

Invariantteori for Endelige Matrixgrupper

Tarik Rian og Michael Knudsen

I det følgende betegner k et algebraisk lukket legeme, og $\text{GL}_n(k)$ betegner gruppen af invertible $(n \times n)$ -matricer med indgange i k .

1 Ringe af Invarianter

Lad $f \in k[X_1, \dots, X_n]$ være et polynomium i n variable over k . Vi vil ofte bruge notationen $f(X_1, \dots, X_n) = f(\mathbf{X})$, hvor \mathbf{X} betegner vektoren (X_1, \dots, X_n) . Lad $A \in \text{GL}_n(k)$ være en matrix. Da betegner $A\mathbf{X}$ det sædvanlige matrixprodukt, hvor vi tænker på \mathbf{X} som en søjlevektor.

Lad G være en undergruppe af $\text{GL}_n(k)$. Vi definerer en gruppevirkning

$$G \times k[X_1, \dots, X_n] \rightarrow k[X_1, \dots, X_n], \quad (A, f) \mapsto A \cdot f,$$

af G på $k[X_1, \dots, X_n]$ ved $(A \cdot f)(\mathbf{X}) = f(A^{-1}\mathbf{X})$. Det er let at tjekke, at dette rent faktisk *er* en gruppevirkning. Et polynomium $f \in k[X_1, \dots, X_n]$ kaldes **G -invariant**, hvis $A \cdot f = f$ for alle $A \in G$. Mængden af G -invariante polynomier betegnes $k[X_1, \dots, X_n]^G$.

Proposition 1.1. *Lad G være en undergruppe i $\text{GL}_n(k)$. Da er $k[X_1, \dots, X_n]^G$ en delring af $k[X_1, \dots, X_n]$, som indeholder de konstante polynomier.*

Bevis. Det er klart, at de konstante polynomier er G -invariante. Dermed gælder specielt $1 \in k[X_1, \dots, X_n]^G$. Lad $f, g \in k[X_1, \dots, X_n]^G$. Da gælder for alle $A \in G$, at

$$A \cdot (f + g) = A \cdot f + A \cdot g = f + g$$

$$A \cdot (fg) = (A \cdot f)(A \cdot g) = fg$$

$$A \cdot (-f) = -(A \cdot f) = -f,$$

så $k[X_1, \dots, X_n]^G$ er lukket under addition, multiplikation og inversdannelse. \square

Eksempel. Lad

$$G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\}.$$

Da er G en undergruppe af $\text{GL}_2(k)$. Lad $f = \sum_{i,j} a_{ij} X^i Y^j$ være et polynomium i $k[X, Y]$. Vi ser, at $f \in k[X, Y]^G$, hvis og kun hvis $f(X, Y) = f(-X, Y)$, hvis og kun hvis $\sum_{i,j} a_{ij} X^i Y^j = \sum_{i,j} (-1)^i a_{ij} X^i Y^j$, hvis og kun hvis $a_{ij} = 0$ for i ulige.

I det ovenstående eksempel var det let at beregne $k[X, Y]^G$ direkte. Her følger et mindre trivielt eksempel:

Eksempel. Lad S_n betegne den symmetriske gruppe. For $\sigma \in S_n$ definerer vi $A_\sigma \in \text{GL}_n(k)$ ved $A_\sigma = (a_{ij})$, hvor

$$a_{ij} = \begin{cases} 1 & \text{hvis } j = \sigma(i) \\ 0 & \text{ellers} \end{cases}.$$

Lad

$$f = \sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} X_1^{i_1} \cdots X_n^{i_n}$$

være et polynomium i $k[X_1, \dots, X_n]$. Da er

$$f(A_\sigma \mathbf{X}) = \sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} X_{\sigma(1)}^{i_1} \cdots X_{\sigma(n)}^{i_n}.$$

Bemærk, at der for $\sigma, \tau \in S_n$ gælder, at $A_\sigma A_\tau = A_{\tau\sigma}$, så vi har en gruppehomomorfi

$$\varphi: S_n \rightarrow \text{GL}_n(k), \quad \sigma \mapsto A_\sigma^{-1}.$$

Da $\sigma \in S_n$ bestemmer A_σ (og dermed også A_σ^{-1}) entydigt, er φ injektiv, og vi vil i det følgende identificere S_n med $\varphi(S_n) \subset \text{GL}_n(k)$. Et polynomium i $k[X_1, \dots, X_n]^{S_n}$ kaldes **symmetrisk**. Betragt følgende polynomier i $k[X_1, \dots, X_n]$:

$$\begin{aligned} s_1 &= X_1 + \cdots + X_n \\ &\vdots \\ s_j &= \sum_{i_1 < \cdots < i_j} X_{i_1} \cdots X_{i_j} \\ &\vdots \\ s_n &= X_1 \cdots X_n. \end{aligned}$$

Det er klart, at s_1, \dots, s_n alle er symmetriske. Det kan vises (se f.eks. [1] kapitel 7, theorem 3 eller [2] theorem 2.6.4), at ethvert symmetrisk polynomium i $k[X_1, \dots, X_n]$ er et polynomium i s_1, \dots, s_n . Altså er

$$k[X_1, \dots, X_n]^{S_n} = k[s_1, \dots, s_n].$$

I eksemplet ovenfor siger vi, at $k[X_1, \dots, X_n]^{S_n}$ er **frembragt** af s_1, \dots, s_n . Vi skal senere se, at $k[X_1, \dots, X_n]^G$ altid er endeligt frembragt, hvis G er endelig. Vi afslutter dette afsnit med en proposition, som viser sig at være meget nyttig.

Proposition 1.2. *Lad G være en undergruppe i $\text{GL}_n(k)$, og lad f være et polynomium i $k[X_1, \dots, X_n]$. Da er f G -invariant, hvis og kun hvis alle de homogene komponenter af f er G -invariante.*

Bevis. Det er klart, at f er G -invariant, hvis alle de homogene komponenter af f er G -invariante. Antag omvendt, at f er G -invariant, og lad $f = \sum_{i=0}^d h_i$ være en opskrivning af f som en sum af homogene komponenter, hvor h_i har grad i . Antag, at der findes et j , så h_j ikke er G -invariant. Da gælder for alle $A \in G$, at $A \cdot f = \sum_{i=0}^d A \cdot h_i = A \cdot f_j + \sum_{i \neq j} A \cdot h_i \neq f$, da G -virkningen bevarer grader. \square

2 Frembringere for Ringe af Invarianter

Vi vil fra og med dette afsnit koncentrere os om *endelige* undergrupper af $\text{GL}_n(k)$. Målet er at vise, at $k[X_1, \dots, X_n]^G$ er endeligt frembragt, hvis G er endelig.

Lad G være en endelig undergruppe af $\text{GL}_n(k)$. Vi vil i det følgende altid lade det være antaget, at karakteristikken af k ikke deler $|G|$. Da definerer vi **Reynoldsoperatoren** $R_G : k[X_1, \dots, X_n] \rightarrow k[X_1, \dots, X_n]$ ved, at

$$R_G(f) = \frac{1}{|G|} \sum_{A \in G} A \cdot f$$

for $f \in k[X_1, \dots, X_n]$. Reynoldsoperatoren tager så at sige *gennemsnittet* af G 's virkning på $k[X_1, \dots, X_n]$. Det er klart, at R_G er k -lineær.

Proposition 2.1. *Lad G være en endelig undergruppe af $\text{GL}_n(k)$, og lad f være et polynomium i $k[X_1, \dots, X_n]$. Da gælder*

- (1) $R_G(f) \in k[X_1, \dots, X_n]^G$.
- (2) Hvis f er G -invariant, så er $R_G(f) = f$.

Bevis. (1) Lad $B \in \text{GL}_n(k)$. Da gælder for alle $f \in k[X_1, \dots, X_n]$, at

$$B \cdot R_G(f) = \frac{1}{|G|} \sum_{A \in G} B \cdot (A \cdot f) = \frac{1}{|G|} \sum_{A \in G} (BA) \cdot f = \frac{1}{|G|} \sum_{C \in G} C \cdot f = R_G(f),$$

så $R_G(f)$ er G -invariant. (2) Antag, at f er G -invariant. Da er

$$R_G(f) = \frac{1}{|G|} \sum_{A \in G} A \cdot f = \frac{1}{|G|} \sum_{A \in G} f = f. \quad \square$$

Vi har altså nu et redskab til at producere G -invariante polynomier med, og R_G spiller da også en vigtig rolle i beviset for, at $k[X_1, \dots, X_n]^G$ er endeligt frembragt.

Proposition 2.2. *Lad G være en endelig undergruppe af $\mathrm{GL}_n(k)$, og lad f og g være polynomier i $k[X_1, \dots, X_n]$. Antag, at g er G -invariant. Da er $R_G(fg) = R_G(f)g$.*

Bevis. Der gælder, at

$$\begin{aligned}
 R_G(fg) &= \frac{1}{|G|} \sum_{A \in G} A \cdot (fg) \\
 &= \frac{1}{|G|} \sum_{A \in G} (A \cdot f)(A \cdot g) \\
 &= \frac{1}{|G|} \sum_{A \in G} (A \cdot f)g \\
 &= \left(\frac{1}{|G|} \sum_{A \in G} (A \cdot f) \right) g \\
 &= R_G(f)g. \quad \square
 \end{aligned}$$

Vi er nu i stand til at vise den ønskede sætning.

Sætning 2.3 (Hilbert). *Lad G være en endelig undergruppe af $\mathrm{GL}_n(k)$. Da er $k[X_1, \dots, X_n]^G$ endeligt frembragt.*

Bevis. Lad I betegne idealet i $k[X_1, \dots, X_n]$ frembragt af alle homogene, G -invariante polynomier af positiv totalgrad. I følge Hilberts Basissætning findes endeligt mange polynomier $g_1, \dots, g_s \in k[X_1, \dots, X_n]$, så $I = \langle g_1, \dots, g_s \rangle$. Definitionen af I giver, at ethvert g_i er på formen $g_i = \sum_j h_{ij} f_{ij}$, hvor $h_{ij}, f_{ij} \in k[X_1, \dots, X_n]$, og hvor f_{ij} er homogent og G -invariant for alle i og j . Da g_1, \dots, g_s frembringer I , gør mængden af alle f_{ij} 'erne det også, og efter en omnummerering har vi, at I er frembragt af endeligt mange homogene, G -invariante polynomier f_1, \dots, f_m .

Vi vil vise, at $k[X_1, \dots, X_n]^G = k[f_1, \dots, f_m]$. Da f_1, \dots, f_m alle er G -invariante, følger det af proposition 1.1, at $k[f_1, \dots, f_m] \subset k[X_1, \dots, X_n]^G$. Antag nu modstridvist, at $k[X_1, \dots, X_n]^G \not\subset k[f_1, \dots, f_m]$, og vælg et polynomium $g \in k[X_1, \dots, X_n]^G$ af positiv totalgrad, så $g \notin k[f_1, \dots, f_m]$. Et sådan polynomium findes, idet alle polynomier af totalgrad 0 ligger i $k[f_1, \dots, f_m]$. Vælg en homogen komponent h af g af positiv totalgrad. I følge proposition 1.2 er h ligeledes G -invariant. Da $k[f_1, \dots, f_m]$ ikke kan indeholde alle de homogene komponenter af g , slutter vi, at der findes et homogent, G -invariant polynomium af positiv totalgrad i $k[X_1, \dots, X_n]^G$, som ikke ligger i $k[f_1, \dots, f_m]$. Vælg et sådan polynomium f af minimal, positiv totalgrad d .

Da $f \in I = \langle f_1, \dots, f_m \rangle$, kan vi skrive $f = \sum_{i=1}^m h_i f_i$, hvor $h_i \in k[X_1, \dots, X_n]$ for alle i . Vi kan antage, at der for alle i gælder, at $h_i f_i$ enten er 0 eller homogent af totalgrad d , thi antag, at $h_i f_i \neq 0$ ikke er homogent

af grad d . Da kan vi skrive

$$h_i f_i = \text{led af grad } d + \text{resterende led},$$

og da f er homogent af grad d , må de resterende led modsvares af tilsvarende, resterende led fra andre $h_j f_j$, og vi kan forkorte udtrykket for $h_i f_i$.

Da f er G -invariant, gælder i følge proposition 2.1, at $f = R_G(f)$, og af proposition 2.2 følger da, idet f_i er G -invariant for alle i , at

$$f = R_G(f) = R_G\left(\sum_{i=1}^m h_i f_i\right) = \sum_{i=1}^m R_G(h_i f_i) = \sum_{i=1}^m R_G(h_i) f_i.$$

Da R_G oplagt bevarer totalgraden af polynomier, slutter vi, at $R_G(h_i) f_i$ enten er 0 eller homogent af totalgrad d for alle i , da det tilsvarende gælder for $h_i f_i$. Idet f_i har positiv totalgrad, har $R_G(h_i)$ totalgrad $< d$. Da $R_G(h_i) f_i$ er homogent, og da f_i er homogent, må også $R_G(h_i)$ være homogent, og i følge proposition 2.1 er $R_G(h_i)$ G -invariant. Minimaliteten af d giver dermed, at $R_G(h_i) \in k[f_1, \dots, f_m]$ for alle i , så

$$f = \sum_{i=1}^m R_G(h_i) f_i \in k[f_1, \dots, f_m],$$

hvilket er en modstrid. □

Det ovenstående bevis er et rent eksistensbevis, og det giver ikke nogen metode til at beregne de endeligt mange frembringere. Der gælder dog følgende sætning (se f.eks. [1] kapitel 7, theorem 5):

Sætning 2.4 (Noether). *Lad G være en endelig undergruppe af $\text{GL}_n(k)$. Da er $k[X_1, \dots, X_n]^G$ frembragt af alle $R_G(\mathbf{X}^\alpha)$, hvor $|\alpha| \leq |G|$.*

Bemærk, at antallet af frembringere, som optræder i sætningen ovenfor, er meget stor selv for forholdsvis små gruppeordener. I praksis betyder det, at sætningen er svær at anvende selv for en computer.

3 Relationer blandt Frembringere

Lad G være en endelig undergruppe af $\text{GL}_n(k)$, og lad f_1, \dots, f_m være polynomier i $k[X_1, \dots, X_n]$, som opfylder $k[X_1, \dots, X_n]^G = k[f_1, \dots, f_m]$. Lad F betegne det ordnede m -tupel (f_1, \dots, f_m) . Vi definerer

$$I_F = \{h \in k[Y_1, \dots, Y_m] \mid h(f_1, \dots, f_m) = 0 \text{ i } k[X_1, \dots, X_n]\}.$$

Det er klart, at I_F er et ideal i $k[Y_1, \dots, Y_m]$. Idealet I_F kaldes **relationsidealet** for F .

Proposition 3.1. *Lad G være en endelig undergruppe af $GL_n(k)$, og lad $F = (f_1, \dots, f_m)$ være en mængde af polynomier i $k[X_1, \dots, X_n]$, som opfylder $k[X_1, \dots, X_n]^G = k[f_1, \dots, f_m]$. Lad I_F betegne relationsidealet for F . Da er I_F et primideal i $k[Y_1, \dots, Y_m]$, og der findes en ringisomorfi*

$$k[X_1, \dots, X_n]^G \simeq k[Y_1, \dots, Y_m]/I_F.$$

Bevis. Vi har bemærket ovenfor, at I_F er et ideal i $k[Y_1, \dots, Y_m]$. Antag nu, at g_1 og g_2 er polynomier i $k[Y_1, \dots, Y_m]$, som ikke ligger i I_F . Da er $g_1(f_1, \dots, f_m) \neq 0$ og $g_2(f_1, \dots, f_m) \neq 0$. Da $k[X_1, \dots, X_n]^G$ som delring af $k[X_1, \dots, X_n]$ er et integritetsområde, gælder $g_1(f_1, \dots, f_m)g_2(f_1, \dots, f_m) \neq 0$, og dermed ligger produktet g_1g_2 heller ikke i I_F .

Definer $\varphi : k[Y_1, \dots, Y_m] \rightarrow k[X_1, \dots, X_n]^G$ ved $\varphi(g) = g(f_1, \dots, f_m)$. Det er klart, at φ er en ringhomomorfi, og da $k[X_1, \dots, X_n]^G = k[f_1, \dots, f_m]$, er φ surjektiv. Definitionen af I_F giver umiddelbart, at $\ker(\varphi) = I_F$, så φ inducerer en ringisomorfi $k[X_1, \dots, X_n]^G \simeq k[Y_1, \dots, Y_m]/I_F$. \square

Proposition 3.2. *Lad G være en endelig undergruppe af $GL_n(k)$, og lad $F = (f_1, \dots, f_m)$ være en mængde af polynomier i $k[X_1, \dots, X_n]$, som opfylder $k[X_1, \dots, X_n]^G = k[f_1, \dots, f_m]$. Sæt*

$$J_F = \langle f_1 - Y_1, \dots, f_m - Y_m \rangle \subset k[X_1, \dots, X_n, Y_1, \dots, Y_m].$$

Da er $I_F = J_F \cap k[Y_1, \dots, Y_m]$. Altså er I_F det n -te eliminationsideal for J_F .

Bevis. Vi viser først, at der for et polynomium $p \in k[X_1, \dots, X_n, Y_1, \dots, Y_m]$ gælder, at $p \in J_F$, hvis og kun hvis $p(X_1, \dots, X_n, f_1, \dots, f_m)$ er 0 i polynomiumsringen $k[X_1, \dots, X_n]$. Af definitionen af J_F følger det umiddelbart, at alle $p \in J_F$ opfylder den ønskede betingelse. For at vise den anden implikationen bemærker vi, at der for et vilkårligt $p \in k[X_1, \dots, X_n, Y_1, \dots, Y_m]$ gælder, at

$$\begin{aligned} p(\mathbf{X}, Y_1, \dots, Y_m) &= p(\mathbf{X}, f_1 - (f_1 - Y_1), \dots, f_m - (f_m - Y_m)) \\ &= p(\mathbf{X}, f_1, \dots, f_m) + \sum_{i=1}^m A_i(f_i - Y_i), \end{aligned}$$

hvor $A_i \in k[X_1, \dots, X_n, Y_1, \dots, Y_m]$ for alle $i = 1, \dots, m$, hvilket viser, at $p \in J_F$, hvis $p(X_1, \dots, X_n, f_1, \dots, f_m) = 0$.

Af den netop viste påstand følger nu, at $p \in J_F \cap k[Y_1, \dots, Y_m]$, hvis og kun hvis $p(f_1, \dots, f_m) = 0$, hvis og kun hvis $p \in I_F$. \square

Korollar 3.3. *Lad $V_F = \mathbf{V}(I_F)$ betegne den affine varietet hørende til idealet I_F . Da er V_F den mindste varietet i k^n , som indeholder parametriseringen*

$$\begin{aligned} y_1 &= f_1(x_1, \dots, x_n) \\ &\vdots \\ y_m &= f_m(x_1, \dots, x_n). \end{aligned}$$

Bevis. Da I_F er det n -te eliminationsideal for J_F , følger påstanden umiddelbart ved brug af eliminationsteori (se [1] kapitel 3, §3). \square

4 Baners Geometri

Lad G være en endelig undergruppe af $\mathrm{GL}_n(k)$. Da virker G på k^n ved sædvanlig matrixmultiplikation. Vi vil i dette afsnit vise, at mængden k^n/G af baner for G -virkningen kan gives en struktur som en affin varietet. Faktisk vil det vise sig, at k^n/G bliver isomorf med V_F .

Proposition 4.1. *Lad G være en endelig undergruppe af $\mathrm{GL}_n(k)$, og lad $F = (f_1, \dots, f_m)$ være en mængde af polynomier i $k[X_1, \dots, X_n]$, som opfylder $k[X_1, \dots, X_n]^G = k[f_1, \dots, f_m]$. Da er $\mathbf{I}(V_F) = I_F$.*

Bevis. Det er klart, at $I_F \subset \mathbf{I}(V_F)$. Lad omvendt $h \in \mathbf{I}(V_F)$ være vilkårlig. Da $(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)) \in V_F$ for alle $(x_1, \dots, x_n) \in k^n$ gælder, at $h(f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)) = 0$ for alle $(x_1, \dots, x_n) \in k^n$. Da legemet k er algebraisk lukket, er k uendeligt, så $h(f_1, \dots, f_m)$ er nulpolynomiet (se f.eks. [1] kapitel 1, proposition 5). i $k[X_1, \dots, X_n]$. Altså er $h \in I_F$. \square

Som trivielt korollar af den ovenstående proposition får vi, idet $\mathbf{I}(V_F) = I_F$ er et primideal, af V_F er en irreducibel, affin varietet. Vi får desuden følgende vigtige resultat:

Korollar 4.2. *Lad $k[V_F]$ være koordinatringen for V_F . Der er en ringisomorfi $k[V_F] \simeq k[X_1, \dots, X_n]^G$. Desuden gælder, at hvis $F = (f_1, \dots, f_m)$ og $F' = (f'_1, \dots, f'_{m'})$ er to sæt frembringere for $k[X_1, \dots, X_n]^G$, da er varieteterne V_F og $V_{F'}$ isomorfe.*

Bevis. Der gælder, at

$$k[V_F] = k[X_1, \dots, X_n]/I_F = k[X_1, \dots, X_n]/\mathbf{I}(V_F) \simeq k[X_1, \dots, X_n]^G,$$

hvor det andet lighedstegn følger af proposition 4.1, og hvor isomorfien kommer fra proposition 3.1. Vi ser specielt, at koordinatringene $k[V_F]$ og $k[V_{F'}]$ er isomorfe. Det følger nu af [1] kapitel 5, sætning 9, at V_F og $V_{F'}$ er isomorfe. \square

For at vise, at k^n/G har en struktur som en affin varietet, har vi brug for følgende, tekniske lemma:

Lemma 4.3. *Lad G være en endelig undergruppe af $\mathrm{GL}_n(k)$, og lad f_1, \dots, f_m være frembringere for $k[X_1, \dots, X_n]^G$. Sæt $N = |G|$. Da findes for hvert $i = 1, \dots, n$ et polynomium $p_i \in J_F \cap k[X_i, \dots, X_n, Y_1, \dots, Y_m]$ på formen*

$$p_i = X_i^N + \text{led hvor } X_i \text{ optræder med grad } < N.$$

Bevis. Vi indfører en ny variabel X og bemærker, at der for alle $f \in k[X_1, \dots, X_n]$ gælder, at

$$\prod_{A \in G} (X - A \cdot f) = X^N + g_1 X^{N-1} + \dots + g_N,$$

for passende $g_j \in k[X_1, \dots, X_n]$. Vi påstår, at alle g_j er G -invariante: Lad $B \in G$. Da gælder for alle \mathbf{X} , at

$$\begin{aligned} X^N + g_1(\mathbf{X})X^{N-1} + \dots + g_N(\mathbf{X}) &= \prod_{A \in G} (X - (A \cdot f)(\mathbf{X})) \\ &= \prod_{A \in G} (X - (AB \cdot f)(\mathbf{X})) \\ &= \prod_{A \in G} (X - (A \cdot f)(B^{-1}\mathbf{X})) \\ &= X^N + g_1(B^{-1}\mathbf{X})X^{N-1} + \dots + g_N(B^{-1}\mathbf{X}), \end{aligned}$$

og ved at sammeligne koefficienter ser vi, at $(B \cdot g_j)(\mathbf{X}) = g_j(B^{-1}\mathbf{X}) = g_j(\mathbf{X})$ for alle $j = 1, \dots, N$, så alle g_j er G -invariante.

Bemærk, at f er rod i $\prod (X - A \cdot f)$, idet en af faktorerne er $X - I \cdot f = X - f$. Heraf følger ved at betragte tilfældet $f = X_i$, at

$$X_i^N + g_1 X_i^{N-1} + \dots + g_N = 0$$

for passende $g_j \in k[X_1, \dots, X_n]^G$. Da $k[X_1, \dots, X_n]^G = k[f_1, \dots, f_m]$, findes for hvert $j = 1, \dots, N$ et polynomium $h \in k[Y_1, \dots, Y_m]$, så $g_j = h_j(f_1, \dots, f_m)$. Sæt

$$p_i(X_i, Y_1, \dots, Y_m) = X_i^N + h_1(Y_1, \dots, Y_m)X_i^{N-1} + \dots + h_N(Y_1, \dots, Y_m).$$

Da er $p_i(X_i, f_1, \dots, f_m) = 0$, så $p_i \in J_F$ (jævnfør første del af beviset for proposition 3.2). \square

Vi er nu klar til at vise det ønskede.

Sætning 4.4. *Lad G være en endelig undergruppe af $\text{GL}_n(k)$, og lad $F = (f_1, \dots, f_m)$ være en mængde af frembringere for $k[X_1, \dots, X_n]^G$. Da findes en bijektion mellem k^n/G og V_F .*

Bevis. Vi definerer en afbildning $\psi : k^n/G \rightarrow V_F$ ved, at

$$\psi(G\mathbf{x}) = (f_1(\mathbf{x}), \dots, f_m(\mathbf{x})).$$

Bemærk, at ψ er veldefineret, idet alle f_i er G -invariante og dermed konstante på baner. Vi viser først, at ψ er surjektiv. Lad $(b_1, \dots, b_n) \in V_F$. Da

I_F er det n -te eliminationsideal for J_F , er (b_1, \dots, b_m) en partikulær løsning til systemet

$$\begin{aligned} y_1 &= f_1(x_1, \dots, x_n) \\ &\vdots \\ y_m &= f_m(x_1, \dots, x_n). \end{aligned}$$

Vi påstår, at (b_1, \dots, b_m) kan udvides til et punkt $(a_1, \dots, a_n, b_1, \dots, b_m) \in \mathbf{V}(J_F)$. Hvis det er tilfældet, gælder $(f_1(a_1), \dots, f_n(a_n)) = (b_1, \dots, b_m)$, så ψ er surjektiv. Vi benytter et induktionsargument: Antag, at (b_1, \dots, b_m) er udvidet til

$$(a_{i+1}, \dots, a_n, b_1, \dots, b_m) \in \mathbf{V}(J_F \cap k[X_{i+1}, \dots, X_n, Y_1, \dots, Y_m]).$$

Fra eliminationsteorien ved vi, at $(a_{i+1}, \dots, a_n, b_1, \dots, b_m)$ kan udvides til et punkt $(a_i, a_{i+1}, \dots, a_n, b_1, \dots, b_m)$, hvis der findes en frembringer for idealet $J_F \cap k[X_i, \dots, X_n, Y_1, \dots, Y_m]$, hvis ledende koefficient, når polynomiet ses som polynomium i X_i , ikke nul evalueret i $(a_{i+1}, \dots, a_n, b_1, \dots, b_m)$. Vælg p_i som i lemma 4.3. Den ledende koefficient til X_i i p_i er konstant 1, og da $p_i \in J_F \cap k[X_i, \dots, X_n, Y_1, \dots, Y_m]$, kan p_i føjes til listen af frembringere for idealet, og påstanden følger ved induktion.

Tilbage er nu at vise, at ψ er injektiv. Antag, at $G\mathbf{x} \neq G\mathbf{y}$, og sæt $S = (G\mathbf{x} \cup G\mathbf{y}) \setminus \{\mathbf{y}\}$. Da G er endelig, er S endelig, så S er en affin varietet i k^n . Da $\mathbf{y} \notin S$, findes et polynomium $f \in \mathbf{I}(S)$ med $f(\mathbf{y}) \neq 0$. Betingelsen $f \in \mathbf{I}(S)$ betyder, at $f(A\mathbf{x}) = 0$ for alle $A \in G$, og at

$$f(A\mathbf{y}) = \begin{cases} f(\mathbf{y}) & \text{hvis } A\mathbf{y} = \mathbf{y} \\ 0 & \text{ellers} \end{cases}.$$

Sæt $g = R_G(f)$. Da er g i følge proposition 2.1 G -invariant, og da $f(A\mathbf{x}) = 0$ for alle $A \in G$, får vi, at

$$g(\mathbf{x}) = \frac{1}{|G|} \sum_{A \in G} (A \cdot f)(\mathbf{x}) = \frac{1}{|G|} \sum_{A \in G} f(A^{-1}\mathbf{x}) = 0.$$

Desuden ser vi, idet vi lader M betegne ordenen af stabilisatoren af \mathbf{y} i G , at

$$g(\mathbf{y}) = \frac{1}{|G|} \sum_{A \in G} (A \cdot f)(\mathbf{y}) = \frac{1}{|G|} \sum_{A \in G} f(A^{-1}\mathbf{y}) = \frac{1}{|G|} \sum_{A \in G} f(A\mathbf{y}) = \frac{M}{|G|} f(\mathbf{y}).$$

Da I stabiliserer \mathbf{y} , er $M > 1$, så $g(\mathbf{y}) \neq 0 = g(\mathbf{x})$. Idet g er G -invariant, er g på formen $g = h(f_1, \dots, f_m)$ for et polynomium $h \in k[Y_1, \dots, Y_m]$, så da $g(\mathbf{x}) \neq g(\mathbf{y})$, må der findes et i , så $f_i(\mathbf{x}) \neq f_i(\mathbf{y})$. Heraf følger, at $\psi(G\mathbf{x}) \neq \psi(G\mathbf{y})$, så ψ er injektiv. \square

Sætningen ovenfor viser, at k^n/G har en struktur som en affin varietet, nemlig som V_F . Bemærk, at denne struktur i følge korollar 4.2 op til isomorfi ikke afhænger af valget af F .

Litteratur

- [1] D.Cox, J. Little, D. O'Shea, *Ideals, Varieties, and Algorithms (Second Edition)*, Undergraduate Texts in Mathematics, Springer-Verlag, 1997.
- [2] J. C. Jantzen, *Algebra 2*, Notes, Aarhus University, 2001.