Polynomier, rødder og division

Sebastian Ørsted

20. november 2016

Jeg foretager her en kort indføring af *polynomier* over såvel de reelle som de komplekse tal, hvor fokus er på at opbygge værktøjer til at finde rødder i og faktorisere polynomier. Der lægges vægt på metode frem for teori, hvilket afspejler den måske lidt utraditionelle rækkefølge, hvori resultaterne præsenteres, samt den hyppige anvendelse af eksempler. Målgruppen er matematikstuderende på første år på universitetet med forudsætninger svarende til et indledende Calculus-kursus ud fra f.eks. James Stewarts *Calculus – Concepts & Contexts*. Herunder forudsættes et elementært kendskab til de komplekse tal, om end dette kun anvendes i begrænset omfang. Samtlige resultater bevises foruden et enkelt (Algebraens Fundamentalsætning), men beviserne er forsøgt holdt i en så klar og enkel formulering som muligt uden at give køb på formaliteten.

De fleste af følgende resultater gælder såvel over de reelle som over de komplekse tal. Det er derfor praktisk på én gang at behandle polynomier over begge disse talkonstruktioner. Vi lader derfor i det følgende $\mathbb{K}$ betegne enten $\mathbb{R}$ eller $\mathbb{C}$; dette skal forstås på den måde, at resultaterne gælder både, hvis $\mathbb{K} = \mathbb{R}$, og hvis $\mathbb{K} = \mathbb{C}$.

Definition 1. *Et **polynomium** over $\mathbb{K}$ er en funktion $f : \mathbb{K} \to \mathbb{K}$ på formen*

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \qquad (x \in \mathbb{K}), \tag{1}$$

hvor $a_0, a_1, \ldots, a_n$ alle er elementer i $\mathbb{K}$.

Lad et polynomium f forskelligt fra 0 være opskrevet som i ligning (1). Da lader vi **graden** af f være det største heltal k, $0 \leq k \leq n$, som opfylder $a_k \neq 0$. Graden af f betegnes $\deg(f)$. Vi siger da, at $a_k x^k$ er **højestegradsleddet** for f. Højestegradsleddet er med andre ord det led i f (forskelligt fra nul), som indeholder den højeste potens af x, og graden er størrelsen af denne potens. Hvis $\deg(f) = 0$, er f konstant. Graden af nulpolynomiet $f = 0$ defineres normalt ikke. Proposition 2(ii) nedenfor viser, at graden og højestegradsleddet af et polynomium er veldefinerede. For to polynomier f og g over $\mathbb{K}$ siger vi, at f **går op i** g, hvis der findes et polynomium h over $\mathbb{K}$, så $f = gh$.

Vi noterer følgende vigtige regneregler for polynomier:

Proposition 2. *Lad f og g være polynomier over $\mathbb{K}$. Så gælder følgende regneregler:*

(i) Summen $f+g$, produktet $f \cdot g$ og sammensætningen $f \circ g$ er polynomier. Endvidere er λf et polynomium for alle λ i $\mathbb{K}$.

(ii) Koefficienterne $a_0, a_1, \dots, a_n$ i ligning (1) er entydigt bestemte (dvs. det samme polynomium kan ikke opskrives med flere forskellige valg af koefficienter).

(iii) Hvis $f \neq 0$ og $g \neq 0$, så er $fg \neq 0$, og $\deg(fg) = \deg(f) + \deg(g)$.

Bevis. (i) er oplagt gyldig.

Skriv f på formen fra ligning (1). Hvis $\mathbb{K} = \mathbb{R}$, får vi ved udledninger helt analoge til dem i begyndelsen af afsnit 8.7 i Stewart, at den i'te koefficient a_i i f er givet ved den i'te afledte $f^{(i)}$ af f ved formlen

$$a_i = \frac{f^{(i)}(0)}{i!}.$$

Hvis derimod $\mathbb{K} = \mathbb{C}$, er denne metode ikke mulig, da vi endnu ikke har defineret differentiation af funktioner $\mathbb{C} \to \mathbb{C}$. Hvis vi derimod lader $h\colon \mathbb{R} \to \mathbb{C}$ betegne restriktionen af f til $\mathbb{R}$, får vi ved helt tilsvarende overvejelser, at a_i er givet ved

$$a_i = \frac{h^{(i)}(0)}{i!}.$$

Specielt er a_i entydigt bestemt, hvilket viser (ii).

For at vise (iii) skriver vi

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + \cdots + a_1 x + a_0 \quad \text{og} \quad g(x) = \sum_{j=0}^{m} b_j x^j = b_m x^m + \cdots + b_1 x + b_0$$

for passende $a_0, a_1, \dots, a_n, b_0, b_1, \dots, b_m \in \mathbb{K}$ med $a_n, b_m \neq 0$. Idet $(a_i x^i)(b_j x^j) = a_i b_j x^{i+j}$ for alle i, j, består koefficienten til x^k i produktet fg af summen af alle produkter $a_i b_j$, hvor $i + j = k$. Med andre ord er

$$(fg)(x) = \sum_{k=0}^{m+n} \sum_{i+j=k} a_i b_j x^k.$$

Da $a_n b_m \neq 0$, er højestegradsleddet i fg netop $a_n b_m x^{n+m}$. Specielt er $fg \neq 0$, og $\deg(fg) = n + m = \deg(f) + \deg(g)$. Dette viser (iii). □

Vi vil ofte for nemhedens skyld tillade os at skrive polynomiet i ligning (1) som

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

Det er således underforstået, at der er tale om den *funktion*, som sender $x \in \mathbb{K}$ over i dette udtryk. Denne konvention er standard i algebraiske behandlinger af polynomier.

Der går ikke lang tid fra indførslen af polynomier, til vi nødvendigvis må begynde at snakke om *rødder*:

Definition 3. *Et $\alpha \in \mathbb{K}$ kaldes en* **rod** *i et polynomium f forskelligt fra nul, hvis der gælder $f(\alpha) = 0$.*

Følgende lille resultat er en ualmindeligt motiverende grund til at indføre de komplekse tal:

Sætning 4 (Algebraens Fundamentalsætning).
Ethvert ikke-konstant polynomium over $\mathbb{C}$ har en rod i $\mathbb{C}$.

Sætningen er kendt for at have mange forskellige kreative beviser, der tager udgangspunkt i resultater fra hver sin gren af matematikken. Ingen af disse beviser er dog helt trivielle, og at medtage ét af dem her vil gå for vidt. Der gælder ikke et tilsvarende resultat over de reelle tal; eksempelvis har polynomiet $x^2 + 1$ som bekendt ikke nogen rod i $\mathbb{R}$. Vi kan faktisk tænke på de komplekse tal som de reelle tal, hvor vi har tilføjet en rod i polynomiet x^2+1, nemlig tallet i. Algebraens Fundamentalsætning fortæller os nu, at vi ved tilføjelsen af denne rod automatisk også får rødder i alle andre ikke-konstante polynomier, hvilket jo på ingen måde er åbenlyst.

1 Faktorisering af polynomier

For polynomier af grad 1 og 2 er det nemt at finde rødder; i begge tilfælde har vi lukkede formler, der altid giver os rødderne. For polynomier af grad 3 og 4 er det langt sværere, men det er stadig muligt at give løsningsformler. For grad 5 og derover er det generelt ikke muligt. Vi er derfor nødt til at anvende andre metoder til at finde rødder.

Følgende lille resultat er i denne forbindelse af største vigtighed. Beviset gives sidst i kapitlet (se alternativt Opgave 26 for et andet bevis, som ikke kræver yderligere forudsætninger).

Sætning 5. *Lad $\alpha \in \mathbb{K}$ være en rod i et polynomium f over $\mathbb{K}$ forskelligt fra nul. Så går $x - \alpha$ op i f. Med andre ord findes et polynomium g over $\mathbb{K}$, så*

$$f(x) = (x - \alpha)g(x) \qquad \text{for alle } x \in \mathbb{K}.$$

Dette resultat er nyttigt, hvis vi er i stand til at *gætte* en rod α: Thi i så fald kan vi faktorisere $x - \alpha$ uden for vores polynomium som ovenfor. Hvis vi derefter ønsker at finde flere rødder, skal vi altså løse ligningen $f(x) = (x - \alpha)g(x) = 0$. Nulreglen giver, at enten $(x - \alpha) = 0$ eller $g(x) = 0$; i første tilfælde finder vi blot roden $x = \alpha$, som vi allerede kender. I det andet tilfælde skal vi altså finde en rod i et nyt polynomium g. Kernen i det hele er dog, at vi altid vil have, at $\deg(g) = \deg(f) - 1$; vi har altså reduceret problemet til at finde rødder i et polynomium af lavere grad, hvilket ofte kan være lettere.

Eksempel 6. Vi betragter polynomiet $f(x) = x^4 - 3x^3 + x^2 + 3x - 2$ (det kommer ikke til at gøre nogen forskel, om vi betragter f som et polynomium over $\mathbb{R}$ eller $\mathbb{C}$). Vi starter med at prøve at gætte en rod. En tommelfingerregel på Institut for Matematik er, at alle polynomier har rødder at finde blandt tallene $0, \pm 1, \pm 2$ (sandsynligvis fordi forelæserne heller ikke selv gider regne med alt for svære polynomier). Vi konstaterer derfor ved efterprøvning, at 1 er en rod. Sætning 5 fra før giver så, at vi kan faktorisere $x - 1$ ud af vores polynomium.

Det er dog ikke på nuværende tidspunkt klart, hvordan denne faktorisering kan bestemmes. Lad os derfor for en kort stund lege, at vi er meget gode til at gætte og er nået frem til, at

$$x^4 - 3x^3 + x^2 + 3x - 2 = (x-1)(x^3 - 2x^2 - x + 2) \tag{2}$$

(vi vil senere vise en systematisk metode til at nå frem til denne faktorisering). Vi kan derefter gentage spørgsmålet med polynomiet $x^3 - 2x^2 - x + 2$. Igen ser vi ved direkte efterprøvning, at 1 er en rod. Ergo kan vi igen faktorisere $x - 1$ udenfor endnu en gang. Vi har stadig heldet med os og gætter faktoriseringen

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

Vi kan nu finde samtlige rødder i polynomiet $x^2 - x - 2$ via diskriminantformlen: Det er $x = 2$ og $x = -1$. Vi kan med andre ord vælge enten at faktorisere $x - 2$ eller $x - (-1)$ uden for dette polynomium. Det viser sig imidlertid, at vi slet ikke behøver at vælge, for der gælder $x^2 - x - 2 = (x-2)(x-(-1))$.

Vi sammenfatter ovenstående resultater i formlen

$$\begin{aligned} x^4 - 3x^3 + x^2 + 3x - 2 &= (x-1)(x-1)(x-2)(x-(-1)) \\ &= (x-1)^2(x-2)(x-(-1)). \end{aligned}$$

Hvis nu $x^4 - 3x^3 + x^2 + 3x - 2 = 0$, giver nulreglen, at én af faktorerne $(x-1), (x-2)$ eller $(x-(-1))$ er 0. Vi konkluderer, at *alle* rødderne i f udgøres af $1, -1$ og 2. ○

Vi generaliserer metoden herover med følgende resultat:

Sætning 7 (Faktorisering af polynomier). *Lad f være et polynomium forskelligt fra nul over $\mathbb{K}$. Så kan f faktoriseres på formen*

$$f(x) = (x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_r)^{n_r} g(x) \qquad (x \in \mathbb{K}), \tag{3}$$

*hvor $\alpha_1, \alpha_2, \ldots, \alpha_r$ er **forskellige** tal i $\mathbb{K}$, $n_1, n_2, \ldots, n_r \geq 1$ er hele tal, og $g \neq 0$ er et polynomium over $\mathbb{K}$, som ikke har nogen rødder. Ydermere gælder, at $\alpha_1, \alpha_2, \ldots, \alpha_r$ er samtlige rødder i f, samt at denne faktorisering er entydig op til ombytning af faktorerne $(x-\alpha_i)^{n_i}$.*

Hvis $\mathbb{K} = \mathbb{C}$, gælder endvidere, at g er et konstant polynomium, så $g = a$ for et komplekst tal a. Med andre ord har vi da

$$f(x) = a(x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_r)^{n_r} \qquad (x \in \mathbb{C}). \tag{4}$$

At faktoriseringen er »entydig op til ombytning af faktorerne $(x-\alpha_i)^{n_i}$«, betyder, at enhver anden tilsvarende faktorisering blot er den samme, men hvor rækkefølgen af faktorerne $(x-\alpha_i)^{n_i}$ er ændret. Tallet n_i omtales ofte som **multipliciteten** af roden α_i i f. Hvis $\alpha \in \mathbb{K}$ *ikke* er en rod i f, siges α at have *multiplicitet 0*.

Bevis. Sæt $f_0 = f$. Hvis f_0 har en rod β_1, kan vi jf. Sætning 5 skrive

$$f_0(x) = (x-\beta_1)f_1(x) \qquad (x \in \mathbb{K})$$

for et passende polynomium f_1. Hvis f_1 har en rod β_2, kan vi så gentage proceduren og skrive

$$f_1(x) = (x-\beta_2)f_2(x) \qquad (x \in \mathbb{K})$$

for et passende polynomium f_2. Denne proces kan ikke fortsætte for evigt, thi graden falder med 1 hver gang. Så efter $k \geq 0$ trin står vi med en faktorisering

$$f(x) = (x-\beta_1)(x-\beta_2)\cdots(x-\beta_k)g(x),$$

hvor $g = f_k$ ikke har nogen rødder (det kunne muligvis være konstant). Det kan nu sagtens hænde, at nogle af β_i'erne er ens. I så fald kan vi frasortere gengangerne og så skrive de tilbageværende rødder som $\alpha_1, \alpha_2, \ldots, \alpha_r$ (hvor $r \leq k$), som alle er *forskellige*. Ved at lade n_i være antallet af forekomster af α_i blandt $\beta_1, \beta_2 \ldots, \beta_k$ fås en faktorisering som den i ligning (3). Hvis nu

$$f(x) = (x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_r)^{n_r}g(x) = 0, \tag{5}$$

giver nulreglen, at én af faktorerne $(x-\alpha_1), (x-\alpha_2), \ldots, (x-\alpha_r), g(x)$ er 0. Det kan ikke være $g(x)$, da g ingen rødder har. Vi slutter, at alle rødderne i f er at finde blandt $\alpha_1, \alpha_2, \ldots, \alpha_r$.

Da $\alpha_1, \alpha_2, \ldots, \alpha_r$ er samtlige rødder i f, er det klart, at enhver anden tilsvarende faktorisering af f må have formen

$$f(x) = (x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}\cdots(x-\alpha_r)^{m_r}h(x),$$

hvor $m_1, m_2, \ldots, m_r \geq 1$ er heltal, og h er et polynomium uden rødder. For at vise entydigheden af vores faktorisering må vi således vise, at $m_i = n_i$ for alle i, samt at $h = g$. Vælg derfor en vilkårlig rod α_i, og lad os vise, at de tilhørende multipliciteter m_i og n_i er ens. Bemærk, at vi ved at bytte om på rækkefølgen af α_j'erne kan antage, at $i = 1$. Da ét af tallene m_1 og n_1 nødvendigvis må være størst, kan vi antage, at $n_1 \leq m_1$. Med andre ord er

$$f(x) = (x-\alpha_1)^{n_1}\Big((x-\alpha_1)^{m_1-n_1}(x-\alpha_2)^{m_2}(x-\alpha_3)^{m_3}\cdots(x-\alpha_r)^{m_r}h(x)\Big). \tag{6}$$

Idet vi fratrækker ligning (5) fra dette, får vi

$$0 = (x-\alpha_1)^{n_1}\Big((x-\alpha_1)^{m_1-n_1}(x-\alpha_2)^{m_2}\cdots(x-\alpha_r)^{m_r}h(x)-(x-\alpha_2)^{n_2}\cdots(x-\alpha_r)^{n_r}g(x)\Big).$$

Da $(x-\alpha_1)^{n_1}$ ikke er nulpolynomiet, giver Proposition 2(iii), at det må være parentesen til højre, der er 0, altså at

$$(x-\alpha_1)^{m_1-n_1}(x-\alpha_2)^{m_2}\cdots(x-\alpha_r)^{m_r}h(x) - (x-\alpha_2)^{n_2}\cdots(x-\alpha_r)^{n_r}g(x) = 0,$$

dvs.

$$(x-\alpha_1)^{m_1-n_1}(x-\alpha_2)^{m_2}\cdots(x-\alpha_r)^{m_r}h(x) = (x-\alpha_2)^{n_2}\cdots(x-\alpha_r)^{n_r}g(x).$$

Da α_1 ikke er en rod på højresiden, kan den heller ikke være det på venstresiden, og vi har $m_1 - n_1 = 0$, dvs. $m_1 = n_1$. Som nævnt tidligere viser dette mere generelt, at $m_i = n_i$ for alle i. Fra ligning (6) er nu

$$f(x) = (x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_r)^{n_r}h(x).$$

Fratrækkes igen ligning (5), får vi

$$\Big((x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_r)^{n_r}\Big)\Big(g(x)-h(x)\Big) = 0.$$

Parentesen til venstre er igen ikke nulpolynomiet, så ligesom før må vi have $g(x) - h(x) = 0$, dvs. $g = h$. Dette færdiggør beviset for entydighedsudsagnet.

Hvis $\mathbb{K} = \mathbb{C}$, får vi fra Algebraens Fundamentalsætning, at de eneste polynomier (forskellige fra nul) uden rødder er konstanter. Dette viser, at g er konstant som ønsket. $\square$

Ovenstående resultat gør os nu i stand til at tælle antallet af rødder i et polynomium.

Korollar 8. *Et polynomium over $\mathbb{K}$ af grad n har højst n forskellige rødder.*

Bevis. Skriv som i Sætning 7 polynomiet f på formen

$$f(x) = (x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_r)^{n_r}g(x) \qquad (x \in \mathbb{K}).$$

Så giver gentagne anvendelser af gradsformlen (Proposition 2(iii)), at

$$\begin{aligned}\deg(f) &= \deg\Big((x-\alpha_1)^{n_1}\Big) + \deg\Big((x-\alpha_2)^{n_2}\Big) + \cdots + \deg\Big((x-\alpha_r)^{n_r}\Big) + \deg(g)\\ &= n_1 + n_2 + \cdots + n_r + \deg(g) \geq r + \deg(g) \geq r.\end{aligned}$$

Ergo er antallet af forskellige rødder $\alpha_1, \alpha_2, \ldots, \alpha_r$ mindre end eller lig graden af f. Dette viser påstanden. □

2 Polynomiers division

Jeg smed i Eksempel 6 bare faktoriseringer ud i hovedet på jer. Men der er faktisk en smart algoritme kaldet *polynomiers division*, som altid gør det muligt at finde dem. Mere generelt tillader algoritmen os at foretage *division med rest* af polynomier, ligesom vi kender det fra heltallene. Denne mulighed har stor teoretisk såvel som praktisk betydning. Vi lægger ud med et par eksempler, før vi i fuld generalitet formulerer og beviser divisionsalgoritmen.

Eksempel 9. Idet vi ved, at $x-1$ går op i $x^4 - 3x^3 + x^2 + 3x - 2$, kan vi altid finde polynomiet fra ligning (2) via polynomiers division. Denne algoritme illustreres oftest med et skema på følgende måde. Vi starter med at skrive polynomierne op med en åben parentes til højre:

$$x^4 - 3x^3 + x^2 + 3x - 2 = (x-1)($$

Polynomiers division går nu frem efter følgende princip: Vi spørger os selv, hvor mange gange højestegradsleddet i $x-1$ (som er x) går op i højestegradsleddet i $x^4 - 3x^3 + x^2 + 3x - 2$ (som er x^4). Det gør det x^3 gange. Vi skriver derfor x^3 i parentesen til højre. Men $x^3(x-1) = x^4 - x^3$ er ikke lig det ønskede polynomium $x^4 - 3x^3 + x^2 + 3x - 2$; der er en rest tilbage. Vi trækker derfor $x^4 - x^3$ fra $x^4 - 3x^3 + x^2 + 3x - 2$ og finder, at denne rest er $-2x^3 + x^2 + 3x - 2$, hvilket vi skriver ind i skemaet:

$$\begin{array}{l} x^4 - 3x^3 + x^2 + 3x - 2 = (x-1)(x^3 \\ \underline{x^4 \;\; - x^3 \quad} \\ \quad -2x^3 + x^2 + 3x - 2 \end{array}$$

Vi gentager så spørgsmålet med vores rest: Hvor mange gange går højestegradsleddet i $x-1$ (som er x) op i højestegradsleddet i $-2x^3 + x^2 + 3x - 2$ (som er $-2x^3$)? Det gør det $-2x^2$ gange; vi skriver derfor $-2x^2$ i parentesen til højre. Men $-2x^2(x-1) = -2x^3 + 2x^2$ er ikke lig $-2x^3 + x^2 + 3x - 2$; der er en rest, nemlig

$-2x^3 + x^2 + 3x - 2 - (-2x^3 + 2x^2) = -x^2 + 3x$. Vi skriver så også denne rest ind i vores skema:

$$\begin{array}{l}
x^4 - 3x^3 \quad + x^2 + 3x - 2 = (x-1)(x^3 - 2x^2 \\
\underline{x^4 \quad - x^3} \\
\quad -2x^3 \quad + x^2 + 3x - 2 \\
\quad \underline{-2x^3 + 2x^2} \\
\qquad\qquad -x^2 + 3x - 2
\end{array}$$

Vi gentager så spørgsmålet med resten $-x^2 + 3x - 2$ og fortsætter på samme måde. Før eller senere må algoritmen determinere, idet graden af polynomiet falder hver gang. Vi får til sidst resten 0 forneden:

$$\begin{array}{l}
x^4 - 3x^3 \quad + x^2 + 3x - 2 = (x-1)(x^3 - 2x^2 - x + 2) \\
\underline{x^4 \quad - x^3} \\
\quad -2x^3 \quad + x^2 + 3x - 2 \\
\quad \underline{-2x^3 + 2x^2} \\
\qquad\qquad -x^2 + 3x - 2 \\
\qquad\qquad \underline{-x^2 \quad + x} \\
\qquad\qquad\qquad 2x - 2 \\
\qquad\qquad\qquad \underline{2x - 2} \\
\qquad\qquad\qquad\qquad 0
\end{array}$$

Det betyder, at algoritmen gik op, og vi har vores faktorisering

$$x^4 - 3x^3 + x^2 + 3x - 2 = (x-1)(x^3 - 2x^2 - x + 2).$$ ○

Det er dog langt fra altid, at vi er så heldige at få resten 0 forneden.

Eksempel 10. Vi vil forsøge at dividere polynomiet $x^3 + x^2 - 1$ med $x + 2$. Dette giver

$$\begin{array}{l}
x^3 + x^2 \quad - 1 \qquad = (x+2)(x^2 - x + 2) - 5 \\
\underline{x^3 + 2x^2} \\
\quad -x^2 \quad - 1 \\
\quad \underline{-x^2 - 2x} \\
\qquad\quad 2x - 1 \\
\qquad\quad \underline{2x + 4} \\
\qquad\qquad -5
\end{array}$$

Algoritmen går langt hen ad vejen på samme måde som i sidste eksempel. Men når vi får resten -5, er vi nødt til at stoppe; højestegradsleddet i $x + 2$ er x, og dette går ikke op i højestegradsleddet i -5, som er -5. Vi konkluderer, at algoritmen ikke gik op; vi fik resten -5. Ergo er

$$x^3 + x^2 - 1 = (x+2)(x^2 - x + 2) - 5$$

det nærmeste, vi kommer en faktorisering. ○

Efter disse indledende eksempler er vi klar til at formulere polynomiers division formelt og give et generelt bevis for, at algoritmen altid virker. Beviset er da også i det store hele blot algoritmen nedskrevet i fuld generalitet.

Sætning 11 (Division med rest). *Lad f og $d \neq 0$ være polynomier over $\mathbb{K}$. Så findes entydigt bestemte polynomier q og r over $\mathbb{K}$, så*

$$f = qd + r, \tag{7}$$

og hvor restpolynomiet r opfylder enten $r = 0$ eller $\deg(r) < \deg(d)$.

Bevis. Vi viser først eksistensen af den ønskede opskrivning fra ligning (7). Sæt $f_0 = f$. Hvis $f_0 \neq 0$ og $\deg(f_0) \geq \deg(d)$, går højestegradsleddet i d op i højestegradsleddet i f_0. Lad $h_1(x)$ være det antal gange, det går op, hvor h_1 er et polynomium. Sæt så

$$f_1 = f_0 - h_1 d.$$

Da f_0 og $h_1 d$ har samme højestegradsled, går disse led ud med hinanden i f_1. Ergo er f_1 enten 0 eller har lavere grad end f_0.

Hvis der igen gælder $f_1 \neq 0$ og $\deg(f_1) \geq \deg(d)$, går højestegradsleddet i d igen et antal gange op i højestegradsleddet i f_1. Lad dette antal være $h_2(x)$, hvor h_2 er et polynomium. Sæt så

$$f_2 = f_1 - h_2 d.$$

Igen har f_1 og $h_2 d$ samme højestegradsled, så disse led går ud med hinanden i f_2, og f_2 er 0 eller har lavere grad end f_1.

Sådan fortsættes. Da graden bliver ved med at falde fra gang til gang, kan vi ikke fortsætte for evigt. Det må altså på et tidspunkt efter $k \geq 0$ trin gælde, at $f_k = 0$ eller $\deg(f_k) < \deg(d)$. Ud fra, hvordan vi definerede vores f_i'er, er nu

$$\begin{aligned}
f_k &= f_{k-1} - h_k d \\
&= (f_{k-2} - h_{k-1} d) - h_k d = f_{k-2} - (h_{k-1} + h_k) d \\
&= (f_{k-3} - h_{k-2} d) - (h_{k-1} + h_k) d = f_{k-3} - (h_{k-2} + h_{k-1} + h_k) d \\
&= \cdots = f_0 - (h_1 + h_2 + \cdots + h_k) d.
\end{aligned}$$

Ergo er

$$f = f_0 = (h_1 + h_2 + \cdots + h_k) d + f_k.$$

Vi sætter så $r = f_k$ og $q = h_1 + h_2 + \cdots + h_k$ og noterer os, at vi pr. antagelse har enten $r = 0$ eller $\deg(r) < \deg(d)$. Derved har vi vist det ønskede.

Vi viser derefter entydigheden af denne opskrivning. Antag derfor, at $f = qd + r = q'd + r'$ er to opskrivninger med de ønskede egenskaber. Så er

$$0 = (q - q')d + (r - r'), \qquad \text{dvs.} \quad (q - q')d = r' - r.$$

Pr. antagelse er r og r' begge enten 0 eller har strengt mindre grad end d, så ovenstående kan kun lade sig gøre, hvis begge sider af lighedstegnet er 0. Ergo er $q = q'$ og $r = r'$, hvilket viser entydighedsudsagnet. □

Lad os sammenfatte og skitsere divisionsalgoritmen med notationen fra beviset:

Bemærkning 12 (Polynomiers division). Antag, at vi ønsker at dividere et polynomium f med et polynomium $d \neq 0$. Sæt da $f_0 = f$ og $j = 0$. Så udføres algoritmen således:

(1) Antag, at $f_j \neq 0$ og $\deg(f_j) \geq \deg(d)$. I så fald går højestegradsleddet i d et antal gange op i højestegradsleddet i f_j. Lad da dette antal være $h_{j+1}(x)$, hvor h_{j+1} er et polynomium. Læg da $h_{j+1}(x)$ til parentesen til højre. Sæt nu $f_{j+1} = f_j - h_{j+1}d$, og start så denne liste forfra med j udskiftet med $j+1$.

(2) Hvis $f_j = 0$, er algoritmen gået op, og vi får resten $r = f_j = 0$.

(3) Hvis $f_j \neq 0$, men $\deg(f_j) < \deg(d)$, går algoritmen ikke op, og vi får resten $r = f_j$.

Skemaet ved polynomiers division ser i fuld generalitet således ud:

$$
\begin{array}{l}
f = f_0 = (d)(h_1 + h_2 + \cdots + h_k) + r \\
\underline{\quad h_1 d} \\
\quad f_1 = f_0 - h_1 d \\
\quad \underline{\qquad h_2 d} \\
\qquad f_2 = f_1 - h_2 d \\
\qquad \underline{\qquad h_3 d} \\
\qquad\qquad \ddots \\
\qquad\qquad \underline{\qquad\quad} \\
\qquad\qquad\quad f_{k-1} = f_{k-2} - h_{k-1} d \\
\qquad\qquad\quad \underline{\qquad\qquad h_k d} \\
\qquad\qquad\qquad\qquad r = f_k = f_{k-1} - h_k d.
\end{array}
$$

△

Eksempel 13. For fuldstændighedens skyld følger her, hvorledes de øvrige faktoriseringer fra Eksempel 6 kan findes via polynomiers division:

$$
\begin{array}{rrrl}
x^3 - 2x^2 & - x & + 2 & = (x-1)(x^2 - x - 2) \\
\underline{x^3 - x^2} & & & \\
-x^2 & - x & + 2 & \\
\underline{-x^2} & \underline{+ x} & & \\
 & -2x & + 2 & \\
 & \underline{-2x} & \underline{+ 2} & \\
 & & 0 &
\end{array}
$$

$$
\begin{array}{rrl}
x^2 - x & - 2 & = (x-2)(x+1) \\
\underline{x^2 - 2x} & & \\
x & - 2 & \\
\underline{x} & \underline{- 2} & \\
 & 0 &
\end{array}
$$

Resultaterne er præcist de samme, som jeg dér postulerede.

At finde den sidste faktorisering $x^2 - x - 2 = (x-2)(x+1)$ via polynomiers division er dog strengt taget lidt at skyde gråspurve med kanoner. Sagen er, at vi jo som sagt via diskriminantformlen kan finde frem til, at de eneste rødder er $x = 2$ og $x = -1$. Vi kan derfor jf. Sætning 7 skrive polynomiet som

$$x^2 - x - 2 = (x-(-1))^{n_1}(x-2)^{n_2} g(x)$$

for passende heltal $n_1, n_2 \geq 1$ samt et polynomium g, som ikke har nogen rødder. Men da venstresiden skal være et andengradspolynomium, må $n_1 = n_2 = 1$, og g må have grad 0, så g er konstant. Skriv derfor $g = k \in \mathbb{R}$, så

$$x^2 - x - 2 = k(x-(-1))(x-2).$$

Højestegradsleddet på venstresiden er x^2, mens højestegradsleddet på højresiden er kx^2. Ergo er $k = 1$. Derved slap vi for at bruge algoritmen på dette simple andengradspolynomium. ○

Fordi faktorisering af andengradspolynomiet optræder så ofte, vil vi behandle dette emne særskilt ved at generalisere slutningen af sidste eksempel. Beviset overlades til læseren.

Korollar 14. *Lad $a, b, c \in \mathbb{K}$ med $a \neq 0$, og og betragt andengradspolynomiet $f(x) = ax^2 + bx + c$ over $\mathbb{K}$. Hvis f kun har én rod α i $\mathbb{K}$, så er*

$$f(x) = a(x-\alpha)^2.$$

Hvis f har to forskellige rødder α_1 og α_2 i $\mathbb{K}$, så er

$$f(x) = a(x-\alpha_1)(x-\alpha_2).$$

Vi afslutter dette kapitel med som lovet at give et bevis for Sætning 5. Resultatet er faktisk et umiddelbart korollar til Sætning 11.

Bevis for Sætning 5. Anvend Sætning 11 på $d(x) = x - \alpha$ til at finde polynomier q og r, så

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

hvor $r = 0$ eller $\deg(r) < \deg(x-\alpha) = 1$, dvs. $\deg(r) = 0$. I begge tilfælde er r et konstant polynomium. Anvendes venstre- og højresiden i $x = \alpha$, fås

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

Men r var konstant, så $r = 0$. Ergo er $f(x) = (x-\alpha)q(x)$, og $g = q$ opfylder de ønskede egenskaber. □

Opgaver

Hvis det i følgende opgaver ikke angives, om polynomiet er over $\mathbb{R}$ eller $\mathbb{C}$, skyldes det, at det ikke kommer til at gøre nogen forskel.

1. Find samtlige rødder i $x^3 - 3x^2 + 2x$.

2. Går $x - 1$ op i $x^2 - x - 6$?

3. Går $x + 2$ op i $x^2 + x - 2$?

4. Find samtlige rødder i polynomiet $2x^3 - 2x^2 - 10x - 6$, og faktoriser polynomiet som i Sætning 7.

5. Find samtlige rødder i polynomiet $-x^3 + x^2 + 22x - 40$, og faktoriser polynomiet som i Sætning 7.

6. Find samtlige rødder i polynomiet $x^4 - 6x^3 + 13x^2 - 12x + 4$.

7. Find samtlige rødder i polynomiet $x^4 + 2x^3 + 2x^2 + 2x + 1$ over $\mathbb{R}$.

8. Divider polynomiet $3x^3 + 10x^2 - 1$ med $3x + 1$.

9. Divider polynomiet $3x^4 + 2x^2 - 8$ med $x^2 + 2$.

10. Divider $x^3 - x^2 + 3x - 1$ med $x - 1$, og find resten.

11. Divider $2x^4 - x^3 - 2x^2 + x$ med $x^2 - 1$, og find resten.

12. Faktoriser polynomiet $x^4 - 2x^3 - 3x^2 + 4x + 4$ som i Sætning 7.

13. Faktoriser polynomiet $x^3 - 9x^2 + 24x - 16$ som i Sætning 7.

14. Faktoriser polynomiet $x^3 - 11x^2 + 35x - 25$ som i Sætning 7.

15. Faktoriser polynomiet $-2x^3 - 8x^2 + 62x + 140$ som i Sætning 7.

16. Faktoriser polynomiet $x^4 - 12x^3 + 46x^2 - 60x + 25$ som i Sætning 7.

17. Faktoriser polynomiet $-x^4 - 2x^3 + 36x^2 - 88x + 64$ som i Sætning 7.

18. Faktoriser polynomiet $-2x^4 - 14x^3 + 26x^2 + 86x + 48$ som i Sætning 7.

19. Lineær algebra virker lige så godt (i nogle tilfælde endda bedre) over $\mathbb{C}$ som over $\mathbb{R}$, og alle de sædvanlige sætninger gælder også her (dog med undtagelse af egenskaberne ved skalarproduktet). Vis, at der for enhver kvadratisk matrix A af orden n med indgange i $\mathbb{C}$ findes en vektor $\mathbf{v} \in \mathbb{C}^n \setminus \{\mathbf{0}\}$ og et $\lambda \in \mathbb{C}$, så $A\mathbf{v} = \lambda\mathbf{v}$.

20. Lad f være et polynomium med koefficienter i $\mathbb{R}$, men betragt det som et polynomium over $\mathbb{C}$. Antag, at $\alpha \in \mathbb{C}$ er en rod i f. Vis, at det kompleks-konjugerede $\overline{\alpha}$ af α også er en rod, og at multipliciteterne af α og $\overline{\alpha}$ er ens.

21. Vis, at ethvert polynomium over $\mathbb{R}$ af *ulige grad* har en rod i $\mathbb{R}$. *Vink: Opgave 20.*

22. Lad n være et *lige*, ikke-negativt tal. Vis, at der findes et polynomium af grad n over $\mathbb{R}$, som ikke har nogen rødder i $\mathbb{R}$.

23. Lad f være et ikke-konstant polynomium over $\mathbb{C}$ med højestegradsled $a_n x^n$ (som i ligning (1)). Vis, at hvis f faktoriseres som i ligning (4), så er $a = a_n$.

24. Lad f være et ikke-konstant polynomium over $\mathbb{C}$ af grad n. Vis, at med notationen fra Sætning 7 er

$$n = n_1 + n_2 + \cdots + n_r.$$

25. Lad f være et ikke-konstant polynomium over $\mathbb{C}$ på formen

$$f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x + a_0$$

(dvs. $a_n = 1$ med notationen fra ligning (1)). Lad $\alpha_1, \alpha_2, \ldots, \alpha_r$ være de forskellige rødder i f, og lad n_i være multipliciteten af α_i for alle i. Vis, at

$$\alpha_1^{n_1}\alpha_2^{n_2}\cdots\alpha_r^{n_r} = (-1)^n a_0,$$

og at

$$n_1\alpha_1 + n_2\alpha_2 + \cdots + n_r\alpha_r = -a_{n-1}.$$

26. Giv et bevis for Sætning 5, som ikke anvender Sætning 11.
Vink: Betragt polynomiet $h(x) = f(x+\alpha)$, og bemærk, at $x = 0$ er en rod i h. Udled, at $h(x) = xp(x)$ for et polynomium p, og brug p smart.

27. Kan man bruge Euklids algoritme på polynomier? (*Vink: Sammenlign Sætning 11 herover med Korollar 14.11 i Tal og Mængder.*) I bekræftende fald: Find største fælles divisor d imellem polynomierne $f(x) = -2x^4 + 2x^2 + 4$ og $g(x) = 5x^3 - 8x^2 + 5x - 8$. Find også polynomier p og q, så $d = pf + qg$.

28. Vis, at ethvert ikke-konstant polynomium over $\mathbb{R}$ uden rødder kan skrives som et produkt af andengradspolynomier over $\mathbb{R}$ (*Vink: Opgave 20.*) Konkluder, at *alle* ikke-konstante polynomier over $\mathbb{R}$ kan skrives som et produkt af første- og andengradspolynomier over $\mathbb{R}$, hvor sidstnævnte ikke har nogen rødder i $\mathbb{R}$.

29. Et ikke-konstant polynomium f over $\mathbb{K}$ kaldes *irreducibelt*, hvis det om enhver faktorisering $f = gh$ af f i polynomier g og h over $\mathbb{K}$ gælder, at enten g eller h er konstant; med andre ord er irreducible polynomier en slags »primtal« blandt polynomier. Karakteriser de irreducible polynomier over $\mathbb{R}$ og $\mathbb{C}$. (*Vink: I tilfældet $\mathbb{R}$, brug Opgave 28.*)

30. Lad f være et ikke-konstant polynomium over $\mathbb{C}$. Vis følgende:

(i) Billedet $f(\mathbb{C})$ er hele $\mathbb{C}$.

(ii) Hvis $\deg(f) > 1$, har f et *fikspunkt*, dvs. et punkt t i $\mathbb{C}$ med $f(t) = t$.

31. Lad f være et ikke-konstant polynomium over $\mathbb{R}$ og α et reelt tal. Vis, at multipliciteten af α som rod i f er det minimale heltal $n \geq 0$, hvorom det gælder, at $f^{(n)}(\alpha) \neq 0$. (Husk, at $f^{(0)} = f$.)