M A T E M A T I K

1 0 1

A L G E B R A O G G E O M E T R I .

FØRSTE DEL

fra REELLE TAL til DETERMINANTER

forelæsningsnoter

udarbejdet 1975-76.

omarbejdet 1977

INDHOLDSFORTEGNELSE

7

Rettelser og kommentarer til noter til matematik 101.

3.7. Afsnit 2) af beviset er blevet skrevet lidt kortfattet. Midvejs har vi erstattet $\underline{x}$ og $\underline{y}$ med $\mu\underline{e}_1$ og $\underline{y}$. Ifølge bemærkningen øverst på siden ændrer det hverken determinanten eller den lineære afhængighed eller uafhængighed. Determinanten er 0, hvis og kun hvis $\mu = 0$ eller $y_2 = 0$. Vektorerne $\mu\underline{e}_1$ og $y_1\underline{e}_1 + y_2\underline{e}_2$ er åbenbart lineært afhængige, hvis $\mu = 0$ eller $y_2 = 0$, men hvis $\mu \neq 0$ og $y_2 \neq 0$ er det klart, at de begge er $\neq \underline{0}$, og at de ikke har samme retning, altså er lineært uafhængige.

5.16. Det er nok heldigere at bruge "antisymmetrisk" istedet for "usymmetrisk". Det synes de fleste andre i hvert fald at gøre.

5.20. Måske burde den tomme mængde være udtalt mere udførligt. Vi har $\emptyset \times A = A \times \emptyset = \emptyset$ for enhver mængde A, idet $\emptyset \times A = \{(x,y) \mid x \in \emptyset, y \in A\} = \emptyset$. Der findes en tom afbildning $\theta: \emptyset \to A$ for enhver mængde A, medens der for $A \neq \emptyset$ ikke findes afbildninger $A \to \emptyset$. En familie med tom indexmængde får den tomme afbildning af $\emptyset$ ind i sig selv som det eneste element. På side 5.14 afstod vi fra at tale om produktet af en tom mængde af rum. Hvis vi insisterer på at indføre dette tomme produkt, må vi således lade det være mængden $\{\emptyset\}$ med den tomme mængde som det eneste element.

6.15 Ved omtalen af orden og index for en gruppe i afsnittet midt på siden er der kun tænkt på endelige grupper. For en uendelig gruppe kan ordenen defineres som kardinaltallet for mængden af dens elementer. Det hænder, at en uendelig undergruppe i en uendelig gruppe har endelig index, og i det tilfælde kunne man tvivle på, om undergruppen nødvendigvis har lige mange venstre og højre sideklasser. Det er imidlertid let at se, at en højre sideklasse netop har en venstre sideklasse som invers mængde, og derfor er der altid lige mange.

6.16. De i linie 5 og 6 fra oven omtalte undergrupper er normale.

7.8. Beviset for sætning 7.8 er helt forkert. Lad $g \in S_n$ være en permutation. Vi kan tænke os, at g er sammensætning af ν ombytninger. Det er nok at vise, at det for enhver ombytning φ gælder, at forskellen mellem antallet af inversioner i $\varphi\, g$ og i g er ulige. For et par $(\nu,\nu+1)$ gælder nu, at $(g(\nu), g(\nu+1))\circ g$ har netop 1 inversion mere eller mindre end g. Nu kan $\varphi\circ g$ fås af g ved sammensætning med ombytninger af formen $(g(\nu), g(\nu+1))$, og da disse ombytninger sammensættes til φ, som er ulige, er deres antal ulige. Deraf følger sætningen.

8.4. Det burde nævnes i tilslutning til denne side, at det for enhver homomorfi $f:\Gamma \to \Lambda$ gælder, at originalmængden til et venstre (højre) ideal er et venstre (højre) ideal. Billedet af et venstre (højre) ideal er ikke nødvendigvis et venstre (højre) ideal, men dette gælder dog, hvis f er surjektiv. Disse resultater, som er ganske lette at vise benyttes i de to afsnit efter beviset på side 8.13.

3.8. I linie 5 fra neden optræder et V_0, der ved en beklagelig fejltagelse ikke er blevet introduceret på behørig vis. Det burde have været sagt, at V_0 er det af $\underline{v}_0$ udspændte 1-dimensionale underrum.

3.9. Eksistensen af afbildningen $\underline{\gamma}'$ i linie 5 fra oven følger af sætning 11.9.

3.10. Uanset påstanden i første afsnit på denne side går det udmærket at lade f og f^* bytte roller i sætning 13.6. Den tredie formel i sætning 13.5 giver nemlig umiddelbart, at f^* er surjektiv, hvis f er injektiv. Hvis f^* er surjektiv, giver den fjerde formel i sætning 13.5, at kern f er fællesmængde for alle kerner for linearformer på U, og sætning 13.4 fortæller, at den fællesmængde er $\{\underline{0}\}$.

3.19. Sætningerne på denne side er blot en omformulering af sætningerne 13.5 og 13.6 for det endeligdimensionale tilfælde.

16.5. Linie 2-4 på denne side kan udelades, da det samme blev sagt i bevisets indledende afsnit.

Rettelser og kommentarer til noter til MAT 101, 1977-78.

2.10. Efter første afsnit kan tilføjes, at det komplekse tal $(a_1,0) = a_1+i0$ naturligt kan identificeres med det reelle tal a_1. Bag dette ligger følgende: Lad os definere en afbildning $f:\mathbb{R} \to \mathbb{C}$ ved

$$f(x) = (x,0) = x + i0 , \qquad x \in \mathbb{R} .$$

Afbildningen f er åbenbart injektiv, og der gælder

$$f(x+y) = f(x)+f(y), \; f(xy) = f(x)f(y),$$

(hvor der på højre siderne regnes i $\mathbb{C}$). Under henvisning til senere omtalte begreber og resultater følger heraf, at $f(\mathbb{R})$ er et dellegeme af det komplekse tallegeme $\mathbb{C}$, og at f er en isomorfi af det reelle tallegeme $\mathbb{R}$ på dellegemet $f(\mathbb{R})$ af $\mathbb{C}$. Der er ikke anledning til at skelne mellem $\mathbb{R}$ og andre med $\mathbb{R}$ isomorfe legemer (såsom $f(\mathbb{R})$) ; sådanne legemer er blot at anse som "andre eksemplarer af $\mathbb{R}$". Herefter vil vi ikke skelne mellem $\mathbb{R}$ og $f(\mathbb{R})$, idet vi som nævnt identificerer $x \in \mathbb{R}$ med $x+i0 \in \mathbb{C}$, svarende til at vi opfatter $\mathbb{R}$ selv som et dellegeme af det komplekse tallegeme $\mathbb{C}$.

2.15. På højre side af ligningen i næstsidste linie har vi valgt en vilkårlig af de to værdier af kvadratroden af det komplekse tal $\frac{1}{4}b^2 + \frac{1}{27}a^3$ (hvis dette er $\neq 0$).

3.7. Afsnit 2) af beviset er blevet skrevet lidt kortfattet. Midtvejs har vi erstattet $\underline{x}$ og $\underline{y}$ med $\mu\underline{e}_1$ og $\underline{y}$. Ifølge bemærkningen øverst på siden ændrer det hverken determinanten eller den lineære afhængighed eller uafhængighed. Determinanten er 0, hvis og kun hvis $\mu = 0$ eller $y_2 = 0$. Vektorerne $\mu\underline{e}_1$ og $y_1\underline{e}_1 + y_2\underline{e}_2$ er åbenbart lineært afhængige, hvis $\mu = 0$ eller $y_2 = 0$, men hvis $\mu \neq 0$ og $y_2 \neq 0$ er det klart, at de begge er $\neq \underline{0}$, og at de ikke har samme retning, altså er lineært uafhængige. (For øvrigt kommer muligheden $y_2 = 0$ ikke i betragtning her, da vi er i det tilfælde, hvor linien gennem endepunktet af $\underline{x}$ parallel med $\underline{y}$ skærer linien gennem e_1.)

3.12. Anvendes relationen nederst på siden med $(\underline{e}_1'', \underline{e}_2'', \underline{e}_3'') = (\underline{e}_1, \underline{e}_2, \underline{e}_3)$, fås endvidere

$$\det_{\underline{e}_1', \underline{e}_2', \underline{e}_3'}(\underline{e}_1, \underline{e}_2, \underline{e}_3) = 1/\det_{\underline{e}_1, \underline{e}_2, \underline{e}_3}(\underline{e}_1', \underline{e}_2', \underline{e}_3').$$

3.22. Den anførte ligning for planen gennem A og indeholdende vektorerne $\underline{h}$ og $\underline{k}$ er åbenbart af 1. grad.

Omvendt fremstiller enhver ligning af 1. grad:

$$c_1x_1 + c_2x_2 + c_3x_3 = p$$

(hvor c_1, c_2, c_3 og p er reelle konstanter) en plan. Thi er f.eks. $c_3 \neq 0$, får ligningen efter forkortning med c_3 formen

$$x_3 = b_1x_1 + b_2x_2 + q \ ,$$

og her kan x_1 og x_2 benyttes som parametre t_1 og t_2, hvorved vi når til parameterfremstillingen $\underline{x} = \underline{a} + t_1\underline{h} + t_2\underline{k}$ med

$$\underline{a} = q\underline{e}_3, \quad \underline{h} = \underline{e}_1 + b_1\underline{e}_3, \quad \underline{k} = \underline{e}_2 + b_2\underline{e}_3 \ .$$

4.2. Ved definitionen af vinklen $\angle(\underline{a},\underline{b})$ og skalarproduktet $\underline{a}\cdot\underline{b} = \|\underline{a}\| \, \|\underline{b}\| \cos(\underline{a},\underline{b})$ er stiltiende forudsat, at $\underline{a} \neq \underline{0}$ og $\underline{b} \neq 0$. Hvis $\underline{a} = \underline{0}$ eller $\underline{b} = \underline{0}$, sættes $\underline{a}\cdot\underline{b} = 0$ (men $\angle(\underline{a},\underline{b})$ tillægges ingen bestemt værdi).

4.18. I linie 7 skal længden af projektionen af $\underline{z}$ på $\underline{x}\times\underline{y}$ regnes med fortegn.

4.18. I formlen for rumproduktet $[\underline{x},\underline{y},\underline{z}] = \underline{x}\times\underline{y}\cdot\underline{z}$ midt på siden skal højre side ganges med $[\underline{e}_1,\underline{e}_2,\underline{e}_3]$.

5.17. Den i andet afsnit omhandlede ækvivalensrelation kaldes ofte ækvipotens. Kardinaltallet kard A for en mængde A kan defineres som klassen af alle med A ækvipotente mængder.

5.18. I tilslutning til lemma 5.1 kan det nævnes, at en foreningsmængde af en følge af tællelige mængder er tællelig.

5.19. Er P nulpolynomiet, sættes $\nu(P) = 0$.

5.20. Måske burde den tomme mængde være udtalt mere udførligt. Vi har $\emptyset \times A = A \times \emptyset = \emptyset$ for enhver mængde A, idet $\emptyset \times A = \{(x,y) \mid x \in \emptyset, y \in A\} = \emptyset$. Der findes en tom afbildning $\theta: \emptyset \to A$ for enhver mængde A, medens der for $A \neq \emptyset$ ikke findes afbildninger $A \to \emptyset$. Den eneste familie med tom indexmængde er denne tomme afbildning θ. På side 5.14 afstod vi fra at tale om produktet af en tom mængde af rum. Hvis vi insisterer på at indføre dette tomme produkt, må vi således lade det være mængden $\{\theta\}$ med den tomme afbildning som det eneste element.

FORORD.

Hensigten med denne udgave af forelæsningsnoterne til matematik 101 var oprindelig at forny de indledende afsnit, således at diverse emner, i første række komplekse tal, som ikke mere kan påregnes kendt fra skolen, fik en passende udførlig omtale, medens det så til gengæld var meningen at udelade noget af den logik og mængdelære, der nu med sikkerhed kan påregnes at være kendt på forhånd af alle vore studerende.

Så tog det ene ord det andet, og på indeværende tidspunkt ser det ud til, at omarbejdelsen vil resultere i et fuldstændigt sæt nye forelæsningsnoter. Nu, efter at skaden er sket, er det let for forfatteren af disse noter at give en ganske uærlig begrundelse for sit initiativ. De gamle noter havde mange forfattere, og derfor passede de forskellige afsnit ikke helt godt sammen. Det indtraf for ofte, at samme sag var omtalt på to måder, og netop så forskelligt at for mange studerende ikke ville se, at det var samme sag. Trykkeriets gengivelse af de håndskrevne afsnit var for ringe osv.

Når man først har efterrationaliseret på den måde, er det svært at finde den helt ærlige årsag. Det kan godt tæn-

kes at det for mig afgørende var, at forelæsningsnoterne kedede mig (når jeg skal være ærlig, er jeg "jeg", men når jeg efterrationaliserer, er jeg "forfatteren"). Alligevel har jeg skrevet udførligt om de komplekse tal som planlagt, og den elementære vektorregning er da også kommet med.

I stedet for logik og mængdelære er der kommet et ret langt kapitel om grundlagsforskningens historiske udvikling siden mængdelærens indførelse. Der er en hel del filosofisk snak om paradokserne og om aksiomatik, men der er også en omtale af Zorn's lemma, så det er til rådighed for vektorrumsteorien.

De fundamentale algebraiske strukturer er behandlet en hel del mere udførligt end i de gamle noter. Der er medtaget, hvad det er rimeligt at have til rådighed til vektorrumsteorien.

Der er ikke ændret drastisk i vektorrumsteorien. Det væsentligste er, at der er tilføjet et kapitel om multilineære afbildninger.

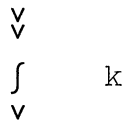
•

Den første del af noterne slutter med behandlingen af determinanter. Anden del vil behandle resten af vektorrumsteorien omtrent som de gamle noter. Der sker nogle ændringer i rækkefølgen, og derved opnås en vis rationalisering.

Så langt er udarbejdelsen af kladden til noterne på indeværende tidspunkt. Resten af anden del skal omfatte teorien for affine rum og kvadrikker. Det er planen at skære behandlingen af affine rum ned til et minimum, men at behandle kvadrikker en hel del mere udførligt end de gamle noter.

I nogle afsluttende kapitler i anden del af noterne er det planlagt at omtale nogle teknisk-fysiske anvendelser af vektorrumsteorien, samt at anføre en del nyttige geometriske resultater, som for tiden er gledet helt ud af undervisningen. Jeg har også planer om en ganske kort omtale af grafer og matroider, måske også lidt om kategoriteori, men jeg tør dog ikke love, at disse planer bliver til virkelighed.

Det er meningen, at de nye noter skal være rummelige nok. De kommer til at indeholde en hel del mere information end de gamle, selv om sidetallet ikke er forøget. Det skulle således ikke være nødvendigt at tilføje stof til de nye noter. Til gengæld vil det nok være realistisk at regne med, at nogle afsnit under alle omstændigheder må overspringes.



Adskillige steder er noterne udstyret med pillignende dekorationer i marginen som her. De betyder, at det pågældende afsnit er beregnet til fornøjelseslæsning, og at det vil være mod forfatterens hensigter at kræve det opgivet til eksamen. Det kan være spændende matematik, der falder udenfor emnet.

Det kan også være eksempler på anvendelser i andre fag eller blot en omtale af sammenhæng med andre fag. Sommetider er det historiske oplysninger, og forfatteren kan godt lejlighedsvis forfalde til mere filosofiske bemærkninger. Med andre ord: Tegnet betyder, at det pågældende afsnit måske er værd at læse.

En overordentlig varm tak skal rettes til Søren Jøndrup for godt samarbejde, da vi forelæste matematik 101 i fællesskab i 1975/76. Søren har modigt om end ofte med bange anelser fulgt mit arbejde med disse noter, han har læst dem og kommenteret dem, og han har standset mig, når jeg ville helt ud, hvor jeg ikke kunne bunde. Der er meget at være taknemmelig for.

Hans Tornehave

KAPITEL 1

De reelle tal.

Vi vil forudsætte de reelle tal kendt fra skolen, og hensigten med det følgende er ikke at genindføre de reelle tal på en ny og bedre måde, men dels at præsentere de betegnelser og den jargon, vi anvender, og dels at fortælle ganske kort om den historiske udvikling af vort syn på talbegrebet.

De reelle tal er en mængde $\mathbb{R}$ med de to kompositionsregler $+$ og $\cdot$, samt ordningsrelationen $\leq$, således at en lang række aksiomer, som vi nu skal opregne, er opfyldt.

I. Aksiomer vedrørende regneoperationerne.

1. De associative og kommutative love

$$(a+b) + c = a + (b+c) \ , \ (ab)c = a(bc)$$

$$a + b = b + a \qquad ab = ba \ .$$

Heraf følger, at vi for givne reelle tal $x_1,\cdots,x_n$ kan tillægge summen $x_1 +\cdots+ x_n$ og produktet $x_1 \cdots x_n$ bestemte reelle værdier, som ikke afhænger af rækkefølgen.

2. Enhver ligning $a + x = b$ har én og kun én løsning. Heraf følger eksistens af 0 og modsat tal til a.

3. De distributive love $(a+b)c = ac + bc$ og $a(b+c) = ab + ac$. Takket være den kommutative lov for multiplikationen implicerer de gensidigt hinanden. De sikrer, at $a \cdot 0 = 0 \cdot a = 0$ for alle $a \in \mathbb{R}$.

4. Enhver ligning $ax = b$ med $a \neq 0$ har én og kun én løsning. Heraf følger eksistens af 1, samt at et fra 0 forskelligt tal har et reciprokt.

II. Ordningsaksiomer.

1. Hvis $a \leqq b$ og $b \leqq a$, da er $a = b$. Hvis $a = b$, da er $a \leqq b$. Dette berettiger indførelsen af $a < b$, som betyder $a \leqq b$ og $a \neq b$.

2. Af $a \leqq b$ og $b \leqq c$ følger $a \leqq c$.

3. For vilkårlige reelle tal a og b gælder enten $a \leqq b$ eller $b \leqq a$.

Hertil kommer to aksiomer, der knytter ordningsrelationen sammen med kompositionsreglerne. Vi vil bruge tegnene $\geqq$ og $>$ for de modsatte relationer, og vi vil sige, at a er positiv, hvis $a \geqq 0$, strengt positiv, hvis $a > 0$, negativ, hvis $a \leqq 0$ og strengt negativ, hvis $a < 0$.

4. At $a < b$ er ensbetydende med, at $b - a$ er positiv.

5. Produktet af to positive tal er positivt.
Nu kan vi slutte, at de reelle tal 1, $2 = 1 + 1$, $3 = 2 + 1$, o.s.v. er indbyrdes forskellige, og de udgør delmængden $\mathbb{N}$ af naturlige tal. Ved yderligere at medtage deres modsatte samt 0 får vi mængden $\mathbb{Z}$ af hele tal. Ved at medtage løsningen af ligningen $ax = b$, hvor $a, b \in \mathbb{Z}$ og $a \neq 0$, får vi mængden $\mathbb{Q}$ af rationale tal.

Vi indfører symbolerne ∞ og $-\infty$ og indfører den udvidede reelle akse $\mathbb{R}^* = \mathbb{R} \cup \{-\infty,\infty\}$, idet ordningsrelationen på $\mathbb{R}$ udvides til $\mathbb{R}^*$ ved at $-\infty < a < \infty$ for alle $a \in \mathbb{R}$.

For $a, b \in \mathbb{R}^*$ og $a < b$ indfører vi intervallerne $]a,b[$, $[a,b]$, $]a,b]$ og $[a,b[$, som er mængden af elementer af $\mathbb{R}^*$ mellem a og b, således at et endepunkt a eller b skal inkluderes, hvis parentesen i vedkommende side vender fligene indad. Et interval kaldes afsluttet, hvis begge endepunkter regnes med, og åbent, hvis ingen af endepunkterne regnes med. Det kaldes en halvlinie, hvis det ene endepunkt er ∞ eller $-\infty$ og ikke regnes med, medens det andet endepunkt er et reelt tal. Det er klart, at $]-\infty,\infty[= \mathbb{R}$. Det lader sig ikke gøre at udvide kompositionsreglerne på $\mathbb{R}$ til hele $\mathbb{R}^*$, så aksiomerne i gruppe I bevarer gyldigheden. Ikke desto mindre definerer man ofte visse regneoperationer med ∞ og $-\infty$. For $a \in \mathbb{R}$ sætter man således $a + \infty = \infty$, selv om det strider mod aksiomet I, 2.

Vi bemærker, at vort aksiomsystem ikke er færdigt, idet det er let at se, at $\mathbb{Q}$ tilfredsstiller samtlige aksiomer. Da vi ønsker at have irrationale tal med må vi tilføje endnu et aksiom (eller to). Dette sidste aksiom kaldes ofte kontinuitets- eller fuldstændighedsaksiomet, og det hører hjemme i matematisk analyse snarere end i algebra.

III. Fuldstændighedsaksiomet. Hvis $\mathbb{Q}$ deles i to ikke tomme mængder A og B, således at ethvert element i A er mindre end ethvert element i B, da findes der et og kun et reelt tal, som er større eller lig ethvert element i A og mindre eller lig ethvert element i B.

En opdeling af $\mathbb{Q}$ i to mængder som beskrevet i dette aksiom kaldes et snit i $\mathbb{Q}$. Det ville nok være naturligere at lade $\mathbb{R}$ indgå i aksiomet i stedet for $\mathbb{Q}$, og en nærmere undersøgelse afslører faktisk, at aksiomet III og det således ændrede vil kunne erstatte hinanden.

Vi skal ikke ved denne lejlighed trænge dybere ind i problematikken omkring de reelle tal, men vi tilføjer nogle bemærkninger om den historiske udvikling.

De tidligste matematiske ræsonnementer, vi kender, stammer fra Grækenlands storhedstid i oldtiden. Vi kender dog en hel del "regnestykker" fra Ægypten og Babylon, og disse synes at vise, at man også i den førgræske periode kunne gennemføre ret komplicerede ræsonnementer, men disse er ikke blevet nedskrevet.

I det overleverede materiale fra den førgræske periode optræder der således udelukkende rationale tal. De græske matematikere opdagede tidligt, at den pytagoræiske sætning forudsætter irrationale tal, og hos Euklid optræder de irrationale tal realiserede som forhold mellem geometriske objekter af samme slags. Sammen med et forhold $\frac{a}{b}$ betragter Euklid alle forhold $\frac{ma}{nb}$; $m, n \in \mathbb{N}$, og for hvert par (m,n) tænker han sig undersøgt, om forholdet er over 1 eller under 1 . To forhold $\frac{a}{b}$ og $\frac{a'}{b'}$ regnes ens, hvis denne undersøgelse giver samme resultat for dem for alle valg af m og n . Euklid arbejder således med "kun-et"-delen af vort aksiom III, og en mere dybtgående undersøgelse vil vise, at det kommer ud på, at Euklid arbejder med en ikke nærmere bestemt delmængde af $\mathbb{R}$ omfattende $\mathbb{Q}$.

Det varede mange århundreder, før der indtraf en afgørende ændring i opfattelsen af de reelle tal. Den mest iøjnefaldende årsag til en sådan ændring var indførelsen af differentialregningen ved Leibniz og Newton omkring år 1700, idet der efterhånden opstod et behov for kriterier, der sikrede eksistens af grænseværdier for visse følger. Sådanne kriterier formuleredes af flere matematikere hen mod slutningen af det attende århundrede, og dermed kom opfattelsen af de reelle tal i overensstemmelse med det her anførte aksiomsystem. Det er den samme opfattelse, der ligger til grund for undervisningen i skolen.

KAPITEL 2

De komplekse tal.

Oldtidens matematikere kendte kunsten at løse en andengradsligning

$$y^2 + A_1 y + A_2 = 0$$

ved at indføre $y = x - \frac{1}{2}A_1$, hvorefter x bestemmes af ligningen

$$x^2 = a_2 = \frac{1}{4} A_1^2 - A_2 .$$

Heraf ses, at ligningen får løsninger, hvis og kun hvis $A_2 \leq \frac{1}{4} A_1^2$.

Det er nærliggende analogt at behandle

$$y^n + A_1 y^{n-1} + \cdots + A_n = 0$$

ved at sætte $y = x - \frac{1}{n} A_1$, hvilket giver en ligning af formen

$$x^n + a_2 x^{n-2} + \cdots + a_n = 0 ,$$

men dette er selvfølgelig kun et yderst beskedent skridt på vejen mod en løsning.

Omkring år 1500 fandt Scipio del Ferro en metode til løsning af trediegradsligningen

$$x^3 + ax + b = 0 \ ,$$

men det kan ikke udelukkes, at metoden har været kendt tidligere.

For at løse trediegradsligningen indfører vi en ny variabel u ved at substituere

$$x = u - \frac{a}{3u} \ .$$

Indsættelse i ligningen giver

$$u^3 - au + \frac{a^2}{3u} - \frac{a^3}{27u^3} + au - \frac{a^2}{3u} + b = 0 \ ,$$

og i betragtning af, at muligheden $u = 0$ som løsning er uden interesse, er dette ensbetydende med

$$(u^3)^2 + bu^3 - \frac{1}{27} a^3 = 0 \ ,$$

som giver

$$(1) \qquad u^3 = -\tfrac{1}{2}b \pm \sqrt{\tfrac{1}{4}b^2 + \frac{1}{27} a^3} \ .$$

De to fundne løsninger for u^3 har produkt $-\frac{1}{27} a^3$, og det medfører, at de to løsninger for u^3 giver de samme værdier for x. Traditionelt angives løsningen ved Cardano's formel

$$x = \sqrt[3]{-\tfrac{1}{2}b + \sqrt{\tfrac{1}{4}b^2 + \tfrac{1}{27}a^3}} + \sqrt[3]{-\tfrac{1}{2}b - \sqrt{\tfrac{1}{4}b^2 + \tfrac{1}{27}a^3}} ,$$

men det er nu en ret upræcis formulering.

Helt præcist har vi fundet ligningens eventuelle løsninger af formen $x = u - \frac{a}{3u}$. For en kendt rod x fås u af ligningen $u^2 - xu - \frac{1}{3}a = 0$, og for at den skal have løsninger, må x tilfredsstille betingelsen $x^2 \geqq -\frac{4}{3}a$.

Således har ligningen

(2) $$x^3 - 7x + 6 = 0$$

rødderne 1, 2 og -3 , men den svarer til, at $-\frac{4}{3}a = 9\frac{1}{3}$, så ingen af rødderne kan skrives på formen $u - \frac{a}{3u}$, og i overensstemmelse hermed får vi $\frac{1}{4}b^2 + \frac{1}{27}a^3 = -\frac{100}{27}$, så vor løsningsmetode virker ikke i dette tilfælde.

Det var disse omstændigheder, der førte til, at matematikerne begyndte at regne med kvadratrødder af negative tal. For roden 2 i ligningen (2) bestemmes den tilsvarende værdi af u således af ligningen

$$u^2 - 2u + \frac{7}{3} = 0 ,$$

som har de imaginære rødder

$$u = 1 \pm \sqrt{-\frac{4}{3}} = 1 \pm \frac{2}{\sqrt{3}} \cdot \sqrt{-1} ,$$

og binomialformlen giver

$$u^3 = 1 \pm 2\sqrt{3} \cdot \sqrt{-1} - 4 \mp \frac{8\sqrt{3}}{9} \cdot \sqrt{-1} = -3 \pm \frac{10\sqrt{3}}{9}\sqrt{-1} \quad ,$$

hvilket præcis stemmer med, hvad (1) giver for $a = -7$, $b = 6$.

Det fremgår heraf, at forsøg på at løse trediegradsligninger opfordrer til at regne med kvadratrødder af negative tal. Det bør tilføjes, at det endnu ikke på den tid var blevet almindeligt at bruge bogstaver som betegnelser for vilkårlige tal, og at negative tal heller ikke rigtigt eksisterede. Indholdet af en ligning udtryktes i ord snarere end i en formel. Hos René Descartes (1596-1650) finder man nogen brug af et matematisk formelsprog, og hos Leibniz og Newton er det færdigudviklet.

I mellemtiden var også fjerdegradsligningen blevet løst, og mod slutningen af det attende århundrede påstod d'Alembert, at man ved regning med tal af formen $a + b\sqrt{-1}$ ville opnå, at ethvert polynomium med sådanne tal som koefficienter, ville have et tal af samme slags som rod. Hans bevis var dog ikke fyldestgørende, hvilket blev påpeget af Gauss i 1798, næsten samtidig med, at vor kendte digter Johan Hermannn Wessels flittige broder Casper Wessel i sin afhandling "Om Directionens analytiske Betegning" opstillede en helt eksakt teori for komplekse tal. Denne afhandling forblev upåagtet ligesom en senere afhandling af svejtseren Argand, og først i 1817 indførte Gauss selv de komplekse tal og gav et tilfredsstillende bevis for d'Alembert's sætning.

Vort udgangspunkt for indførelsen af komplekse tal skal være den sædvanlige Euklidiske plan, som vi tænker os udstyret med et fast valgt retvinklet koordinatsystem, så hvert punkt er givet ved et koordinatpar (x_1,x_2) , og vi vil også benytte (x_1,x_2) som betegnelse for punktet med dette koordinatpar, men vi vil dog også anvende en betegnelse ved et enkelt bogstav og skrive $x = (x_1,x_2)$, $y = (y_1,y_2)$ etc. Fremtidig vil vi også kalde $x = (x_1,x_2)$ et komplekst tal, og vi vil kalde x_1 dets reelle del eller realdel og x_2 dets imaginære del eller imaginærdel.

Vi definerer nu addition af komplekse tal $x = (x_1,x_2)$ og $y = (y_1,y_2)$ ved

$$x + y = (x_1 + y_1 , x_2 + y_2) \quad .$$

Det er klart at den associative og den kommutative lov

$$(x+y) + z = x + (y+z) , \quad x + y = y + x$$

tilfredsstilles. For $a = (a_1,a_2)$ og $b = (b_1,b_2)$ vil ligningen $a + x = b$ have løsningen $x = (b_1 - a_1 , b_2 - a_2)$, og vi vil betegne dette tal med $b - a$. Et komplekst tal $a = (a_1, a_2)$ har det modsatte tal $-a = (-a_1, -a_2)$. Det komplekse tal $(0,0)$ er det komplekse nul.

For $\alpha \in \mathbb{R}$ og et komplekst tal $x = (x_1,x_2)$ definerer vi

$$\alpha x = (\alpha x_1 , \alpha x_2) \quad .$$

Det ses da helt umiddelbart, at vi har de distributive love

$$\alpha(x+y) = \alpha x + \alpha y \ , \ (\alpha+\beta)x = \alpha x + \beta x \ ,$$

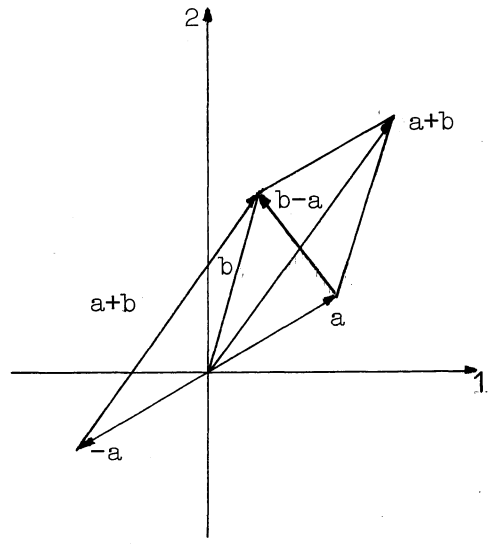
samt den associative lov

$$(\alpha\beta)x = \alpha(\beta x) \ .$$

Vi vedtager, at $x\alpha$ skal betyde ganske det samme som αx .

Vi indfører nu de specielle komplekse tal $e = (1,0)$ og $i = (0,1)$, og vi får så for ethvert komplekst tal $x = (x_1,x_2)$, at

$$x = x_1 e + x_2 i \ .$$

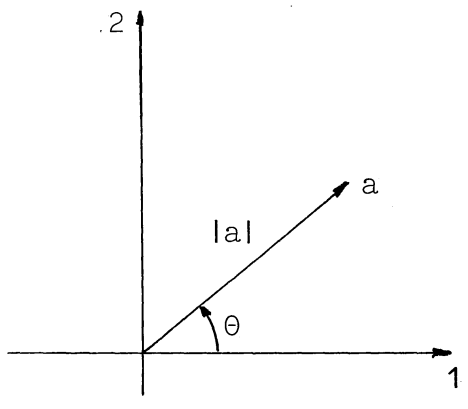


Det komplekse tal $a = (a_1,a_2)$ er et punkt i planen, og det bestemmer liniestykket fra $(0,0)$ til (a_1,a_2) . Vi kan også lade dette liniestykke med orienteringen angivet ved en pil repræsentere $a = (a_1,a_2)$. Så er det hensigtsmæssigt også at lade alle andre liniestykker med samme længde og retning repræsentere det komplekse tal a . Som antydet på figuren, opnår vi derved, at komplekse tal adderes, ved at deres repræsenterende liniestykker sættes efter hinanden (eller ved "kræfternes parallelogram"). Særlig bekvemt er det, at $b - a$ repræsenteres ved liniestykket fra a til b .

Det liniestykke, som repræsenterer $a = (a_1, a_2)$, har længden $|a| = \sqrt{a_1^2 + a_2^2}$, som kaldes den numeriske værdi af a eller modulus af a. Det er næsten helt indlysende, at $|\alpha x| = |\alpha||x|$, og af figuren ovenfor fås ved hjælp af trekantsuligheden, at

$$||b| - |a|| \leqq |b \pm a| \leqq |a| + |b| \ .$$

Det komplekse tal $a = (a_1, a_2)$ er også fastlagt ved den numeriske værdi $|a|$ og vinklen fra den første akse i koordinatsystemet til det liniestykke, der repræsenterer a.



Vinklen θ har uendelig mange talværdier, og enhver sådan talværdi kaldes et argument for a. Argumenter for a betegnes arg a, $\arg_1 a$, $\arg_2 a$, etc. Med Arg a betegner vi det specielle argument, som falder i $]-\pi, \pi]$, og det kaldes hovedargumentet for a. Med {arg a} betegner vi mængden af argumenter for a.

Hvis $a = (a_1, a_2)$ har numerisk værdi $|a| = r$ og argument $\arg a = \theta$, har vi også

$$a = (a_1, a_2) = (r \cos \theta \ , \ r \sin \theta) \ ,$$

altså

$$a = a_1 e + a_2 i = r(e \cos \theta + i \sin \theta) .$$

For komplekse tal $a = (a_1, a_2)$ og $b = (b_1, b_2)$ definerer vi produktet

$$ab = (a_1 b_1 - a_2 b_2 , a_1 b_2 + a_2 b_1) .$$

Hvis vi udtrykt ved numerisk værdi og argument har

$$a = (r \cos \theta , r \sin \theta) , b = (r' \cos \theta' , r' \sin \theta') ,$$

får vi

$$ab = (rr'(\cos \theta \cos \theta' - \sin \theta \sin \theta'), rr'(\sin \theta \cos \theta' + \cos \theta \sin \theta')) ,$$

og additionsformlerne for cosinus og sinus giver

$$ab = (rr' \cos(\theta+\theta') , rr' \sin(\theta+\theta')) .$$

Heraf følger umiddelbart, at multiplikationen er associativ og kommutativ. Endvidere slutter vi, at

$$|ab| = |a||b|, \arg(ab) = \arg a + \arg b ,$$

hvor den sidste formel skal forstås på den måde, at det for vilkårligt valg af argumentværdier $\arg a$ og $\arg b$ gælder, at $\arg a + \arg b$ er en argumentværdi for ab .

For $x, y \in \mathbb{R}$ får vi

$$xe + ye = (x+y)e , \quad (xe)(ye) = xye .$$

For $x \in \mathbb{R}$ og et komplekst tal $a = a_1 e + a_2 i$ får vi

$$xe \cdot a = xe(a_1 e + a_2 i) = xa_1 e + xa_2 i = xa \ .$$

Heraf fremgår, at regning med de komplekse tal xe med imaginærdel 0 foregår helt som regning med reelle tal. Desuden ser vi, at e er neutralelement ved multiplikation af komplekse tal. Vi tillader os derfor at udelade e, så vi vil fra nu af skrive

$$a = (a_1, a_2) = a_1 + ia_2 \ .$$

For $y \in \mathbb{R}$ og et komplekst tal $a = a_1 + ia_2$ har vi nu

$$iy \cdot a = -ya_2 + iya_1 \ ;$$

og hvis yderligere $x \in \mathbb{R}$, får vi

$$(x+iy)a = xa + iy \cdot a \ .$$

For $y_1, y_2 \in \mathbb{R}$ og $a = a_1 + ia_2$ har vi

$$i(y_1 + y_2)a = iy_1 a + iy_2 a \ .$$

For komplekse tal $x + iy$, $x_1 + iy_1$ og $a = a_1 + ia_2$ får vi dernæst

$$((x+iy) + (x_1+iy_1))a = (x+x_1)a + i(y+y_1)a =$$

$$(x+iy)a + (x_1+iy_1)a \ .$$

Dette er den distributive lov for multiplikation af komplekse tal.

Multiplikationens definition giver, at $i^2 = -1$, og multiplikationen

$$(a_1+ia_2)(b_1+ib_2) = a_1b_1 - a_2b_2 + i(a_1b_2 + a_2b_1)$$

kan derefter udføres ganske som man på gammeldags vis multiplicerer toleddede størrelser.

Et komplekst tal $a_1 + ia_2$ kaldes reelt, hvis $a_2 = 0$, og det kaldes rent imaginært, hvis $a_1 = 0$. Det kaldes imaginært, hvis $a_2 \neq 0$. Ud fra $a = a_1 + ia_2$ kan vi danne det komplekse tal $a_1 - ia_2$, der betegnes $\overline{a}$ og kaldes det konjugerede tal til a . Vi har $|\overline{a}| = |a|$ og $\arg \overline{a} = -\arg a$. Et komplekst tal a er reelt, hvis og kun hvis $\overline{a} = a$ og det er rent imaginært, hvis og kun hvis $\overline{a} = -a$.

For $a = a_1 + ia_2$, hvor $a_1 , a_2 \in \mathbb{R}$ skriver vi

$$a_1 = \operatorname{Re} a \ , \ a_2 = \operatorname{Im} a \ ,$$

og vi har

$$a + \overline{a} = 2 \operatorname{Re} a \ , \ a - \overline{a} = 2i \operatorname{Im} a \ .$$

Endvidere er

$$a\overline{a} = |a|^2 = |\overline{a}|^2 = a_1^2 + a_2^2 \ .$$

Vi vil fra nu af benytte betegnelsen $\mathbb{C}$ for mængden af komplekse tal med de ovenfor indførte regneregler. For $a \in \mathbb{C}$, $a \neq 0$ har vi $|a| \neq 0$ og

$$a \cdot \frac{\overline{a}}{|a|^2} = \frac{a\overline{a}}{|a|^2} = \frac{|a|^2}{|a|^2} = 1 \ ,$$

så $\frac{1}{|a|^2}\bar{a}$ er det til a reciproke komplekse tal. Udførligt er

$$(a_1+ia_2)^{-1} = \frac{a_1}{a_1^2+a_2^2} - i\,\frac{a_2}{a_1^2+a_2^2} \quad .$$

For $a,b \in \mathbb{C}$, $a \neq 0$ og et ubekendt $z \in \mathbb{C}$ er ligningen $az = b$ ensbetydende med $z = a^{-1}b$, så division er mulig og entydig. I praksis kan division gennemføres ved at "skaffe reel nævner"

$$\frac{b_1+ib_2}{a_1+ia_2} = \frac{(b_1+ib_2)(a_1-ia_2)}{(a_1+ia_2)(a_1-ia_2)} = \frac{a_1b_1+a_2b_2}{a_1^2+a_2^2} + i\,\frac{a_1b_2-a_2b_1}{a_1^2+a_2^2} \quad .$$

Vi har følgende regler for regning med konjugerede tal:

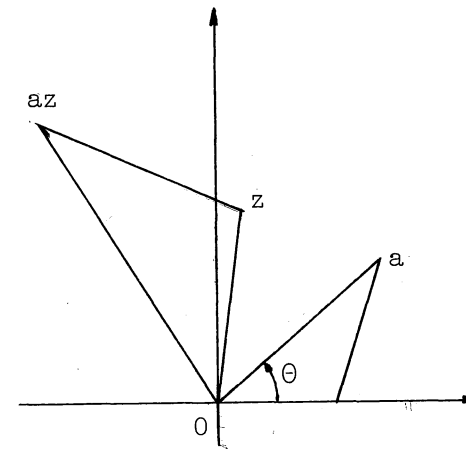
$$\bar{\bar{a}} = a \;,\; \bar{a}^{-1} = \overline{a^{-1}} \;,\; \overline{a+b} = \bar{a} + \bar{b} \;,\; \overline{ab} = \bar{a}\,\bar{b} \quad .$$

Hvis de komplekse tal er udtrykt ved numerisk værdi og argument, dannes reciprok og kvotient ved formlerne

$$(r(\cos\theta + i\sin\theta))^{-1} = r^{-1}(\cos\theta - i\sin\theta)$$

$$\frac{r'(\cos\theta' + i\sin\theta')}{r(\cos\theta + i\sin\theta)} = \frac{r'}{r}(\cos(\theta'-\theta) + i\sin(\theta'-\theta)) \quad .$$

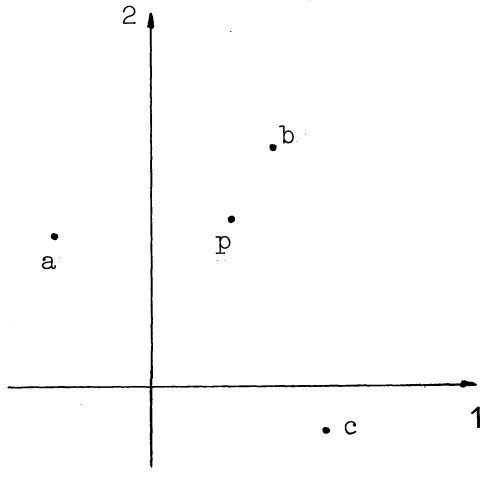
For $a = r(\cos\theta + i\sin\theta)$ kan den ved $\varphi(z) = az$ definerede afbildning $\varphi\colon \mathbb{C} \to \mathbb{C}$ beskrives som en drejning om 0 med drejningsvinklen θ efterfulgt af en ligedannethed med centrum 0 og ligedannetheds-



forhold $|a|$. Det går også med de to operationer i omvendt orden. De to trekanter $01a$ og $0z(az)$, som er vist på figuren, bliver ligedannede.

Hvis $a,b \in \mathbb{C}$ og $a \neq 0$, $b \neq 0$, vil $a\bar{b}$ være et reelt tal, hvis og kun hvis a og b har samme eller modsat retning i planen, medens $a\bar{b}$ vil være rent imaginært, hvis og kun hvis a og b har på hinanden vinkelrette retninger.

Eksempel: For vilkårlige komplekse tal a,b,c,p får vi ved direkte udregning, at $(p-a)(\bar{c}-\bar{b}) + (p-b)(\bar{a}-\bar{c}) + (p-c)(\bar{b}-\bar{a}) = (b\bar{c}-\bar{b}c) + (c\bar{a}-\bar{c}a) + (a\bar{b}-\bar{a}b)$. Her står på højre side i hver parentes forskellen mellem et tal og dets konjugerede, altså noget rent imaginært. Derfor kan vi slutte, at hvis to af produkterne på venstre side er rent imaginære, er også det tredie rent imaginært. Geometrisk betyder det for trekanten abc, at hvis p ligger sådan, at dets forbindelseslinier til to af vinkelspidserne er vinkelrette på siden overfor, vil det tilsvarende gælde for den tredie vinkelspids. Dette resultat er ensbetydende med den kendte sætning, at højderne i en trekant går gennem samme punkt. Vort resultat omfatter ganske vist nogle udartede tilfælde, f.eks. hvis punkterne a, b og c ligger på en ret linie, men i alle sådanne til-



fælde bliver resultatet helt uden interesse.

Potensopløftning med heltallig eksponent defineres ganske som potenser af reelle tal, så a^n med $n \in \mathbb{N}$ er produkt af n faktorer, der alle er a, og for $a \neq 0$ er $a^0 = 1$ og $a^{-n} = (a^n)^{-1}$. For $a = r(\cos\theta + i\sin\theta)$ giver multiplikationsformlen umiddelbart Moivres formel

$$a^n = (r(\cos\theta + i\sin\theta))^n = r^n(\cos n\theta + i\sin n\theta)$$

for $n \in \mathbb{N}$, og det følger derefter umiddelbart, at formlen gælder for alle $n \in \mathbb{Z}$, når $a \neq 0$.

Idet vi stadig har $a = r(\cos\theta + i\sin\theta) \neq 0$ og $n \in \mathbb{N}$, vil vi finde alle løsninger til den binome ligning

$$z^n = a \ .$$

Vi kan skrive $z = \rho(\cos\xi + i\sin\xi)$, og vi får da

$$z^n = \rho^n(\cos n\xi + i\sin n\xi) \ ,$$

og z er en løsning til ligningen, hvis og kun hvis

$$\rho^n = r \ , \ n\xi = \theta + 2p\pi \ , \ p \in \mathbb{Z} \ ,$$

og vi får derfor løsningsmængden

$$\{\sqrt[n]{r}(\cos\frac{\theta+2p\pi}{n} + i\sin\frac{\theta+2p\pi}{n}) \mid p \in \mathbb{Z}\} \ ,$$

men i virkeligheden får vi bare n indbyrdes forskellige løsninger, idet $p = p_1$ og $p = p_2$ giver samme løsning, hvis n går op i $p_2 - p_1$. Vi får derfor alle løsninger ved at be-

nytte n på hinanden følgende værdier for p, f.eks. $p = 0,1,\cdots,n-1$. De n løsninger er vinkelspidser i en regulær n-kant indskrevet i cirklen med centrum 0 og radius $\sqrt[n]{r}$. Hvis z_o er en af løsningerne og vi sætter $\varepsilon_n = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$, er mængden af løsninger $\{z_o, z_o\varepsilon_n, z_o\varepsilon_n^2, \cdots, z_o\varepsilon_n^{n-1}\}$. Tallene $1, \varepsilon_n, \varepsilon_n^2, \cdots, \varepsilon_n^{n-1}$ er netop løsningerne til ligningen $z^n = 1$, og de kaldes de n^{te} enhedsrødder.

Vi giver en tabel over de n^{te} enhedsrødder for nogle værdier af n

n	enhedsrødder
2	$1, -1$
3	$1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}$
4	$1, i, -1, -i$
5	$1, \frac{\sqrt{5}-1}{4} \pm \frac{i}{4}\sqrt{10+2\sqrt{5}}, -\frac{\sqrt{5}+1}{4} \pm \frac{i}{4}\sqrt{10-2\sqrt{5}}$
6	$\pm 1, \frac{1\pm i\sqrt{3}}{2}, \frac{-1\pm i\sqrt{3}}{2}$
8	$\pm 1, \pm i, \pm\frac{\sqrt{2}}{2} \pm i\frac{\sqrt{2}}{2}$

For $n = 7$ og $n = 9$ får vi ikke tilsvarende pæne udtryk ved kvadratrødder, idet vi kommer til at løse en tredjegradsligning. For $n = 10, 12, 15$ og 16 får vi enhedsrødderne udtrykt ved kvadratrødder, men ikke for $n = 11, 13$ og 14.

Overraskende nok viste C.F. Gauss i en meget ung alder, at også de syttende enhedsrødder kan udtrykkes ved kvadratrødder, og deraf følger, at en regulær syttenkant lader sig konstruere ved hjælp af passer og lineal.

Af $z^2 = a$ med $a = a_1 + ia_2$ fås ved $z = x + iy$ ligningen

$$x^2 - y^2 = a_1 \ , \ 2xy = a_2 \ ,$$

hvoraf vi finder $(x^2+y^2)^2 = a_1^2 + a_2^2$, altså

$$x^2 + y^2 = +\sqrt{a_1^2 + a_2^2} \ ,$$

så vi får løsningerne

$$z = \pm\left\{ \sqrt{\tfrac{1}{2}(\sqrt{a_1^2 + a_2^2} + a_1)} + i\frac{a_2}{|a_2|} \sqrt{\tfrac{1}{2}(\sqrt{a_1^2 + a_2^2} - a_1)} \right\} .$$

For $a_2 = 0$ må resultatet modificeres lidt, da $\frac{a_2}{|a_2|}$ ikke har mening i dette tilfælde. En tilsvarende behandling af ligningen $z^3 = a$ vil ikke lykkes.

Vi vender nu tilbage til løsningen af trediegradsligningen

$$x^3 + ax + b = 0 \ ,$$

hvor vi nu kan tillade a og b at være komplekse tal. Lad u_0 være en løsning til ligningen (1)

$$u_0^3 = -\tfrac{1}{2}b + \sqrt{\tfrac{1}{4}b^2 + \tfrac{1}{27}a^3} \ .$$

Så er $v_0 = -\frac{a}{3u_0}$ en løsning til den ligning, der fås ved at

vælge den anden værdi af kvadratroden, og trediegradsligningens løsningsmængde bliver

$$\{u_0 + v_0 \, , \; u_0\varepsilon_3 + v_0\overline{\varepsilon}_3 \, , \; u_0\overline{\varepsilon}_3 + v_0\varepsilon_3\} \, ,$$

hvor $\varepsilon_3 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

Fjerdegradsligningen

$$x^4 = ax^2 + bx + c$$

er for hvert $z \in \mathbb{C}$ ensbetydende med ligningen

$$(x^2 + z)^2 = (a + 2z)x^2 + bx + (c + z^2) \quad .$$

Hvis vi nu vælger z som en rod i trediegradsligningen

$$4(a + 2z)(c + z^2) = b^2 \, ,$$

bliver ligningens højre side kvadratet på et førstegradspolynomium, og så går det let nok at løse ligningen.

For ligninger af højst fjerde grad har vi således løsningsformler, der udtrykker den ubekendte ved rodstørrelser og elementære regneoperationer. Den norske matematiker Niels Henrik Abel (1801 - 29) viste, at tilsvarende formler ikke kunne gælde for ligninger af grad $\geqq 5$.

For $a \in \mathbb{C}$, $r > 0$ er relationen $|z-a| = r$ udtryk for, at $z \in \mathbb{C}$ ligger på cirklen med centrum a og radius r . Relationen er ensbetydende med, at $(z-a)(\overline{z}-\overline{a}) = |z-a|^2 = r^2$, hvilket også kan skrives

$$|z|^2 - \bar{a}z - a\bar{z} + |a|^2 - r^2 = 0 \ .$$

Mere generelt kan man for $a \in \mathbb{C}$, $\beta, \gamma \in \mathbb{R}$ spørge om løsningsmængden for ligningen

(3) $$\beta|z|^2 - \bar{a}z - a\bar{z} + \gamma = 0 \ ,$$

og vi får da følgende muligheder:

1) $a = \beta = \gamma = 0$. Hele planen.

2) $a \neq 0$, $\beta = \gamma = 0$. Ret linie gennem 0 .

3) $a \neq 0$, $\beta = 0$, $\gamma \neq 0$. Ret linie, ikke gennem 0 .

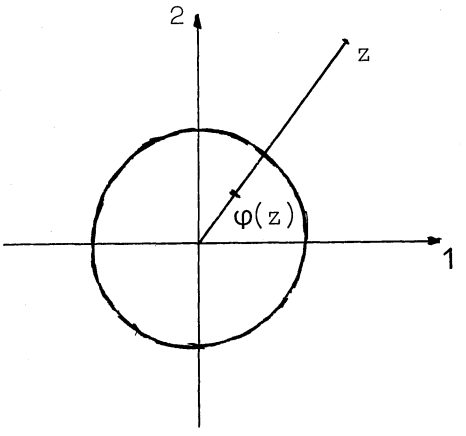
4) $a = \beta = 0$, $\gamma \neq 0$. Den tomme mængde.

5) $\beta \neq 0$, $\frac{\gamma}{\beta} < |\frac{a}{\beta}|^2$. Cirklen med centrum $\frac{a}{\beta}$ og radius $\sqrt{|\frac{a}{\beta}|^2 - \frac{\gamma}{\beta}}$.

6) $\beta \neq 0$, $\frac{\gamma}{\beta} = |\frac{a}{\beta}|^2$. Punktet $\frac{a}{\beta}$.

7) $\beta \neq 0$, $\frac{\gamma}{\beta} > |\frac{a}{\beta}|^2$. Den tomme mængde.

Ligningen (3) kan som løsningsmængde have hvilken som helst cirkel eller ret linie i $\mathbb{C}$. Disse punktmængder kaldes derfor generaliserede cirkler (i $\mathbb{C}$) . De særlige løsningsmængder i tilfældene 4), 6) og 7) regner vi ikke rigtigt med, men de kaldes dog "udartede generaliserede cirkler".



Ved $\varphi(z) = \overline{z}^{-1}$ defineres en bijektiv afbildning af $\mathbb{C} \setminus \{0\}$ på sig selv. Som antydet på figuren ligger z og $\varphi(z)$ på samme halvlinie ud fra 0, og deres afstande fra 0 har produktet 1. Afbildningen φ kaldes en inversion i enhedscirklen eller en spejling i enhedscirklen. Hvis vi erstatter z med $\overline{z}^{-1}$ i ligningen (3) og derefter bringer ligningen på "hel form" ved multiplikation med $|z|^2 = z\overline{z}$, har det blot den virkning, at β og γ bytter plads i ligningen. Deraf slutter vi, at en inversion fører en generaliseret cirkel over i en generaliseret cirkel. Mere detaljeret får vi, at en ret linie gennem 0, afbildes på sig selv, at en ret linie, der ikke går gennem 0 svarer til en cirkel gennem 0 og omvendt, samt at en cirkel, der ikke går gennem 0, svarer til en cirkel, der heller ikke går gennem 0.

Ved $\varphi_1(z) = z^{-1}$ defineres ligeledes en bijektiv afbildning af $\mathbb{C} \setminus \{0\}$ på sig selv, og da φ_1 kan sammensættes af φ og en spejling i den reelle akse, gælder det også for φ_1, at den afbilder generaliseret cirkel i generaliseret cirkel. For $a, b, c, d \in \mathbb{C}$ og $ad - bc \neq 0$ definerer $\gamma(z) = \frac{az+b}{cz+d}$ i tilfældet $c = 0$ en bijektiv afbildning $\gamma: \mathbb{C} \to \mathbb{C}$ og i tilfældet $c \neq 0$ en bijektiv afbildning $\gamma: \mathbb{C} \setminus \{-\frac{d}{c}\} \to \mathbb{C} \setminus \{\frac{a}{c}\}$. For $c \neq 0$ er

$$\gamma(z) = \frac{bc-ad}{c^2}\,(z + \frac{d}{c})^{-1} + \frac{a}{c} \quad ,$$

og det viser, at γ fås ved først at anvende parallelforskydningen $z \to z + \frac{d}{c}$, dernæst afbildningen φ_1, så $z \to \frac{bc-ad}{c^2} z$, altså en drejning og en ligedannethed, og endelig tilsidst parallelforskydningen $z \to z + \frac{a}{c}$. Afbildningen γ vil derfor også afbilde generaliseret cirkel i generaliseret cirkel. At dette også gælder for $c \neq 0$ ses meget let. Afbildningerne γ har mange anvendelser og de optræder i litteraturen med mange navne: brudne lineære substitutioner, projektiviteter, homografier etc.

Nu er vi færdige med vor indførelse af komplekse tal. Vi kunne været gået videre ad nærliggende veje, f.eks. ved den nærliggende definition

$$(r(\cos\theta + i\sin\theta))^{\frac{p}{q}} = \{r^{\frac{p}{q}}(\cos\tfrac{p}{q}(\theta + 2in\pi) + i\sin\tfrac{p}{q}(\theta + 2in\pi) \mid n \in \mathbb{Z}\} ,$$

hvor udtrykket på højre side er en endelig mængde, som virkelig kun afhænger af det rationale tal $\frac{p}{q}$, men så vil $a^{\frac{p}{q}}$ ikke være det samme som $(a^p)^{\frac{1}{q}}$, hvis $\frac{p}{q}$ kan forkortes.

Til gengæld går det fint at definere potenser af reelle tal med komplekse eksponenter. Allerede Euler indførte

$$e^{x+iy} = e^x(\cos y + i \sin y) ,$$

som tilfredsstiller eksponentialfunktionens funktionalligning

$$e^{z+w} = e^z\, e^w$$

for alle komplekse z,w. Derved fås de Euler'ske formler

$$\cos y = \tfrac{1}{2}(e^{iy} + e^{-iy}) \ , \ \sin y = \frac{1}{2i}(e^{iy} - e^{-iy}) \ ,$$

der kan benyttes til definition af de trigonometriske funktioner også som funktioner af komplekse variable, og de bevirker desuden, at de trigonometriske formler nu kan udledes af eksponentialfunktionens funktionalligning.

Vi burde slutte med nogle bemærkninger om anvendelser af komplekse tal, men det emne er faktisk for omfattende for os. De fleste og vigtigste anvendelser beror på, at differential- og integralregning kan udstrækkes til funktioner af komplekse variable. Desuden er der en intim sammenhæng mellem funktioner af komplekse variable og problemer vedrørende mere komplicerede differentialligninger af den slags, der optræder i fysiske og tekniske problemer. Elementær regning med komplekse tal letter behandlingen af mange mere elementære differentialligninger og optræder som et hjælpemiddel i elektrisk kredsløbsteori. De simple geometriske anvendelser (inversion og homografier) giver en alternativ analytisk geometri. Den er ikke bedre end den sædvanlige, men den fremhæver andre fænomener, så den er nyttig til behandling af visse specielle problemer.

ØVELSER TIL KAPITEL 2.

Som hjælp til kontrol af indlæring anføres i tilfældig rækkefølge stikord til de vigtigste af de i kapitlet behandlede emner. Ved at læse dem langsomt igennem og for hvert stikord prøve, hvad man kan huske om det, kan man kontrollere, om man efterhånden har lært noget af det.

Argument, potenser af komplekse tal, modulus, distributive love, realdel, binom ligning, rent imaginær, associative og kommutative love, modulus, enhedsrødder, cirkelligning på kompleks form, numerisk værdi, at "skaffe reel nævner", kvadratrod, hovedargument, imaginær, inversion, konjugeret.

2.1. Indøv regnereglerne ved at skrive nedenstående udtryk på formen a+ib.

2.1.1. $(8+i)+(4-i7)+(-6+i2)-(5+i4)$

2.1.2. $(3+i4)(4+i3)-(4-i3)(3-i4)$

2.1.3. $((2+\sqrt{3})+i(2-\sqrt{3}))((2-\sqrt{3})+i(2+\sqrt{3}))$.

2.1.4. $\frac{1+i7}{4+i3} + \frac{7+i}{3+i4}$

2.1.5. $\sqrt{5+i12}$, $\sqrt{3+i2\sqrt{10}}$

2.2. Et fjerdegradspolynomium $x^4 - 2ax^2 + b^2$ kan opløses i to andengradsfaktorer på flere måder, f.eks.

$$((x^2-a) + \sqrt{a^2-b^2})((x^2-a) - \sqrt{a^2-b^2})$$

eller

$$((x^2+b) + \sqrt{2(a+b)}x)((x^2+b) - \sqrt{2(a+b)}x)$$

Det kan man udnytte til at finde rødderne, men til det formål er de to spaltninger ikke altid lige bekvemme. Prøv med x^4-4x^2-5 og med x^2+4x^2+16.

2.3 Find rødderne i polynomiet z^5-1 ved hjælp af omskrivningen

$$(z^5-1) = (z-1)(z^4+z^3+z^2+z+1) =$$
$$z^2(z-1)((z+\tfrac{1}{z})^2 + (z+\tfrac{1}{z})-1).$$

Find derved $\cos\frac{\pi}{10}$ og $\sin\frac{\pi}{10}$ ($\frac{\pi}{10} = 18°$).

2.4. Udregn $\sqrt{\frac{\sqrt{3}+i}{2}}$, og find derved $\cos\frac{\pi}{12}$ og $\sin\frac{\pi}{12}$. Ved at kombinere resultatet med det fra opgave 2.3. kan det lade sig gøre at finde $\cos\frac{\pi}{60}$ og $\sin\frac{\pi}{60}$.

2.5. Lad a og b være fra 0 forskellige komplekse tal. Vis, at $\frac{\sqrt{ab}}{|b|a+|a|b}$ er reelt (det er selvfølgelig

2.11. Er følgende påstand rigtig? Lad A,B og C være vilkårlige komplekse tal. Hvis der findes to rent imaginære tal u og v, som tilfredsstiller betingelsen $Au+Bv = C$, da findes der også to reelle tal x og y, som tilfredsstiller betingelsen $Ax+By = C$.

2.12. Lad u,x,y,z være 4 indbyrdes forskellige komplekse tal. Vis, at "dobbeltforholdet" $\frac{u-y}{u-z} / \frac{x-y}{x-z}$ er reelt, hvis og kun hvis de 4 tal ligger på en cirkel eller en ret linie.

2.13 Ved $f(z) = z^2$ defineres en afbildning $f:\mathbb{C} \to \mathbb{C}$. Vis nogle af de følgende påstande:

2.13.1. Billedet af en ret linie, der ikke går gennem 0, er en parabel med brændpunkt i 0. Benyt, at drejning af en figur om 0 blot bevirker, at billedet drejes den dobbelte vinkel om 0. Det er derfor nok at vise påstanden for en lodret linie.

2.13.2. Originalmængden til en ret linie, der ikke går gennem 0, er en ligesidet hyperbel med centrum i 0. Se vink i 2.13.1.

2.13.3. Originalmængden til en cirkel med centrum i a^2, hvor a er strengt positiv, er en kurve, der består af net-

først rigtig defineret, når der er valgt en værdi af kvadratroden). Det hænger sammen med, at både $\sqrt{ab}$ og $|b|a+|a|b$ ligger på den linie gennem 0, som halverer vinklen mellem liniestykkerne fra 0 til a og b. Det punkt, hvor halveringslinien skærer liniestykket fra a til b er $\frac{|b|a+|a|b}{|a|+|b|}$.

2.6. Find alle de 12te enhedsrødder.

2.7. Udregn med tilnærmelse alle 3 værdier af $\sqrt[3]{\sqrt{3}\sqrt{5}+i4\sqrt{5}}$. Lykkelige ejere af en lommeregner kan i stedet prøve med $\sqrt[3]{3,1872+i2,915}$.

2.8. Anvend Eulers formler og formlen for summen af en kvotientrække til et bevis for formlen

$$\tfrac{1}{2}+\cos x+\cos 2x+\ldots+\cos nx = \frac{\sin(n+\frac{1}{2})x}{2\sin\frac{1}{2}x}$$

2.9. Find rødderne i polynomiet $x^2 + (7+i6)x - (1+i15)$.

2.10. Det er klart, at to ligninger af første grad med to ubekendte og med komplekse koefficienter og ubekendte kan behandles på samme måde, som tilsvarende ligninger med reelle koefficienter og reelle ubekendte. Find løsningerne til

$$(2+i)x + (3-i2)y = -1-i3$$
$$(4+i3)x + (2-i3)y = -6+i4.$$

op de punkter, hvis afstande fra a og -a har produkt b^2, hvor b^2 er cirklens radius. Kurven kaldes en lemniskat. Særlig interesse har lemniskaten gennem (0,0). I retvinklede (x,y)-koordinater er den løsningsmængden til ligningen $(x^2+y^2)^2-2a^2(x^2-y^2) = 0$. I polære (r,θ)-koordinater er den bestemt ved $r^2 = 2a^2\cos 2\theta$.

2.13.4. Billedet af en cirkel gennem 0 og med centrum i $a > 0$ er en kurve, der kaldes en cardioide (hjertekurve), selv om den måske snarere minder om snitfladen i et overskåret æble.

2.14. Den ved $f(z) = \frac{1}{z}$ definerede afbildning $f:\mathbb{C}\setminus\{0\} \to \mathbb{C}\setminus\{0\}$ afbilder en ligesidet hyperbel med centrum i 0 og første akse på den reelle akse i en kurve, der ved nærmere studium viser sig at være identisk med den i 2.13.3 omtalte lemniskat gennem 0.

2.15. Ved $f(z) = z + \frac{1}{z}$ defineres en afbildning $f:\mathbb{C}\setminus\{0\} \to \mathbb{C}$. Det er let at se, at f afbilder enhedscirklen $U = \{z \in C \mid |z| = 1\}$ på liniestykket med endepunkter i z og -z. Det er også let at se, at f afbilder $\mathbb{C}\setminus\{-1,0,1\}$ surjektivt på $\mathbb{C}\setminus\{-2,2\}$, således at hver punkt af denne mængde får netop 2 originalpunkter. Endvidere afbilder f mængden af

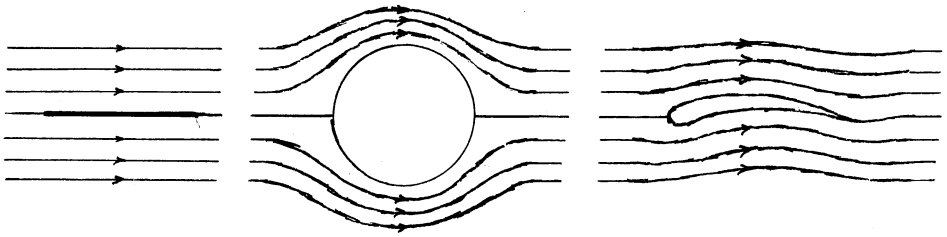
punkter udenfor enhedscirklen bijektivt på mængden af punkter, der ikke ligger på liniestykket med endepunkter 2 og -2.
En vilkårlig cirkel U_1 gennem 1 og -1 afbildes ved f på en cirkelbue med endepunkter 2 og -2. Vælg U_1 tæt ved U og tegn billedet af en cirkel U_2, der omslutter U_1, rører U_1 i punktet 2, men ikke særlig meget større end U_2. Den fremkomne kurve kaldes en Joukowski-profil efter den russiske hydrodynamiker N.E. Joukowski som virkede i begyndelsen af dette århundrede.

∫ Man kan differentiere afbildninger $f:O \subseteq \mathbb{C}$, hvor $O \subseteq \mathbb{C}$ er en åben mængde, ganske som funktioner af reelle variable. Simple udtryk som z^4+2z, $\frac{z+4}{(2z+3)^2}$, ze^z definerer differentiable funktioner. Det viser sig til gengæld, at så pæne udtryk som Re z, $|z|$ og $\overline{z}$ definerer funktioner, som er intet steds differentiable. Derfor har differentiable funktioner også fået andre navne. Mest bruges "holomorf", men "analytisk" bruges næsten lige så tit. Man har også brugt "regulær", men denne betegnelse har man sat på næsten alt pænt - det må være matematikkens mest misbrugte glose.

Holomorfe funktioner spiller en vældig rolle for anvendelserne, til dels som mere regnetekniske hjælpe-

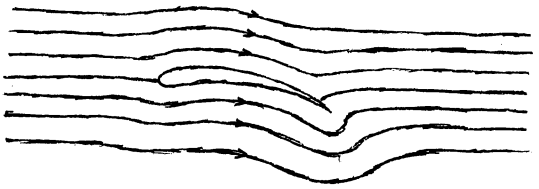
midler. Der er imidlertid en meget direkte forbindelse til de teknisk-fysiske anvendelser, og det beror på, at strømlinierne for plane strømninger i en ideal væske, samt kraftlinierne for plane elektriske og magnetiske felter i det tomme rum netop er niveaukurver for realdele af holomorfe funktioner.

Dette bevirker, at afbildninger ved holomorfe funktioner afbilder feltlinier i feltlinier for de her omtalte felter. Derfor kan man ved passende udnyttelse af den ved $z+\frac{1}{z}$ definerede afbildning få den serie af strømliniebilleder, der er vist på figurerne her.



Som antydet på den sidste figur, der viser strømningen om Joukowski-profilet, minder dette en hel del om profiler af skibsskruer, propeller, aeroplanvinger, turbineskovle etc. De her omhandlede afbildninger var et væsentligt led i bestræbelserne i begyndelsen af dette århundrede for at forstå kraftpåvirkninger og energiomsætning ved disse vigtige tekniske hjælpemidler.

Nu har vi begået et mindre snyderi, idet vi har ladet strømmene over og under Joukowski-profilet mødes netop ved den skarpe kant. Det sker selvfølgelig kun, når den er drejet i den helt rigtige stilling. hvis vi vipper forenden lidt opad, skilles strømningen på ryggen.



Beregningen i denne situation vil vise, at profilet ikke påvirkes af nogen kraft. Det er Joukowski's paradoks. Nu er strømningen stærkt ustabil. Det har den virkning, at der opstår en hvirvelstrøm om profilet (i retning med uret på figuren), og den skubber delingspunktet på ryggen hen i spidsen, så vi får glat afstrømning, og det viser sig, at så påvirkes profilet af en kraft, der er opadrettet, og så kan det altså lade sig gøre at flyve.

KAPITEL 3

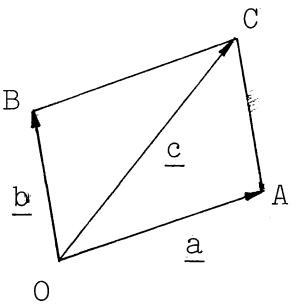
Lineær vektorregning.

I dette kapitel vil vi med E^3 betegne det 3-dimensionale Euklidiske rum, med E^2 den Euklidiske plan og med E^1 den Euklidiske rette linie. Hver plan i E^3 er en kopi af E^2, og hver ret linie i E^2 eller E^3 er en kopi af E^1. Vi vil somme tider skrive E^n, og så er det underforstået, at n kan betyde 1, 2 eller 3.

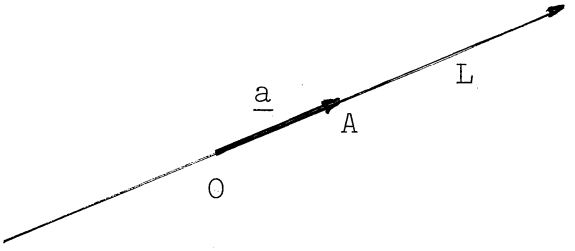
Lad $O \in E^m$ være et fast valgt punkt. Så er ethvert punkt $P \in E^m$ entydigt fastlagt ved det orienterede liniestykke $OP=\underline{p}$. Et sådan orienteret liniestykke kaldes en vektor, og vi siger, at det orienterede liniestykke OP repræsenterer vektoren $\underline{p}$, men vi vil også sige, at ethvert andet orienteret liniestykke AB med samme retning og samme længde som OP repræsenterer vektoren $\underline{p}$. Så er $OPBA$ et (eventuelt fladklemt) parallelogram, og AB fås ved at parallelforskyde OP stykket OA. At liniestykket AB skal repræsentere vektoren $\underline{p}$ antydes på en figur ved at forsyne AB med en pilespids i endepunktet B. Når vi siger, at vektoren $\underline{p}$ ligger på den rette linie L (eller i planen F), mener vi, at $\underline{p}$ er repræsenteret ved et orienteret liniestykke AB, som ligger på L (eller i F). Når vi siger, at $\underline{p}$ er afsat ud fra A, mener vi, at $\underline{p}$ er repræsenteret

ved et liniestykke AB. Når $\underline{p}$ er afsat ud fra O, altså repræsenteret ved OP, siger vi, at $\underline{p}$ er stedvektor for punktet P. For P = O udarter liniestykket OP til selve punktet O, som vi betragter som et udartet liniestykke, der har længde 0 og alle retninger, og det repræsenterer en vektor, der kaldes nulvektor og betegnes $\underline{0}$. Den er stedvektor for O.

Lad $\underline{a}$ og $\underline{b}$ være stedvektorer for A og B. Hvis $\underline{b}$ afsat ud fra A får endepunkt C med stedvektor $\underline{c}$ definerer vi $\underline{a}+\underline{b}=\underline{c}$. Så er OACB et (eventuelt fladklemt) parallelogram, og vi har derfor også $\underline{b}+\underline{a}=\underline{c}$. Det er klart at additionen også bliver associativ, og at $\underline{0}$ bliver neutralelement. En vektor $\underline{a}$ får en modsat vektor $-\underline{a}$, og O er midtpunkt af liniestykket, der forbinder punkterne med stedvektoren $\underline{a}$ og $-\underline{a}$. Vi får en subtraktion af vektorer, og med samme betegnelser som ovenfor vil liniestykket AB repræsentere $\underline{b}-\underline{a}$.

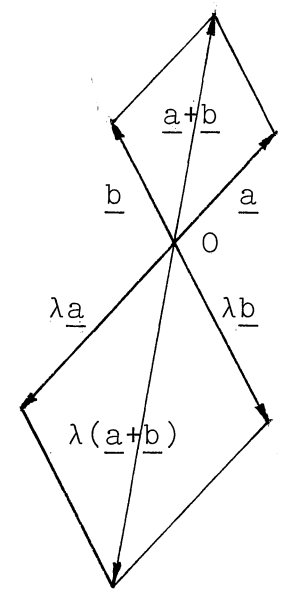


En stedvektor $\underline{a}$ for et punkt A ligger på en ret linie L gennem O, og hvis $\underline{a}\neq\underline{0}$ bestemmer $\underline{a}$ en orientering på L, så vi kan regne længder på L med fortegn. Idet $\|\underline{a}\|$ betegner længden af vektoren $\underline{a}$, bliver $\|\underline{a}\|$ også den med fortegn regnede længde af OA. For $\lambda \in \mathbb{R}$ findes der netop et punkt B på L,



for hvilket den med fortegn regnede længde af OB er $\lambda\|\underline{a}\|$, og hvis $\underline{b}$ er stedvektor for B definerer vi $\underline{b}=\lambda\underline{a}$. For $\underline{a}=\underline{0}$ kan enhver orienteret linie gennem O benyttes som L, og vi får $\lambda\underline{0}=\underline{0}$ for alle $\lambda \in \mathbb{R}$. Endvidere ses det umiddelbart, at vi har regnereglerne $(\lambda+\mu)\underline{a}=\lambda\underline{a}+\mu\underline{a}$, $(\lambda\mu)\underline{a}=\lambda(\mu\underline{a})$, $0\underline{a}=\underline{0}$, $1\underline{a}=\underline{a}$.

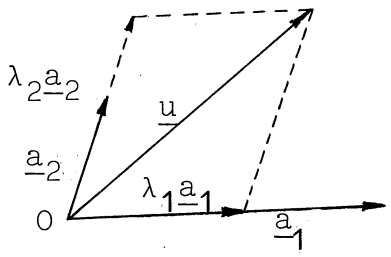
Idet billedet af et parallelogram ved en ligedannethedstransformation igen er et parallelogram, viser figuren umiddelbart, at vi også har regnereglen $\lambda(\underline{a}+\underline{b})=\lambda\underline{a}+\lambda\underline{b}$.



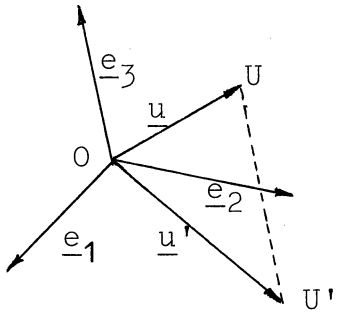
Med $\mathbb{E}^n$ betegner vi mængden af vektorer i E^n organiseret ved de to ovenfor indførte regneregler addition $\underline{a}+\underline{b}$ og multiplikation med et reelt tal $\lambda\underline{a}$. Et reelt tal kaldes i denne sammenhæng ofte en skalar, men vi skal dog senere nærmere præcisere brugen af dette særlige ord.

For $\underline{a}_1,\ldots,\underline{a}_p \in \mathbb{E}^n$ og $\lambda_1,\ldots,\lambda_p \in \mathbb{R}$ kan vi udregne vektoren $\lambda_1\underline{a}_1+\ldots+\lambda_p\underline{a}_p$, der kaldes en linearkombination af vektorerne $\underline{a}_1,\ldots,\underline{a}_p$. En linearkombination af $\underline{0}$ altså $\lambda\underline{0}$ kan kun give $\underline{0}$. For $\underline{a}\neq\underline{0}$ ligger $\underline{a}$ på en ret linie L, og enhver vektor på L er en linearkombination $\lambda\underline{a}$. Hvis $\underline{a}_1,\ldots,\underline{a}_p$ er vektorer på L og ikke alle $\underline{0}$, vil mængden af

linearkombinationer af $\underline{a}_1,\ldots,\underline{a}_p$ netop være mængden af vektorer på L. Hvis $\underline{a}_1$ og $\underline{a}_2$ ikke ligger på samme rette linie, ligger $\underline{a}_1$ og $\underline{a}_2$ i en plan F. Det ses umiddelbart af figuren, at enhver vektor $\underline{u}$, der ligger i F, på én og kun én måde kan skrives som en linearkombination $\lambda_1\underline{a}_1+\lambda_2\underline{a}_2$, og at enhver sådan linearkombination er en vektor i F.



I $\mathbb{E}^3$ kan vi finde tre vektorer $\underline{e}_1$, $\underline{e}_2$ og $\underline{e}_3$, der ikke ligger i samme plan. Enhver vektor $\underline{u} \in \mathbb{E}^3$ kan da på én og kun én måde skrives som en linearkombination $\underline{u}=\lambda_1\underline{e}_1+\lambda_2\underline{e}_2+\lambda_3\underline{e}_3$. Lad $\underline{u}$ være stedvektor for U, og lad U' være det punkt, hvor den rette linie gennem U parallel med $\underline{e}_3$ skærer planen gennem $\underline{e}_1$ og $\underline{e}_2$ og lad $\underline{u}'$ være stedvektor for U'. Så vil U'U repræsentere en vektor $\lambda_3\underline{e}_3$ og vi har $\underline{u}=\underline{u}'+\lambda_3\underline{e}_3$, hvor $\underline{u}'$ på én og kun én måde kan skrives $\underline{u}'=\lambda_1\underline{e}_1+\lambda_2\underline{e}_3$. Dette viser eksistensen af fremstillingen. Endvidere fremgår det umiddelbart, at spaltningen $\underline{u}=\underline{u}'+\lambda_3\underline{e}_3$ en entydig, og deraf følger entydigheden.



Vi siger, at en mængde M af vektorer i $\mathbb{E}^n$ er lineært afhængig, hvis vi kan vælge indbyrdes forskellige vektorer $\underline{a}_1,\ldots,\underline{a}_p \in M$ og reelle

tal $\lambda_1,\ldots,\lambda_p$, som ikke er 0, således at $\lambda_1\underline{a}_1+\ldots+\lambda_p\underline{a}_p=\underline{0}$.

Denne definition er ækvivalent med den vi får ved at erstatte bisætningen "som ikke er 0" med "som ikke alle er 0". Hvis $\underline{0} \in M$, er M lineært afhængig. Hvis M ikke er lineært afhængig, kaldes M lineært uafhængig. En mængde M, der kun omfatter én vektor $\underline{a} \in \mathbb{E}^n$ er lineært afhængig, hvis og kun hvis $\underline{a}=\underline{0}$. En mængde $M=\{\underline{a}_1,\underline{a}_2\}$ er lineært afhængig, hvis og kun hvis $\underline{a}_1$ og $\underline{a}_2$ ligger i samme rette linie, og $\{\underline{a}_1, \underline{a}_2, \underline{a}_3\}$ er lineært afhængig, hvis og kun hvis $\underline{a}_1, \underline{a}_2, \underline{a}_3$ ligger i samme plan. I $\mathbb{E}^n$ findes maksimalt n lineært uafhængige vektorer.

En mængde M af n lineært uafhængige vektorer i $\mathbb{E}^n$ kaldes en basis for $\mathbb{E}^n$.

Lad $\{\underline{e}_1, \underline{e}_2, \underline{e}_3\}$ være en basis for $\mathbb{E}^3$. Enhver vektor $\underline{a} \in \mathbb{E}^3$ har da én og kun én fremstilling som en linearkombination $\underline{a}=a_1\underline{e}_1+a_2\underline{e}_2+a_3\underline{e}_3$. Man vil i reglen arrangere basisvektorerne i en bestemt rækkefølge som en ordnet basis $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$ og hver vektor $\underline{a}$ får da et bestemt koordinatsæt (a_1, a_2, a_3) af reelle tal, således at $\underline{a}=a_1\underline{e}_1+a_2\underline{e}_2+a_3\underline{e}_3$. Vi vil også sige, at (a_1, a_2, a_3) er koordinatsæt for punktet A med stedvektor $\underline{a}$. Et punkts koordinatsæt afhænger således af valget af begyndelsespunkt og ordnet basis.

Vi tænker os nu den ordnede basis $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$ fast valgt. Hvis $\underline{a}$ har koordinatsættet (a_1, a_2, a_3) og $\underline{b}$ har koordi-

natsættet (b_1, b_2, b_3), vil $\underline{a}+\underline{b}$ have koordinatsættet $(a_1+b_1, a_2+b_2, a_3+b_3)$, og $\lambda\underline{a}$ vil have koordinatsættet $(\lambda a_1, \lambda a_2, \lambda a_3)$.

Hvad vi har sagt om $\mathbb{E}^3$ i de to sidste afsnit kan kopieres for $\mathbb{E}^2$ med indlysende ændringer, og vi får også en helt triviel kopi for $\mathbb{E}^1$.

Vi minder om begrebet determinant, som er kendt fra skolen. For vilkårlige reelle tal x_1, x_2, y_1, y_2 defineres determinanten

$$\begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} = x_1y_2 - x_2y_1.$$

Når vi har valgt en ordnet basis $\underline{e}_1, \underline{e}_2$ for $\mathbb{E}^2$ og $\underline{x} = x_1\underline{e}_1 + x_2\underline{e}_2$ og $\underline{y}=y_1\underline{e}_1+y_2\underline{e}_2$, sætter vi

$$\det_{\underline{e}_1,\underline{e}_2}(\underline{x},\underline{y}) = \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}.$$

Vi ser umiddelbart, at $\det_{\underline{e}_1,\underline{e}_2}(\underline{x},\underline{y})$ skifter fortegn ved ombytning af $\underline{x}$ og $\underline{y}$ og ligeledes ved ombytning af $\underline{e}_1$ og $\underline{e}_2$. Desuden ses det umiddelbart, at vi for $\lambda \in \mathbb{R}$ har

$$\det_{\underline{e}_1,\underline{e}_2}(\underline{x},\underline{y}) = \det_{\underline{e}_1,\underline{e}_2}(\underline{x},\underline{y}+\lambda\underline{x}) = \det_{\underline{e}_1,\underline{e}_2}(\underline{x}+\lambda\underline{y}, \underline{y}).$$

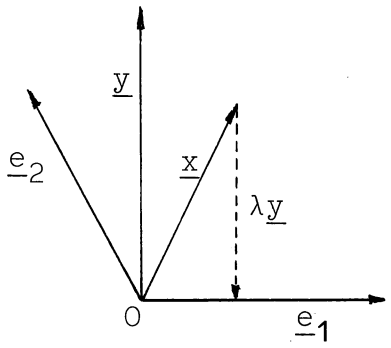
Vi har nu følgende sætning:

Vektorerne $\underline{x}$ og $\underline{y}$ er lineært afhængige, hvis og kun hvis $\det_{\underline{e}_1,\underline{e}_2}(\underline{x},\underline{y}) = 0$.

Bevis. Vi udnytter, at vi kan erstatte $\underline{x}$ med $\underline{x}+\lambda\underline{y}$ eller $\underline{y}$ med $\underline{y}+\lambda\underline{x}$ uden at ændre værdien af $\det_{\underline{e}_1,\underline{e}_2}(\underline{x},\underline{y})$, og uden at ændre den lineære afhængighed eller uafhængighed af $\underline{x}$ og $\underline{y}$. Vi fører beviset ved at dele i to tilfælde.

1). Hvis $\underline{x}=\underline{0}$ eller $\underline{y}=\underline{0}$ er $\underline{x}$ og $\underline{y}$ lineært afhængige, og $\det_{\underline{e}_1,\underline{e}_2}(\underline{x},\underline{y})=0$, så påstanden er rigtig i dette tilfælde.

2). Hvis $\underline{x}\neq\underline{0}$ og $\underline{y}\neq\underline{0}$, og alle vektorerne afsættes ud fra et punkt 0, vil linien gennem endepunktet af $\underline{x}$ parallel med $\underline{y}$ skære en af de linier, hvorpå $\underline{e}_1$ og $\underline{e}_2$ ligger, lad os sige $\underline{e}_1$. Vi kan da vælge $\lambda,\mu \in \mathbb{R}$, så $\underline{x}+\lambda\underline{y}=\mu\underline{e}_1$ og ifølge bemærkningen øverst på siden er det nok at vise påstanden for vektorerne $\mu\underline{e}_1$ og $\underline{y}$. Vi får



$$\det_{\underline{e}_1,\underline{e}_2}(\mu\underline{e}_1,\underline{y}) = \begin{vmatrix} \mu & y_1 \\ 0 & y_2 \end{vmatrix} = \mu y_2 ,$$

hvilket viser, at $\det_{\underline{e}_1,\underline{e}_2}(\mu\underline{e}_1,y_2)$ er ensbetydende med, at $\mu = 0$ eller $y_2 = 0$. Men $\mu\underline{e}_1$ og $\underline{y}$ er netop lineært afhængige, hvis og kun hvis $\mu\underline{e}_1 = 0$ altså $\mu = 0$ eller $\underline{y}$ er ensrettet med $\mu\underline{e}_1$, altså $y_2 = 0$. Dermed er sætningen bevist.

Det kunne vi nok have klaret lettere, men vi har valgt at indrette beviset, så vi kan lave noget lignende i $\mathbb{E}^3$ ved hjælp af en determinant

$$\begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} = \begin{matrix} x_1y_2z_3 + y_1z_2x_3 + z_1x_2y_3 \\ -x_1z_2y_3 - y_1x_2z_3 - z_1y_2x_3. \end{matrix}$$

Hvis vi skriver første og anden søjle op engang til til højre, altså

$$\begin{matrix} x_1 & y_1 & z_1 & x_1 & y_1 \\ x_2 & y_2 & z_2 & x_2 & y_2 \\ x_3 & y_3 & z_3 & x_3 & y_3, \end{matrix}$$

optræder de tre produkter med plus i de rækker, der går skråt nedad mod højre, medens de tre produkter med minus optræder i de rækker, der går skråt opad mod højre. Det er nu let at konstatere symmetriegenskaben

$$\begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} = \begin{vmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{vmatrix}.$$

Det vigtigste hjælpemiddel er de følgende udviklingsformler, der umiddelbart afledes af selve definitionen ovenfor.

$$\begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} = x_1 \begin{vmatrix} y_2 & z_2 \\ y_3 & z_3 \end{vmatrix} + x_2 \begin{vmatrix} y_3 & z_3 \\ y_1 & z_1 \end{vmatrix} + x_3 \begin{vmatrix} y_1 & z_1 \\ y_2 & z_2 \end{vmatrix} =$$

$$y_1 \begin{vmatrix} z_2 & x_2 \\ z_3 & x_3 \end{vmatrix} + y_2 \begin{vmatrix} z_3 & x_3 \\ z_1 & x_1 \end{vmatrix} + y_3 \begin{vmatrix} z_1 & x_1 \\ z_2 & x_2 \end{vmatrix} =$$

$$z_1 \begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix} + z_2 \begin{vmatrix} x_3 & y_3 \\ x_1 & y_1 \end{vmatrix} + z_3 \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}.$$

Heraf fremgår umiddelbart, at determinantens værdi forbliver uændret ved kredsforskydning af søjlerne eller rækkerne, men skifter fortegn ved ombytning af to søjler, og ifølge symmetriegenskaben også ved ombytning af to rækker.

Hvis $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$ er en ordnet basis for $\mathbb{E}^3$, og

$$\underline{x} = x_1\underline{e}_1 + x_2\underline{e}_2 + x_3\underline{e}_3$$
$$\underline{y} = y_1\underline{e}_1 + y_2\underline{e}_2 + y_3\underline{e}_3$$
$$\underline{z} = z_1\underline{e}_1 + z_2\underline{e}_2 + z_3\underline{e}_3$$

er vilkårlige vektorer, definerer vi

$$\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\underline{y},\underline{z}) = \begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix}.$$

Af de tre udviklingsformer ovenfor fremgår umiddelbart, at vi for $\underline{x}',\underline{y}',\underline{z}',\underline{x}'',\underline{y}'',\underline{z}'' \in \mathbb{E}^3$ og $\lambda',\mu',\nu',\lambda'',\mu'',\nu'' \in \mathbb{R}$ har

$$\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\lambda'\underline{x}'+\lambda''\underline{x}'',\underline{y},\underline{z}) = \lambda'\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x}',\underline{y},\underline{z}) + \lambda''\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x}'',\underline{y},\underline{z}),$$

$$\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\mu'\underline{y}'+\mu''\underline{y}'',\underline{z}) = \mu'\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\underline{y}',\underline{z}) + \mu''\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\underline{y}'',\underline{z}),$$

$$\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\underline{y},\nu'\underline{z}'+\nu''\underline{z}'') = \nu'\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\underline{y},\underline{z}') + \nu''\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(x,y,z'').$$

På grund af disse egenskaber vil vi sige, at afbildningen

$$\det_{\underline{e}_1\underline{e}_2\underline{e}_3} : \mathbb{E}^3 \times \mathbb{E}^3 \times \mathbb{E}^3 \to \mathbb{R}.$$

er trilineær.

Vi vil nu indføre to slags "elementære operationer", der kan anvendes på ordnede sæt $(\underline{x},\underline{y},\underline{z})$ af vektorer i $\mathbb{E}^3$, og som overfører lineært afhængige sæt i lineært afhængige sæt og lineært uafhængige sæt i lineært uafhængige sæt, og som desuden lader $\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\underline{y},\underline{z})$ uændret.

Den første slags elementær operation på $(\underline{x},\underline{y},z)$ består i ombytning af to af vektorerne kombineret med fortegnsskift på én af de tre vektorer. Derved kan $(\underline{x},\underline{y},\underline{z})$ omformes til $(\underline{y},\underline{x},-\underline{z})$, $(-\underline{y},\underline{x},\underline{z})$ etc. Det er helt klart, at disse operationer ikke vil ændre lineær afhængighed eller uafhængighed, og vi bemærkede ovenfor, at ombytning af søjler bevirkede fortegnsskift i determinanten og dette ophæves igen af fortegnsskiftet på den ene vektor, så operationen har de ønskede egenskaber.

Hvis to af vektorerne $\underline{x},\underline{y},\underline{z}$ er ens, vil ombytning af disse lade $\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\underline{y},\underline{z})$ være uændret, og da den også må skifte fortegn, kan vi slutte, at $\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\underline{y},\underline{z})=o$, hvis to af vektorerne $\underline{x},\underline{y},\underline{z}$ er identiske. Idet vi udnytter trilineariteten får vi derefter for vilkårlige vektorer $\underline{x},\underline{y},\underline{z}$, at $\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\underline{y},\underline{z})$ forbliver uændret, når en linearkombination af to af vektorerne adderes til den tredie, altså f.eks.

$$\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\underline{y},\underline{z}) = \det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\underline{y} + \lambda\underline{x} + \nu\underline{z},\underline{z}),$$

for vilkårlige $\lambda,\nu \in \mathbb{R}$. Dette er den anden slags elementære operationer. Hvis $\underline{x},\underline{y},\underline{z}$ er lineært afhængige, ligger de i en plan, og det er da klart, at de også efter ændringen vil ligge i den samme plan. Hvis $\underline{x},\underline{y},\underline{z}$ er lineært uafhængige, ligger den ændrede vektor ikke i planen gennem de to andre, og da den ændres med en vektor i denne plan, vil den også efter ændringen ligge udenfor denne plan. Altså har også denne slags elementær operation de ønskede egenskaber.

Vi understreger, at selve basen $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$ ikke indgår i de elementære operationer. Vi viser nu følgende sætning:

Lad $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$ være en given basis for $\mathbb{E}^3$, og lad $(\underline{x},\underline{y},\underline{z})$ være et ordnet sæt af lineært uafhængige vektorer i $\mathbb{E}^3$. Der findes da et sæt (λ,μ,ν) af reelle tal, for hvilket $(\underline{x},\underline{y},\underline{z})$ ved elementære operationer kan overføres i $(\lambda\underline{e}_1,\mu\underline{e}_2,\nu\underline{e}_3)$, og for et sæt (λ,μ,ν) af reelle tal med denne egenskab gælder $\lambda\mu\nu = \det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\underline{y},\underline{z})$.

Bevis. Den sidste påstand følger af, at

$$\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\underline{y},\underline{z}) = \det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\lambda\underline{e}_1,\mu\underline{e}_2,\nu\underline{e}_3) = \begin{vmatrix} \lambda & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & \nu \end{vmatrix} = \lambda\mu\nu.$$

Ved om nødvendigt at benytte en elementær operation af den første slags opnår vi, at $\underline{e}_1$ ikke er parallel med planen p

gennem $\underline{y}$ og $\underline{z}$. Vektoren $\underline{x}$ er da sum af en vektor $\lambda\underline{e}_1$, og en vektor $\underline{u} = \mu'\underline{y} + \nu'\underline{z}$. Den elementære operation, der erstatter $\underline{x}$ med $\underline{x}-(\mu'\underline{y}+\nu'\underline{z})$ fører da $(\underline{x},\underline{y},\underline{z})$ over i $(\lambda\underline{e}_1,\underline{y},\underline{z})$. Ved om nødvendigt at benytte en elementær operation, der bytter $\underline{y}$ og $\underline{z}$ og skifter fortegn på én af dem, opnår vi, at $\underline{e}_2$ ikke er parallel med planen gennem $\underline{e}_1$ og $\underline{z}$, og på samme måde som før kan vi så ved en elementær operation føre $(\lambda\underline{e}_1,\underline{y},\underline{z})$ over i $(\lambda\underline{e}_1,\mu\underline{e}_2,\underline{z})$ for et passende μ, og endelig vil en sidste elementær operation føre $(\lambda\underline{e}_1,\mu\underline{e}_2,\underline{z})$ over i $(\lambda\underline{e}_1,\mu\underline{e}_2,\nu\underline{e}_3)$. Dermed er sætningen bevist.

Hvis $(\underline{x},\underline{y},\underline{z})$ er lineært afhængige, er én af dem en linearkombination af de to andre, og derfor kan $(\underline{x},\underline{y},\underline{z})$ ved en elementær operation af den anden slags overføres i et sæt, hvor den ene vektor er $\underline{0}$, så vi har $\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\underline{y},\underline{z})=0$ i dette tilfælde. Ved at sammenholde dette med sætningen ovenfor får vi følgende sætning.

For enhver basis $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$ for $\mathbb{E}^3$ og et vilkårligt sæt $(\underline{x},\underline{y},\underline{z})$ af vektorer fra $\mathbb{E}^3$ gælder, at $(\underline{x},\underline{y},\underline{z})$ er lineært afhængigt, hvis og kun hvis $\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\underline{y},\underline{z})=0$.

Vi har desuden følgende sætning:

For vilkårlige baser $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$, $(\underline{e}_1',\underline{e}_2',\underline{e}_3')$ og $(\underline{e}_1'',\underline{e}_2'',\underline{e}_3'')$ for $\mathbb{E}^3$ gælder relationen

$$\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{e}_1'',\underline{e}_2'',\underline{e}_3'')=$$

$$\det_{\underline{e}_1'\underline{e}_2'\underline{e}_3'}(\underline{e}_1'',\underline{e}_2'',\underline{e}_3'')\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{e}_1',\underline{e}_2',\underline{e}_3')$$

Bevis. Ved elementære operationer kan $(\underline{e}_1'',\underline{e}_2'',\underline{e}_3'')$ føres over i $(\lambda_1\underline{e}_1',\lambda_2\underline{e}_2',\lambda_3\underline{e}_3')$ med $\lambda_1\lambda_2\lambda_3 = \det_{\underline{e}_1'\underline{e}_2'\underline{e}_3'}(\underline{e}_1'',\underline{e}_2'',\underline{e}_3'')$, og sætningen følger derefter af, at

$$\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{e}_1'',\underline{e}_2'',\underline{e}_3'')=\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\lambda_1\underline{e}_1',\lambda_2\underline{e}_2',\lambda_3\underline{e}_3')=$$
$$\lambda_1\lambda_2\lambda_3 \det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{e}_1',\underline{e}_2',\underline{e}_3').$$

Heraf følger umiddelbart, at relationen

$$\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{e}_1',\underline{e}_2',\underline{e}_3') > 0$$

mellem baser $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$ og $(\underline{e}_1',\underline{e}_2',\underline{e}_3')$ for $\mathbb{E}^3$ er en ækvivalensrelation på mængden af baser for $\mathbb{E}^3$, og at der bliver netop 2 ækvivalensklasser. At hverken $(\underline{e}_1',\underline{e}_2',\underline{e}_3')$ eller $(\underline{e}_1'',\underline{e}_2'',\underline{e}_3'')$ er i klasse med $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$ betyder nemlig, at

$$\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{e}_1',\underline{e}_2',\underline{e}_3') < 0 \quad \text{og} \quad \det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{e}_1'',\underline{e}_2'',\underline{e}_3'') < 0,$$

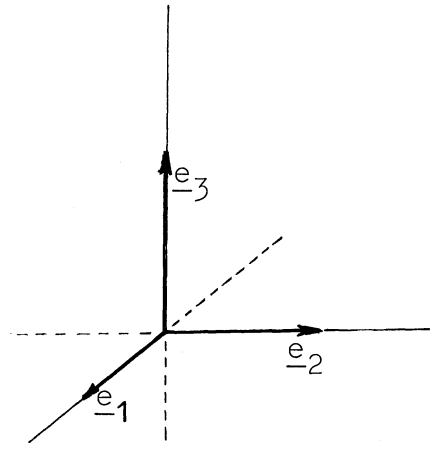
og det medfører, at $\det_{\underline{e}_1'\underline{e}_2'\underline{e}_3'}(\underline{e}_1'',\underline{e}_2'',\underline{e}_3'') > 0$, altså at baserne $(\underline{e}_1',\underline{e}_2',\underline{e}_3')$ og $(\underline{e}_1'',\underline{e}_2'',\underline{e}_3'')$ er i samme klasse.

Vi siger, at det Euklidiske rum E^3 er orienteret, når vi har truffet et valg mellem de to klasser af baser for mængden $\mathbb{E}^3$ af vektorer i E^3. Vi vil så tale om positive baser og negative baser. Nu er der det helt specielle ved rummet E^3, at det er det rum, vi selv lever i, og det har den virkning, at valg af orientering bliver et fysisk problem, og som så man-

ge andre fysiske problemer klares det ved, at man vælger sig en normal. Man kan have en model i sterlingsølv på sit skrivebord visende tre lineært uafhængige vektorer, der udgår fra samme punkt, og så kan man vedtage, at denne model skal være positiv. Man forestiller sig, at ved omflytning af modellen vil den determinant, der fastlægger orienteringen i relation til en fast model, variere kontinuert, så den ikke kan springe over den forbudte værdi 0 og blive negativ. I fysik foretrækker man at bruge et normalsystem, der er fastlagt ved retningerne af højre hånds tommel- pege- og langefinger i den nævnte rækkefølge, når man holder hånden, så tommel- og pegefingeren er vinkelrette på hinanden i håndfladens plan, medens langefingeren er vinkelret på håndfladens plan. Baser for $\mathbb{E}^3$ med hertil svarende orientering kaldes højrekoordinatsystemer, og baser med den modsatte orientering kaldes venstresystemer. Den danske fysiker Holten har formuleret en regel, som mange finder bekvem:

Grib om en koordinatakse med højre hånd, så tommelfingeren vender i den positive retning. Hvis fingerspidserne på de andre fingre så viser i den ved de to andre koordinatakser bestemte omløbsretning, er koordinatsystemet et højresystem.

Rummets orientering spiller en væsentlig rolle ved formuleringen af de elektromagnetiske love, men sammenhængen af disse love med rummets orientering beror igen på en række valg: Hvilken magnetpol skal hedde nordpol, hvilken slags elektricitet kaldes positiv, og hvordan defineres retningen af en elektrisk strøm?



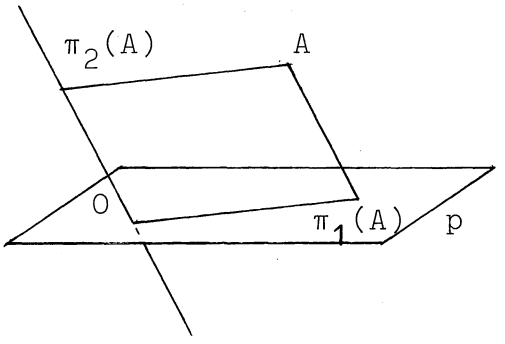
I abstrakt matematik har vi slet ingen mulighed for at give en standardregel, der fastlægger en orientering, men så snart vi tegner noget på papiret arbejder vi med noget materielt, og vi vil da regne højrekoordinatsystemer positivt orienterede. Man ser hyppigt et højrekoordinatsystem tegnet som vist, altså første akse fremad fra papiret, anden akse rettet mod højre i papirets plan og tredie akse rettet opad i papirets plan. Dette stemmer med de ovenfor givne "højrehåndsregler". En del danske lærebøger fra mellemkrigstiden brugte den samme model med $\underline{e}_1$ og $\underline{e}_2$ byttet, altså et venstrekoordinatsystem. Endnu tidligere brugtes især højrekoordinatsystemer med akserne kredsforskudt i forhold til vor model, så den tredie akse pegede fremad fra papiret.

I $\mathbb{E}^2$ har vi ganske analogt (og en hel del lettere) indført det$_{\underline{e}_1,\underline{e}_2}(\underline{x},\underline{y})$, og det giver på samme måde en inddeling af mængden af baser for $\mathbb{E}^2$ i to klasser, og dermed får vi en orientering af den Euklidiske plan E^2. Nu er E^2 jo noget, vi ser udefra, og E^2 kan ses fra to sider. Vi vælger en side at se E^2 fra, den positive side, og så er det sædvanligt at vælge orienteringen, så drejningsretningen fra den første til den anden basisvektor set fra den positive side er mod urvisernes bevægelsesretning.

Vi vil nu slutte kapitlet med lidt analytisk geometri.

Først vil vi dog anføre en enkelt bemærkning, som vil være nyttig senere.

Lad $P \subsetneq E^3$ være en plan, og lad $L \subsetneq E^3$ være en ret linie, som skærer P i et punkt O. Lad $A \in E^3$ være et vilkårligt punkt. Den rette linie gennem A parallel med L skærer da P i et punkt $\pi_1(A)$, som vi kalder projektionen af A på P i retningen L. Planen gennem A parallel med P skærer L i et punkt $\pi_2(A)$, som vi kalder projektionen af A på L i retningen P.



Derved fås et (måske fladklemt) parallelogram $O\pi_1(A)A\pi_2(A)$.
Vi indfører nu et koordinatsystem med begyndelsespunkt O, basisvektorer $\underline{e}_1$ og $\underline{e}_2$ i P, samt $\underline{e}_3$ på L. Hvis nu stedvektor for A er

$$\underline{a} = a_1\underline{e}_1 + a_2\underline{e}_2 + \underline{a}_3\underline{e}_3.$$

får vi, at stedvektorerne $\pi_1(\underline{a})$ og $\pi_2(\underline{a})$ for $\pi_1(A)$ og $\pi_2(A)$ er givet ved

$$\pi_1(\underline{a}) = a_1\underline{e}_1 + a_2\underline{e}_2 \ , \ \pi_2(\underline{a}) = a_3\underline{e}_3.$$

Hvis punkter A og B har stedvektorer $\underline{a}$ og $\underline{b}$, medens $\underline{a}+\underline{b}$ er stedvektor for C, og vi skriver $\pi_1(\underline{a})$, $\pi_1(\underline{b})$ og $\pi_1(\underline{a}+\underline{b})$ for stedvektorerne for $\pi_1(A)$, $\pi_1(B)$ og $\pi_1(C)$ og analogt for π_2, har vi regnereglerne

$$\pi_1(\underline{a}+\underline{b}) = \pi_1(\underline{a}) + \pi_1(\underline{b}), \quad \pi_2(\underline{a}+\underline{b}) = \pi_2(\underline{a}) + \pi_2(\underline{b}),$$

som umiddelbart følger af de udtryk, vi ovenfor fandt for $\pi_1(\underline{a})$ og $\pi_2(\underline{a})$. Liniestykket fra A til B repræsenterer vektoren $\underline{b}-\underline{a}$, og regnereglen ovenfor medfører, at $\pi_1(\underline{b}-\underline{a}) = \pi_1(\underline{b})-\pi_1(\underline{a})$, som netop repræsenteres af vektoren fra $\pi_1(A)$ til $\pi_1(B)$. Det analoge gælder for π_2. Heraf fremgår, at vi kan definere projektionen af en vektor $\underline{a}$ på P eller L, som vektoren repræsenteret ved projektionen af et liniestykke, der repræsenterer $\underline{a}$. For vilkårlige vektorer $\underline{a}$ og $\underline{b}$ og vilkårlige tal x og y har vi desuden

$$\pi_1(x\underline{a}+y\underline{b}) = x\pi_1(\underline{a})+y\pi_1(\underline{b}), \quad \pi_2(x\underline{a}+y\underline{b}) = x\pi_2(\underline{a}) + y\pi_2(\underline{b}).$$

Så skal vi i gang med analytisk geometri. En ret linie L er fastlagt ved et punkt A på L og en vektor $\underline{h} \neq \underline{0}$ på L. Hvis $\underline{a}$ er stedvektor for A er

$$\{\underline{a} + t\underline{h} \mid t \in \mathbb{R}\}$$

netop mængden af stedvektorer for punkter på linien, og hver sådan stedvektor fås for netop en værdi af t.

Ved

$$\underline{r} = \underline{f}(t) = \underline{a} + t\underline{h}$$

defineres en bijektiv afbildning $\underline{f}$ af $\mathbb{R}$ ind i mængden af stedvektorer for punkter på L. Afbildningen $\underline{f}$ kaldes en parameterfremstilling for L.

Hvis vi indfører en basis $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$ for $\mathbb{E}^3$, har vi udtryk $\underline{a} = a_1\underline{e}_1 + a_2\underline{e}_2 + a_3\underline{e}_3$ og $\underline{h} = h_1\underline{e}_1 + h_2\underline{e}_2 + h_3\underline{e}_3$, og hvis vi også skriver $\underline{r} = r_1\underline{e}_1 + r_2\underline{e}_2 + r_3\underline{e}_3$, får parameterfremstillingen formen

$$r_j = a_j + h_j t, \; j = 1,2,3.$$

I plan analytisk geometri falder $j = 3$ væk.

For den rette linie gennem to (forskellige) punkter med stedvektorer $\underline{a}$ og $\underline{b}$ vælger vi blot $\underline{h} = \underline{b}-\underline{a}$ og får parameterfremstillingen

$$r = (1-t)\underline{a} + t\underline{b}$$

og i koordinater for $\underline{b} = b_1\underline{e}_1 + b_2\underline{e}_2 + b_3\underline{e}_3$

$$r_j = (1-t)a_j + tb_j, \; j = 1,2,3.$$

For $t \in [0,1]$ får vi punkterne af liniestykket fra $\underline{a}$ til $\underline{b}$. For $t \neq 0,1$ er $\frac{t}{t-1}$ det forhold, hvori det til t svarende punkt deler liniestykket fra $\underline{a}$ til $\underline{b}$. Dette forhold er negativt for punkter på liniestykket, men positivt på dets forlængelser.

Lad os nu betragte en plan gennem et punkt med stedvektor $\underline{a} = a_1\underline{e}_1 + a_2\underline{e}_2 + a_3\underline{e}_3$ og indeholdende to lineært uafhængige vektorer $\underline{h} = h_1\underline{e}_1 + h_2\underline{e}_2 + h_3\underline{e}_3$ og $\underline{h}' = h_1'\underline{e}_1 + h_2'\underline{e}_2 + h_3'\underline{e}_3$. Mængden af stedvektorer for punkter i planen

er da

$$\{\underline{a} + t\underline{h} + t'\underline{h}' \mid t,t' \in \mathbb{R}\},$$

og vi siger derfor, at planen har parameterfremstillingen

$$\underline{r} = \underline{a} + t\underline{h} + t'\underline{h}',$$

som i koordinater får formen

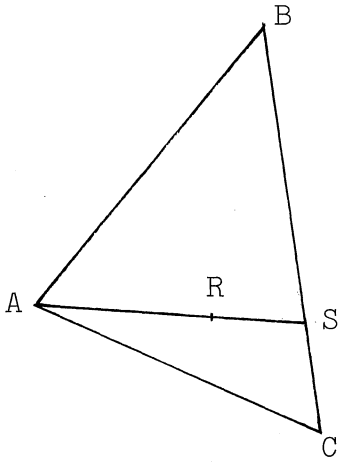
$$r_j = a_j + h_j t + h_j' t', \quad j = 1,2,3.$$

En plan gennem tre punkter med stedvektorer $\underline{a} = a_1\underline{e}_1 + a_2\underline{e}_2 + a_3\underline{e}_3$, $\underline{b} = b_1\underline{e}_1 + b_2\underline{e}_2 + b_3\underline{e}_3$ og $\underline{c} = c_1\underline{e}_1 + c_2\underline{e}_2 + c_3\underline{e}_3$, som ikke ligger på ret linie, indeholder de lineært uafhængige vektorer $\underline{b}-\underline{a}$ og $\underline{c}-\underline{a}$, så dens parameterfremstilling bliver

$$\underline{r} = (1-t-t')\underline{a} + t\underline{b} + t'\underline{c}.$$

Det lyder nok pænere at sige, at planen består af alle punkter $t\underline{a} + u\underline{b} + v\underline{c}$, hvor t, u og v er reelle tal med sum 1.

Idet vi som før betegner et punkt med et stort bogstav og dets stedvektor med det tilsvarende lille bogstav, har hvert punkt i planen gennem A,B og C stedvektor $\underline{r} = t\underline{a} + u\underline{b} + v\underline{c}$, hvor $t+u+v = 1$. Talsættet (t,u,v) kaldes de barycentriske koordinater eller trekantskoordinater

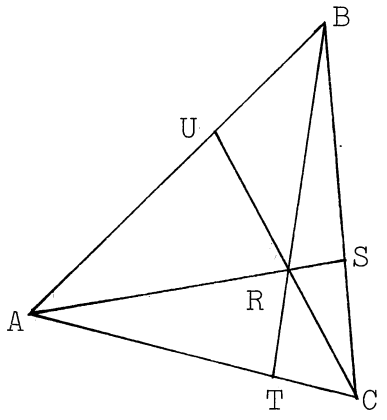


for punkter i trekantens plan. Hvis R ligger i det indre af trekanten ABC, vil linien AR skære BC i et punkt S med stedvektor $(1-v)\underline{b} + v\underline{c}$, hvor $v \in]0,1[$, og R har derfor stedvektor $(1-t)\underline{a} + t(1-v)\underline{b} + tv\underline{c}$, så R får trekantskoordinater $(1-t, t(1-v), tv)$, der alle tre er positive. Hvis det på den anden side gælder, at $t+u+v=1$ og t,u og v alle er positive, er $t\underline{a} + u\underline{b} + v\underline{c} = t\underline{a} + (1-t)\underline{s}$, hvor $\underline{s} = (1-\frac{v}{1-t})\underline{b} + \frac{v}{1-t}\underline{c}$ er et punkt af BC, så (t,u,v) er trekantskoordinater for et punkt i trekantens indre. Punktet med trekantskoordinater $(\frac{1}{3},\frac{1}{3},\frac{1}{3})$ kaldes trekantens barycenter eller tyngdepunkt (det som fysikerne kalder massemidtpunktet, hvis trekanten er en homogen plade). Da vi har

$$\tfrac{1}{3}\underline{a} + \tfrac{1}{3}\underline{b} + \tfrac{1}{3}\underline{c} = \tfrac{1}{3}\underline{a} + \tfrac{2}{3}(\tfrac{1}{2}\underline{b} + \tfrac{1}{2}\underline{c})$$

og to analoge relationer, ligger barycentret på medianerne og deler dem i forholdet 1:2.

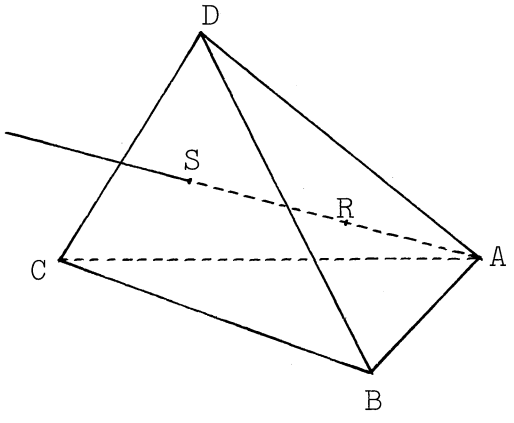
Hvis R har stedvektor $t\underline{a} + u\underline{b} + v\underline{c}$ vil S som ovenfor udregnet have stedvektor $\frac{u}{1-t}\underline{b} + \frac{v}{1-t}\underline{c}$, så S deler siden BC i forholdet $-\frac{v}{u}$. Med betegnelserne på figuren vil T dele CA i forholdet $-\frac{t}{v}$, og U vil dele AB i forholdet $-\frac{u}{t}$, så produktet af de tre delingsforhold bliver -1. Dette resultat er kendt som Cevas sætning.



Fire punkter ABCD, som ikke ligger i samme plan, er hjørner i et tetraeder. Stedvektor for et vilkårligt punkt R i rummet kan da fremstilles på formen

$$\underline{r} = \underline{a} + u(\underline{b}-\underline{a}) + v(\underline{c}-\underline{a}) + w(\underline{d}-\underline{a}) = t\underline{a} + u\underline{b} + v\underline{c} + w\underline{d},$$

hvor $t+u+v+w = 1$. Sættet (t,u,v,w) er da barycentriske koordinater for R, og hvert talsæt (t,u,v,w) med $t+u+v+w=1$ er barycentriske koordinater for netop et punkt R. Hvis R ligger i tetraedrets indre, vil AR skære trekanten BCD i et indre punkt S med $\underline{s} = u\underline{b} + v\underline{c} + w\underline{d}$, hvor u, v og w er positive med sum 1, så vi får $\underline{r} = t\underline{a} + (1-t)\underline{s}$ med $t \in]0,1[$, og vi ser, at R får alle sine barycentriske koordinater positive. Omvendt giver $\underline{r} = t\underline{a} + u\underline{b} + v\underline{c} + w\underline{d}$, hvor t,u,v og w er positive og har sum 1, at $\underline{s} = \frac{u}{1-t}\underline{b} + \frac{v}{1-t}\underline{c} + \frac{w}{1-t}\underline{d}$ er et indre punkt i trekanten BCD, og $\underline{r} = t\underline{a} + (1-t)\underline{s}$ ligger på liniestykket AS, altså i det indre af tetraedret.



Punktet M med stedvektor $\underline{m} = \frac{1}{4}\underline{a} + \frac{1}{4}\underline{b} + \frac{1}{4}\underline{c} + \frac{1}{4}\underline{d}$ kaldes barycentret for tetraedret. Af $\underline{m} = \frac{1}{4}\underline{a} + \frac{3}{4}(\frac{1}{3}\underline{b} + \frac{1}{3}\underline{c} + \frac{1}{3}\underline{d})$ og de analoge ses, at M ligger på liniestykkerne fra hjørner til medianernes skæringspunkter i den modstående sideflade og deler disse i forholdet 3:1. Disse 4 linier kaldes tetraedrets

medianer. Af $\underline{m} = \frac{1}{2}(\frac{1}{2}\underline{a} + \frac{1}{2}\underline{b}) + \frac{1}{2}(\frac{1}{2}\underline{c} + \frac{1}{2}\underline{d})$ og de analoge fås, at M er midtpunkt af hvert af de tre liniestykker, der forbinder midtpunkterne af modstående kanter i tetraedret. De 6 planer, som går gennem en kant og midtpunktet af den modstående kant, skærer hinanden i barycentret.

En nødvendig og tilstrækkelig betingelse, for at punktet X ligger i planen gennem punkt A, som indeholder de lineært uafhængige vektorer $\underline{h}$ og $\underline{k}$, er, at $\underline{x}-\underline{a}$, $\underline{h}$ og $\underline{k}$ er lineært afhængige. Med vilkårlig basis finder vi derfor, at koordinaterne til planens punkter netop udgør løsningsmængden til ligningen

$$\begin{vmatrix} x_1-a_1 & h_1 & k_1 \\ x_2-a_2 & h_2 & k_2 \\ x_3-a_3 & h_3 & k_3 \end{vmatrix} = 0.$$

Denne ligning kaldes planens ligning. Planen gennem A,B og C får ligningen

$$\begin{vmatrix} x_1-a_1 & b_1-a_1 & c_1-a_1 \\ x_2-a_2 & b_2-a_2 & c_2-a_2 \\ x_3-a_3 & b_3-a_3 & c_3-a_3 \end{vmatrix} = 0.$$

Linien gennem $\underline{A}$ indeholdende vektoren $\underline{h}$ og linien gennem B indeholdende $\underline{k}$ ligger i samme plan, hvis og kun hvis $\underline{b}-\underline{a}$, $\underline{h}$ og $\underline{k}$ er lineært afhængige, altså hvis og kun hvis

$$\begin{vmatrix} b_1-a_1 & h_1 & k_1 \\ b_2-a_2 & h_2 & k_2 \\ b_3-a_3 & h_3 & k_3 \end{vmatrix} = 0.$$

ØVELSER TIL KAPITEL 3.

Som i det foregående kapitel starter vi øvelserne med en liste, der i tilfældig rækkefølge nævner stikord til de kapitlet omtalte begreber og sætninger. Listen er ment som en hjælp ved indlæring af kapitlet, idet man under langsom gennemlæsning prøver, hvad man kan huske om hvert punkt, der er nævnt.

Linearkombination, orienteret rum, vektor, projektion, basis, determinant, ligning for plan, koordinatsæt, barycenter, lineært afhængig, elementær operation, Ceva's sætning, stedvektor, $\det_{\underline{e}_1,\underline{e}_2}(\underline{x},\underline{y})$, massemidtpunkt, skalar, ordnet basis, ombytning af søjler og af rækker i determinant, trekantskoordinater, lineært uafhængig, tyngdepunkt, addition af vektorer, delingsforhold, udviklingsformler for determinant, højrekoordinatsystem, barycentriske koordinater, parameterfremstilling for ret linie, multiplikation af vektor med tal, tetraeder, nulvektor, parameterfremstilling for plan, trilineær, orienteret plan, højrehåndsregler.

3.1. I E^3 har vi valgt et begyndelsespunkt O og basis $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$. Punkterne A,B og C har stedvektorer $\underline{a} = -\underline{e}_1+4\underline{e}_2-2\underline{e}_3$, $\underline{b} = \underline{e}_1-\underline{e}_2+5\underline{e}_3$ og $\underline{c} =$

$2\underline{e}_1 - 6\underline{e}_2 + 3\underline{e}_3$. Dette indgår i de følgende opgaver til indøvelse af regnereglerne.

3.1.1. Find $4\underline{a} - \underline{b} + 2\underline{c}$.

3.1.2. Find $\lambda\underline{a} + \underline{b}$ indeholdt i planen gennem O bestemt ved $\underline{e}_1$ og $\underline{e}_2$, idet λ er et tal.

3.1.3. Find $\mu\underline{a} + \underline{b}$ indeholdt i planen gennem O bestemt ved $\underline{c}$ og $\underline{e}_3$, idet μ er et tal.

3.1.4. Undersøg om $\underline{a}, \underline{b}$ og $\underline{c}$ er lineært uafhængige.

3.1.5. Angiv en parameterfremstilling for den rette linie gennem A med retning bestemt ved $\underline{b}$.

3.1.6. Angiv en parameterfremstilling for planen gennem A bestemt ved $\underline{b}$ og $\underline{c}$.

3.1.7. Angiv en parameterfremstilling for planen gennem A, B og C.

3.1.8. Angiv stedvektor for barycentret for trekanten ABC og for tetraedret OABC.

3.1.9. Angiv en ligning for planen gennem A, B og C.

3.2. Find et nemt bevis for, at

$$\begin{vmatrix} 0 & a & b \\ -a & 0 & c \\ -b & -c & 0 \end{vmatrix} = 0,$$

idet a,b og c er vilkårlige tal.

3.3. Udregn

$$\begin{vmatrix} a & b & b \\ b & a & b \\ b & b & a \end{vmatrix},$$

idet a og b er vilkårlige tal.

3.4. Undersøg om de rette linier med parameterfremstillingen

$$\begin{aligned} x_1 &= 13 + 3t & x_1 &= -9 - 4t \\ x_2 &= 12 + 8t & x_2 &= 8 + 3t \\ x_3 &= -1 - 6t & x_3 &= -9 - 5t \end{aligned}$$

skærer hinanden.

3.5. Find en parameterfremstilling for en ret linie, som går gennem punktet (3,1,3) og skærer de to rette linier med parameterfremstillingerne

$$\begin{aligned} x_1 &= 2 - 3t & x_1 &= -10 + 4t \\ x_2 &= 9 + 2t & x_2 &= 7 - 3t \\ x_3 &= -2 - t & x_3 &= -1 + 2t. \end{aligned}$$

3.6. Undersøg om den rette linie og planen med parameterfremstillingerne

$$\begin{aligned} x_1 &= -3 + 5t & x_1 &= -4 + 3t - 4u \\ x_2 &= 7 - 6t & x_2 &= -6 - 5t + u \\ x_3 &= -4 + 3t & x_3 &= 2t - u \end{aligned}$$

skærer hinanden og find i bekræftende fald skæringspunktets koordinater.

3.7. Lad L og M være rette linier i E^3. Er det rigtigt, at midtpunkterne af alle liniestykker med det ene endepunkt på L og det andet på M ligger i en plan.

3.8. Find en parameterfremstilling for en ret linie, som går gennem punktet med koordinater $(-3,6,10)$, skærer en ret linie L og er parallel med en plan P, idet L og P har parameterfremstillingerne

$$\begin{aligned} x_1 &= 3 - 2t & x_1 &= t - u \\ x_2 &= -7 + 9t & x_2 &= 5t - 4u \\ x_3 &= -1 - t & x_3 &= 9t - 7u \end{aligned}$$

3.9. Lad $\underline{a}$, $\underline{b}$, $\underline{c}$ være stedvektorer for vinkelspidserne A,B og C i en trekant, der ikke er udartet (dvs. A,B og C ligger ikke på ret linie). Vis, at der for enhver ret linie L i trekantens plan findes tre reelle tal p,q,r, så L netop omfatter de

punkter, hvis trekantskoordinater (x,y,z) tilfredsstiller ligningen $px+qy+rz = 0$. Vis også, at det for enhver sådan ligning, hvor p,q og r ikke alle er 0, gælder at løsningsmængden netop er mængden af punkter på en ret linie L. Vi siger så, at $px+qy+rz = 0$ er en ligning for L i (de ved trekant ABC fastlagte) trekantskoordinater. Vis, at $p_1x+q_1y+r_1z = 0$ og $p_2x+q_2y+r_2z = 0$ fremstiller samme rette linie, hvis og kun hvis vektorerne i $\mathbb{E}^3$ med koordinatsættene (p_1,q_1,r_1) og (p_2,q_2,r_2) er lineært afhængige.

Angiv ligningerne i trekantskoordinater for trekantens sider, midtpunktstransversaler (dvs. linier gennem midtpunkterne af to sider), samt medianerne.

Vis at tre punkter, af hvilke der ligger et på hver trekantsside eller forlængelsen af en sådan, men som ikke falder i vinkelspidserne, ligger på ret linie, hvis og kun hvis de forhold, hvori de deler siderne har produkt +1. Det forhold hvori punkt P på linien gennem A og B deler liniestykket AB, defineres som brøken $\frac{PA}{PB}$, hvor liniestykkerne regnes med fortegn. I påstanden ovenfor skal siderne i denne sammenhæng tages i kredsforskydningsorden, altså BC, CA, AB. Påstanden kaldes Menelaos' sætning.

KAPITEL 4

Produkter af vektorer.

Regning med vektorer har mange anvendelser i matematik og fysik. Når stof er i bevægelse har hvert massepunkt en hastighed, der hensigtsmæssigt angives ved en vektor. På den måde får vi en hastighedsvektor i hvert punkt af E^3 eller i hvert punkt af en del af E^3. Vi kan tænke på et vektorfelt som en afbildning $f:A \to \mathbb{E}^3$, hvor $A \subseteq E^3$ er en punktmængde.

Kræfter angives ligeledes ved vektorer. I teorien for et stift legemes dynamik tænkes et eller flere stive legemer angrebet af et system af kræfter. Hver kraft angives ved en vektor, som ligger i en linie, og virker i et punkt, angrebspunktet, som tilhører fællesmængden for det stive legeme og virkelinien, men det gør ingen forskel, om angrebspunktet flyttes til et andet punkt af denne virkelinie. I denne sammenhæng taler man om liniebundne vektorer.

Man taler også om kraftfelter, men det er egentlig noget helt andet. Stoffet har en virkning på hele rummet - også dele af rummet, hvor der ikke er stof, således at en stofparti-

kel, der anbringes i et punkt af rummet påvirkes af en kraft. En sådan feltkraft er i reglen proportional med partiklens masse, elektriske ladning eller lignende, og man angiver feltet i punktet ved feltstyrken, som er kraften pr. enhedsmasse, enhedsladning, eller hvad der nu er relevant i den foreliggende situation.

Når man vælger et koordinatsystem i E^3, kan vektorer angives ved koordinater, som er talstørrelser, der er basisafhængige, og derfor kan de ikke i sig selv have en fysisk betydning. Ved siden af sådanne basisafhængige talstørrelser optræder der invariante (dvs. basisuafhængige) talstørrelser, der angiver fysiske egenskaber som massefylde, temperatur, tryk, koncentration, energitæthed etc. Sådanne talstørrelser kaldes skalarer.

Hvis $\underline{a}$ er en vektor, har liniestykker, der repræsenterer $\underline{a}$ alle samme længde $\|\underline{a}\|$, længden af vektoren $\underline{a}$. Den er en skalar. To vektorer $\underline{a}$ og $\underline{b}$ danner en vinkel, som har en veldefineret værdi $\angle(\underline{a},\underline{b})$ i intervallet $[0,\pi]$, og denne værdi er også en skalar. Størrelsen

$$\|\underline{a}\| \, \|\underline{b}\| \cos\angle(\underline{a},\underline{b})$$

er en skalar. Den kaldes skalarproduktet af $\underline{a}$ og $\underline{b}$ og betegnes $\underline{a}\cdot\underline{b}$, hvor prikken ikke må udelades. Ud over denne betegnelse møder man i litteraturen $(\underline{a},\underline{b})$ og $\langle\underline{a},\underline{b}\rangle$. Vi skriver $\underline{a}^2$ for $\underline{a}\cdot\underline{a}$, og vi har åbenbart

$$\underline{a}^2 = \|\underline{a}\|^2 .$$

Det fremgår af definitionen, at

$$\underline{a}\cdot\underline{b} = \underline{b}\cdot\underline{a}.$$

For $x \in \mathbb{R}$ har vi desuden

$$x(\underline{a}\cdot\underline{b}) = (x\underline{a})\cdot\underline{b} = \underline{a}\cdot x\underline{b}.$$

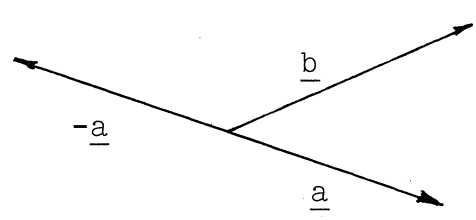
For $x \geqq 0$ følger dette af den for alle x gyldige trivielle relation

$$\|x\underline{a}\| = |x|\,\|\underline{a}\|,$$

og at det også gælder for $x < 0$ følger af relationen

$$\angle(\underline{a},\underline{b}) + \angle(-\underline{a},\underline{b}) = \pi.$$

Hvis L er en ret linie, som $\underline{a}$ ligger på, og $p: E^3 \to L$ er retvinklet projektion, er $\|\underline{b}\|\cos\angle(\underline{a},\underline{b})$ længden af $p(\underline{b})$ regnet med fortegn i overensstemmelse med retningen af $\underline{a}$. Derfor er



$$\underline{a}\cdot\underline{b} = \|\underline{a}\|\,p(\underline{b}).$$

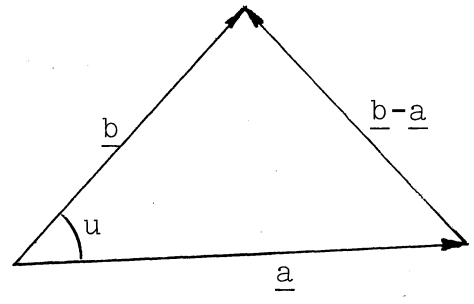
For vilkårlige vektorer $\underline{b}'$ og $\underline{b}''$ har vi ifølge et resultat fra det foregående kapitel, at $p(\underline{b}'+\underline{b}'') = p(\underline{b}') + p(\underline{b}'')$, og formlen ovenfor giver derfor

$$\underline{a}\cdot(\underline{b}' + \underline{b}'') = \underline{a}\cdot\underline{b}' + \underline{a}\cdot\underline{b}''.$$

Da $\underline{a}\cdot\underline{b} = \underline{b}\cdot\underline{a}$, kan vi lade de to faktorer bytte rolle, og vi har derfor også

$$(\underline{a}' + \underline{a}'')\cdot\underline{b} = \underline{a}'\cdot\underline{b} + \underline{a}''\cdot\underline{b}.$$

Specielt får vi med figurens betegnelser



$$\|\underline{b}-\underline{a}\|^2 = (\underline{b}-\underline{a})\cdot(\underline{b}-\underline{a}) =$$

$$\underline{b}\cdot\underline{b} - \underline{a}\cdot\underline{b} - \underline{b}\cdot\underline{a} + \underline{a}\cdot\underline{a} =$$

$$\underline{a}^2 + \underline{b}^2 - 2\underline{a}\cdot\underline{b} = \|\underline{a}\|^2 + \|\underline{b}\|^2 - 2\|\underline{a}\|\,\|\underline{b}\|\cos u.$$

Dette er cosinusrelationen for en trekant. Den kaldes også den udvidede pytagoræiske sætning, fordi specialtilfældet $u = \frac{\pi}{2}$ netop er den pytagoræiske sætning.

Hvis $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$ er en basis for $\mathbb{E}^3$, og vi har $\underline{a} = a_1\underline{e}_1 + a_2\underline{e}_2 + a_3\underline{e}_3$ og $\underline{b} = b_1\underline{e}_1 + b_2\underline{e}_2 + b_3\underline{e}_3$, får vi

$$\underline{a}\cdot\underline{b} = a_1b_1\underline{e}_1^2 + a_2b_2\underline{e}_2^2 + a_3b_3\underline{e}_3^2 +$$

$$(a_2b_3+a_3b_2)\underline{e}_2\cdot\underline{e}_3 + (a_3b_1+a_1b_3)\underline{e}_3\cdot\underline{e}_1 + (a_1b_2+a_2b_1)\underline{e}_1\cdot\underline{e}_2 .$$

Nu er det hensigtsmæssigt at lade $\underline{e}_1$, $\underline{e}_2$ og $\underline{e}_3$ være vektorer med længde 1 og to og to vinkelrette på hinanden. Så kaldes $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$ en ortonormal (sprogligt misfoster, opstået ved krydsning af "ortogonal" og "normeret") basis. For en

sådan er

$$\underline{e}_j \cdot \underline{e}_k = \begin{cases} 1, & \text{hvis } j = k \\ 0, & \text{hvis } j \neq k. \end{cases}$$

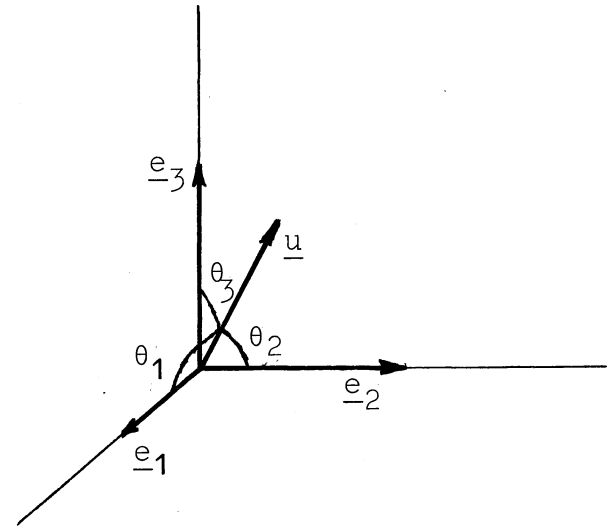
Dette skrives kort $\underline{e}_j \cdot \underline{e}_k = \delta_{jk}$, hvor δ_{jk}, som kaldes Kroneckers symbol, betyder 1, hvis $j = k$, men 0, hvis $j \neq k$. Hvis $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$ er en ortonormal basis, gælder den enkle formel

$$\underline{a} \cdot \underline{b} = a_1 b_1 + a_2 b_2 + a_3 b_3 .$$

Lad nu $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$ være en ortonormal basis, og lad $\underline{u} = u_1\underline{e}_1 + u_2\underline{e}_2 + u_3\underline{e}_3$ og $\underline{v} = v_1\underline{e}_1 + v_2\underline{e}_2 + v_3\underline{e}_3$ være enhedsvektorer, dvs. vektorer med længde 1.

Så er $u_1 = \cos\theta_1$, $u_2 = \cos\theta_2$, $u_3 = \cos\theta_3$ cosinusserne af de vinkler, $\underline{u}$ danner med koordinatakserne, og disse vinkler tilfredsstiller derfor relationen

$$\cos^2\theta_1 + \cos^2\theta_2 + \cos^2\theta_3 = 1.$$



Idet vi analogt har $v = \cos\phi_1$, $v_2 = \cos\phi_2$, $v_3 = \cos\phi_3$, hvor ϕ_1, ϕ_2 og ϕ_3 er de vinkler, $\underline{v}$ danner med koordinatakserne, bliver vinklen β mellem $\underline{u}$ og $\underline{v}$ bestemt ved

$$\cos\beta = \underline{u}\cdot\underline{v} = \cos\theta_1 \cos\phi_1 + \cos\theta_2 \cos\phi_2 + \cos\theta_3 \cos\phi_3.$$

Dette er det 3-dimensionale sidestykke til formlen for cosinus til en differens.

En reel 3×3-matrix er et skema af 9 reelle tal

$$\begin{pmatrix} u_{11} & u_{12} & u_{13} \\ u_{21} & u_{22} & u_{23} \\ u_{31} & u_{32} & u_{33} \end{pmatrix}.$$

Med en sådan matrix kan vi definere

(1) $$\underline{e}_j' = u_{1j}\underline{e}_1 + u_{2j}\underline{e}_2 + u_{3j}\underline{e}_3, \quad j = 1,2,3.$$

og vi ser, at $(\underline{e}_1', \underline{e}_2', \underline{e}_3')$ er en ny ortonormal basis, hvis og kun hvis

(2) $$u_{1j}u_{1k} + u_{2j}u_{2k} + u_{3j}u_{3k} = \delta_{jk}, \quad j,k = 1,2,3,$$

og i så fald er u_{ij} netop cosinus til vinklen mellem $\underline{e}_i$ og $\underline{e}_j'$ for $i,j = 1,2,3$. Men så kan vi slutte, at

(3) $$\underline{e}_i = u_{i1}\underline{e}_1' + u_{i2}\underline{e}_2' + u_{i3}\underline{e}_3', \quad i = 1,2,3,$$

og deraf kan vi slutte, at relationerne (2) mellem matricens søjler medfører de analoge relationer

$$u_{i1}u_{j1} + u_{i2}u_{j2} + u_{i3}u_{j3} = \delta_{ij}$$

mellem matricens rækker.

En vektor $\underline{x}$ får to fremstillinger

$$\underline{x} = x_1\underline{e}_1 + x_2\underline{e}_2 + x_3\underline{e}_3 = x_1'\underline{e}_1' + x_2'\underline{e}_2' + x_3'\underline{e}_3',$$

og hvis vi udregner det sidste udtryk ved hjælp af (1), opdager vi, at

$$x_i = u_{i1}x_1' + u_{i2}x_2' + u_{i3}x_3' \ , \quad i = 1,2,3,$$

og analogt får vi ved hjælp af (3)

$$x_j' = u_{1j}x_1 + u_{2j}x_2 + u_{3j}x_3, \quad j = 1,2,3.$$

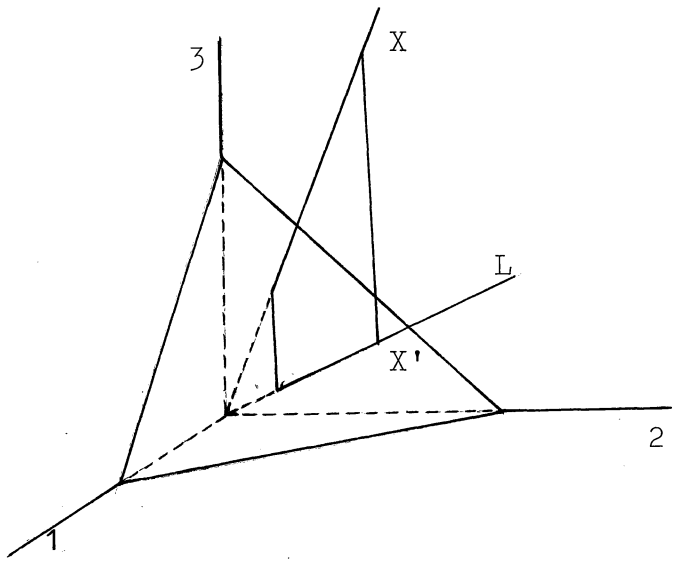
Vi betragter en fast ortonormal basis $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$, samt en vektor $\underline{a} \neq \underline{0}$, som ligger på en linie L gennem O. Lad X være et punkt med stedvektor $\underline{x}$. Idet $\frac{\underline{a}}{\|\underline{a}\|}$ er en enhedsvektor på L, er afstanden fra O til den retvinklede projektion Y af X på L da givet ved

$$\frac{\underline{a}\cdot\underline{x}}{\|\underline{a}\|} = \frac{a_1x_1+a_2x_2+a_3x_3}{\sqrt{a_1^2+a_2^2+a_3^2}},$$

idet den regnes med fortegn i overensstemmelse med den orientering $\underline{a}$ fastlægger på L. Stedvektor for Y er

$$\underline{y} = \frac{(\underline{a}\cdot\underline{x})\underline{a}}{\underline{a}^2} = \frac{a_1x_1+a_2x_2+a_3x_3}{a_1^2+a_2^2+a_3^2}(a_1\underline{e}_1+a_2\underline{e}_2+a_3\underline{e}_3).$$

En plan kan tænkes fastlagt ved, at den er vinkelret på en given enhedsvektor $\underline{u}$, og at den skærer den ved $\underline{u}$ bestemte linie gennem O i den med fortegn regnede afstand p fra O. Lad X være et punkt med stedvektor $\underline{x}$. Da er



den retvinklede projektion X' af X på den orienterede linie L gennem O med retningen $\underline{u}$ bestemt ved, at OX' regnet med fortegn er $\underline{u}\cdot\underline{x}$, så den med fortegn regnede afstand fra planen til X bliver

$$\underline{u}\cdot\underline{x} - p = u_1x_1 + u_2x_2 + u_3x_3 - p.$$

Ligningen

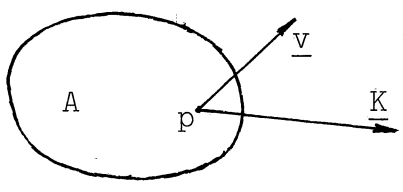
$$u_1x_1 + u_2x_2 + u_3x_3 - p = 0$$

er planens ligning på normalform. Enhver ligning

$$a_1x_1 + a_2x_2 + a_3x_3 - b = 0,$$

hvor koefficienterne a_1,a_2,a_3 ikke alle er 0, er ligning for en plan. En sådan ligning har netop to normalformer, der fås af hinanden ved fortegnsskift. De fås ved at dividere ligningen igennem med $\pm\sqrt{a_1^2+a_2^2+a_3^2}$.

Det fremgår umiddelbart af definitionen, at skalarproduktet er uafhængigt af valg af basis. Det kan derfor også i adskillige situationer tillægges en fysisk betydning. Bedst kendt er den følgende: Hvis en kraft $\underline{K}$ angriber i et punkt P af et stift legeme, og P har hastigheden $\underline{v}$, da er $\underline{K}\cdot\underline{v}$ ef-



fekten af kraften $\underline{K}$, og det er den energitilførsel pr. tidsenhed, legemet A modtager fra kraften K, og tillige det af $\underline{K}$ udførte arbejde pr. tidsenhed.

Det volder ikke vanskeligheder at specialisere teorien for skalarproduktet til $\mathbb{E}^2$, og det vil vi ikke opholde os ved. Hvis vi har indført en orientering i $\mathbb{E}^2$, kan vi definere en afbildning $\tau:\mathbb{E}^2 \to \mathbb{E}^2$ ved at $\tau\underline{x}$ for hver $\underline{x} \in \mathbb{E}^2$ skal have samme længde som $\underline{x}$, medens vinklen fra $\underline{x}$ til $\tau\underline{x}$ skal være $\frac{\pi}{2}$. Vi skriver $\tau^2\underline{x}$ for $\tau\tau\underline{x}$, og for $\underline{x},\underline{y} \in \mathbb{E}^2$, $\lambda \in \mathbb{R}$ har vi så regnereglerne

$$\tau(\underline{x}+\underline{y}) = \tau\underline{x} + \tau\underline{y},\ \tau(\lambda\underline{x}) = \lambda\tau\underline{x},\ \tau^2\underline{x} = -\underline{x}\ .$$

Endvidere er $\underline{x}\cdot\tau\underline{x} = 0$, og for $\underline{x} \neq \underline{0}$ er $\underline{x}$ og $\tau\underline{x}$ lineært uafhængige. Hvis $\underline{e}_1$ er en enhedsvektor og $\underline{e}_2 = \tau\underline{e}_1$, er $(\underline{e}_1,\underline{e}_2)$ en positivt orienteret basis, og vi har

$$\tau(x_1\underline{e}_1 + x_2\underline{e}_2) = -x_2\underline{e}_1 + x_1\underline{e}_2.$$

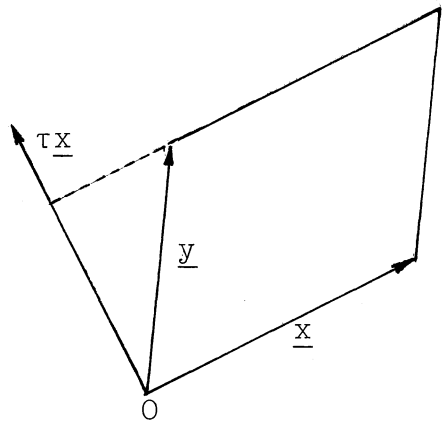
Vi definerer planproduktet af $\underline{x},\underline{y} \in \mathbb{E}^2$ ved

$$[\underline{x},\underline{y}] = \tau\underline{x}\cdot\underline{y},$$

og vi får umiddelbart regnereglerne

$[\underline{x}'+\underline{x}'',\underline{y}] = [\underline{x}',\underline{y}] + [\underline{x}'',\underline{y}]$; $[\underline{x},\underline{y}'+\underline{y}''] = [\underline{x},\underline{y}'] + [\underline{x},\underline{y}'']$,
$[\lambda\underline{x},\underline{y}] = [\underline{x},\lambda\underline{y}] = \lambda[\underline{x},\underline{y}]$; $[\underline{x},\underline{y}] = -[\underline{y},\underline{x}]$.

Det ses også umiddelbart, at $[\underline{x},\underline{y}] = 0$ er ensbetydende med, at $\underline{x}$ og $\underline{y}$ er lineært afhængige.



Når vi udnytter definitionen af skalarproduktet, ser vi let af figuren, at $[\underline{x},\underline{y}]$ er arealet af det af $\underline{x}$ og $\underline{y}$ udspændte parallelogram regnet med fortegn, således at det er positivt, hvis $(\underline{x},\underline{y})$ er positivt orienteret.

Hvis $(\underline{e}_1,\underline{e}_2)$ er en positivt orienteret ortonormal basis, får vi

$$[\underline{x},\underline{y}] = [x_1\underline{e}_1+x_2\underline{e}_2, y_1\underline{e}_1+y_2\underline{e}_2] = x_1y_2 - x_2y_1 = \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}.$$

Planproduktet svarer til to forskellige produkter i $\mathbb{E}^3$. Vi vil først omtale vektorproduktet. For $\underline{x},\underline{y} \in \mathbb{E}^3$ er vektorproduktet $\underline{x}\times\underline{y}$ en vektor med længde

$$\|\underline{x}\times\underline{y}\| = \|\underline{x}\|\,\|\underline{y}\| \sin\angle(\underline{x},\underline{y}),$$

og med retning vinkelret på både $\underline{x}$ og $\underline{y}$, således at $(\underline{x},\underline{y}, \underline{x}\times\underline{y})$ er et højresystem eller lineært afhængigt.

Som vi har formuleret det, er det ikke helt oplagt, at definitionen virkelig fastlægger vektorproduktet. Det fremgår imidlertid af udtrykket for $\|\underline{x}\times\underline{y}\|$, at $\underline{x}\times\underline{y}=\underline{0}$, hvis $\underline{x}$ og $\underline{y}$ er lineært afhængige. Hvis $\underline{x}$ og $\underline{y}$ er li-

neært uafhængige, fastlægger $\underline{x}$ og $\underline{y}$ en plan gennem O, samt en orientering i denne plan, og så er retningen af $\underline{x}\times\underline{y}$ fastlagt ved definitionen, og samtidig ser vi, at $\underline{x}\times\underline{y} \neq \underline{0}$. Dermed har vi også vist følgende sætning.

Vektorerne $\underline{x}$ og $\underline{y}$ er lineært afhængige, hvis og kun hvis $\underline{x}\times\underline{y} = \underline{0}$.

Af definitionen får vi også umiddelbart regnereglen

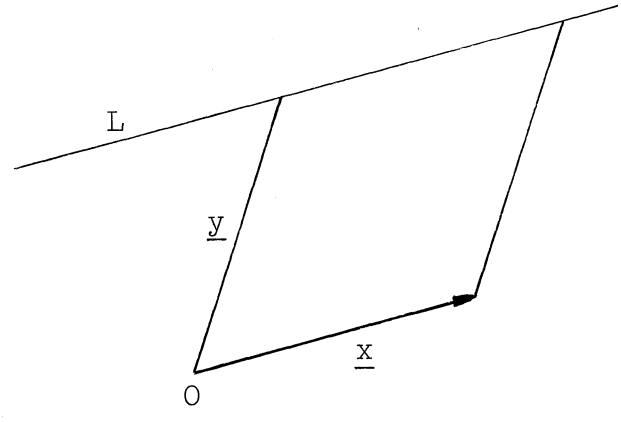
$$\underline{y}\times\underline{x} = -\underline{x}\times\underline{y}.$$

For $\lambda \in \mathbb{R}$ har vi desuden

$$\lambda\underline{x}\times\underline{y} = \underline{x}\times\lambda\underline{y} = \lambda(\underline{x}\times\underline{y}).$$

Dette er klart for $\lambda \geq 0$, og resten følger af, at vektorpunktet åbenbart blot skifter fortegn, hvis den ene faktor gør det.

Hvis vi som vist på figuren har en vektor $\underline{x}$ og en ret linie L parallel med $\underline{x}$, vil $\underline{x}\times\underline{y}$, hvor $\underline{y}$ er stedvektor for et vilkårligt punkt på L, have arealet af det indtegnede parallelogram som længde, og retningen af $\underline{x}\times\underline{y}$ vil blive den samme for alle sådanne $\underline{y}$. Heraf følger regnereglen



$$\underline{x}\times(\underline{y}+\lambda\underline{x}) = \underline{x}\times\underline{y}.$$

Vi har selvfølgelig også den analoge

$$(\underline{x}+\lambda\underline{y})\times\underline{y} = \underline{x}\times\underline{y}.$$

Nu vil vi vise de distributive love

$$\underline{a}\times(\underline{x}+\underline{y}) = \underline{a}\times\underline{x} + \underline{a}\times\underline{y}, \quad (\underline{x}+\underline{y})\times\underline{a} = \underline{x}\times\underline{a} + \underline{y}\times\underline{a}.$$

Den sidste går over i den første ved et fortegnsskift. Derfor er det nok at vise den første. Vi viser den først i det specielle tilfælde, hvor $\underline{a} = \underline{e}$ er en enhedsvektor vinkelret på en plan P, der indeholder $\underline{x}$ og $\underline{y}$. Hvis vi indfører en orientering i P, kan vi tale om $\tau\underline{x}$ og $\tau\underline{y}$ som vektorer i P, og vi kan vælge orienteringen, således at $\underline{e}\times\underline{z} = \tau\underline{z}$ for enhver vektor $\underline{z}$ i P. Så får vi

$$\underline{e}\times(\underline{x}+\underline{y}) = \tau(\underline{x}+\underline{y}) = \tau\underline{x} + \tau\underline{y} = \underline{e}\times\underline{x} + \underline{e}\times\underline{y},$$

så sætningen gælder i dette specielle tilfælde. Dernæst får vi for $\lambda \in \mathbb{R}$

$$\lambda\underline{e}\times(\underline{x}+\underline{y}) = \lambda(\underline{e}\times(\underline{x}+\underline{y})) = \lambda(\underline{e}\times\underline{x} + \underline{e}\times\underline{y}) =$$
$$\lambda(\underline{e}\times\underline{x}) + \lambda(\underline{e}\times\underline{y}) = \lambda\underline{e}\times\underline{x} + \lambda\underline{e}\times\underline{y}.$$

Dermed er den distributive lov vist i det specielle tilfælde, hvor $\underline{a}$ er vinkelret på $\underline{x}$ og $\underline{y}$. Hvis $\underline{a}$ ikke er vinkelret på $\underline{x}$ og $\underline{y}$, er $\underline{a} \neq \underline{0}$, og så kan vi vælge $\lambda, \mu \in \mathbb{R}$, så $\underline{x} + \lambda\underline{a}$ og $\underline{y} + \mu\underline{a}$ er vinkelrette på $\underline{a}$. Men så giver det allerede viste tilfælde af den distributive lov, at

$$\underline{a}\times(\underline{x}+\underline{y}+(\lambda+\mu)\underline{a}) = \underline{a}\times(\underline{x}+\lambda\underline{a}) + \underline{a}\times(\underline{y}+\mu\underline{a}),$$

og ifølge reglerne ovenfor er

$$a\times(\underline{x}+\underline{y}+(\lambda+\mu)\underline{a}) = \underline{a}\times(\underline{x}+\underline{y})$$

og

$$\underline{a}\times(\underline{x}+\lambda\underline{a}) = \underline{a}\times\underline{x}, \quad \underline{a}\times(\underline{y}+\mu\underline{a}) = \underline{a}\times\underline{y}.$$

Dermed er den distributive lov bevist.

Nu får vi umiddelbart for vilkårligt valg af basis $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$, at

$$\underline{x}\times\underline{y} = (x_1\underline{e}_1+x_2\underline{e}_2+x_3\underline{e}_3)\times(y_1\underline{e}_1+y_2\underline{e}_2+y_3\underline{e}_3) =$$

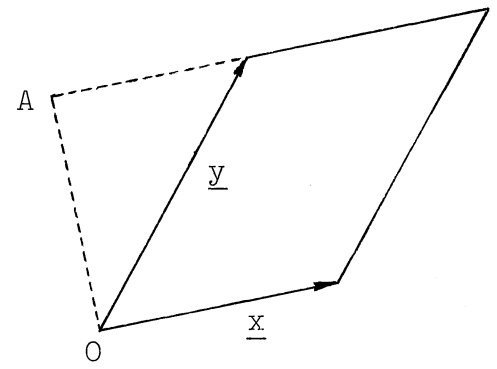
$$(x_2y_3-x_3y_2)(\underline{e}_2\times\underline{e}_3)+(x_3y_1-x_1y_3)(\underline{e}_3\times\underline{e}_1)+(x_1y_2-x_2y_1)(\underline{e}_1\times\underline{e}_2) =$$

$$\begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix}(\underline{e}_2\times\underline{e}_3) + \begin{vmatrix} x_3 & y_3 \\ x_1 & y_1 \end{vmatrix}(\underline{e}_3\times\underline{e}_1) + \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}(\underline{e}_1\times\underline{e}_2).$$

Hvis $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$ er ortonormal og et højresystem, er $\underline{e}_2\times\underline{e}_3 = \underline{e}_1$, $\underline{e}_3\times\underline{e}_1 = \underline{e}_2$ og $\underline{e}_1\times\underline{e}_2 = \underline{e}_3$, så vi får den simple formel

$$\underline{x}\times\underline{y} = \begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix}\underline{e}_1 + \begin{vmatrix} x_3 & y_3 \\ x_1 & y_1 \end{vmatrix}\underline{e}_2 + \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}\underline{e}_3.$$

Da afstanden OA på figuren netop er $\|\underline{y}\| \sin\angle(\underline{x},\underline{y})$, er $\|\underline{x}\times\underline{y}\| = \|\underline{x}\|\,\|\underline{y}\| \sin\angle(\underline{x},\underline{y})$ netop arealet af det af $\underline{x}$ og $\underline{y}$ udspændte parallelogram, og vektorproduktet kan derfor fortolkes som dette areal angivet ved størrelse og retning. Ved anvendelse af et ortonormalt højresystem får vi derfor, at parallelogrammets areal er



$$\|\underline{x}\times\underline{y}\| = \sqrt{\begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix}^2 + \begin{vmatrix} x_3 & y_3 \\ x_1 & y_1 \end{vmatrix}^2 + \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}^2}\,.$$

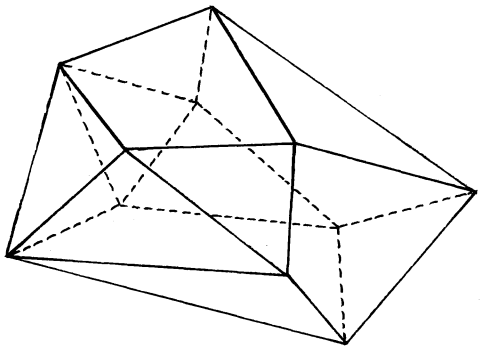
Kvotienten

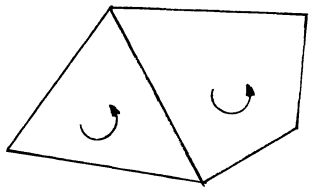
$$\frac{\begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix}}{\sqrt{\begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix}^2 + \begin{vmatrix} x_3 & y_3 \\ x_1 & y_1 \end{vmatrix}^2 + \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix}^2}},$$

og de to analoge er cosinusserne af vinklerne mellem $\underline{x}\times\underline{y}$ og koordinatakserne, og derfor også af vinklerne mellem parallelogrammets plan og koordinatplanerne.

Nu gælder det selvfølgelig også for en trekant, at dens areal er kvadratroden af kvadratsummen af projektionerne på koordinatplanerne i et ortonormalt koordinatsystem, og at arealet af dens projektion på en plan fås ved multiplikation

med cosinus til vinklen mellem denne plan og trekantens plan. Dernæst gælder de samme påstande for vilkårlige polygoner, idet de deles i trekanter. Figuren viser et polyeder projiceret på papirets plan. Vi orienterer sidefladerne, så de "anskueligt" er orienteret samme vej "set udefra". Det svarer til, at orienteringen i sammenstødende sideflader "løber modsat" på den fælles kant som vist på den næste figur. Så fremgår det af den øverste figur, at de projicerede arealer regnet med fortegn i overensstemmelse med orienteringen netop giver 0, og det medfører, at sidefladernes arealer regnet vektorielt har summen af projektionerne på papirets normal lig med $\underline{0}$. Det samme gælder ved projektion på alle andre retninger, så arealerne af sidefladerne regnet som vektorer har summen $\underline{0}$.





Højden fra A i trekanten ABC har længden

$$\frac{\|(\underline{c}-\underline{b})\times(\underline{a}-\underline{b})\|}{\|\underline{c}-\underline{b}\|} = \frac{\|(\underline{c}-\underline{b})\times(\underline{a}-\underline{c})\|}{\|\underline{c}-\underline{b}\|}\,.$$

Skæringslinien mellem planerne med ligningerne

$$a_1x_1 + a_2x_2 + a_3x_3 = p$$

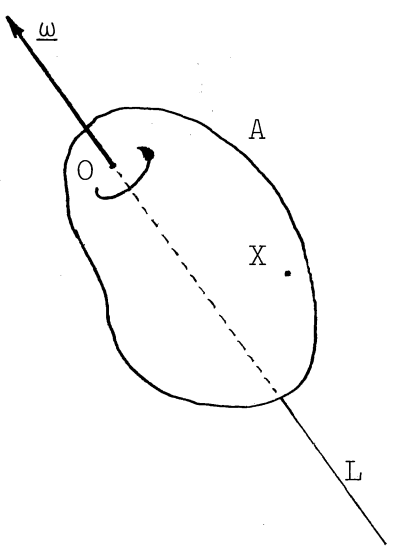
$$b_1x_1 + b_2x_2 + b_3x_3 = q$$

har retning som vektoren $\underline{a}\times\underline{b}$, altså som

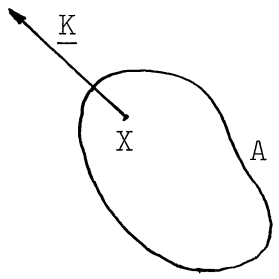
$$\begin{vmatrix} a_2 & b_2 \\ a_3 & b_3 \end{vmatrix}\underline{e}_1 + \begin{vmatrix} a_3 & b_3 \\ a_1 & b_1 \end{vmatrix}\underline{e}_2 + \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}\underline{e}_3,$$

når $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$ er en ortonormal basis.

$\overset{v}{\underset{v}{\int_v}}$ Et stift legeme A roterer om en akse L med en vinkelhastighed ω. Vi angiver dette ved en vektor $\underline{\omega}$ med $\|\underline{\omega}\| = \omega$ på drejningsaksen og orienteret positivt i forhold til omdrejningsretningen. Lad den angribe i et punkt O af L. Vi tager O som begyndelspunktet. Et punkt X af legemet får da hastigheden $\underline{\omega}\times\underline{x}$. Det stemmer med, at $\underline{\omega}\times\underline{x}$ ikke kommer til at afhænge af, hvor O vælges på L.



Det stive legeme A påvistes af en kraft $\underline{K}$, der angriber i et punkt X. Ved momentet af $\underline{K}$ i et punkt O, der vælges som begyndelsespunkt, forstår



vi vektoren $\underline{x}\times\underline{K}$. Derved får $\underline{K}$ et moment i ethvert punkt af rummet, altså et momentfelt. Momentfeltet for en kraft har helt samme udseende som hastighedsfeltet ved en drejning om en akse.

En ret linie L i E^3 med begyndelsespunkt O kan fastlægges ved en enhedsvektor $\underline{u}$ på L samt momentet $\underline{m}$ af $\underline{u}$ i punktet O, idet dette moment er uafhængigt af valget af angrebspunktet for $\underline{u}$. Derved får vi L fastlagt ved et talsæt $(u_1,u_2,u_3;\ m_1,m_2,m_3)$, som tilfredsstiller betingelserne

$$u_1^2 + u_2^2 + u_3^2 = 1, \quad u_1m_1 + u_2m_2 + u_3m_3 = 0.$$

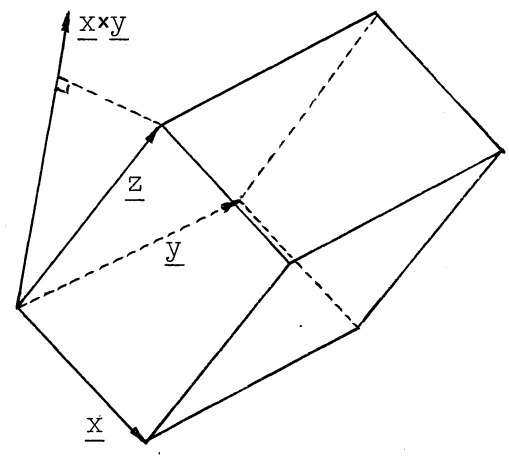
Derved får vi mulighed for at opbygge en analytisk geometri med de rette linier som de fundamentale elementer. Denne såkaldte "Plücker'ske" liniegeometri dyrkedes en hel del i begyndelsen af dette århundrede.

Ved rumproduktet af tre vektorer $\underline{x},\underline{y}$ og $\underline{z}$ forstås udtrykket

$$[\underline{x},\underline{y},\underline{z}] = \underline{x}\times\underline{y}\cdot\underline{z}\ .$$

Det er unødvendigt at sætte parentes i det sidste udtryk, da kun fortolkningen $(\underline{x}\times\underline{y})\cdot\underline{z}$ giver mening. Vi ved, at $\underline{x}\times\underline{y}$ er en vektor, hvis længde er lig med arealet af det af $\underline{x}$ og $\underline{y}$

udspændte parallelogram, og at $\underline{x}\times\underline{y}$ er vinkelret på $\underline{x}$ og $\underline{y}$, samt at $(\underline{x},\underline{y},\underline{x}\times\underline{y})$ er et højresystem. Så er $\underline{x}\times\underline{y}\cdot\underline{z}$ arealet af det af $\underline{x}$ og $\underline{y}$ udspændte parallelogram gange længden af projektionen af $\underline{z}$ på $\underline{x}\times\underline{y}$, og det er rumfanget af det af $\underline{x},\underline{y}$ og $\underline{z}$ udspændte parallelepipedum regnet positivt, hvis $(\underline{x},\underline{y},\underline{z})$ er et højresystem, og negativt, hvis $(\underline{x},\underline{y},\underline{z})$ er et venstresystem.



Hvis vi benytter et ortonormalt højresystem $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$, får vi direkte ved udregning

$$\underline{x}\times\underline{y}\cdot\underline{z} = \begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix} z_1 + \begin{vmatrix} x_3 & y_3 \\ x_1 & y_1 \end{vmatrix} z_2 + \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} z_3 = \begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix} ,$$

og det er netop det udtryk, vi tidligere har betegnet $\det_{\underline{e}_1\underline{e}_2\underline{e}_3}(\underline{x},\underline{y},\underline{z})$. Vi behøver derfor ikke at diskutere dets egenskaber igen, men vi vil dog bemærke, at $\times$ og $\cdot$ kan byttes, da vi får

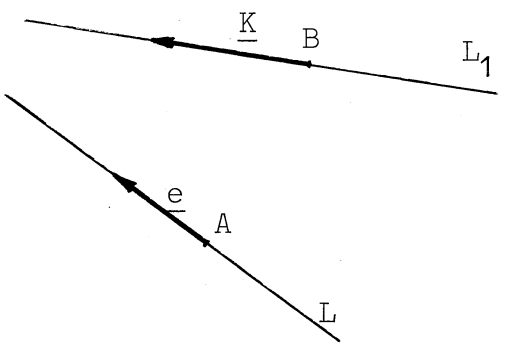
$$\underline{x}\times\underline{y}\cdot\underline{z} = \underline{y}\times\underline{z}\cdot\underline{x} = \underline{x}\cdot\underline{y}\times\underline{z} .$$

Hvis to rette linier er fastlagt ved, at den ene går gennem A og indeholder vektoren $\underline{u} \neq \underline{0}$, medens den anden går gennem B og indeholder vektoren $\underline{v} \neq \underline{0}$, og $\underline{u}$ og $\underline{v}$ er lineært uafhængige, vil det af $\underline{u},\underline{v}$ og $\underline{b}-\underline{a}$ udspændte pa-

rallelepipedum som højde på den af $\underline{u}$ og $\underline{v}$ udspændte side netop have den korteste afstand mellem de to linier, og denne korteste afstand er derfor bortset fra fortegnet givet ved

$$\frac{\underline{u}\times\underline{v}\cdot(\underline{b}-\underline{a})}{\|\underline{u}\times\underline{v}\|} .$$

∨∨ En linie L er fastlagt
∫ ved en enhedsvektor $\underline{e}$, samt et
∨ punkt A af L. En kraft $\underline{K}$ har angrebspunkt B og vinkellinie L_1. Så er $(\underline{b}-\underline{a})\times\underline{K}$ momentet af $\underline{K}$ i punktet A, og $\underline{e}\cdot(\underline{b}-\underline{a})\times\underline{K} = [\underline{e}, \underline{b}-\underline{a}, \underline{K}]$ er dette moments projektion på L. Vi ser, at det er uafhængigt af valget af punktet A på L, så vi kan slutte, at alle momentvektorer for $\underline{K}$ i punkter af L har ens projektioner på L. Den således definerede skalar kaldes momentet af $\underline{K}$ om L. Det skifter fortegn med orienteringen af L.



∧∧
∫
∧∧

Lad $\underline{x},\underline{y}$ og $\underline{z}$ være vektorer i $\mathbb{E}^3$. Da er

$$(\underline{x}\times\underline{y})\times\underline{z} = -(\underline{y}\cdot\underline{z})\underline{x} + (\underline{x}\cdot\underline{z})\underline{y}.$$

Bevis. Venstre side forbliver uændret, når $\underline{y}$ erstattes med $\underline{y}+\lambda\underline{x}$, og højre side ændres med bidraget

$$-(\lambda\underline{x}\cdot\underline{z})\underline{x} + (\underline{x}\cdot\underline{z})\lambda\underline{x} = \underline{0} .$$

Altså er det nok at vise sætningen i det specielle tilfælde, hvor $\underline{y}$ er vinkelret på $\underline{x}$. Hvis $\underline{x}$ eller $\underline{y}$ er $\underline{0}$ er påstanden triviel. Hvis $\underline{x}$ erstattes med $\lambda\underline{x}$ og $\underline{y}$ med $\mu\underline{y}$ bliver begge sider af ligningen ganget med $\lambda\mu$. Altså kan vi antage, at $\underline{x}$ og $\underline{y}$ er på hinanden vinkelrette enhedsvektorer. Vi kan så anvende en ortonormal højrebasis $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$ med $\underline{e}_1 = \underline{x}$ og $\underline{e}_2 = \underline{y}$, og så får vi

$$(\underline{e}_1\times\underline{e}_2)\times\underline{z} = (\underline{e}_1\times\underline{e}_2)\times(z_1\underline{e}_1 + z_2\underline{e}_2 + z_3\underline{e}_3) =$$

$$\underline{e}_3\times(z_1\underline{e}_1+z_2\underline{e}_2+z_3\underline{e}_3) = z_1\underline{e}_2 - z_2\underline{e}_1 = -(\underline{e}_2\cdot\underline{z})\underline{e}_1 + (\underline{e}_1\cdot\underline{z})\underline{e}_2 .$$

Dermed er formlen bevist.

Formlen er ofte nyttig. Den giver også mulighed for at udlede flere interessante relationer. Vi skal først nævne, at den helt umiddelbart giver den pæne formel

$$(\underline{x}\times\underline{y})\times\underline{z} + (\underline{y}\times\underline{z})\times\underline{x} + (\underline{z}\times\underline{x})\times\underline{y} = \underline{o}.$$

Ved at benytte reglen om, at $\times$ og $\cdot$ kan byttes i rumproduktet, får vi

$$(\underline{u}\times\underline{x})\cdot(\underline{y}\times\underline{z}) = ((\underline{u}\times\underline{x})\times\underline{y})\cdot\underline{z} = -(\underline{x}\cdot\underline{y})(\underline{u}\cdot\underline{z}) + (\underline{u}\cdot\underline{y})(\underline{x}\cdot\underline{z}),$$

og det kan også skrives

$$(\underline{u}\times\underline{x})\cdot(\underline{y}\times\underline{z}) = \begin{vmatrix} \underline{u}\cdot\underline{y} & \underline{u}\cdot\underline{z} \\ \underline{x}\cdot\underline{y} & \underline{x}\cdot\underline{z} \end{vmatrix} .$$

Som specialtilfælde heraf får vi

$$(\underline{x}\times\underline{y})^2 + (\underline{x}\cdot\underline{y})^2 = \underline{x}^2\,\underline{y}^2 ,$$

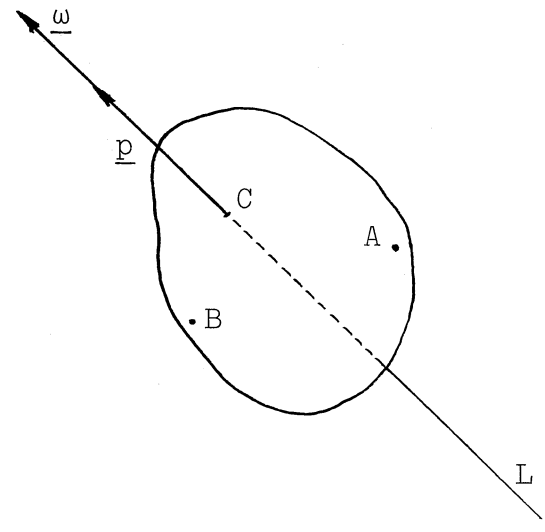
men den kunne nu fås trivielt af produkternes definitioner. Endelig får vi direkte af formlen

$$(\underline{u}\times\underline{x})\times(\underline{y}\times\underline{z}) = -[\underline{x},\underline{y},\underline{z}]\underline{u} + [\underline{u},\underline{y},\underline{z}]\underline{x} =$$

$$[\underline{u},\underline{x},\underline{z}]\underline{y} - [\underline{u},\underline{x},\underline{y}]\underline{z}.$$

Det er en vektor i skæringslinien mellem en plan, der indeholder $\underline{u}$ og $\underline{x}$, og en plan, der indeholder $\underline{y}$ og $\underline{z}$.

Vi vil slutte vor gennemgang af vektorregning med nogle udregninger, der kan være til nytte i teorien for stive legemers mekanik. Vi vil antage, at legemet udfører en skruebevægelse, idet det roterer om en akse L med den vektorielle vinkelhastighed $\underline{\omega}$ og forskydes langs L med en hastighed $\underline{p}$. Vi kan lade både $\underline{\omega}$ og $\underline{p}$ angribe i et punkt C af L. Hastighederne i de vilkårlige punkter A og B betegnes $\underline{v}_A$ og $\underline{v}_B$, og de er bestemt ved



$$\underline{v}_A = \underline{p} + \underline{\omega}\times(\underline{a}-\underline{c}) = \underline{p} + (\underline{c}-\underline{a})\times\underline{\omega},$$

$$\underline{v}_B = \underline{p} + \underline{\omega}\times(\underline{b}-\underline{c}) = \underline{p} + (\underline{c}-\underline{b})\times\underline{\omega},$$

$$\underline{v}_B = \underline{v}_A + (\underline{a}-\underline{b})\times\underline{\omega}.$$

Hastighedsfeltet er således helt bestemt ved $\underline{\omega}$ og hastigheden af et vilkårligt givet punkt. Vi kan godt tænke os hastighedsfeltet defineret i hele rummet, idet ethvert punkt i rummet kan tænkes i fast forbindelse med legemet.

Hvis vi nu har givet $\underline{\omega}$ og $\underline{v}_A$ som vilkårligt fast valgte vektorer, får vi hastigheden $\underline{v}_B$ af B som ovenfor. Vi får nu

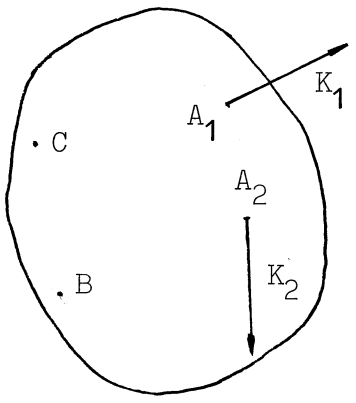
$$\underline{v}_B\times\underline{\omega} = \underline{v}_A\times\underline{\omega} + ((\underline{a}-\underline{b})\times\underline{\omega})\times\underline{\omega} = \underline{v}_A\times\underline{\omega} + \underline{\omega}^2(\underline{b}-\underline{a})+((\underline{a}-\underline{b})\cdot\underline{\omega})\underline{\omega} .$$

Hvis vi vælger

$$\underline{b} = \underline{a} - \frac{\underline{v}_A\times\underline{\omega}}{|\underline{\omega}|^2} ,$$

får vi $\underline{v}_B\times\underline{\omega} = o$. Der findes således et punkt, hvis hastighed er lineært afhængig af $\underline{\omega}$, og hastighedsfeltet bliver netop hastighedsfeltet for en skruebevægelse om en akse gennem dette punkt.

Lad os nu antage, at det stive legeme er angrebet af kræfterne $\underline{K}_1,\ldots,\underline{K}_n$ i punkterne $A_1,\ldots,A_n$. Momentvektorerne i punkterne B og C er da bestemt ved



$$\underline{m}_B = (\underline{a}_1-\underline{b})\times\underline{K}_1+\ldots+(\underline{a}_n-\underline{b})\times\underline{K}_n,$$

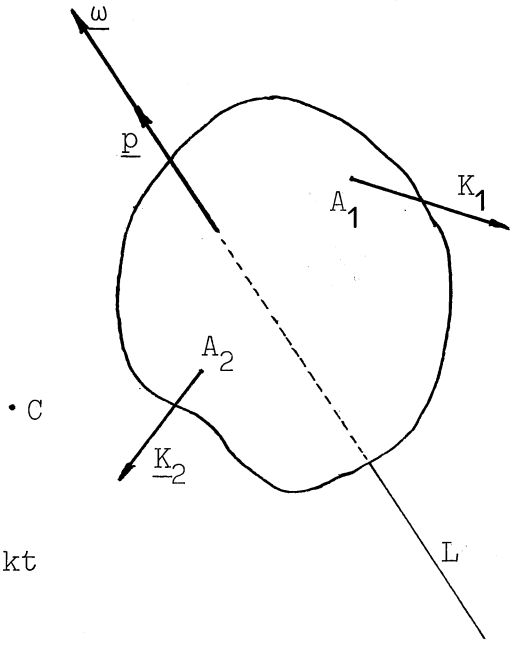
$$\underline{m}_C = (\underline{a}_1-\underline{c})\times\underline{K}_1+\ldots+(\underline{a}_n-\underline{c})\times\underline{K}_n,$$

og idet vi indfører kraftsummen $\underline{K} = \underline{K}_1+\ldots+\underline{K}_n$, får vi

$$\underline{m}_C = \underline{m}_B + (\underline{b}-\underline{c})\times\underline{K}.$$

Heraf fremgår, at et momentfelt for et kraftsystem har præcis samme udseende som hastighedsfeltet ved en skruebevægelse.

Lad os nu antage, at legemet udfører en skruebevægelse om en akse L med vinkelhastighed $\underline{\omega}$ og er påvirket af samme kraftsystem, som ovenfor. Kræfternes samlede effekt er da, idet C er et vilkårligt punkt



$$E = \underline{K}_1\cdot\underline{v}_{A_1}+\ldots+\underline{K}_n\cdot\underline{v}_{A_n} =$$

$$\underline{K}_1\cdot(\underline{v}_C+(\underline{c}-\underline{a}_1)\times\underline{\omega})+\ldots+\underline{K}_n\cdot(\underline{v}_C+(\underline{c}-\underline{a}_n)\times\underline{\omega}) =$$

$$\underline{K}\cdot\underline{v}_C+((\underline{a}_1-\underline{c})\times\underline{K}_1+\ldots+(\underline{a}_n-\underline{c})\times\underline{K}_n)\cdot\underline{\omega} =$$

$$\underline{K}\cdot\underline{v}_C + \underline{m}_C\cdot\underline{\omega}.$$

Med dette pæne resultat vil vi slutte vor gennemgang af vektorregning.

ØVELSER TIL KAPITEL 4.

Først stikordsliste til støtte ved indlæring.

Vektorprodukt, længde af vektor, hastighedsvektor, moment af kraft, skalarprodukt, vektorfelt, enhedsvektor, rumprodukt, skruebevægelse, areal af parallelogram, cosinusrelation, skæring mellem planer, plans ligning på normalform, dobbelt vektorprodukt, effekt, feltstyrke, distributive love for vektorproduktet, vinkelhastighed, ortonormalt system, krafts angrebspunkt, skalar, Plücker's liniegeometri, hastighedsfelt, højde i trekant, Kronecker's symbol, arbejde, vektorprodukt i koordinater, den pytagoræiske sætning, kraft, skalarprodukt af vektorprodukter, planprodukt, kræfters effekt ved skruebevægelse, matrix, momentfelt, vektorprodukt af vektorprodukter, energi, krafts moment om linie, areal som vektor, invariant, afstand mellem rette linier, projektion af vektor på linie, kraftfelt, vinkel melmel vektorer, liniebunden vektor.

4.1. I E^3 tænkes valgt et begyndelsespunkt O og et højrekoordinatsystem svarende til en ortonormal basis $(\underline{e}_1,\underline{e}_2,\underline{e}_3)$ for $\mathbb{E}^3$. Lad A,B,C og D være punkter med stedvektorer $\underline{a} = 2\underline{e}_1-\underline{e}_2+2\underline{e}_3$, $\underline{b} = \underline{e}_1+2\underline{e}_2-2\underline{e}_3$, $\underline{c} = 6\underline{e}_1+2\underline{e}_2-3\underline{e}_3$, $\underline{d} = \underline{e}_1+4\underline{e}_2+8\underline{e}_3$.

4.1.1. Find koordinater for enhedsvektorer med retning som $\underline{a},\underline{b},\underline{c},\underline{d}$.

4.1.2. Find længden af projektionen af $\underline{d}$ på den rette linie OA. Find vinklen mellem $\underline{a}$ og $\underline{d}$. Find koordinaterne til projektionen af D på OA.

4.1.3. Find en ligning for planen gennem C vinkelret på $\underline{a}$, og find afstandene fra denne plan til punkterne B og D.

4.1.4. Find arealet af trekanterne OAB og ABC.

4.1.5. Find volumen af tetraedret OABC.

4.1.6. Find vinklen mellem $\underline{a}$ og planen gennem B,C og D.

4.1.7. Find vinklen mellem planen gennem O,A og B og planen gennem O,A og C.

4.1.8. Find afstanden mellem den rette linie AC og den rette linie BD.

4.1.9. Undersøg, om højderne i tetraedret OABC går gennem samme punkt.

4.2. Vi fortsætter med at bruge betegnelserne fra 4.1.

Angiv to helt forskellige metoder til bestemmelse af den retvinklede projektion af B på planen gennem O,A og D. Prøv, om den ene metode går væsentligt lettere end den anden.

4.3. Vi fortsætter stadig med betegnelserne fra 4.1. Angiv en enhedsvektor $\tilde{\underline{e}}_1$ med retning som $\underline{a}$, dernæst en enhedsvektor $\tilde{\underline{e}}_2$ vinkelret på $\tilde{\underline{e}}_1$ og i planen gennem $\underline{a}$ og $\underline{b}$ (der er 2 løsninger - vælg den ene). Find $\tilde{\underline{e}}_3$, så $(\tilde{\underline{e}}_1,\tilde{\underline{e}}_2,\tilde{\underline{e}}_3)$ er et ortonormalt højrekoordinatsystem. Angiv koordinaterne for $\underline{c}$ og $\underline{d}$, samt for $\underline{e}_1,\underline{e}_2,\underline{e}_3$ i dette nye koordinatsystem. Opgaven giver lidt regnearbejde, men hvis man ved, at 153 er produkt af 9 og 17, kan det da gennemføres.

4.4. En hel masse relationer mellem vektorer kan fortolkes som elementærgeometriske sætninger. Således siger relationen $\frac{1}{2}(\underline{a}+\underline{b}) = \underline{b} + \frac{1}{2}(\underline{a}-\underline{b})$, at diagonalerne i et parallelogram halverer hinanden. Relationen $\underline{a}\cdot\underline{b} = 0 \Leftrightarrow \|\underline{a}+\underline{b}\| = \|\underline{a}-\underline{b}\|$ fortæller, at et parallelogram er et rektangel, hvis og kun hvis dets diagonaler er lige lange. Relationen $\|\underline{a}\| = \|\underline{b}\| \Leftrightarrow (\underline{a}+\underline{b})\cdot(\underline{a}-\underline{b}) = 0$ fortæller, at et parallelogram er en rombe, hvis og kun hvis diagonalerne er vinkelrette på hinanden. Relationen $\|\underline{a}+\underline{b}\|^2+\|\underline{a}-\underline{b}\|^2 = 2\|\underline{a}\|^2+2\|\underline{b}\|^2$

siger, at kvadratsummen af diagonalerne i et parallelogram er lig med kvadratsummen af de fire sider. Den er nok snarere kendt fra skolen som en formel til beregning af en median i en trekant.

4.5. I en plan firkant er de to linier, der forbinder midtpunkterne af modstående sider, vinkelrette på hinanden, hvis og kun hvis diagonalerne er lige lange. Vis dette ved regning med skalarprodukter. Studer derefter beviset og læg mærke til, at "plan" er en irrelevant oplysning. Formuler det mere generelle resultat, der faktisk blev vist.

4.6. Find afstanden mellem et punkt, som i et ortonormalt koordinatsystem i E^3 har koordinaterne (6, 8,1), og den rette linie, som i det samme koordinatsystem har parameterfremstillingen

$$(x_1, x_2 x_3) = (2+2t,\ 4-t,\ 6+2t).$$

4.7. Find en parameterfremstilling for en ret linie, der ligger i den plan, der i et ortonormalt koordinatsystem har ligningen $x_3 = 0$, skærer den linie, der i det samme koordinatsystem har parameterfremstillingen $(x_1, x_2 x_3) = (t,t,t)$ og danner en vinkel på $\frac{\pi}{3}$ med denne.

4.8. Find den retvinklede projektion af et punkt, der i et ortonormalt koordinatsystem har koordinaterne (1,16,0) på skæringslinien mellem de to planer, der i det samme koordinatsystem har ligningerne

$$8x_1-x_2+4x_3 = 41 \quad \text{og} \quad 3x_1-2x_3 = -7.$$

4.9. Find en parameterfremstilling for den retvinklede projektion af en ret linie, der i et ortonormalt koordinatsystem har parameterfremstillingen

$$(x_1,x_2,x_3) = (6+9t,\ 1-4t,\ -1-5t)$$

på den plan, der i det samme koordinatsystem har ligningen

$$4x_1+x_2-2x_3 = 6.$$

4.10. I et ortonormalt koordinatsystem har et tetraeders hjørnespidser koordinaterne (0,0,0), (3,0,0), (3,4,0) og (3,0,1). Find centrum i tetraedrets indskrevne kugle, samt kuglens radius.

4.11. Angiv en ligning for en plan i et koordinatsystem, hvis akser skærer planen i punkter A,B og C med koordinater (a,0,0), (0,b,0) og (0,0,c), hvor a, b og c er givne tal, der gerne må antages strengt positive. Find volumet af tetraedret OABC samt arealet af trekanten ABC.

4.12. Lad A,B og C være punkter på den kugleflade F i E^3, som har centrum i begyndelsespunktet O. Vi tænker os nu, at vi har målt storcirkelbuerne AB og AC, samt vinklen mellem dem, altså mellem planerne OAB og OAC. Målene er vinkelmål angivet i radianer. Vi stiller os opgaven at udregne storcirkelbuen BC. Idet $\underline{a},\underline{b}$ og $\underline{c}$ er stedvektorerne til A,B og C, altså enhedsvektorer, er $\underline{b}\cdot\underline{c}$ netop cosinus af den søgte vinkel. Analogt er $\|\underline{a}\times\underline{b}\|$ sinus af AB, og $(\underline{a}\times\underline{b})\cdot(\underline{a}\times\underline{c})$ $\|\underline{a}\times\underline{b}\|\,\|\underline{a}\times\underline{c}\|$ er cosinus af den kendte toplansvinkel. Vi finder en ligning, der bestemmer cosinus af den søgte vinkel. Den fundne formel er et første hjælpemiddel til trekantsberegning for sfæriske trekanter, sfærisk trigonometri.
Sfærisk trigonometri er vigtigt, hvis man vil arbejde med astronomi, geodæsi eller navigation.

4.13. Lad $(\underline{a}_1,\underline{b}_1)$ og $(\underline{a}_2,\underline{b}_2)$ være 2 par af på hinanden vinkelrette vektorer i E^3. Det antages, at $\underline{a}_1$ og $\underline{a}_2$ er lineært uafhængige, og at $\underline{b}_1$ og $\underline{b}_2$ er lineært uafhængige. Hvilke yderligere betingelser er nødvendige og tilstrækkelige, for at der findes netop 1 vektor $\underline{r}$, som tilfredsstiller begge relationerne $\underline{a}_1\times\underline{r} = \underline{b}_1$ og $\underline{a}_2\times\underline{r} = \underline{b}_2$. Find også $\underline{r}$ udtrykt ved $\underline{a}_1,\underline{a}_2,\underline{b}_1$ og $\underline{b}_2$, når betingelsen er opfyldt. Hvordan forholder det sig, når betingelserne om lineær uafhængighed ikke begge er opfyldt.

4.14. Opstil ligninger for omdrejningscylinder og omdrejningskegle i et ortonormalt koordinatsystem i E^3. Aksen tænkes givet ved en parameterfremstilling (det skal være en tilfældig ret linie, ikke f.eks. en koordinatakse). For cylinderen er desuden opgivet radius. For keglen kendes toppunktet (som gerne må svare til parameterværdien 0 på aksen) og den halve topvinkel.

KAPITEL 5

Mængdelære.

Vi vil gå ud fra at mængdelæren er kendt fra skolen, og vi vil ikke tage den op til revision. Vi bruger betegnelsen $a \in A$ for "a er et element i mængden A". For to mængder A og B skriver vi

$A \subseteq B$ for "A er delmængde af B",

$A \subset B$ for "A er ægte delmængde af B",

$A \cup B$ for "foreningsmængden af A og B",

$A \cap B$ for "fællesmængden af A og B",

$A \setminus B$ for "overskudsmængden af A over B".

Det sidste symbol forudsætter ikke, at $B \subseteq A$. Det hænder ofte, at vi udelukkende beskæftiger os med delmængder af en fast mængde M, og så kaldes $M \setminus A$ komplementærmængden til A og den betegnes så også CA.

Udsagnsregning beskæftiger sig med udsagn. Et udsagn siger noget om noget, sætter ting i relation til hinanden. Udsagn kan indeholde variable. Eksempler på udsagn er "ræve er røde", "$x \in A$", "$5 > \pi$", men ikke "skudens kaptajn", "$A \cap B$" eller "alle røde ræve". Vi vil tænke os, at udsag-

nene ved tilladelige valg af de variable kan klassificeres som sande eller falske. Vi kan så koble udsagn med de logiske tegn

$A \vee B$ for "A eller B"

$A \wedge B$ for "A og B"

$A \Rightarrow B$ for "hvis A så B"

$A \Leftrightarrow B$ for "hvis og kun hvis A, da B".

Desuden bruger vi $\neg A$ for negationen "ikke A".

Der er en nær sammenhæng mellem operationer med mængder og operationer med udsagn. Et udsagn A, i hvilket der indgår en variabel x, som kan variere i en mængde M, er forbundet med mængden $\tilde{A}$ af "de $x \in M$, for hvilke A". Hvis $\tilde{B}$ er mængden, der på samme måde svarer til B, vil $\tilde{A} \cup \tilde{B}$ svare til $A \vee B$ og $\tilde{A} \cap \tilde{B}$ til $A \wedge B$. Ligeledes vil $\tilde{A} \subseteq \tilde{B}$ svare til $A \Rightarrow B$ og $\tilde{A} = \tilde{B}$ til $A \Leftrightarrow B$. Endelig vil $C\tilde{A}$ svare til $\neg A$.

På grund af disse omstændigheder gælder de samme regler for operationer med mængder og for operationer med udsagn, og den rent formelle manipulation med mængder eller udsagn efter disse regler kaldes Boole'sk algebra efter George Boole (1815-1864). Vi anfører et par eksempler på regneregler

$$C(\tilde{A} \cup \tilde{B}) = C\tilde{A} \cap C\tilde{B} \; ; \neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B$$

$$\tilde{A} \cup (\tilde{B} \cap \tilde{C}) = (\tilde{A} \cup \tilde{B}) \cap (\tilde{A} \cup \tilde{C}) \; ; (A \vee (B \wedge C)) \Leftrightarrow ((A \vee B) \wedge (A \wedge C))$$

$$\tilde{A} \cap (\tilde{B} \cup \tilde{C}) = (\tilde{A} \cap \tilde{B}) \cup (\tilde{A} \cap \tilde{C}) \; ; (A \wedge (B \vee C)) \Leftrightarrow ((A \wedge B) \vee (A \wedge C)).$$

Analogien er dog ikke fuldkommen, da alle de logiske tegn er relationstegn, medens mængdelærens tegn er kompositionstegn på nær $\subseteq$ og $\in$, som er relationstegn. Derfor bliver analogien lidt anderledes, hvor $\subseteq$ er med. Vi nævner et eksempel

$$\tilde{A} \subseteq \tilde{B} \Leftrightarrow C\tilde{A} \cup \tilde{B} = M \; ; \quad (A \Rightarrow B) \Leftrightarrow (\neg A \vee B).$$

Boole'sk algebra har en hel del anvendelser ved benyttelse af problemer i forbindelse med automatisk styring og automatisk kontrol, og derved får den også anvendelser i datalogi.

Logikken bliver interessant ved indførelsen af kvantorerne $\forall$ og $\exists$. Et sæt regler for brug af noget, der minder meget om kvantorer findes allerede hos Aristoteles, der opstillede et system af såkaldte figurer, der hver bestod af to udsagn, præmisserne, samt en konklusion, hvis en sådan kunne drages. Vi anfører nogle enkelte eksempler.

Alle A er B Alle B er C Alle A er C	Nogle A er B Alle B er C Nogle A er C	Alle A er ikke B Alle B er C Ingen konklusion	Nogle A er ikke B Alle B er C Ingen konklusion
Alle A er B Nogle B er C Ingen konklusion	Nogle A er B Alle B er ikke C Nogle A er ikke C	Alle A er ikke B Alle B er ikke C Ingen konklusion	Nogle A er B Nogle B er C Ingen konklusion

Aristoteles behøvede et anseligt antal figurer, og det lykkedes ikke helt at undgå fejl. Vore moderne kvantorer er enklere. Nogle matematikere bruger også en ekstra kvantor, som betyder "der eksisterer én og kun én", og den skrives ofte $\exists!$, men den kan nu sagtens undværes.

Hvis R er en relation, hvori der indgår et bogstav x, betyder

$\forall x(R)$: Ethvert x tilfredsstiller relationen R

$\exists x(R)$: Der findes et x, som tilfredsstiller R.

Kvantorerne er næsten altid betingede i den forstand, at der er lagt visse bånd på x, f.eks. at x skal være en mængde, et komplekst tal, en vektor etc. Somme tider anføres betingelsen sammen med kvantoren, f.eks.

$$\forall x > 0\ \exists y > 0(y^2=x),$$

der siger, at ethvert positivt tal har en positiv kvadratrod. Det må så være gjort klart i teksten, at der er tale om reelle tal og ikke f.eks. rationale tal eller hele tal.

Lad R og S være relationer, hvori x indgår. Vi har da parentesreglerne

$$\forall x(R \wedge S) \Leftrightarrow \forall x(R) \wedge \forall x(S)$$

$$\exists x(R \vee S) \Leftrightarrow \exists x(R) \vee \exists x(S),$$

medens der kun gælder ensidig implikation i reglerne

$$\forall x(R) \vee \forall x(S) \Rightarrow \forall x(R \vee S)$$

$$\exists x(R \wedge S) \Rightarrow \exists x(R) \wedge \exists x(S).$$

Hvis relationen R indeholder x og y, har vi

$$\exists x \forall y(R) \Rightarrow \forall y \exists x(R)$$

Hvis x og y er reelle tal, og R relationen x+y=0, gælder relationen på højre side, medens relationen på venstre side ikke gælder. Når kvantorer af samme slags følger lige efter hinanden, kan de byttes, og så vil man ofte erstatte dem med én kvantor. Det kan være nødvendigt at omforme betingelser ved ombytning af kvantorer. Således er

$$\forall x > o \; \forall y \in]o,x[\; (R) \Leftrightarrow \forall y > o \; \forall x > y \; (R),$$

og her vil man ofte blot sætte et komma i stedet for det sidste $\forall$.

Når en relation kaldes en identitet, en formel eller en sætning, ligger der i det, at den gælder for alle sådanne værdier af de variable, som i henhold til den ledsagende tekst kan indgå i den. Derfor udelades kvantoren $\forall$ i sådanne tilfælde.

Når Cantor og hans samtidige var i stand til at opnå vældig interessante resultater ved mængdelærens hjælp, beroede det på en dristig anvendelse af uendelige mængder, og det blev allerede på Cantors tid klart, at en sådan ukritisk

anvendelse af mængdelæren førte til paradokser. Således vil mængden af alle mængder være element i sig selv, hvilket allerede har en urimelig klang. Endnu værre går det med mængden Æ af de mængder, der ikke er element i sig selv, idet såvel antagelsen $Æ \in Æ$, som antagelsen $Æ \notin Æ$ let ses at føre til en modstrid.

Det er et logisk paradoks af samme art som det, der ligger i udsagnet:

"Barberen i landsbyen barberer alle de beboere i landsbyen, som ikke barberer sig selv".

Hvem barberer så barberen?

Der blev opdaget mange mængdeteoretiske paradokser, og der opstod megen mistillid til mængdelæren. På den anden side havde allerede Cantor udnyttet mængdelæren til at opnå interessante nye resultater og enklere beviser for kendte resultater, og der var uvilje mod at kaste disse fordele over bord. Der opstod derfor en mere kritisk mængdelære, en forsigtig brug af mængdelæren, hvor man forsøgte at holde sig i sikker afstand fra paradokserne.

Vi vil altså også være lidt mere forsigtige. Vi vil ikke finde os i, at der er modsigelser i matematikkens grundlag. Det er da nærliggende at forsøge at bortoperere paradoksets årsag, altså fradømme mængden af alle mængder retten til at eksistere, f.eks. ved blandt aksiomerne også at have et,

der siger, at en mængde ikke er element i sig selv. Det kan vi imidlertid kun, hvis vi til gengæld sørger for, at de tilladte operationer med mængder kun kan føre til mængder, som opfylder denne betingelse.

Lad os filosofere lidt over, hvad det egentlig er, vi har brug for, hvis vi skal kunne lave matematiske teorier, hvori mængdebegrebet indgår, og som skal kunne bruges som matematiske modeller af væsentlige sider af den virkelighed vi lever i og er en del af. Som fysikerne har vi brug for noget, vi godt kan kalde partikler - altså noget, der ikke har elementer i sig, men som hver for sig er et element. Hvis vi f.eks. vil lave geometri, vil vi da i hvert fald gerne kunne opfatte punkterne sådan. Vi vil gerne kunne tale om mængden af alle sådanne partikler. Så får vi delmængder af denne mængde, og de kan igen indgå som elementer i mængder osv. Vi får så også en tom mængde $\emptyset$ - den eneste mængde, som har partikelkarakter. Det vil i reglen være en partikel, der afviger fra alle de andre partikler i teorien. Ved denne fremgangsmåde opnår vi en væsentlig indsnævring af mængdebegrebet.

Når vi nu filosoferer videre, opdager vi, at vi stadig kan tale om "alle mængder, der kan fås ved de tilladte processer" (såsom valg af delmængder, foreningsmængder, osv.), og hvis vi taler om "mængden af alle sådanne mængder", vil der igen opstå paradokser. Der opstår således et behov for

helheder, der ikke er mængder. Sådanne helheder er sædvanligvis blevet betegnet som klasser, en uheldig betegnelse på grund af vor sædvanlige og hyppige brug af begrebet klasseinddeling. I disse forelæsningsnoter vil vi derfor bruge en anden betegnelse, nemlig ordet art, som vi har hentet fra de biologiske videnskaber. Vi vil altså tale om arten M af mængder, og $A \in M$ betyder, at A er en mængde. For at være en mængde må A have visse kvalifikationer, og hvis vi får A udleveret, kan det meget vel tænkes, at vi slet ikke på tilfredsstillende måde kan undersøge, om A har de nødvendige kvalifikationer. Med en biologisk art som f.eks. "kanin" forholder det sig på lignende måde. Der er vanskeligheder med afgrænsningen af begrebet kanin, fordi der findes døde kaniner, kaninfostre, misfostre, kaniner, intet menneske har set osv. Desuden er der vanskeligheder med identifikationen, og for mængder er det helt væsentligt, at vi helt magter lighedstegnets brug.

Vi kan godt bruge kvantorer om elementer, der kan vælges frit indenfor en art. Således gælder for mængder, at

$$\forall A,B\ ((A \setminus B) \cup (A \cap B) = A).$$

Vi ser nu, at den Boole'ske algebra fra logik snarere kopieres på arter end på mængder. Ved regning med arter bruger vi de samme betegnelser som ved regning med mængder. Iøvrigt

er en mængde altid en art. Der er selvfølgelig stadig en art af arter, idet vi ovenfor netop forklarede, hvilke kvalifikationer artsbegrebet i sig selv måtte have. Derved løber vi igen ind i en form for logisk modstrid af lignende art som den, man møder, hvis man vil definere begrebet "definition" eller holde et foredrag om kunsten at holde foredrag.

Når R er en relation, hvori der indgår en variabel x, betegner $\{x|R\}$, mængden eller arten af de x for hvilke R gælder. Hvis x skal være element af en mængde, eller art A, skriver vi $\{x \in A|R\}$, og hvis A er en mængde, bliver det altid en mængde igen. Hvis A og B er mængder eller arter og $a \in A$, $b \in B$ vilkårlige elementer, kan vi danne det ordnede par (a,b). Vi definerer

$$A \times B = \{(a,b) \mid a \in A,\ b \in B\}.$$

og det er en mængde, hvis både A og B er det. En delmængde af $A \times B$ kaldes en relation, og en sådan angives i reglen ved et relationstegn $\dashv$, idet vi skriver $a \dashv b$, hvis (a,b) ligger i delmængden. Vi møder også relationer, der defineres ved en delart af arten $A \times B$, og hvor delarten ikke er en mængde. Relationen kaldes funktionel, hvis det for ethvert element $x \in A$ gælder, at der findes ét og kun ét element $y \in B$, som tilfredsstiller $x \dashv y$, og vi betegner da relationen ved et bogstav f og skriver $y = f(x)$, eventuelt $y = fx$, men det vil dog ofte kunne misforstås. En sådan relation siges at være en afbildning $f: A \to B$.

Hvis M er arten af mængder, kan vi definere en afbildning $F:M\times M \to M$ ved $F(A,B) = A \cup B$ og iøvrigt mange lignende. Vi kan også definere $\subseteq$ som en relation svarende til delarten $\{(A,B) \in M\times M \mid A \subseteq B\}$ af $M\times M$. Hvis $\bar{M}$ er den art, der omfatter M samt alle partiklerne, bliver $a \in A$ en relation, der svarer til en delart af $\bar{M}\times M$.

Vi minder om, at afbildninger $f: A_1 \to A_2$, $g:A_2 \to A_3$ og $h:A_3 \to A_4$ giver sammensatte afbildninger $g\circ f:A_1 \to A_3$ og $h\circ g:A_2 \to A_4$ og at denne operation er associativ, altså $h\circ(g\circ f)=(h\circ g)\circ f$. For enhver mængde A har vi en identisk afbildning $Id_A:A \to A$ defineret ved $Id_A(x) = x$ for hvert element $x \in A$. Den betegnes på forskellig vis i litteraturen, f.eks. I_A, E_A, e_A eller 1_A. For enhver afbildning $f:A \to B$ gælder $f = f\circ 1_A = 1_B\circ f$.

Til en mængde A og en delmængde $B \subseteq A$ hører en inklusionsafbildning $j:B \to A$ defineret ved $j(x) = x$ for ethvert $x \in B$. Hvis $f:A \to A_1$ er en vilkårlig afbildning, kaldes $f\circ j:B \to A_1$ restriktionen af f til B, og betegnes $f|B$. Hvis vi nu yderligere har $A_1 \subseteq B_1$ og inklusionsafbildningen $j_1:A_1 \to B_1$, får vi en afbildning $j_1\circ f:A \to B_1$. Vi siger, at $j_1\circ f:A \to B_1$ er $f:A \to A_1$ opfattet som afbildning ind i B_1, og at $f:A \to A_1$ er $j_1\circ f:A \to B_1$ opfattet som afbildning ind i A_1.

Lad $f:X \to Y$ være en afbildning. For en delmængde $A \subseteq X$

har vi dens billede $f(A) = \{f(x) \mid x \in A\}$, og for en delmængde $B \subseteq Y$ har vi dens originalmængde $f^{-1}(B) = \{x \in X \mid f(x) \in B\}$. Hvis $B = \{b\}$ er en mængde, der består af et eneste element b, skriver vi $f^{-1}(b)$ for $f^{-1}(B)$.

Lad $f:X \to Y$ være en afbildning, lad A_1 og A_2 være delmængder af X og B_1 og B_2 delmængder af Y. Vi minder om reglerne

$$f(A_1 \cup A_2) = f(A_1) \cup f(A_2), \quad f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$$

$$f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2), \quad f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$$

$$f(A_1 \setminus A_2) \supseteq f(A_1) \setminus f(A_2), \quad f^{-1}(B_1 \setminus B_2) = f^{-1}(B_1) \setminus f^{-1}(B_2)$$

For $B \subseteq Y$ gælder endvidere, at $f^{-1}(Y \setminus B) = X \setminus f^{-1}(B)$ (originalmængder til komplementærmængder er komplementærmængder). For $A \subseteq X$ behøver $f(A)$ og $f(X \setminus A)$ ikke at have Y som foreningsmængde, og de behøver heller ikke at have tom fællesmængde.

En afbildning $f:X \to Y$ kaldes injektiv (eller entydig) hvis $f(x_1) = f(x_2)$ for $x_1, x_2 \in X$ kun er opfyldt, når $x_1 = x_2$. Det er ensbetydende med at $f^{-1}(y)$ for hvert $y \in Y$ er tom eller består af et enkelt element af x. Afbildningen kaldes surjektiv, hvis $f(X) = Y$, altså, hvis $f^{-1}(y) \neq \emptyset$ for alle $y \in Y$. En afbildning kaldes bijektiv, hvis den er både injektiv og surjektiv, og hvis $f:X \to Y$ er bijektiv, kan $f^{-1}(y)$ tolkes som definerende en invers afbildning $f^{-1}:Y \to X$. At

$f:X \to Y$ er bijektiv med $f^{-1}:Y \to X$ som invers afbildning er ensbetydende med, at $f^{-1} \circ f = Id_X$ og $f \circ f^{-1} = Id_Y$. For afbildningen $f:X \to Y$ og $g:Y \to Z$ gælder, at $g \circ f$ er injektiv, hvis g og f er injektive og analoge udsagn om surjektiv og bijektiv. Hvis $g \circ f$ er injektiv, er f injektiv, og hvis $g \circ f$ er surjektiv, er g surjektiv. Alt dette er ret selvfølgeligt.

I matematisk jargon spiller ordet "familie" en ganske stor rolle. Det dækker egentlig slet ikke over noget selvstændigt begreb, men er bare en betegnelse for noget, som allerede er velkendt. En familie er helt det samme som en afbildning. Til en familie hører en mængde J, indexmængden, og en afbildning $f:J \to M$, hvor M er en art eller en mængde. Vi betegner $f(j)$ med x_j, og bruger betegnelsen $(x_j \mid j \in J)$ for familien. Betegnelsen kan forkortes til (x_j), hvis det er klart, hvad indexmængden skal være. For $J = \{0,1\}$ bliver en familie $(x_j \mid j \in J)$ det samme som et ordnet par. En talfølge (a_n) er en familie med indexmængde $\mathbb{N}$ (eventuelt $\mathbb{N} \cup \{0\}$ eller noget i den retning).

Vi kan således tale om en familie $(A_j \mid j \in J)$ af mængder i en matematisk teori. For en sådan familie kan vi definere foreningsmængden $\bigcup_{j \in J} A_j$ og hvis $J \neq \emptyset$ tillige fællesmængden $\bigcap_{j \in J} A_j$ ved definitionerne

$$x \in \bigcup_{j \in J} A_j \Leftrightarrow \exists j \in J (x \in A_j)$$

$$x \in \bigcap_{j \in J} A_j \Leftrightarrow \forall j \in J(x \in A_j).$$

Hvis $J = \emptyset$ bliver foreningsmængden tom. Fællesmængden ville komme til at omfatte alt, og det er der jo ikke mening i. I en teori, der kun opererer med delmængder af en fast mængde M, bliver M fælllesmængden for den tomme familie af delmængder.

Til familien $(A_j \mid j \in J)$ svarer også en mængde $\prod_{j \in J} A_j$, altså

$$\prod_{j \in J} A_j = \{(a_j \mid j \in J) \mid \forall j \in J(a_j \in A_j)\}.$$

Hvis mængden J specielt er endelig, $J = \{j_1, \ldots, j_n\}$, skriver vi også

$$\prod_{j \in J} A_j = A_{j_1} \times \ldots \times A_{j_n}$$

Mængden $\prod_{j \in J} A_j$ kaldes familiens produktmængde (produktet af mængderne i familien). Hvis vi har en familie $(A \mid j \in J)$ af eksemplarer af en og samme mængde, skriver vi A^J for $\prod_{j \in J} A$. Når vi erindrer, hvad en familie er for noget, ser vi, at A^J også er mængden af afbildninger af J ind i A. I det specielle tilfælde $J = \{1, \ldots, n\}$ skriver vi A^n for A^J.

Endelig har en familie $(A_j \mid j \in J)$ en disjunkt forening $\bigvee_{j \in J} A_j$ defineret ved

$$\bigvee_{j \in J} A_j = \{(j,a) \mid j \in J, a \in A_j\}.$$

For $J = \{j_1,\ldots,j_n\}$ skriver vi

$$\bigvee_{j\in J} A_j = A_{j_1} \vee \ldots \vee A_{j_n}.$$

Det er klart, at $\bigvee_{j\in\emptyset} A$ bare er $\emptyset$. For $J = \emptyset$ består produktmængden af 1 element, den tomme familie (dvs. den tomme afbildning $\emptyset \to \emptyset$).

I formalistisk matematik regner man med, at de fire her nævnte operationer anvendt på mængder igen fører til mængder. Desuden skal man altid kunne tale om mængden af delmængder i en mængde.

Vi skal ikke gå i detaljer med regneregler for de fire nye mængdeoperationer. Der er en forfærdelig masse regneregler, og de følger alle helt umiddelbart af reglerne for regning med kvantorer. Vi skal nævne et par eksempler senere i forbindelse med nye begreber, men lige nu vil vi blot anføre en enkelt sætning.

Sætning. For en familie $(A_j \mid j \in J)$ af delmængder af en mængde M gælder relationerne

$$M \setminus \bigcup_{j\in J} A_j = \bigcap_{j\in J} (M \setminus A_j), \quad M \setminus \bigcap_{j\in J} A_j = \bigcup_{j\in J} (M \setminus A_j).$$

Disse regneregler er næsten helt trivielle. I den første relation står der på venstre side mængden af elementer i M der ikke tilhører nogen som helst af mængderne i familien, og på højre side står mængden af elementer i M, der ligger udenfor enhver af mængderne i familien.

Læg mærke til, at vi var nødt til at definere produktet af to mængder, før vi kunne definere selve begrebet familie, så vi kunne ikke undgå at definere produktmængde i to omgange.

En familie $(A_j \mid j \in J)$ af delmængder af en mængde M kaldes en overdækning af M, hvis $M = \bigcup_{j \in J} A_j$. Familien kaldes en klasseinddeling af M, hvis mængderne i familien er disjunkte, altså hvis det for alle valg af $j, k \in J$ med $j \neq k$ gælder, at $A_j \cap A_k = \emptyset$, og hvis det desuden for alle $j \in J$ gælder, at $A_j \neq \emptyset$. Mængderne A_j kaldes da klasser, og mængden $K = \{A_j \mid j \in J\}$ kaldes klassemængden. Der findes en afbildning $f:M \to K$, som er helt fastlagt ved, at det for ethvert element $x \in M$ skal gælde, at $x \in f(x)$. Denne afbildning kaldes den til klasseinddelingen hørende kanoniske afbildning.

Lad $f:X \to Y$ være en afbildning. Da er $(f^{-1}(y) \mid y \in f(X))$ en klasseinddeling af X. Lad K være klassemængden. Så inducerer f en afbildning $f_1 : K \to f(X)$ defineret ved $f_1(f^{-1}(y)) = y$. Det er klart, at f_1 er bijektiv, og at f bliver identisk med den sammensatte afbildning

$$X \xrightarrow{k} K \xrightarrow{f_1} f(X) \xrightarrow{j} Y$$

hvor k er den kanoniske afbildning og j inklusionsafbildningen.

Hvis $(A_j \mid j \in J)$ er en familie af mængder, og $A = \prod_{j\in J} A_j$ produktmængden, findes der for hvert $k \in J$ en afbildning $pr_k : A \to A_k$ defineret ved $pr_k(a_j \mid j \in J) = a_k$. Den kaldes projektionen af A på A_k. Lad X være en mængde og $(f_j : X \to A_j \mid j \in J)$ en familie af afbildninger. Der findes da én og kun én afbildning $f : X \to A$, som for hvert $j \in J$ tilfredsstiller betingelsen $pr_k \circ f = f_j$, nemlig den afbildning, der defineres ved $f(x) = (f_j(x) \mid j \in J)$. Hvis $J_1 \subseteq J$ er en vilkårlig delmængde, har hver familie (det er jo i virkeligheden en afbildning) $(a_j \mid j \in J)$ en restriktion $(a_j \mid j \in J_1)$ og derved defineres en projektion $pr_{J_1} : A \to \prod_{j\in J_1} A_j$. Alle de her omtalte projektioner giver klasseinddelinger af A, og klasserne kaldes ofte fibre.

En relation R på en mængde X er en delmængde $R \subseteq X \times X$. Vi skriver xRy for $(x,y) \in R$. Vi minder om, at relationen kaldes

refleksiv, hvis $\forall x \in X(xRx)$

symmetrisk, hvis $\forall x,y \in X(xRy \Leftrightarrow yRx)$

transitiv, hvis $\forall x,y,z \in X(xRy \wedge yRz \Rightarrow xRz)$

antisymmetrisk, hvis $\forall x,y \in X(xRy \wedge yRx \Rightarrow x = y)$.

En relation, som er refleksiv, symmetrisk og transitiv kaldes en ækvivalensrelation og læses "ækvivalent med". En ækvivalensrelation er ensbetydende med en klasseinddeling i klasser af indbyrdes ækvivalente elementer.

Vi kan godt have en relation på en art, og det giver ikke anledning til ændring i definitionerne af de fire egenskaber ovenfor. Relationen =, altså "lig med" er et eksempel på en sådan ækvivalensrelation, men den indtager en særstilling derved, at den må indføres, før det overhovedet er muligt at komme i gang med mængdelæren. Et vigtigt aksiom i mængdelæren siger, at to mængder er identiske, hvis og kun hvis de indeholder netop de samme elementer. For to mængder A og B forlanger vi således at

$$A = B \Leftrightarrow \forall x(x \in A \Leftrightarrow x \in B).$$

Af denne forudsætning følger specielt, at enhver mængde helt uden elementer er lig med $\emptyset$, så der ikke findes flere forskellige tomme mængder.

På arten af mængder har vi en ækvivalensrelation $A \sim B$, som betyder, at der findes en bijektiv afbildning $\varphi: A \to B$. Når dette er opfyldt, siger vi, at A og B har samme kardinaltal, og vi skriver kard A = kard B. Det er nu let at se, at en mængde er endelig, hvis og kun hvis den ikke er ækvivalent med nogen ægte delmængde af sig selv.

Vi definerer kard $\mathbb{N} = \text{Alef}_0$, idet Alef er det første bogstav i det hebraiske alfabet. Det ser ud som vist på figuren. Mængder med kardinaltal Alef_0 kaldes tællelige eller numerable. At en mængde er tællelig betyder, at den kan arrangeres som en familie $(a_j | j \in \mathbb{N})$, alt-

så som en følge. En delmængde af en tællelig mængde er endelig eller tællelig. En mængde er uendelig, hvis og kun hvis den har en tællelig delmængde.

Det var først og fremmest studiet af mængders tællelighed, der på Cantors tid afslørede mængdelærens styrke. Det vigtigste hjælpemiddel ved beviser for tællelighed er følgende lemma:

Lemma 5.1. Foreningsmængden af en følge af endelige mængder er endelig eller tællelig.

Bevis. Lad (A_n) være en følge af endelige mængder. Vi sætter $B_n = A_n \setminus (A_1 \cup \ldots \cup A_{n-1})$, og så er (B_n) en følge af disjunkte endelige mængder. Lad ν_n være antallet af elementer i B_n. Vi kan da skrive $B_n = \{b_{n,1}, \ldots, b_{n,\nu_n}\}$, og når vi så sætter

$$b_{n,j} = c_{\nu_1+\ldots+\nu_{n-1}+j},$$

har vi fået alle elementerne i $\bigcup A_n$ ordnet i følgen (c_n), som eventuelt kan være endelig. Dermed er Lemmaet bevist.

Sætning 5.2. Mængden af polynomier med hele tal som koefficienter er tællelig.

Bevis. For et polynomium

$$P(x) = a_0 + a_1 x + \ldots + a_n x^n$$

definerer vi $\nu(P) = n+|a_0|+|a_1|+\ldots+|a_n|$. Derved defineres en afbildning $\nu:A \to \mathbb{N}$, hvor A er mængden af polynomier med hele tal som koefficienter, og da $\nu^{-1}(p)$ er endelig for hvert $p \in \mathbb{N}$, følger sætningen umiddelbart af lemma 5.1.

Definition 5.3. Et tal $a \in \mathbb{C}$ kaldes algebraisk, hvis der findes et polynomium med hele tal som koefficienter, i hvilket a er rod. Komplekse tal, som ikke er algebraiske kaldes transcendente.

Sætning 5.4. Mængden af algebraiske tal er tællelig.

Bevis. Af vor foregående sætning fremgår, at der findes en følge (P_n) omfattende alle polynomier med hele tal som koefficienter. Idet mængden A_n af rødder i P_n er endelig fås sætningen ved anvende lemma 5.1 på følgen (A_n).

Det er nu klart at mængden af alle sæt $(\nu_1,\ldots,\nu_p)$ af hele tal og af alle mulige længder er tællelig, for hvert sådan talsæt svarer jo netop til et polynomium $\nu_1+\nu_2x+\ldots+\nu_px^{p-1}$. Dernæst får vi umiddelbart, at mængden af endelige sæt af algebraiske tal er tællelig.

For en vilkårlig mængde A vil vi med $\hat{D}(A)$ betegne mængden af delmængder i A.

Sætning 5.4. Der findes ikke nogen surjektiv afbildning $\varphi:A \to \hat{D}(A)$.

Bevis. For $A = \emptyset$ består $\hat{D}(A)$ af det ene element $\emptyset$, og for en afbildning $\varphi:\emptyset \to \hat{D}(\emptyset)$ er billedmængden tom, altså en ægte delmængde i $\{\emptyset\}$, så φ er ikke surjektiv. Generelt indfører vi $B = \{x \in A | x \in A \setminus \varphi(x)\} \in \hat{D}(A)$. For $y \in B$ har vi da $y \in A \setminus \varphi(y)$, altså $\varphi(y) \neq B$. For $y \in A \setminus B$ har vi $y \in \varphi(y)$, altså $\varphi(y) \neq B$. Altså hører B ikke til $\varphi(A)$. Dermed er sætningen bevist.

Sætning 5.5. $\mathbb{R}$ er ikke tællelig.

Bevis. Hvis $\mathbb{R}$ var en tællelig mængde, ville også delmængden af decimalbrøker $0,x_1x_2x_3\ldots$ med alle decimalerne x_n lig med 0 eller 1 være en tællelig mængde. Det ville betyde, at mængden M af afbildninger $f:\mathbb{N} \to \{0,1\}$ var tællelig. Nu kan vi definere en bijektiv afbildning $\varphi:M \to \hat{D}(\mathbb{N})$ ved $\varphi(f) = f^{-1}(1)$, så også $\hat{D}(\mathbb{N})$ måtte være numerabel. Det strider imidlertid mod den foregående sætning, og dermed er påstanden vist.

Det fremgår af vore resultater, at der findes reelle tal, som ikke er algebraiske. Nu havde Liouville 50 år før Cantor indførte mængdelæren bevist, at tallet $0,11000100\ldots010\ldots$, hvor det nte 1-tal står på plads nr. n!, er transcendent. Det interessante ved Cantors bevis er netop, at det ikke er konstruktivt, at det end ikke hjælper os bare en lille smule med virkelig at angive et transcendent tal. Her har vi netop det mest håndgribelige stridsspørgsmål mellem formalisterne og intuitionisterne. Disse sidste nægter at tro på begrebers eksi-

stens, når denne ikke er bevist ved en virkelig gennemførlig konstruktion.

En relation, som er refleksiv, transitiv og antisymmetrisk kaldes en ordningsrelation, og en mængde med en ordningsrelation kaldes en ordnet mængde. Ordningsrelationer betegnes oftest ved et usymmetrisk tegn som de velkendte eksempler $\leqq$ og $\subseteq$. De bruges også uden lighedstegnet, således at $a < b$ betyder $a \leqq b$ og $a \neq b$. Vi kan godt have en ordningsrelation på en art.

En relation $\dashv$ kaldes en præordningsrelation, hvis den er refleksiv og transitiv. Så vil relationen $\sim$ defineret ved, at $a \sim b$ skal betyde $a \dashv b \wedge b \dashv a$ være en ækvivalensrelation, og mængden vil falde i ækvivalensklasser $A,B,\ldots,$ og for elementer a_1 og a_2 fra samme klasse A gælder da altid både $a_1 \dashv a_2$ og $a_2 \dashv a_1$. Hvis vi nu har elementer $a_1,a_2 \in A$ og $b_1,b_2 \in B$, da vil relationen $a_1 \dashv b_1$ give $a_2 \dashv a_1 \dashv b_1 \dashv b_2$, altså $a_2 \dashv b_2$. Derfor inducerer $\dashv$ en relation $\leqq$ på mængden af klasser, og denne relation bliver en ordensrelation.

Det lyder mere indviklet end det er. Det er nemlig i virkeligheden bare, hvad man gør, når man prøver at ordne nogle mennesker efter alder og kommer til at anerkende nogle grupper af lige gamle som ligestillede i ordningen.

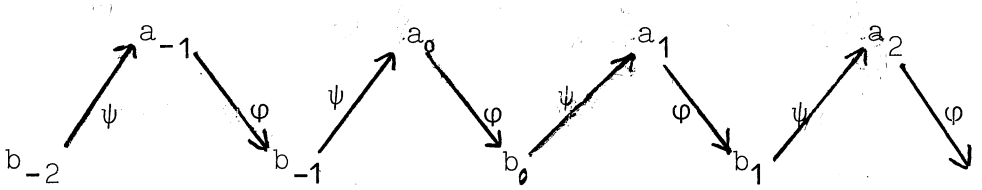
Lad X og A være ordnede mængder. Vi tillader os at

skrive begge ordningsrelationer $\leqq$. En afbildning $f:X \to A$ kaldes voksende, hvis det for alle $x,y \in X$ med $x \leqq y$ gælder, at $f(x) \leqq f(y)$. Den kaldes strengt voksende, hvis det for alle $x,y \in X$ med $x < y$ gælder, at $f(x) < f(y)$. Undertiden siger vi monoton i stedet for voksende. Vi kalder $f:X \to A$ aftagende, hvis det for alle $x,y \in X$ med $x \leqq y$ gælder, at $f(y) \leqq f(x)$, og analogt med strengt aftagende. En injektiv voksende afbildning er strengt voksende. En bijektiv voksende afbildning $f:X \to A$ kaldes en ordningsisomorfi og dens inverse vil da også være en ordningsisomorfi. Når der findes en ordningsisomorfi $f:X \to A$, kaldes X og A ordningsisomorfe.

Det er klart, at vi kan definere en præordningsrelation på arten af kardinaltal, ved at kard A $\leqq$ kard B, hvis og kun hvis der findes en injektiv afbildning $\varphi:A \to B$. Nu er det så heldigt, at vi endda får en ordningsrelation. Dette følger af vor næste sætning, der går under navnet Bernsteins sætning.

Sætning 5.6. Hvis det for to mængder A og B gælder, at der findes injektive afbildninger $\varphi:A \to B$ og $\psi:B \to A$, da findes der en bijektiv afbildning $\chi:A \to B$.

Bevis. Lad $a = a_0 \in A$ være et vilkårligt element. Vi skal definere $\chi(a_0)$. Dertil benytter vi, at afbildningerne φ og ψ giver os en kæde af elementer, en afbildningskæde



Kæden fortsætter i det uendelige mod højre, og eventuelt også mod venstre, men her kan den ende med et element i $A \setminus \psi(B)$ eller et element i $B \setminus \varphi(A)$. Det er klart, at hvert element af A og hvert element af B hører til netop 1 afbildningskæde. En afbildningskæde, der fortsætter i det uendelige til begge sider, kan være periodisk - altså løbe i kreds. Vi definerer nu $\chi(a_0) = \varphi(a_0)$, hvis afbildningskæden ikke starter i et element af $B \setminus \varphi(A)$, men $\chi(a_0) = \psi^{-1}(a_0)$, hvis afbildningskæden starter i et element af $B \setminus \varphi(A)$. Det ses umiddelbart, at den således definerede afbildning $\chi: A \to B$ bliver bijektiv, og dermed er sætningen bevist.

Lad M være en mængde, som er ordnet ved en ordningsrelation $\leqq$. Et element $a \in M$ kaldes et første element i M, hvis $\forall b \in M(a \leqq b)$. Et element $a \in M$ kaldes et sidste element i M, hvis $\forall b \in M(b \leqq a)$. Undertiden foretrækker vi at sige "mindste" i stedet for "første og "største" i stedet for "sidste". Et element $a \in M$ kaldes minimalt, hvis M ikke indeholder noget element $b < a$, og $a \in M$ kaldes maksimalt, hvis M ikke indeholder noget element $b > a$.

En mængde M, som er ordnet ved en ordningsrelation kaldes totalt ordnet, såfremt ordningsrelationen opfylder betingelsen

$$\forall x,y \in M(x \leqq y \vee y \leqq x).$$

Således er $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ og $\mathbb{R}$ totalt ordnede ved $\leqq$, medens mængden af delmængder i en mængde med mindst 2 elementer ikke er totalt ordnet ved $\subseteq$. Mængden $\mathbb{N}$ er ordnet, men ikke totalt ordnet ved relationen "går op i". Menneskeheden er ordnet, men ikke totalt ordnet ved relationen "nedstammer fra".

En mængde M kaldes velordnet, hvis den er totalt ordnet og enhver delmængde har et første element. Hvis M er velordnet ved en ordningsrelation $\leqq$ og $a \in M$ er et element, kaldes $M_a = \{b \in M | b < a\}$ det ved a bestemte afsnit af M. Ved et afsnit af M forstås et afsnit M_a bestemt ved et $a \in M$ eller hele M. Det er let at vise, at det for to velordnede mængder altid gælder, at den ene er ordensisomorf med et afsnit af den anden.

En totalt ordnet endelig mængde er altid velordnet. Derimod er $\mathbb{Q}$ og $\mathbb{R}$ totalt ordnede, men ikke velordnede ved $\leqq$.

Mængden $\mathbb{N} \cup \{0\}$ er velordnet ved $\leqq$, og hvert $n \in \mathbb{N}$ angiver antallet af elementer i afsnittet $(\mathbb{N} \cup \{0\})_n$, men samtidig kan vi sige, at n er ordinaltallet for denne velordnede mængde, idet vi tildeler hver art af ordensisomorfe mængder et ordinaltal. Med ω betegner vi ordenstallet for $\mathbb{N} \cup \{0\}$, hvilket er akkurat det samme som ordenstallet for $\mathbb{N}$. Mængden $\mathbb{N} \cup \{0\}$ med ω føjet til som et sidste element har ordningstype, som vi betegner $\omega+1$. Vi fortsætter denne konstruktion og får de transfinite ordenstal

$$0,1,2,3,\ldots,\omega,\omega+1,\omega+2,\ldots 2\omega,2\omega+1,\ldots,3\omega\ldots\omega^2,\ldots\omega^\omega\ldots,$$

Arten af transfinite ordenstal er velordnet ved $\leqq$, og hvert transfinit ordenstal betegner ordenstallet for det afsnit i arten af transfinite ordenstal, det selv bestemmer.

Enhver velordnet mængde er ordensisomorf med et afsnit af arten af transfinite tal.

Det er klart, at arten af transfinite tal ikke kan være en mængde. Det ville den være efter det naive mængdebegreb, og man opdagede allerede på Cantors tid, at det førte til ubehagelige paradokser.

Den alvorligste af de mange kriser i forbindelse med matematikkens grundlag indtraf, da E. Zermelo i 1904 publicerede en tre sider lang afhandling i Mathematische Annalen bd. 59 med titlen: Beweis dass jede Menge wohlgeordnet werden kann. Vi formulerer sætningen.

Velordningssætningen. På enhver mængde M findes en ordningsrelation, med hvilken M er velordnet.

Vi vil ikke omtale Zermelos bevis her, men vi vil dog nævne, at Zermelo indleder sit bevis ved af hver ikke tom delmængde $A \subseteq M$ at udvælge et element $u_A \in A$. I 1905

fremkom adskillige kritiske kommentarer til Zermelos bevis, og de fleste matematikere syntes at mene, at Zermelo ikke havde bevist noget som helst, og det var først og fremmest det samtidige udvalg af elementer fra en mængde af mængder, der ikke vandt anerkendelse som en forsvarlig bevismetode. Diskussionen kulminerede med et interessant indlæg fra den franske matematiker H. Lebesgue, som påviste, at tilsvarende udvalgsprocedurer havde fundet anvendelse også i traditionel matematik uden at nogen var blevet foruroligede over det.

Den antagelse, Zermelos bevis byggede på, er siden blevet kaldt udvalgsaksiomet.

Udvalgsaksiomet. For enhver mængde M findes en afbildning $u:\hat{D}(M)\setminus\{\emptyset\} \to M$, som for hver ikke tom mængde $A \subseteq M$ tilfredsstiller betingelsen $u(A) \in A$.

Zermelo publicerede i 1908 et nyt bevis for, at velordningssætningen følger af udvalgsaksiomet. Det nye bevis blev ikke kritiseret. Fra moderne synspunkt er begge Zermelos beviser tilfredsstillende.

Efter Zermelo stod intuitionisterne væsentligt stærkere, men det var dog tydeligt, at det kostede meget mere arbejde at nå de tilsvarende resultater af intuitionistisk vej, så der var et udbredt ønske om på en eller anden måde at redde mængdelæren. De fleste matematikere fortsatte dog en vis forsigtig brug af naiv mængdelære, men undgik helst at bygge på udvalgs-

aksiomet og undlod i øvrigt at beskæftige sig med grundlagsspørgsmål. En erstatning for et gennemarbejdet grundlag for matematikken fik man ved at tage den naive mængdelære for givet, og så indføre de naturlige tal som en mængde $\mathbb{N}$ organiseret ved et udvalgt element $1 \in \mathbb{N}$ og en injektiv afbildning $\varphi:\mathbb{N} \to \mathbb{N}\setminus\{1\}$, samt induktionsaksiomet

$$\forall A \subseteq \mathbb{N}\,((1 \in A \wedge \forall a \in A(\varphi(a) \in A)) \Rightarrow A = \mathbb{N}).$$

Man viste så, at disse forudsætninger helt fastlægger alle egenskaber ved $\mathbb{N}$. (Peanos aksiomer).

Inden vi forlader udvalgsaksiomet skal vi nævne at Kuratowski i 1922 fandt en sætning, som er ækvivalent med udvalgsaksiomet, og som er bekvemmere at bruge end velordningssætningen. Denne sætning kaldes Zorns lemma efter M. Zorn, som genopdagede den i 1935. Vi anfører den her, da vi har i sinde at bruge den en gang eller to.

Zorns lemma. Lad M være en ordnet mængde. Vi betragter alle delmængder $A \subseteq M$, som med den fra M inducerede ordning er totalt ordnede. Det antages, at enhver sådan mængde er majoriseret i M, altså at der til A svarer et element $b \in M$, således at $a \leq b$ for alle $a \in A$. Da har M mindst 1 maksimalt element.

Vi skitserer ganske kort og uden at udføre detaljer et bevis for ækvivalensen mellem udvalgsaksiomet, velordningssætningen og Zorns lemma.

Zorns lemma ⇒ velordningssætningen. Lad M være en mængde, og lad $V(M)$ være mængden af alle delmængder $A \subseteq M$ med alle mulige velordningsrelationer. Så er $V(M)$ partielt ordnet ved relationen "afsnit af". Det vises let, at enhver totalt ordnet delmængde af $V(M)$ majoriseres af foreningsmængden, så Zorns lemma giver et maksimalt element, og det må åbenbart omfatte hele M.

Velordningssætningen ⇒ udvalgsaksiomet. Lad M være en mængde. Vi velordner M og definerer udvalgsfunktionen $u: \hat{D}(M) \setminus \{\emptyset\} \to M$ ved, at $u(A)$ skal være det første element i A.

Udvalgsaksiomet ⇒ Zorns lemma. Lad M være en mængde med ordningsrelation $\leqq$. Vi vælger en udvalgsfunktion $u: \hat{D}(M) \setminus \{\emptyset\} \to M$. Hvis $A \subseteq M$ er velordnet ved $\leqq$, og $x \in A$ er et vilkårligt element, betegner vi med $e(x)$ mængden af elementer i M, som er $>$ samtlige elementer i afsnittet A_x. Vi kalder A en kæde, hvis $x = u(e(x))$ for alle $x \in A$. Specielt har enhver kæde $u(M)$ som første element. Det vises nu uden større besvær, at mængden af kæder er totalt ordnet ved relationen "afsnit af". Det medfører, at foreningsmængden af alle kæder er en kæde A^*, der indeholder alle andre kæder. Hvis $\leqq$ opfylder betingelsen i

Zorns lemma, majoriseres A^* af et element $b \in M$. Hvis b har efterfølgere, har A^* en ikke tom mængde e af efterfølgere, og $A^* \cup \{u(e)\}$ bliver en kæde med A^* som ægte delmængde i modstrid med definitionen af A^*. Altså er b et maksimalt element.

Den aksiomatiske metode har sin rod i Euklids elementer, og den optræder i mere og mere præcis form op gennem historien, indtil den formuleres skarpt ved dette århundredes begyndelse af D. Hilbert, som definitivt præciserer grundlaget for den Euklidiske geometri og viser, at dette grundlag er modsigelsesfrit, hvis grundlaget for de reelle tal er det. Derved er sorteper spillet videre, og det er ikke svært at få sorteper lokaliseret til matematikkens basale suppe, der omfatter teorien for logik, mængdelære og naturlige tal. Man kan ikke nå til bunds i problemerne ved hjælp af den aksiomatiske metode i dens traditionelle form.

B. Russell og A.N. Whitehead publicerede 1910-13 et 3 binds værk, Principia Mathematica, som var et forsøg på en formalistisk fremstilling af matematikkens grundlag. Det er klart, at problemerne ikke kunne løses på den måde, men sådan et forsøg har nu alligevel stor værdi, fordi man kun ved at forsøge at fremstille hele sagen i sammenhæng kan konstatere, hvor vanskelighederne i virkeligheden ligger. D. Hilbert og

flere medarbejdere arbejdede på at forbedre fremstillingen.

Et afgørende vendepunkt indtrådte, da K. Gödel i 1931 viste, at en formel logik, som var generel nok til at tjene som grundlag for indførelse af mængden $\mathbb{N}$ af naturlige tal ikke kunne undgå at omfatte relationer, der hverken kunne bevises eller modbevises. I 1941 viste Gödel yderligere om en nærmere præciseret art af sådanne teorier, at en modsigelsesfri teori ville forblive modsigelsesfri ved tilføjelse af udvalgsaksiomet. Desuden viste han, at den stadig ville forblive modsigelsesfri, hvis man tilføjede den generelle kontinuumhypotese, som vi skal omtale nedenfor. Dermed er det slået fast, at man har løbet den fulde risiko ved anvendelse af mængdelæren, så snart man overhovedet inddrager uendelige mængder. I 1973 viste P.J. Cohen, at en modsigelsesfri formel teori, som de af Gödel betragtede også ville forblive modsigelsesfri, hvis man i stedet for at udvide den med den generelle kontinuumhypotese tilføjede den forudsætning, at ikke engang den specielle kontinuumhypotese gælder. Dermed er det også fastslået, at Peanos aksiomer ikke helt fastlægger de naturlige tal.

Vi skylder at forklare, hvad kontinuumhypotesen er. Velordningssætningen sikrer at enhver mængde er ækvivalent med et afsnit af den tranfinite talrække, ordinaltallene

$$0,1,2,3,\ldots,\omega,\omega+1,\ldots 2\omega,\ldots\omega^2,\ldots\omega^\omega\ldots\Omega,\Omega+1,\ldots\Omega+\omega,\ldots 2\Omega,\ldots$$

Derfor vil der være et første ordinaltal, hvis afsnit er ækvi-

valent med en given mængde, og derved får vi kardinaltallene indplaceret som en del af ordinaltallene, og vi kan slutte, at også kardinaltallene er velordnede. Kardinaltallet Alef_0 svarer til ω, hvis afsnit er det første uendelige afsnit. Det næste kardinaltal Alef_1 svarer til et ordinaltal Ω, som er det første ordinaltal, hvis afsnit ikke er endeligt eller tælleligt. Den specielle kontinuumhypotese siger, at Alef_1 er kardinaltallet for $\mathbb{R}$, altså at der ikke findes yderligere kardinaltal mellem kard $\mathbb{N}$ og kard $\mathbb{R}$. Det er ikke særlig svært at vise, at $\hat{D}(\mathbb{N}) \sim \mathbb{R}$. Den generelle kontinuumhypotese siger, at det for enhver uendelig mængde M gælder, at kard $\hat{D}(M)$ er det kardinaltal, der følger lige efter kard M.

Det er lykkedes under anvendelse af udvalgsaksiomet at konstruere nogenlunde konkrete modeller af en ny slags naturlige tal, der tilfredsstiller Peanos aksiomer, og det har vist sig, at der er visse fordele ved at udnytte disse moderne tal i matematisk analyse. Derved er der opstået en ny gren af matematikken, non-standard analyse. Endvidere har også intuitionisterne arbejdet videre med matematikken på deres egen besværlige facon, og det lykkes dem efterhånden at eftergøre flere og flere af formalisternes resultater, selv om de intuitionistiske udgaver af sætninger som differentialligningens middelværdisætning får en ret besværlig formulering. Dette kan ses som et tegn på, at mængdelæren alligevel ikke er så letsindig.

Til slut nogle ord om moderne formel logik og mængdelære. Det er indlysende, at det er svært overhovedet at komme i gang. Under alle omstændigheder må de allerførste skridt på vejen være i nøje sammenhæng med den måde, vor bevidsthed arbejder på, og med vore muligheder for at kommunikere med andre. Man må så begynde forfra med at fortælle, hvilke tegn man vil bruge, og hvad de betyder. Der må i hvert fald være bogstaver, som betegner alle mulige slags variable. Der må eventuelt være nogle tegn, der reserveres til at betegne konstanter, i reglen yderst få. Der må være nogle matematiske relationstegn, i første omgang i hvert fald = og $\in$. Der må være logiske relationstegn, i hvert fald $\vee$ og $\neg$. Desuden behøves et symbol for den helt uundværlige proces at vælge et element (eller hvad det nu skal være) i overensstemmelse med givne betingelser.

Tegn og symboler kan skrives efter hinanden som symbolstrenge. De kan eventuelt suppleres med ekstra udstyr som forbindelseslinier, parenteser etc. Nu må man fastlægge det symbolske sprogs grammatik, idet visse symbolstrenge udnævnes til udtryk eller relationelle strenge. Det enkelte bogstav er et udtryk. Udtryk kan kombineres sammen til relationelle strenge ved hjælp af de matematiske relationstegn. Relationelle strenge kan kombineres sammen til nye relationelle strenge ved de logiske relationstegn. Udvalgssymbolet giver nye udtryk, når det anvendes på relationelle strenge. Udtryk og relationelle strenge giver symbolstrenge af samme slags, når bogstaver erstattes med udtryk.

Selve teorien startes med aksiomer. De fleste af disse vil være generelle i den forstand, at de indeholder bogstaver, for hvilke der kan indsættes enten vilkårlige relationelle strenge eller vilkårlige udtryk. Dernæst må der indføres slutningsregler, som beskriver, hvordan nye sætninger udledes ud fra aksiomerne. Det viser sig, at man hurtigt får brug for utåleligt lange symbolstrenge, så man må hjælpe sig ved at indføre en række forkortelser.

Det er rimeligt først at behandle de logiske formler, altså Boole's algebra. Så følger kvantorer og lighedstegn. Dernæst mængdelære, som vi skrev om den i begyndelsen af kapitlet. De naturlige tal kommer ind som de endelige ordinaltal.

Man kan med rette spørge, om det er rimeligt, at matematikerne spilder tiden med disse grundlagsundersøgelser, som måske slet ikke har nogen praktisk betydning. Dertil må man vel sige, at det nok ville være uheldigt, hvis alle matematikere ofrede en masse tid på den slags, men at det dog nok er lykkeligt, at nogle få matematikere har undersøgt disse problemer med så stor grundighed. Måske kan vi endda tillade os at sige, at de har givet os retten til at tro på mængdelæren, og det gør nu tilværelsen en hel del lettere.

ØVELSER TIL KAPITEL 5

Antallet af stikord til kapitel 5 er meget stort, da der indføres mange begreber. På grund af kapitlets særlige karakter, har vi anført stikordene i den rækkefølge, hvori de omtales, og vi har ikke medtaget de begreber, der må antages at være særdeles velkendte fra skolen. Dog har vi medtaget begreber, hvis betydning vi har ændret en smule i forhold til det fra skolen kendte. Når vi siger "udsagn", mener vi det, skolen kaldte "åbent udsagn", for det er det eneste udsagnsbegreb, der virkelig har interesse.

Udsagn, Boole'sk algebra, kompositionstegn, relationstegn, præmisser, konklusion, parentesregler for kvantorer, regler for ombytning af kvantorer, partikel, art, funktionel relation, inklusionsafbildning, injektiv, surjektiv, bijektiv, familie, disjunkt forening, overdækning, kanonisk afbildning, Alef, kardinaltal, numerabel eller tællelig, algebraisk tal, transcendent tal, formalisme, intuitionisme, præordning, strengt voksende, ordningsisomorfi, Bernsteins sætning, første og sidste (mindste og største) element, minimalt og maksimalt element, totalt ordnet, velordnet, ordinaltal eller ordenstal, transfinite ordenstal, velordningssætningen, udvalgsaksiomet, induktionsaksiomet, Zorns lemma, aksiomatisk metode, kontinuumhypotese.

5.1. Om en mængde M af strengt positive tal gælder, at der findes et tal K med den egenskab, at summen af elementerne i enhver endelig delmængde af M er $\leq K$. Vis, at M er tællelig eller endelig.

5.2. Lad I være intervallet $[0,1]$, så I^2 er kvadratet med side 1. Vi kan definere en afbildning $f: I \to I^2$ ved at skrive $x \in I$ som en uendelig decimalbrøk, og sætte $f(x) = (y,z)$, hvor y og z er decimalbrøker, der fås ved at bruge decimalerne med ulige nummer til y og dem med lige nummer til z, altså f.eks.

$$f(0,1374298643\ldots) = (0,17284\ldots, 0,34963\ldots).$$

Det giver ikke helt en bijektiv afbildning. Det kommer af, at visse tal kan skrives som decimalbrøk på to måder, f.eks. er $0,359999\ldots = 0,360000\ldots$. Vis, at ideen alligevel kan udbygges til et bevis for, at $\text{kard}I = \text{kard}I^2$.

5.3. Da relationer på en mængde M er delmængder af $M \times M$, bliver mængdeteoriens relationer $\subseteq$ og operationer $\cup, \cap$, samt C anvendelige på relationerne. I første omgang er dette bare endnu en konstatering af, at den Boole'ske algebra kan anvendes parallelt på mængder og relationer.

Læg mærke til, at fællesmængden for en vilkårlig mængde af ækvivalensrelationer igen er en ækvivalensrelation. For endelig mange ækvivalensrelationer kommer det bare ud på at forbinde dem til 1 relation ved at sætte dem efter hinanden med $\wedge$ imellem. For uendelig mange relationer $xR_jy; j \in J$ kommer det ud på at danne $\forall_j(xR_jy)$. Ud fra dette synspunkt svarer al-kvantoren til en "uendelig konjunktion".

På tilsvarende måde kommer foreningsmængde af relationer til at svare til $\vee$ i det endelige tilfælde og $\exists$ i det uendelige tilfælde, men en foreningsmængde af ækvivalensrelationer er ikke altid en ækvivalensrelation.

Svarende til en given mængde af relationer på M, kan man betragte mængden af ækvivalensrelationer på M, som indeholder dem alle. Fællesmængden af alle disse mængder giver den mindste ækvivalensrelation, der indeholder alle de givne relationer.

Specielt har 1 relation på M en mindste udvidelse til en ækvivalensrelation. Hvis relationen $\curlywedge$ i forvejen er refleksiv og symmetrisk, kan vi udvide den til en ækvivalensrelation $\curlywedge$ ved at definere $x \curlywedge y$ ved kravet om, at der skal findes en kæde $x \curlywedge t_1 \curlywedge t_2 \curlywedge \ldots \curlywedge t_n \curlywedge y$, og derved fås netop den mindste udvidelse til en ækvivalensrelation.

5.4. Lad A og B være mængder og $f:A \to B$ en afbildning. For $A^2 = A\times A$ og $B^2 = B\times B$ definerer vi da $f^2 = f\times f:A^2 \to B^2$ ved $f^2(x,y) = (f(x),f(y))$. En relation $R \subseteq A\times A$ får derved et billede $f^2(R) = f_*R \subseteq B\times B$, og uf_*Rv kommer til at betyde $\exists x,y \in A$ $f(x) = u \wedge f(y) = v \wedge xRy)$. En relation $S \subseteq B\times B$ får en tilbagetrækning $(f^2)^{-1}(S) = f^*S$, og xf^*Sy kommer til at betyde $f(x)Sf(y)$. En tilbagetrækning af en ordningsrelation er en præordningsrelation. De analoge påstande om billedet af en relation gælder sædvanligvis ikke.

En overdækning af B vil ligeledes have en tilbagetrækning, som er en overdækning af A. Matematikken er rig på strukturer, der således kan overføres ved tilbagetrækning (oversættelse af pull-back) altså mod afbildningsretningen. Der findes også strukturer, der kan overføres med afbildningsretningen, men de er tilsyneladende sjældnere. Sandheden er nok snarere, at de ikke så ofte optræder på elementært niveau.

5.5. Lad $(\sim_j | j \in J)$ være en familie af ækvivalensrelationer på en mængde A. Så er hver relation $\sim_j$ en delmængde $\sim_j \subseteq A\times A$. Vis, at hvis mængden $\{\sim_j | j \in J\}$ er totalt ordnet ved inklusion, da er $\bigcup_{j\in J} \sim_j = \sim \subseteq A\times A$ en ækvivalensrelation. Lad nu $R \subseteq A\times A$ være en vil-

kårlig relation. Det følger da af Zorns lemma, at R indeholder en maksimal ækvivalensrelation. Vis, ved et eksempel, at R sædvanligvis vil indeholde flere maksimale ækvivalensrelationer. Lad f.eks. A være mængden af alle mennesker med en nøjagtig fødselsattest, og lad relationen R være "aldersforskel mindre end 3 år". Så er R reflexiv og symmetrisk, men ikke transitiv. Vi kan inddele tidsintervallet fra 1800 til 2000 i intervaller af længde a. Vi har da ækvivalensrelationen "født i samme tidsinterval". Den bliver $\subseteq R$, hvis a er kortere end 3 år, og den bliver maximal, hvis a desuden er længere end $1\frac{1}{2}$ år.

KAPITEL 6.

Algebraisk struktur.

Algebra beskæftiger sig med mængder, som er organiserede ved kompositionsregler. Vi skal først og fremmest beskæftige os med vektorrum, flerdimensionale generalisationer af rummene E ,E^2 og E^3, som vi studerede i kapitlerne 3 og 4. Vektorrum har en kompliceret algebraisk struktur, og vi vil først give en kort beskrivelse af mængder med mere enkel algebraisk struktur. Nu vil det være forkert at tro, at den komplicerede struktur gør vektorrummene særligt vanskelige at arbejde med. Den hindrer dem tværtimod i at være alt for vilde.

I dette kapitel begynder vi forfra med en omtale af de fundamentale ting, der indgår eller kan indgå i en algebraisk struktur. Desuden giver vi en kortfattet skematisk oversigt over de hyppigst forekommende algebraiske strukturer, samt eksempler på disse hentede fra den verden, vi kender. Vektorrumsteorien vil levere os mange flere eksempler på sådanne strukturer.

Definition 6.1. En intern kompositionsregel på en mængde M er en afbildning $\mu: M\times M \to M$.

En kompositionsregel udtrykkes i reglen ved et eller andet kompositionstegn, f.eks. $*$, idet vi skriver $x*y$ for $\mu(x,y)$.

Eksempler. Addition og multiplikation er kompositionsregler på $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R}$ og $\mathbb{C}$. På mængden af strengt positive reelle tal er potensopløftning $\mu(x,y) = x^y$ en kompositionsregel, selv om den for det meste ikke skrives med et egentligt kompositionstegn. På $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$ er subtraktion en kompositionsregel, og på $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ og $\mathbb{C} \setminus \{0\}$ er division en kompositionsregel. Største fælles divisor og mindste fælles multiplum er kompositionsregler på $\mathbb{N}$. Addition er en kompositionsregel på E^1, E^2 og E^3, og vektorproduktet er en kompositionsregel på E^3. For en vilkårlig mængde M er mængden M^M af afbildninger $\varphi,\psi: M \to M$ organiseret ved sammensætningen $\psi \circ \varphi$ som kompositionsregel. Mængden $\hat{D}(M)$ af delmængder af M er organiseret ved kompositionsreglerne $\cup, \cap$ og $\setminus$.

Der er flere kompositionsregler. På enhver mængde vil $\mu(x,y) = x$ og $\mu(x,y) = y$ definere kompositionsregler. For enhver ikke tom mængde M kan vi vælge et fast element $a \in M$ og definere en kompositionsregel ved $\mu(x,y) = a$ for alle $x,y \in M$.

For det meste vil vi glemme ordet "intern", som vi allerede har gjort det i eksemplerne ovenfor.

Definition 6.2. Lad * være en intern kompositionsregel på en mængde M. For vilkårlige delmængder $A,B \subseteq M$ og vilkårlige elementer $a,b \in M$ indfører vi betegnelserne

$$A * B = \{x*y \mid x \in A,\ y \in B\}$$

$$a * B = \{a*y \mid y \in B\} = \{a\} * B$$

$$A * b = \{x*b \mid x \in A\} = A * \{b\}.$$

Således inducerer kompositionsreglen på M en kompositionsregel på mængden $\hat{D}(M)$ af delmængder af M. Betegnelserne er i øvrigt en naturlig udvikling af den sædvanlige betegnelse for billedmængde ved en afbildning.

Eksempler. For intervaller på $\mathbb{R}$ gælder

$$[a_1,b_1] + [a_2,b_2] = [a_1+a_2,b_1+b_2]$$

$$[a_1,b_1] + [a_2,b_2[= [a_1+a_2,b_1+b_2[.$$

Mængden af de lige tal og mængden af de ulige tal har mængden af ulige tal som sum, men mængden af lige tal som produkt.

Definition 6.3. Lad M være en mængde med en kompositionsregel *. En delmængde $A \subseteq M$ kaldes stabil med hensyn til *, hvis $A * A \subseteq A$.

Dette er ensbetydende med, at * har en restriktion til $A \times A$, som afbilder ind i A. Denne restriktion er en kompositionsregel på A, og vi benytter den samme betegnelse for den.

Eksempel. Mængden af lige tal er stabil med hensyn til addition og multiplikation, men mængden af ulige tal kun med hensyn til multiplikation. Mængden af komplekse tal på enhedscirklen er stabil med hensyn til multiplikation.

En kompositionsregel på en endelig mængde kan angives i form af en tabel. Vi viser som eksempel en tabel over en kompositionsregel * på en mængde {u,v,x,y} med 4 elementer.

	u	v	x	y
u	x	x	u	u
v	y	y	v	v
x	u	x	x	u
y	y	v	v	y

Vi aflæser af tabellen, at $u*u = x$, $u*v = x$, $v*u = y$ etc. De 16 felter kan udfyldes helt vilkårligt, så vi får 4^{16} forskellige kompositionsregler på den måde. De

er dog ikke "rigtigt forskellige". Hvis vi f.eks. skriver samme bogstav i alle 16 felter, er det egentlig ligegyldigt, hvilket af de 4 bogstaver vi vælger.

Vi går nu over til at omtale kompositionsregler med særlige egenskaber.

Definition 6.4. En intern kompositionsregel $*$ på en mængde M kaldes associativ, hvis det for vilkårlige elementer $a,b,c \in M$ gælder, at $(a*b)*c = a*(b*c)$. Den kaldes kommutativ, hvis det for vilkårlige elementer $a,b \in M$ gælder, at $a*b = b*a$.

For vilkårlige elementer $a_1,\ldots,a_n \in M$ giver udtryk som $a_1*\ldots*a_n$ ikke mening. Vi kan reducere sådan et udtryk ved at vælge to på hinanden følgende elementer a_ν, $a_{\nu+1}$ og erstatte $a_\nu*a_{\nu+1}$ med værdien af dette udtryk. Derved reduceres antallet af elementer i udtrykket med 1, og efter $n-1$ gentagelsen får vi hele udtrykket reduceret til 1 element af M. Vi kan angive dette ved hver gang at sætte parentes om de elementer, der kombineres sammen. Vi får åbenbart frygtelig mange (for resten lige præcis $(n-1)!$) frie valg, og for en tilfældig kompositionsregel vil resultatet af reduktionen afhænge af disse valg. Vi vil vise, at det netop for associative kompositionsregler gælder, at

resultatet af reduktion af et udtryk er helt uafhængigt af de frie valg.

Sætning 6.5. For en associativ kompositionsregel giver reduktion af et udtryk $a_1*\ldots*a_n$ en værdi, som er uafhængig af, hvilke naboelementer man vælger at kombinere sammen.

Bevis. For $n = 3$ er der kun 2 valgmuligheder, og betingelsen $(a_1*a_2)*a_3 = a_1*(a_2*a_3)$ fortæller netop, at de to valg giver samme resultat. For $n \geq 3$ viser vi påstanden ved induktion efter n, idet vi antager, at den er rigtig for $n-1$ vilkårlige elementer. Det indebærer, at resultatet af reduktionen af $a_1*\ldots*a_n$ er helt fastlagt, så snart vi har valgt de to elementer, der først skal kombineres sammen. Vi skal således bare vise, at vi får samme resultat hvad enten vi starter med a_j*a_{j+1} eller med a_k*a_{k+1}. Hvis a_j, a_{j+1}, a_k, a_{k+1} er 4 forskellige elementer, kan vi åbenbart blot vælge næste reduktionstrin, så vi får begge par kombineret sammen, og så er udtrykkene blevet ens og giver derfor samme resultat. Hvis a_j, a_{j+1}, a_k, a_{k+1} er 3 på hinanden følgende elementer, vælger vi næste reduktionstrin, så vi får disse 3 kombineret sammen, og det giver jo samme resultat i begge tilfælde. Dermed er sætningen bevist.

I eksemplerne ovenfor er potensopløftning og vektorprodukt samt subtraktion og division ikke er associative. Tabellen efter definition 6.3 giver også en kompositionsregel, der ikke er associativ.

For en mængde M med 2 eller flere elementer er sammensætning af afbildninger $\varphi,\psi,\chi:M \to M$ associativ, men ikke kommutativ. Hvis f.eks. $\varphi,\psi:M \to M$ hver afbilder hele M på 1 element af M (altså er konstante), gælder $\varphi\circ\psi = \psi\circ\varphi$ åbenbart kun, hvis det er det samme element, de afbildes på. Hvis $\varphi,\psi:\mathbb{R} \to \mathbb{R}$ er givet ved $\varphi(x) = a_1x+b_1$, $\psi(x) = a_2x + b_2$, hvor a_1, b_1, a_2, b_2 er reelle tal, får vi

$$(\varphi\circ\psi)(x) = a_1a_2x + a_1b_2 + b_1$$
$$(\psi\circ\varphi)(x) = a_1a_2x + a_2b_1 + b_2 .$$

Vi ser, at $\varphi\circ\psi = \psi\circ\varphi$, hvis og kun hvis $a_1b_2 + b_1 = a_2b_1 + b_2$. Vi siger, at φ kommuterer med ψ, hvis $\varphi\circ\psi = \psi\circ\varphi$, men det sker altså kun under heldige omstændigheder.

Sætning 6.6. Lad $*$ være en associativ og kommutativ kompositionsregel på en mængde M. Da er værdien af et udtryk $a_1*\ldots*a_n$ uafhængigt af elementernes rækkefølge.

Bevis. Vi kan starte reduktionen af $a_1*\ldots*a_n$ med at udregne a_j*a_{j+1} , men da $a_{j+1}*a_j = a_j*a_{j+1}$ ændres værdien af $a_1*\ldots*a_n$ ikke ved ombytning af a_j med a_{j+1} . Generelt kan vi slutte, at udtrykket ikke ændres ved ombytning af naboelementer. Vi skal vise, at

$$a_1*\ldots*a_n = b_1*\ldots*b_n ,$$

hvor $b_1,\ldots,b_n$ er elementerne $a_1,\ldots,a_n$ taget i en anden rækkefølge. Så forekommer b_1 mindst 1 gang blandt $a_1,\ldots,a_n$, lad os sige, at $b_1 = a_j$. Hvis $j > 1$, ombytter vi $j-1$ gange a_j med elementet umiddelbart til venstre for a_j , og derved får vi b_1 yderst til venstre. Dernæst bringer vi på samme måde b_2 på anden plads osv. Da disse ombytninger ikke ændrer udtrykkets værdi, får vi påstanden vist i endelig mange trin.

Det kan være noget frustrerende at have kommutativitet uden associativitet. Som eksempel har vi i E^2 og E^3 kompositionsreglen A*B, hvor A*B er midtpunktet af liniestykket AB. Man plejer ikke at tænke på denne midtpunktsdannelse som en kompositionsregel, og sådan er det også med de fleste af de i øvrigt mangfoldige eksempler på fænomenet.

Det skal tilføjes, at de oplagt kommutative komposi-

tionsregler "største fælles divisor" og "mindste fælles multiplum" på $\mathbb{N}$ faktisk er associative. Det er ikke svært at bevise det.

Definition 6.7. Lad $*$ være en kompositionsregel på en mængde M. Et element $e \in M$ kaldes venstre neutralelement for $*$, hvis $e*x = x$ for alle $x \in M$, og højre neutralelement, hvis $x*e = x$ for alle $x \in M$. Vi kalder e et (2-sidet) neutralelement, hvis det er både venstre og højre neutralelement.

Hvis $*$ er kommutativ, vil et venstre eller højre neutralelement for $*$ selvfølgelig automatisk være 2-sidet. Vi har iøvrigt den følgende sætning (læg mærke til, at associativitet slet ingen rolle spiller).

Sætning 6.8. Lad $*$ være en kompositionsregel på en mængde M. Hvis der findes såvel venstre som højre neutralelementer for $*$, findes der et 2-sidet neutralelement for $*$, og dette er det eneste venstre eller højre neutralelement. Hvis $*$ er kommutativ, findes der højst 1 neutralelement for $*$.

Bevis. Det hele følger umiddelbart af, at et venstre neutralelement e_1 og et højre neutralelement e_2 må tilfredsstille, at $e_1 = e_1*e_2 = e_2$.

Eksempler. Addition på $\mathbb{Z},\mathbb{Q},\mathbb{R}$ og $\mathbb{C}$ har 0 som neutralelement, medens multiplikation har 1 som neutralelement. Addition på $\mathbb{E}^\nu$ har $\underline{0}$ som neutralelement. Sammensætning af afbildninger $\varphi,\psi:M \to M$ har den identiske afbildning $\mathrm{id}(M)$ som 2-sidet neutralelement. Potensopløftning $\mu(x,y) = x^y$ på de strengt positive reelle tal har 1 som højre neutralelement, men intet venstre neutralelement. På $\hat{D}(M)$ er $\emptyset$ neutralelement for $\cup$, medens M er neutralelement for $\cap$. Den ved $\mu(x,y) = x$ definerede kompositionsregel på en mængde M er associativ, men ikke kommutativ, og den har intet venstre neutralelement, medens ethvert element af M er højre neutralelement.

Definition 6.9. Lad $*$ være en kompositionsregel på en mængde M. Lad e være 2-sidet neutralelement for $*$, og lad $a \in M$ være et vilkårligt element. Et element $b \in M$ kaldes venstreinverst til a, hvis $ba = e$, og b kaldes højreinverst til a, hvis $ab = e$. Hvis $ab = ba = e$ kaldes b et (2-sidet) inverst element til a.

Hvis b er venstreinverst til a er a højreinverst til b etc. For en associativ kompositionsregel har vi et sidestykke til sætning 6.8.

Sætning 6.10. Lad $*$ være en associativ kompositionsregel på en mængde M, og lad e være 2-sidet neutralele-

ment for $*$. Hvis et element $a \in M$ har både venstreinverse og højreinverse, har a netop 1 (2-sidet) inverst element og ikke andre venstre- eller højreinverse. Hvis $*$ desuden er kommutativ har hvert element i M højst 1 inverst element.

Bevis. Det hele følger umiddelbart af, at et venstreinverst element b til a og et højreinverst element c til a må tilfredsstille, at $b = b*e = b*(a*c) = (b*a)*c = e*c = c$.

Eksempler. For addition i $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$ samt $\mathbb{E}^\nu$ gælder, at $-a$ er inverst til a. I disse tilfælde plejer man at sige "modsat" i stedet for "inverst". For multiplikationen på $\mathbb{Z}$ gælder, at 1 og -1 er inverse til sig selv, medens ingen andre elementer har inverse. For multiplikationen på $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$ gælder, at alle elementer undtagen 0 har inverse. I disse tilfælde plejer man at sige "reciprok" for "inverst". For mængden af afbildninger $\varphi,\psi:M \to M$ gælder, at netop de bijektive har inverse. Hvis en afbildning $\varphi:M \to M$ har en venstre invers ψ, altså $\psi\circ\varphi = \mathrm{id}_M$, er φ injektiv. Hvis φ er injektiv, kan vi først definere $\psi|\varphi(M)$ som den inverse til φ opfattet som afbildning på $\varphi(M)$, og dernæst kan vi udvide definitionen af ψ til hele M ved f.eks. at afbilde alle elementer uden for $\varphi(M)$ på et og samme element. Derved bliver $\psi\,\varphi = \mathrm{id}_M$.

Når et element a har et 2-sidet inverst, betegnes dette ofte med a^{-1}, hvis der ikke i forvejen er en særlig betegnelse som $-a$, $\frac{1}{a}$, etc. Vi har nu en interessant sætning.

Sætning 6.11. Lad $*$ være en associativ kompositionsregel på en mængde M. Da er følgende 3 betingelser indbyrdes ækvivalente

1). Der findes et neutralelement e for $*$ og hvert element af M har et inverst.

2). For vilkårlige $a,b \in M$ har hver af ligningerne $a*x = b$ og $x*a = b$ netop 1 løsning.

3). For vilkårlige $a,b \in M$ har hver af ligningerne $a*x = b$ og $x*a = b$ mindst 1 løsning.

Bevis. 1) $\Rightarrow$ 2). Lad 1 være opfyldt. Af $a*x = b$ følger da $x = (a^{-1}*a)*x = a^{-1}*(a*x) = a^{-1}*b$, og af $x = a^{-1}*b$ følger $a*x = a*(a^{-1}*b) = (a*a^{-1})*b = b$. Dermed har vi vist, at $a*x = b$ har 1 og kun 1 løsning, nemlig $x = a^{-1}*b$. Helt analogt vises, at $x*a = b$ har 1 og kun 1 løsning, nemlig $x = b*a^{-1}$.

2) $\Rightarrow$ 3). Det er helt indlysende.

3) $\Rightarrow$ 1). Lad 3 være opfyldt, og lad $a \in M$ være et vilkårligt element. En løsning e til $a*x = a$ til-

fredsstiller, at $a*e = a$. Hvis $b \in M$ er et vilkårligt element, findes der et element y, som tilfredsstiller, at $y*a = b$, men så er $b*e = (y*a)*e = y*(a*e) = y*a = b$. Altså er e et højre neutralelement. Helt analogt finder vi et venstre neutralelement, og af sætning 6.8 følger så, at e er neutralelement. For et vilkårligt $a \in M$ gælder dernæst, at $a*x = e$ og $x*a = e$ har løsninger, så a har både venstre og højre inverst element, altså ifølge sætning 6.10 et inverst element. Dermed er sætningen bevist.

Definition 6.12. En addition på en mængde M er en kompositionsregel, der betegnes med $+$, er associativ og kommutativ og opfylder betingelserne i sætning 6.11.

Betingelsen, at tegnet $+$ skal benyttes, kan selvfølgelig altid opfyldes, hvis tegnet blot er ledigt. Eksempler er den sædvanlige addition på $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ samt $\mathbb{E}^{\nu}$. Men bortset fra tegnet, som ikke er ledigt, er multiplikation på $\mathbb{Q}\setminus\{0\}$, $\mathbb{R}\setminus\{0\}$ og $\mathbb{C}\setminus\{0\}$ ligeledes eksempler på addition. Mængden af bijektive afbildninger $\varphi: M \to M$ med sammensætning som komposition opfylder alle betingelserne i sætning 6.11.

Vi vil nu gå over til at se på mængder med 2 kompositionsregler. Det har vi jo allerede mødt mange eksempler på.

Definition 6.13. Lad $\perp$ og $*$ være kompositionsregler på en mængde M. Vi siger, at $*$ er distributiv med hensyn til $\perp$ hvis vi for alle $a,b,x \in M$ har

$$x*(a\perp b) = (x*a)\perp(x*b);\ (a\perp b)*x = (a*x)\perp(b*x) .$$

Vi siger venstre distributiv, hvis kun den første betingelse er opfyldt og højre distributiv, hvis kun den sidste er opfyldt, men de tilfælde vil vi slet ikke interessere os for. Hvis $*$ er kommutativ, følger hver af de to betingelser af den anden.

Eksempel. Multiplikation er distributiv med hensyn til addition på $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$. Endvidere er vektorproduktet distributivt med hensyn til addition på $\mathbb{E}^3$. Kompositionsreglerne $\cap$ og $\cup$ på mængden $D(M)$ af delmængder af M er distributive med hensyn til hinanden.

I "rigtig" algebra optræder distributivitet mest med hensyn til en addition, og så kommer de sædvanlige regler for multiplikation med 0 til at gælde. Vi vil så kalde den anden kompositionsregel multiplikation og betegne den med en prik, der kan udelades.

Sætning 6.14. Lad M være en mængde med en addition $+$ og en multiplikation $\cdot$, som er distributiv med hensyn til $+$. For alle $x \in M$ gælder da, at $0\cdot x = x\cdot 0 = 0$.

For alle $x,y \in M$ gælder, at $-x\cdot y = x\cdot -y = -(xy)$, og at $-x\cdot -y = xy$.

Bevis. Da vi har $0\cdot x = (0+0)\cdot x = 0\cdot x + 0\cdot x$ og enhver ligning $a+x = b$ har højst 1 løsning, er $0\cdot x = 0$. Analogt fås, at $x\cdot 0 = 0$. Af $-x\cdot y + xy = (-x+x)\cdot y = 0\cdot y = 0$ følger på samme måde, at $-x\cdot y = -(xy)$. Analogt fås, at $x\cdot -y = -(xy)$. Endelig følger heraf, at $-x\cdot -y = -(-(xy)) = xy$. Dermed er sætningen bevist.

Eksempel. På $\mathbb{R}\times\mathbb{R}$ indfører vi + og $\cdot$ ved

$$(x_1,x_2) + (y_1,y_2) = (x_1+y_1, x_2+y_2),$$
$$(x_1,x_2)\cdot(y_1,y_2) = (x_1y_1, x_2y_2).$$

Det ses umiddelbart, at + er en addition med (0,0) som neutralelement, at $\cdot$ er associativ og kommutativ med (1,1) som neutralelement, og at $\cdot$ er distributiv med hensyn til +. Vi bemærker, at $(x,0)\cdot(0,y) = (0,0)$ for alle $x,y \in \mathbb{R}$, så et produkt kan blive 0, selv om ingen af faktorerne er 0. Endvidere ser vi, at + og $\cdot$ ved restriktion giver kompositionsregler på delmængden af elementer $(x,0)$, og at denne delmængde ikke indeholder neutralelementet $(1,1)$, men at $\cdot$ på delmængden alligevel har et neutralelement, nemlig $(1,0)$.

Nu er tiden inde til en oversigt over de vigtigste af de algebraiske strukturer, som kun omfatter interne

kompositionsregler.

Definition 6.15. En mængde med en associativ kompositionsregel med neutralelement kaldes en gruppe, hvis hvert element har et inverst. En gruppe kaldes abelsk eller kommutativ, hvis kompositionsreglen er kommutativ. Kompositionsreglen i en gruppe betegnes oftest med en prik $\cdot$, som kan udelades. I en abelsk gruppe betegner man ofte kompositionsreglen med $+$, neutralelementet med 0, og det inverse element til a med $-a$, således at en abelsk gruppe med disse betegnelser er en mængde med en addition.

Definition 6.16. En mængde med en addition $+$ og en associativ kompositionsregel $\cdot$, som er distributiv med hensyn til $+$, kaldes en ring, og $\cdot$ kaldes multiplikation. En ring kaldes kommutativ, hvis multiplikationen er kommutativ. Et neutralelement for multiplikationen kaldes 1-element, og betegnes med 1, hvis det ikke kan føre til misforståelse.

Definition 6.17. Et element a i en ring Λ kaldes en venstre 0-divisor, hvis der findes et element $x \in \Lambda \setminus \{0\}$, for hvilket $ax = 0$, og a kaldes en højre 0-divisor, hvis der findes et element $y \in \Lambda \setminus \{0\}$, for hvilket $ya = 0$.

Definition 6.18. En kommutativ ring med 1-element og uden 0-divisorer kaldes en integritetsring (mange siger "integritetsområde").

Definition 6.19. Et legeme er en kommutativ ring K, i hvilken enhver ligning $ax = b$ med $a \neq 0$ har 1 og kun 1 løsning. Hvis ringen ikke er kommutativ, medens til gengæld også ligningen $xa = b$ har 1 og kun 1 løsning, kaldes den et ikke kommutativt legeme.

En gruppe kan ikke være tom, da den i det mindste må have neutralelementet som element. En ring kan bestå af 0-elementet alene, men vi burde egentlig have præciseret i definitionen, at vi ikke i sådan en ring vil anerkende 0 som 1-element. En ring med 1-element har derfor mindst 2 elementer.

Eksempel. Hvis en ring kun har elementerne 0 og 1 er både additions- og multiplikationstabellen helt fastlagt. Det er tvunget, at $0 + 0 = 0$, og at $0 + 1 = 1 + 0 = 1$. Da $1 + x = 0$ skal have en løsning påtvinges vi, at $1 + 1 = 0$. På den anden side er det også tvunget, at $0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0$, og at $1 \cdot 1 = 1$. Hvis vi kalder 0 lige og 1 ulige, er disse tabeller netop reglerne for regning med "lige" og "ulige". Vi ser, at ringen endda bliver et legeme. Der findes også en ring med kun 2 ele-

menter, og uden 1-element. I den er alle produkter 0.

Sætning 6.20. Lad a være et element i en ring Λ. Da er følgende 3 egenskaber ensbetydende

1). a er venstre 0-divisor.

2). Der findes et element $b \in \Lambda$, for hvilket ligningen $ax = b$ har mindst 2 løsninger.

3). Der findes intet element $b \in \Lambda$, for hvilket ligningen $ax = b$ har 1 og kun 1 løsning.

Bevis. Først 1) $\Leftrightarrow$ 2). Hvis a er venstre 0-divisor findes $b \neq 0$, så $ab = 0$, og så har $ax = 0$ løsningerne 0 og b. Hvis $ax = b$ har de indbyrdes forskellige løsninger x_1 og x_2 er $a(x_1-x_2) = 0$, så a er venstre 0-divisor.

Dernæst 1) $\Rightarrow$ 3). Hvis a er venstre 0-divisor, findes $c \neq 0$, så $ac = 0$. Hvis $ax = b$ så har løsningen x_1, vil også x_1+c være en løsning.

Endelig 3) $\Rightarrow$ 1). Af 3) følger, at ligningen $ax = 0$ har mindst 2 løsninger, altså mindst 1 fra 0 forskellig løsning, men så er a 0-divisor. Dermed er sætningen bevist.

Eksempler. $\mathbb{Z}$ er en integritetsring, og $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ er legemer. $\mathbb{E}^3$ med vektorprodukt er ikke en ring, da multiplikationen ikke er associativ. Endvidere er $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ og $\mathbb{E}^3$ med addition, samt $\mathbb{Q}\setminus\{0\}$, $\mathbb{R}\setminus\{0\}$, $\mathbb{C}\setminus\{0\}$ med multiplikation abelske grupper. Mængden af bijektive afbildninger $\varphi: M \to M$ med sammensætning som multiplikation er et eksempel på en gruppe, der ikke er abelsk. For et interval I gælder, at mængden af kontinuerte, voksende, bijektive afbildninger $\varphi: I \to I$ med sammensætning som komposition udgør en gruppe, som ikke er abelsk.

Vi nævner endnu engang ganske kort de vigtigste af de ovenfor indførte arter af algebraisk struktur:

Grupper.
Abelske grupper.
Ringe.
Kommutative ringe.
Ringe med 1-element.
Kommutative ringe med 1-element.
Integritetsringe.
Legemer.

For mængder med sådan en algebraisk struktur, kan man undersøge om restriktion af kompositionsreglerne til stabile delmængder fører til, at delmængderne igen får den

betragtede algebraiske struktur. Nu kan en delmængde eventuelt være stabil overfor en kompositionsregel med neutralelement uden at indeholde neutralelementet. Man må også sikre sig eksistens af de inverse, der skal eksistere. For delmængder, der på denne måde arver strukturen, bruger vi betegnelser som undergruppe, delring, delintegritetsring, dellegeme.

Eksempler. For mængderne $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$ gælder, at enhver er undergruppe, delring og delintegritetsområde i den følgende. Bortset fra $\mathbb{Z}$ er de endda dellegemer. De lige tal udgør en delring i ringen $\mathbb{Z}$, men uden 1-elementet.

Det er klart, at associativitet, kommutativitet og distributivitet nedarves helt automatisk til delmængder, så en undergruppe i en abelsk gruppe bliver abelsk.

Den næste sætning kan måske sommetider være nyttig.

Sætning 6.21. Lad M være en mængde med en kompositionsregel $*$ med neutralelement e, for hvilken ethvert element $a \in M$ har en invers a^{-1}. Hvis en ikke tom delmængde $A \subseteq M$ er stabil overfor en kompositionsregel $\perp$ defineret ved $a \perp b = a^{-1} * b$, er A stabil overfor $*$, og A indeholder e og er stabil med hensyn til invers.

Bevis. Af $a,b \in A$ følger $e = a^{-1}*a \in A$, $a^{-1} = a^{-1}*e \in A$ og $a*b = (a^{-1})^{-1}*b \in A$. Dermed er sætningen bevist.

Sammen med mængder med en bestemt algebraisk struktur betragter man også afbildninger af sådanne mængder på hinanden og i harmoni med den algebraiske struktur.

Definition 6.22. Lad M_1 og M_2 være mængder med ensartet algebraisk struktur i den forstand, at hver kompositionsregel i den ene svarer til en bestemt kompositionsregel i den anden, samt at krav om associativitet, kommutativitet, distributivitet, eksistens af neutralelementer og af inverse er helt ens for M_1 og M_2. En afbildning $\varphi: M_1 \to M_2$ kaldes da en homomorfi, hvis det for hver kompositionsregel $*$ på M_1 med tilsvarende $\tilde{*}$ på M_2 for vilkårlige elementer $x,y \in M_1$ gælder, at

$$\varphi(x*y) = \varphi(x) \,\tilde{*}\, \varphi(y) ,$$

og hvis det desuden gælder, at neutralelementer afbildes på neutralelementer. En bijektiv homomorfi kaldes en isomorfi, og M_1 siges at være isomorf med M_2, hvis der findes en isomorfi $\varphi: M_1 \to M_2$. For en enkelt mængde M kaldes en homomorfi $\varphi: M \to M$ også en endomorfi, og en isomorfi $\varphi: M \to M$ kaldes en automorfi.

Det er klart, at disse begreber er relative, idet vi kan se bort fra en del af strukturen. I praksis præciserer man ved at sige "gruppehomomorfi", automorfi på ring med 1-element, ring-endomorfi osv. Vi nævner nogle eksempler.

i. Hvis $n > 1$ er et helt tal, definerer $\varphi(x) = nx$ afbildninger af $\mathbb{Z}$ ind i $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$, og disse er alle gruppehomomorfier med hensyn til addition, men de er ikke ringhomomorfier. Hvis $\mathbb{Z}_2$ er det i eksemplet lige før sætning 6.20 omtalte legeme med 2 elementer, kan en ringhomomorfi $\varphi:\mathbb{Z} \to \mathbb{Z}_2$ defineres ved, at $\varphi(x) = 0$, hvis x er lige, men $\varphi(x) = 1$, hvis x er ulige. Hvis $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$ er en basis for $\mathbb{E}^3$, er den ved $\varphi(x_1\underline{e}_1+x_2\underline{e}_2+x_3\underline{e}_3) = x_1\underline{e}_1+x_2\underline{e}_2$ definerede projektion af $\mathbb{E}^3$ på det af $\underline{e}_1$ og $\underline{e}_2$ udspændte 2-dimensionale vektorrum en gruppehomomorfi. Den ved $\varphi(z) = \overline{z}$ definerede afbildning $\varphi:\mathbb{C} \to \mathbb{C}$ er en legeme-automorfi.

Den følgende sætning sparer en del arbejde.

<u>Sætning</u> 6.23. Lad M_1 og M_2 være mængder med kompositionsregler $*$ og $\tilde{*}$, og lad $\varphi:M_1 \to M_2$ være en homomorfi blot med hensyn til denne struktur. Lad os antage, at det for $\tilde{*}$ gælder, at den har et neutralelement $\tilde{e}$, og at ligninger $a\tilde{*}x = b$ og $x\tilde{*}a = b$ højst har 1

løsning. Da vil et eventuelt neutralelement e for $*$ afbildes på $\tilde{e}$, og hvis et element $a \in M_1$ har et inverst element a^{-1}, har også $\varphi(a)$ et inverst element nemlig $\varphi(a^{-1})$.

Bevis. Da $\varphi(e)\tilde{*}\varphi(e) = \varphi(e*e) = \varphi(e)$, er $\varphi(e) = \tilde{e}$. Endvidere er $\varphi(a)\tilde{*}\varphi(a^{-1}) = \varphi(a*a^{-1}) = \varphi(e) = \tilde{e}$, og analogt fås $\varphi(a^{-1})\tilde{*}\varphi(a) = \tilde{e}$, så $\varphi(a^{-1})$ bliver invers til $\varphi(a)$. Dermed er sætningen bevist.

For at vise, at en afbildning $f:G \to H$, hvor G og H er grupper, er en homomorfi, er det således nok at vise, at $f(xy) = f(x)f(y)$ for alle $x,y \in G$. For at vise, at $f:\Lambda \to \Xi$, hvor Λ og Ξ er ringe, er en ringhomomorfi, er det nok at vise, at $f(x+y) = f(x)+f(y)$, og at $f(y) = f(x)f(y)$. Hvis Λ og Ξ er ringe med 1-element, følger det imidlertid ikke, at f afbilder 1-element på 1-element. Det vil dog være tilfældet, hvis Ξ er en ring uden 0-divisorer.

Eksempel. I eksemplet efter sætning 6.14 optræder en ring Ξ med en delring Λ, og den ved $\varphi(x) = x$ definerede inklusionsafbildning $\varphi:\Lambda \to \Xi$ er en ringhomomorfi, men ikke en homomorfi af ringe med 1-element. Ved $\psi(x_1,x_2) = (x_1,0)$ defineres en ringhomomorfi $\psi:\Xi \to \Lambda$, og den er heller ikke en homomorfi af ringe med 1-element. I øvrigt er $\psi \circ \varphi = \mathrm{id}_\Lambda$.

Sætning 6.24. Hvis M_1, M_2 og M_3 er mængder med algebraiske strukturer af samme slags, og $\varphi: M_1 \to M_2$ og $\psi: M_2 \to M_3$ er homomorfier med hensyn til disse strukturer, da er også $\psi \circ \varphi: M_1 \to M_3$ en homomorfi med hensyn til de samme strukturer.

Bevis. Det er næsten helt indlysende. Lad $*$ være en kompositionsregel på M_1, og lad os for nemheds skyld også betegne de tilsvarende kompositionsregler på M_2 og M_3 med $*$. For $x, y \in M_1$ får vi da $(\psi \circ \varphi)(x*y) = \psi(\varphi(x*y)) = \psi(\varphi(x)*\varphi(y)) = \psi(\varphi(x))*\psi(\varphi(y)) = (\psi \circ \varphi)(x)*(\psi \circ \varphi)(y)$. De andre ting, der skal ses efter, går endnu lettere, og vi vil ikke spilde plads på det.

Sætning 6.25. Hvis M_1 og M_2 er mængder med algebraisk struktur af samme slags, og $\varphi: M_1 \to M_2$ er en isomorfi, da er $\varphi^{-1}: M_2 \to M_1$ ligeledes en isomorfi. Relationen "isomorf med" er en ækvivalensrelation på arten af mængder med den pågældende algebraiske struktur.

Bevis. Lad $*$ være en kompositionsregel på M_1 og $\tilde{*}$ den tilsvarende på M_2. For $x, y \in M_2$ skal vi vise, at $\varphi^{-1}(x)*\varphi^{-1}(y)$ netop er $\varphi^{-1}(x \tilde{*} y)$. Det følger imidlertid af, at φ er bijektiv, og at $\varphi(\varphi^{-1}(x)*\varphi^{-1}(y)) = \varphi(\varphi^{-1}(x)) \tilde{*} \varphi(\varphi^{-1}(y)) = x \tilde{*} y$. At φ^{-1} afbilder neutralelement i neutralelement og invers i invers, hvis φ gør det,

er indlysende. Lad os skrive $\approx$ for "isomorf med". Så er $\approx$ reflexiv, fordi $id_M: M \to M$ er en isomorfi. Den del af sætningen, vi allerede har vist, fortæller, at $\approx$ er symmetrisk, og det følger af sætning 6.24, at $\approx$ er transitiv. Dermed er sætningen bevist.

Indbyrdes isomorfe mængder er fra algebraisk synspunkt nøjagtige kopier af hinanden. De mest velbekendte som $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$ møder vi i mange forklædninger (5, fünf, five, cinq, cinque, V, osv.), og vi føler næppe noget behov for at udnævne en af disse udgaver til den rigtige. Det hænder dog også, at mængder er isomorfe på knap så åbenlys vis. Således får vi for hvert strengt positivt tal $a \neq 1$ ved $\varphi(x) = a^x$ defineret en isomorfi fra den abelske gruppe $\mathbb{R}$ med + til den abelske gruppe af strengt positive tal med multiplikation.

Hvis M er en mængde med en eller anden algebraisk struktur, og A er en vilkårlig mængde, vil en kompositionsregel $*$ på M inducere en kompositionsregel $\overline{*}$ på mængden af afbildninger $f,g: A \to M$, idet vi definerer $(f\overline{*}g)(x) = f(x)*g(x)$ for alle $x \in A$. Det er jo netop sådan, vi adderer og multiplicerer reelle funktioner. Egenskaber som associativitet, kommutativitet og distributivitet overføres på mængden af funktioner. Det samme gælder eksistens af invers, hvis alle elementer i M har

inverse. På den anden side bliver mængden af reelle (kontinuerte) funktioner på et inverval en ring med 0-divisorer, selv om de reelle tal er et legeme.

Sætning 6.26. Lad G være en abelsk gruppe og H en gruppe. Mængden af homomorfier $\varphi,\psi:H \to G$ udgør da en abelsk gruppe, en undergruppe i mængden af afbildninger af H ind i G.

Bevis. Vi skriver kompositionsreglen i G med +, men i H med $\cdot$. Vi skal blot for homomorfierne φ og ψ vise, at $\varphi-\psi$ er en homomorfi, og så følger resten af sætning 6.21. Vi får

$$(\varphi-\psi)(xy) = \varphi(xy)-\psi(xy) = \varphi(x)+\varphi(y)-(\psi(x)+\psi(y)) =$$
$$(\varphi(x)-\psi(x)) + (\varphi(y)-\psi(y)) = (\varphi-\psi)(x) + (\varphi-\psi)(y).$$

Dermed er sætningen bevist.

Det tredie lighedstegn beror på, at + er kommutativ, og uden kommutativitet bliver sætningen åbenbart forkert.

Sætning 6.27. Mængden $\mathrm{End}G$ af endomorfier på en abelsk gruppe G er en ring med addition induceret af additionen i G og med sammensætning som multiplikation.

Bevis. Af sætning 6.26 fremgår, at additionen på G inducerer en addition på $\mathrm{End}G$. Vi ved allerede, at

sammensætning af endomorfier er associativ, så vi mangler kun at vise de distributive love, altså at vi for endomorfier $\varphi_1, \varphi_2, \psi : G \to G$ har, at $\psi \circ (\varphi_1 + \varphi_2) = (\psi \circ \varphi_1) + (\psi \circ \varphi_2)$ og $(\varphi_1 + \varphi_2) \circ \psi = (\varphi_1 \circ \psi) + (\varphi_2 \circ \psi)$. Vi prøver efter med et element $x \in G$ og får

$$(\psi \circ (\varphi_1 + \varphi_2))(x) = \psi((\varphi_1 + \varphi_2)(x)) = \psi(\varphi_1(x) + \varphi_2(x)) =$$
$$\psi(\varphi_1(x)) + \psi(\varphi_2(x)) = (\psi \circ \varphi_1)(x) + (\psi \circ \varphi_2)(x) = ((\psi \circ \varphi_1) + (\psi \circ \varphi_2))(x)$$

og

$$((\varphi_1 + \varphi_2) \circ \psi)(x) = (\varphi_1 + \varphi_2)(\psi(x)) = \varphi_1(\psi(x)) + \varphi_2(\psi(x)) =$$
$$(\varphi_1 \circ \psi)(x) + (\varphi_2 \circ \psi)(x) = ((\varphi_1 \circ \psi) + (\varphi_2 \circ \psi))(x).$$

Dermed er sætningen bevist.

Eksempel. Mængden $C(\mathbb{R})$ af kontinuerte afbildninger $\mathbb{R} \to \mathbb{R}$ er en "dobbeltring" med en addition og to multiplikationer. Additionen og den ene multiplikation er induceret af addition og multiplikation på $\mathbb{R}$, og de giver en kommutativ ring med 1-element og med 0-divisorer. Den anden multiplikation er sammensætning af afbildninger, og den giver en ikke kommutativ ring med 1-element og med 0-divisorer. Desuden er den sidste multiplikation højre distributiv med hensyn til den første.

Definition 6.28. Ved en extern kompositionsregel mellem en mængde Ω og en mængde M forstås en afbild-

ning $\nu:\Omega\times M \to M$. Vi skriver $\nu(\omega,x) = \omega x$, eventuelt $\omega(x)$, $(\omega)x$ eller $(\omega)(x)$ for at undgå misforståelser.

Eksempel. På $\mathbb{E}^\nu$ er en extern kompositionsregel $\nu:\mathbb{R}\times\mathbb{E}^\nu \to \mathbb{E}^\nu$ defineret ved $\nu(\lambda,\underline{u}) = \lambda\underline{u}$. På mængden $C(\mathbb{R})$ af kontinuerte afbildninger $\varphi:\mathbb{R} \to \mathbb{R}$ defineres en extern kompositionsregel mellem $\mathbb{R}$ og $C(\mathbb{R})$ ved $(\lambda\varphi)(x) = \lambda\varphi(x)$. På mængden $V(E^3)$ af vektorfelter $\underline{f}:E^3 \to \mathbb{E}^3$ har vi en extern kompositionsregel mellem mængden $C(E^3)$ af kontinuerte funktioner $\varphi:E^3 \to \mathbb{R}$ og $V(E^3)$ defineret ved, at $\varphi\underline{f}(x) = \varphi(x)\underline{f}(x)$.

Definition 6.29. Ved en modul G over en kommutativ ring Λ forstås en abelsk gruppe G (kompositionsregel +) med en extern kompositionsregel mellem Λ og G, således at følgende betingelser er opfyldt

1). For alle $\lambda \in \Lambda$; $g_1,g_2 \in G$ er $\lambda(g_1+g_2)=\lambda g_1+\lambda g_2$

2). For alle $\lambda_1,\lambda_2 \in \Lambda$; $g \in G$ er $(\lambda_1+\lambda_2)g = \lambda_1 g+\lambda_2 g$ og $(\lambda_1\lambda_2)g = \lambda_1(\lambda_2 g)$.

Modulen kaldes unitær, hvis Λ har et 1-element, som tilfredsstiller at $1g = g$ for alle $g \in G$. Modulen kaldes et vektorrum over Λ, hvis det yderligere gælder, at Λ er et legeme.

Eksempler. For $\nu = 1,2,3$ er $\mathbb{E}^\nu$ et vektorrum over $\mathbb{R}$. For enhver mængde M gælder, at mængden af funktioner $f:M \to \mathbb{R}$ er et vektorrum over $\mathbb{R}$, idet additionen er den sædvanlige addition af funktioner, og den externe multiplikation er sædvanlig multiplikation med reelt tal. Tilsvarende får vi vektorrum af begrænsede funktioner, af differentiable funktioner, af vilkårlig ofte differentiable funktioner etc. For $M = \mathbb{N}$ for vi vektorrum af talfølger, af begrænsede talfølger, af konvergente talfølger etc. For et legeme L med et dellegeme K gælder, at L er et vektorrum over K med sædvanlig addition og multiplikation. Mængden $\mathbb{V}(E^3)$ af vektorfelter $f:E^3 \to \mathbb{E}^3$ er ligeledes et vektorrum over $\mathbb{R}$, men med den externe komposition, der omtaltes lige før definition 6.29 er den en modul over ringen $C(E^3)$ af reelle funktioner.

Definition 6.30. Lad G være en gruppe med kompositionsregel $\cdot$. For $g \in G$ betegner vi et produkt $gg...g$ med n faktorer som g^n, og desuden skriver vi $g^1 = g$ og $g^0 = e$ (neutralelementet). Endelig skriver vi g^{-n} for $(g^{-1})^n$. Hvis G er en abelsk gruppe med $+$ skriver vi ng i stedet for g^n for alle $n \in \mathbb{Z}$.

Sætning 6.31. En abelsk gruppe G er en modul over $\mathbb{Z}$ med det i definition 6.30 indførte produkt ng.

Bevis. For $n > 0$ har vi

$$n(g_1+g_2)=(g_1+g_2)+\ldots+(g_1+g_2)=(g_1+\ldots+g_1)+(g_2+\ldots+g_2)=$$
$$ng_1 + ng_2 ,$$

og

$$-n(g_1+g_2)=n(-(g_1+g_2))=n(-g_1-g_2)=n\cdot -g_1+n\cdot -g_2=-ng_1-ng_2 .$$

De andre regneregler vises lige så let.

Vi skal ikke beskæftige os med moduler, men de optræder ret hyppigt i teorien for vektorrum, og når de optræder, vil vi henlede opmærksomheden på dem.

Vi møder oven i købet også eksempler på moduler over en ikke kommutativ ring Λ. Vi får da to slags, venstre-moduler, der er præcis som definerede i definition 6.29, og højre-moduler, der afviger ved at den sidste af betingelserne 2) skal ændres til $\lambda_1(\lambda_2 g) = (\lambda_2\lambda_1)g$. For højre-moduler foretrækker vi at skrive det ydre produkt $g\lambda$, så reglen bliver $(g\lambda_2)\lambda_1 = g(\lambda_2\lambda_1)$, hvilket falder mere naturligt.

Eksempel. For abelske grupper G og H har vi mængden $\mathrm{Hom}(G,H)$ af homomorfier $f:G \to H$, og denne mængde er en abelsk gruppe. Vi har også ringen $\mathrm{End}G$ af endomorfier $\varphi:G \to G$ og ringen $\mathrm{End}H$ af endomorfier $\psi:H \to H$.

Det er let at se, at $\mathrm{Hom}(G,H)$ er en venstre-modul over $\mathrm{End}H$ med ydre komposition $\psi \circ f$ og højre-modul over $\mathrm{End}G$ med komposition $f \circ \varphi$. De to kompositioner "kommuterer", idet associativiteten $(\psi \circ f) \circ \varphi = \psi \circ (f \circ \varphi)$ udtrykker, at det er ligegyldigt, hvilken af de externe multiplikationer, der udføres først.

En delmodul af en Λ-modul G over en ring Λ er en undergruppe H i den abelske gruppe G med den egenskab, at det for $\lambda \in \Lambda$, $x \in H$ gælder, at $\lambda x \in H$. Dette kan også skrives $\Lambda H \subseteq H$. For hvert element $g \in G$ bliver $\Lambda g = \{\lambda g \mid \lambda \in \Lambda\}$ en delmodul af G. En delmodul af et vektorrum kaldes et underrum.

Definition 6.32. Lad G og H være moduler over samme ring Λ. En Λ-homomorfi $f:G \to H$ er en gruppehomomorfi, som for alle $\lambda \in \Lambda$, $g \in G$ tilfredsstiller betingelsen $f(\lambda g) = \lambda f(g)$. Specielt taler vi om Λ-isomorfi, Λ-endomorfi og Λ-automorfi. Hvis G og H er vektorrum over samme legeme K, kaldes en K-homomorfi en K-linear afbildning. Derimod bruges K-isomorfi, K-endomorfi, K-automorfi også for vektorrum. Vi udelader K i betegnelserne, når det ikke kan føre til misforståelser. I stedet for K-isomorfi siger vi ofte vektorrumsisomorfi.

ØVELSER TIL KAPITEL 6

Stikordsliste til brug ved indlæring.

Intern og extern kompositionsregel, induceret kompositionsregel på mængder af delmængder, associativ, kommutativ, distributiv, neutralelement og inverst element, venstre, højre, ring, gruppe, modul, vektorrum, addition, regning med 0, 0-divisor, legeme, integritetsring, 1-elementer, stabil delmængde, undergruppe, delring, delmodul, dellegeme, homomorfi, isomorfi, endomorfi, automorfi, tabel, abelsk gruppe som modul over $\mathbb{Z}$, grupper af homomorfier og ringe af endomorfier, unitær modul.

6.1. Lad M være en mængde. For delmængder A og B definerer vi $A*B$ som foreningsmængden $A \cup B$, hvis A og B er disjunkte, men ellers som M. Vis, at $*$ er en associativ kompositionsregel.

6.2. For par $(a,x),(b,y)$ af positive reelle tal definerer vi $(a,x)*(b,y) = (a+b,(a+b)^{-1}(ax+by))$. Vis, at $*$ er en associativ og kommutativ kompositionsregel.

6.2.1. Vis, at $\mathbb{Q}$ er stabil for $*$.

6.2.2. Er det muligt for et givet par (a,x) at vælge (b,y), således at $(a,x)*(b,y) = (2a,2x)$?

6.3. Lad M være en mængde med en kompositionsregel $*$. Vi siger, at den associative lov gælder for et element $x \in M$, hvis det for alle $y,z \in M$ gælder, at $(x*y)*z = x*(y*z)$. Vis, at mængden $A \subseteq M$ af elementer, for hvilke den associative lov gælder, er stabil, og at $*$ er associativ på A.

6.4. Lad M være en mængde med en associativ kompositionsregel $*$, og lad a og b være elementer af M. Vis, at delmængderne $a*M$, $M*b$, $a*M*b$ og $M*a*M$ er stabile.

6.4.1. Lad $A \subseteq M$ og $B \subseteq M$ være stabile delmængder, som tilfredsstiller betingelsen $B*A \subseteq A*B$. Vis, at $A*B$ er stabil.

6.5. På mængden af tripler (a_0,a_1,a_2), (b_0,b_1,b_2),... af komplekse tal indføres en kompositionsregel defineret ved

$$(a_0,a_1,a_2)\ (b_0,b_1,b_2) =$$
$$(a_0+b_0,\ a_1+2a_0b_0+b_1,\ a_2+2a_1b_0+a_0^2b_0+3a_0b+b_2).$$

Vis, at mængden af tripler derved bliver en (ikke abelsk) gruppe (det giver en del regnearbejde).

6.5.1. Undersøg om triplerne af hele tal (rationale tal, lige tal) udgør en undergruppe.

6.5.2. Vis, at triplerne med 0 som sidste element udgør en abelsk undergruppe.

6.5.3. Gruppen i 6.5 udvides til kvadrupler, idet produktet defineres som i 6.5 for de tre første pladsers vedkommende, medens der på fjerde plads skal anbringes

$$a_3+2a_2b_0+2a_0a_1b_0+3a_0^2b_1+3a_1b_1+4a_0b_2+b_3\ .$$

Det bliver dog besværligt at eftervise den associative lov. I øvrigt kan man også udvide til quintupler, men det bliver endnu besværligere.

6.6. Lad M være en mængde af tegn, som kan skrives på papiret, f.eks. det danske alfabet. Lad S være mængden af symbolstrenge, dvs. endelige kæder af tegn sat lige efter hinanden. Matematiken plejer at kalde dem "ord", og det vil vi også gøre her. To ord A og B kan sættes sammen til et ord $AB \in S$,

og derved defineres en kompositionsregel på S. Den er associativ, men ikke kommutativ, og der gælder forkortningsregler $AB = AB_1 \Rightarrow B = B_1$ og $AB = A_1B \Rightarrow A = A_1$. Den tomme symbolstreng kan inkluderes i S som neutralelement. En ligning $AX = B$ har højst 1 løsning, men for det meste ingen løsning.

6.6.1. Vi supplerer M med endnu en mængde M' af præcis lige så mange symboler, samt en bijektiv afbildning $\varphi: M \to M'$. For $x \in M$ skriver vi $x^{-1} = \varphi(x)$. Vi får nu en mængde T af ord dannet af symboler fra $M \cup M'$. Vi vil nu indføre en reduktionsproces for ord fra T, idet vi vedtager, at et $x \in M$ og et $x^{-1} \in M'$ må slettes, hvis de følger lige efter hinanden, uanset hvilket der kommer først og uanset hvad der kommer foran eller følger efter. Et ord er reduceret, når der slet ikke findes kombinationer som aa^{-1} eller $x^{-1}x$ i det. Vis, at hvert ord reduceres til et ganske bestemt reduceret ord uafhængigt af reduktionsprocessens forløb. Det reducerede ord kan eventuelt være tomt.

6.6.2. Vis, at kompositionsreglen fra 6.6 inducerer en kompositionsregel på mængden G af reducerede ord i 6.6.1., og at G med denne kompositionsregel er en gruppe.

6.6.3. Vi danner som beskrevet i opgavens foregående afsnit en gruppe G ud fra mængden $\{a,b\}$ af symboler. Endvidere danner vi på samme måde en gruppe H ud fra mængden $\{x,y,z\}$ af symboler. Vis (det er ikke spor svært), at der findes en og kun en homomorfi $\varphi: H \to G$ med $\varphi(x) = b$, $\varphi(y) = aba^{-1}$ og $\varphi(z) = aaba^{-1}a^{-1}$.

6.6.4. Vis, at den således definerede homomorfi er injektiv. Den er vel ikke en isomorfi?

6.7. Vis, at mængden $\{x+y\sqrt{2} \mid x,y \in \mathbb{Q}\}$ er et dellegeme af $\mathbb{R}$.

6.7.1. Vis, at mængden $\{x+iy\sqrt{3} \mid x,y \in \mathbb{Q}\}$ er et dellegeme af $\mathbb{C}$.

6.8. Lad r være et positivt tal og θ et reelt tal. Vis, at der ved $\varphi(x) = r^x(\cos \theta x + i \sin \theta x)$ defineres en homomorfi af $\mathbb{R}$ med + ind i $\mathbb{C}$ med multiplikation. For hvilke valg af r og θ er φ injektiv.

6.9. Lad M være en mængde med en addition + og med endnu en kompositionsregel *, der er distributiv med hensyn til +. Vis ved et eksempel, at de di-

stributive love ikke behøver at gælde for de inducerede kompositionsregler på mængden af delmængder af M. Det er fornuftigt at vælge $M = \mathbb{Z}$ og forsøge med delmængder med 2 elementer i hver.

6.10. Lad $a \in \mathbb{Z}$ være givet. Vis, at der findes netop 1 kompositionsregel $*$ på $\mathbb{Z}$, som er distributiv med hensyn til $+$ og tilfredsstiller, at $1*1 = a$. For hvilke valg af a er $\mathbb{Z}$ med $+$ og $*$ en ring med 1-element.

6.11. Angiv alle ringhomomorfier $\varphi:\mathbb{Z} \to \mathbb{C}$.

6.12. Vis, at der ved $\varphi(x+y\sqrt{2}) = x-y\sqrt{2}$ defineres en ringhomomorfi af det i opgave 6.7 omtalte dellegeme af $\mathbb{R}$ på sig selv. Heraf følger, at et trediegradspolynomium med rationale koefficienter, der har et af tallene $x+y\sqrt{2}$, $x,y \in \mathbb{Q}$ som rod, også har $x-y\sqrt{2}$ som rod, og da røddernes sum er rational, bliver den tredie rod rational.

6.13. Lad M være en mængde med en associativ kompositionsregel $\perp$, samt en kompositionsregel $*$, der er distributiv med hensyn til $\perp$. Et element $a \in M$ kaldes regulært, hvis $a\perp x = a\perp y \Rightarrow x = y$ for alle $x,y \in M$. Lad nu $u,v,x,y \in M$ være ele-

menter, for hvilke $u*v$ og $x*y$ er regulære. Vis, at $(u*y)\perp(x*v) = (x*v)\perp(u*y)$. Idet det yderligere antages, at der findes et neutralelement for $*$, skal det vises, at det for regulære elementer x og y gælder, at $x*y = y*x$.

6.14. Lad G være mængden af kontinuerte funktioner $f:[0,1] \to \mathbb{R}$, som tilfredsstiller følgende betingelser: Der findes et interval med midtpunkt i $\frac{1}{2}$, i hvilket f har en kontinuert differentialkvotient. Desuden er $f(\frac{1}{2}) = f'(\frac{1}{2}) = 0$ og $f(1) = 2f(0)$. Lad Λ være mængden af kontinuerte funktioner $\gamma:[0,1] \to \mathbb{R}$, som har kontinuert differentialkvotient på hele $[0,1]$ og tilfredsstiller, at $\gamma(0) = \gamma(1)$. Vis, at Λ med sædvanlig addition og multiplikation er en ring, medens G med sædvanlig addition og multiplikation er en Λ-modul, men ikke en ring.

6.15. Vis, at mængden $\{a\cos(x+\theta) \mid a,\theta \in \mathbb{R}\}$ af periodiske funktioner er et vektorrum over $\mathbb{R}$ med sædvanlig addition og multiplikation.

KAPITEL 7

Grupper og permutationer.

I dette kapitel skal vi se lidt nærmere på gruppeteori, og specielt skal vi interessere os for grupper af permutationer, dvs. bijektive afbildninger af en endelig mængde på sig selv. Disse grupper spiller en ganske væsentlig rolle i teorien for lineære ligninger, som skal omtales i et senere kapitel.

Vi minder om, at en gruppe G er en mængde med en associativ kompositionsregel med neutralelement e, og med den egenskab, at alle elementer har inverse. Kompositionsreglen skrives som en multiplikation, men hvis kompositionsreglen er kommutativ kaldes gruppen abelsk, og så kan kompositionsreglen eventuelt skrives additivt.

For at sikre, at en mængde G med en associativ kompositionsregel er en gruppe, er det (sætning 6.11) nok at vise, at enhver ligning $ax = b$ og $xa = b$ har en løsning, og så har de kun 1 løsning.

En undergruppe i en gruppe G er en delmængde $H \subseteq G$, der med restriktionen af kompositionsreglen på

G er en gruppe, og det gælder (sætning 6.21), hvis det for alle $a,b \in H$ gælder, at $a^{-1}b \in H$. Vi skal nu vise et par meget simple sætninger om undergrupper.

Sætning 7.1. For en vilkårlig mængde $\{H_j | j \in J\}$ af undergrupper H_j i en gruppe G gælder, at fællesmængden $\bigcap_{j\in J} H_j = H$ er en undergruppe i G.

Bevis. Det er næsten helt trivielt. Af $a,b \in H$ følger $a,b \in H_j$ for alle $j \in J$, altså $a^{-1}b \in H_j$ for alle j, altså $a^{-1}b \in H$. Dermed er sætningen bevist.

Sætning 7.2. Lad G være en gruppe, og $A \subseteq G$ en vilkårlig mængde. Der findes da en undergruppe $H \subseteq G$, som indeholder A, men er indeholdt i enhver anden undergruppe, der indeholder A. Undergruppen H er således den mindste undergruppe, der indeholder A.

Bevis. Fællesmængden af alle undergrupper, der indeholder A er en undergruppe, der indeholder A, og den er indeholdt i enhver undergruppe, som indeholder A. Dermed er sætningen bevist.

Defintion 7.3. Den i sætning 7.2 omtalte undergruppe H kaldes den af A frembragte undergruppe. Hvis $H = G$,

siger vi, at A frembringer G.

Definition 7.4. Lad H være en undergruppe i en gruppe G. For $g \in G$ kaldes $gH = \{gh \mid h \in H\}$ en venstre sideklasse til H, og Hg kaldes en højre sideklasse til H.

Sætning 7.5. Lad H være en undergruppe i en gruppe G. De venstre sideklasser til H udgør en klasseinddeling af G, og de højre sideklasser til H udgør ligeledes en klasseinddeling af G.

Bevis. Vi definerer en relation $\equiv$ mellem elementer af G ved at $x \equiv y$ skal betyde $x \in yH$. Da $e \in H$ gælder $x = xe \in xH$, så $\equiv$ er refleksiv. Endvidere er $x \in yH$ ensbetydende med $y^{-1}x \in H$, og deraf følger $x^{-1}y = (y^{-1}x)^{-1} \in H$, så $\equiv$ er symmetrisk. At $x \equiv y$ og $y \equiv z$ betyder, at $y^{-1}x \in H$ og $z^{-1}y \in H$, altså $z^{-1}x = z^{-1}yy^{-1}x \in H$, så vi får $x \equiv z$. Altså er $\equiv$ transitiv. Ækvivalensrelationen $\equiv$ giver en inddeling i ækvivalensklasser. Alle elementer i xH er ækvivalente med x, så xH er indeholdt i en ækvivalensklasse. På den anden side er alle elementer, som er ækvivalente med x, elementer af xH, så xH er netop en ækvivalensklasse. Dermed har vi vist påstanden om venstre sideklasse. Påstanden om højre sideklasser vises analogt.

Sætning 7.6. Lad H være en undergruppe i en gruppe G, og lad $a \in G$ være et vilkårligt element. Den ved $\varphi(x) = ax$ bestemte afbildning $\varphi: G \to G$ vil afbilde den venstre sideklasse gH bijektivt på den venstre sideklasse agH, og derved inducere en bijektiv afbildning af mængden af venstre sideklasser på sig selv. Analogt vil den ved $\psi(x) = xa$ definerede afbildning $\psi: G \to G$ afbilde hver højre sideklase bijektivt på en anden og derved inducere en bijektiv afbildning af mængden af højre sideklasser på sig selv.

Bevis. Da ligningen $ax = b$ har 1 og kun 1 løsning, er φ bijektiv. Et element af gH har formen gh, $h \in H$, og vi får $\varphi(gh) = agh \in agH$. Altså afbilder φ sideklassen gH injektivt i agH. Nu er $\varphi^{-1}: G \to G$ givet ved $\varphi^{-1}(x) = a^{-1}x$, og φ^{-1} afbilder derfor agH ind i gH. Altså afbildes gH bijektivt på agH ved φ. Deraf følger, at φ inducerer en afbildning $\tilde{\varphi}$ af mængden af venstre sideklasser til H ind i sig selv. Det ses umiddelbart, at φ^{-1} inducerer en afbildning invers til $\tilde{\varphi}$. Derfor er $\tilde{\varphi}$ bijektiv, og dermed er sætningen bevist.

Nu skal vi se lidt på antal i forbindelse med grupper. De antal, der omtales i den næste definition, kan selvfølgelig være ∞, og så er sagen ikke frygtelig interessant.

Definition 7.7. Antallet af elementer i en gruppe G kaldes gruppens orden. Ordenen af et element $g \in G$ er ordenen af den af $\{g\}$ frembragte undergruppe. Index af en undergruppe $H \subseteq G$ er antallet af venstre sideklasser til H.

Sætning 7.8. En gruppe G med en undergruppe H har endelig orden $n(G)$, hvis og kun hvis H har både endelig orden $n(H)$ og endelig index index H, og hvis dette er opfyldt, er $n(G) = n(H)$ index H.

Bevis. Hvis $n(G)$ er endelig er $n(H)$ og index H selvfølgelig også endelige og $\leq n(G)$. Hvis $n(H)$ er endelig har hver sideklasse til H ifølge sætning 7.6 også $n(H)$ elementer, så hvis index H er endelig bliver det samlede antal elementer netop $n(H)$ index H. Dermed er sætningen bevist.

Vi minder om, at en homomorfi $\varphi: G_1 \to G_2$, hvor G_1 og G_2 er grupper, er en afbildning, som for alle $x,y \in G$ tilfredsstiller at $\varphi(xy) = \varphi(x)\varphi(y)$, og at det så også vil gælde (sætning 6.23), at $\varphi(e) = e$ og at $\varphi(x^{-1}) = (\varphi(x))^{-1}$. Alt dette må omformuleres en smule, hvis en af grupperne eller begge skrives additivt. Vi viser en næsten helt triviel sætning, der også gælder for andre algebraiske strukturer.

Sætning 7.9. Lad G_1 og G_2 være grupper, $H_1 \subseteq G_1$ og $H_2 \subseteq G_2$ undergrupper og $\varphi: G_1 \to G_2$ en homomorfi. Da er $\varphi(H_1) \subseteq G_2$ og $\varphi^{-1}(H_2) \subseteq G_1$ undergrupper.

Bevis. Af $x_2, y_2 \in \varphi(H_1)$ følger, at der findes $x_1, y_1 \in H_1$ med $\varphi(x_1) = x_2$ og $\varphi(y_1) = y_2$. Så er $x_1 y_1^{-1} \in H_1$ og $x_2 y_2^{-1} = \varphi(x_1 y_1^{-1}) \in \varphi(H_1)$, og det viser, at $\varphi(H_1)$ er en undergruppe. Af $x_1, y_1 \in \varphi^{-1}(H_2)$ følger $\varphi(x_1), \varphi(y_1) \in H_2$, altså $\varphi(x_1 y_1^{-1}) = \varphi(x_1)\varphi(y_1)^{-1} \in H_2$, altså $x_1 y_1^{-1} \in \varphi^{-1}(H_2)$, og det viser, at $\varphi^{-1}(H_2)$ er en undergruppe. Dermed er sætningen bevist.

Specielt er $\{e\} \subseteq G_2$ en undergruppe, så $\varphi^{-1}(e)$ bliver en undergruppe i G_1, ligesom $\varphi(G_1)$ er en undergruppe i G_2.

Definition 7.10. Lad G_1 og G_2 være grupper og $\varphi: G_1 \to G_2$ en homomorfi. Billedet $\varphi(G_1)$ ved φ betegnes da også im φ (im = image), og $\varphi^{-1}(e)$ (eller $\varphi^{-1}(0)$ hvis G_2 er en gruppe med +) kaldes kernen for φ og betegnes også kern φ.

Det er på forhånd klart, at enhver undergruppe i en gruppe G kan være billede ved en homomorfi, nemlig i hvert fald for inklusionsafbildningen af undergruppen

i G. Hvis G er en ikke abelsk gruppe, viser det sig til gengæld, at en undergruppe må være i besiddelse af en særlig egenskab for at kunne være kerne for en homomorfi. Dette fremgår af den følgende definition og de to påfølgende sætninger.

Definition 7.11. En undergruppe H i en gruppe G kaldes normal (eller invariant), hvis det for alle $x \in G$ gælder, at $xHx^{-1} = H$, altså at $xH = Hx$, så de venstre sideklasser er identiske med de højre. Mængden af sideklasser til H betegnes så $\frac{G}{H}$ og kaldes den til H svarende faktorgruppe (det vil fremgå af den næste sætning, at der induceres en gruppestruktur på $\frac{G}{H}$).

Undergrupper i en abelsk gruppe er således altid normale. En undergruppe H med index 2 er normal, da vi for $a \in G \setminus H$ har $aH = Ha = G \setminus H$, idet der blot er sideklassen H og 1 sideklasse til.

Sætning 7.12. Lad H være en normal undergruppe i en gruppe G. Ved $(xH)(yH) = xyH$ defineres da en kompositionsregel på $\frac{G}{H}$, som derved bliver en gruppe. Den ved $k(x) = xH$ definerede kanoniske afbildning $k: G \to \frac{G}{H}$ er en surjektiv homomorfi med kerne H.

Bevis. Da vi har $(xH)(yH) = x(Hy)H = x(yH)H = (xy)(HH) = xyH$, er kompositionsreglen veldefineret og associativ.

Vi ser, at H bliver neutralelement og $x^{-1}H$ invers til xH. Altså er $\frac{G}{H}$ en gruppe. Endvidere får vi $k(xy) = xyH = (xH)(yH) = k(x)k(y)$, så k er en homomorfi.

Sætning 7.13. Lad G_1 og G_2 være grupper og $\varphi: G_1 \to G_2$ en homomorfi. Da er $\text{kern}\varphi$ en normal undergruppe i G_1, og hvis vi for $x \in G_1$ har $\varphi(x) = y$, er $\varphi^{-1}(y)$ sideklassen x kern φ. Ved $\tilde{\varphi}(x\text{kern}\varphi) = \varphi(x)$ defineres en isomorfi $\tilde{\varphi}: \frac{G_1}{\text{kern}\varphi} \to \text{im}\varphi$, og φ er identisk med den sammensatte afbildning

$$G_1 \xrightarrow{k} \frac{G_1}{\text{kern}\varphi} \xrightarrow{\tilde{\varphi}} \text{im}\varphi \xrightarrow{j} G_2 ,$$

hvor k er den kanoniske afbildning, og j er inklusionsafbildningen.

Bevis. Vi ved allerede, at $H = \text{kern}\varphi$ er en undergruppe i G_1. For $x \in G_1$, $a \in \text{kern}\varphi$ får vi $\varphi(xax^{-1}) = \varphi(x)\varphi(a)\varphi(x^{-1}) = \varphi(x)e(\varphi(x))^{-1} = e$, altså $xax^{-1} \in \text{kern}\varphi$. Heraf følger, at $xHx^{-1} \subseteq H$ for ethvert $x \in H$, men så gælder også $x^{-1}Hx \subseteq H$, altså $H \subseteq xHx^{-1}$, så vi får $xHx^{-1} = H$. Dermed har vi vist, at $\text{kern}\varphi$ er normal. Af $\varphi(x) = y$, $a \in \text{kern}\varphi$ følger $\varphi(xa) = \varphi(x)\varphi(a) = \varphi(x)e = y$, altså $xa \in \varphi^{-1}(y)$. Dermed har vi vist, at $x\text{kern}\varphi \subseteq \varphi^{-1}(y)$. Hvis også $z \in \varphi^{-1}(y)$, er $\varphi(z) = y$ og $\varphi(x^{-1}z) = y^{-1}y = e$, altså $x^{-1}z \in \text{kern}\varphi$, $z \in x\text{kern}\varphi$.

Dermed har vi vist, at $x\text{kern}\varphi = \varphi^{-1}(y)$. Det følger nu, at $\tilde{\varphi}$ er veldefineret og injektiv, og da det er klart på forhånd, at $\tilde{\varphi}$ er surjektiv, er $\tilde{\varphi}$ bijektiv. De øvrige påstande er helt indlysende. Dermed er sætningen bevist.

Vi går nu over til at studere de simpleste grupper. Aller simplest er den trivielle gruppe, som har neutralelementet som eneste element. De næstsimpleste indføres i den næste definition.

Definition 7.14. En ikke triviel gruppe kaldes cyklisk, når den kan frembringes af 1 element.

Sætning 7.15. En cyklisk gruppe er isomorf med en faktorgruppe svarende til en undergruppe i $\mathbb{Z}$.

Bevis. Lad G være en cyklisk gruppe frembragt af et element a. Vi definerer en afbildning $\varphi:\mathbb{Z} \to G$ ved $\varphi(n) = a^n$ (se definition 6.30). Så bliver φ en homomorfi, da vi har $\varphi(n_1+n_2) = a^{n_1+n_2} = a^{n_1}a^{n_2} = \varphi(n_1)\varphi(n_2)$. Da $\text{im}\varphi$ bliver en undergruppe, der indeholder a, bliver φ surjektiv. Men så fortæller sætning 7.14, at G er isomorf med $\frac{\mathbb{Z}}{\text{kern}\varphi}$, altså med faktorgruppen svarende til undergruppen $\text{kern}\varphi \subseteq \mathbb{Z}$. Dermed er sætningen bevist.

Sætning 7.16. Undergrupperne i $\mathbb{Z}$ er $n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ for $n = 0,1,\ldots$.

Bevis. For $n = 0$ fås den trivielle undergruppe $\{0\}$, og for $n = 1$ fås $\mathbb{Z}$ selv. Da $\mathbb{Z}$ frembringes af $\{1\}$, må enhver anden undergruppe have et mindste positivt element $n>1$, og så indeholder den undergruppen $n\mathbb{Z}$. Hvis undergruppen også indeholder et element $a \in \mathbb{Z} \setminus n\mathbb{Z}$, kan vi finde et helt tal x, så $nx < a < n(x+1)$. Men så er $a-nx$ element af gruppen, og da $0 < a-nx < n$, strider det mod, at n var det mindste positive element i undergruppen. Altså er undergruppen netop $n\mathbb{Z}$.

Sætning 7.17. Enhver uendelig cyklisk gruppe er isomorf med $\mathbb{Z}$. For ethvert naturligt tal $n > 1$ findes der cykliske grupper af orden n, og de er alle isomorfe med $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Bevis. Det følger umiddelbart af sætningerne 7.15-7.16.

Den cykliske gruppe $\frac{\mathbb{Z}}{n\mathbb{Z}}$ har som elementer sideklasserne $p+n\mathbb{Z}$, $p = 0,1,\ldots,n-1$. Vi kan mærke dem med disse p på hinanden følgende naturlige tal, og så adderes de ved addition af disse tal, idet eventuelle for store tal erstattes med deres rest ved division med p. Gruppen $\frac{\mathbb{Z}}{n\mathbb{Z}}$ er isomorf med gruppen af n^{te} enhedsrødder

$$e^{\frac{p}{n}\cdot 2\pi i} = \cos\frac{2\pi p}{n} + i \sin\frac{2\pi p}{n}, \quad p = 0,1,\ldots,n-1$$

med multiplikation som kompositionsregel. For ethvert komplekst tal z, der hverken er 0 eller enhedsrod, er $\{z^n | n \in \mathbb{Z}\}$ med multiplikation en uendelig cyklisk gruppe.

Vi bemærker, at cykliske grupper er abelske.

Sætning 7.18. En gruppe, hvis orden er et primtal p, er cyklisk.

Bevis. Da ordenen er mindst 2, indeholder gruppen mindst 1 element a forskelligt fra enhedselementet, og $\{a\}$ frembringer en undergruppe, som er cyklisk. Ifølge sætning 7.8 er denne undergruppes orden en divisor i p, altså p, da p er et primtal. Så er hele gruppen identisk med den af $\{a\}$ frembragte cykliske undergruppe, og dermed er sætningen bevist.

En gruppe har således altid ikke trivielle abelske undergrupper, selv om den ikke selv er abelsk.

Vi går nu over til et nærmere studium af nogle specielle grupper, som spiller en rolle i teorien for lineære ligninger. Vi vil straks definere dem.

Definition 7.19. Lad A være en mængde. Gruppen af bijektive afbildninger $p: A \to A$ med sammensætning som

kompositionsregel, kaldes den symmetriske gruppe på A og betegnes S_A. Specielt betegner vi med S_n den symmetriske gruppe på mængden $\{1,\ldots,n\}$.

Det er klart, at S_A er uendelig, hvis A er det, og at S_A har $n!$ elementer, hvis A har n elementer, idet en bijektiv afbildning $p:A \to A$ kan opfattes som en omordning af elementerne i A. Mere konkret kan vi opfatte de n elementer i A som anbragt på hver sin plads (som f.eks. i et fodboldhold), og hver afbildning p kommer så til at svare til en omplacering.

Når vi regner indbyrdes isomorfe grupper ens, bliver der ikke så mange symmetriske grupper. Det fremgår af den følgende sætning.

Sætning 7.20. Hvis A og B er indbyrdes ækvivalente mængder er de symmetriske grupper S_A og S_B isomorfe. Hvis $f:A \to B$ er en bijektiv afbildning, kan en isomorfi $\varphi:S_A \to S_B$ defineres ved $\varphi(p) = f\circ p\circ f^{-1}:B \to B$. Specielt er alle symmetriske grupper på mængder med n elementer isomorfe med S_n.

Bevis. Da relationen $q = f\circ p\circ f^{-1}$ er ensbetydende med $f^{-1}\circ q\circ f = p$, er φ en bijektiv afbildning. For $p_1,p_2:A \to A$ får vi $\varphi(p_1)\circ\varphi(p_2) = f^{-1}\circ p_1\circ f\circ f^{-1}\circ p_2\circ f = f^{-1}\circ p_1\circ p_2\circ f = \varphi(p_1\circ p_2)$, så φ er en isomorfi. Dermed

er sætningen bevist.

Definition 7.21. Hvis A er en endelig mængde, kaldes en bijektiv afbildning også en permutation af A, og en undergruppe i S_A kaldes også en permutationsgruppe.

Databehandling er manipulation med endelige mængder, og permutationer spiller en stor rolle. I praksis manipulerer man med navne eller numre i stedet for objekterne selv, og derved udnytter man netop sætning 7.20. I denne sammenhæng er elementerne af $\mathbb{N}$ brugt som etiketter, og strukturen af $\mathbb{N}$ ved ordningsrelation og kompositionsregler er derfor irrelevant. Således bruges elementerne af $\mathbb{N}$ ved programmering også som adresser, men den i sig irrelevante ordnings- og algebrastruktur på $\mathbb{N}$ udnyttes alligevel rent teknisk ved programmeringsarbejdet.

Når vi i det følgende studerer S_n, må vi huske, at den struktur vi har på mængden $\{1,\ldots,n\}$ som delmængde af $\mathbb{N}$, er helt irrelevant, og når den alligevel sommetider kommer ind i billedet, er det højst af rent bevistekniske grunde.

Et element $p \in S_n$ kan angives som en tabel, der bedst opskrives vandret, som i følgende eksempler fra S_5

$$p_1=\begin{pmatrix}1&2&3&4&5\\3&5&1&4&2\end{pmatrix}\quad p_2=\begin{pmatrix}1&2&3&4&5\\2&5&3&1&4\end{pmatrix}=\begin{pmatrix}4&1&3&5&2\\1&2&3&4&5\end{pmatrix}=\begin{pmatrix}3&5&1&4&2\\3&4&2&1&5\end{pmatrix}.$$

Som vi har antydet det for p_2, er det komplet ligegyldigt, i hvilken rækkefølge vi skriver søjlerne. Den midterste form er fremkommet ved ordning efter billederne. Ved ombytning af rækkerne får vi den inverse permutation. I den sidste form for p_2 har vi ordnet indgangsværdierne som udgangsværdierne for p_1. Det gør det nemt at konstruere

$$p_2 \circ p_1 = \begin{pmatrix}1&2&3&4&5\\3&4&2&1&5\end{pmatrix}.$$

Definition 7.22. Lad $\{a_1,\ldots,a_m\}$ være en delmængde omfattende m indbyrdes forskellige elementer af $\{1,\ldots,n\}$. Med $(a_1,\ldots,a_m)$ betegner vi da den permutation $p \in S_n$, som er defineret ved $p(a_j) = a_{j+1}$ for $j = 1,\ldots,m-1$, og $p(a_m) = a_1$, medens $p(x) = x$ for alle øvrige $x \in \{1,\ldots,n\}$. En sådan permutation siges at være cyklisk af orden m. Den kaldes mere præcist en cyklisk permutation af delmængden $\{a_1,\ldots,a_m\}$. En cyklisk permutation (a_p,a_q) kaldes en simpel ombytning.

En cyklisk permutation af en delmængde med kun 1 element, bliver den identiske permutation. Det er klart, at $(a_1,\ldots,a_m) = (a_2,\ldots,a_m,a_1) = (a_3,\ldots,a_m,a_1,a_2)$ etc., så vi får mange betegnelser for samme gruppeelement.

Vi vil nu angive nogle delmængder af S_n, som frembringer S_n. Den sidste er nu ikke noget, vi får brug for, men vi har taget den med, fordi det er ganske flot, at S_n kan frembringes af en delmængde med kun 2 elementer.

Sætning 7.23. Den symmetriske gruppe S_n frembringes af mængden af simple ombytninger. For enhver permutation $p \in S_n$ vil mængden $\{(p(1),p(2)),(p(2),p(3)),\ldots,(p(n-1),p(n))\}$ af $n-1$ simple ombytninger frembringe S_n. Endelig vil en mængde omfattende den cykliske permutation $(1,2,\ldots,n)$ og den simple ombytning $(1,2)$ frembringe S_n.

Bevis. Vi beviser den første påstand ved induktion efter n. For $n \leq 2$ er påstanden triviel. Vi antager, at den allerede er vist for S_{n-1}, og vi betragter så $q \in S_n$. Hvis $q(n) = n$ er restriktionen $q|\{1,\ldots,n-1\}$ et element af S_{n-1} og derfor et produkt af simple ombytninger fra S_{n-1}, men de tilhører også S_n, så påstanden er rigtig i dette tilfælde. Er $q(n) \neq n$, betragter vi $q_1 = (n,q(n))\circ q$. Så er $q_1(n) = n$, og i det tilfælde har vi netop vist, at q_1 er produkt af simple ombytninger, og da $q = (n,q(n))\circ q_1$ gælder det samme for q. Dermed er den første påstand bevist.

Lad os nu betragte en undergruppe $H \subseteq S_n$, som indeholder $(p(1),p(2)),\ldots,(p(n-1),p(n))$, og lad j og k være hele tal og $1 \leq j < k \leq n$. Det er da let at se, at

$$(p(j),p(k)) = (p(k-1),p(k)) \circ \ldots \circ (p(j+1),p(j+2)) \circ (p(j),p(j+1)) \circ \ldots \circ (p(k-1),p(k)).$$

Deraf følger, at H indeholder alle ombytninger $(p(j), p(k))$, altså hele mængden af simple ombytninger, og så giver den første påstand, at $H = G$, og dermed er den anden påstand bevist.

For permutationen $p = (1,\ldots,n)$ gælder for $j = 0,1,2,\ldots,n-2$, at $p^j(1) = j+1$ og $p^j(2) = j+2$. Heraf følger, at $p^j \circ (1,2) \circ p^{-j} = (j+1,j+2)$, så den undergruppe H, der indeholder $(1,2)$ og $(1,\ldots,n)$, indeholder $(j,j+1)$, $j = 1,2,\ldots,n-1$, og den anden påstand giver så, at $H = G$, og dermed er sætningen bevist.

Vi illustrerer dette ved at vise, hvordan 1 2 3 4 5 6 7 kan omordnes til 4 2 7 1 3 5 6 ved hele tiden kun at bytte par $(j,j+1)$.

Til sammenligning har vi i kolonnen til højre gjort det samme ved i hvert skridt at bytte tal, der står ved siden af hinanden. Det var det vi brugte, da vi beviste uafhængighed af rækkefølgen ved kommutativitet. I kolonnen

til venstre bringes tallene på plads efter størrelse. I kolonnen til højre bringes de på ret plads fra højre mod venstre.

1 2 3 4 5 6 7	1 2 3 4 5 6 7
1 2 4 3 5 6 7	1 2 3 4 5 7 6
1 2 5 3 4 6 7	1 2 3 4 7 5 6
1 2 6 3 4 5 7	1 2 4 3 7 5 6
1 2 7 3 4 5 6	1 2 4 7 3 5 6
2 1 7 3 4 5 6	2 1 4 7 3 5 6
3 1 7 2 4 5 6	2 4 1 7 3 5 6
4 1 7 2 3 5 6	2 4 7 1 3 5 6
4 2 7 1 3 5 6	4 2 7 1 3 5 6

Der blev oven i købet brug for lige mange ombytninger i de to tilfælde.

Inden vi går over til de helt afgørende sætninger, nævner vi en, som er meget let.

Sætning 7.24. Lad $p,q \in S_n$ være cykliske permutationer på disjunkte delmængder A og B af $\{1,\ldots,n\}$. Da er $p \circ q = q \circ p$.

Bevis. For $x \in A$ er $p(q(x)) = q(p(x)) = p(x)$. For $x \in B$ er $p(q(x)) = q(p(x)) = q(x)$. Hvis x hverken tilhører A eller B, er $p(q(x)) = q(p(x)) = x$. Dermed er sætningen bevist.

Nu fortsætter vi med de afgørende sætninger.

Sætning 7.25. Lad $p \in S_n$ være en permutation på $M = \{1,\ldots,n\}$. Der er da en entydig bestemt klasseind-

deling af M i klasser $M_1,\ldots,M_q$, således at p er produkt af cykliske permutationer $p_1,\ldots,p_q$, hvor p_j er cyklisk på M_j for $j = 1,\ldots,q$. Derved kan nogle af klasserne p_j bestå af kun 1 element, og den tilsvarende permutation p_j er da den identiske afbildning og p afbilder elementet på sig selv. Klasserne $M_1,\ldots,M_q$ er de mindste delmængder af M, som afbildes på sig selv ved p.

Bevis. Hvis $A \subseteq M$ og $B \subseteq M$ opfylder betingelserne $p(A) = A$ og $p(B) = B$ får vi åbenbart $p(A\cap B) \subseteq p(A) = A$ og analogt $p(A\cap B) \subseteq B$, altså $p(A\cap B) \subseteq A\cap B$, men da $A \cap B$ er endelig og p er bijektiv, medfører det, at $p(A\cap B) = A\cap B$. For et element $a \in M$ vil der være endelig mange mængder $A \subseteq M$, for hvilke $a \in A$ og $p(A) = A$. Fællesmængden for disse mængder vil indeholde a, afbildes i sig selv ved p og være den mindste mængde ved denne egenskab. Således bliver hvert element af M indeholdt i en minimal invariant mængde, og det er klart, at disse udgør en klasseinddeling af M.

Den klasse, der indeholder a, indeholder også $p(a)$, $p(p(a)) = p^2(a)$, $p^3(a),\ldots$. Da klassen er endelig, kan disse elementer ikke blive ved at være forskellige, så der må være et første $p^j(a)$, der er identisk med et af de foregående, men da p er bijektiv, bliver a selv det eneste element, der kan være billede af $p^j(a)$, og

vi får så, at restriktionen af p til $A = \{a, p(a), p^2(a), \ldots, p^{j-1}(a)\}$ bliver den cykliske permutation $(a, p(a), \ldots, p^{j-1}(a))$. Så bliver A afbildet på sig selv ved p, og ingen ægte delmængde af A har denne egenskab, så A er en af klasserne vi fandt overfor. Dermed er sætningen bevist.

Nu nærmer vi os det egentlige formål med denne undersøgelse af permutationers egenskaber. Den næste sætning er et vigtigt supplement til den foregående.

Sætning 7.26. Lad $p \in S_n$ være en permutation, for hvilken den i sætning 7.25 omtalte klasseinddeling af M omfatter q klasser. Lad $(j,k) \in S_n$ være en simpel ombytning (altså $0 \leqq j < k \leqq n$). Da vil den tilsvarende klasseinddeling for $(j,k) \circ p$ omfatte netop $q-1$ eller netop $q+1$ klasser.

Bevis. Lad os først se på det tilfælde, hvor en af de q klasser indeholder både j og k. En af cyklerne i p har da formen $(\alpha_1, \ldots, \alpha_r, \ldots, \alpha_s)$ med $\alpha_1 = j$, $\alpha_r = k$. Vi ser, at denne cykel i $(j,k) \circ p$ bliver erstattet med $(\alpha_1, \ldots, \alpha_{r-1}) \circ (\alpha_r, \ldots, \alpha_s)$, medens de andre cykler forbliver uændrede, så $(j,k) \circ p$ får $q+1$ klasser. Hvis ingen af de q klasser indeholder både j og k omfatter p cykler $(\alpha_1, \ldots, \alpha_r)$ og $(\beta_1, \ldots, \beta_s)$ med $\alpha_1 = j$, $\beta_1 = k$,

og disse 2 cykler bliver i $(j,k)\circ p$ erstattet med $(\alpha_1,\ldots,\alpha_r,\beta_1,\ldots,\beta_s)$, medens de øvrige cykler forbliver uændrede, så $(j,k)\circ p$ får i dette tilfælde $q-1$ klasser.

Defintion 7.27. Det i sætningerne 7.25 og 7.26 omtalte antal q af klasser kaldes cykel-tallet for permutationen p og betegnes $c(p)$.

Når en kvalitet ved et begreb som f.eks. et naturligt tal angives ved "lige" eller "ulige", kaldes kvaliteten "paritet". At nogle hele tal har samme paritet betyder således, at de enten alle er lige eller alle er ulige.

Nu er vi nået til selve hovedsagen.

Sætning 7.28. Lad $p \in S_n$ være skrevet som et produkt af m simple ombytninger. Da har m samme paritet som $n-c(p)$.

Bevis. Den identiske permutation har n cykler på 1 element hver, altså $n-c(id) = 0$, og den er produkt af 0 simple ombytninger. Vi sammensætter id med de simple ombytninger taget 1 ad gangen, og får dermed efter hinanden permutationer $id = p_0,p_1,p_2,\ldots,p_m = p$. Af sætning 7.26 følger, at $n-c(p_j)$ skifter paritet i hvert trin,

og derfor vil den hele tiden have samme paritet som j. Dermed er sætningen bevist.

Med denne sætning har permutationer fået paritet, idet der er blevet mening i følgende definition.

Definition 7.29. En permutation $p \in S_n$ kaldes lige, hvis den er produkt af et lige antal simple ombytninger, og ulige, hvis den er produkt af et ulige antal simple ombytninger.

Eksempler. En cyklisk permutation af orden q er produkt af $q-1$ ombytninger, så den har modsat paritet af q. Hvis $p \in S_n$ er permutationen, der vender rækkefølgen, altså $p(x) = n+1-x$, og n er et tal af form $4q$ eller $4q+1$, er p produkt af $2q$ ombytninger, altså lige, men hvis n har form $4q+2$ eller $4q+3$, er p ulige.

Når man skal undersøge, om en given permutation p er lige eller ulige, er det sædvanligvis nemmest at skrive p som produkt af cykliske permutationer på disjunkte mængder og tælle sig til $c(p)$. Det er vigtigt at medregne cykliske permutationer på mængder med kun et element. I praksis er det måske mere hensigtsmæssigt at tælle $n-c(p)$ ved at tælle elementerne i de disjunkte mængder, men passe på at glemme et fra hver mængde.

Eksempel. Lad $p \in S_{15}$ være givet ved

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 5 & 9 & 2 & 15 & 8 & 3 & 14 & 1 & 10 & 6 & 12 & 11 & 7 & 4 \end{pmatrix}.$$

Vi aflæser umiddelbart, at

$$p = (1,13,11,6,8,14,7,3,9) \circ (2,5,15,4) ,$$

idet vi ser, at p afbilder 1 i 13 og 13 i 11 og 11 i 6 osv. til vi når 9 med $p(9) = 1$. Så fortsætter vi med det første element, der ikke er blevet brugt, osv. Vi tæller så $n-c(p) = 11$, så p er ulige.

Sætning 7.30. Et produkt af permutationer har samme paritet som antallet af ulige permutationer i produktet. For $n > 1$ er der lige mange lige og ulige permutationer i S_n. Mængden af lige permutationer er for $n > 1$ en normal undergruppe med index 2 i S_n. Den betegnes A_n, og kaldes den alternerende gruppe på n elementer. Dens orden er $\frac{n!}{2}$.

Bevis. Den første påstand vises ved at skrive hver permutation som produkt af simple ombytninger. Så følger påstanden af, at den samme påstand gælder ved addition af naturlige tal. Den ved $\varphi(p) = (1,2) \circ p$ definerede afbildning $\varphi: S_n \to S_n$ er bijektiv. Da den afbilder lige permutationer på ulige og ulige på lige (sætning 7.26), må der være lige mange af de to slags. Den første påstand

viser, at mængden A_n af lige permutationer er stabil med hensyn til multiplikationen i S_n. Når en permutation er skrevet som et produkt af simple ombytninger, fås den inverse som produktet af de samme simple ombytninger i den modsatte rækkefølge, så p og p^{-1} har samme paritet. Men så er A_n en undergruppe. Den anden påstand viser, at A_n har index 2, og bemærkningen efter definition 7.11 fortæller, at A_n er normal. Dermed er sætningen bevist.

Faktorgruppen $\frac{S_n}{A_n}$ er isomorf med $\mathbb{Z}_2$, altså med $\{1,-1\}$ med multiplikation. Den kanoniske afbildning $k:S_n \to \frac{S_n}{A_n}$ sammensat med isomorfien med $\mathbb{Z}_2$ giver en homomorfi, som vi betegner med $\text{sign}:S_n \to \{1,-1\}$. Derfor den næste definition.

Definition 7.31. For $p \in S_n$ er $\text{sign } p = 1$, hvis p er lige, og $\text{sign } p = -1$, hvis p er ulige. Vi kalder $\text{sign } p$ fortegnet for p.

Det er dette fortegnsbegreb, der spiller en rolle i teorien for lineære ligninger. I lærebøger omtales ofte en metode til bestemmelse af fortegnet for en permutation, men den er ikke så praktisk som den her omtalte metode til bestemmelse af paritet. Vi omtaler den derfor bare kort uden at anføre resultaterne i form af sætninger.

Et talpar (j,k) med $1 \leqq j < k \leqq n$ kaldes en inversion for permutationen $p \in S_n$, hvis $p(k) < p(j)$, altså hvis p vender rækkefølgen af de to elementer. Vi kan tælle antallet $J(p)$ af inversioner for p, og antallet af inversioner vil da have samme paritet som p. Vi kan nemlig skrive p som produkt af ombytninger $(j,j+1)$ af naboelementer, og sammensætning med en sådan ombytning ændrer antallet af inversioner med 1 eller -1. Heraf følger relationen

$$\prod_{1 \leqq j < k \leqq n} \frac{p(k)-p(j)}{k-j} = \operatorname{sign} p \ .$$

Tallene $|p(k)-p(j)|$ er nemlig netop tallene $k-j$ i en anden rækkefølge, så produktet får numerisk værdi 1, og leddet med j og k er negativt, hvis og kun hvis (j,k) er en inversion for p.

Som en illustration til det foregående vil vi give en oversigt over grupper af lav orden og påpege nogle af deres mere interessante egenskaber. Vi anfører først et par kendsgerninger, som er nyttige ved diskussionen.

1). Ordenen af et element i en gruppe er divisor i gruppens orden (sætning 7.8).

2). Hvis en gruppe frembringes af elementer, der kommuterer 2 og 2, er gruppen abelsk (hvert gruppeelement kan skrives som produkt af frembringere og inverse frembringere).

3). Hvis alle elementer i en gruppe på nær neutralelementet har orden 2, er gruppen kommutativ (ethvert element bliver inverst til sig selv, så vi får $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$).

Så begynder vi forfra. Da 2 og 3 er primtal, har vi kun cykliske grupper af disse ordener. Den alternerende gruppe A_3 har orden $\frac{3!}{2} = 3$, og er cyklisk. Den frembringes af den cykliske permutation (1,2,3).

Hvis en gruppe af orden 4 ikke er cyklisk, må den bestå af e, samt 3 elementer af orden 2, så den bliver kommutativ, og additionstabellen bliver helt fastlagt ved kravet om entydig division, som betyder at hvert element optræder netop 1 gang i hver række og hver søjle.

e	a	b	c
a	e	c	b
b	c	e	a
c	b	a	e

Det er let nok, at efterprøve den associative lov. Gruppen kaldes Kleins 4-gruppe.

Da 5 er primtal er en gruppe af orden 5 cyklisk.

Vi kender allerede S_3, som er en ikke cyklisk gruppe af orden 6. Den har 2 frembringere $a = (1,2,3)$ og $b = (2,3)$, idet vi har elementerne

id	(1,2,3)	(1,3,2)	(2,3)	(1,3)	(1,2)
e	a	a^2	b	ba	ba^2

Vi får gruppetabellen

e	a	a^2	b	ba	ba^2
a	a^2	e	ba^2	b	ba
a^2	e	a	ba	ba^2	b
b	ba	ba^2	e	a	a^2
ba	ba^2	b	a^2	e	a
ba^2	b	ba	a	a^2	e

Enhver gruppe af orden 6 er isomorf med $\mathbb{Z}_6$ eller S_3, men det kræver lidt omtanke at vise det. Lad G være en gruppe af orden 6. Hvis G har et element af orden 6, er G cyklisk, altså isomorf med $\mathbb{Z}_6$. Hvis alle elementer i G undtagen e har orden 2, er G abelsk, og en cyklisk undergruppe af orden 2 vil være normal og have en faktorgruppe af orden 3, frembragt af en sideklasse $a\mathbb{Z}_2$, men da a har orden 2, får $a\mathbb{Z}_2$ også orden ≤ 2, så det går slet ikke. Altså vil G under alle omstændigheder have et element a af orden 3, altså en cyklisk undergruppe $\{e,a,a^2\}$ som i eksemplet ovenfor, og den vil have 1 højre sideklasse. Hvis b er et vilkårligt af gruppens øvrige elementer, kommer denne sideklasse til at bestå af elementerne b, ba og ba^2 som i tabellen ovenfor. Af $b^2 = a$ følger $b^3 = ab$, $b^4 = a^2$ etc. og G bliver cyklisk. Det samme sker, hvis $b^2 = a^2$. Det er klart, at $b^2 = ba$ eller $b^2 = ba^2$ ikke går, da vi kan

forkorte med b. Altså er enten G cyklisk eller $b^2 = e$. Af $b^2 = e$ følger $bba = a$, $bba^2 = a^2$. Udfyldningen af tabellens nederste venstre hjørne går tvangsmæssigt. Da elementerne ba og ba^2 kunne være brugt i stedet for b, har vi også $(bc)^2 = e$ og $(ba^2)^2 = e$. Derefter går udfyldningen af nederste højre hjørne tvangsmæssigt. Af $ab = x$ følger $xb = ab^2 = a$, og af den allerede konstaterede del af tabellen får vi $ab = ba^2$. Derefter går udfyldningen af øverste højre hjørne igen tvangsmæssigt, og vi har fået vist, at der kun er de to omtalte isomorfiklasser af grupper af orden 6.

Da 7 er et primtal er en gruppe af orden 7 cyklisk.

Der er flere grupper af orden 8. Der er den cykliske $\mathbb{Z}_8$. Der er mængden af de 8 sæt (x_1,x_2,x_3), hvor hvert $x_j \in \mathbb{Z}_2$, som vi her skriver med +, og hvor addition er givet ved $(x_1,x_2,x_3)+(y_1,y_2,y_3) = (x_1+y_1,x_2+y_2,x_3+z_3)$. Det er en abelsk gruppe, hvis elementer alle har orden 2. Et eksempel på en ikke abelsk gruppe af orden 8 er kvaternion-gruppen, som har elementerne ± 1, $\pm i$, $\pm j$, $\pm k$, hvor $i^2 = j^2 = k^2 = -1$ og $jk = -kj = i$, $ki = -ik = j$ og $ij = -ji = k$, og hvor regning med fortegnene sker som ved multiplikation af tal. Kvaterniongruppen har den særlige egenskab, at alle dens undergrupper er normale. Der findes mindst endnu en isomorfiklasse af ikke abelske grupper af orden 8.

I stedet for at gå videre med dette vil vi se lidt på S_4, som har orden 24. Den har den normale undergruppe A_4, som har orden 12. I A_4 finder vi permutationerne $(1,2)\circ(3,4)$, $(1,3)\circ(2,4)$ og $(1,4)\circ(2,3)$, der sammen med neutralelementet danner en undergruppe H isomorf med Kleins 4-gruppe, og den er normal i både A_4 og S_4. Til gengæld er de 3 undergrupper af orden 2 i H nok normale i H, men ikke i A_4, og derfor heller ikke i S_4. De 8 andre elementer i A_4 er de cykliske permutationer $(1,2,3)$, $(1,2,4)$, $(1,3,4)$ og $(2,3,4)$ samt deres inverse. De frembringer undergrupper af orden 3 og ikke normale. I $S_4 \setminus A_4$ finder vi 6 simple ombytninger $(1,2)$, $(1,3)$, $(1,4)$, $(2,3)$, $(2,4)$ og $(3,4)$, samt de cykliske permutationer $(1,2,3,4)$, $(1,2,4,3)$, $(1,3,2,4)$, $(1,3,4,2)$, $(1,4,2,3)$ og $(1,4,3,2)$. Disse falder i par af inverse, nemlig den første sammen med den sidste, den anden med den fjerde og den tredie med den femte. Anden potens af hver af dem er lig anden potens af den inverse, og den er et af elementerne i 4-gruppen.

Vi bemærker, at S_4 har ægte undergrupper, der ikke er undergrupper i A_4. Således udgør $(1,3)$, $(2,4)$ og $(1,3)\circ(2,4)$ sammen med neutralelementet endnu en kopi af 4-gruppen. Den er ikke normal, men den af dens sideklasser, som indeholder $(1,2,3,4)$, er både venstre og højre sideklasse på en gang. Denne sideklasse omfatter elementerne $(1,2,3,4)$, $(1,2)\circ(3,4)$, $(1,4)\circ(2,3)$, $(1,4,3,2)$. Undergrup-

pen sammen med denne sideklasse udgør en undergruppe med 8 elementer i S_4. Den er ikke normal. Den kaldes diedergruppen. Dens undergrupper af orden 2 er ikke normale, og derfor er den ikke isomorf med kvaterniongruppen.

I nutiden er gruppeteori en omfattende videnskab. Her skal vi ganske kort omtale nogle af de spørgsmål, gruppeteorien beskæftiger sig med. Hvis G er en gruppe og $\varphi: G \to G$ er en automorfi, vil φ selvfølgelig afbilde elementer af orden q på elementer af orden q, undergruppe på undergruppe, normal undergruppe på normal undergruppe osv. Blandt automorfierne udmærkes de indre, som defineres ved $\varphi(x) = axa^{-1}$, hvor a er et element af G. Elementer der svarer til hinanden ved en indre automorfi kaldes konjugerede. Ligeledes undergrupper. "Konjugeret med" er en ækvivalensrelation. En normal undergruppe er en undergruppe, der er identisk med sin konjugerede.

En undergruppe i G kaldes fuldstændig invariant, hvis den afbildes på sig selv ved enhver automorfi $\varphi: G \to G$. Mængden af elementer i G, som kommuterer med alle elementer i G, udgør en fuldstændig invariant undergruppe, der kaldes centrum i G.

Et element af formen $aba^{-1}b^{-1}$ kaldes en kommutator, fordi $ab = (aba^{-1}b^{-1})(ba)$, så den kan ombytte elementer.

Enhver automorfi afbilder kommutator i kommutator, og derfor bliver den af alle kommutatorer frembragte undergruppe $K \subseteq G$ fuldstændig invariant. For normale undergrupper $H \subseteq G$ gælder, at $\frac{G}{H}$ er abelsk, hvis og kun hvis $H \supseteq K$.

For givne grupper H og A kan man prøve at bestemme de grupper, der har en undergruppe isomorf med H og tilsvarende faktorgruppe isomorf med A. Dette problem har altid løsninger, men at få overblik over løsningsmængden er et vanskeligt problem, der kaldes extensionsproblemet. For abelske grupper er man nået langt i retning af en løsning. Problemet behandler i en vis forstand spørgsmålet om opbygning af grupper af simplere bestanddele, og byggestenene bliver de grupper, der ikke har andre normale undergrupper end de trivielle. Sådanne grupper kaldes derfor simple. Medens mange ikke abelske grupper er opbygget af abelske, findes der også en uoverskuelig masse af simple ikke abelske grupper, men de er alle ganske indviklede. Det bedst kendte eksempel er, at A_n er en simpel gruppe for $n \geq 5$. Der findes ikke simple ikke-abelske grupper af lavere orden end 60 svarende til A_5. Dette er baggrunden for Abels sætning, om at rødderne i polynomier af grad ≥ 5 ikke kan udtrykkes ved rodstørrelser.

Til en geometrisk figur med en eller anden form for regelmæssighed hører en gruppe af bevægelser, som fører

figuren over i sig selv. Således er atomkernerne i en krystal arrangeret i et regelmæssigt mønster, der kan tænkes fortsat i hele rummet, og man får så en gruppe af drejninger og forskydninger, der fører mønstret over i sig selv. Hvis visse drejninger om en bestemt akse L fører mønstret over i sig selv, vil røntgenstråler i retningen L ved passage gennem krystallen give et interferensmønster, der går over i sig selv ved de samme drejninger. Derfor kan man ved interferensforsøg skaffe sig oplysninger om gruppen af flytninger, der fører gitret af atomkerner over i sig selv, og eventuelt kan man derved få bestemt gitrets struktur. Andre anvendelser af gruppeteori er ikke så direkte.

ØVELSER TIL KAPITEL 7

Stikord.

Gruppe, permutation, permutationsgruppe, symmetrisk gruppe, alternerende gruppe, cyklisk gruppe, cyklisk permutation, fortegn for permutation, paritet, undergruppe, sideklasse, orden, index, undergruppe frembragt af mængde, normal undergruppe, faktorgruppe, homomorfi, 4-gruppen, kvaterniongruppen (indre automorfi, konjugeret, fuldstændig invariant, centrum, kommutator, extension, simpel gruppe).

7.1. Permutationer u,v,x og y i S_8 defineres ved følgende tabeller

t	1	2	3	4	5	6	7	8
$u(t)$	6	2	5	1	3	8	7	4
$v(t)$	3	6	2	5	8	1	4	7
$x(t)$	2	1	4	3	6	5	8	7
$y(t)$	2	3	4	5	6	7	8	1

7.1.1. Udregn $v\circ u$, $u\circ v$, $y\circ x$ og $x\circ y$.

7.1.2. Udregn $u\circ v\circ u^{-1}\circ v^{-1}$.

7.1.3. Udregn $y^{-1}\circ x\circ y$, $y\circ x\circ y^{-1}$, $x^{-1}\circ y\circ x$ og $x\circ y\circ x^{-1}$.

7.1.4. Skriv u,v,x og y som produkter af cykler.

7.1.5. Angiv ordenen af gruppeelementerne u,v,x og y.

7.1.6. Angiv pariteten af u,v,x og y.

7.1.7. Skriv u,v,x og y som produkter af ombytninger af naboelementer.

7.1.8. Skriv u,v,x og y som produkter af så få ombytninger som muligt.

7.2. Hvor mange permutationer i S_n permuterer alle n elementer cyklisk.

7.2.1. Hvor mange elementer i S_n har ordenen 2.

7.2.2. For hvilke værdier af n kan et element i S_n have orden n uden at permutere alle elementer cyklisk. Svaret på sådan et spørgsmål må være en karakterisering af n ved talteoretiske egenskaber. Er det mon nok, at mindst 2 forskellige primtal går op i n, og er det nødvendigt?

7.3. Vælg et element af S_{10} med så høj orden som muligt.

7.4. Lad G være en gruppe, og $A \subseteq G$ en endelig delmængde, som er stabil med hensyn til multiplikationen. Vis, at A er en undergruppe. Det beror på den simple kendsgerning, at en in- eller surjektiv afbildning $\varphi: A \to A$ vil være bijektiv, fordi A er endelig. Den tyske matematiker E. Landau kaldte denne form for slutning et "skuffeprincip". Vi giver endnu 2 eksempler samt et modeksempel.

7.4.1. Lad G være en endelig mængde med en associativ kompositionsregel $*$. Det antages, at det for alle $a,b \in G$ gælder, at hver af ligningerne $a*x = b$ har højst 1 løsning. Vis, at G er en gruppe.

7.4.2. Lad G være en gruppe og $H \subseteq G$ en endelig undergruppe, der for alle $x \in G$ tilfredsstiller, at $xHx^{-1} \subseteq H$. Vis, at H er normal.

7.4.3. Lad G være mængden af alle bijektive afbildninger $\varphi: \mathbb{Z} \to \mathbb{Z}$, og lad H være delmængden af afbildninger, som tilfredsstiller, at $\varphi(x) = x$ for alle $x < 0$. Lad $\psi \in G$ være defineret ved $\psi(x) = x+1$ for alle $x \in \mathbb{Z}$. Vis, at H er en ikke normal undergruppe, for hvilken vi har $\psi H \psi^{-1} \subset H$.

7.5. Lad G være en gruppe, $A \subseteq G$ en undergruppe og $H \subseteq G$ en normal undergruppe. Vis, at $AH = \{ah \mid a \in A, h \in H\}$ er en undergruppe i G.

7.5.1. Find et eksempel på en gruppe G med undergrupper A og B for hvilke AB ikke er en undergruppe. Prøv med $G = S_3$ og lad A og B være 2 forskellige undergrupper af orden 2.

7.5.2. Lad G, A og H være som i 7.5. Vis, at H er en normal undergruppe i AH, og at $A \cap H$ er en normal undergruppe i A.

7.5.3. Vis, at faktorgrupperne $\frac{A}{A \cap H}$ og $\frac{AH}{H}$ er isomorfe. Dette resultat kaldes Noethers isomorfisætning efter den tyske matematiker Emmy Noether, som har bidraget meget til udviklingen af moderne algebra.

7.6. Lad $p = p_1 \ldots p_q \in S_n$ være en permutation skrevet som sammensætning af cykliske permutationer af disjunkte delmængder $A_1, \ldots, A_q$ af $\{1, \ldots, n\}$. Lad $\varphi \in S_n$ være en permutation. Vis, at $\varphi \circ p \circ \varphi^{-1}$ er sammensætning af cykliske permutationer af de disjunkte delmængder $\varphi(A_1), \ldots, \varphi(A_q)$.

7.6.1. Til 2 permutationer $p,p' \in S_n$ svarer en permutation $\varphi \in S_n$ med $p' = \varphi \circ p \circ \varphi^{-1}$, hvis og kun hvis det for fremstillingerne af p og p' som sammensætninger af cykliske permutationer på disjunkte delmængder af $\{1,\ldots,n\}$ gælder, at der bliver lige mange disjunkte delmængder for p og p', og at de kan parres, så sammenparrede delmængder indeholder lige mange elementer.

7.6.2. En ægte normal undergruppe af S_n kan ikke indeholde en simpel ombytning.

7.7. Vi vil udnytte opgave 7.6 til et bevis for, at den alternerende gruppe A_n er simpel for $n \neq 4$, altså at A_n ikke indeholder andre normale undergrupper end A_n selv og den trivielle. Vi har set i teksten, at A_4 ikke er simpel, og vi ved allerede, at A_2 er triviel og A_3 isomorf med $\mathbb{Z}_3$, så vi kan nøjes med at se på tilfældet $n \geq 5$. Vi gennemfører beviset i en række trin.

7.7.1. Først ser vi på A_5. Vi begynder med at skaffe os et overblik over elementerne i A_5. Der er 60 ialt. Ud over neutralelementet er der

1). 15 elementer $(a_1,a_2)\,(a_3,a_4)$, hvor $a_1,\ldots,a_4$ er forskellige.

2). 20 elementer (a_1,a_2,a_3).

3). 24 elementer (a_1,a_2,a_3,a_4,a_5). Sml. opgave 7.2.

7.7.2. Opgave 7.6.1 viser nu, at der gælder et "alt eller intet"-princip for elementerne af type 1) eller 2). Derimod falder elementerne af typen 3) i 2 klasser med 12 i hver, og princippet gælder for hver af klasserne.

7.7.3. Et element af type 2) kan skrives som produkt af 2 elementer af type 1 og omvendt. Deraf følger ved sætning 7.8, at en undergruppe, der indeholder alle elementer af type 1 eller alle af type 2 er hele A_n.

7.7.4. Vi mangler at se på en normal undergruppe, der indeholder alle 12 elementer fra den ene klasse af type 3). Et produkt af 2 forskellige vil give et element af type 1) eller 2). Dermed er beviset fuldført for A_5.

7.7.5. For $n > 5$ indeholder A_n en kopi af A_5 (egentlig mange, idet vi udvælger 5 elementer blandt $\{1,\ldots,n\}$ og bruger delmængden af lige permutationer, der afbilder de andre elementer på sig selv).

Hvis nu $B \subseteq A_n$ er en normal undergruppe, bliver $B \cap A_5$ (en af kopierne) normal undergruppe i A_5 altså triviel eller hele A_5. Det går kun med "triviel", hvis B er triviel, så vi kan slutte, at B må indeholde samtlige kopier af A_5.

7.7.6. Lad nu $p \in A_n$ være skrevet som produkt af cykliske permutationer af disjunkte mængder. Hvis $(a_1,\ldots,a_6,\ldots)$ er en sådan permutation på mere end 5 elementer, splittes den op ved multiplikation med $(a_1,a_2)\,(a_4,a_5)$. Tilsvarende kan $(a_1,\ldots,a_4)\,(a_5,\ldots,a_8)$ splittes op ved multiplikation med $(a_1,a_3)\,(a_5,a_7)$. Endelig splittes $(a_1,\ldots,a_4)(a_5,a_6)$ op ved multiplikation med $(a_1,a_3)\,(a_5,a_6)$ og $(a_1,\ldots,a_4)\,(a_5)\,(a_6)$ forvandles til et produkt af par på samme måde. Under alle omstændigheder får vi p skrevet som et produkt af permutationer, der hver ligger i en kopi af A_5. Derefter går det let at vise påstanden.

7.7.7. Det er nu let at vise, at A_n for $n \neq 4$ er den eneste ikke trivielle, ægte, normale undergruppe i S_n.

7.8. Lad G være en gruppe, og $A \subseteq G$ en delmængde. Mængden N af elementer $x \in G$, som tilfredsstiller, at $xA = Ax$, er en undergruppe i G. Hvis

A er en undergruppe i G, er A en normal undergruppe i N, og enhver undergruppe i G, i hvilken A er normal undergruppe, er undergruppe i N. Gruppen N kaldes normalisator for A.

7.8.1. Lad G være en gruppe, og $A \subseteq G$ en delmængde. Mængden Z af elementer $x \in G$, som for hvert element $a \in A$ tilfredsstiller at $xa = ax$ kaldes centralisator for A. Vis, at Z er en undergruppe i N. Vis, at Z er normal undergruppe i N.

7.9. Lad G være en abelsk gruppe, og lad A og B være undergrupper i G. Vis, at følgende 2 betingelser er ækvivalente:

1). Ethvert element i G kan på 1 og kun 1 måde skrives som sum af et element af A og et element af B.

2). $A + B = G$ og $A \cap B = \{0\}$.

7.9.1. Lad G være en abelsk gruppe og B en undergruppe i G. Da findes der en undergruppe A, så betingelserne i opgave 7.9 er opfyldt, hvis og kun hvis der findes en homomorfi $p:G \to B$, for hvilken $p|B$ er den identiske afbildning.

7.9.2. Lad G være en abelsk gruppe og A en undergruppe i G. Da findes der en undergruppe B, så betingelserne i opgave 7.9 er opfyldt, hvis og kun hvis der findes en homomorfi $j:\frac{G}{A} \to G$, som afbilder hver sideklasse på et element af den selv.

7.9.3. For $G = \mathbb{Z}$ og $A = n\mathbb{Z}$, $n \in \mathbb{N}$, $n > 1$ findes der ikke en undergruppe B, så betingelserne i opgave 7.9 er opfyldt.

7.10. Lad p være et primtal. Lad G være gruppen af komplekse tal $e^{2\pi i n p^{-k}}$, hvor $n \in \mathbb{Z}$ og $k \in \mathbb{N}$. Vis, at enhver ægte undergruppe $H \subsetneq G$ er endelig, og at $\frac{G}{H}$ er isomorf med G.

7.11. Forsøg at finde alle grupper med 8 elementer. Det er ikke så svært, som man skulle tro. Bortset fra den hvis elementer alle har orden 2, og den cykliske af orden 8, må de have en cyklisk undergruppe af orden 4, og vi kan så kalde gruppens elementer $e, a, a^2, a^3, b, ab, a^2b$ og a^3b. Så kan alle produkter $a^p \cdot a^q b$ straks udregnes, og det er halvdelen af multiplikationstabellen. Valget $ba = ab$ giver en ny abelsk gruppe, hvis tabel umiddelbart kan opskrives. Det ses let, at $ba = a^2b$ fører til noget helt absurd. Tilbage er muligheden $ba = a^3b$. Med denne kan alle produkter $a^p b \cdot a^q$ regnes ud, og

der mangler en fjerdedel af gruppetavlen. Når b^2 er valgt, kan resten fyldes ud. Mulighederne $b^2 = a$ og $b^2 = a^3$ ser i første omgang plausible ud, men en nærmere undersøgelse viser, at de må forkastes. Tilbage er mulighederne $b^2 = e$, som giver diedergruppen, og $b^2 = a^2$, som giver kvaterniongruppen.

7.12. Det går lettere at finde samtlige grupper med 9 elementer. Hvis en gruppe med 9 elementer ikke er cyklisk, har alle dens elementer orden 3. Den har da en undergruppe $\{e,a,a^2\}$ og endnu en undergruppe $\{e,b,b^2\}$, og det er nu let at se, at gruppen består af elementerne

$$e,a,a^2,b,ab,a^2b,\ b^2,ab^2,a^2b^2\ .$$

Så må ba være ab, a^2b, ab^2 eller a^2b^2. Men $ba = a^2b^2$ medfører $abab = e$, og ab kan ikke have orden 2. Af $ba = a^2b$ fås efterhånden $ba^2 = ab$, $b^2a = ab^2$, altså $ab = ba$. Muligheden $ba = ab^2$ udelukkes på lignende vis. Vi ender således med $ba = ab$, så en gruppe med 9 elementer er abelsk. Så fastlægger multiplikationstabellen sig selv. Vi får således i alt 2 muligheder.

7.13. Lad G være en mængde med en associativ kompositionsregel $*$. Det antages, at der findes et venstre

neutralelement e, og at hvert element $x \in G$ har et venstre inverst element, altså et element x, som tilfredsstiller, at $x'*x = e$. Vis, at G er en gruppe. Det kræver nogen opfindsomhed.

7.14. Tallene 0,1,...,15 er arrangeret i et kvadrat, som vist i skemaet til venstre

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	0

1	10	2	9
4	7	12	0
11	14	8	6
15	3	13	5

Vi spiller et spil, i hvilket de tilladte træk i enhver situation består i at lade 0 bytte plads med et af sine højst 4 naboelementer. I stillingen til højre kan 0 således bytte med 9, 12 eller 6. Hvilke permutationer af tallene kan man få frem ved gentalgelse af tilladte træk udfra udgangsstillingen til venstre.

Spillet har ofte været forhandlet som legetøj. Det er udformet som en æske med kvadratiske brikker med tallene 1,...,15, medens 0 repræsenteres ved en tom plads.

KAPITEL 8

Ring.

Definition 8.1. Lad Λ være en mængde, på hvilken der er givet 2 kompositionsregler $*$ og $\times$. Vi siger, at $\times$ er distributiv med hensyn til $*$, hvis relationerne

$$(a*b)\times c = (a\times c)*(b\times c), \quad a\times(b*c) = (a\times b)*(a\times c)$$

gælder for alle $a,b,c \in \Lambda$.

De to relationer kaldes de distributive love. Der er mange velkendte eksempler. Således er multiplikation af tal distributiv med hensyn til addition, og det tilsvarende gælder for vektorproduktet. Potensopløftning som komposition af positive tal giver et eksempel på, at kun den ene distributive lov gælder med hensyn til ~~addition og kun den anden med hensyn til~~ multiplikation. På mængden af delmængder af en mængde har vi kompositionsreglerne $\cup$ og $\cap$, som er gensidigt distributive med hensyn til hinanden.

Hvis $\times$ er kommutativ, vil den ene af de distributive love følge af den anden.

Definition 8.2. En mængde Λ med 2 kompositionsregler +

og $\cdot$ kaldes en ring, hvis Λ med $+$ er en abelsk gruppe, medens $\cdot$ er distributiv med hensyn til $+$, samt associativ.

Tegnet $\cdot$ udelades sædvanligvis. Der findes et neutralelement 0 for $+$, og $a \in \Lambda$ har et modsat element $-a$. For alle $a \in \Lambda$ gælder, at $0 \cdot a = a \cdot 0 = 0$, idet $0 \cdot a + 0 \cdot a = (0+0) \cdot a = 0 \cdot a$, hvoraf vi slutter, at $0 \cdot a = 0$. Den anden ligning fås analogt.

Af $(-a) \cdot b + a \cdot b = (-a+a) \cdot b = 0 \cdot b = 0$ følger, at $(-a) \cdot b = -(ab)$, og analogt får vi $a \cdot -b = -ab$, altså $-a \cdot -b = ab$, så sædvanlig fortegnsregning vil gælde.

Nærliggende eksempler på ringe er $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$. Mængden End G af homomorfier $\varphi : G \to G$ af en abelsk gruppe G er en ring, idet vi for $\varphi, \psi : G \to G$ definerer $\varphi + \psi : G \to G$ ved $(\varphi+\psi)(x) = \varphi(x) + \psi(x)$ for alle $x \in G$, medens multiplikationen er sammensætningen $\varphi \circ \psi$. Det eneste, der ikke er helt oplagt, er de distributive love. Vi viser, at $(\varphi_1 + \varphi_2) \circ \psi = \varphi_1 \circ \psi + \varphi_2 \circ \psi$ ved at prøve med et $x \in G$, altså

$$((\varphi_1+\varphi_2)\circ\psi)(x) = (\varphi_1+\varphi_2)(\psi(x)) = \varphi_1(\psi(x)) + \varphi_2(\psi(x)) = (\varphi_1\circ\psi + \varphi_2\circ\psi)(x).$$

Den anden distributive lov $\varphi \circ (\psi_1 + \psi_2) = \varphi\circ\psi_1 + \varphi\circ\psi_2$ vises ved regningen

$$(\varphi\circ(\psi_1+\psi_2))(x) = \varphi((\psi_1+\psi_2)(x)) = \varphi(\psi_1(x)+\psi_2(x)) = \varphi(\psi_1(x)) + \varphi(\psi_2(x)) =$$

$$(\varphi\circ\psi_1 + \varphi\circ\psi_2)(x).$$

En delring i en ring Λ er en undergruppe Γ i gruppen Λ med $+$, som er stabil med hensyn til $\cdot$; således er $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, så hver er delring i de efterfølgende.

Hvis G er en abelsk gruppe og $H \subseteq G$ en undergruppe, vil ringen End G af endomorfier have en delring, der omfatter de endomorfier, der afbilder H ind i sig selv.

Lad Λ og Γ være ringe. En (ring-)homomorfi $f:\Gamma \to \Lambda$ er en afbildning f, som er en homomorfi med hensyn til både $+$ og $\cdot$. Vi har en kategori af ringe og ringhomomorfier. Det er klart, at billedet $f(\Gamma) \subseteq \Lambda$ er en delring, og det er også klart, at originalmængden til en delring af Λ er en delring af Γ. Specielt er kern $f = f^{-1}(0) \subseteq \Gamma$ en delring. For ethvert element $a \in \Gamma$ får vi imidlertid for ethvert $x \in$ kern f, at $f(ax) = f(a)f(x) = f(a)\,0 = 0$ og analogt $f(xa) = 0$, hvilket viser, at a kern $f \subseteq$ kern f og (kern $f)\cdot a \subseteq$ kern f. Vi definerer derfor

Definition 8.3. En delring $\Gamma \subseteq \Lambda$ kaldes et venstre ideal, hvis $a\Gamma \subseteq \Gamma$ for ethvert $a \in \Lambda$, og Γ kaldes et højre ideal, hvis $\Gamma \cdot a \subseteq \Gamma$ for ethvert $a \in \Lambda$. Vi kalder Γ et 2-sidet ideal, hvis Γ er både venstre- og højreideal.

Sætning 8.4. Kernen for en ringhomomorfi er et 2-sidet ideal. Hvis $\Gamma \subseteq \Lambda$ er et tosidet ideal, vil ringstrukturen på Λ inducere en ringstruktur på faktorgruppen $\frac{\Lambda}{\Gamma}$, og den kano-

niske afbildning $k:\Lambda \to \frac{\Lambda}{\Gamma}$ bliver en ringhomomorfi.

Bevis. Den første påstand blev bevist ovenfor. Faktorgruppen $\frac{\Lambda}{\Gamma}$ er mængden af sideklasser $a + \Gamma$, $a \in \Lambda$. For $a,b \in \Lambda$ og $x,y \in \Gamma$ får vi

$$(a+x)(b+y) = ab + xb + ay + xy \in ab + \Gamma,$$

hvilket viser, at $(a+\Gamma)(b+\Gamma) \subseteq ab + \Gamma$. Heraf følger de to sidste påstande.

En ringhomomorfi $f:\Gamma \to \Lambda$ inducerer en isomorfi $f': \frac{\Gamma}{\text{kern } f} \to f(\Gamma)$, og f er identisk med sammensætningen

$$\Gamma \xrightarrow{k} \frac{\Gamma}{\text{kern } f} \xrightarrow{f'} f(\Gamma) \xrightarrow{j} \Lambda,$$

hvor k er kanonisk og j inklusionafbildningen.

Lad Λ være en ring og $\Gamma \subseteq \Lambda$ et ideal. En ringhomomorfi $f:\Lambda \to \Lambda_1$ kan faktoriseres på formen $\Lambda \xrightarrow{k} \frac{\Lambda}{\Gamma} \xrightarrow{f'} \Lambda_1$, hvis og kun hvis kern $f \supseteq \Gamma$. At f kan faktoriseres som $f' \circ k$ er nemlig ensbetydende med, at f er konstant på hver restklasse $a + \Gamma$, $a \in \Lambda$, og det er ensbetydende med, at $f(\Gamma) = 0$.

Et ideal i $\mathbb{Z}$ må være en undergruppe i $\mathbb{Z}$, altså en mængde $n\mathbb{Z}$ for et $n \in \mathbb{Z}$. Det ses umiddelbart, at $n\mathbb{Z}$ er et ideal. Altså induceres en ringstruktur på $\mathbb{Z}_n = \frac{\mathbb{Z}}{n\mathbb{Z}}$. Med denne struktur kaldes $\mathbb{Z}_n$ en restklassering. Vi angiver multiplikationstabeller for $\mathbb{Z}_6$ og $\mathbb{Z}_8$, idet vi udelader (0)

samt (1), som er neutralelement for multiplikationen. Vi har udeladt parenteserne.

1	2	3	4	5
2	4	0	2	4
3	0	3	0	3
4	2	0	4	2
5	4	3	2	1

1	2	3	4	5	6	7
2	4	6	0	2	4	6
3	6	1	4	7	2	5
4	0	4	0	4	0	4
5	2	7	4	1	6	3
6	4	2	0	6	4	2
7	6	5	4	3	2	1

Lad Λ være en ring, og $(\Gamma_j | j \in J)$ en familie af idealer af samme slags i Λ. Det er da klart, at $\bigcap_{j\in J}\Gamma_j$ er et ideal i Λ. Hvis $M \subseteq \Lambda$ er en vilkårlig mængde, vil de idealer i Λ, som indeholder M, have en fællesmængde $I(M)$, det af M frembragte ideal, og $I(M)$ er det mindste ideal, der indeholder M. For $a_1,\ldots,a_m \in \Lambda$ bruger vi $I(a_1,\ldots,a_m)$ som betegnelse for det af $\{a_1,\ldots a_m\}$ frembragte ideal.

Disse resultater gælder både for venstre-idealer, for højreidealer og for 2-sidede idealer, og de gælder selvfølgelig også for delringe, men vi tænker først og fremmest på 2-sidede idealer.

Hvis $\Gamma_1 \subseteq \Lambda$ og $\Gamma_2 \subseteq \Lambda$ er idealer af samme slags, er $\Gamma_1 + \Gamma_2$ et ideal, men $\Gamma_1\Gamma_2$ behøver ikke at være et ideal.

Det følger umiddelbart af definitionen af ideal, at det for et højre-ideal Γ_1 og et venstre-ideal Γ_2 gælder, at $\Gamma_1\Gamma_2 \subseteq \Gamma_1 \cap \Gamma_2$, men hverken $\Gamma_1 \cap \Gamma_2$ eller $\Gamma_1 + \Gamma_2$ behøver i dette tilfælde at være et ideal.

Hvis Λ_1 og Λ_2 er ringe, har vi for de abelske grupper Λ_1 og Λ_2 med + den direkte sum $\Lambda_1 \oplus \Lambda_2$ bestående af alle par (u_1,u_2) med $u_1 \in \Lambda_1$ og $u_2 \in \Lambda_2$ og med kompositionsreglen $(u_1,u_2)+(v_1,v_2) = (u_1+v_1, u_2+v_2)$. Undergruppen $\tilde{\Lambda}_1$ af elementer $(u_1,0)$ er isomorf med Λ_1 og analogt har vi $\tilde{\Lambda}_2$, som er isomorf med Λ_2. Med produktet $(u_1,u_2)(v_1,v_2)= (u_1v_1,u_2v_2)$ bliver $\Lambda_1 \oplus \Lambda_2$ en ring, og $\tilde{\Lambda}_1$ og $\tilde{\Lambda}_2$ bliver 2-sidede idealer. Som ringe er de isomorfe med Λ_1 og Λ_2. Projektionerne af $\Lambda_1 \oplus \Lambda_2$ på Λ_1 og Λ_2 er ringhomomorfier med kerner $\tilde{\Lambda}_2$ og $\tilde{\Lambda}_1$.

Vi nævner lige kort, at man undertiden har lejlighed til at betragte ikke associative ringe, altså mængder, der er organiserede som ringe på det nær, at multiplikationen ikke forudsættes associativ. Vi har allerede haft et eksempel på det, nemlig mængden $\mathbb{E}^3$ af vektorer i $\mathbb{R}^3$ organiseret ved + og ×. På en ring kan vi iøvrigt altid definere et nyt produkt $[x,y]= xy-yx$, og med dette produkt i stedet for det rigtige fås, hvis det oprindelige produkt ikke er kommutativt, en ikke associativ ring, en såkaldt Lie algebra efter den norske matematiker Sophus Lie (1842-99). Det skal vi ikke gå ind på. I stedet vil vi gå over til at omtale diverse mere specielle slags ringe.

Som det fremgår af multiplikationstabellerne ovenfor for $\mathbb{Z}_6$ og $\mathbb{Z}_8$, indtræffer det sommetider for en ring Λ, at der findes elementer $x,y \in \Lambda\setminus\{0\}$ med $xy=0$. I så fald siger vi, at x er en venstre og y en højre 0-divisor. Hvis $a,u,v \in \Lambda$ og $au=av$, men $u \neq v$, får vi $a(v-u) = 0$, så a er venstre 0-divisor. Af $ab = 0$, $b \neq 0$ følger på den anden side, at $au = a(u+b)$. Heraf fremgår, at det, at a ikke er venstre 0-divisor, er ensbetydende med, at man kan tillade sig at forkorte med a, når a optræder som venstre faktor.

Vi kan således tale om en ring Λ uden 0-divisorer. I en sådan ring går det altid at bortforkorte fra 0 forskellige elementer i ligninger.

Ringen $\mathbb{Z}_n$ er en ring uden 0-divisorer, hvis og kun hvis n er et primtal. Af $n = rs$ følger nemlig $(r)(s) = (n) = 0$, men hvis $n = p$ er et primtal, får vi $(r)(s) = (rs)$; og $(r) \neq 0$, $(s) \neq 0$ betyder, at p ikke går op i r eller i s. Så har vi en sætning fra skolen, der siger, at så går p heller ikke op i rs. Altså er $(rs) \neq 0$.

Hvis Λ_1 og Λ_2 er ringe, som begge har elementer $\neq 0$, vil $\Lambda_1 \oplus \Lambda_2$ altid have 0-divisorer, da $(x_1,0)(0,x_2) = (0,0)$.

En ring med 1-element, er en ring med et element $1 \neq 0$, som er 2-sidet neutralelement for multiplikationen.

Hvis Λ har et 1-element, er $I(1) = \Lambda$, endda det af $\{1\}$ frembragte venstre-ideal er hele Λ. Vi kalder $I(1)$ enhedsidealet. Den modsatte yderlighed er 0-idealet $I(0) = \{0\}$. En ringhomomorfi $f:\Lambda \to \Lambda'$ med $f(1) = 0$ afbilder hele Λ ind i 0. En delring $\Gamma \in \Lambda$ kan have et 1-element, som er forskelligt fra 1-elementet i Λ. Hvis Λ og Λ' har 1-elementer 1 og 1' har $\Lambda \oplus \Lambda'$ 1-elementet (1,1'), men $\tilde{\Lambda} \subseteq \Lambda \oplus \Lambda'$ har 1-elementet (1,0).

Der er en kategori af ringe med 1-element og ringhomomorfier, som afbilder 1-element i 1-element. Den har været genstand for mange interessante undersøgelser, men vi vil slet ikke komme ind på dem her.

En kommutativ ring er selvfølgelig bare en ring, i hvilken den kommutative lov gælder for multiplikationen. I en kommutativ ring er alle idealer 2-sidede, og det samme gælder for alle 0-divisorer. Så er det klart, at et produkt bliver 0-divisor, hvis blot en af faktorerne er det, og deraf følger, at mængden af elementer, som ikke er 0-divisorer, er stabilt med hensyn til multiplikation.

En kommutativ ring med 1-element og uden 0-divisorer kaldes en integritetsring eller et integritetsområde, idet der har været en tendens til at benytte et betegnelsessystem, der til dels er hentet fra topologi. Eksempler på integritetsringe er $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$, samt $\mathbb{Z}_p$, når p er et primtal.

Som et ikke helt så velkendt eksempel på en integritetsring nævner vi, at ringen $\mathbb{Z}_2$ kan udvides til en slags kompleks ring med 4 elementer $0, 1, i$ og $1+i$, som vi regner med efter regler, der i det væsentlige er selvfølgelige bortset fra, at $i^2 = 1 + i$. Vi anfører additions- og multiplikationstabellerne.

0	1	i	1+i
1	0	1+i	i
i	1+i	0	1
1+i	i	1	0

1	i	1+i
i	1+i	1
1+i	1	i

Vi bemærker, at ringen er 4-gruppen udstyret med en multiplikation. De fra 0 forskellige elementer med multiplikation er en gruppe isomorf med $\mathbb{Z}_3$.

Et legeme er en ring K, i hvilken $K\setminus\{0\}$ med multiplikation udgør en gruppe. Sædvanligvis forudsættes det også, at multiplikationen er kommutativ, og hvis man ikke vil antage dette, kaldes K et ikke kommutativt legeme. Eksempler på legemer er $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$, medens $\mathbb{Z}$ er en integritetsring, som ikke er et legeme. Ringene $\mathbb{Z}_2$ og $\mathbb{Z}_3$ er legemer. Den i eksemplet ovenfor omtalte udvidelse af $\mathbb{Z}_2$ er et legeme. Vi skal senere give et eksempel på et ikke kommutativt legeme.

En endelig integritetsring Λ er et legeme. For $a \in \Lambda$ er den ved $\varphi(x) = a\,x$ bestemte afbildning $\varphi: \Lambda\setminus\{0\} \to \Lambda\setminus\{0\}$

nemlig injektiv, og en injektiv afbildning af en endelig mængde ind i sig selv er selvfølgelig nødt til at være bijektiv. Den tyske matematiker Edmund Landau, som var en af de karakteristiske personligheder i Göttingen under dette universitets storhedstid, før nazismen ødelagde det, kaldte denne slutning et skuffeprincip: Hvis man har n ting i n skuffer, og man ved, at der er højst én ting i hver skuffe, er der noget i alle skufferne; hvis man har n ting i n skuffer, og ingen skuffer er tomme, er der kun én ting i hver skuffe; hvis man har flere end n ting i n skuffer, må der være mere end én ting i mindst én skuffe. Hvis man har uendelig mange ting i n skuffer, må mindst en af skufferne indeholde uendelig mange ting. Der er flere variationer endnu. Skuffeprincipperne kommer i anvendelse i mange situationer.

Lad Λ være en kommutativ ring med 1-element. Et element $x \in \Lambda$ siges at være divisor (eller faktor) i et element $z \in \Lambda$, hvis der findes et element $y \in \Lambda$, som tilfredsstiller betingelsen $xy = z$. At $x \in \Lambda$ har et reciprokt element, er ensbetydende med, at x er divisor i 1. Sådanne elementer kaldes invertible elementer i Λ. Hvis x er et invertibelt element og $xy = 0$ får vi $y = 1 \cdot y = x^{-1}xy = x^{-1} \cdot 0 = 0$, så invertible elementer kan ikke være 0-divisorer. Hvis x og y er invertible, er $y^{-1}x^{-1}$ reciprok til xy, så xy er invertibelt. Altså udgør mængden af invertible elementer i Λ en gruppe med multiplikationen fra Λ som kompositionsregel. Invertible elementer i Λ kaldes også enheder i Λ.

Lad Λ være en kommutativ ring med 1-element. Et ideal $\Gamma \subseteq \Lambda$ kaldes et hovedideal, hvis der findes et element $\gamma \in \Lambda$ således at γ frembringer Γ. Nu er det klart, at $\gamma\Lambda$ er et ideal, der indeholder γ, og ethvert ideal, der indeholder γ, må indeholde $\gamma\Lambda$. Altså er $\Gamma = \gamma\Lambda$. Der findes altid hovedidealer, og blandt disse har 0-idealet $0\cdot\Lambda = \{0\}$ og enhedsidealet $1\cdot\Lambda = \Lambda$ særlig interesse. Et hovedideal Γ har i reglen flere frembringere, men af $\Gamma = \gamma_1\Lambda = \gamma_2\Lambda$ følger, at γ_1 og γ_2 er divisorer i hinanden. Kvotienterne $\gamma_1^{-1}\gamma_2$ og $\gamma_2^{-1}\gamma_1$ er hinandens reciproke, så vi ser, at frembringerne for hovedidealet afviger indbyrdes ved invertible faktorer. Det er på den anden side klart, at en frembringer for Γ gange en invertibel faktor giver en frembringer for Γ.

Lad Λ være en integritetsring, altså en kommutativ ring med 1-element og uden 0-divisorer. Et element $p \in \Lambda$ kaldes et primelement, hvis det hverken er 0 eller invertibelt, og hvis det heller ikke kan skrives som produkt af to faktorer, hvoraf ingen er invertible. Primelementerne i $\mathbb{Z}$ er således primtallene og deres modsatte tal.

Lad $M \subseteq \Lambda$ være en vilkårlig mængde. Et element $d \in \Lambda$ kaldes en største fælles divisor for M, hvis mængden af fælles divisorer for elementerne i M er identisk med mængden af divisorer i d. Det medfører, at hovedidealet $d\Lambda$ indeholder M og dermed det af M frembragte ideal. En (største) fælles divisor for M er helt det samme som en (største) fælles divisor for det af M frembragte ideal. Der findes integritetsringe med delmæng-

der, som ikke har nogen største fælles divisor. En største fælles divisor for M er helt det samme som en frembringer for det mindste hovedideal, der indeholder M, og den største fælles divisor er derfor, hvis den eksisterer, bestemt pånær en invertibel faktor.

Definition 8.5. Ved en hovedidealring forstås en integritetsring, i hvilken ethvert ideal er et hovedideal.

Vi har vist tidligere, at $\mathbb{Z}$ er en hovedidealring. Et legeme er en hovedidealring af særlig enkel karakter, idet 0-idealet og 1-idealet er de eneste idealer. Det følger af, at alle fra 0 forskellige elementer i et legeme er invertible og følgelig frembringer 1-idealet. Vi skal bruge resten af kapitlet til en nærmere diskussion af hovedidealringe.

Definition 8.6. Ved et maksimalt ideal i en ring Λ forstås et ideal, som er maksimalt i mængden af alle idealer i Λ på nær Λ selv (1-idealet).

Det er klart, at 1-idealet er det største ideal, men det holdes altså udenfor konkurrencen, når der tales om et maksimalt ideal.

Sætning 8.7. Lad Λ være en hovedidealring og $p \in \Lambda$ et element, som ikke er 0 eller invertibelt. Følgende tre betingelser er da indbyrdes ækvivalente:

1). p er et primelement,

2). $p\Lambda$ er et maksimalt ideal,

3). $\frac{\Lambda}{p\Lambda}$ er et legeme.

Bevis. Vi viser først, at 1) $\Rightarrow$ 2). Lad p være et primelement og $\Gamma \supseteq p\Lambda$ et ideal. Da Γ er et hovedideal, kan vi vælge $\gamma \in \Lambda$, så $\Gamma = \gamma\Lambda$. Men deraf følger, at der findes et element $\varepsilon \in \Lambda$, så $p = \gamma\varepsilon$. Da p er et primelement, er enten γ eller ε invertibelt, men det medfører, at $\Gamma = \Lambda$ eller $\Gamma = p\Lambda$. Dermed er påstanden vist.

Vi viser, at 2) $\Rightarrow$ 3). Hvis $\frac{\Lambda}{p\Lambda}$ ikke er et legeme, findes der et element $x \in \Lambda \setminus p\Lambda$, for hvilket $x + p\Lambda \in \frac{\Lambda}{p\Lambda}$ ikke er invertibelt. Så er $(x+p\Lambda)\frac{\Lambda}{p\Lambda} \subseteq \frac{\Lambda}{p\Lambda}$ et ideal, der hverken er 0-idealet eller 1-idealet. Dets originalmængde bliver et ideal $\Gamma \subseteq \Lambda$, og det er klart, at $p\Lambda \subset \Gamma \subset \Lambda$, så $p\Lambda$ er ikke maksimalt. Dermed er påstanden bevist.

Vi viser, at 3) $\Rightarrow$ 1). Vi antager, at $\frac{\Lambda}{p\Lambda}$ er et legeme. For $p = \lambda\mu$ får vi idealer $\lambda\Lambda$ og $\mu\Lambda$, der begge indeholder Λ. Ved den kanoniske afbildning $k:\Lambda \to \frac{\Lambda}{p\Lambda}$ bliver $k(\lambda\Lambda)$ og $k(\mu\Lambda)$ idealer, altså $\{0\}$ eller $\frac{\Lambda}{p\Lambda}$. Men så må $\lambda\Lambda$ og $\mu\Lambda$ være at finde blandt idealerne $p\Lambda$ og Λ. Deraf følger, at λ og μ må være enhed eller enhed gange p. Dermed er påstanden bevist.

Sætning 8.8. Enhver mængde M i en hovedidealring Λ har en største fælles divisor.

Bevis. Det følger umiddelbart af, at det af M frembragte ideal er et hovedideal.

Sætning 8.9. Lad Λ være en hovedidealring. Da kan en voksende følge $\Gamma_1 \subseteq \Gamma_2 \subseteq \Gamma_3 \subseteq \ldots$ af idealer i Λ højst indeholde endeligt mange forskellige idealer.

Bevis. Vi viser først, at $\Gamma = \Gamma_1 \cup \Gamma_2 \cup \Gamma_3 \cup \ldots$ er et ideal. Af $x,y \in \Gamma$ følger, at der findes tal j,k så $x \in \Gamma_j$, $y \in \Gamma_k$, men for $n \geq j,k$, har vi så $x,y \in \Gamma_n$, altså $x+y \in \Gamma_n \subseteq \Gamma$. For $\lambda \in \Lambda$, $x \in \Gamma$ findes et j, så $x \in \Gamma_j$, og så har vi $\lambda x \in \Gamma_j \subseteq \Gamma$. Altså er Γ et ideal og endda et hovedideal, så vi har et element $\lambda \in \Gamma$, for hvilket $\Gamma = \lambda\Lambda$. Så findes der imidlertid et n, for hvilket $\lambda \in \Gamma_n$, og det medfører, at $\Gamma_n \supseteq \Gamma$, og dermed er sætningen bevist.

Sætning 8.10. Lad Λ være en hovedidealring, $p \in \Lambda$ et primelement og $x,y \in \Lambda$ vilkårlige elementer. Hvis p er divisor i xy, er p divisor i x eller y.

Bevis. I $\frac{\Lambda}{p\Lambda}$ har vi $(x+p\Lambda)(y+p\Lambda) = 0+p\Lambda$, og da $\frac{\Lambda}{p\Lambda}$ er et legeme, får vi $x+p\Lambda = 0 + p\Lambda$ eller $y + p\Lambda = 0 + p\Lambda$, altså $x \in p\Lambda$ eller $y \in p\Lambda$. Dermed er sætningen bevist.

Sætning 8.11. Lad Λ være en hovedidealring og $a \in \Lambda$ et element, der hverken er 0 eller enhed. Da kan a skrives som produkt af primelementer, og af én fremstilling af a som produkt af primelementer fremkommer alle andre ved at omordne

rækkefølgen af faktorerne, samt tilføje invertible faktorer, som hæver hinanden.

Bevis. Hvis a ikke er et primelement, har vi $a = a_1b_1$, hvor $a\Lambda \subset a_1\Lambda \subset \Lambda$. Hvis a_1 heller ikke er primelement får vi $a_1 = a_2b_2$ og $a\Lambda \subset a_1\Lambda \subset a_2\Lambda \subset \Lambda$. Ifølge sætning 8.9 kan denne proces ikke fortsætte i det uendelige. Den må ende med, at vi finder en primdivisor p_1 i a, altså $a = p_1q_1$. Hvis q_1 ikke er primelement, får vi et primelement p_2 og $a = p_1p_2q_2$. Da følgen af idealer $a\Lambda \subset q_1\Lambda \subset q_2\Lambda \subset \ldots$ heller ikke kan fortsætte i det uendelige, ender vi med en opløsning i primelementer $a = p_1p_2\ldots p_n$. Dermed har vi vist eksistensen af en opløsning i primelementer.

Hvis $a = p'_1,\ldots,p'_m$ er en anden opløsning i primelementer, får vi $p_1\ldots p_n = p'_1\ldots p'_m$. Da p_1 er divisor i $p'_1\ldots,p'_m$, er p_1 divisor i p'_1 eller i $p'_2\ldots p'_m$, altså i p'_1 eller p'_2 eller $p'_3\ldots,p'_m$ osv. For et eller andet ν_1 er p_1 således divisor i p'_{ν_1}, og vi har $p'_{\nu_1} = p_1\varepsilon_{\nu_1}$, hvor ε_{ν_1} er et invertibelt element. Vi bortforkorter p_1 og får

$$p_2\ldots p_n = p'_1\ldots p'_{\nu_1-1}\varepsilon_{\nu_1}p'_{\nu_1+1}\ldots p'_m.$$

Nu går p_2 op i højre side, og der findes et $\nu_2 \neq \nu_1$, så $p'_{\nu_2} = p_2\varepsilon_{\nu_2}$, hvor ε_{ν_2} er en enhed. Vi bortforkorter p_2 osv. Hvis $n < m$, får vi tilsidst 1 på venstre side, og de tiloversblevne primelementer på højre side må så være divisorer i 1, hvilket er umuligt. Altså er $n \geq m$. Vi ender så

med et produkt af enheder på højre side, og da eventuelle tiloversblevne primfaktorer på venstre side måtte gå op i dette produkt, kan der ikke være nogen til overs, så vi har $n = m$, og produktet på højre side kommer til at bestå af faktorerne $p_j\varepsilon_{\nu_j}$, $j = 1,\ldots,n$, hvor $\varepsilon_{\nu_1},\ldots,\varepsilon_{\nu_n}$ er enheder og $(\nu_1,\ldots,\nu_n)$ er en permutation af $(1,\ldots,n)$. Dermed er sætningen bevist.

For den specielle hovedidealring $\mathbb{Z}$ er den her gennemgåede teori kendt fra skolen. Som det fremgår af teorien, er restklasseringen $\frac{\mathbb{Z}}{n\mathbb{Z}}$ et legeme, hvis og kun hvis n er et primtal.

Den franske matematiker Pierre de Fermat (1601-65) skrev i marginen i en af sine bøger, at han havde fundet et vidunderligt bevis for, at der ikke fandtes naturlige tal x,y,z og n med $n \geq z$, for hvilke ligningen $x^n+y^n = z^n$ var opfyldt. Man har ikke fundet det omtalte bevis, og alle forsøg på at vise sætningen, har været forgæves. Forsøgene på at vise Fermat's store sætning, som den nu kaldes, førte til at man studerede visse legemer af algebraiske tal, i hvilke man kunne indføre nogle hele algebraiske tal, som generaliserede de traditionelle hele tal. Derved fik man en generaliseret talteori. Det viste sig, at adskillige af de således indførte integritetsringe ikke havde entydig primtalopløsning, og endda ikke største fælles divisor. Så viste det sig imidlertid, at man kunne indføre nogle såkaldte "ideale" tal, som ikke "rigtigt" eksisterede, og derved få entydig primtalopløsning. Disse ideale tal er på det

nærmeste det samme som det, vi kalder idealer, og dette er forklaringen på det sære navn.

Den generaliserede talteori, som gav stødet til indførelsen af idealbegrebet, var et bekvemt hjælpemiddel i beviser for en række elementære talteoretiske sætninger, men ellers varede det længe, før den fandt anvendelser udenfor talteorien. I mere moderne matematik indgår idealer i meget mere forskelligartede anvendelser. Lad os f.eks. se på ringen af funktioner $f:\mathbb{R} \to \mathbb{R}$. Mængden af funktioner med fast givne nulpunkter udgør et ideal. Man kan derfor studere nulpunktsmængder ved at studere idealer. Dette bliver først interessant i flere dimensioner og for ringe af mere specielle funktioner.

Fermat's store sætning er stadig ikke bevist. Blandt de mange ting vort sidste århundredeskifte fejredes med var oprettelsen af en pris på 100.000 tyske mark for et bevis for sætningen. Der indkom et meget stort antal forkerte beviser, mest fra amatører. Prisbelønningen fik lov at dø i ubemærkethed i inflationen efter første verdenskrig.

Lad K være et legeme. En ringhomomorfi $\varphi:\mathbb{Z} \to K$ med $\varphi(1) = 1$ afbilder $\mathbb{Z}$ på en delring af K, og denne må være en integritetsring, altså isomorf med $\mathbb{Z}$ eller med $\frac{\mathbb{Z}}{p\mathbb{Z}}$ for et primtal p. I det sidste tilfælde bliver ringen et legeme, så K indeholder et dellegeme isomorft med $\frac{\mathbb{Z}}{p\mathbb{Z}}$. Legemet siges da at have karakteristik p. For $x \in K$ har vi da $px =$

$(p\cdot 1)x = 0\cdot x = 0$. Dellegemet, som er isomorft med $\frac{\mathbb{Z}}{p\mathbb{Z}}$ er det mindste dellegeme i K, og det kaldes primlegemet i K.

I det andet tilfælde er $\varphi:\mathbb{Z} \to K$ en injektiv homomorfi. For $p,q \in \mathbb{Z}$, $q \neq 0$ kan vi definere $\overline{\varphi}(\frac{p}{q})$ som løsningen til $\varphi(q)\cdot x = \varphi(p)$. Det vil blive det samme som løsningen til $\varphi(rq)\cdot x = \varphi(rp)$ for ethvert $r \in \mathbb{Z}\setminus\{0\}$. Altså får vi defineret en afbildning $\overline{\varphi}:\mathbb{Q} \to K$ med $\overline{\varphi}|\mathbb{Z} = \varphi$. Det ses ved direkte udregning, at φ er en homomorfi. For addition får vi således

$$\varphi\left(\frac{p_1}{q_1}+\frac{p_2}{q_2}\right) = \left(\frac{p_1q_2+p_2q_1}{q_1q_2}\right) = \varphi(q_1q_2)^{-1}\varphi(p_1q_2+p_2q_1) =$$

$$\varphi(q_1)^{-1}\varphi(q_2)^{-1}(\varphi(p_1)\varphi(q_2)+\varphi(p_2)\varphi(q_1)) = (\varphi(q_1)^{-1}\varphi(p_1)+$$

$$\varphi(q_2)^{-1}\varphi(p_2) = \overline{\varphi}\left(\frac{p_1}{q_1}\right) + \overline{\varphi}\left(\frac{p_2}{q_2}\right) \quad .$$

Vi ved nu også, at $\overline{\varphi}:\mathbb{Q} \to K$ er injektiv, så K indeholder en kopi af $\mathbb{Q}$, primlegemet i K. I dette tilfælde har K altså ikke endelig karakteristik. Man plejer i dette tilfælde at sige, at legemet har karakteristik 0.

ØVELSER TIL KAPITEL 8

Stikordsliste til brug ved indlæring.

Ring, delring, venstre, højre, 2-sidet ideal, faktorring, restklassering, nuldivisor, ételement, kommutativ ring, integritetsring, legeme, distributive love, modsat element, multiplikation med nul, fortegnsregning, sum og produkt af idealer, direkte sum af ringe, reciprok, invertibel, enhed, primelement, største fælles divisor, ring af homomorfier af abelsk gruppe, ideal frembragt af delmængde, hovedideal, hovedidealring, maksimalt ideal, opløsning i primfaktorer, karakteristik af legeme, skuffeprincip, Fermats store sætning.

8.1. Lad M være en mængde med en associativ kompositionsregel $*$, samt en kompositionsregel $\times$, der tilfredsstiller begge de distributive love. Vi vil kalde et element $a \in M$ regulært med hensyn til $*$, hvis $a*x = a*y \Rightarrow x=y$ for alle $x,y \in M$. Lad nu u,v,x,y være elementer af M, og lad $u\times v$ og $x\times y$ være regulære med hensyn til $*$. Vis, at $(u\times y)*(x\times v) = (x\times v)*(u\times y)$. Det antages nu, at der findes et tosidet neutralelement for x. Vis så, at regulære elementer x,y med hensyn til $*$ tilfredsstiller $x*y =$

y*x.

8.2. Distributive regler nedarves ikke på de inducerede kompositionsregler for delmængder. Prøv med små delmængder af $\mathbb{Z}$.

8.3. Lad A være en cyklisk gruppe med + som gruppeoperation, og lad $e \in A$ være et element, som frembringer A_1 og lad $a \in A$ være et vilkårligt element. Vis, at der findes netop en multiplikation på A, som er distributiv med hensyn til + og tilfredsstiller betingelsen e*e = a. Vis, at A med den således fastlagte multiplikation bliver en ring. For a = 0 fås 0-ringstrukturen, i hvilken alle produkter er 0.

8.3.1. Vis, at der eksisterer uendelig mange forskellige ringstrukturer på den uendelige cykliske gruppe $\mathbb{Z}$.

8.3.2. Vis, at bortset fra 0-ringstrukturen er alle ringstrukturer på en cyklisk gruppe af primtalorden indbyrdes isomorfe.

8.3.3. Vis, at der findes netop 3 isomorfiklasser af ringe med $\mathbb{Z}_4$ som den additive gruppe. Denne gang er 0-ringstrukturen talt med.

8.3.4. Angiv alle ringe med 6 elementer.

8.4. De ringe, der er konstrueret i opgave 8.3 med underafdelinger, er alle kommutative. Prøv at konstruere en ikke kommutativ ring med 4-gruppen som den additive gruppe.

8.5. Angiv alle ringe med 4-gruppen som additiv gruppe og med 1-element.

8.6. Lad Λ være en ring. Vi definerer en addition + og en multiplikation $\cdot$ på $\mathbb{Z}\times\Lambda$ ved $(x,\lambda) + (y,\mu) = (x+y,\ \lambda+\mu)$ og $(x,\lambda)(y,\mu) = xy + x\cdot\mu+y\cdot\lambda + \lambda\mu$. Vis, at $\mathbb{Z}\times\Lambda$ derved bliver en ring med $(1,0)$ som 1-element og med en kopi af Λ som et 2-sidet ideal.

8.7. Lad Λ være en ring med 1-element 1, og lad $\lambda \in \Lambda$ være et element, for hvilket der findes netop 1 element $\mu \in \Lambda$, som tilfredsstiller $\lambda\mu = 1$. Vis, at λ er invertibelt.

8.8. Vis, at det mindste højre ideal, der indeholder et givet venstre ideal er 2-sidet.

8.9. Lad Λ være en ring og $J \subseteq \Lambda$ et venstre ideal. Vis, at mængden $I = \{\lambda \in \Lambda \mid \forall\mu \in J(\lambda\mu=0)\}$ er et 2-sidet ideal.

8.10. Lad Λ være en ring. Vis at mængden af elementer i Λ, som hverken er venstre eller højre nuldivisorer, er stabil med hensyn til multiplikation.

8.11. Mængden $\Gamma = \{x+iy \mid x,y \in \mathbb{Z}\}$ er en delring i $\mathbb{C}$. Beskriv et vilkårligt hovedideal i Γ. Vis, at ethvert ideal $J \subseteq \Gamma$ (på nær 0-idealet) er identisk med idealet frembragt af et af de numerisk mindste fra 0 forskellige elementer i J. Altså er J en hovedidealring, og sætningen om entydig primtalsopløsning gælder i J.

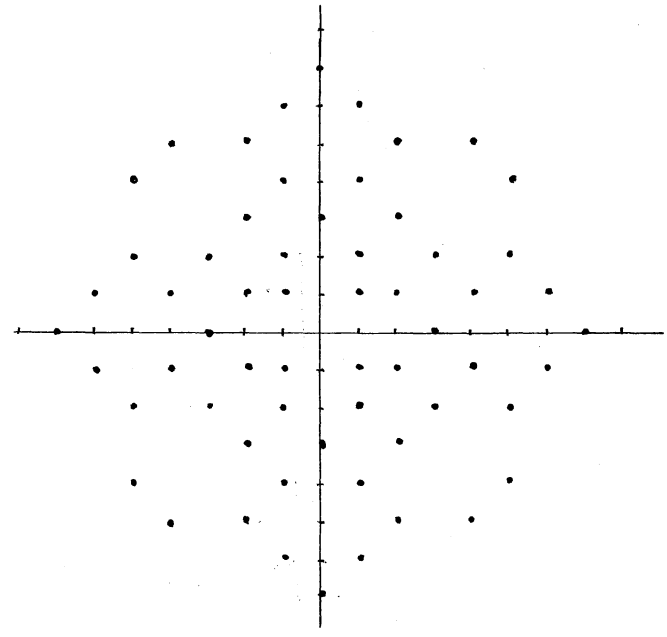
Lad $x+iy$, $x,y \in \mathbb{Z}$ være et ikke reelt primelement i Γ. Vis, at $x-iy$ også er et primelement, og at x^2+y^2 er et primelement i $\mathbb{Z}$ (altså et gammeldags primtal). Vis dernæst, at x^2+y^2 enten er 2 eller et primtal af formen $4n+1$. Heraf følger, at alle gammeldags primtal af form $4n+3$ er primelementer i Γ.

Fermat viste, at ethvert primtal af form $4n+1$ kan skrives som sum af to kvadrattal, og det spaltes derfor i to indbyrdes konjugerede primelementer i Γ.

Integritetsområdet Γ er først undersøgt af Gauss, og det kaldes derfor det Gaussiske integritetsområde. Det har en del anvendelser i talteori.

Enhederne i Γ er ± 1, $\pm i$, og de numerisk mindste primtal er $\pm 1 \pm i$, $\pm 2 \pm i$, $\pm 1 \pm i 2$, ± 3, $\pm i 3$, $\pm 2 \pm i 3$, $\pm 3 \pm i 2$, $\pm 4 \pm i$, $\pm 1 \pm i 4$, $\pm 5 \pm i 2$, $\pm 2 \pm i 5$, $\pm 6 \pm i$, $\pm 1 \pm i 6$, $\pm 5 \pm i 4$, $\pm 4 \pm i 5$, ± 7, $\pm i 7$, ...

På figuren er afsat de Gaussiske primtal, hvis numeriske værdi har sit kvadrat $\leqq 50$.



8.12. Lad Γ være en ring med 1-element 1. Lad M være en mængde af venstre idealer i Γ totalt ordnet ved inklusion. Det antages, at enhedsidealet ikke tilhører M. Vis, at foreningsmængden J af idealerne i M er et ideal forskelligt fra enhedsidealet. Benyt dernæst Zorns lemma til et bevis for, at ethvert ideal forskelligt fra enhedsidealet i en ring med 1-element kan udvides til et maksimalt ideal.

8.13. Lad K være et legeme, og lad $f:K \to K$ være en afbildning som for alle $x,y \in K$ tilfredsstiller betingelsen $f(x+y) = f(x)+f(y)$, og som desuden for

alle $x \in K \setminus \{0\}$ tilfredsstiller betingelsen $f(x)f(x^{-1}) = 1$. Vis, at f eller $-f$ for alle $x \in K$ tilfredsstiller betingelsen $f(x^2) = (f(x))^2$. Vis dernæst, at hvis K ikke har karakteristik 2, er enten f eller $-f$ en homomorfi af K på et dellegeme af K. Godt råd: Benyt identiteterne

$$x^2 = ((x-1)^{-1} - x^{-1})^{-1} + x$$

$$4xy = (x+y)^2 - (x-y)^2 .$$

8.14. Vis, at summen af elementerne i et endeligt legeme, der ikke har karakteristik 2, er lig med 0.

8.15. Lad Λ være en kommutativ ring med 1-element, og lad $I \subseteq \Lambda$ være et ideal med den egenskab, at for ethvert element $x \in I$ er $1+x$ invertibel. Vis, at ethvert maksimalt ideal indeholder I, og dernæst at fællesmængderne for alle maksimale idealer i Λ er det største ideal med den nævnte egenskab. Det kaldes radikalet for Λ. Til det sidste spørgsmål må resultatet for opgave 8.12. benyttes.

8.16. Lad Λ være en integritetsring. På mængden M_1 af alle par (x,y) af elementer fra Λ indfører vi kompositionsreglerne $(x_1,y_1)+(x_2,y_2) = (x_1y_2+x_2y_1, y_1y_2)$, $(x_1,y_1)(x_2,y_2) = (x_1x_2, y_1y_2)$. Vis, at disse er associative og kommutative, men at multiplikationen ikke

er distributiv med hensyn til additionen.

Lad $M_2 \subseteq M_1$ være mængden af par (x,y) med $y \neq 0$. Det er klart, at M_2 er stabil med hensyn til kompositionsreglerne. Vi skriver $(x,y) \sim (u,v)$, hvis $xv = yu$. Vis, at $\sim$ er ækvivalensrelation.

Vis, at de ovenfor definerede kompositionsregler definerer kompositionsregler på mængden K af ækvivalensklasser i M_2. Det er klart, at disse kompositionsregler bliver associative og kommutative. Vis, at de distributive love gælder, så K bliver en ring.

Vis, at ringen K er et legeme, og at en injektiv homomorfi $\varphi:\Lambda \to K$ kan defineres, ved at $\varphi(\lambda)$ skal være den ækvivalensklasse, der indeholder $(\lambda,1)$. Vis, at hvert element $k \in K$ er løsning til en ligning $\varphi(\lambda)x = \varphi(\mu)$, hvor $\lambda,\mu \in \Lambda$ og $\lambda \neq 0$.

Legemet K kaldes kvotientlegeme for ringen Λ. Det kan vises, at det i en vis forstand er entydigt bestemt ved Λ. Konstruktionen går med en beskeden modifikation, hvis Λ ikke har 1-element. Hvis Λ har 0-divisorer må betingelsen $y \neq 0$ i definitionen af K_2 ændres til, at y ikke må være 0-divisor, og så er det ikke mere sikkert, at φ bliver

injektiv. Det kan vises (ved temmelig komplicerede eksempler), at der ikke er nogen rimelig generalisation af teorien for kvotientlegeme til det ikke kommutative tilfælde.

KAPITEL 9

Nogle interessante ringe.

Lad Λ være en kommutativ ring og G en gruppe. Mængden M af afbildninger $f:G \to \Lambda$ er da en kommutativ ring, idet $f+g$ og fg defineres ved $(f+g)(x) = f(x)+g(x)$ og $(fg)(x) = f(x)g(x)$. Delmængden M' af afbildninger $f:G \to \Lambda$, for hvilke $f^{-1}(\Lambda \setminus \{0\})$ er en endelig mængde, (altså de afbildninger, der højst for endelig mange $x \in G$ har $f(x) \neq 0$) er åbenbart en delring, og det er for resten helt oplagt, at den er et ideal.

Ved gruppe-ringen for G over Λ forstår vi mængden M' med + og med en multiplikation defineret ved

$$(f*g)(x) = \sum_{yz=x} f(y)g(z),$$

hvor udtrykket på højre side skal forstås som summen af elementerne i mængden $\{f(y)g(z) \mid y \in G, z \in G, yz = x\}$, og det må indrømmes at dette udtryk egentlig ikke er meningsfyldt, da mængden kan være uendelig. Den indeholder imidlertid højst endelig mange elementer, som ikke er 0, og vi fortolker summen som summen af en vilkårlig endelig delmængde, der blot skal omfatte alle de fra 0 forskellige elementer.

Vi vil bruge betegnelsen ΛG for gruppe-ringen for G over Λ. Hvis $f,g,h \in \Lambda G$ er vilkårlige elementer af gruppe-ringen, har vi

$$(f*(g+h))(x) = \sum_{yz=x} f(y)(g(z)+h(z)) = \sum_{yz=x} (f(y)g(z)+f(y)h(z)) =$$

$$\sum_{yz=x} f(y)g(z) + \sum_{yz=x} f(y)h(z) = (f*g)(x)+(f*h)(x) = ((f*g)+(f*h))(x).$$

Det andet lighedstegn følger af, at multiplikationen på Λ er distributiv med hensyn til additionen. Det tredie lighedstegn kommer af, at addendernes orden ved ringaddition er uden betydning for summens værdi. Vi har bevist, at den ene distributive lov gælder i ΛG og den anden bevises selvfølgelig helt analogt. Endvidere er

$$((f*g)*h)(u) = \sum_{vz=u} \Big(\sum_{xy=v} f(x)g(y)\Big)h(z) = \sum_{xyz=u} f(x)g(y)h(z)$$

og

$$(f*(g*h))(u) = \sum_{xw=u} f(x) \sum_{yz=w} g(y)h(z) = \sum_{xyz=u} f(x)g(y)h(z) .$$

Det sidste lighedstegn i de to ligninger fremkommer, ved at summen ganges igennem med $h(z)$ i den første og med $f(x)$ i den sidste relation og derefter erstattes de dobbelte summationer med en enkelt summation. I den første relation drejer det sig om leddene $f(x)g(y)h(z)$ svarende til de sæt (x,y,z) for hvilke der findes et v, så $xy = v$ og $vz = u$, men det er netop alle (x,y,z) med $xyz = u$. For den anden

relation gælder en analog betragtning. Dermed har vi vist den associative lov, og vi ved således nu, at gruppe-ringen ΛG virkelig er en ring. Multiplikationstegnet * udelades i det følgende.

For $\lambda \in \Lambda$, $g \in G$ indfører vi betegnelsen λg for det element i ΛG, der defineres ved

$$\lambda g(x) = \begin{cases} \lambda, & \text{hvis } x = g \\ 0, & \text{hvis } x \neq g. \end{cases}$$

Den valgte betegnelse kan give anledning til misforståelse, hvis der i forvejen er defineret et ydre produkt som $\Lambda \times G \to G$, og i så fald må vi altså ændre betegnelserne.

Lad nu $f \in \Lambda G$ være et vilkårligt element. Vi kan da vælge indbyrdes forskellige $g_1,\ldots,g_n \in G$, således at $f(x) = 0$, hvis $x \in G$ ikke er et af elementerne g_ν. Hvis vi nu har $f(g_\nu) = \lambda_\nu \in \Lambda$ for $\nu = 1,\ldots,n$, får vi

$$f = \lambda_1 g_1 + \ldots + \lambda_n g_n.$$

For elementerne $\lambda g \in \Lambda G$ har vi regnereglerne

$$(\lambda_1+\lambda_2)g = \lambda_1 g + \lambda_2 g, \quad \lambda_1 g_1 \lambda_2 g_2 = \lambda_1 \lambda_2 g_1 g_2.$$

Gruppe-ringen består således af alle elementer af formen $\lambda_1 g_1 + \ldots + \lambda_n g_n$ med $n \in \mathbb{N}$, $g_1,\ldots,g_n \in G$, $\lambda_1,\ldots,\lambda_n \in \Lambda$, og to sådanne elementer er ens, hvis og kun hvis alle led λg, der optræder i det ene, men ikke det andet, har $\lambda = 0$. Vi regner iøvrigt med udtrykkene ganske som med sædvanlige flerleddede udtryk.

Lad $e \in G$ være neutralelement. Afbildningen $\varphi:\Lambda \to \Lambda G$ defineret ved $\varphi(\lambda) = \lambda e$ er da en injektiv ringhomomorfi, og billedmængden $\{\lambda e | \lambda \in \Lambda\}$ er en kopi af Λ. Vi finder det praktisk at skrive λ i stedet for λe og betragte Λ selv som en delring af ΛG.

Hvis $1 \in \Lambda$ er 1 1-element får vi en afbildning $\psi:G \to \Lambda G$ defineret ved $\psi(g) = 1 \cdot g$ for alle $g \in \Lambda$, og det er klart, at ψ bliver en injektiv homomorfi af G ind i ΛG med multiplikation. Vi skriver g i stedet for $1g$ og regner, som om G er en delmængde af ΛG. Elementet $1 \cdot e$ er neutralelement for gruppe-ringen, og vi betegner det med 1 eller e, som det passer os.

Eksempel. Elementerne i $\mathbb{R}\mathbb{Z}_2$ kan skrives a_0+a_1x med $a_0,a_1 \in \mathbb{R}$, medens x er det ikke neutrale element i $\mathbb{Z}_2$, så vi har $x^2 = e = 1$. Kompositionsreglerne i gruppe-ringen bliver

$$(a_0+a_1x) + (b_0+b_1)x = (a_0+b_0) + (a_1+b_1)x$$

$$(a_0+a_1x)(b_0+b_1x) = (a_0b_0+a_1b_1) + (a_0b_1+a_1b_0)x$$

Elementerne $a \pm ax$ bliver 0-divisorer, idet $(a \pm ax)(a \mp ax) = 0$.

Vi kan bruge $\{1,i,-1,-i\}$ med multiplikation som en kopi af $\mathbb{Z}_4$, og vi får da en gruppe-ring $\mathbb{R}\mathbb{Z}_4$ bestående af elementer af formen

$$a_0 + a_1' \cdot\!- 1 + a_1 \cdot i + a_1' \cdot\!- i,$$

hvor $a_0, a_0', a_1, a_1' \in \mathbb{R}$. Additionen sker på den helt selvfølgelige måde, og det samme gælder multiplikationen, som defineres ved

$$(a_0+a_0' \cdot\!-1+a_1 \cdot i + a_1' \cdot\!- i)\,(b_0+b_0' \cdot\!-1+b_1 \cdot i + b_1' \cdot\!- i) =$$

$$(a_0b_0+a_0'b_0'+a_1b_1'+a_1'b_1)+(a_0b_0'+a_0'b_0+a_1b_1+a_1'b_1') \cdot\!-1+$$

$$(a_0b_1+a_1b_0+a_0'b_1'+a_1'b_0')i+(a_0b_1'+a_1'b_0+a_0'b_1+a_1b_0') \cdot\!- i.$$

Det er ikke $\mathbb{C}$, vi finder igen på den måde, men vi kan få $\mathbb{C}$ til at opstå som kvotientring. Lad J være mængden af elementer af den specielle form

$$x = a_0 + a_0 \cdot\!-1 + a_1 \cdot i + a_1 \cdot\!- i\ .$$

Det er klart, at addition af elementer i J giver elementer i J, og det er klart, at multiplikation af et element fra J med et reelt tal igen giver et element fra J. Nu er

$$x(b_0+b_0' \cdot\!-1+b_1 \cdot i + b_1' \cdot\!- i) = b_0x+b_0'(x \cdot\!-1) + b_1(x \cdot i)+b_1'(x \cdot\!- i)),$$

og det ses umiddelbart, at $x \cdot\!-1$, $x \cdot i$ og $x \cdot\!- i$ igen tilhører J. Dermed har vi vist, at $J \subseteq \mathbb{R}\mathbb{Z}_4$ er et ideal. Det ses nu let, at hver restklasse $a_0+a_0' \cdot\!-1+a_1 \cdot i+a_1' \cdot\!- i + J$ indeholder netop et element, i hvilket -1 og $-i$ har koefficient 0, nemlig $(a_0-a_0') + (a_1-a_1')i$, og regningen med disse repræsentanter bliver netop regningen med komplekse tal.

I kapitlet om grupper omtalte vi kvaterniongruppen K bestående af $\pm 1, \pm i, \pm j, \pm k$ med kompositionsregler

$$i^2 = j^2 = k^2 = -1,\ jk = -kj = i,\ ki = -ik = j,\ ij = -ji = k,$$

og sædvanlige fortegnsregler. Vi får en gruppe-ring $\mathbb{R}K$ bestående af elementer

$$a_0+a_0'\cdot -1+a_1\cdot i+a_1'\cdot -i+a_2\cdot j+a_2'\cdot -j+a_3\cdot k+a_3'\cdot -k.$$

Vi vil ikke skrive multiplikationsreglen op - der kommer 64 led, og det er jo lidt rigeligt. Det ses imidlertid helt som før, at elementerne med $a_0=a_0' = a_1=a_1' = a_2=a_2' = a_3=a_3' = 0$ udgør et ideal, så vi får en kvotientring $\mathbb{K}$ bestående af sideklasser, der hver indeholder netop én repræsentant af formen $a_0+a_1i + a_2j + a_3k$, og regning med disse repræsentanter foregår efter reglerne

$$(a_0+a_1i+a_2j+a_3k) + (b_0+b_1i+b_2j+b_3k) =$$

$$(a_0+b_0)+(a_1+b_1)i+(a_2+b_2)j+(a_3+b_3)k,$$

og

$$(a_0+a_1i+a_2j+a_3k)(b_0+b_1i+b_2j+b_3k) =$$

$$(a_0b_0-a_1b_1-a_2b_2-a_3b_3)+(a_0b_1+a_1b_0+a_2b_3-a_3b_2)i +$$

$$(a_0b_2+a_2b_0+a_3b_1-a_1b_3)j+(a_0b_3+a_3b_0+a_1b_2-a_2b_1)k.$$

Vi ved, at $\mathbb{K}$ med disse regneregler bliver en ikke kommutativ ring. For

$$u = a_0 + a_1 i + a_2 j + a_3 k$$

definerer vi det konjugerede element

$$\bar{u} = a_0 - a_1 i - a_2 j - a_3 k,$$

og regnereglerne giver

$$u\bar{u} = a_0^2 + a_1^2 + a_2^2 + a_3^2,$$

så vi kan indføre numerisk værdi ved

$$|u| = \sqrt{u\bar{u}}.$$

Det ses endvidere umiddelbart, at vi har regnereglerne

$$\overline{u + v} = \bar{u} + \bar{v}; \quad \overline{uv} = \bar{v}\bar{u}.$$

Derfor er

$$|uv|^2 = uv\overline{uv} = uv\bar{v}\bar{u} = u|v|^2\bar{u} = u\bar{u}|v|^2 = |u|^2|v|^2,$$

så vi har $|uv| = |u||v|$. Da $|u| = 0$ er ensbetydende med $u = 0$, finder vi, at $\mathbb{K}$ er uden 0-divisorer. Men vi ser yderligere, at $u \neq 0$ har $\frac{\bar{u}}{|u|^2}$ som inverst element, og dermed har vi vist, at $\mathbb{K}$ er et legeme. Det kaldes legemet af kvaternioner.

Kvaternionerne indførtes af Sir William Hamilton (1805-65). Vi skal ikke gå nærmere ind på dem, blot nævne, at de er et eksempel på et ikke kommutativt legeme. De har været meget grundigt undersøgt, og de har været anvendt i mekanisk fysik. De spiller stadig en vis rolle.

Det skal tilføjes, at det kan vises, at alle endelige legemer er kommutative, men det er ikke helt let.

Kvaternionerne af form $x+iy$ udgør en kopi af komplekse tal, og ved omskrivningen

$$x_0 + ix_1 + jx_2 + kx_3 = x_0 + ix_1 + (x_2+ix_3)j = z_1 + z_2j,$$

får vi en fremstilling af kvaternioner ved komplekse tal. Vi kan regne med disse udtryk på sædvanlig vis, men vi må huske, at vi har $z_2j = j\overline{z}_2$ i stedet for den kommutative lov.

Lad nu Λ og Λ_1 være kommutative ringe og G en gruppe. Lad $\varphi:\Lambda \to \Lambda_1$ være en ringhomomorfi. Lad $f, f_1, f_2: G \to \Lambda$ være elementer af gruppe-ringen ΛG. Vi definerer $\varphi_G:\Lambda G \to \Lambda_1 G$ ved $\varphi_G(f) = \varphi \circ f$. Vi har da trivielt $\varphi_G(f_1+f_2) = \varphi_G(f_1) + \varphi_G(f_2)$ og knap så trivielt for ethvert $x \in G$

$$\varphi_G(f_1f_2)(x) = (\varphi \circ f_1f_2)(x) = \varphi(f_1f_2(x)) = \varphi(\sum_{yz=x} f_1(y)f_2(z)) =$$

$$\sum_{yz=x} \varphi(f_1(y))\varphi(f_2(z)) = \sum_{yz=x} (\varphi_G(f_1)(y))(\varphi_G(f_2)(z)) =$$

$$(\varphi_G(f_1)\varphi_G(f_2))(x).$$

Altså er φ_G en ringhomomorfi, induceret af φ. Iøvrigt er

$$\varphi_G(\lambda_1 g_1 + \ldots + \lambda_n g_n) = \varphi(\lambda_1)g_1 + \ldots + \varphi(\lambda_n)g_n.$$

Hvis Λ og Λ_1 har 1-elementer, og φ afbilder 1-element i 1-element, vil også φ_G afbilde 1-element i 1-element.

Gruppe-ringen $\Lambda\mathbb{Z}$ er ringen af generaliserede polynomier

$$\lambda_p X^p + \lambda_{p+1} X^{p+1} + \ldots + \lambda_{p+n} X^{p+n}$$

hvor X er frembringer for $\mathbb{Z}$. Specielt har vi 0-polynomiet med alle koefficienter 0 som neutralelement for +. For alle andre polynomier findes der netop ét udtryk med $\lambda_p \neq 0$ og $\lambda_{p+n} \neq 0$, og så er p den mindste og $p+n$ den højeste forekommende eksponent. For $n=0$ består polynomiet af et eneste led. Multiplikation foregår efter reglen

$$(\lambda_p X^p + \ldots + \lambda_{p+n} X^{p+n})(\lambda'_{p'} X^{p'} + \ldots + \lambda'_{p'+n'} X^{p'+n'}) =$$

$$\lambda_p \lambda'_{p'} X^{p+p'} + (\lambda_p \lambda'_{p+1} + \lambda_{p+1} \lambda'_p) X^{p+p'+1} + \ldots + \lambda_{p+n} \lambda'_{p'+n'} X^{p+p'+n+n'}$$

Hvis Λ er en ring uden 0-divisorer, vil de mindste og de højeste forekommende eksponenter adderes ved multiplikation af de generaliserede polynomier, og $\mathbb{Z}$ bliver en ring uden 0-divisorer.

Ringen $\Lambda[X]$ af polynomier over Λ er delringen af $\Lambda\mathbb{Z}$ omfattende de generaliserede polynomier, der ikke indeholder negative eksponenter. Graden af et polynomium er

den højeste forekommende eksponent. Hvis Λ ikke har 0-divisorer, adderes graderne ved multiplikation af polynomier. Polynomierne af grad 0 udgør sammen med 0-polynomiet en kopi af Λ, delringen af "konstante" polynomier.

For et polynomium i $\Lambda[X]$ vil vi anvende en betegnelse

$$P(X) = a_0 + a_1X+\ldots+a_nX^n$$

hvori frembringeren X for $\mathbb{Z}$ er anført eksplicit. For $\lambda \in \Lambda$ er

$$P(\lambda) = a_0 + a_1\lambda+\ldots+a_n\lambda^n$$

et element af Λ, så polynomiet $P(X)$ inducerer en afbildning $P:\Lambda \to \Lambda$. For $\lambda \in \Lambda$ definerer $ev_\lambda(P(X)) = P(\lambda)$ en afbildning $ev_\lambda:\Lambda(X) \to \Lambda$, evaluationsafbildningen eller værdiafbildningen.

Sætning 9.1. Afbildningen $ev_\lambda:\Lambda(X) \to \Lambda$ er en homomorfi.

Bevis. Det er klart for vilkårlige polynomier

$$P(X) = a_0 + a_1X+\ldots+a_pX^p,\ Q(X) = b_0 + b_1X+\ldots+b_qX^q,$$

at $ev_\lambda(P(X)+Q(X)) = ev_\lambda P(X) + ev_\lambda Q(X)$. Desuden er

$$\mathrm{ev}_\lambda(P(X)Q(X)) = \mathrm{ev}_\lambda\Big(\sum_{j=0}^{p}\sum_{k=0}^{q} a_j b_k X^{j+k}\Big) = \sum_{j=0}^{p}\sum_{k=0}^{q} a_j b_k \lambda^{j+k} =$$

$$\sum_{j=0}^{p} a_j \lambda^j \sum_{k=0}^{q} b_k \lambda^k = \mathrm{ev}_\lambda P(X)\mathrm{ev}_\lambda Q(X).$$

Dermed er sætningen bevist.

Populært sagt er sætningen rigtig, fordi vi regner med de abstrakte polynomier ganske som vi lærte i skolen at regne med rigtige polynomier. Fordelen ved den abstrakte definition er, at vi har givet den "ubestemte" X en helt konkret betydning, og alligevel undgået, at X er et element af ringen.

Lad $L \supseteq \Lambda$ være en ring, der har Λ som delring. Så inducerer inklusionsafbildningen $j:\Lambda \to L$ en injektiv afbildning $\bar{j}:\Lambda\mathbb{Z} \to L\mathbb{Z}$, og ved restriktion giver denne en injektiv afbildning $\tilde{j}:\Lambda[X] \to L[X]$. Der ligger ikke andet i dette, end at et polynomium over Λ kan fortolkes som et polynomium over L. Derved bliver $\mathrm{ev}_\lambda(P(X))$ defineret også for $\lambda \in L$.

Nu vil vi gå over til specielt at undersøge ringen $K[X]$ af polynomier over et legeme K. Det fremgår af hvad vi allerede har vist, at $K[X]$ er en integritetsring. Vi vil nu vise den vigtige sætning om ufuldstændig division af polynomier. Den er kendt fra skolen.

Sætning 9.2. Lad K være et legeme, og lad $D(X)$ og $E(X)$ være polynomier i $K[X]$. Hvis $D(X)$ ikke er 0-polynomiet, findes der et og kun et polynomium $Q(X) \in K[X]$, for hvilket vi har

$$E(X) = D(X)Q(X) + R(X),$$

hvor $R(X) \in K[X]$ er et polynomium af effektivt lavere grad end $D(X)$, eventuelt 0-polynomiet.

Bevis. Hvis der findes to polynomier $Q_1(X)$ og $Q_2(X)$ med den omtalte egenskab, gælder en relation

$$D(X)Q_1(X) + R_1(X) = D(X)Q_2(X) + R_2(X),$$

hvor $R_1(X)$ og $R_2(X)$ har lavere grad end $D(X)$. Idet vi skriver ligningen på formen

$$D(X)(Q_1(X) - Q_2(X)) = R_2(X) - R_1(X)$$

ser vi at $D(X)(Q_1(X)-Q_2(X))$ har effektivt lavere grad end $D(X)$, og det sker kun for $Q_1(X) = Q_2(X)$. Dermed har vi vist entydigheden.

For at vise eksistensen, bemærker vi først, at vi for hvilket som helst polynomium $\tilde{Q}(X)$ kan vælge $\tilde{R}(X)$, så vi har relationen

$$E(X) = D(X)\tilde{Q}(X) + \tilde{R}(X).$$

Lad os antage, at $\tilde{R}(X)$ har mindst samme grad som $D(X)$.

Vi har udtryk

$$D(X) = d_0 + d_1X+\ldots+d_pX^p,\ d_p \neq 0,$$

$$\tilde{R}(X) = \tilde{r}_0 + \tilde{r}_1X+\ldots+\tilde{r}_qX^q,\ \tilde{r}_q \neq 0,\ q \geqq p.$$

Vi indfører

$$\bar{Q}(X) = \tilde{Q}(X) + \frac{\tilde{r}_q}{d_p} X^{q-p}$$

$$\bar{R}(X) = \tilde{R}(X) - \frac{\tilde{r}_q}{d_p} X^{q-p}D(X),$$

og vi ser da, at $\bar{R}(X)$ har grad $\leqq q - 1$, og at vi har

$$E(X) = D(X)\bar{Q}(X) + \bar{R}(X).$$

Efter højst $q - p + 1$ gentagelser af denne proces får vi en fremstilling med de i sætningen påståede egenskaber. Processen kaldes ufuldstændig division eller division med rest.

I denne sammenhæng skal vi kort gentage nogle resultater, der kendes fra skolen, med den tilføjelse, at de i det store og hele (vi lover at fremhæve undtagelsen, når vi når til den) gælder for polynomier over vilkårlige legemer. For $D(X) = X - \lambda$, hvor $\lambda \in K$, får vi specielt

$$E(X) = (X-\lambda)E_1(X) + \rho,$$

hvor ρ er et polynomium af grad 0, eller eventuelt nulpolynomiet, altså $\rho \in K$. Ved at anvende ev_λ på begge sider får vi

$$E(\lambda) = \rho.$$

Hvis $E(\lambda) = 0$, kalder vi λ en rod i $E(X)$. Der findes da et naturligt tal p, således at $E(X) = (X-\lambda)^p E_p(X)$ og $E_p(\lambda) \neq 0$. Tallet p kaldes multipliciteten af λ. Da $K[X]$ er en integritetsring, vil de fra λ forskellige rødder i $E(X)$ netop være rødderne i $E_p(X)$. Generelt har vi en opløsning i faktorer

$$E(X) = (X-\lambda_1)^{p_1}\ldots(X-\lambda_\nu)^{p_\nu}\tilde{E}(X),$$

hvor $\tilde{E}(X)$ er et polynomium, som ingen rødder har. Tallet $p_1+\ldots+p_\nu$ er antallet af rødder i $E(X)$ talt med multiplicitet. Det følger heraf, at en ligning af grad n har højst n rødder, selv om rødderne tælles med multiplicitet. For polynomier $P_1(X)$ og $P_2(X)$ af grad $\leq n$ finder vi, at afbildningerne $P_1, P_2 : K \to K$ ikke vil være indbyrdes identiske, med mindre $P_1(X) = P_2(X)$ eller K er et legeme med højst n elementer. (Dette forbehold er den ovenfor nævnte undtagelse).

Eksempel. I legemet $\mathbb{Z}_p$ med p elementer, hvor p er et primtal, er $\mathbb{Z}_p \setminus \{0\}$ med multiplikation som operation en gruppe af orden $p-1$. Derfor tilfredsstiller ethvert element $\lambda \in \mathbb{Z}_p \setminus \{0\}$ betingelsen $\lambda^{p-1} = 1$. Heraf følger, at polynomiet $P(X) = X^p - X$ tilfredsstiller betingelsen $P(\lambda) = 0$ for alle $\lambda \in \mathbb{Z}_p$, så $P(X)$ definerer den samme afbildning $\mathbb{Z}_p \to \mathbb{Z}_p$ som 0-polynomiet.

Sætning 9.3. For ethvert legeme K er $K[X]$ en hovedidealring.

Bevis. Lad $J \subseteq K[X]$ være et ideal. Hvis $J = \{0\}$ er $J = (0)$, altså et hovedideal. Hvis $J \neq 0$, kan vi vælge et polynomium $D(X) \in J \setminus \{0\}$ af lavest mulig grad. For $E(X) \in J$ kan vi så vælge et polynomium $Q(X)$, så $E(X) - Q(X)D(X) = R(X)$ har effektivt lavere grad end $D(X)$. Men vi har $R(X) \in J$ og vi kan derfor slutte, at $R(X) = 0$, altså $E(X) = Q(X)D(X)$. Dermed har vi vist, at $J = (D(X))$, og dermed er sætningen bevist.

Det er klart, at elementerne af $K \setminus \{0\}$, altså de konstante polynomier undtagen 0-polynomiet, er de invertible elementer i $K[X]$. Frembringerne for et hovedideal J afviger indbyrdes ved invertible faktorer, så et ideal J har netop 1 frembringer af den specielle form

$$D(X) = X^p + a_{p-1}X^{p-1} + \ldots + a_0.$$

Et polynomium af denne form kaldes normeret.

Vilkårlige polynomier $P_1(X), \ldots, P_n(X)$ frembringer et ideal

$$J = \{P_1(X)Q_1(X) + \ldots + P_1(X)Q_n(X) \mid Q_1(X), \ldots, Q_n(X) \in K[X]\},$$

og dette ideal er et hovedideal, så det frembringes af 1 polynomium

$$D(X) = P_1(X)H_1(X) + \ldots + P_n(X)H_n(X),$$

hvor $H_1(X), \ldots, H_n(X) \in K[X]$. Altså er $D(X)$ divisor i

$P_1(X),\ldots,P_n(X)$, og udtrykket for $D(X)$ ved disse polynomier viser, at mængden af divisorer i $D(X)$ netop er mængden af fælles divisorer i $P_1(X),\ldots,P_n(X)$, og $D(X)$ er således en største fælles divisor for $P_1(X),\ldots,P_n(X)$.

Et polynomium $P(X)$ kaldes irreducibelt, hvis det ikke kan skrives som produkt af 2 polynomier af grad > 0, altså hvis $P(X)$ er et primelement i $K[X]$, og det er ifølge sætning 8.7 ensbetydende med, at idealet $(P(X))$ er maksimalt, og med, at restklasseringen $\frac{K[X]}{(P(X))}$ er et legeme.

Hvis $P(X)$ har grad 1, er det irreducibelt, og hver restklasse $Q(X) + (P(X))$ indeholder netop et konstant polynomium $\lambda \in K$, så restklassen er $\lambda + (P(X))$, og $\frac{K[X]}{(P(X))}$ bliver så isomorf med K.

Ifølge sætning 8.11 kan et polynomium $P(X)$ skrives som produkt af irreducible polynomier og bortset fra konstante faktorer kun på 1 måde.

Efter disse generalisationer af resultater, som er velkendte fra skolen, vil vi fortsætte med en sætning, som vi skal bruge i teorien for vektorrum. Vi minder om, at ikke alle andengradspolynomier i $\mathbb{R}[X]$ har løsninger, og det var motiveringen for vor indførelse af $\mathbb{C}$, idet vi har $\mathbb{R}[X] \subseteq \mathbb{C}[X]$, og alle andengradspolynomier i $\mathbb{C}[X]$ har løsninger. Den følgende sætning generaliserer denne situation.

Sætning 9.4. Lad K være et legeme og $P(X) \in K[X]$ et polynomium af grad ≥ 2. Der findes da et legeme L og en injektiv homomorfi $j:K \to L$, for hvilken det gælder, at den inducerede homomorfi $\bar{j}:K[X] \to L[X]$ afbilder $P(X)$ på et polynomium, der opløses i førstegradsfaktorer i $L[X]$.

Bevis. Vi ser først på det specielle tilfælde, hvor $P(X)$ er irreducibelt. Idet Y er frembringer for en uendelig cyklisk gruppe, der ikke har elementer fælles med den af X frembragte, betragter vi $K[Y]$, som blot er en kopi af $K[X]$, samt $P(Y) \in K[Y]$, hvor $P(Y)$ fås af $P(X)$ ved at skrive Y i stedet for X. Vi definerer nu $L = \frac{K[Y]}{(P(Y))}$. Inklusionsafbildningen $K \to K[Y]$ sammensat med den kanoniske afbildning $K[Y] \to \frac{K[Y]}{(P(Y))}$ giver en injektiv afbildning $K \to L$, og derved kan $P(X)$ fortolkes som et polynomium over L. Men indsættelse af $Y + (P(Y))$ for X i $P(X)$ giver $P(Y) + (P(Y)) = (P(Y))$, og det er 0-elementet i L, så Y er rod i $P(X)$. Altså er $P(X)$ ikke irreducibelt over L.

Lad nu $P(X)$ være vilkårligt. Vi opløser $P(X)$ i irreducible faktorer i $K[X]$. Hvis alle disse faktorer har grad 1, kan vi blot vælge $L = K$. Ellers kan vi vælge L_1, så L_1 indeholder en kopi af K, og således at mindst en af de irreducible faktorer ikke mere er irreducibel over L_1.

Så opløser vi igen i irreducible faktorer, og vi får mindst én faktor mere end før. Hvis der stadig er irreducible faktorer af grad ≥ 2, kan vi vælge et nyt legeme $L_2 \supset L_1$ på samme måde, så vi over L_2 får mindst én irreducibel faktor mere. Efter endelig mange skridt bliver antallet af faktorer lige så stort som graden af $P(X)$, og så er alle faktorerne af første grad. Dermed er sætningen bevist.

Det er bare selve sætningen, vi får brug for, så det er ikke rimeligt at ofre tid på en mere dybtgående undersøgelse af sagen. Hvis K er et legeme og $P(X) \in K[X]$ irreducibelt af grad ≥ 2, og $L > K$ et legeme, i hvilket $P(X)$ har en rod α, da findes der et mindste legeme $L_1 \subseteq L$, som indeholder K og α. Hvis $L_1 \supset K$ og $L_2 \supset K$ er sådanne mindste udvidelser, i hvilke $P(X)$ har en rod, da findes en isomorfi $\varphi: L_1 \to L_2$, som afbilder hvert element af K på sig selv. Hvis $P(X)$ er et vilkårligt polynomium, gælder der et tilsvarende resultat om eksistens og entydighed på nær isomorfi af en mindste udvidelse $L \supset K$, i hvilken $P(X)$ kan opløses i faktorer af grad 1. Vi får nu en gruppe af automorfier $L \to L$, som lader hvert element af K ligge fast, og med sammensætning som komposition. Denne gruppe kaldes Galoisgruppen for P. Det viser sig nu, at der er en bijektiv forbindelse mellem de legemer M, der tilfredsstiller $L \supseteq M \supseteq K$, og Galoisgruppens undergrupper. Af denne forbindelse udledes bl.a. Abels sætning om, at der ikke findes nogen formel, der udtrykker løsningen i en vilkårlig femtegrads-

ligning med komplekse koefficienter ved hjælp af elementære regneoperationer og roduddragning.

Sætning 9.5. Lad L være et legeme, og $K \subseteq L$ et dellegeme, og lad $P_1(X)$ og $P_2(X)$ være polynomier i $K[X]$. Hvis $P_1(X)$ og $P_2(X)$ har største fælles divisor $D(X)$, vil de også som elementer af $L[X]$ have største fælles divisor $D(X)$. Hvis $P_1(X)$ og $P_2(X)$ har en fælles rod i L, vil deres største fælles divisor i $K[X]$ være af grad ≥ 1.

Bevis. At $P_1(X)$ og $P_2(X)$ har $D(X)$ som største fælles divisor i $K[X]$ betyder, at $P_1(X)$ og $P_2(X)$ i $K[X]$ frembringer idealet $(D(X)) = D(X)K[X]$ Et ideal i $L[X]$, som indeholder $P_1(X)$ og $P_2(X)$, må indeholde $D(X)K[X]$ og derfor er $D(X)L[X]$ det af $P_1(X)$ og $P_2(X)$ frembragte ideal i $L[X]$ og deraf følger, at $D(X)$ er største fælles divisor i $L[X]$ for $P_1(X)$ og $P_2(X)$. Hvis $P_1(X)$ og $P_2(X)$ har en fælles rod i L, er $D(X)$ af grad ≥ 1, da $D(X)$ også er fælles divisor i $L[X]$ for $P_1(X)$ og $P_2(X)$. Dermed er sætningen bevist.

Sætningen giver udtryk for, at det at være største fælles divisor er en absolut egenskab i modsætning til de egenskaber, der kun har gyldighed i relation til et bestemt legeme, f.eks. irreducibilitet.

Et polynomium

$$P(X) = a_0 + a_1X+\ldots+a_pX^p$$

har en differentialkvotient

$$P'(X) = a + 2a_2X+\ldots+pa_pX^p.$$

Dette begreb er indført i skolen for polynomier over de reelle tal, men det er klart, at $P'(X)$ er et udtryk, der giver mening for et vilkårligt legeme. Det kan så eftervises ved blot at regne efter, at $P(X) + Q(X)$ har differentialkvotient $P'(X) + Q'(X)$, medens $P(X)Q(X)$ har differentialkvotient $P'(X)Q(X) + P(X)Q'(X)$. Af

$$P(X) = (X-\lambda)^q P_1(X),$$

hvor $P_1(\lambda) \neq 0$ følger

$$P'(X) = q(X-\lambda)^{q-1}P_1(X) + (X-\lambda)^qP_1'(X) = (X-\lambda)^{q-1}P_2(X),$$

hvor $P_2(X) = qP_1(X) + (X-\lambda)P_1'(X)$. Heraf følger, at en q-dobbelt rod i $P(X)$ er mindst q-1-dobbelt rod i $P'(X)$. Vi får $P_2(\lambda) = qP_1(\lambda)$. Vi får således $P_2(\lambda) \neq 0$, hvis legemets karakteristik ikke er divisor i multipliciteten q. I legemer, som ikke har endelig karakteristik, vil et element λ være q-dobbelt rod i et polynomium $P(X)$, hvis og kun hvis den er rod i $P(X)$ og i differentialkvotienterne op til orden q-1. Derimod kan det for polynomier over legemer med endelig karakteristik indtræffe, at en rod i et polynomium er rod med endnu højere multiplicitet i differentialkvotienten.

Et særlig interessant specialtilfælde er legemet $\mathbb{C}$ af komplekse tal med dellegemet $\mathbb{R}$ af reelle tal. Lad $P(X) \in \mathbb{C}[X]$ være et polynomium

$$P(X) = a_0 + a_1X+\ldots+a_nX^n.$$

Automorfien $\kappa:\mathbb{C} \to \mathbb{C}$ defineret ved $\kappa(z) = \overline{z}$ udvides til en automorfi $\tilde{\kappa}:\mathbb{C}[X] \to \mathbb{C}[X]$ ved

$$\kappa(P(X)) = \overline{a}_0 + \overline{a}_1X+\ldots+\overline{a}_nX^n = \overline{P}(X)$$

Sammenhængen mellem afbildningerne $P:\mathbb{C} \to \mathbb{C}$ og $\overline{P}:\mathbb{C} \to \mathbb{C}$ er givet ved

$$\overline{P(z)} = \overline{P}(\overline{z}).$$

Af

$$P(X) = (X-\lambda)^q P_1(X)$$

følger

$$\overline{P}(X) = (X-\overline{\lambda})^q \overline{P}_1(X),$$

så vi kan slutte, at det konjugerede tal til en q-dobbelt rod i $P(X)$ er en q-dobbelt rod i $\overline{P}(X)$.

De elementer af $\mathbb{C}[X]$, der afbildes på sig selv ved κ, er netop polynomier i $\mathbb{R}[X]$, altså polynomierne med reelle koefficienter, og for disse giver vort sidste resultat specielt, at rødderne i et polynomium $P(X) \in \mathbb{R}[X]$ er dels reelle, dels komplekse, og disse sidste falder i par af konjugerede, således at konjugerede rødder har sam-

me multiplicitet.

Algebraens fundamentalsætning siger, at polynomierne i $\mathbb{C}[X]$ opløses helt i faktorer af første grad. Da

$$(X-\lambda)(X-\overline{\lambda}) = X^2 - (\lambda+\overline{\lambda})X + |\lambda|^2$$

er et polynomium med reelle koefficienter, vil polynomier i $\mathbb{R}[X]$ opløses i irreducible faktorer af grad ≤ 2. Specielt kan vi slutte, at et polynomium $P(X) \in \mathbb{R}[X]$ af ulige grad har mindst én rod.

ØVELSER TIL KAPITEL 9

Stikord:

Kvaternioner, komplekse rødder i reelle polynomier, rod, multiplicitet, irreducibel, opløsning i faktorer, største fælles divisor, gruppe-ring, udvidelse af ringhomomorfi til gruppe-ringen, grad, konstant polynomium, nulpolynomiet, evaluationsafbildningen, ufuldstændig division, differentialkvotient af polynomium, konstruktion af udvidelseslegeme, i hvilket et givet polynomium kan opløses i faktorer af første grad.

9.1. Angiv kompositionsreglerne i grupperingen $\mathbb{R}\,\mathbb{Z}_2{}^2$, hvor $\mathbb{Z}_2{}^2$ er 4-gruppen.

9.2. Find kvaternioner u og v som tilfredsstiller

$$u(2+i3-j-k2) = 2+i6-j3+k4$$
$$(2+i3-j-k2)v = 2+i6-j3+k4.$$

9.3. I legemet af kvaternioner har 0 kun én kvadratrod, medens ethvert negativt reelt tal har mange forskellige kvadratrødder, og enhver anden kvaternion har netop 2 kvadratrødder. Eftervis dette - det er ikke frygtelig svært.

9.4. Forsøg at bestemme kommutatorundergruppen i den multiplikative gruppe $\mathbb{K}\setminus\{0\}$ af kvaternioner. For det første er det let at se, at enhver kommutator har numerisk værdi 1, så kommutatorundergruppen er del af undergruppen S^3 af kvaternioner med numerisk værdi 1. For enhver kvaternion x gælder relationen $x\,xjx^{-1}(xj)^{-1} = |x|^{-2}x^2$, og derfor giver opgave 9.3, at ethvert element i S^3 endda er en kommutator. Gruppen S^3 er identisk med sin kommutatorundergruppe.

9.5. Angiv centrum for den multiplikative gruppe af kvaternioner.

9.6. Vis, at følgende relationer gælder for polynomier over $\mathbb{Z}_n$:

$$(X+1)^n = X^n+1,\ (X-1)^n = X^n+(-1)^n.$$

9.7. Vis for et primtal $p > 2$, at følgende relation gælder for polynomier over $\mathbb{Z}_p$

$$(X-1)^{p-1} = X^{p-1}+X^{p-2}+\ldots+X+1$$

9.8. Find en største fælles divisor for polynomierne (over $\mathbb{R}$)

$$x^8+x^7+2x^5+x^4+x^3+x^2+1 \quad \text{og} \quad x^7+2x^3-x+2.$$

9.9. Find polynomier $P(x)$ og $Q(x)$ over $\mathbb{R}$ af lavest mulig grad, og som tilfredsstiller ligningen

$$(x^3+4x^2-1)P(x)-(x^3+4x-1)Q(x) = x^4-4x^2-x\ .$$

9.10. Løs ligningen (over $\mathbb{C}$)

$$x^4+3x^2+4 = 0.$$

9.11. Lad L være et legeme med et dellegeme $K \subseteq L$. Lad $\xi \in L$ være et vilkårligt element. Vis, at der findes netop 1 irreducibelt normeret polynomium $P(X) \in K[X]$ med ξ som rod. Vis, at værdiafbildningen $ev : K[X] \to L$ inducerer en homomorfi φ: $\frac{K[X]}{(P(X))} \to L$, og at billedmængden $L_1 \subseteq L$ er det mindste dellegeme af L, som indeholder både K og ξ. Vis, at hvert element i L_1 på netop 1 måde kan skrives på formen $c_{n-1}\xi^{n-1}+\ldots+c_1\xi+c_0$, hvor $c_0,\ldots,c_{n-1} \in K$.

9.12. Vis, at $P(X) = X^3-X+\frac{1}{3}$ er irreducibelt over $\mathbb{Q}$ (hvis $P(X)$ kan opløses i faktorer af positiv grad, må en af dem være af første grad, så $P(X)$ må have en rationalrod). Vis, at $P(X)$ har 3 reelle rødder (ved hjælp af sætningen om, at kontinuerte funktioner ikke kan springe værdier over). Lad ξ være en rod i $P(X)$. Benyt opgave 9.11 til at udtrykke ξ^3, ξ^4, ξ^{-1}, $(1-\xi^2)^{-1}$ samt $(1+\xi)^{-1}$ ved ξ og ξ^2.

9.13. Angiv en største fælles divisor for polynomierne

$$x^6+2x^3-x^2+1 \quad \text{og} \quad x^6+2x^4+x^2-1.$$

9.14. Lad $I \subsetneq \mathbb{R}[X]$ være idealet frembragt af X^2+1. Vis, at $\frac{\mathbb{R}[X]}{I}$ er et legeme isomorft med $\mathbb{C}$.

9.15. Ringen $\mathbb{Z}_2[X]$ af polynomier over legemet $\mathbb{Z}_2$ omfatter kun endelig mange polynomier af hver grad, og derfor lader det sig gøre at finde alle irreducible polynomier af en given grad. Prøv at udføre dette for graderne 2,3,4 og eventuelt 5.

9.16. Prøv at indføre en gruppe-ring $\Lambda\mathbb{Z}^n$ for en kommutativ ring Λ, og indfør derved en ring $\Lambda[X_1,\ldots,X_n]$ af polynomier i n variable over Λ. Det går i princippet helt som for $\Lambda[X]$. Vis, at der for $p = 2, \ldots,n-1$ er naturlige isomorfier mellem $\Lambda[X_1,\ldots,X_n]$ og $\Lambda[X_1,\ldots,X_p][X_{p+1},\ldots,X_n]$. Derfor er der også en naturlig injektiv homomorfi $\Lambda[X_1,\ldots,X_p] \to \Lambda[X_1,\ldots,X_n]$.

9.17. Et polynomium $P(X) \in \Lambda[X]$, hvor Λ er en kommutativ ring, kan på naturlig måde opfattes som et polynomium over ringen $P(X)$, og for $Q(X) \in \Lambda[X]$ får vi derfor en værdi $P(Q(X)) \in \Lambda[X]$. Derved får vi det sammensatte polynomium $P \circ Q$.

§ 9.7
Generel teori om kvadrikker.

Vi betragter $\mathbb{R}^n$ både som et vektorrum og som en punktmængde.

Vi har, at der til ethvert ordnet punktpar $(0,P)$ i $\mathbb{R}^n$ er knyttet en vektor $\underline{0P}$. Givet et punkt P_0 og en vektor $\underline{v}$ findes netop et punkt P så $\underline{v} = \underline{P_0P}$.

Ved et ortonormalt eller sædvanligt retvinklet koordinatsystem $(0 ; \underline{e}_1,\ldots,\underline{e}_n)$ i $\mathbb{R}^n$ vil vi nu forstå et punkt $0 \in \mathbb{R}^n$ (hvorfra vektorerne tænkes afsat) og en ortonormal basis $\underline{e}_1,\ldots,\underline{e}_n$ for $\mathbb{R}^n$. Vi siger, at et punkt P har koordinaterne $(x_1,\ldots,x_n)$ med hensyn til $(0 ; \underline{e}_1,\ldots,\underline{e}_n)$, hvis $\underline{0P} = x_1\underline{e}_1 +\ldots+ x_n\underline{e}_n$.

Ved en kvadrik Q forstås en mængde af punkter i $\mathbb{R}^n$, hvis koordinater netop er løsningerne til en ligning af formen

$$F(x_1,\ldots,x_n) = \sum_{1\le i\le j\le n} a_{ij}x_ix_j + \sum_{1\le i\le n} c_ix_i + d = 0 ,$$

hvor a_{ij} , $1 \le i \le j \le n$, c_i , $1 \le i \le n$, og d er reelle tal, og ikke alle a_{ij} er 0 .

Vi bemærker, at blot en mængde Q i ét koordinatsystem kan fremstilles ved en ligning af formen (1), da vil Q i ethvert koordinatsystem være fremstillet ved en ligning af samme form.

Lad nemlig $(0 ; \underline{e}_1,\ldots,\underline{e}_n)$, $(\hat{0} ; \underline{\hat{e}}_1,\ldots,\underline{\hat{e}}_n)$ være to koordinatsystemer. Lad P have koordinatsættene $(x_1,\ldots,x_n)$ og $(\hat{x}_1,\ldots,\hat{x}_n)$ med hensyn til disse to koordinatsystemer.

Hvis $\underline{0\hat{0}} = \hat{a}_1\underline{\hat{e}}_1 +\ldots+ \hat{a}_n\underline{\hat{e}}_n$ og $(\underline{e}_1,\ldots,\underline{e}_n) = (\underline{\hat{e}}_1,\ldots,\underline{\hat{e}}_n)\underline{\underline{S}}$ fås let $\underline{\underline{x}} = \underline{\hat{a}} + \underline{\underline{S}}\,\underline{\hat{x}}$ eller $\underline{\hat{x}} = -\underline{\underline{S}}^{-1}\underline{a} + \underline{\underline{S}}^{-1}\underline{x}$.

Lad $\hat{F}(\hat{x}_1,\ldots,\hat{x}_n)$ være det polynomium som fremgår af $F(x_1,\ldots,x_n)$ ved at indsætte udtrykkene for $\hat{x}_1,\ldots,\hat{x}_n$.

For ethvert punkt P fås nu samme tal hvad enten man indsætter $x_1,\ldots,x_n$ i $(F(x_1,\ldots,x_n)$ eller $\hat{x}_1,\ldots,\hat{x}_n$ i $F(\hat{x}_1,\ldots,\hat{x}_n)$.

Specielt fås tallet 0 for de samme punkter. Det er klart, at $F(\hat{x}_1,\ldots,\hat{x}_n)$ er et polynomium af højst anden grad og af anden grad netop når $F(x_1,\ldots,x_n)$ er det.

I resten af kapitel 9.7 skal man ved det affine rum (A,V) blot forstå $\mathbb{R}^n$ opfattet dels som punktmængde (A) , dels som vektorrum (V) .

Lad K være en kvadrik i et euklidisk affint rum (A,V) af dimension $n \geq 2$. Der findes da et sædvanligt retvinklet koordinatsystem i A m.h.t. hvilket K har en ligning af en af følgende tre normalformer, hvor $\alpha_1,\ldots,\alpha_r$, γ og δ alle er $\neq 0$:

$$(C) \qquad \sum_{i=1}^{r} \alpha_i x_i^2 + \delta = 0.$$

$$(P) \qquad \sum_{i=1}^{r} \alpha_i x_i^2 + \gamma x_{r+1} = 0.$$

$$(K) \qquad \sum_{i=1}^{r} \alpha_i x_i^2 = 0.$$

Bevis. Lad K have ligningen (2) m.h.t. et sædvanligt retvinklet koordinatsystem $(O;\underline{e}_1,\ldots,\underline{e}_n)$. Ved

$$x_1\underline{e}_1+\ldots..+x_n\underline{e}_n \mapsto \sum_{1\leqq i\leqq j\leqq n} a_{ij}x_ix_j$$

er da bestemt en kvadratisk form K_B på V. (Matricen $\underline{\underline{B}} = (b_{ij})$ for den tilhørende symmetriske bilinearform B er bestemt ved, at $b_{ii} = a_{ii}$ for $i = 1,\ldots,n$ og $b_{ij} = b_{ji} = \frac{1}{2}a_{ij}$ for $1 \leqq i < j \leqq n$.) Ifølge en tidligere sætning (side 8.3.1) findes da en ortonormal basis $(\hat{\underline{e}}_1,\ldots,\hat{\underline{e}}_n)$ i V m.h.t. hvilken K_B antager normalform,

$$K_B(x_1\hat{\underline{e}}_1+\ldots+x_n\hat{\underline{e}}_n) = \sum_{i=1}^{n} \alpha_i x_i^2,$$

(hvor koefficienterne α_i er de karakteristiske rødder for $\underline{\underline{B}}$.) Uden indskrænkning kan antages, at $\alpha_1,\ldots,\alpha_r$ er de fra 0 forskellige koefficienter. M.h.t. koordinatsystemet $(O;\hat{\underline{e}}_1,\ldots,\hat{\underline{e}}_n)$ har K da en ligning af formen

$$\sum_{i=1}^{r} \alpha_i x_i^2 + \sum_{i=1}^{n} \hat{c}_i x_i + d = 0,$$

hvilket kan omskrives til

$$\sum_{i=1}^{r} \alpha_i\left(x_i + \frac{\hat{c}_i}{2\alpha_i}\right)^2 + \sum_{i=r+1}^{n} \hat{c}_i x_i + \hat{d} = 0,$$

hvor $d_1 = d - \sum_{i=1}^{r} \hat{c}_i^2 (4\alpha_i)^{-1}$.

Er nu $r = n$, eller $r < n$ og $\hat{c}_{r+1} = \ldots = \hat{c}_n = 0$, betegnes med $\hat{O}$ det punkt, som m.h.t. koordinatsystemet $(O;\hat{\underline{e}}_1,\ldots,\hat{\underline{e}}_n)$ har koordinatsættet

$$\left(-\frac{\hat{c}_1}{2\alpha_1},\ldots,-\frac{\hat{c}_r}{2\alpha_r},\ 0,\ldots,0\right).$$

M.h.t. koordinatsystemet $(\hat{O};\hat{\underline{e}}_1,\ldots,\hat{\underline{e}}_n)$ vil K da have ligningen

$$\sum_{i=1}^{r}\alpha_i x_i^{\,2} + \hat{d} = 0,$$

altså en ligning af formen (C) eller (K).

Er derimod $r < n$ og $\hat{c}_i \neq 0$ for mindst eet $i \geqq r+1$, vælges et nyt sædvanligt retvinklet koordinatsystem $(\hat{O};\hat{\underline{e}}_1,\ldots,\hat{\underline{e}}_r,\ \tilde{\underline{e}}_{r+1},\ldots,\tilde{\underline{e}}_n)$ på følgende måde. Vi sætter

$$c = \left(\sum_{i=r+1}^{n}\hat{c}_i^{\,2}\right)^{\frac{1}{2}}$$

og

$$\sum_{i=r+1}^{n}\frac{\hat{c}_i}{c}\,\hat{\underline{e}}_i = \tilde{\underline{e}}_{r+1}\ .$$

Sættet $(\hat{\underline{e}}_1,\ldots,\hat{\underline{e}}_r,\tilde{\underline{e}}_{r+1})$ er da ortonormalt, og kan derfor suppleres til en ortonormal basis $(\hat{\underline{e}}_1,\ldots,\hat{\underline{e}}_r,\ \tilde{\underline{e}}_{r+1},\ldots,\tilde{\underline{e}}_n)$ for V. Koordinattransfomrationsmatricen $\underline{\underline{S}}$ hørende til overgangen fra basen $(\hat{\underline{e}}_1,\ldots,\hat{\underline{e}}_n)$ til basen $(\hat{\underline{e}}_1,\ldots,\hat{\underline{e}}_r,\ \tilde{\underline{e}}_{r+1},\ldots,\tilde{\underline{e}}_n)$ er ortogonal, og den j'te søjle i $\underline{\underline{S}}^{-1}$ er koordinatsøjlen for den nye j'te basisvektor m.h.t. den gamle basis. Af det første følger, at $\underline{\underline{S}} = (\underline{\underline{S}}^{-1})'$, og ved brug af det andet følger derefter, at $\underline{\underline{S}}$ har formen

$$\begin{pmatrix} \underline{\underline{E}}_{r,r} & \underline{\underline{O}}_{r,n-r} \\ \underline{\underline{O}}_{n-r,r} & \underline{\underline{T}}_{n-r,n-r} \end{pmatrix},$$

hvor den første række i $\underline{\underline{T}}_{n-r,n-r}$ er

$$\left(\frac{\hat{c}_{r+1}}{c} \ \ldots \ \frac{\hat{c}_n}{c}\right).$$

Heraf fremgår, at K i koordinatsystemet $(O;\underline{\hat{e}}_1,\ldots,\underline{\hat{e}}_r,\underline{\tilde{e}}_{r+1},\ldots,\underline{\tilde{e}}_n)$ har ligningen

$$\sum_{i=1}^{r} \alpha_i\left(x_i + \frac{\hat{c}_i}{2\alpha_i}\right)^2 + cx_{r+1} + \hat{d} = 0,$$

hvilket kan omskrives til

$$\sum_{i=1}^{r} \alpha_i\left(x_i + \frac{\hat{c}_i}{2\alpha_i}\right)^2 + c\left(x_{r+1} + \frac{\hat{d}}{c}\right) = 0.$$

Betegnes derfor med $\hat{O}$ det punkt, som m.h.t. koordinatsystemet $(O;\underline{\hat{e}}_1,\ldots,\underline{\hat{e}}_r,\underline{\tilde{e}}_{r+1},\ldots,\underline{\tilde{e}}_n)$ har koordinatsættet

$$\left(-\frac{\hat{c}_1}{2\alpha_1},\ldots,-\frac{\hat{c}_r}{2\alpha_r}, -\frac{\hat{d}}{c}, 0,\ldots,0\right),$$

har K i koordinatsystemet $(\hat{O};\underline{\hat{e}}_1,\ldots,\underline{\hat{e}}_r,\underline{\tilde{e}}_{r+1},\ldots,\underline{\tilde{e}}_n)$ ligningen

$$\sum_{i=1}^{r} \alpha_i x_i^2 + cx_{r+1} = 0,$$

altså en ligning af formen (P). []

Et punkt P siges at være et *centrum* for en kvadrik K, dersom det for ethvert punkt $Q_1 \in K$ gælder, at også det ved $PQ_2 = -PQ_1$ bestemte punkt Q_2 tilhører K.

En kvadrik K kan ikke både have et centrum, som tilhører K, og et centrum, som ikke tilhører K.

Bevis. Lad K have ligningen (2) m.h.t. et sædvanligt retvinklet koordinatsystem. Antag, at punkterne $P_0 \in K$ og $P_1 \notin K$ med koordinatsættene $(y_1,\ldots,y_n)$ hhv. $(y_1+z_1,\ldots,y_n+z_n)$ begge er centrer for K. Punktet P_2 med koordinatsættet $(y_1+2z_1,\ldots,y_n+2z_n)$ vil da tilhøre K, idet $P_0 \in K$ og P_1 er et centrum. Da P_0 er et centrum, sluttes dernæst, at også punktet P_{-2} med koordinatsættet $(y_1-2z_1,\ldots,y_n-2z_n)$ tilhører K. Heraf fås ialt, at polynomiet

$$p(t) = \sum_{1\leqq i\leqq j\leqq n} \alpha_{ij}(y_i+tz_i)(y_j+tz_j) + \sum_{i=1}^{n} c_i(y_i+tz_i) + d$$

har tre rødder, nemlig $-2, 0$ og 2, og følgelig er nulpolynomiet. Men heraf følger videre, at hele linien bestemt ved P_0 og P_1 er indeholdt i K, i strid med, at $P_1 \notin K$. []

En kvadrik K, som har en ligning af normalformen (P), *har intet centrum.*

Bevis. Antag, at punktet P med koordinatsættet $(y_1,\ldots,y_n)$ er et centrum. Lad z_r være et vilkårligt reelt tal. Det er da oplagt muligt at bestemme et reelt tal z_{r+1}, således at punktet Q_1 med koordinatsættet $(y_1,\ldots,y_{r-1},y_r+z_r,y_{r+1}+z_{r+1},y_{r+2},\ldots,y_n)$ tilhører K. Da P er et centrum, vil også punktet Q_2 med koordinatsættet $(y_1,\ldots,y_{r-1},y_r-z_r,y_{r+1}-z_{r+1},y_{r+2},\ldots,y_n)$ tilhører K. Vi har derfor

$$\sum_{i=1}^{r} \alpha_i y_i^2 + \alpha_r z_r^2 + 2\alpha_r y_r z_r + \gamma(y_{r+1} + z_{r+1}) = 0$$

og

$$\sum_{i=1}^{r} \alpha_i y_i^2 + \alpha_r z_r^2 - 2\alpha_r y_r z_r + \gamma(y_{r+1} - z_{r+1}) = 0.$$

Heraf følger, at

$$\sum_{i=1}^{r} \alpha_i y_i^2 + \alpha_r z_r^2 + \gamma y_{r+1} = 0.$$

Idet z_r er valgt vilkårligt, og $\alpha_r \neq 0$, giver dette en modstrid. □

Det bemærkes nu, at hvis en kvadrik har en ligning af formen (K) hhv. (C), så har den et centrum, som tilhører hhv. ikke tilhører kvadrikken, nemlig begyndelsespunktet. Af de to foregående sætninger fremgår derfor følgende:

En kvadrik har en ligning af formen (C), *hvis og kun hvis den har mindst et centrum og intet centrum tilhører kvadrikken.* - Sådanne kvadrikker kaldes (egentlige) *centrumskvadrikker.*

En kvadrik har en ligning af formen (P), *hvis og kun hvis den intet centrum har.* - Sådanne kvadrikker kaldes *paraböIske kvadrikker.*

En kvadrik har en ligning af formen (K), *hvis og kun hvis den har mindst et centrum og ethvert centrum tilhører kvadrikken.* - Sådanne kvadrikker kaldes *keglekvadrikker.*

Vi skal til sidst give en skematisk oversigt over kvadrikkerne i euklidisk affine rum af dimension 2 ("keglesnit") og dimension 3 ("keglesnitsflader"). Vi skal her omskrive ligningerne til de gængse former.

KEGLESNIT.

Centrumskvadrikker:

$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$	Ellipse
$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$	Hyperbel
$-\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$	$\emptyset$
$\frac{x^2}{a^2} = 1$	To parallelle linier
$-\frac{x^2}{a^2} = 1$	$\emptyset$

Parabolske kvadrikker:

$x^2 = py$	Parabel

Keglekvadrikker:

$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 0$	Punkt
$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 0$	To skærende linier
$\frac{x^2}{a^2} = 0$	Linie

KEGLESNITSFLADER.

Centrumskvadrikker:

$\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} = 1$	Ellipsoide
$\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2} = 1$	Hyperboloide med 1 net
$\frac{x^2}{a^2} - \frac{y^2}{b^2} - \frac{z^2}{c^2} = 1$	Hyperboloide med 2 net
$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$	Elliptisk cylinder
$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$	Hyperbolsk cylinder
$-\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$	$\emptyset$
$\frac{x^2}{a^2} = 1$	To parallelle planer
$-\frac{x^2}{a^2} = 1$	$\emptyset$

Parabolske kvadrikker:

$\frac{x^2}{a^2} + \frac{y^2}{b^2} = \frac{2z}{c}$	Elliptisk paraboloide
$\frac{x^2}{a^2} - \frac{y^2}{b^2} = \frac{2z}{c}$	Hyperbolsk paraboloide
$x^2 = py$	Parabolsk cylinder

Keglekvadrikker:

$\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} = 0$	Punkt
$\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2} = 0$	Keglesnitskegle
$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 0$	Linie
$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 0$	To skærende planer
$\frac{x^2}{a^2} = 0$	Plan

4.4. Matrixrang.

Lad $\underline{\underline{A}}$ være en $m \times n$-matrix med elementer fra legemet L. Vi har definieret <u>rangen</u> af $\underline{\underline{A}}$, $\operatorname{rg} \underline{\underline{A}}$, som rangen af de n søjler $\underline{\underline{a}}_{/1}, \dots, \underline{\underline{a}}_{/n}$ opfattet som vektorer i vektorrummet $(L^m; L)$. Vi har set, at hvis en lineær afbildning $f: U \to V$ i passende baser beskrives ved matricen $\underline{\underline{A}}$, da gælder $\dim f(U) = \operatorname{rg}(f) = \operatorname{rg} \underline{\underline{A}}$. Specielt er altså $\operatorname{rg} \underline{\underline{A}} = \operatorname{rg}(m_{\underline{\underline{A}}})$, hvor $m_{\underline{\underline{A}}}$ er den ved $\underline{\underline{x}}_{/1} \longmapsto \underline{\underline{A}}\,\underline{\underline{x}}_{/1}$ bestemte afbildning $: L^n \to L^m$. Det fremgår heraf, at $\operatorname{rg} \underline{\underline{A}} = n$ netop når $m_{\underline{\underline{A}}}$ er injektiv, og at $\operatorname{rg} \underline{\underline{A}} = m$ netop når $m_{\underline{\underline{A}}}$ er surjektiv. Da $m_{\underline{\underline{A}}}$ er bijektiv, hvis og kun hvis $\underline{\underline{A}}$ er regulær, har vi altså

<u>$\underline{\underline{A}}$ er (kvadratisk og) regulær, hvis og kun hvis $m = n = \operatorname{rg} \underline{\underline{A}}$.</u>

Da dimensionen af billedrummet for $m_{\underline{\underline{A}}}: L^n \to L^m$ ikke ændrer sig ved sammensætning med en isomorfi, ser vi, at der gælder

<u>$\operatorname{rg}(\underline{\underline{S}}\,\underline{\underline{A}}) = \operatorname{rg} \underline{\underline{A}}$, når $\underline{\underline{S}}$ er en regulær $(m \times m)$-matrix</u>

<u>$\operatorname{rg}(\underline{\underline{A}}\,\underline{\underline{T}}) = \operatorname{rg} \underline{\underline{A}}$, når $\underline{\underline{T}}$ er en regulær $(n \times n)$-matrix.</u>

<u>For en $(m \times n)$-matrix $\underline{\underline{A}}$ stemmer (søjle)rang og rækkerang overens.</u> (d.v.s. $\operatorname{rg} \underline{\underline{A}} = \operatorname{rg} \underline{\underline{A}}'$).

Bevis. Der findes (4.2.4) nye baser for L^n og L^m, således at der m.h.t. disse baser til $m_{\underline{\underline{A}}}$ hører matricen $\underline{\underline{E}}^{(r)}_{m,n}$, hvor $r = \operatorname{rg}(m_{\underline{\underline{A}}}) = \operatorname{rg} \underline{\underline{A}}$. Heraf følger (4.3.3), at der findes regulære matricer $\underline{\underline{T}}$ og $\underline{\underline{S}}$, så at $\underline{\underline{E}}^{(r)}_{m,n} = \underline{\underline{T}}\,\underline{\underline{A}}\,\underline{\underline{S}}^{-1}$, eller $\underline{\underline{A}} = \underline{\underline{T}}^{-1}\,\underline{\underline{E}}^{(r)}_{m,n}\,\underline{\underline{S}}$. Heraf fås $\underline{\underline{A}}' = \underline{\underline{S}}'\,[\underline{\underline{E}}^{(r)}_{m,n}]'\,\underline{\underline{T}}'^{-1}$, og da $\underline{\underline{S}}'$ og $\underline{\underline{T}}'^{-1}$ er regulære, og $[\underline{\underline{E}}^{(r)}_{m,n}]' = \underline{\underline{E}}^{r}_{n,m}$ har rang r, slutter vi, at også $\operatorname{rg} \underline{\underline{A}}' = r$. □

1. Lad (V,L) være et vektorrum. Vi har sat $\mathrm{rg}V$ = det største antal vektorer, der danner et lineært uafhængigt system, og vi sætter (midlertidigt) $\dim V$ = det mindste antal vektorer, der dannet et frembringersystem. Bemærk, at $\dim V < \infty$ netop hvis V er endligt frembragt.

a. Et *minimalt frembringersystem*, er et frembringersystem, som ikke indholder noget mindre frembringersystem. Vis, at et sådant system er en basis for V (og omvendt), og slut heraf, at hvis $\dim V < \infty$, da har V en basis.

b. Et *maksimalt frit system* i V er et lineært uafhængigt system, der ikke er indeholdt i noget større lineært uafhængigt system. Vis, at et sådant system er en basis (og omvendt), og slut heraf, at hvis $\mathrm{rg}V < \infty$, da har V en basis.

c. Vis, at hvis en basis indholder |basis| elementer, da gælder

$$\dim V \leqq |\text{basis}| \leqq \mathrm{rg}V,$$

og slut heraf, at der altid gælder

$$\dim V \leqq \mathrm{rg}V.$$

d. Lad $M \subseteqq V$ være en delmængde. Et *maksimalt frit system fra* M er et lineært uafhængigt system af vektorer fra M, der ikke er indeholdt i noget større lineært uafhængigt system af vektorer fra M. Vis, at et sådant system er en basis for $\mathrm{Span}(M)$, og slut heraf, at hvis $\mathrm{rg}V < \infty$, da gæl-

der følgende: Hvis $(\underline{v}_i, i \in I)$ er et system af vektorer i V, og hvis $(\underline{u}_1, \ldots, \underline{u}_p)$ er et lineært uafhængigt sæt i V, så at $\underline{u}$'erne supleret med alle $\underline{v}$'erne er et frembringersystem for V, da kan $\underline{u}$'erne suppleres med visse $\underline{v}$'er til en basis for V.

e. Vis, at hvis et maksimalt frit system fra M indeholder |maks. frit syst. fra M| elementer, da gælder

$$\dim\mathrm{Span}(M) \leqq |\text{maks. frit syst. fra } M| \leqq \mathrm{rg}M \leqq \mathrm{rgSpan}(M),$$

og slut heraf, at der altid gælder

$$\dim\mathrm{Span}(M) \leqq \mathrm{rg}M \leqq \mathrm{rgSpan}(M)$$

f. Vis, at udskiftningssætningen medfører, at

$$\dim V \geqq \mathrm{rg}V,$$

og forstærk derved ovenstående resultater.

2. Lad T være en endelig mængde. Angiv en basis for vektorrummet $\mathsf{F}(T,L)$ og bestem dette vektorrums dimension.

3. Lad G være en gruppe, og lad L^* være den multiplikative gruppe i legemet L (altså $L^* = L \setminus \{0\}$, med multiplikation som komposition). En *L-karakter* er en homomorfi $\chi : G \to L^*$. Vi kan opfatte mængden af L-karakterer som en delmængde i vektorrummet $\mathsf{F}(G,L)$ af alle afbildninger $\varphi : G \to L$. Vis, at mængden af L-karakterer er en lineært uafhængig delmæng-

de af $\mathsf{F}(G,L)$, og slut heraf at

$$|\{L\text{-karakterer}\}| \leqq |G|.$$

Vink. Antag, at der fandtes lineære relationer mellem karaktererne, og betragt en, der involverer det mindst mulige antal karakterer.

4. Lad F_0 være mængden af afbildninger $\varphi : \mathbb{R} \to \mathbb{R}$, som opfylder: $\varphi(t) \neq 0$ gælder kun for endelig mange $t \in \mathbb{R}$. Vis, at F_0 er et underrum i $F = \mathsf{F}(\mathbb{R},\mathbb{R})$, og vis, at F_0 ikke har nogen numerabel basis.

5*. Vis, at vektorrummet $L^{\mathbb{N}}$ af alle følger $(\lambda_1,\lambda_2,\ldots)$ ikke har en numerabel basis.

6. (Fortsættelse af 1. øv. 36). Vis, at $\underline{v}_i \mapsto (\underline{o},\ldots,\underline{v}_i,\ldots,\underline{o})$ definerer en isomorfi: $V_i \xrightarrow{\sim} W_i$. Antag at $V_1,\ldots,V_n$ er underrum i vektorrummet (V,L). Find en "naturlig" lineær afbildning

$$\kappa : V_1 \times\ldots\times V_n \to V,$$

og bestem κ's billede. Hvad betyder det, at κ er surjektiv? injektiv? bijektiv? Vis, i tilfældet $n = 2$, at $\underline{v} \to (\underline{v},-\underline{v})$ definerer en isomorfi $V_1 \cap V_2 \xrightarrow{\sim} \mathrm{Ker}(\kappa)$, og slut heraf Grassmann's dimensionsformel ved hjælp af dimensionsformlen for en lineær afbildning.

7. Lad $(\tilde{V},\mathbb{C})$ være den komplekse udvidelse af et reelt vektorrum $(V,\mathbb{R})$, jfr. 1. øv. 2. Vis, at den ved $k : (\underline{v}_1,\underline{v}_2) \mapsto (\underline{v}_1,-\underline{v}_2)$ bestemte afbildning $k : \tilde{V} \to \tilde{V}$ er en *konjugering*, d.v.s. at der gælder: $k^2 = 1_{\tilde{V}}$, $k(\tilde{\underline{u}}+\tilde{\underline{v}}) = k(\tilde{\underline{u}}) + k(\tilde{\underline{v}})$, $k(\lambda\tilde{\underline{v}}) = \overline{\lambda}\cdot k(\tilde{\underline{v}})$, for $\tilde{\underline{u}},\tilde{\underline{v}} \in \tilde{V}$, $\lambda \in \mathbb{C}$. Vis, at den ved $\underline{v} \to (\underline{v},\underline{0})$ bestemte afbildning $V \to \tilde{V}$ er injektiv og $\mathbb{R}$-lineær. Identificeres V med sit billede kan hver vektor $\tilde{\underline{v}} \in \tilde{V}$ entydigt skrives $\tilde{\underline{v}} = \underline{v}_1 + i\underline{v}_2$, $\underline{v}_1,\underline{v}_2 \in V$, og der gælder

$$\tilde{\underline{v}} \in V \Leftrightarrow k(\tilde{\underline{v}}) = \tilde{\underline{v}}.$$

Lad $f : V \to W$ være en $\mathbb{R}$-lineær afbildning, hvor W er et vektorrum over $\mathbb{R}$. Vis, at $\underline{v}_1 + i\underline{v}_2 \mapsto f(\underline{v}_1) + if(\underline{v}_2)$ bestemmer en $\mathbb{C}$-lineær afbildning $\tilde{f} : \tilde{V} \to \tilde{W}$. $\tilde{f}$ kaldes den komplekse udvidelse af f.

8. Et *frembringersystem* i den endelige gruppe G er en delmængde $T \subseteq G$ med den egenskab at ethvert $s \in G$ har en fremstilling $s = t_1\cdot\ldots\cdot t_r$, hvor $r \geq 0$, og $t_1,\ldots,t_r$ er (ikke nødvendigvis forskellige) elementer af T. Definer *minimalt frembringersystem* og dim$G$ som i opgave 1. Vis, at et frembringersystem for S_n bestående af transpositioner mindst har $n - 1$ elementer, og vis, at $(1,2)$, $(1,3),\ldots,(1,n)$ er et minimalt frembringersystem. Lad c_i, $i = 1,\ldots,n$ betegne cyklen $c_i = (1,2,\ldots,i)$, og vis, at $c_{i-2} = c_{i-1}c_i^{-2}c_{i-1}c_i$, $i = 3,\ldots,n$, og slut heraf

ved induktion, at $\{c_{n-1}, c_n\}$ er et frembringersystem for S_n, og dermed, at $\dim S_n = 2$, $n \geqq 3$. Vis, at transpositionerne $(1,2)$, $(3,4)$, $(5,6)$ frembringer en (kommutativ) undergruppe G i S_6, med $|G| = 8$, og $\dim G = 3$.

9. Betragt vektorrummet (P, L) af polynomier med koefficienter fra L (= $\mathbb{R}$ eller = $\mathbb{C}$), med underrummene P_n af polynomier af grad $\leqq n$. Vis, at hvis f er et polynomium af grad $\geqq 0$, da defineres ved $\varphi \mapsto \varphi f$ en injektiv, lineær afbildning: $P \to P$. Vi sættet $Uf = \{\varphi f | \varphi \in U\}$ (= billedmængden ved denne afbildning) når $U \subseteqq P$.

a. Vis, at hvis f har grad $n \geqq 0$, da er $P_d f \cap P_{n-1} = \{0\}$, og slut heraf, at

$$P_d = P_{d-n} f \oplus P_{n-1} \quad \text{for} \quad d \geqq n - 1,$$

og dernæst, at

$$P = Pf \oplus P_{n-1}.$$

(Entydig division med rest).

b. En endelig mængde $\{f_1, \ldots, f_r\} \subseteqq P$ kaldes *primisk*, hvis $Pf_1 + \ldots + Pf_r = P$. Vis, at dette er tilfældet hvis og kun hvis der findes $\varphi_1, \ldots, \varphi_r \in P$, så at $\varphi_1 f_1 + \ldots + \varphi_r f_r = 1$. Vis, at hvis $L = \mathbb{R}$, da er $\{f_1, \ldots, f_r\} \subseteqq P$ primisk netop hvis $\{f_1, \ldots, f_r\}$ opfattet som en mængde af polynomier med koefficienter fra $\mathbb{C}$ er primisk [Vink: definer "realdelen" af et komplekst poly-

nomium]. Vis, at $\{fg, f_2, \ldots, f_r\}$ er primisk hvis og kun hvis både $\{f, f_2, \ldots, f_r\}$ og $\{g, f_2, \ldots, f_r\}$ er primiske, og slut under brug af algebraens fundamentalsætning, at $\{f_1, \ldots, f_r\}$ er primisk netop hvis f'erne ikke har nogen fælles rod i $\mathbb{C}$.

c. Givet et polynomium $f = \varphi_1 \ldots \varphi_r$ af grad n, hvor φ'erne er *parvis* primiske, og φ_i har grad n_i. Sæt $f_i = \frac{f}{\varphi_i} = \varphi_1 \ldots \varphi_{i-1}\varphi_{i+1}\ldots\varphi_r$ af grad $n - n_i$. Vis, at $\{f_1, \ldots, f_r\}$ er primisk, og slut nu under brug af a., at der gælder $P = P_{n_1-1}f_1 + \ldots + P_{n_r-1}f_r + Pf$, og dermed $P_d \subseteq P_{n_1-1}f_1 + \ldots + P_{n_r-1}f_r + P_{d-n}f$ for $d \geq n - 1$. Forstærk dette til

$$P_d = P_{n_1-1}f_1 \oplus \ldots \oplus P_{n_r-1}f_r \oplus P_{d-n}f, \quad d \geq n - 1.$$

specielt

$$P_{n-1} = P_{n_1-1}f_1 \oplus \ldots \oplus P_{n_r-1}f_r.$$

d. Antag, at $\varphi_i = (t-\lambda_i)^{n_i}$, og vis, at opspaltningen i c. medfører, at polynomierne

$$f_{i\nu} = \frac{f}{(t-\lambda_i)^\nu} \quad \begin{matrix} i = 1, \ldots, r \\ \nu = 1, \ldots, n_i \end{matrix} \quad \text{og} \quad f, tf, \ldots, t^{d-n}f$$

udgør en basis for P_d, $d \geq n - 1$. [Vink: udnyt, at $1, t-\lambda_i, (t-\lambda_i)^2, \ldots, (t-\lambda_i)^{n_i-1}$ er en basis for P_{n_i-1}]. Vis, at de rationale funktioner

$$\frac{1}{(t-\lambda_i)^{\nu}} \quad \begin{matrix} i = 1,\ldots,r \\ \nu = 1,\ldots,n_i \end{matrix} \quad \text{og } t^k \; k = 0,\ldots,d-n$$

danner en basis for de rationale funktioner af formen $\frac{h}{f}$, med h af grad $\leqq d$. $(d \geqq n-1)$.

e. Hvilket resultat fås i tilfældet, hvor
$f = (t-\lambda_1)^{n_1}\ldots(t-\lambda_r)^{n_r}(t^2+2a_1t+b_1)^{m_1}\ldots(t^2+2a_st+b_s)^{m_s}$.
[Vink: udnyt, at der for polynomiet $t^2 + 2at + b$ af grad 2 gælder, at $1,t,\varphi,t\varphi,\ldots,\varphi^{m-1},t\varphi^{m-1}$ er en basis for P_{2m-1}].

Algebraens fundamentalsætning udsiger, at ethvert polynomium $f = t^n + a_1t^{n-1} +\ldots+ a_{n-1}t + a_n$, med $a_1,\ldots,a_n \in \mathbb{C}$ kan skrives $f = (t-\lambda_1)^{n_1}\ldots(t-\lambda_r)^{n_r}$. Dette medfører i tilfældet $L = \mathbb{R}$, at ethvert polynomium f kan skrives på den i e. omtalte måde.

10. Vis, at der ved $(\Delta f)(t) = f(t+1) - f(t)$ bestemmes en lineær afbildning $\Delta : P \to P$, og bestem Δ's kerne. Vis, at underrummet $U_a \subseteq P$ bestående af polynomier f med $f(a) = 0$ er et kompelemnt til Δ's kerne. Vis, at polynomierne $\binom{}{i} : t \mapsto \binom{t}{i} = \frac{t(t-1)\ldots(t-i+1)}{i!}$, $i \geqq 1$ sammen med $\binom{}{0} = 1$ er basis for P, bestem $\Delta(\binom{}{i})$, og slut dernæst, at Δ er surjektiv. Vis, at der findes netop en lineær afbildning $\Sigma_a : P \to U_a$ som opfylder $\Delta \circ \Sigma_a = 1_P$, og bestem $\Sigma_0(\binom{}{i})$. Vis, at for $n \in \mathbb{N}$ gælder $(\Sigma_0 f)(n) = \sum_{i=0}^{n-1} f(i)$. Vis, at der findes polynomier p_r, $r = 0,1,2,\ldots$ så at $p_r(n) = 1 + 2^r +\ldots+ n^r$ for $n \in \mathbb{N}$, og bestem p_1, p_2 og p_3.

11. Lad U være mængden af talfølger

(*) $$u_0, u_1, u_2, \ldots ,$$

hvor $u_i \in \mathbb{R}$ for $i \in \mathbb{N}_0$, og hvor

$$u_n = u_{n-1} + u_{n-2} \quad \text{for} \quad n \geq 2.$$

Vis, at U er et underrum i vektorrummet $(V, \mathbb{R})$ bestående af alle talfølger (*) med $u_i \in \mathbb{R}$ for $i \in \mathbb{N}_0$.

Vis, at $\dim U = 2$.

Find samtlige kvotientrækker

$$1, q, q^2, \ldots$$

i U, og vis, at de udgør en basis for $(U, \mathbb{R})$.

Fibonnacifølgen

$$f_0, f_1, f_2, \ldots$$

er defineret ved

$$f_0 = f_1 = 1, \; f_n = f_{n-1} + f_{n-2}, \; n \geq 2.$$

Vis formlen

$$f_n = \frac{1}{\sqrt{5}} \left\{ \left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right\}, \; n \in \mathbb{N}_0,$$

og vis herved, at

$$\frac{f_n}{f_{n-1}} \to \frac{1+\sqrt{5}}{2} \quad \text{for} \quad n \to \infty.$$

Hvilke følger i U er begrænsede?

Matematik 101

Skriftlig prøve til hjemmeregning i 4 timer.

Alle hjælpemidler er tilladt.

Sættet består af 4 opgaver.

Opgave nr. 1.

Lad $N = \{p \in S_n \mid p \circ (12) = (12) \circ p\}$, $n \geq 2$.

1° Vis, at N er en undergruppe i S_n.

2° Vis, at $p = \begin{pmatrix} 1 & 2 & \cdots & n \\ a & b & \cdots & p(n) \end{pmatrix} \in N$, hvis og kun hvis $\{a,b\} = \{1,2\}$.

3° Vis, at N har orden $(n-2)!2$.

Opgave nr. 2.

Lad V være et n-dimensionalt vektorrum over $\mathbb{R}$. En endomorfi $f : V \to V$ kaldes en *involution*, hvis $f^2 = e$, hvor $e : V \to V$ er den identiske afbildning.

1° Lad f være en vilkårlig endomorfi af V.

Vis, at mængderne

$$V_+ = \{\underline{v} \in V \mid f(\underline{v}) = \underline{v}\}, \quad V_- = \{\underline{v} \in V \mid f(\underline{v}) = -\underline{v}\}.$$

er underrum i V.

2° Vis, at $V = V_+ \oplus V_-$, hvis og kun hvis f er en involution.

3° Antag, at f er en involution. Vis, at der findes en basis $(\underline{e}_1, \ldots, \underline{e}_n)$ for V, så at den til f m.h.t. denne basis hørende matrix har formen

$$\text{diag}(1,\ldots\ 1,-1,\ldots,-1).$$

Opgave nr. 3.

1° Vis, at matricen $\underline{\underline{A}} = \begin{pmatrix} 1 & s & t \\ -s & 1 & u \\ -t & -u & 1 \end{pmatrix}$, $s,t,u \in \mathbb{R}$ er regulær, og bestem $\underline{\underline{A}}^{-1}$.

2° Lad $\underline{\underline{S}}$ være en kvadratisk matrix med reelle koefficienter, så at matricen $\underline{\underline{E}} + \underline{\underline{S}}$ er regulær. Vis, at $\underline{\underline{S}}$ kommuterer med $(\underline{\underline{E}}+\underline{\underline{S}})^{-1}$, altså at $\underline{\underline{S}}(\underline{\underline{E}}+\underline{\underline{S}})^{-1} = (\underline{\underline{E}}+\underline{\underline{S}})^{-1}\underline{\underline{S}}$.

3° Antag yderligere, at $\underline{\underline{S}}$ er antisymmetrisk. Vis, at matricen $(\underline{\underline{E}}-\underline{\underline{S}})(\underline{\underline{E}}+\underline{\underline{S}})^{-1}$ er ortogonal.

4° Bestem $(\underline{\underline{E}}-\underline{\underline{S}})(\underline{\underline{E}}+\underline{\underline{S}})^{-1}$ når $\underline{\underline{S}} = \begin{pmatrix} 0 & s & t \\ -s & 0 & u \\ -t & -u & 0 \end{pmatrix}$, $s,t,u \in \mathbb{R}$.

Opgave nr. 4.

Lad $\underline{\underline{A}} \in \mathrm{M}_{3,4}(\mathbb{R})$ være matricen

$$\underline{\underline{A}} = \begin{pmatrix} 1 & 2 & 1 & 4 \\ -1 & 0 & 1 & 2 \\ 0 & 3 & 3 & 1 \end{pmatrix},$$

og lad $f : \mathbb{R}^4 \to \mathbb{R}^3$ være den ved $\underline{x}_{|} \mapsto \underline{\underline{A}}\underline{x}_{|}$ givne afbildning.

1° Find f's rang, og angiv en basis for f's kerne.

2° Find for $i = 1,2$ og 3 en løsning til matrixligningen $\underline{\underline{A}}\underline{x}_{|} = \underline{e}_{|i}$, hvor $\underline{e}_{|1} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$, $\underline{e}_{|2} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ og $\underline{e}_{|3} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$.

3° Find en matrixfremstilling for en lineær afbildning $g : \mathbb{R}^3 \to \mathbb{R}^4$, som opfylder, at $f \circ g$ er den identiske afbildning.

12. Lad U og W være underrum i vektorrummet V, og lad $\kappa : V \to V/U$ være restklasseafbildningen. Vis, at $\kappa^{-1}(\kappa(W)) = W + U$, og find en naturlig isomorfi $(W+U)/U \xrightarrow{\sim} \kappa(W)$. Vis, at kernen for den ved $\underline{w} \mapsto \kappa(\underline{w})$ bestemte afbildning : $W \to \kappa(W)$ er $W \cap U$ og find nu en isomorfi

$$W/W \cap U \xrightarrow{\sim} (W+U)/U$$

Antag nu, at $W \supseteq U$, og find en isomorfi $V/W \xrightarrow{\sim} (V/U)/\kappa(W)$. Identificerer vi $\kappa(W)$ med W/U (jfr. det ovenfor fundne), kan denne isomorfi skrives

$$V/W \xrightarrow{\sim} (V/U)/(W/U)$$

13. Lad $V,V',<,>$ være et dualt par, og lad V_1 og V_2 være underrum i V. Vis relationerne

$$(V_1+V_2)^\circ = V_1^\circ \cap V_2^\circ.$$
$$(V_1 \cap V_2)^\circ \supseteq V_1^\circ + V_2^\circ.$$

Vis, at = gælder i den sidste relation når V har endelig dimension.

14. Vis, at vektorrummene F og $F_\circ$ fra suppl. øv. 4 er i dualitet ved bilinearformen $<,> : F \times F_\circ \to \mathbb{R}$ defineret ved $<f,\varphi> = \sum_{t \in \mathbb{R}} f(t)\varphi(t)$.
Betragt $U = F_\circ$ som underrum i F, og vis, at $U^{\circ\circ} = F \supset U$.

15. Lad V være et vektorrum over $\mathbb{C}$. V "består" altså af en *mængde* V_o og en *addition* : $V_o \times V_o \to V_o$ betegnet $(\underline{u},\underline{v}) \mapsto \underline{u} + \underline{v}$ og en *multiplikation med skalar* : $\mathbb{C} \times V_o \to V_o$ betegnet $(\lambda,\underline{v}) \to \lambda\underline{v}$, så at visse aksiomer er opfyldte. Vis, at vi kan definere et nyt vektorrum $\overline{V}$ over $\mathbb{C}$ ved som mængde at bruge V_o, som addition at bruge additionen i V og som multiplikation med skalar at bruge afbildningen $(\lambda,\underline{v}) \mapsto \overline{\lambda}\underline{v}$. [som f.eks. betegnes $(\lambda,\underline{v}) \mapsto \lambda \cdot_k v$; $\overline{V}$ kaldes V's konjugerede vektorrum]. Overvej, at en delmængde $M \subseteq V_o$ er et frembringersystem (resp. et lin.uafh. syst., resp. en basis, resp. et underrum,...) i V, hvis og kun hvis M er et frembringersystem (resp. .....) i $\overline{V}$. Specielt er altså $\dim V = \dim\overline{V}$. Lad nu $f : V \to W$ være en lineær afbildning. f er da en afbildning (af en speciel type) mellem de underliggende mængder $V_o \to W_o$, og kan derfor også opfattes som en afbildning $\overline{V} \to \overline{W}$. Vis, at denne afbildning er lineær. Denne afbildning kaldes f's konjugerede afbildning og betegnes $\overline{f}$. Antag nu at f i baser fra V og W beskrives ved matricen $\underline{\underline{A}} \in \mathrm{M}_{m,n}(\mathbb{C})$, og vis, at $\overline{f}$ i de samme baser (opfattet som baser for de konjugerede rum) beskrives ved matricen $\overline{\underline{\underline{A}}} \in \mathrm{M}_{m,n}(\mathbb{C})$.

Skønt $\dim V = \dim\overline{V}$, er den normalt ikke noget naturligt valg af en isomorfi $V \xrightarrow{\sim} \overline{V}$. Lad $(V,\mathbb{C})$ være den komplekse udvidelse af et reelt vektorrum. Vis, at konjugering (Suppl. øv. 7) er en (lineær) isomorfi $k : V \xrightarrow{\sim} \overline{V}$. Vis, at et indre produkt $V \times V \to \mathbb{C}$ i et vektorrum V over $\mathbb{C}$ kan opfattes som en dualitet $V \times \overline{V} \to \mathbb{C}$.

16. For en lineær afbildning $f : U \to V$ med kerne $\mathrm{Ker}(f)$ gælder dimensionsformlen

$$\dim\mathrm{Ker}(f) + \dim f(U) = \dim U.$$

Ofte har man mere nytte af følgende
Opskrift: "Man tager en basis $(\underline{v}_1,\ldots,\underline{v}_m)$ for $f(U)$, man "løfter" den til vektorer $(\underline{u}_1,\ldots,\underline{u}_m)$ i U [d.v.s. man vælger vektorer u_i i U, så $\underline{u}_i \overset{f}{\mapsto} \underline{v}_i$], og man supplerer disse vektorer med en basis $(\underline{w}_1,\ldots,\underline{w}_p)$ for $\mathrm{Ker}(f)$. Man har da en basis $(\underline{u}_1,\ldots,\underline{u}_m,\underline{w}_1,\ldots,\underline{w}_p)$ for U".
Prøv denne opskrift.

17. Læs omhyggeligt følgende bevis for sætningen om Jordans normalform:

(a) Lemma. Lad $g : V \to V$ være en endomorfi i et endeligdimensionalt vektorrum. Der findes en opspaltning $V = U \oplus W$ i invariante underrum, så at g er nilpotent på U og bijektiv i W.

Bevis: I følgen $V \supseteq g(V) \supseteq g^2(V) \supseteq \ldots$ af invariante underrum må der gælde = fra et vist trin. Af $g^{\nu+1}(V) = g^{\nu}(V)$ følger, at g er bijektiv (= surjektiv) på $g^{\nu}(V)$. Hvis $\underline{v} \in \mathrm{Ker}(g^{\nu}) \cap g^{\nu}(V)$, har vi $g^{\nu}(\underline{v}) = \underline{o}$, og dermed $\underline{v} = \underline{o}$, da g er injektiv på $g^{\nu}(V)$. Altså er $\mathrm{Ker}(g^{\nu}) \cap g^{\nu}(V) = \{\underline{o}\}$, og da $\dim V = \dim\mathrm{Ker}(g^{\nu}) + \dim g^{\nu}(V)$, slutter vi, at $V = \mathrm{Ker}(g^{\nu}) \oplus g^{\nu}(V)$.

(b) Sætning Lad $f : V \to V$ være en endomorfi af et endeligdimensionalt vektorrum over $\mathbb{C}$ med egenværdierne $\lambda_1,\ldots,\lambda_r$. Der findes en opspaltning $V = U_1 \oplus \ldots \oplus U_r$ i invariate underrum, så at $f - \lambda_i e$ er nilpotent på U_i.

Bevis. Vi har

$$V = U_1 \oplus W_1 \qquad \left(\begin{array}{l}\text{(a) anvendt på } f - \lambda_1 e : V \to V \text{ med } f - \lambda_1 e \\ \text{nilpotent på } U_1,\ f - \lambda_1 e \text{ bijektiv på } W_1.\end{array}\right)$$

$$= U_1 \oplus U_2 \oplus W_2 \qquad \left(\begin{array}{l}\text{(a) anvendt på } f - \lambda_2 e : W_1 \to W_1 \text{ med} \\ f - \lambda_2 e \text{ nilpotent på } U_2,\ f - \lambda_2 e \text{ bi-} \\ \text{jektiv på } W_2.\end{array}\right)$$

$$\vdots$$

$$= U_1 \oplus \ldots \oplus U_r \oplus W_r \qquad \left(\begin{array}{l}\text{(a) anvendt på } f - \lambda_r e : W_{r-1} \to W_{r-1} \text{ med} \\ f - \lambda_r e \text{ nilpotent på } U_r,\ f - \lambda_r e \text{ bijektiv} \\ \text{på } W_r.\end{array}\right)$$

Nu er $f - \lambda_i e$ specielt injektiv på W_i, og dermed også injektiv på $W_r \subseteq W_i$. Intet af tallene $\lambda_1,\ldots,\lambda_r$ er derfor egenværdi for $f : W_r \to W_r$. Heraf følger (da legemet er $\mathbb{C}$) at $W_r = \{\underline{o}\}$.

(c) *Jordans normalform for en nilpotent endomorfi* $h : U \to U$. Påstanden er, at der findes en basis (en "Jordanbasis for h") i hvilken h beskrives ved en blokmatrix:

$$\begin{pmatrix} \underline{\underline{B}}_1 & & 0 \\ & \ddots & \\ 0 & & \underline{\underline{B}}_p \end{pmatrix}$$

hvor hver blok $\underline{\underline{B}}_i$ har formen $\begin{pmatrix} 0 & 1 & & 0 \\ 0 & 0 & 1 & \\ & & \ddots & \\ & & 0 & 1 \\ 0 & & & 0 \end{pmatrix}$

At en basis er en Jordanbasis for h betyder at den kan deles i grupper: $(\underline{u}_0, \underline{u}_1, \ldots, \underline{u}_k; \underline{v}_0, \ldots, \underline{v}_l; \underline{w}_0, \ldots, \underline{w}_m; \ldots)$ [svarende til hver af blokkene] så at

$$(*) \qquad \begin{array}{l} u_k \overset{h}{\mapsto} \ldots \overset{h}{\mapsto} \underline{u}_1 \overset{h}{\mapsto} \underline{u}_0 \overset{h}{\mapsto} \underline{0} \\ \underline{v}_l \overset{h}{\mapsto} \ldots \overset{h}{\mapsto} \underline{v}_1 \overset{h}{\mapsto} \underline{v}_0 \overset{h}{\mapsto} \underline{0} \\ \underline{w}_m \overset{h}{\mapsto} \ldots \overset{h}{\mapsto} \underline{w}_1 \overset{h}{\mapsto} \underline{w}_0 \overset{h}{\mapsto} \underline{0} \\ \vdots \end{array}$$

At der til hver nilpotent endomorfi $h : U \to U$ findes en Jordanbasis vises nu ved induktion efter dim$U$. h definerer en surjektiv lineær afbildning: $U \to h(U)$. Hvis $h(U) = \{\underline{o}\}$, altså $h = 0$ er påstanden triviel. Hvis $h(U) \neq \{\underline{o}\}$, er dim$U$ > dim$h(U)$! Antag derfor, at vi har fundet en Jordanbasis som i (*) for den nilpotente endomorfi $h : h(U) \to h(U)$. Ifølge "opskriften" får vi en basis for U ved at "løfte" basen for $h(U)$ og supplere med en basis for Ker(h). Vi "løfter" nu vektorerne i (*) ved at vælge $\underline{u}_{k+1}$, $\underline{v}_{l+1}$, $\underline{w}_{m+1}$ ... i U, så at $\underline{u}_{k+1} \overset{h}{\mapsto} \underline{u}_k$, $\underline{v}_{l+1} \overset{h}{\mapsto} \underline{v}_l$, $\underline{w}_{m+1} \overset{h}{\mapsto} \underline{w}_m, \ldots$, og ved som "løftning" hver af de øvrige vektorer i (*) at vælge den vektor i (*) der står umiddelbart til venstre. De "løftede" vektorer har nu index > 0. Vi skal supplere med en basis for Ker(h).

Vi har allerede de lineært uafhængige vektorer $\underline{u}_0, \underline{v}_0, \underline{w}_0, \ldots$ i denne kerne, og vi supplerer disse vektorer med vektorer $\underline{x}_0, \underline{y}_0, \ldots$ til en basis for Ker(h). Den således bestemte basis for U er klart en Jordanbasis:

$$\begin{array}{llllllll}
\underline{u}_{k+1} & \overset{h}{\mapsto} \underline{u}_k & \overset{h}{\mapsto} \ldots & \overset{h}{\mapsto} \underline{u}_1 & \overset{h}{\mapsto} \underline{u}_0 & \overset{h}{\mapsto} \underline{o} \\
\underline{v}_{l+1} & \overset{h}{\mapsto} \underline{v}_l & \overset{h}{\mapsto} \ldots & \overset{h}{\mapsto} \underline{v}_1 & \overset{h}{\mapsto} \underline{v}_0 & \overset{h}{\mapsto} \underline{o} \\
\underline{w}_{m+1} & \overset{h}{\mapsto} \underline{w}_m & \overset{h}{\mapsto} \ldots & \overset{h}{\mapsto} \underline{w}_1 & \overset{h}{\mapsto} \underline{w}_0 & \overset{h}{\mapsto} \underline{o} \\
 & & & & \vdots & \\
 & & & & \underline{x}_0 & \overset{h}{\mapsto} \underline{o} \\
 & & & & \underline{y}_0 & \overset{h}{\mapsto} \underline{o} \\
 & & & & \vdots &
\end{array}$$

[I $\boxed{}$ står de "løftede vektorer; udenfor står en basis for kernen]

(d) *Jordans normalform* for en endomorfi $f : V \to V$. Vi betragter opspaltningen $V = U_1 \oplus \ldots \oplus U_r$ fra (b). $f - \lambda_i e$ er nilpotent på U_i, så vi kan finde en Jordanbasis for $f - \lambda_i e$ på U_i. Nu er $f = \lambda_i e + (f - \lambda_i e)$ så $f : U_i \to U_i$ beskrives i denne basis ved en Jordan matrix med λ_i i hoveddiagonalen. Forenes de for hvert i fundne vektorer i U_i fås en basis for $V = U_1 \oplus \ldots \oplus U_r$ i hvilken f beskrives ved en Jordanmatrix.

(e) Normalformen for endomorfien f er entydig, bortset fra permutation af blokkene.

Lad der være givet en basis for V i hvilken f er bestemt ved en Jordanmatrix. For hvert $\lambda \in \mathbb{C}$, og $i = 1,2,\ldots$ betegner vi med $\alpha(i,\lambda)$ det antal gange $i\times i$ blokken

$$\left.\begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & 1 & \\ & & \ddots & \ddots \\ & & & 1 \\ 0 & & & \lambda \end{pmatrix}\right\} i$$

forekommer i denne Jordanmatrix. Påstanden er, at disse tal $\alpha(i,\lambda)$ kan bestemmes alene ud fra endomorfien f. Hvis λ ikke er egenværdi for f, har vi øjensynlig $\alpha(i,\lambda) = 0$ for alle i. Antag nu, at λ er en egenværdi, og sæt $\alpha(i,\lambda) = \alpha_i$. En passende permutation af vektorerne i den givne basis vil permutere blokkene i Jordanmatricen, og vil altså ikke ændre α_i'erne. Vi kan derfor for overskuelighedens skyld antage, at Jordanmatricen "begynder" (øverst til venstre) med alle de blokke, der har λ i diagonalen. I den givne basis beskrives $f - \lambda e$ altså ved en blokmatrix

$$\begin{pmatrix} \underline{\underline{N}} & \underline{\underline{0}} \\ \underline{\underline{0}} & \underline{\underline{S}} \end{pmatrix}$$ hvor

$$\underline{\underline{N}} = \begin{pmatrix} \underline{\underline{N}}_1 & & \underline{\underline{0}} \\ & \ddots & \\ & \underline{\underline{N}}_i & \\ & & \ddots \\ \underline{\underline{0}} & & \underline{\underline{N}}_i \end{pmatrix} \left.\begin{matrix} \\ \\ \\ \\ \\ \end{matrix}\right\} \alpha_i \text{ gange} \qquad \underline{\underline{N}}_i = \left.\begin{pmatrix} 0 & 1 & & 0 \\ & 0 & 1 & \\ & & \ddots & \ddots \\ & & & 1 \\ 0 & & & 0 \end{pmatrix}\right\} i$$

og hvor $\underline{\underline{S}}$ er en regulær matrix (øvre trekantsmatrix med diagonalelementer $\lambda_j - \lambda \neq 0$). $(f-\lambda e)^k$ beskrives nu ved matricen $\begin{pmatrix} \underline{\underline{N}}^k & \underline{\underline{0}} \\ \underline{\underline{0}} & \underline{\underline{S}}^k \end{pmatrix}$ og

$$\underline{\underline{N}}^k = \begin{pmatrix} \ddots & & \\ & \underline{\underline{N}}_i^k & 0 \\ & 0 & \underline{\underline{N}}_i^k \\ & & \ddots \end{pmatrix} \quad \alpha_i \text{ gange}$$

og $\underline{\underline{N}}_i^k = \underline{\underline{0}}$ når $k \geq i$.

Følgelig er $\operatorname{rg}(f-\lambda e)^k = \sum_i \alpha_i \operatorname{rg}\underline{\underline{N}}_i^k + \operatorname{rg}\underline{\underline{S}}^k$. Her er

$$\operatorname{rg}\underline{\underline{N}}_i^k = \begin{cases} i-k & \text{når } k \leq i \\ 0 & \text{når } k \geq i \end{cases} \quad \text{og} \quad \operatorname{rg}\underline{\underline{S}}^k = \operatorname{rg}\underline{\underline{S}} \text{ da } \underline{\underline{S}} \text{ er regulær.}$$

Betragtes følgen $n_k = \operatorname{rg}(f-\lambda e)^k$, $k = 0,1,2,\ldots$ har vi altså $n_k = \sum_{i>k} \alpha_i(i-k) + \operatorname{rg}\underline{\underline{S}}$. Følgen af 1^{ste}-differencer i følgen $n_0, n_1, n_2, \ldots$ er altså følgen

$$n_k - n_{k+1} = \alpha_{k+1} + \alpha_{k+2} + \ldots \qquad k = 0,1,\ldots$$

og 2^{den}-differencerne i følgen $n_0, n_1, n_2, \ldots$ bliver altså α_{k+1}, $k = 0,1,\ldots$. Vi har vist:

Sætter vi (for et fast $\lambda \in \mathbb{C}$) $n_k = \operatorname{rg}(f-\lambda e)^k$ og $\alpha_i = \alpha(i,\lambda)$, da gælder: *Følgen* $n_0, n_1, n_2, \ldots$ *har udseendet*

$$n_0 > n_1 > \ldots > n_{p-1} > n_p = n_{p+1} = \ldots$$

og 2^{den}*-differencerne i denne følge er netop følgen* $\alpha_1, \alpha_2, \alpha_3, \ldots$.

(f) Opspaltningerne i (a) og (b) er entydige.

Bevis. Hvis $V = U \oplus W$ er en opspaltning som i (a), da er $U \subseteq \mathrm{Ker}(g^\nu)$ for alle "store" ν, og $W = g(W) = \ldots = g^\nu(W) \subseteq g^\nu(V)$, da g specielt er surjektiv på W. Altså $U \subseteq \mathrm{Ker}(g^\nu)$, $W \subseteq g^\nu(V)$ for alle "store" ν. Da $V = \mathrm{Ker}(g^\nu) \oplus g^\nu(V)$ for alle "store" ν, følger det, at $U = \mathrm{Ker}(g^\nu)$, $W = g^\nu(V)$ for alle store ν.

Hvis $V = U_1 \oplus \ldots \oplus U_r$ er en opspaltning som i (b), bemærker vi, at $(f-\lambda_2 e) \circ \ldots \circ (f-\lambda_r e)$ er nilpotent på $U_2 \oplus \ldots \oplus U_r$, og injektiv og dermed bijektiv på U_1. Af entydigheden fra (a) følger nu, at U_1 er entydig, og ved permutation, at U'erne er entydige.

18. Lad $(\tilde{V}, \mathbb{C})$ være den komplekse udvidelse af et vektorrum $(V, \mathbb{R})$, og betragt V som en delmængde af $\tilde{V}$. For $\underline{\tilde{v}} \in \tilde{V}$ sætter vi $\frac{1}{2}(\underline{\tilde{v}} + k(\underline{\tilde{v}})) = \mathrm{Re}(\underline{\tilde{v}})$, og $\frac{1}{2i}(\underline{\tilde{v}} - k(\underline{\tilde{v}})) = \mathrm{Im}(\underline{\tilde{v}})$. Vis, at $\mathrm{Re}(\underline{\tilde{v}})$ og $\mathrm{Im}(\underline{\tilde{v}})$ er reelle (d.v.s. $\in V$), og at $\underline{\tilde{v}} = \mathrm{Re}(\underline{\tilde{v}}) + i\,\mathrm{Im}(\underline{\tilde{v}})$.

(a) Lad $(\underline{v}_1, \ldots, \underline{v}_n)$ være en basis for $(V, \mathbb{R})$. Vis, at disse vektorer også er en basis for $(\tilde{V}, \mathbb{C})$. Vis, at hvis en endomorfi $f : V \to V$ i basen $(\underline{v}_1, \ldots, \underline{v}_n)$ beskrives ved matricen $\underline{\underline{A}} \in \mathrm{M}_{n,n}(\mathbb{R})$, så vil den komplekse udvidelse $\tilde{f} : \tilde{V} \to \tilde{V}$ i basen $(\underline{v}_1, \ldots, \underline{v}_n)$ være beskrevet ved den samme matrix $\underline{\underline{A}} \in \mathrm{M}_{n,n}(\mathbb{R}) \subseteq \mathrm{M}_{n,n}(\mathbb{C})$.

(b) Lad $W \subseteq \tilde{V}$ være et komplekst underrum, som opfylder $W = k(W)$. Vis, at W har en (kompleks) basis bestående af vektorer fra V (reelle vektorer).

(c) Lad $W \subseteq \tilde{V}$ være et komplekst underrum, som opfylder $W \cap k(W) = \{\underline{o}\}$, og lad $\underline{w}_1,\ldots,\underline{w}_r$ være en (kompleks) basis for W. Vis, at vektorerne $\mathrm{Re}(\underline{w}_1)$, $\mathrm{Im}(\underline{w}_1),\ldots,\mathrm{Re}(\underline{w}_r),\mathrm{Im}(\underline{w}_r)$ er en (kompleks) basis for $W + k(W)$.

(d) Lad $f : V \to V$ være en endomorfi, og sæt $W_\lambda = \mathrm{Ker}(\tilde{f}-\lambda e) \subseteq \tilde{V}$, for $\lambda \in \mathbb{C}$. Vis, at $k(W_\lambda) = W_\lambda$. Slut heraf: Hvis en (og dermed alle!) matricer hørende til f er en komplekst diagonaliserbar, da findes en (reel) basis for V, i hvilken der til f hører en matrix af formen

$$\begin{pmatrix} \lambda_1 & & & & & \\ & \ddots & & & & \\ & & \lambda_t & & & \\ & & & \begin{pmatrix} \alpha_1 & \beta_1 \\ -\beta_1 & \alpha_1 \end{pmatrix} & & \\ & & & & \ddots & \\ & & & & & \begin{pmatrix} \alpha_s & \beta_s \\ -\beta_s & \alpha_s \end{pmatrix} \end{pmatrix};$$

her kommer diagonal elementerne λ_i fra egenværdierne dvs. fra de reelle rødder i $p_f(t)$ og blokkene $\begin{pmatrix} \alpha_\nu & \alpha_\nu \\ \alpha_\nu & \alpha_\nu \end{pmatrix}$ kommer fra par af komplekst konjugerede rødder $\alpha_\nu \pm i\beta_\nu$ i $p_f(t)$.

19. Lad $(V,\mathbb{R},\cdot)$ være et reelt vektorrum med indre produkt. Vis, at der ved

$$(\underline{v}'+i\underline{v}'')\cdot(\underline{u}'+i\underline{u}'') = [(\underline{v}'\cdot\underline{u}')+(\underline{v}''\cdot\underline{u}'')] + i[\underline{v}''\cdot\underline{u}'-\underline{v}'\cdot\underline{u}'']$$

$\underline{v}',\underline{v}'',\underline{u}',\underline{u}'' \in V$, defineres et indre produkt i $(\tilde{V},\mathbb{C})$. Den komplekse udvidelse af et Euklidisk vektorrum er altså på naturlig måde et unitært vektorrum.

(a) Lad $f : V \to V$ være en endomorfi. Vis, at $\tilde{f}^* = \widetilde{f^*}$, og slut, at der gælder

$$f \text{ er normal} \Leftrightarrow \tilde{f} \text{ er normal}$$
$$f \text{ er ortogonal} \Leftrightarrow \tilde{f} \text{ er unitær.}$$

(b) Lad $W \subseteq \tilde{V}$ være et komplekst underrum, som opfylder, at W og $k(W)$ er ortogonale, og lad $\underline{w}_1,\ldots,\underline{w}_r$ være en ortonormal basis for W. Vis, at vektorerne

$\frac{1}{\sqrt{2}}\mathrm{Re}(\underline{w}_1)$, $\frac{1}{\sqrt{2}}\mathrm{Im}(\underline{w}_1),\ldots,\frac{1}{\sqrt{2}}\mathrm{Re}(\underline{w}_r)$, $\frac{1}{\sqrt{2}}\mathrm{Im}(\underline{w}_r)$ er en ortonormal basis for $W + k(W)$.

(c) Vis, at en normal endomorfi $f : V \to V$ i en passende ortonormal basis for V kan beskrives ved en matrix af formen

$$\begin{pmatrix} \lambda_1 & & & & & & \\ & \lambda_2 & & & & 0 & \\ & & \ddots & & & & \\ & & & \lambda_s & & & \\ & & & & \begin{pmatrix} \alpha_1 & \beta_1 \\ -\beta_1 & \alpha_1 \end{pmatrix} & & \\ & 0 & & & & \ddots & \\ & & & & & & \begin{pmatrix} \alpha_t & \beta_t \\ -\beta_t & \alpha_t \end{pmatrix} \end{pmatrix}$$

[Sammenlign med suppl. øv. 18 ⓓ].

Slut heraf:

ⓓ En selvadjungeret endomorfi $f : V \to V$ kan i en passende ortonormal basis beskrives ved en diagonalmatrix. Og

ⓔ En ortogonal endomorfi $f : V \to V$ kan i en passende ortonormal basis beskrives ved en matrix af formen

$$\begin{pmatrix} 1 & & & & & & & & \\ & 1 & & & & & & & \\ & & \ddots & & & & & & \\ & & & 1 & & & & & \\ & & & & -1 & & & & \\ & & & & & -1 & & & \\ & & & & & & \ddots & & \\ & & & & & & & -1 & \\ & & & & & & & & \begin{pmatrix} \cos\theta_1 & \sin\theta_1 \\ -\sin\theta_1 & \cos\theta_1 \end{pmatrix} \\ & & & & & & & & & \ddots \\ & & & & & & & & & & \begin{pmatrix} \cos\theta_t & \sin\theta_t \\ -\sin\theta_t & \cos\theta_t \end{pmatrix} \end{pmatrix}$$

[Benyt at en matrix som i ⓒ er ortogonal netop når $\lambda_\nu^{\,2} = 1$, $\alpha_\nu^{\,2} + \beta_\nu^{\,2} = 1$].

20. Vis, at $\underline{\underline{A}} \to \|\underline{\underline{A}}\|_\infty = \sup_{i,j} |a_{ij}|$ definerer en norm i vektorrummet $M_{m,n}(L)$. (L er $\mathbb{R}$ eller $\mathbb{C}$). Vektorrummene $M_{m,n}(\mathbb{R})$ og $M_{m,n}(\mathbb{C})$ bliver herved metriske rum. Lad T være et metrisk rum. En afbildning $\underline{\underline{F}} : T \to M_{m,n}(L)$ er klart helt bestemt ved sine mn koordinatfunktioner $F_{ij} : T \to L$. Vis, at $\underline{\underline{F}}$ er kontinuert netop når alle koordiantfunktionerne $F_{ij} : T \to L$

er kontinuerte. Vis, at hvis $\underline{\underline{F}}$ er kontinuert, og $\underline{\underline{S}} \in \mathrm{M}_{p,m}(L)$, så er også den ved $\underline{\underline{S}}\underline{\underline{F}} : t \mapsto \underline{\underline{S}}\underline{\underline{F}}(t)$ bestemte afbildning: $T \to \mathrm{M}_{p,n}(L)$ kontinuert.

(a) Lad $\underline{\underline{A}} \in GL_n(\mathbb{C})$ $(\subseteq \mathrm{M}_{n,n}(\mathbb{C}))$. Der findes da en regulær matrix $\underline{\underline{S}} \in GL_n(\mathbb{C})$, så at $\underline{\underline{B}} = \underline{\underline{S}}\underline{\underline{A}}\underline{\underline{S}}^{-1}$ er en øvre trekantsmatrix, med diagonalelementerne $b_{\nu\nu} \neq 0$. Skriv nu hvert $b_{\nu\nu}$ på formen $b_{\nu\nu} = r_\nu e^{i\theta_\nu}$, hvor $r_\nu > 0$, $\theta_\nu \in \mathbb{R}$. Lad (for $0 \leq t \leq 1$) $\underline{\underline{B}}(t)$ være den ved

$$b_{\nu\mu}(t) = \begin{cases} \dfrac{r_\nu}{t+(1-t)r_\nu} e^{it\theta_\nu} & \nu = \mu \\ tb_{\nu\mu} & \nu \neq \mu . \end{cases}$$

Vis, at $\underline{\underline{B}}(t) \in GL_n(\mathbb{C})$, at $t \mapsto \underline{\underline{B}}(t)$ er kontinuert, at $\underline{\underline{B}}(0) = \underline{\underline{E}}$ og at $\underline{\underline{B}}(1) = \underline{\underline{B}}$. Den ved $\underline{\underline{F}} : t \mapsto \underline{\underline{S}}^{-1}\underline{\underline{B}}(t)\underline{\underline{S}}$ bestemte afbildning $[0,1] \to GL_n(\mathbb{C})$ er altså kontinuert, og opfylder $\underline{\underline{F}}(0) = \underline{\underline{E}}$, $\underline{\underline{F}}(1) = \underline{\underline{A}}$. Vi har vist: *$GL_n(\mathbb{C})$ er en kurve sammenhængende delmængde af $\mathrm{M}_{n,n}(\mathbb{C})$*. Vis, at $GL_n(\mathbb{R})$ ikke er kurvesammenhængende.

(b) Vis, at $SL_n(\mathbb{C})$, $U(n)$ og $SU(n)$ er kurvesammenhængende.

(c) Gør rede for at en basis $\underline{u}_1, \ldots, \underline{u}_n$ i et vektorrum med indre produkt kontinuert kan overføres i en ortonormal basis (kig på Gram-Schmidt's ortonormalisering), og slut heraf, at enhver matrix $\underline{\underline{A}} \in GL_n(\mathbb{R})$ kan kurveforbindes indenfor $GL_n(\mathbb{R})$ med en ortogonal matrix.

ⓓ Vis, at $O^+(n) = SO(n,\mathbb{R})$ er kurvesammenhængende.[Benyt normalformen fra Suppl. øv. 19 ⓔ og udnyt, at

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} \cos\pi & \sin\pi \\ -\sin\pi & \cos\pi \end{pmatrix}]$$

ⓔ Vis, at $GL_n^+(\mathbb{R}) = \{\underline{\underline{A}} \in GL_n(\mathbb{R}) \mid \det\underline{\underline{A}} > 0\}$ er kurvesammenhængende, og vis, at $SL_n(\mathbb{R})$ er kurvesammenhængende.

21. Lad V være et unitært vektorrum, og lad $f_1,\ldots,f_p$ være normale endomorfier, og antag, at f'erne kommuterer, d.v.s. at $f_i\, f_j = f_j\, f_i$. Vis, at der findes en ortonormal basis for V, i hvilken alle f'erne beskrives ved diagonalmatricer [Vink: For $(\lambda_1,\ldots,\lambda_p) \in \mathbb{C}^p$ sættes $V_{\lambda_1,\ldots,\lambda_p} = \mathrm{Ker}(f_1-\lambda_1 e) \cap \ldots \cap \mathrm{Ker}(f_p-\lambda_p e)$. Vis, at underrummene $V_{\lambda_1,\ldots,\lambda_p} \subseteq V$ er ortogonale, og (f.eks. ved induktion) at deres sum er hele V].

22. ⓐ Lad G være en endelig gruppe af orden n, med elementerne $\{e = s_1, s_2, \ldots, s_n\}$, og betragt det n-dimensionale vektorrum $F = Afb(G,\mathbb{C})$ af alle afbildninger $G \to \mathbb{C}$. Vis, at der ved

$$\varphi\cdot\psi = \frac{1}{n}\,\Sigma\varphi(t)\overline{\psi(t)}$$

defineres et indre produkt i F. Lad $\delta_i \in F$ være den ved

$$\delta_i(t) = \begin{cases} 1 & \text{når } t = s_i \\ 0 & t \neq s_i \end{cases}$$ bestemte afbildning. Vis, at

$(\frac{1}{\sqrt{n}}\delta_1,\ldots,\frac{1}{\sqrt{n}}\delta_n)$ er en ortonormal basis for F.

(b) For $s \in G$ og $\varphi \in F$ betegner vi med $r_s\varphi$ det ved $r_s\varphi : t \mapsto \varphi(ts)$ bestemte element i F. Vis, at $r_s : F \to F$ er unitær, og at $r_{ss'} = r_s \circ r_{s'}$.

(c) Antag nu, at G er kommutativ, og dermed, at r'erne kommuterer. Der findes følgelig en ortonormal basis $(\chi_1,\ldots,\chi_n)$ for F i hvilken hver af endomorfierne r_s, $s \in G$ beskrives ved en diagonalmatrix. For $s \in G$, $i = 1,\ldots,n$ har vi altså

$$(*) \qquad r_s(\chi_i) = \lambda_i(s)\chi_i \quad \text{med} \quad \lambda_i(s) \in \mathbb{C},$$

og da r_s er unitær, gælder $|\lambda_i(s)| = 1$. Slut nu, at der gælder $|\chi_i(s)| = 1$, $s \in G$, $i = 1,\ldots,n$, specielt $|\chi_i(e)| = 1$. Uden at ændre ortonormaliteten og relationen (*) kan vi derfor antage, at $\chi_i(e) = 1$, $i = 1,\ldots,n$. Vis, at dette medfører, at $\chi_i = \lambda_i$ er en $\mathbb{C}$-karakter på G, og at funktionerne χ_i, $i = 1,\ldots,n$ er samtlige $\mathbb{C}$-karakterer på G (jfr. suppl øv. 3). Altså: En kommutativ gruppe af orden n har netop n $\mathbb{C}$-karakterer $\chi : G \to \mathbb{C}^*$, og disse er en ortonormal basis for $Afb(G,\mathbb{C})$, dvs.

$$\sum_{s\in G} \chi(s)\overline{\psi(s)} = \begin{cases} n & \text{når } \chi = \psi \\ 0 & \text{når } \chi \neq \psi \end{cases}.$$

Disse relationer er ensbetydende med at matricen $\frac{1}{\sqrt{n}}\chi_i(s_j)$ er unitær. Slut heraf, at de medfører, at

$$\sum_{\chi} \chi(s)\overline{\chi(t)} = \begin{cases} n & \text{når } s = t \\ 0 & s \neq t \end{cases} .$$

Vis, at produktet $\chi\psi : t \to \chi(t)\psi(t)$ af to $\mathbb{C}$-karakterer χ og ψ igen er en $\mathbb{C}$-karakter, og slut, at {$\mathbb{C}$-karakterer} er en gruppe af orden n. Den betegnes ofte $\hat{G}$. Find en naturlig homomorfi $G \to \hat{\hat{G}}$, og vis, at den er en isomorfi.

23. På side 5.3.3. er vist, hvordan man kan bestemme den inverse til en regulær matrix $\underline{\underline{A}}$, idet der gælder

$$\underline{\underline{A}}^{-1} = \frac{1}{\det \underline{\underline{A}}} \left((-1)^{i+j} \det \underline{\underline{A}}_{ij} \right)' .$$

Matricen $((-1)^{i+j}\det \underline{\underline{A}}_{ij})$ kan naturligvis dannes for enhver matrix $\underline{\underline{A}} \in M_{n,n}(L)$, og den betegnes ofte $\underline{\underline{A}}^J$. Det er ofte nyttigt at vide, at der for enhver matrix $\underline{\underline{A}} \in M_{n,n}(L)$ gælder

$$\underline{\underline{A}}\underline{\underline{A}}^J = \underline{\underline{A}}^J\underline{\underline{A}} = (\det \underline{\underline{A}})\underline{\underline{E}}.$$

Vis, at dette følger af udregningerne side 5.3.2 - 5.3.3.

24. Lad V være et n-dimensionalt vektorrum over L. Vis, at mængden $\mathrm{Alt}^p(V)$ af alternerende p-linearformer (i det følgende kaldet p-former) er et underrum i vektorrummet $Afb(V\times\ldots\times V, L)$ af alle afbildninger $V\times\ldots\times V \to L$. $\mathrm{Alt}^1(V)$ er V's duale vektorrum V^*, og vi sætter ofte $\mathrm{Alt}^0(V) = L$.

ⓐ Lad $f \in \mathrm{Alt}^1(V)$, $\varphi \in \mathrm{Alt}^p(V)$ og definer en afbildning $f\wedge\varphi : \overbrace{V\times\ldots\times V}^{p+1} \to L$ ved

$$f\wedge\varphi : (\underline{v}_1,\ldots,\underline{v}_{p+1}) \mapsto \sum_{i=1}^{p+1}(-1)^{i-1} f(\underline{v}_i)\varphi(\underline{v}_1,\ldots,\not{\underline{v}}_i,\ldots,\underline{v}_{p+1})$$

($\varphi(\underline{v}_1,\ldots,\not{\underline{v}}_i,\ldots,\underline{v}_{p+1})$ betyder $\varphi(\underline{v}_1,\ldots,\underline{v}_{i-1},\underline{v}_{i+1},\ldots,\underline{v}_{p+1})$).
Vis, at $f\wedge\varphi \in \mathrm{Alt}^{p+1}(V)$. Vis, at $f\wedge(f\wedge\varphi) = 0$ i $\mathrm{Alt}^{p+2}(V)$.

ⓑ Ved induktion kan vi til p linearformer $(f_1,\ldots,f_p)$ knytte en p-form

$$f_1 \wedge\ldots\wedge f_p = f_1\wedge(f_2\wedge\ldots\wedge f_p),$$

kaldet det ydre produkt af linearformerne $(f_1,\ldots,f_p)$. Vis, at den herved definerede afbildning

$$V^* \times\ldots\times V^* \to \mathrm{Alt}^p(V)$$

er alternerende (d.v.s. den er lineær i hver variabel, og opfylder, at $f_1 \wedge\ldots\wedge f_p = 0$ når et $f_i = f_j$ for $i \neq j$).

ⓒ Lad $f_1,\ldots,f_n$ være en basis for V^*, og lad $\underline{e}_1,\ldots,\underline{e}_n$ være den duale basis for V (bestemt ved $f_i(\underline{e}_j) = \delta_{ij}$).
Lad I,J være to delmængder af $\{1,\ldots,n\}$ med p elementer:
$I = \{i_1,\ldots,i_p\}$ med $1 \leqq i_1 < i_2 <\ldots< i_p \leqq n$,
$J = \{j_1,\ldots,j_p\}$ med $1 \leqq j_1 <\ldots< j_p \leqq n$. Vis, at

$$(f_{i_1}\wedge\ldots\wedge f_{i_p})(\underline{e}_{j_1},\ldots,\underline{e}_{j_p}) = \begin{cases} 1 & \text{når } I = J \\ 0 & \text{når } I \neq J \end{cases}.$$

Slut heraf: p-formerne

$$f_{i_1}\wedge\ldots\wedge f_{i_p},\quad 1 \leqq i_1 < i_2 <\ldots< i_p \leqq n$$

er en basis for $\mathrm{Alt}^p(V)$. [Benyt, at en p-form er helt bestemt ved sine værdier på $(\underline{e}_{j_1},\ldots,\underline{e}_{j_p})$, $1 \leqq j_1 <\ldots< j_p \leqq n$, og at det foregående viser, at disse kan foreskrives vilkårligt]. Bestem $\dim\mathrm{Alt}^p(V)$, $p = 0,1,\ldots$ og fremhæv tilfældet $p = n$.

25. Tilføjelser til Kap. 7, øv. 32.

Tilføj efter øvelsens linie 7: Vis, at der for alle $\underline{u}_1,\underline{u}_2,\underline{u}_3,\underline{v}_1,\underline{v}_2,\underline{v}_3 \in V$ gælder:

$$(*)\qquad \det(\underline{u}_i\cdot\underline{v}_j) = \varphi_o(\underline{u}_1,\underline{u}_2,\underline{u}_3)\varphi_o(\underline{v}_1,\underline{v}_2,\underline{v}_3).$$

[Vink: For faste $\underline{u}_1,\underline{u}_2,\underline{u}_3 \in V$ er den ved

$$(\underline{v}_1,\underline{v}_2,\underline{v}_3) \mapsto \det(\underline{u}_i\cdot\underline{v}_j)$$

bestemte afbildning $V\times V\times V \to \mathbb{R}$ alternerende, altså af formen $\lambda\varphi_o$, hvor proportionalitetsfaktoren $\lambda = \lambda(\underline{u}_1,\underline{u}_2,\underline{u}_3)$ naturligvis afhænger af $\underline{u}_1,\underline{u}_2,\underline{u}_3$, altså

$$\det(\underline{u}_i\cdot\underline{v}_j) = \lambda(\underline{u}_1,\underline{u}_2,\underline{u}_3)\varphi_o(\underline{v}_1,\underline{v}_2,\underline{v}_3).$$

Hvis $(\underline{v}_1,\underline{v}_2,\underline{v}_3)$ er en positiv ortonormal basis, finder vi $\lambda(\underline{u}_1,\underline{u}_2,\underline{u}_3) = \det(\underline{u}_i\cdot\underline{v}_j)$, hvoraf fremgår, at $\lambda : V\times V\times V \to \mathbb{R}$ er alternerende, og da $\lambda(\underline{v}_1,\underline{v}_2,\underline{v}_3) = \det(\underline{v}_i\cdot\underline{v}_j) = \det\underline{\underline{E}} = 1$, må vi have $\lambda = \varphi_o$].

Tilføj efter øvelsens linie 24: [Vink: Anvend (*) på sættene $(\underline{u}_1,\underline{u}_2,\underline{v}_1\times\underline{v}_2)$ og $(\underline{v}_1,\underline{v}_2,\underline{v}_1\times\underline{v}_2)$].
Tilføj "positiv" før "basis" i øvelsens linie 31.
Tilføj efter øvelsen: Vis også relationerne fra EV øv. 28 og øv. 30.

26. Lad V være et n-dimensionalt vektorrum over $\mathbb{R}$ og lad B være en *regulær* symmetrisk bilinearform på V, som i en given basis $(\underline{e}_1,\ldots,\underline{e}_n)$ beskrives ved matricen $\underline{\underline{B}}$. Vis, at $\operatorname{sign}(\det\underline{\underline{B}}) = (-1)^{\operatorname{ind}_- B}$

ⓐ Sæt $\underline{\underline{B}}_\nu = (b_{ij})_{i,j=1,\ldots,\nu}$, og $d_\nu = \det\underline{\underline{B}}_\nu$, $\nu = 1,\ldots,n$ og *antag*, at tallene $d_1,\ldots,d_n$ alle er $\neq 0$. Vis, at $\operatorname{ind}_- B$ = (antallet af fortegnsskift i følgen $1,d_1,d_2,\ldots,d_n$)
[Vink: Sæt $V_\nu = \operatorname{Span}\{\underline{e}_1,\ldots,\underline{e}_\nu\}$, $B_\nu = B$'s restriktion til V_ν, $p_\nu = \operatorname{ind}_+ B_\nu$ og $q_\nu = \operatorname{ind}_- B_\nu$, $\nu = 1,\ldots,n$. $\underline{\underline{B}}_\nu$ er da matricen hørende til B_ν, og der gælder

$$0 \leqq p_1 \leqq p_2 \leqq \cdots \leqq p_n$$
$$0 \leqq q_1 \leqq q_2 \leqq \cdots \leqq q_n.$$

Ifølge antagelsen er B_ν'erne regulære, og der gælder følgelig $p_\nu + q_\nu = \nu$ og $\operatorname{sign}(d_\nu) = (-1)^{q_\nu}$. Heraf følger påstanden let].

ⓑ I et tilfælde, hvor antagelsen i ⓐ ikke er opfyldt (men stadig B regulær) kan $\operatorname{ind}_- B$ bestemmes ved "pertubationsmetoden", idet der løst sagt gælder: En tilstrækkelig lille ændring af koefficienterne i $\underline{\underline{B}}$ vil ikke ændre

ind_+ og ind_-, og efter en lille, passende ændring af koefficienterne i $\underline{\underline{B}}$ vil antagelsen i (a) være opfyldt. Mere præcist:

Lad $\underline{\underline{F}}$ være en symmetrisk matrix, hvis elementer alle er $\in \{0,1\}$ og sæt $\underline{\underline{B}}_\varepsilon = \underline{\underline{B}} + \varepsilon\underline{\underline{F}}$, $\varepsilon \in \mathbb{R}$. Vis, at

$$\text{ind}_+\underline{\underline{B}}_\varepsilon \geq \text{ind}_+\underline{\underline{B}}$$

$$\text{ind}_-\underline{\underline{B}}_\varepsilon \geq \text{ind}_-\underline{\underline{B}}$$

når ε er tilstrækkelig tæt ved 0.

[Vink: Vælg et indre produkt (og dermed en metrik) i V. Lad B_ε være den symmetriske bilinearform på V, der i den givne basis beskrives ved $\underline{\underline{B}}_\varepsilon$. Lad U være et positivitetsrum for B og sæt $K = \{\underline{u} \in U \mid \|\underline{u}\| = 1\}$. Der gælder da: $B > 0$ på K, og vi skal vise, at også $B_\varepsilon > 0$ på K, når ε er tilstrækkelig tæt ved 0. Hertil udnyttes, at den ved $(\underline{u},\varepsilon) \mapsto B_\varepsilon(\underline{u},\underline{u})$ bestemte afbildning $K\times\mathbb{R} \to \mathbb{R}$ er kontinuert, med værdi > 0 i ethvert $(\underline{u},0)$, $\underline{u} \in K$, i forbindelse med at K er kompakt].

Bemærk dernæst, at disse uligheder må være "ligheder" når $\underline{\underline{B}}$ er regulær.

Vis, endelig, at vi til den givne matrix $\underline{\underline{B}}$ altid kan bestemme $\underline{\underline{F}}$, så at $\underline{\underline{B}}_\varepsilon$ opfylder antagelsen i (a) når ε er tilstrækkelig tæt ved 0, $\varepsilon \neq 0$. [Vink: Vi kan faktisk altid bruge $\underline{\underline{F}} = \underline{\underline{E}}$].

Eksempel: Bestem $\text{ind}_+\underline{\underline{B}}$ og $\text{ind}_-\underline{\underline{B}}$ for

$$\underline{\underline{B}} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Brug f.x.

$$\underline{\underline{F}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

27. Lad (A,V) være et affint rum. For fast $P \in A$ er $Q \to \underline{PQ}$ en bijektiv afbildning $A \to V$; den inverse afbildning betegnes ofte $\underline{v} \to P + \underline{v}$, og for en delmængde $U \subseteq V$ betegner $P + U$ billedet ved denne afbildning, altså $P + U = \{P + \underline{v} \mid \underline{v} \in U\} = \{Q \mid \underline{PQ} \in U\}$. Lad nu $B \subseteq A$ være en delmængde, lad $U \subseteq V$ være et underrum, og lad $P \in B$. Vis, at følgende betingelser er ækvivalente: (i) B er et affint underrum med retning U. (ii) $\{\underline{PQ} \mid Q \in B\} = U$ (iii) $B = P + U$.

28. Lad K være en kvadrik i et euklidisk affint rum (A,V) og lad $B \subseteq A$ være et affint underrum. Vis, at $K \cap B$ er en kvadrik i B.

29. I stedet for § 6.3 (Triagonalisering) kan læses følgende, der bygger på Jordan's normalform. Vi har set, at der for enhver endomorfi af et n-dimensionalt komplekst vektorrum $(V,\mathbb{C})$ findes en basis for V, m.h.t. hvilken matricen for f er en Jordan-matrix, og dermed specielt en øvre trekantsmatrix. I det *reelle* tilfælde gælder:

For enhver endomorfi f af et n-dimensionalt reelt vektorrum $(V,\mathbb{R})$ er følgende tre udsagn ensbetydende:

1) *Der findes en basis for V, m.h.t. hvilken matricen for f er en Jordan-matrix.*
2) *Der findes en basis for V, m.h.t. hvilken matricen for f er en øvre trekantsmatrix.*
3) *Alle de karakteristiske rødder for f er reelle.*

Bevis. 1) ⇒ 2) fremgår af, at enhver Jordan-matrix er en øvre trekantsmatrix. 2) ⇒ 3) følger af, at hvis matricen for f er en øvre trekantsmatrix $\underline{\underline{A}} = (a_{ij})_{n,n}$, så er $p_f(t) = (a_{11}-t)\ldots(a_{nn}-t)$, hvoraf ses, at de karakteristiske rødder er diagonalelementerne $a_{11},\cdots,a_{nn}$ i $\underline{\underline{A}}$, og dermed reelle. Endelig fremgår 3) ⇒ 1) af, at beviset i Suppl. opg. 17 b også fungerer i det reelle tilfælde, når 3) er opfyldt. (I resten af beviset for eksistensen af en Jordanbasis for V mærkes slet intet til koefficientlegemet.) ∎

Resultatet kan åbenbart også udtrykkes således:

For enhver reel matrix $\underline{\underline{A}} \in \mathsf{M}_{n,n}(\mathbb{R})$ *er følgende tre udsagn ensbetydende:*

1) $\underline{\underline{A}}$ *er regulær-ækvivalent med en Jordan-matrix.*

2) $\underline{\underline{A}}$ *er regulær-ækvivalent med en øvre trekantsmatrix.*

3) *Alle de karakteristiske rødder for* $\underline{\underline{A}}$ *er reelle.*

For et vilkårligt polynomium p :

$$p(t) = \alpha_r t^r + \cdots + \alpha_1 t + \alpha_0$$

med koefficienter $\alpha_r, \cdots, \alpha_0 \in L$ (= $\mathbb{R}$ eller $\mathbb{C}$) og for enhver endomorfi f af et n-dimensionalt vektorrum (V,L) defineres en endomorfi $p(f)$ af (V,L) ved

$$p(f) = \alpha_r f^r + \cdots + \alpha_1 f + \alpha_0 e$$

idet f^r betyder f o...o f (r gange), og specielt $f^0 = e$ (den identiske endomorfi).

For to polynomier p (som anført) og q gælder:

$$(*) \qquad (pq)(f) = p(f) \circ q(f) \ .$$

Analogt for et produkt af flere polynomier, lad nemlig:

$$q(t) = \beta_s t^s + \cdots + \beta_1 t + \beta_0 \ .$$

Så er produktpolynomiet pq definitionsmæssigt givet ved

$$(pq)(t) = p(t)q(t) = \sum_{j=0}^{r} \alpha_j t^j \sum_{k=0}^{s} \beta_k t^k =$$

$$= \sum_{j,k} \alpha_j \beta_k t^{j+k} = \sum_{m=0}^{r+s} \Big(\sum_{j+k=m} \alpha_j \beta_k \Big) t^m \ .$$

Tilsvarende fås, da $f^j \circ f^k = f^{j+k}$,

$$p(f) \circ q(f) = \sum_{j=0}^{r} \alpha_j f^j \circ \sum_{k=0}^{s} \beta_k f^k =$$

$$= \sum_{j,k} \alpha_j \beta_k f^{j+k} = \sum_{m=0}^{r+s} \Big(\sum_{j+k=m} \alpha_j \beta_k \Big) f^m ,$$

hvilket netop er $(pq)(f)$.

Analogt defineres for $\underline{\underline{A}} \in \mathbb{M}_{n,n}(L)$ matricen

$$p(\underline{\underline{A}}) = \alpha_r \underline{\underline{A}}^r + \cdots + \alpha_1 \underline{\underline{A}} + \alpha_0 \underline{\underline{E}} \quad \in \mathbb{M}_{n,n}(L) ,$$

og det ses, at der for to polynomier p og q gælder

$$(pq)(\underline{\underline{A}}) = p(\underline{\underline{A}}) q(\underline{\underline{A}}) .$$

Hvis nu f har matricen $\underline{\underline{A}}$ m.h.t. en valgt basis for (V,L), så har $f^2 = f \circ f$ matricen $\underline{\underline{A}}^2 = \underline{\underline{A}} \cdot \underline{\underline{A}}$ (se side 4.2.5), og almindeligt har f^j matricen $\underline{\underline{A}}^j$. Heraf følger let, at

(**) $p(f)$ har matricen $p(\underline{\underline{A}})$.

Vi kan nu vise *Hamilton-Cayley's sætning:*

Enhver endomorfi f af (V,L) er "rod" i sit karakteristiske polynomium: $p_f(f) = o$ (nul-endomorfien).

Enhver matrix $\underline{\underline{A}} \in \mathbb{M}_{n,n}(L)$ er "rod" i sit karakteristiske polynomium: $p_{\underline{\underline{A}}}(\underline{\underline{A}}) = \underline{\underline{0}}$.

Bevis. Da $p_f = p_{\underline{\underline{A}}}$, og da $p_f(f)$ således ifølge (**) har matricen $p_{\underline{\underline{A}}}(\underline{\underline{A}})$ (når f har matricen $\underline{\underline{A}}$), er de to formuleringer åbenbart ækvivalente. Det er derfor nok at betragte tilfældet

$L = \mathbb{C}$, idet enhver reel matrix $\underline{\underline{A}}$ kan opfattes som en kompleks matrix (naturligvis med samme karakteristiske polynomium).

For nu at vise sætningen for $L = \mathbb{C}$ og i den første formulering, benyttes Suppl. opg. 17 b og de dér anvendte betegnelser. Da $V = U_1 \oplus \cdots \oplus U_r$, er det nok at vise for ethvert $j = 1, \cdots, r$, at $p_f(f)(\underline{u}) = \underline{o}$ for enhver vektor $\underline{u} \in U_j$. Sættes rm $\lambda_j = n_j$, haves

$$p_f(t) = (\lambda_1 - t)^{n_1} \cdots (\lambda_r - t)^{n_r} = q_j(t)\,(t-\lambda_j)^{n_j},$$

hvor q_j er et polynomium. Så er ifølge (*)

$$p_f(f) = q(f) \circ (f - \lambda_j e)^{n_j},$$

og vi mangler derfor kun at vise, at

$$(***) \qquad (f-\lambda_j e)^{n_j}(\underline{u}) = \underline{o}.$$

Ved betragtning af diagonalelementerne i en Jordan-matrix $\underline{\underline{C}}$ for f ses, at blokken $\underline{\underline{C}}_j$ med λ_j i diagonalen har $n_j = \text{rm } \lambda_j$ rækker og søjler, og da de søjler i $\underline{\underline{C}}$, som "går igennem" denne blok, svarer til en basis for U_j, er dim $U_j = n_j$. Nu er restriktionen h_j af $f - \lambda_j e$ til U_j nilpotent; og nærmere gælder $h_j^{n_j} = 0$, og dermed (***). Der gælder nemlig alment $h^n = o$ for en nilpotent endomorfi h af et n-dimensionalt vektorrum U (aflæses let af beviset for a eller c i Suppl. opg. 17). ∎

KAPITEL 10

Basis

I dette kapitel skal vi indføre et vigtigt hjælpemiddel til studiet af vektorrum, og vi skal også se de første anvendelser af dette nye hjælpemiddel, den såkaldte basis for et vektorrum. Vort udgangspunkt er begrebet linearkombination, som blev indført i definition 9.1.

Dengang betragtede vi en mængde A i et vektorrum U over et legeme K, og vi minder om, at en linearkombination af elementer fra A er et udtryk $\lambda_1\underline{u}_1+\ldots+\lambda_n\underline{u}_n$, hvor $n = 0$ eller $n \in \mathbb{N}$ og $\underline{u}_1,\ldots,\underline{u}_n \in A$, $\lambda_1,\ldots,\lambda_n \in K$. Vi er nødt til at tale ret præcist om linearkombinationer i det følgende, og derfor bliver vi nu temmelig pedantiske.

En linearkombination har selvfølgelig en værdi, idet den ganske enkelt er en vektor i U. På den anden side har den et udseende, idet der optræder et antal led, hvert af dem produkt af et element fra K og et element fra A.

Definition 10.1. En linearkombination $\lambda_1\underline{u}_1+\ldots+\lambda_n\underline{u}_n$ kaldes reduceret, hvis $\underline{u}_1,\ldots,\underline{u}_n$ er indbyrdes forskellige. En linearkombination reduceres, ved at led, hvor samme vek-

tor optræder, erstattes med et eneste led, hvis koefficienter bliver summen af vedkommende vektors koefficienter. Ved reduktion af en linearform fremkommer en reduceret linearform. Reducerede linearformer regnes for ens, hvis de indeholder de samme led bortset fra eventuelle led med koefficient 0. Vilkårlige linearformer regnes for ens, hvis reduktion af dem giver ens reducerede linearformer. En linearform kaldes tom, hvis den ved reduktion giver en linearform, der slet ikke har nogen fra 0 forskellig koefficient.

Det er klart, at en linearform ved reduktion giver en ganske bestemt reduceret linearform. Det følger af definitionen af et vektorrum, at en linearforms værdi ikke ændres ved reduktion. En linearform med $n = 0$ er selvfølgelig tom. Vi har ikke noget tegn for den, men vi har jo muligheden for at skrive $0 \cdot \underline{0}$, hvilket jo efter konventionerne ovenfor betyder det samme. Vi kan også skrive $0 \cdot \underline{u}$ med en vilkårlig vektor $\underline{u}$.

Hvis $\underline{u}, \underline{v}$ og $\underline{w}$ er vektorer i A, er $\underline{u}-\underline{u}$ og $2\underline{u}-\underline{v}+3\underline{w}+\underline{v}-\underline{w}-2\underline{u}-2\underline{v}$ tomme linearkombinationer af $\underline{u}, \underline{v}$ og $\underline{w}$. Linearkombinationen $3\underline{u}-2\underline{v}+\underline{w}+\underline{v}-2\underline{u}+\underline{w}-\underline{u}$ reduceres til $2\underline{w}-\underline{v}$.

Sætning 10.2. Lad A være en mængde i et vektorrum U over et legeme K. Da er følgende 4 betingelser indbyrdes

ækvivalente.

1). Enhver vektor i span A har kun 1 fremstilling som linearkombination af vektorer fra A.

2). I span A findes en vektor, der kun har 1 fremstilling som linearkombination af vektorer fra A.

3). Kun den tomme linearkombination af vektorer fra A har værdi $\underline{0}$.

4). Ingen vektor $\underline{u} \in A$ kan skrives som en linearkombination af vektorer fra $A \setminus \{\underline{u}\}$.

Bevis. Vi beviser først, at 1) $\Leftrightarrow$ 2) $\Leftrightarrow$ 3). Det følger umiddelbart af, at en vektor $\underline{u} \in$ span A på 2 måder kan skrives som linearkombination af vektorer fra A, hvis og kun hvis $\underline{0}$ kan skrives som en ikke tom linearkombination, så vi skal blot vise rigtigheden af denne påstand. Hvis L_1 og L_2 er indbyrdes forskellige linearkombinationer af elementer fra A og med værdi $\underline{u}$, er $L_1 - L_2$ en ikke tom linearkombination af vektorer fra A og med værdi $\underline{0}$. Hvis N er en ikke tom linearkombination af elementer fra A og med værdi $\underline{0}$, og $\underline{u} \in$ span A er værdien af en linearkombination L af vektorer fra A, er L+M forskellig fra L og har værdi $\underline{u}$. Dermed er ækvivalensen af de tre første påstande bevist.

Hvis $\underline{u} \in A$ kan skrives som en linearkombination L af

vektorer fra $A \setminus \{\underline{u}\}$, bliver $L - \underline{u}$ en ikke tom (da $\underline{u}$ også efter reduktion har koefficient -1) linearkombination af vektorer fra A og med værdi $\underline{0}$, så 3) er ikke opfyldt. Dermed har vi vist, at 3) $\Rightarrow$ 4). Hvis 3) ikke gælder, findes der en reduceret linearform, der opfylder $\lambda_1\underline{u}_1+\ldots+\lambda_n\underline{u}_n = 0$, $n \in \mathbb{N}$, $\underline{u}_1,\ldots,\underline{u}_n \in A$, $\lambda_1,\ldots,\lambda_n \in K \setminus \{0\}$. Så får vi $\underline{u}_1 = -\lambda_1^{-1}\lambda_2\underline{u}_2-\ldots-\lambda_1^{-1}\lambda_n\underline{u}_n$, så 4) er ikke opfyldt. Dermed har vi vist, at 4) $\Rightarrow$ 3), og dermed er sætningen bevist.

Definition 10.3. Hvis en mængde A i et vektorrum U over et legeme K opfylder de 4) indbyrdes ækvivalente betingelser i sætning 10.2 kaldes A en lineært uafhængig mængde eller en mængde af lineært uafhængige vektorer. Hvis A ikke opfylder de 4 betingelser, kaldes A en lineært afhængig mængde eller en mængde af lineært afhængige vektorer.

For $A = \emptyset$ har vi kun den tomme linearkombination af vektorer fra A, og dens værdi er $\underline{0}$, så $\emptyset$ er lineært uafhængig og span $\emptyset = \{\underline{0}\}$. I det følgende vil vi for det meste snyde for at diskutere det uinteressante specialtilfælde, hvor en mængde er tom.

Hvis $\underline{0} \in A$, er A lineært afhængig, da $1\cdot\underline{0}$ har værdi $\underline{0}$ uden at være tom. Hvis $A = \{\underline{e}\}$ og $\underline{e} \neq \underline{0}$, er A lineært uafhængig, da $\lambda\underline{e} \neq \underline{0}$, hvis $\lambda \neq 0$.

Det er klart, at enhver delmængde af en lineært uafhængig mængde selv er lineært uafhængig. Det er også klart, at

en mængde A er lineært uafhængig, hvis og kun hvis enhver endelig delmængde af A er det.

Mængden af lineært uafhængige mængder i vektorrummet U er (partielt) ordnet ved inklusion. En lineært uafhængig mængde er maksimal, hvis den ikke er ægte delmængde af nogen lineært uafhængig mængde. Vi vil nu vise 2 sætninger om eksistens af maksimale, lineært uafhængige mængder. Den første er ganske enkel og elementær. Den anden er subtil og bygger på Zorn's lemma, som vi omtalte i kapitel 5.

Sætning 10.4. Lad U være et vektorrum over et legeme K. Da gælder enten, at U indeholder en uendelig, lineært uafhængig mængde, eller, at enhver lineært uafhængig mængde $A \subseteq U$ er delmængde af en maksimal, lineært uafhængig mængde $B \subseteq U$.

Bevis. Lad $A \subseteq U$ være en lineært uafhængig mængde. Hvis A er uendelig, indeholder U en uendelig, lineært uafhængig mængde. Hvis A er maksimal er A delmængde af den maksimale, lineært uafhængige mængde A. Hvis A er endleig og ikke maksimal, er A ægte delmængde af en lineært uafhængig mængde A_1, og vi kan så gentage ræsonnementet for A_1. Enten fører denne proces efter endelig mange trin til en endelig, maksimal, lineært uafhængig mængde A_q, eller vi får en uendelig følge $A \subset A_1 \subset A_2 \subset \ldots$ af lineært uafhængige mængder. Lad B være foreningsmængden af

disse mængder. For en endelig delmængde $\tilde{B} = \{\underline{b}_1,\ldots,\underline{b}_s\} \subset A$ gælder nu, at hvert element $\underline{b}_j$ tilhører en af mængderne A_j, og den sidste af disse udvalgte indeholder hele $\tilde{B}$. Så er $\tilde{B}$ delmængde i en lineært uafhængig mængde, og derfor selv lineært uafhængig. Altså er enhver endelig delmængde af B lineært uafhængig. Men så er B lineært uafhængig. Vi har således fundet en uendelig, lineært uafhængig mængde i U, og dermed er sætningen bevist.

Den næste sætning har en enklere formulering.

Sætning 10.5. Lad U være et vektorrum over et legeme K og $A \subseteq U$ en lineært uafhængig mængde. Der findes da en maksimal, lineært uafhængig mængde $B \supseteq A$.

Bevis. Lad M være mængden af lineært uafhængige mængder, som indeholder A. Så er M partielt ordnet ved inklusion. Lad $\{A_j \mid j \in J\}$ være en delmængde af M, som er totalt ordnet ved inklusion. Vi indfører $\tilde{A} = \bigcup_{j\in J} A_j$. Lad $\{\underline{a}_1,\ldots,\underline{a}_s\} \subset \tilde{A}$ være en endelig delmængde af $\tilde{A}$. Så er hvert a_j element i en mængde A_j, $j \in J$, og den af disse, som kommer sidst i den totale ordning, indeholder $\{\underline{a}_1,\ldots,\underline{a}_s\}$. Så er $\{\underline{a}_1,\ldots,\underline{a}_s\}$ delmængde af en lineært uafhængig mængde, altså lineært uafhængig. Men så er enhver endelig delmængde af $\tilde{A}$ og dermed $\tilde{A}$ selv lineært uafhængig. Dermed har vi bevist, at enhver totalt ordnet delmængde af M har en majorant, og så fortæller Zorn's lemma, at M har et maksimalt elemnt. Dermed er sætningen bevist.

Vi skal nu indføre det særlige begreb, der er hovedemnet for dette kapitel.

Definition 10.6. Lad U være et vektorrum over et legeme K. En mængde $B \subseteq M$ kaldes en basis for U, hvis enhver vektor $\underline{u} \in U$ har en og kun en fremstilling som linearkombination af vektorer fra B.

At enhver vektor $\underline{u} \in U$ kan skrives som linearkombination af vektorer fra B er ganske ensbetydende med, at $U = \text{span } B$. At hver vektor fra B kun har en sådan fremstilling er ensbetydende med, at B er lineært uafhængig.

Sætning 10.7. Lad U være et vektorrum over et legeme K. En basis for U er ganske det samme som en maksimal lineært uafhængig mængde af vektorer fra U.

Bevis. Af bemærkningerne før sætningen fremgår, at en basis B er en lineært uafhængig mængde. Da enhver vektor i U kan skrives som linearkombination af elementer fra B, er B en maksimal, lineært uafhængig mængde. Hvis B er en maksimal, lineært uafhængig mængde, er $B \cup \{\underline{u}\}$, hvor $\underline{u} \in U \setminus B$, lineært afhængig, så vi har en ikke tom linearkombination $\lambda_1\underline{u}_1+\ldots+\lambda_n\underline{u}_n + \lambda\underline{u} = \underline{0}$, hvor $\lambda_1 \neq 0,\ldots,\lambda_n \neq 0$, $\underline{u}_1,\ldots,\underline{u}_n \in B$. Her er $\lambda \neq 0$, da linearkombinationen ellers måtte være tom. Vi får så $\underline{u} = -\lambda^{-1}\lambda_1\underline{u}_1-\ldots-\lambda^{-1}\lambda_n\underline{u}_n$, altså $\underline{u} \in \text{span } B$. Dermed er sætningen bevist.

Vi kan nu omformulere sætning 10.5 til udsagn om eksistens af basis for vektorrum.

Sætning 10.8. Ethvert vektorrum har en basis. En lineært uafhængig mængde i et vektorrum kan udvides til en basis for vektorrummet. En basis for et underrum i et vektorrum kan udvides til en basis for hele rummet.

Bevis. Den midterste påstand er blot en omformulering af sætning 10.5. Den første påstand er det specielle tilfælde, hvor den lineært uafhængige mængde er tom. Den sidste påstand følger af, at en basis for et underrum er en lineært uafhængig mængde.

Eksempler. Vektorrummet $\{\underline{0}\}$ har $\emptyset$ som basis, og det er den eneste. Vektorrummet $\mathbb{Z}_2$ over legemet $\mathbb{Z}_2$ har $\{1\}$ som basis, og det er igen den eneste. Eller har vektorrum sædvanligvis mange baser. Et legeme K som vektorrum over K har basis $\{e\}$, hvor $e \in K \setminus \{0\}$ er vilkårligt valgt. Vektorrummet K^n har basis bestående af $\underline{e}_1 = (1,0,\ldots,0), \ldots, \underline{e}_n = (0,\ldots,0,1)$. Vektorrummet af reelle talfølger med kun endelig mange elementer $\neq 0$ har en basis bestående af $(1,0,0,\ldots)$, $(0,1,0,\ldots), \ldots$. Denne basis kan udvides til en basis for vektorrummet af alle reelle talfølger. Det er let nok at finde talfølger at føje til de

allerede valgte, men hvor meget man end slider i det med at udvælge sådanne følger, når man aldrig til virkelig at have den basis, hvis eksistens vi har bevist.

Lad nu U og V være vektorrum over K. Vi vil nu studere vektorrummet $\mathrm{Hom}(U,V)$ af lineære afbildninger $f:U \to V$. Vi har jo altid $\underline{0}$-afbildningen, som afbilder hele U på $\underline{0} \in V$, men i kapitel 9 vidste vi ikke, om der overhovedet fandtes andre afbildninger. Nu er vi i stand til at udtale os mere præcist om vektorrummet af afbildninger.

Lad B være en basis for U. Så har hver lineær afbildning en restriktion $f|B:B \to V$, og da B ikke er et vektorrum, er $f|B$ blot en afbildning, et element af V^B. Det viser sig nu, at den lineære afbildning $f:U \to V$ er helt bestemt ved sin restriktion $f|B$, og det viser sig også, at enhver afbildning $g:B \to V$ er restriktion af en lineær afbildning $f:U \to V$. Dette er emnet for den næste sætning, som dog også indeholder lidt mere information.

<u>Sætning</u> 10.9. Lad U og V være vektorrum over et legeme K, og lad B være en basis for U. Ved $\Gamma(f) = f|B$ defineres da en vektorrumsisomorfi $\Gamma:\mathrm{Hom}(U,V) \to V^B$.

Bevis. For lineære afbildninger $f_1, f_2:U \to V$ og ele-

menter $\lambda_1,\lambda_2 \in K$ er $(\lambda_1 f_1+\lambda_2 f_2)|B = \lambda_1(f_1|B)+\lambda_2(f_2|B)$. Derfor er Γ en homomorfi. Vi mangler at vise, at Γ er bijektiv. Lad $g:B \to V$ være en given afbildning. Hvis g er restriktion af f til B, får vi, idet ethvert element $\underline{u} \in U$ kan skrives som en linearkombination $\underline{u} = \lambda_1\underline{b}_1+\ldots+\lambda_n\underline{b}_n$ af basiselementer, at $f(\underline{u}) = f(\lambda_1\underline{b}_1+\ldots+\lambda_n\underline{b}_n) = \lambda_1 f(\underline{b}_1)+\ldots+\lambda_n f(\underline{b}_n) = \lambda_1 g(\underline{b}_1)+\ldots+\lambda_n g(\underline{b}_n)$. Det viser, at f er bestemt ved g, altså at Γ er injektiv. Desuden ved vi, at f må defineres ved $f(\underline{u}) = \lambda_1 g(\underline{b}\ )+\ldots+\lambda_n g(\underline{b}_n)$. Vi må først vise, at der er mening i denne definition, altså at ens linearkombinationer giver samme funktionsværdi. Nu fås ens linearkombinationer af hinanden ved, at udtryk som $\mu_1\underline{b}+\ldots+\mu_q\underline{b}$ erstattes med $(\mu_1+\ldots+\mu_q)\underline{b}$, og vi ser straks, at det ikke ændrer værdien af $f(\underline{u})$. Altså er f veldefineret. Det ses umiddelbart, at f er lineær. Dermed er sætningen bevist.

Eksempel. Vektorrummet K som vektorrum over K har basis $\{1\}$, og en lineær afbildning $f:K \to K$ er derfor givet ved $f(x) = kx$, hvor $k = f(1)$ er et vilkårligt element af K. I eksemplet efter definition 9.12 er det samme udført for linearformer $f:K^n \to K$. Vektorrummet $\mathbb{R}_0^\infty$ af reelle talfølger med kun endelig mange led $\neq 0$ har basis bestående af $\underline{e}_1 = (1,0,0,\ldots)$, $\underline{e}_2 = (0,1,0,\ldots),\ldots$. For hver reel talfølge

$(y_1, y_2, \ldots)$ findes der én og kun én linearform $f: \mathbb{R}_0^\infty \to \mathbb{R}$ med $f(\underline{e}_n) = y_n$, $n = 1,2,\ldots$. Heraf følger, at det duale rum til $\mathbb{R}_0^\infty$ er isomorft med hele talfølgerummet $\mathbb{R}^\infty$.

Vor næste sætning følger helt umiddelbart af sætning 10.8 og 10.9. Den fungerer som en i visse situationer særdeles nyttig hjælpesætning.

Sætning 10.10. Lad U og V være vektorrum over et legeme K, lad $W \subset U$ være et underrum, og lad $\underline{b} \in U \setminus W$ og $\underline{a} \in V$ være givne vektorer. Enhver lineær afbildning $f: W \to V$ kan da udvides til en lineær afbildning $\tilde{f}: U \to V$, som tilfredsstiller betingelsen $\tilde{f}(\underline{b}) = \underline{a}$.

Bevis. Vi vælger en basis B_0 for W. Så er $B_0 \cup \{\underline{b}\}$ en lineært uafhængig mængde, som ifølge sætning 10.8 kan udvides til en basis B. Vi definerer $g: B \to V$ ved $g(\underline{x}) = f(\underline{x})$, hvis $\underline{x} \in B$, medens vi vælger $g(\underline{b}) = \underline{a}$ og $g(\underline{x}) = \underline{0}$ (eller hvad som helst) på resten af B. Så har g ifølge sætning 10.9 en udvidelse $\tilde{f}: U \to V$, og det fremgår af sætning 10.9 anvendt på W, at $\tilde{f}|W = f$, så $\tilde{f}$ er en udvidelse af f. Vi har $f(\underline{b}) = g(\underline{b}) = \underline{a}$. Dermed er sætningen vist.

Som en anvendelse heraf viser vi nu det supplement til sætning 9.13, som vi stillede i udsigt i bemærkningen lige før definition 9.14.

Sætning 10.11. Den i sætning 9.13 omtalte lineære afbildning $\Phi_U: U \to U^{**}$ er injektiv.

Bevis. Vi skal blot for $\underline{u} \in U$ vise, at den ved $\underline{u}^{**}(\underline{u}^*) = \underline{u}^*(\underline{u})$ definerede afbildning $\underline{u}^{**}: U^* \to K$ ikke er $\underline{0}$-afbildningen, hvis $\underline{u} \neq 0$. Men sætning 10.10 fortæller, at vi for $\underline{u} \neq 0$ kan vælge en linearform $\underline{u}^*: U \to K$ med $\underline{u}^*(\underline{u}) \neq \underline{0}$, og så er $\underline{u}^{**}$ ikke $\underline{0}$-afbildningen. Dermed er sætningen bevist.

Med denne tilføjelse fortæller sætning 9.13, at U^{**} indeholder en kopi af U.

Vi indfører en talemåde, som vil gøre det muligt at formulere nogle af de næste sætninger mere kortfattet.

Definition 10.12. Lad U være et vektorrum over et legeme K. For en mængde $A \subseteq U$ vil vi ved annihilatoren til A i U^* forstå mængden af linearformer $\underline{u}^* \in U^*$ med $u^*(A) = \{0\}$. For en mængde $A^* \subseteq U^*$ vil vi ved annihilatoren til A^* i U forstå mængden af vektorer $\underline{u} \in U$, for hvilke $\underline{u}^*(\underline{u}) = 0$ for alle $\underline{u}^*$ i A^*. Vi skriver $\mathrm{Ann}^* A$ for annihilatoren til A i U^* og $\mathrm{Ann}\, A^*$ for annihilatoren til A^* i U. Analogt skriver vi $\mathrm{Ann}^{**} A^*$ for annihilatoren til A^* i U^{**}.

Sætning 10.13. $\Phi_U^{-1}(\text{Ann}^{**}A^*) = \text{Ann } A^*$.

Bevis. At $\underline{u} \in \text{Ann } A^*$ betyder netop, at $\underline{u}^{**}(\underline{u}^*) = \underline{u}^*(\underline{u}) = 0$ for alle $\underline{u}^* \in A^*$. Dermed er sætningen bevist.

Sætning 10.14. Annihilatorer er underrum.

Bevis. Af $\underline{u}_1^*, \underline{u}_2^* \in \text{Ann}^*(A)$ og $\lambda_1, \lambda_2 \in K$ følger

$$(\lambda_1\underline{u}_1^* + \lambda_2\underline{u}_2^*)(\underline{u}) = \lambda_1\underline{u}_1^*(\underline{u}) + \lambda_2\underline{u}_2^*(\underline{u}) = 0$$

for alle $\underline{u} \in A$, altså $\lambda_1\underline{u}_1^* + \lambda_2\underline{u}_2^* \in \text{Ann}^*(A)$. Dermed har vi vist, at $\text{Ann}^*(A)$ er et underrum i U^*. Anvendt på $A^* \subseteq U^*$ giver dette resultat, at $\text{Ann}^{**}(A^*)$ er et underrum i U^{**}, og derefter følger det af sætning 10.13 og sætning 9.8, at $\text{Ann}(A^*)$ er et underrum i U. Dermed er sætningen bevist.

Et underrum $V \subseteq U$ og et underrum $V^* \subseteq U^*$ kan eventuelt være annihilatorer for hinanden. Den næste sætning fortæller om nogle situationer, hvor dette faktisk indtræffer.

Sætning 10.15. Lad U og V være vektorrum over et legeme K og $f: U \to V$ en lineær afbildning og med den duale afbildning $f^*: V^* \to U^*$. Da er kern $f \subseteq U$ og im $f^* \subseteq U^*$ hinandens annihilatorer og im $f \subseteq V$ og kern $f^* \subseteq V^*$ er ligeledes hinandens annihilatorer.

Bevis. Vi skal ialt vise 4 påstande. Lad os begynde med at vise, at $\text{Ann}^*(\text{im } f) = \text{kern } f^*$. Vi minder om, at $f^*:V^* \to U^*$ er defineret ved, at vi for $\underline{v}^* \in V^*$, altså $\underline{v}^*:V \to K$ har $f^*(\underline{v}^*) = \underline{v}^* f$. At $v^* \in \text{kern } f^*$ betyder derfor, at vi for alle $\underline{u} \in U$ har $v^*(f(\underline{u})) = 0$, altså at $\underline{v}^* \in \text{Ann}^*(\text{im } f)$. Dermed er den første påstand bevist.

Vi viser dernæst, at $\text{Ann}^*(\text{kern } f) = \text{im } f^*$. At $\underline{u}^* \in U^*$, altså $\underline{u}^*:U \to K$ tilhører im f^*, betyder, at der findes en linearform $\underline{v}^* \in V^*$, altså $\underline{v}^*:V \to K$, for hvilken vi har $\underline{u}^* = f^*(\underline{v}^*) = \underline{v}^* f$. Ifølge sætning 9.10 vil dette være opfyldt, hvis og kun hvis kern $\underline{u}^* \supseteq$ kern f, altså hvis og kun hvis $\underline{u}^* \in \text{Ann}^*(\text{kern } f)$. Dermed er den anden påstand bevist.

Vi vil nu vise, at $\text{Ann}(\text{kern } f^*) = \text{im } f$. At $\underline{v} \in V$ tilhører ann(kern f^*) er ifølge sætning 10.13 ensbetydende med, at $\underline{v}^{**} \in \text{Ann}^{**}(\text{kern } f^*)$, og ifølge den anden allerede viste påstand er det ensbetydende med, at $\underline{v}^{**} \in \text{im } f^{**}$. Af sætning 9.16 følger nu, at det er ensbetydende med, at $\underline{v} \in \text{im } f$. Dermed er den tredie påstand bevist.

Vi mangler nu at vise, at $\text{Ann}(\text{im } f^*) = \text{kern } f$. At $f(\underline{u}) = \underline{0}$ er ifølge sætning 9.16 ensbetydende med, at $f^{**}(\underline{u}^{**}) = \underline{0}$, altså med, at $\underline{u}^{**} \in \text{kern } f^{**}$. Ifølge den

første af de viste påstande, er det ensbetydende med, at $\underline{u}^{**} \in \text{Ann}^{**}(\text{im } f^*)$, og det er ifølge sætning 10.13 ensbetydende med, at $\underline{u} \in \text{Ann}(\text{im } f^*)$. Dermed er sætningen bevist.

Læg mærke til, at sætning 10.8 ikke kom i brug ved beviset for de 2 første påstande. Til gengæld kan de 2 sidste påstande ikke bevises uden brug af en af vore dybere sætninger. Vi har foretrukket at bruge sætning 3.16, men der var flere muligheder.

Vi anfører en oplagt følgesætning.

Sætning 10.16. En lineær afbildning er injektiv, hvis og kun hvis dens duale er surjektiv, og den er surjektiv, hvis og kun hvis dens duale er injektiv. En lineær afbildning er en vektorrumsisomorfi, hvis og kun hvis dens duale er det.

Bevis. Det er klart, at $\text{Ann}^*\{\underline{0}\} = U^*$ og $\text{Ann}^*(U) = \{\underline{0}\}$. Af $\text{Ann}^{**}\{\underline{0}\} = U^{**}$ og $\text{Ann}^{**}(U^*) = \{\underline{0}\}$ fås ved sætning 10.13, at $\text{Ann}\{\underline{0}\} = U$ og $\text{Ann}\{U^*\} = \{\underline{0}\}$. Derefter giver sætning 10.15, at $\text{im } f = V \Leftrightarrow \text{kern } f^* = \{\underline{0}\}$, og at $\text{kern } f = \{\underline{0}\} \Leftrightarrow \text{im } f^* = U^*$. Heraf følger sætningen umiddelbart.

Det følger af sætningen, at egenskaberne "injektiv", "surjektiv", "bijektiv" nedarves til den biduale afbildning.

Eksempel. Lad $\mathbb{R}_0^\infty$ være vektorrummet af reelle talfølger med kun endelig mange led $\neq 0$. Så er $(\mathbb{R}_0^\infty)^* = \mathbb{R}^\infty$ i den forstand at en følge $(y_1, y_2, \ldots)$ fra $\mathbb{R}^\infty$ skal repræsentere den ved $\underline{y}^*(\underline{x}) = x_1y_1 + x_2y_2 + \ldots$ definerede linearform $\underline{y}^* : \mathbb{R}_0^\infty \to \mathbb{R}$. Lad nu $f : \mathbb{R}_0^\infty \to \mathbb{R}_0^\infty$ være givet ved $f(x_1x_2, \ldots) = (x_1, x_1, x_3, x_3, x_5, x_5, \ldots)$. Så er kern f mængden af følger i $\mathbb{R}_0^\infty$ med 0 på pladser med ulige nummer, medens im f er mængden af følger i $\mathbb{R}_0^\infty$ med hvert led med ulige nummer lig med det følgende. Vi ser, at $f^*(y_1, y_2, \ldots)$ er den linearform $z^* : \mathbb{R}_0^\infty \to \mathbb{R}$, som er givet ved, at $z^*(x_1, x_2, \ldots) = (x_1y_1 + x\ y_2 + x_3y_3 + x_3y_4 + \ldots$, og det betyder, at $f^*(y_1, y_2, \ldots) = (y_1 + y_2, 0, y_3 + y_4, 0, \ldots)$. Altså er kern f* mængden af følger af formen $(z_1, -z_1, z_2, -z_2, \ldots)$, og det er netop Ann*(im f). Endvidere er im f* mængden af følger med 0 på pladser med lige nummer, og det er netop Ann*(kern f).

Vi går nu over til at anvende vore nye hjælpemidler på begreberne direkte sum og direkte produkt. Vi begynder med endnu lidt jargon.

Definition 10.17. Lad U være et vektorrum over et legeme K, og lad V og W være underrum i U. Hvis $U = V \oplus W$, siger vi, at V og W er indbyrdes komplementære underrum af U.

Det er klart, at "komplementært underrum til" er en symmetrisk relation.

Sætning 10.18. Til ethvert underrum i et vektorrum findes der et (sædvanligvis ikke entydigt bestemt) komplementært underrum.

Bevis. Lad U være et vektorrum over K, og lad $V \subseteq U$ være et underrum. Vi vælger en basis B_1 for V og udvider den til en basis B for U. Vi sætter $B \setminus B_1 = B_2$ og $W = \operatorname{span} B_2$. For hvert $\underline{u} \in U$ har vi en fremstilling

$$\underline{u} = \lambda_1\underline{b}_1+\ldots+\lambda_p\underline{b}_p + \lambda'_1\underline{b}'_1+\ldots+\lambda'_{p'}\underline{b}'_{p'}$$

med $\underline{b}_1,\ldots,\underline{b}_p \in B_1$; $\underline{b}'_1,\ldots,\underline{b}'_{p'} \in B_2$; $\lambda_1,\ldots,\lambda_p, \lambda'_1,\ldots,\lambda'_{p'} \in K$. Her er $\lambda_1\underline{b}_1+\ldots+\lambda_p\underline{b}_p \in V$ og $\lambda'_1\underline{b}'_1+\ldots+\lambda'_{p'}\underline{b}'_{p'} \in W$, så vi har $U = V + W$. For et element $\underline{u} \in V \cap W$ har vi

$$\underline{u} = \mu_1\underline{b}_1+\ldots+\mu_p\underline{b}_p = \mu'_1\underline{b}'_1+\ldots+\mu'_{p'}\underline{b}'_{p'}$$

med $\underline{b}_1,\ldots,\underline{b}_p \in B_1$, $\underline{b}'_1,\ldots,\underline{b}'_{p'} \in B_2$; $\mu_1,\ldots,\mu_p$; $\mu'_1,\ldots,\mu'_{p'} \in B_2$, men det medfører, at $\mu_1 = \ldots = \mu_p = \mu'_1 = \ldots = \mu'_{p'} = 0$, så vi har $V \cap W = \{\underline{0}\}$, altså $U = V \oplus W$. Dermed er sætningen vist.

Det komplementære underrum er en kopi af faktorrummet. Den næste sætning, som iøvrigt er elementær, sætter dette i forbindelse med tilvante geometriske forestillinger.

Sætning 10.19. Lad U være et vektorrum over et legeme K. Lad V og W være delrum af U, og $U = V \oplus W$. Lad $p:U \to W$ være den ved $p(\underline{v}+\underline{w}) = \underline{w}$ definerede projektion, idet $\underline{v} \in V$, $\underline{w} \in W$. Lad $k:U \to \frac{U}{V}$ være den kanoniske afbildning, og lad $\chi:W \to \frac{U}{V}$ være den ved $\chi(\underline{w}) = \underline{w}+V$ definerede lineære afbildning. Da er χ en vektorrumsisomorfi, og $k = \chi\, p$.

Bevis. Det er klart, at χ er lineær. Lad $\underline{u}+V \in \frac{U}{V}$ være et vilkårligt siderum. Da der findes én og kun én opspaltning $\underline{u} = \underline{v}+\underline{w}$ med $\underline{v} \in V$, $\underline{w} \in W$, tilhører $\underline{u}$ et og kun et siderum $\underline{w} + V = p(\underline{u}) + V$. Heraf følger begge påstande, og dermed er sætningen bevist.

Eksempel. Lad os se på $\mathbb{E}^3$ som mængde af stedvektorer til punkter i E^3 svarende til et fast valgt begyndelsespunkt O. Lad $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$ være en basis. Så er vektorerne i $V = \text{span}\{\underline{e}_1, \underline{e}_2\}$ mængden af stedvektorer til punkterne i en plan P gennem O, og $W = \text{span}\{\underline{e}_3\}$ mængden af stedvektorer til punkterne i en ret linie L gennem O. Vi har $\mathbb{E}^3 = V \oplus W$,

og projektionen $p:\mathbb{E}^3 \to W$ svarer til den sædvanlige projektion på L. Et siderum $\underline{w}+V$ bliver mængden af stedvektorer til punkterne i en plan parallel med p, og ved χ^{-1} svarer den til $\underline{w}$, som er stedvektor for skæringspunktet med L. Overgangen fra $\frac{\mathbb{R}^3}{V}$ til W kommer altså blot ud på at fastlægge planerne parallelle med P ved deres skæringspunkt med L.

Hvis vi regner isomorfe vektorrum ens, findes der slet ikke særlig mange forskellige vektorrum. Den næste sætning siger, at der højst er 1 isomorfiklasse af vektorrum for hvert kardinaltal, altså at 2 vektorrum er isomorfe, hvis de har baser med samme kardinaltal. Det kræver andre hjælpemidler at vise, at vektorrum ikke kan være isomorfe, hvis de har baser med forskellige kardinaltal, men det spørgsmål vil vi udskyde til næste kapitel, og ivørigt vil vi ikke gennemføre det for uendelige kardinaltal.

Sætning 10.20. Et vektorrum over et legeme K og med basis B er isomorft med $\bigoplus_{j\in B} K$. To vektorrum er isomorfe, hvis og kun hvis de har baser med samme kardinaltal.

Bevis. Et vektorrum U over K med basis B er mængden af alle linearkombinationer $\lambda_1\underline{b} +\ldots+\lambda_n\underline{b}_n$ med $n = 0$ eller $n \in \mathbb{N}$ og $\underline{b}_1,\ldots,\underline{b}_n \in B$ og $\lambda_1,\ldots,\lambda_n \in K$. Nu er

$\bigoplus_{j\in B} K$ defineret som mængden af alle familier $(\lambda_{\underline{b}} | \underline{b}=B)$ med $\lambda_{\underline{b}} \neq 0$ for højst endelig mange $\underline{b} \in B$. En vektorrumsisomorfi $\varphi_{(U,B)} : \bigoplus_{j\in B} K \to U$ defineres ved $\varphi_{(U,B)}(\lambda_{\underline{b}} | \underline{b} \in B) = \sum_{\underline{b}\in B} \lambda_{\underline{b}}\underline{b}$, hvilket giver mening, da summen højst har endelig mange led $\neq 0$. Det er helt indlysende, at afbildningen er bijektiv og en homomorfi.

Hvis U_1 og U_2 er vektorrum over K, og B_1 er basis for U_1 og B_2 for U_2, og B_1 og B_2 har samme kardinaltal, findes der en bijektiv afbildning $\beta:B_1 \to B_2$, og af sætning 10.9 følger, at β har en udvidelse $\overline{\beta}:U_1 \to U_2$. Da $\beta^{-1}:B_2 \to B_1$ ifølge samme sætning har en udvidelse $\gamma:U_2 \to U_1$ og $\gamma\,\overline{\beta}$ og $\overline{\beta}\,\gamma$ bliver udvidelser af $id(B_1)$ og $id(B_2)$, altså $\gamma\,\overline{\beta} = id(U_1)$ og $\overline{\beta}\,\gamma = id(U_2)$, bliver $\overline{\beta}$ en vektorrumsisomorfi.

Hvis U_1 og U_2 er vektorrum over K og $\varphi:U_1 \to U_2$ en vektorrumsisomorfi og B en basis for U_1, bliver $\varphi(B)$ en basis for U_2 med samme kardinaltal som B. Dermed er sætningen bevist.

Hvad vi mangler at vise er, at forskellige baser for samme rum nødvendigvis må have samme kardinaltal, men det er ikke helt simpelt.

Eksempel. Resultaterne i dette kapitel bygger på sætning 10.8, som afledtes af sætning 10.5 som bevistes ved

hjælp af Zorn's lemma. Vi har således ikke givet et konstruktivt bevis for eksistensen af en basis, og i mere komplicerede tilfælde er vi slet ikke i stand til at angive basis for et vektorrum på en bare nogenlunde eksplicit form. Vi skal nu angive et eksempel, hvor konsekvenserne af eksistensen af en basis er ret overraskende.

Vi betragter $\mathbb{R}$ som vektorrum over $\mathbb{Q}$, og vi vil specielt se på lineære afbildninger $\varphi:\mathbb{R}\to\mathbb{R}$ og linearformer $\gamma:\mathbb{R}\to\mathbb{Q}$. At $\varphi:\mathbb{R}\to\mathbb{R}$ er en linearform betyder, at vi for vilkårlige reelle tal x,y og vilkårlige rationale tal λ,μ skal have relationen $\varphi(\lambda x+\mu y) = \lambda\varphi(x)+\mu\varphi(y)$. Med $\varphi(1) = a$ og $\lambda \in \mathbb{Q}$ får vi specielt $\varphi(\lambda) = a\lambda$. Hvis φ skal opfylde dette og være kontinuert, får vi specielt $\varphi(x) = ax$. På den anden side er det klart, at dette definerer en lineær afbildning. Dermed har vi vist, at der blandt de $\mathbb{Q}$-lineære afbildninger $\varphi:\mathbb{R}\to\mathbb{R}$ ikke findes andre kontinuerte end de for $a \in \mathbb{R}$ ved $\varphi(x) = ax$ definerede. Specielt bliver 0-afbildning den eneste kontinuerte $\mathbb{Q}$-linearform.

Da $\mathbb{R}$ som vektorrum over $\mathbb{Q}$ har en basis, findes der masser af diskontinuerte $\mathbb{Q}$-lineære afbildninger $\varphi:\mathbb{R}\to\mathbb{R}$. For en sådan gælder, at vi kan finde $\alpha,\beta \in \mathbb{R}$ og $\lambda,\mu \in \mathbb{Q}$, således at

$$\varphi(\alpha) = \lambda\alpha\ , \quad \varphi(\beta) = \mu\beta\ , \quad \lambda \neq \mu, \quad \alpha \neq 0, \quad \beta \neq 0\ .$$

Lad nu p og q være givne reelle tal. Det er da let at vælge $x_0 y_0 \in \mathbb{R}$, således at vi har relationerne $x_0+y_0 = p$ og $x_0+ y_0 = q$. De to lineære ligninger med x_0 og y_0 som ubekendte har nemlig determinant $\mu-\lambda \neq 0$.

Nu kan vi vælge følger (t_n) og (u_n) af rationale tal, således at $(\alpha t_n) \to x_0$ og $(\beta u_n) \to y_0$. Vi har da $(\alpha t_n+\beta u_n) \to p$ og $\varphi(\alpha t_n+\beta u_n) = t_n\varphi(\alpha)+u_n\varphi(\beta) = \lambda\alpha t_n+\mu\beta u_n$, så vi ser, at $(\varphi(\alpha t_n+\beta u_n)) \to q$. Dermed har vi vist, at φ vilkårlig tæt ved værdien p antager værdier vilkårligt tæt ved værdien q, og det gælder for hvilke som helst reelle tal p og q.

Hvis vi ville tegne det grafiske billede af φ, ville vi således løbe ind i alvorlige vanskeligheder, idet vi har vist, at der i en vilkårlig omegn af et vilkårligt punkt i planen findes punkter af det grafiske billede af φ. I virkeligheden er det grafiske billede af φ ret jævnt fordelt i hele planen, og fra et anskueligt synspunkt er det jo slet ikke til at leve med.

Eksempler som dette har bidraget til at skærpe matematikeres skeptiske holdning til mængdelæren. Det har imidlertid vist sig, at regning med funktioner som de her omtalte fører til fornuftige og i hvert fald fra matematisk synspunkt nyttige resultater.

KAPITEL 11

Vektorrum

Definition 11.1. Hvis K er et legeme, kaldes en unitær K-modul U et vektorrum over K.

Man betragter også vektorrum over ikke kommutative legemer, men det vil vi ikke komme ind på.

Mængden $\mathbb{E}^\nu$ af vektorer i E^ν er for $\nu = 2,3$ et vektorrum over $\mathbb{R}$, og det er netop dette eksempel, vi generaliserer med de abstrakte vektorrum. Ringene $\mathbb{C}$ og $\mathbb{K}$ er vektorrum over $\mathbb{R}$. Et legeme K er vektorrum over sig selv. Et legeme K er også et vektorrum over ethvert dellegeme $L \subseteq K$. Hvis M er en mængde og K et legeme, er mængden K^M af afbildninger $\varphi: M \to K$ et vektorrum over K med den sædvanlige addition og multiplikation med konstant.

Vi skriver K^n for $K^{\{1,\ldots,n\}}$. Et element af K^n er et sæt (en familie) $(x_1,\ldots,x_n)$ af elementer fra K. For $\underline{x} = (x_1,\ldots,x_n)$, $\underline{y} = (y_1,\ldots,y_n)$ og $\lambda \in K$ er

$$\underline{x} + \underline{y} = (x_1+y_1,\ldots,x_n+y_n),\ \lambda\underline{x} = (\lambda x_1,\ldots,\lambda x_n).$$

Definition 11.2. Lad U være et vektorrum over K. Lad $\underline{x}_1,\ldots,\underline{x}_n$ være elementer af U og lad $\lambda_1,\ldots,\lambda_n$ være elementer af K. Elementet $\underline{x} = \lambda_1\underline{x}_1+\ldots+\lambda_n\underline{x}_n$ kaldes en linearkombination af $\underline{x}_1,\ldots,\underline{x}_n$ med koefficienter $\lambda_1,\ldots,\lambda_n$. Hvis $M \subseteq U$ er en vilkårlig mængde og $\underline{x}_1,\ldots,\underline{x}_n \in M$, kaldes $\underline{x}$ en linearkombination af elementer i M.

Definition 11.3. En delmodul af et vektorrum U over et legeme K kaldes et underrum af U.

En fællesmængde af underrum er et underrum. En vilkårlig mængde $M \subseteq U$ frembringer et underrum V, som er fællesmængde for de underrum der indeholder M. Vi kalder V det af M udspændte underrum eller spandet af M, og vi skriver $V = \text{span}M$.

Sætning 11.4. Lad U være et vektorrum over et legeme K, og $M \subseteq U$ en vilkårlig delmængde. Så er spanM netop mængden af linearkombinationer af elementer i M.

Bevis. Det er klart, at mængden af linearkombinationer af elementer i M er et underrum, som indeholder M, og som er indeholdt i ethvert underrum, der indeholder M.

Lemma 11.5. Lad U være et vektorrum over et legeme K, og lad A og B være delmængder af U. Relationen "ethvert element i B er linearkombination af vektorer i A" er ækvivalent med "$\text{span}B \subseteq \text{span}A$" og er derfor en transitiv relation på mængden af delmængder af U (en præordning).

Bevis. Relationen er ensbetydende med, at $B \subseteq \text{span}\, A$, og da $\text{span}B$ er det mindste underrum, der indeholder B, er denne relation ækvivalent med den tilsyneladende stærkere relation $\text{span}B \subseteq \text{span}A$.

Vektorrum er jo en speciel slags moduler, og vi har omtalt dem i de vendinger, der bruges i modulteori. Fra nu af vil et element i et vektorrum også blive kaldt en vektor. Vi vil systematisk anvende understregede bogstaver som betegnelse for vektorer, og 0-elementet i et vektorrum vil blive betegnet $\underline{0}$ og det kaldes $\underline{0}$-vektor.

Definition 11.6. Lad U og V være vektorrum over et legeme K. En K-homomorfi $\varphi: U \to V$ kaldes en K-lineær afbildning.

Når der ikke kan være tvivl om, hvad K er, siger vi lineær i stedet for K-lineær. En K-isomorfi kaldes således også en bijektiv K-lineær afbildning. En K-lineær afbildning $\psi: U \to U$ kaldes som sædvanlig en endomorfi, og den kaldes en automorfi, hvis den er bijektiv.

For hvert legeme K har vi en kategori af vektorrum over K og K-lineære afbildninger.

Sætning 11.7. Lad U og V være vektorrum over et legeme K, og $\varphi: U \to V$ en K-lineær afbildning. Lad $U_1 \subseteq U$ og $V_1 \subseteq V$ være underrum. Da er $\varphi(U_1)$ et underrum i V, og $\varphi^{-1}(V_1)$ er et underrum i U. Specielt er billedet $\operatorname{im}\varphi = \varphi(U)$ et underrum i V, og kernen $\operatorname{kern}\varphi = \varphi^{-1}(\underline{0})$ er et underrum i U.

Bevis. Det er bare et specialtilfælde af det tilsvarende resultat for moduler.

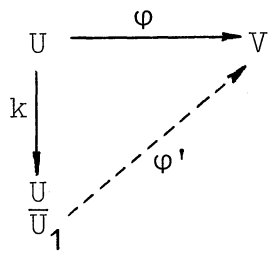
Definition 11.8. Lad U være et vektorrum over et legeme K og $V \subseteq U$ et underrum. Faktormodulen $\frac{U}{V}$ kaldes da faktorrummet.

Vi har selvfølgelig også den kanoniske afbildning $k: U \to \frac{U}{V}$. Faktorrummet $\frac{U}{V}$ består af alle sideklasser $\underline{u} + V = \{\underline{u}+\underline{v} \mid \underline{v} \in V\}$ for hvert $\underline{u} \in U$. Vektorerne $\underline{u}_1, \underline{u}_2 \in U$ hører til samme sideklasse, hvis og kun hvis $\underline{u}_2 - \underline{u}_1 \in V$.

Sætning 11.9. Lad U og V være vektorrum over et legeme K, lad $U_1 \subseteq U$ være et underrum og $\varphi: U \to V$ en lineær afbildning. Lad $k: U \to \frac{U}{U_1}$ være den kanoniske afbildning. Nødvendigt og tilstrækkeligt for, at der findes en

lineær afbildning $\varphi' : \frac{U}{U_1} \to V$, således at $\varphi = \varphi' \circ k$, er det, at $U_1 \subseteq$ kern φ, og φ' er så entydigt bestemt.

Bevis. For $\underline{x} \in \frac{U}{U_1}$ har vi originalvektorer $\underline{u}_1, \underline{u}_2 \in U$ med $k(\underline{u}_1) = k(\underline{u}_2) = \underline{x}$, altså $k(\underline{u}_2 - \underline{u}_1) = 0$, så vi har $\underline{u}_2 - \underline{u}_1 \in U_1 \subseteq$ kern φ, så vi kan definere $\varphi'(\underline{x}) = \varphi(\underline{u}_1)$.



Dette er tvunget, og deraf følger éntydigheden. Det er en meningsfyldt definition, idet $\varphi(\underline{u}_1) = \varphi(\underline{u}_2)$, så φ har samme værdi på alle originalelementer til $\underline{x}$. Vi skal for $\underline{x}, \underline{y} \in \frac{U}{U_1}$ vise, at $\varphi'(\underline{x}+\underline{y}) = \varphi'(\underline{x}) + \varphi'(\underline{y})$. Lad $\underline{u}, \underline{v} \in U$ være valgt, så $k(\underline{u}) = \underline{x}$, $k(\underline{v}) = \underline{y}$, så er $k(\underline{u}+\underline{v}) = \underline{x}+\underline{y}$, og vi får

$$\varphi'(\underline{x}+\underline{y}) = \varphi(\underline{u}+\underline{v}) = \varphi(\underline{u}) + \varphi(\underline{v}) = \varphi'(\underline{x}) + \varphi'(\underline{y}).$$

Det går nemmere at vise, at $\varphi'(\lambda\underline{x}) = \lambda\varphi'(\underline{x})$ for $\lambda \in K$. Dermed er sætningen bevist.

Vi siger, at $\varphi : U \to V$ inducerer $\varphi' : \frac{U}{U_1} \to V$.

Sætning 11.10. Lad U og V være vektorrum over et legeme K, og lad $\varphi : U \to V$ være en lineær afbildning. Da inducerer φ en bijektiv lineær afbildning $\varphi' : \frac{U}{\text{kern}\varphi} \to \varphi(U)$,

og idet $k:U \to \frac{U}{\text{kern}\varphi}$ er den kanoniske afbildning, og $j:\varphi(U) \to V$ er inklusionsafbildningen, er φ identisk med den sammensatte afbildning

$$U \xrightarrow{k} \frac{U}{\text{kern}\varphi} \xrightarrow{\varphi'} \varphi(U) \xrightarrow{j} V$$

Bevis. Det fremgår af den foregående sætning, at φ inducerer $\varphi'':\frac{U}{\text{kern}\varphi} \to V$, og da kern $\varphi'' = \underline{0} \in \frac{U}{\text{kern}\varphi}$, er φ'' injektiv, og således en bijektiv lineær afbildning på $\varphi(U) \subseteq V$. Dermed er sætningen bevist.

Det er klart, at den inverse afbildning til en bijektiv lineær afbildning $\varphi:U \to V$ er lineær. Hvis $\underline{v}_1, \underline{v}_2 \in V$ er billeder af $\underline{u}_1, \underline{u}_2 \in U$, vil $\varphi(\underline{u}_1+\underline{u}_2) = \underline{v}_1 + \underline{v}_2$, altså $\varphi^{-1}(\underline{v}_1+\underline{v}_2) = \underline{u}_1 + \underline{u}_2 = \varphi^{-1}(\underline{v}_1) + \varphi^{-1}(\underline{v}_2)$. At $\varphi^{-1}(\lambda\underline{v}) = \lambda\varphi^{-1}(\underline{v})$ vises endnu lettere.

Det er let nok at give eksempler på lineære afbildninger. Hvis K er et legeme, og $(a_{ij} | i = 1,\ldots,m,\ j = 1,\ldots n)$ et sæt af mn elementer af K, kan vi definere en lineær afbildning $\varphi:K^n \to K^m$ ved $\varphi(x_1,\ldots,x_n) = (a_{11}x_1+\ldots+a_{1n}x_n,\ldots, a_{m1}x_1+\ldots+a_{mn}x_n)$.

Det går helt elementært at eftervise, at afbildningen er lineær. Det vil vise sig, at enhver lineær afbildning af K^n ind i K^m har denne form. Som et mindre oplagt eksem-

kan vi nævne, at vektorrummet $C^1[a,b]$ af funktioner $f:[a,b] \to \mathbb{R}$ med kontinuert differentialkvotient afbildes lineært på rummet $C[a,b]$ af kontinuerte funktioner $g:[a,b] \to \mathbb{R}$ ved at hver funktion afbildes på sin differentialkvotient. Mere generelt kunne vi lade billedet af f være $af'+bf$, hvor a og b er vilkårlige kontinuerte funktioner. Hvis R betegner rektanglet $[a,b]\times[c,d]$, og $A:R \to \mathbb{R}$ er en kontinuert funktion, da kan vi for hver kontinuert funktion $f:[c,d] \to \mathbb{R}$ definere

$$g(x) = \int_c^d A(x,y)f(y)dy.$$

Det vides fra skolen, at integralet eksisterer for hvert $x \in [a,b]$, og det definerer derfor en funktion $g:[a,b] \to \mathbb{R}$. Det sorterer under analysekurset at vise, at g bliver kontinuert. Med $F(f) = g$ får vi defineret en afbildning $F:C[c,d] \to C[a,b]$, og det følger helt elementært af regnereglerne for integration, at den bliver lineær.

Lad U og V være vektorrum over et legeme K. Mængden $\mathrm{Hom}(U,V)$ af lineære afbildninger $f:U \to V$ er da et vektorrum over K ved de sædvanlige definitioner

$$(f+g)(\underline{u}) = f(\underline{u}) + g(\underline{u}), \quad (\lambda f)(\underline{u}) = \lambda f(\underline{u}).$$

Dertil kommer, at $\mathrm{End}U = \mathrm{Hom}(U,U)$ er en algebra over K med sammensætningen $g \circ f$ som kompositionsregel. Det er klart, at $g \circ f$ er distributiv med hensyn til $+$, og associativ, samt at vi har reglen $g \circ \lambda f = \lambda g \circ f = \lambda(g \circ f)$. Mængden $\mathrm{Aut}U$ af automorfier $\varphi: U \to U$ er en gruppe med sammensætning som komposition. For $\lambda \in K$ er den ved $\varphi(\underline{u}) = \lambda \underline{u}$ definerede afbildning en automorfi, hvis $\lambda \neq 0$, men en afbildning af hele U i $\underline{0}$, hvis $\lambda = 0$. Heraf fremgår, at $\mathrm{Aut}U$ ikke er et underrum i $\mathrm{End}U$. De ved $\varphi(\underline{u}) = \lambda \underline{u}$ definerede automorfier $\varphi: U \to U$ kaldes ligedannetheder.

Idet vi husker, at legemet K selv er et vektorrum over K, definerer vi nogle vigtige begreber.

Definition 11.11. Lad U være et vektorrum over et legeme K. En lineær afbildning $\varphi: U \to K$ kaldes en linearform. Vektorrummet $U^* = \mathrm{Hom}(U,K)$ af linearformer på U kaldes det til U duale vektorrum. Det til U^* duale vektorrum $U^{**} = \mathrm{Hom}(U^*,K)$ kaldes det til U biduale vektorrum.

En linearform $\varphi: K \to K$ tilfredsstiller betingelsen $\varphi(x) = \varphi(x \cdot 1) = x\varphi(1)$, så φ er en afbildning af formen $\varphi(x) = ax$ for et $a \in K$. Omvendt er enhver sådan afbildning lineær. For $a \in K$ definerer vi $a^* \in K^*$ ved

$a^*(x) = ax$. Ved $\psi(a) = a^*$ får vi defineret en vektorrumsisomorfi $\psi: K \to K^*$. Vi kan således identificere vektorrummet K med dets duale rum.

Lad igen $C[a,b]$ være mængden af kontinuerte funktioner $f:[a,b] \to \mathbb{R}$. For hvert $x \in [a,b]$ har vi en linearform $\varphi_1: C[a,b] \to \mathbb{R}$ defineret ved $\varphi_1(f) = f(x)$. En anden linearform $\varphi_2: C[a,b] \to \mathbb{R}$ er defineret ved $\varphi_2(f) = \int_a^b f(x)dx$. En tredie linearform defineres ved $\varphi_2(f) = \int_a^b (x^3 - e^x) f(x)dx$.

Vi har et vektorrum over $\mathbb{R}$ bestående af reelle talfølger $\underline{x} = (x_1, x_2, \ldots)$ med de nærliggende kompositionsregler

$$\underline{x} + \underline{y} = (x_1+y_1, x_2+y_2, \ldots) \qquad \lambda\underline{x} = (\lambda x_1, \lambda x_2, \ldots).$$

Lad U være dette vektorrum. For hvert naturligt tal n har vi linearform $\varphi: U \to \mathbb{R}$ givet ved $\varphi(\underline{x}) = x_n$. For delrummet U_k af konvergente talfølger har vi en linearform, der afbilder hver følge på dens grænseværdi. Der er også et delrum U_r af følger $\underline{x}$, for hvilke rækken $x_1+x_2+\ldots$ er konvergent, og på dette rum har vi en linearform, der afbilder hver følge på summen af rækken.

Sætning 11.12. Lad U være et vektorrum over et legeme K, lad U^* være det duale og U^{**} det biduale vektorrum til U. Der findes en naturlig lineær afbildning

$\Phi: U \to U^{**}$, hvor vi for $\underline{u} \in U$ definerer $\Phi(\underline{u}) = \underline{u}^{**}$ ved at vi for et $\varphi \in U^*$, altså en lineær afbildning $\varphi: U \to K$ sætter $\underline{u}^{**}(\varphi) = \varphi(\underline{u})$.

Bevis. Vi har $\underline{u}^{**}(\varphi_1+\varphi_2) = (\varphi_1+\varphi_2)(\underline{u}) = \varphi_1(\underline{u}) + \varphi_2(\underline{u}) = \underline{u}^{**}(\varphi_1) + \underline{u}^{**}(\varphi_2)$ og $\underline{u}^{**}(\lambda\varphi) = (\lambda\varphi)(\underline{u}) = \lambda\varphi(\underline{u}) = \lambda\underline{u}^{**}(\varphi)$, så $\underline{u}^{**}: U^* \to K$ er lineær, altså $\underline{u}^{**} \in U^{**}$. Endvidere er $(\underline{u}_1+\underline{u}_2)^{**}(\varphi) = \varphi(\underline{u}_1+\underline{u}_2) = \varphi(\underline{u}_1)+\varphi(\underline{u}_2) = \underline{u}_1^{**}(\varphi) + \underline{u}_2^{**}(\varphi)$, så vi har $\Phi(\underline{u}_1+\underline{u}_2) = (\underline{u}_1+\underline{u}_2)^{**} = \underline{u}_1^{**} + \underline{u}_2^{**} = \Phi(\underline{u}_1) + \Phi(\underline{u}_2)$. Endelig har vi $\Phi(\lambda\underline{u}) = (\lambda\underline{u})^{**} = \lambda\underline{u}^{**} = \lambda\Phi(\underline{u})$, idet $(\lambda\underline{u})^{**}(\varphi) = \varphi(\lambda\underline{u}) = \lambda\varphi(\underline{u}) = \lambda\underline{u}^{**}(\varphi)$. Dermed er sætningen bevist.

Definition 11.13. Lad U og V være vektorrum over et legeme K, og lad U^* og V^* være de duale rum. For en lineær afbildning $f: U \to V$ definerer vi den duale afbildning $f^*: V^* \to U^*$, idet vi for $\varphi \in V^*$, altså $\varphi: V \to K$ definerer $f^*(\varphi) = \varphi \circ f: U \to K$.

Det er klart, at $f^*: V^* \to U^*$ er lineær.

Sætning 11.14. Lad U,V og W være vektorrum over et legeme K, og lad $f: U \to V$ og $g: V \to W$ være lineære afbildninger. For de duale afbildninger $f^*: V^* \to U^*$, $g^*: W^* \to V^*$ og $(g\circ f)^*: W^* \to U^*$ gælder da $(g\circ f)^* = f^* \circ g^*$.

Bevis. $(g\circ f)^*(\varphi) = \varphi\circ g\circ f = f^*(\varphi\circ g) = f^*(g^*(\varphi))$.

Sætning 11.15. Lad U og V være vektorrum over et legeme K. Så definerer $\Delta(f) = f^*$ en lineær afbildning $\Delta:\mathrm{Hom}(U,V) \to \mathrm{Hom}(V^*,U^*)$.

Bevis. For $\varphi \in V^*$, altså $\varphi:V \to K$ får vi

$$\Delta(f+g)(\varphi) = \varphi\circ(f+g) = \varphi\circ f+\varphi\circ g = \Delta(f)(\varphi) + \Delta(g)(\varphi) =$$

$$(\Delta(f) + \Delta(g))(\varphi).$$

Endvidere får vi

$$\Delta(\lambda f)(\varphi) = \varphi\circ\lambda f = \lambda(\varphi\circ f) = \lambda\Delta(f)(\varphi).$$

Dermed er sætningen bevist.

For vektorrum U og V over et legeme K er den direkte sum $U \oplus V$ igen et vektorrum over K.

Hvis U er et vektorrum over et legeme K, og V og W er underrum i U er $V+W$ et underrum i U. Vi siger, at $V+W$ er direkte sum af V og W såfremt den ved $\varphi(\underline{v},\underline{w}) = \underline{v}+\underline{w}$ definerede lineære afbildning $\varphi:V\oplus W \to V+W$ er en isomorfi, og i så fald tillader vi os at skrive $V \oplus W$ for $V + W$.

Sætning 11.16. Lad U være et vektorrum over et

legeme K, og lad $V \subseteq U$ og $W \subseteq U$ være underrum i U. Følgende 3 egenskaber er da indbyrdes ækvivalente:

1). V + W er direkte sum af V og W.

2). Et element $\underline{u} \in V + W$ kan på højst én måde skrives som $\underline{v} + \underline{w}$, hvor $\underline{v} \in V$ og $\underline{w} \in W$.

3). $V \cap W = \{\underline{0}\}$.

Bevis. Vi bemærker, at betingelsen 2) blot er et udtryk for, at den ved $\varphi(\underline{v},\underline{w}) = \underline{v} + \underline{w}$ definerede afbildning $\varphi: V \oplus W \to V + W$ er injektiv. Da φ ifølge definitionen af V + W er surjektiv, kan vi slutte, at 1) $\Leftrightarrow$ 2). Af $\underline{u} = \underline{v} + \underline{w} = \underline{v}' + \underline{w}'$ følger $\underline{v}-\underline{v}' = \underline{w}'-\underline{w}$, så $\underline{v}-\underline{v}'$ bliver fælles for V og W. Hvis 3) gælder, kan vi slutte, at $\underline{v}-\underline{v}' = \underline{w}'-\underline{w} = 0$, altså at 2) gælder. Af $\underline{z} \in V \cap W$ følger $\underline{0} = \underline{0}+\underline{0} = \underline{z} + (-\underline{z})$, hvor $\underline{0},\underline{z} \in V$ og $\underline{0},-\underline{z} \in W$. Hvis 2) gælder, kan vi slutte, at $\underline{z} = 0$, altså at 3) gælder. Dermed er sætningen bevist.

Sætning 11.17. Lad U og V være vektorrum over et legeme K. For $\underline{u}^* \in U^*$ og $\underline{v}^* \in V^*$ definerer vi $\Phi(\underline{u}^*,\underline{v}^*): U \times V \to K$ ved $\Phi(\underline{u}^*,\underline{v}^*)(\underline{x},\underline{y}) = \underline{u}^*(\underline{x}) + \underline{v}^*(y)$. Derved defineres en isomorfi $\Phi: U^* \oplus V^* \to (U \oplus V)^*$.

Bevis. Det er klart, at $\Phi(\underline{u}^*,\underline{v}^*)$ bliver en linearform på $U \oplus V$, og at Φ bliver lineær. Vi skal vise, at Φ er bijektiv, altså en isomorfi.

Af $\underline{u}^* \neq \underline{0}$ følger, at vi kan finde $\underline{x} \in U$, så $\underline{u}^*(\underline{x}) \neq 0$, og så er $(\underline{u}^*,\underline{v}^*)(\underline{x},\underline{0}) = \underline{u}^*(\underline{x}) \neq 0$. Analogt for $\underline{v}^* \neq \underline{0}$. Altså er $\ker\Phi = \{\underline{0}\}$, og vi kan slutte, at Φ er injektiv. For $\underline{w}^* \in (U \oplus V)^*$ definerer vi $\underline{u}^*(\underline{x}) = \underline{w}^*(\underline{x},0)$ og $\underline{v}^*(\underline{y}) = \underline{w}^*(0,\underline{y})$, og derved får vi $\underline{u}^* \in U^*$ og $\underline{v}^* \in V^*$ med $\Phi(\underline{u}^*,\underline{v}^*) = \underline{w}^*$. Altså er Φ surjektiv, og dermed er sætningen bevist.

Vi kan i praksis lade $U^* \oplus V^*$ spille rollen som dualrum til $U \oplus V$, idet $(\underline{u}^*,\underline{v}^*) \in U^* \oplus V^*$ defineres som linearform på $U+V$ ved $(\underline{u}^*,\underline{v}^*)(\underline{x},\underline{y}) = \underline{u}^*(\underline{x}) + \underline{v}^*(\underline{y})$.

Lad U,V,U_1,V_1 være vektorrum over K, og lad $f:U \to U_1$ og $g:V \to V_1$ være lineære afbildninger. Vi har da en lineær afbildning $f \oplus g: U \oplus V \to U_1 \oplus V_1$ defineret ved $(f \oplus g)(\underline{x},\underline{y}) = (f(\underline{x}),g(\underline{y}))$. Lad $\underline{u}_1^* \in U_1^*$ og $\underline{v}_1^* \in V_1^*$ være linearformer. Vi har da

$$(f \oplus g)^*(\underline{u}_1^*,\underline{v}_1^*) = (\underline{u}_1^*,\underline{v}_1^*) \circ (f \oplus g) = (\underline{u}_1^* \circ f, \underline{v}_1^* \circ g) = (f^*(\underline{u}_1^*), g^*(\underline{v}_1^*)).$$

Vi har således $(f \oplus g)^* = f^* \oplus g^*$.

Lad $(U_j \mid j \in J)$ være en familie af vektorrum over K. Da er $\prod_{j \in J} U_j$ et vektorrum over K bestående af alle familier $(\underline{u}_j \mid j \in J)$ med $\underline{u}_j \in U_j$ for alle $j \in J$. Regning foregår efter reglerne

$$(\underline{u}_j \mid j \in J) + (\underline{v}_j \mid j \in J) = (\underline{u}_j + \underline{v}_j \mid j \in J); \quad \lambda(u_j \mid j \in J) =$$

$$(\lambda u_j \mid j \in J).$$

Den direkte sum $\bigoplus_{j\in J} U_j$ er det underrum af $\prod_{j\in J} U_j$, som består af de af familierne $(\underline{u}_j \mid j \in J)$, der har $\underline{u}_j = \underline{0}$ undtagen for endelig mange $j \in J$.

En familie $(\varphi_j : V \to U_j \mid j \in J)$ af lineære afbildninger inducerer en lineær afbildning $\varphi : V \to \prod_{j\in J} U_j$ ved $\varphi(\underline{v}) = (\varphi_j(\underline{v}) \mid j \in J)$. En familie $(\varphi_j : U_j \to V \mid j \in J)$ af lineære afbildninger inducerer en lineær afbildning $\varphi : \bigoplus_{j\in J} U_j \to V$ defineret ved $\varphi(\underline{u}_j \mid j \in J) = \sum_{j\in J} \varphi_j(u_j)$, hvilket har mening da summen bare indeholder endelig mange fra $\underline{0}$ forskellige elementer.

Det er let at vise, at $(\bigoplus_{j\in J} U_j)^*$ er isomorft med $\prod_{j\in J} U_j^*$, men det vil vi dog ikke udføre. Til gengæld er det ikke så let at sige noget generelt og rigtigt om $(\prod_{j\in J} U_j)^*$.

KAPITEL 12

Basis for vektorrum.

Lad U være et vektorrum over et legeme K. Lad $M \subseteq U$ være endelig mængde. Vi har da linearkombinationerne $\lambda_1\underline{u}_1+\ldots+\lambda_n\underline{u}_n$ af vektorer i M, og mængden af alle sådanne er spanM, spandet af M, det af M udspændte vektorrum.

Linearkombinationen $\lambda_1\underline{u}_1+\ldots+\lambda_n\underline{u}_n$ kan eventuelt reduceres. Hvis nogle af vektorerne $\underline{u}_1,\ldots,\underline{u}_n$ er ens, kan nogle led trækkes sammen. Endvidere kan led med koefficient 0 udelades. Derved får vi eventuelt den tomme linearkombination, hvis værdi er $\underline{0}$. Enhver linearkombination giver ved reduktion enten den tomme form eller en form $\mu_1\underline{v}_1+\ldots+\mu_q\underline{v}_q$, hvor $\underline{v}_1,\ldots,\underline{v}_q$ er indbyrdes forskellige.

For $\underline{u} \in$ spanM har vi mindst én fremstilling som en linearkombination af elementer fra M. Hvis vi har to fremstillinger $\underline{u} = L_1$ og $\underline{u} = L_2$, hvor L_1 og L_2 er indbyrdes forskellige linearkombinationer af elementer i M, får vi $\underline{0} = L_2 - L_1$, så også $\underline{0}$ har en fremstilling som en ikke tom linearkombination ud over den tomme. Hvis $\underline{0} = L$ er en fremstilling af $\underline{0}$ ved en ikke tom linearkombination, har

$\underline{u} = L_1 \in \text{span}M$ også en yderligere fremstilling, nemlig $\underline{u} = L_1 + L$.

Vi ser således, at fremstillingen af vektorer i spanM som linearkombinationer af vektorer i M enten er éntydig for alle vektorer i spanM eller ikke éntydig for nogen vektor i spanM.

Enhver vektor $\underline{u} \in M$ har den trivielle fremstilling som linearkombinationen $1 \cdot \underline{u}$. Hvis $\underline{u}$ kan skrives som en linearkombination af de øvrige vektorer i M er vi derfor i den situation, at vektorerne i U ikke fremstilles éntydigt som linearkombinationer af vektorerne i M. Hvis vi på den anden side antager, at vi har en fremstilling $\underline{0} = \lambda_1\underline{u}_1+\ldots+\lambda_n\underline{u}_n$ med $\underline{u}_1,\ldots,\underline{u}_n \in M$ og $\lambda_1 \neq 0,\ldots,\lambda_n \neq 0$, $n \geq 1$, da får vi $\underline{u}_1 = \lambda_1^{-1}\lambda_2\underline{u}_2+\ldots+\lambda_1^{-1}\lambda_n\underline{u}_n$, så $\underline{u}_1$ kan skrives som linearkombination af de øvrige elementer i M. På baggrund af disse overvejelser har vi følgende definition:

Definition 12.1. Lad U være et vektorrum over et legeme K. En mængde $M \subseteq K$ kaldes lineært uafhængig, hvis følgende 3 indbyrdes ækvivalente betingelser er opfyldt:

1). Enhver vektor $\underline{u} \in \text{span}M$ kan kun på én måde skrives som en linearkombination af elementer i M.

2). Kun den tomme linearkombination af elementer i M giver $\underline{0}$.

3). Ingen vektor i M er en linearkombination af de øvrige.

I stedet for at sige, at M er lineært uafhængig, siger vi også, at M er en mængde af lineært uafhængige vektorer. Hvis M ikke er lineært uafhængig, kalder vi M lineært afhængig, og vektorerne i M lineært afhængige.

Enhver delmængde af en lineært uafhængig mængde er lineært uafhængig. Den tomme mængde er lineært uafhængig. En lineært uafhængig mængde indeholder ikke $\underline{0}$. En mængde af kun én vektor $\underline{u}$ er lineært uafhængig, hvis og kun hvis $\underline{u} \neq \underline{0}$. To vektorer er lineært afhængige, hvis og kun hvis én af dem kan fås ved at gange den anden med en konstant.

Det følgende lemma, som kaldes udskiftningslemmaet, vil hjælpe os med opklaringen af en hel del ikke trivielle problemer.

Sætning 12.2. Lad U være et vektorrum over et legeme K. Lad $A \subseteq U$ være en uafhængig endelig mængde med p elementer, og lad $M \subseteq U$ være en mængde, for hvilken $\text{span}M = U$. Da findes en mængde $B \subseteq M$ med netop p elementer, for hvilken det gælder, at $\text{span}((M \setminus B) \cup A) = U$; med andre ord: Egenskaben $\text{span}M = U$ bevares, når delmængden $B \subseteq M$ udskiftes med A.

Bevis. Vi vil vise lemmaet ved induktion efter p. For $p = 0$ er $A = \emptyset$, og valget $B = \emptyset$ giver det ønskede. Lad $\overline{A} \subseteq U$ være en lineært uafhængig mængde med $p + 1$ elementer, og lad os antage, at $\overline{A} = A \cup \{\underline{a}\}$, $a \notin A$, og at påstanden i sætningen gælder for mængden A. Vi skal så blot vise, at påstanden i sætningen også gælder for mængden $\overline{A}$. Da $\underline{a} \in U = \text{span}((M \setminus B) \cup A)$, er $\underline{a} = L$, hvor L er en linearkombination af elementer i $(M \setminus B) \cup A$. Da $\overline{A}$ er lineært uafhængig, er $\underline{a}$ ikke linearkombination af elementerne i A, og L indeholder derfor et element $\underline{b} \in M \setminus B$. Ved løsning af ligningen $\underline{a} = L$ får vi $\underline{b}$ udtrykt som linearkombination af $\underline{a}$ samt de fra $\underline{b}$ forskellige elementer i $(M \setminus B) \cup A$. Vi sætter $\overline{B} = B \cup \{\underline{b}\}$. Så har $\overline{B}$ netop $p + 1$ elementer, og $(M \setminus \overline{B}) \cup \overline{A}$ fås af $(M \setminus B) \cup A$ ved at erstatte $\underline{b}$ med $\underline{a}$. Men $\underline{b}$ er netop en linearkombination af elementerne i $(M \setminus \overline{B}) \cup \overline{A}$, og dermed er alle elementerne i $(M \setminus B) \cup A$ linearkombinationer af elementerne i $(M \setminus \overline{B}) \cup \overline{A}$. Det er ensbetydende med, at $U = \text{span}((M \setminus B) \cup A) \subseteq \text{span}((M \setminus \overline{B}) \cup \overline{A})$, altså $U = \text{span}((M \setminus \overline{A}) \cup \overline{B})$. Dermed er sætningen bevist.

Definition 12.3. Lad U være et vektorrum over et legeme K. En mængde $B \subseteq U$ kaldes en basis for U, hvis ethvert element $\underline{u} \in U$ har én og kun én fremstilling som linearkombination af elementer i B.

Det stillede krav ses at være helt ensbetydende med, at B er lineært uafhængig, og at $\text{span}B = U$.

Sætning 12.4. Hvis et vektorrum U over et legeme K har en endelig basis med p elementer, vil enhver basis for U være endelig med netop p elementer.

Bevis. Lad $B \subseteq U$ være en basis med p elementer. Da $\text{span}B = U$, viser udskiftningslemmaet, at lineært uafhængige delmængder af U indeholder højst p elementer. Hvis $B_1 \subseteq V$ er en anden basis, har B_1 altså $q \leq p$ elementer. Nu er $\text{span}B_1 = U$, så udskiftningslemmaet giver også, at $p \leq q$, altså $q = p$. Dermed er sætningen bevist.

Vi kan således påstå, at alle baser for et vektorrum U indeholder lige mange elementer, i den forstand, at de enten alle består af samme endelige antal elementer eller alle består af uendelig mange elementer.

Definition 12.5. Et vektorrum U over et legeme K kaldes p-dimensionalt, hvis det har en basis med p elementer, endeligdimensionalt, hvis det har en endelig basis, og uendeligdimensionalt, hvis det ikke har en endelig basis. Hvis U er p-dimensionalt, skriver vi $\dim U = p$.

Eksempler. Det trivielle vektorrum, der bare består af $\underline{0}$, er 0-dimensionalt. Legemet K er selv et 1-dimensionalt vektorrum over K. Vektorrummet $\mathbb{E}^2$ er 2-dimensionalt, og $\mathbb{E}^3$ er 3-dimensionalt over $\mathbb{R}$. Kvaternionlege-

met $\mathbb{K}$ er et 4-dimensionalt vektorrum over $\mathbb{R}$. Vektorrummet af kontinuerte funktioner $f:\mathbb{R} \to \mathbb{R}$ er et uendelig dimensionalt vektorrum over $\mathbb{R}$. Identitetssætningen for polynomier viser nemlig, at mængden $\{\varphi_n \mid n \in \mathbb{N}\}$, hvor $\varphi_n(x) = x^{n-1}$, er en lineært uafhængig uendelig mængde.

I et vektorrum U over et legeme K kan vi betragte mængden af lineært uafhængige delmængder. Denne mængde er ordnet ved inklusion, men kun i trivielle tilfælde totalt ordnet. Der er således mening i at tale om en maksimal lineært uafhængig mængde.

Sætning 12.6. En lineært uafhængig mængde M i et vektorrum U over et legeme K er en basis for U, hvis og kun hvis den er maksimal.

Bevis. Vi ved, at M er en basis, hvis og kun hvis $\text{span}M = U$, og det er netop ensbetydende med, at ingen vektor i $U \setminus M$ sammen med M giver et lineært uafhængigt system.

Lad U være et vektorrum over et legeme K, og $M = \{\underline{e}_1, \underline{e}_2, \ldots, \underline{e}_q\} \subseteq U$ lineært uafhængig. Hvis M ikke er maksimal, kan vi få en lineært uafhængig mængde $\{\underline{e}_1, \ldots, \underline{e}_q, \underline{e}_{q+1}, \ldots, \underline{e}_r\}$ med flere elementer i. Hvis vi ved således at tilføje endelig mange elementer kommer til en maksimal li-

neært uafhængig mængde $B = \{\underline{e}_1,\ldots,\underline{e}_n\} \subseteq U$, er U endeligdimensionalt, og vi har fundet en basis. Hvis vi ikke opnår dette, får vi en numerabel mængde af lineært uafhængige elementer, og så er U uendelig dimensionalt. Dermed har vi vist følgende sætning.

Sætning 12.7. Lad U være et vektorrum over et legeme K, og lad $M \subseteq U$ være en endelig lineært uafhængig delmængde. Hvis U er endeligdimensionalt, har U en basis $B \supseteq M$. Hvis U er uendeligdimensionalt, findes der en numerabel lineært uafhængig delmængde $A \supset M$.

Groft sagt fortæller sætningen, at en lineært uafhængig delmængde af et endeligdimensionalt vektorrum U kan udvides til en basis for U.

Sætning 12.8. Lad U være et endeligdimensionalt vektorrum over et legeme K, og lad $V \subseteq U$ være et underrum. Der findes da et underrum $W \subseteq U$ isomorft med $\frac{U}{V}$, som tilfredsstiller betingelsen $U = V \oplus W$. Hvis $U = V \oplus W$, da er $\dim U = \dim V + \dim W$.

Bevis. Den foregående sætning giver, at der findes en basis $\{\underline{e}_1,\ldots,\underline{e}_p\}$ for V, og at den kan udvides til en basis $\{\underline{e}_1,\ldots,\underline{e}_p, \underline{e}_{p+1},\ldots\underline{e}_{p+q}\}$ for U. Vi definerer $W = \text{span}\{\underline{e}_{p+1},\ldots,\underline{e}_{p+q}\}$. Et element $\underline{u} \in U$ har en frem-

stilling $\underline{u} = \lambda_1\underline{e}_1+\ldots+\lambda_{p+q}\underline{e}_{p+q}$. Vi sætter $\underline{v} = \lambda_1\underline{e}_1+\ldots+\lambda_p\underline{e}_p \in V$ og $\underline{w} = \lambda_{p+1}\underline{e}_{p+1}+\ldots+\lambda_{p+q}\underline{e}_{p+q} \in W$. Så er $\underline{u} = \underline{v} + \underline{w}$, og dermed har vi vist, at $U = V + W$. Af $\underline{u} \in V \cap W$ følger, at vi har en relation $\underline{u} = \lambda'_1\underline{e}_1+\ldots+\lambda'_p\underline{e}_p = \lambda''_{p+1}\underline{e}''_{p+1}+\ldots+\lambda'_{p+q}\underline{e}_{p+q}$, men det går kun for $\lambda'_1 = \ldots = \lambda'_{p+q} = 0$, altså $\underline{u} = \underline{0}$. Altså er $U \cap W = \{0\}$, så vi har $U = V\oplus W$. Restklasserne, som udgør $\frac{U}{V}$, bliver netop klasserne $w + V$, $w \in W$, og deraf følger, at $\frac{U}{V}$ er isomorf med W. Den sidste påstand følger af, at $\dim U = p+q$, $\dim V = p$ og $\dim W = q$. Dermed er sætningen bevist.

Definition 12.9. To delrum V og W af et vektorrum U over et legeme K kaldes komplementære, hvis $U = V\oplus W$. Ved for $\underline{u} \in U$ at definere $p_1(\underline{u}) \in V$ og $p_2(\underline{u})$ i W som de elementer, der tilfredsstiller $\underline{u} = p_1(\underline{u}) + p_2(\underline{u})$ får vi defineret de til spaltningen $U = V\oplus W$ hørende projektioner $p_1: U \to V$ og $p_2: U \to W$.

Det er næsten helt indlysende, at p_1 og p_2 bliver lineære. Af $\underline{u}_1 = p_1(\underline{u}_1) + p_2(\underline{u}_1)$ og $\underline{u}_2 = p_1(\underline{u}_2) + p_2(\underline{u}_2)$ fås nemlig

$$\underline{u}_1 + \underline{u}_2 = (p_1(\underline{u}_1)+p_1(\underline{u}_2)) + (p_2(\underline{u}_1) + p_2(\underline{u}_2)),$$

hvilket netop viser, at $p_1(\underline{u}_1+\underline{u}_2) = p_1(\underline{u}_1) + p_1(\underline{u}_2)$ og analogt for p_2. Den anden regneregel går lettere.

Projektionerne p_1 og p_2 kan opfattes som afbildninger $p_1, p_2 : U \to U$ med $p_1(U) = V$, $p_2(U) = W$, kern p_1 = W, kern p_2 = V. Endvidere er $p_1 \circ p_1 = p_1$ og $p_2 \circ p_2 = p_2$.

Definition 12.10. En afbildning $f : M \to M$ af en mængde ind i sig selv kaldes idempotent, hvis $f \circ f = f$.

Projektionerne p_1 og p_2 er således idempotente. Det viser sig, at alle idempotente endomorfier af et vektorrum er projektioner.

Sætning 12.11. Lad U være et vektorrum over et legeme K, og $p : U \to U$ en idempotent endomorfi, da er $U = p(U) \oplus$ kern p, og p er projektionen på p(U).

Bevis. For $\underline{u} \in U$ vil $\underline{v} = \underline{u} - p(\underline{u})$ tilfredsstille $p(\underline{v}) = p(\underline{u}) - p(p(\underline{u})) = p(\underline{u}) - p(\underline{u}) = \underline{0}$, altså $\underline{v} \in$ kern p, så ligningen $\underline{u} = p(\underline{u}) + \underline{v}$ viser, at U = p(U) + kern p. Af $\underline{u} = \underline{w} + \underline{v}$, $\underline{w} \in p(U)$, $\underline{v} \in$ kern p følger, at $p(\underline{w}) = \underline{w}$, altså $p(\underline{u}) = \underline{w}$, så spaltningen er den samme som før. Dermed er sætningen bevist.

Sætning 12.12. Lad V og W være underrum af et vektorrum U over et legeme K. Da er V + W endeligdimensionalt, hvis og kun hvis V og W er endeligdimensionale,

og i så fald er $\dim V + \dim W = \dim(V \cap W) + \dim(V + W)$ (dimensionsformlen).

Bevis. Udskiftningssætningen fortæller, at en lineært uafhængig mængde i et n-dimensionalt vektorrum højst har n elementer, og det samme vil da gælde for en lineært uafhængig mængde i et underrum. Altså er V og W endeligdimensionale, hvis V+W er det. Hvis V og W er endeligdimensionale, er $V \cap W$ endeligdimensionalt, og V indeholder et underrum T komplementært til $V \cap W$, så vi har $V = T+(V \cap W)$. Endvidere er $V+W = T+(V \cap W) + W = T + W$, da $V \cap W + W = W$. Men $T \cap W$ er indeholdt i $V \cap W$ og $T \cap (V \cap W) = \{\underline{0}\}$, så vi har $T \cap W = \{\underline{0}\}$, hvilket medfører, at $V + W = T \oplus W$. Vi har således $\dim(V+W) = \dim T + \dim W$ og $\dim V = \dim T + \dim(V \cap W)$. Heraf følger påstanden umiddelbart.

Sætning 12.13. Lad U være et vektorrum over et legeme K og lad $B \subseteq U$ være en basis for U. Da findes der en isomorfi $\varphi: \bigoplus_{\underline{e} \in B} K \to U$ defineret ved $\varphi(\lambda_{\underline{e}} | \underline{e} \in B) = \sum_{\underline{e} \in B} \lambda_{\underline{e}} \underline{e}$.

Bevis. Da $\bigoplus_{\underline{e} \in B} K$ består af familier $(\lambda_{\underline{e}} | \underline{e} \in B)$ med alle $\lambda_{\underline{e}} \in K$ og højst endelig mange $\lambda_{\underline{e}} \neq 0$, er $\sum_{\underline{e} \in B} \lambda_{\underline{e}} \underline{e}$ en linearkombination af elementer fra B, og φ er bijektiv, fordi hvert element af U har netop én fremstilling

som en sådan linearkombination. Det ses umiddelbart, at φ er lineær. Dermed er sætningen bevist.

Sætningen fortæller os, at vektorrum over samme legeme er isomorfe, hvis de blot har baser med samme kardinaltal. Specielt er endeligdimensionale vektorrum isomorfe, hvis og kun hvis de har samme dimension. En isomorfi må nemlig afbilde basis i basis, derfor gælder "kun hvis". Læg mærke til, at denne del af sagen indirekte bygger på udskiftningslemmaet. Det kan vises også for et uendeligdimensionalt vektorrum, at alle baser har samme kardinaltal. Dette kardinaltal er det uendeligdimensionale vektorrums dimension.

KAPITEL 13

Vektorrum med basis.

Vi vil studere vektorrum over et legeme K, som skal være det samme legeme hele tiden, så vi vil ikke nævne det eksplicit i dette afsnit.

Vi vil specielt interessere os for par (U,B) af et vektorrum og en basis B for U. Hver vektor $\underline{u} \in U$ har da netop én fremstilling som en linearkombination $\underline{u} = \lambda_1\underline{e}_1+\ldots+\lambda_n\underline{e}_n$, hvor $\underline{e}_1,\ldots,\underline{e}_n \in B$, $\lambda_1,\ldots,\lambda_n \in K\setminus\{0\}$, og hvor n er et naturligt tal undtagen for $\underline{u} = \underline{0}$, som udtrykkes ved den tomme linearkombination, der har $n = 0$.

Lad nu V være et andet vektorrum. Så er $\mathrm{Hom}(U,V)$ et vektorrum. Mængden V^B af alle afbildninger $\tilde{\varphi}:B \to V$ er også et vektorrum med sædvanlig addition af funktioner og multiplikation af funktioner med en konstant faktor.

Sætning 13.1. Vektorrummene $\mathrm{Hom}(U,V)$ og V^B er isomorfe. En isomorfi $\rho:\mathrm{Hom}(U,V) \to V^B$ er givet ved, at vi for hver lineær $\varphi:U \to V$ definerer $\rho(\varphi) = \varphi|B$. Den

omvendte isomorfi $\varepsilon: V^B \to \mathrm{Hom}(U,V)$ er givet ved, at vi for hver afbildning $\tilde{\varphi}: B \to V$ definerer $\varepsilon(\tilde{\varphi}) = \varphi: U \to V$ ved $\varphi(\lambda_1 \underline{e}_1 + \ldots + \lambda_n \underline{e}_n) = \lambda_1 \tilde{\varphi}(\underline{e}_1) + \ldots + \lambda_n \tilde{\varphi}(\underline{e}_n)$.

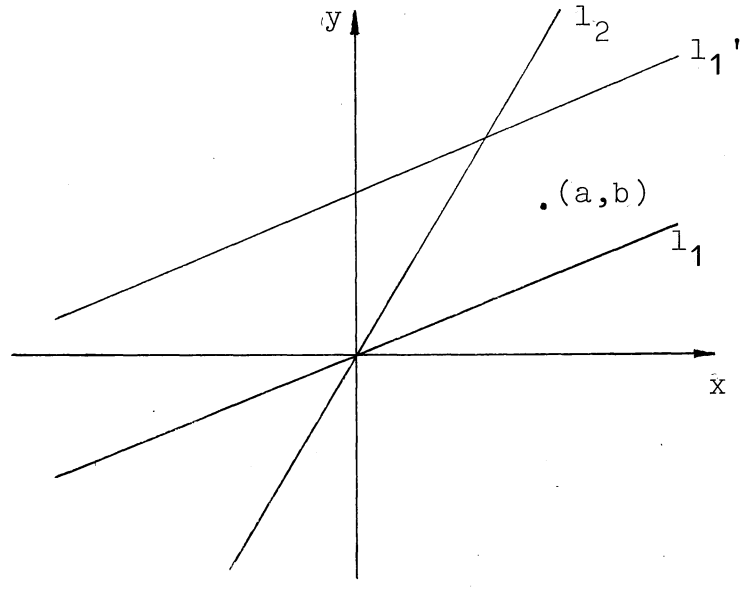
Bevis. Det er klart, at ρ er en homomorfi. For en afbildning $\tilde{\varphi}: B \to V$ kan vi virkelig definere φ som anført, idet hvert $\underline{u} \in U$ har netop én fremstilling som linearkombination af basiselementer. At den således definerede afbildning $\varphi: U \to V$ bliver lineær, ses umiddelbart. Dernæst ses lige så umiddelbart, at ε bliver en homomorfi. Det er også klart, at $\rho \circ \varepsilon: V^B \to V^B$ er den identiske afbildning. At $\varepsilon \circ \rho: \mathrm{Hom}(U,V) \to \mathrm{Hom}(U,V)$ er den identiske afbildning følger af, at vi for $\varphi \in \mathrm{Hom}(U,V)$ har $\varphi(\lambda \underline{e}_1 + \ldots + \lambda \underline{e}_n) = \lambda_1 \varphi(\underline{e}_1) + \ldots + \lambda_n \varphi(\underline{e}_n)$. Dermed er sætningen bevist.

Sætningen siger groft udtrykt, at en lineær afbildning $f: U \to V$ en entydigt fastlagt ved sine værdier på elementerne i en basis for U, og at ethvert valg af disse værdier virkelig svarer til en lineær afbildning af U ind i V.

For ethvert vektorrum V har vi altid visse lineære afbildninger $\varphi: V \to V$, nemlig ligedannethedsafbildninger $h_\lambda: V \to V$ definerede ved $h_\lambda(\underline{v}) = \lambda \underline{v}$, hvor λ er et element af K. For et vektorrum (U,B) med en basis, har vi lige så mange lineære afbildninger $\varphi: U \to U$, som der er afbildninger $\varphi: B \to U$. Således er $\mathbb{R}$ et vektorrum over $\mathbb{Q}$, og af $\mathbb{Q}$-lineære afbildninger $\varphi: \mathbb{R} \to \mathbb{R}$ har vi jo li-

gedannethedsafbildningerne, og det er faktisk svært at angive andre.

Lad os et øjeblik studere en eventuel $\mathbb{Q}$-lineær afbildning $\varphi:\mathbb{R} \to \mathbb{R}$, som ikke er en ligedannethed. Så skulle der være to tal $x_1, x_2 \in \mathbb{R}$, samt $k_1, k_2 \in \mathbb{R}$, $k_1 \neq k_2$, således at $\varphi(x_1) = k_1 x_1$, $\varphi(x_2) = k_2 x_2$. For alle $r \in \mathbb{Q}$ har vi da $\varphi(rx_1) = k_1(rx_1)$ og $\varphi(rx_2) = k_2(rx_2)$. Punkterne $(rx_1, \varphi(rx_1))$ og $(rx_2, \varphi(rx_2))$ af funktionens graf ligger overalt tæt på de rette linier l_1 og l_2 med ligninger $y = k_1 x$ og $y = k_2 x$. Lad nu (a,b) være et helt vilkårligt punkt i planen. Linien l'_1 symmetrisk til l_1 med hensyn til (a,b) skærer l_2 i et punkt $(x', k_2 x')$, og dettes symmetriske punkt $(x'', k_1 x'')$ med hensyn til (a,b) vil tilfredsstille betingelserne $a = \frac{1}{2}(x'+x'')$, $b = \frac{1}{2}(k_2 x' + k_1 x'')$. Nu kan vi vælge $r_1, r_2 \in \mathbb{Q}$, så $r_1 x_1$ og $r_2 x_2$ ligger så tæt det skal være ved x'' og x'. Derved kan $(\frac{1}{2}(r_1 x_1 + r_2 x_2), \frac{1}{2}(k_1 r_1 x_1 + k_2 r_2 x_2))$ kommer til at ligge vilkårlig tæt ved (a,b), og det er et punkt af grafen for φ, for vi har



$$\varphi(\tfrac{1}{2}(r_1x_1+r_2x_2)) = \tfrac{1}{2}(\varphi(r_1x_1)+\varphi(r_2x_2)) = \tfrac{1}{2}(k_1r_1x_1+k_2r_2x_2).$$

Dermed har vi vist, at grafen for φ indeholder punkter i enhver omegn af (a,b). Da (a,b) var et vilkårligt punkt, får vi, at grafen for φ er overalt tæt i hele planen.

Det fremgår af denne overvejelse, at de $\mathbb{Q}$-lineære afbildninger af $\mathbb{R}$ ind i sig selv, som ikke er ligedannetheder, er ganske overordentlig diskontinuerte - der findes ikke engang intervaller, i hvilke de er begrænsede.

Nu må det tilføjes, at det aldrig er lykkedes explicit at angive en diskontinuert $\mathbb{Q}$-lineær afbildning $\varphi:\mathbb{R} \to R$. På grund af de her omtalte egenskaber har intuitionistisk indstillede matematikere været utilbøjelige til at tro på disse funktioners eksistens.

Linearformerne $\mathbb{R} \to \mathbb{Q}$ må søges blandt de endomorfier $\mathbb{R} \to \mathbb{R}$, som afbilder ind i $\mathbb{Q}$. Det gør rigtige ligedannetheder ikke, så 0-formen bliver den eneste kontinuerte linearform på vektorrummet $\mathbb{R}$ over $\mathbb{Q}$.

Lad nu igen U være et vektorrum, og lad $(M_j \mid j \in J)$ være en familie af lineært uafhængige delmængder af U, totalt ordnet ved inklusion. Så er $\bigcup_{j\in J} M_j = M$ lineært uaf-

hængig. For $\underline{e}_1,\ldots,\underline{e}_n \in M$ vil jo ligge i mængder $M_{j_1},\ldots,M_{j_n}$, der alle er delmængder af et eller andet M_j, og den eneste fremstilling af $\underline{0}$ som linearkombination af elementer af M_j er den tomme. Dermed har vi vist påstanden.

Mængden af lineært uafhængige delmængder af U er ordnet ved inklusion. Af den foregående bemærkning følger, at enhver total ordnet delmængde kan majoriseres ved sin foreningsmængde. Hvis vi så tror på Zorns lemma, får vi, at der i U findes maksimale lineært uafhængige delmængder. Men en sådan delmængde er en basis. Altså har ethvert vektorrum en basis. Hvis $A \subset U$ er en lineært uafhængig mængde, kan vi anvende ræsonnementet på mængden af de lineært uafhængige delmængder af U, der indeholder en A, og vi slutter, at U har en basis, der indeholder mængden A.

Hvis $V \subseteq U$ er et underrum, har V en basis B_V, og den kan udvides til en basis B for U. Så er $B_W = B \setminus B_V$ basis for et underrum W, der kun har $\underline{0}$ fælles med U. Enhver vektor $\underline{u} \in U$ er en linearkombination af vektorer fra B altså sum af en linearkombination af vektorer fra B_V og en linearkombination af vektorer fra B_W. Altså er $U = V \oplus W$, og W er komplementært underrum til V.

Vi formulerer de opnåede resultater i en sætning.

Sætning 13.2. Ethvert vektorrum U har en basis. Enhver lineært uafhængig delmængde af U kan udvides til en basis for U. Ethvert underrum af U har et komplementært underrum.

Specielt har $\mathbb{R}$ som vektorrum over $\mathbb{Q}$ en basis. Det medfører, at der findes mange linearformer $\mathbb{R} \to \mathbb{Q}$, og bortset fra 0-formen er de alle groteske diskontinuerte funktioner, som vi ikke kan give explicite udtryk for. Da et endeligdimensionalt vektorrum over $\mathbb{Q}$ vil være numerabelt, er $\mathbb{R}$ uendeligdimensionalt over $\mathbb{Q}$. Det er endda også rigtigt, at et numerabelt-dimensionalt vektorrum over $\mathbb{Q}$ bliver numerabelt. En nærmere undersøgelse, som vi ikke skal udføre, vil afsløre, at en basis for $\mathbb{R}$ over $\mathbb{Q}$ har samme kardinaltal som $\mathbb{R}$ selv. Det er let nok at angive en numerabel lineært uafhængig delmængde af $\mathbb{R}$. Som eksempel kan vi nævne mængden $\{\log p \mid p \text{ primtal}\}$. En relation $r_1 \log p_1 + \ldots + r_n \log p_n = 0$ med rationale koefficienter giver nemlig ved multiplikation med fællesnævneren en relation $k_1 \log p_1 + \ldots + k_n \log p_n = 0$ med hele koefficienter, og den er ensbetydende med $p_1^{k_1} \ldots p_n^{k_n} = 1$, og så følger det af sætningen om entydighed af opløsning i primfaktorer, at det kun går, når produktet på venstre side er tomt.

Sætning 13.3. Lad U og V være vektorrum, og $U_1 \subset U$ et underrum. Enhver lineær afbildning $\overline{\varphi}:U_1 \to V$ kan udvides til en lineær afbildning $\overline{\varphi}:U \to V$.

Bevis. Vi vælger et komplementært underrum $U_2 \subset U$ til U_1, samt en lineær afbildning $\varphi':U_2 \to V$ (f.eks. 0-afbildningen). For $\underline{u} = \underline{u}_1 + \underline{u}_2$ med $\underline{u}_1 \in U_1$, $\underline{u}_2 \in U_2$ definerer vi nu $\overline{\varphi}(\underline{u}) = \varphi(\underline{u}_1) + \varphi'(\underline{u}_2)$, og så er $\overline{\varphi}$ den ønskede udvidelse af φ.

Sætning 13.4. Lad U og V være vektorrum, og $\underline{u}_0 \in U$, $\underline{v}_0 \in V$ vilkårlige vektorer, dog således at $\underline{v}_0 = \underline{0}$, hvis $\underline{u}_0 = \underline{0}$. Da findes der en lineær afbildning $\varphi: U \to V$ med $\varphi(\underline{u}_0) = \underline{v}_0$.

Bevis. Ved $\varphi'(k\underline{u}_0) = k\underline{v}_0$ defineres en lineær afbildning $\varphi':U_1 \to V$, hvor $U_1 \subseteq U$ er det ved $U_1 = \{k\underline{u}_0 | k \in K\}$ bestemte underrum. Ifølge den foregående sætning kan φ' udvides til en afbildning $\varphi_1:U \to V$. Dermed er sætningen bevist.

Lad U og V være vektorrum, og $f:U \to V$ en lineær afbildning. Vi har da de duale vektorrum U^* og V^* bestående af lineære afbildninger $\underline{\alpha}:U \to K$ og $\underline{\gamma}:V \to K$. Desuden har f en dual afbildning $f^*:V^* \to U^*$ givet ved $f^*(\underline{\gamma}) = \underline{\gamma} \circ f$.

Sætning 13.5. Lad $f:U \to V$ være en lineær afbildning og $f^*:V^* \to U^*$ dens duale afbildning. Vi har da relationerne

$$\ker f^* = \{\underline{\gamma} \in V^* \mid f(U) \subseteq \ker\underline{\gamma}\}.$$

$$f(U) = \bigcap_{\underline{\gamma}\in\ker f^*} \ker\underline{\gamma}$$

$$f^*(V^*) = \{\underline{\alpha} \in U^* \mid \ker f \subseteq \ker\underline{\alpha}\}$$

$$\ker f = \bigcap_{\underline{\alpha}\in f^*(V^*)} \ker\underline{\alpha} .$$

Bevis. Af $f(U) \subseteq \ker\underline{\gamma}$ følger $\underline{\gamma}(f(U)) = \{\underline{0}\}$, altså at $f^*(\underline{\gamma}) = \underline{\gamma}\circ f$ er 0-afbildningen. Hvis $f^*(\underline{\gamma}) = \underline{\gamma}\circ f$ er 0-afbildningen, er $\underline{\gamma}(f(U)) = \{\underline{0}\}$, altså $f(U) \subseteq \ker\underline{\gamma}$. Dermed er den første påstand bevist.

Den første påstand medfører, at $f(U) \subseteq \bigcap_{\underline{\gamma}\in\ker f^*} \ker\underline{\gamma}$. Her er $f(U)$ et underrum i V. Vi betragter en vilkårlig vektor $\underline{v}_0 \in V\setminus f(U)$, og vi vælger en basis $\tilde{B}$ for $f(U)$. Så er $\tilde{B} \cup \{\underline{v}_0\}$ en lineært uafhængig mængde, der kan udvides til en basis B for V. Altså er $B\setminus\{\underline{v}_0\}$ basis for et underrum $V_1 \subseteq V$, og vi har $f(U) \subseteq V_1$, og V_1 er komplementært til V_0. Men så findes der en linearform $\underline{\gamma}_0:V \to K$, som er $\underline{0}$ på $f(U)$, men $\neq \underline{0}$ i $\underline{v}_0$, og så har vi $\underline{\gamma}_0 \in \ker f^*$ og $\underline{v}_0 \notin \ker\underline{\gamma}_0$. Heraf følger, at kun punkterne af $f(U)$ er fælles for alle $\ker\underline{\gamma}$ med $\underline{\gamma} \in \ker f^*$, og dermed er den anden påstand bevist.

Relationen $\underline{\alpha} \in f^*(V^*)$ er ensbetydende med, at der findes en linearform $\underline{\gamma}:V \to K$, således at $\underline{\alpha} = \underline{\gamma} \circ f$. Dette medfører, at $\text{kern} f \subseteq \text{kern}\underline{\alpha}$. Hvis $\text{kern} f \subseteq \text{kern}\underline{\alpha}$ har vi på den anden side, at der findes en linearform $\underline{\gamma}':f(U) \to K$, således at $\underline{\alpha} = \underline{\gamma}' \circ f$. Nu kan $\underline{\gamma}'$ udvides til en linearform $\underline{\gamma}:V \to K$, og vi har så $\underline{\alpha} = \underline{\gamma} \circ f$. Dermed er den tredie påstand bevist.

Den tredie påstand medfører, at $\text{kern} f \subset \bigcap_{\underline{\alpha} \in f^*(V^*)} \text{kern}\underline{\alpha}$. Her er $\text{kern} f \subseteq U$ et underrum. Et punkt $\underline{u}_0 \in U \setminus \text{kern} f$ udspænder et 1-dimensionalt underrum $U_0 \subseteq U$, og hvis $\tilde{B}$ er en basis for $\text{kern} f$ er $\tilde{B} \cup \{\underline{u}_0\}$ en lineært uafhængig mængde, der kan udvides til en basis B for U. Så er $B \setminus \{\underline{u}_0\}$ basis for et underrum $U_1 \subseteq U$, som tilfredsstiller $\text{kern} f \subseteq U_1$ og er komplementært til U_0. Så findes der en linearform $\underline{\alpha}_0:U \to K$ med $\text{kern}\underline{\alpha}_0 \supseteq U_1$ og $\underline{\alpha}_0(\underline{u}_0) \neq 0$. Men så gælder $\underline{\alpha}_0 \in f^*(V^*)$, og vi kan slutte, at $\underline{u}_0 \notin \bigcap_{\underline{\alpha} \in f^*(V^*)} \text{kern}\underline{\alpha}$. Dermed er sætningen bevist.

Sætning 13.6. Lad $f:U \to V$ være en lineær afbildning og $f^*:V^* \to U^*$ den duale afbildning. Så er f surjektiv, hvis og kun hvis f^* er injektiv.

Bevis. Det fremgår af den anden relation i sætning 13.5 at f er surjektiv, altså $f(U) = V$, hvis og kun hvis det for alle $\underline{\gamma} \in \text{kern} f^*$ gælder, at $\text{kern}\underline{\gamma} = V$, altså at $\underline{\gamma}$ er $\underline{0}$-afbildningen. Men det er netop helt ensbetydende med, at $\text{kern} f^* = \{\underline{0}\}$, altså at f^* er injektiv. Dermed er sætningen bevist.

Det går ikke an at lade f og f^* bytte roller i sætningen. Den derved fremkomne påstand vil kun være rigtig, hvis V er et endeligdimensionalt vektorrum. Dertil kommer så, at f ikke kan være injektiv, når V er endeligdimensionalt, uden at U også er det. Dette følger af, at $f(U) \subseteq V$ er isomorf med U, hvis f er injektiv.

Vi vil fortsætte med nogle sætninger om det biduale rum U^{**} til U. Vi minder om den lineære afbildning $\Phi: U \to U^{**}$, hvor $\Phi(\underline{u}) = \underline{u}^{**}$ for $\underline{u} \in U$ er defineret ved, at vi for hvert $\underline{\alpha} \in U^*$ har $\underline{u}^{**}(\underline{\alpha}) = \underline{\alpha}(\underline{u})$.

Sætning 13.7. Homomorfien $\Phi: U \to U^{**}$ er injektiv.

Bevis. Vi skal vise, at $\ker\Phi = \underline{0}$. Nu betyder $\underline{u}^{**} = \underline{0}$, at $\underline{\alpha}(\underline{u}) = 0$ for alle linearformer $\underline{\alpha}: U \to K$. Men hvis $\underline{u} \neq \underline{0}$, findes der altid en linearform $\underline{\alpha}: U \to K$ med $\underline{\alpha}(\underline{u}) \neq 0$. Dermed er sætningen bevist.

Sætning 13.8. Lad U og V være vektorrum og $f: U \to V$ en lineær afbildning. Vi har da homomorfierne $\Phi_U: U \to U^{**}$ og $\Phi_V: V \to V^{**}$, og sammen med den biduale afbildning $f^{**}: U^{**} \to V^{**}$ tilfredsstiller de relationen $\Phi_V \circ f = f^{**} \circ \Phi_U: U \to V^{**}$.

Bevis. Vi har $(\Phi_V \circ f)(\underline{u}) = \Phi_V(f(\underline{u})) = f(\underline{u})^{**}$. Her er $f(\underline{u})^{**}$ en linearform $f(\underline{u})^{**}: V^* \to K$. Et element $\underline{\gamma} \in V^*$ er en linearform $\underline{\gamma}: V \to K$, og efter definitionen

af Φ er $f(\underline{u})^{**}(\underline{\gamma}) = \underline{\gamma}(f(\underline{u}))$. På den anden side er $(f^{**} \circ \Phi_U(\underline{u}) = f^{**}(\underline{u}^{**})$, og her er $\underline{u}^{**}$ en linearform $\underline{u}^{**}: U^* \to K$. Efter definitionen af dual afbildning er $f^{**}(\underline{u}^{**}) = \underline{u}^{**} \circ f^*$, og vi får derfor $f^{**}(\underline{u}^{**})(\underline{\gamma}) = (\underline{u}^{**} \circ f^*)(\underline{\gamma}) = \underline{u}^{**}(f^*(\underline{\gamma})) = \underline{u}^{**}(\underline{\gamma} \circ f) = \underline{\gamma}(f(\underline{u}))$. Dermed har vi vist sætningen.

Vi har kaldt visse afbildninger naturlige, men vi har ikke givet nogen forklaring på betydningen af dette ord. Den ganske meget omtalte afbildning Φ er "naturlig" - men hvad mener vi egentlig med det? Glosen hører egentlig hjemme i kategoriteori, og vi har ikke lyst til at ofre alt for megen tid på denne gren af matematikken. Lad os nøjes med at vedtage, at vi har lov at kalde en afbildning af et vektorrum U ind i et vektorrum V naturlig, hvis afbildningen er defineret for en omfattende klasse af par (U,V) af vektorrum, og når den desuden er uafhængig af valget af basis for disse vektorrum.

Som eksempel på en generel afbildning, der ikke er naturlig, skal vi nævne den for ethvert vektorrum U med basis B definerede isomorfi $\varphi: \bigoplus_{b \in B} K \to U$, hvor φ er defineret ved, at $\varphi(\lambda_b \mid b \in B) = \sum_{b \in B} \lambda_b b$. Her er φ på væsentlig måde afhængig af valget af basis.

For et vektorrum (U,B) med basis har vi ifølge sætning 13.1 en isomorfi $\varepsilon: K^B \to \mathrm{Hom}(U,K)$, altså $\varepsilon: K^B \to U^*$.

Nu har vi jo $\bigoplus_{b\in B} K \subseteq \prod_{b\in B} K = K^B$, og den ovenfor nævnte isomorfi φ giver os derfor en ved basis B fastlagt injektiv lineærafbildning $\psi: U \to U^*$. Det er klart, at ψ bliver bijektiv, altså en isomorfi, hvis og kun hvis U er endeligdimensionalt. Billedet $\psi(B)$ af basis bliver et lineært uafhængigt system, som kan udvides til en basis B^* for det duale rum. Vi siger, at B^* er en dual udvidelse af B. I det endeligdimensionale tilfælde siger vi, at B^* er dual basis til B. Vi udtrykker disse resultater i en sætning.

Sætning 13.9. Lad (U,B) være et vektorrum med basis. Der findes en injektiv lineær afbildning $\psi: U \to U^*$ fastlagt ved, at vi for $\underline{b} \in B$ har $\psi(\underline{b}) = \underline{b}^*$, hvor $\underline{b}^*: U \to K$ tilfredsstiller betingelserne $\underline{b}^*(\underline{b}) = 1$ og $\underline{b}^*(\underline{x}) = 0$ for $\underline{x} \in B$, $\underline{x} \neq \underline{b}$. Billedet $\psi(B)$ er en basis for U^*, hvis og kun hvis U er endeligdimensionalt. I så fald siges $B^* = \psi(B)$ at være den duale basis til B, og for $\underline{b} \in B$ kaldes $\underline{b}^* = \psi(\underline{b})$ det til $\underline{b}$ duale basiselement. Et endeligdimensionalt vektorrum er således isomorft med sit duale. Hvis U er uendeligdimensionalt, kan $\psi(B)$ udvides til en basis B^* for U^*, og B^* kaldes så en dual udvidelse af B.

Hvis U er uendeligdimensionalt, får B^* større kardinaltal end B, så U^* bliver i dette tilfælde ikke isomorft med U. Så vil U^* også være uendeligdimensionalt, og basis for U^{**} vil få endnu større kardinaltal end B^*. Vi skal ikke opholde os ved beviset for dette, men vi fremhæver, at

disse resultater udelukker, at den naturlige afbildning $\Phi: U \to U^{**}$ kan være en isomorfi, hvis U er uendeligdimensionalt.

På grund af disse omstændigheder får den rent algebraiske vektorrumsteori kun begrænset interesse i det uendeligdimensionale tilfælde. Det er mere interessant at dyrke vektorrum med yderligere struktur, så man kan tale om kontinuerte afbildninger, og derved får man et dualrum af kontinuerte linearformer og af langt større interesse. Dette synspunkt er emnet for funktionalanalysen, som er udsprunget af matematikkens anvendelser i kvantemekanik, men som nu har et langt bredere anvendelsesområde.

Vi skal nu se lidt nærmere på det endeligdimensionale tilfælde, men først vil vi vise nogle sætninger om dimension og afbildninger.

Sætning 13.10. For et vektorrum U med et underrum V gælder, at U er endeligdimensionalt, hvis og kun hvis V og $\frac{U}{V}$ begge er endeligdimensionale, og så er

$$\dim U = \dim V + \dim \frac{U}{V} .$$

Bevis. Der findes et underrum $W \subseteq U$ komplementært til V, og $\frac{U}{V}$ er isomorft med W, så vi har $\dim W = \dim \frac{U}{V}$. Derefter følger påstanden af sætning 12.12.

Sætning 13.11. Lad U og V være vektorrum og f: $U \to V$ en lineær afbildning. Så er U endeligdimensionalt, hvis og kun hvis kernf og f(U) begge er endeligdimensionale, og så er

$$\dim U = \dim \text{kern} f + \dim f(U).$$

Bevis. Da f(U) er isomorft med $\frac{U}{\text{kern}U}$ følger påstanden umiddelbart af sætning 13.10.

Sætning 13.12. Hvis U og V er endeligdimensionale vektorrum med samme dimension, og $f:U \to V$ er en lineær afbildning, som er enten injektiv eller surjektiv, da er f bijektiv.

Bevis. Hvis f er injektiv, har f(U) ifølge sætning 13.11 samme dimension som V, og det medfører, at f(U) = V. Hvis f(U) = V, giver sætning 13.11, at dim kernf = 0, altså at f er injektiv. Dermed er sætningen bevist.

Sætning 13.13. Hvis U er endeligdimensionalt, er $\dim U = \dim U^* = \dim U^{**}$, og den naturlige lineære afbildning $\Phi:U \to U^{**}$ er en isomorfi.

Bevis. Ifølge sætning 13.9 er U og U^* isomorfe. Deraf følger, at U, U^* og U^{**} har samme dimension. Den samme sætning fortæller, at Φ er injektiv, og så giver sæt-

ning 13.12, at Φ er bijektiv, altså en isomorfi. Dermed er sætningen bevist.

Sætning 13.14. Lad U være et n-dimensionalt og V et p-dimensionalt vektorrum og $f:U \to V$ en lineær afbildning. Der findes da et tal r, som er $\leqq n$ og $\leqq p$, samt en basis $\{\underline{b}_1,\ldots,\underline{b}_n\}$ for U og en basis $\{\underline{e}_1,\ldots,\underline{e}_p\}$ for V, således at $f(\underline{b}_\nu) = \underline{e}_\nu$ for $\nu = 1,\ldots,r$ og $f(\underline{b}_\nu) = \underline{0}$ for $\nu = r+1,\ldots,n$.

Bevis. Vi vælger $\{\underline{b}_{r+1},\ldots,\underline{b}_n\}$, som en basis for kernf, og $\{\underline{b}_1,\ldots,\underline{b}_r\}$ som en basis for et underrum $W \subseteqq U$ komplementært til kernf. Så er restriktionen $f|W:W \to f(U)$ en isomorfi, og med $\underline{e}_\nu = f(\underline{b}_\nu)$ for $\nu = 1,\ldots,r$, er $\{\underline{e}_1,\ldots,\underline{e}_r\}$ en basis for f(U), og den udvides til en basis $\{\underline{e}_1,\ldots,\underline{e}_p\}$ for V. Det er klart, at disse baser har de i sætningen påståede egenskaber.

Definition 13.15. Lad U og V være vektorrum, og $f:U \to V$ en lineær afbildning. Ved rgf, rangen af f, forstår vi tallet $rgf = dimf(U)$.

Vi bemærker, at rgf netop er det tal r, der optræder i sætning 13. 4. Det er en størrelse, der ikke afhænger af valget af basis. En sådan størrelse siges at være invari-

ant, men det må erindres, at betydningen af "invariant" er afhængig af situationen.

Definition 13.16. Lad U være et vektorrum og $M \subseteq U$ en delmængde. Ved rgM, rangen af M, forstår vi tallet $rgM = \dim spanM$.

For et underrum $V \subseteq U$ har vi således $rgV = \dim V$. Det er kun vektorrum der har en dimension. I rum med mere geometrisk struktur, kan man godt tillægge mere generelle mængder en dimension. Vi er jo vant til at betragte kurver som 1-dimensionale og flader som 2-dimensionale. I en sådan sammenhæng bliver endelige mængder 0-dimensionale, medens en endelig mængde i et vektorrum for det meste vil have positiv rang. Derfor kan vi ikke tillade os at sige dimension i stedet for rang.

Sætning 13.17. Lad U være et underrum, $M \subseteq U$ en vilkårlig delmængde og $B \subseteq M$ en maksimal lineært uafhængig mængde i M. Da er B en basis for $spanM$. Altså er rgM antallet af elementer i en maksimal lineært uafhængig delmængde af M.

Bevis. Hvis B er maksimal i M, er $M \subseteq spanB$, og det medfører, at $spanM \subseteq spanB$, altså $spanM = spanB$. Dermed er påstanden bevist.

Definition 13.18. Lad U være et vektorrum. Et sæt

$(\underline{e}_1,\ldots,\underline{e}_n)$ kaldes en ordnet basis for U, hvis $\{\underline{e}_1,\ldots\underline{e}_n\}$ er en basis for U. Ved den til $(\underline{e}_1,\ldots,\underline{e}_n)$ duale basis for U^*, forstår vi det sæt $(\underline{e}_1^*,\ldots\underline{e}_n^*)$ af vektorer fra U^*, som tilfredsstiller betingelsen $\underline{e}_j^*(\underline{e}_k) = \delta_{jk}$.

Det følger af egenskaberne ved den i sætning 13.9 omtalte bijektive lineære afbildning $\psi:U \to U^*$, at $\{\underline{e}_1^*,\ldots,\underline{e}_n^*\}$ virkelig netop bliver den duale basis til $\{\underline{e}_1,\ldots,\underline{e}_n\}$. I virkeligheden er ordningen irrelevant, medens sammenparringen af elementerne i de to baser er relevant. Når vi alligevel operer med ordnede baser, skyldes det, at de benyttede kommunikationsmidler er af en sådan art, at de af sig selv vil anføre basiselementerne i en rækkefølge. Derfor er det slet ikke nemt at undgå at ordne endelige mængder.

Sætning 13.19. Lad U og V være endeligdimensionale vektorrum og $f:U \to V$ en lineær afbildning. Lad $(\underline{b}_1,\ldots\underline{b}_n)$ være en basis for U med den duale basis $(\underline{b}_1^*,\ldots,\underline{b}_n^*)$ for U^*. Lad $(\underline{e}_1,\ldots,\underline{e}_p)$ være en basis for V med den duale basis $(\underline{e}_1^*,\ldots,\underline{e}_p^*)$ for V^*. Hvis der findes et tal r, således at $f(\underline{b}_\nu) = \underline{e}_\nu$ for $\nu = 1,\ldots,r$ og $f(\underline{b}_\nu) = \underline{0}$ for $\nu = r+1,\ldots,n$, da vil den duale afbildning f^* tilfredsstille betingelsen $f^*(\underline{e}_\nu^*) = \underline{b}_\nu^*$ for $\nu = 1,\ldots,r$ og $f^*(\underline{e}_\nu^*) = \underline{0}$ for $\nu = r+1,\ldots,p$.

Bevis. Vi har $f^*(\underline{e}_j^*)(\underline{b}_k) = (\underline{e}_j^* \circ f)\underline{e}_k = \underline{e}_j^*(f(\underline{b}_k))$. For $k \leq r$ får vi således $f^*(\underline{e}_j^*)(\underline{b}_k) = \underline{e}_j^*(\underline{e}_k) = \delta_{jk}$, og for $k > r$ får vi $f^*(\underline{e}_j^*)(\underline{b}_k) = \underline{e}_j^*(\underline{0}) = 0$, så vi får $f^*(\underline{e}_j)(\underline{b}_k) = \delta_{jk}$, altså $f^*(\underline{e}_j) = \underline{b}_j$, hvis $j \leq r$, medens vi får $f^*(\underline{e}_j)(\underline{b}_k) = 0$, hvis $j > k$. Dermed er sætningen bevist.

Vi har tidligere vist, at vi altid kan vælge baser for U og V, så sætningens betingelser bliver opfyldt. Da tallet r, som optræder i sætningen, er rangen af både f og f^* får vi umiddelbart følgende korollar:

Sætning 13.20. Lad U og V være endeligdimensionale vektorrum og $f:U \to V$ en lineær afbildning. Så har f og dens duale $f^*:V^* \to U$ samme rang.

Idet vi stadig benytter de samme betegnelser, har vi $\text{kern}f = \text{span}\{\underline{b}_{r+1},\ldots,\underline{b}_n\}$, $f(U) = \text{span}\{\underline{e}_1,\ldots,\underline{e}_r\}$ og $\text{kern}f^* = \text{span}\{\underline{e}_{r+1}^*,\ldots,\underline{e}_p^*\}$, $f^*(V^*) = \text{span}\{\underline{b}_1^*,\ldots,\underline{b}_r^*\}$. Heraf fremgår, at $f^*(V^*)$ netop er mængden af linearformer, som afbilder kernf over i $\underline{0}$, medens f(U) netop er mængden af vektorer, som afbildes i 0 ved alle linearformer i $\text{kern}f^*$. Endvidere er $\text{kern}f^*$ netop mængden af linearformer, der afbilder f(U) over i $\underline{0}$, medens kernf er mængden af vektorer, som afbildes i $\underline{0}$ ved alle linearformer i $f^*(V^*)$. Vi har derfor følgende sætning:

Sætning 13.21. Lad U og V være endeligdimensionale vektorrum og $f:U \to V$ en lineær afbildning med den duale afbildning $f^*:V^* \to U^*$. Da gælder følgende 4 relationer.

$$f(U) = \{\underline{v} \in V \mid \forall \underline{\alpha} \in \text{kern} f^* (\underline{\alpha}(\underline{v}) = 0)\}$$

$$f^*(V^*) = \{\underline{\alpha} \in U^* \mid \forall \underline{u} \in \text{kern} f (\underline{\alpha}(\underline{u}) = 0)\}$$

$$\text{kern} f = \{\underline{u} \in U \mid \forall \underline{\alpha} \in f^*(V^*)(\underline{\alpha}(\underline{u}) = 0)\}$$

$$\text{kern} f^* = \{\underline{\alpha} \in V^* \mid \forall \underline{v} \in f(U) \ (\underline{\alpha}(\underline{v}) = 0)\}$$

Som et umiddelbart korollar har vi sætningen

Sætning 13.22. Lad U og V være endeligdimensionale vektorrum. For en afbildning $f:U \to V$ og dens duale $f^*:V^* \to U^*$ gælder da, at en af dem er injektiv, hvis og kun hvis den anden er surjektiv.

Bevis. Lad os antage, at f er injektiv, altså $\text{kern} f = \{\underline{0}\}$. Så giver den anden relation i den foregående sætning, at $f^*(V^*)$ omfatter alle $\underline{\alpha} \in U^*$ som er 0 på $\text{kern} f = \{\underline{0}\}$, men det er jo dem alle, så vi får, at f^* er surjektiv. Hvis f er surjektiv, er $f(U) = V$, og 0-formen er den eneste linearform $\underline{\alpha} \in V^*$, som er $\underline{0}$ på hele f(U). Derfor giver den fjerde betingelse i den foregående sætning, at $\text{kern} f^* = \{\underline{0}\}$, altså at f^* er injektiv. De to sidste tilfælde går helt analogt. Dermed er sætningen bevist.

KAPITEL 14

Matrixregning

Lad U og V være endeligdimensionale vektorrum over et legeme K, som vi ellers ikke vil nævne i dette kapitel, da det skal være det samme hele tiden. Vi vil studere vektorrummet $\mathrm{Hom}(U,V)$ af lineære afbildninger $f:U \to V$. Vi kan vælge en basis $(\underline{b}_1,\ldots,\underline{b}_n)$ for U og en basis $(\underline{e}_1,\ldots\underline{e}_m)$ for V. Så har hvert punkt $\underline{u} \in U$ netop en fremstilling $\underline{u} = x_1\underline{b}_1+\ldots+x_n\underline{b}_n$, og talsættet $(x_1,\ldots,x_n)$ kaldes koordinatsættet for $\underline{u}$ svarende til basis $(\underline{b}_1,\ldots,\underline{b}_n)$. For $\underline{v} \in V$ har vi analogt $\underline{v} = y_1\underline{e}_1+\ldots+y_m\underline{e}_m$, så vi får et koordinatsæt $(y_1,\ldots,y_m)$ for $\underline{v}$ svarende til basis $(\underline{e}_1,\ldots,\underline{e}_m)$. Ved $\varphi(\underline{u}) = (x_1,\ldots,x_n)$, $\psi(\underline{v}) = (y_1,\ldots,y_m)$ defineres isomorfier $\varphi:U \to K^n$; $\psi:V \to K^m$. Ved $\mu(f) = \psi\circ f\circ\varphi^{-1}:K^n \to K^m$ får vi defineret en afbildning $\mu:\mathrm{Hom}(U,V) \to \mathrm{Hom}(L^n,L^m)$. Det er klart, at μ er bijektiv, da vi umiddelbart udleder, at $f = \psi^{-1}\circ\mu(f)\circ\varphi$. Endvidere ses det umiddelbart, at μ er en isomorfi.

Lad os nu antage, at $\underline{u}$ og $\underline{v}$ er valgt, så $\underline{v} = f(\underline{u})$. Nu er $f(\underline{b}_1),\ldots,f(\underline{b}_n)$ vektorer i V, så vi har fremstil-

linger

$$f(\underline{b}_k) = a_{1k}\underline{e}_1+\ldots+a_{mk}\underline{e}_m, \quad k = 1,\ldots,n,$$

og vi får derfor

$$y_1\underline{e}_1+\ldots+y_m\underline{e}_m = \underline{v} = f(\underline{u}) = f(x_1\underline{b}_1+\ldots+x_n\underline{b}_m) =$$

$$x_1f(\underline{b}_1)+\ldots+x_nf(\underline{b}_n) = (\sum_{k=1}^{n} a_{1k}x_k)\underline{e}_1+\ldots+(\sum_{k=1}^{n} a_{mk}x_k)\underline{e}_m.$$

så $\mu(f):L^n \to L^m$ er givet ved ligningerne

$$y_j = a_{j1}x_1+\ldots+a_{jn}x_n, \quad j = 1,\ldots,m.$$

Lad os nu omvendt tænke os, at vi har givet en familie $(c_{jk}|j = 1,\ldots,m;\ k = 1,\ldots,n)$ af elementer af K. Der findes da netop en lineær afbildning $g:U \to V$ med

$$g(\underline{b}_k) = c_{1k}\underline{e}_1+\ldots+c_{mk}\underline{e}_m, \quad k = 1,\ldots,n,$$

så er $\mu(g):L^n \to L^m$ givet ved ligningerne

$$y_j = c_{j1}x_1+\ldots+c_{jn}x_n, \quad j = 1,\ldots,m.$$

Hvis $\hat{M}(K;m,n)$ betegner mængden af alle familier $(h_{jk}|j = 1,\ldots,m;\ k = 1,\ldots,n)$ har vi således bijektive afbildninger $\nu:\mathrm{Hom}(K^n,K^m) \to \hat{M}(K;m,n)$ og $\lambda = \nu\circ\mu:\mathrm{Hom}(U,V) \to \hat{M}(K;m,n)$.

Sætning 14.1. De således definerede afbildninger ν og λ er vektorrumsisomorfier, når $\hat{M}(K;m,n)$ på sædvanlig måde

organiseres som et mn-dimensionalt vektorrum over K.

Bevis. Med de samme betegnelser som ovenfor har vi

$$(f+g)(\underline{b}_k) = f(\underline{b}_k) + g(\underline{b}_k) =$$

$$(a_{1k}+c_{1k})\underline{e}_1+\ldots+(a_{mk}+c_{mk})\underline{e}_m,\ k = 1,\ldots n,$$

hvilket viser, at

$$\lambda(\mu(f)+\mu(g)) = (a_{jk}+c_{jk}|j = 1,\ldots,m;\ k = 1,\ldots n).$$

For $\kappa \in K$ får vi endnu lettere

$$\lambda(\kappa\mu(f)) = (\kappa a_{jk}|j = 1,\ldots,m;\ k = 1,\ldots,n).$$

Dermed er sætningen bevist.

Vi ser således, at Hom(U,V) er et mn-dimensionalt vektorrum over K. Hvis vi for $j = 1,\ldots,m;\ k = 1,\ldots,n$ definerer $\varepsilon_{jk}:U \to V$ ved $\varepsilon_{jk}(\underline{b}_k) = \underline{e}_j$ og $\varepsilon_{jk}(\underline{b}_l) = \underline{0}$ for $l \neq k$, altså

$$\varepsilon_{jk}(x_1\underline{b}_1+\ldots+x_n\underline{b}_n) = x_k\underline{e}_j,$$

er $(\varepsilon_{jk}|j = 1,\ldots,m;\ k = 1,\ldots,n)$ en basis for Hom(U,V).

Et talsæt $(a_{jk}|j = 1,\ldots,m;\ k = 1,\ldots,n)$ kaldes en matrix, eller mere præcist en mxn-matrix med elementer fra K. Vi vil betegne matricer med dobbelt understregede bogstaver, altså $\underline{\underline{A}} = (a_{jk}|j = 1,\ldots,m;\ k = 1,\ldots,n)$. Princi-

pielt er en matrix ikke anderledes end ethvert andet sæt af mn elementer fra K, men vore regninger ovenfor viser, at venstre index j systematisk korresponderer med et basiselement $\underline{b}_k$ fra U, og derfor er det praktisk at skrive matricen som et rektangulært skema

$$\underline{\underline{A}} = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

I overensstemmelse hermed siges a_{jk} at høre til række nummer j og til søjle nummer k. Række nummer j er en vektor $(a_{j1},\ldots,a_{jn}) \in K^n$, medens søjle nummer k er en vektor $(a_{1k},\ldots,a_{mk}) \in K^m$.

Vi vil nu betragte vektorrum U,V og W og en basis $(\underline{e}_1,\ldots,\underline{e}_p)$ for U, en basis $(\underline{e}'_1,\ldots,\underline{e}'_n)$ for V og en basis $(\underline{e}''_1,\ldots,\underline{e}''_m)$ for W. Endvidere betragter vi lineære afbildninger $f:U \to V$ og $g:V \to W$. Vi har isomorfierne $\varphi:U \to K^p$ $\psi:V \to K^n$ og $\chi:W \to K^m$. Vi definerer $\mu(f) = \psi \circ f \circ \varphi^{-1}$ og $\mu'(g):\chi \circ g \circ \psi^{-1}$, så vi har isomorfierne $\mu:\mathrm{Hom}(U,V) \to \mathrm{Hom}(K^p,K^n)$ og $\mu':\mathrm{Hom}(V,W) \to \mathrm{Hom}(K^n,K^m)$. Vi har således følgende diagram af afbildninger

$$\begin{array}{ccccc} U & \xrightarrow{f} & V & \xrightarrow{g} & W \\ \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\psi} & & \downarrow{\scriptstyle\chi} \\ K^p & \xrightarrow{\mu(f)} & K^n & \xrightarrow{\mu'(g)} & K^m. \end{array}$$

Vi har selvfølgelig også en isomorfi $\mu'':\mathrm{Hom}(U,W) \to \mathrm{Hom}(K^p,K^m)$ defineret ved $\mu''(h) = \chi\circ h\circ\varphi^{-1}$. Vi får nu

$$\mu''(g\circ f) = \chi\circ g\circ f\circ\varphi^{-1} = \chi\circ g\circ\psi^{-1}\circ\psi\circ f\circ\varphi^{-1} = \mu'(g)\circ\mu(f).$$

Lad nu $\underline{u} = x_1\underline{e}_1+\ldots+x_p\underline{e}_p \in U$, $\underline{v} = y_1\underline{e}'_1+\ldots+y_n\underline{e}'_n$ og $\underline{w} = z_1\underline{e}''_1+\ldots+z_m\underline{e}''_m$ tilfredsstille ligningerne $\underline{v} = f(\underline{u})$ og $\underline{w} = g(\underline{v})$. Hvis nu de matricer, der svarer til f og g er

$$\underline{\underline{A}} = \begin{pmatrix} a_{11} & \cdots & a_{1p} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{np} \end{pmatrix} \quad \text{og} \quad \underline{\underline{B}} = \begin{pmatrix} b_{11} & \cdots & b_{1m} \\ \vdots & & \vdots \\ b_{m1} & \cdots & b_{mn} \end{pmatrix}$$

medens $g\circ f$ har matricen

$$\underline{\underline{C}} = \begin{pmatrix} c_{11} & \cdots & c_{1p} \\ \vdots & & \vdots \\ c_{m1} & \cdots & c_{mp} \end{pmatrix},$$

har vi

$$y_j = a_{j1}x_1+\ldots+a_{jp}x_p, \quad j = 1,\ldots,n$$

$$z_i = b_{i1}y_1+\ldots+b_{in}y_n, \quad i = 1,\ldots,m$$

$$z_i = c_{i1}x_1+\ldots+c_{ip}x_p, \quad i = 1,\ldots,m.$$

Ved indsætning af udtrykkene for y_j i de første udtryk for z_i får vi ved sammenligning af det andet udtryk for z_i, at

$$c_{ik} = b_{i1}a_{1k}+\ldots+b_{in}a_{nk}.$$

Definition 14.2. Hvis $\underline{\underline{A}} = (a_{jk})$ er en nxp-matrix, og $\underline{\underline{B}} = (b_{ij})$ er en mxn-matrix, definerer vi produktet $\underline{\underline{B}}\,\underline{\underline{A}} = \underline{\underline{C}} = (c_{ik})$ ved

$$c_{ik} = b_{i1}a_{1k}+\ldots+b_{in}a_{nk} = \sum_{j=1}^{n} b_{ij}a_{jk};\ i=1,\ldots,m;\ k=1,\ldots,p.$$

Med denne definition kan resultatet ovenfor udtrykkes i den næste sætning.

Sætning 14.3. Lad U med basis $(\underline{e}_1,\ldots,\underline{e}_p)$ og V med basis $(\underline{e}'_1,\ldots,\underline{e}'_n)$ samt W med basis $(\underline{e}''_1,\ldots,\underline{e}''_m)$ være vektorrum og lad $f:U \to V$ og $g:V \to W$ være lineære afbildninger. Hvis $\underline{\underline{A}}$ er matrix for f og $\underline{\underline{B}}$ er matrix for g, er $\underline{\underline{B}}\,\underline{\underline{A}}$ matrix for $g\circ f$.

Sætning 14.4. Hvis m,n,p og q er naturlige tal, $\underline{\underline{A}}$ er en mxn-matrix, $\underline{\underline{B}}$ er nxp-matrix og $\underline{\underline{C}}$ en pxq-matrix, er $(\underline{\underline{A}}\,\underline{\underline{B}})\,\underline{\underline{C}} = \underline{\underline{A}}\,(\underline{\underline{B}}\,\underline{\underline{C}})$. (Matrix multiplikation er associativ).

Bevis. Vi ved, at $\underline{\underline{C}}$ er matrix for en afbildning $h:K^q \to K^o$, at B er matrix for en afbildning $g:K^p \to K^n$, og at $\underline{\underline{C}}$ er matrix for en afbildning $f:K^n \to K^m$. Så er

$(\underline{\underline{A}}\ \underline{\underline{B}})\ \underline{\underline{C}}$ matrix for $(f\circ g)\circ h: K^q \to K^m$, medens $\underline{\underline{A}}(\underline{\underline{B}}\ \underline{\underline{C}})$ er matrix for $f\circ(g\circ h): K^q \to K^m$. Sætningen følger derefter af, at $(f\circ g)\circ h = f\circ(g\circ h)$.

Mængden $\hat{M}(K)$ af alle matricer med elementer fra K er således organiseret ved en ikke overalt defineret addition, en overalt defineret ydre multiplikation med elementer fra K og en ikke overalt defineret indre multiplikation. Der gælder også distributive love, således som det fremgår af den næste sætning.

Sætning 14.5. Hvis m,n og p er hele tal, $\underline{\underline{A}}$ og $\underline{\underline{B}}$ er mxn-matricer og $\underline{\underline{C}}$ en nxp-matrix er $(\underline{\underline{A}}+\underline{\underline{B}})\underline{\underline{C}} = \underline{\underline{A}}\underline{\underline{C}} + \underline{\underline{B}}\underline{\underline{C}}$. Hvis $\underline{\underline{A}}$ er en mxn-matrix, medens $\underline{\underline{B}}$ og $\underline{\underline{C}}$ er nxp-matricer, er $\underline{\underline{A}}(\underline{\underline{B}}+\underline{\underline{C}}) = \underline{\underline{A}}\underline{\underline{B}} + \underline{\underline{A}}\underline{\underline{C}}$.

Bevis. I det første tilfælde er $\underline{\underline{A}}, \underline{\underline{B}}$ og $\underline{\underline{C}}$ matricer for lineære afbildninger $f: K^n \to K^m$, $g: K^n \to K^m$ og $h: K^p \to K^n$, så sætningen følger af, at $(f+g)\circ h = f\circ h + g\circ h$. Den anden påstand fås analogt.

Vi anfører nogle eksempler på matrixmultiplikation. Først et par eksempler med $K = \mathbb{R}$.

$$\begin{pmatrix} 1 & -1 & 2 \\ 0 & 3 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 2 \\ -1 & -3 \end{pmatrix} = \begin{pmatrix} -3 & -7 \\ 2 & 3 \end{pmatrix}$$

$$\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}\begin{pmatrix}4 & 3\\ 2 & 1\end{pmatrix} = \begin{pmatrix}8 & 5\\ 20 & 13\end{pmatrix},$$

$$\begin{pmatrix}4 & 3\\ 2 & 1\end{pmatrix}\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix} = \begin{pmatrix}13 & 20\\ 5 & 8\end{pmatrix}$$

Vi ser, at produktet af 2×2-matricer ikke er kommutativt.

Vi anfører nogle specielle tilfælde af multiplikation af matricer over et vilkårligt legeme K.

$$(a_1,\ldots,a_n)\begin{pmatrix}b_1\\ \vdots\\ b_n\end{pmatrix} = (a_1b_1+\ldots+a_nb_n),$$

$$\begin{pmatrix}a_1\\ \vdots\\ a_m\end{pmatrix}(b_1,\ldots,b_n) = \begin{pmatrix}a_1b_1 & \cdots & a_1b_n\\ \vdots & & \vdots\\ a_mb_1 & \cdots & a_mb_n\end{pmatrix}.$$

En matrix med kun 1 række kaldes en rækkematrix. En matrix med kun 1 søjle kaldes en søjlematrix. Med 1×1-matrix regnes helt som med elementer fra K, og for $a \in K$ vil vi ofte tillade os at identificere 1×1-matricen (a) med elementet a. Vi må dog huske, at a kan multipliceres med enhver matrix, medens $(\underline{a})\underline{\underline{A}}$ kun har mening, hvis $\underline{\underline{A}}$ er en rækkematrix, og $\underline{\underline{A}}(a)$ kun har mening, når $\underline{\underline{A}}$ er en søjlematrix.

For $n < m$ er inklusionsafbildningen $j:K^n \to K^m$ givet ved, at $j(x_1,\ldots,x_n) = (y_1,\ldots y_m)$ har matrixformen

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} .$$

For $n > m$ har vi en projektion $p:K^n \to K^m$ givet ved $p(x_1,\ldots,x_n) = (x_1,\ldots,x_m) = (y_0,\ldots y_m)$, og på matrixform kan det skrives

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} .$$

For hvert naturligt tal n har vi en enhedsmatrix

$$\underline{\underline{E}}_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

som svarer til den identiske afbildning $\mathrm{id}_{K^n}:K^n \to K^n$. Vi vil ofte skrive $\underline{\underline{E}}$ for $\underline{\underline{E}}_n$, da værdien af index næsten altid vil fremgå af sammenhængen.

Lad U være et vektorrum med basis $(\underline{b}_1,\ldots,\underline{b}_n)$, og lad $(\underline{b}_1^*,\ldots,\underline{b}_n^*)$ være den duale basis for U^*. Lad V være et vektorrum med basis $(\underline{e}_1,\ldots,\underline{e}_m)$, og lad $(\underline{e}_1^*,\ldots,\underline{e}_m^*)$ være den duale basis for V^*. Lad $f:U \to V$ være en lineær

afbildning, og $\underline{\underline{A}}$ dens tilsvarende matrix. Under disse omstændigheder definerer vi.

Definition 14.6. Ved den transponerede matrix $\underline{\underline{A}}'$ til $\underline{\underline{A}}$ forstår vi matrix for den duale afbildning, idet vi benytter de duale baser for vektorrummene.

Den transponerede matrix skulle egentlig betegnes $\underline{\underline{A}}^*$, men det ville komme i konflikt med traditionelle betegnelser i forbindelse med vektorrum over $\mathbb{C}$.

Sætning 14.7. Hvis $\underline{\underline{A}} = (a_{jk} | j = 1,\ldots,m;\ k = 1,\ldots,n)$, er $\underline{\underline{A}}' = (a'_{jk} | j = 1,\ldots,n;\ k = 1,\ldots,m)$, hvor $a'_{jk} = a_{kj}$.

Bevis. Afbildningen $f:U \to V$ er bestemt ved, at

$$f(\underline{b}_k) = a_{1k}\underline{e}_1 + \ldots + a_{mk}\underline{e}_m,\quad k = 1,\ldots,n.$$

Derfor er $f^*(\underline{e}_j^*)(\underline{b}_k) = e_j^*(f(\underline{b}_k)) = a_{jk}$, så vi får

$$f^*(\underline{e}_j^*) = a_{j1}\underline{b}_1^* + \ldots + a_{jn}\underline{b}_n^*,\quad j = 1,\ldots,m$$

og på den anden side har vi jo

$$f^*(\underline{e}_j^*) = a'_{1j}\underline{b}_1^* + \ldots + a'_{nj}\,b_n^*.\quad j = 1,\ldots,m$$

Dermed er sætningen bevist.

Sætning 14.8. Hvis $\underline{\underline{A}}$ og $\underline{\underline{B}}$ er mxn-matricer, og $\lambda \in K$, har vi $(\underline{\underline{A}}+\underline{\underline{B}})' = \underline{\underline{A}}'+\underline{\underline{B}}'$ og $(\lambda\underline{\underline{A}})' = \lambda\underline{\underline{A}}'$. Hvis $\underline{\underline{A}}$ er en mxn-

matrix, og $\underline{\underline{B}}$ en nxp-matrix, er $(\underline{\underline{A}}\ \underline{\underline{B}})' = \underline{\underline{B}}'\underline{\underline{A}}'$.

Bevis. Det følger umiddelbart af de tilsvarende sætninger om duale afbildninger.

Lad Λ være en ring. Vi kan da betragte matricer med elementer fra Λ. Det går helt umiddelbart, at definere summen af mxn-matricer med elementer fra Λ og at definere produkter af sådanne matricer. Derved bliver mængden af mxn-matricer med elementer fra λ både en venstre Λ-modul og en højre Λ-modul, og de to modulstrukturer "kommuterer", idet vi får regnereglen $(\lambda\underline{\underline{A}})\mu = \lambda(\underline{\underline{A}}\mu)$. Hvis G er en venstre Λ-modul, giver det også mening at betragte mxn-matricer $\underline{\underline{A}},\underline{\underline{B}},\ldots$ af elementer af G, og det går pænt at definere addition af sådanne, ligesom også produkter $\lambda\underline{\underline{A}}$ for $\lambda \in \Lambda$ umiddelbart kan defineres, og det er klart, at mængden $\hat{M}(G;m,n)$ af mxn-matricer med elementer fra G bliver en venstre Λ-modul. Hvis $\Gamma = (\gamma_{ij} | i = 1,\ldots,m;\ j = 1,\ldots,n)$ er en mxn-matrix med elementer fra Λ, og $\underline{\underline{A}} = (a_{jk} | j = 1,\ldots,n;\ k = 1,\ldots,p)$ er en nxp-matrix med elementer fra G, kan vi udmærket definere $\underline{\underline{\Gamma}}\ \underline{\underline{A}} = (\gamma_{i1}a_{1k}+\ldots+\gamma_{in}a_{nk} | i = 1,\ldots,m;\ k = 1,\ldots,p)$. Da gælder de regneregler, vi kan håbe på, f.eks.

$$\underline{\underline{\Gamma}}(\underline{\underline{A}}+\underline{\underline{B}}) = \underline{\underline{\Gamma}}\ \underline{\underline{A}}+\underline{\underline{\Gamma}}\ \underline{\underline{B}};\quad (\underline{\underline{\Gamma}}+\underline{\underline{\Delta}})\underline{\underline{A}} = \underline{\underline{\Gamma}}\ \underline{\underline{A}}+\underline{\underline{\Delta}}\ \underline{\underline{A}};\quad (\underline{\underline{\Gamma}}\ \underline{\underline{\Delta}})\underline{\underline{A}} = \underline{\underline{\Gamma}}(\underline{\underline{\Delta}}\ \underline{\underline{A}}).$$

Vi vil vise den sidste relation. Lad os antage, at

$$\underline{\underline{\Gamma}} = (\gamma_{ij} | i = 1,\ldots,m;\ j = 1,\ldots,n)$$

$$\underline{\underline{\Delta}} = (\delta_{jk} | j = 1,\ldots,n;\ k = 1,\ldots,p)$$

$$\underline{\underline{A}} = (a_{kl} | k = 1,\ldots,p;\ l = 1,\ldots,q) .$$

Vi ser da umiddelbart, at $(\underline{\underline{\Gamma\Delta}})\underline{\underline{A}} = \underline{\underline{\Gamma}}(\underline{\underline{\Delta A}}) = (b_{il} | i = 1,\ldots,m;\ l = 1,\ldots,q)$, hvor $b_{il} = \sum_{j=1}^{n} \sum_{k=1}^{p} \gamma_{ij}\delta_{jk}a_{kl}$, og dermed er påstanden vist. Det er klart, at også begrebet "transponeret" matrix kan generaliseres på samme måde og at regnereglerne kommer til at gælde, idet reglen $(\underline{\underline{\Gamma A}})^* = \underline{\underline{A}}^*\underline{\underline{\Gamma}}^*$ dog kun gælder, når Λ er kommutativ, og det samme gælder for den tilsvarende regel for matricer af ringe.

Matrixregning anvendes som et vigtigt hjælpemiddel i teorien for moduler, algebraer og ringe. Vi vil helt holde os til vektorrumsteorien, men vi vil udnytte de foregående bemærkninger ved også at inddrage matricer af vektorer. I et produkt må der højst være én sådan matrix. Som en anvendelse vil vi bemærke, at relationen

$$f(\underline{b}) = a_{1k}\underline{e}_1 + \ldots + a_{mk}\underline{e}_m;\ k = 1,\ldots,n,$$

hvor f er en lineær afbildning $f:U \to V$ med matrix $\underline{\underline{A}}$, medens $(\underline{b}_1,\ldots,\underline{b}_n)$ og $(\underline{e}_1,\ldots,\underline{e}_m)$ er baser for U og V, kan skrives på matrixform

$$(f(\underline{b}_1),\ldots,f(\underline{b}_n)) = (\underline{e}_1,\ldots,\underline{e}_n)\underline{\underline{A}}.$$

Hvis $f(x_1\underline{b}_1 + \ldots + x_n\underline{b}_n) = y_1\underline{e}_1 + \ldots + y_m\underline{e}_m$, får vi

$$(\underline{e}_1,\ldots,\underline{e}_m)\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = (y_1\underline{e}_1+\ldots+y_m\underline{e}_m) = (f(x_1\underline{b}_1+\ldots+x_n\underline{b}_n)) =$$

$$(x_1f(\underline{b}_1)+\ldots+x_nf(\underline{b}_n)) = (f(\underline{b}_1),\ldots f(\underline{b}_n))\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = (\underline{e}_1,\ldots,\underline{e}_m)\underline{\underline{A}}\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},$$

hvilket giver, at

$$\begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix} = \underline{\underline{A}}\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \quad .$$

Regningerne i begyndelsen af dette kapitel kan således nu formuleres som matrixregning. Vi var imidlertid nødt til at gennemføre regningerne for overhovedet at komme i gang med matrixregning. Læg mærke til, hvordan der optræder 1×1-matricer i regningen. Som de optræder her, ville det ikke skade at identificere dem med et element af legemet.

Lad U være et vektorrum med basis $(\underline{e}_1,\ldots,\underline{e}_n)$. En endomorfi $f:U \to U$ svarer til en nxn-matrix $\underline{\underline{A}}$. Nu er vektorrummet $\mathrm{End}U = \mathrm{Hom}(U,U)$ organiseret som en algebra med sammensætning som multiplikation. Derved bliver så også mængden $\hat{M}(K,n,n)$ af nxn-matricer (kvadratiske matricer af orden n) en algebra, den n-dimensionale matrixalgebra over K. Den er associativ, men for $n > 1$ er den ikke kommutativ. Den har enhedsmatrix $\underline{\underline{E}}_n = \underline{\underline{E}}$ som 1-element. For $n > 1$ er der altid 0-divisorer. Således har vi

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Det er en interessant egenskab ved matrixalgebraer, at en énsidig invers altid er en 2-sidig invers, idet vi har følgende sætning:

Sætning 14.9. Hvis nxn-matricer $\underline{\underline{A}}$ og $\underline{\underline{B}}$ med elementer fra legemet K tilfredsstiller betingelsen $\underline{\underline{A}}\,\underline{\underline{B}} = \underline{\underline{E}}$, er de hinandens inverse.

Bevis. Hvis $f,g:K^n \to K^n$ er lineære afbildninger med matricer $\underline{\underline{A}}$ og $\underline{\underline{B}}$, har vi $f \circ g = id_{K^n}$. Det medfører, at g er injektiv og f surjektiv. Men så er f og g bijektive. Som følge deraf har f en invers, og det må jo netop være g. Altså er f og g hinandens inverse, og det medfører, at $\underline{\underline{A}}$ og $\underline{\underline{B}}$ er hinandens inverse.

I overensstemmelse med den jargon, vi bruger i ringteori, vil vi kalde en matrix invertibel, hvis den har en invers, altså hvis den svarer til en bijektiv afbildning. Heraf fremgår, at invertible matricer må være kvadratiske.

Vi vender nu tilbage til studiet af vilkårlige matricer. I en matrix

$$\underline{\underline{A}} = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

er hver række en vektor i K^n, og hver søjle er en vektor i K^m. Vi har nu følgende sætning.

Sætning 14.10. Alle lineære afbildninger $f:U \to V$, som for et eller andet valg af basis har $\underline{\underline{A}}$ som matrix, har samme rang r, og såvel mængden af rækker i $\underline{\underline{A}}$ som mængden af søjler i $\underline{\underline{A}}$ har ligeledes rang r.

Bevis. Valget af baser i U og V giver isomorfier $\varphi:U \to L^n$ og $\psi:V \to L^m$. Afbildningen $\psi \circ f \circ \varphi^{-1}:L^n \to L^m$ har matrix $\underline{\underline{A}}$, og den afbilder basisvektorerne i søjlevektorerne i $\underline{\underline{A}}$. Altså er rangen af f lig med rangen af mængden af søjlerne i $\underline{\underline{A}}$. Dermed har vi vist sætningen på nær påstanden om rækkevektorerne, og den følger umiddelbart, når vi anvender det allerede viste på den duale afbildning $f^*:V^* \to U^*$, idet f har matrix $\underline{\underline{A}}'$ og samme rang som f. Dermed er sætningen bevist.

Definition 14.11. Ved rangen af en matrix $\underline{\underline{A}}$ forstås den i den foregående sætning omtalte rang r.

En $n \times n$ matrix er således invertibel, hvis og kun hvis den har rang n.

Ved numerisk behandling af lineære afbildninger må man arbejde med matricerne. Disse afhænger helt væsentligt af valget af baser, og elementerne i matricerne er derfor størrelser uden nogen fysisk betydning. Det fremgår af den sid-

ste sætning, at rangen af en matrix er invariant, altså uafhængig af valget af baser. Indtil videre er det den eneste invariant, vi har fundet, bortset fra rummenes dimensioner. Nu er invarians et meget relativt begreb. Hvis vi studerer afbildninger $f:U \to V$, afhænger matrix for f af valget af to baser, men ved studiet af $\mathrm{End}U$ optræder der kun ét rum, og så er det rimeligt at nøjes med at kræve invarians overfor valget af kun én basis. Det er et svagere krav, og derfor er det rimeligt at håbe på flere invarianter i dette specielle tilfælde.

Nu kan matricer bruges til beskrivelse af andet end lineære afbildninger, og det vil vise sig, at det afhænger af anvendelsen, hvordan matricer ændres ved skift af basis. I det næste kapitel skal vi omtale nogle afbildninger, som ikke er lineære, men som alligevel beskrives ved hjælp af matricer.

KAPITEL 15

Multilinearformer.

Vi vil stadig holde os til studiet af vektorrum over et legeme K, som vi i øvrigt ikke nævner, da det hele tiden skal være det samme. Vi vil betragte endelig mange vektorrum $U_1,\ldots,U_m$, samt yderligere et vektorrum V. Så har vi et produktrum $U_1 x \ldots x U_m$, og vi vil interessere os for afbildninger $f: U_1 x \ldots x U_m \to V$. Hvis $\underline{a}_1 \in U_1,\ldots,\underline{a}_m \in U_m$ og j er et af tallene $1,\ldots,m$, vil vi definere

$$f_{\underline{a}_1,\ldots,\hat{\underline{a}}_j,\ldots,\underline{a}_m}(\underline{u}) = f(\underline{a}_1,\ldots,\underline{a}_{j-1},\underline{u},\underline{a}_{j+1},\ldots,\underline{a}_m),$$

og derved får vi en afbildning $f_{\underline{a}_1,\ldots,\hat{\underline{a}}_j,\ldots,\underline{a}_m}: U_j \to V$. Vi ser, at $f_{\underline{a}_1,\ldots,\hat{\underline{a}}_j,\ldots,\underline{a}_m}$ er afbildningen f betragtet for $\underline{u}_k$ fastholdt på værdien $\underline{a}_k$ for alle $k \neq j$ eller, mere upræcist, afbildningen f betragtet for fastholdte værdier af de variable på nær $\underline{u}_j$.

Vi følger her et princip, der anvendes en hel del i de eksperimentelle videnskaber, idet vi studerer afbildningen f ved kun at ændre på én variabel ad gangen. Kvantitativt kan det godt lade sig gøre, at få tilstrækkelig viden om f på

den måde, men visse mere kvalitative egenskaber kommer først til syne, når alle de variable får lov at variere samtidigt.

Definition 15.1. Lad $U_1,\ldots,U_m$, samt V være vektorrum. En afbildning $f:U_1 x \ldots x U_m \to V$ kaldes m-lineær, hvis alle afbildninger, der kan fås af f ved at fastholde alle de variable på én nær, bliver lineære. Når værdien af m ikke ønskes nærmere specificeret, siger vi multilineær i stedet for m-lineær.

En 1-lineær afbildning er det samme som en lineær afbildning. Vi siger bilineær i stedet for 2-liniær, trilineær i stedet for 3-lineær, osv.

Sætning 15.2. Lad $f:U_1 \times U_2 \to V$ være bilineær. For $\underline{u}_1,\underline{v}_1 \in U_1$; $\underline{u}_2,\underline{v}_2 \in U_2$; λ_1, μ_1, λ_2, $\mu_2 \in K$ har vi da

$$f(\lambda_1\underline{u}_1+\mu_1\underline{v}_1,\ \lambda_2\underline{u}_2+\mu_2\underline{v}_2) =$$

$$\lambda_1\lambda_2 f(\underline{u}_1,\underline{u}_2)+\lambda_1\mu_2 f(\underline{u}_1,\underline{v}_2)+\mu_1\lambda_2 f(\underline{v}_1,\underline{u}_2)+\mu_1\mu_2 f(\underline{v}_1,\underline{v}_2)\ .$$

Bevis. Da f er lineær for fast $\lambda_1\underline{u}_1+\mu_1\underline{v}_1$, er

$$f(\lambda_1\underline{u}_1+\mu_1\underline{v}_1,\ \lambda_2\underline{u}_2+\mu_2\underline{v}_2) = \lambda_2 f(\lambda_1\underline{u}_1+\mu_1\underline{v}_1,\underline{u}_2)+\mu_2 f(\lambda_1\underline{u}_1+\mu_1\underline{v}_1;\underline{v}_2),$$

og resultatet fremkommer ved at indsætte de relationer, der fås ved at udnytte, at f er lineær for den sidste variabel fastholdt, altså

$$f(\lambda_1\underline{u}_1+\mu_1\underline{v}_1,\underline{u}_2) = \lambda_1 f(\underline{u}_1,\underline{u}_2)+\mu_1 f(\underline{v}_1,\underline{u}_2)$$

og den analoge relation med $\underline{v}_2$ i stedet for $\underline{u}_2$. Dermed er sætningen bevist.

For en m-lineær afbildning $f:U_1x\ldots xU_m \to V$ får vi selvfølgelig helt analogt

$$f(\underline{u}_1,\ldots,\underline{u}_{j-1},\lambda\underline{u}_j+\mu\underline{v}_j,\underline{u}_{j+1},\ldots,\underline{u}_{k-1},\lambda'\underline{u}_k+\mu'\underline{v}_k,\underline{u}_{k+1},\ldots,\underline{u}_m) =$$

$$\lambda\lambda' f(\underline{u}_1,\ldots,\underline{u}_m)+\lambda\mu' f(\underline{u}_1,\ldots,\underline{u}_{k-1},\underline{v}_k,\underline{u}_{k+1},\ldots,\underline{u}_m) +$$

$$\mu\lambda' f(\underline{u}_1,\ldots,\underline{u}_{j-1},\underline{v}_j,\underline{u}_{j+1},\ldots,\underline{u}_m) +$$

$$\mu\mu' f(\underline{u}_1,\ldots,\underline{u}_{j-1},\underline{v}_j,\underline{u}_{j+1},\ldots,\underline{u}_{k-1},\underline{v}_k,\underline{u}_{k+1},\ldots,\underline{u}_m).$$

Vanskeligheden ved det regnestykke er jo kun, at det er lovlig langt at skrive op. Vi vil ofte nøjes med at skrive udførlige formler for bilineære afbildninger.

En lineær afbildning $g:U_1\times U_2 \to V$ er noget helt andet end en bilineær afbildning $f:U_1\times U_2 \to V$. For $\underline{u}_1,\underline{v}_1 \in V_1$, $\underline{u}_2,\underline{v}_2 \in U_2$ og $\lambda,\mu \in K$ får vi

$$f(\lambda\underline{u}_1+\mu\underline{v}_1,\lambda\underline{u}_2+\mu\underline{v}_2) = \lambda^2 f(\underline{u}_1,\underline{u}_2)+\lambda\mu(f(\underline{u}_1,\underline{v}_2)+f(\underline{v}_1,\underline{u}_2))+\mu^2 f(\underline{v}_1,\underline{v}_2),$$

$$g(\lambda\underline{u}_1+\mu\underline{v}_1,\lambda\underline{u}_2+\mu\underline{v}_2) = \lambda g(\underline{u}_1,\underline{u}_2)+\mu g(\underline{v}_1,\underline{v}_2).$$

og det er jo slet ikke det samme. Bortset fra særligt trivielle tilfælde, f.eks. hvis et af rummene er 0-dimensionalt, er $\underline{0}$-afbildningen den eneste afbildning, som er både

lineær og bilineær.

Definition 15.3. En m-lineær afbildning $f:U_1x...xU_m \to K$ kaldes en m-linearform.

Vi siger multilinearform, når vi ikke ønsker at nævne m eksplicit. Vi siger bilinearform for $m = 2$, trilinearform for $m = 3$, quadrilinearform for $m = 4$, osv.

Sætning 15.4. Lad $f:U_1x...xU_m \to V$ være en m-lineær afbildning, og $g:V \to W$ en lineær afbildning. Da er $g\circ f:U_1x...xU_m \to W$ en m-lineær afbildning.

Bevis. Hvis $\tilde{f}:U_j \to V$ fås af f ved at fastholde de variable på nær $\underline{u}_j$, fås $g\circ\tilde{f}$ af $g\circ f$ ved at fastholde de samme variable på de samme værdier. Men $g\circ\tilde{f}$ bliver lineær, da g og $\tilde{f}$ er lineære. Dermed er sætningen bevist.

Sætning 15.5. Hvis $f,g:U_1x...xU_m \to V$ er m-lineære afbildninger er $f+g:U_1x...xU_m \to V$ en m-lineær afbildning. For $\lambda \in K$ er $\lambda f:U_1x...xU_m \to V$ en m-lineær afbildning.

Bevis. Hvis $\tilde{f},\tilde{g}:U_j \to V$ fås af f og g ved at fastholde de variable på nær $\underline{u}_j$, fås $\tilde{f}+\tilde{g}$ af f+g på samme måde, og $\tilde{f}+\tilde{g}:U_j \to V$ bliver lineær, da $\tilde{f}$ og $\tilde{g}$ er lineære.

Heraf følger den første påstand. Den anden vises på samme måde.

Mængden af m-lineære afbildninger $f:U_1x...xU_m \to V$ er således et vektorrum over K med sædvanlig addition og multiplikation med elementer af K.

Bortset fra $\underline{0}$-afbildningen har vi endnu ikke givet eksempler på m-lineære afbildninger for $m > 1$, så vi ved ikke engang, om der findes nogen. Det gør der nu altid, og i det endeligdimensionale tilfælde kan vi endda opnå at få et vist overblik over dem, ligesom vi kunne opnå det samme for lineære afbildninger ved hjælp af matricer. Vi vil først reducere problemet til studiet af linearformer.

Sætning 15.6. Lad $f:U_1x...xU_m \to V$ være en m-lineær afbildning og lad $\underline{e}_1,...,\underline{e}_p$ være en basis for V. Da findes der m-linearformer $f^k:U_1x...xU_m \to K$, $k = 1,...,m$, således at vi for alle $(\underline{u}_1,...,\underline{u}_m) \in U_1x...xU_m$ har relationen

$$f(\underline{u}_1,...,\underline{u}_m) = f^1(\underline{u}_1,...,\underline{u}_m)\underline{e}_1+...+f^p(\underline{u}_1,...,\underline{u}_p)\underline{e}_n.$$

På den anden side vil denne relation for vilkårligt valg af m-linearformerne $f^1,...,f^p$ definere en m-lineær afbildning $f:U_1x...xU_m \to V$.

Bevis. Idet $p_k:V \to K$ er den ved $p_k(x_1\underline{e}_1+...+x_p\underline{e}_p) = x_k$ definerede projektion, er $f^k = p_k \circ f$ en m-linearform,

og med denne definition af f^k for $k = 1,\ldots,p$ kommer den i sætningen anførte relation til at gælde. Hvis $j_k:K \to V$ er den ved $j_k(x) = x\underline{e}_k$ definerede inklusion, og f^k er en m-linearform, er $j_k \circ f^k:U_1 x \ldots x U_m \to V$ en m-lineær afbildning. Heraf følger, at udtrykket på højre side af relationen i sætningen for vilkårligt valg af m-linearformerne $f^1,\ldots,f^p$ bliver en sum af p m-lineære afbildninger, altså en m-lineær afbildning.

Sætning 15.7. Lad $f:U_1 x \ldots x U_m \to K$ være en m-linearform, og lad $(\underline{b}_1,\ldots,\underline{b}_n)$ være en basis for U_m. Der findes da m-1-linearformer $f_\nu:U_1 x \ldots x U_{m-1} \to K$, $\nu = 1,\ldots,n$, for hvilke vi for alle $(\underline{u}_1,\ldots,\underline{u}_m) \in K$, hvor $\underline{u}_m = \lambda_1\underline{b}_1 + \ldots+\lambda_n\underline{b}_n$, $\lambda_1,\ldots,\lambda_n \in K$, har relationen

$$f(\underline{u}_1,\ldots,\underline{u}_m) = \lambda_1 f_1(\underline{u} ,\ldots,\underline{u}_{m-1})+\ldots+\lambda_n f_n(\underline{u}_1,\ldots,\underline{u}_{m-1}) .$$

Hvis $f_1,\ldots,f_n:U_1 x \ldots x U_{m-1}$ er vilkårlige m-1-linearformer, vil relationen definere en m-linearform $f:U_1 x \ldots x U_m \to K$.

Bevis. Vi definerer $f_\nu(\underline{u}_1,\ldots,\underline{u}_{m-1}) = f(\underline{u}_1,\ldots,\underline{u}_{m-1}, \underline{b}_\nu)$, $\nu = 1,\ldots,n$. Det er klart, at f_ν bliver lineær i hver variabel, altså en m-1-linearform. Relationen gælder, fordi f er lineær i $\underline{u}_m$ for fastholdte værdier af $\underline{u}_1,\ldots,\underline{u}_{m-1}$. Dermed er den første påstand bevist. Hvis $f_1,\ldots,f_n$ er m-1-linearformer, og f defineres ved relationen, er det klart, at f bliver lineær i hver af de variable, altså en m-linearform. Dermed er sætningen bevist.

Sætning 15.8. Lad U være et vektorrum med basis $\underline{e}'_1,\ldots,\underline{e}'_n$. For enhver matrix $\underline{\underline{A}} = (a_{jk} | j = 1,\ldots,m;\ k = 1,\ldots,n)$ definerer

$$f(x_1\underline{e}_1+\ldots+x_m\underline{e}_m,\ y_1\underline{e}'_1+\ldots+y_n\underline{e}'_n) = (x_1,\ldots,x_m)\underline{\underline{A}}\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

en bilinearform $f:U\times V \to K$, og til enhver sådan bilinearform svarer der netop én matrix $\underline{\underline{A}}$ ved hjælp af hvilken den kan udtrykkes som anført.

Bevis. Det ses umiddelbart, at f defineret ved det anførte udtryk bliver lineær i hver variabel. Hvis $f:U\times V \to K$ er en bilinearform, kan f ifølge den foregående sætning udtrykkes på formen

$$f(x_1\underline{e}_1+\ldots+x_m\underline{e}_m,\underline{v}) = x_1f_1(\underline{v})+\ldots+x_mf_m(\underline{v}),$$

hvor $f_1,\ldots,f_m$ er linearformer, så vi har udtryk

$$f_j(y_1\underline{e}'_1+\ldots+y_n\underline{e}'_n) = a_{j1}y_1+\ldots+a_{jn}y_n,\ j = 1,\ldots,m.$$

Heraf følger påstanden umiddelbart.

En bilinearform er således givet ved et udtryk af formen

$$\sum_{j=1}^{m}\sum_{k=1}^{n} a_{jk}x_jy_k = (x_1,\ldots,x_m)\underline{\underline{A}}\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = (y_1,\ldots,y_n)\underline{\underline{A}}'\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}.$$

Den udtrykkes altså lige godt ved matricen $\underline{\underline{A}}$ og ved dens transponerede matrix $\underline{\underline{A}}'$.

Det volder ikke vanskeligheder at gennemføre det analoge for en trilinearform. Det vil føre til et udtryk af formen

$$\sum_{i=1}^{l} \sum_{j=1}^{m} \sum_{k=1}^{n} a_{ijk} x_i y_j z_k,$$

og det kan altså ikke udtrykkes ved en matrix. Så måtte man i hvert fald indføre tredimensionale matricer, og det er ikke typografisk tilfredsstillende.

For en multilinearform $f: U_1 x \ldots x U_m \to K$, hvor U_ν har basis $(\underline{e}_1^\nu, \ldots, \underline{e}_n^\nu)$, $\nu = 1, \ldots, m$, får vi for $\underline{u}_\nu = x_1^\nu \underline{e}_1^\nu + \ldots + x_{n_\nu}^\nu \underline{e}_{n_\nu}^\nu$, at $f(\underline{u}_1, \ldots, \underline{u}_m)$ er givet ved et udtryk af formen

$$\sum_{j_1=1}^{n_1} \ldots \sum_{j_m=1}^{n_m} a_{j_1,\ldots,j_m} x_{j_1}^1 \ldots x_{j_m}^m$$

For en multilineær afbildning $f: U_1 x \ldots x U_m \to V$, hvor V har basis $\underline{b}_1, \ldots, \underline{b}_p$, og hvor vi iøvrigt bruger de samme betegnelser som før, gælder, at $f(\underline{u}_1, \ldots, \underline{u}_m) = y_1 \underline{b}_1 + \ldots + y_p \underline{b}_p$, hvor

$$y_k = \sum_{j_1=1}^{n_1} \ldots \sum_{j_m=1}^{n_m} a^k_{j_1,\ldots,j_m} x_{j_1}^1 \ldots x_{j_m}^m, \quad k = 1, \ldots, p.$$

Som koefficienter i multilineære afbildninger får vi således systemer med flere indices af elementer fra K. Matricerne er bare det enkleste eksempel på sådanne skemaer.

Multilinearformerne $f:U_1x...xU_m \to V$ er invariante i den forstand, at de er uafhængige af valget af baser for vektorrummene $U_1,...,U_n$ og V. På den anden side afhænger begrebet multilinearform væsentlig af, hvordan vektorrummet $U_1x...xU_m$ er skrevet som produkt af m vektorrum. Til gengæld afhænger koefficenterne $a^k_{j1,...,jm}$ væsentligt af valget af baser for vektorrummene.

Definition 15.9. Lad U og V være vektorrum. Ved en dualitet mellem U og V forstås en bilinearform $\varphi:U\times V \to K$ med den egenskab, at der for hver vektor $\underline{u} \in U\setminus\{\underline{0}\}$ findes en vektor $\underline{v} \in V$ med $\varphi(\underline{u},\underline{v}) \neq 0$, og at der for hver vektor $\underline{v} \in V\setminus\{\underline{0}\}$ findes en vektor $\underline{u} \in U$ med $\varphi(\underline{u},\underline{v}) \neq 0$.

Som et eksempel kan vi se på et vektorrum U og dets duale vektorrum U^*. For $\underline{u} \in U$, $\underline{u}^* \in U^*$ definerer vi $\varphi(\underline{u},\underline{u}^*) = \underline{u}^*(\underline{u})$. Vi ved jo, at $\underline{u}^* \neq \underline{0}$ netop betyder, at $\underline{u}^*$ ikke er 0-formen, altså at der findes en vektor $\underline{u} \in U$ med $\underline{u}^*(\underline{u}) \neq 0$. Det er lidt mere subtilt, at vi for $\underline{u} \in U$, $\underline{u} \neq \underline{0}$ kan finde en linearform $\underline{u}^*$ med $\underline{u}^*(\underline{u}) \neq 0$, men det følger af sætning 13.4.

Sætning 15.10. Lad U og V være vektorrum, og $\varphi: U \times V \to K$ en dualitet. Så kan vi ved $\lambda_1(\underline{u}) = \varphi_{\underline{u}}: V \to K$ definere en injektiv lineær afbildning $\lambda_1: U \to V^*$. Analogt giver $\lambda_2(\underline{v}) = \varphi_{\underline{v}}: U \to K$ en injektiv lineær afbildning $\lambda_2: V \to U^*$.

Bevis. Vi minder om, at $\varphi_{\underline{u}}$ defineres ved $\varphi_{\underline{u}}(\underline{v}) = \varphi(\underline{u},\underline{v})$. Deraf fremgår, at $\varphi_{\underline{u}} \in V^*$, og det ses umiddelbart, at λ_1 er en homomorfi. At φ er en dualitet medfører, at $\varphi_{\underline{u}}$ ikke er 0-formen, hvis $\underline{u} \neq 0$, altså at kern $\lambda_1 = \{\underline{0}\}$, men det medfører netop, at λ_1 er injektiv. Det går analogt med λ_2. Dermed er sætningen bevist.

Sætning 15.11. De i den foregående sætning omtalte lineære afbildninger λ_1 og λ_2 er begge isomorfier, hvis og kun hvis U og V er endeligdimensionale.

Bevis. Hvis λ_1 og λ_2 er isomorfier er V isomorft med U^* og U isomorft med V^* altså med U^{**}, og vi har tidligere set, at det medfører, at U er endeligdimensionalt, og så er U^* og dermed V også endeligdimensionalt. Hvis U og V er endeligdimensionale er $\dim U^* = \dim U$ og $\dim V^* = \dim V$, men da λ_1 og λ_2 er injektive, er $\dim V \leq \dim U$ og $\dim U \leq \dim V^*$. Heraf følger, at U, V, U^* og V^* har samme dimension. Men så er λ_1 og λ_2 bijektive, da de er injektive. Dermed er sætningen bevist.

I det endeligdimensionale tilfælde realiserer en dualitet $\varphi: U \times V \to K$ således hvert af rummene U og V som en kopi af det andets duale rum. Ved udnyttelse af dette synspunkt får vi U og V som gensidigt duale, så vi får "dual med" som en symmetrisk relation. En sådan symmetrisk dualitetsrelation kan også godt bestå mellem uendeligdimensionale rum, men det bliver noget helt andet end den sædvanlige relation mellem et vektorrum og dets duale.

Definition 15.12. Ved en m-linearform på et vektorrum U forstår vi en m-linearform $\varphi: U^m = U \times \ldots \times U \to K$. Hvis φ er en sådan m-linearform, kaldes den ved $\tilde{\varphi}(\underline{u}) = \varphi(\underline{u}, \ldots, \underline{u})$ definerede afbildning $\tilde{\varphi}: U \to K$ en form af grad n på U.

En form af grad 1 er en linearform. En form af grad 2 kaldes en kvadratisk form. En form af grad 3 kaldes en kubisk form.

For $U = K$ har m-linearformer for $m = 1, 2$ og 3 følgende udseende:

$$ax,\ axy,\ axyz.$$

En form af grad p har udseende som ax^p.

For $U = K^2$ opskriver vi m-linearformer for $m = 1,2,3$:

$$a_1x_1+a_2x_2;\ a_{11}x_1y_1+a_{12}x_1y_2+a_{21}x_2y_1+a_{22}x_2y_2;$$

$$a_{111}x_1y_1z_1+a_{112}x_1y_1z_2+a_{121}x_1y_2z_1+a_{122}x_1y_2z_2+a_{211}x_2y_1z_1+$$
$$a_{212}x_2y_1z_2+a_{221}x_2y_2z_1+a_{222}x_2y_2z_2.$$

Former af grader 1,2 og 3 har følgende udseende:

$$a_1x_1+a_2x_2;\quad a_{11}x_1^2+2a_{12}x_1x_2+a_{22}x_2^2;$$

$$a_{111}x_1^3+3a_{112}x_1^2x_2+3a_{122}x_1x_2^2+a_{222}x_2^3.$$

Med forenklede betegnelser opskriver vi generelle kvadratiske og kubiske former i tre variable

$$a_1x_1^2+a_2x_2^2+a_3x_3^2+b_1x_2x_3+b_2x_3x_1+b_3x_1x_2.$$

$$a_1x_1^3+a_2x_2^3+a_3x_3^3+b_1x_1^2x_2+b_2x_1^2x_3+b_3x_1x_2^2+b_4x_2^2x_3+$$
$$b_5x_1x_3^2+b_6x_2x_3^2+cx_1x_2x_3.$$

I tilfældet $U = K^2$ har vi skrevet $2a_{12}$ for $a_{12}+a_{21}$, endvidere $3a_{112}$ for $a_{112}+a_{121}+a_{211}$ og $3a_{122}$ for $a_{122}+a_{212}+a_{221}$. Det svarer til, at vi regner med, at koefficientsættene har symmetriegenskaber, så koefficienter er ens, når de fås af hinanden ved permutation af indices. For karakteristik 2 er $2 = 0$ og for karakteristik 3 er $3 = 0$, og i disse til-

fælde bliver den ene eller den anden af de anførte former ikke helt generelle.

Definition 15.13. En m-lineær afbildning $f:U^m \to V$ kaldes symmetrisk, når det for enhver permutation $p \in S_m$ gælder, at $f(\underline{u}_1,\ldots,\underline{u}_m) = f(\underline{u}_{p(1)},\ldots,\underline{u}_{p(m)})$ for alle $\underline{u}_1,\ldots,\underline{u}_m \in U$.

Det kommer ud på, at f ikke ændrer værdi ved permutation af de variable. Hvis vi tænker os f givet ved et sæt ligninger

$$y_k = \sum_{j_1,\ldots,j_m=1}^{n} a^k_{j_1,\ldots,j_m} x^1_{j_1}\cdots x^m_{j_m},\ k = 1,\ldots,p,$$

kommer symmetri ud på, at koefficienter, der fås af hinanden ved permutation af indices $j_1,\ldots,j_m$, er indbyrdes lige store.

Lad $f:U^2 \to V$ være bilineær. For $\underline{u}_1,\underline{u}_2 \in U$ får vi da

$$f(\underline{u}+\underline{v},\underline{u}+\underline{v}) = f(\underline{u},\underline{u})+f(\underline{u},\underline{v})+f(\underline{v},\underline{u})+f(\underline{v},\underline{v})$$

$$f(\underline{u}-\underline{v},\underline{u}-\underline{v}) = f(\underline{u},\underline{u})-f(\underline{u},\underline{v})-f(\underline{u},\underline{v})+f(\underline{v},\underline{v}).$$

Ved subtraktion får vi

$$2(f(\underline{u},\underline{v})+f(\underline{v},\underline{u})) = f(\underline{u}+\underline{v},\underline{u}+\underline{v})-f(\underline{u}-\underline{v},\underline{u}-\underline{v}).$$

Hvis nu f er symmetrisk og K ikke har karakteristik 2, får vi heraf

$$f(\underline{u},\underline{v}) = \tfrac{1}{4}(f(\underline{u}+\underline{v},\underline{u}+\underline{v})-f(\underline{u}-\underline{v},\underline{u}-\underline{v})).$$

Heraf fremgår, at en symmetrisk bilinearform er fastlagt ved den tilsvarende kvadratiske form, hvis legemet blot ikke har karakteristik 2.

Der er endnu en omfattende klasse af m-lineære afbildninger, som har særlig interesse. Det må indrømmes, at det er svært at forklare lige nu, hvad denne særlige interesse består i, men vi vil få at se, at de efterhånden kommer til at optræde i sammenhæng med flere og flere problemer. Den symmetriske gruppe S_n af permutationer $p: \{1,\ldots,n\} \to \{1,\ldots,n\}$ kommer til at optræde, og vi minder om, at permutationer falder i to klasser, idet vi har en homomorfi $\varepsilon: S_n \to \{-1,1\}$. For en permutation p har vi $\varepsilon(p) = 1$, hvis permutationen kan sammensættes af et lige antal simple ombytninger, og vi har $\varepsilon(p) = -1$, hvis permutationen kan sammensættes af et ulige antal simple ombytninger. Efter denne korte dvælen ved fortiden definerer vi det nye begreb.

<u>Definition 15.14</u>. En m-lineær afbildning $f: U^m \to V$ kaldes alternerende, hvis det for enhver permutation $p \in S_n$ og alle $\underline{u}_1,\ldots,\underline{u}_m \in U$ gælder, at

$$f(\underline{u}_{p(1)},\ldots,\underline{u}_{p(m)}) = \varepsilon(p) f(\underline{u}_1,\ldots,\underline{u}_m).$$

Hvis K har karakteristik 2, er der slet ingen forskel

på symmetriske og alternerende lineære afbildninger. Hvis K ikke har karakteristik 2, er $\underline{0}$-afbildningen den eneste m-lineære afbildning, der er både symmetrisk og alternerende. Lineære afbildninger (tilfældet m=1) er alle symmetriske.

For bilineære afbildninger siger man oftest "antisymmetrisk" eller "skævsymmetrisk" i stedet for alternerende.

Sætning 15.15. Lad $f:U^m \to V$ være en m-lineær afbildning. Da er f alternerende, hvis og kun hvis $f(\underline{u}_1,\ldots,\underline{u}_m)$ for alle $\underline{u}_1,\ldots,\underline{u}_m \in U$ skifter fortegn ved enhver ombytning af to af de variable.

Bevis. Det følger umiddelbart af, at enhver permutation p er sammensætning af simple ombytninger, hvis antal bliver lige hvis $\varepsilon(p) = 1$, men ulige, hvis $\varepsilon(p) = -1$.

Sætning 15.16. Lad U og V være vektorrum over et legeme K, der ikke har karakteristik 2. Så er en m-lineær afbildning $f:U^m \to V$ alternerende, hvis og kun hvis det for alle sæt $(\underline{u}_1,\ldots,\underline{u}_m)$ af vektorer, blandt hvilke mindst 2 er ens, gælder, at $f(\underline{u}_1,\ldots,\underline{u}_m) = \underline{0}$.

Bevis. Lad os antage, at $\underline{u}_j = \underline{u}_k$ og $j \neq k$. Så skal $f(\underline{u}_1,\ldots,\underline{u}_m)$ både skifte fortegn og forblive uændret ved ombytning af $\underline{u}_j$ og $\underline{u}_k$, og når K ikke har karakteristik 2, kræver det, at $f(\underline{u}_1,\ldots,\underline{u}_m) = \underline{0}$. Lad os dernæst antage, at

$f(\underline{u}_1,\ldots,\underline{u}_m) = \underline{0}$, når to af de variable er ens. For $j \neq k$ får vi da, idet vi helt snyder for at skrive de øvrige variable, som bare er statister

$$0 = f(\underline{u}_j+\underline{u}_k,\underline{u}_j+\underline{u}_k) = f(\underline{u}_j,\underline{u}_j)+f(\underline{u}_j,\underline{u}_k)+f(\underline{u}_k,\underline{u}_j)+f(\underline{u}_k,\underline{u}_k) =$$

$$f(\underline{u}_j,\underline{u}_k)+f(\underline{u}_k,\underline{u}_j),$$

hvilket netop viser, at f skifter fortegn, når $\underline{u}_j$ og $\underline{u}_k$ byttes. Dermed er sætningen bevist.

Definition 15.17. En matrix $\underline{\underline{A}}$ kaldes symmetrisk, hvis $\underline{\underline{A}} = \underline{\underline{A}}'$, og skævsymmetrisk, hvis $\underline{\underline{A}} = -\underline{\underline{A}}'$.

Symmetriske og skævsymmetriske matricer er kvadratiske. En mxm-matrix $\underline{\underline{A}} = (a_{jk}|j,k = 1,\ldots,m)$ er symmetrisk, hvis $a_{jk} = a_{kj}$ for alle j og k. Den er skævsymmetrisk, hvis $a_{jk} = -a_{kj}$ for alle j og k. For matricer med elementer fra et legeme med karakteristik 2 gælder, at symmetrisk er ensbetydende med skævsymmetrisk. Hvis legemet ikke har karakteristik 2, er 0-matrix den eneste mxm-matrix, der er både symmetrisk og skævsymmetrisk, og i en skævsymmetrisk matrix gælder, at diagonalelementerne a_{jj} alle er 0.

Sætning 15.18. En symmetrisk bilinearform $f:U^2 \to K$ har symmetrisk matrix for ethvert valg af basis for U. Hvis der findes en basis for U, for hvilken bilinearformen $f:U^2 \to K$ har en symmetrisk matrix, er f symmetrisk.

Bevis. For basis $(\underline{e}_1,\ldots,\underline{e}_n)$ har f en matrix $\underline{\underline{A}}$, og for $\underline{u} = x_1\underline{e}_1+\ldots+x_n\underline{e}_n$ og $\underline{v} = y_1\underline{e}_1+\ldots y_n\underline{e}_n$, er

$$(f(\underline{u},\underline{v})) = (x_1,\ldots,x_n)\underline{\underline{A}}\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = (y_1,\ldots,y_n)\underline{\underline{A}}'\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Hvis f skal forblive uændret ved ombytning af $\underline{u}$ og $\underline{v}$, må vi således have $\underline{\underline{A}} = \underline{\underline{A}}'$. Hvis $\underline{\underline{A}} = \underline{\underline{A}}'$ forbliver $f(\underline{u},\underline{v})$ uændret ved ombytning af $\underline{u}$ og $\underline{v}$. Dermed er sætningen bevist.

Sætning 15.19. En skævsymmetrisk bilinearform $f:U^2 \to K$ har skævsymmetrisk matrix for ethvert valg af basis for U. Hvis der findes en basis for U, for hvilken bilinearformen $f:U^2 \to K$ har en skævsymmetrisk matrix, er f skævsymmetrisk.

Beviset kopieres efter det foregående under tilføjelse af et par minustegn.

Sætning 15.20. Vektorrummet $\hat{B}(U)$ af bilinearformer $f:U^2 \to K$, hvor K ikke har karakteristik 2, er direkte sum af underrummet $\hat{B}_S(U)$ af symmetriske bilinearformer og underrummet $\hat{B}_A(U)$ af skævsymmetriske bilinearformer.

Bevis. Det er klart, at $\hat{B}_S(U)$ og $\hat{B}_A(U)$ virkelig er underrum. Vi har allerede set, at de kun har 0-formen fælles,

så deres sum er direkte sum. Vi mangler blot at vise, at enhver bilinearform $f:U^2 \to K$ er sum af en symmetrisk bilinearform og en skævsymmetrisk bilinearform. Som den symmetriske bilinearform vælger vi $f_S:U^2 \to K$ defineret ved

$$f_S(\underline{u},\underline{v}) = \tfrac{1}{2}(f(\underline{u},\underline{v})+f(\underline{v},\underline{u})),$$

og som den skævsymmetriske bilinearform vælger vi $f_A:U^2 \to K$ defineret ved

$$f_A(\underline{u},\underline{v}) = \tfrac{1}{2}(f(\underline{u},\underline{v})-f(\underline{v},\underline{u})).$$

Dermed er sætningen vist.

Analogt får vi selvfølgelig, at vektorrummet $\hat{M}(K;m,m)$ af mxm-matricer med elementer fra K er direkte sum af underrummet af symmetriske matricer og underrummet af skævsymmetriske matricer.

KAPITEL 16

Determinant.

Lad U være et vektorrum med basis $(\underline{e}_1,\ldots,\underline{e}_n)$, og lad $f:U^n \to K$ være en alternerende n-linearform. Vi betragter vilkårlige vektorer $\underline{u}_1,\ldots,\underline{u}_n \in U$. Vi har da en n×n matrix $\underline{\underline{A}} = (a_{jk})$, således at

$$(\underline{u}_1,\ldots,\underline{u}_n) = (\underline{e}_1,\ldots,\underline{e}_n)\underline{\underline{A}},$$

altså

$$\underline{u}_k = a_{1k}\underline{e}_1+\ldots+a_{nk}\underline{e}_n = \sum_{j=1}^{n} a_{jk}\underline{e}_j.$$

Vi vil udtrykke $f(\underline{u}_1,\ldots,\underline{u}_n)$ ved $f(\underline{e}_1,\ldots,\underline{e}_n)$. Ved at udnytte at f er n-lineær, får vi

$$f(\underline{u}_1,\ldots,\underline{u}_n) = \sum_{j_1,\ldots,j_n=1}^{n} a_{j_1 1},\ldots,a_{j_n n}\, f(\underline{e}_{j_1},\ldots,\underline{e}_{j_n}).$$

Nu har vi $f(\underline{e}_{j_1},\ldots,\underline{e}_{j_n}) = 0$, hvis ikke $j_1,\ldots,j_n$ er indbyrdes forskellige, altså hvis ikke der findes en permutation $p: \{1,\ldots,n\} \to \{1,\ldots,n\}$ med $p(\nu) = j_\nu$ for $\nu = 1,\ldots,n$. Vi får derfor

$$f(\underline{u}_1,\ldots,\underline{u}_n) = \sum_{p\in S_n} a_{p(1),1}\cdots a_{p(n),n}\, f(\underline{e}_{p(1)},\ldots,\underline{e}_{p(n)}).$$

Da f er alternerende, har vi

$$f(\underline{e}_{p(1)},\ldots,\underline{e}_{p(n)}) = \varepsilon(p)f(\underline{e}_1,\ldots,\underline{e}_n),$$

og idet vi indfører betegnelsen

$$\det \underline{\underline{A}} = \sum_{p\in S_n} \varepsilon(p)a_{p(1),1}\cdots a_{p(n),n},$$

får vi

$$f(\underline{u}_1,\ldots,\underline{u}_n) = f(\underline{e}_1,\ldots,\underline{e}_n)\det \underline{\underline{A}}.$$

Definition 16.1. Ved determinanten af n×n-matricen $\underline{\underline{A}}$ forstår vi den ovenfor indførte størrelse $\det \underline{\underline{A}}$.

I regningen ovenfor benyttede vi ikke, at $\underline{e}_1,\ldots,\underline{e}_n$ var lineært uafhængige, men vi benyttede, at $\underline{u}_1,\ldots,\underline{u}_n \in \operatorname{span}(\underline{e}_1,\ldots,\underline{e}_n)$. Vi kan derfor udtrykke resultatet af regningen i følgende sætning.

Sætning 16.2. Lad U være et vektorrum, $f:U^n \to K$ en n-linearform, $\underline{u}_1,\ldots,\underline{u}_n \in U$ vilkårlige vektorer, $\underline{\underline{A}}$ en n×n-matrix og lad $\underline{v}_1,\ldots,\underline{v}_n \in U$ være bestemte ved

$$(\underline{v}_1,\ldots,\underline{v}_n) = (\underline{u}_1,\ldots,\underline{u}_n)\cdot\underline{\underline{A}}.$$

Da er

$$f(\underline{v}_1,\ldots,\underline{v}_n) = f(\underline{u}_1,\ldots,\underline{u}_n)\cdot\det \underline{\underline{A}}.$$

Dette her ville være ganske uinteressant, hvis der ikke fandtes andre alternerende n-linearformer $f:U^n \to K$ end 0-formen. Derfor er det væsentligt at vise, at der findes fra 0 forskellige alternerende n-linearformer $f:U^n \to K$ hvis U har tilstrækkelig høj dimension. Vi har følgende sætning:

Sætning 16.3. Lad U være et vektorrum med basis $(\underline{e}_1,\ldots,\underline{e}_n)$, og lad $\kappa \in K$ være et vilkårligt element. Der findes da netop én alternerende n-linearform $f:U^n \to K$ med $f(\underline{e}_1,\ldots,\underline{e}_n) = \kappa$, og den er bestemt ved, at vi for enhver n×n-matrix $\underline{\underline{A}}$ og $(\underline{u}_1,\ldots,\underline{u}_n) = (\underline{e}_1,\ldots,\underline{e}_n)A$ har $f(\underline{u}_1,\ldots,\underline{u}_n) = \kappa \det A$.

Bevis. Det fremgår af den foregående sætning, at en n-linearform $f:U^n \to K$ med $f(\underline{e}_1,\ldots,\underline{e}_n) = \kappa$ må tilfredsstille ligningen $f(\underline{u}_1,\ldots,\underline{u}_n) = \kappa \det \underline{\underline{A}}$. Da hvert sæt $(\underline{u}_1,\ldots,\underline{u}_n) \in V$ på netop én måde kan skrives som $(\underline{e}_1,\ldots,\underline{e}_n)\underline{\underline{A}}$, definerer relationen $f(\underline{u}_1,\ldots,\underline{u}_n) = \kappa \det \underline{\underline{A}}$ i hvert fald en afbildning $f:U^n \to K$, og det er den eneste afbildning, der kan tænkes at være en alternerende n-linearform med den ønskede egenskab. Vi får umiddelbart af definitionen, at $\det \underline{\underline{E}} = 1$, så f tilfredsstiller betingelsen $f(\underline{e}_1,\ldots,\underline{e}_n) = \kappa$.

Vi mangler at vise, at f er en alternerende n-linearform. Vi betragter $(\underline{u}_1,\ldots,\underline{u}_n) = (\underline{e}_1,\ldots,\underline{e}_n)\underline{\underline{\tilde{A}}}$, hvor $\underline{\underline{\tilde{A}}}$ blot

afviger fra A ved at den k^{te} søjle har andre elementer $a'_{1k},\ldots,a'_{nk}$. Til $(\underline{u}_1,\ldots,\underline{u}_{k-1}, \underline{u}_k+\underline{u}'_k, \underline{u}_{k+1},\ldots,\underline{u}_n)$ hører en matrix $\underline{\underline{A}}$, som kun afviger fra $\underline{\underline{A}}$ ved, at den k^{te} søjle består af $a_{1k}+a'_{1k},\ldots,a_{nk}+a'_{nk}$. Derfor får vi

$$f(\underline{u}_1,\ldots,\underline{u}_{k-1}, \underline{u}_k+\underline{u}'_k, \underline{u}_{k+1},\ldots,\underline{u}_n) = \kappa \det \overline{A} =$$

$$\sum_{p\in S_n}\varepsilon(p)a_{p(1),1}\cdots a_{p(k-1),k-1}(a_{p(k),k}+a'_{p(k),k})a_{p(k+1),k+1}\cdots a_n =$$

$$\sum_{p\in S_n}\varepsilon(p)a_{p(1),1}\cdots a_{p(n),n} + \sum_{p\in S_n}\varepsilon(p)a_{p(1),1}\cdots a_{p(k-1),k-1}a'_{p(k),k}$$

$$a_{p(k+1),k+1}\cdots a_{p(n),n} = f(\underline{u}_1,\ldots,\underline{u}_n)+f(\underline{u}_1,\ldots,\underline{u}_{k-1},\underline{u}'_k,\underline{u}_{k+1},\ldots,\underline{u}_n).$$

Analogt, men en lille smule lettere viser vi, at

$$f(\underline{u}_1,\ldots,\underline{u}_{k-1},\lambda\underline{u}_k, \underline{u}_{k+1},\ldots,\underline{u}_n) = \lambda f(\underline{u}_1,\ldots,\underline{u}_n).$$

Dermed har vi vist, at f er n-lineær.

For at vise, at f er alternerende skal vi blot vise, at $f(\underline{u}_1,\ldots,\underline{u}_n)$ for $j \neq k$ skifter fortegn ved ombytning af $\underline{u}_j$ og $\underline{u}_k$, og det kommer ud på at vise, at det $\underline{\underline{A}}$ skifter fortegn ved ombytning af 2 søjler. Et vilkårligt led i den sum, hvorved det $\underline{\underline{A}}$ defineres, har formen

$$\varepsilon(p)a_{p(1),1}\cdots a_{p(n),n}.$$

Ved ombytning af de to søjler optræder det samme led stadig, men svarende til en ny permutation p' der er sammensat af en ombytning af to indices efterfulgt af p. Derfor er $\varepsilon(p')=$

$-\varepsilon(p)$. Deraf følger påstanden.

Endelig ser vi umiddelbart, at det $\underline{\underline{E}} = 1$, hvilket medfører, at $f(\underline{e}_1,\ldots,\underline{e}_n) = \kappa\cdot 1 = \kappa$. Dermed er sætningen bevist.

Sætning 16.4. For vilkårlige n×n-matricer $\underline{\underline{A}}$ og $\underline{\underline{B}}$ gælder

$$\det(\underline{\underline{A}}\ \underline{\underline{B}}) = \det \underline{\underline{A}} \det \underline{\underline{B}}.$$

Bevis. Lad U være et n-dimensionalt vektorrum med basis $(\underline{e}_1,\ldots,\underline{e}_n)$. Vi definerer $(\underline{u}_1,\ldots,\underline{u}_n) = (\underline{e}_1,\ldots,\underline{e}_n)\underline{\underline{A}}$ og $(\underline{v}_1,\ldots,\underline{v}_n) = (\underline{u}_1,\ldots,\underline{u}_n)\underline{\underline{B}}$, altså $(\underline{v}_1,\ldots,\underline{v}_n) = (\underline{e}_1,\ldots,\underline{e}_n)\underline{\underline{A}}\ \underline{\underline{B}}$. For den alternerende n-linearform $f:U^n \to K$, der tilfredsstiller $f(\underline{e}_1,\ldots,\underline{e}_n)$ har vi da

$$\det(\underline{\underline{A}}\ \underline{\underline{B}}) = f(\underline{v}_1,\ldots,\underline{v}_n) = f(\underline{u}_1,\ldots,\underline{u}_n)\det \underline{\underline{B}} = \det \underline{\underline{A}} \det \underline{\underline{B}}.$$

Dermed er sætningen bevist.

Sætningen udtrykker, at vi har afbildningen $\det:\hat{M}(K;n,n)\to K$, som er en homomorfi med hensyn til multiplikation.

Den næste sætning har vi vist tidligere, men vi måtte undtage det tilfælde, hvor K havde karakteristik 2. Det behøver vi ikke mere.

Sætning 16.5. Lad U være et vektorrum over K, og lad $f:U^m \to K$ være en alternerende m-linearform. Da er $f(\underline{u}_1,\ldots,\underline{u}_m) = 0$, når $\underline{u}_1,\ldots,\underline{u}_m$ ikke alle er indbyrdes forskellige.

Bevis. Vi antager, at der findes to indices j og k, for hvilke vi har $j \neq k$, $\underline{u}_j = \underline{u}_k$. Vi kan vælge $\underline{e}_i = \underline{u}_i$ for $i \neq k$ og $\underline{e}_k$ vælges vilkårligt. Vi sætter $a_{\mu\nu} = 1$, hvis $\mu = \nu \neq k$, og hvis $\mu = j$, $\nu = k$, og iøvrigt $a_{\mu\nu} = 0$ i alle andre tilfælde. Matricen $\underline{\underline{A}} = (a_{\mu\nu})$ har altså følgende udseende

$$\underline{\underline{A}} = \begin{pmatrix} 1 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 & \cdots & 1 & \cdots & 0 \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots & & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & 0 & \cdots & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \text{række } j \\ \text{række } k \\ \\ \\ \end{matrix}$$

søjle j søjle k

Vi ser, at $(\underline{u}_1,\ldots,\underline{u}_m) = (\underline{e}_1,\ldots,\underline{e}_m)\underline{\underline{A}}$. Endvidere er det $\underline{\underline{A}} = 0$, fordi hvert led indeholder et element fra den k^{te} række, der kun indeholder nuller. Men ifølge en sætning, som vi viste ovenfor, har vi

$$f(\underline{u}_1,\ldots,\underline{u}_m) = f(\underline{e}_1,\ldots,\underline{e}_m)\det \underline{\underline{A}} = 0.$$

Dermed er sætningen bevist.

Sætning 16.6. Lad U være et vektorrum over K, og lad $f:U^m \to K$ være en alternerende m-linearform. Da er $f(\underline{u}_1,\ldots,\underline{u}_n) = 0$, hvis $\underline{u}_1,\ldots,\underline{u}_m$ er lineært afhængige.

Bevis. Hvis $\underline{u}_1,\ldots,\underline{u}_n$ er lineært afhængige, er en af dem en linearkombination af de øvrige, og der er ikke noget specielt i at antage, at det er $\underline{u}_m$. Vi har da en relation $\underline{u}_m = \lambda_1\underline{u}_1+\ldots+\lambda_{m-1}\underline{u}_{m-1}$, som medfører en relation

$$f(u_1,\ldots,\underline{u}_m) = \sum_{j=1}^{m-1}\lambda_j f(\underline{u}_1,\ldots,\underline{u}_{m-1},\underline{u}_j) = 0,$$

ifølge den foregående sætning, da hvert af sættene $(\underline{u}_1,\ldots,\underline{u}_{m-1},\underline{u}_j)$ har to elementer ens.

Sætning 16.7. En n×n-matrix $\underline{\underline{A}}$ er invertibel, hvis og kun hvis $\det \underline{\underline{A}} \neq 0$.

Bevis. Hvis $\underline{\underline{A}}$ er invertibel, har $\underline{\underline{A}}$ en invers matrix $\underline{\underline{A}}^{-1}$, og af $\underline{\underline{A}}\,\underline{\underline{A}}^{-1} = E$ følger $\det \underline{\underline{A}}(\det \underline{\underline{A}}^{-1}) = \det E = 1$. Altså er $\det \underline{\underline{A}} \neq 0$. Hvis $\underline{\underline{A}}$ ikke er invertibel, har $\underline{\underline{A}}$ rang $r < n$, og hvis U er et vektorrum med basis $(\underline{e}_1,\ldots,\underline{e}_n)$ og $(\underline{u}_1,\ldots,\underline{u}_n) = (\underline{e}_1,\ldots,\underline{e}_n)\underline{\underline{A}}$, er $\underline{u}_1,\ldots,\underline{u}_n$ lineært afhængige. Der findes en n-linearform $f:U^n \to K$ med $f(\underline{e}_1,\ldots,\underline{e}_n) \neq 0$, og da

$$0 = f(\underline{u}_1,\ldots,\underline{u}_n) = f(\underline{e}_1,\ldots,\underline{e}_n)\det \underline{\underline{A}},$$

er $\det \underline{\underline{A}} = 0$. Dermed er sætningen bevist.

Sætning 16.8. For enhver n×n-matrix $\underline{\underline{A}}$ er det $\underline{\underline{A}}'$ = det $\underline{\underline{A}}$.

Bevis. For $\underline{\underline{A}} = (a_{jk})$ har vi

$$\det \underline{\underline{A}}' = \sum_{p\in S_n} \varepsilon(p) a_{1,p(1)} \cdots a_{n,p(n)} = \sum_{p\in S_n} \varepsilon(p^{-1}) a_{1,p^{-1}(1)} \cdots a_{n,p^{-1}(n)} = \sum_{p\in S_n} \varepsilon(p) a_{p(1),1} \cdots a_{p(n),n} = \det \underline{\underline{A}}.$$

Det andet lighedstegn beror på, at den ved $\varphi(p) = p^{-1}$ definerede afbildning $\varphi: S_n \to S_n$ er bijektiv. Det næste lighedstegn kommer af, at $\varepsilon(p^{-1}) = \varepsilon(p)$, og at faktorerne i produktet omordnes, så de bliver ordnede efter anden index i stedet for efter første. Dermed er sætningen bevist.

En matrix, der fås af matricen $\underline{\underline{A}}$ ved at udelade nogle rækker og/eller søjler, kaldes en delmatrix af $\underline{\underline{A}}$. Hvis vi har $\underline{\underline{A}} = (a_{jk} | j = 1,\ldots,m;\ k = 1,\ldots,n)$, og vi har voksende sekvenser $1 \leq j_1 < j_2 < \ldots < j_p \leq m$ og $1 \leq k_1 < k_2 < \ldots < k_q \leq n$, er $\underline{\underline{\tilde{A}}} = (a_{j_\mu k_\nu} | \mu = 1,\ldots,p;\ \nu = 1,\ldots,q)$ en delmatrix af $\underline{\underline{A}}$, og enhver delmatrix af $\underline{\underline{A}}$ fås på denne måde. Vi regner $\underline{\underline{A}}$ selv for en delmatrix af $\underline{\underline{A}}$, og der er også en tom delmatrix. Den er kvadratisk, og dens determinant er en sum med det tomme produkt som det eneste led, så den har værdien 1.

Sætning 16.9. Lad matricen $\underline{\underline{A}}$ have rang r. Så vil alle ν×ν-delmatricer af $\underline{\underline{A}}$ for $\nu > r$ have determinant 0,

medens der for hvert $\nu \leqq r$ findes $\nu\times\nu$-delmatricer af $\underline{\underline{A}}$ med determinant $\neq 0$.

Bevis. Lad os først antage, at $\nu > r$. Vi betragter en delmatrix $\underline{\underline{B}} = (a_{j_\alpha k_\beta} \mid \alpha,\beta = 1,\ldots,\nu)$. Mængden M af søjlevektorerne med numre $k_1,\ldots,k_\nu$ har rang $\leqq r$. Vi betragter afbildningen $\varphi: K^m \to K$ defineret ved $\varphi(x_1,\ldots,x_m) \to (x_{j_1},\ldots,x_{j_\nu})$. Den afbilder M på mængden af søjlevektorer i $\underline{\underline{B}}$, og denne mængde har derfor rang $\leqq r$. Men så er $\underline{\underline{B}}$ ikke regulær, og det medfører, at det $\underline{\underline{B}} = 0$.

Lad os dernæst antage, at $\nu \leqq r$. Så kan vi vælge ν lineært uafhængige søjler i $\underline{\underline{A}}$, og disse søjler udgør en $m\times\nu$-delmatrix $\underline{\underline{B}}$ med rang ν. Så vil også mængden af rækkevektorer i $\underline{\underline{B}}$ have rang ν, og ν lineært uafhængige rækker af $\underline{\underline{B}}$ udgør en regulær $\nu\times\nu$-delmatrix af $\underline{\underline{A}}$, og en sådan har determinant $\neq 0$. Dermed er sætningen bevist.

Vi har således set, at determinantbegrebet kan spille en rolle ved bestemmelsen af matricers rang. De har imidlertid også på anden måde stor betydning. Vi vil derfor ofre endnu et kapitel på determinantbegrebet.

KAPITEL 17

Udvikling af determinanter

For en $n\times n$-matrix $\underline{\underline{A}} = (a_{jk})$ er determinanten givet ved

$$\det\underline{\underline{A}} = \sum_{p\in S_n} \varepsilon(p) a_{p(1),1}\cdots a_{p(n),n}$$

Hvert led i summen indeholder netop et led fra søjle nummer k. Vi definerer:

Definition 17.1. Ved komplementet A_{jk} til elementet a_{jk} i matrix $\underline{\underline{A}}$ forstår vi den størrelse, der optræder i udtrykket

$$\det\underline{\underline{A}} = a_{1k}A_{1k}+\ldots+a_{nk}A_{nk},$$

som fås ved at ordne leddene i den sum, der optræder i definitionen af $\det\underline{\underline{A}}$, og så trække den fælles faktor a_{jk} ud af den delsum, der udgøres af de led, hvor denne faktor optræder.

Lad $S_n^{j,k}$ betegne den delmængde af S_n, der består af de permutationer $p: \{1,\ldots,n\} \to \{1,\ldots,n\}$, som opfylder

$p(k) = j$, altså

$$S_n^{jk} = \{p \in S_n \mid p(k) = j\}.$$

Det er da klart, at

$$A_{jk} = \sum_{p \in S_n^{jk}} \varepsilon(p) a_{p(1),1} \cdots a_{p(k-1),k-1} a_{p(k+1),k+1} \cdots a_{p(n),n}.$$

Lad os nu skrive $\underline{\underline{A}}_{jk}$ for den delmatrix af $\underline{\underline{A}}$, der fås ved at slette række nummer j og søjle nummer k. Vi ser, at produktet i hvert led i A_{jk} indeholder en faktor fra hver søjle i $\underline{\underline{A}}_{jk}$ og en faktor fra hver række i $\underline{\underline{A}}_{jk}$, og derfor optræder netop de samme produkter som i $\det \underline{\underline{A}}_{jk}$. Spørgsmålet er så, hvordan det passer med fortegnene. I $\det \underline{\underline{A}}_{jk}$ optræder jo et fortegn $\varepsilon(p')$, hvor $p' \in S_{n-1}$ er induceret af p, ved at j og k med $k = p(j)$ udelades. Så må de resterende elementer af $\{1,\ldots,n\}$ jo nummereres om i rækkefølge. Vi får altså p' som en sammensat afbildning, vi kan opskrive i tabelform

$$\begin{array}{ccc}
1 & 2 \ \ldots \ k-1, & k, \ k+1, \ \ldots \ n-1 \\
\downarrow & \downarrow \quad\quad \downarrow & \searrow \quad\quad \searrow \quad\quad \searrow \\
1 & 2 \ \ldots \ k-1, & k, \ k+1, \ \ldots \ n-1, n \\
p\downarrow & & \downarrow \\
1 & 2 \ \ldots \ j-1, & j, \ j+1, \ \ldots \ n-1, n \\
\downarrow & \downarrow \quad\quad \downarrow & \swarrow \quad\quad \swarrow \quad\quad \swarrow \\
1 & 2 \ \ldots \ j-1, & j, \ j+1, \ \ldots \ n-1
\end{array}$$

Tilfældet $j = k$ er særlig enkelt, idet delmængden $\{k\} \subseteq \{1,\ldots,n\}$ da udgør en cykel, og ved at udskyde $k = j$ ændrer vi ikke antallet af elementer minus antallet af cykler.

For $k = j$ har vi derfor $\varepsilon(p') = \varepsilon(p)$ for alle $p \in S_n^{j,j}$, og vi har derfor $A_{jj} = \det A_{jj}$. For $j \neq k$ kan vi erstatte p med p efterfulgt af $|k-j|$ simple ombytninger, og derved overføre p i en permutation med $p(k) = k$. Det ses, at de simple ombytninger slet ikke ændrer p'. Vi får således $\varepsilon(p') = (-1)^{k-j}\varepsilon(p)$, så vi har generelt $A_{jk} = (-1)^{k-j}\det \underline{\underline{A}}_{jk}$. Vi formulerer dette resultat i en sætning.

Sætning 17.2. Lad $\underline{\underline{A}}$ være en $n\times n$-matrix, og lad $\underline{\underline{A}}_{jk}$ være den delmatrix, der fås af $\underline{\underline{A}}$ ved at udelade række nummer j og søjle nummer k. Da er komplementet A_{jk} til a_{jk} bestemt ved, at $A_{jk} = \pm \det \underline{\underline{A}}_{jk}$, idet + anvendes, hvis j og k har samme paritet, medens - anvendes, hvis j og k har forskellig paritet.

Vi har således $A_{jk} = (-1)^{j-k}\det \underline{\underline{A}}_{jk} = (-1)^{j+k}\det \underline{\underline{A}}_{jk}$. Det viser sig nu, at den fremstilling af $\det \underline{\underline{A}}$ ved hjælp af elementerne i en søjle og deres komplementer, således som omtalt i definitionen af komplementet A_{jk}, kommer til at indgå i et sæt af formler, der er emnet for den næste sætning.

Sætning 17.3. For en $n\times n$-matrix $\underline{\underline{A}}$ gælder

$$a_{1j}A_{1k}+\ldots+a_{nj}A_{nk} = \begin{cases} \det\underline{\underline{A}} & \text{for } j = k \\ 0 & \text{for } j \neq k \end{cases}$$

$$a_{j1}A_{k1}+\ldots+a_{jn}A_{kn} = \begin{cases} \det\underline{\underline{A}} & \text{for } j = k \\ 0 & \text{for } j \neq k. \end{cases}$$

Bevis. Den øverste formel er for $j = k$ bare gentagelse af definitionen af komplementet. For $j \neq k$ giver den samme formel determinanten af den matrix der fås af $\underline{\underline{A}}$ ved at erstatte den k^{te} søjle med en kopi af den j^{te}. Derved fremkommer en matrix med to ens søjler, og den har determinant 0. Da kvadratiske matricer bevarer deres determinant ved transponering og pariteterne af række- og søjlenummer for et element blot byttes, får vi præcis de samme komplementer til de samme elementer (men flyttet til den symmetriske plads) i $\underline{\underline{A}}'$. Derfor fås de sidste formler ved at anvende de første på $\underline{\underline{A}}'$. Dermed er sætningen bevist.

Sætning 17.4. Lad $\underline{\underline{A}} = (a_{jk})$ være en regulær n×n-matrix. Da er den inverse matrix $\underline{\underline{A}}^{-1} = \underline{\underline{B}} = (b_{jk})$ bestemt ved, at

$$b_{jk} = \frac{A_{kj}}{\det||A||} .$$

Bevis. Den første formel i den foregående sætning giver netop, at $\underline{\underline{A}}\,\underline{\underline{B}} = \underline{\underline{E}}$, og dermed er sætningen bevist, så

vi får ikke udnyttet, at det andet sæt formler giver, at $\underline{\underline{B}}\,\underline{\underline{A}} = \underline{\underline{E}}$.

Den næste definition indfører en operation, der ofte anvendes i matrixregning, f.eks. ved udregning af determinanten af en matrix.

Definition 17.5. At udføre en søjleoperation på en matrix $\underline{\underline{A}} = (a_{jk} | j = 1,\ldots,m;\ k = 1,\ldots,n)$ består i at erstatte elementerne $a_{1k},\ldots,a_{mk}$ i en søjle med $a_{1k}+\lambda a_{1i},\ldots,$ $a_{nk}+\lambda a_{ni}$ for et $i \neq k$ og et $\lambda \in K$. At udføre en rækkeoperation på $\underline{\underline{A}}$ består i at erstatte elementerne $a_{j1},\ldots,a_{jn}$ i en række med $a_{j1}+\lambda a_{i1},\ldots,a_{jn}+\lambda a_{in}$ for et $i \neq j$ og et $\lambda \in K$.

En rækkeoperation på $\underline{\underline{A}}$ bliver således en søjleoperation på $\underline{\underline{A}}'$.

Sætning 17.6. Hvis $\underline{\underline{A}}$ er en kvadratisk matrix vil søjle- eller rækkeoperationer ikke ændre værdien af $\det\underline{\underline{A}}$.

Bevis. Lad $\underline{\underline{B}}$ være den matrix, der fås af $\underline{\underline{A}}$ ved at erstatte den k^{te} søjle med en kopi af den i^{te}. Lad $\underline{\underline{\tilde{A}}}$ være den matrix, der fås ved den i definitionen ovenfor beskrevne søjleoperation. Da det er multilineær i søjlevektorerne, er $\det\underline{\underline{A}} = \det\underline{\underline{A}} + \lambda\det\underline{\underline{B}}$, og påstanden følger af, at $\det\underline{\underline{B}} = 0$,

fordi $\underline{\underline{B}}$ har to ens søjler. Den tilsvarende påstand for rækkeoperationer følger nu ved skifte til den transponerede matrix $\underline{\underline{A}}'$.

Vi vil nu diskutere fremgangsmåder ved praktisk udregning af determinanter. Vi vil først forestille os, at matricens elementer er hele tal, polynomier eller andre eksakte udtryk. Bagefter vil vi sige lidt om fremgangsmåden, når elementerne er reelle tal, der kun kendes bortset fra en vis usikkerhed. I begge tilfælde består fremgangsmåden af de samme elementer.

1. Række- og søjleoperationer bruges til at skaffe små tal og derefter nuller i en søjle eller række bortset fra et element eller to.

2. Udvikling efter en række eller søjle, i hvilken næsten alle elementer er 0. Derved bringes ordenen ned.

3. Fælles divisorer i alle elementer i en række eller søjle kan trækkes ud.

4. Rækker og søjler kan permuteres, eventuelt på bekostning af et fortegnsskift. En sådan ændring vil ikke være et virkeligt fremskridt, men den kan hjælpe på overskueligheden.

Som eksempel vil vi udregne

$$\det\underline{\underline{A}} = \det\begin{pmatrix} 5 & 4 & -3 & -10 & 2 \\ -2 & 3 & 0 & -9 & 3 \\ 3 & -1 & 2 & 3 & 0 \\ -4 & 3 & -6 & -5 & 4 \\ 6 & 5 & -7 & -12 & 6 \end{pmatrix}$$

Vi mærker os, at $a_{32} = -1$, og da der allerede er et 0 i tredie række, bruger vi søjleoperationer for at skaffe nuller i denne række undtagen på anden plads. Vi adderer anden søjle multipliceret med 3 til første søjle, og derefter også til fjerde søjle. Endvidere adderer vi anden søjle multipliceret med 2 til tredie søjle. Derved får vi

$$\det\underline{\underline{A}} = \det\begin{pmatrix} 17 & 4 & 5 & 2 & 2 \\ 7 & 3 & 6 & 0 & 3 \\ 0 & -1 & 0 & 0 & 0 \\ 5 & 3 & 0 & 4 & 4 \\ 21 & 5 & 3 & 3 & 6 \end{pmatrix}$$

Udvikling efter tredie række giver nu

$$\det\underline{\underline{A}} = \det\begin{pmatrix} 17 & 5 & 2 & 2 \\ 7 & 6 & 0 & 3 \\ 5 & 0 & 4 & 4 \\ 21 & 3 & 3 & 6 \end{pmatrix} = 3\det\begin{pmatrix} 17 & 5 & 2 & 2 \\ 7 & 6 & 0 & 3 \\ 5 & 0 & 4 & 4 \\ 7 & 1 & 1 & 2 \end{pmatrix}$$

Vi trækker nu tredie søjle fra fjerde, og dernæst fjerde række multipliceret med 3 fra anden række.

$$\det\underline{\underline{A}} = 3\det\begin{pmatrix} 17 & 5 & 2 & 0 \\ 7 & 6 & 0 & 3 \\ 5 & 0 & 4 & 0 \\ 7 & 1 & 1 & 1 \end{pmatrix} = 3\det\begin{pmatrix} 17 & 5 & 2 & 0 \\ -14 & 3 & -3 & 0 \\ 5 & 0 & 4 & 0 \\ 7 & 1 & 1 & 1 \end{pmatrix}$$

Vi udvikler efter fjerde søjle og får

$$\det\underline{\underline{A}} = 3\det\begin{pmatrix} 17 & 5 & 2 \\ -14 & 3 & -3 \\ 5 & 0 & 4 \end{pmatrix}$$

Vi trækker tredie søjle fra første søjle. Dernæst trækker vi første søjle multipliceret med 4 fra tredie søjle. Endelig udvikles efter tredie række.

$$\det\underline{\underline{A}} = 3\det\begin{pmatrix} 15 & 5 & 2 \\ -11 & 3 & -3 \\ 1 & 0 & 4 \end{pmatrix} = 3\det\begin{pmatrix} 15 & 5 & -58 \\ -11 & 3 & 41 \\ 1 & 0 & 0 \end{pmatrix} = 3\det\begin{pmatrix} 5 & -58 \\ 3 & 41 \end{pmatrix}$$

Nu kan direkte udregning betale sig. Vi får

$$\det\underline{\underline{A}} = 3(205+174) = 3\cdot 379 = 1137.$$

Ved udregning af determinanter af heltalsmatricer lader det sig altid gøre at skaffe 1-taller, så man bagefter kan skaffe nuller ved søjle- eller rækkeoperationer, som vi gjorde det i eksemplet.

Ved tilnærmet beregning af determinanter af matricer med reelle elementer, f.eks. ved hjælp af elektronregnemaskine, er det mest hensigtsmæssigt at opsøge en række eller søjle med et element, der er meget større end de andre, og så skaffer man nuller ved at bortskaffe de små elementer ved søjle- eller rækkeoperationer, og dernæst udvikles, så ordenen bringes én ned. Derved bliver den faktor λ, der optræder i operationerne, forholdsvis lille, så man undgår at mul-

tiplicere afrundingsfejlene op. Det er dog svært at finde en strategi, der altid virker godt, og det kan hænde, at usikkerheden på de enkelte elementer bevirker, at determinanten overhovedet ikke er bestemt med rimelig nøjagtighed. Matricer med store elementer men lille determinant er altid vanskelige at arbejde med. Således er

$$\det\begin{pmatrix} 2000 & 2001 \\ 1999 & 2000 \end{pmatrix} = 1$$

$$\det\begin{pmatrix} 2000 & 2001 \\ 2000 & 2000 \end{pmatrix} = -2000 \qquad \det\begin{pmatrix} 2000 & 2000 \\ 1999 & 2000 \end{pmatrix} = 2000,$$

hvilket viser, at en ændring af et element med en sølle halv promille kan ændre determinanten drastisk. I 2×2-matricer er fænomenet til at overse, men i 17×17-matricer kan det være umuligt at forudse.

Som et eksempel på udregning af determinanten af en matrix ved en knap så ortodoks metode vil vi bevise sætningen om Vandermonde's determinant.

Sætning 17.7.

$$\det\begin{pmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_n \\ x_1^2 & \cdots & x_n^2 \\ \vdots & & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} \end{pmatrix} = \prod_{1 \le j < k \le n} (x_k - x_j)$$

Bevis. Vi vil vise sætningen ved induktion. For $n = 1$ siger den blot, at 1 er værdien af det tomme produkt. Vi kan derfor antage, at den anførte formel er rigtig, og vi skal så vise den tilsvarende formel med n erstattet med $n+1$. Denne formel fremkommer imidlertid ved at indsætte $x = x_{n+1}$ i ligningen

$$\det \begin{pmatrix} 1 & \cdots & 1 & 1 \\ x_1 & \cdots & x_n & x \\ x_1^2 & \cdots & x_n^2 & x^2 \\ \vdots & & \vdots & \vdots \\ x_1^{n-1} & \cdots & x_n^{n-1} & x^{n-1} \\ x_1^n & \cdots & x_n^n & x^n \end{pmatrix} =$$

$$\left(\prod_{1 \leq j < k \leq n} (x_k - x_j) \right) (x-x_1) \ldots (x-x_n).$$

Vi skal derfor blot vise denne identitet. Udvikling efter den sidste søjle viser, at determinanten bliver et polynomium af grad n i x med den i sætningen omtalte determinant som koefficient til x^n. Da polynomiet har rødderne $x_1, \ldots, x_n$, er dets opløsning i førstegradsfaktorer netop som anført. Dermed er sætningen bevist.

STIKORDSREGISTER KAPITEL 1-17.

Henvisning til et tal n er til kapitel n, medens p,q betyder kapitel p side q, og øv p,q øvelser til kapitel p side q.