SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

# Ett försök att generalisera konjugatregeln

av

**Ulrika Söderberg**

2016 - No 17

# Ett försök att generalisera konjugatregeln

Ulrika Söderberg

---

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Samuel Lundqvist

2016

**Sammanfattning**

Konjugatregeln säger att $(x + y)(x - y) = x^2 - y^2$. Vi tittar på om denna kan generaliseras till flera variabler. I detta fall innebär det att formeln är symmetrisk, det vill säga att den inte påverkas av permutation utav variablerna, samt att den är invariant, det vill säga att formeln inte påverkas av vissa bestämda avbildningar. Men även att koefficienterna framför monomen i uttrycket följer att visst mönster. I arbetet presenteras bakomliggande teorier inom området och sedan testar vi om vår definition av generalisering gäller. Vi har arbetat med mindre exempel i Mathematica.

# 1 Inledning

*Konjugatregeln* är en polynomidentitet, nämligen att produkten $(x+y)(x-y)$ är lika med $x^2-y^2$. Om vi skriver om detta som $(x+(1)y)(x+(-1)y)$ ser vi att koefficienterna framför $y$ är 1 samt $-1$, vilka är lösningen till ekvationen $a^2=1$. Det blir då naturligt att fråga sig om det finns en motsvarande identitet när man istället tittar på koefficienter $(\epsilon^0,\ldots,\epsilon^{d-1})$ som är lösningarna till ekvationen $a^d=1$, d.v.s. produkten blir:

$$(x_0+x_1)(x_0+\epsilon x_1)\cdots(x_0+\epsilon^{d-1}x_1).$$

När vi till exempel har två variabler och $d=3$ får vi $(x_0+(1)x_1)(x_0+(e^{2\pi i/3})x_1)(x_0+(e^{4\pi i/3})x_1)$ som blir $x_0^3+x_1^3$, där $1, e^{2\pi i/3}$ och $e^{4\pi i/3}$ är lösningarna till ekvationen $a^3=1$. Om vi istället tar tre variabler och lösningarna till $a^2=1$ framför $x_1$ och $x_2$ får vi:

$$(x_0+x_1+x_2)(x_0+x_1-x_2)(x_0-x_1+x_2)(x_0-x_1-x_2)=$$
$$x_0^4+x_1^4+x_2^4-2x_0^2x_1^2-2x_0^2x_2^2-2x_1^2x_2^2.$$

Uttrycket är inte lika enkelt som för två variabler eller som när vi använde lösningarna till $a^3=1$. Vi kan dock se att uttrycket är invariant vid permutation av variablerna $x_0, x_1$ samt $x_2$ och är därför symmetriskt.

I sats 3.2 bevisar vi polynomidentiteten $(x_0+x_1)(x_0+\epsilon x_1)\cdots(x_0+\epsilon^{d-1}x_1)=x_0^d-(-1)^dx_1^d$ och man kan då säga att konjugatregeln är specialfallet $d=2$ av denna identitet. Nästa steg är att försöka generalisera detta till flera variabler.

Produkten kan skrivas som:

$$f_{d,n}(x_0,\ldots,x_n)=\prod(x_0+\epsilon_1x_1+\cdots+\epsilon_nx_n)$$

där $\epsilon_i$ varierar över alla lösningar till ekvationen $a^d=1$ och där antal variabler är $n+1$. Den generalisering som vi har tittat på är att symmetri gäller för $f_{d,n}(x_0,\ldots,x_n)$, det vill säga att formeln inte påverkas av permutation utav index på variablerna och att uttrycket även är invariant under avbildningen $x_i\to\epsilon x_i$, där $\epsilon$ är en primitiv enhetsrot. Vi tittar även på att koefficienterna framför monomen i formeln följer ett visst mönster.

Vi tittar på vilka egenskaper produkten $f_{d,n}(x_0,\ldots,x_n)$ har. Först tar vi upp tidigare teorier för att sedan visa att uttrycket $f_{d,n}(x_0,\ldots,x_n)$ är invariant under avbildningen $x_i\to\epsilon x_i$. Vi arbetar i kroppen $\mathbb{C}$, de komplexa talen, samt i de ändliga kropparna $\mathbb{Z}_p$, där $d\mid p-1$. Med hjälp av invarians samt faktorsatsen visar vi vilka egenskaper koefficienterna framför variablerna $x_1^{d^n},\ldots,x_n^{d^n}$ samt monomen $x_0^{\alpha_0}\cdot x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ har, där $0\le\alpha_i<d^n$.

Vi gör beräkningarna på mindre $n$ och $d$ i Mathematica [4] för att testa de olika påståendena och teorierna om egenskaperna (se Apendix A).

Vi har inte lyckats hitta en liknande polynomidentitet som den för konjugatregeln, men vi visar i sats 3.5 att i $f_{d,n}(x_0, \ldots, x_n)$, när $n \geq 2$, är koefficienterna framför monomen $x_0^{\alpha_0} \cdot x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ noll då $d$ inte delar $\alpha_i$. Vi tittar även på tidigare forskning inom området för att se om något samband finns mellan den produkt vi kommer fram till och resultatet från den tidigare forskningen [2].

# 2 Bakomliggande teori

**Definition 2.1** (Enhetsrötter)**.** En $d$:te enhetsrot är en lösning till ekvationen $x^d = 1$, där $d$ är ett positivt heltal. I polär form skrivs enhetsrötterna som:

$$e^{\frac{2k\pi i}{d}} = \cos\tfrac{2k\pi}{d} + i \sin\tfrac{2k\pi}{d}, \qquad k = 0, \ldots, d-1.$$

En $d$:te enhetsrot kallas primitiv om den inte är en $k$:te enhetsrot för något $k < d$, d.v.s.

$$x^k \neq 1 \qquad (k = 1, 2, 3, \ldots, d-1)$$

**Definition 2.2** (Invariant, se [3])**.** $G$ är en ändlig grupp av automorfismer som verkar på $k[x_0, \ldots, x_n]$. Ett polynom $f(x) \in k[x_1, \ldots, x_n]$ är invariant under verkan av $G$ om:

$$f(x) = f(\alpha x)$$

för alla $\alpha \in G$.

**Sats 2.1** (Faktorsatsen, se [1])**.** *Låt $k$ vara en kropp och anta att $f(x)$ är ett polynom i $k[x]$. Då är $x - \alpha$ en delare till $f(x)$ i $k[x]$ om och endast om $f(\alpha) = 0$ i $k$.*

*Bevis.* Anta att $x - \alpha$ är en delare till $f(x)$ så att

$$f(x) = (x - \alpha)g(x) \quad \text{i } k[x] \ .$$

Sätt $x = \alpha$ i bägge led och vi får följande:

$$f(\alpha) = (\alpha - \alpha)g(\alpha) = 0 \cdot g(\alpha) = 0.$$

$\alpha$ är därför ett nollställe. Anta nu att $f(\alpha) = 0$ i $k$. Då finns det polynom $q(x)$ samt $r(x)$ i $k[x]$ så att

$$f(x) = (x - \alpha)q(x) + r(x),$$

där antingen $\deg r(x) < \deg(x - \alpha)$ eller $r(x) = 0$. Om vi nu sätter $x = \alpha$ (där $f(\alpha) = 0$) får vi följande:

$$0 = f(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) = r(\alpha).$$

Om $\deg r(x) < \deg(x - \alpha)$ så måste $\deg r(x)$ vara noll och $r(x)$ är därför en konstant $C$. Vi har att $r(\alpha) = C = 0$. Därför måste $r(x) = 0$, vilket ger oss att $x - \alpha$ är en delare till $f(x)$.

□

**Sats 2.2** (se [1]). *Om $k$ är en kropp och $f(x)$ är ett polynom av grad $n \geq 1$ i $k[x]$ så har ekvationen $f(x) = 0$ som mest $n$ rötter i $k$.*

*Bevis.* Anta att ekvationen har $m$ distinkta rötter $\alpha_1, \alpha_2, \ldots, \alpha_m$ i $k$. Enligt faktorsatsen så delar $x - \alpha_1, x - \alpha_2, \ldots, x - \alpha_m$, $f(x)$ och är alla irreducibla. Faktoriseringen av $f(x)$ i $k[x]$ blir då följande:

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m)g(x)$$

för något polynom $g(x)$ i $k[x]$. Då koefficienterna finns i kroppen $k$ så är graden av en produkt summan av graderna på faktorerna, därav är graden av $f(x)$ som minst $m$. Detta innebär att antal rötter av $f(x) = 0$ är som flest $n$.

□

**Sats 2.3** (Lagranges sats, se [3]). *Om $G$ är en ändlig grupp av ordning $n$ och $H$ är en delgrupp av ordning $m$, så delar $m$ $n$.*

*Bevis.* Vi vet från egenskaper hos delgrupper att vänstersidoklassen $aH$ har samma antal element som $H$, det vill säga $|aH| = |H|$. Vi vet även att vänstersidoklasser antingen är lika eller disjunkta vilket innebär att varje element i $G$ tillhör exakt en vänstersidoklass.

Vi låter $k$ vara antal väntersidoklasser, $a_1H, \ldots, a_kH$, av $G$ vi har då att $|G| = |a_1H| + \cdots + |a_kH|$ vilket ger $|G| = k|H|$ och $m$ delar därför $n$.

□

**Sats 2.4** (se [1]). *För $d, p > 1$ så innehåller den multiplikativa gruppen i $\mathbb{Z}_p$ en primitiv $d$:te enhetsrot om och endast om $d$ delar $p - 1$.*

*Bevis.* Om $\alpha$ är en primitiv $d$:te enhetsrot i $\mathbb{Z}_p$ så är mängden

$$\lambda = \{1, \alpha, \ldots, \alpha^{d-1}\}$$

en cyklisk delgrupp, se [1], $H$ av den multiplikativa gruppen $G_{p-1}$ av $\mathbb{Z}_p$. Enligt Lagranges sats så delar ordningen av $H$ ordningen av $G_{p-1}$. Eftersom $G_{p-1}$ har $p - 1$ element delar $d$, $p - 1$. $G_{p-1}$ är en cyklisk grupp, se [1]. Låt $\beta$ vara en generator till denna grupp så att:

$$G_{p-1} = \{1, \beta, \beta^2, \ldots, \beta^{p-2}\}$$

där $\beta^{p-1} = 1$. Låt $d > 1$ vara ett tal som delar $p - 1$ och definiera

$$\alpha = \beta^{(p-1)/d}$$

då har vi att $\alpha^d = 1$. För alla $0 < k < d$ har vi att $k\frac{p-1}{d} < p-1$

$$\alpha^k = \beta^{k(p-1)/d} \neq 1$$

vilket visar att $\alpha$ är en primitiv $d$:te enhetsrot.

□

**Exempel 1.** Om vi har den multiplikativa gruppen $\mathbb{Z}_{31}$ så har vi att $p-1 = 31-1 = 30$. I $\mathbb{Z}$ delar följande tal $30 : 1, 2, 3, 5, 6, 10, 15, 30$. Om vi väljer ett tal som delar 30, låt säga 6 så har vi att $d = 6$. Vi har då följande lösningar för $a^6 = 1$:

$$1^6 = 1,$$
$$5^6 = 1,$$
$$6^6 = 1,$$
$$25^6 = 1,$$
$$26^6 = 1,$$
$$30^6 = 1.$$

Det vill säga när $d = 6$ har vi sex lösningar till ekvationen $a^d = 1$. Enhetsroten 6 är den enda primitiva enhetsroten, detta då för alla $k < d$ så är $6^k \neq 1$. Eftersom 31 är ett primtal så är $\mathbb{Z}_{31}$ en kropp. Enligt sats 2.2 så har därför polynomet $x^6 - 1 = 0$ i $\mathbb{Z}_{31}$ maximalt 6 stycken rötter, när alla rötter är distinkta. Om vi tar rötterna och skapar en produkt av de linjära faktorerna får vi följande:

$$(a-1)(a-5)(a-6)(a-25)(a-26)(a-30) = a^6 - 31a^5 + 31a^4 - 31a^3 - 31a + 30$$

vilket i $\mathbb{Z}_{31}$ ger $a^6 - 1$ eller att $a^6 = 1$

Om vi istället väljer $d = 7$ där 7 inte delar 30 har vi endast en lösning till ekvationen $a^d = 1$ vilken är

$$1^7 = 1.$$

# 3 Resultat

## 3.1 Beteckningar

Vi befinner oss i ringen $k[x_0, \ldots, x_n]$ där $k$ är de komplexa talen $\mathbb{C}$ eller en ändlig ring $\mathbb{Z}_p$, där $d \mid p-1$. Vi definierar:

$$f_{d,n}(x_0, \ldots, x_n) = \prod_{\substack{0 \leq i_j \leq d-1 \\ j=1,\ldots,n}} (x_0 + \epsilon^{i_1} x_1 + \cdots + \epsilon^{i_n} x_n),$$

där $\epsilon$ är en $d$:te enhetsrot.

## 3.2 Invarians

**Lemma 1** (Invarians)**.** *Polynomet $f_{d,n}(x_0, \ldots, x_n)$ är invariant under avbildningen $x_i \to \epsilon x_i$ där $0 \leq i \leq n$.*

*Bevis.* Efter avbildningen $x_0 \to \epsilon x_0$ får vi produkten:

$$\prod_{\substack{0 \leq i_j \leq d-1 \\ j=1,\ldots,n}} (\epsilon x_0 + \epsilon^{i_1} x_1 + \cdots + \epsilon^{i_n} x_n).$$

Eftersom $1 = \epsilon^d$ kan vi lägga till $\epsilon^d$ där $i_j = 0$ för alla $1 \leq j \leq n$ och sedan bryta ut $\epsilon$ ur varje parentes och vi får:

$$\epsilon^{d^n} \cdot \prod_{\substack{0 \leq i_j \leq d-1 \\ j=1,\ldots,n}} (x_0 + \epsilon^{i_1} x_1 + \cdots + \epsilon^{i_n} x_n).$$

Vi vet att $\epsilon^d = 1$ vilket ger att $\epsilon^{d^n} = 1$. Vi har alltså visat att $f_{d,n}(x_0, \ldots, x_n) = f_{d,n}(\epsilon x_0, \ldots, x_n)$

Vi ska nu visa att produkten är invariant under avbildningen $x_i \to \epsilon x_i$ där $1 \leq i \leq n$. Om vi väljer $i = 1$ så får vi följande uttryck för avbildningen:

$$\prod_{\substack{0 \leq i_j \leq d-1 \\ j=1,\ldots,n}} (x_0 + \epsilon^{i_1}(\epsilon x_1) + \cdots + \epsilon^{i_n} x_n),$$

som vi kan skriva som:

$$\prod_{\substack{0 \leq i_j \leq d-1, 1 \leq i_1+1 \leq d \\ j=2,\ldots,n}} (x_0 + \epsilon^{i_1+1}(x_1) + \cdots + \epsilon^{i_n} x_n). \tag{1}$$

Eftersom $\epsilon^{d-1}(\epsilon) = \epsilon^d = 1 = \epsilon^0$ så är (1) lika med

$$\prod_{\substack{0 \leq i_j \leq d-1 \\ j=1,\ldots,n}} (x_0 + \epsilon^{i_1} x_1 + \cdots + \epsilon^{i_n} x_n).$$

Samma princip kan tillämpas på alla $x_i$ där $1 \leq i \leq n$.

□

**Exempel 2.** Vi har när $n = 1$ och $d = 3$, där enhetsrötterna är $\epsilon^0 = 1$, $\epsilon^1$ och $\epsilon^2$:

$$(x_0 + x_1)(x_0 + \epsilon^1 x_1)(x_0 + \epsilon^2 x_1),$$

vilket efter avbildningen $x_0 \to \epsilon x_0$ ger

$$(\epsilon x_0 + x_1)(\epsilon x_0 + \epsilon^1 x_1)(\epsilon x_0 + \epsilon^2 x_1).$$

vi lägger till $\epsilon^3$, där vi har 1 som koefficient och får:

$$\begin{aligned}(\epsilon x_0 + \epsilon^3 x_1)(\epsilon x_0 + \epsilon^1 x_1)(\epsilon x_0 + \epsilon^2 x_1) = \\ \epsilon^3(x_0 + \epsilon^2 x_1)(x_0 + x_1)(x_0 + \epsilon^1 x_1) = \\ (x_0 + x_1)(x_0 + \epsilon^1 x_1)(x_0 + \epsilon^2 x_1)\end{aligned}$$

**Sats 3.1.** *Koefficienten framför alla monom $x_0^a x_1^b$ i $f_{d,1}(x_0, x_1)$ är lika med* 0 *när $1 \leq a, b \leq d - 1$.*

*Bevis med hjälp av invariantteori:* Vi har att

$$f_{d,1}(x_0, x_1) = c_0 x_0^d + c_1 x_0^{d-1} x_1 + \cdots + c_{d-1} x_0 x_1^{d-1} + c_d x_1^d$$

och om vi avbildar $x_0 \to \epsilon x_0$, där $\epsilon$ är en primitiv $d$:te enhetsrot, får vi följande:

$$\begin{aligned}f_{d,1}(\epsilon x_0, x_1) &= c_0(\epsilon x_0)^d + c_1(\epsilon x_0)^{d-1} x_1 + \cdots + c_{d-1}(\epsilon x_0) x_1^{d-1} + c_d x_1^d \\ &= c_0 \epsilon^d x_0^d + c_1 \epsilon^{d-1} x_0^{d-1} x_1 + \cdots + c_{d-1} \epsilon x_0 x_1^{d-1} + c_d x_1^d.\end{aligned}$$

Vi har att $\epsilon^d = 1$ och får:

$$= c_0 x_0^d + c_1 \epsilon^{d-1} x_0^{d-1} x_1 + \cdots + c_{d-1} \epsilon x_0 x_1^{d-1} + c_d x_1^d.$$

Från Lemma 2 vet vi att $f_{d,1}(x_0, x_1) = f_{d,1}(\epsilon x_0, x_1)$ och får att

$$\begin{aligned}c_0 x_0^d + c_1 x_0^{d-1} x_1 + \cdots + c_{d-1} x_0 x_1^{d-1} + c_d x_1^d = \\ c_0 x_0^d + c_1 \epsilon^{d-1} x_0^{d-1} x_1 + \cdots + c_{d-1} \epsilon x_0 x_1^{d-1} + c_d x_1^d.\end{aligned}$$

Vi får dessa likheter mellan koefficienterna framför monomen $x_0^a x_1^b$;

$$c_1 \epsilon^{d-1} = c_1, \ldots, c_{d-1}\epsilon = c_{d-1}.$$

Vi har att $\epsilon^k \neq 1 \quad \forall \quad 1 \leq k < d$, eftersom $\epsilon$ är en primitiv $d$:te enhetsrot.
Om vi antar att $c_i \neq 0 \quad \forall \quad 1 \leq i \leq d - 1$ så får vi då att

$$c_i \epsilon^k = c_i \Rightarrow \epsilon^k = 1,$$

men eftersom vi vet att $\epsilon^k \neq 1$ då $1 \leq k < d$ har vi en motsägelse. Därför måste $c_i$ vara 0 och alla koefficienter framför alla monom $x_0^a x_1^b$ i $f_{d,1}(x_0, x_1)$ måste vara 0. □

*Bevis med hjälp av faktorsatsen:* Vi har att $f_{d,1}(x_0, x_1) = (x_0+x_1)(x_0+\epsilon x_1)\cdots(x_0+\epsilon^{d-1}x_1)$, om vi bryter ut $x_1$ får vi följande:

$$x_1^d(\frac{x_0}{x_1}+1)(\frac{x_0}{x_1}+\epsilon)\cdots(\frac{x_0}{x_1}+\epsilon^{d-1}).$$

Vi gör variabelbytet $-a = x_0/x_1$ och får:

$$x_1^d(-a+1)(-a+\epsilon)\cdots(-a+\epsilon^{d-1}).$$

om vi multiplicerar med $(-1)^d$ får vi:

$$x_1^d(a-1)(a-\epsilon)\cdots(a-\epsilon^{d-1}).$$

Vi vet att $1, \epsilon, \epsilon^2, \ldots, \epsilon^{d-1}$ är lösningar till ekvationen $a^d = 1$ eller $a^d - 1 = 0$, vi kan då använda faktorsatsen som ger att $(a-1)(a-\epsilon)\cdots(a-\epsilon^{d-1}) = a^d - 1$ vi får därför att:

$$x_1^d(a^d-1).$$

Vi byter tillbaka till $a = -(x_0/x_1)$ och får:

$$x_1^d((-(x_0/x_1))^d - 1).$$

Vi kan då multiplicera med $(-1)^d$ och får:

$$x_1^d(\frac{x_0^d}{x_1^d} - (-1)^d 1) = (x_0^d - (-1)^d x_1^d).$$

Vi kan se att beviset med hjälp av faktorsatsen bevisar sats 3.1 på ett enklare sätt än med hjälp av invarians.

□

**Exempel 3.** Om vi har $n = 1$ och $d = 3$ får vi följande:

$$\begin{aligned}
f_{3,1}(x_0, x_1) = (x_0 + x_1)(x_0 + \epsilon x_1)(x_0 + \epsilon^2 x_1) = \\
x_1^3(\frac{x_0}{x_1}+1)(\frac{x_0}{x_1}+\epsilon)(\frac{x_0}{x_1}+\epsilon^2) = \\
x_1^3(-a+1)(-a+\epsilon)(-a+\epsilon^2) = \\
x_1^3(a-1)(a-\epsilon)(a-\epsilon^2) = \\
x_1^3(a^3-1) = \\
x_1^3(-\frac{x_0}{x_1}-1) = x_1^3((-1)^3(-\frac{x_0}{x_1}) - (-1)^3\cdot 1) = \\
x_1^3(\frac{x_0^3}{x_1^3}-1) = x_0^3 - x_1^3
\end{aligned}$$

**Sats 3.2.** *Polynomet $f_{d,n}(x_0, \ldots, x_n)$ är ett element i delringen $k[x_0^d, x_1^d, \ldots, x_n^d]$.*

*Bevis med hjälp av invariantteori:* Vi har produkten:

$$f_{d,n}(x_0, \ldots, x_n) = \prod_{\substack{0 \leq i_j \leq d-1 \\ j=1,\ldots,n}} (x_0 + \epsilon^{i_1} x_1 + \cdots + \epsilon^{i_n} x_n).$$

Om vi avbildar alla $x_0 \to \epsilon x_0$ får vi följande produkt:

$$f_{d,n}(\epsilon x_0, \ldots, x_n) = \prod_{\substack{0 \leq i_j \leq d-1 \\ j=1,\ldots,n}} (\epsilon x_0 + \epsilon^{i_1} x_1 + \cdots + \epsilon^{i_n} x_n).$$

Samma avbildning, $x_i \to \epsilon x_i$ där $1 \leq i \leq n$, kan göras för varje $i$.

För alla monom $x_0^{\alpha_0} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ där $0 \leq \alpha_i < d^n$ och $\alpha_i \neq 0$ har vi en koefficient $C$. Efter avbildningen får vi koefficienten $C\epsilon^{\alpha_i}$. Vi har enligt lemma 1 att $f_{d,n}(x_0, \ldots, x_n) = f_{d,n}(\epsilon x_0, \ldots, x_n)$ och får likheten mellan koefficienterna $C = C\epsilon^{\alpha_i}$. Då har vi att $C = C\epsilon^{\alpha_i}$ om $C = 0$ eller om $d|\alpha_i$.

□

**Exempel 4.** När $n = 3$, $d = 2$ har vi:

$f_{2,3} = (x_0 + x_1 + x_2 + x_3) \cdot (x_0 + x_1 + x_2 - x_3) \cdot (x_0 + x_1 - x_2 + x_3) \cdot (x_0 + x_1 - x_2 - x_3) \cdot$
$(x_0 - x_1 + x_2 + x_3) \cdot (x_0 - x_1 + x_2 - x_3) \cdot (x_0 - x_1 - x_2 + x_3) \cdot (x_0 - x_1 - x_2 - x_3)$
$= x_0^8 - 4x_0^6x_1^2 + 6x_0^4x_1^4 - 4x_0^2x_1^6 + x_1^8 - 4x_0^6x_2^2 +$
$4x_0^4x_1^2x_2^2 + 4x_0^2x_1^4x_2^2 - 4x_1^6x_2^2 + 6x_0^4x_2^4 +$
$4x_0^2x_1^2x_2^4 + 6x_1^4x_2^4 - 4x_0^2x_2^6 - 4x_1^2x_2^6 + x_2^8 -$
$4x_0^6x_3^2 + 4x_0^4x_1^2x_3^2 + 4x_0^2x_1^4x_3^2 - 4x_1^6x_3^2 +$
$4x_0^4x_2^2x_3^2 - 40x_0^2x_1^2x_2^2x_3^2 + 4x_1^4x_2^2x_3^2 + 4x_0^2x_2^4x_3^2 +$
$4x_1^2x_2^4x_3^2 - 4x_2^6x_3^2 + 6x_0^4x_3^4 + 4x_0^2x_1^2x_3^4 + 6x_1^4x_3^4 +$
$4x_0^2x_2^2x_3^4 + 4x_1^2x_2^2x_3^4 + 6x_2^4x_3^4 - 4x_0^2x_3^6 - 4x_1^2x_3^6 -$
$4x_2^2x_3^6 + x_3^8$

Vi kan se att varje monom är ett element i delringen $\mathbb{C}[x_0^2, x_1^2, x_2^2, x_3^2]$ och att koefficienterna är 0 framför alla monom $x^{\alpha_i}$ om för något $i$ gäller att $d$ inte delar $\alpha_i$.

## 3.3 Symmetriegenskaper

**Sats 3.3.** *Låt $n \geq 2$ och $d \geq 2$. Då gäller att $f_{d,n}(x_0, \ldots, x_n)$ är ett element i delringen $k[x_0^d, \ldots, x_n^d]$ och $k$ är $\mathbb{C}$ eller $\mathbb{Z}_p$ där $d \mid p-1$. Koefficienten framför $x_n^{d^n}$ kommer att vara 1 för både jämna och udda $d$.*

*Bevis.* Koefficienten $c_d$ framför variablerna $x_1^{d^n}, \ldots, x_n^{d^n}$ är följande:

$$c_d = 1^{d^n} \cdot \epsilon^{d^n} \cdot (\epsilon^2)^{d^n} \cdots (\epsilon^{d-1})^{d^n} = (\epsilon^{\frac{(d-1)}{2} \cdot d})^{\frac{d^n}{d}} = (\epsilon^{\frac{(d-1)}{2}})^{d^n} = \epsilon^{\frac{d^{n+1}-d^n}{2}}.$$

Vi vet att $\epsilon^k$ är lika med 1 då $k > 2$ och $k$ är ett jämnt tal eller då $k$ är en multipel av $d$.
När $d$ är udda, låt $d = 2k+1$,

$$(\epsilon^{\frac{2k+1-1}{2}})^{d^n} = \epsilon^{k \cdot d^n}$$

$c_d$ är därför 1 för udda $d$.
När $d$ är jämn, låt $d = 2k$ och låt

$$c_d = \epsilon^{\frac{2^{n+1}k^{n+1}-2^n k^n}{2}} = \epsilon^{2^n k^{n+1} - 2^{n-1}k^n} = \frac{\epsilon^n k^{n-1}}{\epsilon^{2^{n-1}k^n}}$$

Eftersom $2^n k^{n-1}$ och $2^{n-1}k^n$ är ett jämna tal, när $n \leq 2$ så har vi att $\epsilon^{2^n k^{n-1}} = 1$ och $\epsilon^{2^{n-1}k^n} = 1$.

□

Vi har, för $n = 1$, visat i sats 3.1 att för udda $d$ är koefficienten framför $x_1$ lika med 1, vi vet då att för udda $d$ är

$$f_{d,1}(x_0, x_1) = x_0^d + x_1^d = x_1^d + x_0^d = f(x_1, x_0)$$

Uttrycket $f_{d,1}(x_0, x_1)$ är därför symmetriskt för udda $d$.
Vi har, för $n > 1$, uttrycket

$$f_{d,n}(x_0, \ldots, x_n) = \prod_{\substack{0 \leq a_j \leq d-1 \\ j=1,\ldots,n}} (x_0 + \epsilon^{a_1} x_1 + \cdots + \epsilon^{a_n} x_n).$$

Vi kan multiplicera varje faktor med $\epsilon^{d-a_1}$

$$\prod_{\substack{0 \leq a_j \leq d-1 \\ j=1,\ldots,n}} \epsilon^{d-a_1}(x_0 + \epsilon^{a_1} x_1 + \cdots + \epsilon^{a_n} x_n) =$$

$$\prod_{\substack{0 \leq a_j \leq d-1 \\ j=1,\ldots,n}} (\epsilon^{d-a_1} x_0 + \epsilon^{d-a_1}\epsilon^{a_1} x_1 + \cdots + \epsilon^{d-a_1}\epsilon^{a_n} x_n) =$$

$$\prod_{\substack{0 \leq a_j \leq d-1 \\ j=1,\ldots,n}} (\epsilon^{d-a_1} x_0 + \epsilon^{d-a_1+a_1} x_1 + \cdots + \epsilon^{d-a_1+a_n} x_n). \tag{2}$$

Vi har att $\epsilon^{d-a_1+a_1} = \epsilon^d$ och $\epsilon^d = 1$.Vi vet att $1 \leq d - a_1 \leq d$ och vi kan skriva om detta som

$$1 \leq d - a_1 \leq d \Rightarrow 1 - d \leq -a_1 \leq 0 \Rightarrow 0 \leq a_1 \leq d - 1$$

och (2) ger:

$$\prod_{\substack{0 \leq a_j \leq d-1 \\ j=1,\ldots,n}} (\epsilon^{a_1} x_0 + x_1 + \cdots + \epsilon^{a_1+a_n} x_n).$$

Låt $j = \alpha_i$ för $0 \leq i \leq n$ då vet vi att den ordnade mängden $(a_{\alpha_1}, a_{\alpha_2}, \ldots, a_{\alpha_n})$ endast förekommer en gång i produkten $f_{d,n}(x_0, \ldots, x_n)$. Låt $(a_{\beta_1}, \ldots, a_{\beta_n})$ vara en annan ordnad mängd. När vi har $a_{\alpha_1} + a_{\alpha_i}$ kan vi anta att den ordnade mängden $(a_{\alpha_1}, a_{\alpha_1} + a_{\alpha_2}, a_{\alpha_1} + a_{\alpha_3}, \ldots, a_{\alpha_1} + a_{\alpha_n})$ endast förekommer en gång i produkten (3.3) vi sätter då:

$$(a_{\alpha_1}, a_{\alpha_1}+a_{\alpha_2}, a_{\alpha_1}+a_{\alpha_3}, \ldots, a_{\alpha_1}+a_{\alpha_n}) = (a_{\beta_1}, a_{\beta_1}+a_{\beta_2}, a_{\beta_1}+a_{\beta_3}, \ldots, a_{\beta_1}+a_{\beta_n})$$

eftersom vi har likheten $a_{\alpha_1} = a_{\beta_1}$ följer resterande likheter, exempelvis $a_{\alpha_1} + a_{\alpha_2} = a_{\beta_1} + a_{\beta_2} \Rightarrow a_{\alpha_2} = a_{\beta_2}$. Uttrycket $f_{d,n}(x_0, \ldots, x_n)$ är därför symmetriskt.

# 4 Tidigare forskning

En *Waring decomposition* av ett polynom är ett uttryck av polynomet som en summa potenser av linjära former, där antalet potenser är de lägsta möjliga. I tidigare forskning [2] har man bland annat visat vilka koefficienterna framför monomen i denna summa av potenser är.

**Sats 4.1.** *Låt $d = d_0 + \cdots + d_n$ där $0 < d_0 \leq \ldots \leq d_n$. Låt $\epsilon_i$ vara en $d_i + 1$ enhetsrot för $i = 1, \ldots, n$. Då gäller det att:*

$$x_0^{d_0} \cdot x_1^{d_1} \cdots x_n^{d_n} = \frac{1}{C} \sum_{\substack{0 \leq a_i \leq d_i \\ i=1,\ldots,n}} (x_0 + \epsilon_1^{a_1} x_1 + \cdots + \epsilon_n^{a_n} x_n)^d (\epsilon_1^{a_1} \cdots \epsilon_n^{a_n}),$$

*där*

$$C = \binom{d}{d_0, \ldots, d_n} (d_1 + 1) \cdots (d_n + 1),$$

*och där $\binom{d}{d_0, \ldots, d_n}$ är multinomialkoefficienten $d!/(d_0! \cdots d_n!)$.*

*Bevis.* Se [2] □

Vi ska nu bevisa sats 4.1 i specialfallet där alla $d_i = 1$

**Sats 4.2.** *Låt $d_0 = \cdots = d_n = 1$, då är $d = n+1$. Då gäller det att*

$$(n+1)!2^n x_0 \cdots x_n = \sum_{\substack{0 \le a_i \le 1 \\ i=1,\ldots n}} (x_0 + (-1)^{a_1} x_1 + \cdots + (-1)^{a_n} x_n)^{n+1} (-1)^{a_1} \cdots (-1)^{a_n}$$

*Bevis.* Om vi betraktar monomet $x^m = x_0^{m_0} \cdots x_n^{m_n}$ där $m_0 + \ldots + m_n = n+1$ har vi då att koefficienten framför $x^m$ i utvecklingen av

$$\sum_{\substack{0 \le a_i \le 1 \\ i=1,\ldots,n}} (x_0 + (-1)^{a_1} x_1 + \cdots + (-1)^{a_n} x_n)^{n+1} (-1)^{a_1} \cdots (-1)^{a_n}$$

är lika med

$$\binom{n+1}{m_0, \ldots, m_n} \cdot \sum_{\substack{0 \le a_i \le 1 \\ i=1,\ldots,n}} ((-1)^{a_1(m_1+1)} \cdots (-1)^{a_n(m_n+1)}) =$$

$$\binom{n+1}{m_0, \ldots, m_n} \cdot \sum_{0 \le a_1 \le 1} (-1)^{a_1(m_1+1)} \cdots \sum_{0 \le a_n \le 1} (-1)^{a_n(m_n+1)}$$

Om $m_i$ är udda så är

$$\sum_{0 \le a_i \le 1} (-1)^{a_i(m_i+1)} = \sum_{0 \le a_i \le 1} 1^{a_i} = 1 + 1 = 2.$$

Om $m_i$ är jämnt så är

$$\sum_{0 \le a_i \le 1} (-1)^{a_1(m_i+1)} = \sum_{0 \le a_i \le 1} (-1)^{a_i} = 1 + (-1) = 0.$$

Alltså har $x_0^{m_0} \cdots x_n^{m_n}$ nollskild koefficient i

$$\sum_{0 \le a_i \le 1 i=1,\ldots,n} (x_0 + (-1)^{a_1} x_1 + \cdots + (-1)^{a_n} x_n)^{n+1} (-1)^{a_1} \cdots (-1)^{a_n}$$

om och endast om alla $m_i$ är udda. Vi vet att $m_i$ är udda $(i = 1, \ldots n)$ eftersom $m_1 + \cdots + m_n \le n+1$ så måste $m_i = 1$ för $i = 1, \ldots n$, från vilket det följer att även $m_0 = 1$. Vi har visat att

$$\sum_{\substack{0 \le a_i \le 1 \\ i=1,\ldots,n}} (x_0 + (-1)^{a_1} x_1 + \cdots + (-1)^{a_n} x_n)^{n+1} (-1)^{a_1} \cdots (-1)^{a_n} =$$

$$(n+1)! \cdot 2^n \cdot x_0 x_1 \cdots x_n$$

□

### 4.1 Samband

Om vi har produkten $f_{d,n}(x_0, \ldots, x_n)$ som vi definierat tidigare kan vi skriva den som följande:

$$f_{d,n}(x_0, \ldots x_n) = \prod_{\substack{0 \leq a_j \leq d-1 \\ j=1,\ldots,n}} (x_0 + \epsilon^{a_1} x_1 + \cdots + \epsilon^{a_n} x_n) = y_0 y_1 \cdots y_{d^n-1}.$$

Vi kan nu skriva om faktorerna som summan från sats 4.1:

$$y_0^1 \cdot y_1^1 \cdots y_{d^n-1}^1 =$$
$$\frac{1}{C} \sum_{\substack{0 \leq a_i \leq 1 \\ i=1,\ldots,d^n-1}} (y_0 + (-1)^{a_1} y_1 + \cdots + (-1)^{a_{d^n-1}} y_{d^n-1})^{d^n} ((-1)^{a_1} \cdots (-1)^{a_{d^n-1}}),$$

där $C = d^n! \cdot 2^{d^n-1}$. Omskrivningen av $f_{d,}(x_0, \ldots, x_n)$ vi gjort med hjälp av 4.1 kan vara ett sätt att bestämma koefficienterna framför monomen i uttrycket.

## 5 Avslutande diskussion

Det vi har visat är att $f_{d,n}(x_0, \ldots, x_n)$ är invariant under både avbildning på en primitiv enhetsrot samt under permutation av variablerna. Detta innebär att vi har ett symmetriskt uttryck. Vi har även visat att när $n = 1$ då är koefficienterna framför variabeln $x_1^d$ lika med 1 för udda $d$ och lika med $-1$ för jämna $d$, men att för $n > 1$ är koefficienten framför $x_i^d$ där $1 \leq i \leq n$ lika med 1 för alla $d$. Vi har även visat att $f_{d,n}(x_0, \ldots, x_n)$ är ett element i delringen $k[x_0^d, \ldots, x_n^d]$. Det som återstår är att bestämma koefficienterna framför monomen $x_0^{\alpha_1} \cdots x_n^{\alpha_n}$ där $d$ delar $\alpha_i$. Nyligen har Christian Gottlieb, Stockholms universitet, visat att dessa koefficienter är heltal, men det kvarstår därför att hitta vilka dessa heltal är.

# Referenser


[1] N. L. Biggs, Discrete mathematics (2002).

[2] W. Buczynska, J. Buczynski och Z. Teitler. Waring decompositions of monomials, Journal of Algebra 378 (2013) s. 45-57.

[3] R. P. Grimaldi. Discrete and Combinatorial mathematics. An pplies Intruduction. (1999) s. 714.

[4] Wolfram Research, Inc., Mathematica, Version 10.3, Champaign, IL (2015).

# A Appendix

Beräkningar gjorda i Mathematica. Vi har använt "ComplexExpand" för beräkningarna och i fallen med fler variabler även "Simplify".

$$(-\mathrm{x}_0 - 1)(-\mathrm{x}_0 - e^{-\frac{2i\pi}{5}})(-\mathrm{x}_0 - e^{\frac{2i\pi}{5}})(-\mathrm{x}_0 - e^{-\frac{4i\pi}{5}})(-\mathrm{x}_0 - e^{\frac{4i\pi}{5}}) = -\mathrm{x}_0^5 - 1$$

$$(\mathrm{x}_0 + \mathrm{x}_1)\left(\mathrm{x}_0 + e^{-\frac{2i\pi}{5}}\mathrm{x}_1\right)\left(\mathrm{x}_0 + e^{\frac{2i\pi}{5}}\mathrm{x}_1\right)\left(\mathrm{x}_0 + e^{-\frac{4i\pi}{5}}\mathrm{x}_1\right)\left(\mathrm{x}_0 + e^{\frac{4i\pi}{5}}\mathrm{x}_1\right) = \mathrm{x}_0^5 + \mathrm{x}_1^5$$

$$(\mathrm{x}_0 - \mathrm{x}_1)(\mathrm{x}_0 + \mathrm{x}_1)\left(\mathrm{x}_0 + e^{-\frac{i\pi}{3}}\mathrm{x}_1\right)\left(\mathrm{x}_0 + e^{\frac{i\pi}{3}}\mathrm{x}_1\right)\left(\mathrm{x}_0 + e^{-\frac{2i\pi}{3}}\mathrm{x}_1\right)\left(\mathrm{x}_0 + e^{\frac{2i\pi}{3}}\mathrm{x}_1\right) = \mathrm{x}_0^6 - \mathrm{x}_1^6$$

$$(\mathrm{x}_0 - 1)(\mathrm{x}_0 + 1)\left(\mathrm{x}_0 - e^{-\frac{i\pi}{3}}\right)\left(\mathrm{x}_0 - e^{\frac{i\pi}{3}}\right)\left(\mathrm{x}_0 - e^{-\frac{2i\pi}{3}}\right)\left(\mathrm{x}_0 - e^{\frac{2i\pi}{3}}\right) = \mathrm{x}_0^6 - 1$$

$$\begin{aligned}&(e\mathrm{x}_0 + \mathrm{x}_1)(e\mathrm{x}_0 + e\mathrm{x}_1)(e\mathrm{x}_0 + e^2\mathrm{x}_1)(e\mathrm{x}_0 + e^3\mathrm{x}_1)(e\mathrm{x}_0 + e^4\mathrm{x}_1)(e\mathrm{x}_0 + e^5\mathrm{x}_1)\\&= x_0 - x_1\end{aligned}$$

$$\begin{aligned}&(-\mathrm{x}_0 + \mathrm{x}_1 - \mathrm{x}_2)(\mathrm{x}_0 + \mathrm{x}_1 - \mathrm{x}_2)(-\mathrm{x}_0 + \mathrm{x}_1 + \mathrm{x}_2)(\mathrm{x}_0 + \mathrm{x}_1 + \mathrm{x}_2)\\&= -2\mathrm{x}_0^2\mathrm{x}_1^2 - 2\mathrm{x}_0^2\mathrm{x}_2^2 + \mathrm{x}_0^4 - 2\mathrm{x}_1^2\mathrm{x}_2^2 + \mathrm{x}_1^4 + \mathrm{x}_2^4\end{aligned}$$

$$\begin{aligned}&(\mathrm{x}_0 - \mathrm{x}_1 - \mathrm{x}_2 - \mathrm{x}_3)(\mathrm{x}_0 + \mathrm{x}_1 - \mathrm{x}_2 - \mathrm{x}_3)(\mathrm{x}_0 - \mathrm{x}_1 + \mathrm{x}_2 - \mathrm{x}_3)(\mathrm{x}_0 + \mathrm{x}_1 + \mathrm{x}_2 - \mathrm{x}_3)\\&(\mathrm{x}_0 - \mathrm{x}_1 - \mathrm{x}_2 + \mathrm{x}_3)(\mathrm{x}_0 + \mathrm{x}_1 - \mathrm{x}_2 + \mathrm{x}_3)(\mathrm{x}_0 - \mathrm{x}_1 + \mathrm{x}_2 + \mathrm{x}_3)(\mathrm{x}_0 + \mathrm{x}_1 + \mathrm{x}_2 + \mathrm{x}_3)\\&= -40\mathrm{x}_0^2\mathrm{x}_1^2\mathrm{x}_2^2\mathrm{x}_3^2 + 4\mathrm{x}_0^4\mathrm{x}_1^2\mathrm{x}_2^2 + 4\mathrm{x}_0^2\mathrm{x}_1^2\mathrm{x}_2^4 + 4\mathrm{x}_0^2\mathrm{x}_1^4\mathrm{x}_2^2 + 4\mathrm{x}_0^4\mathrm{x}_1^2\mathrm{x}_3^2 + 4\mathrm{x}_0^2\mathrm{x}_1^2\mathrm{x}_3^4\\&+4\mathrm{x}_0^2\mathrm{x}_1^4\mathrm{x}_3^2 - 4\mathrm{x}_0^6\mathrm{x}_1^2 + 6\mathrm{x}_0^4\mathrm{x}_1^4 - 4\mathrm{x}_0^2\mathrm{x}_1^6 + 4\mathrm{x}_0^4\mathrm{x}_2^2\mathrm{x}_3^2 + 4\mathrm{x}_0^2\mathrm{x}_2^2\mathrm{x}_3^4 + 4\mathrm{x}_0^2\mathrm{x}_2^4\mathrm{x}_3^2\\&-4\mathrm{x}_0^6\mathrm{x}_2^2 + 6\mathrm{x}_0^4\mathrm{x}_2^4 - 4\mathrm{x}_0^2\mathrm{x}_2^6 - 4\mathrm{x}_0^6\mathrm{x}_3^2 + 6\mathrm{x}_0^4\mathrm{x}_3^4 - 4\mathrm{x}_0^2\mathrm{x}_3^6 + \mathrm{x}_0^8 + 4\mathrm{x}_1^2\mathrm{x}_2^2\mathrm{x}_3^4 + 4\mathrm{x}_1^2\mathrm{x}_2^4\mathrm{x}_3^2\\&+4\mathrm{x}_1^4\mathrm{x}_2^2\mathrm{x}_3^2 - 4\mathrm{x}_1^2\mathrm{x}_2^6 + 6\mathrm{x}_1^4\mathrm{x}_2^4 - 4\mathrm{x}_1^6\mathrm{x}_2^2 - 4\mathrm{x}_1^2\mathrm{x}_3^6 + 6\mathrm{x}_1^4\mathrm{x}_3^4 - 4\mathrm{x}_1^6\mathrm{x}_3^2 + \mathrm{x}_1^8 - 4\mathrm{x}_2^2\mathrm{x}_3^6\\&+6\mathrm{x}_2^4\mathrm{x}_3^4 - 4\mathrm{x}_2^6\mathrm{x}_3^2 + \mathrm{x}_2^8 + \mathrm{x}_3^8\end{aligned}$$

$$\begin{aligned}&(\mathrm{x}_0 + \mathrm{x}_1)(\mathrm{x}_0 + e\mathrm{x}_1)\left(\mathrm{x}_0 + e^2\mathrm{x}_1\right)\left(\mathrm{x}_0 + e^3\mathrm{x}_1\right)\\&= x_0^4 - x_1^4\end{aligned}$$

$$\begin{aligned}&\sum_{a_1=0}^{1}\sum_{a_2=0}^{1}\sum_{a_3=0}^{1}((-1)^{a_0}(-1)^{a_1}(-1)^{a_2})(y_0 + (-1)^{a_0}y_1 + (-1)^{a_1}y_2 + (-1)^{a_3}y_3)^4 =\\&-(y_0 - y_1 - y_2 - y_3)^4 + (y_0 - y_1 - y_2 + y_3)^4 + (y_0 + y_1 - y_2 - y_3)^4\\&-(y_0 + y_1 - z_2 + y_3)^4 + (y_0 - y_1 + y_2 - y_3)^4 - (y_0 - y_1 + y_2 + y_3)^4 - (y_0 + y_1 + y_2 - y_3)^4\\&+(y_0 + y_1 + y_2 + y_3)^4 = 192y_0y_1y_2y_3\end{aligned}$$