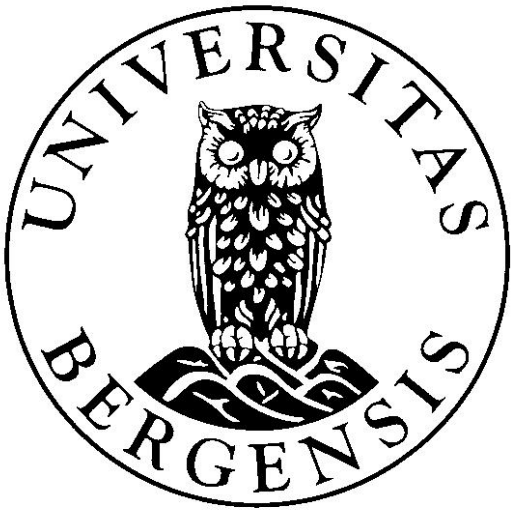
Tokamerarekonstruksjon og Gröbnerbasar

Universitetet i Bergen



Master i matematikk
Lektorutdanning i realfag
Matematisk institutt

Vår 2016

Kristine Njøs Slinde

1. juni 2016

Innhald

Kapittel 1

Innleiing

I denne oppgåva skal me sjå på korleis ein skal gå fram for å rekonstruere ei scene frå to bilete. Dette kan brukast når ein skal evaluere satellittbilete og gjere ei kalibrering av kamera.
Me skal sjå på geometrien og matematikken bak tilfellet der ein har eit punkt i rommet, som blir avbilda i to bilete. Dette punktet vil bli avbilda i eit punkt i det eine kamera, og i eit anna punkt i det andre. Sidan desse punkta svarar til det same punktet, vil dei vere korresponderande punkt. Det er denne korrespondansen me vil utforske nærmare. Me vil også finne ut kor mange korresponderande punkt ein må ha for å finne ei endeleg løysing for den essensielle matrisa, og dermed kunne finne kameraforskyvinga. Deretter vil me finne ut kor mange moglegheitar dette gir, generelt. For å finne svaret på dette, må me introdusere fundamentalmatrisa og den essensielle matrisa.
Me byrjar med å gi ein introduksjon til det projektive planet, og deretter ser me på projektiv geometri og transformasjonar i tre dimensjonar. Dette brukar me når me skal sjå på ulike kameramodellar, og den essensielle matrisa. For å kunne dekomponere den essensielle matrisa og finne kameraforskyvinga, må me løyse ei mengde med polynomlikningar. For å kunne finne ei løysing på denne mengda med polynomlikningar, i fleire variablar, må ein bruke gröbnerbasar.

Oppgåva byrjar med ein introduksjon til transformasjonar og det projektive planet i to og tre dimensjonar, i kapittel to og tre. I det neste kapittelet blir det forklart korleis ein kan finne og nytte gröbnerbasar til å løyse ikkje-lineære likningar, i kapittel fire. Gröbnerbasar vil bli nytta i kapittel sju, om den essensielle matrisa, når me skal lage ein rekonstruksjonsmetode. I kapittel fem ser me på ein enkel kameramodell, som stegvis blir generalisert til eit endeleg projektiv kamera. Me er då klare for å sjå nærmare på geometrien til eit system med eit punkt i rommet, og to bilete. Etter dette kan me introdusere fundamentalmatrisa, i kapittel seks, og den essensielle matrisa, i kapittel sju.
I kapittel sju vil me løyse ulike problem ved å nytte gröbnerbasar, og Macaulay2-programmet. Macaulay2 er eit program som blir brukt innan algebraisk geometri og kommutativ algebra. I denne oppgåva skal me bruke Macaulay2 til å finne ut om ei matrise er ei essensiell matrise. Og lage ein metode for å dekomponere ei essensiell matrise, og ein metode som finn ut om ein rekonstruksjon har ei endeleg løysing.
I kapittel 2, 3, 5 og 6 vil boka "Multiple View Geometry in computer vision" [4] vere hovudkjelda. Det vil bli oppgjeve om det er brukt andre kjelder. Kapittel 4 er boka "Ideals, Varieties, and Algorithms" [1] brukt som hovudreferanse, med "Gröbner bases in Comutative algebra" [2], og "Concrete Abstract Algebra" [3] som støttelitteratur. Det sjuande kapittelet vil ta utgangspunkt i Tutorial 72 frå "Computational Commutative Algebra" [5].

Kapittel 2

Introduksjon til det projektive planet

I dette kapittelet skal me forklare kva eit projektiv plan er for noko. Me vil også forklare kva ein transformasjon er, og introduserei fire ulike transformasjonar i to dimensjonar.
Me startar med å forklare korleis ein kan finne ut om eit punkt ligg på ei linje. Deretter vil me finne skjeringspunktet til to linjer, og definere korleis me kan finne ei linje som går igjennom to punkt. Dermed kan me sjå på kva som er skjeringspunktet til to parallelle linjer, og ved hjelp av dette definere det projektive planet.
I del 2.2 vil me forklare kva ein transformasjon er, og sjå på korleis linjer blir transformerte. Etterpå ser me på fire ulike transformasjonar: isometri, similaritet, affinitet og projektivitet. Dette kapittelet er ein introduksjon til kapittel tre om projektiv geometri og transformasjonar i tre dimensjonar.

2.1 Det projektive planet

Eit punkt i planet kan representerast med koordinatparet (a, b) i $\mathbb{R}^2$. Dette punktet kan også bli representert som ein vektor $\mathbf{x} = (x, y)^T$ (notasjonen ^{T} betyr transponert), der me tenkjer på $\mathbb{R}^2$ som eit vektorrom.
Ei linje i planet har likninga $ax + by + c = 0$, og kan representerast av vektoren $(a, b, c)^T$. Denne linja, og linja gjeven ved likninga $(ka)x + (kb)y + (kc) = 0$, der $k \neq 0$, representerer same linja. Derfor gir vektorane $(a, b, c)^T$ og $k(a, b, c)^T$ same linja, og er ekvivalente. Slike vektorar hamnar i same ekvivalensklasse og blir kalla homogene vektorar.
Mengda av homogene vektorar i $\{\mathbb{R}^3 - (0, 0, 0)^T\}$ dannar det projektive rommet $\mathbb{P}^2$, der notasjonen $-(0, 0, 0)^T$ betyr at vektoren $(0, 0, 0)^T$, som ikkje gir ei linje, ikkje er med i planet.
Eit punkt $X = (x, y)^T$ ligg på linja $l = (a, b, c)^T$, viss og berre viss $ax + by + c = 0$. Dette kan skrivast som:
$\Rightarrow (x, y, 1)(a, b, c)^T = (x, y, 1) \cdot l = 0.$

Resultat 2.1. *Punktet x ligg på linja l viss og berre viss, $x^T l = l x^T = 0$. Der $x^T l$ er skalarproduktet til dei to vektorane x og l.*

Punktet $X = (x, y)^T$ kan skrivast som ein 3-vektor ved å legge til ein sistekoordinat 1, $X = (x, y, 1)^T$. Me har også at $(kx, ky, k) \cdot l = 0$ viss og berre viss $(x, y, 1) \cdot l = 0$. Derfor kan

punkt skrivast som homogene vektorar akkurat som med linjer. Ein homogen representasjon for ein vektor til eit punkt, er på forma: $X = (x_1, x_2, x_3)^T$, og representerer punktet $(x_1/x_3, x_2/x_3)$ i $\mathbb{R}^2$.
For å kunne spesifisera eit punkt, $X = (x, y)^T$, må ein vite x- og y-koordinatar. Medan ei linje blir spesifisert ved hjelp av to parameter, på grunn av dei uavhengige ratane $\{a : b : c\}$, og har to fridomsgrader.

Resultat 2.2. *Skjeringspunktet til to linjer l og l' er punktet $x = l \times l'$.*

Prov. Me har to linjer $l = (a, b, c)^T$ og $l' = (a', b', c')^T$, og definerer vektoren $x = l \times l'$, der $\times$ er vektor- eller kryssproduktet. Då får me

$$x = l \times l' = (a, b, c)^T \times (a', b', c')^T = \begin{pmatrix} bc' - cb' \\ ca' - ac' \\ ab' - ba' \end{pmatrix}.$$

Me kan finne ut om dette punktet ligg på linja l ved å bruke resultat 2.1,

$$l^T(l \times l') = \begin{bmatrix} a & b & c \end{bmatrix} \cdot \begin{bmatrix} bc' - cb' \\ ca' - ac' \\ ab' - ba' \end{bmatrix} = abc' - ab'c + a'bc - abc' + ab'c - a'bc = 0$$

$$\Rightarrow l^T x = 0.$$

Me ser at dersom x representerer eit punkt, ligg dette punktet på begge linjene. Punktet x er derfor skjeringspunktet til linjene. □

Ved å definere ei linje som $l = x \times x'$, kan ein gjere som over, og få at punkta x og x' ligg på same linje. Dermed få me eit resultat som liknar resultat 2.2.

Resultat 2.3. *Linja gjennom to punkt x og x' er gitt ved: $l = x \times x'$.*

I det projektive planet skjerer to linjer kvarandre i eit enkelt punkt. Og to distinkte punkt ligg på ei enkel linje. Likninga $l^T x = 0$ for ei linje og eit punkt, er symmetrisk sidan det fører til at $x^T l = 0$, der posisjonen til linja og punktet er bytt om, dei er tosidige. Dette gir at resultat 2.2 og resultat 2.3 essensielt er like.

Ideelle punkt og linja i det uendelege

Homogene vektorar $x = (x_1, x_2, x_3)^T$, der $x_3 \neq 0$, korresponderer til punkt i $\mathbb{R}^2$. Ein kan gjere $\mathbb{R}^2$ større ved å leggje til punkt der $x_3 = 0$. Dette rommet inneheld alle dei homogene vektorane og blir kalla det projektive rommet $\mathbb{P}^2$. Punkta med siste koordinat $x_3 = 0$ blir kalla ideelle punkt, eller punkt i det uendelege. Mengda av ideelle punkt ligg på ei linje som blir kalla linja i det uendelege, og er gitt ved $l_\infty = (0, 0, 1)^T$. Me kan sjekk om dette stemmer ved å bruke resultat 2.1, $(0, 0, 1)^T(x_1, x_2, 0) = 0$.
Når $x_3 \neq 0$, kan $\mathbb{P}^2$ bli representert i $\mathbb{R}^3$.
Me har to linjer $l = (a, b, c)$ og $l' = (a, b, c')$ som er parallelle, og nyttar resultat 2.2 for å finne skjeringspunktet,

$$l \times l' = (a, b, c)^T \times (a, b, c')^T = \begin{pmatrix} bc' - cb \\ ac - ac' \\ ab - ba \end{pmatrix} = (c' - c) \begin{pmatrix} b \\ -a \\ 0 \end{pmatrix}.$$

Når me ignorerer skaleringsfaktoren $(c' - c)$ er dette punktet $(b, -a, 0)^T$. Slike punkt gir ikkje endelege punkt i $\mathbb{R}^2$, og det stemmer med at parallelle linjer skjerer kvarandre i det uendelege.

Linja l og den parallelle linja l' skjerer linja i det uendelege, l_∞, i punktet $(b, -a, 0)^T$. I uhomogen notasjon er $(b, -a)$ ein vektor tangent til linja, og ortonormal til linjenormalen (a, b) og representerer retninga til linja. Når linja si retning varierer, varierer også det ideelle punktet $(b, -a, 0)^T$ over l_∞. På grunn av dette kan ein tenkje på linja i det uendelege som mengda av retningar til linjene i planet.
Mengda av vektorar $k(x_1, x_2, x_3)$, der k varierer, dannar ein stråle gjennom origo. Ein slik stråle er representert som eit enkelt punkt i $\mathbb{P}^2$. Denne modellen gir at linjer i $\mathbb{P}^2$, er plan som går gjennom origo, i $\mathbb{R}^3$. To strålar ligg i eit plan, og to plan skjærer kvarandre i ein stråle. Ein kan finne punkt og linjer ved å skjære mengda av strålar og plan med planet $x_3 = 1$. Strålar som representerer ideelle punkt, og planet som representerer l_∞ ligg parallelt til dette planet.

2.2 Transformasjonar

I denne delen blir det gitt ei forklaring på projektive transformasjonar. I tillegg blir også ulike typar projektive transformasjonar, av den projektive lineære gruppa, i tre dimensjonar introdusert. Me byrjar me å sjå på korleis linjer blir transformerte.

Transformering av linjer

Me vil no sjå på korleis linjer blir transformert.

Setning 2.4. Dersom punkt x_i ligg på linja l, då ligg dei transformerte punkta $x_i' = Hx_i$ under ein projektiv transformasjon på linja $l' = (H^{-1})^T l$. Då får ein at under punkttransformasjonen $x' = Hx$ blir ei linje transformert:

$$l' = (H^{-1})^T l. \tag{2.1}$$

Dette også kan skrivast $l'^T = l^T H^{-1}$. Punkt blir transformert i samsvar med H, medan linjer blir transformert i samsvar med H^{-1}.

Prov. Sidan x ligg på linja l har me at $l^T x = lx^T = 0$. Dersom H er ei ikkje-singulær matrise, då er

$$\begin{aligned} & l^T H^{-1} H x = 0 \\ \Rightarrow\ & l^T H^{-1} x' = 0 = x' l'^T \\ \Rightarrow\ & l^T H^{-1} = l'^T. \end{aligned}$$

Punktet Hx, som også kan bli representert som x', ligg på linja $l^T H^{-1}$. Det vil seie at $l'^T = l^T H^{-1} \Leftrightarrow l' = l(H^{-1})^T$. Under transformasjonen er skjeringspunkt på linjer uendra sidan $l'^T x' = l^T H^{-1} H x = l^T x = 0$. □

Projektive transformasjonar dannar ei gruppe som blir kalla den projektive lineære gruppa. Spesialiseringane som blir gjevne i dette delkapittelet er ei delmengd av denne gruppa.
Gruppa av invertible $n \times n$-matriser med reelle element, gir den generelle lineære gruppa på n dimensjonar, $GL(n)$. For å få den projektive lineære gruppa, må matrisene som er relatert

til kvarandre med ein skalarmultiplikasjon, bli identifisert. Då får ein gruppa $PL(n)$, som er ei kvotientgruppe av $GL(n)$. Me skal sjå på projektive transformasjonar i planet $n = 3$.
Viktige delmengder av $PL(3)$ inneheld den affine gruppa, som er ei undergruppe til $PL(3)$, med matriser der den siste raden er $(0, 0, 1)$. Og den euklidske gruppa som er ei undergruppe av den affine gruppa, der addisjon av øvre venstre 2×2-matrisa er ortogonal, dvs. $R^T R = RR^T = I$ og $det(R) = \pm 1$.
No følgjer ein liten presentasjon av fire ulike transformasjonar.

Klasse I: Isometri

Ein isometri er ein transformasjon i planet $\mathbb{R}^2$, som ivaretek euklidisk avstand. Ein isometri er representert som

$$\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = \begin{bmatrix} \epsilon\cos\theta & -\sin\theta & t_x \\ \epsilon\sin\theta & \cos\theta & t_y \\ 0 & 0 & 1 \end{bmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}.$$

Der $\epsilon = \pm 1$. Når $\epsilon = 1$, er orienteringa bevart, og når $\epsilon = -1$ er orienteringa reversert.
Me vil konsentrera oss om euklidske transformasjonar, der $\epsilon = 1$. Ein planar euklidisk transformasjon kan skrivast som

$$\mathbf{x}' = H_E\mathbf{x} = \begin{bmatrix} R & \mathbf{t} \\ \mathbf{0}^T & 1 \end{bmatrix} \mathbf{x}. \tag{2.2}$$

Der R er ei 2×2 ortogonal rotasjonsmatrise (slik at $R^T R = RR^T = I$), $\mathbf{t}$ er ein translasjonsvektor og $\mathbf{0}$ er ein null 2-vektor.
Når ein kun har ein rotasjon, er $\mathbf{t}$ lik 0, og $R = \begin{bmatrix} \epsilon\cos\theta & -\sin\theta \\ \epsilon\sin\theta & \cos\theta \end{bmatrix}$.
Når ein kun har ein translasjon, er $R = I$ og H_E er gjeven ved $\begin{bmatrix} 1 & 0 & t_x \\ 0 & 1 & t_y \\ 0 & 0 & 1 \end{bmatrix}$.
Ein planar euklidisk transformasjon har tre fridomsgrader: ein for rotasjonen og to for transformasjonen. Transformasjonen kan bli funnen frå to punktkorrespondansar. Både lengd, vinkel og areal er invariante eigenskapar.

Klasse II: Similaritetstransformasjon

Ein similaritetstransformasjon er ein isometri, kombinert med ein isotropisk/uniform skalering. I ein euklidisk transformasjon med skalering og utan rotasjon, kan similariteten representerast som

$$\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = \begin{bmatrix} s\cos\theta & -s\sin\theta & t_x \\ s\sin\theta & s\cos\theta & t_y \\ 0 & 0 & 1 \end{bmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix},$$

$$\Rightarrow \mathbf{x}' = H_s\mathbf{x} = \begin{bmatrix} sR & t \\ 0^t & 1 \end{bmatrix} \mathbf{x}, \tag{2.3}$$

der s representerer den isotropiske skaleringa. Skaleringa er den same i alle retningane og fører til at figuren blir forstørra eller forminska.
Ein planar similaritetstransformasjon har fire fridomsgrader. Skaleringa gir ein fridomsgrad meir enn ein euklidisk transformasjon, og kan blir funnen frå to punktkorrespondansar. Vinkel, lengderatar og arealratar er alle invariante eigenskapar.

Klasse III: Affin Transformasjon

Ein affin transformasjon, også kalla ein affinitet, er ein ikkje-singulær lineær transformasjon i lag med ein translasjon. Den kan representerast som

$$\begin{pmatrix} x' \\ y' \\ 1 \end{pmatrix} = \begin{bmatrix} a_{11} & a_{12} & t_x \\ a_{21} & a_{22} & t_y \\ 0 & 0 & 1 \end{bmatrix}.$$

Dette kan skrivast som

$$\mathbf{x}' = H_A\mathbf{x} = \begin{bmatrix} A & \mathbf{t} \\ \mathbf{0}^T & 1 \end{bmatrix}\mathbf{x}, \tag{2.4}$$

der A er ei ikkje-singulær 2×2-matrise.
Transformasjonen har seks fridomsgrader, fordi den har seks element. Og kan finnast frå tre punktkorrespondansar. Invariantar er: parallelle linjer, raten av lengda til parallelle linjesegment og arealraten.
Ein kan dekomponere matrisa: $A = R(\theta)R(-\phi)DR(\phi)$, der $R(\phi)$ og $R(\theta)$ er rotasjonar med ϕ og θ. Og D er diagonalmatrisa $D = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$.
Den affine matrisa A er derfor ein rotasjon med ϕ, ein skalering med λ_1 i x-retning og λ_2 i y-retning. Deretter ein rotasjon tilbake med $-\phi$ og ein rotasjon med θ. Det einaste som er endra i forhold til ein similaritet er den ikkje-isotropiske skaleringa. Det vil seie at skaleringa kan vere ulik i x- og y-retning. Dette gir dei to ekstra fridomsgradene, vinkelen ϕ som gir skaleringsretninga og raten til skaleringsparametra $\{\lambda_1 : \lambda_2\}$. Ein affinitet ivaretek orienteringa dersom $det(A)$ er positiv, og orienteringa er reversert når $det(A)$ er negativ. Sidan $det(A) = \lambda_1\lambda_2$, er eigenskapen kun avhengig av forteiknet til skaleringa.

Klasse IV: Projektive transformasjonar

Ein projektiv transformasjon, er ein generell ikkje-singulær transformasjon av homogene koordinatar og ein translasjon. Ein projektiv transformasjon kan skrivast som,

$$\begin{pmatrix} x'_1 \\ x'_2 \\ x'_3 \end{pmatrix} = \begin{bmatrix} a_{11} & a_{12} & t_x \\ a_{21} & a_{22} & t_y \\ v_1 & v_2 & u \end{bmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

$$\Rightarrow \mathbf{x}' = H_p\mathbf{x} = \begin{bmatrix} A & \mathbf{t} \\ \mathbf{v}^T & u \end{bmatrix}\mathbf{x}, \tag{2.5}$$

der $\mathbf{v} = (v_1, v_2)^T$.
Transformasjonen er spesifisert av åtte parameter. Ein projektiv transformasjon mellom to plan kan bli funnen frå fire punktkorrespondansar. Det er ikkje mogleg å skilje mellom projektivitetar som ivaretek orienteringa og reverserer orienteringa i $\mathbb{P}^2$.

I det neste kapittelet får me brukt for det som er gitt i dette kapittelet.

Kapittel 3

Projektiv geometri og transformasjonar i 3D

I dette kapittelet skal me sjå på det projektive planet i tre dimensjonar, eller $\mathbb{P}^3$. Det er fleire likskapar til det førre kapittelet. Både dette kapittelet og kapittel to gir ei forståing for projektiv geometri som er greit å ha seinare i oppgåva. Når me i seinare kapittel skal sjå på situasjonen der me har to kamera og eit verdspunkt, gir kapittel to og tre ei betre forståing for situasjonen. Me vil vise korleis punkt og plan blir representerte som homogene vektorar. Og deretter vil me sjå på to spesielle situasjonar. Nemleg at tre punkt definerer eit plan, og at tre plan definerer eit punkt.
I $\mathbb{P}^3$ er mengda av ideelle punkt, på planet i det uendelege. Dette planet blir kalla π_∞. Dette er analogt til linja i det uendelege, l_∞, i $\mathbb{P}^2$. Og me har derfor at i $\mathbb{P}^3$ skjerer parallelle linjer, og parallelle plan kvarandre på planet i det uendelege, π_∞.

3.1 Punkt og projektive transformasjonar

Eit 3D-punkt i homogene koordinatar er ein 4-vektor som kan skrivast som: $X = (x_1, x_2, x_3, x_4)^T$. Når $x_4 \neq 0$ representerer dette punktet $(x, y, z)^T$, i $\mathbb{R}^3$, med dei inhomogene koordinatane:

$$x = x_1/x_4, y = x_2/x_4, z = x_3/x_4.$$

Homogene punkt med $x_4 = 0$ er punkt som ligg på planet i det uendelege.
Ein projektiv transformasjon som verkar på $\mathbb{P}^3$, er ein lineær transformasjon på homogene 4-vektorar representert av ei ikkje-singulær 4×4-matrise: $X' = HX$. Matrisa H er homogen og har 15 fridomsgrader.
Transformasjonen fungerer slik som i $\mathbb{P}^2$. Og som planare transformasjonar er avbildinga kolineær (linjer blir avbilda til linjer), og forhold som skjeringspunkt for ei linje og eit plan blir ikkje endra.

3.2 Representasjon og transformasjon av plan

I $\mathbb{P}^3$ er punkt og plan tosidige. Det er tilsvarande til at punkt og linjer er tosidige i $\mathbb{P}^2$, sjå kapittel to. Det vil seie at me kan bytte om på rollene deira, og dermed få "like" formlar. Eit plan i 3-rom kan skrivast som

$$\pi_1 x + \pi_2 y + \pi_3 z + \pi_4 = 0. \tag{3.1}$$

Plan har tre fridomsgrader og er uendra ved multiplikasjon med ein skalar som er ulik null. Ein homogen representasjon av 4-vektoren er $\pi = (\pi_1, \pi_2, \pi_3, \pi_4)^T$.
Homogeniseringa av planet får ein ved å gjere byta: $x \to x_1/x_4, y \to x_2/x_4$ og $z \to x_3/x_4$. Dette gir $\pi_1 x_1 + \pi_2 x_2 + \pi_3 x_3 + \pi_4 x_4 = 0$, som forkorta blir

$$\pi^T X = 0. \tag{3.2}$$

Ein har då at punktet X ligg i planet π. Eit plan er definert eintydig ved å samanføye tre punkt, eller ei linje og eit punkt. To distinkte plan skjerer kvarandre i ei eintydig linje. Og tre distinkte plan har skjeringspunkt i eit eintydig punkt. Me skal no sjå nærmare på tilfella der tre punkt definerer eit plan, og der tre plan definerer eit punkt.

Tre punkt definerer eit plan

Me har tre punkt X_1, X_2 og X_3, som ligg på planet π. Punkta tilfredsstillar derfor likning (3.2) og $\pi^T X_i = 0$ for $i = 1, 2, 3$. Dette gir

$$\begin{bmatrix} X_1^T \\ X_2^T \\ X_3^T \end{bmatrix} \pi = 0. \tag{3.3}$$

I generell posisjon er punkta lineært uavhengige, og 3×4-matrisa, laga av punkta, har rang tre. Planet π, definert av punkta er funnen unikt som det ein-dimensjonale nullrommet. Dersom matrisa har rang 2 er nullrommet todimensjonalt. Punkta er kolineære (dei ligg på same linje), og definerer ein pensel av plan ("pencil of planes"), med linja danna av dei kolineære punkta som akse. Ein pensel av plan er mengda av alle plan gjennom ei linje/akse.
Me definerer matrisa M som $\{X, X_1, X_2, X_3\}$. Denne matrisa er laga av det generelle punktet X og dei tre andre punkta X_i, som definerer planet π. Determinanten $det(M) = 0$ når X ligg på π, sidan ein då kan uttrykke X som ein lineær kombinasjon av punkta $X_i, i = 1, 2, 3$. Ved å utvide determinanten om kolonna X får ein at,
$det(M) = x_1 D_{234} - x_2 D_{134} + x_3 D_{124} - x_4 D_{123}$.
Der D_{jkl} er determinanten frå jkl -rada av 3×4-matrisa $[X_1, X_2, X_3]$ og $X = (x_1, x_2, x_3, x_4)^T$.
Sidan $det(M) = 0$ for punkt på π, er koeffisientane til planet:

$$\pi = (D_{234}, -D_{134}, D_{124}, -D_{123})^T. \tag{3.4}$$

Dette er nullrommet til likning (3.3).

Tre plan definerer eit punkt

Dette er likt med tilfellet der tre punkt definerer eit plan. Skjeringspunktet mellom punktet X og dei tre plana π_i, kan bli funnen som det høgre nullrommet til 3×4-matrisa gjeve av,

$$\begin{bmatrix} \pi_1^T \\ \pi_2^T \\ \pi_3^T \end{bmatrix} X = 0. \tag{3.5}$$

Løysinga er analog til likning (3.4).

Dei to neste resultata er analog til resultat i 2D, sjå transformering av linjer.

Resultat 3.1. *Projektiv transformasjon. Under punkttransformasjonen $X' = HX$, blir planet transformert som:*

$$\pi' = (H^{-1})^T \pi. \tag{3.6}$$

Resultat 3.2. *Parametriserte punkt på eit plan. Punkta X på planet π, kan skrivast som*

$$X = Mx. \tag{3.7}$$

Kolonnane til 4×3-matrisa M genererer nullrommet (med rang 3) av π^T, ($\pi^T M = 0$). Me har at 3-vektoren x, som er eit punkt på det projektive planet $\mathbb{P}^2$, parametriserer punkt på planet π.

Kapittel 4

Gröbnerbasar

I dette kapittelet skal me beskrive ein metode som gir ein enkel beskriving av felles nullpunkt, for ei endeleg mengde med polynomlikningar. Dei fleste har erfaring med å løyse ei mengd av lineære likningar, der ein brukar Gaussisk eliminering eller rekkereduksjon.
Me har gitt likningssystemet

$$2x + y = 1$$
$$x - y = 5.$$

Me kan bruke ein av likningane til å finne eit uttrykk for x (eller y), og set det inn i den andre likninga. Me vil då få ut ein verdi for y, slik at me kan finne verdi av x. Men korleis kan ein løyse ikkje-lineære likningar, der variablane har større grad enn ein? Til dette treng ein gröbnerbasar, som er ei generalisering av Gaussisk eliminering/rekkereduksjon.
Me byrjar kapittelet med å definere omgrepet monom og forklare kva ei monomialordning er. Seinare blir desse ordningane brukt når me skal finne ein gröbnerbase. Me vil også definere ideal og monomialideal. Og deretter forklare nokre av eigenskapane til ideal, som me skal bruke i kapittel sju. Det vil bli gitt ein definisjon på affinitet, og ei forklaring av divisjonsalgoritmen i ein og fleire variablar. Når me har gjort dette er me klare til å forklare Hilbert sitt basisteorem, som seier at alle ideal er endeleg genererte. Me kan då gi ein definisjon på gröbnerbasar og forklare korleis me kan konstruere ein gröbnerbase ved å bruke Buchberger sin algoritme. Kapittelet sluttar med ein introduksjon til eliminasjonsordningar som i kapittel sju blir brukt når me skal dekomponere ei essensiell matrise.

4.1 Monomialordningar

Når me skal finne ein fin base for eit ideal I, må me ha ein systematisk måte for å byte ut polynom, med polynom av lågare grad eller med færre ubestemte variablar. For dei som har lært om lineær algebra, er det dette ein gjer når ein vil redusere ei matrise.
Me byrjar dette delkapittelet med å gi ein definisjon på monom og polynom. Deretter vil me forklare omgrepet monomialordningar og gi døme på slike ordningar.

Definisjon 4.1. Eit monom gitt i variablane $x_1, \ldots, x_n$ er eit produkt på forma $x_1^{a_1} \cdot x_2^{a_2} \cdot \ldots \cdot x_n^{a_n} = \mathbf{x^a}$, der eksponentane $a_1, \ldots, a_n$ ikkje er negative tal, $\mathbf{a} \geq 0$. Den totale graden til monomet er summen $a_1 + \ldots + a_n$.

Nokre døme på monom er x_1^2 og $x_1^2 x_2^2 x_3$. Me vil også definere omgrepet polynom, trass i at det er eit omgrep som mange kjenner til.

Definisjon 4.2. Eit polynom f i $x_1, \ldots, x_n$ med koeffisientar i kroppen k er ein endeleg lineær kombinasjon av monom. Me skriv eit polynom f på forma $f = \sum_{\mathbf{a}} b_{\mathbf{a}} x^{\mathbf{a}}, b_{\mathbf{a}} \in k$,
der summen er over eit endeleg tal med n-tuplar, $\mathbf{a} = (a_1, \ldots, a_n)$. Mengda av alle polynom i $x_1, \ldots, x_n$ med koeffisientar i k, skriv me som $k[x_1, \ldots, x_n]$.

Av definisjonen har me at eit polynom er bygd opp av monom, og at eit monom også er eit polynom. Me ser på polynomet $f = 2x^2 + x$, dette er ikkje eit monom. Me har derfor at eit polynom kan vere eit monom, men at dette ikkje alltid er tilfellet.

Me har at eit polynom er ein sum av monom og me vil skrive polynomet slik at det største monomet står først, og resten av monoma står i minkande orden. For å gjere dette må me ha ein måte som samanliknar monoma og bestemmer kva monom som er størst. Me krev derfor at ordninga er ei total ordning. Det vil seie at for kvart par av monom x^a og x^b så er kun ein av desse sanne:

$$x^a > x^b, x^a = x^b, x^a < x^b.$$

Ein total ordning er også transitiv slik at dersom $x^a > x^b$ og $x^b > x^c$ fører dette til at $x^a > x^c$.
Når me har likningar i ein variabel kan ein enkelt finne ut kva monom som er størst ved å sjå på graden til variabelen. Men når me har likningar med fleire ukjende er det ikkje intuitivt å vite kva monom som er størst, og kva som er minst. Me må derfor introdusere ei ordning slik at me kan samanlikne monom av fleire variablar, og dermed bestemme kva monom som er størst av t.d. x_2^2 og $x_1 x_3^2$ (for $x_1 > x_2 > x_3$).
Ei monomialordning brukar ein når ein skal rekkeredusere ei matrise til redusert trappeform. Monomialordningar blir også nytta når ein skal dividere. Dette kjem me nærmare inn på under delkapittelet om divisjonsalgoritmen.
Me vil først definere omgrepet monomialordning, og vise korleis ei monomialordning fungerer ved å vise ulike ordningar. Det fins mange ulike monomialordning, men i denne oppgåva vil me presentere leksikografisk ordning, og forklare omvendt og gradert leksikografisk ordning. For å forstå forskjellen på desse vil me gi nokre dømer.

Definisjon 4.3. Ei monomialordning $>$ på $k[x_1, \ldots, x_n]$ er ein relasjon på $\mathbb{Z}_{\geq 0}^n$, eller ein relasjon på mengda av monom $x^a, a \in \mathbb{Z}_{\geq 0}^n$, som tilfredsstillar:
i) $>$ er ein total (eller lineær) ordning på $\mathbb{Z}_{\geq 0}^n$.
ii) viss $a > b$ og $c \in \mathbb{Z}_{\geq 0}^n$, då er $a + c > b + c$.
iii) $>$ er ein velordning på $\mathbb{Z}_{\geq 0}^n$. Dette betyr at alle ikkje-tomme delmengder av $\mathbb{Z}_{\geq 0}^n$ har eit minsteelement under $>$.

Det neste lemmaet blir brukt i provet av divisjonsalgoritmen, for å vise at algoritmen til slutt må stoppe. Dette er fordi nokre ledd minkar strengt ved kvart steg i algoritmen. Lemmaet vil også bli brukt til å vise at ei leksikografisk ordning er ei monomialordning.

Lemma 4.4. *Ei ordning $>$ på $\mathbb{Z}_{\geq 0}^n$ er ei velordning viss og berre viss alle strengt minkande sekvensar i $\mathbb{Z}_{\geq 0}^n$*

$$a(1) > a(2) > \ldots$$

til slutt stoppar.

Prov. Gå utifrå at $>$ ikkje er ein velordning. Det skjer viss og berre viss det er ein uendeleg strengt minkande sekvens i $\mathbb{Z}_{\geq 0}^n$. Då fins det ei delmengd S i $\mathbb{Z}_{\geq 0}^n$ som ikkje har noko minste element. Me vel $a(1) \in S$. Sidan $a(1)$ ikkje er det minste elementet, kan me finne ein $a(2)$ slik at $a(1) > a(2)$ i S. Igjen er ikkje $a(2)$ det minste elementet, så då fins det ein $a(3)$ slik at $a(2) > a(3)$ i S. Når ein fortset slik får me ei uendeleg strengt minkande rekkjefølgje

$$a(1) > a(2) > a(3) > \ldots.$$

Omvendt, gitt ei slik uendeleg rekkjefølgje då er $\{a(1), a(2), a(3), \ldots\}$ ei delmengd av $\mathbb{Z}_{\geq 0}^n$ utan minste element, og derfor er ikkje $>$ ei velordning. Ei velordning må derfor ha ei endeleg rekkjefølgje. □

Me skal no gi nokre døme på monomialordningar og vise forskjellen ved å gi nokre eksempel. Me seier at x^a og x^b er to monom og gir definisjonen på leksikografisk ordning.

Definisjon 4.5. Leksikografisk ordning, (lex). Me har at $x^a < x^b$, viss enten $\sum_{i=1}^n a_i < \sum_{i=1}^n b_i$ eller $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$. Og komponenten lengst til venstre av $a - b$ (som ikkje er null) er positiv. Me skriv $x^a <_{lex} x^b$. [2]

I leksikografisk ordning set ein den komponenten med størst førstekomponent, som det største elementet. Det er dette systemet som blir brukt til å ordne ord i ordbøker, derfor har ordninga fått namnet leksikografisk. I ei ordbok ser me at ordet *val* står før ordet *vri*. Sidan begge orda byrjar med bokstaven v ser me på den andre bokstaven. Den andre bokstaven det i første ordet er a som kjem før r i alfabetet, og me har derfor at $val >_{lex} vri$. Me vil no gå tilbake til å snakke om monom og me har at $x_1 > x_2 > x_3$. Og sidan x_1^3 er større enn x_1^2, er også x_1^3 større enn $x_1^2 x_2^3$. For å få ei betre forståing for ordninga gir me eit eksempel som ordnar monom ved å bruke lex-orden.

Eksempel 1. Me får denne rekkjefølgja av monom:

$$x_1^3 >_{lex} x_1^2 x_2^2 >_{lex} x_1^2 x_2 >_{lex} x_1^2 x_3^2 >_{lex} x_2^2 >_{lex} x_3^2,$$

der $x_1 > x_2 > x_3$ og ein brukar leksikografisk ordning.

Resultat 4.6. *Leksikografisk ordning på $\mathbb{Z}_{\geq 0}^n$ er ei monomialordning.*

Prov. Brukar definisjon 4.3:
i) $>_{lex}$ er ein total ordning følgjer frå definisjonen på lex-orden.
ii) Viss $a >_{lex} b$, då er komponenten lengst til venstre, som me kallar $a_k - b_k$, i $a - b$ positiv. Og me har $x^a \cdot x^c = x^{a+c}$ og $x^b \cdot x^c = x^{b+c}$. Då har me $(a + c) - (b + c) = a - b$, og komponenten lengst til venstre er framleis $a_k - b_k$, som er positiv. Me får då at $a + c > b + c$.
iii) Antek at $>_{lex}$ ikkje er ei velordning. Då ved lemma 4.4 fins det ei uendeleg strengt minkande rekkjefølgje

$$a(1) >_{lex} a(2) >_{lex} \ldots$$

på element av $\mathbb{Z}_{\geq 0}^n$. Me vil vise at dette fører til ei motseiing.
Me ser på dei første komponentane til vektoren $a(i) \in \mathbb{Z}_{\geq 0}^n$. Frå definisjonen på leksikografisk ordning dannar desse ei rekkjefølgje av ikkje-negative tal, som ikkje aukar. Sidan $\mathbb{Z}_{\geq 0}^n$ er ei velordning må komponentane til $a(i)$ til slutt bli stabiliserte. Det vil seie at det eksisterer ein k slik at alle komponentar av $a(i)$ med $i \geq k$ er like.
Me byrjar ved $a(k)$, den neste og etterfølgjande komponentar blir brukt for å bestemme den leksikografiske ordninga. Den andre komponenten av $a(k)$, $a(k+1)$, ... dannar ei rekkjefølgje som ikkje aukar. Ved å nytta same argumentasjon som over vil også dei andre komponentane til slutt stabilisera seg. Ved å fortsette på denne måten ser ein at for nokre m er alle $a(m), a(m+1), \ldots$ like. Dette er ei motseiing sidan me har at $a(m) >_{lex} a(m+1)$. □

Me gir no definisjonen på to monomialordningar; omvendt leksikografisk ordning og gradert leksikografisk ordning. Prov for at desse to ordningane er monomialordningar vil ikkje bli gjeve, men ein kan vise det ved å bruke definisjonen på ei monomialordning.

Definisjon 4.7. Omvendt leksikografisk ordning. Me har at $x^a < x^b$, viss enten $\sum_{i=1}^n a_i < \sum_{i=1}^n b_i$ eller $\sum_{i=1}^n a_i = \sum_{i=1}^n b_i$. Og komponenten lengst til høgre av $a - b$ (som ikkje er null), er positiv. [2]

I omvendt leksikografisk ordning set ein det monomet med største minste-komponent, som det minste elementet. Sidan x_2^3 er mindre enn x_2^2, er også $x_1^2 x_2^3$ mindre enn x_2^2.

Eksempel 2. Eit døme på omvendt leksikografisk ordning:

$$x_1^3 > x_1^2 x_2 > x_1^2 x_2 > x_2^2 > x_1^2 x_3^2 > x_3^2,$$

der $x_1 > x_2 > x_3$. Me har brukt dei same monoma som i eksempel 1, og når me samanliknar desse eksempla ser me at $x_1^2 x_3^2 >_{lex} x_2^2$, medan i omvendt leksikografisk har me $x_2^2 > x_1^2 x_3^2$. Det er fordi x_3^2 er den største minste-komponenten.

I leksikografisk ordning dominerar alle monom med mindre variabel uansett total grad. Viss me har $x > y > z$, så er $x >_{lex} y^7 z^5$. Dersom me vil ta omsyn til dette kan me bruke gradert leksikografisk ordning.

Definisjon 4.8. Gradert Leksikografisk ordning, (grlex). La $a, b \in \mathbb{Z}_{\geq 0}^n$. Me seier at $a >_{grlex} b$ viss

$$|a| = \sum_{i=1}^n a_i > |b| = \sum_{i=1}^n b_i,$$

eller

$$|a| = |b| \text{og} a >_{lex} b.$$

Gradert leksikografisk ordning ordnar først etter total grad, deretter brukar den leksikografisk ordning for å skilje dei monoma som har lik grad.

Eksempel 3. Me brukar dei same monoma som i eksempel 1 og 2, og ordnar dei etter gradert leksikografisk ordning. Då får ein

$$x_1^2 x_2^2 >_{grlex} x_1^2 x_3^2 >_{grlex} x_1^3 >_{grlex} x_1^2 x_2 >_{grlex} x_2^2 >_{grlex} x_3^2,$$

der $x_1 > x_2 > x_3$. Me ser først på graden til monoma og dersom graden er lik, ordnar me monoma ved å bruke *lex*-orden.

Me har no definert omgrepet monomialordning og sett på dømer med *lex*-orden, og gradert og omvendt leksikografisk orden. Desse ordningane blir brukt seinare i kapittelet.

4.2 Affin varitet og ideal i polynomringar

Me byrjar dette delkapittelet med å gi ein definisjon og eit eksempel på affin varitet. Deretter definerer me kva eit ideal er, og korleis ein kan finne summen og skjeringa til to ideal. Når me har gjort dette vil me relatere ideal til affin varitet, og gi Dickson sitt lemma. Seinare i dette kapittelet skal me bruke dette til å løyse ikkje-lineære likningar.

Definisjon 4.9. La k vere eit felt, og la $f_1, \ldots, f_s$ vere polynom i $k[x_1, \ldots, x_n]$. Då set me

$$V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n : f_i(a_1, \ldots, a_n) = 0, \ \forall 1 \leq i \leq s\}.$$

Me kallar $V(f_1, \ldots, f_s)$ for den affine variteten definert av $f_1, \ldots, f_s$.

Ein affin varitet er derfor mengda av alle løysingar til likningssystemet

$$f_1(x_1, \ldots, x_n) = \ldots = f_s(x_1, \ldots, x_n) = 0.$$

Altså alle felles nullpunkt til $f_1, \ldots, f_s$.

Dersom me har ei kjegle $\{(x, y, z) : x^2 + y^2 + z^2 = 0\}$, kan me uttrykke dette som ein varitet $V(x^2 + y^2 + z^2)$. Denne variteten korresponderer til likninga $x^2 + y^2 + z^2 = 0$. Det er også fleire polynom som forsvinn på denne variteten.

Eksempel 4. Me set $k = \mathbb{R}$, og ser på planet $\mathbb{R}^2$. Me har variteten $V(x^2 + y^2 - 1)$. Dette er ein sirkel med radius ein og sentrum i origo.

Me vil no definere ideal og gi nokre døme på ideal.

Definisjon 4.10. Ei delmengd $I \subset k[x_1, \ldots, x_n]$, er eit ideal viss det tilfredsstillar:
i) $0 \in I$.
ii) Viss $f, g \in I$, då er $f + g \in I$.
iii) Viss $f \in I$, og $h \in k[x_1, \ldots, x_n]$, då er $h \cdot f \in I$.

Her er eit eksempel på eit ideal generert av ei endeleg mengd med polynom.

Definisjon 4.11. La $f_1, \ldots, f_s$ vere polynom i $k[x_1, \ldots, x_n]$. Då let me

$$\langle f_1, \ldots, f_s \rangle = \Big\{ \sum_{i=1}^{s} h_i f_i : h_1, \ldots, h_s \in k[x_1, \ldots, x_n] \Big\}.$$

Me har at $\langle f_1, \ldots, f_s \rangle$ er eit ideal. Dette viser me i det neste lemmaet.

Lemma 4.12. *Viss $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, då er $\langle f_1, \ldots f_s \rangle$ eit ideal av $k[x_1, \ldots, x_n]$. Me seier at $\langle f_1, \ldots f_s \rangle$ er idealet generert av $f_1, \ldots, f_s$.*

Prov. Må finne ut om $\langle f_1, \ldots f_s \rangle$ er eit ideal, og sjekkar om krava i definisjon 4.10 er oppfylt:
i) $0 \in \langle f_1, \ldots f_s \rangle$, sidan $0 = \sum_{i=0}^{s} 0 \cdot f_i$.
ii) Antek at $f = \sum_{i=1}^{s} p_i f_i$ og $g = \sum_{i=1}^{s} q_i f_i$. Då får ein

$$f + g = \sum_{i=1}^{s} (p_i + q_i) f_i$$

som ligg i $k[x_1, \ldots, x_n]$.
iii) Let h vere i $k[x_1, \ldots, x_n]$. Og me har at

$$hf = \sum_{i=1}^{s} (hp_i) f_i$$

som ligg i $k[x_1, \ldots, x_n]$. Og me har at $\langle f_1, \ldots f_s \rangle$ er eit ideal. □

Me seier at eit ideal I er endeleg generert, viss det eksisterer $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$, slik at $I = \langle f_1, \ldots, f_s \rangle$. Me kallar $\langle f_1, \ldots, f_s \rangle$ for ein basis av I. Dette skal me komme tilbake til under avsnittet om Hilbert sitt basisteorem, der viser me at alle ideal av $k[x_1, \ldots, x_n]$ er endeleg generert. Me kan finne fleire ulike basar for eit ideal. Seinare i kapittelet skal me finne ein spesiell basetype, som blir kallar gröbnerbase.

Resultat 4.13. *Viss $f_1, \ldots, f_s$ og $g_1, \ldots, g_t$ er basis for same ideal i $k[x_1, \ldots, x_n]$, slik at $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$, då har me $V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t)$. s. 32, [1].*

Dette betyr at me kan byte basis utan at variteten blir endra. Og dette fører til observasjonen, at affine varitetar er bestemt av ideal, og ikkje likningar, som me skal komme inn på under kapittel 4.4. Me vil også sjå at dette resultatet saman med gröbnerbasar gir ein måte å forstå affine varitetar på.
No vil me sjå på alle polynom som forsvinner på ein gjeven varitet.

Definisjon 4.14. La $V \subset k^n$ vere ein affin varitet. La

$$I(V) = \{f \in k[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0,\ \forall (a_1, \ldots a_n) \in V\}.$$

Me har at $I(V)$ er eit ideal, som me viser i provet for det neste lemma.

Lemma 4.15. *Viss $V \subset k^n$ er ein affin varitet, då er $I(V) \subset k[x_1, \ldots, x_n]$ eit ideal. Me kallar $I(V)$ for idealet til V.*

Prov. Brukar definisjon 4.10.
i) $0 \in I(V)$, sidan nullpolynomet forsvinner for alle k^n, forsvinn det også på V.
ii) Anta at $f, g \in I(V)$ og la $(a_1, \ldots a_n)$ vere eit punkt i V. Då er

$$f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) = 0 + 0 = 0.$$

iii) Anta at $h \in k[x_1, \ldots, x_n]$. Då er

$$h(a_1, \ldots, a_n) f(a_1, \ldots, a_n) = h(a_1, \ldots, a_n) \cdot 0 = 0.$$

Og me har at $I(V)$ er eit ideal. □

I kapittel sju vil me vise om eit ideal er eit radikalt ideal. Me gir derfor ein definisjon på kva eit radikalt ideal er.

Definisjon 4.16. Eit ideal I er eit radikalt ideal viss $f^m \in I$ for nokre $m \leq 1$ gjer at $f \in I$.

Sum og skjering av ideal

I denne delen blir det gjeve ein definisjon på summen og skjering av to ideal. Og me vil vise at desse mengdene også er eit ideal. Desse resultata blir brukt i kapittel sju, når me skal skrive metodar i Macaulay2.

Definisjon 4.17. Viss I og J er ideal til ringen $k[x_1, \ldots, x_n]$, då er summen av I og J, $I + J$, mengda

$$I + J = \{f + g : f \in I, g \in J\}.$$

Me har no ein definisjon på summen av to ideal og me vil vise at denne summen også er eit ideal.

Resultat 4.18. *Viss I og J er ideal i $k[x_1, \ldots, x_n]$, då er $I + J$ eit ideal i $k[x_1, \ldots, x_n]$. Idealet $I + J$ er det minste idealet som inneheld I og J. Viss $I = \langle f_1, \ldots, f_r \rangle$ og $J = \langle g_1, \ldots, g_s \rangle$, då er $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$.*

Prov. Brukar definisjon 4.10 for å vise at $I + J$ er ei ideal.
i) Me har at $0 = 0 + 0 \in I + J$.
ii) Anta at $h_1, h_2 \in I + J$. Frå definisjonen av $I + J$ finns det $f_1, f_2 \in I$ og $g_1, g_2 \in J$ slik at

$$\begin{aligned} h_1 = f_1 + g_1, h_2 = f_2 + g_2 \\ \Rightarrow h_1 + h_2 = (f_1 + f_2) + (g_1 + g_2). \end{aligned}$$

Sidan I er eit ideal har me at $f_1 + f_2 \in I$, og $g_1 + g_2 \in J \Rightarrow h_1 + h_2 \in I + J$.
iii) Må sjekke om $I + J$ er lukka under multiplikasjon. La $h \in I + J$ og $l \in k[x_1, \ldots, x_n]$ vere eit tilfeldig polynom. Då fins det $f \in I$ og $g \in J$, slik at $h = f+g$. Me har at $l \cdot h = l \cdot (f+g) = lf+lg$, og at $lf \in I$ og $lg \in J$. Derfor må me ha $lh \in I + J$.
Me har vist at $I+J$ er eit ideal. Og vil no vise at dette idealet er det minste idealet som inneheld I og J.
Viss H er eit ideal som inneheld I og J, då må H innehalde alle element $f \in I$ og $g \in J$. Sidan H er eit ideal må det innehalde alle $f + g$, og $H \supset I + J$. Alle ideal som inneheld I og J må innehalde $I + J$, og derfor må $I + J$ vere det minste idealet.
Til slutt vil me vise den siste delen av resultatet. Viss $I = \langle f_1, \ldots, f_r \rangle$ og $J = \langle g_1, \ldots, g_s \rangle$ då er $\langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$ eit ideal som inneheld $I + J$, slik at $I + J \subset \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$. Me har også $\langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle \subset I + J$ slik at $I + J = \langle f_1, \ldots, f_r, g_1, \ldots, g_s \rangle$. □

Definisjon 4.19. Skjeringa $I \cap J$ av to ideal I og J i $k[x_1, \ldots, x_n]$ er mengda av polynom som høyrer til både I og J.

Me vil no vise at denne skjeringa også er eit ideal.

Resultat 4.20. *Viss I og J er ideal i $k[x_1, \ldots, x_n]$, då er $I \cap J$ eit ideal.*

Prov. Brukar definisjonen av eit ideal.
i) Ser at $0 \in I \cap J$ sidan $0 \in I$ og $0 \in J$.
ii) Viss $f, g \in I \cap J$ då er $f + g \in I$ fordi $f, g \in I$. På same måte har me $f + g \in J$. Og ein ser at me må ha $f + g \in I + J$.
iii) Må sjekke at idealet er lukka under multiplikasjon. La $f \in I \cap J$ og la h vere eit polynom i $k[x_1, \ldots, x_n]$. Sidan $f \in I$ og I er eit ideal har me at $fh \in I$, og like eins for idealet J har me at $fh \in J$. Derfor må $fh \in I \cap J$. □

Både summen av ideal og skjering av ideal blir brukt når me skal lage metodar i kapittel 7.

4.3 Divisjonsalgoritmen

Byrjinga av dette kapittelet starta med ein forklaring på monomialordningar. Dette skal me no gjere oss nytte av når me skal gjere polynomdivisjon i fleire variablar. Divisjonsalgoritmen skal me bruke for å finne ut om eit polynom ligg i eit ideal. Gitt ein $f \in k[x_1, \ldots, x_n]$ og eit ideal $I = \langle f_1, \ldots, f_s \rangle$, vil me finne ut om me har $f \in I$.
For å få ei forståing for korleis me skal gjere polynomdivisjon med fleire polynom, gir me først divisjonsalgoritmen i ein variabel. Me byrjar med å definere kva eit leiande ledd er for noko, og deretter kjem divisjonsalgoritmen i ein variabel. For å forklare korleis me brukar algoritmen viser me eit eksempel før me gir provet for algoritmen. Når ein har fått ein forståing av korleis denne algoritmen fungerer kan me utvide algoritmen til tilfella med fleire variablar. Me vil avslutte dette delkapittelet med å gjere eit eksempel der me må bruke divisjonsalgoritmen for fleire variablar.

Definisjon 4.21. Gitt eit polynom $f \in k[x]$, la

$$f = a_0 x^m + a_1 x^{m-1} + \ldots + a_m,$$

der $a_i \in k$ og $a_0 \neq 0$. Då seier me at $a_0 x^m$ er det leiande leddet til f, og skriv $LT(f) = a_0 x^m$. Og me har at graden til f er lik m, som kan skrivast $deg(f) = m$.

Me ser på polynomet $f = 4x^3 + 2x^2 + 3$. For dette polynomet er det leiande leddet $4x^3$, altså at $LT(f) = 4x^3$. Og graden til polynomet er tre, $deg(f) = 3$.
Me har også at

$$deg(f) \leq deg(g) \Leftrightarrow LT(f) delerLT(g). \tag{4.1}$$

Denne observasjonen blir brukt når me skal gi eit prov for divisjonsalgoritmen.

Resultat 4.22. ***Divisjonsalgoritmen i ein variabel.*** *La k vere ein kropp og la g vere eit polynom i $k[x]$. Då kan alle $f \in k[x]$ skrivast som*

$$f = qg + r,$$

der $q, r \in k[x]$, og enten er $r = 0$ eller $deg(r) < deg(g)$. Me har også at q og r er unike og det eksisterer ein algoritme for å finne dei.
Algoritmen byrjar med at me har

$$f = pq + r,$$

viss $r \neq 0$ og $LT(g)$ delar $LT(r)$ gjer me eit byte; $q' = q + \frac{LT(r)}{LT(g)}$ og $r' = r - \frac{LT(r)}{LT(g)}g$. Me fortset med å byte fram til $r = 0$ eller at $LT(g)$ ikkje delar $LT(r)$.

Viser først korleis algoritmen fungerer ved å gi eit eksempel, deretter kjem provet for algoritmen.

Eksempel 5. Me har $f = 2x^2 + 1$ og $g = x + 1$. Bruk divisjonsalgoritmen til å finne resten.
Når me startar har me at $q = 0$ og $r = f$, og har at $LT(g) = x$ og $LT(r) = 2x^2$. Då får ein

$$q' = q + \frac{LT(r)}{LT(g)} = 0 + \frac{2x^2}{x} = 2x$$

og

$$r' = r - \frac{LT(r)}{LT(g)}g = 2x^2 + 1 - \frac{2x^2}{x}(x + 1) = 2x^2 + 1 - 2x(x + 1) = -2x + 1.$$

Då kan me skrive $f = q'g + r' = 2x(x + 1) - 2x + 1$. Men sidan $LT(g)$ deler $LT(r') = -2x$ må me gjere endå eit byte og får

$$q'' = q' + \frac{LT(r')}{LT(g)} = 2x + \frac{-2x}{x} = 2x - 2$$

og

$$r'' = r' - \frac{LT(r')}{LT(g)}g = -2x + 1 - \frac{(-2x)}{x}(x + 1) = -2x + 1 + 2(x + 1) = 3.$$

No kan me skrive $f = q''g + r'' = (2x - 2)(x + 1) + 3$. Og sidan $LT(g)$ ikkje deler $LT(r'') = 3$ endar algoritmen.

Prov. Me må vise at algoritmen til slutt stoppar, og at r og q er på den forma me vil ha dei. Deretter vil me vise at løysinga me har funne er unik.
For å sjå kvifor algoritmen fungerar ser me på kva som skjer når me gjer eit byte

$$f = qg + r = \left(q + \frac{LT(r)}{LT(g)}\right) \cdot g + r - \frac{LT(r)}{LT(g)} \cdot g.$$

Me ser at $f = pq + r$ også gjeld etter at me har gjort byte.
Det er gitt at algoritmen vil stoppe opp når $r = 0$ eller $LT(g)$ ikkje deler $LT(r)$. Frå (4.1) er

dette det same som at $deg(r) < deg(g)$, då har q og r dei eigenskapane me ynskjer. Me vil no vise at algoritmen til slutt endar. Og at me får at $r - \frac{LT(r)}{LT(g)}g$ enten er null, eller har mindre grad enn r. For å sjå kvifor dette stemmer, anta at:

$$r = a_0x^m + \ldots + a_m,\ LT(r) = a_0x^m,$$
$$g = b_0x^k + \ldots + b_k,\ LT(g) = b_0x^k,$$

Me antek også at $k \leq m$, då er

$$r' = r - \frac{LT(r)}{LT(g)} \cdot g = (a_ox^m + \ldots) - (\frac{a_0}{b_0}) \cdot x^{m-k}(b_0x^k + \ldots),$$

og ein ser at graden til r' må minske. Sidan graden er endeleg kan den minskast endeleg gonger, og etter eit endeleg tal med byter vil algoritmen til slutt stoppe.
Til slutt vil me vise at løysinga er unik. Anta at $f = qg + r = q'g + r'$, der både r og r' har grad mindre enn g. Viss $r \neq r'$, då er $deg(r' - r) < deg(g)$. Og frå

$$qg + r = q'g + r' \Leftrightarrow (q - q')g = r' - r, \tag{4.2}$$

har me at $q - q' \neq 0$. Sidan me har

$$deg(r' - r) = deg((q - q')g) = deg(q - q') + deg(g) \leq deg(g)$$

har me fått ei motseiing. Derfor er $r = r'$ og frå likning (4.2) er $q = q'$. Løysinga er unik. □

Me vil no forklare nokre omgrep som me treng seinare i kapittelet. Deretter viser me eit døme.

Definisjon 4.23. La $f = \sum_\alpha a_\alpha x^\alpha$ vere eit polynom i $k[x_1, \ldots, x_n]$ og la $>$ vere ei monomialordning.
i) Multigraden av f er: $multideg(f) = max(\alpha \in \sum_{\geq 0}^n : a_\alpha \neq 0)$.
ii) Det leiande monomet til f er: $LM(f) = x^{multideg(f)}$.
iii) Den leiande koeffisienten til f er: $LC(f) = a_{multideg(f)} \in k$.
iv) Det leiande leddet til f er: $LT(f) = LC(f) \cdot LM(f)$.

Eksempel 6. $f = 4x^3 + 3x^2z + 7yz - 6z^2$, med lex-ordning $x > y > z$. Då er $multideg(f) = (3, 0, 0)$, $LC(f) = 4$, $LM(f) = x^3$, $LT(f) = 4x^3$.

Divisjonsalgoritme i $k[x_1, \ldots, x_n]$.

Divisjonsalgoritmen for fleire variablar er ei utviding av divisjonsalgoritmen for $k[x]$. Denne algoritmen skal me bruke når me vil dele $f \in k[x_1, \ldots, x_n]$, med $f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$. Dette betyr at me vil skrive f som

$$f = a_1f_1 + \ldots, +a_sf_s + r,$$

der $a_1, \ldots, a_s$ og resten r ligg i kroppen $k[x_1, \ldots, x_n]$. For å gjere dette får me bruk for monomialordningar, og følgjande lemma:

Lemma 4.24. *La $f, g \in k[x_1, \ldots, x_n]$ vere polynom. Då har ein at:*
i) $multideg(fg) = multideg(f) + multideg(g)$
ii) Viss $f + g \neq 0$, då er $multideg(f + g) \leq max(multideg(f), multideg(g))$. Viss ein i tillegg har $multideg(f) \neq multideg(g)$ då er $multideg(f + g) = max(multideg(f), multideg(g))$. [1] s. 60.

Me viser først eit eksempel på korleis me kan dele eit polynom på eit anna polynom.

Eksempel 7. Me har $f = 2x^2y + 1$ og $f_1 = xy + 1$ og $f_2 = x + 1$, og brukar lex-orden: $x > y$. Me har $LT(f) = 2x^2y$, $LT(f_1) = xy$ og $LT(f_2) = x$ som begge deler $LT(f) = 2x^2y$. Me deler først med f_1.

$$\begin{aligned} &2x^2y + 1 : (xy + 1) = 2x \\ &\underline{2x^2y + 2x} \\ &-2x + 1 \end{aligned}$$

Då har me resten $r = -2x + 1$ og $LT(r) = -2x$. Sidan $LT(f_1)$ ikkje deler det leiande leddet til r må me dele med f_2.

$$\begin{aligned} &2x^2y + 1 : (xy + 1, x + 1) = 2x - 2 \\ &\underline{2x^2y + 2x} \\ &-2x + 1 \\ &\underline{-2x - 2} \\ &3 \end{aligned}$$

Og sidan verken $LT(f_1)$ eller $LT(f_2)$ deler resten som er 3, har me

$$f = 2x(xy + 1) - 2(x + 1) + 3.$$

Der me kan kalle $a_1 = 2x$ og $a_2 = -2$, og dette er "koeffisientane" til f_1 og f_2.
Ein annan måte å gjere dette på er å trekke $\frac{LT(f)}{LT(f_1)} \cdot f_1 = 2x \cdot f_1$ frå f, som gir resten

$$r' = f - 2x \cdot f_1 = 2x^2y + 1 - 2x \cdot (xy + 1) = -2x + 1$$

Då har me $LT(r') = -2x$, og $LT(f_1)$ deler ikkje denne. Vidare brukar me derfor f_2, og får $\frac{-2x}{x} = -2$ og trekker $(-2) \cdot f_2$ frå r'.

$$r'' = r' - (-2) \cdot f_2 = -2x + 1 + 2(x + 1) = 3$$

Då kan me skrive

$$f = 2x \cdot f_1 - 2 \cdot f_1 + r'' = 2x(xy + 1) - 2(x + 1) + 3.$$

Dersom me hadde delt med f_2 først hadde me fått at $f = (2xy - 2y)(x + 1) + (2y + 1)$, der resten er $2y + 1$ og $LT(2y + 1) = 2y$ er ikkje deleleg med $LT(f_1)$ eller $LT(f_2)$.

Me skal no beskrive divisjonsalgoritmen i fleire variablar og gi prov for at den stemmer. Sjølve algoritmen blir forklart i provet.

Teorem 4.25. ***Divisjonsalgoritme i*** $k[x_1, \ldots, x_n]$**.** *Bestem ei monomialordning* $>$ *på* $\mathbb{Z}^n_{\geq 0}$*, og la* $F = (f_1, \ldots, f_s)$ *vere ein ordna s-tuppel av polynom i* $k[x_1, \ldots, x_n]$*. Då kan alle* $f \in k[x_1, \ldots, x_n]$*, bli uttrykt som*

$$f = a_1 f_1 + \ldots a_s f_s + r, \tag{4.3}$$

der $a_i, r \in k[x_1, \ldots, x_n]$*. Og me har at* r *er null, eller ein lineær kombinasjon av monom (med koeffisientar i* k*), der ingen er delelege med* $LT(f_1), \ldots, LT(f_s)$*. Me kallar* r *resten til* f *ved divisjon av* F*. Og viss* $a_i f_i \neq 0$*, då har me at*

$$multideg(f) \geq multideg(a_i f_i)$$

Prov. Viser eksistens av $a_1, \ldots, a_s$ og r ved å gi ein algoritme og viser at den fungerer korrekt for alle input.
Me startar me at me har $f_1, \ldots, f_s$ og f, og vil få ut $a_1, \ldots, a_s, r$.
Me skriv $a_1 := 0; \ldots; a_s := 0; r := 0$ og $p := f$. Når $p \neq 0$ må me finne ut om $LT(p)$ er deleleg med nokre av $LT(f_i)$. Og viss nokre $LT(f_i)$ deler $LT(p)$ vel me den første, og gjer to byter:

$$p' = p - \frac{LT(p)}{LT(f_i)} \cdot f_i, \text{ og}$$

$$a_i' = a_i - \frac{LT(p)}{LT(f_i)}.$$

Viss $LT(p)$ ikkje er delelege med nokre av $LT(f_i)$ legg me det leiande leddet til resten, slik

$$r' = r + LT(p),$$
$$p' = p - LT(p).$$

For å vise at algoritmen fungerer viser me først at likning (4.3) gjeld ved alle steg. Deretter må me vise at algoritmen til slutt vil stoppe.
Anta at (4.3) gjeld for eit steg av algoritmen. Viss neste steg er eit divisjonssteg, då er det nokre $LT(f_i)$ som delar $LT(p)$, og ein får

$$a_i f_i + p = \left(a_i + \frac{LT(p)}{LT(f_i)}\right) f_i + p - \frac{LT(p)}{LT(f_i)} f_i.$$

Ein ser at summen $a_i f_i + p$ er uendra. Sidan ingen annan variabel er upåverka, er likning (4.3) framleis sann.
Viss det neste steget var eit reststeg vil p og r bli endra, men summen $p + r$ er uendra sidan

$$p + r = (p - LT(p)) + (r + LT(p)),$$

og likning (4.3) held framleis.
Legg merke til at algoritmen stoppar når $p = 0$. I denne situasjonen blir likning (4.3)

$$f = a_1 f_1 + \ldots + a_s f_s + r.$$

Sidan ledd blir lagt til r kun når dei ikkje er delelege med nokre $LT(f_i)$, følgjer det at $a_1, \ldots, a_s$ og r har ynskja eigenskapar når algoritmen stoppar.
Til slutt må me vise at algoritmen til slutt stoppar opp. Ein viktig observasjon er at kvar gong me omdefinerer p, vil anten multigraden minke eller bli null. For å sjå dette, anta først at i eit divisjonssteg blir p omdefinert til å vere

$$p' = p - \frac{LT(p)}{LT(f_i)} f_i.$$

Frå lemma 4.24 har me at

$$LT\left(\frac{LT(p)}{LT(f_i)} f_i\right) = \frac{LT(p)}{LT(f_i)} LT(f_i) = LT(p),$$

slik at p og $(LT(p)/LT(f_i))f_i$ har same leiande ledd. Derfor må differansen p', ha strengt mindre multigrad når $p' \neq 0$.
Anta at under eit reststeg blir p definert som

$$p' = p - LT(p).$$

Her har ein at $multideg(p') < multideg(p)$ når $p \neq 0$. Derfor vil multigraden minke for begge byta. Me antek at algoritmen aldri stoppar. Då får me ein uendeleg rekkjefølgje med minkande multigrader. Men sidan me har ei velordning med eigenskap $>$ som i lemma 4.4, kan ikkje dette vere tilfelle. Derfor må p til slutt bli null og algoritmen vil stoppe etter endeleg mange steg.
Me lyt også sjå på forholdet mellom $multideg(f)$ og $multideg(a_i f_i)$. Alle ledd i a_i har forma $LT(p)/LT(f_i)$ for nokre verdiar av variabelen p. Algoritmen startar med at $p = f$, og me veit at $multideg(p)$ minkar. Derfor har ein at $LT(p) \leq LT(f)$ og ved å bruke definisjon 4.3, at $multideg(a_i f_i) \leq multideg(f)$ når $a_i f_i \neq 0$. □

Frå førre eksempel ser me at resten me får ikkje er unik. Men viss me følgjer algoritmen presist, og testar om $LT(f)$ er deleleg med $LT(f_1), LT(f_2), \ldots$ i den rekkjefølgja, får me ein unik rest og unike "koeffisientar" $a_1, a_2, \ldots, a_s$.

Eksempel 8. La $f_1 = xy + 1$ og $f_2 = y^2 - 1$, der $f_1, f_2 \in k[x, y]$ og *lex*-orden. Ved å dele $f = xy^2 - x$ med (f_1, f_2) får me

$$f = y \cdot f_1 - (x + y).$$

Og ved å dele med (f_2, f_1) får me

$$f = x \cdot f_2 + 0.$$

Denne likninga viser at $f \in \langle f_2, f_1 \rangle$. Men den første likninga viser at me likevel kan få ein rest som ikkje er null når me deler med (f_1, f_2).

Når me har fleire polynom er det ynskjeleg å bruke idealet dei genererer, slik at me kan gå frå $f_1, \ldots, f_s$ til ei anna genererande mengd for I. Me ynskjer å få ei mengd der resten er unik. Og når resten er null betyr det at, viss me har $f \in k[x_1, \ldots, x_n]$ og eit ideal I så er $f \in I$.
Me ynskjer å ha ei genererande mengd av eit ideal, med den eigenskapen at resten frå divisjonsalgoritmen, er uavhengig av orden på elementa. Me vil seinare vise at gröbnerbasar har denne eigenskapen.

Monomialideal og Dickson sitt lemma

I denne delen kjem definisjonen på monomialideal. Og me vil vise korleis me kan finne ut om eit monom ligg i eit monomialideal. Deretter gir me teoremet, Dickson sitt lemma. Dette teoremet seier at alle monomialideal i $k[x_1, \ldots, x_n]$ er endeleg genererte, og blir brukt i delkapittel 4.4. Me kan dermed finne ut om eit polynom ligg i eit monomialideal.

Definisjon 4.26. Eit ideal $I \subset k[x_1, \ldots, x_n]$ er eit monomialideal viss det fins ei delmengd $A \subset \mathbb{Z}^n_{\geq 0}$, slik at I inneheld alle polynom som er endelege summar på forma $\sum_{a \in A} h_a x^a$, der $h_a \in k[x_1, \ldots, x_n]$. Då kan me skrive $I = \langle x^a : a \in A \rangle$.

Monomialideal er bygd opp av monom og eit døme på eit monomialideal er $I = \langle x^4y^2, x^3y^4, x^2y^5 \rangle \subset k[x, y]$.

Lemma 4.27. *La $I = \langle x^a : a \in A \rangle$ vere eit monomialideal. Då ligg monomet x^b i I viss og berre viss x^b er deleleg med x^a for nokre $a \in A$.*

Prov. Viss x^b er ein multippel av x^a for nokre $a \in A$, då er $x^b \in I$ frå definisjonen av ideal.
Og omvendt, viss $x^b \in I$, då er

$$x^b = \sum_{i=1}^{s} h_i x^{a(i)},$$

der $h_i \in k[x_1, \ldots, x_n]$ og $a(i) \in A$. Viss me utvidar kvar h_i som ein lineær kombinasjon av monom, ser me at alle ledd på høgresida av likninga er deleleg av nokre $x^{a(i)}$. Då må venstresida også vere det. Og me har at x^b er deleleg med x^a, for nokre $a \in A$ slik at $x^b \in I$. □

Me ser at x^b er deleleg med x^a når me kan skrive $x^b = x^a \cdot x^y$ for nokre $y \in \mathbb{Z}^n_{\geq 0}$.
Det me vil fram til i denne delen er at monomialideal er endeleg genererte, og me har då Dickson sitt lemma.

Teorem 4.28. ***Dickson sitt lemma.*** *La $I = \langle x^a : a \in A \rangle \subseteq k[x_1, \ldots, x_n]$ vere eit monomialideal. Då kan I skrivast på forma $I = \langle x^{a(1)}, \ldots, x^{a(s)} \rangle$, der $a(1), \ldots, a(s) \in A$. Og I har ein endeleg basis.*

Prov. Brukar induksjon. Viss $n = 1$, då er I generert av monoma x^a, der $a \in A \subset \mathbb{Z}_{\geq 0}$. La b vere det minste elementet av $A \subset \mathbb{Z}_{\geq 0}$. Då er $b \leq a$ for alle $a \in A$, slik at x_1^b deler alle andre generatorar x_1^a. Og me har då at $I = \langle x_1^b \rangle$.
Anta at $n > 1$ og at teoremet stemmer for $n - 1$. Me brukar variablane $x_1, \ldots, x_{n-1}, y$, slik at monom i $k[x_1, \ldots, x_{n-1}, y]$ kan skrivast som $x^a y^m$, der $a = (a_1, \ldots, a_{n-1}) \in \mathbb{Z}^{n-1}_{\geq 0}$ og $m \in \mathbb{Z}_{\geq 0}$.

Anta at $I \subset k[x_1, \ldots, x_{n-1}, y]$ er eit monomialideal. For å finne generatorar til I, la J vere eit ideal i $k[x_1, \ldots, x_{n-1}]$ generert av monoma x^a, der $x^a y^m \in I$ for nokre $m \geq 0$. Sidan J er eit monomialideal i $k[x_1, \ldots, x_{n-1}]$, vil induksjonshypotesen antyde at endeleg mange x^a genererer J. Idealet J kan bli forstått som "projeksjonen" av I på $k[x_1, \ldots, x_{n-1}]$.
For alle i, mellom 1 og s, fortel definisjonen av J oss at $x^{a(i)} y^{m_i} \in I$, for nokre $m_i \geq 0$. La m vere den største av m_i-ane. For kvar k, mellom 0 og $m - 1$, sjå på idealet $J_k \subset k[x_1, \ldots, x_{n-1}]$ generert av monoma x^b slik at $x^b y^k \in I$. Ein kan tenkje på J_k som ein bit at I generert av monom som inneheld y opphøgd i akkurat k. Ved å bruke induksjonshypotesen har J_k ei endeleg genererande mengde med monom, og me kan skrive $J_k = \langle x^{a_k(1)}, \ldots, x^{a_k(s_k)} \rangle$.

Me hevdar at I er generert av monoma:
frå J: $x^{a(1)} y^m, \ldots, x^{a(s)} y^m$,
frå J_0: $x^{a_0(1)} y^m, \ldots, x^{a_0(s_0)} y^m$,
$\vdots$
frå J_{m-1}: $x^{a_{m-1}(1)} y^{m-1}, \ldots, x^{a_{m-1}(s_{m-1})} y^{m-1}$.
Merk at alle monom i I er deleleg med eit av monoma i lista. For å sjå kvifor, la $x^a y^p \in I$. Dersom $p \geq m$, då er $x^a y^p$ deleleg av nokre $x^{a(i)} y^m$ i konstruksjonen til J. Men viss $p \leq m - 1$, då er $x^a y^p$ deleleg med nokre $x^{a_p(j)} y^p$ av konstruksjonen til J_p. Det følgjer frå lemma 4.27 at monoma over, genererer eit ideal som har same monom som I. Og ideala må vere like.
Me må vise at den endelege mengda av generatorar, kan bli valt frå ei gitt mengd av generatorar for idealet. Viss me går tilbake til å kalle variablane $x_1, \ldots, x_n$, då blir monomialidealet $I = \langle x^a : a \in A \rangle \subset k[x_1, \ldots, x_n]$. Me må vise at I er generert av endeleg mange x^a, der $a \in A$. Frå førre avsnitt veit me at $I = \langle x^{b(1)}, \ldots, x^{b(s)} \rangle$ for nokre monom $x^{b(i)}$ i I. Sidan $x^{b(i)} \in I$, seier lemma 4.27 at alle $x^{b(i)}$ er delelege av $x^{a(i)}$ for nokre $a(i) \in A$. Frå dette kan ein vise at $I = \langle x^{a(1)}, \ldots, x^{a(s)} \rangle$. □

Dette teoremet fortel oss at eit monomialideal har ein endeleg base. Me har monomialidealet $I = \langle x^{a(1)}, \ldots, x^{a(s)} \rangle$. Og me kan vise at eit polynom ligg i I. Dersom me har eit polynom f, då ligg dette i I viss og berre viss, resten etter divisjon av f med $x^{a(1)}, \ldots, x^{a(s)}$ er null.

4.4 Hilbert sitt basisteorem og Gröbnerbasar

Me vil i dette delkapittelet vise at alle ideal har ei endeleg genererane mengd. Dette resultatet blir kalla Hilbert sitt basisteorem. Deretter ser me på affine varitetar, introduserar omgrepet gröbnerbasar. Det vil bli gitt nokre eigenskapar på gröbnerbasar, og vist korleis me kan lage ein gröbnerbase. Gröbnerbasane skal me bruke til å løyse problem som involverer ideal, på ein algebraisk eller utrekningsorientert måte. Ved å nytte gröbnerbasar kan me løyse system av ikkje-lineære likningar. Me vil avslutte dette delkapittelet med å gi Buchberger sin algoritme som gir metoden me nyttar for å lage ein gröbnerbase. Målet for dette kapittelet er framleis å kunne løyse ikkje-lineære likningar og etter dette delkapittelet er me nesten i mål.

Definisjon 4.29. La $I \subset k[x_1, \ldots, x_n]$ vere eit ideal.

i) Me let $LT(I)$ vere mengda av ledande ledd i I, slik at

$$LT(I) = \{cx^a : \exists f \in I \text{ med } LT(f) = cx^a\}.$$

ii) Me kallar $\langle LT(I)\rangle$ for idealet generert av elementa i $LT(I)$.

Me skal no sjå på eit eksempel som illustrerer at gitt $I = \langle f_1, \ldots, f_s\rangle$, så kan idealet $\langle LT(I)\rangle$ vere større enn idealet $\langle LT(f_1), \ldots, LT(f_s)\rangle$.

Eksempel 9. Me har $f_1 = x + 1$ og $f_2 = xy + 1$ og at $I = \langle f_1, f_2\rangle$. Me brukar lex-ordning på monoma i $k[x, y]$. Og me har at $LT(f_1) = x$ og $LT(f_2) = xy$.

$$y \cdot f_1 - f_2 = y(x + 1) - xy + 1 = y + 1,$$

slik at $(y+1) \in I$. Og $LT(y+1) = y \in \langle LT(I)\rangle$, men y er ikkje deleleg med $LT(f_1)$ eller $LT(f_2)$. Då har me at $y \notin \langle LT(f_1), LT(f_2)\rangle$, frå lemma 4.27.

Frå dette eksempelet ser at $\langle LT(f_1), LT(f_2)\rangle \subset \langle LT(I)\rangle$. Og at $\langle LT(I)\rangle$ er større enn $\langle LT(f_1), LT(f_2)\rangle$.
Me vil no vise at $\langle LT(I)\rangle$ er eit monomialideal. Frå resultata i delen om monomialideal og Dickson sitt lemma, vil $\langle LT(I)\rangle$ ha ein endeleg basis.

Resultat 4.30. *La $I \subset k[x_1, \ldots, x_n]$ vere eit ideal. Då er:*

i) $\langle LT(I)\rangle$ eit monomialideal.

ii) Det eksisterer $g_1, \ldots, g_t \in I$ slik at $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$.

Prov. i) Dei leiande monoma $LM(g)$ av element $g \in I - \{0\}$ genererer monomialidealet $\langle LM(g) : g \in I - \{0\}\rangle$. Sidan $LM(g)$ og $LT(g)$ er ulike ved multiplikasjon av ein konstant, er dette idealet lik $\langle LT(g) : g \in I - \{0\}\rangle = \langle LT(I)\rangle$. Og me har derfor at $\langle LT(I)\rangle$ er eit monomialideal.
ii) Sidan $\langle LT(I)\rangle$ er generert av monoma $LM(g)$, for $g \in I - \{0\}$, kan me bruke Dickson sitt lemma 4.28 og får at $\langle LT(I)\rangle = \langle LM(g_1), \ldots, LM(g_t)\rangle$ for endeleg mange $g_1, \ldots, g_t \in I$. Sidan $LM(g_i)$ er forskjellig frå $LT(g_i)$ med ein konstant følgjer det at $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. □

Me vil no bruke dette resultatet og divisjonsalgoritmen til å vise at det eksisterer ei endeleg genererande mengde for alle polynomideal.

Teorem 4.31. ***Hilbert sitt basisteorem.*** *Alle ideal $I \subset k[x_1, \ldots, x_n]$ har ei endeleg genererande mengde. Det betyr at $I = \langle g_1, \ldots, g_t\rangle$, for nokre $g_1, \ldots, g_t \in I$.*

Prov. Viss $I = \{0\}$, er den genererande mengda $\{0\}$, som er endeleg.
Viss I inneheld eit polynom kan me lage ei generande mengd $g_1, \ldots, g_t$ for I. på følgjande måte: Me har $g_1, \ldots, g_t \in I$, og brukar resultat 4.30 slik at $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. Me hevdar at $I = \langle g_1, \ldots, g_t\rangle$.
Me ser at $\langle g_1, \ldots, g_t\rangle \subset I$ sidan kvar $g_i \in I$. La $f \in I$ vere eit polynom. Viss me brukar divisjonsalgoritmen til å dele f med $\langle g_1, \ldots, g_t\rangle$, får me

$$f = a_1 g_1 + \ldots + a_t g_t + r,$$

der ingen ledd av r er delelege med nokon av $LT(g_1), \ldots, LT(g_t)$. Me ser på tilfellet der $r = 0$. Då har me at

$$r = f - a_1 g_1 - \ldots - a_t g_t \in I$$

Viss $r \neq 0$, då er $LT(r) \in \langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$, og frå lemma 4.27 har me at $LT(r)$ må vere deleleg med nokre $LT(g_i)$. Dette motseier tydinga av det å vere ein rest, og r må derfor vere null. Derfor er

$$f = a_1 g_1 + \ldots a_t g_t + 0 \in \langle g_1, \ldots, g_t\rangle,$$

som viser at $I \subset \langle g_1, \ldots, g_t\rangle$. Me har derfor at $I = \langle g_1, ..., g_t\rangle$. □

Basisen me brukar i provet for Hilbert sitt basisteorem har den eigenskapen at $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_t)\rangle$. Som me såg i eksempel 9 har ikkje alle basar denne eigenskapen. Me vil gi ein slik base namnet gröbnerbasar.

Definisjon 4.32. Me vel ei monomialordning. Ei endeleg delmengd $G = \{g_1, \ldots, g_t\}$ av eit ideal I er ein Gröbnerbase, viss

$$\langle LT(g_i), \ldots, LT(g_t)\rangle = \langle LT(I)\rangle.$$

Ei mengde $\{g_1, \ldots, g_t\} \subset I$ er ein gröbnerbase til I, viss og berre viss dei leiande ledda til element i I, er deleleg med ein av $LT(g_i)$. Viss me ser på eksempelet i byrjinga av denne delen der me fann at $y + 1 \in I$. Men $LT(f_1) = x$ og $LT(f_2) = xy$ deler ikkje y, då er (f_1, f_2) ikkje ein gröbnerbase. Me vil vise korleis ein kan finne ein gröbnerbase seinare i kapittelet.

Tidlegare har me sett på affine varitetar som ei mengd av løysingar til ei endelege mengd med polynomlikningar,

$$V(f_1, \ldots, f_s) = \{(a_1, \ldots, a_n) \in k^n : f_i(a_1, \ldots, a_n) = 0 \ \forall\ i\}.$$

Hilbert sitt basisteorem viser at me også kan snakke om at ein affin varitet er bestemt av eit ideal $I \subset k[x_1, \ldots, x_n]$. Viss me har ein gröbnerbase $(g_1, \ldots, g_t)$ av I har me at

$$V(f_1, \ldots, f_s) = V(g_1, \ldots, g_t).$$

Dette systemet med likningane $g_1, \ldots, g_t$, er ofte enklare å løyse. Og me kan bruke eliminasjonsteoremet som er gitt i kapittel 4.5, for å finne ei løysing for variablane $x_1, \ldots, x_n$.

Definisjon 4.33. La $I \subset k[x_1, \ldots, x_n]$ vere eit ideal. Me kallar $V(I)$ for mengda

$$V(I) = \{(a_1, \ldots, a_n) \in k^n : f(a_1, \ldots, a_n) = 0 \ \forall f \in I\}$$

Sjølv om eit ideal I alltid inneheld uendeleg mange ulike polynom, så kan mengda $V(I)$ framleis bli definert som ei endeleg mengde av polynomlikningar.

Resultat 4.34. *$V(I)$ er ein affin varitet. Me har at viss $I = \langle f_1, \ldots, f_s \rangle$, då er $V(I) = V(f_1, \ldots, f_s)$.*

Prov. Brukar Hilbert sitt basisteorem, og har at $I = \langle f_1, \ldots, f_s \rangle$, for ei endeleg genererande mengd. Me hevdar at $V(I) = V(f_1, \ldots, f_s)$.
Sidan $f_i \in I$, når $f(a_1, \ldots, a_n) = 0$ for alle $f \in I$. Då er $f_i(a_1, \ldots, a_n) = 0$, slik at $V(I) \subset V(f_1, \ldots, f_s)$.
For å vise omvendt, la $(a_1, \ldots, a_n) \in V(f_1, \ldots f_s)$ og la $f \in I$. Sidan $I = \langle f_1, \ldots, f_s \rangle$ kan me skrive

$$f = \sum_{i=1}^{s} h_i f_i,$$

for nokre $h_i \in k[x_1, \ldots, x_n]$. Men då er

$$f(a_1, \ldots, a_n) = \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) \cdot f_i(a_1, \ldots, a_n) = \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) \cdot 0 = 0.$$

Og me har derfor at $V(f_1, \ldots, f_s) \subset V(I)$. Då får me $V(f_1, \ldots, f_s) = V(I)$. □

Ein konsekvens av dette resultatet er at varitetar blir bestemt av ideal. Me skal no sjå nærmare på nokre eigenskapar ved gröbnerbasar. Deretter skal me gi Buchberger sin algoritme, som gir ein metode for å konstruere ein gröbnerbase.

Resultat 4.35. *La $G = \{g_1, \ldots, g_t\}$ vere ein Gröbnerbase for eit ideal $I \subset k[x_1, \ldots, x_n]$, og la $f \in k[x_1, \ldots, x_n]$. Då fins det ein unik $r \in k[x_1, \ldots, x_n]$, med følgjande to eigenskapar:*

i) Ingen ledd av r er delelege med $LT(g_1), \ldots, LT(g_t)$.

ii) Det er ein $g \in I$ slik at $f = g + r$.

Me har at r er resten etter divisjon av f og G, uansett kva rekkjefølgje elementa til G har når me brukar divisjonsalgoritmen.

Prov. Divisjonsalgoritmen gir $f = a_1 g_1 + \ldots + a_t g_t + r$, der r tilfredsstillar i). Ved å setje $g = a_1 g_1 + \ldots + a_t g_t \in I$ er også krav ii) oppfylt. Dette gjer at det eksisterar ein r.
Me må no vise at r er unik. Anta at $f = g + r = g' + r'$ og oppfyller krav i) og ii). Då har me at $r - r' = g' - g \in I$, slik at viss $r \neq r'$ då er $LT(r - r') \in \langle LT(I) \rangle = \langle LT(g_1), \ldots, LT(g_t) \rangle$. Brukar lemma 4.27, og ein har at $LT(r - r')$ er deleleg av nokre $LT(g_i)$. Dette er umogleg sidan ingen ledd av r og r' er deleleg med $LT(g_1), \ldots, LT(g_t)$. Derfor må $r - r'$ vere null, og resten er unik. Siste delen av resultatet følgjer frå unikheita til r. □

Sjølv om resten r er unik kan "kvotientane" $a_1, \ldots, a_n$ frå divisjonsalgoritmen vere avhengig av rekkjefølgja til generatorane. Me kan no gi eit kriteriet for når eit polynom ligg i eit ideal.

Korolar 4.36. *La $G = \{g_1, \ldots, g_t\}$ vere ein gröbnerbase for idealet $I \subset k[x_1, \ldots, x_n]$ og la $f \in k[x_1, \ldots, x_n]$. Då er $f \in I$ viss og berre viss resten etter divisjon med G er lik null.*

Prov. Viss resten er null har me at $f \in I$. Gitt $f \in I$, då oppfyller $f = f + 0$ krava i resultat 4.35. Og 0 må vere resten når f blir delt av G. □

Ved å bruke denne korolaren har me ein algoritme til å finne ut om eit polynom ligg i eit ideal, viss me har gitt ein gröbnerbase for idealet. Me trenger kun å finne resten med omsyn på G for å vurdere om polynomet er i idealet.
Me vil no innføre ein notasjon for denne resten, som vil bli nytta i fleire dømer, og i Buchberger sin algoritme.

Definisjon 4.37. Me skriv $\overline{f}^F$ for resten etter divisjon av f med den ordna s-tuppelen $F = (f_1, \ldots, f_s)$. Viss F er ein gröbnerbase for $\langle f_1, \ldots, f_s \rangle$, då kan me sjå på F som mengda (utan ei spesiell orden), frå resultat 4.35.

Me vil no diskutere korleis me kan finne ut om ei genererande mengde til eit ideal, er ein gröbnerbase. Me vil finne ut $\{f_1, \ldots, f_s\}$ er ein gröbnerbase. Viss me har nokre kombinasjonar av polynoma f_i, som har leiande ledd som ikkje er i idealet generert av $LT(f_i)$, er ikkje mengda ein gröbnerbase. Det kan skje ved at dei leiande ledda blir kansellerte, og gir eit polynom av mindre grad. Me er då klare til å gi ein definisjon på S-polynom.

Definisjon 4.38. La $f, g \in k[x_1, \ldots, x_n]$ vere eit polynom som ikkje er null.

i) Viss $multideg(f) = \alpha$ og $multideg(g) = \beta$. La $y = (y_1, \ldots, y_n)$, der $y_i = max(\alpha_i, \beta_i)$ for kvar i. Me kallar x^y det minste felles multiplum av $LM(f)$ og $LM(g)$ og skriv $x^y = LCM(LM(f), LM(g))$.

ii) S-polynomet til f og g er kombinasjonen:

$$S(f,g) = \frac{x^y}{LT(f)} \cdot f - \frac{x^y}{LT(f)} \cdot g$$

Me skal no sjå på eit eksempel som viser korleis me finner S-polynomet til to polynom.

Eksempel 10. La $f = 2x^2y + 1$ og $g = xy^2 + 1$ i $\mathbb{R}[x, y]$. Då har me at $x^y = x^2y^2$, og me får S-polynomet

$$S(f,g) = \frac{x^2y^2}{2x^2y} \cdot f - \frac{x^2y^2}{xy^2} \cdot g = 1/2y \cdot f - x \cdot g = x^2y^2 + 1/2y - x^2y^2 - x = 1/2y - x.$$

Me ser at det leiande leddet blir kansellert, og det er det som er meininga med å finne S-polynom. Og det neste lemmaet viser at kansellering av leiande ledd mellom polynom av same multigrad skjer ved S-polynommetoden.

Lemma 4.39. *Anta at me har ein sum $\sum_{i=1}^s c_i f_i$, der $c_i \in k$ og $multideg(f_i) = d \in \mathbb{Z}_{\geq 0}^n$ for alle i. Viss $multideg(\sum_{i=1}^s c_i f_i) < d$, då er $\sum_{i=1}^s c_i f_i$ ein lineær kombinasjon, med koeffisientar i k, av S-polynoma $S(f_j, f_k)$ for $1 \leq j, k \leq s$. Og kvar $S(f_j, f_k)$ har multigrad mindre enn d.*

Prov. La $p_i = LC(f_i)$, slik at $c_i p_i$ er den leiande koeffisienten til $c_i f_i$. Sidan alle $c_i f_i$ har multigrad d, og me har gitt at summen har mindre multigrad, då må $\sum_{i=1}^s c_i p_i = 0$.
Me definerer $m_i = f_i / p_i$, og ser at m_i har leiande koeffisient ein. Då kan me skrive summen som

$$\sum_{i=1}^s c_i f_i = \sum_{i=1}^s c_i p_i m_i = c_i p_i (m_1 - m_2) + (c_1 p_1 + c_2 p_2)(m_2 - m_2) + \ldots +$$
$$(c_1 p_1 + \ldots + c_{s-1} p_{s-1})(m_{s-1} - m_s) + (c_1 p_1 + \ldots + c_s p_s) m_s.$$

Ved å anta $LT(f_i) = p_i x^d$, som typar på at det minste felles multiplum til $LM(f_j)$ og $LM(f_k)$ er x^d, slik at

$$S(f_j, f_k) = \frac{x^d}{LT(f_j)} f_j - \frac{x^d}{LT(f_k)} f_k = \frac{x^d}{p_j x^d} f_j - \frac{x^d}{p_k x^d} f_k = m_j - m_k. \tag{4.4}$$

Ved å bruke denne likninga og $\sum_{i=1}^s c_i p_i = 0$, blir summen:

$$\sum_{i=1}^s c_i f_i = c_1 p_1 \cdot S(f_1, f_2) + (c_1 p_1 + c_2 p_2) \cdot S(f_2, f_3) + \ldots + (c_1 p_1 + \ldots + c_{s-1} p_s) \cdot S(f_{s-1}, f_s).$$

Sidan m_j og m_k har multigrad d, og den leiande koeffisient er 1, og differansen $m_j - m_k$ har $multideg < d$, er summen på ynskja form. Ved likning (4.4) er det same sant for $S(f_j, f_k)$. □

Ved å bruke S-polynom og lemma 4.39 kan me bevise kriteriet til Buchberger for når ein base til eit ideal er ein gröbnerbase.

Teorem 4.40. ***Buchberger sitt kriterium.*** *La I vere eit polynomideal. Då er ein basis $G = \{g_1, \ldots, g_t\}$ ein gröbnerbase for I, viss og berre viss (for alle par $i \neq j$) resten etter divisjon av $S(g_i, g_j)$ med G, er null.*

Bevis. Prov $\Rightarrow$: Viss G er ein gröbnerbase då er resten etter divisjon med G null frå korolar 4.36, sidan $S(g_i, g_j) \in I$.
$\Leftarrow$: La $f \in I$ vere eit polynom. Me må vise at viss alle S-polynom har rest lik null etter divisjon med G, då er $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$. Først kjem framgangsmåten for korleis me vil vise dette.
Gitt $f \in I = \langle g_1, \ldots, g_t\rangle$, fins det polynom $h_i \in k[x_1, \ldots, x_n]$ slik at

$$f = \sum_{i=1}^{t} h_i g_i. \tag{4.5}$$

Frå lemma 4.24 har me at

$$multideg(f) \leq max(multideg(h_i g_i)). \tag{4.6}$$

Viss det ikkje er likskap, då må det skje ein kansellering av nokre leiande ledd i likning (4.5). Ved å nytte Lemma 4.39 kan me skrive dette som S-polynom. Då vil antakinga vår om at S-polynom har null rest, gjere at me kan byte S-polynoma til uttrykk som involverer mindre kansellering. Me vil då få eit uttrykk for f, som ha færre kanselleringar av leiande ledd. Ved å fortsette på denne måten vil me til slutt finne eit uttrykk som likning (4.5) for f, som gjer at me får likskap i uttrykk (4.6). Då har me at $multideg(f) = multideg(h_i g_i)$ for nokre i, og det vil følgje at $LT(f)$ er deleleg med $LT(g_i)$. Dette vil vise at $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$.

No kjem provet. Gitt uttrykket (4.5) for f, la $m(i) = multideg(h_i g_i)$, og definer
$\delta = max(m(1), \ldots, m(t))$. Då blir ulikskap (4.6)

$$multideg(f) \leq \delta.$$

Sjå på alle måtar der f kan skrivast som likning (4.5). For kvart uttrykk får me, muligens, ein ulik δ. Fordi ei monomialordning er ei velordning, kan me velje eit uttrykk for (4.5) slik at δ er minimal.
Me vil vise at ved denne minimale δ, då har me $multideg(f) = \delta$. Ein ser då at me har likskap i uttrykk (4.6) og at $LT(f) \in \langle LT(g_1), \ldots, LT(g_t)\rangle$.

Me må vise at $multideg(f) = \delta$. Dette gjer me ved å anta at me ikkje har likskap, og vise at me kjem til ei motseiing.
Me har ikkje likskap når $multideg(f) < \delta$. For å isolera ledd med multigrad δ, la oss skrive f som

$$\begin{aligned} f &= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i \\ &= \sum_{m(i)=\delta} LT(h_i) g_i + \sum_{m(i)=\delta} (h_i - LT(h_i)) g_i + \sum_{m(i)<\delta} h_i g_i. \end{aligned} \tag{4.7}$$

Monoma i andre og tredje sum på den andre linja, har multigrad mindre enn δ. Og antakinga vår gjer at også den første summen må ha multigrad mindre enn δ. Me ser no nærmare på den første summen.
Og skriv $LT(h_i) = c_i x^{a(i)}$. Då kan me skrive den første summen som

$$\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{m(i)=\delta} c_i x^{a(i)} g_i,$$

som er lik summen i lemma 4.39 med $f_i = x^{a(i)} g_i$. Frå lemma 4.39 er dette ein sum av lineære kombinasjonar av S-polynom $S(x^{a(j)}g_j, x^{a(k)}g_k)$. Men me har

$$S(x^{a(j)}g_j, x^{a(k)}g_k) = \frac{x^\delta}{x^{a(j)}LT(g_j)} \cdot x^{a(j)}g_j - \frac{x^\delta}{x^{a(k)}LT(g_k)} \cdot x^{a(k)}g_k = x^{\delta - y_{jk}} S(g_j, g_k),$$

der $x^{y_{jk}} = LCM(LM(g_j), LM(g_k))$. Då har me konstantar $c_{jk} \in k$ slik at me kan skrive summen som

$$\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{j,k} c_{jk} x^{\delta - y_{jk}} S(g_j, g_k). \tag{4.8}$$

I det neste steget må me bruke hypotesen om at resten til $S(g_j, g_k)$ etter divisjon med $g_1, \ldots, g_t$, er null. Ved å bruke divisjonsalgoritmen, betyr dette at alle S-polynom kan skrivast som

$$S(g_j, g_k) = \sum_{i=1}^{t} a_{ijk} g_i,$$

der $a_{ijk} \in k[x_1, \ldots, x_n]$. Divisjonsalgoritmen gir også at

$$multideg(a_{ijk}g_i) \leq multideg(S(g_j, g_i)) \tag{4.9}$$

for alle i, j, k. Dette seier oss at når resten er null, kan me finne eit uttrykk for $S(g_j, g_i)$ i termar av G, der ikkje alle dei leiande ledda blir kansellert.
For å bruke dette multipliserer me uttrykket for $S(g_j, g_k)$ med $x^{\delta - y_{jk}}$, og får

$$x^{\delta - y_{jk}} S(g_j, g_k) = \sum_{i=1}^{t} b_{ijk} g_i,$$

der $b_{ijk} = x^{\delta - y_{jk}} a_{ijk}$. Frå likning (4.9) og lemma 4.39 har me

$$multideg(b_{ijk}g_i) \leq multideg(x^{\delta - y_{jk}} S(g_j, g_k)) < \delta.$$

Dersom me substituerer uttrykket for $x^{\delta - y_{jk}} S(g_j, g_k)$ inn i likning (4.8), får me

$$\sum_{m(i)=\delta} LT(h_i)g_i = \sum_{j,k} c_{jk} x^{\delta - y_{jk}} S(g_j, g_k) = \sum_{j,k} c_{jk} \Big(\sum_i b_{ijk} g_i \Big) = \sum_i \tilde{h}_i g_i,$$

som ved ulikskapen over, har eigenskapen at

$$multideg(\tilde{h}_i g_i) < \delta,$$

for alle i. I det siste steget av provet, substituerer me $\sum_{m(i)=\delta} LT(h_i)g_i = \sum_i \tilde{h}_i g_i$ inn i likning (4.7), for å få f uttrykt som ein kombinasjon av polynom av g_i, der alle ledd har multigrad mindre enn δ. Men då er ikkje δ minimal, og me har komme til ei motseiing. □

Dette teoremet gir oss ein måte for å vise om ein basis av eit ideal er ein gröbnerbase. Og det er dette teoremet me skal bruke i det neste eksempelet. Seinare skal me bruke dette teoremet for å gi ein algoritme til å finne gröbnerbasar.

Eksempel 11. Me har eit ideal $I = \langle 2x-1, y+2\rangle$ i $\mathbb{R}[x,y]$. Me hevdar at $G = \{2x-1, y+2\}$ er ein gröbnerbase når me har lex-orden $x > y$. Me finn S-polynomet

$$S(2x-1, y+2) = \frac{xy}{2x}(2x-1) - \frac{xy}{y}(y+2) = xy - 1/2y - xy - 2x = -2x - 1/2y.$$

Me brukar divisjonsalgoritmen og får

$$-2x - 1/2y = (-1)(2x-1) + (-1/2)(y+2) + 0,$$

slik at $\overline{S(2x-1, y+2)}^{G} = 0$. Frå teorem 4.40, er G ein gröbnerbase for idealet I.

Det neste teoremet blir brukt i provet for Buchberger sin algoritme.

Teorem 4.41. *La*

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

vere ei stigande rekkje med ideal i $k[x_1, \dots, x_n]$. Då eksisterer det ein $N \geq 1$, slik at

$$I_N = I_{N+1} = I_{N+2} = \dots,$$

[1], s. 79.

Frå dette teoremet vil ei stigande rekkjefølgje bli stabiliser ved I_N. Og alle etterfølgjande ideal vil vere lik I_N. Me skal no gi Buchberger sin algoritme som me brukar når me skal konstruere ein gröbnerbase.

Teorem 4.42. ***Buchberger sin algoritme.*** *La $I = \langle f_1, \dots, f_s\rangle \neq \{0\}$ vere eit polynomideal. Då kan ein gröbnerbase bli konstruert ved eit endeleg tal steg, ved å bruke følgjande algoritme. Me har $F = (f_1, \dots, f_s)$ og vil finne ein gröbnerbase $G = (g_1, \dots, g_t)$ for I, med $F \subset G$.*
Me byrjar med å setje $G = F$, og $G' := G$. Me finn $\overline{S(p,q)}^{G'}$ for kvart par $\{p, q\}$, der $p \neq q$ i G'. Viss $S \neq 0$ legg me resten til gröbnerbasen, G. Me fortset på denne måten heilt til $S = 0$ og $G = G'$.

Prov. Viss $G = \{g_1, \dots, g_t\}$, då er:

$$\langle G\rangle = \langle g_1, \dots, g_t\rangle \text{ og}$$
$$\langle LT(G)\rangle = \langle LT(g_1), \dots, LT(g_t)\rangle.$$

Me viser først at $G \subset I$ gjeld for alle steg i algoritmen. Dette er sant frå byrjinga, deretter legg me resten $\overline{S(p,q)}^{G'}$ for $p, q \in G$ til G. Viss $G \subset I$, då er p, q og derfor også $S(p,q)$ i I, og sidan me deler med $G' \subset I$ får me $G \cup \{S\} \subset I$. Me ser også at G inneheld basisen F av I, slik at G også er ein basis for I.
Algoritmen stoppar når $G = G'$ som betyr at $\overline{S(p,q)}^{G'} = 0$ for alle $p, q \in G$. Me har at G er ein gröbnerbase for $\langle G\rangle = I$ frå teorem 4.40.
Nå skal me vise at algoritmen stoppar. Me må sjå på kva som skjer ved kvart steg av algoritmen. Mengda G består av G' (den gamle G) og resten av S-polynom av element i G'. Då er

$$\langle LT(G')\rangle \subset \langle LT(G)\rangle \tag{4.10}$$

sidan $G' \subset G$. Viss $G' \neq G$ er $\langle LT(G')\rangle$ strengt mindre enn $\langle LT(G)\rangle$. For å sjå dette, anta at resten r, til eit S-polynom, har blitt lagt til G. Sidan r er ein rest etter divisjon med G', er $LT(r)$ ikkje deleleg med nokre av dei leiiande ledda til element i G', og $LT(r) \notin \langle LT(G')\rangle$. Men me har at $LT(r) \in \langle LT(G)\rangle$. Då må $\langle LT(G')\rangle$ vere mindre.
Me ser av likning (4.10) at ideala $\langle LT(G')\rangle$ etter fleire repetisjonar av algoritmen, vil danne ei stigande rekkje med ideal i $k[x_1, \ldots, x_n]$. Frå teorem 4.41 har me at etter endeleg mange repetisjonar, vil rekkja bli stabilisert slik at $\langle LT(G')\rangle = \langle LT(G)\rangle$. Då har me at $G = G'$, og algoritmen må stoppe etter eit endeleg tal steg. □

Det neste eksempelet viser korleis me kan bruke denne algoritmen.

Eksempel 12. Me har $F = (x^2 + y, x^2y + 1)$ og lex-orden $x > y$ på $k[x, y]$. Skjekk om F er ein gröbnerbase, viss ikkje finner me ein gröbnerbase. Me byrjar med å finne S-polynomet

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

Sidan ingen av dei leiande ledda i F (x^2 og x^2y) deler y^2 eller -1. Då har me at

$$\overline{S(x^2 + y, x^2y + 1)}^{F} = y^2 - 1.$$

No skriv me $F' = F \cup \{y^2 - 1\} = (x^2 + y, x^2y + 1, y^2 - 1)$. For å sjekke om dette er ein gröbnerbase, må me finne ut om $S_1 = \overline{S(x^2 + y, y^2 - 1)}^{F'} = 0$ og om $S_2 = \overline{S(x^2 + y, x^2y + 1)}^{F'} = 0$. Me veit at $S(x^2 + y, x^2y + 1) = y^2 - 1 + 0$, slik at resten er null. Me får

$$S(x^2 + y, y^2 - 1) = y^2(x^2 + y) - x^2(y^2 - 1) = y^3 + x^2.$$

Når ein brukar divisjonsalgoritmen får ein at $x^2 + y^3 = (x^2 + y) + y(y^2 - 1) + 0$. Me ser at resten er null. No finn me S-polynomet

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

og me ser at resten er null. Frå Buchberger sin algoritme (teorem 4.42), er F' ein gröbnerbase.

Ved å bruke Buchberger sin algoritme får me ofte unødvendig store gröbnerbasar. Me vil derfor ta vekk nokon generatorar ved å bruke følgjande lemma.

Lemma 4.43. *La G vere ein gröbnerbase for polynomidealet I. La $p \in G$ vere eit polynom slik at $LT(P) \in \langle LT(G - \{p\}\rangle$. Da er $G - \{p\}$ også ein gröbnerbase for I.*

Prov. Me veit at $\langle LT(G)\rangle = \langle LT(I)\rangle$. Viss $LT(p) \in\in \langle LT(G - \{p\}\rangle$ har me at $\langle LT(G - \{p\}\rangle = \langle LT(G)\rangle$. Frå definisjonen på ein gröbnerbase følgjer det at $G - \{p\}$ også er ein gröbnerbase. □

For at ein gröbnerbase skal vere unik må me finne den reduserte gröbnerbasen, s.92 [1].

Definisjon 4.44. Ein redusert gröbnerbase for eit polynomideal I er ein gröbnerbase G for I slik at:

i) $LC(p) = 1$ for alle $p \in G$,

ii) for alle $p \in G$ ligg ingen monom av p i $\langle LT(G - \{p\})\rangle$.

Når me finn gröbnerbasar ved å nytte Macaulay2 i kapittel sju, er det den redusert gröbnerbasen me finn. Me avsluttar dette delkapittelet med å gi eit eksempel på ein redusert gröbnerbase.

Eksempel 13. Me har $f_1 = 3x - 6y - 2z, f_2 = 2x - 4y + 4w$ og $f_3 = x - 2y - z - w$. Og me let idealet I vere $I = \langle f_1, f_2, f_3 \rangle$, og brukar lex-orden $x > y > z > w$. Me finn S-polynomet

$$f_4 = S(f_1, f_2) = x - 2y - 2/3z - x + 2y - z - w = z + 3w,$$

og legg f_4 til basen. Og finn

$$S(f_3, f_4) = x - 2y - z - w + (z + 3w) = x - 2y + 2w.$$

Me har då fått ein redusert gröbnerbase $G = \{x - 2y + 2w, z + 3w\}$, fordi den oppfyller krava til ein redusert gröbnerbase.

4.5 Eliminasjonsordningar

Me skal no sjå på eliminasjonsordningar, som me må bruke for å eliminere variablar frå eit system av polynomlikningar. Målet med dette er å få likningar med kun ein ukjend, slik at me enkelt kan løyse systemet. Strategien for å systematisk eliminera variablar vil bli gitt i eliminasjonsteoremet, og utvidingsteoremet blir nytta for å finne løysinga til systemet. Me vil brukar gröbnerbasar for å gi eit prov for eliminasjonsteoremet. Til slutt vil me vise eit eksempel på korleis dette blir brukt. Seinare i oppgåva vil ei eliminasjonsordning vil bli nytta for å finne ein rekonstruksjon av (R, a), sjå kapittel sju.

Definisjon 4.45. Gitt $I = \langle f_1, \ldots, f_s \rangle \subset k[x_1, \ldots, x_n]$. Då er det l-te eliminasjonsidealet I_l, eit idealet av $k[x_{l+1}, \ldots, x_n]$, definert som:

$$I_l = I \cap k[x_{l+1}, \ldots, x_n].$$

Derfor består I_l av alle konsekvensar der $f_1 = \ldots = f_s = 0$, som eliminerar variablane $x_1, \ldots, x_l$. Me ser for å eliminere $x_1, \ldots, x_n$ må me finne polynom i det l-te eliminasjonsidealet I_l. Derfor må me ha ein systematisk måte å gjere dette på. Og det er det eliminasjonsteoremet gir oss.

Teorem 4.46. ***Eliminasjonsteoremet.*** *La $I \subset k[x_1, \ldots, x_n]$ vere eit ideal og la G vere ein gröbnerbase av I med omsyn på lex-orden der $x_1 > x_2 > \ldots > x_n$. Då har me at for alle $0 \leq l \leq n$, er*

$$G_l = G \cap k[x_{l+1}, \ldots, x_n]$$

ein gröbnerbase av det l-te eliminasjonsidealet I_l.

Prov. Vel ein l mellom 0 og n. Sidan me har at $G_l \subset I_l$, treng ein kun å vise at

$$\langle LT(I_l) \rangle = \langle LT(G_l) \rangle,$$

på grunn av definisjonen til ein gröbnerbase. Me ser at $\langle LT(G_l) \rangle \subset \langle LT(I_l) \rangle$, og me må vise at $\langle LT(I_l) \rangle \subset \langle LT(G_l) \rangle$. Me treng å vise at $LT(f)$ for ein tilfeldig valt $f \in I_l$, er deleleg med $LT(g)$ for nokre $g \in G_l$.
Me veit at f også ligg i I. Då har me at $LT(f)$ er deleleg med $LT(g)$ for nokre $g \in G$, sidan G er ein gröbnerbase av I. Og fordi $f \in I_l$, betyr det at $LT(g)$ kun har variablane $x_{l+1}, \ldots, x_n$. Sidan me brukar lex-orden er alle monom som involverar $x_1, \ldots, x_l$ større enn alle monom i $k[x_{l+1}, \ldots, x_n]$. Då følgjer det av $LT(g) \in k[x_{l+1}, \ldots, x_n]$ at $g \in k[x_{l+1}, \ldots, x_n]$, då må g vere i G_l. □

Dette teoremet viser at ein gröbnerbase for *lex*-orden ikkje berre eliminerar den første variabelen, men også dei to første variablane, dei tre første og så vidare. I kapittel sju skal me bruke dette teoremet til å eliminere bestemte variablar.

No skal me sjå på utvidingsteoremet.
Anta at me har eit ideal $I \subset k[x_1, \ldots, x_n]$. Som tidlegare har me den affine variteten,

$$V(I) = \{(a_1, \ldots, a_n) \in k : f(a_1, \ldots, a_n) = 0 \ \forall f \in I\}.$$

For å beskrive punkt i $V(I)$ må me bygge opp løysingar, ein koordinat om gongen. Me vel ein l mellom 0 og n. Dette gir eliminasjonsidealet I_l. Då er løysinga $(a_{l+1}, \ldots, a_n) \in V(I_l)$ ei delvis løysing av det originale likningssystemet. Me må utvie denne løysinga for å få ei løysing i $V(I)$. Me byrjar med å legge til ein koordinat, og finn a_l slik at $(a_l, a_{l+1}, \ldots, a_n)$ ligg i $V(I_{l-1})$. For å gjere dette meir konkret, anta at $I_{l-1} = \langle g_1, \ldots, g_t \rangle$ er i $k[x_1, \ldots, x_n]$. Me vil finne løysingar $x_l = a_l$ av

$$g_1(x_l, a_{l+1}, \ldots, a_n) = \ldots = g_t(x_l, a_{l+1}, \ldots, a_n) = 0.$$

Då får me polynom av ein variabel x_l, og at moglege a_l er røttene til den største felles divisoren til t-polynoma.

Dersom me avgrensar oss til å sjå om me kan eliminere kun den første variabelen x_1. Då vil me finne ut om ei delvis løysing $(a_2, \ldots, a_n) \in V(I_l)$ kan bli utvia til ei løysing for $(a_1, a_2, \ldots, a_n) \in V(I)$. Det neste teoremet gir oss at dette er mogleg.

Teorem 4.47. ***Utvidingsteoremet.*** *La $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{C}[x_1, \ldots, x_n]$, og la I_l vere det første eliminasjonsidealet til I. For kvar $1 \leq i \leq s$, skriv f_i som*

$$f_i = g_i(x_2, \ldots, x_n)x_1^{N_i} + \ \textit{termar der } x_1 \textit{ har grad } < N_i,$$

der $N_i \geq 0$. Og $g_i \in \mathbb{C}[x_2, \ldots, x_n]$, er ulik null. Anta at me har ei delvis løysing $(a_2, \ldots, a_n) \in V(I_1)$. Viss $(a_2, \ldots, a_n) \in V(g_1, \ldots, g_s)$ då eksisterar det ein $a_1 \in \mathbb{C}$, slik at $(a_1, a_2, \ldots, a_n) \in V(I)$.

Prov. Sjå s. 165, [1]. □

I det neste eksempelet får me brukt for eliminasjonsorden og utvidingsteoremet for å finne ei løysing på problemet.

Eksempel 14. Me har eit ideal $I = \langle x^2+y+z-1, x+y^2+z-1, x+y+z^2-1 \rangle$ i $k[x, y, z]$ og me har lex-orden $x > y > z$. Me kan finne ein gröbnerbase G for I ved å bruke Macaulay2-programmet. Basen er gjeve ved fire polynomlikningar

$$\begin{aligned} g_1 &= x + y + z^2 - 1, \\ g_2 &= y^2 - y - z^2 + z, \\ g_3 &= 2yz^2 + z^4 - z^2, \\ g_4 &= z^6 - 4z^4 + 4z^3 - z^2. \end{aligned}$$

Sidan g_4 kun er gjeve ved variabelen z, og dei andre variablane er eliminert kan me enkelt finne ei løysing. Me har $z = 0, 1, -1 \pm \sqrt{2}$. Ved å substituera desse verdiane inn i dei andre likningane, finn me løysingar for x og y. Me får då dei fem løysingane:

$$(1,0,0), (0,1,0), (0,0,1), (-1+\sqrt{2}, -1+\sqrt{2}, -1+\sqrt{2}) \text{ og } (-1-\sqrt{2}, -1-\sqrt{2}, -1-\sqrt{2}).$$

Grunnen til at me kunne løyse dette systemet var at me fann ei likning som kun involverte ein variabel. Dei andre variablane var eliminerte. Me kunne dermed finne verdiar for z. Og ved å substituere desse inn i dei andre likningane, gjere ei utviding. Då fekk me ut verdiar for x og y.

Kapittel 5

Kameramodellar

Eit kamera er ei avbilding mellom den tredimensjonale verda og eit todimensjonalt bilete. I dette kapittelet skal me sjå på fleire kameramodellar. Desse modellane er kameraavbildingar representert som matriser, med spesielle eigenskapar. Når me studerar desse matrisene får me brukt for det som står i tildlegare kapittel om projektiv geometri. Me vil sjå at både projeksjonssenteret og biletplanet er enkle å finne utifrå matriserepresentasjonen. Me skal kun sjå på projeksjon av punkt, og ikkje linjer.
Me byrjar denne delen med på sjå på den enklaste kameramodellen og deretter generalisere den. Deretter skal me sjå nærmare på det projektive kameraet og kameraanatomi. Og så skal me forklare geometrien og matematikken bak kamerasenteret, prinsipalplanet og prinsipalpunktet.

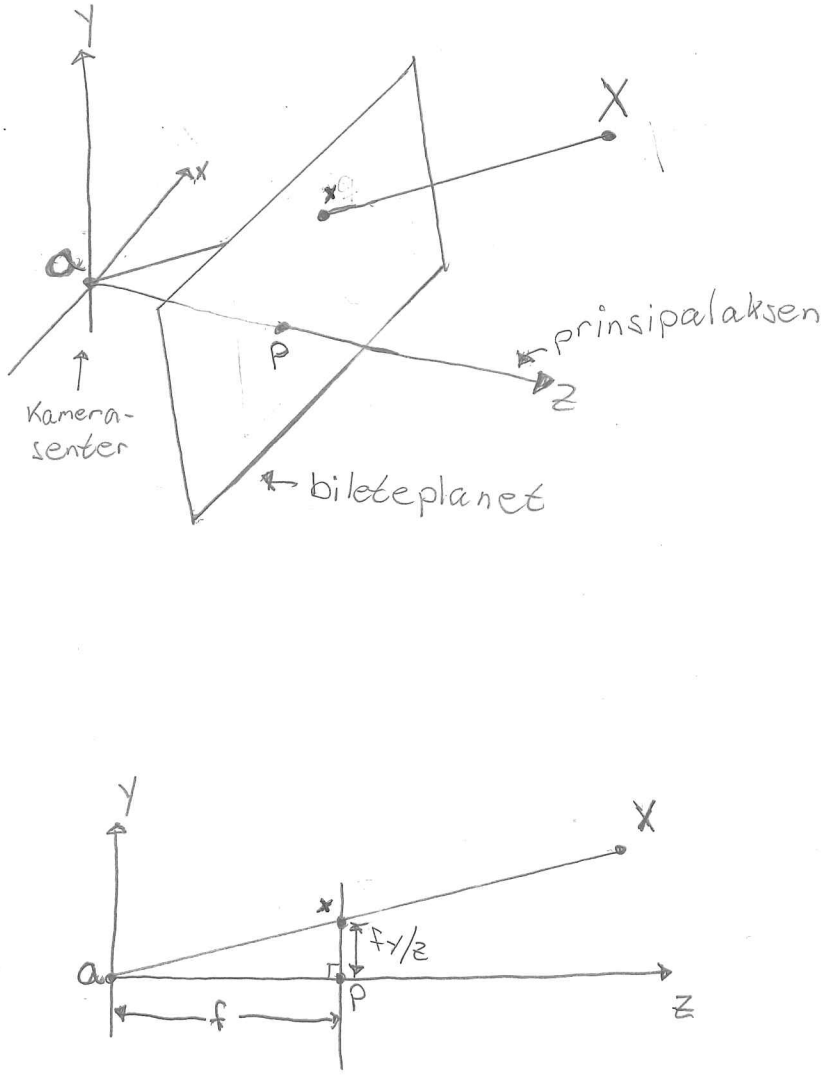
5.1 Endelege kamera

Me byrjar med ein basis nøkkelholsmodell, d.v.s at me ser på sentralprojeksjonen frå punkt i rommet til punkt på eit plan. Og let senteret til projeksjonen vere origo, i eit euklidisk/kartesisk koordinatsystem. Me skal sjå på planet $Z = f$ (der f er fokallengda), som blir kalla biletplanet eller fokalplanet. Dette planet er parallelt med (x, y)-planet. Under nøkkelholsmodellen vil eit punkt i rommet, $X = (x, y, z)^T$, bli avbilda til eit punkt på biletplanet. Det avbilda punktet vil liggje der ei linje gjennom punktet X og projeksjonssenteret møter biletplanet. Punktet X blir avbilda slik:

$$(x, y, z)^T \to (fx/z, fy/z)^T \tag{5.1}$$

og $\mathbb{R}^3 \to \mathbb{R}^2$. Likning (5.1) beskriver sentralprojeksjonsavbildinga frå verda til biletekoordinatar.

Projeksjonssenteret blir kalla kamerasenteret, eller det optiske senteret. Linja frå kamerasenteret vinkelrett på biletplanet, blir kalla prinsipalaksen til kameraet. Punktet der prinsipalaksen møter biletplanet blir kalla prinsipalpunktet. Planet gjennom kamerasenteret, som ligg parallelt med biletplanet, blir kalla prinsipalplanet til kameraet. Dette er illustrert i figuren på neste side, figur 1: Kamerageometri for eit nøkkelholskamera.



Figur 1: Kamerageometri for eit nøkkelholskamera. Me har kamerasenteret a, som ligg i origo i eit koordinatsystem med x, y og z-akse. Punktet X i rommet blir avbilda i biletet, og f er fokallengda til kamera. Biletplanet ligg framfør kameraet. Punktet p er prinsipalpunktet, og er skjeringa av biletplanet og prinsipalaksen.
I det nederste koordinatsystemet ser ein at bildepunktet x sin y-koordinat kan skrivast som fy/z.

Dersom verda og biletpunkt er representert av homogene vektorar, kan ein skrive likning (5.1):

$$\begin{pmatrix} x \\ y \\ z \\ 1 \end{pmatrix} \rightarrow \begin{pmatrix} fx \\ fy \\ z \end{pmatrix} = \begin{bmatrix} f & & & 0 \\ & f & & 0 \\ & & 1 & 0 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \\ 1 \end{pmatrix}, \tag{5.2}$$

som også kan skrivast $diag(f, f, 1)[I \mid 0]$.
Me seier at X er verdspunktet representert av den homogene 4-vektoren $(x, y, z, 1)^T$. Og me har bildepunktet respresentert som ein 3-vektor, $\mathbf{x} = (fx, fy, z)^T$, og P er ei 3×4-kameraprojeksjonsmatrise, som er homogen. Då kan ein skrive likning (5.2) som

$$\mathbf{x} = PX.$$

Denne likninga definerer kameramatriser for nøkkelholsmodellen til sentralprojeksjonen, som $P = diag(f, f, 1)[I \mid 0]$.

Prinsipalpunktforskyving

I uttrykk (5.1) antek ein at origo til koordinatane i biletplanet er i prinsipalpunktet. Dersom origo ikkje er i prinsipalpunktet har me ei avbilding,

$$(x, y, z)^T \rightarrow (fx/z + p_x, fy/z + p_y)^T.$$

Vektoren $(p_x, p_y)^T$ er koordinatane til prinsipalpunktet. Denne avbildinga "flyttar" origo (i biletplanet) til prinsipalpunktet. No kan me skrive dette i homogene koordinatar,

$$\begin{pmatrix} x \\ y \\ z \\ 1 \end{pmatrix} \rightarrow \begin{pmatrix} fx + zp_x \\ fy + zp_y \\ z \end{pmatrix} = \begin{bmatrix} f & & p_x & 0 \\ & f & p_y & 0 \\ & & 1 & 0 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \\ 1 \end{pmatrix}. \tag{5.3}$$

Matrisa $K = \begin{bmatrix} f & & p_x \\ & f & p_y \\ & & 1 \end{bmatrix}$, blir kalla kalibreringsmatrisa. Ein kan då skrive likning (5.3), som

$$\mathbf{x} = K[I \mid 0]X_{cam}, \tag{5.4}$$

der $X_{cam} = \begin{pmatrix} x \\ y \\ z \\ 1 \end{pmatrix}$. Her antek ein at kameraet er lokalisert i origo i eit euklidisk koordinatsystem med prinsipalaksen peikande langs z-aksen. Ein kan kalla dette koordinatsystemet for kamerakoordinatramma.

Kamerarotasjon og translasjon

Generelt vil punkt i rommet bli uttrykt i ei anna euklidisk koordinatramme, kalla verdskoordinatramma. Dei to rammene (kameraramma og verdsramma) er relatert til kvarandre ved ein rotasjon og ein translasjon.
Me seier at $\tilde{X}$ er ein inhomogen 3-vektor som representerar koordinatane til eit punkt i verdskoordinatramma, og $\tilde{X}_{cam}$ representerar same punkt i kamerakoordinatramma. Då kan me skrive

$$\tilde{X}_{cam} = R(\tilde{X} - a),$$

der a er koordinatane til kamerasenteret i verdskoordinatramma, og R er ei 3×3-rotasjonsmatrise som representerar orienteringa av kameraramma. Denne likninga kan skrivast i homogene koordinatar

$$X_{cam} = \begin{bmatrix} R & -Ra \\ 0 & 1 \end{bmatrix} \begin{pmatrix} x \\ y \\ z \\ 1 \end{pmatrix} = \begin{bmatrix} R & -Ra \\ 0 & 1 \end{bmatrix} X. \tag{5.5}$$

Når ein set dette saman med likning (5.4), får ein

$$\mathbf{x} = KR[I \mid -a]X, \tag{5.6}$$

der X er i verdsramma. Dette er den generelle avbildinga til eit nøkkelholskamera. Og avbildinga har ni fridomsgrader; 3 for K, 3 for R og 3 for a. Parametrane i K blir kalla indre kameraparameter, eller den indre orientasjonen til kameraet. Parametrane R og a, som relaterar kameraorientasjonen og posisjonen til eit verdskoordinassystem, blir kalla eksterne parameter eller ytre orientasjon.
Det er ofte nyttig å ikkje uttrykke kamerasenteret eksplisitt, men heller representere verda til biletetransformasjonen som $\tilde{X}_{cam} = R\tilde{X} + t$, då er kameramatrisa: $P = K[R \mid t]$, der $t = -Ra$ i likning (5.6).

CCD kamera

Når ein brukar nøkkelholskamera-modellen, antek ein at biletkoordinatane er euklidiske koordinatar som har lik skalering i begge retningane til aksane. I CCD-kamera (CCD="charge-coupled device"), er det mogleg å ha ikkje-kvadratiske pixlar. Viss biletekoordinatane er målt i pixlar, gir dette ulik skaleringsfaktor i kvar retning. Me har at tal på pixlar per einheitsavstand i biletekoordinatane, er m_x i x-retning, og m_y i y-retning. Transformasjonen frå verdskoordinatar til pixelkoordinatar blir då gjeven ved å multiplisere kalibreringsmatrisa for eit nøkkelholskamera, med den ekstra faktoren $diag(m_x, m_y, 1)$. Den generelle forma til kalibreringsmatrisa for eit CCD-kamera blir då

$$K = \begin{bmatrix} \alpha_x & & x_0 \\ & \alpha_y & y_0 \\ & & 1 \end{bmatrix}, \tag{5.7}$$

der $\alpha_x = fm_x$ og $\alpha_y = fm_y$ representerar fokallengda til kameraet, i form av pixeldimensjonar i x- og y-retninga. Og $\tilde{x}_0 = (x_0, y_0)$ er prisipialpunktet, i form av pixeldimensjonar med koordinatar $x_0 = m_x p_x$ og $y_0 = m_y p_y$. Ein ser at eit CCD-kamera har ti fridomsgrader.

Endelege projektive kamera

Me kan sjå på kalibreringsmatrisa,

$$K = \begin{bmatrix} \alpha_x & s & x_0 \\ & \alpha_y & y_0 \\ & & 1 \end{bmatrix}. \tag{5.8}$$

Denne matrisa skil seg frå kalibreringsmatrisa gjeven i (5.7), ved ein tilleggsparameter s. Denne parameteren blir kalla skrå/forskyvnings-parameteren, og er lik null for dei fleste normale kamera. Eit kamera $P = KR[I \mid -a]$ med K som i likning (5.8), blir kalla eit endeleg projektiv kamera, og har elleve fridomsgrader.
Tilleggsparameteren s er ei forskyving i pixelelementa i CCD-matrisa, slik at x-aksen og y-aksen ikkje står vinkelrett på kvarandre.

5.2 Det projektive kamera og kameraanatomi

I denne delen skal me bli betre kjent med anatomien til eit kamera, og det projektive kamera. Me skal sjå nærmare på kamerasenteret, prinsipalplanet og prinsipalpunktet.
Eit generelt projektivt kamera P avbildar verdspunkt X til biletpunkt $\mathbf{x}$ ifølgje likninga

$$\mathbf{x} = PX.$$

Denne avbildinga er representert av ei homogen 3×4-matrise av rang 3, og har elleve fridomsgrader.

Kamerasenter

Matrisa P har eit eindimensjonalt høgre nullrom, fordi den er av rang 3 og har fire kolonner. Anta at nullrommet er generert av ein 4-vektor O, slik at $PO = 0$. Då er O kamerasenteret representert som ein homogen 4-vektor.
Me ser på linja som inneheld O, og eit anna punkt A (i 3D). Punkt på denne linja kan skrivast som

$$X(\lambda) = \lambda A + (1 - \lambda)O.$$

Under avbildinga $\mathbf{x} = PX$, blir alle punkt på denne linja projesert til:

$$\mathbf{x} = PX(\lambda) = \lambda PA + (1 - \lambda)PC = \lambda PA,$$

sidan $PO = 0$. Alle punkt på linja er avbilda til same biletpunkt PA, og det betyr at linja må vere ein stråle frå kamerasenteret. Sidan linja $X(\lambda)$ ein stråle gjennom kamerasenteret, for alle A. Frå dette følgjer det at O er den homogene representasjonen av kamerasenteret.
Ein slik representasjon av ei linje kjem me tilbake til i kapittel 6,2 under avsnittet om den algebraiske utleiinga av fundamentalmatrisa.

Kolonne- og rekkjevektorar

Kolonnane til det projektive kamera er 3-vektorar, som frå ei geometrisk tolking er bestemte biletpunkt. Med notasjonen at kolonnene til P er p_i for $(i = 1, \ldots, 4)$, då er p_1 forsvinningspunktet til verdskoordinatane på x-aksen. Og p_2 og p_3 er forsvinningspunkt av verdskoordinatane ved $y-$ og z-aksen. Desse punkta er bilete av akseretninga, t.d. har x-aksen retning $D = (1, 0, 0, 0)^T$, som er bilda i $p_1 = PD$. Og kolonna p_4 er bilete av verdsorigo.

Rekkjene til det projektive kamera er 4-vektorar og kan tolkast geometrisk som bestemte verdsplan. Me introduserer notasjonen at rekkene til P er p^{iT}.

$$P = \begin{bmatrix} p_{11} & p_{12} & p_{13} & p_{14} \\ p_{21} & p_{22} & p_{23} & p_{24} \\ p_{31} & p_{32} & p_{33} & p_{34} \end{bmatrix} = \begin{bmatrix} p^{1T} \\ p^{2T} \\ p^{3T} \end{bmatrix}.$$

Prinsipalplanet

Prinsipalplanet er planet gjennom kamerasenteret parallelt til biletplanet. Det består av punktmengda X. Denne punktmengda er avbilda på linja i det uendelege, i bilete. Eksplisitt er $PX = (x, y, 0)^T = l_\infty$. Eit punkt ligg på prinsipalplanet til kamera viss og berre viss $p^{3T}X = 0$. Med andre ord er p^3 vektoren som representerer prinsipalplanet til kamera. Viss O er kamerasenteret, er både PO og $p^{3T}O$ lik null. Det vil seie at kamerasenteret O, ligg på prinsipalplanet til kamera.

Akseplan

Me ser på punktmengda X på planet p^1. Denne mengda tilfredsstillar $p^{1T}X = 0$, og er bilete til $PX = (0, y, w)$, som er punkt på biletet sin y-akse. Det følgjer frå $PO = 0$ at $p^{1T}O = 0$, og kamerasenteret O ligg på planet p^1. Dermed er planet p^1 definert av kamerasenteret og linja $x = 0$ i bilete. Tilsvarande er planet p^2 definert av kamerasenteret O, og linja $y = 0$.
Til forskjell frå prinsipalplanet p^3, er akseplana p^1 og p^2 avhengig av bilete sine x- og y-aksar. Det vil seie at dei er avhengig av valet av biletkoordinatsystem. Skjeringslinja til plana p^1 og p^2 er ei linje som bind kamerasenteret og biletorigo. Denne linja vil ikkje, generelt, vere samsvarande til kamera sin prinsipalakse.
Me veit at kamerasenteret O, ligg på alle tre plana, og må derfor vere skjeringspunktet. Algebraisk er kravet at kamerasenteret skal liggje på alle plana gjeve ved $PO = 0$, som er likninga for kamerasenteret.

Prinsipalpunktet

Prinsipalaksen er ei linje gjennom kamerasenteret O, med retning vinkelrett på prinsipalplanet p^3. Denne aksen skjærer biletplanet i prinsipalpunktet. Me vil no finne ein måte å bestemme dette punktet.
Normalen til eit plan $\pi = (\pi_1, \pi_2, \pi_3, \pi_4)^T$ er ein vektor $(\pi_1, \pi_2, \pi_3)^T$. Denne vektoren kan bli representert som punktet $(\pi_1, \pi_2, \pi_3, 0)^T$, på planet i det uendelege. For prinsipalplanet p^3 for eit kamera, er dette punktet gjeve ved $(p_{31}, p_{32}, p_{33}, 0)^T$, som me kallar $\hat{p}^3$. Ved å projesere dette punktet ved hjelp av kameramatrisa P, får ein at prinsipalpunktet til kamera er gitt ved likninga, $P\hat{p}^3$.

Kapittel 6

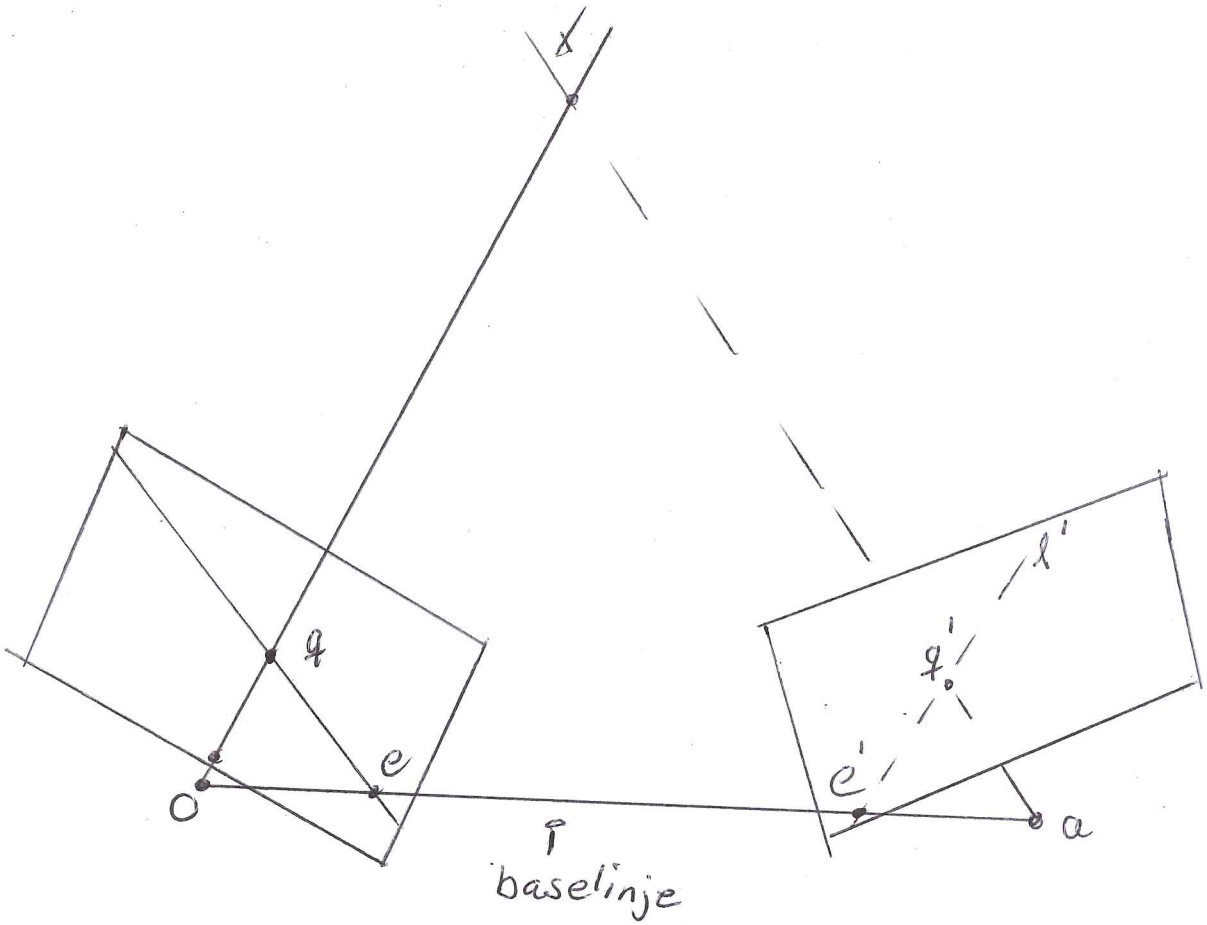
Epipolar geometri og den fundamentale matrisa

I dette kapittelet skal me sjå på tilfellet der me har to bilete, og eit verdspunkt. Den projektive geometrien mellom to bilete kallar me for epipolar geometri. Epipolar geometri er uavhengig av scenestrukturen. Den er kun avhengig av kameraene sine indre parameter og relative posisjon. Me ska sjå at fundamentalmatrisa F, innkapslar denne indre geometrien. Den er ei 3×3-matrise av rang 2. Og me skal sjå at dersom eit punkt i 3-rom X er avbilda som q i første bilete, og q' i det andre bilete, då tilfredsstillar biletpunkta $q'^T F q = 0$. I denne delen skal det bli forklart kvifor dette stemmer.
Me vil først beskrive epipolar geometri. Deretter vil me utleie fundamentalmatrisa på ein geometrisk, og ein algebraisk måte. Deretter vil me vise at me kan finne kameramatrisene, opp til ein multiplikasjon med ein projektiv transformasjon. Dette kapittelet gir basisen for korleis me kan finne ei essensiell matrise, i kapittel sju.

6.1 Epipolar geometri

Byrjar først med litt terminologi innan epipolargeometri (sjå Figur 2: Epipolar geometri, på neste side):
- epipolen er skjeringspunktet til linja mellom kamerasentera, med biletplanet. Med andre ord skjeringspunktet av baselinja med biletplanet. Epipolen er biletet i eine bilete av kamerasenteret til det andre biletet. Det er også forsvinningspunktet av baselinjaretninga.
- eit epipolart plan er eit plan som inneheld baselinja. Det er ein einparameterfamilie (ein pensel) av epipolare plan.
- ei epipolar linje er skjeringa til eit epipolart plan med biletplanet.

Den epipolare geometrien mellom to kameraposisjonar, er geometrien til skjeringa av biletplana med penslane av linjer som har baselinja som akse. Baselinja er den linja som går igjennom begge kamerasentera.



Figur 2: Epipolar geometri. Me har kamerasenteret O i det første bilete, og a i det andre. Biletet av verdspunktet X, er punktet q i det første bilete, og q' i det andre. Kamersentera og punkta q, q' og X ligg alle i eit plan som me kallar π. Linja l' er epipolarlinja, og går igjennom epipolarpunktet e' og punktet q'. Epipolarlinja i det andre bilete går igjennom punkt q og epipolarpunktet e.

Anta at eit punkt X, blir avbilda i to kamera, q i første bilete og q' i det andre. Me har kamerasenteret O i det første kamera, og a i det andre. Kva er relasjonen mellom korresponderande biletpunkt q og q'?
Biletpunkta q og q', punktet X som ligg i rommet og kamerasentera, er koplanare. Då ligg dei alle i same plan, og me kallar dette planet for π. Med andre ord har me ei linje som går gjennom kamerasenteret O og biletpunktet q, og ei linje gjennom a og q'. Desse linjene skjærer kvarandre i punktet X. Og både linjene og punkta må liggje på same plan, π (sjå figur 2).

Anta at me kun veit q. Korleis er korresponderande punkt q' avgrensa?
Planet π er definert av baselinja og strålen som går gjennom O og q. Me veit også at q' må liggje i planet π. Dette punktet må derfor liggje på skjeringslinja mellom π og biletplanet. Denne skjeringslinja kallar me l', og er bilete av strålen bakprojesert frå q. Denne linja l', er epipolarlinja korresponderande til q. Og punktet q' må liggje på denne linja. Me kan sjå av figur 2, at viss me flyttar verdspunket X, som ligg på linja gjennom O og q, vil punktet q' flytte seg langs epipolarlinja l'.

6.2 Fundamentalmatrisa

Den fundamentale matrisa er den algebraiske representasjonen av epipolar geometri.
Gitt eit biletpar, eksisterer det ei korresponderande epipolar linje l' i det andre bilete for kvart punkt q i det første. Eit punkt q' i det andre bilete, som svarar til punktet q, må liggje på den epipolare linja l'. Den epipolare linja er projeksjonen i det andre bilete av strålen frå punktet q gjennom kamerasenteret O i det første kamera. Det fins derfor ei avbilding: $q \mapsto l'$ frå punkt i eit bilete til korresponderande epipolar linje i det andre bilete. Det er denne avbildinga me no skal utforska.

Geometrisk utleiing

Me byrjar med ei geometrisk utleiing av fundamentalmatrisa. Avbilding frå eit punkt i eit bilete, til korresponderande epipolar linje i det andre bilete, kan dekomponerast i to steg. Her er det første steget at punktet q blir avbilda til eit punkt q' i det andre bilete. Dette punktet ligg på den epipolare linja l', og er eit potensielt korresponderande punkt for punktet q. I det andre steget ser me på den epipolare linja l', som er linja som bind q' til epipolen e'.

Steg 1: Punktoverføring via eit plan
Me har eit plan, π, i rommet som ikkje går igjennom nokon av dei to kamerasentera. Strålen gjennom første kamerasenter, som korresponderer til punktet q, møter planet π i punktet X. Og dette punktet blir projesert til eit punkt q' i det andre bilete. Denne prosedyren blir kalla overføring via planet π. Sidan X ligg på strålen som korresponderer til q, må det projeserte punktet q' liggje på den epipolare linja l'. Punkta q og q' er begge bilete av 3D-punktet X, som ligg på eit plan. Mengda av alle slike punkt q_i i det første bilete, og korresponderande punkt q'_i i det andre bilete, er projektivt ekvivalente. Dei er projektivt ekvivalente til den planare punktmengda X_i. Det eksisterer derfor ein 2D homografi H_π, som avbildar kvar q_i til q'_i.

Steg 2: Konstruering av den epipolare linja
Gitt punktet q' og epipolar linja l', som går gjennom q' og epipolen e'. Ved å bruke resultat 2.3, kan me uttrykke denne linja som $l' = e' \times q'$.

Gitt vektor $b = (b_1, b_2, b_3)$ og $a = (a_1, a_2, a_3)$ i $\mathbb{R}^3$, definerer me den assosierte antisymmetriske matrisa som

$$\mathcal{T}_a = \begin{pmatrix} 0 & -a_3 & a_2 \\ a_3 & 0 & -a_1 \\ -a_2 & a_1 & 0 \end{pmatrix}. \tag{6.1}$$

Matrisa $\mathcal{T}_{e'}$ er ei antisymmetrisk matrise (sjå uttrykk (6.1)) og har rang 2, dette blir vist i provet for lemma 7.8. Den antisymmetriske matrisa blir brukt i det neste resultatet, og også seinare i dette kapittelet.

Resultat 6.1. *Me har at for alle $a, b \in \mathbb{R}^3$ er $\mathcal{T}_a \cdot b = a \times b$.*

Prov. Me viser dette ved å gjere utrekningar.

$$\begin{aligned} \mathcal{T}_a \cdot b &= \begin{pmatrix} 0 & -a_3 & a_2 \\ a_3 & 0 & -a_1 \\ -a_2 & a_1 & 0 \end{pmatrix} \cdot \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix} \\ &= \begin{pmatrix} 0 - a_3 b_2 + a_2 b_3 \\ a_3 b_1 + 0 - a_1 b_3 \\ -a_2 b_1 + a_1 b_2 + 0 \end{pmatrix} \\ &= \begin{pmatrix} -a_3 b_2 + a_2 b_3 \\ -a_1 b_3 + a_3 b_1 \\ -a_2 b_1 + a_1 b_2 \end{pmatrix} \\ &= (a_1, a_2, a_3) \times (b_1, b_2, b_3) = a \times b. \\ \Rightarrow \mathcal{T}_a \cdot b &= a \times b \end{aligned}$$

□

Ved å nytte dette resulatet kan me skrive $l' = e' \times q'$ som

$$l' = \mathcal{T}_{e'} \cdot q'.$$

Frå steg 1 kan me skriva $q' = H_\pi q$ og dermed har me at:

$$l' = \mathcal{T}_{e'} \cdot H_\pi \cdot q = Fq,$$

der me definerar F som $\mathcal{T}_{e'} \cdot H_\pi$. Me kallar denne matrisa F, for fundamentalmatrisa.

Definisjon 6.2. Den fundamentale matrisa F kan skrivast som $F = \mathcal{T}_{e'} \cdot H_\pi$, der H_π er overføringsavbildinga frå eit bilete til eit anna, via eit plan π. Sidan $\mathcal{T}_{e'}$ har rang 2 og H_π har rang 3, har matrisa F rang 2.

Geometrisk representerer F ei avbilding frå det todimensjonale projektive planet $\mathbb{P}^2$ i det første bilete, til penselen av epipolare linjer gjennom epipolen e'. Den representerer derfor ei avbilding frå eit todimensjonalt til eit eindimensjonalt projektivt rom, og må derfor har rang 2. No vil me sjå på korleis fundamentalmatrisa kan blir utleia på ein algebraisk måte.

Algebraisk utleiing

Me skal no algebraisk utleia forma til fundamentalmatrisa utifrå dei to kameraprojeksjonsmatrisene P og P'. Først kjem ein definisjon på pseudo-inversen til ei matrise.

Definisjon 6.3. Pseudo-inversen til P er matrisa $P^+ = P^T(PP^T)^{-1}$. Då ser me at $PP^+ = I$ s. 590-592, [4].

Denne definisjonen blir brukt i provet til den neste setninga, for å vise likning (6.2).

Setning 6.4. Me kan skrive fundamentalmatrisa som

$$F = \mathcal{T}_{e'} \cdot P'P^+, \tag{6.2}$$

og me ser at homografien har den eksplisitte forma: $H_\pi = P'P^+$.

Prov. Strålen som er bakprojesert frå q av P, finn ein ved å løyse $PX = q$. Denne strålen går igjennom kamerasenteret O (der PO=0). Me har også at punktet P^+q ligg på denne strålen, som går igjennom O og q, sidan $P(P^+q) = Iq = q$. Då er strålen ein samanbinding av punkta O og P^+q. Denne strålen kan skrivast som,

$$X(\lambda) = P^+q + \lambda O.$$

Me har at punktet P^+q blir avbilda til $P'P^+q$ i det andre bilete, og punktet O blir avbilda til punktet $P'O$. Linja som bind desse punkta saman kallar me l'. Ved å bruke resultat 2.3 og 6.1 kan me skrive

$$l' = (P'O) \times (P'P^+q) = \mathcal{T}_{P'O} \cdot (P'P^+q).$$

Denne linja er ei epipolarlinja, sidan punktet $P'O$ er epipolen til det andre kamerat. Då kan me skrive $P'O = e'$ og l' som,

$$l' = \mathcal{T}_{e'} \cdot (P'P^+q).$$

Me veit at punktet q' må liggje på epipolarlinja, l', og at $q'^T l' = 0$. Me får at

$$q'^T \cdot \mathcal{T}_{e'} \cdot (P'P^+q) = 0 \Rightarrow q'^T Fq = 0,$$

der $F = \mathcal{T}_{e'} \cdot P'P^+$. □

No vil me vise korleis me kan uttrykke fundamentalmatrisa gitt at me har to kameramatriser. Før me gjer dette treng me eit lemma som me skal bruke i provet eit seinare resultat. Dette resultatet nyttar me når me skal skrive F på ynskja form.

Lemma 6.5. *Viss M er ei 3×3 matrise og, x og y er kolonnevektorar, då har me at*

$$(Mx) \times (My) = M^*(x \times y), \tag{6.3}$$

der $M^* = det(M)(M^{-1})^T$. s.581, [4].

Resultat 6.6. *Me har ei matrise M som er invertibel og at $M^* = det(M)(M^{-1})^T$. For alle vektorar $\mathbf{t}$ og ei ikkje-singulær matrise M, har ein at:*

$$\mathcal{T}_{\mathbf{t}} \cdot M = M^* \cdot \mathcal{T}_{M^{-1}\mathbf{t}}.$$

Sjå s. 581-582, [4].

Prov. Brukar likning (6.3) og resultat 6.1, slik at me kan skrive

$$\begin{aligned} &\mathcal{T}_{My} \cdot Mx = M^*\mathcal{T}_y \cdot x \\ &\Rightarrow \mathcal{T}_{My} \cdot M = M^*\mathcal{T}_y. \end{aligned}$$

Viss me skriv $\mathbf{t} = My$, får me

$$\mathcal{T}_{\mathbf{t}}M = M^*\mathcal{T}_{M^{-1}\mathbf{t}}.$$

Viss M er ei ortonormal matrise er $det(M) = 1$, får me at dette er lik $(M^{-1})^T\mathcal{T}_{M^{-1}\mathbf{t}}$. □

Dette resultatet skal me no bruke for å vise resultat 6.7. I provet til dette resultatet kjem me fram til to viktige formlar. Desse formlane skal me bruke i kapittel sju.

Resultat 6.7. *Anta at me har kameramatriser gitt som* $P = K[I \mid \mathbf{0}]$*, og* $P' = K'[R \mid \mathbf{t}]$*, der den første kameramatrisa er i verdsorigo. Då har me at fundamentalmatrisa kan skrivast som*

$$F = (K'^{-1})^T R K^T \mathcal{T}_{KR^T\mathbf{t}} = (K'^{-1})^T R K^T \mathcal{T}_e.$$

Prov. Me har verdsorigo ved det første kameraet $P = K[I \mid \mathbf{0}]$, og det andre kameraet er gitt som $P' = K'[R \mid \mathbf{t}]$. Då har me at $O = \begin{pmatrix} \mathbf{0} \\ 1 \end{pmatrix}$, og ved å bruke definisjon 6.3 kan me finne P^+.

$$P^+ = P^T(PP^T)^{-1} = \begin{bmatrix} K^T \\ \mathbf{0}^T \end{bmatrix} \left(\begin{bmatrix} K & \mathbf{0} \end{bmatrix} \begin{bmatrix} K^T \\ \mathbf{0}^T \end{bmatrix} \right)^{-1}$$
$$\Rightarrow P^+ = \begin{bmatrix} K^{-1} \\ \mathbf{0}^T \end{bmatrix}.$$

Brukar likning (6.2),

$$F = \mathcal{T}_{P'O} \cdot P'P^+.$$

Me kan skrive $P'O = K'[R \mid \mathbf{t}] \begin{pmatrix} o \\ 1 \end{pmatrix} = K'\mathbf{t}$ og $P'P^+ = (K'[R \mid \mathbf{t}]) \begin{bmatrix} K^{-1} \\ \mathbf{0}^T \end{bmatrix} = K'RK^{-1}$. Dette kan me setje inn i likning (6.2),

$$F = \mathcal{T}_{K'\mathbf{t}} \cdot K'RK^{-1}.$$

Brukar resultat 6.6, og får at $\mathcal{T}_{K'\mathbf{t}} \cdot K' = (K'^{-1})^T \mathcal{T}_{K'^{-1}K'\mathbf{t}} = (K'^{-1})^T \mathcal{T}_{\mathbf{t}}$.

$$\Rightarrow F = (K'^{-1})^T \mathcal{T}_{\mathbf{t}} R K^{-1}$$

Brukar resultat 6.6 to gonger slik at me har, $\mathcal{T}_{\mathbf{t}} R = R\mathcal{T}_{R^T\mathbf{t}}$ og $\mathcal{T}_{R^T\mathbf{t}} K^{-1} = K^T \mathcal{T}_{KR^T\mathbf{t}}$.

$$\Rightarrow F = (K'^{-1})^T R \mathcal{T}_{R^T\mathbf{t}} K^{-1}$$
$$\Rightarrow F = (K'^{-1})^T R K^T \mathcal{T}_{KR^T\mathbf{t}}$$

Set alle stega saman:

$$F = \mathcal{T}_{P'O} \cdot P'P^+ = \mathcal{T}_{K'\mathbf{t}} \cdot K'RK^{-1} = (K'^{-1})^T \mathcal{T}_{\mathbf{t}} \cdot RK^{-1} = (K'^{-1})^T R \mathcal{T}_{R^T\mathbf{t}} \cdot K^{-1} = (K'^{-1})^T R K^T \mathcal{T}_{KR^T\mathbf{t}}. \tag{6.4}$$

Epipolane er $e = P \begin{pmatrix} -R^T\mathbf{t} \\ 1 \end{pmatrix} = KR^T\mathbf{t}$ og $e' = P' \begin{pmatrix} \mathbf{0} \\ 1 \end{pmatrix}$. Då kan me skrive fundamentalmatrisa som:

$$F = \mathcal{T}_{e'} \cdot K'RK^{-1} = (K'^{-1})^T \mathcal{T}_{\mathbf{t}} \cdot RK^{-1} = (K'^{-1})^T R \mathcal{T}_{R^T\mathbf{t}} \cdot K^{-1} = (K'^{-1})^T R K^T \mathcal{T}_e. \tag{6.5}$$

□

Dette resultatet og det me fann i provet blir brukt når me skal definere den essensielle matrisa i kapittel sju.

Teorem 6.8. *Fundamentalmatrisa tilfredsstillar kravet at, for alle punktkorrespondansar* $q \leftrightarrow q'$ *i dei to bilda er:* $q'^T F q = 0$.

Prov. Dette resultatet stemmer fordi dersom punkta q og q' er korresponderande par, då ligg q' på epipolarlinja $l' = Fq$ som korresponderer til punktet q. Det vil seie at $q'l' = 0 \Rightarrow q'^T Fq = 0$. Viss biletpunkta tilfredsstiller $q'^T Fq = 0$, då er strålane definert ved desse punkta, koplanare. Dette resultatet gir ein måte å karakterisere F på, utan å referere til kameramatriser, kun i termar av korresponderande biletpunkt. Minst sju korrespondansar trengs for å bestemme F (sjå eigenskapar til F iv)). □

Ved å bruke dette resultatet kan ein finne fundamentalmatrisa frå korresponderande punkt, utan å finne kameramatrisene. Me har sett at det går an å finne fundamentalmatrisa frå to kameramatriser P og P', sjå kapittel 6,2 under delen om algebraisk utleiing. Sidan fundamentalmatrisa er ei homogen matrise, sjå den neste definisjonen, er den definert opp til multiplikasjon med ein skalar.

Eigenskapar til fundamentalmatrisa

Definisjon 6.9. Anta at me har to bilete frå kamera med ikkje-samanfallande senter. Då er fundamentalmatrisa F den unike 3×3 homogene matrisa med rang 2, som tilfredsstillar:

$$q'^T Fq = 0, \tag{6.6}$$

for alle punktkorrespondansar $q \leftrightarrow q'$.

Eigenskapar til F, s. 245, [4]:
i) Transponering: Viss F er fundamentalmatrisa til kameraparet (P, P'), då er F^T fundamentalmatrisa til paret (P', P).
ii) Epipolare linjer: For punkt q i det første bilete er korresponderande epipolar linje $l' = Fq$. For det andre punktet, q', representerer $l = F^T q'$ den epipolare linja som korresponderer til q' i det andre bilete.
iii) Epipolen: For punkt q er den epipolare linja l' lik Fq, og inneheld e'. Og e' tilfredsstillar $e'^T(Fq) = (e'^T F)q = 0$ for alle q. Det følgjer at $e'^T F = 0$, d.v.s. e' er venstre nullromvektor av F. Og $Fe = 0$ er høgre nullvektor til F.
iv) F har sju fridomsgrader: ei 3×3-homogenmatrise har åtte fridomsgrader, men F må tilfredsstilla at $det(F) = 0$.
v) F er ein korrelasjon, dvs. ei projektiv avbilding som tek eit punkt til ei linje. I dette tilfellet definerer me eit punkt q i det første bilete og ei linje i det andre $l' = Fq$, som er den epipolare linja til q. Viss l og l' er korresponderande epipolare linjer, er alle punkt q på l avbilda på same linje l'. Dette betyr at det ikkje fins ei invers avbilding, og F er ikkje av full rang. På grunn av dette er F ikkje ein ordentleg korrelasjon.

Epipolar linjehomografi

Mengda av alle epipolare linjer i kvart bilete dannar ein pensel av linjer, som går gjennom epipolen. Ein slik pensel av linjer kan sjåast på som eit eitdimensjonalt projektivt rom. Me veit at korresponderande epipolare linjer er relatert til kvarandre. Då fins det ein homografi mellom penselen av epipolare linjer sentrert i e i det første bilete, og penselen sentrert i e' i det andre. Ein homografi mellom to slike eindimensjonale projektive rom har tre fridomsgrader.
Me kan telje fridomsgradene til F som: to for e, to for e' og tre for epipolarlinjehomografien som avbildar linjer gjennom e, til linjer gjennom e'.

Resultat 6.10. *Anta at l og l' er korresponderande epipolare linjer, og k er ei linje som ikkje går gjennom e. Då er l og l' relatert ved: $l' = F\mathcal{T}_k l$. Symmetrisk: $l = F\mathcal{T}_{k'} l'$ alt. $l' = F\mathcal{T}_e l$, $l = F^T \mathcal{T}_{e'} l'$.*

Prov. Uttrykket $\mathcal{T}_k \cdot l = k \times l$, er skjeringspunktet til to linjer k og l og er derfor eit punkt på den epipolare linja, som me kallar x. Derfor er $F\mathcal{T}_k \cdot l = Fx$ den epipolare linja som korresponderer til punktet x, altså linja l'. □

6.3 Korleis kan ein finne kameramatrisene?

Ein av eigenskapane til F er at matrisa kan brukast til å bestemme kameramatrisene, opp til ein multiplikasjon med ein felles projektiv transformasjon til dei to bileta, dette skal me no vise.
Både avbildinga $l' = Fq$ og korresponderande vilkår $q'^T Fq = 0$ er projektive relasjonar. Utleiinga involverte kun projektive geometriske forhold, slik som skjering av linjer og plan. Derfor er relasjonane kun avhengig av projetive koordinatar i bilete, og ikkje t.d. euklidske målingar.
Med andre ord er forholda i bilete projektivt uendra. Under ein projektiv transformasjon av biletkoordinatar $\hat{q} = Hq$ og $\hat{q}' = H'q'$, fins det ein korresponderande avbilding $\hat{l}' = \hat{F}\hat{q}$ med $\hat{F} = H'^{-T} F H^{-1}$. Matrisa $\hat{F}$ er den korresponderande rang 2 fundamentalmatrisa til matrisa F. Liknande, er F kun avhengig av projektive eigenskapar til dei to kamera P og P'. Kameramatrisa relaterar 3-rom målingar til biletmålingar, og er avhengig av både biletkoordinatramma og val av verdskoordinatramma. F er ikkje avhengig av verdsrammeval, og er uendra av ein projektiv transformasjon.

Resultat 6.11. *Viss H er ei 4×4-matrise som representerer ein projektiv transformasjon i 3-rom, då har ein at fundamentalmatrisene som korresponderer til kameramatriseparet (P, P') og $(PH, P'H)$ er like.*

Prov. Viss $x \leftrightarrow x'$ er korresponderande punkt med respekt på kameramatriseparet (P, P'), og eit 3D-punkt X. Då er dei også korresponderandepunkt til kameramatriseparet $(PH, P'H)$, som svarar til punktet $H^{-1}X$, sidan me har at $PX = (PH)(H^{-1}X)$ og $P'X = (P'H)(H^{-1}X)$. □

Frå kapittel 6.2, under avsnittet om algebraisk utleiing, såg me at me kunne finne ei unik fundamentalmatrise frå eit kameramatrisepar (P, P'). Men frå resultatet over har me at fundamentalmatrisa bestemmer kameramatrisepara, opp til ein høgremultiplikasjon av ein 3D projektiv transformasjon. Dette skal me vise i provet for teorem 6.14, i slutten av dette kapittelet.

Kanonisk form av kameramatriser

Det er vanleg å definere ein spesifikk kanonisk form for kameramatriseparet korresponderande til ei gitt fundamentalmatrise, der den første matrisa er på den enkle forma $[I \mid 0]$. For å sjå at dette alltid er mogleg, la P vere utvida av ei rad for å gi ei 4×4 ikkje-singulær matrise, P^*. La $H = P^{*-1}$, då ser ein at $PH = [I \mid 0]$ som ynskja.

Resultat 6.12. *Fundamentalmatrisa korresponderande til kameramatriseparet $P = [I \mid 0]$ og $P' = [M \mid m]$ er lik $\mathcal{T}_m \cdot M$, s. 254, [4].*

Dette resultatet er eit spesialtilfelle av resultat 6.7, og provet som ein finn i avsnittet om algebraisk utleiing av fundamentalmatrisa.
Me vil no gi eit lemma som me skal bruke i provet for det neste teoremet.

Lemma 6.13. *Anta at rang 2 matrisa F, kan bli dekomponert på to ulike måtar: $F = \mathcal{T}_a A$ og $F = \mathcal{T}_{\tilde{a}} \tilde{A}$, då er $\tilde{a} = ka$ og $\tilde{A} = k^{-1}(A + av^T)$ for nokre konstantar k og 3-vektor v.*

Prov. Me ser at $a^T F = a^T \mathcal{T}_a A = 0$, og at $\tilde{a}^T F = 0$. Sidan F har rang to, følgjer det at $\tilde{a} = ka$. Frå $\mathcal{T}_a A = \mathcal{T}_{\tilde{a}} \tilde{A} \Rightarrow \mathcal{T}_a(k\tilde{A} - A) = 0$ slik at $k\tilde{A} - A = av^T$ for nokre v. Derfor har me at $\tilde{A} = k^{-1}(A + av^T)$. □

Teorem 6.14. *La F vere ei fundamentalmatrise og la (P, P') og $(\tilde{P}, \tilde{P}')$ vere to kameramatrisepar slik at F er fundamentalmatrisa, som korresponderer til kvart par. Då eksisterer det ei ikkje-singulær 4×4-matrise H, slik at $\tilde{P} = PH$ og $\tilde{P}' = P'H$.*

Prov. Anta at ei gitt fundamentalmatrise F svarar til to ulike kameramatrisepar (P, P') og $(\tilde{P}, \tilde{P}')$. Me kan forenkle problemet med å anta at to av kameramatrisene er på kanonisk form $\tilde{P} = P = [I \mid 0]$. Dette kan ein gjere ved å gjere ein projektiv transfomasjon på matrisene. Anta no at $P = \tilde{P} = [I \mid 0]$ og at $P' = [A \mid a]$ og $\tilde{P}' = [\tilde{A} \mid \tilde{a}]$. Frå resultat 6.12 kan fundamentalmatrisa skrivast som $F = \mathcal{T}_a A = \mathcal{T}_{\tilde{a}} \tilde{A}$. Brukar lemma 6.13 og får at $\tilde{P}' = [k^{-1}(A + av^T) \mid ka]$, viss kameramatrisene skal gi same F. Må vise at matrisene er relatert til kvarandre projektivt. Me let H vere matrisa $H = \begin{bmatrix} k^{-1}I & 0 \\ k^{-1}v^T & k \end{bmatrix}$. Me har då at $PH = k^{-1}[I \mid 0] = k^{-1}\tilde{P}$, og

$$P'H = [A \mid a]H = [k^{-1}(A + v^t) \mid ka] = [\tilde{A} \mid \tilde{a}] = \tilde{P},$$

då er para P, P' og $\tilde{P}, \tilde{P}'$ projektivt relaterte til kvarandre. □

Dette teoremet seier at ei gitt fundamentalmatrise bestemmer kameramatrisene, opp til ein høgremultiplikasjon med ein projektiv transformasjon. Me kan derfor ikkje finne ei eintydig fundamentalmatrise. Sidan kameramatrisepar som skil seg frå kvarandre me ein projektiv transformasjon gir den same fundamentalmatrisa. Derfor fangar fundamentalmatrisa det projektive forholdet mellom to kamera.

Kapittel 7

Den essensielle matrisa

I dette kapittelet skal me sjå på spesialiseringa av fundamentalmatrisa til tilfellet med normaliserte biletkoordinatar. Når me har at biletkoordinatane er normaliserte får me den essensielle matrisa. Me skal vise fleire av eigenskapane til denne matrisa. Og lage ein metode som gir oss om ei matrise er essensiell, her må me nytte Macaulay2-programmet. Me skal også lage ein metode for å dekomponere den essensielle matrisa til ei ortonormal matrise R, og ei antisymmetrisk matrise $\mathcal{T}_a$. Deretter vil me lage ein metode som tek korresponderande bildepunkt og finn ut om me har ei endeleg løysing.
I denne delen tek me utgangspunkt i "Tutorial 72: Photogrammetry", s. 247-251 [5]. For å løyse nokre av problema må me nytte gröbnerbasar og eliminasjonsordningar, som blei introdusert i kapittel fire.
Me byrjar med å forklare kva ei essensiell matrise er, med å ta utgangspunkt i fundamentalmatrisa.

Normaliserte koordinatar

Me ser på ei kameramatrise som blir dekomponert som $P = K[R \mid \mathbf{t}]$. Lat $q = PX$ vere eit punkt i bilete. Viss kalibreringsmatrisa K er kjend, kan me bruke den inverse og punktet q, og få punktet $\hat{q} = K^{-1}q$. Då er $\hat{q} = [R \mid \mathbf{t}]X$, der $\hat{q}$ er biletpunktet uttrykt i normaliserte koordinatar. Ein kan då tenkje seg at biletpunktet X, med respekt på kamera $[R \mid \mathbf{t}]$, har identitetsmatrisa som kalibreringsmatrise. Kameramatrisa $K^{-1}P = [R \mid \mathbf{t}]$ blir kalla ei normalisert kameramatrise, der verknaden av kalibreringsmatrisa er fjerna.

Definisjon 7.1. Den definerande likninga for den essensielle matrisa er:

$$\hat{q}'^T \mathcal{E} \hat{q} = 0, \tag{7.1}$$

i termar av normaliserte biletkoordinatar for korresponderande punkt $q \leftrightarrow q'$.

Ved å substituera $\hat{q}$ og $\hat{q}'^T$ med q og q'^T, får me likninga $q'^T K'^{-T} \mathcal{E} K^{-1} q = 0$. Og ved å samanlikne dette med teorem 6.8, ser me at forholdet mellom den essensielle matrisa og fundamentalmatrisa er:

$$\mathcal{E} = K'^T F K \tag{7.2}$$

Frå førre kapittel, er fundamentalmatrisa ei homogen matrise som er eintydig bestemt opp til multiplikasjon med ein skalar. Derfor er også den essensielle matrisa eintydig bestemt opp til ein skalar. Me veit også at fundamentalmatrisa kan brukast til å bestemme eit kamerapar opp til ein høgremultiplikasjon med ein projektiv transformasjon.

I dette kapittelet skal me nytte den antisymmetriske matrisa som me skriv på ein litt anna form enn i førre kapittel. Gitt vektoren $a = (a_1, a_2, a_3)$ i $\mathbb{R}^3$, definerer me den assosierte antisymmetriske matrisa som

$$\mathcal{T}_a = \begin{pmatrix} 0 & a_3 & -a_2 \\ -a_3 & 0 & a_1 \\ a_2 & -a_1 & 0 \end{pmatrix}. \tag{7.3}$$

Me skal no sjå på eit par med normaliserte kameramatriser, $P = [I \mid 0]$ og $P' = [R \mid \mathbf{t}]$. Fundamentalmatrisa som korresponderer til paret av normaliserte kamera blir kalla den essensielle matrisa, og er på forma

$$\mathcal{E} = \mathcal{T}_t R = R\mathcal{T}_{R^T t}.$$

Dette formulerer me som eit teorem, og brukar det me fann i kapittel 6,2 under algebraisk derivasjon av fundamentalmatrisa for å vise dette.

Teorem 7.2. *La $\mathcal{E} = R\mathcal{T}_a$ vere ei essensiell matrise, og la $b = Ra$. Då har me at $\mathcal{E} = \mathcal{T}_b R$.*

Prov. Me har $P = [I \mid 0]$ og $P' = [R \mid b]$. Sentrumet til det eine kamerat er $O = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Då finn me at

$$P^+ = [I \mid 0]^T, P'O = b, P'P^+ = [R \mid b] \cdot [I \mid 0] = R,$$

på same måte som i provet for resultat 6.7. Me kan skrive matrisa $\mathcal{E}$ som

$$\begin{aligned} \mathcal{E} &= \mathcal{T}_{P'O} \cdot P'P^+ \\ \Rightarrow \mathcal{E} &= \mathcal{T}_b \cdot R. \end{aligned}$$

Ved å bruke resultat 6.6, kan me skrive dette som

$$\Rightarrow \mathcal{E} = \mathcal{T}_b \cdot R = R \cdot \mathcal{T}_{R^T b}.$$

Me skriv $a = R^T b \Rightarrow b = Ra$. □

Me vil no vise fleire eigenskapar ved den essensielle matrisa.

Setning 7.3. La $\mathcal{E} \in Mat_3(\mathbb{R})$ vere ei essensiell matrise. Me let $U, V \in Mat_3(\mathbb{R})$ vere ortonormale matriser, og $\lambda \in \mathbb{R}$. Då er $\lambda\mathcal{E}$, $U\mathcal{E}V$ og $\mathcal{E}^T$ essensielle matriser.

Prov. Me har at for ei ortonormal matrise, er vektorane ortogonale og har einingslengd. Me deler provet i tre deler.
i) $\lambda\mathcal{E}$ er ei essensiell matrise.
Me veit at $\mathcal{E}$ er ei essensiell matrise, og kan derfor skrive $\mathcal{E} = R\mathcal{T}_a$.

$$\lambda\mathcal{E} = \lambda R\mathcal{T}_a = R\mathcal{T}_{\lambda a} = R\mathcal{T}_d,$$

der $d = \lambda a$. Matrisa $\mathcal{T}_d$ er ei antisymmetrisk matrise.
ii) $U\mathcal{E}V$ er ei essensiell matrise.
Me brukar lemma 7.2 slik at me kan skrive:

$$\begin{aligned} U\mathcal{E}V &= U(R\mathcal{T}_a)V = UR(\mathcal{T}_a V) = URV\mathcal{T}_c \\ &\Rightarrow U\mathcal{E}V = R'\mathcal{T}_c \end{aligned}$$

der $a = cV$. Me kan skrive $URV = R'$ som er ei ortonormal matrise sidan U, R og V er ortonormale.
Me ser at dette er ei essensiell matrise sidan den kan skrivast som ei ortonormal matrise og ei

antisymmetrisk matrise.
iii) $\mathcal{E}^T$ er ei essensiell matrise.

$$\mathcal{E}^T = (R\mathcal{T}_a)^T = (\mathcal{T}_a)^T R^T = -\mathcal{T}_a R^T = \mathcal{T}_{-a} R^T = R^T \mathcal{T}_c,$$

der $-a = R^T c$. Me brukar

$$\mathcal{T}_a^T = \begin{pmatrix} 0 & -a_3 & a_2 \\ a_3 & 0 & -a_1 \\ -a_2 & a_1 & 0 \end{pmatrix} = -\mathcal{T}_a = \mathcal{T}_{-a}.$$

Sidan R er ei ortonormal matrise, er R^T ei ortonormal matrise. □

Denne setninga får me brukt for i nokre prov, i det neste delkapittelet.

7.1 Den karakteristiske likninga

I denne delen skal me komme fram til ulike eigenskapar til den essensielle matrisa. For å studere den essensielle matrisa nærare brukar me at den essensielle matrisa oppfyller den karakteristiske likninga. Den karakteristiske likninga er gitt ved $\mathcal{E}\mathcal{E}^T\mathcal{E} = 1/2 \cdot Spor(\mathcal{E}\mathcal{E}^T)\mathcal{E}$. Me skal vise at dette stemmer i det første resultatet. Dette resultatet og lammaet om ei matrise som oppfyller den karakteristiske likninga har determinant null, skal me bruke når me skal finne ut om ei matrise, er ei essensiell matrise. Me vil også komme fram til at ei essensiell matrise har rang to.

Resultat 7.4. *For ei essensiell matrise $\mathcal{E} \in Mat_3(\mathbb{R})$, er den karakteristiske likninga:*

$$\mathcal{E}\mathcal{E}^T\mathcal{E} = 1/2 \cdot Spor(\mathcal{E}\mathcal{E}^T)\mathcal{E} \tag{7.4}$$

oppfylt.

Prov. Me har at ei essensiell matrise kan skrivast $\mathcal{E} = \mathcal{T}_b R$, og set dette inn i den karakteristiske likninga.
Sidan R er ei ortonormal matrise, har me at $RR^T = R^T R = I$. Den antisymmetriske matrisa er gitt i (7.3). Og sporet til ei matrise A er summen $a_{11} + a_{22} + \ldots + a_{nn}$.

Set $\mathcal{E} = \mathcal{T}_b R$ inn i venstresida av den karakteristiske likninga:
$\mathcal{E}\mathcal{E}^T\mathcal{E} = (\mathcal{T}_b R)(\mathcal{T}_b R)^T(\mathcal{T}_b R) = \mathcal{T}_a \mathcal{T}_a^T(\mathcal{T}_a R)$.

Og gjer det same på høgresida av den karakteristiske likninga:
$1/2 \cdot Spor(\mathcal{E}\mathcal{E}^T) \cdot \mathcal{E} = 1/2 \cdot Spor(\mathcal{T}_b R)(\mathcal{T}_b R)^T \cdot (\mathcal{T}_b R)$.

Me får då at den karakteristiske likninga kan skrivast:

$$\begin{aligned} &\Rightarrow \mathcal{T}_a \mathcal{T}_a^T(\mathcal{T}_a R) = 1/2 \cdot Spor(\mathcal{T}_b R)(\mathcal{T}_b R)^T \cdot (\mathcal{T}_b R) \\ &\Rightarrow \mathcal{T}_b \mathcal{T}_b^T \mathcal{T}_b = 1/2 \cdot Spor(\mathcal{T}_b \mathcal{T}_b^T) \cdot \mathcal{T}_b. \end{aligned}$$

Det er nok å vise at denne likninga er oppfylt. Denne likninga kan løysast ved å bruke matrise-multiplikasjon og likninga til den antisymmetriske matrisa (7.3):

$$\mathcal{T}_b \mathcal{T}_b^T = \begin{pmatrix} 0 & b_3 & -b_2 \\ -b_3 & 0 & b_1 \\ b_2 & -b_1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -b_3 & b_2 \\ b_3 & 0 & -b_1 \\ -b_2 & -b_1 & 0 \end{pmatrix} = \begin{pmatrix} b_3b_3 + b_2b_2 & -b_1b_2 & -b_1b_3 \\ -b_1b_2 & b_3b_3 + b_1b_1 & -b_2b_3 \\ -b_1b_3 & -b_2b_3 & b_2b_2 + b_1b_1 \end{pmatrix}.$$

$$
\begin{aligned}
(\mathcal{T}_b\mathcal{T}_b^T)\mathcal{T}_b &= \begin{pmatrix} 0 & b_3 & -b_2 \\ -b_3 & 0 & b_1 \\ b_2 & -b_1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & -b_3 & b_2 \\ b_3 & 0 & -b_1 \\ -b_2 & -b_1 & 0 \end{pmatrix} \begin{pmatrix} 0 & b_3 & -b_2 \\ -b_3 & 0 & b_1 \\ b_2 & -b_1 & 0 \end{pmatrix} \\
&= \begin{pmatrix} 0 & b_3b_2b_2 + b_3b_3b_3 + b_1b_1b_3 & -b_2b_2b_2 - b_2b_3b_3 - b_1b_1b_2 \\ -b_3b_1b_1 - b_3b_3b_3 - b_2b_2b_3 & 0 & b_1b_3b_3 + b_1b_1b_1 - b_1b_2b_2 \\ b_2b_2b_3 + b_2b_1b_1 + b_2b_2b_2 & -b_1b_3b_3 - b_1b_1b_1 - b_1b_2b_2 & 0 \end{pmatrix} \\
&= \langle b, b\rangle \cdot \mathcal{T}_b = 1/2 \cdot Spor(\mathcal{T}_b\mathcal{T}_b^T) \cdot \mathcal{T}_b.
\end{aligned}
$$

Me har vist at for ei essensiell matrise, er den karakteristiske likninga oppfylt. □

Lemma 7.5. *Alle matriser $\mathcal{E} \in Mat_3(\mathbb{R})$ som tilfredsstillar den karakteristiske likninga, har determinant null.*

Prov. Me har at $\mathcal{E}$ tilfredsstillar den karakteristiske likninga

$$\mathcal{E}\mathcal{E}^T\mathcal{E} = 1/2 \cdot Spor(\mathcal{E}\mathcal{E}^T)\mathcal{E}.$$

Me kallar $1/2 \cdot Spor(\mathcal{E}\mathcal{E}^T) = \lambda$. Då kan me skrive uttrykket (7.4) som:

$$\mathcal{E}\mathcal{E}^T\mathcal{E} = \lambda\mathcal{E}.$$

Me vil finne determinanten:

$$
\begin{aligned}
&det(\mathcal{E}\mathcal{E}^T\mathcal{E}) = det(\lambda\mathcal{E}) = det(I\lambda)det(\mathcal{E}) = \lambda^3 det(\mathcal{E}) \\
&\Rightarrow det(\mathcal{E})det(\mathcal{E}^T)det(\mathcal{E}) = \lambda^3 det(\mathcal{E}).
\end{aligned}
$$

Me antek at: $det(\mathcal{E}) \neq 0$, og vil vise at denne antakinga ikkje stemmer.

$$
\begin{aligned}
&det(\mathcal{E})det(\mathcal{E}^T)det(\mathcal{E}) = \lambda^3 det(\mathcal{E}) \\
&\Rightarrow det(\mathcal{E}^T)det(\mathcal{E}) = \lambda^3 \\
&\Rightarrow (det\mathcal{E})^2 = [1/2 \cdot Spor(\mathcal{E}^T\mathcal{E})]^3 \\
&\Rightarrow 8 \cdot (det\mathcal{E})^2 = [Spor(\mathcal{E}^T\mathcal{E})]^3.
\end{aligned}
$$

Me kan skrive $S = \mathcal{E}^T\mathcal{E}$ som er ei symmetrisk matrise, og $S \in Mat_{3\times 3}(\mathbb{R})$. Då kan me skrive:

$$U^TSU = D \Leftrightarrow S = UDU^T.$$

Mellomrekning:
Skriver $\mathcal{E} = U^TDV$ og får:

$$S = \mathcal{E}\mathcal{E}^T = U^TDV(U^TDV)^T = U^TDVV^TD^TU = U^TDD^TU,$$

der $DD^T = D'$, som også er ei diagonalmatrise.
Dersom me skriver $D = \begin{pmatrix} a' & 0 & 0 \\ 0 & b' & 0 \\ 0 & 0 & c' \end{pmatrix}$, då er $D' = \begin{pmatrix} a'^2 & 0 & 0 \\ 0 & b'^2 & 0 \\ 0 & 0 & c'^2 \end{pmatrix} \Rightarrow a', b', c' \geq 0.$
Me kallar om elementa i D', og skriv $D' = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix}$.

Dette set me inn i likninga, og får:

$$\begin{aligned}
&8 \cdot det(S) = [Spor(S)]^3 \\
\Rightarrow &8 \cdot (U^T D' U) = [Spor(U^T D' U)]^3 \\
\Rightarrow &8 \cdot det(D') = [Spor(D')]^3 \\
\Rightarrow &8abc = (a+b+c)^3 = a^3 + b^3 + c^3 + 3ab^2 + 3a^2b + 3a^2c + 3ac^2 + 3b^2c + 3bc^2 + 6abc \\
\Rightarrow &2abc = a^3 + b^3 + c^3 + 3ab^2 + 3a^2b + 3a^2c + 3ac^2 + 3b^2c + 3bc^2
\end{aligned}$$

Vel ordninga: $0 \leq a \leq b \leq c$, då er $abc \leq bc^2$, og ser at viss:

$$\begin{aligned}
2abc &= 3bc^2 \\
\Rightarrow bc^2 &= 0.
\end{aligned}$$

Me ser at me må ha $b = 0$ eller $c = 0$. Sidan me har at $0 \leq a \leq b \leq c$, må også $a = 0$. Dette gir at:

$$0 = c^3,$$

og c må også vere null. Matrisa D er nullmatrisa. Det gjer at:

$$det(\mathcal{E}\mathcal{E}^T) \neq [1/2 \cdot Spor(\mathcal{E}\mathcal{E}^T)]^3.$$

Då er antakelsen at $det(\mathcal{E}) \neq 0$ feil, sidan

$$det(\mathcal{E}\mathcal{E}^T\mathcal{E}) = det(1/2 \cdot Spor(\mathcal{E}\mathcal{E}^T)\mathcal{E}).$$

Då må $det(\mathcal{E}) = 0$. □

I provet for det neste lemmaet brukar me den karakteristiske likninga.

Lemma 7.6. *La $\mathcal{E}$ vere ei 3×3 matrise av rang 2, som har reelle eller komplekse komponentar og rekkjevektorar z_1, z_2, z_3. Viss $\mathcal{E}$ tilfredsstillar den karakteristiske likninga, då eksisterer det ein indeks $i \in \{1, 2, 3\}$ slik at $\langle z_i, z_i \rangle \neq 0$.*

Prov. Me kan skrive $\mathcal{E} = \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix}$, og me har at $\mathcal{E}\mathcal{E}^T\mathcal{E}$ er lik $1/2 \cdot Spor(\mathcal{E}\mathcal{E}^T)\mathcal{E}$. Me ser først på *sporet* til $\mathcal{E}\mathcal{E}^T$.

$$\mathcal{E}\mathcal{E}^T = \begin{bmatrix} z_1 \\ z_2 \\ z_3 \end{bmatrix} \begin{bmatrix} z_1 & z_2 & z_3 \end{bmatrix} = \begin{bmatrix} \langle z_1, z_1 \rangle & \langle z_1, z_2 \rangle & \langle z_1, z_3 \rangle \\ \langle z_2, z_1 \rangle & \langle z_2, z_2 \rangle & \langle z_2, z_3 \rangle \\ \langle z_3, z_1 \rangle & \langle z_3, z_2 \rangle & \langle z_3, z_3 \rangle \end{bmatrix}$$

Me antek at alle $\langle z_i, z_i \rangle = 0$ for $i = \{1, 2, 3\}$, då blir $Spor(\mathcal{E}\mathcal{E}^T) = 0$. og me får

$$\mathcal{E}\mathcal{E}^T\mathcal{E} = 0.$$

Me skriv $S = \mathcal{E}\mathcal{E}^T$ og $\mathcal{E} = \begin{bmatrix} c_1^T & c_2^T & c_3^T \end{bmatrix}$. Då blir likninga

$$S\mathcal{E} = 0,$$

slik at: $Sc_1^T = 0$, $Sc_2^T = 0$ og $Sc_3^T = 0$. Rangen til S må då vere 1 (eller 0). Me har at:

$$det \begin{bmatrix} \langle z_1, z_1 \rangle & \langle z_1, z_2 \rangle \\ \langle z_2, z_1 \rangle & \langle z_2, z_2 \rangle \end{bmatrix} = 0,$$

frå antakinga, har me då at

$$\Rightarrow \langle z_1, z_2 \rangle = 0.$$

Me må også ha at:

$$det \begin{bmatrix} \langle z_2, z_2 \rangle & \langle z_2, z_3 \rangle \\ \langle z_3, z_2 \rangle & \langle z_3, z_3 \rangle \end{bmatrix} = 0$$

og

$$det \begin{bmatrix} \langle z_1, z_1 \rangle & \langle z_1, z_3 \rangle \\ \langle z_3, z_1 \rangle & \langle z_3, z_3 \rangle \end{bmatrix} = 0.$$

Då må både $\langle z_1, z_3 \rangle$ og $\langle z_2, z_3 \rangle$ vere lik null.
Me får då at:

$$\mathcal{E}\mathcal{E}^T = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Dette er ikkje mogleg når rangen til $\mathcal{E}$ er to. Då må antakinga om at $\langle z_i, z_i \rangle = 0$ vere feil og at $\langle z_i, z_i \rangle \neq 0$ for ein indeks $i \in \{1, 2, 3\}$. □

For ei matrise med rang to, er tal på singulære verdiar som er ulik null også lik to. Me har derfor dette resultatet.

Resultat 7.7. *Ei 3×3-matrise er ei essensiell matrise viss og berre viss to av dei singulære verdiane er like, og den tredje er null. s.257, [4].*

Lemma 7.8. *For ei matrise $\mathcal{E} \in Mat_3(\mathbb{R})$ er følgjande vilkår ekvivalente:*

1) Matrisa $\mathcal{E}$ er ei essensiell matrise

2) Me har at $rk(\mathcal{E}) = 2$, og $\mathcal{E}$ tilfredsstillar den karakteristiske likninga.

Prov. Viser først 1) $\rightarrow$ 2).
Ei essensiell matrise kan skrivast som $\mathcal{E} = R\mathcal{T}_a$ og rangen til $\mathcal{E}$ er lik rangen til $\mathcal{T}_a$.

$$\mathcal{T}_a = \begin{pmatrix} 0 & a_3 & -a_2 \\ -a_3 & 0 & a_1 \\ a_2 & -a_1 & 0 \end{pmatrix}$$

Me kan finne determinanten til denne matrisa. Viss determinanten er null, må matrisa har rang 2 eller mindre.

$$\begin{aligned} det(\mathcal{T}_a) &= 0 \cdot \begin{bmatrix} 0 & a_1 \\ -a_1 & 0 \end{bmatrix} + a_3 \cdot \begin{bmatrix} a_1 & -a_3 \\ 0 & a_2 \end{bmatrix} + (-a_2) \cdot \begin{bmatrix} -a_3 & 0 \\ a_2 & -a_1 \end{bmatrix} \\ &= 0 + a_3 a_1 a_2 - a_2 a_3 a_1 = 0. \end{aligned}$$

Me veit då at matrisa har rang to eller mindre. No antek me at matrisa har rang ein, og vise at dette ikkje kan stemme.
Dersom matrisa har rang ein, er determinanten til 2×2-minorane lik null. Me ser på 2×2-matrisa øverst til venstre, til $\mathcal{T}_a$.

$$det\Big(\begin{bmatrix} 0 & a_3 \\ -a_3 & 0 \end{bmatrix} \Big) = a_3^2.$$

For at denne determinanten skal vere null må a_3 vere null. Vidare ser me på determinanten 2×2-minoren nederst til høgre av matrisa, og får

$$det\Big(\begin{bmatrix} 0 & a_1 \\ -a_1 & 0 \end{bmatrix} \Big) = a_1^2.$$

Me ser på determinanten til minoren laga avl hjørneelementa til den antisymmetriske matrisa,

$$det\Big(\begin{bmatrix} 0 & -a_2 \\ a_2 & 0 \end{bmatrix}\Big) = a_2^2.$$

Me får dermed at når den antisymmetriske matrisa har rang ein, er $a_1, a_2, a_3 = 0$ og $\mathcal{T}_a = \mathbf{0}$. Matrisa $\mathcal{T}_a$ må derfor har rang to. Resten av provet er gitt i lemma 7.4, som viser at ei essensiell matrise oppfyller den karakteristiske likninga.

Vil vise 2) $\rightarrow$ 1).
Me har då at $rk(\mathcal{E}) = 2$, og at den karakteristiske likninga er oppfylt. Me kan gange den essensielle matrisa med ein vektor som me har valt, slik at

$$\mathbf{x} \cdot \mathcal{E} = 0.$$

Me kan skrive $\mathcal{E} = U^T \mathcal{E}' V$, som oppfyller den karakteristiske likninga der U og V er ortonormale. Finn U slik at $\mathbf{x} = (0,0,1)U$, då er $(0,0,1)\mathcal{E}' = 0$. Då har ein at den siste rekkja til $\mathcal{E}'$ er null, og ein kan skrive:

$$U^T \mathcal{E}' = \begin{bmatrix} z_1 \\ z_2 \\ 0 \end{bmatrix}$$

$$U^T \mathcal{E}' V = \begin{bmatrix} z_1 \cdot V \\ z_2 \cdot V \\ 0 \end{bmatrix}$$

Frå n) har me at $\langle z_2, z_2 \rangle$ er ulik null, og ved å velje passande V får ein at den midterste rekka er $(0, \lambda, 0)$. Denne λ må vere ulik null, fordi $\mathcal{E}'$ har rang to. Då blir matrisa,

$$\mathcal{E}' = \begin{bmatrix} z_{11} & z_{12} & z_{13} \\ 0 & \lambda & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Me kan gange vektoren $(0, \lambda, 0)$ med ein konstant slik at me får $z_2 = (0,1,0)$. No vil me finne eit uttrykk for vektoren z_1. Matrisa $\mathcal{E}'$ må oppfylle den karakteristiske likninga,

$$\begin{aligned} \mathcal{E}'\mathcal{E}'^T\mathcal{E}' &= \begin{bmatrix} z_{11} & z_{12} & z_{13} \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} z_{11} & 0 & 0 \\ z_{12} & 1 & 0 \\ z_{13} & 0 & 0 \end{bmatrix} \begin{bmatrix} z_{11} & z_{12} & z_{13} \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \\ &= \begin{bmatrix} z_{11}\langle z_1, z_1 \rangle & z_{12}\langle z_1, z_1 \rangle + z_{12} & z_{13}\langle z_1, z_1 \rangle \\ z_{11}z_{12} & z_{12}z_{12} + 1 & z_{13}z_{12} \\ 0 & 0 & 0 \end{bmatrix}. \end{aligned}$$

Sporet til $(\mathcal{E}'\mathcal{E}'^T)$ er $\langle z_1, z_1 \rangle + 1$, og

$$1/2 \cdot Spor(\mathcal{E}'\mathcal{E}'^T)\mathcal{E}' = 1/2 \cdot \begin{bmatrix} z_{11}\langle z_1, z_1 \rangle + z_{11} & z_{12}\langle z_1, z_1 \rangle + z_{12} & z_{13}\langle z_1, z_1 \rangle + z_{13} \\ 0 & \langle z_1, z_1 \rangle + 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Dersom me ser på elementa i posisjon $(2,1)$ og $(2,3)$ ser me at:

$$z_{11}z_{12} = 0$$
$$z_{13}z_{12} = 0.$$

Då må z_{12} vere null, eller så må z_{11} og z_{13} vere lik null.
Me ser på posisjon $(1,2)$, og får

$$z_{12}\langle z_1, z_1\rangle + z_{12} = 1/2 \cdot (z_{12}\langle z_1, z_1\rangle + z_{12}) \Rightarrow 1/2 \cdot (z_{12}\langle z_1, z_1\rangle + z_{12}) = 0.$$

Dette stemmer viss z_{12} er lik null. Og dersom z_{11} og z_{13} er lik null, får me at z_{12} er null. Me har derfor,

$$z_{12} = 0.$$

Me ser på elementa i posisjon $(2,2)$ i matrisene:

$$\begin{aligned} &z_{12}z_{12} + 1 = 1/2 \cdot \langle z_1, z_1\rangle + 1/2 \\ &\Rightarrow z_{12}z_{12} + 1/2 = 1/2 \cdot \langle z_1, z_1\rangle = 1/2 \cdot z_{11}z_{11} + 1/2 \cdot z_{12}z_{12} + 1/2 \cdot z_{13}z_{13} \\ &\Rightarrow 1/2 \cdot z_{12}z_{12} + 1/2 = 1/2 \cdot z_{11}z_{11} + 1/2 \cdot z_{13}z_{13} \end{aligned}$$

Når $z_{12} = 0$, får me:

$$\Rightarrow z_{11}z_{11} + z_{13}z_{13} = 1,$$

som representerer ein sirkel med radius 1.
Me kan rotera systemet slik at me får at $z_{13} = 0$. Då må $z_{11} = \pm 1$. Me har då at $\pm z_1 = \pm(1,0,0)$. Den essensielle matrisa $\mathcal{E}'$ er,

$$\mathcal{E}' = \begin{bmatrix} \pm 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Denne matrisa kan me dekomponere til ei ortonormal matrise og ei antisymmetrisk matrise, $\mathcal{E}' = R \cdot \mathcal{T}$. Der den ortonormale matrisa er

$$R = \begin{bmatrix} 0 & \pm 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & \mp 1 \end{bmatrix},$$

og den antisymmetriske matrisa er

$$\mathcal{T} = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Me kan skrive

$$\mathcal{E}' = \begin{bmatrix} \pm z_1 \\ z_2 \\ 0 \end{bmatrix}.$$

Sidan denne matrisa har rang to, oppfyller den karakteristiske likninga, og kan dekomponerast til ei ortonormal matrise og ei antisymmetrisk matrise er dette ei essensiell matrise. Og frå setning 7.3, er også $\mathcal{E}$ ei essensiell matrise. □

Eigenskapane til den essensielle matrisa som me har funne i denne delen, får me brukt for i resten av dette kapittelet. Desse eigenskapane gjer at me kan finne ut om ei matrise er ei essensiell matrise.

7.2 Metode for dekomponering av ei essensiell matrise

I denne delen vil det først bli gitt ein metode for korleis ein kan finne ut om ei matrise er ei essensiell matrise. Deretter vil det bli gitt eit døme på korleis ein kan bruke metoden. Til slutt i denne delen, blir det gitt ein metode for korleis ein kan dekomponera ei essensiell matrise. Ved å gi eit eksempel på ei essensiell matrise som blir dekomponert kjem me fram til at dekomposisjonen gir fleire løysingar. Og det blir drøfta kvifor dette skjer.
Me må bruke resultata og teorema i den førre delen for å lage metodar. I den første metoden `IsEssential(...)`, brukar me at ei essensiell matrise oppfyller den karakteristiske likninga, og at den har rang to. Me brukar Macaulay2-programmet for å skrive metoden og sjekke om ei matrise er essensiell.

Metode 1. La $\mathcal{E} \in Mat_3(\mathbb{Q})$. Skriv ein Macaulay-funksjon `IsEssential(...)` som tek $\mathcal{E}$, brukar lemma 7.8 for å sjekke at $\mathcal{E}$ er ei essensiell matrise, og returnerer korresponderande Booliske verdi(sant eller usant).

```
IsEssential = method(TypicalValue => Boolean)
IsEssential(Matrix) := (E) ->(
rkless3 := (detE == 0);
E2 = minors (2,E);
Mg = mingens (E2);
rkgreater1 := not (Mg == 0);
Et = transpose E;
A = E * Et * E;
B = 1/2 * trace(E * Et) * E;
car := (A == B);
return(rkgreater1 and rkless3 and car)
)
```

I det neste eksempelet brukar me denne metoden. Metoden `IsEssential(...)`, vil også bli brukt i seinare eksempel for å finne ut om ei matrise er essensiell.

Eksempel 15. Me har to matriser

$$M = \begin{bmatrix} 1 & 0 & -1 \\ 3 & 2 & 1 \\ 4 & 2 & 0 \end{bmatrix}, D = \begin{bmatrix} 0 & 1 & -2 \\ -1 & 0 & 3 \\ 2 & -3 & 0 \end{bmatrix}.$$

og vil finne ut om desse matrise er essensielle matriser. Brukar metode 1: `IsEssential(...)`, og skriver:

```
IsEssential (M)
IsEssential (D)
```

Den første kommandoen gir: "false". Den andre kommandoen gir den booliske verdien "true". Derfor er M ikkje ei essensiell matrise, medan matrisa D er ei essensiell matrise.

Me veit at ei essensiell matrise kan bli dekomponert til to matriser, $\mathcal{E} = R \cdot \mathcal{T}_a$. Me vil no lage ein metode som dekomponerer ei essensiell matrise, slik at me kan finne R og a.

Metode 2. La $\mathcal{E} \in Mat_3(\mathbb{Q})$ vere ei essensiell matrise. Skriv ein Macaulay-funksjon `Decomposed(...)` som finn alle dekomposisjonar $\mathcal{E} = R \cdot \mathcal{T}_a$, der $R \in Mat_3(\mathbb{R})$ er ei ortonormal matrise og $a \in \mathbb{R}^3$.

Me må bruke at $RR^T = I$. For å lage denne metoden må me bruke gröbnerbasar og ei eliminasjonsordning, sjå kapittel 4. Eliminasjonsordninga i denne metoden eliminerer dei ni første variablane, nemleg r variablane. Dermed kan me finne uttrykk for a_1, a_2 og a_3, for likningane me får ut.

```
A = QQ [ r11,r12,r13,r21,r22,r23,r31,r32,r33,a1,a2,a3, MonomialOrder => Eliminate 9 ]
Deomposed = method (TypicalValue => matrix)
Decomposed(Martix) := (M) ->(
S = genericSkewMatrix(A,a,3);
R = matrix{{r11,r12,r13},{r21,r22,r23},{r31,r32,r33}};
B = R * transpose R;
B11 = B_(0,1) - 1;
B12 = B_(0,1);
B13 = B_(0,2);
B21 = B_(1,0):
B22 = B_(1,1)-1;
B23 = B_(1,2);
B31 = B_(2,0);
B32 = B_(2,1);
B33 = B_(2,2)-1;
J1 = ideal(B11,B12,B13,B21,B22,B23,B31,B32,B33);
E = R * S;
G11 =M_(0,0) - E_(0,0);
G12 = M_(0,1) - E_(0,1);
G13 = M_(0,2) - E_(0,2);
G21 = M_(1,0) - E_(1,0);
G22 = M_(1,1) - E_(1,1);
G23 = M_(1,2) - E_(1,2);
G31 = M_(2,0) - E_(2,0);
G32 = M_(2,1) - E_(2,1);
G33 = M_(2,2) - E_(2,2);
N = ideal(G11,G12,G13,G21,G22,G23,G31,G32,G33);
L = N + J1 + (det R -1);
F1 := gens gb L;
return (F1)
)
```

Når me nyttar denne metoden må me først finne ut om matrisa er ei essensiell matrise ved å bruke `IsEssential(...)`-kommandoen frå metode 1. Deretter kan me bruke `Decomposed(...)`-kommandoen. Me viser korleis ein kan dekomponere ei matrise i det neste eksempelet.

Eksempel 16. Me har matrisa

$$M1 = \begin{bmatrix} -16/9 & 29/9 & -1/9 \\ -5/9 & 4/9 & -2/9 \\ 23/9 & 14/9 & 20/9 \end{bmatrix}.$$

som me vil dekomponere ved å bruke funksjonen i metode 2. Først må me sjekke om matrisa er ei essensiell matrise ved å bruke metode 1.

```
IsEssential (M1)
Decomposed (M1)
```

Matrisa M_1 er ei essensiell matrise og `decomposed`-funksjonen gir:

$$2a_2 + a_3, 2a_1 + 3a_3, a_3^2 - 4, 252r_{33} + 5a_3 - 18, 252r_{32} - 109a_3 + 6,$$
$$126r_{31} + 31a_3 + 6, 252r_{23} + 13a_3 - 198, 252r_{22} + 19a_3 + 66,$$
$$126r_{21} + 5a_3 + 66, 126r_{13} + 37a_3 + 18, 126r_{12} + 25a_3 - 6, 126r_{11} + 43a_3 - 12$$

Frå likninga $a_3^2 - 4 = 0$, kan ein løyse for a_3 og få at det blir ± 2. Deretter finn ein at $a_1 = \pm 3$ og $a_2 = \pm 1$. Til slutt kan ein finne verdiane for $r_{11} \ldots, r_{33}$, og set desse inn i ei matrise. Me får ut to matriser for R og to vektorar a,

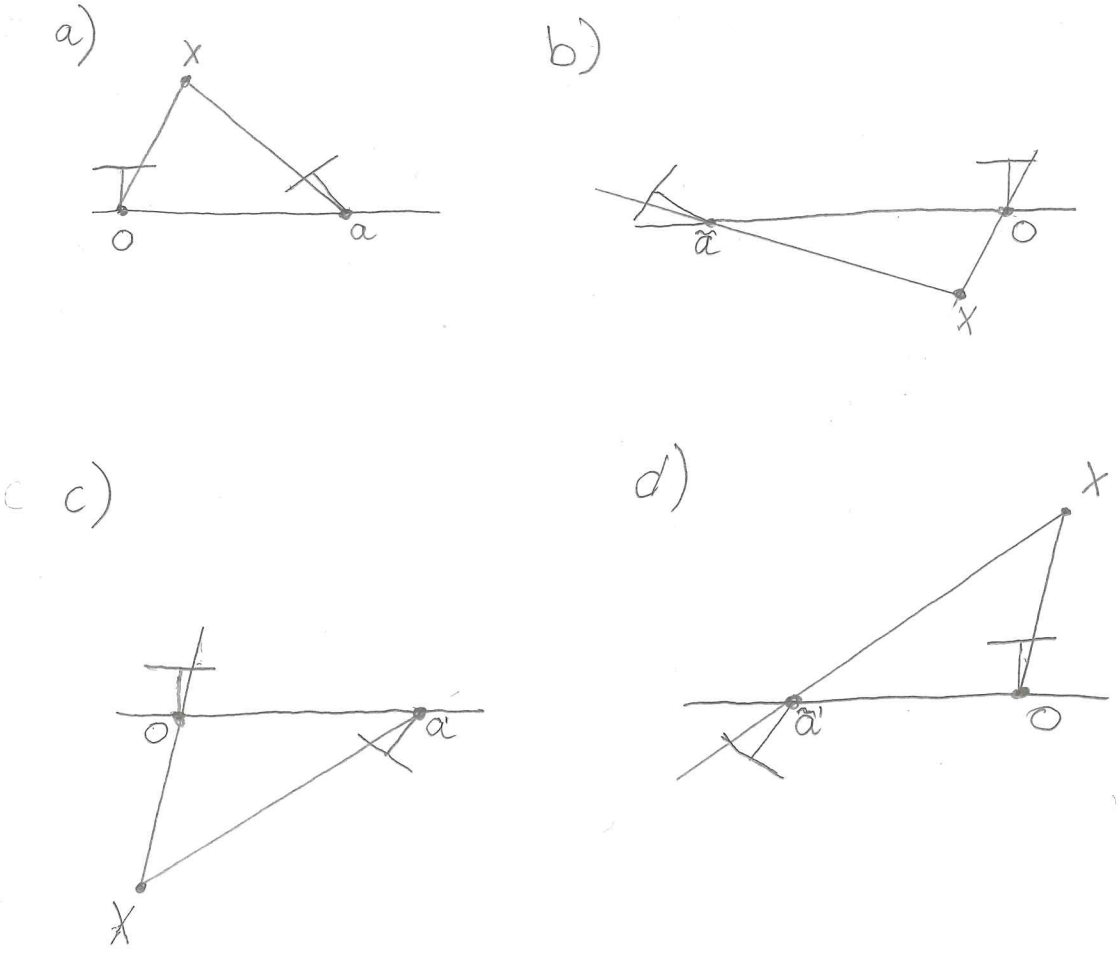
$$\mathbf{a} = \begin{pmatrix} 2 & 3 & 1 \end{pmatrix} \text{ som gir matrisa}$$
$$\Rightarrow R = \begin{bmatrix} -37/63 & -22/63 & -46/63 \\ -38/63 & -26/63 & 43/63 \\ -34/63 & 53/63 & 2/63 \end{bmatrix}, \text{ og}$$
$$\tilde{\mathbf{a}} = \begin{pmatrix} -2 & -3 & -1 \end{pmatrix} \text{ som gir matrisa}$$
$$\Rightarrow \tilde{R} = \begin{bmatrix} 7/9 & 4/9 & 4/9 \\ -4/9 & -1/9 & 8/9 \\ 4/9 & -8/9 & 1/9 \end{bmatrix}$$

Gröbnerbasar saman med ei eliminasjonsordning gjer at me får likningar som ein enkelt kan løyse (sjå kapittel 4). Me finn derfor eit uttrykk for a-ane og kan bruka utvidingsteoremet til å finne resten av løysingane.

Me ser av dette eksempelet at ei essensiell matrise gir to løysingar: (R, a) og $(\tilde{R}, \tilde{a})$. Den eine ortogonale matrisa representerer ein 180° rotasjon rundt $\overline{O\mathbf{a}}$- aksen, av det eine kamera. Dette er situasjonen som er illustrert i figur 3, a) og d). Me ser at for det eine kameramatriseparet er verdspunktet X bak det eine kameraet. For det andre kameramatriseparet er punktet X, framfor begge kamera.
Vektorane $\tilde{\mathbf{a}}$ og $\mathbf{a}$ representerer sentrumet til det andre kameraet. Det andre kamera har sentrumet til i origo. Frå eksempelet ser me at ein får to løysingar $\tilde{\mathbf{a}}$ og $\mathbf{a}$. Me ser at $\mathbf{a} = (-1)\tilde{\mathbf{a}}$, og dette gir ei forskyving av kamerasenteret for det andre kamera. Me har at $\mathbf{a}$ ligg til høgre for kamerasenter O, i eit vanleg koordinatsystem, medan $\tilde{\mathbf{a}}$ ligg til venstre. Dette blir kalla for skaleringstvitydigheita til eit kameramatrisepar.
Me ser på definisjonen til den essensielle matrisa, definisjon 7.1. Frå setning 7.3 veit me at viss $\mathcal{E}$ er ei essensiell matrise, så er $\lambda\mathcal{E}$ ei essensiell matrise. Bruka definisjonen, og ser at

$$q'^T \mathcal{E} q = 0 \Leftrightarrow q'^T(-\mathcal{E})q = 0.$$

Den essensielle matrisa er bestemt opp til ± 1. Dersom me finn løysingane til $-(M1)$-matrisa frå eksempelet over, får me at dette to kameramatrisepar: $(\tilde{R}, a)$ og $(R, \tilde{a})$. Desse løysingane er illustrert i figur 3, c) og b).



Figur 3: Fire moglege løysingar for rekonstruksjon frå den essensielle matrisa. Me har kamerasentera O og a. Verdspunktet X, blir avbilda i dei to kamera. Ein ser situasjonen ovanfrå. Og prinsipalaksen bind saman kamerasenteret og biletplanet, ser ut som ein T.
a) Punktet X ligg framfor begge kamera.
b) Kamerasenteret a har flytta plass, og X ligg bak begge kamera.
c) Kamera a er rotert 180^{circ}-om baselinja, slik at punktet X ligg bak kamera O og framfor kamera a.
d) Kamera a er rotert 180°-om baselinja, og flytta til venstre for O. Punktet X ligg framfor kamera O og bak kamera a.

Når me samanliknar desse fire løysingane, ser me at forskjellen mellom dei er at for to av løysingane er det eine kamera rotert 180° rundt $\overline{O\mathbf{a}}$- aksen, og for to løysingar er kamerasenteret til det eine kamera flytta. Frå figur 3, ser me at punktet X er bak det eine kamera, medan det er framfor det andre kamera for to kameramatrisepar. For eit kameramatrisepar er punktet bak begge kamera, og for eit anna er punktet framfor begge kamera.
Til saman gir dette fire løysingar:

$$(R, \mathbf{a}), (R, \tilde{\mathbf{a}}), (\tilde{R}, \mathbf{a}), (\tilde{R}, \tilde{\mathbf{a}}).$$

Det er kun i den eine løysinga at punktet ligg framfor begge kamera. For å finne ut kva løysing dette er må sjekke for eit av biletpunkta og finne ut for kva løysing punktet ligg framfor begge kamera.

Me skal no samle det me har funne i ei setning, der $Q = \{q_i \leftrightarrow q_i' \mid i = 1, \ldots, n\}$ er mengda med korresponderande punkt i normaliserte koordinatar.

Setning 7.9. Det eksisterer ein rekonstruksjon som er kompatibel med $Q = \{q_i \leftrightarrow q_i' \mid i = 1, \ldots, n\}$, viss og berre viss det eksisterer ei matrise $\mathcal{E} \in Mat_3(\mathbb{R})$, slik at følgjande gjeld:

1) $(q_i')^T \mathcal{E} q_i = 0$ for $i = 1, \ldots, n$.

2) $\mathcal{E}\mathcal{E}^T\mathcal{E} = 1/2 \cdot Spor(\mathcal{E}\mathcal{E}^T)\mathcal{E}$.

3) $rk(\mathcal{E}) = 2$.

Prov. Frå definisjon 7.1, tilfredsstillar ei essensiell matrise krav 1). Dersom me antek at biletkoordinatane er normaliserte, får ein frå teorem 6.8 at den essensielle matrisa oppfyller krav 1). Me veit også at ei essensiell matrise tilfredsstillar krav 2) den karakteristiske likninga, frå lemma 7.4.
I lemma 7.5 oppfyller ei matrise den karakteristiske likninga og har rang to (eller mindre), sidan determinanten til matrisa er null. Og frå lemma 7.6 og lemma 7.8 må ei essensiell matrise ha rang to, krav 3).
Frå lemma 7.8 har me at ei matrise som oppfyller den karakteristiske likninga og har rang to, er ei essensiell matrise. Og frå definisjonen på ei essensiell matrise må denne matrisa oppfylle krav 1). □

Essensiell varitet

Me assosierer ei matrise $\mathcal{E} = (z_{ij}) \in Mat_3(\mathbb{R})$ til punktet $p(\mathcal{E}) = (z_{11} : z_{12} : \ldots : z_{33})$ i $\mathbb{P}^8_{\mathbb{R}}$. Mengda $E = \{p(\mathcal{E}) \in \mathbb{P}^8_{\mathbb{R}} \mid \mathcal{E} \text{ essensiell matrise}\}$, blir kalla ei essensielt mengd i $\mathbb{P}^8_{\mathbb{R}}$, og den projektive variteten:

$$V = \big\{(z_{11} : z_{12} : \ldots : z_{33}) \in \mathbb{P}^8_{\mathbb{R}} \mid \mathcal{E} = (z_{ij}) \text{ tilfredsstillar den karakteristiske likninga}\big\}$$

blir kalla den essensielle variteten i $\mathbb{P}^8_{\mathbb{R}}$.
For å vise påstand 3) og 4) i det neste lemmaet brukar me hilbertpolynom-funksjonen. Me vil ikkje definere eller forklare kva eit hilbertpolynom er for noko, men kun bruke det til å finne dimensjonen og graden til ein varitet. For å gjere dette treng me ein definisjon og eit teorem.

Definisjon 7.10. Dimensjonen til ein projektiv varitet $V \subset \mathbb{P}^n(k)$, er graden til hilbertpolynomet til det korresponderande homogene idealet $I = I(V) \subset k[k_1, \ldots, x_n]$. Me skriv $dim(V)$ for dimensjonen til V.

Me kan finne dimensjonen ved å nytte det neste teoremet.

Teorem 7.11. *Lat $V = V(I) \subset \mathbb{P}^n(k)$ vere ein projektiv varitet, der $I \subset k[x_1, \ldots, x_n]$ er eit homogent ideal. Viss V er ei mengd som ikkje er tom, og k er algebraisk lukka, då har me*

$$dim(V) = deg(hilbertpolynom).$$

Dette gjeld for alle kroppar k når $I = I(V)$.[1] s, 464.

Graden til ein projektiv varitet V, er definert som å vere graden til $I(V)$, som er det same som graden til hilbertpolynomet, [1].

Lemma 7.12. *Bruk Macaulay til å finne idealet $I_V \subseteq \mathbb{Q}[z_{11}, \ldots, z_{33}]$ som definerer den essensielle variteten. Og til å vise at desse påstandane held.*

1. *Idealet I_V er eit homogent radikalt ideal.*
2. *Idealet I_V er eit primideal, det vil seie at den essensielle variteten er ein irreduserbar projektiv varitet.*
3. *Me har $dim(V) = 5$ og $deg(V) = 10$.*
4. *Viss me skjærer V med eit tilfeldig valt lineært rom $L \subseteq \mathbb{P}^8_{\mathbb{R}}$ med dimensjon tre, får me ti skjeringspunkt.*

Prov. 1) Brukar Macaulay2 og skriv:

```
T = QQ [ z11, z12, z13, z21, z22, z23, z31, z32, z33, MonomialOrder => Eliminate 7 ]
E = matrix{{z11, z12, z13}, {z21, z22, z23}, {z31, z32, z33}}
Et = transpose E
A = E * Et * E;
B = 1/2 * trace(E * Et) * E;
I = ideal(A - B)
V = proj(T/I)
J = ideal V
J == I
```

————-> ”true”

```
isHomogeneous J
```

Som gir ”true”. Det blir for omfattande å finne ut om idealet er eit radikalt ideal, men kommandoen for dette er: `radical J`

2) Det er for løysningstungt for programmet å finne ut om idealet er eit primideal, men kommandoen for det er: `isPrime J`.

3) Finn først hilbertpolynomet til variteten og deretter graden og dimensjonen. Brukar Macaulay2 og skriv:

```
P = hilbertPolynomial V
dim P
degree P
```

Får at dimensjonen til P er fem, og graden er 10. Då har ein at $dim(V) = 5$ og $deg(V) = 10$.

4) Me skjærer variteten V med eit tilfeldig valt lineært rom, ved å skrive følgjande kommandoar inn i Macaulay2:

```
L = random (T^1, T^{5:-1})
L1 = ideal image L
S = L + I
hilbertPolynomial (T/S)
```

Får då ut hilbertpolynomet $10 * P_0$, som betyr at snittet av V og L, gir ti skjeringspunkt. □

7.3 Rekonstruksjon frå fem korresponderande punkt

I denne delen skal me lage ein rekonstruksjonsfunksjon som brukar korresponderande punkt til å finne ut om det fins ei endeleg løysing for den essensielle matrisa. Deretter brukar me denne funksjonen i to eksempel for å finne ut om me kan finne ein slik rekonstruksjon. Me finn då at punkta må vere i generell posisjon for at me skal få ei endeleg løysing.

Metode 3. Skriv ein Macaulay-funksjon `Reconstruct(...)`, som tek ei mengd med korresponderande par $Q = \{q_i \leftrightarrow q_i' \mid i = 1, \ldots, n\}$ og utfører følgjande steg:

1. Finn likningane til hyperplana i $\mathbb{P}^8_{\mathbb{R}}$ definert ved $(q_i')^T \mathcal{E} q_i = 0$ for $i = 1, \ldots, n$.
2. Skjær V med desse hyperplana.
3. Sjekk om det er endeleg mange rekonstruksjonar kompatible med Q.

```
W = QQ [ z11, z12, z13, z21, z22, z23, z31, z32, z33, MonomialOrder => Eliminate 7 ]
E = matrix{{z11, z12, z13}, {z21, z22, z23}, {z31, z32, z33}}
Q = {q1,q2,q3,q4,q5,q'1,q'2,q'3,q'4,q'5}
Reconstruct = method (TypicalValue => matrix)
Reconstruct(Matrix) := (Q) ->(
Et = transpose E;
A = E * Et * E;
B = 1/2 * trace(E * Et) * E;
car := (A == B);
I = ideal(A - B);
Q1 = (q'1 * E * (transpose q1);
Q2 = (q'2 * E * (transpose q2);
Q3 = (q'3 * E * (transpose q3);
Q4 = (q'4 * E * (transpose q4);
Q5 = (q'5 * E * (transpose q5);
D = matrix {{Q1},{Q2},{Q3},{Q4},{Q5}};
C = ideal D;
X = I + C;
return (X)
)
F = hilbertPolynomial (W/X)
```

Dersom hilbertpolynomet er på forma: $m * P_0$ har problemet ei endeleg løysing.
Det går då an å finne ei essensiell matrise som svarar til dei korresponderande biletpunkta. Og til slutt kan me bruke metode-funksjonen `Decomposed` frå metode 2 til å finne kameramatrisepara.

Eksempel 17. Bruk funksjonen `Reconstruct(...)` på mengda av fem korresponderande punkt $Q = \{q_1 \leftrightarrow q_1', \ldots, q_5 \leftrightarrow q_5'\}$ gitt ved $q_1 = q_1' = (1,0,0)$, $q_2 = q_2' = (0,1,0)$, $q_3 = q_3' = (0,0,1)$, $q_4 = q_5' = (1,1,1)$ og $q_5 = q_4' = (3,7,2)$. Vis at det eksisterer ein eindimensjonal familie av rekonstruksjonar kompatible med desse fem korresponderande para.

$q_1 = (1,0,0)$
$q_2 = (0,1,0)$
$q_3 = (0,0,1)$
$q_4 = (1,1,1)$
$q_5 = (3,7,2)$
$q_1' = (1,0,0)$
$q_2' = (0,1,0)$
$q_3' = (0,0,1)$
$q_4' = (3,7,2)$
$q_5' = (1,1,1)$

```
L= matrix {{q1},{q2},{q3},{q4},{q5},{q1'},{q2'},{q3'},{q4'},{q5'}}
K= Reconstruct L
F= hilbertPolynomial(W1/X)
```

Me får då ut hilbertpolynomet $6 \cdot P_0 + P_1$, som betyr at løysinga er ein eindimensjonal familie av løysinga. Det betyr at det er ei kurve med uendeleg mange løysingar.

Eksempel 18. Bruk funksjonen `Reconstruct(...)` på mengda av fem korresponderande par $Q = \{q_i \leftrightarrow q_i' \mid i = 1, \ldots, n\}$ som ein får ved å gjere ein perturbasjon av para i oppgåve v). Vis at det eksisterer ti rekonstruksjonar kompatible med para.
Me har para:
$q_1 = (1,0,0)$, $q_2 = (0,1,0)$, $q_3 = (0,0,1)$,$q_4 = (1,1,1)$,$q_5 = (3,7,2)$,$q_1' = (1,0,0)$,$q_2' = (0,1,0)$,$q_3' = (0,0,1)$,$q_4' = (16/5,7,2)$,$q_5' = (1,1,1)$,
der me har gjort ein perturbasjon på q_4'. Me skriv:

```
L= matrix {{q1},{q2},{q3},{q4},{q5},{q1'},{q2'},{q3'},{q4'},{q5'}}
Reconstruct L
F= hilbertPolynomial(W1/X)
```

Dette gir hilbertpolynomet $10 \cdot P_0$ som svarar til ti punkt, og me har ei endeleg løysing.

Me ser på desse to eksempla og trekker ein konklusjon.

Setning 7.13. Me konkluder med at ein generelt treng minst fem korresponderande par for å redusere den kompatible rekonstruksjonen til ei endeleg mengd av moglegheiter. Og generelt gir dette ti moglegheitar som då vidare kan bestemmast av fleire korresponderande par, eller ved andre metodar.

Prov. Me ser av eksempelet over at fem korresponderande par kan gi ein endeleg rekonstruksjon. Desse korresponderande para må vere i generell posisjon. Viss ikkje får me ikkje ei endeleg løysing, som me såg i det førre eksempelet. □

Me veit no at når me har fem korresponderande punkt, kan me finne ei endeleg løysing for den essensielle matrisa. Og så kan me dekomponere den og finne fire ulike kameraforskyvingspar. Ved å teste når eit av punkta ligg framfor begge kamera, kan me finne kameraforskyvingsparet som svarar til den situasjonen.
Sidan me har gitt definisjonen på ei essensiell matrise, $q'^T Eq = 0$, som er gjeven for eit kamera der den eine kameramatrisa er $P = [I \mid 0]$. Og me har fem korresponderande punkt, då kan me finne den essensielle matrisa. Denne matrisa kan me dekomponere, sidan $\mathcal{E} = R \cdot \mathcal{T}_a$. Då finn me to ortogonale matriser R og $\tilde{R}$, og to vektorar a og $\tilde{a}$ som me set inn i den antisymmetriske matrisa. Ved å nytte det eine punktet kan me finne ut for kva $R, \tilde{R}, a, \tilde{a}$ at punkta ligg framfor begge kamera. Me kallar kameraforskyvingsparet der punkta er framfor kamera for (R, a). Då er kameramatrisa som svarar til dei korresponderande punkta, $P' = [R \mid a]$.

Kapittel 8

Avslutting

8.1 Oppsummering

I denne oppgåva har me funne at for fem korresponderande biletpunkt i generell posisjon, kan me finne ei endeleg løysing for den essensielle matrisa. Me har også sett at når me dekomponerer ei essensiell matrise, til ei ortonormal matrise og ei antisymmetrisk matrise, så får ein fire moglege løysingar for kameramatriseparet (R, a). For den eine løysinga ligg punktet i rommet, framfor begge kamera.
For å komme fram til dette måtte me bruke gröbnerbasar, som ein nyttar for å løyse ikkje-lineære likningar. I lag med dette nytta ein også ei eliminasjonsordning, slik at me fekk ei likning som kun inneheld ein ukjend variabel. Når denne variabelen var funnen kunne me bruke utvidingsteoremet, og sette denne løysinga inn i dei andre likningane. Då fekk me ut verdiar av alle dei ukjende, og systemet var løyst.
Me introduserte fundamentalmatrisa i kapittel seks. Denne matrisa representerer avbildinga frå eit punkt i eit bilete til eit anna punkt i eit anna bilete, der punkta er korresponderande biletpunkt. Deretter såg me på tilfellet der punkta var gjevne i normaliserte koordinatar, der verknaden av kalibreringsmatrisa var fjerna. Då kallar me matrisa som representer avbildinga mellom korresponderande biletpunkt, for den essensielle matrisa. Vidare i kapittel sju kom me fram til fleire eigenskapar til denne matrisa, og lagde blant anna ein metode for å dekomponere matrisa.

Kapittel 9

Referansar

- [1] D.Cox, J.Little, D.O'Shea, *Ideals, varieties and algorithms*, 3.ed. UTM in mathematics, Springer, 2012.
- [2] V.Ene, J.Herzog,*Gröbner bases in comutative algebra*, American Mathematical Society, 2012.
- [3] N.Lauritzen, *Concrete abstract algebra*, Cambridge University Press, 2007.
- [4] R.Hartley, A.Zisserman, *Multiple view geometry in computer vision*, 2.ed. Cambridge University Press, 2003.
- [5] M.Kreuzer, L.Robbiano, *Computational commutative algebra 2*, Springer, 2005.