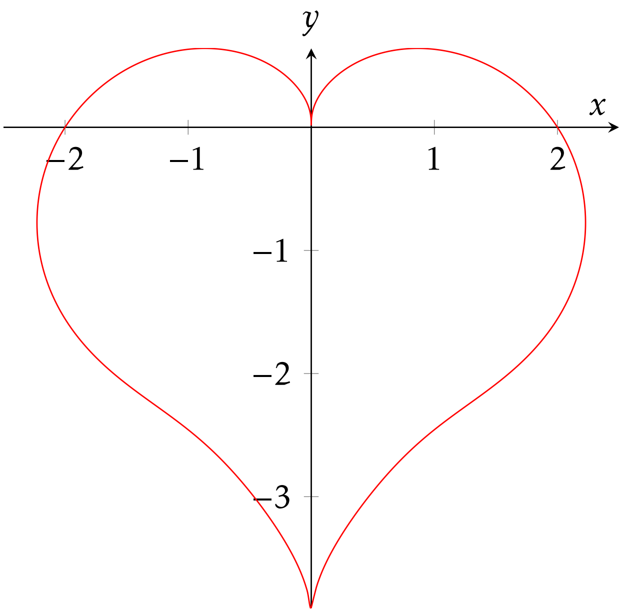
Supplerende noter til *Calculus*

Sebastian Ørsted



$$r(\theta) = 2 - 2\sin\theta + \sin\theta\,\frac{|\cos\theta|^{1/2}}{\sin\theta + 7/5}$$

Efteråret 2016

Forord

Følgende noter er tænkt som et supplement til standardpensum i *Calculus* og er særligt rettet imod matematikere, men kan sagtens benyttes af andre. De introducerer dels en del af de koncepter, som i større eller mindre grad forudsættes velkendte i kurset. Endvidere indføres nogle nye begreber, og der gives alternative og til tider mere fuldendte behandlinger af visse af emnerne fra *Calculus*.

Noterne opdateres løbende, og den nyeste version er tilgængelig på

`http://home.math.au.dk/sorsted/supcalc.pdf`

Kommentarer og fejlrapporteringer er meget velkomne på

`sorsted@math.au.dk`

Nærværende version er udarbejdet 20. november 2016.

Indhold

KAPITEL 1

MÆNGDELÆRE

EN MÆNGDE kan intuitivt opfattes som en samling af objekter. I denne forstand kan vi principielt betragte mængder bestående af (næsten) hvad som helst. Eksempelvis er

$$X = \{2, 3, 7, \pi\}$$

mængden bestående af tallene 2, 3, 7 og π. Vi anvender som ovenfor de såkaldte mængdeklammer eller »Tuborgparenteser« { og } til at betegne mængder. Det, som en mængde indeholder, kaldes mængdens **elementer**. Vi skriver $x \in X$ for udsagnet »x er et element i mængden X«. Det modsatte udsagn skrives $x \notin X$. Eksempelvis er $7 \in X$, men $9 \notin X$, hvis X er mængden herover. Rækkefølgen, som elementerne opskrives i, spiller ingen rolle; vi kunne også have skrevet $X = \{\pi, 3, 2, 7\}$, hvis vi skulle have den slags tendenser.

Der gælder om to mængder X og Y, at $X = Y$, hvis og kun hvis X og Y indeholder præcist de samme elementer. Den **tomme mængde** er mængden $\emptyset = \{\}$, som ikke indeholder nogen elementer.

Ligesom tal har en langt række standardoperationer som $+, \cdot, -$ osv., har mængder det også. Hvis X og Y er mængder, lader vi således $X \cap Y$ betegne **fællesmængden** (ofte lidt uformelt kaldet **snittet**) af X og Y, dvs. mængden af objekter, der er elementer i både X og Y. Ligeså lader vi $X \cup Y$ betegne **foreningsmængden** af X og Y, dvs. mængden af objekter, der er element i mindst én af mængderne X og Y. Hvis X er som ovenfor, og $Y = \{3, 7, 11, \sqrt{2}\}$, er

$$X \cap Y = \{3, 7\} \quad \text{og} \quad X \cup Y = \{2, 3, 7, 11, \pi, \sqrt{2}\}.$$

I *Perspektiver i matematikken* indføres nogle flere mængdeoperationer; men $\cap$ og $\cup$ er klart de vigtigste at kende. Bemærk det vigtige specialtilfælde $X \cap Y = \emptyset$, som svarer til, at X og Y ikke har nogen elementer til fælles; X og Y kaldes i dette tilfælde **disjunkte**.

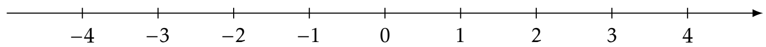
En mængde Z kaldes en **delmængde** af en mængde X, hvis alle elementer i Z også er elementer i X. Dette skrives $Z \subseteq X$. Bemærk, at der for alle mængder X gælder $X \subseteq X$. Hvis vi sætter $Z = \{7, \pi\}$ og lader X være som ovenfor, gælder $Z \subseteq X$. En vigtig pointe, som er et kulturchok for mange nybagte matematikere, er, at vi betragter den tomme mængde $\emptyset$ som en delmængde af *alle* mængder. Dette ser af mange grunde pænere ud, som I sidenhen selv skal få at se.

Hvis X og Y er mængder, er **mængdedifferensen** $X \setminus Y$ mængden af elementer i X, som *ikke* er elementer i Y. Bemærk, at vi i definitionen ikke antager noget om, at Y er en delmængde af X. Hvis X og Y er som ovenfor, er

$$X \setminus Y = \{2, \pi\}.$$

1.1 De reelle tal

Den absolut vigtigste mængde at kende i *Calculus* er de **reelle tal** $\mathbb{R}$. Denne mængde indeholder alt det, som vi i traditionel forstand vil opfatte som »tal«. Man kan således tænke på de reelle tal som mængden af alle punkter på en uendelig tallinje fra minus uendelig til uendelig:



Det er faktisk muligt at give en formel definition af de reelle tal; dette kræver dog en matematisk abstraktion, som ligger langt ud over nærværende kursus.

En anden måde at forstå de reelle tal er som alle tal, der kan skrives som en uendelig række af decimaltal, dvs. »kommatal«. Dette tæller blandt andet tal som $\pi, -\sqrt{2}, \ln(10), \cos(7)$ osv. Eksempelvis kan vi jo skrive

$$\pi = 3.141\,592\,653\,589\,793\,238\,462\,643\,383\,279\,502\,884\,197\,169\,399\ldots$$

1.2 Mængdekonstruktion

En vigtig måde at skabe nye mængder ud fra eksisterende er ved såkaldt **mængdekonstruktion**. Givet en mængde X kan vi danne en mængde bestående af præcist de elementer i X, som opfylder en given betingelse. For eksempel er

$$\{x \in \mathbb{R} \mid x < 5\}$$

mængden af de tal x i $\mathbb{R}$, som opfylder $x < 5$, altså intervallet $(-\infty, 5)$. Den lodrette streg »|« læses »om hvilke gælder«. Sådanne mængdekonstruktioner optræder over alt i matematikken. Hvis vi mere generelt lader X være en mængde og $P(x)$ et udsagn (dvs. en påstand, der afhænger af x, og som enten kan være sand eller falsk), så betegner vi med

$$\{x \in X \mid P(x)\}$$

mængden af de elementer x i X, som opfylder $P(x)$. Denne påstand $P(x)$ kan dække over mangt og meget; faktisk er mængdelæren opbygget så smart, at vi kan tillade $P(x)$ at være noget nær hvad som helst, som vi kan skrive ned. Eksempelvis er

$$\{p \in \mathbb{N} \mid p \text{ er et primtal}\}$$

mængden af de p i de naturlige tal $\mathbb{N} = \{1, 2, 3, \ldots\}$, som opfylder, at p er et primtal.

Der findes en anden type mængdekonstruktion, som er nært beslægtet med den allerede nævnte, og som måske er endda lige så vigtig. Hvis f er en funktion som (eventuelt blandt andet) kan defineres på en mængde X, lader vi

$$\{f(x) \mid x \in X\}$$

betegne mængden af de $f(x)$, hvor x er et element i X. Denne mængde betegnes ofte **billedet** af X under f og skrives kort $f(X)$. Hvis $f(x) = x^2$ og $X = \mathbb{R}$, er

$$\{f(x) \mid x \in \mathbb{R}\} = \{x^2 \mid x \in \mathbb{R}\} = [0, \infty),$$

idet $[0, \infty)$ præcist er mængden af tal, der kan skrives som x^2 for et reelt tal x. Bemærk, at mængden

$$\{x^2 \mid x \in [0, \infty)\}$$

er præcist den samme mængde, idet vi kan skrive alle ikke-negative reelle tal som x^2 for et reelt tal $x \geq 0$. Tilsvarende er

$$\{n + \pi \mid n \in \mathbb{Z}\} = \{\dots, -2 + \pi, -1 + \pi, \pi, 1 + \pi, 2 + \pi, \dots\}$$

mængden af tal, som kan skrives som $n + \pi$ for et heltal n.

1.3 Talmængder og intervaller

Der er en række standardmængder, som er altafgørende at kende. Her bør først og fremmest nævnes de grundlæggende talmængder

$\mathbb{N} = \{1, 2, 3, 4, \dots\}$	(de naturlige tal[1])
$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$	(de hele tal)
$\mathbb{Q} = \left\{\frac{x}{y} \mid x, y \in \mathbb{Z}, y \neq 0\right\}$	(de rationelle tal, dvs. brøker hvor tæller og nævner er heltal)
$\mathbb{R}$	(de reelle tal)
$\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\}$	(de komplekse tal)

Bemærk, at der gælder $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. De komplekse tal er en udvidelse af de reelle tal, som indføres i *Calculus*, og som fremkommer ved at »opfinde« et nyt tal i med egenskaben $i^2 = -1$. De komplekse tal er nu mængden af udtryk på formen $x + iy$ for reelle tal x og y.

Vi har allerede i ovenstående truffet eksempler på **intervaller** i $\mathbb{R}$. For alle a og b i $\mathbb{R}$ med $a < b$ sætter vi[2]

$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\} \qquad (a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$$
$$[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\} \qquad (a, b) = \{x \in \mathbb{R} \mid a < x < b\}.$$

Mængden $[a, b]$ kaldes det *lukkede interval fra a til b*, mens (a, b) kaldes det tilsvarende *åbne interval*. $[a, b)$ og $(a, b]$ omtales begge som *halvåbne intervaller*.

[1] Til tider medtages 0 også i de naturlige tal.

[2] Det skal bemærkes, at man nogle steder, heriblandt på gymnasiet, til tider anvender eksempelvis notationen $[a, b[$ i stedet for $[a, b)$; med andre ord udskiftes de bløde parenteser herover med klammer, som »vender forkert«. Begge notationer forekommer på videregående niveau, men $[a, b[$ er mere sjælden (især i engelsksproget litteratur) og i mine øjne ualmindeligt grim.

Derudover tillader vi også intervaller ikke at have nogen øvre eller nedre grænse. I dette tilfælde anvender vi igen ovenstående notation, men med de pågældende grænser udskiftet med $\pm\infty$:

$$[a,\infty) = \{x \in \mathbb{R} \mid a \leq x\} \qquad (-\infty,b] = \{x \in \mathbb{R} \mid x \leq b\}$$
$$(a,\infty) = \{x \in \mathbb{R} \mid a < x\} \qquad (-\infty,b) = \{x \in \mathbb{R} \mid x < b\}$$
$$(-\infty,\infty) = \mathbb{R}.$$

1.4 Det kartesiske produkt

En vigtig konstruktion er også **mængdeproduktet** $X \times Y$, som også kaldes det **kartesiske produkt**. Det er givet ved

$$X \times Y = \{(x,y) \mid x \in X \text{ og } y \in Y\},$$

altså mængden af par (x,y) (også kaldet dubler), hvor x kommer fra X, og y kommer fra Y. Det læses »X kryds Y«. F.eks. er

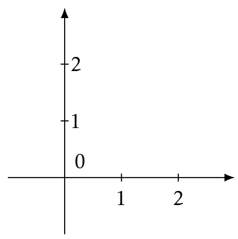
$$\{1,2,3\} \times \{\pi, \sqrt{2}\} = \Big\{(1,\pi),(1,\sqrt{2}),(2,\pi),(2,\sqrt{2}),(3,\pi),(3,\sqrt{2})\Big\}.$$

En dubel (x,y) er ikke andet end to elementer x og y, som er opskrevet som par i en bestemt rækkefølge. For alle x,y,x',y' gælder $(x,y) = (x',y')$, hvis og kun hvis $x = x'$ og $y = y'$; bemærk kontrasten til mængder, hvor der jo altid gælder $\{x,y\} = \{y,x\}$. Hvis x og y er reelle tal med $x < y$, ser vi, at notationen for dublen (x,y) er sammenfaldende med notationen (x,y) for det åbne interval fra x til y. Denne tvetydighed er imidlertid sjældent i praksis et problem, da det som regel er let ud fra sammenhængen at slutte, om der er tale om dubler eller intervaller; det er trods alt to meget forskellige ting.

Et vigtigt specialtilfælde af mængdeproduktet er

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x,y) \mid x,y \in \mathbb{R}\},$$

som er mængden af punkter i et to-dimensionalt koordinatsystem:



Mere generelt lader vi for alle heltal $n \geq 1$

$$\mathbb{R}^n = \underbrace{\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}}_{n \text{ faktorer}} = \{(x_1,x_2,\ldots,x_n) \mid x_1,x_2,\ldots,x_n \in \mathbb{R}\}$$

være mængden af n-dimensionale vektorer, hvor $x_1,x_2,\ldots,x_n$ alle er elementer i $\mathbb{R}$. Med andre ord er $\mathbb{R}^3$ det tre-dimensionale rum, hvor vi til daglig færdes.

Lad os som et eksempel formalisere begrebet om en **linje** i $\mathbb{R}^2$. For $a, b \in \mathbb{R}$ lader vi ℓ betegne linjen med ligningen $y = ax + b$. Hvad vi da faktisk mener, er, at ℓ er mængden af punkter (x, y) i $\mathbb{R}^2$, som opfylder $y = ax + b$. Med notationen herover er

$$\ell = \{(x, y) \in \mathbb{R}^2 \mid y = ax + b\}.$$

Tilsvarende er parablen med ligningen $y = ax^2 + bx + c$ blot lig mængden

$$\{(x, y) \in \mathbb{R}^2 \mid y = ax^2 + bx + c\}.$$

1.5 Funktioner

Jeg vil afslutningsvist tale lidt om **funktioner** (også kaldet **afbildninger**). Hvis X og Y er mængder, er en funktion $f\colon X \to Y$ en *regel*[3], der til ethvert x i X knytter ét og kun ét y i Y. Vi betegner dette y med $f(x)$ og siger, at »y er en funktion af x«. Vi vil ofte sammenfatte ovenstående i diagrammet

$$\begin{aligned} f\colon X &\longrightarrow Y \\ x &\longmapsto y = f(x). \end{aligned}$$

Vi kan eksempelvis betragte $f\colon \mathbb{R} \to \mathbb{R}$ givet ved $f(x) = x^2$ for alle $x \in \mathbb{R}$; tallet x^2 i $\mathbb{R}$ er nemlig entydigt bestemt ud fra tallet x. Ovenstående diagram bliver i dette tilfælde

$$\begin{aligned} f\colon \mathbb{R} &\longrightarrow \mathbb{R} \\ x &\longmapsto x^2. \end{aligned}$$

Tilsvarende kan vi betragte funktionen $g\colon \mathbb{Z} \to \mathbb{R}$ givet ved $g(x) = \pi x$ for $x \in \mathbb{Z}$, som kan illustreres med diagrammet

$$\begin{aligned} g\colon \mathbb{Z} &\longrightarrow \mathbb{R} \\ x &\longmapsto \pi x. \end{aligned}$$

Mængden X, hvorpå f er defineret, kaldes **domænet** (i gymnasiet anvendes ofte betegnelsen *definitionsmængden*). **Billedet** (i gymnasiet kaldet *værdimængden*) er mængden $f(X) = \{f(x) \mid x \in X\}$ bestående af alle de elementer i Y, som kan skrives som $f(x)$ for et passende x i X. Med de konkrete eksempler herover er således

$$f(\mathbb{R}) = [0, \infty)$$

og

$$g(\mathbb{Z}) = \{\pi x \mid x \in \mathbb{Z}\} = \{\ldots, -2\pi, -\pi, 0, \pi, 2\pi, \ldots\}.$$

Vi bemærker, at det sagtens kan gælde, at $f(X)$ er en ægte delmængde af Y; dette er eksempelvis tilfældet med de to funktioner herover. Y er altså blot én eller anden mængde, hvor elementerne $f(x)$ ligger for alle x i X. Vi kunne for så vidt også have valgt at betragte f som en funktion $f\colon \mathbb{R} \to [0, \infty)$. Der er med andre ord for den samme funktion f flere muligheder for valg af Y i

[3] Læsere, der måtte finde udtrykket »regel« en smule upræcist, henvises til lærebogen i *Perspektiver i matematikken*.

notationen $f: X \to Y$. Generelt skal det dog bemærkes, at det på universitet spiller en langt større rolle end på gymnasiet, *hvor* funktioner er defineret henne, og *hvor* de tager værdier. Væn jer derfor til notationen $f: X \to Y$!

Vi træffer også funktioner af flere variable, eksempelvis

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

som vi lader være defineret for alle $x,y,z \in \mathbb{R}$. I dette tilfælde betragtes f betragtes som en funktion $f: \mathbb{R}^3 \to \mathbb{R}$, idet $f(x,y,z)$ så blot er forkortet notation for $f((x,y,z))$, hvor (x,y,z) jo netop er et element i $\mathbb{R}^3$.

Kapitel 2

Lineær algebra

I dette kapitel gives et par ekstra definitioner og resultater fra lineær algebra. Vi giver for det første en eksakt formulering af echelonformerne:

Definition 2.1. *En matrix er på **echelonform**, hvis*

(i) Alle rækker bestående af ene nuller står nederst, og

(ii) det første tal forskelligt fra nul (kaldet pivoten*) i enhver række står til højre for det første tal forskelligt fra nul i alle rækker ovenover.*

*Matricen er på **reduceret echelonform**, hvis der endvidere gælder, at*

(iii) Alle pivoter er 1.

(iv) Der står nul i alle indgange over pivoterne.

Følgende resultat er af ren teoretisk værdi, men stadig vigtigt:

Proposition 2.2. *Lad $A\mathbf{x} = \mathbf{b}$ og $B\mathbf{x} = \mathbf{c}$ være matrixligningssysstemer. Hvis matricerne $(A \mid \mathbf{b})$ og $(B \mid \mathbf{c})$ er rækkeækvivalente, så har de to ligningssystemer ens løsningsmængder.*

Endvidere kobles rækkeækvivalens sammen med echelonformen ved følgende resultat:

Proposition 2.3. *Enhver matrix kan bringes på reduceret echelonform, og denne form er entydig.*

Noget af det smukke ved den lineære algebra er den elegante teori omkring invertible matricer. Der er mange forskellige ækvivalente kriterier, som man kan bruge til at afgøre, om en matrix er invertibel eller ej. Hvis omvendt en matrix er invertibel, får man straks en hel stribe af andre resultater til sin rådighed. I Sætning 2.4 står en række ækvivalente måder at formulere det udsagn, at en matrix er invertibel. Hvis blot ét af disse udsagn er sandt, er alle de andre det også. Hvis omvendt blot ét er falsk, gælder det også de andre. Dette er vist i Sætning 2.5 (for alle m gælder, at $\neg(m)$ er negationen af (m)).

Sætning 2.4. *Lad A være en $n \times n$-matrix. Så er følgende udsagn ækvivalente, hvilket betyder, at hvis blot ét af dem er sandt, så er alle de andre det også.*

(1) *A er invertibel.*

(2) *Der findes en kvadratisk matrix B, så $AB = BA = I$.*

(3) *Der findes en kvadratisk matrix C, så $AC = I$.*

(4) *Der findes en kvadratisk matrix D, så $DA = I$.*

(5) *For* ***enhver*** *vektor $\mathbf{b} \in \mathbb{R}^n$ har matrixligningssystemet $A\mathbf{x} = \mathbf{b}$* ***mindst*** *én løsning.*

(6) *For* ***enhver*** *vektor $\mathbf{b} \in \mathbb{R}^n$ har matrixligningssystemet $A\mathbf{x} = \mathbf{b}$* ***højst*** *én løsning.*

(7) *For* ***enhver*** *vektor $\mathbf{b} \in \mathbb{R}^n$ har matrixligningssystemet $A\mathbf{x} = \mathbf{b}$* ***præcist*** *én løsning.*

(8) *Der* ***findes*** *en vektor $\mathbf{b} \in \mathbb{R}^n$, så matrixligningssystemet $A\mathbf{x} = \mathbf{b}$ har* ***præcist*** *én løsning.*

(9) *Hvis en vektor $\mathbf{x} \in \mathbb{R}^n$ opfylder $A\mathbf{x} = \mathbf{0}$, så er $\mathbf{x} = \mathbf{0}$.*

(10) *A er rækkeækvivalent til identitetsmatricen I, dvs. $A \sim I$.*

(11) *A^T er invertibel.*

(12) *Der* ***findes*** *et heltal $k \geq 1$, så A^k er invertibel.*

(13) *For* ***alle*** *heltal $k \geq 1$ gælder, at A^k er invertibel.*

(14) *Determinanten af A er forskellig fra nul.*

(15) *A har rang n.*

(16) *Nulrummet for A er $N(A) = \{\mathbf{0}\}$.*

(17) *Billedrummet for A er $R(A) = \mathbb{R}^n$.*

(18) *Søjlerne i A udgør en basis for $\mathbb{R}^n$.*

(19) *Rækkerne i A udgør en basis for $\mathbb{R}^n$ (idet de transponeres).*

(20) *A kan skrives som et produkt af elementære matricer.*

(21) *0 er* ***ikke*** *en egenværdi for A.*

Lad nu $L\colon \mathbb{R}^n \to \mathbb{R}^n$ være den lineære afbildning givet ved $L(\mathbf{x}) = A\mathbf{x}$ for $\mathbf{x} \in \mathbb{R}^n$. Så kan vi tilføje et par punkter til listen med begreber fra Perspektiver i matematikken:

(22) *L er bijektiv.*

(23) *L er injektiv.*

(24) *L er surjektiv.*

Sætning 2.5. *Lad A være en $n \times n$-matrix. Så er følgende udsagn ækvivalente:*

¬(1) *A er singulær (dvs. ikke-invertibel).*

¬(2) *For alle kvadratiske matricer B gælder enten $AB \neq I$ eller $BA \neq I$.*

¬(3) *For alle kvadratiske matricer C gælder, at $AC \neq I$.*

¬(4) *For alle kvadratiske matricer D gælder, at $DA \neq I$.*

¬(5) *Der **findes** vektor $\mathbf{b} \in \mathbb{R}^n$, så matrixligningssystemet $A\mathbf{x} = \mathbf{b}$ **ikke** har en løsning.*

¬(6) *Der **findes** en vektor $\mathbf{b} \in \mathbb{R}^n$, så matrixligningssystemet $A\mathbf{x} = \mathbf{b}$ har **uendeligt mange** løsninger.*

¬(7) *Der **findes** en vektor $\mathbf{b} \in \mathbb{R}^n$, så matrixligningssystemet $A\mathbf{x} = \mathbf{b}$ ikke har **præcist én** løsning.*

¬(8) *For **enhver** vektor $\mathbf{b} \in \mathbb{R}^n$ har matrixligningssystemet $A\mathbf{x} = \mathbf{b}$ enten **ingen** eller **uendeligt mange** løsninger.*

¬(9) *Der findes en vektor $\mathbf{x} \in \mathbb{R}^n$ med $\mathbf{x} \neq \mathbf{0}$, men så $A\mathbf{x} = \mathbf{0}$.*

¬(10) *A er ikke rækkeækvivalent til identitetsmatricen I, dvs. $A \nsim I$. Med andre ord: Hvis A bringes på reduceret echelonform, vil der være mindst én nulrække.*

¬(11) *A^T er singulær.*

¬(12) *For **alle** heltal $k \geq 1$ gælder, at A^k er singulær.*

¬(13) *Der **findes** et heltal $k \geq 1$, så A^k er singulær.*

¬(14) *Determinanten af A er nul.*

¬(15) *Rangen af A er strengt mindre end n.*

¬(16) *Nulrummet $N(A)$ for A er et ikke-trivielt underrum af $\mathbb{R}^n$, dvs. et underrum som ikke er det trivielle underrum $\{\mathbf{0}\}$.*

¬(17) *Billedrummet $R(A)$ for A er et ægte underrum af $\mathbb{R}^n$, dvs. et underrum som ikke er hele $\mathbb{R}^n$.*

¬(18) *Søjlerne i A er ikke en basis for $\mathbb{R}^n$.*

¬(19) *Rækkerne i A er ikke en basis for $\mathbb{R}^n$ (idet de transponeres).*

¬(20) *A kan **ikke** skrives som produkt af elementære matricer.*

¬(21) *0 er en egenværdi for A.*

¬(22) *L er ikke bijektiv.*

¬(23) *L er ikke injektiv.*

¬(24) *L er ikke surjektiv.*

2.1 Baser og lineær uafhængighed

I TEORETISK SAMMENHÆNG er følgende lille samling af resultater af største vigtighed.

Proposition 2.6. *Lad $U \subseteq \mathbb{R}^n$ være et underrrum. Så findes en basis for U.*

Man har i mange tilfælde en udspændende mængde for et underrum, men som indeholder for mange vektorer til at udgøre en basis. Imidlertid har vi heldigvis følgende resultat:

Proposition 2.7. *Antag, at U er et underrum af $\mathbb{R}^n$ udspændt af vektorerne $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m$. Så kan disse vektorer udtyndes til en basis. Med dette menes, at der findes en basis $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k$ for U med*

$$\{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_k\} \subseteq \{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m\}.$$

Et system $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m$ af vektorer i $\mathbb{R}^n$ kaldes **lineært uafhængige**, hvis de udgør en basis for det underrum, som de frembringer. En basis er pr. definition lineært uafhængig. Følgende resultat motiverer denne definition:

Proposition 2.8. *Lad $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_m$ være et system af lineært uafhængige vektorer i et underrum U af $\mathbb{R}^n$. Så kan disse udvides til en basis, med hvilket menes, at der findes vektorer $\mathbf{u}_{m+1}, \mathbf{u}_{m+2}, \dots, \mathbf{u}_{m+k}$, så $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_{m+k}$ er en basis for U.*

Endeligt er det i mange sammenhænge både praktisk og teoretisk vigtigt, at vi altid har adgang til en *ortonormalbasis*.

Proposition 2.9. *For ethvert underrum af $\mathbb{R}^n$ findes en ortonormalbasis.*

2.2 Egenværdier og egenvektorer

LAD A VÆRE en kvadratisk matrix af orden n, og lad p_A være det karakteristiske polynomium for A. Vi noterer indledningsvist følgende.

Proposition 2.10.

(i) Højestegradsleddet i $p_A(\lambda)$ er $(-1)^n \lambda^n$.

(ii) Det konstante led i p_A (dvs. a_0 med notationen fra ligning (5.1)) er $\det(A)$.

Bevis. Udsagn (i) ligger uden for rammerne af, hvad det er muligt at bevise her. Men (ii) følger af, at dette led er givet ved $p_A(0) = \det(A - 0I) = \det(A)$. □

Betragt nu p_A som et polynomium over $\mathbb{C}$. Derved får vi jf. Sætning 5.7 en faktorisering af p_A på formen

$$p_A(\lambda) = a(\lambda - \lambda_1)^{n_1}(\lambda - \lambda_2)^{n_2} \cdots (\lambda - \lambda_r)^{n_r},$$

for passende $a, \lambda_1, \lambda_2, \dots, \lambda_r \in \mathbb{C}$ og heltal $n_1, n_2, \dots, n_r \geq 1$. Her udgør tallene $\lambda_1, \lambda_2, \dots, \lambda_r$ samtlige (komplekse) rødder i p_A. Hvis λ_i er reel, er den således en egenværdi for A; hvis λ_i er ikke-reel, er den en egenværdi for A betragtet som kompleks matrix, hvilket imidlertid ligger uden for rammerne af dette kursus.

Proposition 2.11. *Der gælder den nyttige formel*

$$\det(A) = \lambda_1^{n_1} \lambda_2^{n_2} \cdots \lambda_r^{n_r}.$$

Hvis det karakteristiske polynomium for A kun har reelle rødder, gælder således, at produktet af egenværdierne (talt med multiplicitet[1]) er determinanten af A.

Bevis. Grundet Proposition 2.10(i) er højestegradsleddet i $(-1)^n p_A(\lambda)$ lig λ^n. Derved giver Opgave 5.25, at det konstante led i $(-1)^n p_A(\lambda)$ er

$$(-1)^n \lambda_1^{n_1} \lambda_2^{n_2} \cdots \lambda_r^{n_r}.$$

Men samtidigt giver Proposition 2.10(ii), at det konstante led i $(-1)^n p_A(\lambda)$ også er givet ved $(-1)^n \det(A)$. Vi slutter, at $\det(A) = \lambda_1^{n_1} \lambda_2^{n_2} \cdots \lambda_r^{n_r}$ som ønsket. □

Tallet n_i har konkrete konsekvenser inden for den lineære algebra, da det sætter en øvre grænse for dimensionen af egenrummet E_{λ_i} for λ_i:

Sætning 2.12. *Der gælder* $\dim E_{\lambda_i} \leq n_i$.

[1] Med termen »talt med multiplicitet« menes, at hvis λ_i har multiplicitet n_i, tælles λ_i med i produktet n_i gange.

KAPITEL 3

INTEGRALET PÅ GYMNASIET OG UNIVERSITETET

FØLGENDE KAPITEL sammenligner definitionen på *integralet*, som denne blev givet på gymnasiet, og som den nu er indført på universitet. Formålet er først og fremmest at gøre opmærksom på, at der *ikke* er tale om samme definition. Endvidere er én af hovedpointerne, at integralet ikke »bare« er en invers regningsart til differentiation, men en selvstændig og meget dyb matematisk konstruktion.

3.1 På gymnasiet

I DET FØLGENDE introducerer jeg kort integralet, som jeg selv fik det indført i gymnasiet.

Lad $f: [a,b] \to \mathbb{R}$ være en kontinuert funktion. Lad endvidere $A: [a,b] \to \mathbb{R}$ være *arealfunktionen* for f i den forstand, at $A(t)$ er arealet under f fra a til t for alle $t \in [a,b]$.

Sætning 3.1 (Analysens Fundamentalsætning). *Funktionen A er differentiabel, og $A' = f$.*

Med andre ord er A en stamfunktion til f. Lad nu $F: [a,b] \to \mathbb{R}$ være en vilkårlig stamfunktion til f. Så er også funktionen $A - F$ differentiabel grundet elementære regneregler for differentation, og vi har

$$(A-F)' = A' - F' = 0.$$

Ergo er $A - F$ en konstant funktion. Specielt gælder, at $(A-F)(t) = (A-F)(a)$ for alle $t \in [a,b]$, dvs.

$$A(t) - F(t) = A(a) - F(a).$$

Da $A(a) = 0$ (arealet under f fra a til a er nul), kan ovenstående omskrives til

$$A(t) = F(t) - F(a). \tag{3.1}$$

Med udgangspunkt i dette resultat definerer vi

Definition 3.2. *Lad $f : [a,b] \to \mathbb{R}$ være en kontinuert funktion, og lad F være en vilkårlig stamfunktion for f (en sådan findes grundet Analysens Fundamentalsætning). Så definerer vi*

$$\int_a^b f(x)\,dx = F(b) - F(a).$$

Vi ser, at denne definition af integralet er veldefineret, idet den ikke afhænger af valget af stamfunktionen F (der er altid uendeligt mange stamfunktioner til en given funktion). Dette skyldes, at ligning (3.1) er opfyldt for en vilkårlig stamfunktion F.

Bemærkning 3.3. Vi har *kun* defineret integration for kontinuerte funktioner.

Vi har ydermere i en vis forstand *defineret*, at integration er en invers regningsart til differentiation. Nærmere bestemt er differentiation en *venstreinvers* til integration i den forstand, at

$$\frac{d}{dt}\int_a^t f(x)\,dx = f(t) \qquad (t \in [a,b]).$$

Vi noterer, at differentiation ikke nødvendigvis er en *højreinvers* til integration; med andre ord gælder det *ikke* generelt, at

$$\int_a^b F'(x)\,dx = F(b) - F(a)$$

når $F\colon [a,b] \to \mathbb{R}$ er en differentiabel funktion. Dette integral er nemlig ikke nødvendigvis veldefineret; integralet er nemlig som sagt kun defineret for kontinuerte funktioner, og vi ved ikke nødvendigvis, om F' er kontinuert; se Eksempel 3.10 nedenfor for et modeksempel. *Hvis* F' er kontinuert, og det vil ofte være tilfældet, gælder det imidlertid. △

3.2 På universitetet

Jeg giver nu en indføring i integralet, som det præsenteres i Stewart. Denne definition ligger tættere på den formelle definition end den, der præsenteres i gymnasiet.

Lad $f : [a,b] \to \mathbb{R}$ være en vilkårlig (ikke nødvendigvis kontinuert) funktion. For alle heltal $n \geq 1$ lader vi D_n være en *inddeling* af $[a,b]$ med $n+1$ punkter, dvs. en samling punkter $t_0, t_1, \ldots, t_n$ med $a = t_0 < t_1 < \cdots < t_n = b$. For $i = 1, 2, \ldots, n$ vælges et vilkårligt $x_i^* \in [t_{i-1}, t_i]$. Vi lader så

$$R_n(f) = \sum_{i=1}^{n} f(x_i^*)(t_i - t_{i-1})$$

være den n'te *Riemann-sum* hørende til inddelingen D_n og de valgte punkter $x_1^*, x_2^*, \ldots, x_n^*$.

Idet vi for alle heltal $n \geq 1$ har ladet en sådan inddeling D_n være givet, har vi en følge $\{D_n\}$ af inddelinger. Vi antager, at den maksimale forskel $t_i - t_{i-1}$ imellem to inddelingspunkter, altså tallet

$$\max\{t_i - t_{i-1} \mid 1 \leq i \leq n\},$$

går imod 0 for n gående imod uendelig.

Definition 3.4. *Hvis grænseværdien*

$$\lim_{n\to\infty} R_n(f)$$

findes og ikke afhænger af valget af inddelingen D_n eller punkterne $x_1^*, x_2^*, \dots, x_n^*$, så kaldes f ***integrabel****. I bekræftende fald kaldes grænseværdien* ***integralet af f fra a til b*** *og skrives*

$$\int_a^b f(x)\,dx.$$

Som sagt har vi på ingen måde i definitionen antaget, at funktionen f er kontinuert. Men man kan vise, at

Sætning 3.5. *Enhver kontinuert funktion er integrabel.*

Kontinuerte funktioner har en ganske særlig interesse i forbindelse med integration af den simple grund, at følgende overraskende resultat gør integralet af en kontinuert funktion usædvanligt let at udregne:

Sætning 3.6 (Analysens Fundamentalsætning). *Lad f være en kontinuert funktion. Så er funktionen $A\colon [a,b] \to \mathbb{R}$ givet ved*

$$A(t) = \int_a^t f(x)\,dx \qquad (t \in [a,b])$$

differentiabel, og $A' = f$.

Hvis nu F er en vilkårlig stamfunktion, kan vi ligesom før vise, at

$$\int_a^b f(x)\,dx = A(b) = F(b) - F(a).$$

Dermed kan denne stamfunktion F anvendes til at udregne integralet af vores vilkårlige funktion f. A priori har begreberne integration og differentiation for så vidt overhovedet ikke noget med hinanden at gøre. Men Analysens Fundamentalsætning binder dem alligevel på overraskende vis sammen, idet den tillader os at udregne integralet for enhver funktion, hvis vi blot kan finde en stamfunktion for den. Resultatet er yderst anvendeligt af den simple grund, at differentiation er blandt de smukkeste operationer i matematikken; grundet de mange regneregler for differentiation er den afledte af en vilkårlig funktion meget let at finde. Omvendt gælder derfor, at der for en vilkårlig kontinuert funktion er en rigtigt god chance for, at man kan finde en pæn stamfunktion til den.

Bemærkning 3.7. Differentiation og integration er *ikke* inverse regningsarter. For det første findes der integrable funktioner, som ikke er kontinuerte. △

Eksempel 3.8. Funktionen $f\colon [0,2] \to \mathbb{R}$ givet ved

$$f(x) = \begin{cases} 3x^2 & \text{hvis } 0 \le x < 1 \\ 7x^3 & \text{hvis } 1 \le x \le 2 \end{cases}$$

er ikke kontinuert i punktet $x = 1$. Men integralet giver fin mening, da diskontinuiteten her betyder stadig mindre, når inddelingen af $[0,2]$ bliver stadig finere. Faktisk er

$$\int_0^2 f(x)\,dx = \int_0^1 3x^2\,dx + \int_1^2 7x^3\,dx = 1 + \tfrac{7}{4}(2^4 - 1) = \tfrac{109}{4}.$$ ○

Funktionen herover er kun diskontinuert i et enkelt punkt; men hvis man er ond, kan man finde funktioner, der er diskontinuerte i mange flere punkter, men hvor integralet stadigvæk er veldefineret. Disse betragtes dog som for teknisk svære i denne sammenhæng.

Bemærkning 3.9. For det andet gælder *ikke* for en vilkårlig differentiabel funktion $F\colon [a,b] \to \mathbb{R}$, at

$$\int_a^b F'(x)\,dx = F(a) - F(b).$$

Det gælder, *hvis* funktionen F' er kontinuert, i hvilket tilfælde vi kan anvende Analysens Fundamentalsætning til at nå frem til resultatet. Men den afledte af en funktion behøver ikke være kontinuert, som følgende eksempel illustrerer: △

Eksempel 3.10. Lad $f\colon [0,1] \to \mathbb{R}$ være givet ved

$$f(x) = \begin{cases} x^2 \sin\left(\frac{1}{x^2}\right) & \text{hvis } x \neq 0 \\ 0 & \text{hvis } x = 0. \end{cases}$$

For $x \neq 0$ er f differentiabel med

$$f'(x) = 2x\sin\left(\tfrac{1}{x^2}\right) + x^2\left(-\tfrac{2}{x^3}\right)\cos\left(\tfrac{1}{x^2}\right) = 2x\sin\left(\tfrac{1}{x^2}\right) - \tfrac{2}{x}\cos\left(\tfrac{1}{x^2}\right)$$

Endvidere er f er differentiabel i $x = 0$ med $f'(0) = 0$, idet det for alle $x \in (0,1]$ gælder, at

$$\frac{f(x) - f(0)}{x - 0} = \frac{x^2\sin(1/x^2) - 0}{x - 0} = x\sin\left(\tfrac{1}{x^2}\right).$$

Men dette udtryk går imod 0 for x gående imod 0, idet

$$\left|x\sin\left(\tfrac{1}{x^2}\right)\right| \le |x| \to 0 \quad \text{for } x \to 0.$$

Vi konkluderer, at f er differentiabel på hele sit definitionsområde med

$$f'(x) = \begin{cases} 2x\sin\left(\frac{1}{x^2}\right) - \frac{2}{x}\cos\left(\frac{1}{x^2}\right) & \text{for } x \neq 0 \\ 0 & \text{for } x = 0. \end{cases}$$

Vi ser, at denne funktion *ikke* er kontinuert i $x = 0$. Man kan oven i købet (hvis man har lidt mere formel integralteori) overbevise sig om, at f' ikke er integrabel på $[0,1]$. Dette skyldes faktoren $2/x$, som opfører sig meget eksplosivt omkring $x = 0$. ○

KAPITEL 4

DE KOMPLEKSE TAL

DE KOMPLEKSE TAL udgør sammen med de reelle tal de to vigtigste talobjekter i moderne matematik på tværs af alle discipliner. De kan ses som en udvidelse af de reelle tal, og de fremkommer uformelt ved, at vi »opfinder« et nyt tal i med egenskaben $i^2 = -1$, hvorefter vi blot »regner som vi plejer«. Dette er også udgangspunktet for Stewarts indføring af de komplekse tal. Det er dog på ingen måde åbenlyst, at vi ikke støder ind i en modstrid ved blot at antage, at vi kan »regne som vi plejer«. I følgende kapitel gives derfor en mere formel og – ud fra en matematisk synsvinkel – mere tilfredsstillende indføring i teorien om de komplekse tal, end Stewart giver. Grundideen er den samme som hos Stewart, nemlig at lade de komplekse tal bestå af alle summer af et reelt tal samt et reelt multiplum af tallet i, dvs.

$$\mathbb{C} = \{x + yi \mid x, y \in \mathbb{R}\}.$$

Hvis x og y er reelle tal og $z = x + yi$, så kaldes x *realdelen* af z, mens y kaldes *imaginærdelen*.

Lad os lægge ud med at motivere den formelle definition. Vi ønsker som nævnt at konstruere de komplekse tal på en måde, så regnereglerne minder om de velkendte regneregler over $\mathbb{R}$. Vi vil for det første gerne addere komplekse tal ved at addere real- og imaginærdelene hver for sig, altså

$$(x + yi) + (u + vi) = (x + u) + (y + v)i \tag{4.1}$$

for alle $x, y, u, v \in \mathbb{R}$. For det andet vil egenskaben $i^2 = -1$ medføre (hvis vi vel at mærke *kan* regne, som vi plejer), at multiplikation nødvendigvis må have formen

$$(x + yi) \cdot (u + vi) = xu + xvi + yui + yvi^2 = (xu - yv) + (xv + yu)i \tag{4.2}$$

for alle $x, y, u, v \in \mathbb{R}$. Lad os nu forsøge formelt at konstruere et talobjekt, der har præcist de ovenfor nævnte egenskaber. Idet talobjektet skal bestå af par af to reelle tal, er det naturligt at anvende $\mathbb{R}^2$ som udgangspunkt for vores definition.

Definition 4.1. *De **komplekse tal** $\mathbb{C}$ er $\mathbb{R}^2$ udstyret med addition*

$$(x,y)+(u,v)=(x+u,y+v)$$

og multiplikation

$$(x,y)\cdot(u,v)=(xu-yv,xv+yu)$$

for alle $(x,y),(u,v)\in\mathbb{C}=\mathbb{R}^2$.

Vi identificerer det reelle tal x med det komplekse tal $(x,0)$ og sætter $i=(0,1)$. Med andre ord kan det komplekse tal (x,y) skrives $x+yi$. Ved at indsætte dette i definitionen herover fremkommer nu netop formlerne (4.1) og (4.2). Med førnævnte identifikation kan vi således opfatte $\mathbb{R}$ som en delmængde af $\mathbb{C}$.

Følgende egenskaber ved de komplekse tal følger nu umiddelbart af definitionen:

Proposition 4.2. *Lad z,w,q være komplekse tal. Så gælder følgende:*

(i) *Addition er kommutativ:* $z+w=w+z$.

(ii) *Addition er associativ:* $(z+w)+q=z+(w+q)$.

(iii) $0=0+0i$ *er et neutralt element for addition:* $z+0=0+z=z$.

(iv) *Multiplikation er kommutativ:* $z\cdot w=w\cdot z$.

(v) *Multiplikation er associativ:* $(z\cdot w)\cdot q=z\cdot(w\cdot q)$.

(vi) $1=1+0i$ *er et neutralt element for multiplikation:* $z\cdot 1=1\cdot z=z$.

(vii) *Den distributive lov gælder:* $z\cdot(w+q)=z\cdot w+z\cdot q$.

Lad os nu vende os imod spørgsmålet, om *division* er muligt i de komplekse tal, altså om udtrykket z/w er veldefineret for $z,w\in\mathbb{C}$ og $w\neq 0$. Det vil være nok at vise, at der findes et inverst element w^{-1} til w, så $ww^{-1}=1$; thi i dette tilfælde kan vi blot definere $z/w=zw^{-1}$. Det er på ingen måde en selvfølge, at et sådant inverst element w^{-1} findes. Der er mange algebraiske strukturer i matematikken, hvor ikke alle elementer forskellige fra nul har en multiplikativ invers. Matricer er et i nærværende kursus oplagt eksempel. Et andet eksempel (som ellers opfylder samtlige regneregler i Proposition 4.2) er mængden

$$\mathbb{Z}_4=\{[0],[1],[2],[3]\}$$

af restklasser modulo 4 (kendt fra *Perspektiver i matematikken*). Her gælder nemlig, at restklassen $[2]$ ikke har et inverst element. Vi har nemlig

$$\begin{aligned}
&[0][2]=[0] &\qquad& [1][2]=[2]\\
&[2][2]=[0] && [3][2]=[2].
\end{aligned}$$

Der findes altså intet $[x]\in\mathbb{Z}_4$ med $[x][2]=[1]$.

I de komplekse tal er vi imidlertid heldige:

Proposition 4.3. *Lad w være et komplekst tal forskeligt fra nul, og skriv $w = u+vi$ for reelle tal u og v. Sættes*

$$q = \frac{u}{u^2+v^2} - \frac{v}{u^2+v^2}i, \tag{4.3}$$

gælder $wq = 1$. Ydermere er q entydigt bestemt ved denne egenskab.

Bevis. Ud fra definitionen af produktet i de komplekse tal har vi, at

$$\begin{aligned} wq &= (u+vi)\Big(\frac{u}{u^2+v^2} - \frac{v}{u^2+v^2}i\Big) \\ &= \frac{u^2}{u^2+v^2} - \frac{-v^2}{u^2+v^2} + \Big(-\frac{uv}{u^2+v^2} + \frac{uv}{u^2+v^2}\Big)i = \frac{u^2+v^2}{u^2+v^2} + 0i = 1 \end{aligned}$$

som ønsket. Hvis endvidere q' er et vilkårligt komplekst tal med $wq' = 1$, så er

$$q' = q' \cdot 1 = q' \cdot (w \cdot q) = (q' \cdot w) \cdot q = 1 \cdot q = q$$

grundet de allerede indførte egenskaber ved de komplekse tal. Dette viser netop, at q er entydigt bestemt ved egenskaben $wq = 1$. □

Idet q nævnt i propositionen er entydigt, kan vi skrive det som w^{-1}. Idet vi definerer $z/w = zw^{-1}$ for alle komplekse tal z og w med $w \neq 0$, muliggøres division i de komplekse tal. Man kan overbevise sig om, at vi med indførslen af division mere kompakt kan skrive ligning (4.3) som

$$\frac{1}{u+vi} = \frac{u-vi}{u^2+v^2},$$

når $u, v \in \mathbb{R}$ ikke begge er nul. Hvis endvidere x og y er reelle tal, gælder nu formlen

$$\frac{x+yi}{u+vi} = \frac{(x+yi)(u-vi)}{u^2+v^2} = \frac{(x+yi)(u-vi)}{(u+vi)(u-vi)}.$$

Dette viser præcist det trick, som Stewart anvender: Hvis vi skal dividere to komplekse tal, forlænger vi blot brøken med det kompleks-konjugerede af nævneren. Derved bliver nævneren reel, og vi får et komplekst tal på den sædvanlige form som linearkombination af 1 og i.

Vi noterer nu følgende regneregler for division, som følger umiddelbart af definitionen:

Proposition 4.4. *For alle $z, w, q, r \in \mathbb{C}$ med $w, r \neq 0$ gælder*

(i) $\dfrac{z}{w} \cdot \dfrac{q}{r} = \dfrac{zq}{wr}$.

(ii) $\dfrac{z}{w} + \dfrac{q}{r} = \dfrac{zr+qw}{wr}$.

(iii) $\dfrac{rz}{rw} = \dfrac{z}{w}$.

(iv) Hvis endvidere $q \neq 0$, er $\dfrac{z/w}{q/r} = \dfrac{zr}{qw}$.

4.1 Den komplekse eksponentialfunktion

Eksponentialfunktionen

$$\begin{aligned}\exp\colon \mathbb{R} &\to \mathbb{R}\\ x &\mapsto \mathrm{e}^x\end{aligned}$$

defineres løst på gymnasiet som »e ganget med sig selv x gange«. Dette har fin mening, når x tager værdier i $\mathbb{Z}$, og det kan også med god vilje generaliseres til værdier i $\mathbb{Q}$, hvis vi for alle $s, t \in \mathbb{Z}$ med $t \neq 0$ opfatter $\mathrm{e}^{s/t}$ som $(\sqrt[t]{\mathrm{e}})^s$. Men denne logik fejler for $x \notin \mathbb{Q}$; det giver eksempelvis ikke mening at gange noget med sig selv π gange.

På videregående niveau er der kun én korrekt måde at tænke på eksponentialfunktionen på, nemlig som funktionen

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \qquad (x \in \mathbb{R})$$

(okay, der er faktisk to; den anden, som er langt mindre vigtig, er formlen $\exp(x) = \lim_{n\to\infty}(1 + x/n)^n$). Nu er e^x blot en alternativ notation for $\exp(x)$ for $x \in \mathbb{R}$. Vi definerer tallet e ved $\mathrm{e} = \exp(1)$. Alle regneregler for eksponentialfunktionen bør således udledes af ovenstående formel. Eksempelvis får vi ved anvendelse af Sætning 8.6.2 i Stewart, at

$$\begin{aligned}\frac{d}{dx}\exp(x) &= \sum_{n=0}^{\infty} \frac{d}{dx}\frac{x^n}{n!} = \sum_{n=0}^{\infty} n\frac{x^{n-1}}{n!} = \sum_{n=1}^{\infty} n\frac{x^{n-1}}{n!}\\ &= \sum_{n=1}^{\infty} \frac{x^{n-1}}{(n-1)!} = \sum_{m=0}^{\infty} \frac{x^m}{m!} = \exp(x).\end{aligned}$$

Det er også muligt at udlede regnereglen $\exp(x+y) = \exp(x)\exp(y)$ for $x, y \in \mathbb{R}$ med udgangspunkt i samme formel. Vi kan herefter definere eksponenter af vilkårlige reelle tal $a > 0$ ved

$$a^x = \exp(x \ln(a)) \qquad (x \in \mathbb{R}).$$

Her har vi anvendt logaritmefunktionen $\ln\colon (0,\infty) \to \mathbb{R}$, som enten kan defineres som den inverse funktion til eksponentialfunktionen (hvis man viser, at en sådan invers funktion faktisk findes) eller ved formlen

$$\ln(x) = \int_1^x \frac{1}{t}\,dt \qquad (x \in (0,\infty)).$$

Den oplagte måde at generalisere eksponentialfunktionen til komplekse værdier er nu simpelthen at definere

$$\mathrm{e}^z = \exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!} \qquad (z \in \mathbb{C}).$$

Man kan vise, at denne række er konvergent for alle $z \in \mathbb{C}$, og at regnereglen $\mathrm{e}^{z+w} = \mathrm{e}^z\mathrm{e}^w$ også er gyldig for $z, w \in \mathbb{C}$. Endvidere kan man overbevise sig om, at der for alle x i $\mathbb{R}$ gælder formlen

$$\mathrm{e}^{ix} = \cos(x) + i\sin(x),$$

som kaldes *Eulers formel* og regnes som ét af de smukkeste resultater i matematikken.

Idet cosinus er en lige funktion, mens sinus er ulige[1], gælder for alle x i $\mathbb{R}$, at

$$\begin{aligned} e^{ix} + e^{-ix} &= \cos(x) + \cos(-x) + i\sin(x) + i\sin(-x) \\ &= \cos(x) + \cos(x) + i\sin(x) - i\sin(x) = 2\cos(x). \end{aligned}$$

Tilsvarende får vi formlen

$$e^{ix} - e^{-ix} = 2i\sin(x)$$

for alle x i $\mathbb{R}$. Med andre ord er

$$\cos(x) = \tfrac{1}{2}\Big(e^{ix} + e^{-ix}\Big) \quad \text{og} \quad \sin(x) = \tfrac{1}{2i}\Big(e^{ix} - e^{-ix}\Big) \qquad (x \in \mathbb{R}).$$

En oplagt måde at generaliser cosinus- og sinusfunktionerne til komplekse værdier er derfor simpelthen at definere

$$\cos(z) = \tfrac{1}{2}\Big(e^{iz} + e^{-iz}\Big) \quad \text{og} \quad \sin(z) = \tfrac{1}{2i}\Big(e^{iz} - e^{-iz}\Big) \qquad (z \in \mathbb{C}).$$

Disse formler kaldes ofte *Eulers formler* (ikke at forveksle med den netop indførte *Eulers formel*) og er de mest generelle definitioner af cosinus og sinus. Det er ikke svært at udlede de sædvanlige sum- og produktformlen for cosinus og sinus med udgangspunkt i ovenstående formler samt de elementære regneregler for den komplekse eksponentialfunktion.

Stewart indfører den polære form af et komplekst tal som formen

$$z = r(\cos(\theta) + i\sin(\theta)),$$

hvor $r \geq 0$ og $\theta \in \mathbb{R}$. Grundet Eulers formel kan vi omskrive denne formel til

$$z = re^{i\theta}.$$

For mange matematikere (inklusive jeg selv) er det dette den »rigtige« polære form. Formlen

$$(r_1 e^{i\theta_1})(r_2 e^{i\theta_2}) = r_1 r_2 e^{i(\theta_1+\theta_2)} \qquad (r_1, r_2 \geq 0, \theta_1, \theta_2 \in \mathbb{R})$$

følger nu middelbart af elementære regneregler for eksponentialfunktionen.

4.2 Differentiation og integration af komplekse funktioner

Givet en funktion $f : I \to \mathbb{C}$, hvor $I \subseteq \mathbb{R}$ er et interval, kan vi skrive $f = g + hi$ for passende funktioner $g, h : I \to \mathbb{R}$. Vi ønsker at definere et differentiationsbegreb for sådan en funktion. Der er to oplagte måder, hvorpå man kunne gøre dette. Den første indskydelse kunne være at generalisere den sædvanlige definition for reelle funktioner og definere, at f er *differentiabel* i $x_0 \in I$, hvis grænseværdien

$$\lim_{h\to 0} \frac{f(x_0 + h) - f(x_0)}{h}$$

[1] En funktion $f : \mathbb{R} \to \mathbb{R}$ kaldes *lige*, hvis $f(-x) = f(x)$ for alle $x \in \mathbb{R}$. Hvis $f(-x) = -f(x)$, siges f at være *ulige*.

findes og så i bekræftende fald kalde den for den *afledte af f i x_0* og skrive den som $f'(x_0)$. Omvendt kunne man definere, at f er differentiabel i x_0, hvis både g og h er differentiable i dette punkt i sædvanlig forstand og så sætte

$$f'(x_0) = g'(x_0) + h'(x_0)i.$$

Heldigvis er disse to definitioner *ækvialente*, dvs. de giver samme resultat. Endvidere videreføres alle de sædvanlige regneregler (Leibniz' regel, sumreglen osv.) umiddelbart til komplekse funktioner. Hvis således $f_1, f_2 \colon I \to \mathbb{C}$ er differentiable i x_0 og $\alpha, \beta \in \mathbb{C}$, så er $f_1 f_2$ og $\alpha f_1 + \beta f_2$ differentiable i x_0, og

$$(f_1 f_2)'(x_0) = (f_1' f_2 + f_2' f_1)(x_0) \quad \text{og} \quad (\alpha f_1 + \beta f_2)'(x_0) = \alpha f_1'(x_0) + \beta f_2'(x_0).$$

Hvis $f_2(x_0) \neq 0$, er endvidere f_1/f_2 differentiabel i x_0, og

$$\left(\frac{f_1}{f_2}\right)'(x_0) = \frac{f_1'(x_0) f_2(x_0) - f_1(x_0) f_2'(x_0)}{f_2(x_0)^2}.$$

Hvis endeligt $J \subseteq \mathbb{R}$ er et interval og $u \colon J \to I$ er differentiabel i $y_0 \in J$, og hvis $x_0 = u(y_0)$, så er sammensætningen $f \circ u \colon J \to \mathbb{C}$ differentiabel i y_0, og

$$(f \circ u)'(y_0) = u'(y_0) \cdot (f' \circ u)(y_0),$$

præcist som vi er vant til fra *kædereglen*.

Når vi skal definere, at en funktion f er *integrabel*, er det mest oplagt at anvende den anden tilgang fra før og sige, at dette er tilfældet, hvis g og h er integrable. Hvis $I = [a, b]$, sætter vi så

$$\int_a^b f(x)\,dx = \int_a^b g(x)\,dx + i \int_a^b h(x)\,dx.$$

Med denne definition gælder Analysens Fundamentalsætning også over $\mathbb{C}$. Endvidere bliver integralet lineært, dvs. for integrable $f_1, f_2 \colon I \to \mathbb{C}$ og $\alpha, \beta \in \mathbb{C}$ er $\alpha f_1 + \beta f_2$ integrabel, og

$$\int_a^b (\alpha f_1 + \beta f_2)(x)\,dx = \alpha \int_a^b f_1(x)\,dx + \beta \int_a^b f_2(x)\,dx.$$

Hvis f_1 og f_2 endvidere er *kontinuert differentiable*, så gælder *partiel integration*:

$$\int_a^b f(x) g'(x)\,dx = [f(x)g(x)]_a^b - \int_a^b f'(x) g(x)\,dx.$$

Hvis $J = [c, d]$ og $u \colon J \to I$ er kontinuert differentiabel, mens $f \colon I \to \mathbb{C}$ er kontinuert, gælder også en kompleks version af integration ved substitution:

$$\int_c^d f(u(x)) u'(x)\,dx = \int_{u(c)}^{u(d)} f(y)\,dy.$$

Man kan også godt definere differentiation og integration for funktioner af komplekse variable; men teorien om dette er faktisk overraskende kompliceret og behandles først for alvor i kurset *Kompleks funktionsteori*.

Kapitel 5

Polynomier, rødder og division

Jeg foretager her en behandling af *polynomier* og de begreber og resultater relateret til disse, som I forventes at kunne mestre. Disse resultater behandles egentligt først senere i analyse- og algebrakurserne; imidlertid anvendes de ofte allerede i de foregående kurser uden at have fået en ordentlig introduktion. Her giver jeg derfor en kort indføring, hvor der er fokus på metode frem for teori, hvilket afspejler den måske lidt utraditionelle rækkefølge, hvori resultaterne præsenteres, samt den hyppige anvendelse af eksempler. 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 5.1. *Et* ***polynomium*** *over $\mathbb{K}$ er en funktion $f : \mathbb{K} \to \mathbb{K}$ på formen*

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \qquad (x \in \mathbb{K}), \tag{5.1}$$

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 (5.1). Da lader vi **graden** af f være det største heltal k, $0 \le k \le n$, 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 5.2(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 5.2. *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 $a_0, a_1, \ldots, a_n$ i ligning (5.1) 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 (5.1). 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 $a_0, a_1, \ldots, a_n, b_0, b_1, \ldots, b_m \in \mathbb{K}$ 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 (5.1) 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 5.3. *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 5.4 (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.

5.1 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 5.26 for et andet bevis, som ikke kræver yderligere forudsætninger).

Sætning 5.5. *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 5.6. 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 5.5 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

$$x^4 - 3x^3 + x^2 + 3x - 2 = (x-1)(x^3 - 2x^2 - x + 2) \tag{5.2}$$

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

$$f(x) = (x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_r)^{n_r}g(x) \qquad (x \in \mathbb{K}), \tag{5.3}$$

*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

$$f(x) = a(x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_r)^{n_r} \qquad (x \in \mathbb{C}). \tag{5.4}$$

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 5.5 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 (5.3). Hvis nu

$$f(x) = (x - \alpha_1)^{n_1}(x - \alpha_2)^{n_2}\cdots(x - \alpha_r)^{n_r}g(x) = 0, \tag{5.5}$$

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

$$f(x) = (x - \alpha_1)^{n_1}\Big((x - \alpha_1)^{m_1 - n_1}(x - \alpha_2)^{m_2}(x - \alpha_3)^{m_3}\cdots(x - \alpha_r)^{m_r}h(x)\Big). \tag{5.6}$$

Idet vi fratrækker ligning (5.5) 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 5.2(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 (5.6) 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 (5.5), 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. □

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

Korollar 5.8. *Et polynomium over $\mathbb{K}$ af grad n har højst n forskellige rødder.*

Bevis. Skriv som i Sætning 5.7 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 5.2(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. □

5.2 Polynomiers division

Jeg smed i Eksempel 5.6 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 5.9. Idet vi ved, at $x-1$ går op i $x^4-3x^3+x^2+3x-2$, kan vi altid finde polynomiet fra ligning (5.2) 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 5.10. 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 5.11 (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*

$$f = qd + r, \tag{5.7}$$

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

Bevis. Vi viser først eksistensen af den ønskede opskrivning fra ligning (5.7). 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 5.12 (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:

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

△

Eksempel 5.13. For fuldstændighedens skyld følger her, hvorledes de øvrige faktoriseringer fra Eksempel 5.6 kan findes via polynomiers division:

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

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

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 5.7 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 5.14. *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 5.5. Resultatet er faktisk et umiddelbart korollar til Sætning 5.11.

Bevis for Sætning 5.5. Anvend Sætning 5.11 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.

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

5.2. Går $x-1$ op i $x^2 - x - 6$?

5.3. Går $x+2$ op i $x^2 + x - 2$?

5.4. Find samtlige rødder i polynomiet $2x^3 - 2x^2 - 10x - 6$, og faktoriser polynomiet som i Sætning 5.7.

5.5. Find samtlige rødder i polynomiet $-x^3 + x^2 + 22x - 40$, og faktoriser polynomiet som i Sætning 5.7.

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

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

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

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

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

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

5.12. Faktoriser polynomiet $x^4 - 2x^3 - 3x^2 + 4x + 4$ som i Sætning 5.7.

5.13. Faktoriser polynomiet $x^3 - 9x^2 + 24x - 16$ som i Sætning 5.7.

5.14. Faktoriser polynomiet $x^3 - 11x^2 + 35x - 25$ som i Sætning 5.7.

5.15. Faktoriser polynomiet $-2x^3 - 8x^2 + 62x + 140$ som i Sætning 5.7.

5.16. Faktoriser polynomiet $x^4 - 12x^3 + 46x^2 - 60x + 25$ som i Sætning 5.7.

5.17. Faktoriser polynomiet $-x^4 - 2x^3 + 36x^2 - 88x + 64$ som i Sætning 5.7.

5.18. Faktoriser polynomiet $-2x^4 - 14x^3 + 26x^2 + 86x + 48$ som i Sætning 5.7.

5.19. 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 $A\mathbf{v} = \lambda\mathbf{v}$.

5.20. 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.

5.21. Vis, at ethvert polynomium over $\mathbb{R}$ af *ulige grad* har en rod i $\mathbb{R}$. *Vink: Opgave 5.20.*

5.22. 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 $\mathbb{R}$.

5.23. Lad f være et ikke-konstant polynomium over $\mathbb{C}$ med højestegradsled $a_n x^n$ (som i ligning (5.1)). Vis, at hvis f faktoriseres som i ligning (5.4), så er $a = a_n$.

5.24. Lad f være et ikke-konstant polynomium over $\mathbb{C}$ af grad n. Vis, at med notationen fra Sætning 5.7 er

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

5.25. 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 (5.1)). 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

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

5.26. Giv et bevis for Sætning 5.5, som ikke anvender Sætning 5.11.

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.

5.27. Kan man bruge Euklids algoritme på polynomier? (*Vink: Sammenlign Sætning 5.11 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 $d = pf + qg$.

5.28. Vis, at ethvert ikke-konstant polynomium over $\mathbb{R}$ uden rødder kan skrives som et produkt af andengradspolynomier over $\mathbb{R}$ (*Vink: Opgave 5.20.*) 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 $\mathbb{R}$.

5.29. 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 5.28.*)

5.30. 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 $f(t) = t$.

5.31. 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 $f^{(0)} = f$.)