_s \rangle$ være et polynomiumsideal. Så kan en Gröbnerbasis $G$ for $I$ konstrueres i et endeligt antal trin vha. følgende algoritme:

Input: $F = (f_1, \ldots, f_s)$
Output: $G = (g_1, \ldots, g_t)$

$G := F$
REPEAT
    $G' := G$
    FOR hvert par $\{p, q\}$, $p \neq q$ i $G'$ DO
        $S := \overline{S(p,q)}^{G'}$
        IF $S \neq 0$ THEN $G := G' \cup \{S\}$
UNTIL $G = G'$

**Bevis.** Strategien i beviset er først at vise, at $G$ er en Gröbnerbasis for $I$ i tre trin: Først vises, at $G \subseteq I$ i alle skridt i algoritmen. Herefter vises, at $G$ er en basis for $I$, og at denne basis er en Gröbnerbasis. Til sidst vises, at algoritmen slutter i et endeligt antal trin.

I starten af algoritmen er $G = F$ og dermed $G \subseteq I$. Dette er også tilfældet i alle trin af algoritmen, da $G$ bliver udvidet med resten $S = \overline{S(p,q)}^{G'}$, hvor både

$S(p,q)$ og $G'$ er i $I$. Heraf fås, at

$$S(p,q) = h_1g_1 + \cdots + h_rg_r + S \Leftrightarrow S(p,q) - (h_1g_1 + \cdots + h_rg_r) = S,$$

hvor $g_1, \ldots, g_r \in G'$ og $S$ er restleddet. Da $S(p,q) \in I$ og $(h_1g_1 + \cdots + h_rg_r) \in I$, så ses at også $S = \overline{S(p,q)}^{G'} \in I$, hvorved $G = G \cup \overline{S(p,q)}^{G'} \subseteq I$. Da $F \subseteq G$ og $F$ er basis for $I$, så er $G$ også en basis for $I$, og det er en Gröbnerbasis fordi at algoritmen slutter når $G' = G$, dvs. når $\overline{S(p,q)}^{G'} = 0$ for alle $p, q \in G$.

Tilbage er blot at vise, at algoritmen slutter efter endelig tid, altså at $G' = G$ opnås. Lad $\text{LT}(G) = \langle \text{LT}(g_1), \ldots, \text{LT}(g_t) \rangle$. For hver gentagelse er $G' \subseteq G$, dvs. $\langle \text{LT}(G') \rangle \subseteq \langle \text{LT}(G) \rangle$. Hvis $G' \neq G$, så må $\langle \text{LT}(G') \rangle$ være strengt mindre end $\langle \text{LT}(G) \rangle$, hvilket ses af følgende: Når $G' \neq G$, så må der i $G$ være tilføjet en rest $S = \overline{S(p,q)}^{G'}$. Da $S$ er restled ved division med $G'$, så er $\text{LT}(S)$ ikke delelig med nogle af de førende led i $G'$, så $\text{LT}(S) \in G$ men $\text{LT}(S) \notin G'$. Derfor er $\langle \text{LT}(G') \rangle \subsetneq \langle \text{LT}(G) \rangle$.

Idealerne $\langle \text{LT}(G') \rangle$ fra hvert trin i algoritmen danner tilsammen en voksende kæde af idealer, da $\langle \text{LT}(G') \rangle \subseteq \langle \text{LT}(G) \rangle$. Lemma 2.25 medfører dermed at kæden stabiliseres, dvs. at $\langle \text{LT}(G') \rangle = \langle \text{LT}(G) \rangle$ efter et endeligt antal skridt, hvor $G' = G$ og algoritmen stopper. ■

Med Buchbergers algoritme er det altså muligt at konstruere en Gröbnerbasis til ethvert ideal. Algoritmen er her medtaget i en simpel udgave for at vise at konstruktionen er mulig, men skal den bruges i praksis kan man med fordel effektivisere algoritmen. F.eks. udregnes alle restleddene $\overline{S(p,q)}^{G'}$ for hver gentagelse af FOR-løkken, men hvis en rest er nul ved division med $G'$ så ændres dette ikke, selvom der tilføjes nye elementer til $G'$, hvorfor det kun er nødvendigt at udregne restled ifht. de tilføjede polynomier $f_j$, nemlig $\overline{S(f_i,f_j)}^{G'}$, hvor $i < j$.

**Eksempel 2.27.** Find en Gröbnerbasis for $I = \langle x^2y - 1, xy^2 - x \rangle$, hvor der benyttes lex-orden på $\mathbb{F}[x,y]$. Input i Buchbergers algoritme er $F = \{f_1, f_2\}$ hvor $f_1 = x^2y - 1$ og $f_2 = xy^2 - x$, og ved algoritmens start er $G' = G = \{f_1, f_2\}$. Nu udregnes S-polynomiet for $f_1$ og $f_2$:

$$S(f_1,f_2) = \frac{x^2y^2}{x^2y} \cdot f_1 + \frac{x^2y^2}{xy^2} \cdot f_2 = x^2y^2 - y - x^2y^2 + x^2 = x^2 - y.$$

Da restleddet er $\overline{S(f_1,f_2)}^{G'} = x^2 - y$, så tilføjes $f_3 := x^2 - y$ til mængden $G$, og da der ikke er flere polynomier at tjekke i denne gennemkørsel af FOR-løkken, så fås det nye $G' = \{f_1, f_2, f_3\}$. Endnu engang tjekkes alle S-polynomierne i $G'$. Dette kan gøre i Singular med koden

```
> ring R = 8,(x,y),lp;
> poly f1 = x2y-1;
> poly f2 = xy2-x;
```

```
> poly f3 = x2-y;
> ideal I = f1,f2,f3;
> spoly(f1,f3);
y2-1
> reduce(y2-1,I);
y2-1
```

Dette giver følgende rester:

$$\begin{aligned} S(f_1,f_3) &= 1\cdot f_1 - y\cdot f_3 = x^2y - 1 - x^2y + y^2 = y^2 - 1,\\ \overline{S(f_1,f_3)}^{G'} &= y^2-1 =: f_4, \quad G := G\cup\{f_4\}\\ S(f_2,f_3) &= x\cdot f_2 - y^2\cdot f_3 = x^2y^2 - x^2 - x^2y^2 + y^3 = y^3 - x^2,\\ \overline{S(f_2,f_3)}^{G'} &= y^3 - y =: f_5, \quad G := G\cup\{f_5\}. \end{aligned}$$

Da $G'$ er forskellig fra $G$, så sættes $G' = \{f_1,f_2,f_3,f_4,f_5\}$, og FOR-løkken gennemføres endnu engang med de nye polynomier:

$$\begin{aligned} S(f_1,f_4) &= x^2 - y, \quad \overline{S(f_1,f_4)}^{G'} = 0\\ S(f_1,f_5) &= x^2y - y^2, \quad \overline{S(f_1,f_5)}^{G'} = 0, \end{aligned}$$

og det viser sig at alle de resterende S-polynomier også giver nul, hvormed $G = \{f_1,f_2,f_3,f_4,f_5\} = G'$, og ifølge sætning 2.26 er $G$ en Gröbnerbasis for $I$. □

Det kan vises, at $G = \{y^2-1, x^2-y\} = \{f_4,f_5\}$ også er en Gröbnerbasis for idealet i eksemplet. Gröbnerbasen er altså ikke entydigt bestemt, og kan ofte reduceres til færre elementer, som det ses af følgende lemma.

**Lemma 2.28.** Lad $G$ være en Gröbnerbasis for $I$. Lad $g \in G$ være et polynomium så $\text{LT}(g) \in \langle \text{LT}(G - \{g\})\rangle$. Så er $G - \{g\}$ også en Gröbnerbasis for $I$. □

**Bevis.** Pr. definition af Gröbnerbasis er $\langle \text{LT}(G)\rangle = \langle \text{LT}(I)\rangle$, og hvis $\text{LT}(g) \in \langle \text{LT}(G-\{g\})\rangle$, så må $\langle \text{LT}(G-\{g\})\rangle = \langle \text{LT}(G)\rangle = \langle \text{LT}(I)\rangle$. Dermed er $G - \{g\}$ også en Gröbnerbasis for $I$. ■

På den måde fjernes overflødige polynomier fra Gröbnerbasen. Hvis man derudover vælger polynomier med førende koefficienter lig med 1, så opnås en minimal Gröbnerbasis:

**Definition 2.29.** En *minimal Gröbnerbasis* er en Gröbnerbasis $G$ som opfylder:

1. $\text{LC}(g) = 1$ for alle $g \in G$
2. For alle $g \in G$ gælder, at $\text{LT}(g) \notin \langle \text{LT}(G - \{g\})\rangle$. □

I eksempel 2.27 nåede vi frem til at $G = \{x^2y-1, xy^2-x, x^2-y, y^2-1, y^3-y\}$ var en Gröbnerbasis for $I$. Her er alle førende koefficienter 1 og det ses at $\text{LT}(f_1) = x^2y = y \cdot \text{LT}(f_3)$, $\text{LT}(f_2) = x \cdot \text{LT}(f_4)$ og $\text{LT}(f_5) = y \cdot \text{LT}(f_4)$. Dermed kan $f_1, f_2$ og $f_5$ fjernes fra $G$.

Da definition 2.29 kun omhandler de førende led, giver det mulighed for flere forskellige minimale Gröbnerbaser. Derfor følger endnu en definition på en Gröbnerbasis som faktisk er entydigt bestemt:

**Definition 2.30.** En *reduceret Gröbnerbasis* for et polynomiumsideal $I$ er en Gröbnerbasis $G$, hvorom der gælder:

1. $\text{LC}(g) = 1$ for alle $g \in G$
2. For alle $g \in G$ gælder, at ingen af $g$'s monomier ligger i $\langle \text{LT}(G - \{g\}) \rangle$. □

**Proposition 2.31.** Lad $I$ være et polynomiumsideal forskelligt fra nul. For en givet monomiumsordning har $I$ en entydigt bestemt reduceret Gröbnerbasis. □

For bevis henvises til (Cox et al., 2007, prop.6, afsnit 2.7). Dette er en bekvem egenskab, da det så er lettere at se om to idealer er ens.

### 2.4.3 Ideal Membership-problemet

Med Buchbergers algoritme er det nu muligt at løse membership-problemet. Lad $I = \langle f_1, \ldots, f_s \rangle$ være et ideal og $f$ et polynomium. For at bestemme om $f \in I$ benyttes først Buchbergers algoritme til at finde en Gröbnerbasis $G = \{g_1, \ldots, g_t\}$ for $I$, hvorefter korollar 2.17 medfører, at $f \in I$ hvis og kun hvis $\overline{f}^G = 0$. Derfor benyttes divisionsalgoritmen til at bestemme om $\overline{f}^G = 0$.

**Eksempel 2.32.** Lad $f = xy^3 - z^2 + y^5 - z^3$ og $I = \left\langle -x^3 + y, x^2y - z \right\rangle$. Er $f \in I$? Først tjekkes om $f_1 = -x^3 + y$ og $f_2 = x^2y - z$ danner en Gröbnerbasis for $I$. Da

$$\text{LT}(S(f_1, f_2)) = \text{LT}(-xz + y^2) = -xz \in \langle \text{LT}(I) \rangle$$

mens

$$-xz \notin \left\langle -x^3, x^2y \right\rangle = \langle \text{LT}(f_1), \text{LT}(f_2) \rangle ,$$

så er $\{f_1, f_2\}$ ikke en Gröbnerbasis. En sådan basis findes i stedet vha. Buchbergers algoritme, som giver

$$G = \{f_1, f_2, f_3, f_4, f_5\} = \{xz - y^2, x^2y - z, x^3 - y, xy^3 - z^2, y^5 - z^3\}.$$

Nu er der blot tilbage at finde resten af $f$ ved division med $G$. Det ses let, at

$$f = 0 \cdot f_1 + 0 \cdot f_2 + 0 \cdot f_3 + 1 \cdot f_4 + 1 \cdot f_5 + 0.$$

Altså er $\overline{f}^G = 0$ og det er vist, at $f \in I$. □

KAPITEL

# 3

# Ordensfunktioner og evalueringskoder

Sidste kapitel handlede om Gröbnerbasisteori. I dette kapitel beskrives evalueringskoder samt nogle af resultater, der bygger på Gröbnerbaser, og som er relevante mht. koderne. Først defineres polynomiumsafbildninger og kvotientringe, der bruges til at sige noget om længden af en kode. Derefter defineres ordensfunktioner, som anvendes til at give en grænse for minimumsafstanden. Evalueringskoderne introduceres og AG-koder nævnes kort, inden kapitlet munder ud i et afsnit om eksistens af ordensfunktioner.

## 3.1 Varieteter og kvotientringe

Dette afsnit omhandler forskellige områder i forbindelse med kvotientringe og varieteter. Afsnittet er skrevet på baggrund af (Cox et al., 2007, kap. 5). Der indledes med en definition af og resultater for polynomiumsafbildninger, og afsnittet munder ud i nogle grænser for antallet af elementer i $V(I)$, hvor $I$ er et ideal. Disse resultater vil senere være relevante ved arbejdet med evalueringskoder.

### 3.1.1 Polynomiumsafbildninger

Først defineres en *polynomiumsafbildning* mellem to affine varieteter.

**Definition 3.1.** Lad $V \subseteq \mathbb{F}^m$, $W \subseteq \mathbb{F}^n$ være varieteter. En funktion $\varphi : V \to W$ kaldes en polynomiumsafbildning, hvis der eksisterer polynomier $f_1, \ldots, f_n \in \mathbb{F}[x_1, \ldots, x_m]$, så

$$\varphi(\mathbf{a}) = (f_1(\mathbf{a}), \ldots, f_n(\mathbf{a})) \text{ for alle } \mathbf{a} = (a_1, \ldots, a_m) \in V.$$

Da siges $(f_1, \ldots, f_n) \in (\mathbb{F}[x_1, \ldots, x_m])^n$ at *repræsentere* $\varphi$. □

Af definitionen ses altså, at hvis $\varphi : V \to W$ er repræsenteret ved $(f_1, \ldots, f_n)$, så må $(f_1(\mathbf{a}), \ldots, f_n(\mathbf{a}))$ opfylde de definerende ligninger for $W$, for alle $\mathbf{a} \in V$. Specielt er det interessant at se på *polynomiumsfunktionen* $\varphi : V \to \mathbb{F}$, som er repræsenteret ved et enkelt polynomium $f$. Resultaterne herfra kan let generaliseres til polynomiumsafbildninger, $\varphi : V \to \mathbb{F}^n$, med polynomiumsfunktioner som komponenter.

Polynomiumsfunktioner er ofte givet ved deres repræsentant, men desværre er denne sjældent entydigt bestemt.

**Eksempel 3.2.** Lad $V(y^2 - x)$ være en varietet på $\mathbb{R}^2$. Lad $f = x^2 + y^4$ være repræsentant for polynomiumsfunktionen $\varphi : V \to \mathbb{R}$. Men så repræsenterer $g = x^2 + y^4 + (y^2 - x)$ samme funktion, og det samme gør alle polynomier på formen $h = x^2 + y^4 + A(x, y) \cdot (y^2 - x)$, hvor $A \in \mathbb{F}[x, y]$, så $f$ er altså ikke entydigt bestemt. □

Systemet i eksemplet for, hvornår $f$ og $g$ er repræsentanter for samme funktion, generaliseres i følgende proposition.

**Proposition 3.3.** Lad $v \subseteq \mathbb{F}^m$ være en affin varietet.

(i) $f$ og $g \in \mathbb{F}[x_1, \ldots, x_m]$ repræsenterer samme polynomiumsfunktion på $V$ hvis og kun hvis $f - g \in I(V)$.

(ii) $(f_1, \ldots, f_n)$ og $(g_1, \ldots, g_n)$ repræsenterer samme polynomiumsafbildning hvis og kun hvis $f_i - g_i \in I(V)$ for alle $i$. □

**Bevis.** (i) Det ses, at $f - g \in I(V)$, hvis og kun hvis, der for alle $p \in V$ gælder

$$(f - g)(p) = 0 \Leftrightarrow f(p) - g(p) = 0 \Leftrightarrow f(p) = g(p),$$

altså når $f$ og $g$ repræsenterer samme funktion på $V$.

(ii) følger at (i), da enhver polynomiumsafbildning har polynomiumsfunktioner som komponenter. ■

Propositionen viser, at repræsentanterne for polynomiumsfunktioner kan samles i klasser af polynomier, hvilket senere vil blive benyttet til at danne kvotientringe af polynomiumsringe. Disse viser sig nyttige i arbejdet med polynomiumsfunktioner.

**Definition 3.4.** Med $\mathbb{F}[V]$ betegnes mængden af polynomiumsfunktioner $\varphi : V \to \mathbb{F}$. □

Det kan vises, at $\mathbb{F}[V]$ har sum- og produktoperationerne konstrueret som sum og produkt i $\mathbb{F}[x_1, \ldots, x_n]$, hvilket gør $\mathbb{F}[V]$ til en kommutativ ring.

Det følgende resultat viser nogle interessante sammenhænge mellem de algebraiske egenskaber for polynomiumsafbildningerne i $\mathbb{F}[V]$, og de geometriske egenskaber for varieten $V$ og idealet $I(V)$.

**Proposition 3.5.** Lad $V \subseteq k$ være en affin varietet. Da er følgende ækvivalent:

(i) $V$ er irreducibel

(ii) $I(V)$ er et primideal

(iii) $\mathbb{F}[V]$ er et integritetsområde. □

**Bevis.** Beviset for at de første to udsagn er ækvivalente fås af sætning 1.31.

At (i) $\Rightarrow$ (iii), vises ved indirekte bevis. Antag, at $\mathbb{F}[V]$ ikke er et integritetsområde. Så må der findes polynomiumsafbildninger $\varphi, \psi \in \mathbb{F}[V]$, så $\varphi \cdot \psi = 0$ men $\varphi, \psi \neq 0$. Disse har polynomiumsrepræsentanter $f, g \in \mathbb{F}[x_1, \ldots, x_n]$, hvorom der må gælde, at

$$f \cdot g \in I(V), \text{ men } f, g \notin I(V). \tag{3.1}$$

Der gælder altså for alle $x \in V$, at $f(x) \cdot g(x) = 0$, dvs. at $f(x) = 0$ eller $g(x) = 0$. Mængden $V$ kan dermed ses som foreningsmængden af de punkter i $V$, hvor $f$ er nul, og de punkter, hvor $g$ er nul. Hermed fås at

$$V = (V \cap V(f)) \cup (V \cap V(g)) .$$

Det vises ved modstrid, at opdelingen af $V$ er ikke-triviel, dvs. at hverken $V \cap V(f)$ eller $V \cap V(g)$ er lig med hele $V$. Antag først at $V = V \cap V(f)$. Så er $f(x) = 0$ for alle $x \in V$. Men fra (3.1) fås at $f \notin I(V)$, dvs. der findes et $x \in V$ så $f(x) \neq 0$, hvilket er en modstrid, så derfor er $V \cap V(f)$ ikke hele $V$. På samme måde ses at $V \neq V \cap V(g)$, og altså er $V$ reducibel.

(iii) $\Rightarrow$ (i) vises ved indirekte bevis. Antag, at $V$ ej er irreducibel. Dvs. $V$ er reducibel og kan dermed skrives som den ikke-trivielle forening $V = V_1 \cup V_2$. Lad $f_1 \in \mathbb{F}[x_1, \ldots, x_n]$ være et polynomium, som er identisk nul på $V_1$, men ikke på $V_2$ og lad $f_2 \in \mathbb{F}[x_1, \ldots, x_n]$ være nul på hele $V_2$, men ikke på $V_1$. Sådanne polynomier findes, da $V_1$ og $V_2$ er ikke-tomme varieteter, hvoraf ingen af dem er helt indeholdt i den anden. Der gælder nu, at hverken $f_1$ eller $f_2$ er identisk nul på hele $V$, men produktet $f_1(x) \cdot f_2(x) = 0$ for alle $x \in V$, da $x \in V_1$ eller $x \in V_2$. Så produktfunktionen er nul i $\mathbb{F}[V]$, mens hverken $f_1$ eller $f_2$ repræsenterer nulfunktionen i $\mathbb{F}[V]$. Altså er $\mathbb{F}[V]$ ikke et integritetsområde. ■

### 3.1.2 Kvotientringe

Som nævnt i proposition 3.3 kan polynomiumsrepræsentanterne for funktionerne i $\mathbb{F}[V]$ samles i klasser, så $f$ og $g$ repræsenterer samme funktion, hvis og kun hvis $f - g \in I(V)$. Dette princip udnyttes til at danne en *kvotientring*, som det ses i følgende definitioner. For flere detaljer henvises til (Cox et al., 2007, kap. 5.2).

**Definition 3.6.** Lad $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ være et ideal, og lad $f, g \in \mathbb{F}[x_1, \ldots, x_n]$. Da siges $f$ og $g$ at være kongruente modulo $I$, når $f - g \in I$. Dette skrives

$$f \equiv g \pmod{I}. \qquad \square$$

Der gælder, at kongruens modulo $I$ er en ækvivalensrelation på $\mathbb{F}[x_1, \ldots, x_n]$, hvilket giver kvotientringen $\mathbb{F}[x_1, \ldots, x_n]/I$:

**Definition 3.7.** Kvotienten af $\mathbb{F}[x_1, \ldots, x_n]$ modulo $I$ er mængden af ækvivalensklasser modulo $I$, hvilket skrives

$$\mathbb{F}[x_1, \ldots, x_n]/I = \{[f] \mid f \in \mathbb{F}[x_1, \ldots, x_n]\}. \qquad \square$$

Det kan vises, at $\mathbb{F}[x_1, \ldots, x_n]/I$ er en kommutativ ring med sum- og produktoperationerne defineret ved

$$[f] + [g] = [f + g]$$
$$[f] \cdot [g] = [f \cdot g].$$

En interessant følge af 3.3 er at der er en en-til-en korrespondance mellem $\mathbb{F}[V]$ og $\mathbb{F}[x_1, \ldots, x_n]/I$.

**Sætning 3.8.**
Der er en en-til-en korrespondance mellem elementerne i $\mathbb{F}[V]$ og elementerne i $\mathbb{F}[x_1, \ldots, x_n]/I(V)$, som bevarer sum- og produktoperationerne.

Et bevis for sætning 3.8 findes i (Cox et al., 2007, kap. 5.2).

### 3.1.3 Udregninger i kvotientringe

I det følgende antages at der arbejdes i ringen $\mathbb{F}[x_1, \ldots, x_n]$ og at der er valgt en monomiumsordning. Givet et ideal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$, lad så $\langle LT(I) \rangle$ være idealet genereret af de førende led i $I$ i forhold til den valgte monomiumsordning, og lad $\Delta(I)$ være monomierne i komplementærmængden til $\langle LT(I) \rangle$. Da kaldes $\Delta(I)$ for *fodaftrykket* af $I$.

I den næste sætning vises det, at alle elementerne i $\mathbb{F}[x_1, \ldots, x_n]/I$ er linearkombinationer af fodaftrykket, og at monomierne i fodaftrykket er lineært uafhængige, hvorved det danner en basis for kvotientringen.

**Proposition 3.9.** Lad $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ være et ideal. Så gælder der

(i) Ethvert $f \in \mathbb{F}[x_1, \ldots, x_n]$ er kongruent modulo $I$ med et entydigt polynomium $r$, som er en k-linearkombination af monomierne af $\Delta(I)$.

(ii) Elementerne i $\Delta(I) = \{\mathbf{x}^\alpha \mid \mathbf{x}^\alpha \notin \langle \text{LT}(I) \rangle\}$ er lineært uafhængige modulo $I$, dvs. hvis

$$\sum_{\mathbf{x}^\alpha \in \Delta(I)} c_\alpha \mathbf{x}^\alpha \equiv 0 \pmod{I},$$

så er $c_\alpha = 0$ for alle $\alpha$. $\square$

**Bevis.** (i) Lad $G$ være en Gröbnerbasis for $I$ og lad $f \in \mathbb{F}[x_1, \ldots, x_n]$. Af divisionsalgoritmen, sætning 1.46 ses, at $f = q + r$, hvor $q \in I$. Så $f - r = q \in I$, dvs. $f \equiv r \pmod{I}$. Altså er $f$ kongruent modulo $I$ til resten ved division med $G$. At resten er entydig følger af proposition 2.15, og herfra fås også, at ingen led i $r$ er delelig med noget $\text{LT}(g_i)$, for $g_i \in G$, hvoraf det ses, at $r$ er en linearkombination af monomierne $\mathbf{x}^\alpha \notin \langle \text{LT}(I) \rangle$.

(ii) Antag, at $\sum_\alpha c_\alpha \mathbf{x}^\alpha \equiv 0 \pmod{I}$, hvor $x^\alpha \in \Delta(I)$, dvs. $x^\alpha \notin \langle LT(I) \rangle$. Dermed er $\sum_\alpha c_\alpha \mathbf{x}^\alpha \in I$. Hvis $\sum_\alpha c_\alpha \mathbf{x}^\alpha \neq 0$, så er $LT(\sum_\alpha c_\alpha \mathbf{x}^\alpha) \in \langle LT(I) \rangle$, men ingen af monomierne $x^\alpha$ er i $\langle LT(I) \rangle$, hvilket giver en modstrid. Altså må $\sum_\alpha c_\alpha \mathbf{x}^\alpha = 0$ for alle $x$, hvilket kun opnås hvis $c_\alpha = 0$ for alle $\alpha$. ■

Ifølge proposition 3.9 har ethvert polynomium i $\mathbb{F}[x_1, \ldots, x_n]$ en standardrepræsentant i $\mathbb{F}[x_1, \ldots, x_n]/I$, nemlig resten $r$, som fås ved division med en Gröbnerbasis for $I$. Dette polynomium er ifølge (i) en linearkombination af monomierne i fodaftrykket $\Delta(I)$. Da endvidere elementerne i $\Delta(I)$ er lineært uafhængige, ses det, at $\Delta(I)$ danner en basis for kvotientringen $\mathbb{F}[x_1, \ldots, x_n]/I$.

Disse egenskaber eksemplificeres i det følgende.

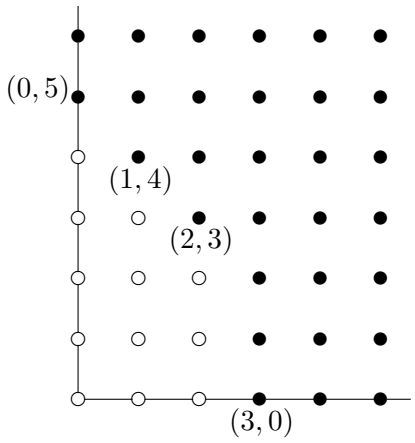
**Eksempel 3.10.** Lad $I = \langle x^2y^3 - x, x^4y^2 - y \rangle$ med glex orden på $\mathbb{F}_3[x, y]$. En Gröbnerbasis kan findes vha. følgende kommandoer i Singular:

```
ring R = 3,(x,y),Dp;
ideal I = x2y3-x,x4y2-y;
ideal sI = groebner(I);
sI;
sI[1]=x3-y2
sI[2]=y5-x2
sI[3]=xy4-y
sI[4]=x2y3-x
```

Så $G = \{x^3 - y^2, y^5 - x^2, xy^4 - y, x^2y^3 - x\}$ er en Gröbnerbasis for $I$. Heraf fås, at $\langle \text{LT}(I) \rangle = \langle x^3, y^5, xy^4, x^2y^3 \rangle$. Eksponenterne for generatorerne til $\langle \text{LT}(I) \rangle$ kan nu indtegnes i et koordinatsystem, for at visualisere monomierne i $\langle \text{LT}(I) \rangle$ og i komplementet $\Delta(I)$. Eksponenterne for monomierne i $\langle \text{LT}(I) \rangle$ består af mængden

$$((3,0) + \mathbb{N}_0^2) \cup ((0,5) + \mathbb{N}_0^2) \cup ((1,4) + \mathbb{N}_0^2) \cup ((2,3) + \mathbb{N}_0^2),$$

som svarer til de sorte punkter på figuren.




Elementerne i $\Delta(I)$ illustreres ved de hvide punkter, og består af de 12 monomier $1, x, x^2, y, xy, x^2y, y^2, xy^2, x^2y^2, y^3, xy^3, y^4$. Dette kan også tjekkes i Singular med

```
kbase(sI);
size(kbase(sI));
```

For ethvert $f \in \mathbb{F}[x, y]$ medfører proposition 3.9, at resten $\overline{f}^G$ vil være en linearkombination af monomierne i $\Delta(I)$. Lad $f = 2x^3y - xy + x^5y^3$ og udregn resten ved division med $G$:

```
poly f = 2x3y - xy + x5y3;
reduce(f,sI);
xy2+2y3-xy
```

Det ses, at $\overline{f}^G = xy^2 + 2y^3 - xy$, som er en linearkombination af monomierne $xy^2, y3, xy \in \Delta(I)$, hvilket stemmer overens med proposition 3.9.

Hvis en anden monomiumsordning benyttes, opnås en ny basis for $\Delta(I)$, men antallet af monomier i basen er dog den samme. Med lex-orden i stedet for glex, fås Gröbnerbasen $G = \{y^{12} - y, x - y^8\}$. Her er $\langle \text{LT}(I) \rangle = \langle y^{12}, x \rangle$ og $\Delta(I) = \{1, y, y^2, y^3, \ldots, y^{11}\}$, hvor antallet af monomier i $\Delta(I)$ stadig er 12. □

I dette eksempel var fodaftrykket endeligt, men ofte kan det være uendeligt. Se f.eks. eksempel 2.6, hvor idealet er $I = \langle x^3y^6, x^6, x^5y^4 \rangle$. Her indeholder fodaftrykket alle monomier på formen $x^a y^b$, hvor $a < 3$, hvilket giver uendeligt mange elementer.

Sammenhængen mellem kvotientringen $\mathbb{F}[x_1, \ldots, x_n]/I$ og vektorrummet udspændt af monomierne i fodaftrykket ses i følgende sætning.

**Proposition 3.11.** Lad $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ være et ideal. Så er $\mathbb{F}[x_1, \ldots, x_n]/I$ isomorf med $S = \text{sp}\{\Delta(I)\}$. □

For bevis for denne og den næste proposition henvises til (Cox et al., 2007, afsnit 5.3, prop. 4 og 5). Om udregninger i $\mathbb{F}[x_1, \ldots, x_n]$ gælder følgende:

**Proposition 3.12.** Lad $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ være et ideal og lad $G$ være en Gröbnerbasis for $I$. For hvert $[f] \in \mathbb{F}[x_1, \ldots, x_n]/I$ findes en standardrepræsentant $\overline{f} = \overline{f}^G$ i $S = \text{sp}\{\Delta(I)\}$. Så gælder

1. $[f] + [g]$ repræsenteres af $\overline{f} + \overline{g}$.
2. $[f] \cdot [g]$ repræsenteres af $\overline{\overline{f} \cdot \overline{g}}^G \in S$. □

I den næste sætning følger nogle udsagn omkring dimensionen af vektorrummet $S$ over $\Delta(I)$. For et detaljeret bevis henvises til (Cox et al., 2007, afsnit 5.3, thm.6). Bemærk, at $\dim(\overline{\mathbb{F}_q}[x_1, \ldots, x_n]/I) = |\Delta(I)|$: Fra proposition 3.11 ses, at $\mathbb{F}[x_1, \ldots, x_n]/I \simeq \text{sp}\{\Delta(I)\}$. Altså har de to vektorrum samme dimension. Da elementerne i $\Delta(I)$ er lineært uafhængige, jvf. proposition 3.9, så er $\Delta(I)$ en basis for $\text{sp}\{\Delta(I)\}$, og da dimensionen er lig med antallet af elementer i basen, så er $\dim(\overline{\mathbb{F}_q}[x_1, \ldots, x_n]/I) = \dim(\text{sp}\{\Delta(I)\}) = |\Delta(I)|$.

**Sætning 3.13.**
Lad $V = V(I)$ være en affin varietet i $\mathbb{F}_q^n$ og vælg en monomiumsordning i $\mathbb{F}_q[x_1, \ldots, x_n]$. Så er følgende udsagn ækvivalente:

(i) For hvert $i$, $1 \leq i \leq n$ findes der et $m_i \geq 0$, sådan at $x_i^{m_i} \in \langle \text{LT}(I) \rangle$.

(ii) Lad $G$ være en Gröbnerbasis for $I$. Så findes der for hvert $i$, $1 \leq i \leq n$ et $m_i \geq 0$, så $x_i^{m_i} = \text{LM}(g)$ for et $g \in G$.

(iii) $\mathbb{F}_q$-vektorrummet $S = \text{sp}\{\Delta(I)\}$ er endeligt dimensionalt.

(iv) $\mathbb{F}_q$-vektorrummet $\mathbb{F}_q[x_1, \ldots, x_n]/I$ er endeligt dimensionalt.

Bemærk, at hvis der arbejdes i det algebraisk lukkede legeme $\overline{\mathbb{F}}_q$, som ikke er endeligt, så er punktet

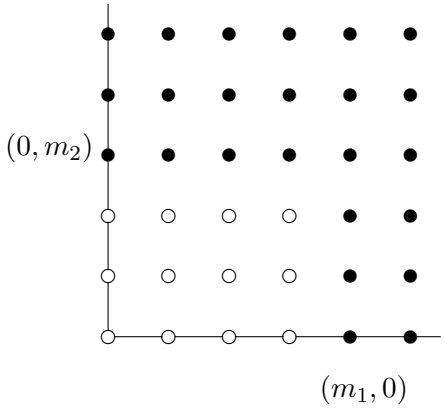
$$(v)\, V \text{ er en endelig mængde}$$

ækvivalt med resten.

Ækvivalensen mellem (i) og (ii) fås af, at $G$ er en Gröbnerbasis, dvs. $\langle \text{LT}(I) \rangle = \langle \text{LT}(g) \mid g \in G \rangle$. Så $x_i^{m_i} \in \langle \text{LT}(I) \rangle \Leftrightarrow \text{LT}(g_i) \mid x_i^{m_i}$, hvorved $\text{LT}(g_i)$ må være en potens af $x_i$.

Som illustration af punkt (i) og (ii) ses på en Gröbnerbasis $G = \{g_1, g_2\}$ for $I$. Hvis $\text{LM}(g_1) = x_1^{m_1}$ og $\text{LM}(g_2) = x_2^{m_2}$, så kan eksponenterne $m_1$, $m_2$ indtegnes i et koordinatsystem, som på figuren. Det ses på figuren, at når der findes et $m_i$

så $x_i^{m_i} \in \langle \text{LT}(I) \rangle$ for $i = 1, \ldots, n$, så sikrer det at fodaftrykket, svarende til de hvide punkter på figuren, bliver endeligt. Dermed har $S$ som vektorrum over $\Delta(I)$ endelig dimension.




Punkt $(iv)$ og $(v)$ er ækvivalente ifølge proposition 3.11, hvoraf det ses, at $\mathbb{F}_q[x_1, \ldots, x_n]/I$ og $S$ er isomorfe. Dvs. hvis $f \in S$, så er

$$[f] = f + I \in \mathbb{F}_q[x_1, \ldots, x_n]/I.$$

**Eksempel 3.14.** Igen ses på idealet fra eksempel 3.10, hvor $G = \{x^3 - y^2, y^5 - x^2, xy^4 - y, x^2y^3 - x\}$ er en Gröbnerbasis for $I$. Her er $x^3$ og $y^5$ i $\langle \text{LT}(I) \rangle$, så $m_1 = 3$ og $m_2 = 5$. Ifølge sætning 3.13 er $S$ endeligt dimensional, i tråd med eksempel 3.10, hvor vi fandt, at der er 12 elementer i fodaftrykket, som altså er endeligt. Ser vi i stedet på idealet $I = \langle x^3y^6, x^6, x^5y^4 \rangle$ fra eksempel 2.6, hvor $G = \{x^3y^6, x^6, x^5y^4\}$ er en Gröbnerbasis, så findes der ikke noget $m \geq 0$, sådan at $y^m = g$ for noget $g \in G$. Dermed giver sætning 3.13 at $S$ ikke er endeligt dimensional. □

I den følgende sætning er det nødvendigt at arbejde over et algebraisk lukket legeme $\overline{F_q}$, hvilket er det mindste legeme med $\mathbb{F}_q \subseteq \overline{\mathbb{F}}_q$, som indeholder alle rødder til alle polynomier over $\mathbb{F}_q$.

**Sætning 3.15.**
Lad $I \subseteq \overline{F_q}[x_1, \ldots, x_n]$ være et ideal så $V = V(I)$ er en endelig mængde. Så gælder, at antallet af punkter i $V$ højst er $\dim(\overline{F_q}[x_1, \ldots, x_n]/I)$.

**Bevis.** Beviset falder i to dele. Først vises, at givet punkterne $P_1, \ldots, P_m \in \overline{F_q}^n$, så eksisterer der polynomier $f_1, \ldots, f_m \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n]$, hvorom der gælder

$$f_i(P_i) = 1 \text{ og } f_i(P_j) = 0 \text{ for } i \neq j. \tag{3.2}$$

Disse polynomier benyttes i anden del af beviset, hvor det vises, at $[f_1], \ldots, [f_m] \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n]/I$ er lineært uafhængige, for $V(I) = \{P_1, \ldots, P_m\}$. Med $m$ lineært uafhængige elementer i $\overline{\mathbb{F}_q}[x_1, \ldots, x_n]/I$, fås at $\dim(\overline{\mathbb{F}_q}[x_1, \ldots, x_n]/I) \geq m$, hvor $m$ er antallet af punkter i $V$, hvilket beviser sætningen.

Først konstrueres polynomier som opfylder (3.2). Betragt $a \neq b$, $a, b \in \overline{F_q}^n$. Så er $a$ og $b$ forskellige i mindst én koordinat. Antag at de er forskellige i det j'te koordinat, så $a[j] \neq b[j]$. Lad

$$g = \frac{(x_j - b[j])}{(a[j] - b[j])}.$$

Ved indsættelse af $a$ og $b$ fås

$$g(a) = \frac{(a[j] - b[j])}{(a[j] - b[j])} = 1 \text{ og } g(b) = \frac{(b[j] - b[j])}{(a[j] - b[j])} = 0.$$

På samme måde konstrueres nu polynomier for alle $P_i \neq P_1$, $i \geq 2$. Antag nu at $P_i$ og $P_1$ er forskellige i det $j$'te koordinat og lad

$$g_i = \frac{(x_j - P_i[j])}{(P_1[j] - P_i[j])}.$$

Så er

$$g_i(P_i) = \frac{(P_i[j] - P_i[j])}{(P_1[j] - P_i[j])} = 0 \text{ og } g_i(P_1) = \frac{(P_1[j] - P_i[j])}{(P_1[j] - P_i[j])} = 1.$$

Lad nu $f_1 = g_2 \cdot g_3 \cdots g_m$. Så er

$$f_1(P_1) = 1 \cdot 1 \cdots 1 = 1 \text{ og } f_1(P_i) = c_2 \cdots c_{i-1} \cdot 0 \cdots c_m = 0.$$

Samme fremgangsmåde benyttes til at konstruere $f_2, \ldots, f_m$, som alle opfylder (3.2).

Lad nu $V = \{P_1, \ldots, P_m\}$, hvor $P_i$'erne er forskellige. Til punkterne i $V$ konstrueres som nævnt polynomierne $f_1, \ldots, f_m$, og det skal nu vises, at $[f_1], \ldots, [f_m] \in \overline{\mathbb{F}_q}[x_1, \ldots, x_n]/I$ er lineært uafhængige.

Antag, at $\sum_{i=1}^m a_i[f_i] = 0$. Lad $f = \sum_{i=1}^m a_i f_i$. Da $[f] = \sum_{i=1}^m a_i[f_i] = 0$, så er $f \in I$. Dette medfører, at $f(P_i) = 0$ for alle $i$, da $P_i \in V(I)$, så $P_i$ er nul for alle funktioner i $I$. Der gælder nu for $i = 1, \ldots, m$:

$$0 = g(P_i) = \sum_{j=1}^{m} a_j f_j(P_i) = a_i f_i(P_i) + \sum_{j \neq i} a_j f_j(P_i) = a_i \cdot 1 + 0 = a_i.$$

Hermed er det vist, at $\sum_{i=1}^m a_i[f_i] = 0$ hvis og kun hvis $a_i$ for alle $i$. Altså er $[f_1], \ldots, [f_m]$ lineært uafhængige, og $m \leq \dim(\overline{\mathbb{F}_q}[x_1, \ldots, x_n]/I)$. ■

I sætningen antages det, at $V$ er en endelig mængde, for at kunne benytte sætning 3.13, da det så er ækvivalent med punkt (i)-(iv). Dette kan sikres ved at tilføje *field equations* til idealet, dvs. hvis $I = \langle f_1, \ldots, f_t \rangle$, så sættes $I' = \langle f_1, \ldots, f_t, x_1^q - x_1, \ldots, x_n^q - x_n \rangle$. Dermed er $x_i^{m_i} \in \langle \text{LT}(I) \rangle$, hvor $m_i = q$ for alle $i$, hvilket opfylder punkt (i) i sætning 3.13.

Det kan vises, at hvis et ideal $I$ er radikalt, så gælder der lighedstegn i sætning 3.15, dvs. at $|V(I)| = \dim(\overline{F_q}[x_1, \ldots, x_n]/I) = |\Delta(I)|$. Se (Cox et al., 2007, afsnit 5.3, prop.8) for bevis. Der gælder, at $I'$ er radikal, se (Andersen og Geil, 2008, prop. 39) og $I' \subseteq \overline{\mathbb{F}}_q[x_1, \ldots, x_n]$, hvormed sætningen giver at $|V_{\overline{\mathbb{F}}_q}(I')| = |\Delta(I')|$. Pga. de tilføjede ligninger til $I'$, så er $V_{\overline{\mathbb{F}}_q}(I') = V_{\mathbb{F}_q}(I') = V_{\mathbb{F}_q}(I)$, da $x_i^q = x_i$ medfører at vi bliver i legemet $\mathbb{F}_q$.

Som korollar til sætning 3.13 og 3.15 fås endnu en grænse for antallet af punkter i $V(I)$.

**Korollar 3.16.** Lad $I \subseteq \overline{F_q}[x_1, \ldots, x_n]$ være et ideal, så der for hvert $i$ gælder, at $x_i^{m_i} \in \langle \text{LT}(I) \rangle$. Så er antallet af punkter i $V(I)$ højst $m_1 \cdot m_2 \cdots m_n$. □

**Bevis.** Fra proposition 3.15 fås at antallet af punkter i $V(I)$ er

$$|V| \leq \dim(\overline{\mathbb{F}_q}[x_1, \ldots, x_n]/I) = |\Delta(I)|.$$

Pr. antagelse er $x_i^{m_i} \in \langle \text{LT}(I) \rangle$ for $i = 1, \ldots, n$, og derved er $x_1^{\alpha_i} \cdots x_n^{\alpha_n} \in \langle \text{LT}(I) \rangle$ for alle $\alpha_i \geq m_i$. Dvs. at for monomier i komplementet til $\langle \text{LT}(I) \rangle$ gælder, at $\alpha_i \leq m_i - 1$, så

$$x_1^{\alpha_i} \cdots x_n^{\alpha_n} \in \Delta(I) \Leftrightarrow \alpha_i \in \{0, 1, \ldots, m_i - 1\}.$$

Antal mulige monomier i $\Delta(I)$ er altså $m_1 \cdot m_2 \cdots m_n$, og

$$|V(I)| \leq |\Delta(I)| = m_1 \cdot m_2 \cdots m_n.$$ ■

Grænsen i sætning 3.15 er bedre end i proposition 3.16, hvilket illustreres ved at se på eksempel 3.10. Her er $\langle \text{LT}(I) \rangle = \langle x^3, y^5, xy^4, x^2y^3 \rangle$, dvs. at $m_1 = 3$ og $m_2 = 5$ fordi $x^3, y^5 \in \langle \text{LT}(I) \rangle$. Ifølge proposition 3.16 er størrelsen af $V(I)$ højst $m_1 \cdot m_2 = 15$. I eksemplet så vi, at dimensionen af $\mathbb{F}[x, y]/I$ er 12, og dermed giver sætning 3.15 en bedre grænse.

## 3.2 Ordensfunktioner

Dette afsnit er skrevet på baggrund af (Høholdt et al., 1998, afsnit 3) og (Pellikaan, 2001, afsnit 3-4). På baggrund af en af de foregående ordninger kan man definere en *ordensfunktion*, der måler hvor „stort“ et polynomium er, ved at nummerere monomierne i rækkefølge ud fra den valgte ordning, og se på hvor store monomier der skal bruges for at danne polynomiet. Dette kan gøres på følgende måde. Lad $<$ være en monomiumsordning, som er isomorf med $\mathbb{N}$, og lad $f_1, f_2, \ldots$ være en

nummerering af alle monomierne i $\mathbb{F}[x_1, \ldots, x_n]$, sådan at $f_i < f_{i+1}$ for alle $i$. Disse monomier danner en basis for $\mathbb{F}[x_1, \ldots, x_n]$ over $\mathbb{F}$, da ethvert polynomium $f \in \mathbb{F}[x_1, \ldots, x_n]$ kan skrives entydigt på formen

$$f = \sum_{i=1}^{j} \lambda_i f_i,$$

hvor $\lambda_i \in \mathbb{F}$ for alle $i$ og $\lambda_j \neq 0$.

Nu defineres funktionen $\rho : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{N}_0 \cup \{-\infty\}$, ved at $\rho(0) = -\infty$ og $\rho(f) = j - 1$, hvor $j$ er det mindste positive heltal, så $f$ kan skrives som en linearkombination af $f_1, \ldots, f_j$.

**Eksempel 3.17.** Lad $n = 2$ med $x > y$, og lad $<$ være glex-orden. Så fås en basis for $\mathbb{F}[x, y]$, ved at sætte

$$f_1 = 1, \quad f_2 = y, \quad f_3 = x, \quad f_4 = y^2, \quad f_5 = yx, \quad f_6 = x^2, \ldots$$

Enhver funktion $f \in \mathbb{F}[x, y]$ kan nu udtrykkes som linearkombination af basismonomierne. Se på funktionen

$$f = 2y^2 + x + 3x^2y = 2 \cdot f_4 + f_3 + 3 \cdot f_9.$$

Her er $\rho(f) = j - 1 = 9 - 1 = 8$. □

Denne funktion $\rho$ er en ordensfunktion, som beskrives nærmere i følgende definition.

**Definition 3.18.** Lad $R$ være en $\mathbb{F}$-algebra. En ordensfunktion på $R$ er en afbildning

$$\rho : R \to \mathbb{N}_0 \cup \{-\infty\},$$

som opfylder følgende betingelser for alle $f, g, h \in R$:

1. $\rho(f) = -\infty \Leftrightarrow f = 0$
2. $\rho(\lambda f) = \rho(f)$ for alle $\lambda \in \mathbb{F}^*$
3. $\rho(f + g) \leq \max\{\rho(f), \rho(g)\}$, hvor der gælder lighed når $\rho(f) < \rho(g)$
4. Hvis $\rho(f) < \rho(g)$ og $h \neq 0$, så er $\rho(fh) < \rho(gh)$
5. Hvis $\rho(f) = \rho(g)$, så eksisterer der et $\lambda \in \mathbb{F}^*$, så $\rho(f - \lambda g) < \rho(g)$. □

En funktion $\rho$ som også opfylder

$$\rho(fg) = \rho(f) + \rho(g) \tag{3.3}$$

kaldes en *vægtfunktion*.

En ordensfunktion som opfylder punkt 1, 2 og 3 i definition 3.18 og også opfylder (3.3) kaldes for en *gradfunktion*. Punkt 4 i definition 3.18 følger i dette tilfælde af (3.3), hvilket ses af følgende: Hvis $\rho(f) < \rho(g)$, $h \neq 0$ og (3.3) er opfyldt, så fås

$$\rho(fh) = \rho(f) + \rho(h) < \rho(g) + \rho(h) = \rho(gh),$$

hvormed punkt 4 er opfyldt.

**Eksempel 3.19.** Et simpelt eksempel på en gradfunktion fås ved at tage $R = \mathbb{F}[x_1, \ldots, x_n]$ og $\rho(f) = \deg(f)$, den totale grad af $f$. Så er punkt 1-4 opfyldt og da $\deg(fg) = \deg(f) + \deg(g)$ er også (3.3) opfyldt, hvilket gør $\rho$ til en gradfunktion. To forskellige monomier i flere variable kan dog godt have samme grad. Derfor er $\rho$ kun er ordensfunktion, når $n = 1$, og er dermed også en vægtfunktion, da (3.3) er opfyldt. □

**Lemma 3.20.** Lad $\rho$ være en ordensfunktion på $R$. Så gælder

1. Hvis $\rho(f) = \rho(g)$, så er $\rho(fh) = \rho(gh)$ for alle $h \in R$.
2. Hvis $f \in R$ og $f \neq 0$, så er $\rho(f) \geq \rho(1)$
3. $\mathbb{F} = \{f \in R \mid \rho(f) \leq \rho(1)\}$
4. Hvis $\rho(f) = \rho(g)$, så findes der et entydigt bestemt $\lambda \in \mathbb{F}$ så $\rho(f - \lambda g) < \rho(g)$.

□

**Bevis.** 1. Lad $\rho(f) = \rho(g)$. Så findes der ifølge punkt 5 i 3.18 et ikke-nul $\lambda \in \mathbb{F}$ så $\rho(f - \lambda g) < \rho(g)$. Fra 4 fås, at $\rho(fh - \lambda gh) < \rho(gh)$. Så vha. 3 og 2 er $\rho(fh) = \rho((fh - \lambda gh) + \lambda gh) = \max\{\rho(fh - \lambda < gh), \rho(\lambda gh)\} = \rho(\lambda gh) = \rho(gh)$.

2. Antag modsætningsvist at $f \in R$, $f \neq 0$ og at $\rho(f) < \rho(1)$. Punkt 4 giver dermed, at $\rho(1) > \rho(f) > \rho(f^2) > \cdots$ er en uendelig, strengt aftagende følge. Dette er i modstrid med lemma 1.34, da $<$ er en velordning på $\mathbb{N}_0 \cup -\infty$. Altså må $\rho(f) \geq \rho(1)$.

3. Først vises inklusionen $\mathbb{F} \subseteq \{f \in R \mid \rho(f) \leq \rho(1)\}$. Mængden $\mathbb{F}$ kan skrives som $\mathbb{F} = \{\lambda \cdot 1 \mid \lambda \in \mathbb{F}\}$. Dvs. for $f \in \mathbb{F}$, så er $\rho(f) = \rho(\lambda \cdot 1) = \rho(1)$ for $\lambda \neq 0$, og ellers $\rho(f) = \rho(0) = -\infty < \rho(1)$ vha. punkt 1 og 2. Den modsatte inklusion vises ved at antage, at $f \neq 0$ og $\rho(f) \leq \rho(1)$. I foregående punkt blev vist for $f \neq 0$, at $\rho(f) \geq \rho(1)$, altså må $\rho(f) = \rho(1)$. Ifølge punkt 5 må der findes et $\lambda$ så $\rho(f - \lambda \cdot 1) < \rho(1)$, så $f - \lambda = 0$, dvs. $f = \lambda \in \mathbb{F}$. Hvis $f = 0$, så $f \in F$ pr. definition.

4. Eksistensen fås af punkt 5 i definition 3.18. Entydigheden vises ved at antage, at $\rho(f - \lambda g) < \rho(g)$ og $\rho(f - \mu g) < \rho(g)$ for ikke-nul $\lambda, \mu \in \mathbb{F}$. Vha. punkt 1 og 2, så er $\rho(f - \lambda g - (f - \mu g)) < \max\{\rho(f - \lambda g), \rho(f - \mu g)\} < \rho(g)$ og derfor er $\rho((\lambda - \mu)g) < \rho(g)$. Hvis $\lambda \neq \mu$, så er $\lambda - \mu \in \mathbb{F}$ og $\rho((\lambda - \mu)g) = \rho(g)$, hvilket giver en modstrid. Altså er $\lambda = \mu$ og entydigheden er vist. ■

**Sætning 3.21.**
Hvis der eksisterer en ordensfunktion på $R$, så er $R$ et integritetsområde.

**Bevis.** At $R$ er et integritetsområde vil sige, at der ikke findes nogen nuldivisorer. Dette vises ved modstrid. Antag, at $f, g \in R$, begge forskellige fra nul, og at $fg = 0$. Da $f \neq 0$, så er $\rho(1) \leq \rho(f)$ ifølge lemma 3.20(2). Ved at benytte punkt 4 i definition 3.18 ses, at $\rho(g) \leq \rho(fg) = \rho(0) = -\infty$, og dermed er $g = 0$, hvilket er i modstrid med antagelsen. Altså har $R$ ingen nuldivisorer, og er derfor et integritetsområde. ■

Denne sætning er specielt interessant, fordi det er det første kriterium omkring eksistensen af ordensfunktioner, som bliver behandlet i dette speciale. Sætningen medfører, at hvis $R$ ikke er et integritetsområde, så findes der ikke nogen ordensfunktion på $R$, som det følgende er et simpelt eksempel på.

**Eksempel 3.22.** Lad $R = \mathbb{Z}/4\mathbb{Z}$. Så er $R$ ikke et integritetsområde, da der gælder at $2 \neq 0 \pmod 4$, men $2 \cdot 2 \equiv 0 \pmod 4$. Med samme fremgangsmåde som i beviset for sætning 3.21 ses, at hvis der fandtes en ordensfunktion $\rho$ på $R$, så er $\rho(1) \leq \rho(2)$, hvilket medfører, at $\rho(2) \leq \rho(2 \cdot 2) = \rho(0) = -\infty$, hvilket giver en modstrid. Altså er der ingen ordensfunktion på $R$. □

Sætning 3.21 gælder dog ikke altid den anden vej, så den kan ikke bruges til at sige noget om hvornår der eksisterer en ordensfunktion på $R$. Det kan derimod den sidste af de to følgende sætninger, som også omhandler ordensfunktioner. Den første sætning viser, at givet en ordensfunktion på $R$, så findes et vektorrum og en funktion $l(i, j)$ med særlige egenskaber. Den anden sætning er omvendt - givet en basis for $R$, et vektorrum $L_i$ og en funktion $l(i, j)$ med passende egenskaber, så findes en ordensfunktion på $R$.

**Sætning 3.23.**
Lad $R$ være en $\mathbb{F}$-algebra med ordensfunktion $\rho$. Så gælder der følgende.

1. Antag $R \neq \mathbb{F}$. Så eksisterer der en basis $\{f_i \mid i \in \mathbb{N}\}$ for $R$ over $\mathbb{F}$, sådan at $\rho(f_i) < \rho(f_{i+1})$ for alle $i$.
2. Hvis $i$ er det mindste positive heltal så $f$ kan skrives som en linearkombination af de første $i$ elementer i basen, så gælder der at $\rho(f) = \rho(f_i)$.
3. Lad $l(i, j)$ være det tal $l$, så $\rho(f_i f_j) = \rho(f_l)$. Så er $l(i, j) < l(i + 1, j)$ for alle $i, j$.
4. Lad $\rho_i = \rho(f_i)$. Hvis $\rho$ er en vægtfunktion, så $\rho_{l(i,j)} = \rho_i + \rho_j$.

**Bevis.** Da $R \neq \mathbb{F}$, så findes et $f \in R$ så $f \notin \mathbb{F}$ og ifølge lemma 3.20(3), så er $\rho(1) < \rho(f)$. Fra punkt 4 i def. 3.18 følger dermed at $\rho(f^n) < \rho(f^{n+1})$ for alle $n \in \mathbb{N}_0$, dvs. der findes en uendelig mængde af $\rho$-værdier. Lad nu $\rho_i$ være den strengt voksende følge af de heltal, der optræder som orden $\rho(f)$ af et $f \in R$. For ethvert $i \in \mathbb{N}$ findes altså et $f_i \in R$, så $\rho(f_i) = \rho_i$. Da $\rho_i < \rho_{i+1}$, så gælder for alle $i$, at

$$\rho(f_i) < \rho(f_{i+1}). \tag{3.4}$$

For alle $f \in R$ findes der et $i$, så $\rho(f) = \rho(f_i)$, da $\{\rho_i | i \in \mathbb{N}\}$ består af alle ordensværdier svarende til $\rho(f)$ for $f \in R$.

Det kan nu vises, at $\{f_i \mid i \in \mathbb{N}\}$ er en basis for $R$. Lad $f \in R$, så skal det vises, at $f$ kan skrives som linearkombination af $f_i$'erne. Antag, at $\rho(f) = \rho(f_i)$, dvs. at $f \in L_i \backslash L_{i-1}$. Så eksisterer der ifølge lemma 3.20(4) et $\lambda_i \in \mathbb{F}$, så $\rho(f - \lambda_i f_i) < \rho(f_i) = \rho_i$. Men $f - \lambda_i \in R$, så $\rho(f - \lambda_i f_i) = \rho(f_j)$ for et $j < i$. Igen benyttes 3.20(4) til at vise, at der findes et $\lambda_j \in \mathbb{F}$, så $\rho((f - \lambda_i f_i) - \lambda_j f_j) < \rho(f_j) = \rho_j$. Dette gentages indtil $f - \lambda_i f_i - \lambda_j f_j - \cdots = 0$, hvoraf det ses, at $f = \sum_{k=1}^{i} \lambda_k f_k$, hvor $\lambda_1, \ldots, \lambda_i$ er entydigt bestemte koefficienter. At dette opnås skyldes, at hver gang $\lambda_k f_k$ trækkes fra et polynomium $f \in R$ fås et nyt polynomium i $R$ med samme orden som et af basispolynomierne. Dermed vil enhver rest fra $f$ kunne gå ud ved at trække en konstant gange et $f_i$ fra $f$. Hermed er det første punkt i sætningen bevist.

Lad nu $i$ være det mindste tal, så $f$ er en linearkombination af $f_1, \ldots, f_i$. Så er $f = a_1 f_1 + \cdots + a_i f_i$. Da $\rho$ er en ordensfunktion, benyttes punkt 2 og 3 i def. 3.18 gentagne gange for at få

$$\rho(f) = \rho(a_1 f_1 + \cdots + a_i f_i) = \max\{\rho(f_1), \ldots, \rho(f_i)\} = \rho(f_i),$$

da $\rho(f_j) < \rho(f_{j+1})$ ifølge (3.4), dvs. at $\rho(f_1) < \rho(f_2) < \cdots < \rho(f_i)$.

At $l(i,j)$ er strengt voksende i første argument ses ved at sætte $l_1 := l(i,j)$ og $l_2 := l(i+1,j)$. Der gælder for ordensfunktionen, at $\rho(f_{l_2}) = \rho(f_{i+1} f_j)$. Fra punkt 4 i def. 3.18 fås, at

$$\begin{aligned} \rho(f_i) &< \rho(f_{i+1}) \\ \rho(f_i f_j) &< \rho(f_{i+1} f_j) \\ \rho(f_{l_1}) &< \rho(f_{l_2}) \\ l_1 &< l_2, \end{aligned}$$

da $\rho$ er strengt voksende.

Hvis $\rho$ er en vægtfunktion, så gælder der, at

$$\rho_{l(i,j)} = \rho(f_{l(i,j)}) = \rho(f_i f_j) = \rho(f_i) + \rho(f_j) = \rho_i + \rho_j. \qquad \blacksquare$$

Når $l(i,j)$ er defineret som i sætning 3.23, så kaldes følgen $\{f_i \mid i \in \mathbb{N}\}$ for *well-behaving*, hvis $l(i,j)$ er strengt voksende i begge argumenter. Dermed siger

sætning 3.23, at eksistensen af en ordensfunktion medfører at der finde en følge, som er well-behaving.

I eksempel 3.19 fandt vi, at funktionen $\rho = \deg$ er en ordensfunktion. Den benyttes i det næste eksempel til at illustrere sætning 3.23.

**Eksempel 3.24.** Lad $R = \mathbb{F}[x]$ og lad $\rho$ være gradfunktionen, så $\rho(f) = \deg(f)$. Så er $\rho$ en ordensfunktion ifølge eksempel 3.19. Vi skal nu se, at påstandene fra sætning 3.23 er opfyldt.

1. En basis for $R$ er $\{1, x, x^2, x^3, \ldots\} = \{x^{i-1} \mid i \in \mathbb{N}\}$. Lad $f_i = x^{i-1}$. Så er $\rho(f_i) < \rho(f_{i+1})$ da $\deg(x^{i-1}) < \deg(x^i)$.

2. Se nu på polynomiet $f = 2x^3 + x^2 + 4$. Så er $f = 2 \cdot f_4 + 1 \cdot f_3 + 4 \cdot f_1$, dvs. $i = 4$ da $f$ er en linearkombination af de første 4 elementer i basen. Dermed er $\rho(f) = \deg(f) = 3 = \deg(f_4) = \rho(f_4)$ da $f_4 = x^3$.

3. Definer nu $l(i,j)$ som det tal $l$ så $\deg(f_i f_j) = \deg(f_l)$. Der gælder, at

$$\deg(f_i f_j) = \deg(x^{i-1}x^{j-1}) = \deg(x^{i+j-2}) = i + j - 2 = \deg(f_{i+j-1}).$$

   Altså er $l(i,j) = i+j-1$ og der gælder, at $i+j-1 < (i+1)+j-1 = i+j$, så $l(i,j) < l(i+1,j)$.

4. Til sidst sættes $\rho_i = \rho(f_i)$. Så er $\rho_{l(i,j)} = \deg(f_{l(i,j)}) = \deg(f_i f_j) = \deg(f_i) + \deg(f_j)$. Dermed er $\rho_{l(i,j)} = \rho_i + \rho_j$, hvilket stemmer overens med at $\rho$ er en vægtfunktion, som fundet i eksempel 3.19.

Heraf ses det, hvordan de fire punkter fra sætning 3.23 er opfyldt i forbindelse med gradfunktionen $\deg(f)$, når $f \in \mathbb{F}[x]$. □

I den følgende sætning bevises det omvendte af sætning 3.23. Sætningen giver altså et bud på hvornår der eksisterer ordensfunktioner på en $\mathbb{F}$-algebra $R$, nemlig når der findes en basis for $R$, som er well-behaving.

**Sætning 3.25.**
Antag følgende

- Lad $R$ være en $\mathbb{F}$-algebra.
- Lad $\{f_i \mid i \in \mathbb{N}\}$ være basis for $R$ med $f_1 = 1$.
- Lad $L_i$ være et vektorrum over $\mathbb{F}$ genereret af $f_1, f_2, \ldots, f_i$.
- Lad $l(i,j)$ være det mindste positive heltal $l$, så $f_i f_j \in L_l$ og antag, at $l(i,j) < l(i+1,j)\ \forall\ i,j \in \mathbb{N}$.

Definer nu en funktion $\rho$. Lad $\{\rho_i | i \in \mathbb{N}\}$ være en strengt voksende følge med $\rho_i \in \mathbb{N}_0$. Sæt $\rho(0) = -\infty$ og $\rho(f) = \rho_i$ hvis $i$ er det mindste positive heltal så $f \in L_i$. Da er $\rho$ en ordensfunktion på $R$.

Hvis derudover $\rho_{l(i,j)} = \rho_i + \rho_j$, så er $\rho$ en vægtfunktion.

**Bevis.** Først vises, at $\rho$ opfylder punkt 1, 2, 3 og 5 i definition 3.18. Punkt 4 kræver lidt mere arbejde.
1) Pr. definition er $\rho(0) = -\infty$ og $\rho(f) = \rho_i$, hvor $\rho_i$ er strengt voksende, dvs. $\rho(f) > \rho(0) = -\infty$. Dermed er $\rho(f) = -\infty \Leftrightarrow f = 0$.
2) Da $L_i$ er et vektorrum over $\mathbb{F}$, så gælder $f \in L_i \Leftrightarrow \lambda f \in L_i$ for $\lambda \in \mathbb{F}$. Altså $\rho(f) = \rho(\lambda f)$ for $\lambda \in \mathbb{F}$.
3) Lad $f \in L_i$, $g \in L_j$ og antag uden tab af generalitet, at $i \leq j$. Så er $\rho(f) = \rho_i \leq \rho_j = \rho(g)$. Da $L_i \subseteq L_j$, så er $f \in L_i \subseteq L_j$, så $f, g \in L_j$ og da $L_j$ er et vektorrum, så er $f + g \in L_j$, dvs.

$$\rho(f + g) \leq \rho_j = \rho(g) = \max\{f, g\}. \tag{3.5}$$

Vi mangler nu blot at vise, at der gælder lighed, når $\rho(f) < \rho(g)$. Lad

$$f = \sum_{k=1}^{i} a_k f_k \qquad g = \sum_{k=1}^{j} b_k f_k.$$

Når $\rho_i = \rho(f) < \rho(g) = \rho_j$, så er

$$f + g = b_j f_j + \sum_{k=1}^{m} c_k f_k, \quad \text{hvor } m < j.$$

Altså er $\rho(f + g) \geq \rho_j = \rho(g)$, hvormed der gælder lighedstegn i (3.5).
5) Lad $\rho(f) = \rho(g)$. Så er $f, g \in L_j$ og ikke i $L_i$ for $i < j$. Altså kan $f$ og $g$ opskrives som

$$f = \sum_{k=1}^{j-1} \mu_k f_k + \mu f_j \quad \text{og} \quad g = \sum_{k=1}^{j-1} \nu_k f_k + \nu f_j.$$

Sæt nu $\lambda = \frac{\mu}{\nu}$. Hermed fås, at

$$\begin{aligned} f - \lambda g &= \sum_{k=1}^{j-1} \lambda_k f_k + (\mu - \frac{\mu}{\nu}\nu) f_j \\ &= \sum_{k=1}^{j-1} \lambda_k f_k, \end{aligned}$$

altså

$$f - \lambda g \in L_i \text{ for et } i < j$$
$$\Rightarrow \rho(f - \lambda g) < \rho(g).$$

4) For at $\rho$ opfylder dette punkt, skal vises, at hvis $\rho(f) < \rho(g)$ og $h \neq 0$, så er $\rho(fh) < \rho(gh)$. Strategien i beviset er at se på en funktion som minder om $\rho$, nemlig $\iota(f)$, som sættes til at være det mindste positive heltal så $f \in L_{\iota(f)}$. Altså svarer $\iota(f)$ til $i$ mht $\rho_i$, sådan at $\rho(f) = \rho_i = \rho_{\iota(f)}$. Det skal nu vises, at $\iota(fh) < \iota(gh)$ for $\iota(f) < \iota(g)$.

Først vises, at $\iota(fh) = l(\iota(f), \iota(h))$, ved at se på koefficienterne til $fg = \sum \mu_l f_l$.

Lad $f, g$ være ikke-nul elementer i $R$. Så er

$$f = \sum_{i \leq \iota(f)} \lambda_i f_i, \quad g = \sum_{j \leq \iota(g)} \nu_j f_j, \quad fg = \sum_{l \leq \iota(fg)} \mu_l f_l,$$

med $\lambda_{\iota(f)} \neq 0$, $\nu_{\iota(g)} \neq 0$ og $\mu_{\iota(fg)} \neq 0$, fordi $f$ er i $L_{\iota(f)}$ og ikke i $L_{\iota(f)}$ per definition af $\iota$.

Fra definitionen af $l(i,j)$ fås, at $f_i f_j \in L_{l(i,j)} \backslash L_{l(i,j)-1}$. Derfor eksisterer der et $\mu_{ijl} \in \mathbb{F}$, så $f_i f_j = \sum_{l \leq l(i,j)} \mu_{ijl} f_l$ og $\mu_{ijl(i,j)} \neq 0$.

Der ses nu på koefficienten til $f_l$ i polynomiet

$$fg = \sum_{l \leq \iota(fg)} \mu_l f_l. \tag{3.6}$$

Der gælder også om dette polynomium, at

$$fg = (\sum_{i \leq \iota(f)} \lambda_i f_i)(\sum_{j \leq \iota(g)} \nu_j f_j) \tag{3.7a}$$
$$= \sum_{\substack{i \leq \iota(f) \\ j \leq \iota(g)}} \lambda_i \nu_j f_i f_j \tag{3.7b}$$
$$= \sum_{\substack{i \leq \iota(f) \\ j \leq \iota(g)}} \lambda_i \nu_j \sum_{l \leq l(i,j)} \mu_{ijl} f_l \tag{3.7c}$$
$$= \sum_{\substack{i \leq \iota(f) \\ j \leq \iota(g) \\ l \leq l(i,j)}} \lambda_i \nu_j \mu_{ijl} f_l. \tag{3.7d}$$

Så koefficienten til $f_l$ er altså

$$\mu_l = \sum_{l(i,j)=l} \lambda_i \nu_j \mu_{ijl}.$$

Det største led i (3.7d) fås for $l = l(\iota(f), \iota(g))$, da $l(i,j)$ er strengt voksende i begge argumenter, så $l(i,j) < l(\iota(f), \iota(g))$ for $i < \iota(f)$, $j < \iota(g)$. Koefficienterne

til $f_{l(\iota(f),\iota(g))}$ fås for $i = \iota(f)$ og $j = \iota(g)$, og da $\lambda_i \nu_j \mu_{ijl(i,j)} \neq 0$ for $i = \iota(f)$ og $j = \iota(g)$, så ses at $\mu_{l(\iota(f),\iota(g))}$ er koefficienten til det største led i $fg$. Fra (3.6) ses at $\mu_{\iota(fg)}$ også er koefficienten til det største led i $fg$, hvoraf fås, at

$$l(\iota(f), \iota(g)) = \iota(fg).$$

Da $l(i,j)$ er strengt voksende, så fås for $\iota(g) < \iota(h)$ :

$$\iota(fg) = l(\iota(f), \iota(g)) < l(\iota(f), \iota(h)) = \iota(fh).$$

Da $\rho(f) = \rho_{\iota(f)}$ og $\rho_i$ er strengt voksende, så følger at

$$\rho(fg) = \rho_{\iota(fg)} < \rho_{\iota(fh)} = \rho(fh)$$

for $\iota(g) < \iota(h)$ og dermed også for $\rho(g) < \rho(h)$. Hermed er det vist, at $\rho$ er en ordensfunktion på $R$.

Hvis der også gælder, at $\rho_{l(i,j)} = \rho_i + \rho_j$, så medfører det, at

$$\rho(fg) = \rho_{\iota(fg)} = \rho_{l(\iota(f),\iota(g))} = \rho_{\iota(f)} + \rho_{\iota(g)} = \rho(f) + \rho(g),$$

hvoraf det ses, at $\rho$ er en vægtfunktion. ■

**Eksempel 3.26.** Lad $R = \mathbb{F}[x_1, \ldots, x_n]$. Ved hjælp af 3.25 kan det vises, at $R$ har en ordensfunktion.

Lad $<$ være en monomiumsordning som er isomorf med den normale ordning på $\mathbb{N}$. Så kan monomierne i $\mathbb{F}[x_1, \ldots, x_n]$ ordnes i følgen $(M_i \mid i \in \mathbb{N})$, sådan at $M_i < M_{i+1}$ for alle $i$. For alle $i, j$ findes der et $l(i,j)$, sådan at $M_i M_j = M_{l(i,j)}$. Funktionen $l(i,j)$ er strengt voksende, da $M_i$ danner en strengt voksende følge, og da $<$ er en monomiumsordning, dvs.

$$M_i < M_{i+1} \Leftrightarrow M_i M_j < M_{i+1} M_j \Leftrightarrow M_{l(i,j)} < M_{l(i+1,j)} \Leftrightarrow l(i,j) < l(i+1,j).$$

Dermed er $(M_i \mid i \in \mathbb{N})$ en well-behaving følge og antagelserne til sætning 3.25 er opfyldt. Derfor findes en ordensfunktion på $R = \mathbb{F}[x_1, \ldots, x_n]$. □

I det følgende kommer et par eksempler på anvendelse af teorien i dette afsnit.

**Eksempel 3.27.** Se på den graderede leksikografiske orden med $m = 2$ og $R = \mathbb{F}[x, y]$. Så er $\{x^\alpha y^\beta \mid \alpha, \beta \in \mathbb{N}_0\}$ en basis for $R$. Monomierne kan nu indtegnes i et skema og nummereres i hht. glex-orden:

| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋱ |
|---|---|---|---|---|---|
| $y^6$ | · | · | · | · | ... |
| $y^5$ | $xy^5$ | · | · | · | ... |
| $y^4$ | $xy^4$ | $x^2y^4$ | · | · | ... |
| $y^3$ | $xy^3$ | $x^2y^3$ | $x^3y^3$ | · | ... |
| $y^2$ | $xy^2$ | $x^2y^2$ | $x^3y^2$ | · | ... |
| $y$ | $xy$ | $x^2y$ | $x^3y$ | $x^4y$ | ... |
| 1 | $x$ | $x^2$ | $x^3$ | $x^4$ | ... |

| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋱ |
|---|---|---|---|---|---|
| 22 | · | · | · | · | ... |
| 16 | 23 | · | · | · | ... |
| 11 | 17 | 24 | · | · | ⋯ |
| 7 | 12 | 18 | 25 | · | ⋯ |
| 4 | 8 | 13 | 19 | · | ⋯ |
| 2 | 5 | 9 | 14 | 20 | ⋯ |
| 1 | 3 | 6 | 10 | 15 | 21 |

Det ses på figuren at nummereringen sker langs med diagonalerne fra øverst til venstre mod nederst til højre. Vi vælger nu to elementer i basen, $f_4 = y^2$ og $f_9 = x^2y$. Så ses det på figuren, at $f_4 f_9 = x^2y^3 = f_{18}$, så $l(4,9) = 18$. □

Med vægtet graderet ordning bliver nummereringen af elementerne mindre oplagt, som det ses i næste eksempel.

**Eksempel 3.28.** I dette eksempel ses på vægtet lex-orden med $m = 2$ og $\mathbf{w} = (4,5)$. Så er $\text{wdeg}(x) = 4, \text{wdeg}(y) = 5$. Lad $R = \mathbb{F}[x,y]$ med $\{x^\alpha y^\beta \mid \alpha, \beta \in \mathbb{N}_0\}$ som basis. Så kan den vægtede grad af elementerne i basen ses i skemaerne sammen med den tilhørende nummerering:

| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋱ |
|---|---|---|---|---|---|---|
| 25 | · | · | · | · | · | ... |
| 20 | 24 | · | · | · | · | ... |
| 15 | 19 | 23 | · | · | · | ⋯ |
| 10 | 14 | 18 | 22 | · | · | ⋯ |
| 5 | 9 | 13 | 17 | 21 | 25 | ⋯ |
| 0 | 4 | 8 | 12 | 16 | 20 | 24 |

| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋮ | ⋱ |
|---|---|---|---|---|---|---|
| 22 | · | · | · | · | · | ... |
| 15 | 20 | · | · | · | · | ... |
| 10 | 14 | 19 | · | · | · | ⋯ |
| 6 | 9 | 13 | 18 | · | · | ⋯ |
| 3 | 5 | 8 | 12 | 17 | 23 | ⋯ |
| 1 | 2 | 4 | 7 | 11 | 16 | 21 |

Som det ses på figuren har flere af basiselementerne samme vægtede grad, fx. $x^6$ og $xy^4$ som begge har vægtet grad 24. Men når de har samme grad, så ordnes efter leksikografisk orden, så $xy^4 <_w x^6$, og derfor er $f_{20} = xy^4$ mens $f_{21} = x^6$. □

I det næste eksempel arbejdes der over kvotientringen $R/I$.

**Eksempel 3.29.** Betragt den *Hermitiske kurve* over $\mathbb{F}_q$: $x^{r+1} - y^r - y = 0$ med $q = r^2$. Lad $r = 4$ og $R = \mathbb{F}_{16}[x,y]/\langle x^5 - y^4 - y \rangle$. Så er $\{x^\alpha y^\beta \mid \alpha < 5\}$ en basis for $R$. Lad som i foregående eksempel $\mathbf{w} = (4,5)$, så $\text{wdeg}(x^\alpha y^\beta = 4\alpha + 5\beta$. For basiselementerne gælder der her at $x$ ikke har nogen eksponenter større end 4, hvilket giver følgende fordeling af vægt og nummerering:

| | | | | |
|---|---|---|---|---|
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| $y^4$ | · | · | · | · |
| $y^3$ | $xy^3$ | · | · | · |
| $y^2$ | $xy^2$ | $x^2y^2$ | · | · |
| $y$ | $xy$ | $x^2y$ | $x^3y$ | $x^4y$ |
| 1 | $x$ | $x^2$ | $x^3$ | $x^4$ |

| | | | | |
|---|---|---|---|---|
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 20 | · | · | · | · |
| 15 | 19 | · | · | · |
| 10 | 14 | 18 | · | · |
| 5 | 9 | 13 | 17 | 21 |
| 0 | 4 | 8 | 12 | 16 |

| | | | | |
|---|---|---|---|---|
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 15 | · | · | · | · |
| 10 | 14 | · | · | · |
| 6 | 9 | 13 | · | · |
| 3 | 5 | 8 | 12 | 16 |
| 1 | 2 | 4 | 7 | 11 |

Her ses det, at nummereringen af monomierne igen foretages langs med diagonalerne, men denne gang omvendt, fra højre mod venstre. Nu vælges to monomier $f_2 = x$ og $f_{11} = x^4$. Så er $f_2 f_{11} = x^5$, men da udregningerne foretages i kvotientringen $\mathbb{F}_{16}[x,y]/\langle x^5 - y^4 - y \rangle$, så er $x^5 = y^4 + y$. Dvs. $f_2 f_{11} = y^4 + y = f_{15} + f_3$, så $l(2,11) = 15$. Senere vil det blive vist, at $\rho = \text{wdeg}$ er en vægtfunktion på $R$. Vægtene kan aflæses på skemaet, og er $\rho_1 = 0, \rho_2 = 4, \rho_3 = 5, \rho_4 = 8$ etc. Faktisk gælder der, at $\rho_l = l + 5$ for $l \geq 7$, hvilket også kan ses på figuren.

Princippet gælder for alle monomier i basen. Se på $l(7,8)$. $f_7 = x^3$ og $f_8 = x^2 y$. Så er $f_7 f_8 = x^5 y = (y^4 + y)y = y^5 + y^2 = f_{20} + f_6$. Altså er $l(7,8) = 20$. □

## 3.3 Evalueringskoder

Det følgende er skrevet på baggrund af (Høholdt et al., 1998, kap. 4). I dette afsnit bliver evalueringskoderne, samt deres dualer introduceret. Derudover bliver der set på grænser for minimumsafstanden af dualkoderne.

Inden koderne bliver defineret, opsummeres først nogle af de antagelser, som vil blive benyttet gennem resten af kapitlet, hvor der blandt andet benyttes en del af teorien omkring ordensfunktioner fra sidste afsnit.

- Lad $R$ være en $\mathbb{F}_q$-algebra med ordensfunktion $\rho$.
- Lad $\{f_i \mid i \in \mathbb{N}\}$ være en basis for $R$ over $\mathbb{F}_q$, sådan at

  $$\rho(f_i) < \rho(f_{i+1}) \ \forall \ i \in \mathbb{N}, \ f \in R.$$

  Sætning 3.23 garanterer, at der for alle $f \in R$ eksisterer et $j$, så $\rho(f) = \rho(f_j) =: \rho_j$.
- Lad $L_l$ være et vektorrum over $\mathbb{F}_q$ genereret af $f_1, f_2, \ldots, f_l$. Så gælder for $f \in R$ at $\rho(f) = \rho(f_l)$ hvis og kun hvis $l$ er det mindste positive heltal så $f \in L_l$.
- Lad $l(i,j)$ være det mindste positive heltal så $f_i f_j \in L_{l(i,j)}$. Så er

  $$l(i,j) < l(i+1,j) \ \forall \ i,j \in \mathbb{N},$$

  dvs. at følgen er well-behaving.

- Lad $\varphi$ være en afbildning $\varphi : R \to \mathbb{F}_q^n$. Så er $\varphi$ en *homomorfi* af $\mathbb{F}_q$-algebraer, hvis der gælder

  1. $\varphi(\lambda f) = \lambda\varphi(f)$ for $f \in R, \lambda \in \mathbb{F}_q$,
  2. $\varphi(f+g) = \varphi(f) + \varphi(g)$, for $f, g \in R$,
  3. $\varphi(fg) = \varphi(f) * \varphi(g)$, hvor $a * b = (a_1b_1, \ldots, a_nb_n)$ for $a = (a_1, \ldots, a_n)$ og $b = (b_1, \ldots, b_n)$,

  hvor punkt 1 og 2 medfører $\mathbb{F}_q$-linearitet.

Med disse antagelser på plads er grunden lagt for at definere evalueringskoderne.

**Definition 3.30.** Lad $\varphi$ være en homomorfi af $\mathbb{F}_q$-algebraer og lad $\mathbf{h}_i = \varphi(f_i)$. Da defineres *evalueringskoden* $E_l$ og dens dual $C_l$ til at være:

$$E_l = \varphi(L_l) = \langle \mathbf{h}_1, \ldots, \mathbf{h}_l \rangle \subseteq \mathbb{F}_q^n$$

og

$$C_l = \{\mathbf{c} \in \mathbb{F}_q^n \mid \mathbf{c} \cdot \mathbf{h}_i = 0 \ \forall\ i \leq l\} \subseteq \mathbb{F}_q^n. \qquad \square$$

Det ses altså at funktionen $\varphi$ sender vektorrummet $L_l$ over i et ideal over $F_q$ som danner evalueringskoden. Der gælder om koderne, at

$$E_1 \subseteq E_2 \subseteq E_3 \subseteq \cdots \quad \text{og} \quad C_1 \supseteq C_2 \supseteq C_3 \supseteq \cdots$$

Men $E_i \subseteq \mathbb{F}_q^n$ for alle $i$, så $E_i$ er altså en endelig følge af koder, hvor der eksisterer et $N$, så $E_l = E_N$ for alle $l \geq N$. Der gælder, at $E_N = \varphi(R)$. Her vil vi kun beskæftige os med surjektive funktioner $\varphi$, hvormed hele $F_q^n$ rammes. Dette medfører, at $E_l = \mathbb{F}_q^n,\ \forall\ l \geq N$ og $C_l = 0,\ \forall\ l \geq N$.

I næste eksempel ses på evalueringsafbildningen $ev$.

**Eksempel 3.31.** Lad $\mathcal{P} = \{P_1, \ldots, P_n\}$ være en mængde af punkter i $\mathbb{F}^m$. Lad $R = \mathbb{F}[x_1, \ldots, x_m]$ og se på *evalueringsafbildningen*:

$$ev_{\mathcal{P}} : R \to \mathbb{F}^n, \text{ hvor } ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n)).$$

Afbildningen er $\mathbb{F}$-lineær og $fg(P) = f(P)g(P)$ for alle polynomier $f, g$ og punkter $P$, dvs.

$$\begin{aligned} ev_{\mathcal{P}}(fg) &= (fg(P_1), \ldots, fg(P_n)) \\ &= (f(P_1)g(P_1), \ldots, f(P_n)g(P_n)) \\ &= (f(P_1), \ldots, f(P_n)) * (g(P_1), \ldots, g(P_n)) \\ &= ev_{\mathcal{P}}(f) * ev_{\mathcal{P}}(g). \end{aligned}$$

Dermed er $ev_{\mathcal{P}}$ en homomorfi af $\mathbb{F}$-algebraer.

Der gælder også, at $ev_{\mathcal{P}}$ er surjektiv. Dette vises ved at konstruere polynomier i $R$ som afbilder over i basiselementerne i $\mathbb{F}^n$, $(1, 0, \ldots)$, $(0, 1, 0, \ldots), \ldots, (0, \ldots, 0, 1)$,

for derved rammes hele $\mathbb{F}^n$. Mængden $\mathcal{P}$ består af punkterne $P_1, \ldots, P_n \in \mathbb{F}^m$, hvor $P_j = (a_{j1}, \ldots, a_{jm})$. Lad $A_{il} = \{a_{jl} \mid j = 1, \ldots, n\} \backslash \{a_{il}\}$ og definér et polynomium $G_i \in R$,

$$\begin{aligned} G_i &= \prod_{l=1}^{m} \prod_{a \in A_{il}} (x_l - a) \\ &= (x_1 - a_{11})(x_1 - a_{21}) \cdots (x_1 - a_{(i-1)1})(x_1 - a_{(i+1)1}) \cdots (x_m - a_{nm}). \end{aligned}$$

Så er $G_i(P_j) = 0$ for alle $i \neq j$. Dette ses af, at $(x_l - a_{jl})$ optræder i $G_i$, dvs. når $P_j$ indsættes, så bliver $(x_l - a_{jl}) = (a_{jl} - a_{jl}) = 0$, så $G_i(P_j) = 0$. For $i = j$ fås, at $G_i(P_i) \neq 0$, da $(x_l - a_{jl})$ ikke optræder i $G_I$ og da punkterne $P_1, \ldots, P_n$ er forskellige, så alle faktorerne $(x_l - a_{jl}) = (a_{il} - a_{jl}) \neq 0$, da $a_{il} \notin A_{il}$.

Altså ses, at $ev_{\mathcal{P}}(G_i) = (0, \ldots, 0, G_i(P_i), 0, \ldots, 0)$, hvor elementet på den $i$'te plads er $G_i(P_i) \neq 0$. Så polynomiet $G_i/G_i(P_i)$ bliver afbildet ind i det $i$'te standard-basiselement for $\mathbb{F}^n$, og $ev_{\mathcal{P}}$ er dermed surjektiv. □

Hvis vi i eksemplet ændrer $R$ til kvotientringen $\mathbb{F}[x_1, \ldots, x_m]/I$, så fås en veldefineret lineær afbildning $ev_{\mathcal{P}}$.

**Eksempel 3.32.** Lad $I$ være et ideal i $\mathbb{F}[x_1, \ldots, x_m]$ og lad $P_1, \ldots, P_n$ være punkter i $V(I)$ med $P_i \in \mathbb{F}^m$. Så er $f(P_j) = 0$ for $j = 1, \ldots, n$ og for $f \in I$. Dermed er

$$ev_{\mathcal{P}} : \mathbb{F}[x_1, \ldots, x_m]/I \to \mathbb{F}^n$$

en veldefineret lineær afbildning, som også er en surjektiv homomorfi, hvilket ses af samme udregninger som i foregående eksempel.

For at se, at afbildningen er veldefineret, vises at hvis $[f]$ og $[g]$ afbildes over i samme element i $\mathbb{F}^n$, så er $[f] = [g]$ i $\mathbb{F}[x_1, \ldots, x_m]/I$. Antag altså at $ev_{\mathcal{P}}(f) = ev_{\mathcal{P}}(g)$. Da $f(P_j) = 0$ for alle $j$ hvis og kun hvis $f \in I$, medfører det at

$$f(P_i) = g(P_i) \Rightarrow (f - g)(P_i) = 0 \Rightarrow (f - g) \in I \Rightarrow f \equiv g \pmod{I},$$

for $i = 1, \ldots, n$. Dermed er $ev_{\mathcal{P}}$ veldefineret. □

### 3.3.1 Sammenhæng mellem kvotientringe og evalueringskoder

Sætning 3.15 og 3.16 er vigtige i forbindelse med evalueringskoder, da de siger noget om længden af koden. Lad $I \subseteq \mathbb{F}_q[x_1, \ldots, x_m]$ være et ideal og se på evalueringskoden givet ved afbildningen

$$ev_{\mathcal{P}} : \mathbb{F}_q[x_1, \ldots, x_m]/I \to \mathbb{F}_q^n, \text{ med } f \mapsto (f(P_1), \ldots, f(P_n)),$$

hvor $P_i \in V(I)$. Længden af koden er $n$ og afhænger af antallet af punkter i $V(I)$. Dette er ifølge sætning 3.15 højest lig med dimensionen af $\mathbb{F}_q[x_1, \ldots, x_m]/I$, så

$$n \leq |V(I)| \leq \dim(\mathbb{F}_q[x_1, \ldots, x_m]/I) = |\Delta(I)|.$$

Det er ikke et krav at man evaluerer i alle punkterne i $V(I)$, men det er ofte tilfældet, og i så fald er $n = |V(I)|$.

Hvis $I = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_m]$, så tilføjes field equations så $I' = \langle f_1, \ldots, f_s, x_1^q - x_1, \ldots, x_m^q - x_m \rangle \subseteq \mathbb{F}_q[x_1, \ldots, x_m] \subseteq \overline{\mathbb{F}}_q[x_1, \ldots, x_m]$. Da er $I'$ radikal, og når der evalueres i alle punkter i $V(I)$, så er $n = |V_{\mathbb{F}_q}(I)| = |\Delta(I')|$, jf. udregningerne efter sætning 3.15.

### 3.3.2 Syndromer

Med samme antagelser som nævnt i starten af afsnittet, vil vi nu definere syndromer og syndrommatricer. Lad $N$ være det tal, så $E_l = \mathbb{F}_q^n$, $\forall\ l \geq N$ og $C_l = 0$, $\forall\ l \geq N$. Så sættes $\mathbf{H}$ til at være den $N \times n$ matrix der har $\mathbf{h}_i$ som den $i$'te række for $1 \leq i \leq N$.

**Definition 3.33.** Lad $\mathbf{y} \in \mathbb{F}_q^n$. Så defineres *syndromerne*

$$s_i(\mathbf{y}) = \mathbf{y} \cdot \mathbf{h}_i \quad \text{og} \quad s_{ij}(\mathbf{y}) = \mathbf{y} \cdot (\mathbf{h}_i * \mathbf{h}_j).$$

*Syndrommatricen* for $\mathbf{y}$ defineres som

$$\mathbf{S}(\mathbf{y}) = (s_{ij}(\mathbf{y}) \mid 1 \leq i, j \leq N). \qquad \square$$

Syndrommatricen vil senere blive benyttet til at bevise nogle grænser for minimumsafstanden for en kode. Som det ses i næste lemma er nemlig rangen af syndrommatricen til en vektor $\mathbf{y}$ lig med vægten af $\mathbf{y}$.

**Lemma 3.34.** Lad $\mathbf{y} \in \mathbb{F}_q^n$. Lad $\mathbf{D}(\mathbf{y})$ være diagonalmatricen med $\mathbf{y}$ på diagonalen. Så er

$$\mathbf{S}(\mathbf{y}) = \mathbf{H}\mathbf{D}(\mathbf{y})\mathbf{H}^T, \tag{3.8}$$

og

$$\operatorname{rang}(\mathbf{S}(\mathbf{y})) = \mathrm{w}(\mathbf{y}). \qquad \square$$

**Bevis.** Hvis matricerne på højresiden ganges sammen fås en matrix, hvor den $i,j$'te indgang er givet ved $\sum_{k=1}^{n} h_{ik} y_k h_{jk}$, hvor $h_{ik}$ er den $k$'te indgang i $\mathbf{h}_i$. Fra definition 3.33 ses, at

$$s_{ij}(\mathbf{y}) = \mathbf{y} \cdot (\mathbf{h}_i * \mathbf{h}_j) = \sum_{k=1}^{n} y_k h_{ik} h_{jk},$$

hvorved (3.8) er vist. Rangen af diagonalmatricen svarer til antallet af pivotelementer, dvs. antal ikke-nul elementer i $\mathbf{y}$, altså $\operatorname{rang}(\mathbf{D}(\mathbf{y})) = \mathrm{w}(\mathbf{y})$. Rækkerne i $\mathbf{H}$ genererer hele $\mathbb{F}_q^n$, da $E_N = \mathbb{F}_q^n$. Dermed har både $\mathbf{H}$ og $\mathbf{H}^T$ fuld rang, hvilket medfører at

$$\operatorname{rang}(\mathbf{S}(\mathbf{y})) = \operatorname{rang}(\mathbf{D}(\mathbf{y})) = \mathrm{w}(\mathbf{y}). \qquad \blacksquare$$

I det følgende bevises to vigtige lemmaer, der bruges til at vise nedre grænser for minimumsafstanden til $C_l$ koderne.

**Lemma 3.35.** Der gælder følgende for syndromerne $s_{ij}(\mathbf{y})$ :

(1) Hvis $\mathbf{y} \in C_l$ og $l(i,j) \leq l$, så er $s_{ij}(\mathbf{y}) = 0$.

(2) Hvis $\mathbf{y} \in C_l \backslash C_{l+1}$ og $l(i,j) = l+1$, så er $s_{ij}(\mathbf{y}) \neq 0$. □

**Bevis.** (1) Lad $\mathbf{y} \in C_l$. Hvis $l(i,j) \leq l$, så er $f_i f_j \in L_l$. Dette ses fordi $l(i,j)$ er det mindste tal, så $f_i f_j \in L_{l(i,j)}$, og $L_{l(i,j)} \subseteq L_l$ når $l(i,j) \leq l$.

Dermed er $\varphi(f_i f_j) \in \varphi(L_l) = E_l$, og da $\varphi$ er en homomorfi, så er $\varphi(f_i f_j) = \varphi(f_i) * \varphi(f_j) = \mathbf{h}_i * \mathbf{h}_j$. Altså er $\mathbf{h}_i * \mathbf{h}_j \in E_l$, dualen til $C_l$. Så $s_{ij}(\mathbf{y}) = \mathbf{y} \cdot (\mathbf{h}_i * \mathbf{h}_j) = 0$, da $\mathbf{y} \in C_l$ og $\mathbf{h}_i * \mathbf{h}_j \in E_l$.

(2) Lad $\mathbf{y} \in C_l \backslash C_{l+1}$. Hvis $l(i,j) = l+1$, så er $f_i f_j \in L_{l+1} \backslash L_l$, da $l+1$ er mindste tal, så $f_i f_j \in L_{l+1}$, dvs. $f_i f_j \notin L_l$. Altså er $\rho(f_i f_j) = \rho(f_{l+1})$. Ser man på $f_i f_j$ modulo $L_l$, så forsvinder alle andre led end det, som indeholder $f_{l+1}$, fordi $f_i f_j = \lambda_1 f_1 + \cdots + \lambda_l f_l + \mu f_{l+1}$, hvor $\mu \neq 0$. Altså er $f_i f_j \equiv \mu f_{l+1} \mod L_l$, for et ikke-nul $\mu \in \mathbb{F}_q$.

Dette medfører ved at tage $\varphi(f_i f_j)$, at

$$\begin{aligned} \varphi(f_i f_j) &\equiv \varphi(\mu f_{l+1}) \mod \varphi(L_l) \\ \mathbf{h}_i * \mathbf{h}_j &\equiv \mu \mathbf{h}_{l+1} \mod \varphi(L_l). \end{aligned}$$

Da $\mathbf{y} \notin C_{l+1}$ og $\mathbf{h}_{l+1} \in E_{l+1}$, så er $s_{l+1}(\mathbf{y}) = \mathbf{y} \cdot \mathbf{h}_{l+1} \neq 0$ og dermed

$$s_{ij}(\mathbf{y}) = \mathbf{y} \cdot (\mathbf{h}_i * \mathbf{h}_j) \equiv \mu \mathbf{y} \cdot \mathbf{h}_{l+1} \mod \varphi(L_l),$$

hvor $\mathbf{y} \cdot \mathbf{h}_{l+1} \neq 0$, hvilket giver, at $s_{ij}(\mathbf{y}) \neq 0$. ■

Til næste lemma er en ny definition nødvendig.

**Definition 3.36.** Lad $l \in \mathbb{N}_0$. Da er

$$N_l = \{(i,j) \in \mathbb{N}^2 \mid l(i,j) = l+1\}.$$

og $\nu_l = |N_l|$, antallet af elementer i mængden $N_l$. □

**Lemma 3.37.** Lad $t = \nu_l$ og lad $(i_1, j_1), \ldots, (i_t, j_t)$ være en nummerering af elementerne i $N_l$ i voksende rækkefølge efter lex-orden på $\mathbb{N}^2$. Da gælder at $i_1 < i_2 < \cdots < i_t$ og $j_1 > j_2 > \cdots > j_t$, dvs. $i$'erne er en strengt voksende følge, mens $j$'erne er strengt aftagende. Ydermere gælder at, hvis $\mathbf{y} \in C_l \backslash C_{l+1}$ så er

$$s_{i_u j_v}(\mathbf{y}) = \begin{cases} 0 & \text{for } u < v \\ \neq 0 & \text{for } u = v. \end{cases}$$ □

**Bevis.** Først vises, at i og j følgerne er henholdsvist strengt voksende og strengt aftagende. Følgen $(i_1, j_1), \ldots, (i_t, j_t)$ er ordnet efter lex-ordning, dvs.

$$i_1 \leq i_2 \leq \cdots \leq i_t \text{ og } j_u < j_{u+1} \text{ hvis } i_u = i_{u+1}.$$

Det vises nu ved modstrid, at følgen er strengt voksende. Antag modsætningsvist, at $i_u = i_{u+1}$. Så er $j_u < j_{u+1}$, men så

$$l + 1 = l(i_u, j_u) < l(i_u, j_{u+1}) = l(i_{u+1}, j_{u+1}) = l + 1,$$

hvor første og sidste lighedstegn kommer af definitionen af $N_l$, hvor $(i_u, j_u)$ er et vilkårligt element i $N_l$. Uligheden følger af definitionen af $l(i, j)$, som er strengt voksende i begge indgange. Dette giver en modstrid. Antagelsen $i_u = i_{u+1}$ må altså være forkert, dvs. $i_u < i_{u+1}$.

Samme fremgangsmåde benyttes til at vise at $j_1, \ldots, j_t$ er en strengt aftagende følge. Antag først, at $j_u = j_{u+1}$ og $i_u < i_{u+1}$, hvilket medfører

$$l + 1 = l(i_u, j_u) < l(i_{u+1}, j_u) = l(i_{u+1}, j_{u+1}) = l + 1,$$

som giver en modstrid. Lad i stedet $j_u < j_{u+1}$ og $i_u < i_{u+1}$, så

$$l + 1 = l(i_u, j_u) < l(i_{u+1}, j_u) < l(i_{u+1}, j_{u+1}) = l + 1,$$

hvilket igen er en modstrid. Altså må der gælde, at $j_u > j_{u+1}$ for alle $u < t$. Hermed er første del af sætningen bevist.

Lad nu $\mathbf{y} \in C_l$. Hvis $u < v$, så er $l(i_u, j_v) < l(i_v, j_v) = l+1$, dvs. at $l(i_u, j_v) \leq l$, og fra lemma 3.35 fås, at $s_{i_u j_v}(\mathbf{y}) = 0$.

Lad endvidere $\mathbf{y} \notin C_{l+1}$. Hvis $u = v$, så er $l(i_u, j_v) = l(i_v, j_v) = l + 1$, så fra lemma 3.35 fås, at $s_{i_u j_v}(\mathbf{y}) \neq 0$, da $\mathbf{y} \in C_l \backslash C_{l+1}$. ■

Den næste sætning sætter en grænse for vægten af et kodeord i $C_l \backslash C_{l+1}$.

**Sætning 3.38.**
Hvis $\mathbf{y} \in C_l \backslash C_{l+1}$, så er $\mathrm{w}(\mathbf{y}) \geq \nu_l$.

**Bevis.** Lad $t = \nu_l$. Fra lemma 3.34 haves, at $\mathrm{w}(\mathbf{y}) = \mathrm{rang}\,(S(\mathbf{y}))$, dvs. antallet af pivotelementer i $S(\mathbf{y})$. Når $\mathbf{y} \in C_l \backslash C_{l+1}$, så ses vha. lemma 3.37, at

$$s_{i_u j_v}(\mathbf{y}) = \begin{cases} 0 & \text{for } u < v \\ \neq 0 & \text{for } u = v, \end{cases}$$

dvs. at $s_{i_u j_v}(\mathbf{y}) \neq 0$ for $(i_u, j_u) \in N_l$. $S(\mathbf{y})$ er altså en matrix, hvor $(i_u, j_u) \in N_l$ er pivotelementer, altså er der mindst $t$ pivotelementer. For $u, v > t$ ved vi intet, så matricen kan evt. have større rang. Så altså fås, at

$$\mathrm{rang}(S(\mathbf{y})) \geq t = \nu_l \Rightarrow \mathrm{w}(\mathbf{y}) \geq \nu_l.$$ ■

Nu introduceres to grænser for minimumsafstanden af en kode $C_l$. Først defineres $\mathrm{d}(l)$ og $\mathrm{d}_\varphi(l)$.

**Definition 3.39.**

$$\mathrm{d}(l) = \min\{\nu_m \mid m \geq l\} \tag{3.9}$$

$$\mathrm{d}_\varphi(l) = \min\{\nu_m \mid m \geq l, C_m \neq C_{m+1}\}. \tag{3.10}$$

□

Herefter vises at de to størrelser er nedre grænser for minimumsafstanden til en evalueringskode.

**Sætning 3.40.**
$\mathrm{d}(l)$ og $\mathrm{d}_\varphi(l)$ er nedre grænser for minimumsafstanden til $C_l$, da

$$\mathrm{d}(C_l) \geq \mathrm{d}_\varphi(l) \geq \mathrm{d}(l).$$

**Bevis.** Minimumsafstanden for koden er $\mathrm{d}(C_l) = \min\{\mathrm{w}(\mathbf{y}) \mid \mathbf{y} \in C_l\}$. Fra sætning 3.38 ved vi, at $\mathrm{w}(\mathbf{y}) \geq \nu_l$ for $\mathbf{y} \in C_l \backslash C_{l+1}$. Da

$$C_l = \{C_l \backslash C_{l+1}\} \cup \{C_{l+1} \backslash C_{l+2}\} \cup \cdots \cup C_N, \text{ hvor } C_N = 0$$

så er

$$\mathrm{d}(C_l) \geq \min\{\nu_l, \nu_{l+1}, \ldots, \nu_{N-1}\} = \min\{\nu_m \mid m \geq l\} = \mathrm{d}(l).$$

Ved at benytte samme fremgangsmåde for $\mathrm{d}_\varphi(l)$, fås at

$$\mathrm{d}(C_l) \geq \mathrm{d}_\varphi(l).$$

Da vi fraregner koderne $C_m$ hvor $C_m = C_{m+1}$, så vil $\mathrm{d}_\varphi(l) \geq \mathrm{d}(l)$, da mængden $\{\nu_m \mid m \geq l\}$ forbliver den samme eller bliver mindre, hvis $\nu_m \neq \nu_{m+1}$. Dvs. at minimumsafstanden bliver større, hvis $\nu_m$ er den mindste værdi i mængden. Hermed er begge uligheder i sætningen vist. ■

Med hensyn til forskellen på de to grænser for minimumsafstand, er det værd at bemærke, at $\mathrm{d}(l)$ ikke afhænger af andet end ordensfunktionen $\rho$, mens $\mathrm{d}_\varphi(l)$ også afhænger af den valgte punktmængde. Dette argumenteres der for i det følgende.

Mængden $N_l$ afhænger kun af ordensfunktionen $\rho$. Dette ses af at $N_l = \{(i,j) \in \mathbb{N}^2 \mid l(i,j) = l+1\}$, dvs. at den afhænger af $l(i,j)$, hvorom der gælder

$$l(i,j) = l+1 \Leftrightarrow \rho(f_i f_j) = \rho_{l+1}.$$

Hvis $\rho(f_i) = \rho(g_i)$ for alle $i \in \mathbb{N}$, så gælder i følge lemma 3.20 at $\rho(f_i f_j) = \rho(g_i g_j)$, og ordensfunktionen er altså uafhængig af den valgte basis $\{f_i \mid i \in \mathbb{N}\}$, så længe kravene til ordensfunktionen er opfyldt.

Da $\nu_l = |N_l|$ og $\mathrm{d}(l) = \min\{\nu_m \mid m \geq l\}$, så afhænger $\mathrm{d}(l)$ også kun af $\rho$ og ikke af hverken valget af basis eller punktmængde. Til gengæld afhænger $\mathrm{d}_{\mathcal{P}}$ udover $\rho$ også af valget af punkter $\mathcal{P}$. Det skyldes at $C_l$ afhænger af funktionen $\varphi$, dvs. hvorvidt $C_m \neq C_{m+1}$ er afhængig af $\varphi(\mathcal{P})$.

Altså når vi frem til følgende udsagn:

$$\text{Hvis } \mathcal{P} \subseteq \mathcal{P}' \text{ så } \mathrm{d}_{\mathcal{P}} \geq \mathrm{d}_{\mathcal{P}'}.$$

Ved større punktmængder fås længere vektorer, dvs. et vektorrum af højere dimension, og dermed bliver sandsynligheden for at ordene er ens mindre, hvorved minimumsafstanden bliver mindre.

**Eksempel 3.41.** I dette eksempel konstrueres en Reed Solomon-kode, hvorefter det vises at koden er MDS og opfylder *singletongrænsen*, $d \leq n - k + 1$. En *Reed Solomon-kode* $\mathcal{C}$ er givet ved

$$\mathcal{C} = \{(f(1), f(\alpha), f(\alpha^2), \ldots, f(\alpha^{q-2})) \mid \deg(f) < k\},$$

hvor $\alpha$ er et primitivt element i $\mathbb{F}_q$ og $0 \leq k \leq n = q - 1$. Der gælder, at hvis $\mathcal{C}$ er en RS-kode, så er $\mathcal{C}^{\perp}$ også en RS-kode. For bevis og mere om RS-koder henvises til (Huffman og Pless, 2003, afsnit 5.2).

Vi kan nu konstruere en RS-kode ud fra begreberne i dette afsnit. Lad $R = \mathbb{F}_q[x]$ og lad $\rho$ være gradfunktionen $\rho(f) = \deg(f)$, som behandlet i eksempel 3.19. Vælg som basis $f_i = x^{i-1}, i \in \mathbb{N}$, dvs. at $f_1 = 1, f_2 = x, f_3 = x^2, \ldots$. Så er $(f_i \mid i \in \mathbb{N})$ er well-behaving følge og $l(i,j) = i + j - 1$.

Lad nu $\alpha \in \mathbb{F}_q$ være primitivt element, $n = q - 1$ og lad $\varphi : R \to \mathbb{F}_q^n$, være evalueringsafbildningen defineret ved

$$\varphi(f) = (f(1), f(\alpha), \ldots, f(\alpha^{q-2})).$$

Da er $\varphi = \mathrm{ev}_{\mathcal{P}}$, hvor $\mathcal{P} = \{\alpha^i \mid 0 \leq i \leq n-1\}$, $P_i = \alpha^{i-1}$ og $n = q - 1$. Herefter defineres evalueringskoden $E_l$ som

$$E_l = \varphi(L_l) = \langle \mathbf{h}_1, \ldots, \mathbf{h}_l \rangle \subseteq \mathbb{F}_q^n,$$

hvor $\mathbf{h}_i = \varphi(f_i)$. Så er $E_l = \{\varphi(f) \mid f \in R, \rho(f) < l\}$, hvoraf det ses, at $E_l$ er en RS-kode med $n(E_l) = q - 1$ og $k(E_l) = l$. Da dualen til en RS-kode selv er en RS-kode, så er

$$\mathcal{C}_l = \{\mathbf{c} \in \mathbb{F}_q^n \mid \mathbf{c} \cdot \varphi(f_i) = 0, 1 \leq i \leq l\}$$

også en RS-kode med definerende mængde $1, \alpha, \ldots, \alpha^{q-2}$ og med samme længde $n(\mathcal{C}_l) = q - 1$ og dimension $k(\mathcal{C}_l) = n - k(E_l) = n - l$.

For at vurdere minimumsafstanden, ses på den nederste grænse fra sætning 3.40.

$$\mathrm{d}(l) = \min\{\nu_m \mid m \geq l\}, \text{ hvor } \nu_m = |N_m| = |\{(i,j) \mid l(i,j) = m + 1\}|.$$

det vil sige at

$$(i,j) \in N_m \text{ hvis } m+1 \text{ er det mindste tal, så } f_i f_j \in L_{m+1}.$$

Altså hvis $\rho(f_i f_j) = \rho(f_{m+1})$. Da $\rho$ er gradfunktionen, og da $\deg(f_i) = \deg(x^{i-1}) = i-1$, så ses at

$$\begin{aligned} \deg(f_i f_j) &= \deg(f_{m+1}) \\ \deg\left(x^{i-1}x^{j-1}\right) &= \deg\left(x^{(m+1)-1}\right) \\ i+j-2 &= m \\ i+j &= m+2. \end{aligned}$$

Altså kan konkluderes, at

$$\begin{aligned} \nu_m &= |\{(i,j) \mid i+j = m+2\}| \\ &= |\{(1,m+1),(2,m),(3,m-1),\ldots,(m+1,1)\}| \\ &= m+1. \end{aligned}$$

Da $\nu_m = m+1$ for alle $m \in \mathbb{N}$, så fås grænsen for minimumsafstanden til

$$\mathrm{d}(l) = \min\{\nu_m \mid m \geq l\} = \min\{l+1, l+2, l+3, \ldots\} = l+1.$$

Singletongrænsen for koden $\mathcal{C}_l$ er $d \leq n-k+1 = n-(n-l)+1 = l+1$. Med ordensgrænsen $\mathrm{d}(l)$ er det altså vist, at RS-koden når singleton-grænsen, som er den størst mulige minimumsafstand der kan opnås. Dermed er Reed-Solomon en MDS kode, se (Huffman og Pless, 2003, afsnit 2.4). □

Også *Generaliserede Reed Muller*-koder (GRM-koder) kan forstås som evalueringskoder.

**Eksempel 3.42.** Lad $P_1, \ldots, P_n \in \mathbb{F}_q^m$ være alle $n = q^m$ punkter i $\mathbb{F}_q^m$. Lad $0 \leq r \leq m(q-1)$ og definer $\mathbb{F}_q[x_1,\ldots,x_m]_r$ til at være alle polynomier i $\mathbb{F}_q[x_1,\ldots,x_m]$ med $\deg(f) \leq r$ og nulpolynomiet. Den $r$'te ordens GRM-kode defineres som

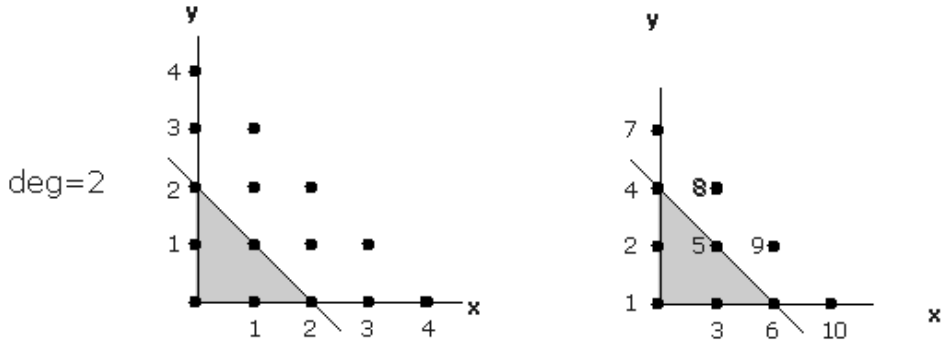
$$RM_r = \{(f(P_1),\ldots,f(P_n)) \mid f \in \mathbb{F}_q[x_1,\ldots,x_m]_r\}$$

Med teorien fra dette afsnit konstrueres GRM-koderne ved at se på

$$R = \mathbb{F}_q[x_1,\ldots,x_m] = \mathbb{F}_q[x_1,\ldots,x_m]/I,$$

hvor $I = \langle 0 \rangle$. Så er $V(I) = \mathbb{F}_q^m = \{P_1,\ldots,P_n\}$ og $ev_P(f) = (f(P_1),\ldots,f(P_n))$. Lad $\rho = \deg$. Så fås RM-koderne som evalueringskoderne $E_l = \langle \mathbf{h}_1 \ldots, \mathbf{h}_l \rangle$, hvor $h_i = ev_P(f_i)$.

Som eksempel ses på $m = 2$. Så er $RM_2$ evalueringen af polynomier med grad højest 2, dvs. polynomier dannet af monomierne $1, y, x, y^2, xy, x^2$, som er markeret på figuren:




Med $f_1 = 1, f_2 = y, f_3 = x, f_4 = y^2, f_5 = xy, f_6 = x^2, \ldots$ så svarer $RM_2$ til $E_6$, som det ses på den anden figur. □

**Eksempel 3.43.** I eksempel 3.29 så vi på den Hermitiske kurve med

$$R = \mathbb{F}_{16}[x, y] / \langle x^5 - y^4 - y \rangle,$$

og i eksempel 3.54 blev det vist at der var en vægtfunktion $\rho$ på $R$. Her fortsættes eksemplet med et skema over funktionerne $f_l$ og deres vægte $\rho_l$, tallet $\nu_l$ og grænsen $d(l)$.

| $l$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| $f_l$ | 1 | $x$ | $y$ | $x^2$ | $xy$ | $y^2$ | $x^3$ | $x^2y$ | $xy^2$ | $y^3$ | $x^4$ |
| $\rho_l$ | 0 | 4 | 5 | 8 | 9 | 10 | 12 | 13 | 14 | 15 | 16 |
| $\nu_l$ | 2 | 2 | 3 | 4 | 3 | 4 | 6 | 6 | 4 | 5 | 8 |
| $d(l)$ | 2 | 2 | 3 | 3 | 3 | 4 | 4 | 4 | 4 | 5 | 8 |

De første to rækker fås fra eksempel 3.29, og resten udregnes på følgende måde. Fra definition 3.36 fås, at $\nu_l = |N_l| = |\{(i,j) \in \mathbb{N}^2 \mid l(i,j) = l+1\}|$. Der gælder, at

$$l(i,j) = l+1 \Leftrightarrow \rho(f_i f_j) = \rho(f_{l+1}) = \rho_{l+1},$$

og da $\rho$ er en vægtfunktion, så er $\rho(f_i f_j) = \rho_i + \rho_j$, hvilket giver

$$\nu_l = |\{(i,j) \mid \rho_i + \rho_j = \rho_{l+1}\}|.$$

Som eksempel udregnes $\nu_1$:

$$\nu_1 = |\{(i,j) \mid \rho_i + \rho_j = \rho_2 = 4\}| = |\{(1,2),(2,1)\}| = 2,$$

da $\rho_1 + \rho_2 = 0 + 4 = 4$.

$$\nu_4 = |\{(i,j) \mid \rho_i + \rho_j = \rho_5 = 9\}| = |\{(2,3),(3,2),(1,5),(5,1)\}| = 4,$$

og på samme måde udregnes resten af $\nu_l$ værdierne. Grænsen $d(l)$ findes som $d(l) = \min\{\nu_m \mid m \geq l\}$. Dette giver

$$d(1) = \min\{\nu_m \mid m \geq 1\} = \nu_1 = 2,$$

da 2 er den mindste af alle $\nu_l$ værdierne. På sammen måde bliver $d(2) = \nu_2 = 2$ og $d(3) = \nu_3 = 3$. Værdierne $\nu_l$ og $d(l)$ er dog ikke altid de samme, som det ses for $l = 4$:

$$d(4) = \min\{\nu_m \mid m \geq 4\} = 3,$$

her er $d(4) \neq \nu_4$ da man finder den mindste af alle $\nu_l$ værdierne for $l \geq 4$, og der gælder at $\nu_5 = 3 < 4$. På denne måde kan alle værdierne til skemaet udregnes. □

## 3.4 Algebraisk geometri-koder

Dette afsnit er skrevet på baggrund af (Høholdt et al., 1998, kap. 2) og (Huffman og Pless, 2003, afsnit 13.4). Formålet med afsnittet er at give et hurtigt indblik i algebraisk geometri og AG-koder. Da emnet er meget omfattende og teorien kompliceret, vil ikke alle begreberne blive defineret formelt her, men blot blive introduceret for at give en forståelse for teorien og sammenhængen til ordensfunktionen $\rho$. For en mere formél gennemgang henvises til (Høholdt et al., 1998, kap. 2).

Inden koderne gennemgåes, vil det mest grundlæggende algebraiske geometri blive introduceret.

### 3.4.1 Algebraisk geometri

Lad $p(x, y, z)$ være et polynomium af positiv grad, som er *homogent*, dvs. at alle led i $p$ har samme totale grad, og lad $p$ definere en projektiv kurve $\chi$ over et legeme $\mathbb{F}$. Legemet af rationelle funktioner på $\chi$ over $\mathbb{F}$ defineres som

$$\mathbb{F}(\chi) = \left(\left\{\frac{g}{h} \mid g, h \in \mathbb{F}[x, y, z] \text{ er homogene af samme grad, } p \nmid h\right\} \cup \{0\}\right) \Big/ \equiv \chi.$$

**Definition 3.44.** En *divisor* er en formél sum

$$D = \sum_{P \in X} n_P P$$

med $n_P \in \mathbb{Z}$ og $n_P = 0$ for alle undtagen et endeligt antal punkter $P$. En divisor skal ej betragtes som sum, men blot som en samling af punkter, som hver får tildelt et tal. Graden af $D$ defineres som $\deg(D) = \sum n_P$. □

En divisor kan også defineres for en givet funktion, som i følgende definition:

**Definition 3.45.** Lad $f$ være en rationel funktion på $\chi$, med $f \neq 0$. Så er divisoren til $f$:

$$(f) = \sum_{P \in \chi} v_P(f)P,$$

hvor $v_P(f)$ er multipliciteten af $P$ som nulplunkt for $f$, hvis $v_P(f) \geq 0$, og ordenen af $P$ som pol for $f$, hvis $v_P(f) < 0$. □

Af divisoren er det altså muligt at aflæse multipliciteter af nulpunkter og orden af poler for $f$.

**Definition 3.46.** Lad $D$ være divisor på en kurve $\chi$. Så defineres vektorrummet $\mathcal{L}(D)$ over $\mathbb{F}$ som

$$\mathcal{L}(D) = \{f \in \mathbb{F}(\chi)^* \mid (f) + D \geq 0\} \cup \{0\},$$

hvor $(f) + D \geq 0$ betyder, at $v_P(f) + n_P \geq 0$ for alle $P \in \chi$. □

### 3.4.2 Konstruktion af AG-koder

AG-koder dannes som billedet af en evalueringsafbildning $ev$, hvor

$$\begin{aligned} ev: \quad & \mathcal{L}(G) \to \mathbb{F}_q^n \\ & f \mapsto (f(P_1), \ldots, f(P_n)). \end{aligned}$$

En AG-kode er givet ved $(\chi, D, G)$, hvor $\chi$ er en kurve i $\mathbb{P}^n$, altså en mængde af punkter, og $D, G$ er to divisorer, hvor skæringsmængden mellem $D$ og $G$ er den tomme mængde.

Konstruktionen af AG-koder foregår på følgende måde:

- Punktmængden $\chi$ deles op i to:

  $$\chi = \{P_1, \ldots, P_n, Q_1, \ldots, Q_m\},$$

  hvor $P$'erne er de punkter der senere evalueres i.

- Lad $D = P_1 + \cdots + P_n$ være divisor for de punkter der evalueres i.

- Lad $G$ være divisor for resten af punkterne, så

  $$G = a_1Q_1 + \cdots + a_mQ_m(+0 \cdot P1 + \cdots + 0 \cdot P_n),$$

  hvor $a_1, \ldots, a_m \in \mathbb{Z}$.

- Lad $\mathcal{L}(G) = \{f \in \mathbb{F}(\chi)^* \mid (f) + G \geq 0\} \cup \{0\}$, dvs. $L(G)$ indeholder funktioner, hvorom der gælder, at $v_{Q_i}(f) + a_i \geq 0$ og $v_{P_i}(f) + 0 \geq 0$ for alle $i$.

  Bemærk, at positive $a_i$ betyder at poler er tilladt i punktet, mens der for $a_i = 0$ ikke er tilladt poler og ved negative $a_i$ kræves at der er nulpunkter.

- Der gælder, at $\mathcal{L}(G)$ er et vektorrum over $\mathbb{F}$. Nu findes en basis $f_1, \ldots, f_k$, så
$$\mathcal{L}(G) = \langle f_1, \ldots, f_k \rangle .$$
- En basis for koden konstrueres ved at evaluere $f_1, \ldots, f_k$ i punkterne $P_1, \ldots, P_n$. Bemærk, at det er muligt at evaluere $f$ i $P$'erne, da de ikke kan være poler, fordi $a_i = 0$ i $G$ for alle $P_i$. Dette giver en basis:
$$(f_1(P_1), \ldots, f_1(P_n)), \ldots, (f_k(P_1), \ldots, f_k(P_n)).$$

AG-koden er så vektorrummet dannet af de basisvektorer som er fundet i det sidste trin, og koden fås som nævnt i starten vha. evalueringsafbildningen

$$\begin{aligned} ev: \quad & \mathcal{L}(G) \to \mathbb{F}^n \\ & f \mapsto (f(P_1), \ldots, f(P_n)). \end{aligned}$$

Med $\varphi = ev$ fås evalueringskoden $E_l = \varphi(L_l) = \langle \mathbf{h}_1, \ldots, \mathbf{h}_l \rangle$, hvor $\mathbf{h}_i = \varphi(f_i) = ev(f_i)$ som vist i forrige afsnit. Her er $ev$ blot afbildningen fra vektorrummet $\mathcal{L}(G)$ ind i $\mathbb{F}^n$ i stedet for $ev : \mathbb{F}[x_1, \ldots, x_n] \to \mathbb{F}^n$, som vist i eksempel 3.31.

For en bedre forståelse følger her et eksempel på konstruktionen af en AG-kode.

**Eksempel 3.47.** Lad $I = \langle x^3y + y^3z + z^3x \rangle$ være idealet, som skal bruges til at danne AG-koden. Så består $V(I)$ af løsningerne til $x^3y + y^3z + z^3x = 0$. Hvis vi arbejder i $\mathbb{F}_2$ er der de tre nulpunkter:

$$(1:0:0),\ (0:1:0),\ (0:0:1) \subseteq \mathbb{P}^2.$$

Lad

$$P_1 = (1:0:0),\ P_2 = (0:1:0),\ Q_1 = (0:0:1).$$

Så er $n = 2$ og $\mathcal{C} \subseteq \mathbb{F}_2^2$. Altså er $\chi = V_{\mathbb{F}_2}(I) = \{P_1, P_2, Q_1\}$. Divisorerne er $D = P_1 + P_2$ og $G = 3Q_1 + 0 \cdot P_1 + 0 \cdot P_2$, hvilket giver vektorrummet

$$\mathcal{L}(G) = \{f \in \mathbb{F}(\chi)^* \mid v_{Q_1}(f) + 3 \geq 0, v_{P_1}(f) \geq 0, v_{P_2}(f) \geq 0\} \cup \{0\}.$$

Heraf fås, at $f \in \mathcal{L}(G)$ hvis og kun hvis $v_{Q_1}(f) \geq -3$, dvs. $\mathcal{L}(G)$ består af alle funktioner med pol af orden mindre end eller lig med 3 i $Q_1$ og ingen poler i $P_1$ og $P_2$.

Herefter findes en basis for vektorrummet $\mathcal{L}(G)$, og basiselementerne evalueres i punkterne $P_1$ og $P_2$ for at danne en basis for koden.

Hvis inddelingen i $D$ og $G$ ændres fås et andet resultat. Lad $P_1 = (1:0:0)$, $Q_1 = (0:1:0)$ og $Q_2 = (0:0:1)$. Da er $D = P_1$ og $G = 3Q_1 - 1 \cdot Q_2 + 0 \cdot P_1$, så her fås, at

$$\mathcal{L}(G) = \{f \in \mathbb{F}(\chi)^* \mid v_{Q_1}(f) + 3 \geq 0, v_{Q_2}(f) - 1 \geq 0, v_{P_1}(f) \geq 0\} \cup \{0\}.$$

Dette betyder, at $f \in \mathcal{L}(G)$ hvis og kun hvis $f$ har en pol af orden højst 3 i $Q_1$, et nulpunkt af mindst første grad i $Q_2$ og ingen pol i $P_1$. □

Det kan vises, at koden $(\chi, D, G)$ har dimension

$$k = \deg(G) - g + 1, \tag{3.11}$$

hvor $g$ er en algebraisk invariant kaldet genus, og minimumsafstand

$$d \geq n - \deg(G). \tag{3.12}$$

Se (Høholdt et al., 1998, thm. 2.65) for bevis. Senere i specialet vil der vha. ordensfunktioner blive vist en grænse for evalueringskoder, som er mindst lige så god.

Generelt gælder der, at hvis der kun er ét $Q$, så er $v_Q$ en ordensfunktion. I (Høholdt et al., 1998, thm 2.16) er det vist, at afbildningen $v_Q$ er en diskret valuation, som opfylder fem kriterier. Sættes $\rho = -v_Q$ medfører disse egenskaber, at $\rho$ er en ordensfunktion. Denne slags koder med kun ét $Q$ kaldes *one-point codes*. Så er $\mathcal{L}(G) = \mathcal{L}(mQ)$, dvs. $\mathcal{L}(G)$ indeholder de funktioner som har poler af højst grad $m$ i $Q$ og ingen poler i $P$'erne. Ordensfunktionen fås ved at evaluere $f \in \mathcal{L}(mQ)$ i $P_1, \ldots, P_n$. Så er $\rho(f) = -v_Q(f)$.

## 3.5 Eksistens af ordensfunktioner

Dette afsnit er skrevet på baggrund af (Pellikaan, 2001). I afsnit 3.3 blev vist, at givet en ordensfunktion på $R$, så eksisterer der en well-behaving følge $f_1, f_2, \ldots$ som er basis for $R$. Ud fra denne basis dannes evalueringskoderne $E_l$ og $C_l$ og det er muligt at give en minimumsafstandsgrænse for $C_l$. I dette afsnit opstilles kriterier for hvornår der eksisterer en ordensfunktion på $R$. Til dette benyttes Gröbnerbasisteori, hvor vi minder om, at fodaftrykket er defineret som $\Delta(I) = \{\mathbf{x}^\alpha \mid \mathbf{x}^\alpha \notin \langle \text{LT}(I) \rangle\}$, hvor $\Delta(I)$ er basis for $\mathbb{F}[x_1, \ldots, x_n]/I$. Derudover anvendes S-polynomier og Buchbergers kriterium, samt den vægtede lex-orden $<_w$.

Først vises et lemma, der udforsker konsekvenserne ved at hvert polynomium i $G$ har to monomier af højest vægtede grad. Dette er det ene af kriterierne for eksistensen af ordensfunktioner.

**Lemma 3.48.** Lad $G$ være en Gröbnerbasis, hvor hvert polynomium i $G$ har præcist to monomier af højest vægtede grad. Hvis $\overline{f}^G = h$ mht. $<_w$ og $f$ har præcist ét monomium af højest vægtede grad, så gælder der at $\text{wdeg}(f) = \text{wdeg}(h)$ og $h$ har præcist ét monomium af højest vægtede grad. □

**Bevis.** Det er pr. induktion nok at vise, at $\overline{f}^g = h$ for et $g \in G$. Antag, at $f$ har præcist ét monomium af højest vægtede grad, nemlig $\text{LT}(f) = \lambda_\alpha \mathbf{x}^\alpha$. Så kan $f$ skrives som $f = f' + \text{LT}(f)$, hvor $\text{wdeg}(f') < \text{wdeg}(f)$, da der kun er ét monomium af højeste grad.

Lad $\overline{f}^g = h$. Så er $h = f - \mu m g$, for et monomium $m$ og $g \in G$, så $\text{LT}(\mu m g) \in f$. Dvs. at $\text{wdeg}(mg) \leq \text{wdeg}(f)$.

Der er nu to muligheder:

- Hvis $\text{wdeg}(mg) < \text{wdeg}(f)$, så går $\text{LT}(f)$ ikke ud ved division, dvs. $h = \text{LT}(f) + (f - \text{LT}(f)) - \mu mg = \lambda_\alpha \mathbf{x}^\alpha + (f' - \mu mg)$. Da $\text{wdeg}(f') < \text{wdeg}(f)$ og $\text{wdeg}(mg) < \text{wdeg}(f)$, så er $\text{wdeg}(f' - \mu mg) < \text{wdeg}(f) = \text{wdeg}(\mathbf{x}^\alpha)$. Heraf ses, at $\text{wdeg}(h) = \text{wdeg}(\mathbf{x}^\alpha) = \text{wdeg}(f)$ og $\lambda_\alpha \mathbf{x}^\alpha$ er eneste monomium i $h$ af højeste grad, hvilket viser sætningen.

- Hvis derimod $\text{wdeg}(mg) = \text{wdeg}(f)$, så går $\text{LT}(f)$ ud ved divisionen, da det er eneste monomium af højeste grad i $f$. Brug nu antagelsen om at $g$ har præcist to monomier af højeste grad, $m_1$ og $m_2$, med $\text{wdeg}(m_1) = \text{wdeg}(m_2) = \text{wdeg}(g)$. Så eksisterer der et polynomium $g'$, så $g = g' + \mu_1 m_1 + \mu_2 m_2$, hvor $\text{wdeg}(g') < \text{wdeg}(g)$, da der kun er de to monomier af højeste grad i $g$.

  Antag nu, at $m_1 <_w m_2$, så er $\text{LT}(g) = \mu_2 m_2$ og $\text{LT}(\mu mg) = \mu m \mu_2 m_2$. Da $\lambda_\alpha \mathbf{x}^\alpha$ går ud ved division medfører det, at $\text{LT}(\mu mg) = \lambda_\alpha \mathbf{x}^\alpha$, da det er eneste led i $f$ med højeste grad.

  Altså er

$$\begin{aligned} h &= f - \mu mg \\ &= f - (\mu mg' + \mu\mu_1 m m_1 + \mu\mu_2 m m_2) \\ &= f - \lambda_\alpha \mathbf{x}^\alpha - (\mu mg' + \mu\mu_1 m m_1) \\ &= (f' - \mu mg') - \mu\mu_1 m m_1, \end{aligned} \tag{3.13}$$

  hvor $\text{wdeg}(mm_1) = \text{wdeg}(mm_2) = \text{wdeg}(f)$, mens $\text{wdeg}(f') < \text{wdeg}(f)$ og $\text{wdeg}(mg') < \text{wdeg}(mm_1) = \text{wdeg}(f)$. Deraf ses, at $\text{wdeg}(f' - \mu mg') < \text{wdeg}(mm_1) = \text{wdeg}(h)$, dvs. $\text{wdeg}(f) = \text{wdeg}(h)$ og $h$ har et entydigt monomium af højeste grad. ■

Antagelserne i sætningen om, at der i $g$ må være præcist to monomier af højeste grad er nødvendige for beviset. Hvis $g$ har flere end to monomier, så er det ikke muligt at vide, at $\text{wdeg}(g') < \text{wdeg}(m_1)$ og dermed, at $g$ kun har ét monomium af højeste grad, som det ses af (3.13). Hvis $g$ kun har ét monomium af højeste grad, så er $h = f - \lambda_\alpha \mathbf{x}^\alpha - \mu mg' = f' - \mu mg'$, så $\text{wdeg}(h) < \text{wdeg}(f)$.

Med lemmaet på plads er det nu muligt at vise hovedsætningen fra (Pellikaan, 2001), som viser at der eksisterer en ordensfunktion på $R$, hvis to kriterier er opfyldt.

**Sætning 3.49.**
Lad $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ være et ideal. Hvis alle monomier i $\Delta(I)$ har indbyrdes forskellig vægt, og hvis ethvert element i $G$ har præcist to elementer af højest vægtede grad, så eksisterer der en vægtfunktion $\rho$ på $R = \mathbb{F}[x_1, \ldots, x_n]/I$, sådan at $\rho([f]) = \text{wdeg}(f)$ for alle $[f] \neq 0$.

**Bevis.** Monomierne i fodaftrykket $\Delta(I)$ har ifølge antagelserne forskellig vægt, og kan derfor nummereres, så der fås en følge $f_1, f_2, \ldots$ med $\text{wdeg}(f_i) < \text{wdeg}(f_{i+1})$. Lad $[f_i] = f_i \pmod I$. Så er $[f_1], [f_2], \ldots$ basis for $R/I$ jvf. proposition 3.9. Lad $\rho_i = \text{wdeg}(f_i)$. Da $\text{wdeg}(f_i) < \text{wdeg}(f_{i+1})$, så er $\rho_i < \rho_{i+1}$, og værdierne af $i$ danner dermed en strengt voksende følge. For at vise, at $\rho$ er en ordensfunktion på $R$, benyttes sætning 3.25, som kræver, at følgen $f_i$ er well-behaving, dvs. at $l(i,j) < l(i+1,j)$. Dette bliver vist i det følgende.

Se på to monomier $f_i, f_j \in \Delta(I)$. Hvis $f_i f_j \in \Delta(I)$, så er $\overline{f_i f_j}^G = f_i f_j \in \Delta(I)$, hvilket svarer til at $R = \mathbb{F}[x_1, \ldots, x_n]$. Så er $\rho(\overline{f_i f_j}^G) = \rho(f_i f_j)$, og da $\rho_i$ er strengt voksende, og $f_i, f_j$ er monomier, så er

$$\rho(f_i f_j) < \rho(f_{i+1} f_j) \Rightarrow \rho_{l(i,j)} < \rho_{l(i+1,j)} \Rightarrow l(i,j) < l(i+1,j).$$

Hvis derimod $f_i f_j \notin \Delta(I)$, så bliver monomiet reduceret mod $I$ i $R = \mathbb{F}[x_1, \ldots, x_n]/I$, og vi er ikke længere garanteret, at $l(i,j)$ er strengt voksende. Som det ses i det følgende, opnår vi det alligevel på grund af kravene til elementerne i Gröbnerbasen, som gør at lemma 3.48 kan benyttes.

Pr. definition er $l(i,j)$ det mindste tal, så $[f_i f_j] \in L_{l(i,j)}$. Dermed er

$$f_i f_j \equiv \sum_{m \le l(i,j)} \lambda_m f_m \pmod I, \text{ hvor } \lambda_m \in \mathbb{F} \,\forall\, m,\ \lambda_{l(i,j)} \neq 0.$$

Altså er

$$\overline{f_i f_j}^G = \sum_{m \le l(i,j)} \lambda_m f_m,$$

da $G$ er en Gröbnerbasis for $I$.

Lad $f = f_i f_j$ og $g = \sum_{m \le l(i,j)} \lambda_m f_m$. Så er $\overline{f}^G = g$. Da alle elementer i $G$ pr. antagelse har præcist to monomier af højest vægtede grad og da $f$ har præcist ét monomium af højest vægtede grad, så er lemma 3.48 nu opfyldt. Dette medfører at $\text{wdeg}(f) = \text{wdeg}(g)$, hvilket betyder at reduktionen modulo $I$ af et monomium $f$ ikke ændrer på den vægtede grad. Dermed er $\rho(\overline{f_i f_j}^G) = \rho(f_i f_j)$.

Dvs. for $[f_i], [f_j] \in \mathbb{F}[x_1, \ldots, x_n]/I$ gælder, at $\rho([f_i f_j]) < \rho([f_{i+1} f_j])$, så $l(i,j) < l(i+1,j)$, hvilket medfører at $[f_i]$ er well-behaving. Dermed giver sætning 3.25, at $\rho$ er en ordensfunktion. Ydermere gælder der, at

$$\begin{aligned} \rho_i + \rho_j &= \text{wdeg}(f_i) + \text{wdeg}(f_j) \\ &= \text{wdeg}(f_i f_j) = \text{wdeg}(f) = \text{wdeg}(g) = \text{wdeg}(f_{l(i,j)} = \rho_{l(i,j)}, \end{aligned}$$

hvoraf det ses, at $\rho$ også er en vægtfunktion. ■

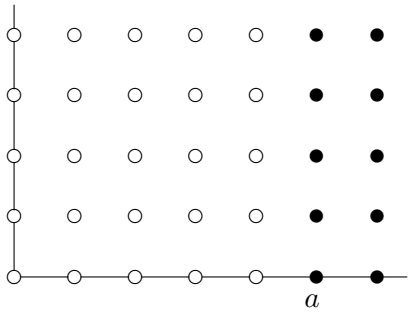
Det er tidligere vist i eksempel 3.26, at der eksisterer en ordensfunktion på $R = \mathbb{F}[x_1, \ldots, x_n]$. Når der arbejdes i $R = \mathbb{F}[x_1, \ldots, x_n]/I$ er det ikke altid tilfældet, men det følgende eksempel viser, at når idealet er på en bestemt form, så

har $R = \mathbb{F}[x_1, \ldots, x_n]/I$ en vægtfunktion. I (Pellikaan, 2001) introduceres dette eksempel inden Gröbnerteorien, hvilket giver en god fornemmelse for, hvor kompliceret det hidtil har været at vise eksistensen af ordensfunktioner. Med artiklens hovedresultat, sætning 3.49, bliver dette dog meget lettere.

**Eksempel 3.50.** Lad $I = \langle x^a + y^b + g(x,y) \rangle \subseteq \mathbb{F}[x,y]$, hvor $\deg(g) < \min\{a,b\}$ og $\gcd(a,b) = 1$. Lad $R = \mathbb{F}[x,y]/I$, så er $x^a \equiv -y^b - g(x,y) \pmod{I}$. Antag uden tab af generalitet, at $x^a > y^b$, så $\text{LM}(x^a + y^b + g(x,y)) = x^a$. Da er

$$\Delta(I) = \{x^\alpha y^\beta \mid 0 < \alpha \leq a\}$$

en basis for $R$, som det ses på figuren.




At der eksisterer en vægtfunktion på $R$, vises i (Pellikaan, 2001, prop. 4.6) vha. et forholdsvist kompliceret induktionsbevis. I stedet benyttes her Gröbnerbasisteori og sætning 3.49.

Da $I$ er et hovedideal, så har $I$ Gröbnerbasen $G = x^a + y^b + g(x,y)$, med kun et basis-polynomium. Først skal det vises, at elementerne i $\Delta(I)$ har indbyrdes forskellig vægtet grad. Lad $\mathbf{w} = (b,a)$ og benyt den vægtede leksikografiske orden $<_w$. Så er $\text{wdeg}(x) = b$ og $\text{wdeg}(y) = a$. Antag modsætningsvist at der findes to forskellige monomier i $\Delta(I)$ med samme orden, dvs. $(\alpha,\beta) \neq (\alpha',\beta')$. Så gælder, at

$$\begin{aligned} \text{wdeg}(x^\alpha y^\beta) = \text{wdeg}(x^{\alpha'} y^{\beta'}) &\Leftrightarrow \\ b \cdot \alpha + a \cdot \beta = b \cdot \alpha' + a \cdot \beta' &\Leftrightarrow \\ b(\alpha - \alpha') = a(\beta' - \beta). & \end{aligned}$$

Hvis $\alpha = \alpha'$ så er $\beta = \beta'$, men så er $(\alpha,\beta) = (\alpha',\beta')$, i modstrid med antagelsen. Derfor må $a \mid b(\alpha - \alpha')$, og $\gcd(a,b) = 1$ medfører så at $a \mid (\alpha - \alpha')$. Dette er dog ikke muligt, da både $\alpha, \alpha' < a$. Altså er opnået en modstrid, og der kan ikke findes to monomier af samme vægt i $\Delta(I)$. Der gælder, at

$$\rho(x^a) = a \cdot b = \rho(y^b) \text{ og } \rho(g(x,y)) < a \cdot b,$$

da $\deg(g) < \min\{a,b\}$, så $\text{wdeg}(g) < \max\{a,b\} \cdot \min\{a,b\} = a \cdot b$. Dermed har basispolynomiet for $G$ præcist to monomier af højest vægtede grad og alle elementer

i $\Delta(I)$ har forskellig vægt. Dermed giver 3.49 at der eksisterer en vægtfunktion på $R$. □

Som specialtilfælde af sætning 3.49 viser næste proposition konstruktionen af et bestemt ideal, som garanterer at $R$ har en vægtfunktion.

**Proposition 3.51.** Lad $I$ være et ideal i $\mathbb{F}[x_1, \ldots, x_n]$ som er genereret af

$$f_i = x_i^{a_i} + x_{i+1}^{b_i} + g_i, \text{ for } i = 1, \ldots, n-1,$$

hvor $g_i \in \mathbb{F}[x_1, \ldots, x_{i+1}]$, $\text{wdeg}(g_i) < a_1 \cdots a_i b_i \cdots b_{n-1}$ og $\gcd(a_i, b_j) = 1$ for alle $i \leq j$. Så har ringen $R = \mathbb{F}[x_1, \ldots, x_n]/I$ en vægtfunktion $\rho$. □

**Bevis.** Lad $w_i = a_1 \cdots a_{i-1} b_i \cdots b_{n-1}$. Det ses da, at $\text{wdeg}(g_i) < w_i \cdot a_i$. Lad $\mathbf{w} = (w_1, \ldots, w_n)$ og lad $<_w$ være den vægtede lex-orden mht. vægtene $\mathbf{w}$. Så er $\text{wdeg}(x_i^{a_i}) = w_i \cdot a_i$ og $\text{wdeg}(x_{i+1}^{b_i}) = w_{i+1} \cdot b_i$. Dermed er $\text{wdeg}(x_i^{a_i}) = \text{wdeg}(x_{i+1}^{b_i}) = a_1 \cdots a_i b_i \cdots b_{n-1} > \text{wdeg}(g_i)$.

Da $x_i^{a_i}$ og $x_{i+1}^{b_i}$ har samme vægtede grad og da $x_i > x_{i+1}$ mht. lex-orden, så er $x_{i+1}^{b_i} <_w x_i^{a_i}$. Altså er $\text{LT}(f_i) = x_i^{a_i}$ og $f_i$ har præcist to monomier af højest vægtede grad, nemlig $x_i^{a_i}$ og $x_{i+1}^{b_i}$, mens resten af monomierne er indeholdt i $g_i$ og har lavere grad.

Lad nu $G = \{f_1, \ldots, f_{n-1}\}$. Vi ønsker at vise, at $G$ er en Gröbnerbasis og at alle monomier i fodaftrykket har forskellig grad for at kunne benytte sætning 3.49. De ledende monomier i $G$ er $x_1^{a_1}, x_2^{a_2}, \ldots, x_{n-1}^{a_{n-1}}$. Dermed er fodaftrykket

$$\Delta(I) = \{\mathbf{x}^\alpha \mid 0 \leq \alpha_i < a_i \forall\, 1 \leq i < n\}.$$

Pr. antagelse er $\gcd(a_i, b_j) = 1$ for $i \leq j$, så

$$\text{wdeg}(\mathbf{x}^\alpha) = \text{wdeg}(\mathbf{x}^\beta) \Leftrightarrow \alpha = \beta. \tag{3.14}$$

Altså har alle elementer i $\Delta(I)$ indbyrdes forskellig vægtet grad. Vi mangler nu blot at vise, at $G$ er en Gröbnerbasis. Se på $S$-polynomiet, hvor der reduceres mht. $g_i$ og $g_j$

$$\begin{aligned}
S(f_i, f_j) &= x_j^{a_j} \cdot f_i - x_i^{a_i} \cdot f_j \\
&= x_j^{a_j}(x_i^{a_i} + x_{i+1}^{b_i} + g_i) - x_i^{a_i}(x_j^{a_j} + x_{j+1}^{b_j} + g_j) \\
&= x_j^{a_j} x_{i+1}^{b_i} + x_j^{a_j} g_i - x_i^{a_i} x_{j+1}^{b_j} - x_i^{a_i} g_j \\
&= x_j^{a_j}(x_{i+1}^{b_i} + g_i) - x_i^{a_i}(x_{j+1}^{b_j} + g_j) \\
&= -x_i^{a_i} x_j^{a_j} - x_i^{a_i}(x_{j+1}^{b_j} + g_j) \\
&= -x_i^{a_i}(x_j^{a_j} + x_{j+1}^{b_j} + g_j) \\
&= -x_i^{a_i} \cdot 0 \\
&= 0.
\end{aligned}$$

Så $\overline{S(f_i, f_j)}^G = 0$ for alle $S$-polynomier med $f_i, f_j \in G$. Derfor er $G$ en Gröbnerbasis jvf. Buchbergers Kriterium, sætning 2.23. Sætning 3.49 medfører da, at $R$ har en vægtfunktion. ■

**Eksempel 3.52.** Vha. 3.51 er det let at se, at $R = \mathbb{F}[x_1, \ldots, x_n]/I$ fra eksempel 3.50 har en vægtfunktion. Lad $I = \langle x^a + y^b + g(x,y) \rangle \subseteq \mathbb{F}[x,y]$, hvor $\deg(g) < \min\{a,b\}$ og $\gcd(a,b) = 1$. Så er $x_1 = x$, $x_2 = y$, $n = 2$, $a_1 = a$, $b_1 = b$, $\text{wdeg}(g) < ab$ og $\gcd(a,b) = 1$, og dermed giver 3.51 at der eksisterer en vægtfunktion på $R$. □

Et mere konkret eksempel på hvordan en sådan ring kan se ud, ses i følgende eksempel.

**Eksempel 3.53.** Lad $I \subseteq \mathbb{F}[x,y,z]$ være et ideal genereret af $f_1 = x^2 + y^3 + xy$ og $f_2 = y^5 + z^3 + y^2$. Så er $n = 3, a_1 = 2, b_1 = 3, g_1 = xy$ og $a_2 = 5, b_2 = 3, g_2 = y^2$, og $\gcd(a_i, b_j) = 1$ for alle $i \leq j$. Lad $\mathbf{w} = (1,2,3)$, så er $\text{wdeg}(g_1) = 1 + 2 = 3 < a_1 \cdot b_1 \cdot b_2 = 2 \cdot 3 \cdot 3 = 18$ og $\text{wdeg}(g_2) = 2 \cdot 2 = 4 < a_1 \cdot a_2 \cdot b_2 = 2 \cdot 5 \cdot 3 = 30$. Dermed er antagelserne i 3.51 opfyldt, hvilket medfører at der findes en vægtfunktion på $R = \mathbb{F}[x,y,z]/I$. □

I næste eksempel vises eksistensen af en vægtfunktion på $R/I$, hvor idealet $I$ er dannet af en hermitisk kurve. Dette er også muligt at vise vha. algebraisk geometri, men er meget simplere med Gröbnerteori, hvor prop. 3.51 kan benyttes.

**Eksempel 3.54.** Den Hermitiske kurve $\mathcal{H}_r$ over $\mathbb{F}_q$ er givet ved

$$x^{r+1} - y^r - y = 0.$$

Vi lader her $q = r^2$, og ser på den Hermitiske kurve med $r = 4$, som tidligere er blevet introduceret i eksempel 3.29. Så er $q = 4^2 = 16$. Lad

$$R = \mathbb{F}_{16}[x,y] / \langle x^5 - y^4 - y \rangle .$$

Så har $R$ mængden $\Delta(I) = \{x^\alpha y^\beta \mid \alpha < 5\}$ som basis.

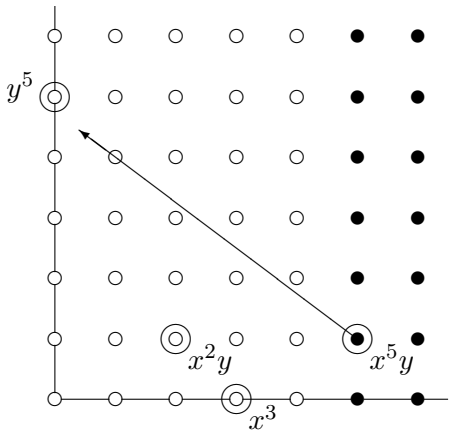
Lad $\mathbf{w} = (4,5)$, så $\text{wdeg}(x^\alpha y^\beta) = 4\alpha + 5\beta$. Da $\gcd(5,4) = 1$ så har alle elementer i fodaftrykket indbyrdes forskellig vægt, som det ses på figuren:

| | | | | |
|---|---|---|---|---|
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| $y^4$ | · | · | · | · |
| $y^3$ | $xy^3$ | · | · | · |
| $y^2$ | $xy^2$ | $x^2y^2$ | · | · |
| $y$ | $xy$ | $x^2y$ | $x^3y$ | $x^4y$ |
| 1 | $x$ | $x^2$ | $x^3$ | $x^4$ |

| | | | | |
|---|---|---|---|---|
| ⋮ | ⋮ | ⋮ | ⋮ | ⋮ |
| 20 | · | · | · | · |
| 15 | 19 | · | · | · |
| 10 | 14 | 18 | · | · |
| 5 | 9 | 13 | 17 | 21 |
| 0 | 4 | 8 | 12 | 16 |

Vægtene medfører også at $x^5 - y^4 - y$ får to monomier af højeste vægt, da $\text{wdeg}(x^5) = 4 \cdot 5 = \text{wdeg}(y^4)$. Fra 3.49 fås, at $\rho = \text{wdeg}$ er en vægtfunktion på $R$.

Nu er det også muligt at se, hvorfor de specielle antagelser i sætning 3.49 er nødvendige. Da alle monomier i fodaftrykket har indbyrdes forskellig vægt, så er det muligt at nummerere dem som i eksempel 3.29, så $f_1 = 1, f_2 = x, f_3 = y, f_4 = x^2, \ldots$ er basis for $R$. For at der kan eksistere en ordensfunktion skal der gælde, at $\rho(f_i f_j) < \rho(f_{i+1} f_j)$. Da fodaftrykket er afgrænset er vi nødt til at tjekke hvad der sker når $f_i f_j$ giver et element udenfor $\Delta(I)$. På figuren ses et eksempel med $f_7 = x^3$ og $f_8 = x^2 y$. Så er $f_7 f_8 = x^5 y = (y^4 + y)y = y^5 + y^2 = f_{20} + f_6$. Dvs. at $f_7 f_8$ har $y^5$ som førende led, og der gælder at $\text{wdeg}(y^5) = 5 \cdot 5 = 25 = \text{wdeg}(x^5 y)$, hvorved vægten er bevaret på trods af at der regnes modulo $I$.




Dette skyldes at alle polynomier i $G$ har to monomier af højeste grad. Dvs. hver gang der foretages en division af $f \in \mathbb{F}[x_1, \ldots, x_n]$ med et polynomium i $G$, så vil det ene monomium gå ud med det førende led i $f$, mens det andet bliver tilføjet resten og sørger for at graden forbliver den samme. I eksemplet sker det ved, at $x^5$ erstattes med $y^4$, hvor begge monomier har samme grad.

Den Hermitiske kurve er også et specialtilfælde af proposition 3.51, med $m = 2, x_1 = x, x_2 = y, g_1 = y, a_1 = 5, b_1 = 4$. Så er $\text{wdeg}(g) = \text{wdeg}(y) = 5 < 5 \cdot 4 = a_1 \cdot b_1$. Dermed er alle antagelser opfyldt og der eksisterer ifølge 3.51 en vægtfunktion på $R$. □

**Eksempel 3.55.** Klein kurven $\mathcal{K}_m$ er defineret som $x^m y + y^m z + z^m x = 0$. Se nu på den affine ligning $x^3 y + y^3 + x = 0$ over $\mathbb{F}_8$. Lad $\mathbf{w} = (2, 3)$. Så er $\gcd(2, 3) = 1$ og alle basiselementerne har indbyrdes forskellig vægt. Der gælder, at $\text{wdeg}(x^3 y) = 2 \cdot 3 + 3 = 9$, $\text{wdeg}(y^3) = 3 \cdot 3 = 9$ og $\text{wdeg}(x) = 2 < 9$, så der er to monomier af højeste grad i basispolynomiet. Sætning 3.49 giver dermed, at der eksisterer en vægtfunktion $\rho = \text{wdeg}$ på $R = \mathbb{F}_8[x, y] / \langle x^3 y + y^3 + x \rangle$. □

Sætning 3.49 gør det altså muligt meget hurtigt at se om der findes en ordensfunktion på området. Givet et ideal $I \subseteq \mathbb{F}[x_1, \ldots, x_n]$ og en vægtet lex-orden $<_w$, så udregnes Gröbnerbasen $G$ mht. $I$ og det er derefter nok at tjekke om idealet opfylder følgende to egenskaber:

1. elementerne i $\Delta(I)$ har indbyrdes forskellig vægtet grad mht. $<_w$,
2. Gröbnerbasen for $I$ mht $<_w$ har præcist to monomier af højest vægtede grad.

Så giver sætning 3.49 at der eksisterer en ordensfunktion på $R = \mathbb{F}[x_1, \ldots, x_n]/I$. Fra afsnit 3.3 ved vi, at der findes evalueringskoder $E_l$ og $C_l$, som sender $R$ ind i $\mathbb{F}_q^n$, og disse resultater giver os nu, uden ekstra arbejde, både en minimumsafstandsgrænse $d(C_l)$, som blev vist i sætning 3.40 for $C_l$ og en dekodningsalgoritme (Majority Voting Dekodningsalgoritmen, som beskrives i (Høholdt et al., 1998, kap. 6)). Med dette resultat bliver arbejdet med at vise eksistensen af ordensfunktionen meget simplere end ved brug af algebraisk geometri, som man har gjort hidtil.

# LITTERATUR


Andersen, H. E. og Geil, H. O. (2008). Evaluation Codes from Order Domain Theory. *Finite Fields and Their Applications*, 14:92-123.

Cox, D., Little, J. og O'Shea, D. (2007). *Ideals, Varieties, and Algorithms.* New York, NY: Springer, 3. udgave.

Greuel, G.-M. og Pfister, G. (2002). *A Singular Introduction to Commutative Algebra.* New York, NY: Springer, 1. udgave.

Huffman, W. C. og Pless, V. (2003). *Fundamentals of Error-Correcting Codes.* New York, NY: Cambridge University Press, 1. udgave.

Høholdt, T., Lint, J. v. og Pellikaan, R. (1998). Algebraic geometry codes. *Handbook of Coding Theory (Pless, Huffman, Brualdi, eds.)*, 1:871-961.

Justesen, J. og Høholdt, T. (2004). *A course in error-correcting codes.* Zürich: European Mathematical Society, 1. udgave.

Lauritzen, N. (2003). *Concrete Abstract Algebra.* New York, NY: Cambridge University Press, 1. udgave.

Pellikaan, R. (2001). On the existence of order functions. *Journal of Statistical Planning and Inference*, 94:287-301.