

Matematik 1, AG, 1961–66

Werner Fenchel og T. Gutmann Madsen
Forelæsningsnoter i Algebra og Geometri

Kap. I. Mængder, afbildninger, relationer

- §1. Matematisk logik
- §2. Mængder og deres delmængder
- §3. Mængdealgebra
- §4. Afbildninger (funktioner)
- §5. Relationer
- §6. Mængders ækvipotens (gamle §8)

Kap. II. Algebraens grundbegreber

- §1. Kompositioner
- §2. Grupper
- §3. Ringe og legemer
- Øvelser til §1-3

Kap. III. Lineær algebra og analytisk geometri

- §1. Vektorrum
- §2. Lineære afbildninger og matricer (tilf. fra 1968–69)
- §3a. Løsning af lineære ligningssystemer (spec. øvelser)
- §4. Volumen og determinanter (tilf. fra 1967–68)
- §11. Determinanter og lineære ligningssystemer (Øvelser fra §4 og §2)
- §5. Egenverdiproblemet. Normalformer
- §12. Bilineære og kvadratiske former

Kap. I. Mængder, afbildninger, relationer.§ 1. Matematisk logik.

I matematikken benytter man som bekendt et stort antal tegn med nøje aftalt betydning. Formålet er dobbelt; dels tilstræbes overskuelighed og bekvem udførelse af matematiske udregninger, dels utvetydighed og nøjagtighed i formuleringen af matematiske sætninger.

Ved nedskrivningen af en matematisk sætning benyttes foruden matematiske symboler sædvanligvis ord og vendinger fra dagligsproget, tjenende til at bygge sætningen op af mere elementære dele. Som eksempel kan nævnes: ...og... , ...eller... , ...ikke... , hvis...så... , ...netop hvis... , for ethvert...gælder..., der findes et...således at... . Der er imidlertid intet til hinder for, at man også for sådanne vendinger benytter særlige tegn. Formålet er det samme som for anvendelsen af de sædvanlige matematiske symboler. Specielt benytter man ved indførelsen af sådanne tegn lejligheden til nøje at præcisere betydningen af hvert enkelt, således at den tvivl, der undertiden kan være om den nøjagtige mening med den tilsvarende sproglige vending, ikke opstår for symbolets vedkommende. Det understreges, at der således ikke blot er tale om stenografi.

Læren om brugen af disse tegn kaldes matematisk logik, undertiden symbolsk logik eller logikkalkyle. Begrundelsen er, at der er tale om logik udtrykt i formelsprog efter matematisk forbillede. Som grundlægger af den matematiske logik regner man George Boole, -1847 udkom "The mathematical analysis of logic, being an essay towards a calculus of deductive reasoning".

Den matematiske logik falder i to hovedafsnit, udsagnskalkylen og prædikatkalkylen.

A. Udsagnskalkylen

er læren om sammenknytning af udsagn til nye, mere sammensatte udsagn.

Vi vil i første række tænke på matematiske udsagn uden her at gå ind på, hvad der skal menes hermed. Som eksempler kan nævnes "2 er større end -1", " $2^{2309}-1$ er et primtal", "alle trekanter er ligebenede". For de udsagn, der tages i betragtning, går vi ud fra, at hvert kan siges at være enten sandt eller falsk, men ikke begge dele. Det kommer herved slet ikke an på, om vi er i stand til at afgøre, om et forelagt udsagn "i virkeligheden" er sandt eller falsk; foreløbig behøver vi end ikke at tænke på, hvad "sandt" og "falsk" i grunden betyder.

Af udsagn dannes nye udsagn på følgende måder:

1. Ethvert udsagn har en negation. Negationen til "2 er større end -1" skrives

" $\neg$ (2 er større end -1)" eller "non(2 er større end -1)" og læses "2 er ikke større end -1".

2. Af to vilkårlige udsagn dannes et nyt, kaldet deres konjunktion. Man skriver konjunktionen ved at sætte tegnet " $\wedge$ " mellem de to udsagn, f. eks.

"(2 er større end -1) $\wedge$ ($2^{2309}-1$ er et primtal)".
" $\wedge$ " læses "og".

3. Af to vilkårlige udsagn dannes et nyt, kaldet deres disjunktion. Man skriver disjunktionen ved at sætte tegnet " $\vee$ " mellem de to udsagn, f.eks.

"(2 er større end -1) $\vee$ ($2^{2309}-1$ er et primtal)".
" $\vee$ " læses "eller". Hertil er at bemærke, at i dagligsproget bruges ordet "eller" i to betydninger: "netop en af delene" og "mindst en af delene"; man har valgt at give " $\vee$ " den sidste be-

tydning, idet det giver de mest bekvemme "regneregler" (se især stykket om dualitet længere fremme). En disjunktion er altså sand, når mindst et af de to sammenknyttede udsagn er sandt. - I matematikken holder man sig gerne til at benytte ordet "eller" med samme betydning som " $\vee$ "; "2 er et lige tal eller (2 er) et primtal" er således et sandt udsagn.

4. Af to vilkårlige udsagn dannes et nyt, kaldet en implikation. Herved er de to udsagns rækkefølge væsentlig. Man skriver implikationen ved at sætte tegnet " $\Rightarrow$ " mellem de to udsagn, f.eks.

"(2 er større end -1) $\Rightarrow$ ($2^{2309}-1$ er et primtal)".

" $\Rightarrow$ " læses "medfører", "hvis...så..." el. lign. Disse ord må ikke forlede til den forestilling, at talen er om, hvorvidt det andet udsagn logisk følger af, er en konsekvens af det første, - tværtimod kan en implikation dannes af hvilkesomhelst to udsagn; hvornår den skal regnes sand, hvornår falsk skal vi gøre rede for om lidt.

5. Af to vilkårlige udsagn dannes et nyt, kaldet deres biimplikation. Man skriver biimplikationen ved at sætte tegnet " $\Leftrightarrow$ " mellem de to udsagn, f.eks.

"(2 er større end -1) $\Leftrightarrow$ ($2^{2309}-1$ er et primtal)".

" $\Leftrightarrow$ " læses "hvis og kun hvis", "da og kun da hvis" el. lign.

En konjunktion er sand, netop hvis begge de indgående udsagn er sande. En disjunktion er sand, når mindst et af de indgående udsagn er sandt. Et afgørende træk er, at "sandhedsværdien" af det sammensatte udsagn i hvert af disse tilfælde er bestemt alene ved sandhedsværdierne af de indgående udsagn, nemlig efter følgende skemaer:

$\wedge$	f	s
f	f	f
s	f	s

$\vee$	f	s
f	f	s
s	s	s

Vi fastsætter nu, at sandhedsværdien af en implikation og en biimplikation ligeledes skal være bestemt alene ved sandhedsværdierne af de indgående udsagn, nemlig efter følgende skemaer:

		2. udsagn	
		$\Rightarrow$	
1. udsagn	f	s	s
	s	f	s

		$\Leftrightarrow$	f	s
f	s	f	f	s
s	f	s	f	s

Også for en negation er sandhedsværdien bestemt ved sandhedsværdien af det udsagn, der negeres; de to udsagn har modsatte sandhedsværdier.

Det bemærkes, at udsagn, der er bygget sammen af andre, igen kan benyttes som byggesten i punkterne 1.-5., hvorved man kan få mere og mere sammensatte og komplicerede udsagn frem. F.eks. kan man af de to udsagn "2.2=5" og "3 går op i 9" danne udsagnet

$$"2.2=5 \Leftrightarrow (2.2=5 \Rightarrow \neg(3 \text{ går op i } 9))";$$

dette kan gengives "2.2=5 netop hvis 2.2=5 medfører, at 3 ikke går op i 9". Iøvrigt er det let at danne sammensatte udsagn, som det er ganske håbløst at gengive sprogligt på en sådan måde, at meningen træder frem; specielt savner man et bekvemt udtryk for parenteser.

Sandhedsværdien af et sammensat udsagn afhænger kun af "grundudsagningenes" sandhedsværdier, ikke af deres indhold. Kendes, som i ovenstående eksempel, "grundudsagningenes" sandhedsværdier, kan man nemlig let bestemme det sammensatte udsagns sandhedsværdi hertil erstattes hvert "grundudsagn" med sin sandhedsværdi, hvorpå skemaerne ovenfor bruges som tabeller for "regning" med de to sandhedsværdier s og f.

F.eks. er

$$"2 \cdot 2 = 5 \iff (2 \cdot 2 = 5 \Rightarrow \neg(3 \text{ går op i } 9))"$$

et falsk udsagn, hvilket fremgår af udregningen

$$f \iff (f \Rightarrow \neg s) = f \iff (f \Rightarrow f) = f \iff s = f.$$

Foruden de anførte tabeller benyttes ved sådanne udregninger $\neg s = f$ og $\neg f = s$.

Udsagnsformer og deres sandhedstavler.

Udsagnsvariable er blot nogle bogstaver, som ikke i sig skal tillægges nogen betydning. Vi vil benytte $p, q, r, \dots$; ved at tilføje indices kan man skaffe sig så mange udsagnsvariable, man vil $p_1, p_2, \dots$. Navnet hidrører fra den anvendelse, vi ofte vil gøre: midlertidigt at lade nogle udsagnsvariable betegne bestemte udsagn.

Udtryk, der er bygget op ved hjælp af tegnene " $\neg, \wedge, \vee, \Rightarrow, \iff$ " ud fra udsagnsvariable i stedet for ud fra udsagn, vil vi kalde udsagnsformer. Eksempler:

$$"\neg q", "p \Rightarrow \neg q", "p \iff (p \Rightarrow \neg q)".$$

En udsagnsvariabel regnes også for en udsagnsform.

Man ser, at en udsagnsform, i det øjeblik man lader hver af de indgående udsagnsvariable betegne et bestemt udsagn, selv vil udtrykke et bestemt (sammensat) udsagn.

Lader man i stedet hver af de indgående udsagnsvariable betegne en bestemt sandhedsværdi, dvs. indsættes sandhedsværdier, får man en bestemt sandhedsværdi ud. For en vilkårlig forelagt udsagnsform kan man opstille en sandhedstavle, der angiver resultatet for hver af de mulige indsættninger af sandhedsværdier. F.eks. har $p \iff (p \Rightarrow \neg q)$ sandhedstavlen

p	q	$p \Leftrightarrow (p \Rightarrow \neg q)$
s	s	f
s	f	s
f	s	f
f	f	f

som man bekvemt kan danne ved at indskyde nogle mellemkolonner:

p	q	$\neg q$	$p \Rightarrow \neg q$	$p \Leftrightarrow (p \Rightarrow \neg q)$
s	s	f	f	f
s	f	s	s	s
f	s	f	s	f
f	f	s	s	f

Vi understreger: Når et sammensat udsagn fremgår ved at indsætte enklere udsagn for de udsagnsvariable i en udsagnsform, da fås det sammensatte udsagns sandhedsværdi ved i stedet at indsætte de respektive sandhedsværdier.

F.eks. fremgår udsagnet

$$"2 \cdot 2 = 5 \Leftrightarrow (2 \cdot 2 = 5 \Rightarrow \neg(3 \text{ går op i } 9))",$$

når man i udsagnsformen

$$"p \Leftrightarrow (p \Rightarrow \neg q)"$$

indsætter " $2 \cdot 2 = 5$ " for p og " $3 \text{ går op i } 9$ " for q, medens udsagnets sandhedsværdi

$$f \Leftrightarrow (f \Rightarrow \neg s), \text{ dvs. } f,$$

fås ved for p og q at indsætte sandhedsværdierne af " $2 \cdot 2 = 5$ " og " $3 \text{ går op i } 9$ ", dvs. henholdsvis f og s. - Når, som i dette eksempel, udsagnsformens sandhedstavle allerede er udregnet, kan man naturligvis aflæse det sammensatte udsagns sandhedsværdi på

den plads i tavlen, der hører til de foreliggende udgangsværdier, her $(p,q)=(f,s)$.

En praktisk bemærkning: Ved parenteser angives, hvorledes en udsagnsform eller et sammensat udsagn skal læses. For at undgå for mange parenteser har man fastsat, at " $\wedge$ " og " $\vee$ " binder mere end " $\Rightarrow$ " og " $\Leftrightarrow$ "; f.eks. er " $p \vee q \Rightarrow r$ " det samme som " $(p \vee q) \Rightarrow r$ ". Står der ingen parentes efter " $\neg$ ", hører tegnet til den umiddelbart følgende udsagnsvariabel; " $\neg p \vee q$ " er det samme som " $(\neg p) \vee q$ ".

Tautologier.

Vi skal nu forklare, hvad der menes med, at et (sammensat) udsagn er sandt "af rent (udsagns-)logiske grunde". Til indledning et par eksempler på sådanne udsagn: " $\pi \Rightarrow \sqrt{2}$ eller $\pi \not\Rightarrow \sqrt{2}$ ", altså

$$(\pi \Rightarrow \sqrt{2}) \vee \neg(\pi \Rightarrow \sqrt{2});$$

"hvis $2+2=4$ eller $2+2=5$, så vil, hvis $2+2$ ikke er 4, $2+2$ være 5", altså

$$[(2+2=4) \vee (2+2=5)] \Rightarrow [\neg(2+2=4) \Rightarrow (2+2=5)].$$

En udsagnsform kaldes en tautologi, når dens sandhedstavle har lutter s'er. Der vil da fremkomme et sandt udsagn, ligegyldig hvilke udsagn, der indsættes for de udsagnsvariable.

Eksempler på tautologier:

$$p \vee \neg p, \quad (p \vee q) \Rightarrow (\neg p \Rightarrow q).$$

Vi anfører bestemmelsen af sandhedstavlen for den sidste udsagnsform:

p	q	$p \vee q$	$\neg p$	$\neg p \Rightarrow q$	$(p \vee q) \Rightarrow (\neg p \Rightarrow q)$
s	s	s	f	s	s
s	f	s	f	s	s
f	s	s	s	s	s
f	f	f	s	f	s

Et (sammensat) udsagn, der kan fremkomme ved indsættelse af enklere udsagn i en tautologi, er nu netop, hvad man regner for et udsagn, som er sandt af rent (udsagns-)logiske grunde.

Indsættes " $\pi \Rightarrow \sqrt{2}$ " for p i tautologien " $p \vee \neg p$ ", fås udsagnet " $\pi \Rightarrow \sqrt{2}$ eller $\pi \nRightarrow \sqrt{2}$ "; det andet indledningsvis nævnte udsagn fremkommer, når man indsætter " $2+2=4$ " og " $2+2=5$ " for p og q i " $(p \vee q) \Rightarrow (\neg p \Rightarrow q)$ ".

Undertiden taler man også om en tautologi efter, at indsætning er foretaget.

En udsagnsform, hvis sandhedstavle har lutter f'er, kaldes en absurditet. Eksempel: " $p \wedge \neg p$ ".

Ækvivalente udsagnsformer.

To udsagnsformer kaldes ækvivalente, når deres biimplikation er en tautologi: Eksempelvis er " $\neg(p \vee q)$ " ækvivalent med " $\neg p \wedge \neg q$ ", da

$$\neg(p \vee q) \iff (\neg p \wedge \neg q)$$

er en tautologi:

p	q	$\neg(p \vee q)$	$\neg p \wedge \neg q$	$\neg(p \vee q) \Leftrightarrow (\neg p \wedge \neg q)$
s	s	f	f	s
s	f	f	f	s
f	s	f	f	s
f	f	s	s	s

Betingelsen for, at man får lutter s'er, når man danner biimplikationens sandhedstavle, er åbenbart, at de to udsagnsformer har ens sandhedstavler. Dette kunne derfor også være benyttet som definition af ækvivalens. - Heraf fremgår umiddelbart, at to udsagnsformer, som er ækvivalente med samme tredje, er indbyrdes ækvivalente. - Den sidste definition må dog fortolkes på passende måde, når de to udsagnsformer ikke rummer helt de samme udsagnsvariable. Eftersom som eksempel

$$\neg((p \Rightarrow q) \wedge r) \Rightarrow \neg q \quad \text{eq} \quad "q \Rightarrow r".$$

"eq" benytter vi her i udsagnskalkylen (senere også i prædikatkalkylen) som forkortelse for "er ækvivalent med".

Det er vigtigt at være fortrolig med en række ækvivalenser mellem simple udsagnsformer. Foretages nemlig en samtidig indsætning af udsagn i to ækvivalente udsagnsformer, fås sammensatte udsagn, der "siger det samme", eller, anderledes udtrykt: hvor det ene kan opfattes blot som en omformulering af det andet; sådanne omformuleringer må en matematiker være fortrolig med.

Eksempelvis: Idet " $\neg(p \vee q)$ " eq " $\neg p \wedge \neg q$ ", kan "det er ikke tilfældet, at 2 er lige eller 7 et primtal" omformuleres til "2 er ikke lige, og 7 er ikke et primtal".

Vi fremhæver især følgende ækvivalenser:

1. " $p \Leftrightarrow q$ " eq " $(p \Rightarrow q) \wedge (q \Rightarrow p)$ ".

Den fælles sandhedstavle er

p	q	
s	s	s
s	f	f
f	s	f
f	f	s

Eksempel. For en given trekant ABC med sider a, b og c kommer det ud på ét at sige " $a=b$ netop hvis $\angle A = \angle B$ " eller "hvis $a=b$, så er $\angle A = \angle B$, og hvis $\angle A = \angle B$, så er $a=b$ ". (Den fælles påstand er iøvrigt sand, ligegyldigt hvilken trekant vi betragter, men det er her uvæsentligt).

2. " $p \Rightarrow q$ " eq " $\neg(p \wedge \neg q)$ " eq " $\neg p \vee q$ ".

Den fælles sandhedstavle er

p	q	
s	s	s
s	f	f
f	s	s
f	f	s

Disse ækvivalenser angiver den betydning, vi tillægger " $\Rightarrow$ ", "hvis...så...", brugt mellem udsagn. At påstå

"hvis 7 går op i 1797, så er 1797 et sammensat tal" kommer ud på at hævde, at ikke begge de følgende udsagn er sande: "7 går op i 1797" og "1797 er ikke sammensat", altså at hævde

" $\neg(7 \text{ går op i } 1797 \wedge 1797 \text{ er ikke sammensat})$ ".

Dette kan også formuleres:

"7 går ikke op i 1797 $\vee$ 1797 er sammensat".

Denne brug af "hvis...så...", som vi her gør, altså som ganske ensgyldigt med "ikke...eller...", virker i reglen stødende påbegynderen. Han accepterer gerne, at "hvis...så..." kan oversættes til "ikke...eller...", men ikke det omvendte: det føles unaturligt at danne implikation af hvilket som helst to udsagn, f.eks.

"hvis $2 \cdot 2 = 5$, så går 3 op i 9",
medens han ikke har noget imod

" $2 \cdot 2$ er ikke 5 eller 3 går op i 9".

De ekstra betingelser, han føler bør være opfyldt for dannelsen af en implikation, det være sig en logisk sammenhæng eller hvad han nu vil forlange, er imidlertid så vage eller så komplicerede (jvf. slutningen af stykket om prædikater længere fremme), at man har bestemt sig for at skyde dem helt til side. Kun herigennem opnås en udsagnskalkyle, som er til at arbejde med. Han må altså vænne sig til, at "hvis...så..." bruges som bindemiddel mellem vilkårlige to udsagn, hvorved altid fås et nyt udsagn; dette kan så være sandt eller falsk.

Af ækvivalenserne 1. og 2. fremgår, at tegnene " $\iff$ " og " $\Rightarrow$ " kunne undværes. Idet

$$3a. \quad "p \wedge q" \text{ eq } "\neg(\neg p \vee \neg q)"$$

$$3b. \quad "p \vee q" \text{ eq } "\neg(\neg p \wedge \neg q)",$$

ser man iøvrigt, at yderligere et vilkårligt af tegnene " $\wedge$ " og " $\vee$ " er undværligt, således at man kan nøjes med " $\neg, \vee$ " eller med " $\neg, \wedge$ ".

$$4a. \quad "\neg(p \wedge q)" \text{ eq } "\neg p \vee \neg q",$$

$$4b. \quad "\neg(p \vee q)" \text{ eq } "\neg p \wedge \neg q",$$

de Morgans regler, der kan opfattes som regler for negering af

en konjunktion, henholdsvis en disjunktion, indses som sædvanlig ved opskrivning af sandhedstavler. De kan dog også afledes af 3a og 3b. ved benyttelse af

$$5. \quad \neg(\neg p) \text{ eq } p.$$

I kraft af

$$6a. \quad p \wedge (q \wedge r) \text{ eq } (p \wedge q) \wedge r, \quad (\text{associativitet})$$

$$6b. \quad p \vee (q \vee r) \text{ eq } (p \vee q) \vee r,$$

behøver man i en konjunktion, henholdsvis disjunktion, af flere udsagn ikke at bekymre sig om parenteser; rækkefølgen er også ligegyldig, idet tillige

$$7a. \quad p \wedge q \text{ eq } q \wedge p, \quad (\text{kommutativitet})$$

$$7b. \quad p \vee q \text{ eq } q \vee p.$$

At hævde

$$(2 \cdot 2 = 5) \wedge (\pi = \sqrt{2}) \wedge (7 \text{ er lige}) \wedge (2 \cdot 3 = 6)$$

vil sige at påstå, at hvert af de enkelte udsagn er sandt; at hævde

$$(2 \cdot 2 = 5) \vee (\pi = \sqrt{2}) \vee (7 \text{ er lige}) \vee (2 \cdot 3 = 6)$$

vil sige at påstå, at mindst et af de enkelte udsagn er sandt.

Lad os til slut notere følgende ækvivalenser:

$$8a. \quad (p \wedge q) \vee (p \wedge r) \text{ eq } p \wedge (q \vee r), \quad (\text{distributivitet})$$

$$8b. \quad (p \vee q) \wedge (p \vee r) \text{ eq } p \vee (q \wedge r),$$

$$9. \quad p \Rightarrow q \text{ eq } \neg q \Rightarrow \neg p, \quad (\text{kontraposition})$$

$$10. \quad p \Rightarrow (q \Rightarrow r) \text{ eq } p \wedge q \Rightarrow r,$$

$$11. \quad p \Leftrightarrow q \text{ eq } q \Leftrightarrow p.$$

Dualitet.

de Morgans regler, 4a. og 4b., er specielle tilfælde af følgende almindelige regel (der iøvrigt kan afledes af dem):

For en vilkårlig udsagnsform dannet alene ved hjælp af tegnene $\neg, \wedge, \vee$ fås en med negationen ækvivalent udsagnsform ved, at man erstatter hver udsagnsvariabel med dens negerede og samtidig ombytter tegnene " $\wedge$ " og " $\vee$ ".

Som eksempel på reglens anvendelse vil vi aflede ækvivalensen 8b. af 8a. Anvendes sidstnævnte på " $\neg p, \neg q, \neg r$ " i stedet for på " p, q, r ", fås

$$(\neg p \wedge \neg q) \vee (\neg p \wedge \neg r) \text{ eq } \neg p \wedge (\neg q \vee \neg r).$$

Ifølge vor regel er nu

$$\neg[(p \vee q) \wedge (p \vee r)] \text{ eq } (\neg p \wedge \neg q) \vee (\neg p \wedge \neg r)$$

$$\text{og} \quad \neg[p \vee (q \wedge r)] \text{ eq } \neg p \wedge (\neg q \vee \neg r),$$

hvorfor

$$\neg[(p \vee q) \wedge (p \vee r)] \text{ eq } \neg[p \vee (q \wedge r)]$$

og dermed

$$(p \vee q) \wedge (p \vee r) \text{ eq } p \vee (q \wedge r).$$

På samme måde kan det vises helt generelt, at en ækvivalens mellem to udsagnsformer, som begge er dannet alene ved hjælp af tegnene $\neg, \wedge, \vee$, atter går over i en ækvivalens ved ombytning af " $\wedge$ " og " $\vee$ ". To ækvivalenser, der fremgår af hinanden på denne måde, kaldes duale. Eksempler er alle med a og b mærkede par af ækvivalenser ovenfor.

(Udsagnslogiske) konsekvenser af givne forudsætninger.

Logikkens hovedemne er problemstillingen: forudsætninger - konsekvenser.

Nu er udsagnskalkylen kun den allerenkleste del af den matematiske logik og slet ikke dybtgående nok til i almindelighed at kunne gøre rede for matematiske følgeslutninger; begrænsningen ligger i, at man ikke indenfor udsagnskalkylen analyserer et udsagn dybere end til de udsagn, det evt. er bygget op af.

Visse enkle slutninger foretages dog på udsagnskalkylens grund. Lad os som eksempel studere, hvilke konsekvenser der kan drages af forudsætningerne

a. "hvis $2 \cdot 2 = 3$ og $7 + 5 = 8$, så er 9 et lige tal",

b. "9 er ikke et lige tal",

når man ser bort fra indholdet af udsagnene " $2 \cdot 2 = 3$ ", " $7 + 5 = 8$ " og "9 er et lige tal". Specielt kan vi spørge: kan man slutte

c. " $2 \cdot 2 \neq 3$ netop hvis 9 er lige".

Hertil bemærkes: a., b. og c. fremgår af udsagnsformerne

" $p \wedge q \Rightarrow r$ ", " $\neg r$ " og " $\neg p \Leftarrow r$ ",

når man lader p, q og r betegne henholdsvis " $2 \cdot 2 = 3$ ", " $7 + 5 = 8$ " og "9 er et lige tal". Vi opskriver sandhedstavler:

p	q	r	$p \wedge q \Rightarrow r$	$\neg r$	$\neg p \Leftarrow r$
s	s	s	s	f	f
s	s	f	f	s	s
s	f	s	s	f	f
s	f	f	s	s	s
f	s	s	s	f	s
f	s	f	s	s	f
f	f	s	s	f	s
f	f	f	s	s	f

Vi skal nu gå ud fra, at " $p \wedge q \Rightarrow r$ " og " $\neg r$ " begge er sande, dvs. det givne er, at vi for p, q, r har at gøre med en af kombinationerne sff, fsf, fff, og spørgsmålet er så, om der her ved sikres, at " $\neg p \Leftarrow r$ " har værdien s. Det er, som et blik på nederste række i tavlen viser, ikke tilfældet. Vi vil derfor ikke regne " $\neg p \Leftarrow r$ " for en (udsagns)logisk konsekvens af " $p \wedge q \Rightarrow r$ " og " $\neg r$ ", og dermed heller ikke c. for en (udsagns)logisk konsekvens af a. og b.

En udsagnsform siges altså at være en udsagnslogisk konsekvens af visse andre udsagnsformer (forudsætninger), når den har s i sandhedstavlen overalt, hvor alle forudsætningerne har det (gerne endnu flere steder). - Danner man konjunktionen af alle forudsætningerne og forbinder denne til den formodede konsekvens med et implikationstegn, i eksemplet

$$"[(p \wedge q \Rightarrow r) \wedge \neg r] \Rightarrow [\neg p \Leftrightarrow r]",$$

er betingelsen altså, at der opstår en tautologi.

Man taler også om udsagnslogisk konsekvens, efter at udsagn er indsat for de udsagnsvariable.

Vi anfører et par hyppigt benyttede slutningsmåder:

1. Af "p" og "p $\Rightarrow$ q" kan sluttes "q" (modus ponens),
thi

$$"p \wedge (p \Rightarrow q) \Rightarrow q"$$

er en tautologi.

2. Af "p $\Rightarrow$ q" og "q $\Rightarrow$ r" kan sluttes "p $\Rightarrow$ r" (kædeslutningsregel),
thi

$$"(p \Rightarrow q) \wedge (q \Rightarrow r) \Rightarrow (p \Rightarrow r)"$$

er en tautologi.

Endvidere bemærkes: Idet "(p $\wedge$ $\neg$ p) $\Rightarrow$ q" er en tautologi, har man, at af et udsagn og dets negation er et hvilket som helst udsagn en konsekvens. Et helt afgørende spørgsmål vedrørende en matematisk teori er derfor, om den rummer en modstrid; gør den det, vil den være uden nogensomhelst værdi.

B. Prædikatkalkylen.Prædikater (åbne udsagn).

Lad os eksempelvis betragte den velkendte matematiske sætning: "hvis et primtal går op i et produkt (af to naturlige tal), så går det op i mindst en af faktorerne".

Sætningen kan også formuleres: "hvis x er et primtal og x går op i yz , så går x op i y eller x går op i z ", - når det tilføjes (eller underforstås), at x , y og z refererer til de naturlige tal $1, 2, \dots$. Denne sidste formulering vil vi studere lidt nøjere:

Man bemærker, at de dele, der er knyttet sammen ved hjælp af "hvis...så...", "og", "eller", nemlig " x er et primtal", " x går op i yz ", " x går op i y ", " x går op i z ", slet ikke er udsagn; ingen af dem kan siges at være sand eller falsk. Dette hænger sammen med, at de indeholder individuevariable, nemlig x , y og z .

Vi kan f.eks. betragte " x er et primtal". Ganske vist er det ikke et udsagn, men i det øjeblik man lader den individvariable x betegne et bestemt naturligt tal, dvs. indsættes for x et naturligt tal, da får man et (sandt eller falsk) udsagn: " 3 er et primtal", " 4 er et primtal", " 15 er et primtal". Vi vil sige, at " x er et primtal" er et åbent udsagn eller et prædikat med én individvariabel refererende til (individ)området de naturlige tal. - Tilsvarende er " x går op i yz " et prædikat med tre individvariable: så snart der for x , y og z indsættes naturlige tal, fås et (sandt eller falsk) udsagn, f.eks. " 7 går op i $2 \cdot 6$ ".

Også prædikater forbindes med tegnene " $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$ " eller med de tilsvarende ord, hvorved igen fås åbne udsagn. Af " x er et primtal", " x går op i yz " kan man således danne

(1) "x er et primtal og x går op i yz";

af "x går op i y", "x går op i z" dannes f.eks.

(2) "x går op i y eller x går op i z".

Videre kan man danne "(1) $\Rightarrow$ (2)", altså

(3) "(x er et primtal) $\wedge$ (x går op i yz)
 $\Rightarrow$ (x går op i y) $\vee$ (x går op i z)",

i ord: "hvis x er et primtal og x går op i yz, så går x op i y eller x går op i z".

For såvel (1) som (2) forholder det sig således, at visse indsætninger for de variable giver et sandt, visse et falsk udsagn. For (3) derimod giver en hvilken som helst indsætning et sandt udsagn: Enhver indsætning, der gør (1) sand, gør også (2) og dermed (1) $\Rightarrow$ (2) sand, medens indsætninger, der gør (1) falsk, jo automatisk gør (1) $\Rightarrow$ (2) sand ifølge tabellen for " $\Rightarrow$ ". Vi vil sige, at (3) er gyldig inden for de naturlige tals område.

Generelt vil vi sige, at et prædikat er gyldigt, når det går over i et sandt udsagn for en hvilken som helst indsætning for udsagnets individvariable. Herved må det, medmindre misforståelser er udelukket, for hver variabel angives, fra hvilket individområde indsætning skal tages i betragtning.

Eksempelvis er

$$"x(y+z) = xy+xz"$$

gyldig i de naturlige tals område, ligeså inden for de rationale tal.

$$"x^m \cdot x^n = x^{m+n}"$$

er gyldig, når f.eks. x refererer til positive tal, m og n til hele tal (positive, negative samt 0).

Mange matematiske sætninger formuleres, ligesom den sætning,

hvor i vi tog vort udgangspunkt, som gyldige implikationer, altså på formen $(1) \Rightarrow (2)$, hvor (1) og (2) er åbne udsagn. Gyldigheden kommer her ud på, at enhver indsætning, der tilfredsstiller (1), også tilfredsstiller (2).

Eksempler:

$$"a < b \wedge c > 0 \Rightarrow ac < bc",$$

altså "hvis $a < b$ og $c > 0$, så er $ac < bc$ ", er gyldig f.eks. i de rationale tals område.

" f er differentiabel i $x \Rightarrow f$ er kontinuert i x " er gyldig, idet f refererer til reelle funktioner defineret på et interval I , medens x refererer til I 's punkter.

Anvendelsen i gyldige implikationer er nok den brug af "hvis...så", " $\Rightarrow$ ", som føles mest naturlig af den ikke specielt logisk skolede. Det ville imidlertid være meget ubekvemt kun at benytte " $\Rightarrow$ " i denne sammenhæng.

Kvantorer.

Hyppigt forekommende vendinger i matematikken er "for enhver gælder..." og "der findes (mindst) et...således at...". De angives i den matematiske logik ved tegnene " $\forall$ " og " $\exists$ ", kaldet henholdsvis alkvantor og eksistenskvantor.

Som eksempel kan vi betragte udsagnet

$$"\text{ ligningen } 2x^2 - 3x + 1 = 0 \text{ har en reel rod}."$$

Det betyder

"der findes (mindst) et reelt tal x , således at

$$2x^2 - 3x + 1 = 0",$$

hvilket skrives

$$"\exists x [2x^2 - 3x + 1 = 0]".$$

Man må dog, hvis det ikke fremgår af sammenhængen, yderligere

anføre det individområde, - her mængden $\mathbb{R}$ af reelle tal -, hvorefter talen er. Man skriver da

$$"\exists_{\mathbb{R}} x [2x^2 - 3x + 1 = 0]" \text{ eller } "\exists x \in \mathbb{R} [2x^2 - 3x + 1 = 0]" .$$

Betydningen af

$$"\forall_{\mathbb{R}} x [2x^2 - 3x + 1 = 0]" \text{ eller } "\forall x \in \mathbb{R} [2x^2 - 3x + 1 = 0]"$$

er: "for ethvert reelt tal x gælder $2x^2 - 3x + 1 = 0$ ", dvs. "ligningen $2x^2 - 3x + 1 = 0$ tilfredsstilles af ethvert reelt tal".

Medens " $2x^2 - 3x + 1 = 0$ " er et prædikat med én variabel, x , har vi, når " $\exists_{\mathbb{R}} x$ ", henholdsvis " $\forall_{\mathbb{R}} x$ ", sættes foran, et udsagn, sandt i første tilfælde, falsk i andet. Vi siger, at den variable x her optræder bundet. Når vi vil understrege, at en individvariabel ikke er bundet af en kvantor, siger vi, at den er fri.

Binder man i et prædikat med to frie variable den ene med en kvantor, fås et prædikat med én fri variabel. Eksempelvis er der i " $x^2 + y^2 > 1$ ", hvor både x og y tænkes at referere til de reelle tal, de to frie variable x og y , medens

$$"\forall y [x^2 + y^2 > 1]"$$

er et prædikat med den ene frie variabel x , ellers falsk for $-1 \leq x \leq 1$, ellers sandt. Binds også x , fås et udsagn; således er

$$"\exists x \forall y [x^2 + y^2 > 1]"$$

et sandt udsagn.

Generelt anbringes en kvantor foran et prædikat, hvorved én af de frie variable "forsvinder" eller "bindes". Det er uvæsentligt, hvilket bogstav der bruges for en bundet variabel, blot man vælger et, som ellers ikke forekommer i den pågældende sammenhæng (sml. integrationsvariablen i et bestemt integral og summationsindex i en sum som f.eks.

$$\sum_{n=1}^{\infty} \frac{1}{n!}).$$

Når flere kvantorer følger efter hinanden, får man i reglen

bedst overblik over meningen som angivet ved følgende eksempel:

$$"\forall x_1 \exists x_2 \exists x_3 \exists x_4 \forall x_5 \forall x_6 \dots"$$

læses "for ethvert x_1 findes x_2 , x_3 og x_4 , således at for ethvert x_5 og x_6 gælder...". Undertiden vil vi også skrive

$$"\forall x_1 \exists x_2, x_3, x_4 \forall x_5, x_6 \dots"$$

Vi bemærker, at en matematisk sætning, der er formuleret som et åbent udsagn gyldigt inden for en mængde M , også kan udtrykkes som et egentligt udsagn blot ved, at hver af de frie variable bindes med kvantoren " $\forall_M$ ".

Gyldigheden af

$$"x(y+z) = xy+xz"$$

inden for de reelle tal kan således udtrykkes ved, at udsagnet

$$"\forall_R x \forall_R y \forall_R z [x(y+z) = xy+xz]"$$

er sandt; tilsvarende kan

$$"a < b \wedge c > 0 \Rightarrow ac < bc"$$

erstattes af

$$"\forall a \forall b \forall c [a < b \wedge c > 0 \Rightarrow ac < bc]"$$

Prædikatkalkylens regler

kan angives under benyttelse af prædikativariable, for hvilke konkrete åbne udsagn så kan indsættes. F.eks. angives ved

$$"\forall y \forall x p(x,y)" \text{ eq } "\forall x \forall y p(x,y)",$$

$$"\exists y \exists x p(x,y)" \text{ eq } "\exists x \exists y p(x,y)",$$

at to på hinanden følgende kvantorer af samme art uden videre kan ombyttes. Her optræder en prædikativariable p med to argumenter, x og y . Udtryk som

$$"p(x,y)", "\forall x p(x,y)", "\forall y \forall x p(x,y)"$$

kalder vi prædikatformer (også når der, som i sidste tilfælde,

ved indsætning for $de(n)$ prædikatvariable fremkommer et udsagn).

I prædikatkalkylen kan man på tilsvarende måde som i udsagnskalkylen føre begreberne ækvivalens samt prædikatlogisk konsekvens af givne forudsætninger tilbage til prædikatlogiske tautologier eller, som man gerne siger, logiske identiteter. I modsætning til, hvad tilfældet var i udsagnskalkylen (sandhedstavler!), findes der imidlertid ingen simple kriterier til afgørelse af, om en forelagt prædikatform er en identitet, hvorfor det vil føre for vidt at gå nærmere ind på disse begreber.

Lad os blot nævne, at de ovenfor anførte ækvivalenser kommer ud på, at

$$"\forall y \forall x p(x,y) \iff \forall x \forall y p(x,y)",$$

$$"\exists y \exists x p(x,y) \iff \exists x \exists y p(x,y)"$$

er logiske identiteter. For to kvantorer af modsat art er der ikke ombyttelighed: kun

$$"\exists y \forall x p(x,y) \Rightarrow \forall x \exists y p(x,y)"$$

er en identitet. " $\forall x \exists y p(x,y)$ " er altså en konsekvens af " $\exists y \forall x p(x,y)$ ", men ikke omvendt. (Find selv en indsætning, en "interpretation", hvor " $\forall x \exists y p(x,y)$ " er sand, men " $\exists y \forall x p(x,y)$ " falsk).

To vigtige ækvivalenser er

$$"\neg \forall x p(x)" \text{ eq } "\exists x \neg p(x)",$$

$$"\neg \exists x p(x)" \text{ eq } "\forall x \neg p(x)",$$

kaldet de Morgans regler, idet de kan opfattes som generalisationer af reglerne med samme navn i udsagnskalkylen. Skrevet på formen

$$"\forall x p(x)" \text{ eq } "\neg \exists x \neg p(x)",$$

$$"\exists x p(x)" \text{ eq } "\neg \forall x \neg p(x)"$$

viser de iøvrigt, at man kunne undvære et af tegnene " $\forall$ ", " $\exists$ ".

Som eksempel på, hvorledes man af kendte ækvivalenser kan

afløede andre, anføres, at

$$\neg \forall x \exists y p(x,y) \text{ eq } \exists x \forall y \neg p(x,y)$$

fås ved succesiv anvendelse af de Morgans regler, nemlig

$$\neg \forall x \exists y p(x,y) \text{ eq } \exists x \neg \exists y p(x,y) \text{ eq } \exists x \forall y \neg p(x,y).$$

Generelt har man følgende regel: For en vilkårlig prædikat form dannet alene ved hjælp af tegnene $\neg, \wedge, \vee, \forall, \exists$ fås en med negationen ækvivalent prædikatform ved, at hver prædikatvariabel (og hver udsagnsvariabel) negeres, medens tegnene " $\wedge$ " og " $\vee$ " og ligeledes tegnene " $\forall$ " og " $\exists$ " ombyttes.

Eksempel:

$$\neg \forall x \exists y [p(x,y) \vee \exists z q(x,y,z)] \text{ eq } \exists x \forall y [\neg p(x,y) \wedge \forall z \neg q(x,y,z)]$$

(Ved hjælp af denne regel kan man overføre udsagnskalkylen dualitetsprincip til prædikatkalkylen. de Morgans regler er et eksempel på duale ækvivalenser).

I almindelighed vil vi i matematikken foretrække det mere smidige sædvanlige sprog for den matematiske logiks symboler. Det er dog herved en forudsætning, at hver vending, der bruges vort "matematiske sprog" tillægges en eksakt mening, som godt kan afvige mere eller mindre fra betydningen i dagligsproget.

I tvivlstilfælde kan det imidlertid være nyttigt at oversætte til den matematiske logiks symboler. Ved nogle eksempler vil vi således vise, hvilken støtte man kan få ved det ellers ofte vanskelige problem at finde en korrekt formulering for negationen af mere komplicerede matematiske udsagn:

1. Lad E_2 betegne mængden af punkter i en plan og Δ mængden af trekanter i planen. Afstanden mellem to punkter P og Q i planen betegner vi $|PQ|$. Udsagnet

$$"\forall_{\Delta} ABC \exists_{E_2} D [|AD| = |BD| = |CD|]",$$

dvs. "for enhver trekant i planen findes et punkt i planen, som har samme afstand fra hver af trekantens vinkelspidser", er som bekendt sandt. Negationen, som altså er falsk, kan formuleres

$$"\exists_{\Delta} ABC \forall_{E_2} D [|AD| \neq |BD| \vee |BD| \neq |CD|]";$$

herved er benyttet, at " $|AD| = |BD| = |CD|$ " er en kort skrivemåde for " $|AD| = |BD| \wedge |BD| = |CD|$ ".

2. Med $\mathbb{C}$ betegnes mængden af alle komplekse tal, med $\mathbb{N}$ mængden af alle naturlige tal. Udsagnet "hver binom ligning har (mindst) en kompleks rod" kan skrives

$$"\forall_{\mathbb{C}} a \forall_{\mathbb{N}} n \exists_{\mathbb{C}} z [z^n = a]".$$

Negationen, som er falsk, er

$$"\exists_{\mathbb{C}} a \exists_{\mathbb{N}} n \forall_{\mathbb{C}} z [z^n \neq a]",$$

dvs. "der findes et komplekst tal a og et naturligt tal n , således at $z^n \neq a$ for ethvert komplekst tal z ". Erstattes mængden $\mathbb{C}$ af komplekse tal med mængden $\mathbb{R}$ af reelle tal, bliver negationen sand ($a = -1$, $n = 2$), altså det oprindelige udsagn falsk.

3. Vi tænker os givet en reel funktion f defineret på et interval I samt et punkt a tilhørende I . Udsagnet " f er kontinuert i a " kan skrives

$$"\forall \varepsilon \exists \delta \forall x [|x-a| < \delta \Rightarrow |f(x)-f(a)| < \varepsilon]",$$

hvor ε og δ refererer til positive reelle tal, medens x refererer til tal i I ; i kraft af ækvivalensen " $p \Rightarrow q$ " eq " $p \vee q$ " kan vi omformulere til

$$"\forall \varepsilon \exists \delta \forall x [|x-a| \geq \delta \vee |f(x)-f(a)| < \varepsilon]".$$

Negationen er da

$$"\exists \varepsilon \forall \delta \exists x [|x-a| < \delta \wedge |f(x)-f(a)| \geq \varepsilon]",$$

dvs. "der findes et $\varepsilon > 0$, således at der til ethvert $\delta > 0$ findes et punkt x tilhørende I , for hvilket ulighederne

$$|x-a| < \delta, \quad |f(x)-f(a)| \geq \varepsilon$$

begge er opfyldt". Dette er altså indholdet af udsagnet "f er ikke kontinuert i a".

En matematisk teori består af visse forudsætninger, aksiomerne, samt konsekvenser deraf. Forudsætninger og konsekvenser kaldes under et for teoriens sætninger eller teoremer. At bevise en sætning vil sige at aflede den ud fra aksiomerne ved hjælp af visse slutningsregler; det vil dog (ifølge kædeslutningsregel) være tilstrækkeligt at føre en sætning tilbage til nogle allerede kendte. Et par eksempler på hyppigt anvendte slutningsregler:

Et teorem af formen " $(1) \Rightarrow (2)$ " kan vises ved, at man (midlertidigt) til teoriens forudsætninger føjer " (1) " og derpå fører et bevis for " (2) ",

antag: " (1) ", bevis: " (2) ".

For sætningen "hvis x er et primtal og x går op i yz , så går x op i y eller x går op i z " (se side 16-17) ser opstillingen således ud:

antag: " x er et primtal og x går op i yz ",

bevis: " x går op i y eller x går op i z ".

Under beviset behandles eventuelle frie variable i " $(1) \Rightarrow (2)$ " som konstanter; - i eksemplet tænker man sig således under bevisførelsen, at x, y og z betegner bestemte tal, hvorom man dog ikke ved andet, end antagelsen siger.

Bemærkning. Idet " $(1) \Rightarrow (2)$ " jo kan omformuleres til " $\neg(2) \Rightarrow \neg(1)$ " (kontraposition), kan man i stedet til teoriens

forudsætninger føje " $\neg(2)$ " og derpå føre et bevis for " $\neg(1)$ ",
antag: " $\neg(2)$ ", bevis: " $\neg(1)$ ".

I vort eksempel:

antag: " $\neg(x$ går op i y eller x går op i $z)$ ",

dvs. " x går ikke op i y og x går ikke op i z ";

bevis: " x er ikke et primtal eller x går ikke op i yz ",

dvs. "hvis x er et primtal, så går x ikke op i yz ".

Et indirekte bevis (reductio ad absurdum) føres ved, at man (midlertidigt) til teoriens forudsætninger føjer negationen af det formodede teorem og derpå søger at udlede en modstrid. Eventuelle frie variable i teoremet behandles herunder som konstanter.

For et teorem af typen " $(1) \Rightarrow (2)$ " består et indirekte bevis således i udledning af en modstrid ud fra teoriens forudsætninger med tilføjelse af antagelsen " $\neg[(1) \Rightarrow (2)]$ ", dvs.

$$(1) \wedge \neg(2).$$

I vort eksempel ovenfor ville antagelsen i et indirekte bevis være

" x er et primtal og x går op i yz ,

men x går ikke op i y og x går ikke op i z ";

her skal x , y og z behandles som konstanter, dvs. under udledelsen af en modstrid tænker man sig, at x , y og z betegner bestemte tal.

§ 2. Mængder og deres delmængder.

Ved en mængde forstås i daglig tale en, undertiden ikke særlig velafgrænset, samling af indbyrdes forskellige objekter. Når der i matematikken tales om en mængde, skal det være utvetydigt fastlagt, hvilke objekter der hører med til den (et krav, som ved ikke-matematiske objekter ikke altid vil kunne opfyldes). De objekter, som udgør en mængde kaldes dens elementer. Både mængder og elementer betegnes med bogstaver eller andre aftalte tegn. At et objekt a er element af mængden A (tilhører A , er indeholdt i A), skrives

$$a \in A,$$

og at a ikke er element af A (ikke tilhører A , ikke er indeholdt i A) skrives

$$a \notin A.$$

At det ovenfor nævnte krav er opfyldt, kommer ud på, at $a \in A$ for hvert forelagt objekt a (blandt dem, som overhovedet tages i betragtning ved den pågældende undersøgelse) er et udsagn, som er sandt, når a tilhører A , og falsk, når a ikke tilhører A . Dette udsagns negation er $a \notin A$.

En mængde kan være givet ved en opremsning af dens elementer, og den angives da ved at sætte elementerne (i en eller anden orden) i en krøllet parentes. For eksempel betegner

$$\{a, b, 5, z, 3, 9, i\}$$

mængden, hvis elementer er bogstaverne a, b, z og cifrene $3, 5, 9$. Denne betegnelses måde kan dog i reglen kun bruges ved endelige mængder, d.v.s. mængder, der består af endelig mange elementer. En uendelig mængde må fastlægges ved angivelse af en eller flere egenskaber, som dens elementer, men ikke nogen andre objekter har. Dette kan ske i almindeligt sprog eller ved hjælp af symbo-

let

$$\{\dots \mid \dots\}.$$

Til venstre for den lodrette streg sættes et tegn, i reglen et bogstav, for eksempel x , som står for et vilkårligt objekt tilhørende samlingen af de objekter, som tages i betragtning. Såfremt det ikke er klart på forhånd, hvilken samling M af objekter talen er om, skrives $x \in M$. Til højre for strengen angives ved en udsagnsform $p(x)$ de for mængdens elementer karakteristiske egenskaber. For hvert enkelt objekt a fra M er altså $p(a)$ et udsagn, som er sandt, når a har de pågældende egenskaber, og ellers falsk. Betegnelsen for mængden af de objekter fra M , som har egenskaberne, bliver da

$$\{x \in M \mid p(x)\}$$

eller, når det fremgår af sammenhængen, hvilken slags objekter der tages i betragtning, blot

$$\{x \mid p(x)\},$$

og dette læses: "mængden af de objekter x fra M (elementer i M), for hvilke $p(x)$ er sandt" eller "... , som har egenskaberne..." eller "... , som opfylder betingelserne..." eller lignende. Man kan også tale om "sandhedsmængden" for udsagnsformen $p(x)$. Det er klart, at der i stedet for x kan sættes et vilkårligt andet tegn, som ikke er brugt til et andet formål; $\{\xi \in M \mid p(\xi)\}$ eller $\{\xi \mid p(\xi)\}$ betegner altså den samme mængde. For hvert enkelt objekt a fra M er $a \in \{x \mid p(x)\}$ det samme udsagn som $p(a)$. Som et eksempel nævnes, at mængden af de reelle tal x , som opfylder ulighederne $1 \leq x < 2$, kan med betegnelsen $\mathbb{R}$ for mængden af alle reelle tal skrives

$$\{x \in \mathbb{R} \mid 1 \leq x < 2\}$$

eller $\{x \mid 1 \leq x < 2\}$, hvis misforståelser er udelukket. At

$a \in \{x \mid 1 \leq x < 2\}$, betyder ikke andet end $1 \leq a < 2$.

En mængdes elementer kan selv være mængder. Idet en ret linie kan opfattes som mængden af sine punkter, vil en mængde af rette linier være et eksempel herpå.

For nogle hyppigt forekommende mængder indføres betegnelser, som uden videre forklaring vil blive brugt overalt i det følgende:

$\mathbb{N}$ = mængden af alle naturlige (d.v.s. positive hele) tal,

$\mathbb{N}_0$ = mængden af alle ikke-negative hele tal,

$\mathbb{Z}$ = mængden af alle hele tal,

$\mathbb{Q}$ = mængden af alle rationale tal,

$\mathbb{Q}_+$ = mængden af alle positive rationale tal,

$\mathbb{R}$ = mængden af alle reelle tal,

$\mathbb{R}_+$ = mængden af alle positive reelle tal,

$\mathbb{C}$ = mængden af alle komplekse tal.

Når en undersøgelse kun vedrører een ret linie (een plan), betegnes mængden af dens punkter med E_1 (E_2). Mængden af rummets punkter betegnes med E_3 .

To mængder A og B siges at være lig med hinanden, og man skriver

$$A = B,$$

når de indeholder de samme elementer, d.v.s. når hvert element indeholdt i A også er indeholdt i B og omvendt. I logiske tegn kan dette skrives

$$\forall_M x [(x \in A) \iff (x \in B)].$$

Man har altså for eksempel

$$\{a,b,c,d\} = \{b,c,a,d\},$$

$$\{p \in \mathbb{N} \mid p \text{ er et primtal og lige}\} = \{2\},$$

$$\{x \in \mathbb{R} \mid x^2 - 3x + 2 = 0\} = \{r \in \mathbb{Q} \mid r^2 - 3r + 2 = 0\} = \{1,2\},$$

$$\begin{aligned} \{x \in \mathbb{R} \mid \sin x = 0\} &= \{y \in \mathbb{R} \mid \cos 2y = 1\} \\ &= \{z \in \mathbb{R} \mid \exists_{\mathbb{Z}} p [z = p\pi]\}. \end{aligned}$$

At to mængder A og B ikke er lig med hinanden, er forskellige, d.v.s. at der findes mindst eet element i en af mængderne, som ikke tilhører den anden, skrives

$$A \neq B.$$

Idet lighedstegnet her benyttes til at udtrykke, at to symboler er navne for den samme ting, er det klart, at man har følgende regler for dets brug:

Refleksivitet: Der gælder altid $A = A$.

Symmetri: Hvis $A = B$, så gælder også $B = A$.

Transitivitet: Hvis $A = B$ og $B = C$, så gælder også $A = C$.

Det bemærkes, at der for tegnet $\Leftrightarrow$ for logisk ækvivalens gælder de samme regler, hvilket fremgår af, at det udtrykker overensstemmelse af sandhedstabeller for sammensatte udsagn. I § 1 blev disse regler benyttet stiltiende.

Af formelle grunde er det hensigtsmæssigt at indføre begrebet tom mængde. Herunder forstås en mængde, der ikke indeholder noget element, f.eks. mængden af alle ligesidede, retvinklede trekanter i planen. Hvilkesomhelst to tomme mængder sættes lig hinanden, hvilket jo også harmonerer med ovenstående definition af lighed, idet to tomme mængder indeholder de samme elementer, nemlig ingen. Man taler altså om den tomme mængde. Den betegnes med $\emptyset$. Man har altså f.eks.:

$$\{x \in \mathbb{R} \mid x^2 < 0\} = \emptyset.$$

Det bemærkes, at det er nødvendigt at skelne mellem en mængde, der kun indeholder eet element, og dette element selv, altså mellem $\{a\}$ og a . Mængden $\{\emptyset\}$, for eksempel, indeholder et element, nemlig $\emptyset$, medens $\emptyset$ selv ifølge definition ikke indeholder noget element. I mange tilfælde, hvor der ikke er fare for misforståelser, tillader man sig dog at skrive a i stedet for $\{a\}$.

En mængde A siges at være en delmængde af mængden B , når hvert element af A også tilhører B , i logiske tegn

$$\forall_M x [(x \in A) \Rightarrow (x \in B)].$$

Man skriver da

$$A \subseteq B \quad \text{eller} \quad B \supseteq A$$

og siger, at A er indeholdt i B , eller at B indeholder A . Det er vigtigt at lægge mærke til, at ifølge denne definition er enhver mængde delmængde af sig selv, altså at der for enhver mængde B gælder

$$B \subseteq B.$$

At mængden A ikke er en delmængde af mængden B , skrives

$$A \not\subseteq B \quad \text{eller} \quad B \not\supseteq A.$$

Dette betyder altså, at der findes mindst eet element i A , som ikke tilhører B .

Til en mængdes delmængder regnes også den tomme mængde, hvilket harmonerer med delmængdens definition, idet udsagnet

$$\forall_M x [(x \in \emptyset) \Rightarrow (x \in B)]$$

er sandt for enhver mængde B , da $x \in \emptyset$ jo er falsk for ethvert objekt x . Man har altså for hver mængde B

$$\emptyset \subseteq B.$$

Vil man udtrykke, at A er en ægte eller egentlig delmængde, skriver man

$$A \subset B \quad \text{eller} \quad B \supset A.$$

Dette er altså ensbetydende med, at A er delmængde af B , og der findes mindst eet element i B , som ikke tilhører A . At A ikke er en ægte delmængde af B skrives

$$A \not\subset B \quad \text{eller} \quad B \not\supset A.$$

(Mange matematikere bruger ikke tegnene $\subseteq$ og $\supseteq$, men kun $\subset$ og $\supset$ til at betegne, at en mængde er en (ægte eller ikke ægte) delmængde af en anden. At A er ægte delmængde af B må da skrives $A \subset B$, $A \not\supset B$. I det følgende bruges $\subseteq$ og $\supseteq$ for stedse at minde om, at $B \subseteq B$.)

For brugen af tegnet $\subseteq$ gælder nogle simple regler, der enten allerede er nævnt eller umiddelbart følger af definitionerne:

Refleksivitet: Der gælder altid $A \subseteq A$.

Asymmetri: Hvis $A \not\subseteq B$ og $A \subseteq B$, gælder $B \not\subseteq A$.

Transitivitet: Hvis $A \subseteq B$ og $B \subseteq C$, gælder $A \subseteq C$.

Tilsvarende gælder naturligvis for $\supseteq$. Man lægger mærke til, at disse regler ganske svarer til dem, der gælder for henholdsvis $\leq$ og $\geq$.

For $\subset$ (og $\supset$) har man regler, som svarer til dem, der gælder for $<$ (og $>$), og som afviger fra de nævnte ved, at refleksiviteten erstattes med: Der gælder altid $A \not\subset A$. (Asymmetrien forenkles til: Hvis $A \subset B$, gælder $B \not\subset A$.)

Endelig nævnes, at man af $A \subseteq B \subset C$ eller af $A \subset B \subseteq C$ kan slutte, at $A \subset C$.

En relation mellem to mængder, som udtrykkes ved et af tegnene $\subseteq$, $\supseteq$, $\subset$, $\supset$, kaldes en inklusion.

Lad $p(x)$ og $q(x)$ være to udsagnsformer vedrørende objekterne x tilhørende en mængde M og

$$A = \{x \in M \mid p(x)\}, \quad B = \{x \in M \mid q(x)\}$$

deres sandhedsmængder. At A er delmængde i B kommer da ud på,

at det for hvert x fra M gælder, at hvis $p(x)$ er sandt, så er $q(x)$ også sandt. Med andre ord, $A \subseteq B$ er ensbetydende med

$$\forall_M x [p(x) \Rightarrow q(x)].$$

Dette benytter man sig af ved løsning af ligninger og uligheder. Mængden af de tal, talpar, ..., som tilfredsstiller en ligning, en ulighed, et system af ligninger eller uligheder, kaldes løsningsmængden. Når man foretager en omformning, en reduktion af en given ligning, erstatter man den med en anden, om hvilken man ved, at den er opfyldt for alle de værdier af den ubekendte, for hvilke den oprindelige er opfyldt. Den oprindelige lignings løsningsmængde er altså en delmængde af den nye lignings løsningsmængde. Tilsvarende gælder for uligheder og systemer af ligninger og uligheder. Dette illustreres ved et eksempel: Man har

$$\forall_{\mathbb{R}} x [(x + \sqrt{1-x} = -1) \Rightarrow (x^2 + 3x = 0)],$$

hvilket viser, at løsningsmængden for $x + \sqrt{1-x} = -1$ er en delmængde af løsningsmængden $\{-3, 0\}$ for $x^2 + 3x = 0$. En prøve viser, at den er $\{-3\}$.

Ud fra en given mængde A kan man danne en ny mængde, nemlig mængden af alle dens delmængder. Vi vil betegne den med $\mathcal{D}(A)$.

Er f.eks.

$$A = \{a, b, c\},$$

fås

$$\mathcal{D}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}.$$

Opgaven at bestemme antallet af delmængder i en endelig mængde A bestående af n elementer hænger nøje sammen med et kendt kombinatorisk problem. Man kan tænke sig, at elementerne af A er n pladser, som skal besættes med to slags brikker (f.eks. hvide og sorte) eller, lad os sige, med cifrene 0 og 1. Man spørger,

på hvor mange forskellige måder dette kan gøres. Til hver fordeling af 0 og 1 på de n pladser svarer en bestemt delmængde af A , bestående af netop de pladser, som er besat med 1, og omvendt hører der til enhver delmængde af A en bestemt fordeling af 0 og 1, nemlig den, hvor delmængdens pladser er besat med 1 og de øvrige med 0; specielt svarer til den tomme mængde den fordeling, ved hvilken alle pladser er besat med 0, og til selve mængden A den, ved hvilken alle pladser er besat med 1. Heraf ses, at det omspurgte antal er lig med antallet af delmængder i A .

Lad der være givet en endelig mængde A bestående af n elementer, og lad p betegne et bestemt af tallene $0, 1, \dots, n$. En delmængde af A bestående af p elementer plejer man at kalde en kombination af p elementer blandt de n . At bestemme antallet $K_{n,p}$ af disse kombinationer er altså ensbetydende med bestemmelsen af antallet af de delmængder af A , som hver består af p elementer.

Øvelser til kap. I, § 2.

1. Søg simple beskrivelser af følgende talmængder:

$$\{x \in \mathbb{Z} \mid \exists_{\mathbb{Z}} m [x = 2m + 1]\},$$

$$\{x \in \mathbb{Z} \mid \exists_{\mathbb{Z}} m [x = 3m]\},$$

$$\{x \in \mathbb{N} \mid \forall_{\mathbb{N}} m, n [(x = mn) \Rightarrow ((m = 1) \vee (n = 1))]\},$$

$$\{x \in \mathbb{Q} \mid \exists_{\mathbb{N}} n [10^n x \in \mathbb{Z}]\},$$

$$\{x \in \mathbb{R} \mid \forall_{\mathbb{Z}} m \forall_{\mathbb{N}} n [x \neq \frac{m}{n}]\}.$$

2. Bestem løsningsmængderne

$$\{x \mid |x - 1| + |x + 1| = 2\},$$

$$\{x \mid |2x + 1| = x\},$$

$$\{x \mid |2x - 1| < 3\},$$

$$\{x \mid |x^2 - 2| \geq 2\},$$

$$\{x \mid |x(x-2)| > 0\},$$

hvor det er underforstået, at $x \in \mathbb{R}$.

Sammenlign de tre sidste med henholdsvis $\{x \mid 2x - 1 < 3\}$, $\{x \mid x^2 - 2 \geq 2\}$ og $\{x \mid x(x-2) > 0\}$, og gør rede for eventuelle inklusioner.

3. Der er givet to forskellige punkter A og B i en plan E_2 , og det er underforstået, at $P \in E_2$. Afstanden mellem to punkter P og Q i planen betegnes med $|PQ|$. Giv geometriske beskrivelser af punktmængderne

$$\{P \mid |AP| + |BP| = |AB|\},$$

$$\{P \mid |AP| - |BP| \geq |AB|\},$$

$$\{P \mid |AP|^2 + |BP|^2 < 2|AB|^2\}.$$

4. I det følgende betegner (x, y) et vilkårligt par af reelle tal. Efter valg af et sædvanligt retvinklet koordinatsystem i planen E_2 svarer der til hvert sådant par et punkt i planen, og omvendt. Angiv ved figurer de punktmængder, som

svarer til følgende mængder af talpar:

- a) $\{(x,y) \mid x = y\}$ og $\{(x,y) \mid |x| = |y|\}$,
 b) $\{(x,y) \mid x + y = 1\}$ og $\{(x,y) \mid |x| + |y| = 1\}$,
 c) $\{(x,y) \mid x - 2y^2 + 1 = 0\}$ og
 $\{(x,y) \mid \exists_{\mathbb{R}} t [(x = \cos 2t) \wedge (y = \cos t)]\}$,
 d) $\{(x,y) \mid xy = 1\}$ og
 $\{(x,y) \mid \exists_{\mathbb{R}} t [(x = \operatorname{tg} t) \wedge (y = \cot t)]\}$,
 e) $\{(x,y) \mid x^2 + y^2 = 1\}$ og
 $\left\{ (x,y) \mid \exists_{\mathbb{R}} t \left[x = \frac{1-t^2}{1+t^2} \wedge \left(y = \frac{2t}{1+t^2} \right) \right] \right\}$.

Konstater i hvert af tilfældene a) - e) eventuelle inklusioner, og eftervis dem.

5. Et system af to førstegradslikninger med to ubekendte

$$a_1x + b_1y = c_1$$

$$a_2x + b_2y = c_2$$

løses hyppigt ved "de lige store koefficienters metode". Denne består i, at man ved multiplikation af ligningerne med passende tal og påfølgende subtraktion udleder et nyt system af to ligninger, som hver kun indeholder een af de ubekendte x og y . Vil løsningsmængderne for de to ligningssystemer (d.v.s. mængderne af de talpar (x,y) , som tilfredsstiller dem) stemme overens, hvilke værdier de givne tal $a_1, b_1, c_1, a_2, b_2, c_2$ end har?

6. I planen tænkes valgt et sædvanligt retvinklet koordinatsystem. Der er givet to cirkler

$$\{(x,y) \mid (x+1)^2 + y^2 = 4\} \text{ og } \{(x,y) \mid (x-1)^2 + y^2 = 1\}.$$

Find for mængden af de punkter i planen, hvorfra tangenterne til de to cirkler er lige store, en fremstilling af formen $\{(x,y) \mid p(x,y)\}$, hvor $p(x,y)$ er en udsagnsform om punkternes koordinatpar (x,y) .

7. Bestem antallet af delmængder af en mængde bestående af n elementer.
8. Vis ud fra definitionen af $K_{n,p}$ som antallet af de delmængder af en mængde bestående af n elementer, som indeholder p elementer, at der for $1 \leq p \leq n$ gælder

$$K_{n,p} = K_{n-1,p} + K_{n-1,p-1},$$

$$p K_{n,p} = n K_{n-1,p-1},$$

$$p K_{n,p} = (n-p+1) K_{n,p-1}.$$

Benyt en af disse formler til at vise, at

$$K_{n,p} = \binom{n}{p} = \frac{n(n-1) \cdots (n-p+1)}{1 \cdot 2 \cdots p}.$$

§ 3. Mængdealgebra.

Lad der være givet en mængde E . I det følgende drejer det sig om at undersøge forskellige forbindelser mellem denne mængdes delmængder. Idet der herved ses bort fra alt uden for E , plejer man i denne sammenhæng at kalde E for universalmængden. Det vedtages for denne paragrafs vedkommende, at små latinske bogstaver betegner (når andet ikke er fremhævet) elementer af E . Idet dette er underforstået, er $x \in E$ et udsagn, som er sandt for hvert x , og $x \notin E$ et udsagn, som er falsk for hvert x . Store latinske bogstaver betegner (når andet ikke er fremhævet) delmængder af E . Vælger man som universalmængde mængden af planens punkter, og tænker man på delmængder, der er begrænsede af simple kurver, f.eks. på cirkelskiver, kan de fleste af de følgende betragtninger anskueliggøres ved diagrammer.

Ud fra en mængde A kan der dannes en ny mængde, kaldet dens komplementærmængde eller komplement. Den består af alle de elementer af E , som ikke tilhører A . Den betegnes med $\bar{A}$. Man har altså

$$\bar{A} = \{x \mid \text{non}(x \in A)\} = \{x \mid x \notin A\}.$$

Ud fra to givne mængder A og B kan der dannes en ny mængde, som består af alle de elementer, der tilhører både A og B . Den kaldes fællesmængden (eller gennemsnittet) af A og B og betegnes med $A \cap B$. Dens definition kan skrives

$$A \cap B = \{x \mid (x \in A) \wedge (x \in B)\}.$$

Endvidere kan man danne mængden af de elementer, som tilhører mindst een af mængderne A og B . Den kaldes de to mængders foreningsmængde og betegnes med $A \cup B$. Dens definition kan skrives

$$A \cup B = \{x \mid (x \in A) \vee (x \in B)\}.$$

For de forskrifter til dannelse af nye mængder ud fra givne, som symboliseres ved tegnene $\bar{C}$, $\cap$ og $\cup$, gælder følgende regler:

$A \cap B = B \cap A$	(kommutative love)
$A \cup B = B \cup A$	
$A \cap (B \cap C) = (A \cap B) \cap C$	(associative love)
$A \cup (B \cup C) = (A \cup B) \cup C$	
$A \cap A = A$	(idempotenslove)
$A \cup A = A$	
$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$	(distributive love)
$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	
$A \cap (A \cup B) = A$	(absorptionslove)
$A \cup (A \cap B) = A$	
$\bar{\bar{C}}A = A$	($\bar{C}$ er involutorisk)
$\bar{C}(A \cap B) = \bar{C}A \cup \bar{C}B$	(dualitetslove)
$\bar{C}(A \cup B) = \bar{C}A \cap \bar{C}B$	
$\emptyset = A \cap \bar{C}A$	(tom mængde)
$E = A \cup \bar{C}A$	(universalmængde)
$\bar{C}\emptyset = E$	
$\bar{C}E = \emptyset$	
$\emptyset \cap A = \emptyset$	
$E \cup A = E$	
$E \cap A = A$	
$\emptyset \cup A = A$	

Det ses, at disse regler stemmer overens med dem, der gælder for udsagn, idet der til $\bar{C}$, $\cap$, $\cup$ og $=$ svarer henholdsvis non, $\wedge$, $\vee$ og $\Leftrightarrow$ (jfr. side I,1,8). Denne overensstemmelse er ikke tilfældig. Den fremgår umiddelbart af den måde, på hvilken de logiske forbindelser optræder i komplementærmængdens, fællesmængdens og foreningsmængdens definition. Til hver udsagnsform $p(x)$ om elementerne i E svarer en delmængde af E , nemlig sandhedsmængden for $p(x)$. Til logisk ækvivalente (sammensatte) udsagnsformer svarer den samme delmængde. Omvendt er hver delmængde A af E sand-

hedsmængde for en udsagnsform, nemlig f.eks. $x \in A$. Er

$$A = \{x \mid p(x)\}, \quad B = \{x \mid q(x)\},$$

har man

$$CA = \{x \mid \text{non } p(x)\},$$

$$A \cap B = \{x \mid p(x) \wedge q(x)\}, \quad A \cup B = \{x \mid p(x) \vee q(x)\}.$$

Opfattet som "bogstavregning" foregår altså "regning med mængder", bortset fra betegnelserne, efter de samme regler som "regning med udsagn". For hver universalmængde E er altså "mængdealgebraen" et eksempel på en Boole'sk algebra (se side I,1,8).

To mængder A og B siges at være disjunkte (eller elementfremmede), hvis de ikke har noget element fælles, hvis altså

$$A \cap B = \emptyset.$$

Det har vist sig at være hensigtsmæssigt at indføre en særlig betegnelse og et navn for mængden af de elementer af E , der tilhører en given mængde B , men ikke tilhører en given mængde A . Det ses, at denne mængde, der betegnes med $B \setminus A$ og kaldes overskudsmængden af B over A , differensmængden mellem B og A eller komplementet af A relativ til B , ikke er andet end fællesmængden af B og CA

$$B \setminus A = \{x \mid (x \in B) \wedge (x \notin A)\} = B \cap CA.$$

Specielt have

$$E \setminus A = CA,$$

og

$$A \setminus A = A \setminus E = \emptyset, \quad A \setminus \emptyset = A.$$

To mængder A og B er disjunkte, hvis og kun hvis $B \setminus A = B$.

Mellem de indførte mængdeoperationer C , $\cap$, $\cup$ og inklusionen $\subseteq$ består der nogle simple forbindelser.

Det er indlysende, at

$$A \subseteq B \iff CB \subseteq CA.$$

Idet $A = B$ er ensbetydende med $A \subseteq B$ og $B \subseteq A$, haves følgende

$$\begin{aligned} A = B &\iff (A \subseteq B) \wedge (B \subseteq A) \\ &\iff (CB \subseteq CA) \wedge (B \subseteq A) \\ &\iff (A \subseteq B) \wedge (CA \subseteq CB) \\ &\iff (CB \subseteq CA) \wedge (CA \subseteq CB). \end{aligned}$$

Man benytter sig hyppigt heraf i beviser for, at to på forskellig måde definerede mængder stemmer overens. "At bestemme et geometrisk sted" (en antikveret glose) går ud på at vise, at mængden

A af punkter, der har en vis egenskab, også kan karakteriseres på anden måde, f.eks. som mængden B af punkter på en vis kurve. At vise f.eks., at hvert punkt, der har egenskaben, tilhører B, og at hvert punkt, der ikke har egenskaben, ligger udenfor B, vil sige at vise, at $A \subseteq B$ og $CA \subseteq CB$.

Af definitionerne følger, at der for vilkårlige delmængder A og B af E gælder

$$\emptyset \subseteq A \cap B \subseteq \left\{ \begin{array}{c} A \\ B \end{array} \right\} \subseteq A \cup B \subseteq E.$$

Ifølge de associative love er der mening i at tale om fællesmængden $A \cap B \cap C$ og om foreningsmængden $A \cup B \cup C$ af tre mængder. De kan dog naturligvis også defineres direkte, nemlig henholdsvis som mængden af alle elementer af E, som tilhører alle tre mængder, og som mængden af de elementer af E, der tilhører mindst een af de tre mængder. Disse definitioner kan generaliseres til et vilkårligt, endeligt eller uendeligt antal mængder.

Lad Φ betegne en mængde af delmængder af E. Ved fællesmængden af mængderne tilhørende Φ forstås mængden af de elementer af E, der hvert tilhører alle mængder $A \in \Phi$. I tegn

$$\bigcap_{A \in \Phi} A = \{x \mid \forall_{\Phi} A [x \in A]\}$$

Ved foreningsmængden af mængderne tilhørende Φ forstås mængden af de elementer, der hvert tilhører mindst een af mængderne $A \in \Phi$. I tegn

$$\bigcup_{A \in \Phi} A = \{x \mid \exists_{\Phi} A [x \in A]\}.$$

I disse symboler kan A (lige som et summationsbogstav) erstattes med et andet bogstav, uden at deres betydning ændres. For fællesmængdens komplementærmængde fås

$$\begin{aligned} C \bigcap_{A \in \Phi} A &= \{x \mid \text{non } \forall_{\Phi} A [x \in A]\} \\ &= \{x \mid \exists_{\Phi} A [x \notin A]\} = \{x \mid \exists_{\Phi} A [x \in CA]\}, \end{aligned}$$

altså

$$C \bigcap_{A \in \Phi} A = \bigcup_{A \in \Phi} CA.$$

Tilsvarende findes for foreningsmængdens komplementærmængde

$$C \bigcup_{A \in \Phi} A = \bigcap_{A \in \Phi} CA.$$

Disse formler, der svarer til dualitetslovene (de Morgan's formler) for kvantorer, kaldes af nogle forfattere ligeledes for de Morgan's formler. Deres indhold kan kort gengives således: Fællesmængdens komplement er komplementernes foreningsmængde, og foreningsmængdens komplement er komplementernes fællesmængde.

En samling af delmængder af E kan være bestemt ved, at der efter en eller anden forskrift til hvert element ι i en såkaldt indexmængde J (som almindeligvis ikke er indeholdt i E) svarer en mængde $A_{\iota} \subseteq E$. Det er herved ikke udelukket, at der til forskellige elementer fra J svarer den samme mængde. Mængden af de indbyrdes forskellige blandt mængderne A_{ι} betegnes med $\{A_{\iota} \mid \iota \in J\}$, og dens fællesmængde og foreningsmængde skrives

$$\bigcap \{A_\iota \mid \iota \in J\} = \bigcap_{\iota \in J} A_\iota, \quad \bigcup \{A_\iota \mid \iota \in J\} = \bigcup_{\iota \in J} A_\iota.$$

I de specielle tilfælde $J = \{1, 2, \dots, m\}$ og $J = \mathbb{N}$ bruges henholdsvis også skrivemåderne

$$\bigcap_{\iota=1}^m A_\iota = A_1 \cap \dots \cap A_m, \quad \bigcup_{\iota=1}^m A_\iota = A_1 \cup \dots \cup A_m$$

og

$$\bigcap_{\iota=1}^{\infty} A_\iota = A_1 \cap A_2 \cap \dots, \quad \bigcup_{\iota=1}^{\infty} A_\iota = A_1 \cup A_2 \cup \dots.$$

I alle disse symboler kan ι (lige som et summationsbogstav) erstattes med et andet bogstav, uden at deres betydning ændres.

Ved en overdækning af en mængde $M \subseteq E$ forstås en mængde Φ af delmængder af E , for hvilken

$$M \subseteq \bigcup_{A \in \Phi} A.$$

En overdækning Φ af M siges at være en klasseinddeling af M , når mængderne i Φ er disjunkte (d.v.s. hvilket som helst to af dem er disjunkte) og

$$M = \bigcup_{A \in \Phi} A.$$

Dette er ensbetydende med følgende: Mængderne i Φ er delmængder af M , og hvert element i M tilhører en og kun een af disse mængder (som da benævnes klasser).

Øvelser til kap. I, § 3.

1. Lad universalmængden E være mængden af alle reelle tal.

a) Gør rede for, at

$$\{x \mid x^2 < 1\} = \{x \mid x < 1\} \cap \{x \mid x > -1\}.$$

Angiv et lignende udtryk for $\{x \mid x^2 \geq 1\}$.

b) Lad $a < b < c$ være givne reelle tal. Udtryk mængden

$\{x \mid (x-a)(x-b)(x-c) > 0\}$ ved mængder af formen $\{x \mid x > d\}$,

hvor d er et af tallene a , b eller c .

Angiv et lignende udtryk for komplementærmængden.

2. Lad E være mængden af alle par (x,y) af reelle tal. Fremstil hver af følgende mængder som fællesmængde eller foreningsmængde af to mængder med simplere definitioner:

$$\{(x,y) \mid (x+y+1 > 0) \wedge (xy \geq 0)\},$$

$$\{(x,y) \mid (x \leq y) \vee (x^2+y^2 < 1)\},$$

$$\{(x,y) \mid (x^2+y^2-1)(x^2-y^2) = 0\},$$

$$\{(x,y) \mid (x^2+y^2-1)^2 + (x^2-y^2)^2 = 0\}.$$

Angiv mængderne ved figurer, idet talparrene fortolkes som par af sædvanlige retvinklede koordinater for punkter i planen.

3. Lad E være mængden af punkter i planen.

Angiv for to givne punkter A og B mængden af de punkter P , hvis afstand $|PA|$ fra A er mindre end afstanden $|PB|$ fra B .

Lad der være givet en trekant ABC og et punkt D . Bestem mængden M af de punkter P i planen, for hvilke afstanden $|PD|$ er mindre end hver af afstandene $|PA|$, $|PB|$, $|PC|$. Tegn figurer, der viser, at M kan være tom, begrænset eller ubegrænset alt efter beliggenheden af D .

Giv en til definitionen af M svarende karakterisering af komplementærmængden til M .

4. Lad E være mængden af punkter i planen, og lad A og B være to cirkelskiver, hvis perimetre inddeler planen i fire områder. Giv for hver af disse fire mængder en fremstilling ved A , B og tegnene $\subset$ og $\cap$.
Løs den tilsvarende opgave for tre cirkelskiver A , B og C .
5. Verificer ved hjælp af diagrammer de ikke helt oplagte blandt reglerne for $\subset$, $\cap$ og $\cup$ (side I, 3, 2). Eftervis med benyttelse af den logiske algebra gyldigheden af en af de distributive love samt af $\subset(A \cap B) = \subset A \cap \subset B$ og $\subset(A \cup B) = \subset A \cup \subset B$.
Udled ved hjælp af de to sidstnævnte regler den anden distributive lov.
6. Både $A \setminus (B \cap C)$ og $A \setminus (B \cup C)$ kan bestemmes, når $A \setminus B$ og $A \setminus C$ kendes. Hvorledes?
7. Verificer ved hjælp af diagrammer og bevis ved hjælp af reglerne på side I, 3, 2 den eller de rigtige blandt ligningerne

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

$$A \cap (B \setminus C) = (A \cap B) \setminus (A \cap C),$$

$$A \cup (B \setminus C) = (A \cup B) \setminus (A \cap C).$$

(Overstreg på dette blad den eller de forkerte ligninger!)

8. Lad E være en endelig mængde. Antallet af elementer i en mængde $M \subseteq E$ betegnes med $n(M)$. Lad A , B og C være vilkårlige delmængder af E . Hvilken relation består da mellem tallene $n(A)$, $n(B)$, $n(A \cap B)$ og $n(A \cup B)$?
Hvordan udtrykkes $n(B \setminus A)$ ved disse tal?
Er tallene $n(A \cup B \cup C)$, $n(\subset A \cap (B \cup C))$, $n(\subset A \cup (B \cap C))$ bestemt, når tallene $n(A)$, $n(B)$, $n(C)$, $n(A \cap B)$, $n(B \cap C)$, $n(C \cap A)$ og $n(A \cap B \cap C)$ er givne? Når desuden $n(E)$ er givet?

Angiv i bekræftende fald fremstillinger af dem ved de givne tal.

9. Om resultatet af en eksamination bestående af tre prøver α , β og γ , der skal bestås hver for sig, foreligger følgende oplysninger: Af ialt 100 eksaminander har 86 bestået α , 82 har bestået β , og 76 har bestået γ . Endvidere har 16 hverken bestået β eller γ , 13 hverken γ eller α , 12 hverken α eller β , og 11 har ikke bestået nogen af prøverne. Hvormange har bestået alle tre prøver?
10. Vis, at der for vilkårlige delmængder A og B af universalmængden gælder
- $$(A \subseteq B) \iff (A \cap B = A) \iff (A \cup B = B) \iff (A \setminus B = \emptyset),$$
- og
- $$(A = B) \iff (A \cup B = A \cap B).$$
11. Undersøg, om nogen af inklusionerne
- $$(A \cap (B \cap C)) \cup ((A \cap B) \cap C) \subseteq (A \cup B) \cap C,$$
- $$(A \cap (B \cap C)) \cup ((A \cap B) \cap C) \supseteq (A \cup B) \cap C$$
- gælder for hvilket som helst delmængder A , B og C af en universalmængde.
- Angiv en nødvendig og tilstrækkelig betingelse, som A , B og C må opfylde, for at begge inklusioner gælder.
12. In a very hotly fought battle, at least 70 per cent. of the combatants lost an eye, at least 75 per cent. an ear, at least 80 per cent. an arm, at least 85 per cent. a leg. How many (at least) lost all four members? (Opgaven skyldes Lewis Carroll, forfatteren til "Alice in Wonderland", lektor i matematik i Oxford.)

13. En fabrik producerer tre slags varer α , β , γ . I løbet af et bestemt år har 70 % af fabrikkens kunder købt α , 60 % har købt β , og 80 % har købt γ . Endvidere vides det, at 40 % har købt både α og β , og 50 % har købt både β og γ . Vis, at mindst 30 % har købt alle tre varer. Procenttallet af de kunder, der ikke har købt nogen af varerne, kan ikke overstige en vis værdi r . Bestem det mindste tal r , for hvilket dette er rigtigt.

14. Vis, at der for hvilket som helst delmængde A og B af en universalmængde gælder

$$\mathcal{A}(A) \cap \mathcal{A}(B) = \mathcal{A}(A \cap B).$$

Undersøg, om også mængderne $\mathcal{A}(A) \cup \mathcal{A}(B)$ og $\mathcal{A}(A \cup B)$ altid stemmer overens, eller om der gælder en inklusion imellem dem.

15. Eftersis, at der for hver delmængde A og hver mængde Φ af delmængder af en universalmængde gælder

$$A \cap \bigcup_{B \in \Phi} B = \bigcup_{B \in \Phi} (A \cap B), \quad A \cup \bigcap_{B \in \Phi} B = \bigcap_{B \in \Phi} (A \cup B).$$

(Generaliseringer af de distributive love.)

16. Lad E være mængden $\mathbb{R}$ af reelle tal. Bestem mængderne

$$\bigcup_{n=1}^{\infty} \{x \mid 0 < x \leq \frac{1}{n}\}, \quad \bigcup_{n=1}^{\infty} \{x \mid \frac{1}{n} \leq x < \frac{n-1}{n}\},$$

$$\bigcap_{n=1}^{\infty} \{x \mid 0 < x \leq \frac{1}{n}\}, \quad \bigcap_{n=1}^{\infty} \{x \mid \frac{1}{n} \leq x < \frac{n-1}{n}\}.$$

17. Lad E være mængden af alle reelle talpar fortolket som par af sædvanlige retvinklede koordinater for punkterne i planen. Bestem fællesmængden og foreningsmængden af hver af følgende mængder af punktmængder.

a) cirkellinierne med radius 1 og centrum på x-aksen, altså

$$A_\tau = \{(x,y) \mid (x-\tau)^2 + y^2 = 1\}, \quad \tau \in \mathbb{R};$$

b) cirkelskiverne, hvis perimetere går gennem punkterne (0,1) og (0,-1), altså

$$A_\tau = \{(x,y) \mid x^2 - 2\tau x + y^2 \leq 1\}, \quad \tau \in \mathbb{R};$$

c) halvplanerne

$$A_\tau = \{(x,y) \mid \tau x + \frac{y}{\tau} \geq 2\}, \quad \tau \in \mathbb{R}_+.$$

(Bevis og benyt f.eks. den for alle positive tal τ, x, y gyldige ulighed $\tau x + \frac{y}{\tau} \geq 2\sqrt{xy}$.)

18. Lad Φ være en mængde af delmængder af en universalmængde E , og lad Ψ betegne mængden af disse delmængders komplementer, altså $(A \in \Phi) \iff (C A \in \Psi)$. Angiv en nødvendig og tilstrækkelig betingelse, som fællesmængden for Ψ må opfylde, for at
a) Φ er en overdækning af E , b) Φ er en overdækning af en given mængde $M \subseteq E$.

19. Om en følge $A_n, n \in \mathbb{N}$, af delmængder af E forudsættes, at den er en overdækning af E . Vis, at de fra den tomme mængde forskellige blandt mængderne

$$A_n \setminus \bigcup_{i=1}^{n-1} A_i, \quad n \in \mathbb{N},$$

danner en klasseinddeling af E .

Find på lignende måde ud fra en følge $A_n, n \in \mathbb{N}$, som er en overdækning af en given mængde M , en klasseinddeling af M .

§ 4. Afbildninger (funktioner).

Lad A og B være to (ikke nødvendigvis forskellige) mængder. En forskrift, der til hvert element $x \in A$ lader svare et bestemt element $y \in B$ kaldes en afbildning af A ind i B eller en funktion fra A til B . (Glossen "funktion" foretrækkes især, når B er en mængde af tal.) En afbildning (funktion) betegnes i reglen med et enkelt bogstav, i nogle tilfælde også med ordforkortelser (log, exp, sin, Arctg, ...). Betegner f en afbildning af A ind i B , skrives

$$f:A \text{ ind i } B \quad \text{eller} \quad f:A \rightarrow B \quad \text{eller} \quad A \xrightarrow{f} B.$$

Mængden A kaldes afbildningens (funktionens) definitions-mængde og B dens dispositions-mængde. Det til et element $x \in A$ svarende element af B betegnes med $f(x)$, undertiden også med andre symboler, som vil blive omtalt senere. Det kaldes billedelementet af x eller den til x svarende funktionsværdi. At $f(x)$ svarer til x skrives også hyppigt

$$x \rightarrow f(x).$$

Mængden af alle billedelementer (funktionsværdier) kaldes billedmængden (værdimængden) og betegnes med $f(A)$. Den er en (ægte eller uægte) delmængde af dispositions-mængden B .

To afbildninger $f:A \text{ ind i } B$ og $g:C \text{ ind i } D$ siges at være lig med hinanden, at stemme overens, hvis og kun hvis $A = C$, $B = D$ og $f(x) = g(x)$ for hvert element $x \in A$.

Er A' en delmængde af A , vil der med $f:A \text{ ind i } B$ tillige være givet en afbildning af A' ind i B , som kaldes restriktionen (eller indskrænkningen) af f til A' . I reglen giver det ikke anledning til misforståelser, når denne også betegnes med f . Man skriver altså $f:A' \text{ ind i } B$.

Er B' en fra B forskellig mængde, som også indeholder $f(A)$

som delmængde, vil der med $f:A \text{ ind i } B$ tillige være givet en afbildning af $A \text{ ind i } B'$. Den kan i reglen betegnes med $f:A \text{ ind i } B'$ uden fare for misforståelser.

En afbildning $f:A \text{ ind i } B$, ved hvilken der til alle elementer af A svarer et og samme element af B , siges at være konstant.

Eksempler:

1) Lad $\mathbb{R}$ betegne mængden af alle reelle tal. De fra den elementære differential- og integralregning kendte funktioner er afbildninger af en mængde $A \subseteq \mathbb{R}$ ind i $\mathbb{R}$. Definitionsmængden A er hyppigt en ægte delmængde af $\mathbb{R}$, nemlig et interval eller foreningsmængden af disjunkte intervaller. Værdimængden $f(A)$ kan være en ægte delmængde af $\mathbb{R}$. Som dispositionsmængde kan da i stedet for $\mathbb{R}$ eksempelvis vælges $f(A)$ eller en vilkårlig anden mængde B , for hvilken $f(A) \subseteq B \subseteq \mathbb{R}$.

2) Lad $A \subseteq \mathbb{R}$ betegne intervallet $a \leq t \leq b$. Mængden af alle kontinuerte funktioner $\varphi:A \text{ ind i } \mathbb{R}$ betegnes med $\hat{C}(A,\mathbb{R})$. Ved til φ at lade svare funktionen $\int_a^b \varphi(t) dt \in \hat{C}(A,\mathbb{R})$ defineres en afbildning af $\hat{C}(A,\mathbb{R})$ ind i $\hat{C}(A,\mathbb{R})$. Ved til φ at lade svare tallet $\int_a^b \varphi(t) dt$ defineres en afbildning af $\hat{C}(A,\mathbb{R})$ ind i $\mathbb{R}$.

3) Lad A være mængden E_2 af alle punkter i planen og $m \subseteq E_2$ en ret linie. Lader man til hvert punkt $P \in E_2$ svare dets retvinklede projektion på linien m , fås en afbildning $f:E_2 \text{ ind i } E_2$ eller $f:E_2 \text{ ind i } m$. Er $l \subseteq E_2$ en anden ret linie, vil restriktionen af f til l være en afbildning $f:l \text{ ind i } m$.

4) Lad der være givet to forskellige punkter P_0 og Q_0 i planen E_2 . Til et vilkårligt punkt P i planen lades svare det punkt Q , for hvilket det orienterede liniestykke fra P til Q har samme længde som og er parallel og ensrettet med liniestyk-

ket fra P_0 til Q_0 (hvorved liniestykker beliggende på samme linie betragtes som parallelle). Herved defineres en afbildning af E_2 ind i E_2 , som kaldes en translation eller parallelforskydning).

5) Lad der være givet et punkt C i planen E_2 og et reelt tal $m \neq 0$. Til et vilkårligt punkt $P \neq C$ i planen lades svare det punkt Q , for hvilket $|CQ| = |m| |CP|$, og som ligger på linien CP på den samme eller den modsatte side af C som P , efter som $m > 0$ eller $m < 0$; til C lades svare C . Herved defineres en afbildning af E_2 ind i E_2 , som kaldes en homoteti (eller multiplikation) med centrum (ud fra) C og med faktoren m .

6) Lad Δ betegne mængden af alle trekanter i en plan. Ved til hver trekant at lade svare dens areal, defineres en funktion fra Δ til $\mathbb{R}_+$.

7) Lad A være en endelig mængde. Ved til hver delmængde $A' \subseteq A$ at lade svare antallet $n(A')$ af dens elementer, defineres en funktion fra (A) til $\mathbb{N}_0$ (mængden af alle ikke-negative hele tal).

8) Lad E være en vilkårlig mængde og A en af dens delmængder. Ved dennes karakteristiske funktion forstås funktionen $\chi_A: E$ ind i $\{0,1\}$ defineret ved

$$\chi_A(x) = \begin{cases} 1 & \text{hvis } x \in A \\ 0 & \text{hvis } x \in \bar{A}, \end{cases}$$

9) Lad A være den endelige mængde $\{1, 2, \dots, m\}$, hvor m betegner et naturligt tal, og B en vilkårlig mængde. Enhver afbildning af A ind i B kaldes et m-sæt af elementer af B og betegnes f.eks. med $(b_1, b_2, \dots, b_m)$. Her er rækkefølgen væsentlig, idet der på første plads står det til 1 svarende element, på anden plads det til 2 svarende o.s.v., medens den ikke er det i $\{b_1, b_2, \dots, b_m\}$, som jo blot betegner mængden af de indbyrdes forskellige blandt elementerne $b_1, b_2, \dots, b_m$.

10) Lad B være en vilkårlig mængde. En afbildning $f: \mathbb{N} \rightarrow B$ kaldes en følge af elementer af B . Det til et naturligt tal n svarende element $f(n)$ plejer man at betegne med et bogstav forsynet med mærketallet n for neden, f.eks. $f(n) = b_n$. Hele afbildningen, altså følgen, angives da ved $(b_1, b_2, \dots)$ eller $(b_n)_{n \in \mathbb{N}}$ eller $b_n, n = 1, 2, \dots$. Det er nødvendigt at skelne mellem en følge af elementer $(b_1, b_2, \dots)$ og mængden $\{b_1, b_2, \dots\}$ af disse elementer. (For følgen $n \rightarrow (-1)^n$ vil mængden af dens elementer være lig med $\{-1, 1\}$.) Eftersom B er en mængde af tal, punkter, funktioner o.s.v., taler man om talfølger, punktfølger o.s.v.

Også i andre tilfælde kan det være hensigtsmæssigt i stedet for den sædvanlige betegnelse for funktionsværdien at bruge en indexbetegnelse. Lad J og B være vilkårlige mængder og f en afbildning af J ind i B . Det til et element $\iota \in J$ svarende element $f(\iota) \in B$ betegnes da f.eks. med b_ι . Definitionsmængden J kaldes i så fald for indexmængden, afbildningen skrives $(b_\iota)_{\iota \in J}$ eller blot $b_\iota, \iota \in J$, og man taler om en indiceret mængde. (Dermed menes altså selve afbildningen og ikke billedmængden $f(J) = \{b_\iota \mid \iota \in J\}$. Ifølge de side 1, 3, 5-6 givne definitioner forstås imidlertid ved fælles- og foreningsmængden for en indexeret mængde $(A_\iota)_{\iota \in J}$ af mængder henholdsvis fælles- og foreningsmængden for mængden $\{A_\iota \mid \iota \in J\}$.)

Lad der være givet tre mængder A, B, C og afbildninger $f: A \rightarrow B$ og $g: B \rightarrow C$. Man kan da definere en afbildning af A ind i C ved til elementet $x \in A$ at lade svare elementet $g(f(x))$ af C . Denne af f og g sammensatte afbildning betegnes med $g \circ f$ (når forveksling med et produkt er udelukket, også med gf). I tegn

$$g \circ f: A \rightarrow C \quad \text{eller} \quad x \rightarrow (g \circ f)(x) = g(f(x)).$$

Er A, B, C, D mængder og $f: A \rightarrow B$, $g: B \rightarrow C$, $h: C \rightarrow D$ afbildninger, kan man danne afbildningerne

$$h \circ (g \circ f): A \rightarrow D \quad \text{og} \quad (h \circ g) \circ f: A \rightarrow D.$$

For den første fås, idet $x \in A$,

$$x \rightarrow (h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))),$$

og for den anden

$$x \rightarrow ((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))),$$

altså det samme. Følgelig kan vi skrive

$$h \circ (g \circ f) = (h \circ g) \circ f = h \circ g \circ f.$$

For sammensætning af afbildninger gælder den associative lov.

Er der givet afbildninger $f: A \rightarrow B$ og $g: B \rightarrow C$, kan man i almindelighed ikke danne $f \circ g$. Dette vil være muligt, hvis $C \subseteq A$. Idet g da kan opfattes som en afbildning af B ind i A , har man $g \circ f: A \rightarrow A$ og $f \circ g: B \rightarrow B$. Almindeligvis er altså disse to afbildningers definitionsmængder forskellige, og alene af denne grund kan afbildningerne ikke stemme overens. Men også hvis $A = B = C$, således at $g \circ f: A \rightarrow A$ og $f \circ g: A \rightarrow A$, vil de i almindelighed være forskellige. Den kommutative lov gælder ikke for sammensætning af afbildninger. Eksempler, der viser dette, dannes let ved hjælp af elementære funktioner. Hvis det for to afbildninger $f: A \rightarrow A$ og $g: A \rightarrow A$ gælder, at $g \circ f = f \circ g$, d.v.s. $f(g(x)) = g(f(x))$ for hvert element $x \in A$, siges de at være ombyttelige.

Blandt afbildningerne af en mængde A ind i sig selv fremhæves den identiske afbildning e_A , ved hvilken hvert element $x \in A$ svarer til sig selv: $x \rightarrow x$. For hver afbildning $f: A \rightarrow B$ gælder

$$f \circ e_A = e_B \circ f = f.$$

En afbildning $f:A \text{ ind i } A$ kan sammensættes med sig selv. Man får da en ny afbildning $f \circ f:A \text{ ind i } A$. Denne kan igen sammensættes med f . På grund af den associative lov bliver resultatet $f \circ f \circ f$ uafhængigt af "fra hvilken af siderne" det sker. På denne måde kan man fortsætte og får da efter i alt $p-1$ sammensætninger, hvor p er et naturligt tal, afbildningens p -te itererede eller p -te potens

$$f^{\circ p} = f \circ f \circ \dots \circ f \quad (p \text{ "faktorer"}).$$

Når forveksling med en sædvanlig potens er udelukket, skrives simpelthen f^p . Som for potenser af tal indses (med gentagen benyttelse af den associative lov), at der for enhver afbildning f af en mængde ind i sig selv og for hvilket som helst naturlige tal p og q gælder, at

$$f^{\circ p} \circ f^{\circ q} = f^{\circ (p+q)}.$$

Af formelle grunde er det hensigtsmæssigt at definere

$$f^{\circ 0} = e_A.$$

"Potensreglen" gælder da for $p \geq 0$, $q \geq 0$. Det er indlysende, at to itererede af den samme afbildning er ombyttelige.

Er to afbildninger $f:A \text{ ind i } A$ og $g:A \text{ ind i } A$ ombyttelige gælder for hvert helt tal $p \geq 0$ også

$$(g \circ f)^{\circ p} = g^{\circ p} \circ f^{\circ p}.$$

Det kan hende, at den anden itererede $f^{\circ 2}$ af en afbildning $f:A \text{ ind i } A$ stemmer overens med f selv:

$$f^{\circ 2} = f.$$

Da gælder $f^{\circ p} = f$ for $p > 0$, og afbildningen kaldes idempotent. Det er klart, at den identiske afbildning samt enhver konstant afbildning af $A \text{ ind i } A$ er idempotent. Men der findes mindre oplagte eksempler. Her kan nævnes den ovenfor omtalte projektion af planens punkter på en ret linie.

En fra den identiske forskellig afbildning $f:A \text{ ind i } A$ kaldes involutorisk eller en involution, hvis

$$f \circ f = e_A.$$

Eksempler på involutioner er: den ved $x \rightarrow -x$ definerede afbildning af $\mathbb{R}$ ind i sig selv, den ved $x \rightarrow 1/x$ definerede afbildning af $\mathbb{R} \setminus \{0\}$ ind i sig selv, den ovenfor omtalte homoteti af planen E_2 , når $m = -1$.

Når der foreligger en afbildning $f:A \text{ ind i } B$, kan man til hver delmængde A' af A lade svare dens billede, altså en delmængde af $f(A)$ og dermed af B . Afbildningen f bestemmer altså en afbildning af $\mathcal{D}(A)$ ind i $\mathcal{D}(B)$. Uheldigvis er det sædvanen at betegne også denne afbildning med f og følgelig den til $A' \subseteq A$ svarende delmængde af B med $f(A')$ (i overensstemmelse med den allerede indførte betegnelse $f(A)$ for billedmængden ved $f:A \text{ ind i } B$). Afbildningen $f:\mathcal{D}(A) \text{ ind i } \mathcal{D}(B)$ vil vi kalde den til $f:A \text{ ind i } B$ hørende mængdeafbildning. Det bemærkes, at for $x \in A$ er

$$f(\{x\}) = \{f(x)\},$$

hvor f på højre side står for den oprindelige afbildning og på venstre side for den tilhørende mængdeafbildning. (Her udelades i reglen de krøllede parenteser; det må da sluttes af sammenhængen, om talen er om den ene eller den anden afbildning f .)

For den til en afbildning $f:A \text{ ind i } B$ hørende mængdeafbildning gælder, når A' og A'' betegner vilkårlige delmængder af A , at

$$f(A' \cap A'') \subseteq f(A') \cap f(A'');$$

thi for hvert element $x \in A' \cap A''$ haves $f(x) \in f(A')$ og

$f(x) \subseteq f(A'')$. Inklusionstegnet kan i almindelighed ikke erstattes med lighedstegnet. Findes der nemlig to forskellige elementer $x_1, x_2 \in A$, for hvilke $f(x_1) = f(x_2)$, og vælges $A' = \{x_1\}$ og $A'' = \{x_2\}$, vil venstre side i inklusionen være tom, medens højre side er $\{f(x_1)\} = \{f(x_2)\}$. Med de samme betegnelser gælder endvidere

$$f(A' \cup A'') = f(A') \cup f(A'').$$

At mængden på venstre side er en delmængde af mængden på højre side følger af, at hvis $x \in A' \cup A''$, vil der gælde $f(x) \in f(A')$ eller $f(x) \in f(A'')$. Gyldigheden af den omvendte inklusion indses således: At y er et element af $f(A') \cup f(A'')$, altså $y \in f(A')$ eller $y \in f(A'')$, vil sige, at der findes et element x tilhørende A' eller A'' , altså $A' \cup A''$, for hvilket $f(x) = y$. Men dette betyder netop, at $y \in f(A' \cup A'')$.

Til en afbildning $f: A \rightarrow B$ er også knyttet en afbildning af $\mathcal{D}(B)$ ind i $\mathcal{D}(A)$ defineret ved, at der til delmængden B' af B svarer den (muligvis tomme) mængde af alle de elementer x af A , for hvilke $f(x)$ tilhører B' , altså ved

$$B' \rightarrow \{x \mid f(x) \in B'\}.$$

Mængden $\{x \mid f(x) \in B'\}$ kaldes originalmængden til B' . Den definerede afbildning kan derfor kaldes den til f hørende originalmængdeafbildning. Den betegnes

$$f^{\circ-1}: \mathcal{D}(B) \rightarrow \mathcal{D}(A)$$

eller, når forvekslinger er udelukket, i reglen $f^{-1}: \mathcal{D}(B) \rightarrow \mathcal{D}(A)$.

Det følger umiddelbart af definitionen, at man for hver delmængde B' af B har

$$f(f^{\circ-1}(B')) \subseteq B'.$$

Lighedstegnet gælder, hvis $B' \subseteq f(A)$, og, idet $f(f^{\circ-1}(B')) \subseteq f(A)$,

kun i dette tilfælde. For hver delmængde A' af A har man

$$f^{\circ-1}(f(A')) \supseteq A';$$

thi for hvert element $x \in A'$ er $f(x) \in f(A')$ og følgelig $x \in f^{\circ-1}(f(A'))$. Heller ikke her gælder lighed generelt, hvilket ses af følgende ekstreme eksempel: Lad A være en mængde, som indeholder mindst to elementer, og $f:A$ ind i B den konstante afbildning $x \rightarrow f(x) = b$, hvor b er et fast valgt element i B . For et vilkårligt element $a \in A$ har man da $f^{\circ-1}(f(\{a\})) = f^{\circ-1}(\{b\}) = A \supset \{a\}$. Endvidere gælder for hvilket som helst delmængder B' og B'' af B , at

$$f^{\circ-1}(B' \cap B'') = f^{\circ-1}(B') \cap f^{\circ-1}(B''),$$

$$f^{\circ-1}(B' \cup B'') = f^{\circ-1}(B') \cup f^{\circ-1}(B'').$$

Den første relation kan bevises således: At et element $x \in A$ tilhører mængden på venstre side, betyder, at $f(x) \in B' \cap B''$. At x hører til mængden på højre side, altså såvel til $f^{\circ-1}(B')$ som til $f^{\circ-1}(B'')$, betyder, at $f(x) \in B'$ og $f(x) \in B''$. De to udsagn er øjensynlig ensbetydende. Tilsvarende indses gyldigheden af den anden relation.

Ved til hvert element $y \in B$ at lade svare originalmængden $f^{\circ-1}(\{y\})$ til mængden $\{y\} \subseteq B$, fås en afbildning af B ind i $\mathcal{P}(A)$. I stedet for $f^{\circ-1}(\{y\})$ skrives i reglen blot $f^{\circ-1}(y)$, og denne mængde kaldes originalmængden til elementet y . Herom gælder følgende:

For hver afbildning $f:A$ ind i B danner mængden af originalmængderne $f^{\circ-1}(y)$ til elementerne $y \in B$ en klasseinddeling af A .

Bevis: Hvert element $x \in A$ tilhører en af mængderne $f^{\circ-1}(y)$, nemlig $f^{\circ-1}(f(x))$, og for to elementer $y_1, y_2 \in B$ er $f^{\circ-1}(y_1) \cap f^{\circ-1}(y_2) = \emptyset$, når $y_1 \neq y_2$. Dette kan slutes af ovenstående formel for originalmængden til en fællesmængde eller

ved at bemærke, at et fælles element for $f^{-1}(y_1)$ og $f^{-1}(y_2)$ måtte have de forskellige billedelementer y_1 og y_2 ved f , hvilket strider mod afbildningens definition.

Hvis det for en afbildning $f:A$ ind i B gælder, at billedmængden $f(A)$ udgør hele dispositionsmængden B , hvis altså

$$\forall_B y \exists_A x [f(x) = y],$$

siges den at være en afbildning af A på B eller en surjektiv afbildning, i tegn

$$f:A \text{ på } B \quad \text{eller} \quad f:A \rightarrow B \text{ surj.}$$

Hver afbildning $f:A$ ind i B kan betragtes som en afbildning af A på $f(A)$.

Eksempler (jfr. side I, 4,2-3):

1) Den ved $x \rightarrow x^3$ bestemte funktion fra $\mathbb{R}$ til $\mathbb{R}$ er surjektiv, den ved $x \rightarrow x^2$ bestemte er ikke surjektiv.

2) Den ved $\varphi \rightarrow \int_a \varphi(t)dt$ bestemte afbildning af $\hat{C}(A,\mathbb{R})$ ind i $\hat{C}(A,\mathbb{R})$ er ikke surjektiv, da integralet af en kontinuert funktion er differentiabel, og ikke alle kontinuerte funktioner er differentiable. Den ved $\varphi \rightarrow \int_a^b \varphi(t)dt$ bestemte afbildning af $\hat{C}(A,\mathbb{R})$ ind i $\mathbb{R}$ er surjektiv, da hvert reelt tal kan fås som det bestemte integral af en passende (f.eks. i intervallet konstant) funktion.

3) Den retvinklede projektion af planens punkter på en linie m er en afbildning af E_2 på m . Men dens restriktion til en linie l er kun surjektiv, hvis l ikke er vinkelret på m .

4) Enhver translation af planen E_2 er en surjektiv afbildning.

5) Enhver homoteti af planen E_2 er en surjektiv afbildning.

6) Afbildningen, der til hver trekant i planen lader svare

dens areal er en afbildning af Δ på $\mathbb{R}_+$.

7) Afbildningen, der til hver delmængde A' af en endelig mængde A lader svare antallet $n(A')$ af elementer i A' , er en afbildning af $\mathcal{D}(A)$ ind i $\mathbb{N}_0$, som ikke er surjektiv.

8) Den karakteristiske funktion for en delmængde A af en mængde E er en afbildning af E på $\{0,1\}$, hvis og kun hvis A er forskellig fra både $\emptyset$ og E .

Er f en afbildning af en mængde A på en mængde B , gælder for hver mængde $B' \subseteq B$, at

$$f(f^{-1}(B')) = B'.$$

Idet her $f(A) = B$, fremgår dette af det, der blev sagt (side I, 4, 8-9) om lighedstegnet i den for vilkårlige afbildninger gyl-dige inklusion.

Er f en afbildning af A på B og g en afbildning af B på C , vil $g \circ f$ være en afbildning af A på C ; med andre ord, ved sammen-sætning af surjektive afbildninger fås igen en surjektiv afbild-ning. Da g er surjektiv, findes der nemlig for hvert element $z \in C$ mindst eet element $y \in B$, for hvilket $g(y) = z$. Da f er surjektiv, findes der mindst eet element $x \in A$, for hvilket $f(x) = y$, og for dette element x er $g(f(x)) = z$.

Hvis det for en afbildning $f:A$ ind i B gælder, at hvilkesom-helst to forskellige elementer af A har forskellige billedelemen-ter, hvis altså

$$\forall_A x_1, x_2 [(x_1 \neq x_2) \Rightarrow (f(x_1) \neq f(x_2))]$$

eller, hvad der kommer ud på det samme,

$$\forall_A x_1, x_2 [(f(x_1) = f(x_2)) \Rightarrow (x_1 = x_2)]$$

siges f at være en enentydig eller injektiv afbildning. (Til den ældre, men endnu overvejende brugte glose "enentydig" bemærkes, at den opstod på en tid, da man kaldte en afbildning som defi-

neret her for en "entydig afbildning". Man talte også om "flertydige afbildninger", ved hvilke der til et element af definitionsmængden kunne svare flere elementer i dispositionsmængden. Man har imidlertid forladt dette begreb, da det har vist sig at være u hensigtsmæssigt i den overvejende del af matematikken. Ifølge den her givne definition gælder

$$\forall_{A} x_1, x_2 [(x_1 = x_2) \Rightarrow (f(x_1) = f(x_2))]$$

for hver afbildning $f:A \text{ ind i } B$.) At en afbildning $f:A \text{ ind i } B$ er injektiv angives ved

$$f:A \text{ ind i } B \text{ (1-1)} \quad \text{eller} \quad f:A \rightarrow B \text{ inj.}$$

Eksempler (jfr. side I, 4, 2-3):

1) Den ved $x \rightarrow x^3$ bestemte funktion fra $\mathbb{R}$ til $\mathbb{R}$ er injektiv. Den ved $x \rightarrow x^2$ bestemte er ikke injektiv, men dens restriktion til $\{x \mid x \geq 0\}$ er det.

2) Den ved $\varphi \rightarrow \int_a \varphi(t)dt$ bestemte afbildning af $\hat{C}(A, \mathbb{R})$ ind i sig selv er injektiv. Den ved $\varphi \rightarrow \int_a^b \varphi(t)dt$ bestemte afbildning af $\hat{C}(A, \mathbb{R})$ ind i $\mathbb{R}$ er ikke injektiv, idet der findes forskellige kontinuerte funktioner i intervallet A , for hvilke det bestemte integral fra a til b har samme værdi.

3) Den retvinklede projektion af planens punkter på en linie m er en ikke injektiv afbildning. Dens restriktion til en linie l er injektiv, hvis og kun hvis l ikke er vinkelret på m .

4) Enhver translation af planen E_2 er en injektiv afbildning.

5) Enhver homoteti af planen E_2 er en injektiv afbildning.

6) Afbildningen, der til hver trekant i planen lader svare dens areal er ikke injektiv.

7) Afbildningen bestemt ved $A' \rightarrow n(A')$ af $\hat{D}(A)$ ind i $\mathbb{N}_0$ er ikke injektiv, når A indeholder mindst to elementer.

8) Den karakteristiske funktion for en delmængde A af E er kun injektiv, hvis E består af to elementer og A af eet af disse.

Er $f:A \rightarrow B$ en injektiv afbildning, gælder for hvilke-
somhelst to delmængder A' og A'' af A , at

$$f(A' \cap A'') = f(A') \cap f(A'').$$

Da dette med $\subseteq$ i stedet for $=$ er rigtigt for vilkårlige afbildninger (se side I, 4, 7), er det tilstrækkeligt at vise, at mængden på højre side er en delmængde af mængden på venstre side. At elementet $y \in B$ tilhører $f(A') \cap f(A'')$ betyder, at der findes et element $x_1 \in A'$ og et element $x_2 \in A''$, således at $f(x_1) = f(x_2)$. Da f er injektiv, medfører dette, at $x_1 = x_2 \in A' \cap A''$. Heraf ses, at y er billedelement af et element i $A' \cap A''$ og følgelig tilhører $f(A' \cap A'')$, som påstået. Er $f:A \rightarrow B$ en injektiv afbildning, har man endvidere for hver delmængde A' af A

$$f^{-1}(f(A')) = A'.$$

Da dette med $\supseteq$ i stedet $=$ er rigtigt for vilkårlige afbildninger, er det tilstrækkeligt at vise, at mængden på venstre side er en delmængde af A' . At elementet $x \in A$ tilhører $f^{-1}(f(A'))$ betyder, at $f(x) \in f(A')$, og dette vil sige, at der findes et element $x' \in A'$, for hvilket $f(x') = f(x)$. Da f er injektiv, medfører dette, at $x = x' \in A'$, som påstået.

Er f en enentydig afbildning af A ind i B og g en enentydig afbildning af B ind i C , vil $g \circ f$ være en enentydig afbildning af A ind i C ; thi af $g(f(x_1)) = g(f(x_2))$ følger $f(x_1) = f(x_2)$, da g er injektiv, og heraf $x_1 = x_2$, da f er injektiv.

At en afbildning $f:A \rightarrow B$ er injektiv er ensbetydende med, at originalmængden $f^{-1}(y)$ for hvert element $y \in B$ består af højst eet element af A . Idet $f^{-1}(y)$ er tom, når $y \notin f(A)$, kommer dette ud på, at $f^{-1}(y)$ består af netop eet element, når $y \in f(A)$. Ved

til hvert $y \in f(A)$ at lade svare det entydig bestemte element af A , som udgør originalmængden $f^{\circ-1}(y)$, og som kaldes original-elementet til y , defineres en afbildning af $f(A)$ ind i A . Denne betegnes ligeledes med $f^{\circ-1}$ (eller i reglen f^{-1}). [Derved kommer $f^{\circ-1}(y)$ altså til at betegne såvel originalmængden som det element denne består af.] Den således definerede afbildning

$$f^{\circ-1}: f(A) \text{ ind i } A$$

kaldes den til f inverse eller omvendte afbildning. Det ses umiddelbart, at den er surjektiv, da jo hvert element $x \in A$ er originalelement til et element i $f(A)$, nemlig $f(x)$. Det er også klart, at den er injektiv; thi to forskellige elementer i $f(A)$ kan ifølge afbildningens definition ikke have samme originalelement.

Lad $f: A$ ind i B være en injektiv afbildning. Det til $y \in f(A)$ ved dens inverse afbildning svarende element $f^{\circ-1}(y)$ af A er ifølge definition det element af A , hvis billede ved f er y . Der gælder altså

$$f(f^{\circ-1}(y)) = y \quad \text{for } y \in f(A),$$

d.v.s.

$$f \circ f^{\circ-1} = e_{f(A)}.$$

Er $x \in A$, vil det til $f(x)$ ved den inverse afbildning svarende element være det, hvis billede ved f er $f(x)$, altså x . Følgelig gælder

$$f^{\circ-1}(f(x)) = x \quad \text{for } x \in A,$$

d.v.s.

$$f^{\circ-1} \circ f = e_A.$$

Den til $f^{\circ-1}: f(A)$ på A inverse afbildning er $f: A$ på $f(A)$, altså

$$(f^{\circ-1})^{\circ-1} = f.$$

Eksempler (se ovenfor):

1) Den injektive funktion $x \rightarrow x^3$ fra $\mathbb{R}$ til $\mathbb{R}$ har den omvendte $y \rightarrow \sqrt[3]{y}$. Funktionen $x \rightarrow x^2$ fra $\mathbb{R}$ til $\mathbb{R}$ er ikke injektiv. Men dens restriktion til $\mathbb{R}_+ \cup \{0\}$ er det og har værdimængden $\mathbb{R}_+ \cup \{0\}$. Dens omvendte funktion er $y \rightarrow \sqrt{y}$. Restriktionen til $\mathbb{R}_- \cup \{0\}$, hvor $\mathbb{R}_-$ betegner mængden af negative tal, er ligeledes injektiv. Dens omvendte er funktionen $y \rightarrow -\sqrt{y}$ fra $\mathbb{R}_+ \cup \{0\}$ til $\mathbb{R}_- \cup \{0\}$. Funktionen $\sin$ fra $\mathbb{R}$ til $\mathbb{R}$ er ikke injektiv. Men dens restriktion til intervallet $-\frac{\pi}{2} \leq x \leq \frac{\pi}{2}$ er det. Idet værdimængden er intervallet $-1 \leq y \leq 1$, er den omvendte funktion Arcsin defineret i dette interval. (Det ses, at den i den engelske og amerikanske matematiske litteratur brugte betegnelse $\sin^{-1}$ for denne omvendte funktion er i overensstemmelse med betegnelsen f^{-1} . Da imidlertid $\sin^p x$ i betydningen $(\sin x)^p$, hvorefter altså $\sin^{-1} x = \frac{1}{\sin x}$, har gammel hævd, undgås brugen af $\sin^{-1}$ i betydningen $\text{Arcsin } x$.)

2) Billedmængden ved den injektive afbildning $\varphi \rightarrow \int_a \varphi(t) dt$ af $\hat{C}(A, \mathbb{R})$ ind i sig selv består af alle i intervallet A definerede funktioner ψ , for hvilke $\psi(a) = 0$, og som er differentiable med kontinuert differentialkvotient ψ' . Den inverse afbildning er defineret i denne mængde og bestemt ved $\psi \rightarrow \psi'$.

3) Den inverse afbildning til den retvinklede projektion af en linie l på en linie m , som ikke er vinkelret på l , lader til hvert punkt Q på m svare skæringspunktet mellem l og den vinkelrette på m gennem Q .

4) Den inverse afbildning til den ved punktparret P_0, Q_0 bestemte translation af planen er den ved punktparret Q_0, P_0 bestemte translation.

5) Den inverse afbildning til homotetien af planen med centrum C og faktoren $m \neq 0$ er homotetien med samme centrum og faktoren $\frac{1}{m}$.

En afbildning f med definitionsmængden A og dispositionsmængden B , som er såvel surjektiv som injektiv, siges at være bijektiv eller at være en enentydig afbildning af A på B . For sådanne afbildninger har altså alt, hvad der blev sagt om surjektive og injektive afbildninger, gyldighed. Specielt fremhæves: Ved sammensætning af bijektive afbildninger fås en bijektiv afbildning. Den inverse til en bijektiv afbildning er en bijektiv afbildning. Er f en enentydig afbildning af en mængde A på en mængde B , altså f^{-1} en enentydig afbildning af B på A , siges disse to afbildninger at bestemme en enentydig korrespondance mellem (elementerne i) A og (elementerne i) B .

Er f en enentydig afbildning af A på B og g en enentydig afbildning af B på C , gælder for den enentydige afbildning $g \circ f$ af A på C , at

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Dette indses således: Begge afbildninger har definitionsmængden C , og denne afbildes ved begge på A . Ved g^{-1} svarer der til $z \in C$ det element $y \in B$, for hvilket $g(y) = z$, og ved f^{-1} svarer der til y det element $x \in A$, for hvilket $f(x) = y$. Dette element x svarer altså til z ved den sammensatte afbildning $f^{-1} \circ g^{-1}$. Men da $g(f(x)) = z$, er x også billedeelementet af z ved $(g \circ f)^{-1}$.

Bijektive afbildninger af en mængde A på sig selv kaldes hyppigt for transformationer eller, især når A er en endelig mængde, for permutationer af A . Til disse hører den identiske afbildning e_A . Den sammensatte af transformationer af A er en transformation af A , og det samme gælder for den inverse til en transformation af A .

Er $f_1, f_2, \dots, f_n$ transformationer af en mængde A , fås ved gentagen anvendelse af ovenstående relation for den inverse til en sammensat afbildning (og af den associative lov)

$$(f_n \circ \dots \circ f_2 \circ f_1)^{\circ -1} = f_1^{\circ -1} \circ f_2^{\circ -1} \circ \dots \circ f_n^{\circ -1}.$$

Specielt har man altså for hver enentydig afbildning f af en mængde A på sig selv og hvert $n \in \mathbb{N}$

$$(f^{\circ n})^{\circ -1} = (f^{\circ -1})^{\circ n}.$$

Denne afbildning betegnes med $f^{\circ -n}$ og kaldes den $(-n)$ -te potens eller itererede af f . Sammen med tidligere indførte giver dette følgende definition af en transformations potens med en vilkårlig eksponent $p \in \mathbb{Z}$:

$$f^{\circ p} = \begin{cases} f \circ f \circ \dots \circ f & (p \text{ "faktorer"}) & \text{for } p > 0 \\ e_A & & \text{for } p = 0 \\ (f^{\circ -p})^{\circ -1} = (f^{\circ -1})^{\circ -p} & & \text{for } p < 0. \end{cases}$$

Det vil blive vist senere, at "potensreglerne"

$$f^{\circ p} \circ f^{\circ q} = f^{\circ (p+q)}, \quad (f^{\circ p})^{\circ q} = f^{\circ pq}$$

gælder for vilkårlige hele eksponenter p og q . Er transformationerne f og g af A ombyttelige, gælder også

$$(f \circ g)^{\circ p} = f^{\circ p} \circ g^{\circ p}$$

for hvert $p \in \mathbb{Z}$.

Eksempler:

Det fremgår af det, der blev sagt om de behandlede eksempler, i hvilke tilfælde der foreligger bijektive afbildninger og specielt transformationer. I det følgende omtales nogle enentydige korrespondancer, som har betydningsfulde anvendelser.

Lad E være en universalmængde og X_E mængden af alle funktioner fra E til $\{0,1\}$, altså mængden af alle i E definerede funktioner, som kun antager værdierne 0 og 1. Ved til hver delmængde $A \subseteq E$ at lade s være dens karakteristiske funktion

$\chi_A \in X_E$ fås en afbildning af $\mathcal{D}(E)$ ind i X_E . Denne afbildning er surjektiv; thi hver funktion $\chi \in X_E$ er karakteristisk funktion for en delmængde af E , nemlig for mængden af de elementer $x \in E$, for hvilke $\chi(x) = 1$. Afbildningen er også injektiv. To forskellige delmængder af E har nemlig forskellige karakteristiske funktioner, idet den ene af disse har værdien 1 og den anden værdien 0 for et element, som tilhører den ene, men ikke den anden delmængde. Der består altså en enentydig korrespondance $A \leftrightarrow \chi_A$ mellem mængden $\mathcal{D}(E)$ af delmængder af E og mængden X_E af funktioner fra E til $\{0,1\}$.

Øvelser til kap. I, § 4.

- Bestem de sammensatte $g \circ f$ og $f \circ g$ samt de itererede $f^{\circ n}$ og $g^{\circ n}$, $n \in \mathbb{N}$, af de ved $x \rightarrow f(x) = x^2$ og $x \rightarrow g(x) = e^x$ bestemte funktioner fra $\mathbb{R}$ til $\mathbb{R}$.
Angiv de fundne funktioners værdimængder.
- Med A betegnes mængden $\mathbb{R} \setminus \{0, 1\}$ af de fra 0 og 1 forskellige reelle tal og med f og g de ved henholdsvis $x \rightarrow 1 - x$ og $x \rightarrow \frac{1}{x}$ bestemte funktioner fra A til $\mathbb{R}$.
Angiv værdimængderne $f(A)$ og $g(A)$.
Find de sammensatte funktioner $g \circ f$ og $f \circ g$, værdimængderne ved disse samt de itererede funktioner $f^{\circ n}, g^{\circ n}, (g \circ f)^{\circ n}, (f \circ g)^{\circ n}$ for $n \in \mathbb{N}$.
- Bestem funktionen $f^{\circ 2}$ og dens værdimængde for den ved $x \rightarrow \frac{1-x^2}{1+x^2}$ bestemte funktion $f: \mathbb{R} \rightarrow \mathbb{R}$. Find værdimængden ved $f^{\circ n}$ for $n \in \mathbb{N}$, $n > 2$.
- I planen E_2 er givet tre rette linier l , m og n gennem samme punkt, således at hverken l eller n er vinkelret på m . Med $f: l \rightarrow m$ og $g: m \rightarrow n$ betegnes den retvinklede projektion af henholdsvis l på m og af m på n . Søg en simpel geometrisk karakterisering af den sammensatte afbildning $g \circ f: l \rightarrow n$, når $l \neq n$, og når $l = n$.
- Lad der være givet to forskellige punkter C og D i planen E_2 samt et fra 0 og 1 forskelligt tal μ . Med $f: E_2 \rightarrow E_2$ betegnes homotetien med $\overset{\text{centrum}}{C}$ og faktoren μ , og med $g: E_2 \rightarrow E_2$ den translation, for hvilken $g(C) = D$. Vis, at såvel $g \circ f$ som $f \circ g$ er en homoteti med faktoren μ .
Konstruer disse homotetiers centre for $\mu = 2$ og $\mu = -1$.

6. Lad A og B være delmængder af en universalmængde E og χ_A og χ_B deres karakteristiske funktioner. Find, udtrykt ved disse, de karakteristiske funktioner $\chi_{\bar{A}}$, $\chi_{A \cap B}$, $\chi_{A \cup B}$ og $\chi_{A \setminus B}$.

7. Mængden $\{(x,y) \mid (x \in \mathbb{R}) \wedge (y \in \mathbb{R})\}$ af alle par af reelle tal betegnes med $\mathbb{R}^2$. Vis, at der ved

$$(x,y) \rightarrow \left(\frac{x}{x^2+y^2}, \frac{y}{x^2+y^2} \right)$$

bestemmes en afbildning f af $\mathbb{R}^2 \setminus \{(0,0)\}$ ind i sig selv, som er involutorisk, og bestem billedmængden.

Bestem billedmængderne ved f af følgende mængder, hvor a , b og $c \neq 0$ er givne reelle tal:

$$\{(x,y) \mid ax + by + c = 0\},$$

$$\{(x,y) \mid ax + by = 0 \wedge (x,y) \neq (0,0)\},$$

$$\{(x,y) \mid x^2 + y^2 + ax + by + c = 0\},$$

$$\{(x,y) \mid x^2 + y^2 + ax + by = 0 \wedge (x,y) \neq (0,0)\}.$$

Søg en geometrisk beskrivelse af afbildningen f , idet talparrene (x,y) fortolkes som par af sædvanlige retvinklede koordinater for punkterne i planen. (Afbildningen kaldes inversion i enhedscirklen.)

8. Find for funktionen $f(x) = x^2 - 1$ fra $\mathbb{R}$ til $\mathbb{R}$ originalmængderne $f^{-1}(\{0\})$, $f^{-1}(\{y \mid -3 < y < 2\})$, $f^{-1}(\{y \mid 2 \leq y \leq 6\})$.

9. Find for funktionen $f(x) = \cos x + \sqrt{3} \sin x$ fra $\mathbb{R}$ til $\mathbb{R}$ værdimængden $f(\mathbb{R})$ samt originalmængderne

$$f^{-1}(\{0\}), \quad f^{-1}(\{y \mid y \geq 0\}).$$

Find endvidere værdimængden og de tilsvarende originalmængder for funktionens restriktion til intervallet $[0, \pi] = \{y \mid 0 \leq y \leq \pi\}$.

10. Bestem værdimængden for funktionen $f(x) = x^2 - 6x + 5$ fra $\mathbb{R}$ til $\mathbb{R}$ samt mængderne $f([-2,4])$, $f^{\circ-1}(f([-2,4]))$, $f^{\circ-1}(]-5,5[)$, $f(f^{\circ-1}(]-5,5[))$ hvor $[-2,4] = \{x \mid -2 \leq x \leq 4\}$ og $]-5,5[= \{y \mid -5 < y < 5\}$.

11. Ved

$$(x,y) \rightarrow (\log \frac{1}{2}(x+y), xy)$$

defineres en afbildning f af delmængden

$$A = \{(x,y) \mid x + y > 0\}$$

af mængden $\mathbb{R}^2$ af alle par af reelle tal ind i $\mathbb{R}^2$.

Find billedmængderne

$$f(A), \quad f(A \cap \{(x,y) \mid x = y\}), \quad f(A \cap \{(x,y) \mid x \leq y\})$$

og originalmængderne

$$f^{\circ-1}((0,0)), \quad f^{\circ-1}((0,1)), \quad f^{\circ-1}(\{(\xi,\eta) \mid \xi = \alpha\}),$$

hvor α er et givet reelt tal.

12. Mængden af de i et interval $]a,b[= \{t \mid a < t < b\}$ vilkårlig ofte differentiable reelle funktioner betegnes med $\hat{C}^\infty(]a,b[, \mathbb{R})$. Ved til hver sådan funktion φ at lade svare dens afledede φ' defineres en afbildning $D: \hat{C}^\infty(]a,b[, \mathbb{R}) \rightarrow \hat{C}^\infty(]a,b[, \mathbb{R})$. Bestem originalmængden $(D^{\circ n})^{\circ-1}(\psi)$, $n \in \mathbb{N}$, til en funktion $\psi \in \hat{C}^\infty(]a,b[, \mathbb{R})$ ved den itererede afbildning $D^{\circ n}$.

13. Lad f og g være afbildninger af en mængde A ind i sig selv. Vis, at hvis $g \circ f = e_A$, så er $f \circ g$ idempotent. Eksempel (jfr. opg. 12): $A = \hat{C}^\infty(]a,b[, \mathbb{R})$, $g = D$ og $f = I$, hvor I er den for et givet tal $c \in]a,b[$ ved $\psi \rightarrow \int_c \psi(t) dt$ bestemte afbildning af $\hat{C}^\infty(]a,b[, \mathbb{R})$ ind i sig selv.

- 14*. Lad A være en endelig mængde og f en afbildning af A ind i sig selv. Vis, at der findes et tal $n \in \mathbb{N}$ og et element $a \in A$, således at $f^{\circ n}(a) = a$.

Undersøg, om en tilsvarende sætning gælder for uendelige mængder.

15. Undersøg, om følgende funktioner er surjektive:

$\tau: \mathbb{N} \rightarrow \mathbb{N}$, hvor $\tau(n)$ er antallet af indbyrdes forskellige positive divisorer i tallet n (1 og n medregnet);

$f: \mathbb{C} \rightarrow \mathbb{C}$, hvor $f(z) = z^n$, $n \in \mathbb{N}$;

$g: \mathbb{C} \setminus \{0\} \rightarrow \mathbb{C}$, hvor $g(z) = z + \frac{1}{z}$;

$h: \mathbb{R} \rightarrow \mathbb{R}$, hvor $h(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$,

$a_0, a_1, \dots, a_n$ er givne reelle tal, $a_n \neq 0$, $n \in \mathbb{N}$. (Skeln mellem ulige og lige n .)

16. For hvilke værdier af konstanten $k \in \mathbb{R}$ er den ved $f(x) = kx + \sin x$ bestemte funktion $f: \mathbb{R} \rightarrow \mathbb{R}$ surjektiv?

For hvilke værdier af k er den injektiv?

17. I planen E_2 er givet to forskellige punkter A og B. Med M betegnes mængden af de punkter af E_2 , som ikke ligger på linien AB.

En afbildning f af M ind i E_2 defineres ved til punktet $P \in M$ at lade svare centret for den i trekant ABP indskrevne cirkel. Bestem billedmængden $f(M)$, og undersøg, om afbildningen er injektiv.

- * En afbildning g af M ind i E_2 defineres ved til punktet $P \in M$ at lade svare højderens skæringspunkt for trekant ABP. Bestem billedmængden $g(M)$, og undersøg om afbildningen er injektiv. Vis, at der findes en delmængde M' af M, således at restriktionen af g til M' er en involutorisk afbildning af M' på M.

18. Angiv en nødvendig og tilstrækkelig betingelse, som reelle tal a, b, c, d må opfylde, for at den ved

$$(x, y) \rightarrow (ax+by, cx+dy)$$

bestemte afbildning af mængden $\mathbb{R}^2$ af reelle talpar ind i sig selv er injektiv.

Vis, at når og kun når denne betingelse er opfyldt, er afbildningen surjektiv.

19. Vis, at en afbildning $f:A \rightarrow B$ er surjektiv, hvis og kun hvis den tilhørende originalmængdeafbildning $f^{\circ-1}: \mathcal{D}(B) \rightarrow \mathcal{D}(A)$ er injektiv, og at $f:A \rightarrow B$ er injektiv, hvis og kun hvis $f^{\circ-1}: \mathcal{D}(B) \rightarrow \mathcal{D}(A)$ er surjektiv.
20. Lad A , B og C være mængder og $f:A \rightarrow B$, $g:B \rightarrow C$ afbildninger, for hvilke $g \circ f:A \rightarrow C$ er injektiv. Vis, at f er injektiv. Vis under den yderligere forudsætning, at f er surjektiv, at også g er injektiv.
21. Lad A , B og C være mængder og $f:A \rightarrow B$, $g_1:B \rightarrow C$, $g_2:B \rightarrow C$ afbildninger, for hvilke $g_1 \circ f = g_2 \circ f$. Man kan da i almindelighed ikke slutte, at $g_1 = g_2$. Angiv et eksempel, der viser dette, og bevis, at $g_1 \circ f = g_2 \circ f$ medfører $g_1 = g_2$, såfremt f er surjektiv.
- Lad $f_1:A \rightarrow B$, $f_2:A \rightarrow B$, $g:B \rightarrow C$ være afbildninger, for hvilke $g \circ f_1 = g \circ f_2$. Man kan da i almindelighed ikke slutte, at $f_1 = f_2$. Angiv et eksempel, der viser dette, og bevis, at $g \circ f_1 = g \circ f_2$ medfører $f_1 = f_2$, såfremt g er injektiv.
22. Med f betegnes en afbildning af en mængde A ind i A . Vis, at

$$A \supseteq f(A) \supseteq f^{\circ 2}(A) \supseteq \dots \supseteq f^{\circ n}(A) \supseteq \dots,$$

og at der for fællesmængden

$$M = \bigcap_{n=0}^{\infty} f^{\circ n}(A)$$

gælder $f(M) \subseteq M$.

Vis, at $f(M) = M$, såfremt f er injektiv. Angiv eksempler på injektive afbildninger, der viser, at både $M = \emptyset$ og $M \neq \emptyset$ kan forekomme.

23. Lad $f:A \rightarrow B$ være en afbildning, $A', A'' \subseteq A$ og $B', B'' \subseteq B$.

Vis, at der for den tilhørende mængdeafbildning $f: \mathcal{D}(A) \rightarrow \mathcal{D}(B)$ gælder

$$f(A'' \setminus A') \supseteq f(A'') \setminus f(A'),$$

og at lighedstegnet gælder, når $f:A \rightarrow B$ er injektiv. Vis endvidere, at der for den til en vilkårlig afbildning

$f:A \rightarrow B$ hørende originalmængdeafbildning $f^{\circ-1}: \mathcal{D}(B) \rightarrow \mathcal{D}(A)$ gælder

$$f^{\circ-1}(B'' \setminus B') = f^{\circ-1}(B'') \setminus f^{\circ-1}(B').$$

24. Bestem billedmængden for hver af følgende afbildninger af mængden $\mathbb{R}^2$ af reelle talpar ind i sig selv:

$$(x, y) \rightarrow (x^2 + y^2, x^2 - y^2),$$

$$(x, y) \rightarrow (x^3 + y^3, x^3 - y^3),$$

$$(x, y) \rightarrow (e^x + e^y, e^x - e^y),$$

$$(x, y) \rightarrow (\operatorname{Arctg} x + \operatorname{Arctg} y, \operatorname{Arctg} x - \operatorname{Arctg} y),$$

$$(x, y) \rightarrow (\sin x + \sin y, \sin x - \sin y).$$

Undersøg, hvilke af afbildningerne der er injektive, og angiv disses inverse afbildninger.

25. Vis, at en involutorisk afbildning $f:A \rightarrow A$ er bijektiv og identisk med sin inverse.

26. Idet $x \in \mathbb{R}$, betegnes med $[x]$ det største hele tal, der er mindre end eller lig med x . (Sættes $x = m + r$, hvor $m \in \mathbb{Z}$ og $0 \leq r < 1$, er $[x] = m$.) Vis, at funktionen $f:\mathbb{R} \rightarrow \mathbb{R}$ bestemt ved $f(x) = 2[x] - x$ er bijektiv.

27. Lad $n \in \mathbb{N}$ være givet, og lad $f:\mathbb{C} \rightarrow \mathbb{C}$ være den ved $z \rightarrow z^n$ bestemte afbildning. Angiv en delmængde M af $\mathbb{C}$, således at restriktionen $f:M \rightarrow \mathbb{C}$ er bijektiv.

* Løs den samme opgave for den ved $z \rightarrow z + \frac{1}{z}$ bestemte afbildning $g:\mathbb{C} \setminus \{0\} \rightarrow \mathbb{C}$.

§5. Relationer.Det cartesiske produkt $A \times B$.

Det ordnede par af to (ens eller forskellige) objekter a og b vil vi betegne (a,b) . Begrebet er således at forstå, at den orden, i hvilken de to objekter optræder, spiller en rolle, altså

$$(a,b) = (c,d) \iff a = c \wedge b = d.$$

Vi advarer mod forveksling med symbolet $\{a,b\}$ for mængden af indbyrdes forskellige blandt objekterne a og b . Medens $\{a,b\} = \{b,a\}$, så er $(a,b) \neq (b,a)$ medmindre $a = b$.

Vi vil også betragte ordnede sæt af flere objekter. Her er rækkefølgen ligeledes væsentlig:

$$(a,b,c) = (d,e,f) \iff a = d \wedge b = e \wedge c = f.$$

Ved det cartesiske produkt eller mængdeproduktet $A \times B$ af to mængder (eller klasser) A og B forstås mængden (klassen) af alle ordnede par (a,b) , hvis første komponent a tilhører A , og hvis anden komponent b tilhører B , altså

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

Det er tilladt, at $A = B$. I stedet for $A \times A$ skrives også A^2 .

Ganske tilsvarende defineres det cartesiske produkt af flere mængder (eller klasser); eksempelvis

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

I stedet for $A \times A \times A$ skrives også A^3 , etc.

Er A og B endelige mængder med henholdsvis p og q elementer, vil $A \times B$ have pq elementer. Er også C endelig med r ele-

menter, vil antallet af elementer i $A \times B \times C$ være pqr; etc.

I visse tilfælde kan man anskueliggøre sig det cartesiske produkt af to eller tre mængder:

Lad l og m være to hinanden skærende linier i planen, A en delmængde af (mængden af punkter på) l og ligeledes $B \subseteq m$. Mængden af skæringspunkter mellem de med m parallelle linier gennem punkterne af A og de med m parallelle linier gennem punkterne af B kan da opfattes som en illustration af $A \times B$. Er A og B specielt liniestykker, fås punkterne i et parallelogram (tegn); for $A = l$, $B = m$ fås hele planen.

Denne illustrationsmåde for $A \times B$ lader sig også anvende på to mængder A og B af reelle tal, idet man først repræsenterer A ved den tilsvarende punktmængde på X_1 -aksen og B ved den tilsvarende punktmængde på X_2 -aksen i et sædvanligt retvinklet koordinatsystem X_1X_2 i planen. Specielt kommer man på denne måde til fortolkningen af $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ som mængden af punkter i planen.

Mængdeproduktet $\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3$ kan man, ved brug af et sædvanligt retvinklet koordinatsystem $X_1X_2X_3$, illustrere ved mængden af punkter i rummet.

Relationsbegrebet.

Ved en relation fra en mængde (eller klasse) A til en mængde (klasse) B forstås en delmængde (delklasse) R af det cartesiske produkt $A \times B$. - Med en mere primitiv sprogbrug kan man sige, at en relation fra A til B foreligger, når visse ordnede par (x,y) af et element x fra A og et element y fra B er udmærket eller udvalgt frem for de øvrige.

En relation fra A til A omtales også som en relation i A .

I stedet for $(x,y) \in R$ vil vi ofte skrive xRy , hvilket læses: x står i relationen R til y .

Relationer spiller en fundamental rolle inden for alle områder af matematikken. Vi nævner en række eksempler:

- 1° Allerede i den mest elementære geometri optræder den relation R fra mængden E_2 af punkter i planen til mængden af rette linier i planen, hvor xRy udtrykkes: punktet x ligger på linien y (eller: linien y går gennem punktet x).
- 2° En vigtig relation R i mængden $\mathbb{R}$ af reelle tal er den, hvor xRy skrives $x < y$.
- 3° En relation R (lighed) i klassen af alle (matematiske) objekter er den, hvor xRy skrives $x = y$.
- 4° En relation R fra klassen af alle (matematiske) objekter til klassen V af alle mængder er den, hvor xRy skrives $x \in y$.
- 5° En relation R (inklusion) i klassen V af alle mængder er den, hvor xRy skrives $x \subseteq y$.

En relation R fra en mængde (eller klasse) A til en mængde (klasse) B vil oftest være givet ved et prædikat $\Theta(x,y)$ med to variable x og y , hvor x refererer til A og y til B :

$$R = \{(x,y) \in A \times B \mid \Theta(x,y)\},$$

dvs. R er den delmængde (eller delklasse) af $A \times B$, hvor for $x \in A$, $y \in B$ gælder

$$(x,y) \in R \iff \Theta(x,y),$$

eller anderledes skrevet

$$xRy \iff \Theta(x,y).$$

Det forekommer hyppigt, at forskellige prædikater $\Theta(x,y)$ og

$\Psi(x,y)$ bestemmer én og samme relation fra A til B, nemlig når der for $x \in A$, $y \in B$ gælder

$$\Theta(x,y) \iff \Psi(x,y).$$

6° En vigtig relation i mængden $\mathbb{N}$ af naturlige tal, kendt fra barneskolen, defineres ved

$$x|y \iff \exists_{\mathbb{N}} z [y = zx].$$

$x|y$ læses: x går op i y, x er divisor i y, y er delelig med x.

7° En relation i mængden $\mathbb{N}$ af naturlige tal defineres ved: x har ingen divisor $\neq 1$ fælles med y, i tegn

$$\neg \exists z [z \neq 1 \wedge z|x \wedge z|y].$$

At x står i denne relation til y, udtrykkes: x er primisk med y.

8° En relation i mængden af rette linier i planen defineres ved: linien x har intet punkt fælles med linien y. At x står i denne relation til y, udtrykkes ofte: x er parallel med y. I reglen vil det dog være mere hensigtsmæssigt (jfr. side 13) også at regne sammenfaldende linier for parallelle; med brug af den under 1° nævnte grundlæggende geometriske relation "punkt på linie" defineres relationen "parallelitet" i mængden af rette linier i planen da ved

$$x||y \iff \neg \exists_{E_2} z [z \text{ på } x \wedge z \text{ på } y] \vee x = y.$$

Vi bemærker, at den samme relation kan defineres ved ganske andre prædikater, f.eks. ved: linierne x og y har en fælles normal.

9° En relation (kongruens) i mængden $\mathcal{D}(E_2)$ af punktmængder i i planen defineres ved $x \cong y \iff$ punktmængden x kan føres over i punktmængden y ved en isometrisk afbildning $f: E_2 \rightarrow E_2$.

Definitionen overføres umiddelbart fra planen til rummet.

10° En relation fra mængden $\mathbb{R}^{\mathbb{N}}$ af alle følger $x = (x_1, x_2, \dots)$ af reelle tal til mængden $\mathbb{R}$ af reelle tal y defineres ved

$$\lim_{n \rightarrow \infty} x_n = y \iff \forall_{\varepsilon > 0} \exists_{N \in \mathbb{N}} \forall_{n \in \mathbb{N}} [n > N \Rightarrow |y - x_n| < \varepsilon].$$

Man læser: talfølgen $x = (x_1, x_2, \dots)$ er konvergent med grænseværdien y .

Foruden relationer R , som har fået et særligt navn, eller hvor man har indført en fast betegnelse eller en særlig sproglig vending for xRy , vil vi træffe utallige "navnløse". Et vigtigt tilfælde nævnes i 11°.

11° Lad $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ være en reel funktion af to variable. En relation R i mængden $\mathbb{R}$ af reelle tal defineres da ved

$$xRy \iff f(x, y) = 0.$$

12° I mængden E_3 af punkter i rummet tænkes valgt et punkt O . En relation R i E_3 defineres da ved: x og y ligger på en ret linie gennem O .

I stedet for den korrekte vending "den ved prædikatet $\Theta(x, y)$ bestemte relation fra A til B " benyttes ofte den løse sprogbrug "relationen $\Theta(x, y)$ fra A til B ". Når man vil pointere, at man ikke tænker på prædikatet $\Theta(x, y)$, men på selve mængden $\{(x, y) \mid \Theta(x, y)\}$, omtaler man da denne som relationens graf.

Som delmængde af $\mathbb{R}^2$ kan en relation i $\mathbb{R}$ (eller relationens graf) anskueliggøres som en punktmængde i planen. For "relationen" $x < y$ i $\mathbb{R}$ er grafen således halvplanen $\{(x, y) \mid x < y\}$.

For en vilkårlig mængde (eller klasse) A kaldes mængden

$$\Delta = \{(x, x) \mid x \in A\}$$

for diagonalen i A^2 . Hermed har vi en betegnelse og et nyt navn for relationen "lighed" i A , - eller for relationens graf.

Lad R_1 være en relation fra A_1 til B_1 og R_2 en relation fra A_2 til B_2 , hvor $A_1 \subseteq A_2$ og $B_1 \subseteq B_2$. I tilfælde af at

$$R_1 = R_2 \cap (A_1 \times B_1),$$

dvs. hvis

$$\forall_{A_1} x \forall_{B_1} y [xR_1 y \iff xR_2 y],$$

siger man, at R_1 er restriktionen af R_2 til en relation fra A_1 til B_1 , eller at R_2 er en udvidelse af R_1 .

Som eksempel kan nævnes, at relationen " $<$ " i $\mathbb{R}$ er en udvidelse af relationen i $\mathbb{N}$ med samme betegnelse. - Betegnelser og navne for relationer bevares ofte uændret efter restriktion eller udvidelse.

Hidtil har der kun været tale om "binære" relationer, dvs. relationer mellem to objekter. En almindeliggørelse af relationsbegrebet er imidlertid nærliggende.

Ved en ternær relation forstås en delmængde af et cartesisk produkt $A \times B \times C$, ved en kvaternær relation en delmængde af et cartesisk produkt $A \times B \times C \times D$, osv.

Også relationer mellem flere objekter vil oftest være givet ved prædikater. En kvaternær relation i mængden E_2 af punkter i planen bestemmes således ved: punkterne v , x , y og z ligger på en cirkel. Relationer i $\mathbb{R}$ vil hyppigt være givet ved systemer af ligninger og/eller uligheder med flere eller færre reelle ubekendte (jfr. 11^o ovenfor).

Som delmængde af $\mathbb{R}^3$ kan en ternær relation i $\mathbb{R}$ anskueliggøres som en punktmængde i rummet.

Også uden for matematikken møder man talrige relationer. Som eksempel kan nævnes de forskellige slægtskabsrelationer mellem mennesker.

Invers relation. Sammensat relation.

Ved den inverse relation til en relation $R \subseteq A \times B$ forstås den relation $R^{-1} \subseteq B \times A$, hvor for $x \in A$, $y \in B$ gælder

$$yR^{-1}x \iff xRy.$$

Definitionen kan også udtrykkes

$$R^{-1} = \{(y, x) \mid (x, y) \in R\}.$$

Det er klart, at $(R^{-1})^{-1} = R$.

I nogle tilfælde har man faste betegnelser både for xRy og for $yR^{-1}x$. Således i eksemplerne 2°, 4° og 5°:

$$x < y \iff y > x, \quad x \in y \iff y \ni x, \quad x \subseteq y \iff y \supseteq x.$$

Når der i stedet for "relationen R , hvor $xRy \iff \Theta(x, y)$ " siges "relationen udtrykt ved $\Theta(x, y)$ " eller blot "relationen $\Theta(x, y)$ ", kan man i almindelighed ikke vide, om der tænkes på R eller R^{-1} . "Relationen i $\mathbb{N}$ udtrykt ved $\exists_{\mathbb{N}^2} [y = zx]$ " kan lige vel være den i 6° definerede relation og dens inverse. I tilfælde af at prædikatet er en sproglig sætning med én af de to variable som subjekt, menes dog sædvanligvis relationen S bestemt ved

$$.S. \iff \text{prædikatet},$$

hvor den pågældende variable skrives i stedet for første prik. Efter dette princip udtrykkes relationen i 6° ved "x går op i y", dens inverse ved "y er delelig med x" eller "y er et multiplum af x", relationen i 1° ved "punktet x ligger på linien y", dens inverse ved "linien y går gennem punkt x".

Lad R være en relation fra A til B og S en relation fra B til C . Ved den af R og S sammensatte relation forstås da den

relation $S \circ R$ fra A til C, hvor for $x \in A$, $z \in C$ gælder

$$(x, z) \in S \circ R \iff \exists_B y [xRy \wedge ySz].$$

Er specielt $A = B = C$ og $R = S$, skrives også R^2 i stedet for $R \circ R$.

Eksempler.

1) Lad A, B og C være mængden af henholdsvis punkter, rette linier og cirkler i planen. Med R betegnes relationen fra A til B udtrykt ved "punktet x ligger på linien y", med S relationen fra B til C udtrykt ved "linien y er tangent til cirklen z". At punkt x står i relationen $S \circ R$ til cirklen z, betyder da, at der findes en linie gennem x, som tangerer z, altså at punkt x ligger uden for eller på cirklen z.

2) Lad R være en relation fra A til B. Da er $R^{-1} \circ R$ en relation i A, medens $R \circ R^{-1}$ er en relation i B, og vi har

$$(x, z) \in R^{-1} \circ R \iff \exists_B y [xRy \wedge zRy] \quad \text{for } x \in A, z \in A,$$

$$(x, z) \in R \circ R^{-1} \iff \exists_A y [yRx \wedge yRz] \quad \text{for } x \in B, z \in B.$$

Betegner R eksempelvis relationen i $\mathbb{N}$ bestemt ved

$$xRy \iff x \neq 1 \wedge x|y,$$

vil " $x \in \mathbb{N}$ står i relationen $R^{-1} \circ R$ til $z \in \mathbb{N}$ " betyde, at x og z begge er $\neq 1$ og har et fælles multiplum, altså at x og z begge er $\neq 1$, medens " $x \in \mathbb{N}$ står i relationen $R \circ R^{-1}$ til $z \in \mathbb{N}$ " betyder, at x og z har en fælles divisor $\neq 1$. Den i 7^o betragtede relation er $\mathbb{N}^2 \setminus R \circ R^{-1}$.

3) Flere slægtskabsrelationer defineres som sammensatte relationer, hvilket i nogle tilfælde direkte udtrykkes i benævnelsen. Betegner R relationen udtrykt ved

$$xRy \iff x \text{ er barn af } y,$$

vil xR^2z betyde, at x er barnebarn af z , medens $(x,z) \in R^{-1} \circ R$ betyder, at x og z er (hel- eller halv-)søskende.

For tre relationer $R \subseteq A \times B$, $S \subseteq B \times C$ og $T \subseteq C \times D$ gælder

$$T \circ (S \circ R) = (T \circ S) \circ R = T \circ S \circ R,$$

hvor relationen $T \circ S \circ R \subseteq A \times D$ kan karakteriseres ved

$$(x,u) \in T \circ S \circ R \iff \exists_B y \exists_C z [xRy \wedge ySz \wedge zTu].$$

For relationer $R \subseteq A \times B$ og $S \subseteq B \times C$ haves

$$(S \circ R)^{-1} = R^{-1} \circ S^{-1},$$

thi for $x \in A$, $z \in C$ gælder

$$\exists_B y [xRy \wedge ySz] \iff \exists_B y [zS^{-1}y \wedge yR^{-1}x],$$

dvs.

$$(z,x) \in (S \circ R)^{-1} \iff (z,x) \in R^{-1} \circ S^{-1}.$$

Betegner R som i 3) relationen " x er barn af y ", vil $R^3 = R \circ R \circ R$ og $R^{-1} \circ (R^{-1} \circ R) \circ R = (R^2)^{-1} \circ R^2$ være velkendte slægtskabsrelationer.

Enentydig korrespondance. Afbildningsrelation.

En relation R fra en mængde (eller klasse) A til en mængde (klasse) B kaldes en enentydig korrespondance mellem A og B , hvis der for hvert $x \in A$ findes et og kun et $y \in B$, således at xRy , og ligeledes for hvert $y \in B$ et og kun et $x \in A$, således at xRy . En enentydig korrespondance mellem A og B er altså en mængde (klasse) R af par $(x,y) \in A \times B$, hvor hvert $x \in A$ er første komponent og hvert $y \in B$ anden komponent i netop ét par $(x,y) \in R$.

Betragtes kun én enentydig korrespondance R , vil vi i stedet for xRy ofte skrive $x \leftrightarrow y$, hvilket læses: x og y er sammenhø-

rende.

Eksempler.

- 1) På et dansegulv foreligger en enentydig korrespondance mellem mængden af dansende herrer og mængden af dansende damer.
- 2) Lad A være mængden af punkter på en kugleflade med undtagelse af ét punkt O ("nordpolen"), medens B er mængden af punkter i tangentplanen til kuglefladen i det diametralt modsatte punkt ("sydpolen"). En enentydig korrespondance mellem A og B defineres da ved

$$x \leftrightarrow y \iff x \text{ og } y \text{ ligger på en ret linie gennem } O.$$

Vi bemærker, at denne korrespondance er restriktionen af den i 12^o betragtede relation R i E_3 til en relation fra A til B .

- 3) Relationen i $\mathbb{R}$ defineret ved

$$xRy \iff x^3 + y^5 = 1$$

er en enentydig korrespondance.

- 4) Kun i ét af eksemplerne 1^o-10^o optræder en enentydig korrespondance, nemlig i 3^o.

En relation R fra en mængde (eller klasse) A til en mængde (klasse) B kaldes en afbildningsrelation, hvis der for hvert $x \in A$ findes et og kun et $y \in B$, således at xRy .

At en relation $R \subseteq A \times B$ er en enentydig korrespondance, er således ensbetydende med, at R og R^{-1} begge er afbildningsrelationer.

Begreberne afbildning og afbildningsrelation hænger nøje sammen:

Er f en afbildning af A ind i B , $f:A \rightarrow B$, vil relationen $R \subseteq A \times B$ bestemt ved

$$(*) \quad xRy \iff f(x) = y$$

være en afbildningsrelation, medens der omvendt for en vilkårlig afbildningsrelation $R \subseteq A \times B$ findes netop én afbildning $f:A \rightarrow B$, således at $(*)$ gælder for $x \in A$, $y \in B$, nemlig den, hvor til hvert $x \in A$ er tilordnet det $y \in B$, for hvilket xRy . - Den til en afbildning $f:A \rightarrow B$ svarende relation $R \subseteq A \times B$, altså $R = \{(x,y) \mid f(x) = y\}$, kaldes afbildningens graf. Er specielt $A \subseteq \mathbb{R}$ og $B = \mathbb{R}$, vil grafen, fortolket som en punktmængde i planen, være det velkendte grafiske billede af funktionen f .

Egentlig er det overflødigt at opretholde begrebet afbildning som et selvstændigt begreb: man kan indordne det under relationsbegrebet ved overalt, hvor talen er om afbildninger, at betragte de tilsvarende afbildningsrelationer.

Idet den indgående behandling af afbildninger, der er givet i de to foregående paragraffer, kan fortolkes som vedrørende afbildningsrelationer, skal vi her kun gøre følgende bemærkninger:

Sammensætning har vi defineret både for afbildninger (I,3,) og for relationer (I,5,7). Der kan dog ikke opstå misforståelser, thi er $R \subseteq A \times B$ og $S \subseteq B \times C$ afbildningsrelationer svarende til afbildninger $f:A \rightarrow B$ og $g:B \rightarrow C$, da svarer den sammensatte relation $S \circ R \subseteq A \times C$ til den sammensatte afbildning $g \circ f:A \rightarrow C$.

At en afbildning $f:A \rightarrow B$ er bijektiv, er ensbetydende med, at den tilsvarende relation $R \subseteq A \times B$ er en enentydig korrespondance. Den inverse relation $R^{-1} \subseteq B \times A$ vil da svare til den inverse afbildning $f^{-1}:B \rightarrow A$.

Eksempler.

Den afbildning af kugleflade \ "nordpol" på tangentplanen i "sydpolen", der svarer til den i 2) betragtede enentydige korrespondance, altså afbildningen, der til hvert $x \in A$ tilordner skæringspunktet y mellem nævnte tangentplan og den rette linie gennem O og x , kaldes stereografisk projektion.

Til den i 3) betragtede enentydige korrespondance R , henholdsvis til R^{-1} , svarer de bijektive afbildninger af $\mathbb{R}$ på $\mathbb{R}$

$$x \rightarrow \sqrt[5]{1 - x^3} \quad \text{og} \quad y \rightarrow \sqrt[3]{1 - y^5}.$$

Ofte træffes en relation $R \subseteq A \times B$, hvor til hvert $x \in A$ findes højst ét $y \in B$, således at xRy , dvs. hvor der for $x \in A$, $y_1 \in B$ og $y_2 \in B$ gælder

$$xRy_1 \wedge xRy_2 \Rightarrow y_1 = y_2.$$

Betragtet som relation fra $\{x \in A \mid \exists_B y: xRy\}$ til B vil R da være en afbildningsrelation.

Eksempler.

Relationen i $\mathbb{R}$ defineret ved

$$xRy \iff 4x^2 + y^2 = 1 \wedge y \geq 0$$

er, betragtet som relation fra intervallet $[-\frac{1}{2}, \frac{1}{2}] = \{x \mid \exists y: xRy\}$ til $\mathbb{R}$, en afbildningsrelation. Den tilsvarende afbildning af $[-\frac{1}{2}, \frac{1}{2}]$ ind i $\mathbb{R}$ er

$$x \rightarrow \sqrt{1 - 4x^2}, \quad -\frac{1}{2} \leq x \leq \frac{1}{2}.$$

Den i 10° definerede relation fra $\mathbb{R}^{\mathbb{N}}$ til $\mathbb{R}$ er af den her betragtede type; enhver talfølge har nemlig højst én grænseværdi. Betragtet som relation fra mængden af konvergente reelle talfølger til $\mathbb{R}$ er det da en afbildningsrelation; ved den tilsvarende afbildning tilordnes til hver konvergent reel talfølge dens

grænseværdi.

Ækvivalensrelation.

En relation R i en mængde (eller klasse) E siges at være refleksiv, hvis der for $x \in E$ gælder

$$xRx,$$

altså hvis hvert element af E står i relationen R til sig selv. Dette er ensbetydende med $\Delta \subseteq R$, hvor $\Delta = \{(x, x) \mid x \in E\}$ er diagonalen i $E \times E$ (jfr. side 5).

De i 3° , 5° , 6° , 8° , 9° og 12° betragtede relationer er refleksive.

En relation $R \subseteq E \times E$ siges at være symmetrisk, hvis der for $x \in E$, $y \in E$ gælder

$$xRy \Rightarrow yRx.$$

Dette er ensbetydende med $R^{-1} = R$.

De i 3° , 7° , 8° , 9° og 12° betragtede relationer er symmetriske.

En relation $R \subseteq E \times E$ siges at være transitiv, hvis der for $x \in E$, $y \in E$, $z \in E$ gælder

$$xRy \wedge yRz \Rightarrow xRz.$$

Dette er ensbetydende med $R^2 \subseteq R$.

De i 2° , 3° , 5° , 6° , 8° og 9° betragtede relationer er transitive. Det bemærkes, at parallelitet mellem rette linier kun er en transitiv relation, når man, som vi har gjort i 8° , regner sammenfaldende linier for parallelle.

Man kunne tro, at en symmetrisk og transitiv relation

$R \subseteq E \times E$ altid er reflektiv, idet man af xRy ved brug af symmetrien kan slutte yRx og videre ved brug af transitiviteten xRx . Dette viser imidlertid ikke, at xRx for alle $x \in E$, men kun for de $x \in E$, der står i relationen R til mindst et $y \in E$.

En relation R i en mængde (eller klasse) E kaldes en ækvivalensrelation i E , hvis den er reflektiv, symmetrisk og transitiv, altså hvis der for $x \in E$, $y \in E$, $z \in E$ gælder

- $\mathbb{E}1.$ $xRx,$
- $\mathbb{E}2.$ $xRy \Rightarrow yRx,$
- $\mathbb{E}3.$ $xRy \wedge yRz \Rightarrow xRz.$

Betragtes kun én ækvivalensrelation R , skrives i stedet for xRy oftest $x \sim y$, hvilket læses: x er ækvivalent med y , eller: x og y er ækvivalente; den sidste sprogbrug afspejler symmetrien. Undertiden bruges også andre tegn.

De i 3° , 8° og 9° betragtede relationer er ækvivalensrelationer. Det samme gælder restriktionen til $E_3 \setminus \{0\}$ af relationen i 12° .

Vi skal nu behandle en vigtig sag, etablering af en enentydig korrespondance mellem ækvivalensrelationerne i og klasseinddelingerne af en vilkårlig mængde E .

Idet vi tænker os givet en mængde E , vil vi med $a, b, \dots, x, y, \dots$ betegne elementer af E , med $A, B, \dots$ delmængder af E , med $\Phi, \Psi, \dots$ mængder af delmængder af E og med $R, S, \dots$ relationer i E .

Er Φ en klasseinddeling af E , altså en mængde af ikke tomme, parvis disjunkte delmængder af E med E som foreningsmængde (I, 2, 18),

vil den ved

(*) $xRy \iff x \text{ og } y \text{ ligger i samme mængde tilhørende } \Phi,$

dvs. ved

(*) $xRy \iff \exists_{\Phi} A [x \in A \wedge y \in A],$

bestemte relation R i E være en ækvivalensrelation. Dette verificeres umiddelbart.

Omvendt vil vi nu vise, at der for hver ækvivalensrelation R i E findes en og kun en klasseinddeling Φ af E , således at (*) gælder for $x \in E, y \in E$. Dermed vil være godtgjort, at der foreligger en enentydig korrespondance mellem mængden af ækvivalensrelationer i E og mængden af klasseinddelinger af E .

Lad da R være en ækvivalensrelation i E . For xRy skrives $x \sim y$.

Først foretages en analyse. Vi tænker os en klasseinddeling Φ af E , således at (*) gælder for $x \in E, y \in E$.

For hvert $a \in E$ ses nu ved brug af (*), at den klasse fra Φ , som a tilhører, består af de med a ækvivalente elementer, dvs. klassen er $\{x \in E \mid x \sim a\}$. Videre fås for $A \in \mathcal{D}(E)$

$$A \in \Phi \iff \exists_{\mathbb{E}} a: A = \{x \mid x \sim a\},$$

eller, idet vi for $\{x \mid x \sim a\}$ indfører betegnelsen F_a ,

$$A \in \Phi \iff \exists_{\mathbb{E}} a: A = F_a,$$

dvs. Φ er mængden af indbyrdes forskellige mængder $F_a = \{x \mid x \sim a\}$,

$$\Phi = \{F_a \mid a \in E\}.$$

Dette kan også opfattes således: Φ er billedmængden ved afbildningen af E ind i $\mathcal{D}(E)$ defineret ved

$$a \rightarrow \{x \mid x \sim a\}.$$

Hermed er analysen ført til ende. Den viste, at en mængde Φ

af delmængder af E , som dels er en klasseinddeling af E , dels sammen med den givne relation R opfylder (*), kun kan være $\{F_a \mid a \in E\}$. Specielt har vi da, at der findes højst én sådan mængde Φ .

Det bemærkes, at vi endnu ikke har benyttet, at R er en ækvivalensrelation. Var dette ikke tilfældet, kunne vi dog på forhånd vide, at ingen mængde af delmængder af E , og altså heller ikke $\{F_a \mid a \in E\}$, ville være en klasseinddeling af E , som sammen med R opfylder (*).

Nu er det imidlertid forudsat, at R er en ækvivalensrelation, og det kan da bevises, at $\{F_a \mid a \in E\}$ virkelig har de ønskede egenskaber.

For $\{F_a \mid a \in E\}$ indføres for kortheds skyld betegnelsen Ψ . Mængden Ψ af delmængder af E karakteriseres da ved, at der for $A \in \mathcal{D}(E)$ gælder

$$A \in \Psi \iff \exists_E a: A = \{x \mid x \sim a\},$$

dvs. mængderne tilhørende Ψ er de delmængder af E , som kan skrives på formen $\{x \mid x \sim a\}$.

Først vises, at Ψ er en klasseinddeling af E . At mængderne tilhørende Ψ er ikke tomme og har E som forening, følger af, at R er refleksiv, hvilken egenskab kan udtrykkes: for $a \in E$ gælder

$$a \in \{x \mid x \sim a\}.$$

Endvidere skal godtgøres, at mængderne tilhørende Ψ er parvis disjunkte, altså at der for $A \in \Psi$, $B \in \Psi$ gælder

$$A \neq B \Rightarrow A \cap B = \emptyset,$$

dvs.

$$A \cap B \neq \emptyset \Rightarrow A = B.$$

Af $c \in \{x \mid x \sim a\} \wedge c \in \{x \mid x \sim b\}$, dvs. $c \sim a \wedge c \sim b$ eller, idet symmetrien benyttes, $a \sim c \wedge c \sim b$, sluttes imidlertid, ved brug også af transitiviteten, $a \sim b$. Heraf fås videre $x \sim a \Rightarrow x \sim b$ (ifølge $\mathbb{E}3$) og $x \sim b \Rightarrow x \sim a$ (ifølge $\mathbb{E}2$ og $\mathbb{E}3$), altså for $x \in E$: $x \sim a \Leftrightarrow x \sim b$, hvilket er ensbetydende med $\{x \mid x \sim a\} = \{x \mid x \sim b\}$.

Endelig vises gyldigheden af

$$(*) \quad a \sim b \Leftrightarrow \exists_{\mathbb{A}} A[a \in A \wedge b \in A].$$

Er $a \sim b$, haves jo $a \in \{x \mid x \sim b\}$, men ifølge $\mathbb{E}1$ også $b \in \{x \mid x \sim b\}$. Omvendt: er $a \in \{x \mid x \sim c\} \wedge b \in \{x \mid x \sim c\}$, dvs. $a \sim c \wedge b \sim c$, fås $a \sim b$ ved brug af $\mathbb{E}2$ og $\mathbb{E}3$.

Hermed er følgende vigtige sætning bevist:

Mellem mængden af klasseinddelinger Φ af en vilkårlig mængde E og mængden af ækvivalensrelationer $\sim$ i E består en enentydig korrespondance, bestemt ved

$$\forall_{E} x, y [x \sim y \Leftrightarrow \exists_{\Phi} A[x \in A \wedge y \in A]].$$

At ækvivalensrelationen $\sim$ svarer til klasseinddelingen Φ , vil således sige, at $x \sim y$ er ensbetydende med, at x og y tilhører samme klasse. Den til en ækvivalensrelation $\sim$ svarende klasseinddeling Φ kan omvendt karakteriseres som den mængde Φ af delmængder af E , hvor

$$\forall_{D(E)} A [A \in \Phi \Leftrightarrow \exists_E a: A = \{x \mid x \sim a\}],$$

dvs. klasserne er de delmængder af E , som kan skrives på formen $\{x \mid x \sim a\}$.

Når en klasseinddeling Φ af E betragtes sammen med den tilsvarende ækvivalensrelation $\sim$, kaldes mængderne tilhørende Φ gerne ækvivalensklasser. Et element $a \in E$ siges at repræsentere eller at være en repræsentant for den ækvivalensklasse, det tilhører.

For restriktionen til $E_3 \setminus \{0\}$ af relationen i 12° er ækvivalensklasserne de rette linier gennem 0, dette punkt ikke medregnet. For relationen lighed, $x = y$, i en vilkårlig mængde E er den tilsvarende klasseinddeling den, hvor hvert element danner en klasse for sig. Til relationen i 8° svarer en inddeling af de rette linier i planen i klasser af indbyrdes parallelle; en ækvivalensklasse kaldes her et parallelbunt, medens en ækvivalensklasse ved relationen parallelitet for rette linier i rummet kaldes et parallelknippe. Til relationen i 9° svarer en inddeling af alle punktmængder i planen (rummet) i klasser af indbyrdes kongruente.

Følgende eksempler fremhæves særligt:

- 1) Lad f være en afbildning af en mængde E ind i en mængde B . Relationen i E defineret ved

$$x \sim y \iff f(x) = f(y)$$

er da en ækvivalensrelation i E . Ækvivalensklasserne er de fra forskellige originalmængder $f^{-1}(z)$ til elementer $z \in B$, (sammenlign I,3,).

Ækvivalensrelationer defineret på denne måde mødes ofte. Som eksempel fra den elementære geometri nævnes for polygoner relationen: x og y har samme areal. At to liniestykker har samme længdetal, er ensbetydende med, at de er kongruente; at to vinkler har samme måltal (mellem 0 og π), er ensbetydende med, at de er kongruente.

I øvrigt svarer enhver ækvivalensrelation i en mængde E på den betragtede måde til en afbildning, nemlig til afbildningen $f: E \rightarrow \hat{D}(E)$, hvor til hvert $a \in E$ er tilordnet den ækvivalensklasse,

der indeholder a .

2) Hvis en mængde T af transformationer af en mængde E er en transformationsgruppe, vil relationen i $\hat{D}(E)$ defineret ved

$$A \sim B \iff \exists_T f: f(A) = B$$

være en ækvivalensrelation i $\hat{D}(E)$.

Indeholder T nemlig den identiske afbildning e_E , vil relationen være reflektiv, idet $e_E(A) = A$ for hvert $A \subseteq E$. Gælder $f \in T \Rightarrow f^{-1} \in T$, vil relationen være symmetrisk; er nemlig $f(A) = B$ og $f \in T$, haves jo $f^{-1}(B) = A$. Gælder $f \in T \wedge g \in T \Rightarrow g \circ f \in T$, vil relationen være transitiv; er nemlig $f(A) = B$, $g(B) = C$, $f \in T$ og $g \in T$, haves jo $(g \circ f)(A) = C$.

Til transformationsgruppen af isometriske afbildninger (kongruenser) $f: E_2 \rightarrow E_2$ af planen svarer på denne måde relationen kongruens i mængden $\hat{D}(E_2)$ af punktmængder i planen, jfr. 9°. - To punktmængder i planen siges at være egentlig kongruente, hvis den ene kan føres over i den anden ved en flytning (egentlig kongruens) $f: E_2 \rightarrow E_2$. Også her foreligger en ækvivalensrelation, idet mængden af flytninger af planen er en transformationsgruppe. - Hvad her er sagt om planen, overføres ord til andet til rummet.

Bemærkning. Undertiden træffes en afvigende sprogbrug: I stedet for "egentlig kongruent" siges blot "kongruent", medens "kongruent" i vor betydning, jfr. 9°, gengives ved "isometrisk" eller "egentlig eller uegentlig kongruent".

3) Geometriske vektorer.

Til ethvert ordnet par (P, Q) af punkter i rummet svarer (jfr. I, 3, 3) en translation af rummet, specielt svarer til et par (P, P) den identiske afbildning. Ved

$(P, Q) \sim (R, S) \iff (P, Q)$ og (R, S) bestemmer samme translation
 defineres da, ifølge 1), en ækvivalensrelation i mængden $E_3 \times E_3$
 af ordnede punktpar. Til hver translation t svarer en ækvivalens-
 klasse bestående af alle punktpar, der bestemmer t ; det er i øv-
 rigt punktparrene $(P, t(P))$, $P \in E_3$.

I fremstillingen af elementær vektorregning er side EV,1,1,
 givet følgende definition: Ved en geometrisk vektor forstås et
 liniestykke i rummet forsynet med en bestemt gennemløbsretning.
 To sådanne liniestykker skal dog opfattes som samme vektor, så-
 fremt de blot har samme størrelse og retning. - Tilføjelsen inde-
 bærer, at en geometrisk vektor dog ikke er det samme som et ori-
 enteret liniestykke. Hvad er det da?

Først bemærkes, at man i stedet for orienterede liniestyk-
 ker kan betragte ordnede par af punkter, idet opgivelse af et
 orienteret liniestykke kommer ud på et med opgivelse af begyndel-
 sespunkt og endepunkt. Hermed er vi imidlertid lige vidt: en geo-
 metrisk vektor er nu et ordnet punktpar; dog skal to punktpar op-
 fattes som samme vektor, såfremt de bestemmer samme translation.

Mystikken hæves, når dette opfattes som en løs formulering
 af følgende definition: Ved en geometrisk vektor forstås en
ækvivalensklasse af ordnede punktpar ved den ovenfor indførte
ækvivalensrelation. Et punktpar (P, Q) er herefter ikke en vektor,
 men det repræsenterer en vektor. Betegnelsen $\vec{PQ}$ skal betyde den
 vektor, som repræsenteres af punktparret (P, Q) ; vektorer betegnes
 også med et enkelt understreget bogstav.

En fordel ved at gå ud fra punktpar i stedet for liniestyk-
 ker er det, at nulvektoren kommer med på naturlig måde, $\underline{0} =$
 $\{(P, P) \mid P \in E_3\}$.

Vi noterer, at der mellem mængden af geometriske vektorer og mængden af translationer af rummet består en naturlig enentydig korrespondance.

Man møder ofte, som i 3), en situation, hvor indbyrdes ækvivalente elementer ved en ækvivalensrelation i en mængde E opfattes som uvæsentligt forskellige, hvorfor man "identificerer" dem, regner dem som blot forskellige eksemplarer af samme ting. Dette kan tillægges den mening, at det i virkeligheden er ækvivalensklasserne, der har interesse; de enkelte elementer i E betragtes blot som repræsentanter for disse.

Når man for en opgave vedrørende konstruktion af en trekant anfører f.eks., at der er to løsninger, menes i reglen: pånar kongruens to løsninger, hvilket betyder, at løsningerne udgør to ækvivalensklasser ved relationen kongruens, $\cong$.

Undertiden (mis)bruges lighedstegnet til at udtrykke ækvivalens. I elementære geometribøger betyder $\angle A = \angle B$ således ikke, at der er tale om samme vinkel, men blot at de to vinkler har samme måltal.

Ordningsrelation.

En relation R i en mængde (eller klasse) A siges at være asymmetrisk, hvis der for $x \in A$, $y \in A$ gælder

$$x \neq y \wedge xRy \Rightarrow \neg yRx$$

eller, ensbetydende hermed,

$$xRy \wedge yRx \Rightarrow x = y.$$

At der blot er tale om en omformulering, beror på den ud-

sagnslogiske ækvivalens

$$\neg r \wedge p \Rightarrow \neg q \text{ eq } p \wedge q \Rightarrow r,$$

som f.eks. kan vises således:

$$\begin{aligned} \neg r \wedge p \Rightarrow \neg q &\text{ eq } \neg r \Rightarrow (p \Rightarrow \neg q) \\ &\text{ eq } \neg r \Rightarrow (\neg p \vee \neg q) \text{ eq } p \wedge q \Rightarrow r. \end{aligned}$$

At en relation $R \subseteq A \times A$ er asymmetrisk, betyder med andre ord, at $R \cap R^{-1} \subseteq \Delta$, hvor $\Delta = \{(x,x) \mid x \in A\}$ er diagonalen i $A \times A$. Med R vil derfor også enhver relation $S \subseteq R$ være asymmetrisk, ligesom asymmetri bevares, når der til R føjes elementer (x,x) af diagonalen.

Transitivitet for en relation $R \subseteq A \times A$ definerede vi (side 13) ved for $x \in A$, $y \in A$, $z \in A$ at kræve

$$xRy \wedge yRz \Rightarrow xRz.$$

Da denne betingelse øjensynlig er opfyldt for $x = y \vee y = z$, vil det være nok at betragte tilfældet $x \neq y \wedge y \neq z$; betingelsen er altså ensbetydende med

$$x \neq y \wedge y \neq z \wedge xRy \wedge yRz \Rightarrow xRz,$$

dvs.

$$(x,y) \in R \setminus \Delta \wedge (y,z) \in R \setminus \Delta \Rightarrow (x,z) \in R.$$

Det fremgår heraf, at transitivitet bevares, når der til en relation $R \subseteq A \times A$ føjes elementer af diagonalen Δ . Fjernes fra en relation elementer af diagonalen, kan transitivitet derimod gå tabt (jfr. 8°); vi skal imidlertid se, at transitivitet sammen med asymmetri bevares:

Lad $R \subseteq A \times A$ være transitiv og asymmetrisk, og lad $R \setminus \Delta \subseteq S \subseteq R$. Det påstår da, at S er transitiv; (at S er asymmetrisk, ved vi på forhånd). - Det vil være nok at vise, at

$R \setminus \Delta$ er transitiv. Vi fører beviset ved ud fra antagelserne R transitiv, men $R \setminus \Delta$ ikke transitiv at slutte, at R ikke er asymmetrisk. Tænker vi os nemlig, efter antagelsen $R \setminus \Delta$ ikke transitiv, elementer a, b og c af A , for hvilke

$(a,b) \in R \setminus \Delta \wedge (b,c) \in R \setminus \Delta$, men $(a,c) \notin R \setminus \Delta$,
fås, da R er transitiv, at $(a,c) \in R$ og dermed $(a,c) \in \Delta$, dvs.
 $a = c$, således at

$$aRb \wedge bRa \wedge a \neq b.$$

Medens en relation $R \subseteq A \times A$ som nævnt (side 13) kaldes refleksiv, hvis $\forall_A x: xRx$, vil vi sige, at R er irrefleksiv, hvis $\forall_A x: \neg xRx$, dvs. hvis $R \cap \Delta = \emptyset$.

En relation R i en mængde (eller klasse) A siges at være en refleksiv ordningsrelation i A , hvis den er refleksiv, asymmetrisk og transitiv, altså hvis der for $x \in A, y \in A, z \in A$ gælder

$$\text{OR1.} \quad xRx,$$

$$\text{OR2.} \quad x \neq y \wedge xRy \Rightarrow \neg yRx,$$

$$\text{OR3.} \quad xRy \wedge yRz \Rightarrow xRz,$$

medens R siges at være en irrefleksiv ordningsrelation, hvis den er irrefleksiv, asymmetrisk og transitiv; her forlanges altså i stedet for OR1, at der for $x \in A$ skal gælde

$$\text{OR1}^{\wedge}. \quad \neg xRx.$$

Vi nævner, at det ved definitionen på irrefleksiv ordningsrelation ville være nok at forlange $\text{OR1}^{\wedge}$ og OR3 gyldige; thi hvis en relation $R \subseteq A \times A$ er irrefleksiv og transitiv, så er den også

asymmetrisk. Beviset herfor kan føres ved ud fra antagelserne R transitiv, men ikke asymmetrisk at slutte, at R ikke er irrefleksiv.

Refleksive og irrefleksive ordningsrelationer i A hører sammen parvis: fra en ordningsrelation af den ene type fås en af den anden ved at fjerne, henholdsvis tilføje diagonalen i $A \times A$; herved bevares nemlig transitivitet og asymmetri, som nærmere omtalt ovenfor.

Betragtes kun én refleksiv ordningsrelation R og den tilsvarende irrefleksive $\hat{R}$, vil vi, når der ikke er indført særlige tegn for relationerne, i stedet for xRy og $x\hat{R}y$ skrive henholdsvis $x \preceq y$ og $x \prec y$. Sammenhængen mellem de to relationer, $\hat{R} = R \setminus \Delta$ og $R = \hat{R} \cup \Delta$, kan da udtrykkes

$$x \prec y \iff x \preceq y \wedge x \neq y,$$

henholdsvis

$$x \preceq y \iff x \prec y \vee x = y.$$

Man bruger den vending, at en (refleksiv eller irrefleksiv) ordningsrelation i A bestemmer en ordning af elementerne i A . Ordningen siges at være total (fuldstændig), hvis der for $x \in A$, $y \in A$ gælder

$$x \neq y \Rightarrow x \preceq y \vee y \preceq x$$

eller, ensbetydende hermed,

$$x \neq y \Rightarrow x \prec y \vee y \prec x,$$

altså hvis vilkærlig to forskellige elementer af A kan "sammenlignes" ved den pågældende ordning. Vil man understrege, at en betragtet ordning ikke nødvendigvis er total, omtales den også som en partiell (delvis) ordning.

Ved en vilkårlig ordning haves

$$x -< y \Rightarrow \neg(y \leq x), \quad \text{dvs. } y \leq x \Rightarrow \neg(x -< y),$$

medens det er karakteristisk for total ordning, at også det omvendte gælder, således at

$$\neg(y \leq x) \Leftrightarrow x -< y, \quad \text{dvs. } \neg(x -< y) \Leftrightarrow y \leq x.$$

Thi $x -< y$ medfører $x \neq y$ ifølge OR1 og videre $\neg(y -< x)$ ifølge OR2, men $x \neq y \wedge \neg(y -< x)$ er ensbetydende med $\neg(x = y \vee y -< x)$, dvs. med $\neg(y \leq x)$. At ordningen er total vil sige, at der for vilkårlige x og y gælder

$$x = y \vee x -< y \vee y -< x, \quad \text{dvs. } y \leq x \vee x -< y,$$

hvilket jo er ensbetydende med $\neg(y \leq x) \Rightarrow x -< y$.

Den i 2° betragtede relation $<$ er en irrefleksiv ordningsrelation; den tilsvarende refleksive ordningsrelation i $\mathbb{R}$ skrives $\leq$; ordningen af $\mathbb{R}$ er total. Relationerne i 3°, 5° og 6° er refleksive ordningsrelationer; den til = svarende irrefleksive ordningsrelation er $\emptyset$, den til $\subseteq$ svarende skrives $\subset$ (jfr. I, 2, 7), medens vi ikke vil indføre nogen særlig betegnelse for $x|y \wedge x \neq y$; i intet af de 3 tilfælde foreligger en total ordning.

Den inverse relation til en refleksiv eller irrefleksiv ordningsrelation er en ordningsrelation af samme type. Eksempelvis gælder dette de inverse til relationerne $<$, $\leq$ og $\subset$, $\subseteq$, som skrives $>$, $\geq$ og $\supset$, $\supseteq$.

Er $B \subseteq A$, vil restriktionen til B af en ordningsrelation i A igen være en ordningsrelation af samme type. Når ordningen af A er total, vil restriktionen til B også være det; derimod forekommer det ofte, at hvilkesomhelst to forskellige elementer i B kan sammenlignes ved ordningen, uden at det tilsvarende gælder for A .

I det følgende defineres en række vigtige begreber i tilknytning til en given ordning af en mængde (eller klasse) E . For den betragtede refleksive ordningsrelation skrives $\preceq$, for den irrefleksive $<$. Elementer af E betegnes med små latinske bogstaver, delmængder (delklasser) af E med store.

Et element $a \in E$ siges at være en minorant for mængden (klassen) $X \subseteq E$, hvis $a \preceq x$ for ethvert $x \in X$, altså hvis

$$\forall x [x \in X \Rightarrow a \preceq x], \text{ dvs. } \forall x [x \in X \Rightarrow a \preceq x].$$

Tilsvarende siges b at være majorant for X , hvis $x \preceq b$ for ethvert $x \in X$.

Findes der en minorant for X , siges X at være nedad begrænset, findes en majorant for X , siges X at være opad begrænset. At X er begrænset, skal betyde, at X er både nedad og opad begrænset.

Hvis X har en minorant a , som tilhører X , siges X at have a som første element, og man skriver $a = \min X$. At X højst kan have ét element med denne egenskab, følger umiddelbart af, at relationen $\preceq$ er asymmetrisk. Hvis X har en majorant b , som tilhører X , siges X at have b som sidste element, og man skriver $b = \max X$. Der findes højst ét element med denne egenskab.

Det kan hælde, at mængden (eller klassen) af minoranter for en nedad begrænset mængde (klasse) $X \subseteq E$ har et sidste element a . Man siger da, at X har den nedre grænse a , og betegner denne $\inf X$ (infimum X). At $a = \inf X$ betyder altså, at a er minorant for X , samt at der for enhver minorant x for X gælder $x \preceq a$. Det er efter definitionen klart, at et $X \subseteq E$ højst kan have én nedre grænse.

Tilsvarende indføres øvre grænse for $X \subseteq E$ som "første majorant" for X . Der er højst én. Nødvendigt, men i almindelighed ik-

ke tilstrækkeligt for eksistensen er det, at X er opad begrænset. Som betegnelse bruges $\sup X$ (supremum X).

At X har et første (sidste) element, er åbenbart ensbetydende med, at X har en nedre (øvre) grænse, som tilhører X ; i så fald er $\inf X = \min X$ ($\sup X = \max X$).

Et element m tilhørende X siges at være et minimalelement af X , hvis der ikke findes noget $x \in X$, for hvilket $x < m$. I tilfælde af, at ordningen er total, falder begreberne minimalelement og første element sammen; thi da gælder

$\neg(x < m) \iff m \leq x$ og dermed

$$\neg \exists_X x [x < m] \iff \forall_X x [m \leq x].$$

Er ordningen ikke total, vil som før et eventuelt første element af X også være et minimalelement af X , og der vil ikke være andre; men har X intet første element, kan der dog være et minimalelement i X , ja der kan være flere, endog uendelig mange. - Ganske tilsvarende bemærkninger gælder begrebet maksimalelement, der indføres ved definitionen: et element m siges at være et maximalelement af X , hvis

$$m \in X \wedge \neg \exists_X x [m < x].$$

Eksempler.

- 1) Mængden $\mathbb{Z}$ med den sædvanlige totale ordning, $\leq, <$. Enhver nedad (opad) begrænset mængde $X \subseteq \mathbb{Z}$ har et første (sidste) element.
- 2) Mængden $\mathbb{Q}$ med den sædvanlige totale ordning, $\leq, <$. Her findes nedad (opad) begrænsede mængder $X \subseteq \mathbb{Q}$ uden nedre (øvre) grænse. F.eks. har $\{x \in \mathbb{Q} \mid x^2 < 2\}$ både minoranter og majoranter, men hverken en nedre eller øvre grænse. Mængden

$\{1/n \mid n \in \mathbb{N}\}$ har et sidste element, 1; den har ikke noget første element, men nok en nedre grænse, 0.

3) Mængden $\mathbb{R}$ med den sædvanlige totale ordning, $\leq, <$. Enhver nedad (opad) begrænset mængde $X \subseteq \mathbb{R}$ har en nedre (øvre) grænse. Dette er en af de fundamentale egenskaber ved de reelle tal.

4) Mængden $\mathcal{D}(A)$ af delmængder af en mængde A , ordnet ved inklusion, $\subseteq, \subset$. Enhver mængde $X \subseteq \mathcal{D}(A)$, altså enhver mængde af delmængder af A , er såvel nedad som opad begrænset, idet $\emptyset$ er en minorant og A en majorant. Enhver mængde $X \subseteq \mathcal{D}(A)$ har en nedre grænse, nemlig $\bigcap \{x \mid x \in X\}$, og en øvre grænse, nemlig $\bigcup \{x \mid x \in X\}$. Disse kan være (men behøver ikke at være) henholdsvis første eller sidste element. En mængde $m \in X$ er minimalelement (maximalelement) af X , hvis ingen mængde $x \in X$ er ægte delmængde af m (har m som ægte delmængde). Som eksempel nævnes, at når elementerne af X er fra $\emptyset$ forskellige, parvis disjunkte mængder, er hver af disse såvel minimal- som maximalelement af X .

5) Mængden $\mathbb{N}$ ordnet ved den refleksive ordningsrelation $x|y$, x er divisor i y . Enhver mængde $X \subseteq \mathbb{N}$ er nedad begrænset, idet 1 er en minorant, og har endvidere en nedre grænse, nemlig største fælles divisor for tallene i X (se øvelse 21). En mængde $X \subseteq \mathbb{N}$ er opad begrænset, hvis og kun hvis den er endelig. I så fald er f.eks. produktet af tallene i X en majorant for X , og tallenes mindste fælles multiplum er øvre grænse. Mængden $\{12, 18, 36\}$ har nedre grænse 6, der ikke er første element, og øvre grænse 36, der er sidste element. Et element m i en mængde $X \subseteq \mathbb{N}$ er minimalelement (maximalelement) af X , hvis intet andet tal tilhørende X er divisor i m (er et multiplum af m). I en

mængde $X \subseteq \mathbb{N}$, som ikke indeholder tallet 1, vil eventuelle primtal tilhørende X være minimalelementer, men muligvis ikke de eneste.

Lad f være en afbildning af en mængde (eller klasse) A ind i en mængde (klasse) A' , og lad der være givet en ordning af A såvel som en ordning af A' . For den refleksive ordningsrelation i A skrives $\leq$, for den tilhørende irrefleksive $<$, medens der for ordningen af A' bruges betegnelserne $\leq'$, $<'$. Man siger da, at f er monoton, hvis der for $x \in A$, $y \in A$ gælder

$$x \leq y \Rightarrow f(x) \leq' f(y)$$

eller, ensbetydende hermed,

$$x < y \Rightarrow f(x) <'_f(y),$$

medens f siges at være ordenstro eller strengt monotont, hvis der for $x \in A$, $y \in A$ gælder

$$x < y \Rightarrow f(x) <'_f(y).$$

Medens endog en konstant afbildning f er monotont, gælder det, at hvis ordningen af A er total og f strengt monotont, så vil f være injektiv. Thi for vilkårlige to forskellige elementer x og y af A haves da enten $x < y$ og dermed $f(x) <'_f(y)$, eller $y < x$ og dermed $f(y) <'_f(x)$; i begge tilfælde er $f(x) \neq f(y)$.

Eksempler.

- 1) Tilordner man til hver endelig mængde antallet af dens elementer, fås en strengt monotont afbildning af klassen af endelige mængder ordnet ved inklusion ind i $(\mathbb{N}_0, <)$.
- 2) Den identiske afbildning af $\mathbb{N}$ er en ordenstro afbildning af $(\mathbb{N}, |)$ ind i $(\mathbb{N}, <)$, idet

$$x|y \wedge x \neq y \Rightarrow x < y.$$

3) De (strengt) monotone afbildninger af $(I, <)$ ind i $(\mathbb{R}, <)$, hvor $I \subseteq \mathbb{R}$ er et interval, er netop de på I definerede (strengt) voksende funktioner, medens de (strengt) monotone afbildninger af $(I, <)$ ind i $(\mathbb{R}, >)$ er de på I definerede (strengt) aftagende funktioner.

Det bemærkes, at vi i disse eksempler såvel som senere angiver en ordnet mængde, dvs. en mængde A samt en refleksiv og den tilhørende irrefleksive ordningsrelation i A , ved at anføre mængden og en af de to relationer. Således betegner både $(\mathbb{N}, <)$ og $(\mathbb{N}, \leq)$ mængden af naturlige tal med den sædvanlige ordning.

Velordning.

En ordning af en mængde (eller klasse) M , givet ved en refleksiv eller den tilhørende irrefleksive ordningsrelation i M , siges at være en velordning, hvis hver ikke tom delmængde (delklasse) af M har et første element.

En velordning er altid total, idet definitionen heraf (side 24) kommer ud på, at enhver delmængde bestående af to elementer skal have et første element.

Er M velordnet, er det endvidere klart, at en vilkårlig delmængde (delklasse) ligeledes vil være velordnet ved restriktionen af ordningen i M .

I det følgende forudsættes M velordnet; vi skriver som sædvanlig $\leq$ og $<$ for de to sammenhørende ordningsrelationer.

Til ethvert element $x \in M$, som ikke er sidste element i M , findes et (og selvfølgelig kun et) umiddelbart følgende, dvs. et element x' , således at $x < x'$ og at der for ethvert $y \in M$, for

hvilket $x \prec y$, gælder $x' \preceq y$.

Bevis: Da ordningen er total og x ikke er sidste element, er mængden $\{y \in M \mid x \prec y\}$ ikke tom. Den har følgelig et første element x' , og dette opfylder de stillede krav.

Med det ved $a \in M$ bestemte afsnit M_a af M menes

$$M_a = \{x \in M \mid x \prec a\}.$$

Ved anvendelse af dette begreb kan den vigtige sætning om transfinit induktion formuleres således:

Er X en delmængde (delklasse) af M , der stadig forudsættes velordnet, gælder det, at hvis

$$\forall_M a [M_a \subseteq X \Rightarrow a \in X],$$

så er $X = M$.

(Bemærk, at kravet omfatter, at det første element a_1 af M tilhører X , idet jo $M_{a_1} = \emptyset$ og $\emptyset \subseteq X$.)

Bevis: Påstanden kan også udtrykkes

$$X \subset M \Rightarrow \exists_M a [M_a \subseteq X \wedge a \notin X].$$

Vi antager, at $X \subset M$, dvs. at $M \setminus X$ ikke er tom, og betegner med a det første element af $M \setminus X$. Vi har da $a \in M \setminus X$ og dermed $a \notin X$. Endvidere er $M_a \subseteq X$, hvilket ses således: idet a er minorant for $M \setminus X$, gælder for $x \in M$

$$x \in M \setminus X \Rightarrow a \preceq x$$

og dermed

$$x \in M \setminus X \Rightarrow \neg(x \prec a),$$

dvs.

$$x \prec a \Rightarrow x \in X,$$

altså

$$x \in M_a \Rightarrow x \in X.$$

Eksempler.

- 1) Enhver totalt ordnet endelig mængde er velordnet.
- 2) Den ordnede mængde $(\mathbb{N}, <)$ er velordnet. Det umiddelbart efter et tal $x \in \mathbb{N}$ følgende er $x + 1$. Sætningen om transfinit induktion udsiger i dette tilfælde: En mængde $X \subseteq \mathbb{N}$ vil være hele $\mathbb{N}$, hvis $1 \in X$ og der for $a > 1$ gælder

$$\{1, \dots, a-1\} \subseteq X \Rightarrow a \in X.$$

Den sædvanlige induktionsslutning beror på, at en mængde $X \subseteq \mathbb{N}$ vil være hele $\mathbb{N}$, hvis $1 \in X$ og der for $a > 1$ gælder

$$a-1 \in X \Rightarrow a \in X.$$

Denne sætning fås af den foregående, idet man benytter

$$\{1, \dots, a-1\} \subseteq X \Rightarrow a-1 \in X.$$

Eksempelvis er det nu ligeledes indlysende, at en mængde $X \subseteq \mathbb{N}$ vil være hele $\mathbb{N}$, hvis $\{1, 2\} \subseteq X$ og der for $a > 2$ gælder

$$\{a-2, a-1\} \subseteq X \Rightarrow a \in X.$$

- 3) Den ordnede mængde $(\mathbb{Z}, <)$ er ikke velordnet, men enhver nedad begrænset delmængde er det. Ligeledes er enhver opad begrænset delmængde af $(\mathbb{Z}, <)$ velordnet ved $>$.

Det cartesiske produkt $\prod_{i \in J} A_i$.

Lad der være givet en indiceret mængde af mængder, $(A_i)_{i \in J}$; hermed menes, jfr. I,3, , en afbildning af indexmængden J ind i klassen af alle mængder. Det givne er med andre ord, at der til hver index $i \in J$ er tilordnet en mængde A_i .

Ved det cartesiske produkt eller mængdeproduktet $\prod_{i \in J} A_i$ forstås mængden af alle afbildninger $(a_i)_{i \in J}$, hvor $\forall i \in J: a_i \in A_i$.

Et element i $\prod_{\iota \in J} A_\iota$ er altså en tilordning: til hver index $\iota \in J$ et element $a_\iota \in A_\iota$.

Er $J = \{1, 2, \dots, m\}$ bruges også skrivemåden $\prod_{\iota=1}^m A_\iota$. Mellem denne mængde og $A_1 \times A_2 \times \dots \times A_m$ består en naturlig enentydig korrespondance, idet der til en afbildning $(a_\iota)_{\iota \in J}$ svarer det ordnede sæt $(a_1, a_2, \dots, a_m)$. Ofte skelner man ikke mellem $(a_\iota)_{\iota \in J}$ og $(a_1, a_2, \dots, a_m)$ og har da

$$\prod_{\iota=1}^m A_\iota = A_1 \times A_2 \times \dots \times A_m.$$

Er $J = \mathbb{N}$ bruges også skrivemåderne

$$\prod_{\iota=1}^{\infty} A_\iota = A_1 \times A_2 \times \dots,$$

ligesom et element i produktmængden betegnes $(a_1, a_2, \dots)$.

Når A_ι er en og samme mængde A for alle $\iota \in J$, er $\prod_{\iota \in J} A_\iota$ simpelthen mængden af alle afbildninger af J ind i A . Denne mængde betegnes også A^J eller $\hat{F}(J \rightarrow A)$. Eksempelvis er $\mathbb{R}^{\mathbb{R}} = \hat{F}(\mathbb{R} \rightarrow \mathbb{R})$ mængden af reelle funktioner af en reel variabel, $\mathbb{R}^{\mathbb{N}}$ mængden af følger af reelle tal.

Afbildningen af $\prod_{\iota \in J} A_\iota$ på den til en index $\nu \in J$ svarende mængde A_ν bestemt ved

$$(a_\iota)_{\iota \in J} \rightarrow a_\nu$$

kaldes den til ν svarende projektion af $\prod_{\iota \in J} A_\iota$ og betegnes pr_ν . Navnet hidrører fra fortolkningen af elementerne i $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \mathbb{R}^{\{1,2\}}$ og $\mathbb{R}^3$ som koordinatsæt for punkter.

Ved brug af begrebet mængdeprodukt kan vi udtrykke et af mængdelærens fundamentale principper, det såkaldte udvalgsaksiom, i følgende form: Er hverken indexmængden J eller nogen af

mængderne A_ι tom, så er også $\bigcap_{\iota \in J} A_\iota \neq \emptyset$. Dette betyder, at der findes en tilordning: til hver index $\iota \in J$ et element $a_\iota \in A_\iota$, eller, med en løs sprogbrug, at man på en gang for hvert ι "kan udvælge" et element af den tilsvarende mængde A_ι .

Dette princip (som i parentes bemærket er blevet betragtet med skepsis af enkelte fremstående matematikere) blev første gang explicit formuleret af E. Zermelo (1904). Han udnyttede det, i en tilsyneladende lidt mere speciel form, i et bevis for velordningssætningen, der udsiger, at enhver mængde kan velordnes. Denne sætning har, som det antydes i næste paragraf, vigtige konsekvenser inden for læren om (uendelige) kardinaltal. - Zermelos udgangspunkt var, at der for en vilkårlig mængde Φ af ikke tomme mængder findes en tilordning: til hver mængde $M \in \Phi$ et af dens elementer. Dette følger af princippet ovenfor, idet man sætter $J = \Phi$ samt $A_M = M$ for hvert $M \in \Phi$.

Når man bruger ordet aksiom, beror det på, at udvalgsprincippet, i en eller anden form, virkelig optræder blandt aksiomerne i de forskellige forslag, der er gjort til opstilling af mængdelæren som en formal, matematisk teori (I,1,24). Det første skyldes Zermelo (1908). - Andre aksiomer vedrører udsorteringen af mængder blandt klasser (jfr. I,2,5); således svarer begge de to side I,2,9 nævnte regler til aksiomer hos Zermelo, hvor det ligeledes er et aksiom, at $\bigcup_{\iota \in J} A_\iota$ er en mængde (og ikke kun en klasse), forudsat at såvel J som samtlige A_ι er mængder, medens det er et teorem, at $\bigcap_{\iota \in J} A_\iota$ er en mængde. I de forskellige systemer optræder altid et aksiom vedrørende eksistensen af uendelige mængder; en mulighed er: klassen $\mathbb{N}$ af naturlige tal er en mængde; det kan derefter sluttes, at også $\mathbb{Q}$, $\mathbb{R}$ og $\mathbb{C}$ er mængder.

Øvelser til kap. I, § 5.

1. Fortolk hver af mængderne $\mathbb{R} \times \mathbb{R}_+$, $\mathbb{R}_+ \times \mathbb{R}_+$, $\mathbb{R} \times \mathbb{Z}$, $\mathbb{R}_+ \times \mathbb{Z}$, $\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z} \times \mathbb{N}$ og $\mathbb{N} \times \mathbb{N}$ som en punktmængde i planen.
2. Lad A betegne mængden af punkter tilhørende et liniestykke, B mængden af punkter på en ret linie, C mængden af punkter i en halvplan, D mængden af punkter på en cirkellinie og E mængden af punkter tilhørende en cirkelskive. Angiv punktmængder i rummet, der kan fortolkes som mængderne $A \times C$, $B \times C$, $A \times D$, $B \times D$, $C \times D$, $A \times E$, $B \times E$, $D \times D$ og $D \times E$.
3. Idet A og B er vilkårlige mængder, $A' \subseteq A$, $A'' \subseteq A$ og $B' \subseteq B$, skal man vise

$$(A' \cup A'') \times B = (A' \times B) \cup (A'' \times B)$$

$$(A' \cap A'') \times B = (A' \times B) \cap (A'' \times B)$$

$$(A \times B) \setminus (A' \times B') =$$

$$[(A \setminus A') \times (B \setminus B')] \cup [(A \setminus A') \times B'] \cup [A' \times (B \setminus B')].$$

4. Skitser grafen for relationen R i $\mathbb{R}$ bestemt ved

$$\text{a)} \quad xRy \iff x \leq y,$$

$$\text{b)} \quad xRy \iff x > y,$$

$$\text{c)} \quad xRy \iff x^2 - y^2 = 0,$$

$$\text{d)} \quad xRy \iff x^2 - y^2 \leq 0,$$

$$\text{e)} \quad xRy \iff x - y^2 = 0,$$

$$\text{f)} \quad xRy \iff x - y^2 > 0,$$

og angiv i hvert tilfælde følgende mængder af reelle tal:

$$\{y \mid (0, y) \in R\}, \quad \{y \mid (1, y) \in R\},$$

$$\{x \mid (0, x) \in R^{-1}\}, \quad \{x \mid (1, x) \in R^{-1}\}.$$

5. Idet A og B er mængden af punkter, henholdsvis rette linier i planen, medens R betegner relationen fra A til B , hvor

$$xRy \iff \text{punktet } x \text{ ligger på linien } y,$$

og Δ_B er diagonalen i B^2 , skal man angive betydningen af relationerne

$$R \circ R^{-1}, \quad R^{-1} \circ R \quad \text{og} \quad \Delta_B \cup (B^2 \setminus (R \circ R^{-1})).$$

6. Vis, at for to ikke tomme mængder A og B er $A \times B \neq B \times A$, medmindre $A = B$. Gør rede for, at der består en naturlig enentydig korrespondance mellem $A \times B$ og $B \times A$.

Gør endvidere rede for, at der mellem produktmængder

$(A \times B) \times C$, $A \times (B \times C)$ og $A \times B \times C$, taget to og to, består naturlige enentydige korrespondancer.

7. Hvorledes giver det sig til kende i grafen for en relation $R \subseteq \mathbb{R} \times \mathbb{R}$, at R er henholdsvis en afbildningsrelation, en enentydig korrespondance, refleksiv, symmetrisk?

8. Find betingelser vedrørende en afbildning $f: A \rightarrow A$, som er nødvendige og tilstrækkelige for, at den tilsvarende afbildningsrelation $R \subseteq A \times A$ er henholdsvis refleksiv, symmetrisk, transitiv.

9. For en vilkårlig relation $R \subseteq A \times A$ gælder

$$R \text{ transitiv} \iff R^2 \subseteq R.$$

Vis, at dette kan føres tilbage til den logiske ækvivalens

$$"\forall y [p(x,y,z) \Rightarrow q(x,z)]" \quad \text{eq} \quad "\exists y p(x,y,z) \Rightarrow q(x,z)"$$

og dermed til

$$"\forall y [p(y) \Rightarrow q]" \quad \text{eq} \quad "\exists y p(y) \Rightarrow q".$$

Vis endvidere, hvorledes sidstnævnte logiske ækvivalens kan afledes af ækvivalenser kendt fra I,1 samt

$$"\forall y [p(y) \vee q]" \quad \text{eq} \quad "\forall y p(y) \vee q".$$

10. En mængde E med mindst to elementer tænkes givet.

1) Til enhver mængde Φ af delmængder af E svarer en relation R i E bestemt ved

$$(*) \quad xRy \iff \exists_{\Phi} A [x \in A \wedge y \in A].$$

Gør rede for, at R kan være en ækvivalensrelation, uden at Φ eller $\Phi \setminus \emptyset$ er en klasseinddeling.

2) Til enhver relation R i E svarer en mængde Φ af delmængder af E bestemt ved

$$A \in \Psi \iff \exists_E a: A = \{x \mid xRa\}.$$

Gør rede for, at Ψ kan være en klasseinddeling, uden at R er en ækvivalensrelation.

11. Angiv den ækvivalensklasse ved relationen $\sin x = \sin y$ i $\mathbb{R}$, der har det reelle tal a som repræsentant. Angiv en mængde af reelle tal omfattende netop én repræsentant for hver klasse.

12. Find en nødvendig og tilstrækkelig betingelse for, at to trekanter er ækvivalente ved den til transformationsgruppen af alle translationer og homotetier af planen E_2 svarende ækvivalensrelation i $\mathcal{D}(E_2)$.

13. Angiv ved en figur en punktmængde i planen, som kan fortolkes som $A \times A$, hvor $A = \{1, 2, 3, 4, 5, 6\}$. Angiv i en sådan figur graferne for følgende relationer i A :

- a) $\{(a, b) \mid ab = 6\},$
- b) $\{(a, b) \mid a+b \text{ er lige}\},$
- c) $\{(a, b) \mid a|b\},$
- d) $\{(a, b) \mid a \text{ og } b \text{ er indbyrdes primiske}\},$

- e) $\{(a,b) \mid 2[\frac{1}{2}a] = b\},$
- f) $\{(a,b) \mid |a-b| \leq 1\},$
- g) $\{(a,b) \mid |a-b| = 3\},$
- h) $\{(a,b) \mid \max\{a, 6-b\} = 4\},$

Undersøg, hvilke af relationerne der er refleksive, irrefleksive, symmetriske, asymmetriske, transitive, og hvilke der er afbildningsrelationer, enentydige korrespondancer.

14. Giv en nødvendig og tilstrækkelig betingelse for, at en relation $R \subseteq A \times A$ er både symmetrisk og asymmetrisk.
15. Ud fra en relation $R \subseteq A \times A$ bestemmes to relationer R_1 og R_2 i A ved

$$xR_1y \iff xRy \wedge \neg yRx,$$

$$xR_2y \iff xRy \wedge x \neq y.$$

- a) Vis, at hvis R er asymmetrisk, så er $R_1 = R_2$.
 - b) Vis, at hvis R er transitiv, så er R_1 en irrefleksiv ordningsrelation.
 - c) Som vist side 22 gælder det, at transitivitet sammen med asymmetri bevares, når man fra en relation $R \subseteq A \times A$ fjerner de eventuelle elementer af diagonalen. Giv et nyt bevis.
16. Afsæt i planen endelig mange punkter. Mængden af disse punkter betegnes med A . Forbind visse par af punkterne med liniestykker (eller kurver, - undgå for overskuelighedens skyld, at disse får andre fællespunkter end de givne). Vælg for hvert af liniestykkerne én eller begge orienteringer, og angiv dem ved pile. Man kan da tale om et liniestykkes begyndelses- og endepunkt. Har et liniestykke begge

orienteringer, kan hvert af de punkter, det forbinder, betragtes som begyndelses- eller som endepunkt. Ved en vej i en sådan figur forstås et ordnet sæt af liniestykker blandt de tegnede, således at det første liniestykkes endepunkt er det andetets begyndelsespunkt, det andetets endepunkt er det tredje begyndelsespunkt, osv. En relation R i A defineres ved fastsættelsen, at aRb betyder, at der findes en vej, der fører fra a til b .

Vis, at R er transitiv. Vis endvidere, at R er asymmetrisk, hvis og kun hvis der ikke findes nogen lukket vej i figuren. Tegn figurer af den betragtede art, således at R er henholdsvis en ækvivalensrelation, en total ordningsrelation, en partiel, men ikke total, ordningsrelation.

17. Lad A være en mængde af tegn, nemlig alfabetets (små) bogstaver samt et mellemrums- eller tomrumstegn, f.eks. en prik. Ved den alfabetiske orden sammen med fastsættelsen, at mellemrumstegnet skal gå forud for bogstavet a , bestemmes en total ordning af A . Ved et "ord" af længden λ , hvor λ er et naturligt tal, forstås et λ -sæt af elementer af A . Lad M betegne en mængde af "ord" af længden λ , altså $M \subseteq A^\lambda$. I M defineres en relation R på følgende måde: Et ord $\Phi \in M$ siges at stå i relationen R til ordet $\Psi \in M$, hvis $\Phi \neq \Psi$ og det første tegn i Φ , som er forskelligt fra det på den tilsvarende plads stående tegn i Ψ , går forud for dette i den for tegnene i A fastsatte orden. Vis, at R er en irrefleksiv total ordningsrelation i M . (Leksikografisk ordning).

18. Lad der være givet en total ordning af en mængde A . For den reflektive ordningsrelation skrives $\leq$, for den irreflektive $<$. Idet a, b og c er tre forskellige elementer af A , skal man vise, at et og kun ét af dem "ligger mellem de to andre". (At et element e ligger mellem elementerne d og f betyder, at $d < e < f$ eller $f < e < d$.)

Ved afsluttede, åbne og halvåbne intervaller i en totalt ordnet mængde forstås delmængder af formerne

$$[a, b] = \{x \mid a \leq x \leq b\}, \quad]a, b[= \{x \mid a < x < b\},$$

$$[a, b[= \{x \mid a \leq x < b\}, \quad]a, b] = \{x \mid a < x \leq b\}.$$

Vis, at hvis J er et interval og $c, d \in J$, så er $[c, d] \subseteq J$.

Bevis endelig følgende sætning: Hvis det for endelig mange intervaller i en totalt ordnet mængde gælder, at fællesmængden for hvilke som helst to af dem ikke er tom, så er fællesmængden for dem alle ikke tom. (Betragt f.eks. først tre intervaller, og anvend induktion.)

- 19*. Lad $A = \{a_1, a_2, \dots, a_n\}$ være en endelig mængde, hvis elementer tænkes repræsenteret ved n punkter i planen, således at ikke tre af punkterne ligger på ret linie. For hvert af de liniestykker, der forbinder to af punkterne, vælges én orientering, der angives ved en pil. Derved defineres en relation R i A , idet $(a_i, a_j) \in R$, hvis $a_i \neq a_j$ og liniestykket, der forbinder de to punkter er orienteret fra a_i mod a_j . Denne relation er irrefleksiv og asymmetrisk, og der gælder

$$(*) \quad a_i \neq a_j \Rightarrow (a_i, a_j) \in R \vee (a_j, a_i) \in R,$$

sml. side 24. Omvendt kan enhver relation i en endelig mængde, som opfylder disse betingelser, anskueliggøres på den angivne måde.

Vis, at der findes mindst ét blandt punkterne i A , fra hvilket man kan komme til ethvert andet punkt i A enten ved at gennemløbe ét af liniestykkerne i den foreskrevne retning eller ved at gennemløbe to af dem i træk i de for dem foreskrevne retninger. Formuleret som et udsagn om relationen R er påstanden: Der findes mindst ét element $a_\mu \in A$, således at der for hvert element $a_i \neq a_\mu$ af A gælder, at $(a_\mu, a_i) \in R$ eller $(a_\mu, a_i) \in R^2$. (Betragt f.eks. et punkt i A , for hvilket antallet af punkter i A , som kan nås fra det på den forlangte måde, er størst muligt.) Slut af resultatet, at påstanden gælder for enhver relation i en endelig mængde, som blot opfylder betingelsen (*).

20. I mængden $\mathbb{R}^2$ af par af reelle tal defineres en relation $\preceq$ ved

$$(x_1, x_2) \preceq (y_1, y_2) \iff x_1 \leq y_1 \wedge x_2 \leq y_2.$$

Gør rede for, at $\preceq$ er en reflektiv ordningsrelation.

Idet $\mathbb{R}^2$ betragtes med den herved bestemte ordning, skal man for nedennævnte delmængder af $\mathbb{R}^2$ angive eventuelle første og sidste elementer, minimal- og maximalelementer samt nedre og øvre grænser:

$$\{(x_1, x_2) \mid x_1 \geq 0 \wedge x_2 \geq 0\}, \quad \{(x_1, x_2) \mid x_1^2 + x_2^2 \leq 1\}.$$

21. Lad X være en, eventuelt uendelig, mængde af naturlige tal. Mængden $A = \{a \in \mathbb{N} \mid \forall_X x: a \mid x\}$ af minoranter for X i $(\mathbb{N}, \mid)$, altså af fælles divisorer for tallene i X , har, da den er opad begrænset i $(\mathbb{N}, \leq)$, et sidste element d ved den sædvanlige ordning $\leq$. Vis, at ethvert $a \in A$ er divisor i d , og

dermed, at d er nedre grænse for X i $(\mathbb{N}, |)$. - Det forudsættes kendt, at mindste fælles multiplum for to tal er divisor i ethvert fælles multiplum.

22*. Idet R er en reflektiv og transitiv relation i en mængde E , skal man vise, at relationen i E givet ved

$$a \sim b \iff aRb \wedge bRa,$$

altså relationen $R \cap R^{-1}$, er en ækvivalensrelation i E .

Vis endvidere, at

$$aRb \wedge a \sim a' \wedge b \sim b' \Rightarrow a'Rb'.$$

I kraft heraf findes en (og naturligvis kun én) relation $\preceq$ i mængden $\tilde{E}$ af ækvivalensklasser ved $\sim$, således at der for $a \in E$, $b \in E$ gælder

$$K_a \preceq K_b \iff aRb,$$

hvor K_a og K_b betegner ækvivalensklasserne repræsenteret ved henholdsvis a og b . Vis, at $\preceq$ er en reflektiv ordningsrelation i $\tilde{E}$.

I en lidt løsere formulering kan ovenstående sammenfattes således: En reflektiv og transitiv relation R i en mængde E går over i en reflektiv ordningsrelation, når man identificerer sådanne elementer a og b , for hvilke både aRb og bRa .

Betragt følgende specielle tilfælde:

1) $E = \mathbb{C}$ er mængden af komplekse tal, og R er givet ved

$$aRb \iff |a| \leq |b|.$$

2) $E = \mathbb{Z}$ er mængden af hele tal, og R er givet ved

$$aRb \iff a|b.$$

3) $E = \hat{F}(A \rightarrow B)$ er mængden af afbildninger af en mængde A

ind i en mængde B , og R er givet ved

$$aRb \iff a(A) \subseteq b(A).$$

4) $E = \mathbb{R}^{\mathbb{N}}$ er mængden af reelle talfølger, og R er givet ved

$$aRb \iff \exists_{\mathbb{N}}^m \forall_{\mathbb{N}}^n [n > m \Rightarrow a_n \leq b_n],$$

hvor $a = (a_1, a_2, \dots)$ og $b = (b_1, b_2, \dots)$.

23. Er delmængderne

$$\{p + 1/q \mid p, q \in \mathbb{N}\}, \quad \{p - 1/q \mid p, q \in \mathbb{N}\}$$

af $\mathbb{Q}$ velordnede ved $\leq$? Ved $\geq$?

24. Lad M være velordnet ved relationen $-<$. Vis, at der for hver ordenstro afbildning $f: (M, -<) \rightarrow (M, -<)$ gælder $x \leq f(x)$ for alle $x \in M$.

Slut heraf, at den eneste surjektive ordenstro afbildning af $(M, -<)$ på $(M, -<)$ er den identiske, og at der ikke findes nogen surjektiv ordenstro afbildning af et afsnit $M_a = \{x \in M \mid x -< a\}$ på et fra dette forskelligt afsnit eller på $(M, -<)$.

25. Bevis ved induktion i den velordnede mængde $(\mathbb{N} \setminus \{1\}, <)$:

a) Ethvert naturligt tal $n \neq 1$ kan opløses i primfaktorer, dvs. n er et primtal eller et produkt af primtal.

b) Ethvert naturligt tal $n \neq 1$ har, bortset fra faktorerens rækkefølge, højst én primfaktoropløsning.

Ved beviset for b) forudsættes det kendt, at et primtal, der går op i et produkt, vil gå op i mindst en af faktorerne. Vedrørende b) bemærkes endvidere, at det vil være bekvemt i sætningen om induktion side 31 at tænke sig

$M_a \subseteq X \Rightarrow a \in X$ kontraponeret, altså erstattet med $a \notin X \Rightarrow M_a \not\subseteq X$.

26. For naturlige tal p og n sættes $s_p(n) = \sum_{\nu=1}^n \nu^p$.

Find $s_p(n)$ udtrykt ved $s_1(n), \dots, s_{p-1}(n)$; - hertil anvendes binomialformlen på $(\nu + 1)^{p+1}$. Vis, at der for hvert $p \in \mathbb{N}$ findes et polynomium P_{p+1} af graden $p + 1$ og med rationale koefficienter, således at $\forall_{n \in \mathbb{N}}: s_p(n) = P_{p+1}(n)$.

AG I,2,18₈

"hvilkesomhelst to", læs: "hvilkesomhelst to forskellige".

AG I,2,øv.6⁴

"tangentterne", læs: "tangentstykkerne".

AG I,3,øv.7²

"på side I,3,2", læs: "1a-10b side I,2,12 ff. i forbindelse
med $B \setminus A = B \cap C$ ".

AG I,4,4₁₁

"I,3,5-6", læs: "I,2,17".

AG I,4,16a¹

"En mængde", læs: "En ikke tom mængde".

AG I,4,øv.12⁴" $\hat{C}^\infty(]a,b[, \mathbb{R})$ ", læs: " $\hat{C}^\infty(]a,b[, \mathbb{R})$ ".AG I,8,7₇

"delmængder", læs: "ikke tomme delmængder".

AG I,8,11⁵ (1962-63)

"endelige", læs: "endelige mængder".

AG I,8,12⁷ ff. (1961-62)" $F(J)$ ", læs: " $\hat{F}(J \rightarrow \mathbb{R})$ "; " $C(J)$ ", læs: " $\hat{C}(J \rightarrow \mathbb{R})$ ".AG I, 8,12₁ (1961-62)

"(se øv.15)", læs: "(se øv. 16)".

AG I, 8.øv.3⁴" $ax + by \equiv 0 \pmod{m}$ ", læs: " $m \mid (ax + by)$ ".

"(Jfr. I,7,øv.7.)" slettes.

§ 6. Mængders ækvipotens.

Ækvipotensbegrebet.

En mængde A siges at være lige mægtig eller ækvipotent med en mængde B , hvis der findes en bijektiv afbildning af A på B , - sagt med andre ord: hvis der findes en enentydig korrespondance mellem A og B . " A er ækvipotent med B " udtrykkes også " A er (i Cantors forstand) ækvivalent med B "; man skriver $A \sim B$.

Den herved definerede relation, ækvipotens, er en ækvivalensrelation i klassen af alle mængder, dvs. for vilkårlige mængder A , B og C gælder

$$A \sim A,$$

$$A \sim B \Rightarrow B \sim A,$$

$$A \sim B \wedge B \sim C \Rightarrow A \sim C.$$

Thi den identiske afbildning e_A er en bijektiv afbildning af A på A ; er f en bijektiv afbildning af A på B , da vil den omvendte afbildning f^{-1} være en bijektiv afbildning af B på A ; er f en bijektiv afbildning af A på B og g en bijektiv afbildning af B på C , da vil den sammensatte afbildning $g \circ f$ være en bijektiv afbildning af A på C .

Bemærkning. Idet klassen V af alle mængder ikke selv er en mængde, kan vi ikke anvende resultatet side I,5,17 vedrørende sammenhæng mellem ækvivalensrelation og klasseinddeling. Til relationen $\sim$ svarer da heller ikke i strengeste forstand nogen klasseinddeling af V ; dette beror dog kun på, at klasserne $\{X \in V \mid X \sim A\}$ ikke er mængder, og derfor ikke kan samles som elementer i en klasse Φ .

At to endelige mængder er lige mægtige, kommer ud på, at de har lige mange elementer. Det er ikke nødvendigt at foretage nogen optælling for at konstatere, at der er lige mange damer og

herrer på et dansegulv, - her foreligger nemlig en enentydig korrespondance mellem de to mængder. Tilsvarende kan man undersøge, om der er lige mange elementer i to vilkårlige endelige mængder ved at prøve, om det er muligt at danne par, uden at noget element bliver tilovers. Georg Cantor (1845-1918) har skabt ækvipotensbegrebet ved at overføre denne idé også til uendelige mængder. Som allerede den enentydige korrespondance

$$\begin{array}{ccccccc} 1, & 2, & 3, & \dots, & n, & \dots \\ \updownarrow & \updownarrow & \updownarrow & & \updownarrow & \\ 2, & 4, & 6, & \dots, & 2n, & \dots \end{array}$$

viser, optræder dog nye momenter: en ægte del af en uendelig mængde kan være ækvipotent med mængden selv. Man har derfor foretrukket at indføre en ny sprogbrug, at tale om samme mægtighed eller ækvipotens i stedet for f.eks. at sige, at der er lige så mange positive lige tal som positive hele tal overhovedet.

Endelige mængder.

En ikke tom mængde siges at være endelig, hvis den er ækvipotent med et afsnit $A_m = \{1, 2, \dots, m\}$ af talrækken.

Antallet af elementer i en mængde M siges at være m , hvis

$$M \sim \{1, 2, \dots, m\}.$$

Denne definition er i overensstemmelse med sædvanlig optælling. At tælle elementerne i en mængde M kommer jo ud på at tilvejebringe en injektiv afbildning af mængden ind i $\mathbb{N}$, således at billedmængden bliver et afsnit: til et vilkårligt valgt element i M knyttes tallet 1, til et fra det første forskelligt element knyttes tallet 2, osv. til M måtte være udtømt.

Fundamentalt er det nu, at har man ved en optælling fundet antallet m af elementer i en mængde, da kan man ikke ved at tælle

elementerne i en anden rækkefølge nå til et andet antal; en mængde kan ikke være ækvipotent med to forskellige afsnit af talrækken.

Dette, som vi allerede stiltiende har benyttet i de foregående paragraffer (specielt ved undersøgelsen af permutationer), kan siges at bero på, at to forskellige afsnit af talrækken ikke kan være ækvipotente. Så fundamental denne sætning om de naturlige tal end er, plejer man dog ikke at tage den som et særskilt aksiom, idet den kan bevises ud fra andre grundlæggende egenskaber; herom senere (Matematik 3).

Enhver ikke tom endelig mængde M har således et bestemt antal elementer, - der findes netop ét naturligt tal m , således at

$$M \sim A_m = \{1, 2, \dots, m\}.$$

Dette tal m kaldes også kardinaltallet for mængden M . - Den tomme mængde $\emptyset$ regnes endelig og tilskrives kardinaltallet 0. Dette indordnes under de almene definitioner, idet man sætter $A_0 = \emptyset$.

Vi noterer:

1. To endelige mængder er ækvipotente, hvis og kun hvis de har samme kardinaltal.

Ved de orienterende bemærkninger ovenfor om ækvipotensbegrebet regnedes dette for indlysende. Efter at der nu er givet en nøjagtig definition af alle de indgående begreber, vil det imidlertid være rimeligt at bevise sætningen. Lad da M og N betegne to endelige mængder, m og n deres kardinaltal. Vi har altså $M \sim A_m$ og $N \sim A_n$. Er nu $M \sim N$, slutter vi $A_m \sim A_n$ og dermed $m = n$, idet to forskellige afsnit af talrækken ikke kan være ækvipotente. Forudsættes omvendt $m = n$, altså $A_m = A_n$, sluttet $M \sim N$.

De følgende påstande om sammenligning af endelige mængders kardinaltal indser man uden vanskelighed ved benyttelse af endnu en sætning om naturlige tal, hvis bevis ud fra andre grundlæggende egenskaber udskydes til senere (Matematik 3), nemlig:

En ægte delmængde M af et afsnit $A_n = \{1, 2, \dots, n\}$ af talrækken vil altid være ækvipotent med et afsnit $A_m = \{1, 2, \dots, m\}$, hvor $m < n$, dvs. M er endelig med kardinaltal $m < n$.

2. En ægte delmængde M af en endelig mængde N er selv endelig og har mindre kardinaltal end N .

Ved en bijektiv afbildning af N på et afsnit A_n af talrækken vil M nemlig gå over i en ægte del af A_n .

Corollar af 1 og 2: En endelig mængde er ikke ækvipotent med nogen af sine ægte delmængder.

3a. Lad M og N være ikke tomme, endelige mængder med kardinaltalene m og n . Da gælder $m \leq n$, hvis og kun hvis der findes en injektiv afbildning af M ind i N .

Thi ved en injektiv afbildning af M ind i N vil M føres over i N eller i en ægte del af N , hvorfor $m = n$ eller $m < n$. Forudsættes omvendt $m \leq n$, da kan den identiske afbildning e_{A_m} af A_m på sig selv opfattes som en injektiv afbildning af A_m ind i A_n ; betegnes med f en bijektiv afbildning af M på A_m , med g en bijektiv afbildning af N på A_n , vil derfor $g^{-1} \circ e_{A_m} \circ f$ være en injektiv afbildning af M ind i N .

Som corollar nævnes det såkaldte skuffeprincip: Er M og N endelige mængder med kardinaltal m og n , hvor $m > n > 0$, da vil der ved enhver afbildning af M ind i N findes et element i N , som er billede af mindst to elementer i M . - Ifølge sætningen vil nemlig ingen afbildning af M ind i N være injektiv. - Idet elementerne i N kaldes skuffer, og en afbildning af M ind i N

fortolkes som en fordeling af M 's elementer i disse skuffer, kan princippet formuleres: Er flere end n ting anbragt i n skuffer, da findes en skuffe med mindst to ting. (Øvelserne 1-3 handler om anvendelser heraf.)

3.b Lad M og N være ikke tomme, endelige mængder med kardinaltallene m og n . Da gælder $m \leq n$, hvis og kun hvis der findes en surjektiv afbildning af N på M .

3b. følger af 3a., idet man bemærker, at hvis der findes en injektiv afbildning af M ind i N , findes der også en surjektiv afbildning af N på M , og omvendt. Dette indses således: Lad $\varphi: M \rightarrow N$ være injektiv. Afbildningen $\psi: N \rightarrow M$ defineret ved

$$\psi(y) = \begin{cases} \varphi^{-1}(y) & \text{for } y \in \varphi(M), \\ a & \text{for } y \in N \setminus \varphi(M), \end{cases}$$

hvor a er et vilkårlig valgt element af M , er da surjektiv, idet jo allerede $\varphi^{-1}: \varphi(M) \rightarrow M$ er det. Omvendt, lad $\psi: N \rightarrow M$ være surjektiv, hvilket jo betyder, at ingen originalmængde $\psi^{-1}(x)$, $x \in M$, er tom. For hvert $x \in M$ vælges ét element tilhørende $\psi^{-1}(x)$. Betegnes dette med $\varphi(x)$, vil $x \rightarrow \varphi(x)$ være en afbildning af M ind i N , som er injektiv, da originalmængderne $\psi^{-1}(x)$ er parvis disjunkte.

Uendelige mængder.

Vi har allerede set (side 2), at en ægte del af en uendelig mængde kan være ækvipotent med mængden selv; af det følgende vil endda fremgå, at enhver uendelig mængde er ækvipotent med ægte delmængder af sig selv. Det ligger da nær at spørge, om alle uendelige mængder er indbyrdes ækvipotente. At dette ikke er tilfældet, er en fundamental opdagelse af G. Cantor (1873), som vil blive omtalt nedenfor. Det er derfor motiveret at opstille føl-

gende definition:

En mængde A siges at være numerabel (eller tællelig), hvis den er ækvipotent med mængden $\mathbb{N}$ af naturlige tal, hvis der altså findes en bijektiv afbildning af $\mathbb{N}$ på A . Dette kommer ud på, at der findes en følge $(a_1, a_2, \dots)$ af elementer af A , som indeholder hvert element af A en og kun én gang.

Eksempler på numerable mængder, foruden $\mathbb{N}$ selv, er:
 $\mathbb{Z}$, idet $(0, 1, -1, 2, -2, \dots, n, -n, \dots)$ er en følge af den forlangte art; endvidere $\mathbb{N} \times \mathbb{N}$, idet følgen

$$((1,1), (1,2), (2,1), (1,3), (2,2), (3,1), (1,4), (2,3), \dots),$$

der er dannet på følgende måde, indeholder hvert par

$(p, q) \in \mathbb{N} \times \mathbb{N}$ en og kun én gang: Man tager først det par (p, q) , for hvilket $p + q = 2$, dernæst de to par, for hvilke $p + q = 3$, ordnet efter voksende $p, \dots$, de n par, for hvilke $p + q = n + 1$, ordnet efter voksende $p, \dots$. Der gælder altså

$$\mathbb{N} \times \mathbb{N} \sim \mathbb{N}.$$

Hvis A og B er numerable mængder, vil $A \times B$ også være numerabel. Af $A \sim \mathbb{N}$ og $B \sim \mathbb{N}$ kan nemlig sluttes, at $A \times B \sim \mathbb{N} \times \mathbb{N}$; thi er $f: A \rightarrow \mathbb{N}$ og $g: B \rightarrow \mathbb{N}$ bijektive afbildninger, bestemmes ved $(a, b) \rightarrow (f(a), g(a))$ en bijektiv afbildning af $A \times B$ på $\mathbb{N} \times \mathbb{N}$. Specielt har man altså $\mathbb{Z} \times \mathbb{Z} \sim \mathbb{N}$.

Enhver delmængde af en numerabel mængde er højst numerabel, dvs. numerabel eller endelig.

Bevis: Lad $(a_1, a_2, \dots)$ være en følge, som indeholder hvert element af den numerable mængde A netop én gang, og lad $A' \neq \emptyset$ være en delmængde af A . Med a_{n_1} betegnes det første af elementerne $a_1, a_2, \dots$, som tilhører A' , med a_{n_2} det første element efter a_{n_1} , som tilhører A' , med a_{n_3} det første element efter a_{n_2} , som tilhører A' , osv. Ender dette ved, at der efter m skridt ikke er

flere elementer af A' tilbage, bestemmes der ved $i \rightarrow a_{n_i}$ en bi-jektiv afbildning af $\{1, 2, \dots, m\}$ på A' , som da er endelig. Ellers fås en følge, som indeholder hvert element af A' netop én gang.

Heraf kan sluttet, at mængden $\mathbb{Q}$ af rationale tal er numerabel; thi der består en enentydig korrespondance mellem $\mathbb{Q}$ og en uendelig delmængde af den numerable mængde $\mathbb{Z} \times \mathbb{Z}$, nemlig mængden af parrene (p, q) , hvor $p \in \mathbb{Z}$, $q \in \mathbb{N}$ og p og q er relativ prime (har største fælles divisor 1).

Enhver uendelig mængde har numerable delmængder.

Bevis: Lad A være en uendelig mængde. Et vilkårlig valgt element af A betegnes med a_1 , et vilkårlig valgt element af $A \setminus \{a_1\}$ med a_2 , et vilkårlig valgt element af $A \setminus \{a_1, a_2\}$ med a_3 , ... , et vilkårlig valgt element af $A \setminus \{a_1, \dots, a_n\}$ med a_{n+1} . Dette kan fortsættes ubegrænset; thi da A er uendelig, kan ingen af mængderne $A \setminus \{a_1, \dots, a_n\}$ være tom. Man får altså en følge af indbyrdes forskellige elementer af A , og mængden af dennes elementer er numerabel.

(Det bemærkes, at man i dette ræsonnement, og også i mange andre, går ud fra den forestilling, at uendelig mange udvalg som de beskrevne kan foretages uden angivelse af en forskrift, der tillader at udpege de pågældende elementer. Dette finder sit udtryk i et af mængdelærens aksiomer, det såkaldte udvalgsaksiom, som kan formuleres således: Er Φ en mængde af delmængder af en mængde M , eksisterer der en afbildning $f: \Phi \rightarrow M$, således at $f(A) \in A$ for hver mængde tilhørende Φ .)

Ingen mængde M er ækvipotent med mængden $\mathfrak{D}(M)$ af sine delmængder.

Bevis: For en vilkårlig mængde M er, som tidligere vist, $\mathfrak{D}(M)$ ækvipotent med mængden X_M af funktioner $\chi: M \rightarrow \{0, 1\}$. Det

er altså tilstrækkeligt at godtgøre, at M ikke er ækvipotent med X_M . Beviset føres ved G. Cantors diagonalmetode. For at idéen kan træde tydeligt frem, vil vi først gennemføre ræsonnementet for tilfældet $M = \mathbb{N}$.

En funktion $\chi: \mathbb{N} \rightarrow \{0,1\}$ vil jo (AG I, 4, 4) sige en følge

$$(0, 1, 1, 1, 0, 1, \dots),$$

hvor vi på hver plads har 0 eller 1. Vi skal vise, at mængden $X_{\mathbb{N}}$ af sådanne følger ikke er numerabel, dvs. ikke selv kan ordnes i en følge. Dette indses derved, at ingen følge $\chi_1, \chi_2, \dots, \chi_n, \dots$ af elementer i $X_{\mathbb{N}}$ kan udtømme $X_{\mathbb{N}}$. For en hvilken som helst følge

$$\chi_1 = (0, 1, 1, 1, \dots),$$

$$\chi_2 = (1, 1, 0, 0, \dots),$$

$$\chi_3 = (1, 1, 1, 0, \dots),$$

$$\chi_4 = (1, 0, 1, 0, \dots),$$

$$\vdots \quad \vdots$$

kan man nemlig angive et element χ i $X_{\mathbb{N}}$, som ikke er med; hertil udtages "diagonalfølgen"

$$(0, 1, 1, 0, \dots),$$

som på n^{te} plads stemmer overens med χ_n , $n = 1, 2, \dots$; derefter udskiftes på hver plads 0 med 1 eller 1 med 0:

$$\chi = (1, 0, 0, 1, \dots).$$

Den således bestemte følge χ er virkelig forskellig fra alle χ_n , $n = 1, 2, \dots$: den afviger fra χ_1 i hvert fald på 1^{ste} plads, fra χ_2 i hvert fald på 2^{den} plads, ... fra χ_n i hvert fald på n^{te} plads,

For en vilkårlig mængde M var det som nævnt vor opgave at vise, at M ikke er ækvipotent med mængden X_M af funktioner $\chi: M \rightarrow \{0,1\}$. Dette indses derved, at ingen afbildning af M ind i X_M er surjektiv. Betegner vi nemlig for en vilkårlig afbildning

$f:M \rightarrow X_M$ den til elementet $a \in M$ ved f svarende funktion fra X_M med χ_a , vil der ved

$$x \mapsto 1 - \chi_x(x), \quad x \in M,$$

bestemmes en funktion $\chi:M \rightarrow \{0,1\}$. Denne funktion $\chi \in X_M$ svarer ikke ved f til noget element i M : χ er forskellig fra hver af funktionerne χ_a , thi funktionsværdierne for elementet a er henholdsvis $\chi(a) = 1 - \chi_a(a)$ og $\chi_a(a)$. - Hermed er bevist fuldført.

Da mængden af delmængder af en endelig mængde med kardinaltallet $n \in \mathbb{N}_0$ har kardinaltallet 2^n , siger sætningen i dette tilfælde, at $2^n \neq n$ for $n \in \mathbb{N}_0$. Det specialtilfælde af sætningen, hvor beviset blev gennemført særskilt, fremhæves som særlig betydningsfuldt:

Mængden af delmængder af mængden $\mathbb{N}$ af naturlige tal er ikke numerabel.

Faktisk viste vi det hermed ensbetydende: mængden $X_{\mathbb{N}}$ af funktioner $\chi:\mathbb{N} \rightarrow \{0,1\}$, dvs. af talfølger, hvis elementer er 0 eller 1, er ikke numerabel. Lader man nu til hver sådan følge $\chi = (a_1, a_2, \dots)$ svare den uendelige decimalbrøk $0,a_1a_2\dots$, fås en bijektiv afbildning af $X_{\mathbb{N}}$ på mængden af de reelle tal i intervallet $[0,1[$, som har en decimalbrøkuudvikling, hvori kun cifrene 0 og 1 forekommer. Mængden af disse reelle tal er altså ikke numerabel. Da en numerabel mængdes delmængder er højst numerable, følger heraf:

Mængden $\mathbb{R}$ af reelle tal er ikke numerabel.

Idet der findes ikke ækvipotente uendelige mængder, ligger det nær at søge kardinaltalbegrebet udvidet, således at også uendelige mængder tilskrives kardinaltal.

Hvert endeligt kardinaltal n hører som omtalt nøje sammen med en "standardmængde", hvis kardinaltal netop er n , nemlig mængden $\{1, 2, \dots, n\}$. Det har vist sig muligt at udvide forrådet af "standardmængder" på en sådan måde, at der for enhver mængde A findes netop én "standardmængde" ækvipotent med A . Hver "standardmængde" opfattes så som repræsenterende sit kardinaltal. Eksempelvis er $\mathbb{N} = \{1, 2, \dots\}$ den simpleste uendelige standardmængde; kardinaltallet betegnes $\aleph_0$ (alef nul). At en mængde har et vist kardinaltal betyder nu blot, at den er ækvipotent med den pågældende standardmængde. At en mængde A er numerabel, altså ækvipotent med $\{1, 2, \dots\}$, kan således udtrykkes: A har kardinaltallet $\aleph_0$; man skriver

$$\text{kt } A = \aleph_0.$$

Det skal nævnes, at man ikke har betegnelser til alle kardinaltal (der er "for mange").

Af det sagte fremgår umiddelbart:

To mængder er ækvipotente, hvis og kun hvis de har samme kardinaltal.

Det er muligt at sammenligne også de uendelige kardinaltal efter størrelse.

Definition: For to kardinaltal α og β fastsættes $\alpha \leq \beta$, hvis der findes en injektiv afbildning af den til α svarende standardmængde S_α ind i den til β svarende standardmængde S_β .

Eksempel: $7 \leq \aleph_0$, thi den identiske afbildning af $\{1, 2, \dots, 7\}$ kan opfattes som en injektiv afbildning ind i $\{1, 2, \dots, 7, \dots\}$.

Lad A og B være vilkårlige (ikke tomme) mængder med kardinaltal α og β . Da gælder $\alpha \leq \beta$, hvis og kun hvis der findes en injektiv afbildning af A ind i B , - med andre ord: hvis og kun hvis A er ækvipotent med en delmængde af B .

Thi lad $f:A \rightarrow S_\alpha$ og $g:B \rightarrow S_\beta$ være bijektive afbildninger. For en injektiv afbildning $\varphi:A \rightarrow B$ vil da $g \circ \varphi \circ f^{-1}:S_\alpha \rightarrow S_\beta$ være injektiv, ligesom for en injektiv afbildning $\psi:S_\alpha \rightarrow S_\beta$ også $g^{-1} \circ \psi \circ f:A \rightarrow B$ er injektiv.

Ganske som for endelige ses, at sætningen har et modstykke:
 $\alpha \leq \beta$, netop hvis der findes en surjektiv afbildning af B på A .

For at undgå paradokser må man afstå fra at regne samlingen af alle kardinaltal for en mængde. Dette forhindrer dog ikke, at man omtaler $\alpha \leq \beta$ som en relation. Ved betegnelsen har vi allerede forudgrebet, at det er en reflektiv ordningsrelation. Hertil må eftervises gyldigheden af

1. $\alpha \leq \alpha$,
2. $\alpha \leq \beta \wedge \beta \leq \alpha \Rightarrow \alpha = \beta$,
3. $\alpha \leq \beta \wedge \beta \leq \gamma \Rightarrow \alpha \leq \gamma$.

1. er umiddelbar; den identiske afbildning $e_{S_\alpha}:S_\alpha \rightarrow S_\alpha$ er injektiv. Også 3. er klar; er $f:S_\alpha \rightarrow S_\beta$ og $g:S_\beta \rightarrow S_\gamma$ injektive afbildninger, så er også $g \circ f:S_\alpha \rightarrow S_\gamma$ injektiv. At relationen er asymmetrisk, altså at 2. gælder, er indholdet af F. Bernsteins ækvivalenssætning:

To mængder, hvor hver er ækvipotent med en delmængde af den anden, er ækvipotente.

Beviset er ikke helt simpelt (jfr. øv. 17) og vil ikke blive gennemgået her.

Endnu står tilbage spørgsmålet, om det er muligt at "sammenligne størrelsen" af vilkårlig to kardinaltal α og β , altså om der gælder

4. $\alpha \leq \beta \vee \beta \leq \alpha$.

At dette virkelig er tilfældet, dvs. at ordningen er total, er indholdet af sætningen:

Er A og B vilkårlige mængder, vil A være ækvipotent med en delmængde af B eller B ækvipotent med en delmængde af A.

Dette ville føre alt for vidt her at gå nærmere ind på beviset. Vi skal blot nævne, at det afgørende punkt er velordnings-sætningen: Enhver mængde kan velordnes (E. Zermelo, 1904).

Af det foregående kan drages nogle konsekvenser vedrørende specielle kardinaltal. Da enhver uendelig mængde har numerable delmængder, er $\aleph_0$ det mindste uendelige kardinaltal. Idet man med $\aleph$ betegner kardinaltallet for mængden $\mathbb{R}$ af reelle tal, er specielt $\aleph_0 \leq \aleph$, og da $\aleph_0 \neq \aleph$, kan man skrive $\aleph_0 < \aleph$. Det er et endnu uløst problem, det såkaldte kontinuumsproblem, om der findes kardinaltal imellem de to, altså om enhver uendelig delmængde af $\mathbb{R}$ er numerabel eller af "kontinuets mægtighed", dvs. ækvipotent med $\mathbb{R}$.

Vi afslutter denne indledning i læren om uendelige mængder med nogle vigtige resultater om specielle mængder og deres kardinaltal.

Som allerede fundet, er mængden $\mathbb{R}$ af reelle tal ikke numerabel. For denne vigtige sætning vil vi give endnu et bevis, meget anskueligt og direkte; beviset skyldes Cantor. Lad $(r_1, r_2, \dots)$ være en følge af indbyrdes forskellige reelle tal. Det drejer sig om at vise, at den ikke kan indeholde alle reelle tal. Lad $[a_1, b_1]$, hvor $a_1 < b_1$, være et afsluttet interval, som ikke indeholder r_1 . Der findes da et interval $[a_2, b_2] \subseteq [a_1, b_1]$, hvor $a_2 < b_2$, som ikke indeholder r_2 . Dette interval har et delinterval $[a_3, b_3]$, hvor

$a_3 < b_3$, som ikke indeholder r_3 . Fortsættes på denne måde fås en følge af intervaller $[a_i, b_i]$, $i = 1, 2, \dots$, der hvert er indeholdt i det foregående. Der findes mindst eet reelt tal r , som er indeholdt i alle disse intervaller, nemlig $r = \sup a_i$. Dette tal kan ikke forekomme i den givne følge, da jo hvert r_i ligger uden for mindst eet af intervallerne, nemlig $[a_i, b_i]$.

Et åbent interval $]a, b[\subseteq \mathbb{R}$, $a < b$, er ækvipotent med $\mathbb{R}$ selv, idet funktionen $x \rightarrow \operatorname{tg}\left(\frac{2x-a-b}{2b-2a}\pi\right)$ afbilder det bijektivt på $\mathbb{R}$. Det samme gælder for halvåbne og afsluttede intervaller, hvilket kan sluttes direkte (jfr. øv.8) eller ved hjælp af ækvivalenssætningen. Heraf fås endvidere, at hvis $J \subseteq \mathbb{R}$ er et vilkårligt interval (som ikke kun består af eet punkt), gælder $J \times J \sim \mathbb{R} \times \mathbb{R}$; thi er $\varphi: J \rightarrow \mathbb{R}$ bijektiv, bestemmes der ved $(x, y) \rightarrow (\varphi(x), \varphi(y))$ en bijektiv afbildning af $J \times J$ på $\mathbb{R} \times \mathbb{R}$.

Der gælder endvidere $\mathbb{R} \times \mathbb{R} \sim \mathbb{R}$. Ifølge det sagte er det tilstrækkeligt at bevise $J \times J \sim J$ for et interval J . Lad J være det halvåbne interval $]0, 1[$. Hvert tal i dette interval har en og kun een fremstilling som uendelig decimalbrøk, som ikke ender med lutter nuller. Lad $x = 0, x_1 x_2 \dots$ være denne decimalbrøkfremstilling af et tal x i intervallet, hvor dog $x_1, x_2, \dots$ i almindelighed ikke skal betegne de enkelte cifre, men sæt af på hinanden følgende: x_1 består af de første decimaler til og med den første, der er forskellig fra 0; x_2 består af de derpå følgende decimaler til og med den første, der er forskellig fra 0, o.s.v. (Hvis alle decimaler er forskellige fra 0, betegner altså $x_1, x_2, \dots$ de enkelte cifre.) Er også $y = 0, y_1 y_2 \dots \in J$, hvor $y_1, y_2, \dots$ har den tilsvarende betydning, kan man til parret $(x, y) \in J \times J$ lade svare tallet $z \in J$ med decimalbrøkfremstillingen $z = 0, x_1 y_1 x_2 y_2 \dots$. Derved fås en bijektiv afbildning af $J \times J$ på J . (Lader man $x_1, x_2, \dots$ betegne de enkelte cifre, får

man på denne måde en injektiv, men ikke surjektiv afbildning, idet f.eks. decimalbrøker, hvor hvert andet ciffer er 0, ikke kan fås ved den angivne "blanding".)

Ved hjælp af et koordinatsystem sluttes af det fundne resultat, at mængderne E_1 , E_2 og E_3 af punkter på en linie, i en plan og i rummet alle er ækvipotente med $\mathbb{R}$.

Endelig nævnes, at mængden $F(J)$ af alle i et interval J definerede reelle funktioner har et kardinaltal større end $\mathbb{R}$. Mængden $F(J)$ har nemlig som delmængde mængden X_J af alle i J definerede funktioner, som kun antager værdierne 0 og 1, og om denne mængde, der er ækvipotent med $\mathcal{P}(J)$, blev det vist, at den ikke er ækvipotent med $J \sim \mathbb{R}$. På den anden side er det klart, at $\text{kt } \mathbb{R} \leq \text{kt } \mathcal{P}(J)$, idet $\mathcal{P}(J)$ har den med $J \sim \mathbb{R}$ ækvipotente delmængde bestående af de delmængder af J , som hver kun indeholder eet tal fra J . Der gælder altså

$$\text{kt } \mathbb{R} = \text{kt } J < \text{kt } \mathcal{P}(J) \leq \text{kt } F(J).$$

Man kan vise, at $\text{kt } \mathcal{P}(J) = \text{kt } F(J)$. Det er værd at bemærke, at mængden $C(J)$ af i J kontinuerte funktioner er ækvipotent med $\mathbb{R}$ (se øv.15).

Øvelser til kap. I, § 8.

1. Den hele del c_0 og cifrene $c_1, c_2, \dots$ i decimalbrøkd udviklingen for en brøk p/q , $p, q \in \mathbb{N}$, bestemmes successivt som kvotienter ved division med rest efter følgende skema:

$$\begin{array}{ll} p = c_0 q + r_1, & 0 \leq r_1 < q, \\ 10r_1 = c_1 q + r_2, & 0 \leq r_2 < q, \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \\ 10r_n = c_n q + r_{n+1}, & 0 \leq r_{n+1} < q, \\ \cdot & \cdot \\ \cdot & \cdot \\ \cdot & \cdot \end{array}$$

Hvis decimalbrøkd udviklingen ikke er endelig, har den en periode bestående af højst $q - 1$ cifre. Hvorfor?

2. Lad α være et irrationalt tal. Vis, at der for hvert tal $n \in \mathbb{N}$ findes tal $p \in \mathbb{Z}$ og $q \in \{1, 2, \dots, n\}$, således at

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{qn} \leq \frac{1}{q^2}.$$

(Inddel intervallet $[0, 1]$ i n lige store delintervaller, betragt tallene $k\alpha - [k\alpha]$, $k = 0, 1, \dots, n$, og anvend skuffeprincippet. For $x \in \mathbb{R}$ betegner $[x]$ det største hele tal, som er mindre end eller lig med x .)

- 3*. Der er givet tallene $a, b \in \mathbb{Z}$ og $m \in \mathbb{N}$. Vis, at der findes mindst et par $(x, y) \neq (0, 0)$ af hele tal, således at

$$|x| \leq \sqrt{m}, \quad |y| \leq \sqrt{m} \text{ og}$$

$$ax + by \equiv 0 \pmod{m}.$$

(Jfr. I, 7, øv. 7.)

4. Vis, at enhver uendelig mængde af parvis disjunkte åbne intervaller i $\mathbb{R}$ er numerabel.

Vis, at enhver uendelig mængde af parvis disjunkte cirkelskiver i en plan er numerabel.

5. I en plan tænkes valgt et sædvanligt retvinklet koordinat-system. Vis, at mængden af alle rette linier, som hver går gennem to forskellige punkter med rationale koordinater, er numerabel.
6. Vis, at hvis A er en endelig delmængde af en uendelig mængde B , så gælder $B \setminus A \sim B$.
7. Vis, at hvis A er en højst numerabel mængde og B en vilkårlig uendelig mængde, så er $A \cup B \sim B$.
8. Vis, at de følgende mængder af reelle tal er indbyrdes ækvipotente: $\{x \mid 0 \leq x \leq 1\}$, $\{x \mid 0 \leq x < 1\}$, $\{x \mid 0 < x < 1\}$, $\{x \mid x > 0\}$, $\{x \mid x^2 > 1\}$. (Benyt f.eks. øv. 6 eller 7.)
9. Er mængden af alle endelige delmængder af en numerabel mængde numerabel?
10. Er mængden af alle følger af naturlige tal, altså mængden $\mathbb{N}^{\mathbb{N}}$ numerabel?
- 11*. Vis, at mængden af alle polynomier med heltallige koefficienter er numerabel.

Et reelt eller komplekst tal, som er rod i et polynomium med heltallige koefficienter, der ikke alle er 0, kaldes et algebraisk tal. De øvrige tal kaldes transcendente tal. Vis, at mængden af algebraiske tal er numerabel, og at mængden af transcendentale tal er ikke numerabel.
12. Vis, at mængden af alle cirkler i en plan er ækvipotent med $\mathbb{R}$.

13. Vis, at ved en vilkårlig deling af $\mathbb{R}$ i to klasser vil mindst én af disse have kardinaltallet $\aleph_1$. (Benyt $\mathbb{R} \sim \mathbb{R} \times \mathbb{R}$).
- 14*. Vis, at mængden $\mathcal{P}(\mathbb{N})$ af alle delmængder af $\mathbb{N}$ er ækvipotent med $\mathbb{R}$. (Benyt f.eks. udviklingen af de reelle tal mellem 0 og 1 i "dualbrøker".)
- 15*. Vis, at mængden $\mathbb{R}^{\mathbb{N}}$ af alle reelle talfølger er ækvipotent med $\mathbb{R}$. (Vis først $\mathbb{R}^{\mathbb{N}} \sim J^{\mathbb{N}}$, hvor $J =]0,1[$; og bestem derpå ved brug af decimalbrøkfremstillinger for tal i J (sml. s. 13) en bijektiv afbildning af $J^{\mathbb{N}}$ på J .)
- 16*. Vis, at mængden af reelle kontinuerte funktioner i et interval, f.eks. $[0,1]$, er ækvipotent med $\mathbb{R}$. (Benyt, at en i et interval kontinuert funktion er fuldstændig bestemt ved sin restriktion til mængden af rationale tal i intervallet, samt ækvivalenssætningen.)
- 17*. Gennemfør beviserne for påstandene i den følgende beskrivelse af et bevis for Bernsteins ækvivalenssætning: Om to mængder A og B forudsættes, at hver af dem er ækvipotent med en delmængde af den anden, altså at der findes injektive afbildninger $f:A \rightarrow B$ og $g:B \rightarrow A$. Det skal vises, at der eksisterer en bijektiv afbildning $h:A \rightarrow B$.
For delmængden Q af A defineret ved

$$Q = \bigcup_{n=0}^{\infty} (g \circ f)^n (A \setminus g(B))$$

gælder $A \setminus Q \subseteq g(B)$. Dette gør det muligt at definere en afbildning $h:A \rightarrow B$ ved

$$h(a) = \begin{cases} f(a) & \text{for } a \in Q, \\ g^{-1}(a) & \text{for } a \in A \setminus Q. \end{cases}$$

Denne afbildning h er injektiv, fordi man af $f(a_1) =$

$g^{-1}(a_2)$, $a_1 \in Q$ og $a_2 \in g(B)$ kan slutte, at $a_2 \in Q$. Den er også surjektiv, fordi man af $b \in B \setminus f(Q)$ kan slutte, $a = g(b) \in A \setminus Q$.

Kap. II. Algebraens grundbegreber.§ 1. Kompositioner.Begrebet komposition.

En afbildning, hvis definitionsmængde (eller definitionsklasse) er et cartesisk produkt $K \times L$, kaldes også en komposition. I algebraen, som er læren om kompositioner, betegnes disse i reglen med tegn som $+$, $\cdot$, $\circ$, $\dots$. Er $*$ en komposition defineret på $K \times L$, skrives i stedet for $*(x,y)$ oftest $x * y$ som betegnelse for det til et ordnet par $(x,y) \in K \times L$ svarende objekt.

En komposition $*: K \times L \rightarrow M$ er således en tilordning, hvorved til hvert ordnet par (x,y) af et $x \in K$ og et $y \in L$ svarer et bestemt element af M ; dette betegnes $x * y$. En komposition $*: M \times M \rightarrow M$, altså en komposition $*$ med definitionsmængde $M \times M$, for hvilken

$$\forall_{M} x, y: x * y \in M,$$

kaldes en komposition inden for M .

Eksempler.

1° Sædvanlig addition og multiplikation af tal

$$(x,y) \rightarrow x + y \quad \text{og} \quad (x,y) \rightarrow xy$$

er, når vi tager $\mathbb{R} \times \mathbb{R}$ som definitionsmængde, kompositioner inden for $\mathbb{R}$. Det samme gælder subtraktion

$$(x,y) \rightarrow x - y.$$

Restriktionen til $\mathbb{N} \times \mathbb{N}$ af de to førstnævnte kompositioner, dvs. addition og multiplikation af naturlige tal, er kompositioner

inden for $\hat{N}$, medens restriktionen af sidstnævnte er en komposition $\hat{N} \times \hat{N} \rightarrow \hat{Z}$.

Regneoperationerne $(x,y) \rightarrow x/y$ og $(x,y) \rightarrow x^y$ er kompositioner, når vi tager $\hat{R} \times (\hat{R} \setminus \{0\})$, henholdsvis $\hat{R}_+ \times \hat{R}$ som definitionsområde.

2° I elementær vektorregning behandles 4 kompositioner:

Addition af vektorer er en komposition inden for mængden V_3 af vektorer i rummet; til hvert par af vektorer $\underline{u}$ og $\underline{v}$ svarer en vektor betegnet $\underline{u} + \underline{v}$.

Multiplikation af vektorer med tal er en komposition $\hat{R} \times V_3 \rightarrow V_3$; til hvert par af et reelt tal a og en vektor $\underline{v}$ svarer en vektor betegnet $a\underline{v}$.

Skalarprodukt af vektorer er en komposition $V_3 \times V_3 \rightarrow \hat{R}$; til hvert par af vektorer $\underline{u}$ og $\underline{v}$ svarer et tal betegnet $\underline{u} \cdot \underline{v}$.

Vektorproduktet er en komposition inden for V_3 ; til hvert par af vektorer $\underline{u}$ og $\underline{v}$ svarer en vektor $\underline{u} \times \underline{v}$.

3° Tre kompositioner inden for klassen V af alle mængder er

$$(A,B) \rightarrow A \cap B, \quad (A,B) \rightarrow A \cup B \quad \text{og} \quad (A,B) \rightarrow A \setminus B.$$

Tages for A og B kun delmængder af en (universal)mængde E i betragtning, fås kompositioner inden for mængden $\hat{D}(E)$ af delmængder i E ; disse kompositioner er behandlet i I, §2.

4° Sammensætning af afbildninger,

$$(g,f) \rightarrow g \circ f,$$

er, når man for f tager i betragtning afbildninger $f: A \rightarrow B$ af en mængde A ind i en mængde B og for g afbildninger $g: B \rightarrow C$ af B ind i en mængde C , en komposition $\hat{F}(B \rightarrow C) \times \hat{F}(A \rightarrow B) \rightarrow \hat{F}(A \rightarrow C)$.

Specielt er sammensætning $(g,f) \rightarrow g \circ f$ en komposition inden for mængden $\hat{F}(A \rightarrow A)$ af afbildninger af en mængde A ind i sig selv.

Er K og L endelige mængder, kan en komposition $*$ defineret på $K \times L$ angives ved en kompositionstavle, dvs. en tabel med dobbelt indgang:

			y
x			$x*y$

Elementerne i K anføres ud for tavlens rækker; elementerne i L over kolonnerne, og for hvert $(x,y) \in K \times L$ angives det tilordnede objekt $x * y$ på den fælles plads for rækken ud for x og søjlen under y .

Alle skolebørn stifter bekendtskab med en sådan tavle, nemlig kompositionstavlen for restriktionen af sædvanlig multiplikation til $\{0,1,\dots,9\} \times \{0,1,\dots,9\}$, den "lille tabel".

Som et yderligere eksempel betragtes sammensætning af permutationer af mængden $\{1,2,3\}$. Idet vi benytter betegnelserne

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad p_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$p_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad p_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad p_6 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

angives den nævnte komposition fuldstændigt ved tavlen

	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_3	p_1	p_6	p_4	p_5
p_3	p_3	p_1	p_2	p_5	p_6	p_4
p_4	p_4	p_5	p_6	p_1	p_2	p_3
p_5	p_5	p_6	p_4	p_3	p_1	p_2
p_6	p_6	p_4	p_5	p_2	p_3	p_1

Det er naturligvis uvæsentligt, at permutationerne er nævnt i samme rækkefølge i tavlens to indgange.

Af tavlen fremgår bl.a., at sammensætning er en komposition inden for mængden $\{p_1, p_2, p_3, p_4, p_5, p_6\}$, såvel som inden for hver af mængderne $\{p_1, p_2, p_3\}$, $\{p_1, p_4\}$, $\{p_1, p_5\}$ og $\{p_1, p_6\}$.

Komposition inden for en mængde.

Lad M være en mængde og $*$ en komposition inden for M .

Som betegnelse for M betragtet med kompositionen $*$ eller, som man siger, for mængden M organiseret ved kompositionen $*$, benyttes $(M, *)$.

Kompositionen $*$ siges at være associativ, hvis der for $x \in M$, $y \in M$, $z \in M$ gælder

$$(x * y) * z = x * (y * z).$$

Dette udtrykkes også: for $(M, *)$ gælder den associative lov. Vi bemærker, at når kravet tager sig så simpelt ud, beror det på

algebraens særlige skrivemåde; kaldes kompositionen f og benyttes de for afbildninger gængse betegnelser, er betingelsen

$$f(f(x,y),z) = f(x,f(y,z)).$$

Et udtryk som $x_1 * x_2 * \dots * x_n$, hvor $x_1, x_2, \dots, x_n \in M$, har ikke i sig nogen mening når $n > 2$, men kan få det, om man på passende måde anbringer parenteser. Er $*$ associativ, kan man nu, ved et induktionsbevis som vi vil forbigå, godtgøre, at

$$x_1 * x_2 * \dots * x_n$$

får samme værdi, hvorledes man end sætter fornødne parenteser; vi kan da tillade os helt at udelade dem, ligesom vi kan hæve og sætte parenteser efter behag.

Kompositionen $*$ siges at være kommutativ, hvis der for $x \in M$, $y \in M$ gælder

$$x * y = y * x.$$

Dette udtrykkes også: for $(M,*)$ gælder den kommutative lov.

Er $*$ både associativ og kommutativ, vil, som man kender det fra sædvanlig addition eller multiplikation af tal, udtryk som

$$x_1 * x_2 * \dots * x_n,$$

hvor $x_1, x_2, \dots, x_n \in M$, ikke blot have mening, men yderligere vil rækkefølgen af elementerne være ligegyldig.

Et element $e \in M$ siges at være neutralt ved kompositionen $*$, hvis

$$\forall_M x [e * x = x * e = x].$$

Dette udtrykkes også: e er neutralt element i $(M,*)$.

Der findes højst ét element af M , som er neutralt ved kompositionen $*$. Her er $*$ en ganske vilkårlig komposition inden for en mængde M .

Thi antages $e \in M$ og $e' \in M$ neutrale ved $*$, haves dels $e * e' = e'$, da e er neutralt, dels $e * e' = e$, da e' er neutralt, og dermed $e = e'$.

Vi forudsætter nu, at der findes et, og dermed netop ét, element $e \in M$, som er neutralt ved kompositionen $*$.

Et element $x' \in M$ siges da at være et inverst til elementet $x \in M$ ved kompositionen $*$, hvis

$$x * x' = x' * x = e.$$

Da der åbenbart er tale om en symmetrisk relation, benytter man også vendingen: x og x' er inverse ved $*$.

Et element $x \in M$ siges at være regulært eller invertibelt ved kompositionen $*$, hvis det har et inverst, dvs. hvis

$$\exists_M x' [x * x' = x' * x = e].$$

Det kan forekomme, at et element har flere inverse (se det følgende eksempel 5°), dog aldrig når kompositionen er associativ:

Findes der et neutralt element e ved en associativ komposition $*$ inden for en mængde M , da har hvert element $x \in M$ højst ét inverst.

Thi af

$$(x' * x) * x'' = x' * (x * x'')$$

fås, når x' og x'' begge antages at være inverse til x ,

$$e * x'' = x' * e$$

og dermed

$$x'' = x'.$$

Vedrørende en associativ komposition $*$ inden for en mængde M med neutralt element e vil vi endnu notere følgende:

Er a regulært, da gælder for $x \in M$, $y \in M$

$$a * x = a * y \Rightarrow x = y$$

og ligeledes

$$x * a = y * a \Rightarrow x = y.$$

Dette udtrykkes kort: et regulært element kan bortforkortes.

Af $a * x = a * y$ fås nemlig, idet vi med a' betegner det til a inverse element,

$$a' * (a * x) = a' * (a * y)$$

og dermed
$$(a' * a) * x = (a' * a) * y,$$

dvs.
$$e * x = e * y,$$

altså
$$x = y.$$

Den anden forkortningsregel eftervises på tilsvarende måde.

Vi bemærker, at resultatet også kan formuleres: for et regulært element $a \in M$ og vilkårligt $b \in M$ findes højst et $x \in M$, således at $a * x = b$, og ligeledes højst et $x \in M$, så $x * a = b$, eller, som man gerne udtrykker det, hver af ligningerne $a * x = b$ og $x * a = b$ har højst én løsning.

Idet man af $a * x = b$ slutter $a' * (a * x) = a' * b$, dvs. $x = a' * b$, ses endvidere, at elementet $a' * b$ er den eneste mulige løsning til ligningen $a * x = b$. En prøve viser, at det virkelig er en løsning:

$$a * (a' * b) = (a * a') * b = e * b = b.$$

Ligningen $x * a = b$ behandles ganske tilsvarende. Vi noterer:

Er a regulært med inverst element a' ved den associative komposition $*$ og b vilkårligt, da har hver af ligningerne

$$a * x = b \quad \text{og} \quad x * a = b$$

netop én løsning, nemlig henholdsvis $a' * b$ og $b * a'$.

En komposition $*$ inden for en mængde M siges at være en gruppekomposition, og $(M, *)$ kaldes en gruppe, hvis $*$ er asso-

ciativ, der findes et neutralt element $e \in M$, og hvert element af M er regulært.

I en gruppe findes kun ét neutralt element, hvert element har netop ét inverst, og de ovenfor noterede resultater om forkortning og om løsning af ligninger kan naturligvis anvendes på vilkårlige elementer a og b i gruppen. I §2 vil vi gå nøjere ind på gruppernes teori.

En gruppe $(M, *)$, hvor kompositionen $*$ er kommutativ, kaldes en kommutativ eller Abelsk gruppe.

Eksempler.

1° $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$ og $(\mathbb{Z}, +)$ er kommutative grupper, 0 er det neutrale element, og det inverse til et tal x er $-x$.

For $(\mathbb{N}, +)$ gælder den associative og den kommutative lov, der er intet neutralt element, men ethvert element kan bortforkortes:

$$a + x = a + y \Rightarrow x = y.$$

For $(\mathbb{R}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{Z}, \cdot)$ og $(\mathbb{N}, \cdot)$ gælder den associative og den kommutative lov, og 1 er neutralt element. I $(\mathbb{R}, \cdot)$ og $(\mathbb{Q}, \cdot)$ er ethvert tal $x \neq 0$ regulært med det inverse x^{-1} , i $(\mathbb{Z}, \cdot)$ er der ikke andre regulære elementer end 1 og -1 , i $(\mathbb{N}, \cdot)$ ikke andre end 1, men i alle tilfælde kan et tal $\neq 0$ bortforkortes:

$$a \neq 0 \wedge ax = ay \Rightarrow x = y.$$

$(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R}_+, \cdot)$ og $(\mathbb{Q}_+, \cdot)$ er kommutative grupper.

2° Mængden V_3 af geometriske vektorer er med vektoraddition en kommutativ gruppe, nulvektoren $\underline{0}$ er det neutrale element, og det inverse element til en vektor $\underline{x}$ er den modsatte vektor $-\underline{x}$.

Vektorproduktet er hverken associativt eller kommutativt, der er intet neutralt element, og en ligning $\underline{a} \times \underline{x} = \underline{b}$ har enten ingen eller uendelig mange løsninger (jfr. III,2,6), tilsvarende gælder ligninger $\underline{x} \times \underline{a} = \underline{b}$.

3° Kompositionerne $\cap$ og $\cup$ er associative og kommutative, den tomme mængde $\emptyset$ er neutral ved $\cup$, og betragtes kompositionerne inden for mængden $\mathcal{D}(E)$ af delmængder i en mængde E , er E neutral ved $\cap$; ingen fra E forskellig delmængde er regulær ved $\cap$, ligesom kun $\emptyset$ er regulær ved $\cup$.

4° Sættelse af afbildninger af en mængde A ind i sig selv er en associativ, men, når A har mindst to elementer, ikke kommutativ komposition inden for $\hat{F}(A \rightarrow A)$. Den identiske afbildning e_A er neutral, medens de bijektive afbildninger er de regulære elementer med de inverse afbildninger som inverse elementer.

Inden for mængden af bijektive afbildninger af A på sig selv, også kaldet transformationer af A , er sættelse en gruppekomposition, som, når A har mindst tre elementer, ikke er kommutativ (betragt kompositionstavlen side 4).

5° Som eksempel på en komposition, der er kommutativ, men ikke associativ, kan nævnes

$$(x,y) \rightarrow (x + y)/2, \quad x,y \in \mathbb{R},$$

samt kompositionen

$$(x,y) \rightarrow (x^3 - x^2y - xy^2 + y^3)^{1/3}, \quad x,y \in \mathbb{R},$$

hvor 0 er neutralt element, og både a og $-a$ er inverse til a .

Er en komposition $*$ inden for en endelig mængde M givet ved en kompositionstavle, vil kommutativitet ytre sig ved, at tavlen er symmetrisk om "hoveddiagonalen", forudsat elementerne i M er nævnt i samme rækkefølge i tavlens to indgange. Associativitet giver sig ikke til kende på en tilsvarende overskuelig måde. Et neutralt element udmærker sig ved, at den tilsvarende række og søjle er identisk med hver ^{sin} af tavlens indgange; er et neutralt element fundet, er det let at overse, om to elementer er inverse; eksempelvis fremgår af tavlen side 4, at p_1 er neutralt, p_2 og p_3 inverse, og hvert af p_1 , p_4 , p_5 og p_6 inverst til sig selv. At hvert element af M forekommer netop én gang i rækken ud for et givet $a \in M$, er ensbetydende med, at ligningen $a * x = b$ for hvert $b \in M$ har netop én løsning, og ligeledes ensbetydende med, at forkortningsreglen

$$\forall_{M,x,y} [a * x = a * y \Rightarrow x = y]$$

gælder for det givne a . Tilsvarende gælder naturligvis det tilfælde, at elementerne forekommer hvert én gang i en søjle.

En kompositionstavle for en gruppekomposition kaldes også en gruppetavle.

Betegnes en komposition inden for en mængde med $\cdot$, skrives for det eventuelle neutrale element gerne e eller 1 . Vi vil næsten udelukkende betragte associative kompositioner; entydighed af inverst element er da sikret; ved multiplikativ skrivemåde, og ofte ellers, benyttes betegnelsen x^{-1} .

Betegnelsen $+$ forbeholdes gerne kompositioner, hvor foruden den associative også den kommutative lov gælder. Her skrives o eller 0 for neutralt element, $-x$ for inverst, eller som man ved denne skrivemåde ofte siger, modsat element.

Isomorfi.

Lad $*$ være en komposition inden for en mængde L og $\S$ en komposition inden for en mængde M .

En enentydig korrespondance mellem L og M siges da at være en isomorfi mellem mængden L betragtet med kompositionen $*$ og mængden M betragtet med kompositionen $\S$, altså mellem $(L, *)$ og $(M, \S)$, hvis der for $x_1, x_2 \in L$ og $y_1, y_2 \in M$ gælder

$$x_1 \leftrightarrow y_1 \wedge x_2 \leftrightarrow y_2 \Rightarrow x_1 * x_2 \leftrightarrow y_1 \S y_2.$$

Udtrykt i ord er betingelsen, at anvendelse af de to kompositioner $*$ og $\S$ på korresponderende elementer igen giver korresponderende elementer. Dette medfører naturligvis en fuldstændig parallelitet mellem alle regninger i $(L, *)$ og $(M, \S)$.

Findes der en isomorfi mellem $(L, *)$ og $(M, \S)$, siges de to organiserede mængder at være isomorfe.

I så fald haves, at gælder den associative eller kommutative lov for den ene, så også for den anden af de to kompositioner. Findes et neutralt element ved den ene komposition, så også et ved den anden; ved enhver isomorfi mellem $(L, *)$ og $(M, \S)$ vil da det ved $*$ neutrale element af L og det ved $\S$ neutrale element af M korrespondere, ligesom der til to inverse elementer ved den ene komposition vil svare to inverse ved den anden, til regulært element vil svare regulært element. Er en af de isomorfe, organiserede mængder $(L, *)$ og $(M, \S)$ en gruppe, så er den anden det også.

Disse påstande verificeres umiddelbart. Antages eksempelvis $*$ associativ, fås

$$(y_1 \S y_2) \S y_3 = y_1 \S (y_2 \S y_3)$$

for vilkårlige $y_1, y_2, y_3 \in M$, idet man betragter de korresponde-

rende $x_1, x_2, x_3 \in L$ ved en isomorfi mellem $(L, *)$ og $(M, \S)$ og benytter dels

$$(x_1 * x_2) * x_3 \leftrightarrow (y_1 \S y_2) \S y_3,$$

$$x_1 * (x_2 * x_3) \leftrightarrow y_1 \S (y_2 \S y_3),$$

dels
$$(x_1 * x_2) * x_3 = x_1 * (x_2 * x_3).$$

At den ved en bijektiv afbildning $f: L \rightarrow M$ bestemte enentydige korrespondance mellem L og M er en isomorfi mellem $(L, *)$ og $(M, \S)$, er ensbetydende med, at der for $x_1, x_2 \in L$ gælder

$$f(x_1 * x_2) = f(x_1) \S f(x_2).$$

Thi dette er blot et forenklet udtryk for, at der for $x_1, x_2 \in L$, $y_1, y_2 \in M$ gælder

$$f(x_1) = y_1 \wedge f(x_2) = y_2 \Rightarrow f(x_1 * x_2) = y_1 \S y_2,$$

$$\text{dvs. } x_1 \leftrightarrow y_1 \wedge x_2 \leftrightarrow y_2 \Rightarrow x_1 * x_2 \leftrightarrow y_1 \S y_2.$$

En bijektiv afbildning $f: L \rightarrow M$, hvor for $x_1, x_2 \in L$ gælder

$$f(x_1 * x_2) = f(x_1) \S f(x_2),$$

kaldes en isomorf afbildning af $(L, *)$ på $(M, \S)$. Af ovenstående bemærkning fremgår, at det kommer ud på et at betragte isomorfier mellem $(L, *)$ og $(M, \S)$ eller isomorfe afbildninger af $(L, *)$ på $(M, \S)$. Specielt kan man som definition på, at $(L, *)$ er isomorf med $(M, \S)$, benytte, at der findes en isomorf afbildning af $(L, *)$ på $(M, \S)$.

I betingelsen for, at en enentydig korrespondance mellem L og M er en isomorfi mellem $(L, *)$ og $(M, \S)$, indgår de to organiserede mængder tydeligvis på ensartet måde. Er f en isomorf afbildning af $(L, *)$ på $(M, \S)$, vil derfor den omvendte afbildning f^{-1} være en isomorf afbildning af $(M, \S)$ på $(L, *)$.

Også sammensætning af isomorfe afbildninger fører igen til en isomorf afbildning: Er $f: L \rightarrow M$ og $g: M \rightarrow N$ isomorfe afbildninger af $(L,*)$ på $(M,\S)$, henholdsvis $(M,\S)$ på (N,Δ) , hvor $*$, $\S$ og Δ er kompositioner inden for mængderne L , M og N , da vil den sammensatte afbildning $g \circ f$ være en isomorf afbildning af $(L,*)$ på (N,Δ) . Thi $g \circ f: L \rightarrow N$ er bijektiv, og for $x_1, x_2 \in L$ haves

$$g(f(x_1 * x_2)) = g(f(x_1) \S f(x_2)) = g(f(x_1)) \Delta g(f(x_2)).$$

Relationen " $(L,*)$ er isomorf med $(M,\S)$ " er en ækvivalensrelation i klassen af alle ved en komposition organiserede mængder.

Af de to foregående bemærkninger følger nemlig, at relationen er symmetrisk, henholdsvis transitiv, og den er tillige reflektiv, idet den identiske afbildning e_L er en isomorf afbildning af $(L,*)$ på sig selv.

Eksempler.

1° $(\mathbb{R}_+, \cdot)$ er isomorf med $(\mathbb{R}, +)$; funktionen $\log: \mathbb{R}_+ \rightarrow \mathbb{R}$ er nemlig bijektiv, og for $x_1, x_2 \in \mathbb{R}_+$ haves

$$\log(x_1 x_2) = \log x_1 + \log x_2.$$

Logaritmfunktionens omvendte, eksponentialfunktionen, er tilsvarende en isomorf afbildning af $(\mathbb{R}, +)$ på $(\mathbb{R}_+, \cdot)$, dvs. $\exp: \mathbb{R} \rightarrow \mathbb{R}_+$ er bijektiv og for $y_1, y_2 \in \mathbb{R}$ haves

$$e^{y_1 + y_2} = e^{y_1} e^{y_2}.$$

I øvrigt bestemmes for hvert $a \in \mathbb{R}_+$, $a \neq 1$, en isomorfi mellem $(\mathbb{R}_+, \cdot)$ og $(\mathbb{R}, +)$ ved funktionen $\log_a$; isomorfien

$$x \leftrightarrow y \iff \log_{10} x = y \iff x = 10^y$$

udnyttes på velkendt måde til udregninger ved logaritmetabel.

2° Mellem mængden V_3 af geometriske vektorer og mængden T_3 af translationer af rummet består som tidligere omtalt (I,5,21) en naturlig enentydig korrespondance; vektoren $\underline{v} = \vec{PQ}$ hører sammen med den translation t , der fører punktet P over i Q . Denne korrespondance er en isomorfi mellem $(V_3, +)$ og $(T_3, \circ)$, dvs.

$$\underline{v}_1 \leftrightarrow t_1 \wedge \underline{v}_2 \leftrightarrow t_2 \Rightarrow \underline{v}_1 + \underline{v}_2 \leftrightarrow t_1 \circ t_2.$$

Idet vektoradditionen er en kommutativ gruppekomposition, er sammensætning af translationer det ligeledes; de neutrale elementer, nulvektoren $\underline{0}$ og den identiske afbildning e_{E_3} af rummet, svarer til hinanden, og der gælder

$$\underline{v} \leftrightarrow t \Rightarrow -\underline{v} \leftrightarrow t^{-1}.$$

At $(L, *)$ er isomorf med $(M, \S)$, hvor $*$ og $\S$ er kompositioner inden for endelige mængder L og M , kommer ud på, at $*$ og $\S$ ved passende valg af betegnelser for elementerne af L og M kan angives ved samme kompositionstavle.

Homomorf afbildning.

Lad $*$ være en komposition inden for en mængde L og $\S$ en komposition inden for en mængde M .

En afbildning $f: L \rightarrow M$, hvor for $x_1, x_2 \in L$ gælder

$$f(x_1 * x_2) = f(x_1) \S f(x_2),$$

kaldes en homomorf afbildning af $(L, *)$ ind i $(M, \S)$. Hvis $f: L \rightarrow M$ tillige er bijektiv, er f en isomorf afbildning af $(L, *)$ på $(M, \S)$, jfr. side 12.

I det følgende antages, at $f: L \rightarrow M$ er surjektiv samt homomorf, idet L betragtes med kompositionen $*$, M med kompositionen $\S$. Vi har da:

Hvis $*$ er associativ, så er også $\S$ associativ.

Bevis: Lad y_1, y_2 og y_3 være vilkårlige elementer af M . Da f er surjektiv, kan vi tænke os $x_1, x_2, x_3 \in L$ valgt, så

$$f(x_1) = y_1, \quad f(x_2) = y_2 \quad \text{og} \quad f(x_3) = y_3.$$

Idet f er homomorf, har vi da

$$\begin{aligned} (y_1 \S y_2) \S y_3 &= (f(x_1) \S f(x_2)) \S f(x_3) \\ &= f(x_1 * x_2) \S f(x_3) = f((x_1 * x_2) * x_3) \end{aligned}$$

og ligeledes

$$y_1 \S (y_2 \S y_3) = f(x_1 * (x_2 * x_3)).$$

Er $*$ associativ, haves imidlertid

$$(x_1 * x_2) * x_3 = x_1 * (x_2 * x_3)$$

$$\text{og dermed} \quad (y_1 \S y_2) \S y_3 = y_1 \S (y_2 \S y_3).$$

Hvis $*$ er kommutativ, så er også $\S$ kommutativ.

Beviset føres på tilsvarende måde som det foregående.

Hvis et element $e \in L$ er neutralt ved $*$, så er $f(e)$ neutralt ved $\S$.

Bevis: Lad y være et vilkårligt element af M og x et element af L , således at $f(x) = y$. Da er

$$f(e) \S y = f(e) \S f(x) = f(e * x)$$

og ligeledes

$$y \S f(e) = f(x * e).$$

Er e neutralt, haves imidlertid

$$e * x = x * e = x$$

$$\text{og dermed} \quad f(e) \S y = y \S f(e) = y.$$

Forudsætter vi, at $(L, *)$ har et, og dermed netop ét, neutralt element e_L , vil $(M, \S)$ således også have ét neutralt element $e_M = f(e_L)$, og der gælder:

Hvis et element $x \in L$ er regulært ved $*$, så er $f(x)$ regulært ved $\S$. Hvis $x' \in L$ er inverst til $x \in L$ ved $*$, så er $f(x')$ inverst til $f(x)$ ved $\S$.

$$\begin{aligned} \text{Thi af} \quad x * x' &= x' * x = e_L \\ \text{følgder} \quad f(x * x') &= f(x' * x) = f(e_L), \\ \text{dvs.} \quad f(x) \S f(x') &= f(x') \S f(x) = e_M. \end{aligned}$$

Vi afrunder rækken af resultater med følgende, der fremgår af de foregående:

Hvis $(L, *)$ er en (kommutativ) gruppe, så er også $(M, \S)$ en (kommutativ) gruppe.

Vi bemærker, at de viste sætninger ikke kan vendes om. Simple modeksemples fås ved at benytte, at for enhver organiseret mængde $(L, *)$ vil den konstante afbildning $x \rightarrow 0$ med L som definitionsmængde være en surjektiv, homomorf afbildning på den kommutative gruppe $(\{0\}, +)$.

Lad nu $f: L \rightarrow M$ være en homomorf afbildning af $(L, *)$ ind i $(M, \S)$, som ikke forudsættes surjektiv. Sætningerne ovenfor kan da ikke opretholdes.

Restriktionen af $\S$ til $f(L) \times f(L)$ vil imidlertid være en komposition inden for $f(L)$; for vilkårlige $y_1, y_2 \in f(L)$ findes jo elementer $x_1, x_2 \in L$, således at $f(x_1) = y_1$ og $f(x_2) = y_2$ og dermed

$$f(x_1 * x_2) = f(x_1) \S f(x_2) = y_1 \S y_2,$$

hvorfor $y_1 \S y_2 \in f(L)$. Og betragtet som afbildning af $(L, *)$

på $(f(L), \S)$ er f både homomorf og surjektiv, således at de foregående resultater kan finde anvendelse her: hvis $*$ er associativ (kommutativ), så er $\S$ associativ (kommutativ) inden for $f(L)$; hvis e er neutralt ved $*$, så er $f(e)$ neutralt ved $\S$ inden for $f(L)$; osv.

Sammensætning af homomorfe afbildninger fører igen til en homomorf afbildning: Er $f: L \rightarrow M$ og $g: M \rightarrow N$ homomorfe afbildninger af $(L, *)$ på $(M, \S)$, henholdsvis $(M, \S)$ på (N, Δ) , hvor $*$, $\S$ og Δ er kompositioner inden for mængderne L , M og N , da vil den sammensatte afbildning $g \circ f$ være en homomorf afbildning af $(L, *)$ på (N, Δ) . Thi for $x_1, x_2 \in L$ have

$$g(f(x_1 * x_2)) = g(f(x_1) \S f(x_2)) = g(f(x_1)) \Delta g(f(x_2)).$$

Eksempler er allerede nævnt side 13-14; vi anfører yderligere:

1° For ethvert $a \in \mathbb{R}$ er afbildningen $x \mapsto ax$, $x \in \mathbb{R}$, en homomorf afbildning af $(\mathbb{R}, +)$ ind i sig selv, idet

$$a(x_1 + x_2) = ax_1 + ax_2,$$

medens $x \mapsto x^a$, $x \in \mathbb{R}_+$, er en homomorf afbildning af $(\mathbb{R}_+, \cdot)$ ind i sig selv, idet

$$(x_1 x_2)^a = x_1^a x_2^a.$$

Begge afbildninger er isomorfe, medmindre $a = 0$.

Afbildningen $x \mapsto x^2$, $x \in \mathbb{R}$, er en homomorf afbildning af $(\mathbb{R}, \cdot)$ ind i sig selv, og en surjektiv homomorf, men ikke isomorf afbildning af $(\mathbb{R}, \cdot)$ på $(\mathbb{R}_+ \cup \{0\}, \cdot)$.

2° Projektion af geometriske vektorer på en given plan eller linie er en homomorf afbildning af $(V_3, +)$ ind i sig selv.

3° Tilordner man til hvert $x \in \mathbb{R}$ drejningen vinklen x om et givet punkt O i en orienteret plan, fås en surjektiv homomorf, men ikke isomorf afbildning af $(\mathbb{R}, +)$ på mængden af drejninger om O med sammensætning som komposition. (Til x og $x + 2\pi$ svarer samme drejning.)

4° Tilordner man til hver permutation x af en given mængde A med n elementer, $n \geq 2$, fortegnet $\text{sgn } x$, altså 1 eller -1 eftersom x er en lige eller ulige permutation, fås en surjektiv homomorf afbildning af den symmetriske gruppe S_n , dvs. mængden af permutationer af A med sammensætning som komposition, på gruppen $(\{1, -1\}, \cdot)$.

En homomorf afbildning kaldes også en homomorfi; en homomorf afbildning af en organiseret mængde ind i sig selv siges også at være endomorf eller en endomorfi; en isomorf afbildning af en organiseret mængde på sig selv siges også at være automorf, medens ordet isomorfi tilsvarende erstattes af automorfi.

Ækvivalensrelation og komposition.

Lad $*$ være en komposition inden for en mængde M og $\sim$ en ækvivalensrelation i samme mængde. Vi betegner med $\tilde{M}$ mængden af ækvivalensklasser, med K_x klassen repræsenteret af et element $x \in M$ (jfr. side I, 5, 17).

Vi vil sige, at ækvivalensrelationen $\sim$ harmonerer med kompositionen $*$, hvis der for $x_1, x_2, y_1, y_2 \in M$ gælder

$$x_1 \sim x_2 \wedge y_1 \sim y_2 \Rightarrow x_1 * y_1 \sim x_2 * y_2.$$

Dette er ensbetydende med, at ligegyldigt hvilke repræsentanter x og y man betragter for to ækvivalensklasser A og B , vil $x * y$ tilhøre samme ækvivalensklasse. Man kan da indføre en komposition $\tilde{*}$ i $\tilde{M}$ ved for $A, B \in \tilde{M}$ at sætte $A \tilde{*} B = K_{x*y}$, hvor x og y er vilkårlige elementer af A og B . Der gælder åbenbart for $x, y \in M$

$$K_x \tilde{*} K_y = K_{x*y},$$

og $\tilde{*}$ er den eneste komposition i $\tilde{M}$ med denne egenskab. Vi tilføjer, at harmoni mellem $\sim$ og $*$, som man let ser, også er en nødvendig betingelse for eksistensen af en komposition i $\tilde{M}$ med nævnte egenskab.

Idet vi nu forudsætter, at $\sim$ harmoniserer med $*$, og bemærker, at betingelsen

$$\forall_{M^x, y}: K_x \tilde{*} K_y = K_{x*y},$$

hvorved kompositionen $\tilde{*}$ i $\tilde{M}$ er bestemt, netop udtrykker, at den naturlige afbildning $x \rightarrow K_x$, $x \in M$, af M på $\tilde{M}$ er homomorf, kan vi anvende resultaterne side 15-16: Hvis $*$ er associativ (kommutativ), så vil $\tilde{*}$ også være det; er $e \in M$ neutralt ved $*$, så er K_e neutral ved $\tilde{*}$; hvis x er regulært ved $*$, så er K_x regulær ved $\tilde{*}$; hvis x' er inverst til x ved $*$, så er $K_{x'}$ invers til K_x ved $\tilde{*}$; hvis $(M, *)$ er en gruppe, så er $(\tilde{M}, \tilde{*})$ en gruppe.

Overgangen fra $(M, *)$ til $(\tilde{M}, \tilde{*})$ kan siges at bestå i, at man ophører med at skelne mellem indbyrdes ækvivalente elementer i M .

Eksempler.

1° Ved

$$x_1 \sim x_2 \iff \exists_{\mathbb{Z}} h [x_2 - x_1 = h2\pi]$$

defineres en ækvivalensrelation i $\mathbb{R}$, som harmonerer med addition, men ikke med multiplikation. Vil man identificere tal, der afviger med et heltalligt multiplum af 2π , kan man derfor stadig addere, dvs. i mængden $\mathbb{R}_{2\pi}$ af ækvivalensklasser kan man addere ved repræsentanter, hvorimod multiplikation bryder sammen. Den Abelske gruppe $(\mathbb{R}_{2\pi}, +)$ er isomorf med gruppen af drejninger af planen om et fast punkt (sml. 3°, side 18). Erstattes 2π med et vilkårligt reelt tal $a > 0$, fås en med $(\mathbb{R}_{2\pi}, +)$ isomorf Abelsk gruppe $(\mathbb{R}_a, +)$. Vi bemærker, at medens de reelle tal jo ofte repræsenteres ved punkterne på en ret linie, kan elementerne i $\mathbb{R}_a$ på naturlig måde repræsenteres ved punkterne på en cirkelperiferi af længde a , for hvilken begyndelsespunkt og gennemløbsretning er valgt.

2° For et vilkårligt helt tal $m > 0$ defineres ved

$$x_1 \sim x_2 \iff \exists_{\mathbb{Z}} h [x_2 - x_1 = hm],$$

dvs. ved

$$x_1 \sim x_2 \iff m \mid x_2 - x_1,$$

en ækvivalensrelation i $\mathbb{Z}$, som harmonerer ikke blot med addition,

$$m \mid x_2 - x_1 \wedge m \mid y_2 - y_1 \Rightarrow m \mid (x_2 + y_2) - (x_1 + y_1),$$

men også med multiplikation,

$$m \mid x_2 - x_1 \wedge m \mid y_2 - y_1 \Rightarrow m \mid x_2 y_2 - x_1 y_1,$$

som man indser ved omskrivningen

$$x_2 y_2 - x_1 y_1 = (x_2 - x_1) y_2 + x_1 (y_2 - y_1).$$

Relationen kaldes kongruens modulo m , medens man for $m \mid x_2 - x_1$ skriver

$$x_1 \equiv x_2 \pmod{m},$$

hvilket læses: x_1 er kongruent med x_2 modulo m . Ækvivalensklassen repræsenteret af et tal $x \in \mathbb{Z}$ vil vi betegne $(x)_m$,

$$(x)_m = \{x + hm \mid h \in \mathbb{Z}\}.$$

Ækvivalensklasserne kaldes restklasser modulo m , idet hver af dem består af alle hele tal, som ved division med m kan give en bestemt rest. Da hvert helt tal ved division med m kan give netop én af resterne $0, 1, \dots, m-1$, findes der m forskellige restklasser modulo m ; blandt tallene $0, 1, \dots, m-1$ er der én repræsentant for hver. Mængden af restklasser modulo m vil vi betegne $\mathbb{Z}(\text{mod } m)$ eller $\mathbb{Z}_m$. - Man bemærker, at $\mathbb{Z}_m$ er en delmængde af $\mathbb{R}_m$ (se eks. 1^o), og føres herved til at repræsentere de m restklasser modulo m ved m punkter liggende ækvidistant på en cirkelperiferi.

Da kongruens modulo m harmonerer med addition og multiplikation af hele tal, kan man i mængden $\mathbb{Z}_m$ af restklasser modulo m addere og multiplicere ved repræsentanter. De to kompositioner, der kaldes addition og multiplikation modulo m og gerne betegnes $+$ og $\cdot$, er bestemt ved

$$(x)_m + (y)_m = (x + y)_m \quad \text{og} \quad (x)_m (y)_m = (xy)_m.$$

Foreløbig skal vi kun beskæftige os med addition modulo m og bemærker her, at $(\mathbb{Z}_m, +)$ er en Abelsk gruppe med $(0)_m$ som neutralt element. For forskellige værdier af m fås naturligvis grupper $(\mathbb{Z}_m, +)$, der ikke er isomorfe; elementantallene er jo forskellige.

§ 2. Grupper.

Gruppe og undergruppe.

En komposition $\cdot$ inden for en mængde G siges, som allerede nævnt side II,1,7, at være en gruppekomposition, og $(G, \cdot)$ kaldes en gruppe, hvis $\cdot$ er associativ, der findes et neutralt element $e \in G$, og hvert element af G er regulært.

En mængde G med en komposition $\cdot$ inden for G er således en gruppe med elementet e tilhørende G som neutralt element, hvis

$$\forall_{G^x, y, z} [(xy)z = x(yz)],$$

$$\forall_{G^x} [ex = xe = x],$$

$$\forall_{G^x} \exists_{G^y} [yx = xy = e].$$

Som anført side II,1,8 findes der i en gruppe $(G, \cdot)$ kun ét neutralt element e , og hvert $x \in G$ har netop ét inverst x^{-1} , bestemt ved

$$x^{-1}x = xx^{-1} = e.$$

For vilkårlige $a, b \in G$ har endvidere hver af ligningerne

$$ax = b \quad \text{og} \quad xa = b$$

netop én løsning, nemlig henholdsvis $a^{-1}b$ og ba^{-1} ; specielt gælder forkortningsreglerne

$$ax = ay \Rightarrow x = y \quad \text{og} \quad xa = ya \Rightarrow x = y$$

for $a, x, y \in G$. Bemærk, at man kan slutte, at $x = e$, blot man for ét element a ved, at $ax = a$ eller $xa = a$. Allerede af $xy = e$ følger, at x og y er inverse.

En gruppe kaldes som nævnt side II,1,8 kommutativ eller Abelsk (efter N.H. Abel), hvis kompositionen er kommutativ. For kommutative grupper benyttes ofte additiv skrivemåde (jfr. II,1,10); kompositionen betegnes da med $+$, for det neutrale element skrives o eller 0 , det inverse til x betegnes $-x$, og løsningen $b + (-a)$ til de ensbetydende ligninger $a + x = b$ og $x + a = b$ betegnes $b - a$.

En gruppe $(G, \cdot)$, hvor G har et endeligt elementantal n , siges at være en endelig gruppe af orden n .

Findes der et neutralt element e ved en associativ komposition $\cdot$ inden for en mængde M , vil gruppeteorien kunne bringes i anvendelse på de regulære elementer. Der gælder nemlig:

Er x og y regulære elementer af M , da vil xy ligeledes være regulært, nemlig med $(xy)^{-1} = y^{-1}x^{-1}$, idet

$$(xy)(y^{-1}x^{-1}) = (y^{-1}x^{-1})(xy) = e.$$

Endvidere er e regulært med $e^{-1} = e$, og er x regulært, vil x^{-1} ligeledes være regulært og $(x^{-1})^{-1} = x$.

Idet vi med G betegner mængden af regulære elementer af M , indebærer den første bemærkning, at restriktionen af $\cdot$ til $G \times G$ er en komposition inden for G . Denne restriktion er naturligvis associativ. Da $e \in G$, er det endvidere klart, at e er et element i $(G, \cdot)$, og idet det i $(M, \cdot)$ inverse element x^{-1} til et vilkårligt $x \in G$ igen tilhører G , ser man, at det også i $(G, \cdot)$ er inverst til x . Specielt er vist, at $(G, \cdot)$ er en gruppe.

Eksempler.

1° Sædvanlig multiplikation er inden for hver af mængderne $\mathbb{N}$, $\mathbb{Q}$ og $\mathbb{R}$ en associativ komposition med 1 som neutralt element. Gruppen af regulære elementer er henholdsvis $(\{1\}, \cdot)$, $(\{1, -1\}, \cdot)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ og $(\mathbb{R} \setminus \{0\}, \cdot)$.

2° Sætningsætning er inden for mængden $\mathcal{F}(A \rightarrow A)$ af afbildninger af en mængde A ind i sig selv en associativ komposition med den identiske afbildning e_A som neutralt element. Gruppen af regulære elementer er $(\Gamma_A, \cdot)$, hvor Γ_A betegner mængden af transformationer af A .

Lad $(G, \cdot)$ være en gruppe og H en ikke tom delmængde af G .

Man siger da, at H er en undergruppe af $(G, \cdot)$, hvis restriktionen af $\cdot$ til $H \times H$ er en komposition inden for H , og hvis H med denne komposition, $(H, \cdot)$, er en gruppe.

Egentlig er det $(H, \cdot)$ og ikke H , der bør kaldes undergruppe; vi vil dog foretrække ikke at lægge sprogbrugen fast, men undertiden bruge ordet i den ene, undertiden i den anden betydning.

Idet vi forudsætter, at H er en undergruppe af gruppen $(G, \cdot)$, vil det neutrale element e i $(G, \cdot)$ tilhøre H og være neutralt i $(H, \cdot)$. Thi betegnes det neutrale element i $(H, \cdot)$ med e_H og vælges et element $a \in H$, har vi $ae_H = ae$ og følgelig, ved forkortning, $e_H = e$. Det inverse element x^{-1} til et element $x \in H$ vil da også være det samme, hvad enten vi regner i $(H, \cdot)$ eller $(G, \cdot)$.

Der kan herefter opstilles simple nødvendige betingelser for, at en delmængde af en gruppe er en undergruppe, betingelser, der, som vi skal vise, tillige er tilstrækkelige:

Idet $(G, \cdot)$ er en gruppe og H en ikke tom delmængde af G , er det nødvendigt og tilstrækkeligt for, at H er en undergruppe af $(G, \cdot)$, at der gælder

$x \in H \wedge y \in H \Rightarrow xy \in H$ og $x \in H \Rightarrow x^{-1} \in H$,
eller, anderledes skrevet, at

$$\forall_H x, y: xy \in H \quad \text{og} \quad \forall_H x: x^{-1} \in H.$$

Den første betingelse kommer nemlig ud på, at restriktionen af $\cdot$ til $H \times H$ er en komposition inden for H , og nødvendigheden af den anden betingelse fremgår af det ovenfor sagte. Vi vil nu antage de to betingelser opfyldt og vise, at $(H, \cdot)$ da er en gruppe. Det er klart, at den associative lov gælder for $(H, \cdot)$. Idet det neutrale element e i $(G, \cdot)$ kan skrives på formen $e = aa^{-1}$ med $a \in H$, ser man, at e tilhører H og dermed naturligvis er neutralt

element i $(H, \cdot)$. Videre bemærkes, at det i $(G, \cdot)$ inverse x^{-1} til et vilkårligt element $x \in H$ tillige er inverst til x i $(H, \cdot)$, således at x er regulært i $(H, \cdot)$.

Er Φ en mængde af undergrupper af en given gruppe $(G, \cdot)$, vil $\bigcap \{H \mid H \in \Phi\}$ igen være en undergruppe af $(G, \cdot)$. Dette ses straks ved brug af de fundne to betingelser; at fællesmængden ikke er tom, sikres ved, at den i hvert fald indeholder det neutrale element e i $(G, \cdot)$.

Blandt undergrupperne af en gruppe $(G, \cdot)$ findes en mindste, $\{e\}$, og en største, G . For enhver mængde $A \subseteq G$ findes en mindste blandt de undergrupper af $(G, \cdot)$, som indeholder A , nemlig deres fællesmængde. Den består, når $A \neq \emptyset$, af de elementer af G , der kan skrives som produkt af endelig mange faktorer, hver tilhørende A eller invers til et element af A . Et sådant produkt vil nemlig tilhøre enhver undergruppe af $(G, \cdot)$, som indeholder A , og mængden af de nævnte elementer er selv en undergruppe af $(G, \cdot)$, som indeholder A .

Eksempler.

1° Mængden V_1 af vektorer på en given linie l og mængden V_2 af vektorer i en given plan π er undergrupper i gruppen $(V_3, +)$ af geometriske vektorer med sædvanlig vektoraddition. Ligger l i π , vil V_1 tillige være en undergruppe af $(V_2, +)$.

I $(V_3, +)$ findes også undergrupper af en helt anden karakter; eksempelvis nævnes den mindste undergruppe indeholdende to givne vektorer $\underline{u}$ og $\underline{v}$, som åbenbart er $\{p\underline{u} + q\underline{v} \mid p, q \in \mathbb{Z}\}$.

2° I hver af nedenstående rækker er en gruppe, der er nævnt tidligere end en anden, undergruppe i denne:

- a) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +).$
- b) $(\mathbb{Q}_+, \cdot), (\mathbb{R}_+, \cdot), (\mathbb{R} \setminus \{0\}, \cdot).$
- c) $(\mathbb{Q}_+, \cdot), (\mathbb{Q} \setminus \{0\}, \cdot), (\mathbb{R} \setminus \{0\}, \cdot).$

3° For et vilkårligt $m \in \mathbb{N}$ er $(\mathbb{Z}_m, +)$ en undergruppe af $(\mathbb{R}_m, +)$, jfr. II, 1, 20-21.

Relationen " $(H, \cdot)$ er en undergruppe af $(G, \cdot)$ " er en reflektiv ordningsrelation i klassen af alle grupper. Specielt noteres: hvis $(K, \cdot)$ er en undergruppe af $(H, \cdot)$ og $(H, \cdot)$ en undergruppe af $(G, \cdot)$, så er $(K, \cdot)$ en undergruppe af $(G, \cdot)$.

Transformationsgruppe.

Som flere gange nævnt (II, 1, 9 og II, 2, 2) er mængden Γ_E af transformationer af en mængde E , dvs. bijektive afbildninger af E på sig selv, med sammensætning som komposition en gruppe, $(\Gamma_E, \circ)$. Denne kaldes den fuldstændige transformationsgruppe for E . Den identiske afbildning e_E er neutralt element, og den inverse afbildning f^{-1} til en transformation f er dennes inverse element.

En transformationsgruppe for en mængde E er i I, §3 defineret som en ikke tom mængde T af transformationer af E , hvor

$$f \in T \wedge g \in T \Rightarrow f \circ g \in T \quad \text{og} \quad f \in T \Rightarrow f^{-1} \in T.$$

Definitionen kan nu også udtrykkes (jfr. side 3): En transformationsgruppe for en mængde E er en undergruppe af den fuldstændige transformationsgruppe $(\Gamma_E, \circ)$, altså en mængde T af transformationer af E , som med sammensætning som komposition er en gruppe, $(T, \circ)$. Egentlig er det gruppen $(T, \circ)$ og ikke mængden T , der bør kaldes transformationsgruppe; vi vil dog foretrække ikke at lægge sprogbrugen fast.

I stedet for transformationsgruppe siges også permutationsgruppe for E , især når E er endelig.

Eksempler.

1° Idet G er en transformationsgruppe for en mængde E , og A er en delmængde af E , vil

$$H = \{f \in G \mid f(A) = A\}$$

være en undergruppe af $(G, \circ)$, altså igen en transformationsgruppe, ligesom

$$K = \{f \in G \mid \forall_A x: f(x) = x\}$$

vil være en undergruppe af $(H, \circ)$.

Thi idet $e_E \in K$, haves $\emptyset \subset K \subseteq H$; endvidere er det klart, at

$$f \in H \wedge g \in H \Rightarrow f \circ g \in H, \quad f \in H \Rightarrow f^{-1} \in H,$$

og analogt for K .

2° Mængden af isometrier af rummet E_3 er en transformationsgruppe, mængden af flytninger (egentlige kongruenser) af E_3 ligeledes. Mængden af isometrier, henholdsvis flytninger, der lader et givet punkt gå over i sig selv, er da igen transformationsgrupper, og det samme gælder mængden af isometrier, henholdsvis flytninger, hvorved f.eks. et givet regulært polyeder går over i sig selv (jfr. 1°). For isometrier af planen haves ganske tilsvarende forhold. Mellem gruppen af flytninger af rummet E_3 , hvorved en given plan E_2 går over i sig selv, og gruppen af alle isometrier af E_2 består en naturlig isomorfi, fastlagt ved at en isometri af E_2 opfattes som restriktion af en flytning af E_3 .

En enentydig korrespondance mellem to mængder A_1 og A_2 giver på naturlig måde anledning til en enentydig korrespondance mellem mængderne $\hat{F}(A_1 \rightarrow A_1)$ og $\hat{F}(A_2 \rightarrow A_2)$ af afbildninger af A_1 , henholdsvis A_2 , ind i sig selv, idet $f_1: A_1 \rightarrow A_1$ og $f_2: A_2 \rightarrow A_2$ regnes at korrespondere, hvis der for $x_1 \in A_1$, $x_2 \in A_2$ gælder

$$x_1 \leftrightarrow x_2 \Rightarrow f_1(x_1) \leftrightarrow f_2(x_2).$$

Idet denne betingelse kan skrives

$$\varphi(x_1) = x_2 \Rightarrow \varphi(f_1(x_1)) = f_2(x_2),$$

hvor $\varphi: A_1 \rightarrow A_2$ er den bijektive afbildning svarende til korrespondancen mellem A_1 og A_2 , ser man, at $f_1: A_1 \rightarrow A_1$ og $f_2: A_2 \rightarrow A_2$ korresponderer, netop hvis

$$\forall_{A_1} x_1: \varphi(f_1(x_1)) = f_2(\varphi(x_1)),$$

dvs. hvis

$$\varphi \circ f_1 = f_2 \circ \varphi.$$

Det er da indlysende, at der til hver afbildning $f_1: A_1 \rightarrow A_1$ svarer netop én afbildning $f_2: A_2 \rightarrow A_2$, nemlig $f_2 = \varphi \circ f_1 \circ \varphi^{-1}$, og ligeledes til hver afbildning $f_2: A_2 \rightarrow A_2$ netop én afbildning $f_1: A_1 \rightarrow A_1$, nemlig $f_1 = \varphi^{-1} \circ f_2 \circ \varphi$.

Til transformationer svarer åbenbart transformationer, og i det man umiddelbart efterviser, at

$$\varphi \circ f_1 = f_2 \circ \varphi \wedge \varphi \circ g_1 = g_2 \circ \varphi \Rightarrow \varphi \circ (f_1 \circ g_1) = (f_2 \circ g_2) \circ \varphi,$$

er korrespondancen mellem Γ_{A_1} og Γ_{A_2} en isomorfi mellem de fuldstændige transformationsgrupper $(\Gamma_{A_1}, \circ)$ og $(\Gamma_{A_2}, \circ)$.

Vi noterer det ikke overraskende resultat:

De fuldstændige transformationsgrupper $(\Gamma_{A_1}, \circ)$ og $(\Gamma_{A_2}, \circ)$ for ækvipotente mængder A_1 og A_2 er isomorfe.

I mange forbindelser regnes isomorfe grupper for uvæsentligt forskellige. Undertiden bruges vendingen, at de er "eksemplarer af samme abstrakte gruppe".

Den netop viste sætning berettiger da til, at man omtaler den fuldstændige permutationsgruppe $(\Gamma_E, \circ)$ for en vilkårlig mængde E med n elementer som den symmetriske gruppe af graden n og tilsvarende benytter en betegnelse $(S_n, \circ)$, hvor mængden E ikke er anført (jfr. I, ,).

Eksempler.

1° En gruppetafle for $(S_3, \circ)$ er opskrevet side II, 1, 4.

2° De lige permutationer af en mængde E med n elementer danner en transformationsgruppe $(A_n, \circ)$, den alternerende gruppe af graden n (jfr. I, ,). Gruppen af permutationer af E , hvorved et givet element $a \in E$ afbildes på sig selv, er tydeligvis isomorf med $\Gamma_E \setminus \{a\}$ og kan da siges at være et eksemplar af $(S_{n-1}, \circ)$. Den symmetriske gruppe $(S_n, \circ)$ indeholder således, for $n > 2$, i det mindste n eksemplarer af $(S_{n-1}, \circ)$ som undergrupper.

Gruppeteorien udvikledes i løbet af det 19. århundrede, længe - til henimod 1880 - næsten udelukkende som en teori om transformationsgrupper (A.-L. Cauchy, E. Galois, C. Jordan). Det almene gruppebegreb går dog tilbage til 1854 (A. Cayley). Ved generaliseringen fra transformationsgrupper til vilkårlige grupper blev der (som Cayley straks bemærkede) i en vis forstand ikke flere grupper at undersøge:

Enhver gruppe $(G, \cdot)$ er isomorf med en transformationsgruppe, nemlig med en transformationsgruppe for mængden G af gruppens elementer. Specielt er enhver endelig gruppe af orden n isomorf med en undergruppe af den symmetriske gruppe $(S_n, \circ)$.

Bevis: Er g et element af G , defineres ved $x \rightarrow gx$, $x \in G$, en afbildning $\tau_g: G \rightarrow G$, som er bijektiv, idet der for hvert $y \in G$ findes et og kun et $x \in G$, således at $gx = y$. Ved $g \rightarrow \tau_g$, $g \in G$, defineres således en afbildning φ af G ind i mængden Γ_G af transformationer af G . Nu gælder åbenbart

$$\tau_{g_2 g_1} = \tau_{g_2} \circ \tau_{g_1},$$

thi for hvert $x \in G$ er

$$\tau_{g_2 g_1}(x) = (g_2 g_1)x = g_2(g_1 x) = \tau_{g_2}(\tau_{g_1}(x)) = \tau_{g_2} \circ \tau_{g_1}(x).$$

Sammensætning er da en komposition inden for $\varphi(G) = \{\tau_g \mid g \in G\}$, og $\varphi: (G, \cdot) \rightarrow (\varphi(G), \circ)$ er homomorf og surjektiv (jfr. II, 1, 16).

Det er endvidere klart, at φ er injektiv: er $g_1 \neq g_2$ haves endog for hvert $x \in G$, at $g_1 x \neq g_2 x$, dvs. $\tau_{g_1}(x) \neq \tau_{g_2}(x)$. Følgelig er $\varphi: (G, \cdot) \rightarrow (\varphi(G), \circ)$ isomorf og $(\varphi(G), \circ)$ en gruppe, hvormed sætningen er vist.

Den bijektive afbildning $\tau_g: G \rightarrow G$ defineret ved $x \rightarrow gx$, $x \in G$, kaldes den ved g bestemte venstre translation af gruppen $(G, \cdot)$. Den isomorfe afbildning $g \rightarrow \tau_g$ af $(G, \cdot)$ på gruppen $(\{\tau_g \mid g \in G\}, \circ)$ af venstre translationer kaldes den regulære fremstilling (repræsentation) af gruppen $(G, \cdot)$.

Er $(G, \cdot)$ en endelig gruppe, kan venstre translationerne, som jo er visse permutationer af G , aflæses af en gruppetavles rækker.

For Abelske gruppers vedkommende vil man naturligvis oftest i stedet for "venstre translation" blot sige "translation".

Eksempler.

1° Den ved en vektor $\underline{a}$ bestemte translation $\tau_{\underline{a}}: V_3 \rightarrow V_3$ af gruppen $(V_3, +)$ af geometriske vektorer med sædvanlig vektoraddition er afbildningen $\underline{x} \rightarrow \underline{x} + \underline{a}$, $\underline{x} \in V_3$. Overføres $\tau_{\underline{a}}$ efter valg af et begyndelsespunkt O for stedvektorer til mængden E_3 af punkter i rummet (jfr. side 6), fås den ved vektoren $\underline{a}$ bestemte translation af E_3 - ordet translation her brugt i sin hidtidige betydning (jfr. I, 3, 3). Gruppen $(V_3, +)$ er således isomorf med gruppen af translationer af rummet E_3 , hvad vi i øvrigt tidligere har bemærket (II, 1, 14).

2° Den ved et $a \in \mathbb{R}$ bestemte translation af gruppen $(\mathbb{R}, +)$ er afbildningen $x \rightarrow x + a$, $x \in \mathbb{R}$, og $(\mathbb{R}, +)$ er isomorf med gruppen af sådanne translationer af tallinien. Den ved et $a \in \mathbb{R} \setminus \{0\}$ bestemte translation af gruppen $(\mathbb{R} \setminus \{0\}, \cdot)$ er homotetien $x \rightarrow ax$, $x \in \mathbb{R} \setminus \{0\}$, og $(\mathbb{R} \setminus \{0\}, \cdot)$ er isomorf med gruppen af homotetier af tallinien med centrum 0.

3° For en gruppe med 6 elementer $p_1, p_2, p_3, p_4, p_5, p_6$, hvor kompositionen er angivet ved gruppetavlen side II, 1, 4, er eksempelvis den ved p_5 bestemte venstre translation

$$\tau_{p_5} = \begin{pmatrix} p_1 & p_2 & p_3 & p_4 & p_5 & p_6 \\ p_5 & p_6 & p_4 & p_3 & p_1 & p_2 \end{pmatrix}.$$

4° Ved til hvert element g af en gruppe $(G, \cdot)$ at tilordne den ved g^{-1} bestemte højre translation $x \rightarrow xg^{-1}$, $x \in G$, fås en isomorf afbildning af $(G, \cdot)$ på gruppen af højre translationer af $(G, \cdot)$.

Potensregler.

Idet $\cdot$ er en komposition inden for en mængde M , defineres potenserne x^n , $n \in \mathbb{N}$, af et element $x \in M$ ved rekursionsformlerne

$$x^1 = x, \quad x^{n+1} = x^n x.$$

Vi vil forudsætte, at $\cdot$ er associativ. For $x, y \in M$ og $p, q \in \mathbb{N}$ gælder da potensreglerne

$$(1) \quad x^p x^q = x^{p+q},$$

$$(2) \quad (x^p)^q = x^{pq},$$

$$(3) \quad xy = yx \Rightarrow (xy)^q = x^q y^q.$$

Regel (1) bevises ved induktion efter q , idet man tænker sig x og p fastholdt. Vi har

$$x^p x^1 = x^p x = x^{p+1},$$

og ud fra induktionsantagelsen $x^p x^q = x^{p+q}$ sluttet

$$x^p x^{q+1} = x^p (x^q x) = (x^p x^q) x = x^{p+q} x = x^{p+q+1}.$$

Derpå kan regel (2) bevises, ligeledes ved induktion efter q .

Vi har

$$(x^p)^1 = x^p = x^{p \cdot 1},$$

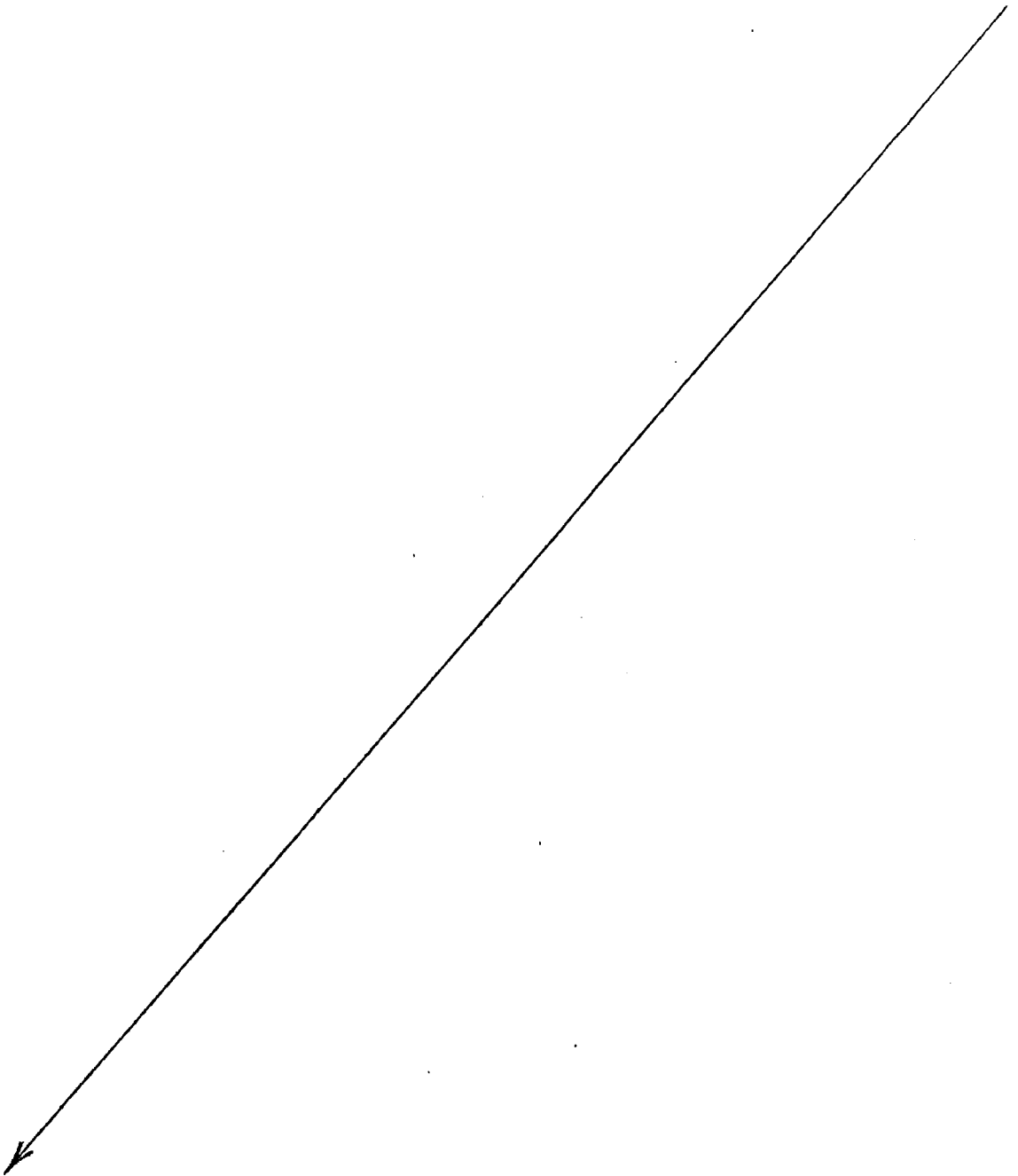
og ud fra induktionsantagelsen $(x^p)^q = x^{pq}$ sluttet

$$(x^p)^{q+1} = (x^p)^q x^p = x^{pq} x^p = x^{pq+p} = x^{p(q+1)}.$$

Med henblik på beviset for regel (3) bemærkes først, at

$$xy = yx \Rightarrow xy^q = y^q x.$$

Antages $xy = yx$, fås nemlig $\forall_{\mathbb{N}} q: xy^q = y^q x$ ved induktion. Vi



har jo $xy^1 = y^1x$, og ud fra induktionsantagelsen $xy^q = y^qx$ sluttes

$$xy^{q+1} = xy^qy = y^qxy = y^qyx = y^{q+1}x.$$

Regel (3) fremgår nu, idet vi under antagelse af $xy = yx$ viser $\forall n \in \mathbb{N}: (xy)^n = x^n y^n$ ved induktion. Vi har jo $(xy)^1 = xy = x^1 y^1$, og ud fra induktionsantagelsen $(xy)^q = x^q y^q$ sluttes

$$(xy)^{q+1} = (xy)^q xy = x^q y^q xy = x^q xy^q y = x^{q+1} y^{q+1}.$$

Vi forudsætter nu, at der ved den associative komposition $\cdot$ inden for mængden M findes et neutralt element $e \in M$.

For hvert $x \in M$ sættes da ved definition

$$x^0 = e.$$

Det verificeres umiddelbart, at potensreglerne (1), (2) og (3) herefter er gyldige for alle $x, y \in M$ og $p, q \in \mathbb{N}_0$.

For elementer af M , der er regulære ved $\cdot$, defineres også potens med negativ hel eksponent.

Først bemærkes, at er x regulær, så er også enhver potens x^n , $n \in \mathbb{N}$, regulær. Ud fra induktionsantagelsen at x^n er regulær, sluttes jo straks, at $x^{n+1} = x^n x$ er regulær (jfr. side 2).

Vi kan da for regulære elementer $x \in M$ og negative hele tal n sætte

$$x^n = (x^{-n})^{-1}.$$

For regulære elementer $x, y \in M$ vil potensreglerne (1), (2) og (3) herefter, som vi skal se, gælde for alle $p, q \in \mathbb{Z}$. Idet mængden af regulære elementer af M med restriktionen af $\cdot$ er en gruppe, som omtalt side 2, og der nu i reglerne kun indgår nævnte restriktion, kan påstanden bringes på en mere bekvem form:

I en gruppe $(G, \cdot)$, hvor jo x^n er defineret for hvert $x \in G$ og hvert $n \in \mathbb{Z}$, gælder potensreglerne

$$(1) \quad x^p x^q = x^{p+q},$$

$$(2) \quad (x^p)^q = x^{pq},$$

$$(3) \quad xy = yx \Rightarrow (xy)^q = x^q y^q$$

for alle $x, y \in G$ og alle $p, q \in \mathbb{Z}$.

Til beviset minder vi (jfr. side 2) om reglen

$$(4) \quad (xy)^{-1} = y^{-1} x^{-1}.$$

Videre bemærker vi, at x^n og x^{-n} er inverse for ethvert $n \in \mathbb{Z}$, nemlig for $n < 0$ ifølge definitionen på x^n , for $n > 0$ ifølge definitionen på x^{-n} , ligesom påstanden er klar for $n = 0$.

Ad(1): Er (1) rigtig for et eksponentpar p, q , da også for eksponentparret $-q, -p$, idet

$$x^{-q} x^{-p} = (x^q)^{-1} (x^p)^{-1} = (x^p x^q)^{-1} = (x^{p+q})^{-1} = x^{-q-p};$$

det betyder derfor ingen indskrænkning at antage $p + q \geq 0$.

Idet (1) vides at gælde for $p \geq 0, q \geq 0$, skal vi da blot betragte tilfældene $p + q \geq 0, p > 0, q < 0$ og $p + q \geq 0, p < 0, q > 0$; eksempelvis tages førstnævnte:

$$x^p x^q = x^{(p+q)+(-q)} x^q = x^{p+q} x^{-q} x^q = x^{p+q}.$$

Ad(2): For $q > 0$ kan (2) nu bevises ved induktion efter q , ganske som side 11. For $q = 0$ er (2) øjensynlig rigtig, og for $q < 0$ har vi

$$(x^p)^q = ((x^p)^{-q})^{-1} = (x^{-pq})^{-1} = x^{pq}.$$

Ad(3): Her mangler kun tilfældet $q < 0$, hvor vi imidlertid under antagelse af $xy = yx$ har

$$(xy)^q = ((yx)^{-q})^{-1} = (y^{-q} x^{-q})^{-1} = x^q y^q.$$

For en komposition betegnet $+$ skrives nx i stedet for x^n . Specielt er $1x = x$, medens $x^0 = e$ erstattes af $0x = o$. Potensreglerne (1) og (2) antager udseendet

$$px + qx = (p+q)x, \quad q(px) = (qp)x,$$

og forudsat $+$ er kommutativ, kan (3) skrives

$$q(x + y) = qx + qy.$$

Cyklisk gruppe.

En gruppe $(C, \cdot)$ siges at være cyklisk, hvis der findes et element $c \in C$, således at

$$C = \{c^p \mid p \in \mathbb{Z}\};$$

hvert sådant element $c \in C$ kaldes da en frembringer for gruppen $(C, \cdot)$.

Man bemærker straks, at enhver cyklisk gruppe er kommutativ, idet jo

$$c^p c^q = c^{p+q} = c^q c^p.$$

Lad nu $(G, \cdot)$ være en vilkårlig gruppe og c et element af G .

Sætter vi $\{c^p \mid p \in \mathbb{Z}\} = C$, er gyldigheden af undergruppebetingelserne (jfr. side 3)

$$x \in C \wedge y \in C \Rightarrow xy \in C \quad \text{og} \quad x \in C \Rightarrow x^{-1} \in C$$

en umiddelbar konsekvens af reglerne

$$c^p c^q = c^{p+q} \quad \text{og} \quad (c^p)^{-1} = c^{-p}.$$

Følgelig er $(C, \cdot) = (\{c^p \mid p \in \mathbb{Z}\}, \cdot)$ en gruppe, som åbenbart er cyklisk med c som frembringer. Den kaldes den af c frembragte cykliske undergruppe af $(G, \cdot)$.

Eksempler.

1° Gruppen $(\mathbb{Z}, +)$ er cyklisk. Hvert af tallene 1 og -1 er frembringer, og der er ikke flere. Den af et tal $m \in \mathbb{Z}$ frembragte cykliske undergruppe $(\{pm \mid p \in \mathbb{Z}\}, +)$ har også $-m$ som frembringer, men ikke flere.

For hvert $n \in \mathbb{N}$ er gruppen $(\mathbb{Z}_n, +)$ cyklisk; hver af restklasserne $(1)_n$ og $(-1)_n$ er frembringer, i almindelighed er der flere. (Jfr. II, 1, 21.)

2° Som andre eksempler på cykliske grupper nævnes gruppen $(\{z \in \mathbb{C} \mid z^n = 1\}, \cdot)$ af komplekse rødder til ligningen $z^n = 1$ for givet $n \in \mathbb{N}$, samt gruppen af flytninger (drejninger) af planen, hvorved en given regulær polygon går over i sig selv.

Vi skal se, at der pånær isomorfi ikke findes andre cykliske grupper end $(\mathbb{Z}, +)$ og $(\mathbb{Z}_n, +)$, $n = 1, 2, \dots$. Først viser vi det vigtige resultat, at $(\mathbb{Z}, +)$ kun har cykliske undergrupper:

Enhver undergruppe i $(\mathbb{Z}, +)$ er af formen $\{pm \mid p \in \mathbb{Z}\}$, hvor $m \in \mathbb{N}_0$.

Bevis. Undergruppen $\{0\}$ kan skrives $\{p0 \mid p \in \mathbb{Z}\}$. En vilkårlig undergruppe $H \supset \{0\}$ indeholder et tal $n \neq 0$, men dermed også $-n$ og følgelig mindst et positivt tal, nemlig $|n|$. Lad m være den mindste positive tal i H . Enhver "potens" pm , $p \in \mathbb{Z}$, tilhører da H , og skrives et tal $x \in H$ på formen

$$x = qm + r, \quad 0 \leq r < m,$$

må resten $r = x - qm$ tilhøre H og følgelig være 0; altså er $H = \{pm \mid p \in \mathbb{Z}\}$.

Lad atter $(G, \cdot)$ være en vilkårlig gruppe og c et element af G .

Vi bemærker først, at

$$c^p = c^q \iff c^q c^{-p} = e, \quad \text{dvs.} \quad c^p = c^q \iff c^{q-p} = e.$$

Mængden $K = \{n \in \mathbb{Z} \mid c^n = e\}$ af eksponenter n , for hvilke c^n er det neutrale element e af $(G, \cdot)$, er imidlertid en undergruppe af $(\mathbb{Z}, +)$; thi af $c^r = e$ og $c^s = e$ følger jo $c^{r+s} = c^r c^s = e$ og $c^{-r} = (c^r)^{-1} = e$, således at

$$r \in K \wedge s \in K \Rightarrow r + s \in K \quad \text{og} \quad r \in K \Rightarrow -r \in K.$$

Vi har da

$$c^p = c^q \iff q - p \in K,$$

hvor ifølge sætningen ovenfor $K = \{0\}$ eller $K = \{hm \mid h \in \mathbb{Z}\}$ med $m \in \mathbb{N}$, altså:

Enten gælder

$$c^p = c^q \iff p = q,$$

eller der findes et $m \in \mathbb{N}$, så

$$c^p = c^q \iff p \equiv q \pmod{m}.$$

I første tilfælde er alle potenser c^p , $p \in \mathbb{Z}$, indbyrdes forskellige, eller sagt med andre ord, afbildningen $p \rightarrow c^p$, $p \in \mathbb{Z}$, er injektiv.

I sidste tilfælde er afbildningen $p \rightarrow c^p$, $p \in \mathbb{Z}$, periodisk med perioden m , og potenser c^p svarende til m på hinanden følgende eksponenter, f.eks. c , c^2 , ..., $c^m = e$ er indbyrdes forskellige. Tallet m kaldes orden af elementet c i gruppen $(G, \cdot)$. Det er lig med ordenen af den cykliske undergruppe $(C, \cdot) = (\{c^p \mid p \in \mathbb{Z}\}, \cdot)$ frembragt af c ; bemærk også, at

$$m = \min\{n \in \mathbb{N} \mid c^n = e\}.$$

I kraft af potensreglen

$$c^{p+q} = c^p c^q$$

er afbildningen $p \rightarrow c^p$, $p \in \mathbb{Z}$, en homomorf afbildning af $(\mathbb{Z}, +)$ ind i $(G, \cdot)$. Er c ikke af endelig orden, nævnte afbildning altså injektiv, foreligger således en isomorf afbildning af $(\mathbb{Z}, +)$ på den cykliske undergruppe $(C, \cdot) = (\{c^p \mid p \in \mathbb{Z}\}, \cdot)$.

Er c af endelig orden m , fås ved til hver restklasse modulo m at tilordne den fælles værdi af c^p for eksponenter p tilhørende restklassen en injektiv afbildning af $\mathbb{Z}_m$ ind i G . Denne afbildning er i kraft af potensreglen

$$c^{p+q} = c^p c^q$$

en isomorf afbildning af $(\mathbb{Z}_m, +)$ på den cykliske undergruppe $(C, \cdot) = (\{c^p \mid p \in \mathbb{Z}\}, \cdot)$, thi for $p, q \in \mathbb{Z}$ haves jo

$$(p)_m \rightarrow c^p, \quad (q)_m \rightarrow c^q \quad \text{og} \quad (p)_m + (q)_m = (p + q)_m \rightarrow c^{p+q}.$$

Vi noterer specielt:

Enhver cyklisk gruppe er isomorf med en, og naturligvis kun en, af grupperne $(\mathbb{Z}, +)$ og $(\mathbb{Z}_m, +)$, $m = 1, 2, \dots$.

Uendelige cykliske grupper er således indbyrdes isomorfe, ligesom endelige cykliske grupper af samme orden er isomorfe.

Sideklasser.

Idet H er en undergruppe af en gruppe $(G, \cdot)$ og a et element af G , kaldes mængden $\{ah \mid h \in H\}$ den ved a bestemte venstre sideklasse til undergruppen H ; den betegnes aH ,

$$aH = \{ah \mid h \in H\}.$$

Sideklassen aH er således billedet af undergruppen H ved den ved a bestemte venstre translation $x \rightarrow ax$, $x \in G$, (jfr. side 9).

Forskellige gruppeelementer kan bestemme en og samme venstre

sideklasse til en given undergruppe. Om mængden af indbyrdes forskellige venstre sideklasser gælder følgende vigtige sætning:

Mængden $\{xH \mid x \in G\}$ af venstre sideklasser til en undergruppe H af en gruppe $(G, \cdot)$ er en klasseinddeling af G .

Vi beviser sætningen ved at godtgøre, at hvert $x \in G$ tilhører en og kun en venstre sideklasse til H , nemlig xH .

Vi skal da for $x, y \in G$ vise, at

$$x \in xH \quad \text{og} \quad x \in yH \Rightarrow yH = xH.$$

Idet det neutrale element e i $(G, \cdot)$ tilhører H , ses straks, at

$$x = xe \in xH.$$

Antag nu, at $x \in yH$, dvs. $x = yh$, hvor $h \in H$. For $k \in H$ har vi da

$$xk = yhk \in yH,$$

idet jo $hk \in H$; dette viser, at $xH \subseteq yH$. Idet $y = xh^{-1}$, hvor jo $h^{-1} \in H$, er imidlertid også $y \in xH$ og følgelig $yH \subseteq xH$, således at $yH = xH$.

Da de venstre sideklasser til H udgør en klasseinddeling af G , og da den sideklasse, der indeholder et element $x \in G$, kan skrives xH , vil hver af betingelserne

$$xH = yH \quad \text{og} \quad y \in xH$$

være nødvendig og tilstrækkelig for, at de to elementer x og y af G tilhører samme sideklasse. Da endvidere $y \in xH$ vil sige, at y kan skrives $y = xh$ med $h \in H$, hvilket atter er ensbetydende med $x^{-1}y \in H$, har vi:

Idet H er en undergruppe af en gruppe $(G, \cdot)$, vil to elementer x og y af G tilhøre samme venstre sideklasse til H , hvis og kun hvis $x^{-1}y \in H$, ligesom

$$xH = yH \iff x^{-1}y \in H.$$

Den ækvivalensrelation R_v i G , der svarer til klasseinddelingen $\{xH \mid x \in G\}$ af G i venstre sideklasser til H , jfr. I, 5, 17, er således bestemt ved

$$xR_v y \iff x^{-1}y \in H.$$

Bemærk, at den venstre sideklasse til H , som indeholder det neutrale element e i gruppen $(G, \cdot)$, er undergruppen H selv, idet $eoH = H$. En fra H forskellig sideklasse kan ikke være undergruppe af $(G, \cdot)$, idet den ikke indeholder e .

Højre sideklasser til en undergruppe H af en gruppe $(G, \cdot)$ defineres i analogi med venstre sideklasser, ligesom ganske tilsvarende sætninger gælder:

Den ved et element $a \in G$ bestemte højre sideklasse Ha til undergruppen H defineres ved

$$Ha = \{ha \mid h \in H\}.$$

Mængden $\{Hx \mid x \in G\}$ af højre sideklasser til H er en klasseinddeling af G , idet hvert $x \in G$ tilhører en og kun en højre sideklasse til H , nemlig Hx .

To elementer x og y af G tilhører samme højre sideklasse til H , hvis og kun hvis $yx^{-1} \in H$.

$$Hx = Hy \iff yx^{-1} \in H.$$

Ækvivalensrelationen R_h i G , der svarer til klasseinddelingen af G i højre sideklasser til H , er altså bestemt ved

$$xR_h y \iff yx^{-1} \in H.$$

Vi skal senere angive betingelser for, at klasseinddelingerne af en gruppe i venstre, henholdsvis højre sideklasser til en given undergruppe falder sammen. Her skal blot nævnes, at i en kommutativ gruppe er der selvfølgelig ingen anledning til at skelne

For en ordens skyld bemærkes, at for en gruppekomposition betegnet f.eks. med $*$ skrives naturligvis $a * H$ og $H * a$ i stedet for aH og Ha .

Eksempler.

- 1° I gruppen $(V_3, +)$ af geometriske vektorer med sædvanlig vektor-
addition kan en sideklasse til undergruppen V_1 af vektorer pågiv-
en linie l efter valg af et begyndelsespunkt O beskrives som mæng-
den af stedvektorer til punkterne på en linie parallel med l .
Klasseinddelingen af V_3 i sideklasser til V_1 modsvarer altså delin-
gen af rummet E_3 i linier parallelle med l . På samme måde svarer
delingen af V_3 i sideklasser til undergruppen V_2 af vektorer i en
given plan π til delingen af rummet E_3 i planer parallelle med π .
- 2° For hvert $m \in \mathbb{N}$ er sideklasserne til undergruppen $\{pm \mid p \in \mathbb{Z}\}$
af $(\mathbb{Z}, +)$ netop restklasserne modulo m , dvs. elementerne i $\mathbb{Z}_m$.
For hvert $m \in \mathbb{R}_+$ er sideklasserne til undergruppen $\{pm \mid p \in \mathbb{Z}\}$
af $(\mathbb{R}, +)$ netop elementerne i $\mathbb{R}_m$ (jfr. II, 1, 20).
- 3° For gruppen $(S_n, \circ)$ af alle permutationer af en mængde E med
 n elementer falder delingerne i venstre og højre sideklasser til
undergruppen A_n af lige permutationer sammen; foruden A_n selv er
der kun én sideklasse, nemlig mængden af ulige permutationer. Thi
for $p, q \in S_n$ vil $p^{-1} \circ q$ og ligeledes $q \circ p^{-1}$ være lige, hvis og kun
hvis p og q begge er lige eller begge ulige.

På tilsvarende måde ses, at i gruppen af isometrier af rummet
 E_3 , henholdsvis planen E_2 , har undergruppen af flytninger foruden
sig selv kun én sideklasse, nemlig mængden af uegentlige kongru-
enser.

- 4° Lad $(G, \circ)$ være en transformationsgruppe for en mængde E , og

lad H være undergruppen bestående af de transformationer $h \in G$, hvorved et givet element $c \in E$ går over i sig selv. To transformationer $f, g \in G$ vil da tilhøre samme venstre sideklasse til H , netop hvis $f^{-1} \circ g \in H$, dvs. hvis $f^{-1}(g(c)) = c$, eller, hvad der kommer ud på det samme, hvis $f(c) = g(c)$; tilsvarende findes, at f og g tilhører samme højre sideklasse til H , netop hvis $f^{-1}(c) = g^{-1}(c)$. Inddelingen af G i venstre sideklasser til H kan således karakteriseres som delingen efter de mulige billeder af c ved transformationer tilhørende G , inddelingen i højre sideklasser som delingen efter elementer, der kan føres over i c . En sideklasse $f \circ H$ består af de transformationer tilhørende G , ved hvilke c har samme billedelement $f(c)$ som ved f , medens sideklassen $H \circ f$ består af de transformationer tilhørende G , ved hvilke c har samme originalelement $f^{-1}(c)$ som ved f .

Tager man som $(G, \circ)$ gruppen $(S_3, \circ)$ af permutationer af en mængde med 3 elementer eller gruppen af flytninger af planen, fås eksempler, hvor inddelingerne i venstre og højre sideklasser til en undergruppe er forskellige.

Lad atter $(G, \circ)$ være en vilkårlig gruppe og H en undergruppe af G . Da en sideklasse aH er billede af H ved venstre translationen $x \rightarrow ax$, som jo er en injektiv afbildning, idet $ax_1 = ax_2 \Rightarrow x_1 = x_2$, fremgår, at enhver venstre sideklasse til H er ækvipotent med H . Tilsvarende gælder enhver højre sideklasse til H .

Dette resultat har en vigtig konsekvens for grupper af endelig orden. Forudsættes G endelig, og betegnes antallet af elementer af G og H henholdsvis $[G]$ og $[H]$, medens vi skriver $[G:H]$ for antallet af venstre sideklasser til H i $(G, \circ)$, er klasseinddelingen af G i venstre sideklasser til H jo en deling af G i $[G:H]$ klasser, hver med $[H]$ elementer, hvorfor

$$[G:H][H] = [G],$$

Specielt har vi:

Enhver undergruppe af en endelig gruppe har en orden, der er divisor i hele gruppens orden. (E. Lagrange.)

Denne sætning er særdeles nyttig, når man søger undergrupperne af en given endelig gruppe. Da et gruppeelements orden er lig med ordenen af den cykliske undergruppe frembragt af elementet (se side 16), gælder specielt:

I en endelig gruppe er hvert elements orden divisor i gruppens orden.

For en undergruppe H af ^{en} endelig gruppe $(G, \cdot)$ er antallet af venstre og af højre sideklasser det samme, nemlig $[G]/[H]$; thi ovenfor kunne vi lige så godt ræsonnere på højre som på venstre sideklasser. Det fælles antal $[G:H]$ kaldes undergruppens index i $(G, \cdot)$. Uden forudsætning om at G er endelig, kan mængden af venstre og mængden af højre sideklasser til en undergruppe H dog vises at være ækvipotente (se øvelse), og index $[G:H]$ kan derfor defineres generelt som det fælles kardinaltal for de nævnte to klasseinddelinger af G .

Eksempel.

En endelig gruppe $(G, \cdot)$, hvis orden er et primtal, er cyklisk med hvert gruppeelement $c \neq e$ som frembringer. Der er ikke andre undergrupper end $\{e\}$ og G .

Homomorf afbildning. Normal undergruppe. Kvotientgruppe.

Vi sammenstiller først nogle simple resultater vedrørende en homomorf afbildning f af en gruppe $(G, \cdot)$ ind i en gruppe $(G', \cdot)$.

Som man ofte gør, har vi brugt samme betegnelse for de to gruppekombinationer, skønt de i almindelighed vil være forskellige.

Det neutrale element e i $(G, \circ)$ har som billede det neutrale element e' i $(G', \circ)$,

$$f(e) = e',$$

og for $x \in G$ er

$$(f(x))^{-1} = f(x^{-1}).$$

Billedet $f(H)$ af en undergruppe H af $(G, \circ)$ er en undergruppe af $(G', \circ)$, og en sideklasse aH til H i $(G, \circ)$ afbildes på sideklassen $f(a)f(H)$ til $f(H)$ i $(G', \circ)$, ligesom $f(Ha) = f(H)f(a)$.

At $f(e) = e'$ fremgår, efter valg af et element $a \in G$, af ligningen

$$f(e)f(a) = f(ea) = f(a) = e'f(a)$$

ved bortforkortning af $f(a)$; derpå har vi straks

$$f(x)f(x^{-1}) = f(xx^{-1}) = f(e) = e' \quad \text{og} \quad f(x^{-1})f(x) = e'.$$

Er $y_1, y_2 \in f(H)$, altså $y_1 = f(x_1)$ og $y_2 = f(x_2)$, hvor $x_1, x_2 \in H$, har vi nu

$$y_1 y_2 = f(x_1 x_2) \in f(H) \quad \text{og} \quad y_1^{-1} = f(x_1^{-1}) \in f(H),$$

hvilket viser, at $f(H)$ er en undergruppe af $(G', \circ)$, jfr. side 3.

Endelig er eksempelvis

$$f(aH) = \{f(ah) \mid h \in H\} = \{f(a)f(h) \mid h \in H\} = f(a)f(H).$$

Vi fremhæver, at uden forudsætningen om, at $(G', \circ)$ er en gruppe, gælder dog, at $(f(G), \circ)$ er en gruppe, jfr. II, 1, 16-17.

Men er $f: G \rightarrow G'$ ikke surjektiv, kan det da f.eks. forekomme, at $f(e)$, som jo er neutralt element i $(f(G), \circ)$, ikke er det i $(G', \circ)$.

I det følgende undersøges homomorfe afbildninger af grupper nærmere. Herved spiller undergrupper med den særlige egenskab, at de venstre og højre ^{sideklasser} stemmer overens en fremtrædende rolle. En undergruppe $(H, \$)$ i en gruppe $(G, \$)$ siges at være en normal (eller invariant) undergruppe, hvis $x \$ H = H \$ x$ for hvert element $x \in G$.

En undergruppe $(H, \$)$ i en gruppe $(G, \$)$ er normal, hvis og kun hvis

$$\forall_G x \forall_H h [x \$ h \$ x^{-1} \in H].$$

Bevis: Hvis $(H, \$)$ er normal, vil hvert element $x \$ h$ af $x \$ H$ tilhøre $H \$ x$, altså kunne skrives på formen $h' \$ x$,

hvor $h' \in H$. Men af $x \$ h = h' \$ x$ fås

$$x \$ h \$ x^{-1} = h' \in H,$$

hvilket viser betingelsens nødvendighed. Omvendt, lad det være givet, at $x \$ h \$ x^{-1} \in H$ for hvert $x \in G$ og hvert $h \in H$. Til givne x og h findes der da et $h' \in H$, således at $x \$ h \$ x^{-1} = h'$. Heraf fås

$$x \$ h = h' \$ x \in H \$ x,$$

hvilket viser, at hvert element $x \$ h$ af $x \$ H$ er indeholdt i $H \$ x$, altså at $x \$ H \subseteq H \$ x$. Anvendes det givne på x^{-1} i stedet for x , fås $x^{-1} \$ h \$ x \in H$, og heraf sluttes på samme måde, at $H \$ x \subseteq x \$ H$. Dermed er også betingelsens tilstrækkelighed bevist.

I en kommutativ gruppe er alle undergrupper normale.

Lad f være en homomorf afbildning af en gruppe $(G, \$)$ på en gruppe $(G', \$')$, hvis neutrale element betegnes med e' . Originalmængden $K = f^{-1}(e')$, altså mængden af de elementer af G , som ved f har billedet e' , kaldes homomorfiens kerne. Om denne gælder følgende sætning:

Kernen $K = f^{-1}(e')$ ved en homomorf afbildning f af en gruppe $(G, \$)$ på en gruppe $(G', \$')$ med det neutrale element e' er en normal undergruppe i $(G, \$)$.

For hvert element $g' \in G'$ er originalmængden $f^{-1}(g')$ en sideklasse til K , nemlig $g \$ K = K \$ g$, hvor g betegner et element af G , for hvilket $f(g) = g'$. Herved bestemmes en enentydig korrespondance mellem sideklasserne til K og elementerne i G' .

Bevis: Er x og y elementer tilhørende $K = f^{-1}(e')$, altså $f(x) = f(y) = e'$, fås

$$f(x \$ y) = f(x) \$' f(y) = e' \$' e' = e',$$

altså $x \$ y \in K$, og

$$f(x^{-1}) = f(x)^{-1} = e'^{-1} = e',$$

altså $x^{-1} \in K$. Dette viser, at K opfylder betingelserne UG 1 og UG 2 (side II, 2, 5) og er følgelig en undergruppe. Endvidere gælder for hvert element $g \in G$ og hvert element $h \in K$, at

$$\begin{aligned} f(g \$ h \$ g^{-1}) &= f(g) \$' f(h) \$' f(g^{-1}) \\ &= f(g) \$' e' \$' f(g)^{-1} = e', \end{aligned}$$

hvilket viser, at $g \$ h \$ g^{-1} \in K$, og altså at $K = f^{-1}(e')$ er en normal undergruppe i $(G, \$)$. Dermed er sætningens første del bevist.

Idet g_1 og g_2 betegner elementer af G , haves

$$f(g_1 \$ g_2^{-1}) = f(g_1) \$' f(g_2^{-1}) = f(g_1) \$' f(g_2)^{-1},$$

og dette er lig med e' , hvis og kun hvis $f(g_1) = f(g_2)$. Heraf ses, at $g_1 \$ g_2^{-1} \in K$, altså at g_1 og g_2 tilhører samme sideklasse til K (jfr. side II, 2, 9), hvis og kun hvis $f(g_1) = f(g_2)$. Alle elementer i samme sideklasse har altså samme billedelement ved f , og elementer af forskellige sideklasser har forskellige billedelementer. Heraf sluttes rigtigheden af sætningens anden del.

Lad $(G, \S)$ igen være en vilkårlig gruppe og H en normal undergruppe i den. Da inddelingerne i venstre og højre sideklasser til H stemmer overens, vil også de to ved H bestemte ækvivalensrelationer R_v og R_h (side II,2,8-9) stemme overens, d.v.s., at $x^{-1} \S x' \in H$ for to elementer $x, x' \in G$ medfører $x' \S x^{-1} \in H$, og omvendt. Lad $x \sim x'$ betyde, at x står i denne relation til x' . Det skal vises, at denne ækvivalensrelation harmonerer med kompositionsforskriften $\S$ (se side II,1,12), d.v.s. at man af $x \sim x'$ og $y \sim y'$ kan slutte, at $x \S y \sim x' \S y'$. Forudsætningen udsiger, at der findes elementer h og k i H , således at $x^{-1} \S x' = h$ og $y' \S y^{-1} = k$. Man har da

$$(x' \S y') \S (x \S y)^{-1} = x' \S y' \S y^{-1} \S x^{-1} = x \S h \S k \S x^{-1},$$

og den højre side ses at tilhøre H , idet $h \S k \in H$ og H er en normal undergruppe. Men dette betyder, at $x \S y \sim x' \S y'$. Ifølge et tidligere resultat defineres altså ved

$$(x \S H) \P (y \S H) = (x \S y) \S H$$

en kompositionsforskrift i mængden G/H af sideklasser til H , og den naturlige afbildning $\nu: G \rightarrow G/H$, ved hvilken der til hvert element $x \in G$ svarer sideklassen $x \S H$, det er indeholdt i, er en surjektiv homomorfi. Heraf følger, at $(G/H, \P)$ er en gruppe. Den kaldes kvotientgruppen (eller faktorgruppen) af $(G, \S)$ over (eller med hensyn til) den normale undergruppe H . Det er sædvanen at betegne kompositionsforskriften i kvotientgruppen på samme måde som kompositionsforskriften i selve gruppen.

Kernen ved homomorfien $\nu: (G, \S) \rightarrow (G/H, \P)$ er den givne normale undergruppe H ; thi H er det neutrale element i $(G/H, \P)$, og det er netop elementerne i H , som ved ν har billedet H . Enhver normal undergruppe i en gruppe er altså kerne ved en homomorf afbildning af denne. De ved en gruppes normale undergrupper bestemte kvotientgrupper er fra et abstrakt synspunkt de eneste

homomorfe billeder, gruppen kan have. Dette er indholdet af gruppeteoriens homomorfisætning:

Er $(G, \$)$ og $(G', \$')$ grupper, $f : (G, \$) \rightarrow (G', \$')$ en surjektiv homomorfi og $K \subseteq G$ dennes kerne, vil $(G', \$')$ være isomorf med $(G/H, \$)$.

Bevis: Ifølge sætningen om kernen (side II,2,19) fås en bijektiv afbildning af G/H på G' ved til sideklassen $x \$ K$ at lade svare elementet $f(x) = x' \in G'$. (Elementerne i sideklassen har alle det samme billede ved f .) Denne afbildning er en homomorfi, altså en isomorfi, da der til klassen $(x \$ K) \$ (y \$ K) = (x \$ y) \$ K$ svarer $f(x \$ y) = f(x) \$ f(y)$.

Ovenstående sætning om cykliske grupper er et specielt tilfælde af homomorfisætningen.

Som eksempel betragtes gruppen af de egentlige flytninger af rummet, ved hvilke et givet regulært tetraeder $A_1 A_2 A_3 A_4$ afbildes på sig selv. Den kaldes tetraedergruppen og betegnes med T . For hver flytning $f \in T$ vil dens restriktion til mængden $\{A_1, A_2, A_3, A_4\}$ være en permutation af denne mængde. Ved til f at lade svare denne permutation, fås øjensynlig en homomorf afbildning af T ind i S_4 . Denne afbildning er injektiv; thi er f og g flytninger, for hvilke $f(A_i) = g(A_i)$, $i = 1, 2, 3, 4$, vil $g^{-1} \circ f$ have de fire hjørner som fixpunkter og følgelig være den identiske afbildning, hvoraf $f = g$. Tetraedergruppen er altså isomorf med en undergruppe i S_4 . For at bestemme gruppen nærmere bemærkes, at centret C for tetraedrets omskrevne kugle må være fixpunkt ved alle gruppens flytninger, idet det er det eneste punkt i rummet, som har lige store afstande fra tetraedrets hjørner. Hver fra den identiske forskellig flytning tilhørende T må følgelig være en drejning om en akse gennem C .

De drejninger, ved hvilke et af hjørnerne A_i er fixpunkt, må have den fra dette hjørne udgående højde h_i som akse. De udgør en cyklisk gruppe C_3 af ordenen 3, som altså indeholder 2 fra den identiske afbildning e forskellige drejninger. Der findes i T 4 sådanne cykliske undergrupper, som to og to kun har e fælles og følgelig tilsammen indeholder 8 fra e forskellige drejninger. Lad nu $f \in T$ være en drejning, ved hvilken ikke noget hjørne forbliver fast. Antag f.eks., at $f(A_1) = A_2$. Drejningsaksen må da være vinkelret på linien A_1A_2 . Var nu $f(A_2) \neq A_1$, altså f.eks. $f(A_2) = A_3$, måtte den også være vinkelret på linien A_2A_3 , altså på trekanten $A_1A_2A_3$. Endvidere måtte den gå gennem denne trekants omskrevne cirkels centrum og altså være h_4 , hvilket ville være i strid med $f(A_4) \neq A_4$. Følgelig er $f(A_2) = A_1$. Hjørnerne A_1 og A_2 ombyttes altså ved f , og det samme gælder for A_3 og A_4 . Drejningsaksen må være forbindelseslinien mellem midtpunkterne af de to modstående kanter A_1A_2 og A_3A_4 , og drejningsvinklen må være lig med π . Idet der findes tre linier, der forbinder modstående kanters midtpunkter, indeholder T foruden e og de 8 nævnte drejninger 3 drejninger, der hver frembringer en cyklisk undergruppe af ordenen 2. Tetraedergruppen T har altså ordenen 12. Idet de til dens flytninger svarende permutationer alle er lige, er T isomorf med den alternerende gruppe A_4 . (Den regulære fremstilling af T er en undergruppe i S_{12} .)

Lad m_1 , m_2 og m_3 betegne linierne, som hver forbinder to modstående kanters midtpunkter. Ved hver flytning tilhørende T permuteres disse linier. Ved til flytningen at lade svare denne permutation fås en homomorf afbildning af T ind i S_3 . Kernen består af de flytninger, ved hvilke hver af de tre linier afbildes på sig selv, altså foruden af e af de tre nævnte drej-

ninger med drejningsvinklen π om m_1 , m_2 og m_3 . Denne gruppe af ordenen 4 (som ikke er isomorf med den cykliske gruppe af ordenen 4) kaldes firgruppen og betegnes med V (fra tysk "Vierergruppe") eller med D_2 . Kvotientgruppen T/V har ordenen 3 og ses let at være isomorf med A_3 , der (som enhver gruppe af ordenen 3) igen er isomorf med den cykliske gruppe af denne orden. Firgruppen er den eneste fra $\{e\}$ og T forskellige normale undergruppe i T . Dette kan indses på følgende måde: Lad $d \in T$ betegne en fra e forskellig drejning og a dennes akse. For hvert punkt $A \in a$ er da $d(A) = A$. Er nu f en vilkårlig flytning tilhørende T , har man altså

$$f \circ d \circ f^{-1}(f(A)) = f \circ d(A) = f(d(A)) = f(A),$$

hvilket viser, at $d_f = f \circ d \circ f^{-1} \neq e$ har punkterne på linien $f(a)$ som fixpunkter og er følgelig en drejning om denne linie. Er $H \subseteq T$ en normal undergruppe, kan man af $d \in H$ slutte, at $d_f \in H$ (ifølge sætningen på side II,2,18). Bemærkes nu, at der for hvilket som helst højder h_i og h_j findes en flytning $f \in T$, for hvilken $f(h_i) = h_j$, ses, at hvis H indeholder en af drejningerne d , og dermed også d^2 , af ordenen 3, må alle 8 drejninger af denne orden tilhøre H . Da 12 ikke har nogen ægte divisor større end 8, må H være hele gruppen T . En tilsvarende betragtning viser, at hvis en normal undergruppe indeholder en af drejningerne af ordenen 2, indeholder den alle 3, altså V . Da den ifølge det viste må være identisk med T , hvis den indeholder andre elementer, er påstanden bevist.

Gruppen af alle isometrier (egentlige og uegentlige flytninger) af rummet, ved hvilke tetraædret $A_1 A_2 A_3 A_4$ afbildes på sig selv, kaldes den udvidede tetraædergruppe og betegnes med T_d . Sådanne isometrier er bl.a. spejlingerne i de 6 "diagonalplaner", som hver forbinder en kant med den modstående kants midtpunkt.

Spejlingernes restriktioner til $\{A_1, A_2, A_3, A_4\}$ er denne mængdes transpositioner. Alle permutationer af hjørnerne kan altså fås som restriktioner af passende sammensætninger af disse spejlinger. Da på den anden side to forskellige isometrier ikke kan fremkalde den samme permutation, ses, at T_d er isomorf med S_4 , altså af ordenen 24. Foruden T og de nævnte spejlinger indeholder T_d 6 såkaldte drejspejlinger, som hver kan tænkes sammensat af en drejning med drejningsvinklen $\frac{1}{2}\pi$ (til den ene eller den anden side) om en af linierne m_i og en spejling i dennes normalplan gennem C .

At $[T_d] = 2[T]$, kan også slutes af en almindelig sætning om grupper af isometrier (af rummet, en plan eller en linie):
Er $(G, \circ)$ en gruppe af egentlige og uegentlige flytninger, vil de i G indeholdte egentlige flytninger udgøre en undergruppe af index 2. Lad $u_0 \in G$ være en fast uegentlig flytning og F mængden af egentlige flytninger i G , som udgør en undergruppe, da jo sammensætninger af og inverse til egentlige flytninger igen er egentlige flytninger. For hver uegentlig flytning u er da $u_0^{-1} \circ u$ en egentlig flytning f , altså $u = u_0 \circ f$ indeholdt i sideklassen $u_0 \circ F$. Der kan altså ikke findes andre sideklasser end F og $u_0 \circ F$. (Det ses, at $u_0 \circ F$ må tillige være højre sideklasse.
 Alment: Enhver undergruppe af index 2 er normal.)

§ 3. Ringe og legemer.Ring, integritetsring og legeme.

Lad $*$ og $\S$ være kompositioner inden for samme mængde M . Som betegnelse for M betragtet med kompositionerne $*$ og $\S$ eller, som man siger, for mængden M organiseret ved kompositionerne $*$ og $\S$, benyttes $(M, *, \S)$.

Man siger, at $\S$ er distributiv med hensyn til $*$, hvis de distributive love

$$x \S (y * z) = (x \S y) * (x \S z)$$

og
$$(y * z) \S x = (y \S x) * (z \S x)$$

gælder for $x, y, z \in M$. I tilfælde af at $\S$ er kommutativ, kommer de to love naturligvis ud på et.

Eksempler.

1° For tal er sædvanlig multiplikation distributiv med hensyn til sædvanlig addition, men ikke omvendt.

2° For geometriske vektorer er vektorproduktet distributivt med hensyn til vektoradditionen, men ikke omvendt.

3° For mængder er hver af kompositionerne $\cap$ og $\cup$ distributiv med hensyn til den anden.

I de fleste tilfælde, der er af betydning for os, vil forholdene være som i 1° og 2°. Den komposition, som er distributiv med hensyn til den anden, kalder man da gerne en multiplikation, den anden en addition; som betegnelse for kompositionerne benyttes sædvanligt multiplikations- og plustegn, $\cdot$ og $+$, medmindre dette kan give anledning til misforståelser (jfr. eks. 2°); fra talregning overføres endvidere tilvante skrivemåder: antallet

af nødvendige parenteser reduceres ved vedtægten, at multiplikation går forud for addition, og man tillader sig at udelade tegnet " $\cdot$ ". De distributive love antager da det velkendte udseende

$$x(y + z) = xy + xz, \quad (y + z)x = yx + zx.$$

En mængde M organiseret ved to kompositioner $+$ og $\cdot$ inden for M kaldes en ring, hvis additionen $+$ er en kommutativ gruppekomposition (II,1,7), hvis multiplikationen $\cdot$ er associativ, og hvis de distributive love

$$x(y + z) = xy + zx \quad \text{og} \quad (y + z)x = yx + zx$$

gælder for $x, y, z \in M$.

Er tillige multiplikationen kommutativ, siges $(M, +, \cdot)$ at være en kommutativ ring.

I en ring $(M, +, \cdot)$ kaldes det neutrale element ved additionen for ringens nulelement og betegnes oftest med 0 . Det inverse til et element $a \in M$ kaldes det modsatte element til a og betegnes $-a$. Da additionen er kommutativ, er ligningerne $a + x = b$ og $x + a = b$ ensbetydende; løsningen (jfr. II,1,7) betegnes $b - a$. Idet

$$b - a = b + (-a),$$

kan vi uden mulighed for misforståelse bruge korte skrivemåder som f.eks. $-a + b - c$ i stedet for $(-a) + b + (-c)$.

I kraft af de distributive love spiller nulelementet en særlig rolle også ved multiplikationen: for $x \in M$ gælder

$$0x = x0 = 0.$$

Vælges et element $a \in M$, f.eks. $a = 0$, har vi nemlig $a + 0 = a$ og dermed $(a + 0)x = ax$, dvs. $ax + 0x = ax$, hvilket viser, at $0x = ax - ax = 0$. På tilsvarende måde indses $x0 = 0$.

Ved fornyet anvendelse af de distributive love fås, at der for $x, y \in M$ gælder

$$x(-y) = -xy \quad \text{og} \quad (-x)y = -xy.$$

Den første regel følger af

$$xy + x(-y) = x(y + (-y)) = x0 = 0,$$

den anden indses på tilsvarende måde. Ved brug af de to regler fås videre for $x, y \in M$

$$(-x)(-y) = xy.$$

Vi nævner yderligere reglerne

$$x(y - z) = xy - xz \quad \text{og} \quad (y - z)x = yx - zx.$$

Den første fremgår af regningen

$$x(y - z) = x(y + (-z)) = xy + x(-z) = xy + (-xz) = xy - xz,$$

den anden fås analogt.

Man kan i det hele taget "gange parenteser ud" ligesom for tal, f.eks,

$$(v + x)(y - z) = vy + xy - vz - xz.$$

Medmindre multiplikationen er kommutativ, må man dog ved en sådan udregning huske i produkterne på højre side at tage faktoren fra den første parentes først.

I en ring $(M, +, \cdot)$ er, som vist ovenfor, et produkt 0, når en af faktorerne er 0,

$$x = 0 \quad \vee \quad y = 0 \quad \Rightarrow \quad xy = 0.$$

Derimod gælder ikke i almindelighed det omvendte, nulreglen

$$xy = 0 \quad \Rightarrow \quad x = 0 \quad \vee \quad y = 0,$$

der også kan skrives

$$x \neq 0 \quad \wedge \quad y \neq 0 \quad \Rightarrow \quad xy \neq 0.$$

Idet elementer $x \neq 0$ og $y \neq 0$ med produkt $xy = 0$ begge kaldes

nuldivisorer, kommer nulreglens gyldighed i en ring ud på, at ringen ikke har nuldivisorer.

Nulreglens gyldighed i en ring $(M, +, \cdot)$ er nødvendig og tilstrækkelig for, at forkortningsreglen

$$ax = ay \quad \wedge \quad a \neq 0 \quad \Rightarrow \quad x = y$$

gælder for $a, x, y \in M$.

Skrevet på formen

$$ax = 0 \quad \wedge \quad a \neq 0 \quad \Rightarrow \quad x = 0$$

ses nulreglen nemlig at være et specialtilfælde af forkortningsreglen, svarende til $y = 0$. Omvendt er forkortningsreglen ensbetydende med

$$a(x - y) = 0 \quad \wedge \quad a \neq 0 \quad \Rightarrow \quad x - y = 0$$

og dermed en følge af nulreglen. På tilsvarende måde indses:

Nulreglens gyldighed i en ring $(M, +, \cdot)$ er nødvendig og tilstrækkelig for, at forkortningsreglen

$$xa = ya \quad \wedge \quad a \neq 0 \quad \Rightarrow \quad x = y$$

gælder for $a, x, y \in M$.

Et eventuelt neutralt element ved multiplikationen i en ring $(M, +, \cdot)$ kaldes ringens etelement. Findes et sådant, kaldes det inverse til et ved multiplikationen regulært element $a \in M$ for det reciprokke element til a og betegnes a^{-1} .

Bortset fra det tilfælde, at M kun har ét element, altså $M = \{0\}$, er nulelementet 0 ikke samtidig etelement, og det har intet reciprok.

En kommutativ ring $(M, +, \cdot)$ med etelement $e \neq 0$, hvor nulreglen

$$x \neq 0 \wedge y \neq 0 \Rightarrow xy \neq 0$$

gælder for $x, y \in M$, kaldes en integritetsring (integritetsområde).

En ring $(M, +, \cdot)$ med etelement $e \neq 0$, hvor ethvert fra 0 forskelligt element af M er regulært ved multiplikationen, kaldes et legeme.

Er $(M, +, \cdot)$ et legeme, da har hver af ligningerne

$$ax = b \quad \text{og} \quad xa = b$$

for vilkårlige elementer $a \neq 0$ og b af M netop én løsning, nemlig henholdsvis $a^{-1}b$ og ba^{-1} , jfr. side II, 1, 7. Specielt gælder forkortningsreglerne

$$ax = ay \wedge a \neq 0 \Rightarrow x = y, \quad xa = ya \wedge a \neq 0 \Rightarrow x = y$$

og dermed nulreglen. Inden for $M \setminus \{0\}$ er multiplikationen en gruppekomposition.

Man bemærker, at ethvert kommutativt legeme er en integritetsring.

Eksempler.

1° $(\mathbb{Z}, +, \cdot)$ er en integritetsring, $(\mathbb{Q}, +, \cdot)$ og $(\mathbb{R}, +, \cdot)$ er kommutative legemer. Begreberne integritetsring og legeme er dannet med disse eksempler som forbillede.

2° Mængden $\{2n \mid n \in \mathbb{Z}\}$ af lige hele tal er med sædvanlig addition og multiplikation en kommutativ ring uden etelement, i hvilken nulreglen gælder.

3° Mængden $\mathbb{R}^2$ af par af reelle tal med kompositioner defineret ved

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2),$$

$$(x_1, x_2)(y_1, y_2) = (x_1 y_1, x_2 y_2),$$

hvor $+$ og $\cdot$ på højre side står for sædvanlig addition og multi-

plikation, er en kommutativ ring. Nulelementet er $(0,0)$, det modsatte element til (x_1, x_2) er $(-x_1, -x_2)$. Ringen har et etelement, $(1,1)$, men da der er nuldivisorer, nemlig alle elementer $(x_1, 0)$, $x_1 \neq 0$ og $(0, x_2)$, $x_2 \neq 0$, er det ikke en integritetsring og følgelig heller ikke et legeme. Talparrene (x_1, x_2) , hvor x_1 og x_2 begge er forskellige fra 0, er de regulære elementer ved multiplikationen.

4° Idet $(M, +, \cdot)$ er en ring, L en vilkårlig, ikke tom mængde, indføres på nærliggende måde kompositioner inden for mængden $\hat{F}(L \rightarrow M)$ af funktioner fra L til M : for f og g tilhørende $\hat{F}(L \rightarrow M)$ forstås ved $f + g$, henholdsvis fg afbildningerne

$$t \rightarrow f(t) + g(t), \quad t \in L, \quad \text{og} \quad t \rightarrow f(t)g(t), \quad t \in L.$$

Man verificerer umiddelbart, at $(\hat{F}(L \rightarrow M), +, \cdot)$ er en ring, kommutativ hvis $(M, +, \cdot)$ er kommutativ. Nulelementet er den konstante afbildning $t \rightarrow 0$, $t \in L$; det modsatte element $-f$ til f er afbildningen $t \rightarrow -f(t)$, $t \in L$. Hvis $(M, +, \cdot)$ har et etelement e , vil $t \rightarrow e$, $t \in L$, være etelement i ringen $(\hat{F}(L \rightarrow M), +, \cdot)$ af funktioner.

Har L mere end et element, vil $(\hat{F}(L \rightarrow M), +, \cdot)$ have nuldivisorer; er $(M, +, \cdot)$ et integritetsområde eller et legeme, vil nuldivisorerne i $(\hat{F}(L \rightarrow M), +, \cdot)$ være de funktioner, som antager værdien 0 uden at være identisk 0. Er $(M, +, \cdot)$ et legeme, vil de ved multiplikationen i $\hat{F}(L \rightarrow M)$ regulære elementer være de funktioner, der ikke antager værdien 0.

Som et vigtigt tilfælde fremhæves addition og multiplikation af reelle funktioner, svarende til $(M, +, \cdot) = (\mathbb{R}, +, \cdot)$. Herunder hører også addition og multiplikation af reelle talsæt og talfølger, idet et talsæt $(x_1, \dots, x_n)$ kan opfattes som en afbild-

ning af $\{1, \dots, n\}$ ind i $\mathbb{R}$, medens en talfølge $(x_1, x_2, \dots)$ er en afbildning af $\mathbb{N}$ ind i $\mathbb{R}$. For talfølger kan definitionen af addition og multiplikation skrives

$$(x_1, x_2, \dots) + (y_1, y_2, \dots) = (x_1 + y_1, x_2 + y_2, \dots),$$

$$(x_1, x_2, \dots)(y_1, y_2, \dots) = (x_1 y_1, x_2 y_2, \dots),$$

for talsæt er tilfældet $n = 2$ omtalt ovenfor (eks. 2°).

Vi vil senere møde eksempler på ringe, der ikke er kommutative (III, §2). I Matematik 2, algebra og talteori, nævnes et ikke kommutativt legeme.

Isomorfi.

Lad $+$ og $\cdot$ være kompositioner inden for en mængde L , medens $*$ og $\S$ er kompositioner inden for en mængde M .

En enentydig korrespondance mellem L og M siges da at være en isomorfi mellem $(L, +, \cdot)$ og $(M, *, \S)$, hvis der for $x_1, x_2 \in L$ og $y_1, y_2 \in M$ gælder

$$x_1 \leftrightarrow y_1 \quad \wedge \quad x_2 \leftrightarrow y_2 \quad \Rightarrow \quad x_1 + x_2 \leftrightarrow y_1 * y_2$$

$$\text{og} \quad x_1 \leftrightarrow y_1 \quad \wedge \quad x_2 \leftrightarrow y_2 \quad \Rightarrow \quad x_1 x_2 \leftrightarrow y_1 \S y_2,$$

altså hvis korrespondancen er en isomorfi såvel mellem $(L, +)$ og $(M, *)$ som mellem $(L, \cdot)$ og $(M, \S)$.

Findes der en isomorfi mellem $(L, +, \cdot)$ og $(M, *, \S)$, siges de to organiserede mængder at være isomorfe.

I så fald finder naturligvis bemærkningerne side II, 1, 11 anvendelse på kompositionerne $+$ og $*$, såvel som på $\cdot$ og $\S$. Yderligere verificeres umiddelbart, at hvis $\cdot$ er distributiv med hensyn til $+$, så er også $\S$ distributiv med hensyn til $*$, og

omvendt. Er en af de organiserede mængder $(L, +, \cdot)$ og $(M, *, \S)$ en ring, så er den anden det også, og ved enhver isomorfi mellem dem vil nulelement svare til nulelement, nuldivisorer til nuldivisorer, et eventuelt etelement i den ene ring vil svare til etelement i den anden, regulære elementer ved en af kompositionerne $\cdot$ og $\S$ til regulære elementer ved den anden. Er en af de isomorfe, organiserede mængder $(L, +, \cdot)$ og $(M, *, \S)$ en integritetsring, henholdsvis et legeme, så er den anden det også.

En bijektiv afbildning $f: L \rightarrow M$, hvor for $x_1, x_2 \in L$ gælder $f(x_1 + x_2) = f(x_1) * f(x_2)$ og $f(x_1 x_2) = f(x_1) \S f(x_2)$, kaldes en isomorf afbildning af $(L, +, \cdot)$ på $(M, *, \S)$. Det kommer ud på et at betragte isomorfier mellem $(L, +, \cdot)$ og $(M, *, \S)$ eller isomorfe afbildninger af $(L, +, \cdot)$ på $(M, *, \S)$, jfr. side II, 1, 12. Specielt kan man som definition på, at $(L, +, \cdot)$ er isomorf med $(M, *, \S)$ benytte, at der findes en isomorf afbildning af $(L, +, \cdot)$ på $(M, *, \S)$.

Er f en isomorf afbildning af $(L, +, \cdot)$ på $(M, *, \S)$, vil den omvendte afbildning f^{-1} være en isomorf afbildning af $(M, *, \S)$ på $(L, +, \cdot)$, jfr. side II, 1, 12. Også sammensætning af isomorfe afbildninger fører igen til en isomorf afbildning, jfr. side II, 1, 13. Herved fås:

Relationen " $(L, +, \cdot)$ er isomorf med $(M, *, \S)$ " er en ækvivalensrelation i klassen af alle ved to kompositioner organiserede mængder.

Som et malende udtryk for overensstemmelsen benytter man undertiden vendingen, at $(L, +, \cdot)$ og $(M, *, \S)$ er "eksemplarer af samme dobbelt organiserede mængde", i stedet for at sige, at de

er isomorfe.

De komplekse tal.

De komplekse tal kan indføres som mængden $\mathbb{R}^2$ af par af reelle tal med kompositionerne

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2),$$

$$(x_1, x_2)(y_1, y_2) = (x_1 y_1 - x_2 y_2, x_1 y_2 + x_2 y_1).$$

Vi vil først gøre rede for, at $\mathbb{R}^2$ med denne addition og multiplikation er et kommutativt legeme:

Additionen er den samme som i eks. 3^o, side 5; det er en kommutativ gruppekomposition med $(0,0)$ som neutralt element. Det ses straks, at multiplikationen er kommutativ; den er også associativ, idet

$$\begin{aligned} [(x_1, x_2)(y_1, y_2)](z_1, z_2) &= (x_1 y_1 - x_2 y_2, x_1 y_2 + x_2 y_1)(z_1, z_2) \\ &= ((x_1 y_1 - x_2 y_2)z_1 - (x_1 y_2 + x_2 y_1)z_2, (x_1 y_1 - x_2 y_2)z_2 + (x_1 y_2 + x_2 y_1)z_1) \end{aligned}$$

$$\begin{aligned} \text{og} \quad (x_1, x_2)[(y_1, y_2)(z_1, z_2)] &= (x_1, x_2)(y_1 z_1 - y_2 z_2, y_1 z_2 + y_2 z_1) \\ &= (x_1(y_1 z_1 - y_2 z_2) - x_2(y_1 z_2 + y_2 z_1), x_1(y_1 z_2 + y_2 z_1) + x_2(y_1 z_1 - y_2 z_2)) \end{aligned}$$

stemmer overens. Ved udregning bekræftes ligeledes, at multiplikationen er distributiv med hensyn til additionen. Hermed er vist, at $\mathbb{R}^2$ med de betragtede kompositioner er en kommutativ ring.

Idet $(1,0)$ ses at være neutralt ved multiplikationen, dvs. etelement, mangler vi at godtgøre, at der til et vilkårligt par $(a_1, a_2) \neq (0,0)$ findes et reciprok, altså et par (x_1, x_2) således at $(a_1, a_2)(x_1, x_2) = (1,0)$, dvs.

$$a_1 x_1 - a_2 x_2 = 1$$

$$a_2 x_1 + a_1 x_2 = 0;$$

for $a_1^2 + a_2^2 \neq 0$ har dette ligningssystem imidlertid virkelig en løsning.

Vi betragter dernæst kompositionerne anvendt på par af formen $(x, 0)$, $x \in \mathbb{R}$:

$$(x, 0) + (y, 0) = (x+y, 0), \quad (x, 0)(y, 0) = (xy, 0).$$

Man ser, at det er kompositioner inden for $\{(x, 0) \mid x \in \mathbb{R}\}$, hvilken mængde vi for kortheds skyld vil betegne $\mathbb{R}'$, og at afbildningen $x \rightarrow (x, 0)$, $x \in \mathbb{R}$, er en isomorf afbildning af $(\mathbb{R}, +, \cdot)$ på $(\mathbb{R}', +, \cdot)$, således at $(\mathbb{R}', +, \cdot)$ blot er et nyt eksemplar af de reelle tals legeme.

Betegner vi endelig med i parret $(0, 1)$, har vi dels $i^2 = -(1, 0)$, dels er for et vilkårligt par (x_1, x_2)

$$(x_1, x_2) = (x_1, 0) + i(x_2, 0),$$

i hvilken fremstilling $(x_1, 0)$ og $(x_2, 0)$ naturligvis ikke kan erstattes af andre elementer af $\mathbb{R}'$.

Vi opsummerer det væsentlige: Der findes et kommutativt legeme $(\mathbb{C}, +, \cdot)$, som indeholder et eksemplar $(\mathbb{R}, +, \cdot)$ af de reelle tals legeme samt et element i med $i^2 = -1$, således at ethvert $z \in \mathbb{C}$ har en og kun én fremstilling af formen

$$z = z_1 + iz_2, \quad z_1, z_2 \in \mathbb{R}.$$

Et sådant legeme kaldes (et eksemplar af) de komplekse tals legeme og betegnes $(\mathbb{C}, +, \cdot)$, dets elementer kaldes komplekse tal.

Efter eksistensbevisets afslutning er der, når talen er om komplekse tal, ingen fordel ved specielt at tænke på det under beviset konstruerede eksemplar; mere anbefalelsesværdigt er det

at tage sit udgangspunkt i de komplekse tals ovenfor opsummerede egenskaber. I opsummeringen nævnes kun ét eksemplar af de reelle tals legeme, hvorfor vi har skrevet $\mathbb{R}$ og ikke $\mathbb{R}'$; med 1 menes naturligvis etelementet.

Ved undersøgelser vedrørende reelle tal er det i øvrigt ofte nyttigt at tænke på et eksemplar, der på den beskrevne måde indgår i de komplekse tals legeme. Dette gør man i praksis uden kommentar, så snart der er behov for det; tilsvarende skrives $\mathbb{R} \subseteq \mathbb{C}$.

Eksempler.

1° Mellem mængden $\mathbb{C}$ af komplekse tal z og mængden $\mathbb{R}^2$ af reelle talpar (z_1, z_2) bestemmes ved

$$z = z_1 + iz_2$$

en enentydig korrespondance, hvorfor de komplekse tal ved hjælp af et sædvanligt retvinklet koordinatsystem kan repræsenteres ved punkterne i en plan. De reelle tal z_1 og z_2 kaldes den reelle, henholdsvis imaginære del af det komplekse tal $z = z_1 + iz_2$. - Det er klart, at man her tænker på reelle tal indeholdt i $\mathbb{C}$; ellers har jo $z_1 + iz_2$ ingen mening.

Omregner man

$$(x_1 + ix_2) + (y_1 + iy_2) \quad \text{og} \quad (x_1 + ix_2)(y_1 + iy_2)$$

til formen $z_1 + iz_2$, vil det tydeligt fremgå, hvorledes man har fået ideen til kompositionerne side 9.

2° Idet $(-i)^2 = -1$ og ethvert $z \in \mathbb{C}$ har en og kun én fremstilling af formen $z = z_1 + (-i)z_2$, $z_1, z_2 \in \mathbb{R}$, er de to rødder i ligningen $x^2 = -1$ i virkeligheden ganske ligeberettigede til betegnelsen i ; man må blot tænke sig et valg truffet.

3° Det kan vises, at der kun findes én isomorfi mellem to eksemplarer af de reelle tals legeme, eller, hvad der kommer ud på det samme, kun én automorfi for (et eksemplar af) de reelle tals legeme, nemlig identiteten. For de komplekse tals legeme er derimod ud over identiteten også den enentydige korrespondance

$$z = z_1 + iz_2 \leftrightarrow \bar{z} = z_1 - iz_2, \quad z_1, z_2 \in \mathbb{R},$$

en automorfi.

Vi understreger, at for konstruktionen ovenfor af (et eksemplar af) de komplekse tals legeme var det en forudsætning, at vi på forhånd rådede over (et eksemplar af) de reelle tals legeme. Ved kurserne Matematik 2 og 3 vil det blive vist, hvorledes (et eksemplar af) de reelle tal kan konstrueres ud fra (et eksemplar af) de rationale tal, de rationale ud fra de hele tal, de hele ud fra de naturlige tal. Af disse successive udvidelser af talsystemet fra de naturlige til de komplekse tal er skridtet fra de reelle til de komplekse tal det simpleste.

Homomorf afbildning.

Lad $+$ og $\cdot$ være kompositioner inden for en mængde L , medens $*$ og $\S$ er kompositioner inden for en mængde M .

En afbildning $f:L \rightarrow M$ siges da at være en homomorf afbildning af $(L, +, \cdot)$ ind i $(M, *, \S)$, hvis der for $x_1, x_2 \in L$ gælder

$$f(x_1 + x_2) = f(x_1) * f(x_2) \quad \text{og} \quad f(x_1 x_2) = f(x_1) \S f(x_2),$$

altså hvis f er en homomorf afbildning såvel af $(L, +)$ ind i $(M, *)$ som af $(L, \cdot)$ ind i $(M, \S)$. Hvis $f:L \rightarrow M$ tillige er bijektiv, er f en isomorf afbildning af $(L, +, \cdot)$ på $(M, *, \S)$, jfr. side 8.

I det følgende antages, at $f: L \rightarrow M$ er surjektiv samt homomorf. Idet L betragtes med kompositionerne $+$ og $\cdot$, M med kompositionerne $*$ og $\S$.

Sætningerne side II, 1, 15-16 kan da anvendes på kompositionerne $+$ og $*$, samt ligeledes på $\cdot$ og $\S$. Yderligere haves:

Hvis $\cdot$ er distributiv med hensyn til $+$, så er også $\S$ distributiv med hensyn til $*$.

Bevis: Lad y_1, y_2 og y_3 være vilkårlige elementer af M . Da f er surjektiv, kan vi tænke os $x_1, x_2, x_3 \in L$ valgt, så

$$f(x_1) = y_1, \quad f(x_2) = y_2 \quad \text{og} \quad f(x_3) = y_3.$$

Idet f er homomorf, har vi nu

$$y_1 \S (y_2 * y_3) = f(x_1(x_2 + x_3))$$

$$\text{og} \quad (y_1 \S y_2) * (y_1 \S y_3) = f(x_1 x_2 + x_1 x_3).$$

$$\text{hvorfor} \quad x_1(x_2 + x_3) = x_1 x_2 + x_1 x_3$$

$$\text{medfører} \quad y_1 \S (y_2 * y_3) = (y_1 \S y_2) * (y_1 \S y_3).$$

Tilsvarende behandles den anden distributive lov.

Af det ovenfor sagte fremgår specielt:

Hvis $(L, +, \cdot)$ er en (kommutativ) ring, så er også $(M, *, \S)$ en (kommutativ) ring. Nulelementet o_L i ringen $(L, +, \cdot)$ afbildes da i nulelementet o_M i $(M, *, \S)$, og for $x \in L$ er $f(-x)$ det modsatte element til $f(x)$. Et eventuelt etelement i $(L, +, \cdot)$ afbildes i etelement i $(M, *, \S)$; er $x \in L$ regulær ved $\cdot$, så er $f(x)$ regulær ved $\S$, og $f(x^{-1})$ er det reciprokke element til $f(x)$.

Selv om vi ser bort fra tilfældet, hvor $M = f(L)$ kun har ét element, kan $(L, +, \cdot)$ derimod være en integritetsring, uden at $(M, *, \S)$ er det (se side 16-17); at nulreglen gælder for $(L, +, \cdot)$, sikrer nemlig ikke, at dette også er tilfældet for $(M, *, \S)$. På

den anden side kan ringen $(L, +, \cdot)$ have nuldivisorer, uden at $(M, *, \S)$ har det (jfr. eksemplet nedenfor).

Er $(L, +, \cdot)$ et legeme, må f være en isomorf afbildning af $(L, +, \cdot)$ på $(M, *, \S)$, medmindre $M = f(L)$ kun har ét element, o_M . Thi er f ikke injektiv, findes jo elementer $a_1 \neq a_2$ tilhørende L , således at $f(a_1) = f(a_2)$, dvs. $f(a_1 - a_2) = o_M$; idet vi sætter $a = a_1 - a_2$, har vi $a \neq o_L$ og $f(a) = o_M$. For ethvert $b \in L$ findes nu et $x \in L$, så $ax = b$, hvorfor

$$f(b) = f(ax) = f(a) \S f(x) = o_M \S f(x) = o_M.$$

Vi understreger, at det er væsentligt for resultaterne ovenfor, at $f: L \rightarrow M$ ikke blot er en homomorf afbildning af $(L, +, \cdot)$ ind i $(M, *, \S)$, men tillige er antaget surjektiv. Udledes sidstnævnte forudsætning, må man overalt erstatte $(M, *, \S)$ med billedmængden $f(L)$ betragtet med restriktionerne af de to kompositioner $*$ og $\S$, jfr. side II, 1, 16.

Eksempel.

Projektionen $\text{pr}_1: \mathbb{R}^2 \rightarrow \mathbb{R}$, bestemt ved $(x_1, x_2) \rightarrow x_1$, er homomorf, når $\mathbb{R}^2$ betragtes med de side 5, eks. 3^o indførte kompositioner $+$ og $\cdot$, medens $\mathbb{R}$ betragtes med sædvanlig addition og multiplikation. Her afbildes således en ring med nuldivisorer surjektivt og homomorft på et legeme.

Lad nu $+$ og $\cdot$ være kompositioner inden for en mængde L , og lad $\sim$ være en ækvivalensrelation i samme mængde. Vi betegner med $\bar{L}$ mængden af ækvivalensklasser, med K_x klassen repræsenteret af et element $x \in L$.

Vi forudsætter, at $\sim$ harmonerer både med $+$ og med $\cdot$, jfr.

side II,1,18, således at der inden for $\tilde{L}$ bestemmes kompositioner $\tilde{+}$ og $\tilde{\cdot}$ ved betingelserne

$$\forall_{L,x,y}: K_x \tilde{+} K_y = K_{x+y} \quad \text{og} \quad \forall_{L,x,y}: K_x \tilde{\cdot} K_y = K_{xy}.$$

Idet disse betingelser netop udtrykker, at den naturlige afbildning $x \rightarrow K_x$, $x \in L$, af L på $\tilde{L}$ er en homomorf afbildning af $(L, +, \cdot)$ på $(\tilde{L}, \tilde{+}, \tilde{\cdot})$, kan resultaterne ovenfor anvendes. Eksempelvis vil $(\tilde{L}, \tilde{+}, \tilde{\cdot})$ være en (kommutativ) ring, hvis $(L, +, \cdot)$ er det.

Overgangen fra $(L, +, \cdot)$ til $(\tilde{L}, \tilde{+}, \tilde{\cdot})$ kan siges at bestå i, at man ophører med at skelne mellem indbyrdes ækvivalente elementer i M .

Vi nævner sluttelig, at sammensætning af homomorfe afbildninger naturligvis igen fører til en homomorf afbildning, også når talen er om mængder med to kompositioner.

Restklassering og restklasselegeme.

Vi minder om en række definitioner og resultater, i det væsentlige fra eks. 2°, side II,1,20-21.

Idet x_1 og x_2 er hele tal og m et positivt helt tal, siges x_1 at være kongruent med x_2 modulo m , i symboler

$$x_1 \equiv x_2 \pmod{m},$$

hvis m går op i $x_2 - x_1$, altså

$$x_1 \equiv x_2 \pmod{m} \iff m \mid x_2 - x_1.$$

I det følgende tænkes m fastholdt.

Relationen udtrykt ved $x_1 \equiv x_2 \pmod{m}$ er da en ækvivalensrelation i $\mathbb{Z}$, kaldet kongruens modulo m . For ækvivalensklassen $(x)_m$ repræsenteret af tallet x har vi

$$(x)_m = \{x + hm \mid h \in \mathbb{Z}\}.$$

Ækvivalensklasserne kaldes restklasser modulo m , idet hver af dem består af alle hele tal, som ved division med m kan give en bestemt rest. Der er m forskellige restklasser modulo m ; blandt tallene $0, 1, \dots, m-1$ er der én repræsentant for hver. Mængden af restklasser modulo m betegner vi $\mathbb{Z}(\text{mod } m)$ eller $\mathbb{Z}_m$. - Vi bemærker, at $(0)_m = \{hm \mid h \in \mathbb{Z}\}$ er en undergruppe i den Abelske gruppe $(\mathbb{Z}, +)$, og at restklasserne modulo m er de tilhørende sideklasser.

Kongruens modulo m harmonerer ikke blot med additionen, men også med multiplikationen i $\mathbb{Z}$ (jfr. II, 1, 20):

$$\begin{aligned} x_1 \equiv x_2 \pmod{m} \wedge y_1 \equiv y_2 \pmod{m} &\Rightarrow x_1 + y_1 \equiv x_2 + y_2 \pmod{m}, \\ x_1 \equiv x_2 \pmod{m} \wedge y_1 \equiv y_2 \pmod{m} &\Rightarrow x_1 y_1 \equiv x_2 y_2 \pmod{m}. \end{aligned}$$

I mængden $\mathbb{Z}_m$ af restklasser modulo m kan man altså både addere og multiplicere ved repræsentanter. De to kompositioner, addition og multiplikation modulo m er bestemt ved

$$(x)_m + (y)_m = (x + y)_m \quad \text{og} \quad (x)_m (y)_m = (xy)_m.$$

Vi nøjedes side II, 1, 21 med at konstatere, at $(\mathbb{Z}_m, +)$ er en Abelsk gruppe. Idet den naturlige afbildning $x \mapsto (x)_m$ af $\mathbb{Z}$ på $\mathbb{Z}_m$ er en homomorf afbildning af $(\mathbb{Z}, +, \cdot)$ på $(\mathbb{Z}_m, +, \cdot)$ og tillige surjektiv, finder vi nu, at $(\mathbb{Z}_m, +, \cdot)$ er en kommutativ ring, jfr. side 13; nulelementet er $(0)_m$, og der er et etelement, $(1)_m$. Under navn af restklasseringen modulo m spiller $(\mathbb{Z}_m, +, \cdot)$ en vigtig rolle i talteorien.

Overgangen fra $(\mathbb{Z}, +, \cdot)$ til restklasseringen $(\mathbb{Z}_m, +, \cdot)$ kan siges at bestå i, at man ophører med at skelne mellem tal, der er kongruente modulo m .

Eksempel.

Vi anfører kompositionstavler for addition og multiplikation i restklasseringen $(\mathbb{Z}_6, +, \cdot)$; i stedet for $(0)_6, (1)_6, \dots, (5)_6$ er der skrevet 0, 1, ..., 5, eller, om man vil, restklasserne modulo 6 er repræsenteret ved hver sit af tallene 0, 1, ..., 5 :

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Man bemærker, at $(2)_6, (3)_6$ og $(4)_6$ er nuldivisorer, medens $(1)_6$ og $(5)_6$ er regulære ved multiplikationen.

Er m et sammensat tal, gælder nulreglen ikke i restklasseringen $(\mathbb{Z}_m, +, \cdot)$; af $xy = m$, hvor $x > 1, y > 1$ og dermed $x < m, y < m$, følger jo $(x)_m (y)_m = (0)_m$ med $(x)_m \neq (0)_m, (y)_m \neq (0)_m$.

Restklasseringen modulo et primtal p er derimod en integritetsring; nulreglens gyldighed i $(\mathbb{Z}_p, +, \cdot)$ kommer nemlig ud på, at der for $x, y \in \mathbb{Z}$ haves

$$xy \equiv 0 \pmod{p} \Rightarrow x \equiv 0 \pmod{p} \vee y \equiv 0 \pmod{p},$$

$$\text{dvs.} \quad p \mid xy \Rightarrow p \mid x \vee p \mid y.$$

For et vilkårligt primtal p er restklasseringen $(\mathbb{Z}_p, +, \cdot)$ endda et kommutativt legeme og kaldes derfor også restklasselegemet modulo p . Der gælder nemlig alment sætningen:

Enhver endelig integritetsring er et legeme.

Bevis: Lad $(M, +, \cdot)$ være en endelig integritetsring; nul- og

etelement betegnes o og e , medens $a_0 = o$, $a_1 = e$, $a_2, \dots, a_n$ er samtlige elementer af M . Ifølge forkortningsreglen (se side 4)

$$a \neq o \wedge x \neq y \Rightarrow ax \neq ay$$

vil for et vilkårligt $a \neq o$ elementerne $aa_0, aa_1, \dots, aa_n$ være indbyrdes forskellige og dermed samtlige elementer af M ; et af dem må da være e , dvs. a har et reciprok.

Delring og dellegeme.

Lad $(M, +, \cdot)$ være en ring og L en ikke tom delmængde af M .

Man siger da, at L er en delring af $(M, +, \cdot)$, hvis restriktionerne af $+$ og $\cdot$ til $L \times L$ er kompositioner inden for L , og hvis L med disse kompositioner, $(L, +, \cdot)$, er en ring.

Egentlig er det $(L, +, \cdot)$ og ikke L , der bør kaldes delring; vi vil dog foretrække ikke at lægge sprogbrugen fast, men undertiden bruge ordet i den ene, undertiden i den anden betydning.

Er $(L, +, \cdot)$ specielt en integritetsring eller et legeme, siger man i stedet for delring også delintegritetsring, henholdsvis dellegeme.

Idet vi forudsætter, at L er en delring af ringen $(M, +, \cdot)$, vil nulelementet o i $(M, +, \cdot)$ tilhøre L og være nulelement i $(L, +, \cdot)$. Thi betegnes nulelementet i $(L, +, \cdot)$ med o_L og vælges et element $a \in L$, har vi $a + o_L = a + o$ og følgelig $o_L = o$. Det modsatte element $-x$ til et element $x \in L$ vil da også være det samme, hvad enten vi regner i $(L, +, \cdot)$ eller $(M, +, \cdot)$.

Er $(M, +, \cdot)$ et legeme og L et dellegeme, vil endvidere etelementet e i $(M, +, \cdot)$ tilhøre L og være etelement i $(L, +, \cdot)$. Thi betegnes etelementet i $(L, +, \cdot)$ med e_L og vælges et fra forskellige element $a \in L$, har vi $ae_L = ae \wedge a \neq o$ og følge-

lig $e_L = e$. Det reciprokke element x^{-1} til et fra o forskelligt element $x \in L$ vil da også være det samme, hvad enten vi regner i $(L, +, \cdot)$ eller $(M, +, \cdot)$.

Der kan herefter opstilles simple nødvendige betingelser for, at en delmængde af en ring er en delring, henholdsvis for at en delmængde af et legeme er et dellegeme, betingelser, der, som vi skal vise, tillige er tilstrækkelige:

Er $(M, +, \cdot)$ en ring og L en ikke tom delmængde af M , er det nødvendigt for, at L er en delring af $(M, +, \cdot)$, at der gælder

$$x \in L \wedge y \in L \Rightarrow x + y \in L, \quad x \in L \wedge y \in L \Rightarrow xy \in L,$$
samt

$$x \in L \Rightarrow -x \in L.$$

Disse betingelser er også tilstrækkelige.

De to første kommer nemlig ud på, at restriktionerne af $+$ og $\cdot$ til $L \times L$ er kompositioner inden for L , medens tilføjelsen af den sidste betingelse sikrer, at $(L, +)$ er en gruppe, jfr. §2; at additionen er kommutativ, multiplikationen associativ samt distributiv med hensyn til additionen i $(L, +, \cdot)$, er en umiddelbar følge af, at dette er tilfældet i $(M, +, \cdot)$.

Er $(M, +, \cdot)$ et legeme og L en delmængde af M med mindst to elementer, er det nødvendigt for, at L er et dellegeme af $(M, +, \cdot)$, at der gælder

$$x \in L \wedge y \in L \Rightarrow x + y \in L, \quad x \in L \wedge y \in L \Rightarrow xy \in L,$$

$$x \in L \Rightarrow -x \in L, \quad \text{samt for } x \neq 0: \quad x \in L \Rightarrow x^{-1} \in L.$$

Disse betingelser er også tilstrækkelige.

De tre første sikrer, at L er en delring af $(M, +, \cdot)$. Idet elementet e i $(M, +, \cdot)$ kan skrives på formen $e = aa^{-1}$, hvor a er et fra o forskelligt element af L , ser vi ved at inddrage den sidste betingelse, at e tilhører L og dermed naturligvis er et-

element i ringen $(L, +, \cdot)$, ligesom jo nulelementet 0 i $(M, +, \cdot)$ tillige er nulelement i $(L, +, \cdot)$. Videre bemærkes, at det i $(M, +, \cdot)$ reciprokke x^{-1} til et fra 0 forskelligt element $x \in M$ tillige er reciprok til x i $(L, +, \cdot)$, således at x er regulært ved multiplikationen i $(L, +, \cdot)$.

Eksempler.

1° $(\mathbb{Z}, +, \cdot)$ er en delintegritetsring, $(\mathbb{Q}, +, \cdot)$ og $(\mathbb{R}, +, \cdot)$ dellegemer af de følgende i rækken $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$.

2° Er L delring af en ring $(M, +, \cdot)$, så er L specielt undergruppe af gruppen $(M, +)$. Det omvendte gælder i almindelighed ikke; dog er enhver undergruppe $\{hm \mid h \in \mathbb{Z}, m \in \mathbb{Z}\}$ af $(\mathbb{Z}, +)$ tillige delring af $(\mathbb{Z}, +, \cdot)$.

3° er
på si-
de 21

4° De to restklasser $(0)_6$ og $(3)_6$ udgør et dellegeme af restklasseringen $(\mathbb{Z}_6, +, \cdot)$; dellegemet $(\{(0)_6, (3)_6\}, +, \cdot)$ er isomorft med restklasselegemet $(\mathbb{Z}_2, +, \cdot)$. Man bemærker, at medens nulelementet $(0)_6$ i ringen $(\mathbb{Z}_6, +, \cdot)$ jo tillige er nulelement i dellegemet, så har ring og dellegeme her forskellige etelementer, nemlig henholdsvis $(1)_6$ og $(3)_6$.

Dellegemer af de komplekse tals legeme $(\mathbb{C}, +, \cdot)$ kaldes tallegemer.

Et tallegeme L indeholder tallene 0 og 1 . Idet

$$1 \in L \quad \text{og} \quad n \in L \Rightarrow n + 1 \in L,$$

fås endvidere ved induktion $\mathbb{N} \subseteq L$. Da nu L med et tal n også indeholder $-n$, finder vi $\mathbb{Z} \subseteq L$, og da ethvert rationalt tal r kan skrives på formen

$$r = p/q = pq^{-1}, \quad p \in \mathbb{Z}, q \in \mathbb{N},$$

sluttes endelig $\mathbb{Q} \subseteq L$:

De rationale tal er indeholdt i ethvert tallegeme.

Idet $\mathbb{Q}$ selv er et tallegeme, kan resultatet også udtrykkes:
De rationale tals legeme er det mindste tallegeme.

Eksempel.

For enhver mængde $A \subseteq \mathbb{C}$ findes et mindste tallegeme indeholdende A , nemlig fællesmængden af alle tallegemer, der indeholder A . I visse tilfælde kan det angives på simpel måde. Eksempelvis er $\{r + s\sqrt{2} \mid r, s \in \mathbb{Q}\}$ det mindste tallegeme, der indeholder $\sqrt{2}$; det er nemlig klart, at tallene $r + s\sqrt{2}$, $r, s \in \mathbb{Q}$, tilhører ethvert tallegeme, som indeholder $\sqrt{2}$, og ved brug af betingelserne side 19 indses, at de nævnte tal selv udgør et tallegeme.

Det manglende eksempel side 20:

3° Mængden $\hat{C}(I \rightarrow \mathbb{R})$ af kontinuerte reelle funktioner på et interval $I \subseteq \mathbb{R}$ er en delring af ringen $(\hat{F}(I \rightarrow \mathbb{R}), +, \cdot)$ af alle reelle funktioner defineret på I . De i I differentiable funktioner udgør atter en delring af $(\hat{C}(I \rightarrow \mathbb{R}), +, \cdot)$. - I ringen $(\mathbb{R}^{\mathbb{N}}, +, \cdot)$ af alle reelle talfølger udgør f.eks. de konvergente talfølger en delring.

Øvelser til Algebraens grundbegreber, § 1.

1. Gør rede for, at hver af følgende kompositioner

$$a) \quad x * y = (x^2 + y^2)^{\frac{1}{2}}, \quad x, y \in \mathbb{R},$$

$$b) \quad x * y = (x^2 + y^2)^{\frac{1}{2}}, \quad x, y \in \mathbb{R}_+ \cup \{0\},$$

$$c) \quad x * y = (xy)^{\frac{1}{2}}, \quad x, y \in \mathbb{R}_+,$$

$$d) \quad x * y = \text{største fælles divisor for } x \text{ og } y, \quad x, y \in \mathbb{N},$$

er en komposition inden for den nævnte mængde, og undersøg, om kompositionen er associativ, kommutativ, om der findes et neutralt element og i bekræftende fald, hvilke elementer der er invertible; undersøg endelig, hvilke elementer der kan bortforkortes.

2. I mængden $\hat{F}(E \rightarrow \mathbb{R})$ af reelle funktioner med en given mængde $E \neq \emptyset$ som definitionsmængde indføres kompositioner $+$ og $\cdot$, idet man for $f, g \in \hat{F}(E \rightarrow \mathbb{R})$ ved $f + g$, henholdsvis fg , forstås funktionerne

$$t \rightarrow f(t) + g(t), \quad t \in E, \quad \text{og} \quad t \rightarrow f(t)g(t), \quad t \in E.$$

Gør rede for, at $+$ er en kommutativ gruppekomposition inden for $\hat{F}(E \rightarrow \mathbb{R})$, medens $\cdot$ er en associativ og kommutativ komposition med neutralt element inden for $\hat{F}(E \rightarrow \mathbb{R})$. Bestem de ved $\cdot$ invertible elementer af $\hat{F}(E \rightarrow \mathbb{R})$.

3. Lad E være en ikke tom mængde og X_E mængden af alle funktioner fra E til $\{0, 1\}$. Idet addition og multiplikation af reelle funktioner med E som definitionsmængde tænkes indført som i øvelse 2, sætter vi for $x_1, x_2 \in X_E$

$$x_1 \dot{+} x_2 = x_1 + x_2 - x_1 x_2.$$

Vis, at $\cdot$ og $\dot{+}$ er kompositioner inden for X_E , og vis, at den enentydige korrespondance mellem mængden $\mathcal{D}(E)$ af delmængder

af E og X_E , hvor $A \in \hat{D}(E) \leftrightarrow \chi \in X_E$ betyder

$$\chi(x) = \begin{cases} 1 & \text{for } x \in A \\ 0 & \text{for } x \in CA, \end{cases}$$

er en isomorfi såvel mellem $(\hat{D}(E), \cap)$ og $(X_E, \cdot)$ som mellem $(\hat{D}(E), \cup)$ og $(X_E, +)$.

4. Idet n er et givet naturligt tal, skal man vise, at den ved $x \rightarrow x^n$ bestemte funktion med definitions­mængde $\hat{Q}$, henholdsvis $\hat{R}$, er en homomorf afbildning af $(\hat{Q}, \cdot)$, henholdsvis $(\hat{R}, \cdot)$ ind i sig selv. Undersøg i hvert af de to tilfælde, for hvilke værdier af n afbildningen er isomorf.

5. Gør rede for, at

a) $z \rightarrow \bar{z}, \quad z \in \hat{C},$

er en endomorf afbildning såvel af $(\hat{C}, +)$ som af $(\hat{C}, \cdot)$,

b) $z \rightarrow (z + \bar{z})/2, \quad z \in \hat{C},$

er en homomorf afbildning af $(\hat{C}, +)$ ind i $(\hat{R}, +)$,

c) $z \rightarrow |z|, \quad z \in \hat{C},$

er en homomorf afbildning af $(\hat{C}, \cdot)$ ind i $(\hat{R}, \cdot)$,

d) $z \rightarrow z/|z|, \quad z \in \hat{C} \setminus \{0\},$

er en endomorf afbildning af $\{\hat{C} \setminus \{0\}, \cdot\}$.

I hvilke tilfælde er afbildningen isomorf?

6. Idet c er et givet positivt reelt tal, sættes

$$v_1 * v_2 = \frac{v_1 + v_2}{1 + v_1 v_2 / c^2} \quad \text{for } v_1, v_2 \in]-c, c[.$$

(Einsteins lov for sammensætning af parallelle hastigheder.)

Vis, at $*$ er en komposition inden for intervallet $]-c, c[$, og at $(]-c, c[, *)$ er en gruppe.

- * Vis, at $(]-c, c[, *)$ er isomorf med $(\mathbb{R}, +)$. (Dette går ud på at finde en bijektiv funktion $f: \mathbb{R} \rightarrow]-c, c[$, således at

$$\forall_{\mathbb{R}} x, y: f(x + y) = f(x) * f(y).$$

7. Er $(\mathbb{R}, +)$ isomorf med $(\mathbb{R}, \cdot)$? med $(\mathbb{R} \setminus \{0\}, \cdot)$?
8. Bestem samtlige automorfe afbildninger af $(\mathbb{N}, \cdot)$. (Undersøg, hvad et primtal kan føres over i ved en sådan afbildning.)
9. Vis, at enhver endomorf afbildning f af $(\mathbb{Z}, +)$, d.v.s. en funktion $f: \mathbb{Z} \rightarrow \mathbb{Z}$, der tilfredsstiller "funktionalligningen"

$$\forall_{\mathbb{Z}} x, y: f(x + y) = f(x) + f(y),$$

er af formen $x \rightarrow ax$, $x \in \mathbb{Z}$, altså at $\exists_{\mathbb{Z}} a \forall_{\mathbb{Z}} x: f(x) = ax$.

Vis samme påstand, idet $\mathbb{Z}$ overalt erstattes med $\mathbb{Q}$.

Vis, at enhver endomorf afbildning f af $(\mathbb{R}, +)$, som tillige er voksende, d.v.s.

$$\forall_{\mathbb{R}} x, y: x < y \Rightarrow f(x) \leq f(y),$$

er af formen $x \rightarrow ax$, $x \in \mathbb{R}$, hvor $a \geq 0$. (Man kan f.eks. benytte, at hvert irrationalt tal er grænseværdi såvel for en voksende som for en aftagende følge af rationale tal.)

10. Benyt det sidste resultat i øvelse 9 til at vise:

a) Enhver homomorf afbildning f af $(\mathbb{R}, +)$ ind i $(\mathbb{R}_+, \cdot)$, d.v.s. en funktion $f: \mathbb{R} \rightarrow \mathbb{R}_+$, der tilfredsstiller funktionalligningen

$$\forall_{\mathbb{R}} x, y: f(x + y) = f(x)f(y),$$

er, hvis den tillige er voksende, af formen $x \rightarrow a^x$, $x \in \mathbb{R}$, hvor $a \geq 1$. (Sammensæt f med en passende isomorf afbildning.)

b) Enhver homomorf afbildning f af $(\mathbb{R}_+, \cdot)$ ind i $(\mathbb{R}, +)$, d.v.s. en funktion $f: \mathbb{R}_+ \rightarrow \mathbb{R}$, der tilfredsstiller funktionalligningen

$$\forall_{\mathbb{R}_+} x, y: f(xy) = f(x) + f(y),$$

er, hvis den tillige er voksende, enten af formen

$x \rightarrow \log_a x$, $x \in \mathbb{R}_+$, hvor $a > 1$, eller den er identisk 0.

c) Enhver endomorf afbildning f af $(\mathbb{R}_+, \cdot)$, d.v.s. en funktion $f: \mathbb{R}_+ \rightarrow \mathbb{R}_+$, der tilfredsstiller funktionalligningen

$$\forall_{\mathbb{R}_+} x, y: f(xy) = f(x)f(y),$$

er, hvis den tillige er voksende, af formen $x \rightarrow x^a$, $x \in \mathbb{R}_+$, hvor $a \geq 0$.

Angiv endelig alle aftagende, homomorfe afbildninger af $(\mathbb{R}, +)$ og $(\mathbb{R}_+, \cdot)$ ind i $(\mathbb{R}, +)$ og $(\mathbb{R}_+, \cdot)$.

11. Opskriv kompositionstavler for $(\mathbb{Z}_m, +)$ og $(\mathbb{Z}_m, \cdot)$ for $m = 2, 3, 4$ og 5 og undersøg i hvert af de 4 tilfælde, om multiplikation modulo m er en komposition, evt. en gruppekomposition inden for $\mathbb{Z}_m \setminus (0)_m$.
12. For $x_1, x_2 \in \mathbb{R}_+$ sættes $x_1 \sim x_2$, hvis de to tal kan skrives som evt. uendelige decimalbrøker med samme cifre i samme rækkefølge, altså afvigende højst ved kommaets placering. Gør rede for, at der herved er defineret en ækvivalensrelation i $\mathbb{R}_+$, som harmonerer med multiplikation. Mængden af ækvivalensklasser med multiplikation ved repræsentanter er da en gruppe; angiv en hermed isomorf gruppe.
13. I $\mathbb{N}^2$ defineres en komposition $+$ ved
- $$(p, q) + (r, s) = (p+r, q+s)$$
- og en relation $\sim$ ved
- $$(p_1, q_1) \sim (p_2, q_2) \Leftrightarrow p_1 + q_2 = p_2 + q_1.$$
- Vis, at $\sim$ er en ækvivalensrelation i $\mathbb{N}^2$, som harmonerer med $+$. Vis, at mængden af ækvivalensklasser med addition ved repræsentanter er en gruppe, isomorf med $(\mathbb{Z}, +)$.

14. Om en associativ og kommutativ komposition $*$ inden for en mængde M forudsættes, at hvert element af M kan bortforkortes. I M^2 defineres en komposition, som vi også vil betegne med $*$, ved

$$(p, q) * (r, s) = (p * r, q * s)$$

og en relation $\sim$ ved

$$(p_1, q_1) \sim (p_2, q_2) \Leftrightarrow p_1 * q_2 = p_2 * q_1.$$

Vis, at $\sim$ er en ækvivalensrelation i M^2 , som harmonerer med $*$. Vis, at mængden af ækvivalensklasser organiseret ved regning med repræsentanter er en kommutativ gruppe.

Gør rede for, at "konstruktionen" for $(M, *) = (\hat{M}, \cdot)$ fører til en med $(\hat{Q}_+, \cdot)$ isomorf gruppe.

Øvelser til Algebraens grundbegreber, § 2.

1. Lad $\cdot$ være en associativ komposition inden for en mængde G .
Det forudsættes, at hver af ligningerne

$$ax = b \quad \text{og} \quad ya = b$$

for vilkårligt opgivne $a, b \in G$ har mindst en løsning. Vis, at $(G, \cdot)$ er en gruppe. (Begynd f.eks. med at vise, at en løsning til en ligning af formen $ya = a$ må være neutralt element.)

2. Lad $\cdot$ være en associativ komposition inden for en endelig mængde G . Det forudsættes, at forkortningsreglerne

$$ax = ay \Rightarrow x = y \quad \text{og} \quad xa = ya \Rightarrow x = y$$

gælder for $a, x, y \in G$. Vis, at $(G, \cdot)$ er en gruppe. (Resultatet fra øv. 1 kan benyttes.)

Vis ved et modeksempel, at tilsvarende ikke gælder for uendelige mængder.

- 3.* Lad $\cdot$ være en associativ komposition inden for en mængde G , og lad e være et element af G . Vis, at det er tilstrækkeligt for, at $(G, \cdot)$ er en gruppe med e som neutralt element, at

$$\forall_G x: ex = x \quad \text{og} \quad \forall_G x \exists_G y: yx = e,$$

altså at e er "venstre neutralt", og at hvert element af G har et "venstre inverst".

4. For hvilke grupper $(G, \cdot)$ er afbildningen $x \rightarrow x^{-1}$, $x \in G$, automorf?

5. Lad $(G, \cdot)$ være en gruppe og $H \neq \emptyset$ en endelig delmængde af G , hvor

$$\forall_H x, y: xy \in H.$$

Vis, at H er en undergruppe af $(G, \cdot)$.

Vis ved et modeksempel, at tilsvarende ikke gælder for H uendelig.

6. Lad H og K være undergrupper af en gruppe $(G, \cdot)$. Vis, at $H \cup K$ ikke er en undergruppe af $(G, \cdot)$, medmindre $H \subseteq K$ eller $K \subseteq H$.
7. Beskriv den mindste undergruppe af $(\mathbb{Q}_+, \cdot)$, der indeholder en given mængde P af primtal.
Vis, at mængden af undergrupper af $(\mathbb{Q}_+, \cdot)$ ikke er numerabel.
8. Idet H er en undergruppe og g et element af gruppen $(G, \cdot)$, skal man vise, at $(gHg^{-1}, \cdot)$, hvor

$$gHg^{-1} = \{ghg^{-1} \mid h \in H\},$$

er en med $(H, \cdot)$ isomorf undergruppe af $(G, \cdot)$. (Den kaldes en til $(H, \cdot)$ konjugeret undergruppe af G .)

Lad specielt $(G, \circ)$ være en transformationsgruppe for en mængde E , og lad H_α betegne undergruppen bestående af de transformationer tilhørende G , der lader elementet $\alpha \in E$ gå over i sig selv. Idet $g \in G$, skal man da vise, at

$$g \circ H_\alpha \circ g^{-1} = H_{g(\alpha)}.$$

9. Vis, at de isometrier af en plan, ved hvilke et givet kvadrat i denne afbildes på sig selv, danner en gruppe $(D_4, \circ)$

af orden 8 (som er isomorf med gruppen af de flytninger af rummet, ved hvilke kvadratet afbildes på sig selv). Undersøg, om gruppen er kommutativ.

De til D_4 hørende flytninger af planen udgør en undergruppe C_4 af orden 4. De til D_4 hørende isometrier, ved hvilke hver af kvadratets diagonaler afbildes på sig selv, danner en anden undergruppe V af orden 4 (som er isomorf med gruppen af flytninger af rummet, ved hvilke hver af tre ^{parvis} givne, vinkelrette linier afbildes på sig selv). Vis, at de to undergrupper ikke er isomorfe.

10. Opstil gruppetavler for de to i øv. 9 omtalte grupper af orden 4, og angiv undergrupper af $(S_4, \circ)$, som de er isomorfe med.

11. Idet $M = \mathbb{R} \setminus \{0, 1\}$, betragtes de for $t \in M$ definerede funktioner

$$\begin{aligned} f_1(t) &= t, & f_2(t) &= 1/t, & f_3(t) &= 1-t, \\ f_4(t) &= t/(t-1), & f_5(t) &= 1/(1-t), & f_6(t) &= (t-1)/t, \end{aligned}$$

Vis, at $(\{f_1, f_2, f_3, f_4, f_5, f_6\}, \circ)$ er en med den symmetriske gruppe $(S_3, \circ)$ isomorf transformationsgruppe for M . (Giv intervallerne $]-\infty, 0[$, $]0, 1[$ og $]1, \infty[$, hvis foreningsmængde er M , numrene 1, 2 og 3, og undersøg, hvorledes de afbildes ved funktionerne f_i .)

givet

12. Lad der være et tal $c \in \mathbb{R}_+$. For et vilkårligt $\alpha \in \mathbb{R}$ betragtes afbildningen $f_\alpha: \mathbb{R}^2 \rightarrow \mathbb{R}^2$, hvorved til hvert $(x, t) \in \mathbb{R}^2$ svarer talparret (x', t') bestemt ved

$$x' = x \cosh \alpha - ct \sinh \alpha$$

$$ct' = -x \sinh \alpha + ct \cosh \alpha.$$

Vis, at $f_\alpha: \mathbb{R}^2 \rightarrow \mathbb{R}^2$ er bijektiv. Idet (x, t) og (x', t') fortolkes som sædvanlige retvinklede koordinater for punkter i planen, skal man tillige vise, at hver af linierne $x = ct$ og $x = -ct$ og ligeledes for vilkårligt $r \in \mathbb{R}_+$ hver gren af hyperblen med ligningen

$$x^2 - ct^2 = r^2$$

afbildes på sig selv. (Parameterfremstillingerne

$$\begin{array}{ll} x = r \cosh u & u \in \mathbb{R}, \\ ct = r \sinh u, & \end{array} \quad \begin{array}{ll} x = -r \cosh u & u \in \mathbb{R}, \\ ct = r \sinh u, & \end{array}$$

for hyperblens grene kan benyttes med fordel.)

Vis, at der for $\alpha, \beta \in \mathbb{R}$ gælder $f_\alpha \circ f_\beta = f_{\alpha+\beta}$, og begrund herved, at $(\{f_\alpha | \alpha \in \mathbb{R}\}, \circ)$ er en med $(\mathbb{R}, +)$ isomorf transformationsgruppe. (Gruppen af specielle Lorentz transformationer. Fortolk c som lysets hastighed, t som tiden og $v = c \tanh \alpha$ som den konstante hastighed af x' -koordinatsystemet i forhold til x -koordinatsystemet på en linie.)

13. Hvilke funktioner $f: \mathbb{R}_+ \rightarrow \mathbb{R}_+$ svarer til translationer $x \rightarrow x + c$, $x \in \mathbb{R}$, og homotetier $x \rightarrow cx$, $x \in \mathbb{R}$, af $\mathbb{R}$ ved den enentydige korrespondance $e^x = y$ mellem $\mathbb{R}$ og $\mathbb{R}_+$?
14. a) Idet f er en drejning af planen om et punkt A og s spejlingen af planen i en linie l , skal man gøre rede for, at $s \circ f \circ s$ er en drejning om spejlbilledet $s(A)$ af punktet A med hensyn til linien l . Er planen orienteret, og φ et vinkeltal for drejningen f , vil $-\varphi$ være et vinkeltal for drejningen $s \circ f \circ s$.
- b) Idet f er en drejning af rummet om en linie l og s spejlingen af rummet i en plan π , skal man gøre rede for,

at $s \circ f \circ s$ er en drejning om spejlbilledet $s(l)$ af linien l med hensyn til planen π . Tænkes linien l orienteret, hvilket giver anledning til en orientering også af spejlbilledet $s(l)$ gælder der endvidere, idet omløbsretningen om en orienteret linie modsat urvisernes, set fra liniens positive ende, regnes positiv: er φ et vinkeltal for drejningen f , vil $-\varphi$ være et vinkeltal for drejningen $s \circ f \circ s$.

c) Lad g og h være drejninger af rummet om to hinanden skærende linier m og n . Idet spejlingen i den ved m og n bestemte plan betegnes med t , skal man påvise, at $t \circ g^{-1} \circ t = g$, og at

$$g \circ h = t \circ (h \circ g)^{-1} \circ t,$$

samt ud fra det sidste resultat beskrive sammenhængen mellem $g \circ h$ og $h \circ g$ geometrisk.

15. Planen tænkes delt i kongruente kvadrater ved et netværk af rette linier. Vis, at enhver flytning af planen, hvorved netværket går over i sig selv, kan sammensættes af en drejning om midtpunktet i et givet af kvadraterne og en translation. Vis, at gruppen af flytninger af planen, hvorved netværket går over i sig selv, kan karakteriseres som den mindste transformationsgruppe indeholdende to passende flytninger, nemlig dels en drejning og en translation, dels to drejninger.
16. Planen tænkes delt i kongruente regulære sekskanter (som en bikage) ved et netværk af rette liniestykker. Vis, at gruppen af flytninger af planen, hvorved netværket går over i sig selv, kan karakteriseres som den mindste transformationsgruppe

indeholdende to passende flytninger, nemlig dels en drejning og en translation, dels to drejninger. Vis, at gruppen og-så kan opfattes som bestående af de flytninger^{af planen}, hvorved et netværk, der deler planen i kongruente ligesidede trekanten, går over i sig selv.

17. Idet a og b er hele tal, som ikke begge er 0, skal man vise, at $H = \{ax + by \mid x, y \in \mathbb{Z}\}$ er en undergruppe af $(\mathbb{Z}, +)$ og følgende kan skrives på formen $H = \{zd \mid z \in \mathbb{Z}\}$, hvor $d \in \mathbb{N}_+$. Vis videre, at d er største fælles divisor for a og b .

Idet også c er et helt tal, skal man angive en nødvendig og tilstrækkelig betingelse for, at den "diofantiske ligning"

$$ax + by = c$$

har en løsning (x, y) bestående af hele tal. (En ligning med ubekendte, for hvilke der søges heltallige værdier, kaldes en diofantisk ligning efter den græske matematiker Diofantos, ca. +250, der har behandlet sådanne opgaver.)

18. Lad a , b og c være hele tal, a og b ikke begge 0. Gør rede for, at mængden af heltallige løsninger (x, y) til ligningen

$$ax + by = 0$$

kan skrives på formen $\{(pt, qt) \mid t \in \mathbb{Z}\}$. Under forudsætning af, at ligningen

$$ax + by = c$$

har en heltallig løsning (x_0, y_0) , skal man dernæst angive alle dens heltallige løsninger.

Eksempler: $3x - 4y = 1$, $6x - 8y = 4$.

19. Vis, at enhver undergruppe $(H, \cdot)$ af en cyklisk gruppe $(G, \cdot)$ ligeledes er cyklisk. (Lad c være en frembringer for $(G, \cdot)$ og betragt mængden $\{n \in \mathbb{Z} \mid c^n \in H\}$.)
20. Idet c er frembringer for en cyklisk gruppe med m elementer, skal man vise, at elementet c^k har ordenen m/d , hvor d er største fælles divisor for m og k .
- Eksempel: Angiv samtlige frembringere i $(\mathbb{Z}_{10}, +)$.
21. Hvilke elementer af $(\mathbb{R}_1, +)$ har endelig orden?
22. Gør rede for, at mængden $\{z \in \mathbb{C} \mid \exists n: z^n = 1\}$ af samtlige komplekse enhedsrødder med multiplikation som komposition er en uendelig kommutativ gruppe, hvor hvert element har endelig orden.
- * Giv et eksempel på en uendelig kommutativ gruppe, hvor hver ægte undergruppe er endelig. (Søg en passende undergruppe af ovennævnte.)
23. Vis, at hvis alle fra det neutrale element forskellige elementer af en gruppe har orden 2, vil gruppen være kommutativ. Angiv en gruppe med førstnævnte egenskab bestående af 4 isometrier af planen, henholdsvis 8 isometrier af rummet.
24. Vis, at antallet af elementer af orden 2 i en endelig gruppe af lige orden er ulige, i en endelig gruppe af ulige orden er lige.
- Vis, at i en endelig kommutativ gruppe er kompositionen af alle elementer, hvis orden er større end 2, lig med det neutrale element.

25. Angiv såvel de venstre som de højre sideklasser til den af permutationen $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ frembragte cykliske undergruppe H af den symmetriske gruppe $(S_3, \circ)$ af alle permutationer af mængden $\{1, 2, 3\}$.
26. Beskriv inddelingen af gruppen af flytninger af planen i venstre (højre) sideklasser til undergruppen af translationer. (Benyt, at enhver flytning af planen er en translation eller en drejning.)

27.

	a_1	a_2	a_3	a_4	a_5	a_6
a_1					a_5	
a_2						
a_3						
a_4		a_1	a_2			a_3
a_5		a_4	a_1			
a_6						

Ovenstående er en delvis udfyldt gruppetafle for en kommutativ gruppe $(G, \cdot)$ med elementerne $a_1, a_2, a_3, a_4, a_5, a_6$.

Opskriv den fuldstændige gruppetafle for $(G, \cdot)$. Undersøg, om den ved a_5 bestemte ^{venstre}translation $x \rightarrow a_5 x$, $x \in G$, er en lige eller ulige permutation af G . Find samtlige undergrupper af $(G, \cdot)$.

28. Vis, at der på nær isomorfi findes netop to grupper af orden 4. (Analysen af en ikke cyklisk gruppe med 4 elementer knyttes med fordel til en kompositionstafle.)

29. En transformationsgruppe $(G, \circ)$ for en mængde E siges at være transitiv, hvis

$$\forall_{E} x, y \exists_{G} f: f(x) = y.$$

Vis, at ordenen af en transitiv gruppe $(G, \circ)$ af permutationer af en mængde E med n elementer er delelig med n . (Søg en undergruppe med index n .) Vis endvidere, idet n forudsættes ≥ 2 , at G må indeholde en permutation, hvorved intet element af E går over i sig selv. (Foreningen af n undergrupper med index n kan ikke være hele G .)

30. Vis, at de inverse til elementerne i en venstre sideklasse til en undergruppe H af en gruppe $(G, \cdot)$ udgør en højre sideklasse til H . Vis, at mængden af venstre og mængden af højre sideklasser til H i $(G, \cdot)$ er ækvipotente.

31. I gruppen $(G, \cdot)$ siges et element $x \in G$ at være konjugeret med et element $y \in G$, hvis

$$\exists_{G} g: gx = yg.$$

Vis, at der herved defineres en ækvivalensrelation i G . Ækvivalensklasserne kaldes klasser af konjugerede elementer.

Vis, at en undergruppe af $(G, \cdot)$ er normal, hvis og kun hvis den er forening af klasser af konjugerede elementer.

32. Beskriv inddelingen af gruppen af flytninger af planen i klasser af konjugerede. Afgør herved, om undergruppen af translationer, henholdsvis af drejninger om et givet punkt, er normal. (Se øv. 31.)

33. Idet $*$ er en komposition med definitionsmængde $L \times M$ og $N \subseteq L$, $P \subseteq M$, sættes

$$N * P = \{n * p \mid n \in N, p \in P\}.$$

Vis, at

$$N * P = \bigcup \{n * P \mid n \in N\} = \bigcup \{N * p \mid p \in P\}.$$

(Som det er sædvane, er her skrevet $h * K$ i stedet for $\{h\} * K$ og analogt.)

Lad nu H og K være undergrupper af en gruppe $(G, \cdot)$.

Vis, at HK er en undergruppe af $(G, \cdot)$, hvis og kun hvis $HK = KH$. Vis, at HK er en undergruppe, hvis H eller K er en normal undergruppe af $(G, \cdot)$, og at HK er en normal undergruppe af $(G, \cdot)$, hvis H og K begge er det.

Vis, at hvis undergrupperne H og K er endelige, vil HK bestå af qr/s elementer, hvor q , r og s er antallet af elementer i H , K og $H \cap K$.

34. Vis, at mængden $\{a \in G \mid \forall_G x: ax = xa\}$ af elementer af en gruppe $(G, \cdot)$, som hvert er ombytteligt med alle elementer af G , er en normal undergruppe af $(G, \cdot)$. Den kaldes gruppens centrum.

Vis, at hvis gruppen har netop ét element af orden 2, må dette tilhøre centret.

35. Idet $a \neq 0$ og b er reelle tal, betegnes med $f_{a,b}$ afbildningen

$$x \rightarrow ax + b, \quad x \in \mathbb{R}.$$

Gør rede for, at $f_{a,b}$ er en homoteti eller translation af tallinien.

Vis, at afbildningerne $f_{a,b}$, $a \in \mathbb{R} \setminus \{0\}$, $b \in \mathbb{R}$, udgør en

transformationsgruppe, og at der ved $f_{a,b} \rightarrow a$ defineres en homomorf afbildning af denne på $(\mathbb{R} \setminus \{0\}, \cdot)$; angiv kernen og beskriv den tilsvarende inddeling af transformationsgruppen i sideklasser.

36. Lad $(G, \cdot)$ være en gruppe, og lad der i G være givet en ækvivalensrelation $\sim$, som harmonerer med kompositionen. Idet gruppens neutrale element betegnes med e , skal man vise, at

$$H = \{x \in G \mid x \sim e\}$$

er en normal undergruppe af $(G, \cdot)$. Vis endvidere, at den givne ækvivalensrelation svarer til klasseinddelingen af G bestående af sideklasserne til H .

Hvilke ækvivalensrelationer harmonerer med kompositionen i en gruppe med 13 elementer?

37. Idet H er en normal undergruppe med endelig index n i en gruppe $(G, \cdot)$, skal man vise, at x^n tilhører H for hvert $x \in G$.

Slut heraf, at ingen af grupperne $(\mathbb{Q}, +)$ og $(\mathbb{R}, +)$ har ægte undergrupper med endelig index.

38. Gruppen af flytninger af rummet, ved hvilke et givet regulært oktaeder afbildes på sig selv, kaldes oktaedergruppen og betegnes med O . (Den er identisk med gruppen af flytninger, ved hvilke terningen, hvis hjørner er midtpunkterne af oktaedrets sideflader, afbildes på sig selv, og kunne derfor også kaldes for hexaedergruppen.)

Find de cykliske undergrupper af $(O, \circ)$ og bestem gruppens orden. Vis, at $(O, \circ)$ er isomorf med den symmetriske gruppe $(S_4, \circ)$.

Giv et geometrisk bevis for, at tetraedergruppen $(T, \circ)$ er en undergruppe af $(O, \circ)$.

Vis, at der findes en homomorf afbildning af $(O, \circ)$ på $(S_3, \circ)$. Bestem denne homomorfis kerne og undersøg, om der findes andre fra $\{e\}$ og 0 forskellige normale undergrupper af $(O, \circ)$.

- 39.* Gruppen af flytninger af rummet, ved hvilke et givet regulært ikosaeder afbildes på sig selv, kaldes ikosaedergruppen og betegnes med I . (Den er identisk med "dodekaedergruppen", idet midtpunkterne af ikosaedrets sideflader er et regulært dodekaeders hjørner.)

Find de cykliske undergrupper af $(I, \circ)$ og bestem gruppens orden. Vis, at $(I, \circ)$ er isomorf med den alternerende gruppe $(A_5, \circ)$.

Vis, at $(I, \circ)$ ikke har andre normale undergrupper end $\{e\}$ og I selv (at $(I, \circ)$ er en "simpel gruppe").

- 40.* Bevis, at hvis en gruppe af isometrier (af planen eller rummet) er endelig, vil alle dens isometrier have et fælles fixpunkt. (Benyt f.eks. følgende sætning: Til endelig mange givne punkter findes der blandt rummets punkter et og kun et, for hvilket kvadratsummen af dets afstande fra de givne punkter antager den mindst mulige værdi. Dette kan sluttes af den for vilkårlige vektorer $\underline{v}, \underline{v}_1, \dots, \underline{v}_n$ gyldige ligning

$$\sum_{\nu=1}^n (\underline{v} - \underline{v}_\nu)^2 = \sum_{\nu=1}^n (\underline{v}^* - \underline{v}_\nu)^2 + n(\underline{v} - \underline{v}^*)^2,$$

hvor

$$\underline{v}^* = \frac{1}{n} \sum_{\nu=1}^n \underline{v}_\nu \quad .)$$

41. Vis, at hver fra $\{e\}$ forskellig endelig gruppe af flytninger af planen er cyklisk og består af drejningerne, ved

hvilke en regulær polygon (i tilfældet af ordenen 2, et linestykke) afbildes på sig selv. (Benyt sætningen i øv. 40, og betragt den drejning i gruppen, der har den mindste positive drejningsvinkel.)

42.* I rummet findes der følgende fra $\{e\}$ forskellige endelige grupper af flytninger:

- 1) De cykliske grupper C_n , $n = 2, 3, \dots$. Gruppen C_n er af orden n og består af drejningerne, ved hvilke en regulær n -sided pyramid (for $n = 2$ en ligebeinet, men ikke ligesidet trekant) afbildes på sig selv. (For $n = 3$ må pyramiden ikke være et regulært tetraeder.)
- 2) Diedergrupperne D_n , $n = 2, 3, \dots$. Gruppen D_n er af orden $2n$ og består af drejningerne, ved hvilke et regulært n -sided prisme (for $n = 2$ en rektangulær, men ikke kvadratisk skive) afbildes på sig selv. (For $n = 4$ må prismet ikke være en terning. For $n > 2$ kan prismet erstattes med en regulær n -kant, der kan opfattes som et regulært "polyeder" med to sideflader, et "dieder".)
- 3) Tetraedergruppen T , oktaedergruppen O , ikosaedergruppen I .

Gennemfør det nedenfor skitserede bevis for, at der ikke findes andre endelige grupper af flytninger af rummet.

Lad N være en sådan gruppes orden. De fra e forskellige $N - 1$ elementer er da drejninger om akser gennem et fast punkt F (se øv. 40) og afbilder derfor en vilkårlig valgt kugleflade med centrum F på sig selv. Skæringspunkterne mellem kuglefladen og gruppens drejningsakser kan fordeles på klasser ved fastsættelsen, at to af dem skal høre til samme klasse, hvis der findes en drejning i gruppen, der fører det ene over i det andet. Lad $K_1, \dots, K_m$ betegne disse klasser og n_μ

antallet af punkter i klassen K_μ . Hvert punkt i K_μ er fixpunkt for en cyklisk undergruppe, og dennes orden ν_μ er den samme for alle punkter i klassen, idet de pågældende undergrupper er indbyrdes konjugerede (øv. 8). Heraf kan man slutte, at $n_\mu \nu_\mu = N$ og

$$2(N - 1) = \sum_{\mu=1}^m n_\mu (\nu_\mu - 1),$$

hvilket giver

$$2\left(1 - \frac{1}{N}\right) = \sum_{\mu=1}^m \left(1 - \frac{1}{\nu_\mu}\right).$$

Da $N \in \mathbb{N}$ og $\nu_\mu \in \mathbb{N}$, kommer kun værdierne $m = 2$ og $m = 3$ i betragtning. For hvert $N > 1$ kan talsættene (ν_1, ν_2) eller (ν_1, ν_2, ν_3) , som tilfredsstiller ligningen, bestemmes, og det kan vises, at de kun kan forekomme hos de ovenfor nævnte grupper.

43.* Lad $(G, \circ)$ være en endelig gruppe af isometrier af rummet, og lad H være undergruppen bestående af flytningerne i G . Alle isometrier tilhørende G har et fælles fixpunkt F (se øv. 40). Med s betegnes spejlingen i punktet F . Nu skelnes mellem to tilfælde: $s \in G$ og $s \notin G$. I det første tilfælde kan den fra H forskellige sideklasse skrives $s \circ H$, og man har $G = H \cup (s \circ H)$, hvor H er en af de i øvelse 42 bestemte flytningsgrupper. I det andet tilfælde kan sideklassen skrives $u \circ H = H \circ u$, hvor u er en uegentlig isometri i G . Da s er ombytkelig med hver isometri med fixpunkt F (vis dette), vil mængden $G' = H \cup (s \circ u \circ H)$ af flytninger være en gruppe, altså en af de i øvelse 42 bestemte. Den forelagte gruppe G kan altså fås ved i en af disse grupper med en undergruppe H af

index 2 at erstatte den fra H forskellige sideklasse $g \circ H$ med $s \circ g \circ H$. Disse resultater tillader at bestemme samtlige endelige grupper af isometrier af rummet.

Øvelser til Algebraens grundbegreber, § 3.

1. Om to kompositioner $+$ og $\cdot$ inden for samme mængde M er givet, at $+$ er associativ, at hvert element af M kan bortforkortes ved $+$, at der findes et neutralt element e ved $\cdot$, og at $\cdot$ er distributiv med hensyn til $+$. Vis, at $+$ er kommutativ.

2. Lad $(M, +, \cdot)$ være en ring. Vis, at der for $a, b \in M$, $m, n \in \mathbb{Z}$ gælder

$$(na)b = n(ab) = a(nb) \quad \text{og} \quad (ma)(nb) = (mn)(ab),$$

hvor potenser i gruppen $(M, +)$ er betegnet som anført side II, 2, 14.

3. Lad $(M, +, \cdot)$ være en ring, hvor nulreglen gælder. Det forudsættes, at M har mindst to elementer. Vis, at der for $a, b \in M \setminus \{0\}$, $n \in \mathbb{Z}$ gælder

$$na = 0 \iff nb = 0,$$

og begrund herved, at alle fra 0 forskellige elementer af M har samme orden i gruppen $(M, +)$. Den fælles orden kaldes ringens karakteristik. Vis, at hvis karakteristikken er endelig, må den være et primtal. (Benyt øv. 2.)

4. Lad $(M, +, \cdot)$ være et kommutativt legeme. For $a, b \in M$, $b \neq 0$, betegnes med a/b løsningen til de ensbetydende ligninger $bx = a$ og $xb = a$. Idet også $c, d \in M$, $d \neq 0$, skal man vise:

$$a/b = c/d \iff ad = bc,$$

$$a/b \pm c/d = (ad \pm bc)/(bd);$$

$$(a/b)(c/d) = (ac)/(bd),$$

samt for $c \neq 0$

$$(a/b)/(c/d) = (ad)/(bc).$$

5. Lad $(G, +)$ være en kommutativ gruppe. Mængden af homomorfe afbildninger af $(G, +)$ ind i sig selv betegnes med $\text{Hom}(G, G)$, og for $f, g \in \text{Hom}(G, G)$ forstås ved $f + g$ afbildningen

$$t \rightarrow f(t) + g(t), \quad t \in G.$$

Vis, at $(\text{Hom}(G, G), +, \circ)$ er en ring. (Den kaldes ringen af endomorfier af $(G, +)$.)

6. Vis, at mængden af reelle, henholdsvis komplekse polynomier med sædvanlig addition og multiplikation er en integritetsring, mængden af rationale funktioner et legeme. (En rational funktion er en kvotient mellem to polynomier; den er defineret overalt på nær i højst endelig mange punkter. Punkter, hvor kontinuitet kan opnås (ved "plombering"), medtages i definitionsmængden for en rational funktion såvel ^{som} for en sum og et produkt af sådanne.)

7. a) Hvor mange gruppekompositioner med o som neutralt element findes der inden for en mængde med 3 elementer o, p og q ? Opskriv kompositionstavle(r).

b) Gør rede for, at der på nær isomorfi højst findes ét legeme med 3 elementer. (Eksistens fremgår af et resultat side II, 3, 17.)

8. Vis, at ringen af endomorfier af $(\mathbb{Z}, +)$ er isomorf med $(\mathbb{Z}, +, \cdot)$. (Se øv. 5 og II, 1, øv. 9.) Vis samme påstand, idet $\mathbb{Z}$ erstattes med $\mathbb{Q}$.
9. Gør rede for, at mængden $\mathbb{C}^2$ af par af komplekse tal med kompositionerne

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2),$$

$$(x_1, x_2)(y_1, y_2) = (x_1 y_1 - x_2 y_2, x_1 y_2 + x_2 y_1)$$

er en kommutativ ring med et element. Bestem de elementer, der ikke er invertible ved multiplikationen. Gælder nulreglen?

10. Bevis, at der findes en og kun en isomorfi mellem en kommutativ ring $(M, +, \cdot)$, som indeholder et eksemplar $(\mathbb{R}, +, \cdot)$ af de reelle tals legeme samt et element ε med $\varepsilon^2 = 0$, således at ethvert $x \in M$ har en og kun en fremstilling af formen

$$x = x_1 + \varepsilon x_2, \quad x_1, x_2 \in \mathbb{R}.$$

(Betragt passende kompositioner $+$ og $\cdot$ inden for $\mathbb{R}^2$.)

Elementerne af en ring med de nævnte egenskaber kaldes duale tal.

11. Ved undersøgelser vedrørende reelle tal kan man tænke på et eksemplar $(\mathbb{R}, +, \cdot)$, som på den i øv. 10 beskrevne måde indgår i de duale tals ring. For et polynomium P med reelle koefficienter har da $P(x)$ mening for ethvert dualt tal x . Vis, at

$$P(x_1 + \varepsilon x_2) = P(x_1) + \varepsilon x_2 DP(x_1),$$

hvor $x_1, x_2 \in \mathbb{R}$ og DP betegner den afledede af P .

12. Inden for mængden $\mathcal{D}(E)$ af delmængder af en mængde E defineres en komposition $+$ ved

$$A + B = (A \cup B) \setminus (A \cap B).$$

a) Vis, at $(\mathcal{D}(E), +, \cap)$ er en kommutativ ring med etelement.
(Benyt figurer.)

b) Hvilken egenskab ved en afbildning $f: E_1 \rightarrow E_2$ er nødvendig og tilstrækkelig for, at den tilsvarende mængdeafbildning er en homomorf afbildning af $(\mathcal{D}(E_1), +)$ ind i $(\mathcal{D}(E_2), +)$? af $(\mathcal{D}(E_1), \cap)$ ind i $(\mathcal{D}(E_2), \cap)$?

13. Vis, at der ikke findes andre endomorfe afbildninger af $(\mathbb{Z}, +, \cdot)$ end nulfunktionen $z \rightarrow 0$, $z \in \mathbb{Z}$, og identiteten $z \rightarrow z$, $z \in \mathbb{Z}$.

Vis det tilsvarende for $(\mathbb{Q}, +, \cdot)$, henholdsvis $(\mathbb{R}, +, \cdot)$. (Slut i sidste tilfælde, at en endomorf afbildning må være voksende, ved at benytte, at hvert positivt tal er kvadrat på et reelt.)

14. Hvilke ækvivalensrelationer harmonerer både med additionen og med multiplikationen i et legeme ?

15. For et vilkårligt primtal p er multiplikation modulo p en gruppekomposition inden for mængden af de $p - 1$ fra $(\mathbb{Z}/p\mathbb{Z})^\times$ forskellige restklasser modulo p . (Hvorfor ?)

Vis ved hjælp heraf Fermats "lille" sætning: For hvert helt tal a og hvert primtal p er

$$a^p \equiv a \pmod{p}.$$

16. Anvend det sidste resultat i II, 2, øv. 24 på gruppen $(\mathbb{Z}_p \setminus \{(0)_p\}, \cdot)$, hvor p betegner et primtal, og bevis derved Wilson's sætning: For hvert primtal p er

$$(p-1)! \equiv -1 \pmod{p}.$$

17. Vis, at restklassen $(a)_m$, hvor $m \in \mathbb{N}$ og $a \in \mathbb{Z}$, er invertibel ved multiplikationen modulo m , hvis og kun hvis a er primisk med m . (Man kan betragte den diofantiske ligning $ax + my = 1$, se II, 2, øv. 17.)

18. Inden for mængden $\hat{D}(E)$ af delmængder af en mængde E defineres en komposition + ved

$$A + B = (A \cup B) \setminus (A \cap B).$$

Vis, at $(\hat{D}(E), +, \cap)$ er isomorf med ringen $(\hat{F}(E \rightarrow \mathbb{Z}_2), +, \cdot)$ af funktioner fra E til restklasselegemet $(\mathbb{Z}_2, +, \cdot)$. Beskriv mængden $A_1 + A_2 + \dots + A_n$, hvor $A_1, A_2, \dots, A_n$ er delmængder af E .

19. Vis, at $A = \{m + n\sqrt{3} \mid m, n \in \mathbb{Z}\}$ er en delring af de reelle talls legeme $(\mathbb{R}, +, \cdot)$.

I A defineres en ækvivalensrelation $\sim$ ved

$$m + n\sqrt{3} \sim m' + n'\sqrt{3} \iff m \equiv m' \pmod{2} \wedge n \equiv n' \pmod{2}.$$

Vis, at $\sim$ harmonerer med kompositionerne i ringen $(A, +, \cdot)$.

Mængden $\tilde{A}$ af ækvivalensklasser organiseres da som en ring $(\tilde{A}, \tilde{+}, \tilde{\cdot})$ ved regning med repræsentanter.

Angiv antallet af ækvivalensklasser samt en mængde bestående af én repræsentant for hver klasse. Opskriv kompositionstavle for $(\tilde{A}, \tilde{\cdot})$. Er $(\tilde{A}, \tilde{+}, \tilde{\cdot})$ en integritetsring?

20. Idet m og k er naturlige tal og Λ en restklasse modulo m , skal man vise, at mængden $\{ka \mid a \in \Lambda\}$ er en restklasse modulo km .

Idet nu m er et givet naturligt tal, skal man undersøge, for hvilke $k \in \mathbb{N}$ afbildningen $f: \mathbb{Z}_m \rightarrow \mathbb{Z}_{km}$ bestemt ved

$$(x)_m \rightarrow (kx)_{km}, \quad x \in \mathbb{Z},$$

er en homomorf afbildning af restklasseringen $(\mathbb{Z}_m, +, \cdot)$ ind i restklasseringen $(\mathbb{Z}_{km}, +, \cdot)$.

Vis som en anvendelse, at restklasseringen $(\mathbb{Z}_{12}, +, \cdot)$ har et med $(\mathbb{Z}_3, +, \cdot)$ isomorft dellegeme.

21. Find den mindste delring L_1 af de rationale tals legeme $(\mathbb{Q}, +, \cdot)$, som indeholder tallet $\frac{1}{10}$. Angiv endvidere de invertible elementer ved multiplikationen inden for L_1 .

Find den mindste delring L_2 af $(\mathbb{Q}, +, \cdot)$, som indeholder begge tallene $\frac{1}{5}$ og $\frac{1}{5}$. Angiv de invertible elementer ved multiplikationen inden for L_2 .

Er ringene $(L_1, +, \cdot)$ og $(L_2, +, \cdot)$ isomorfe? Er grupperne $(L_1, +)$ og $(L_2, +)$ isomorfe?

22. Lad $(M, +, \cdot)$ være en ring med etelement e . Beskriv den mindste delring, som indeholder e , og vis, at den er isomorf med $(\mathbb{Z}, +, \cdot)$ eller med en restklassering $(\mathbb{Z}_n, +, \cdot)$, $n \in \mathbb{N}$.

Det forudsættes nu, at $(M, +, \cdot)$ er en integritetsring. Vis, at en delring da og kun da er en integritetsring, når den indeholder e , og begrund derved, at $(M, +, \cdot)$ har en mindste delintegritetsring, isomorf med $(\mathbb{Z}, +, \cdot)$ eller med restklasselaget $(\mathbb{Z}_p, +, \cdot)$ modulo et primtal p .

Endelig forudsættes, at $(M, +, \cdot)$ er et kommutativt legeme.

Vis, at det mindste dellegeme er isomorft med $(\mathbb{Q}, +, \cdot)$ eller med restklasselegemet $(\mathbb{Z}_p, +, \cdot)$ modulo et primtal p .

23. Gør rede for, at der pånær isomorfi kun findes én ring med et element, hvor antallet af elementer i ringen er et givet primtal p .

24. En integritetsring, der ikke har nogen ægte delintegritetsring, kaldes en primintegritetsring. Et kommutativt legeme, der ikke har noget ægte dellegeme, kaldes et primlegeme. Gør rede for, at der blandt delringene i en vilkårlig integritetsring er netop én primintegritetsring, blandt dellegemerne i et vilkårligt kommutativt legeme netop ét primlegeme.

Vis, at enhver primintegritetsring er isomorf med $(\mathbb{Z}, +, \cdot)$ eller med restklasselegemet $(\mathbb{Z}_p, +, \cdot)$ modulo et primtal p .

Vis, at ethvert primlegeme er isomorft med $(\mathbb{Q}, +, \cdot)$ eller med restklasselegemet $(\mathbb{Z}_p, +, \cdot)$ modulo et primtal p . (Benyt øv. 22.)

25. Lad $L \subseteq \mathbb{C}$ være et tallegeme og $s \in \mathbb{C}$ et tal, hvor $s \notin L$, men $s^2 \in L$. Det mindste tallegeme indeholdende L og s betegnes $L(s)$. Vis, at

$$L(s) = \{x + ys \mid x, y \in L\},$$

og at afbildningen $(x, y) \rightarrow x + ys$, $x, y \in L$, er en bijektiv afbildning af L^2 på $L(s)$. Vis videre, at der ved

$$x + ys \rightarrow x - ys, \quad x, y \in L,$$

defineres en automorf afbildning af $(L(s), +, \cdot)$.

Eksempler: $\mathbb{R}(i) = \mathbb{C}$, $\mathbb{Q}(\sqrt{2})$.

Findes der et $s \notin \mathbb{Q}$ med $s^2 \in \mathbb{Q}$, så $\mathbb{Q}(s) = \mathbb{R}$? Findes der en følge af tallegemer $L_1, L_2, \dots$ og en følge af tal $s_1, s_2, \dots$, hvor $s_n \notin L_n$, $s_n^2 \in L_n$ og $L_n(s_n) = L_{n+1}$, $n = 1, 2, \dots$, således at $L_1 = \mathbb{Q}$ og $\bigcup_{n=1}^{\infty} L_n = \mathbb{R}$?

26. Vis, at tallegemer $(\mathbb{Q}(s), +, \cdot)$ og $(\mathbb{Q}(t), +, \cdot)$, hvor $s, t \notin \mathbb{Q}$, men $s^2, t^2 \in \mathbb{Q}$, kun er isomorfe hvis $\frac{s}{t} \in \mathbb{Q}$, - i hvilket tilfælde jo $\mathbb{Q}(s) = \mathbb{Q}(t)$. (Se øv. 25.)

Kap. III. Lineær algebra og analytisk geometri.§1. Vektorrum.Definition.

Lad $(V, +)$ være en kommutatativ gruppe, hvis komposition betegnes som addition. Elementerne i V betegnes (på samme måde som geometriske vektorer) med understregede bogstaver. Gruppens neutrale element skrives $\underline{0}$ og det til et element $\underline{v} \in V$ inverse $-\underline{v}$. For vilkårligt givne $\underline{u}, \underline{v} \in V$ har ligningen $\underline{u} + \underline{x} = \underline{v}$ en og kun én løsning, nemlig $\underline{x} = \underline{v} + (-\underline{u})$, som også skrives $\underline{v} - \underline{u}$. Specielt er altså $\underline{0} - \underline{v} = -\underline{v}$ og $\underline{v} - \underline{v} = \underline{0}$ for hvert element $\underline{v} \in V$. Hvis $\underline{x} \in V$ blot for ét element $\underline{v} \in V$ tilfredsstiller ligningen $\underline{v} + \underline{x} = \underline{v}$, kan man altså slutte, at $\underline{x} = \underline{0}$. Forkortningsreglerne udsiger her, at man af $\underline{u} + \underline{w} = \underline{v} + \underline{w}$ kan slutte, at $\underline{u} = \underline{v}$.

Lad $(L, +, \cdot)$ være et legeme, hvis kompositioner betegnes som addition og multiplikation. Skønt meget af det følgende også er gyldigt for legemer med ikke-kommutativ multiplikation, vil vi her kun tage kommutive legemer i betragtning.

Det antages, at der er defineret en komposition $L \times V \rightarrow V$, som altså til hvert par $(\lambda, \underline{v})$, $\lambda \in L$, $\underline{v} \in V$, lader svare et element af V , som skrives $\lambda \underline{v}$ eller $\underline{v} \lambda$ og kaldes produktet af λ og $\underline{v}$. Når denne komposition opfylder visse nedenfor angivne krav, siges V at være et vektorrum over legemet L og betegnes da $(V, +, L)$. Elementerne af V kaldes for vektorer og elementerne af L i denne forbindelse hyppigt for skalarer. Brugen af disse gloser er motiveret ved, at mængden V_3 af geometriske vektorer i rummet med vektoradditionen som komposition opfylder kravene med $L = \mathbb{R}$, når produktet af et reelt tal og en geometrisk vektor defineres på den velkendte måde. De geometriske vektorer danner altså et vektor-

rum $(V, +, \cdot)$ over de reelle tals legeme.

Den fuldstændige definition på et vektorrum $(V, +, \cdot)$ kan formuleres således:

Definition. En mængde $V \neq \emptyset$ siges at være et vektorrum over et legeme L , hvis der er defineret en komposition $+$ i V ,

$$\text{VR1. } \forall \underline{u}, \underline{v} : \underline{u} + \underline{v} \in V,$$

for hvilken

$$\text{VR2. } \forall \underline{u}, \underline{v} : \underline{u} + \underline{v} = \underline{v} + \underline{u},$$

$$\text{VR3. } \forall \underline{u}, \underline{v}, \underline{w} : \underline{u} + (\underline{v} + \underline{w}) = (\underline{u} + \underline{v}) + \underline{w}.$$

$$\text{VR4. } \exists \underline{0} \forall \underline{v} : \underline{v} + \underline{0} = \underline{v},$$

$$\text{VR5. } \forall \underline{v} \exists \underline{-v} : \underline{v} + (\underline{-v}) = \underline{0},$$

og hvis der er defineret en komposition $L \times V \rightarrow V$, betegnet som multiplikation,

$$\text{VR6. } \forall \lambda \forall \underline{v} : \lambda \underline{v} = \underline{v} \lambda \in V,$$

for hvilken

$$\text{VR7. } \forall \lambda, \mu \forall \underline{v} : \lambda(\mu \underline{v}) = (\lambda \mu) \underline{v},$$

$$\text{VR8. } \forall \lambda, \mu \forall \underline{v} : (\lambda + \mu) \underline{v} = \lambda \underline{v} + \mu \underline{v},$$

$$\text{VR9. } \forall \lambda \forall \underline{u}, \underline{v} : \lambda(\underline{u} + \underline{v}) = \lambda \underline{u} + \lambda \underline{v},$$

$$\text{VR10. } \forall \underline{v} : \varepsilon \underline{v} = \underline{v},$$

hvor ε betegner etelementet, dvs. det neutrale element for multiplikationen i L .

Af VR3 følger, at man ved additionen af flere end to vektorer kan undvære parenteser til angivelse af den orden, hvori additionerne udføres. Tilsvarende gælder ifølge VR7 for multiplikationen af en vektor med flere skalarer. I almindeliggørelse af VR2 haves, at en sum af flere vektorer ikke afhænger af disses rækkefølge. De distributive love VR8 og VR9 kan udvides til et vilkårligt (endeligt) antal summander.

Om multiplikationen af vektorer med skalarer gælder nogle simple regler, som ofte vil blive anvendt. Med $\underline{o}$ betegnes nulelementet, dvs. det neutrale element for additionen i L , med λ, μ vilkårlige skalarer og med $\underline{u}, \underline{v}$ vilkårlige vektorer.

$$\lambda \underline{0} = \underline{0}$$

$$\text{Bevis: } \lambda \underline{0} = \lambda(\underline{0} + \underline{0}) = \lambda \underline{0} + \lambda \underline{0}.$$

$$\underline{o} \underline{v} = \underline{0}$$

$$\text{Bevis: } \underline{o} \underline{v} = (\underline{o} + \underline{o}) \underline{v} = \underline{o} \underline{v} + \underline{o} \underline{v}.$$

$$\text{Nulreglen: } \lambda \underline{v} = \underline{0} \Rightarrow \lambda = \underline{o} \vee \underline{v} = \underline{0}.$$

Bevis: Er $\lambda \neq \underline{o}$, fås af $\underline{0} = \lambda \underline{v}$, at

$$\underline{0} = \lambda^{-1} \underline{0} = \lambda^{-1}(\lambda \underline{v}) = (\lambda^{-1} \lambda) \underline{v} = \underline{e} \underline{v} = \underline{v}.$$

$$(\mu - \lambda) \underline{v} = \mu \underline{v} - \lambda \underline{v},$$

specielt ($\mu = \underline{o}$)

$$(-\lambda) \underline{v} = -(\lambda \underline{v}).$$

$$\text{Bevis: } (\mu - \lambda) \underline{v} + \lambda \underline{v} = ((\mu - \lambda) + \lambda) \underline{v} = \mu \underline{v}.$$

$$\lambda(\underline{v} - \underline{u}) = \lambda \underline{v} - \lambda \underline{u},$$

specielt ($\underline{v} = \underline{0}$)

$$\lambda(-\underline{u}) = -(\lambda \underline{u}).$$

$$\text{Bevis: } \lambda(\underline{v} - \underline{u}) + \lambda \underline{u} = \lambda((\underline{v} - \underline{u}) + \underline{u}) = \lambda \underline{v}.$$

Eksempel.

En meget omfattende og overordentlig vigtig klasse af vektorrum over et legeme L fås på følgende måde.

Lad der være givet en vilkårlig mængde T . Med $\hat{F}(T \rightarrow L)$ betegnes mængden af alle funktioner med T som definitions-mængde og med værdier i L . For $\varphi, \psi \in \hat{F}(T \rightarrow L)$ forstås ved $\varphi + \psi$ den ved

$$t \rightarrow \varphi(t) + \psi(t) \quad \text{for } t \in T$$

bestemte funktion tilhørende $\hat{F}(T \rightarrow L)$. Det er indlysende, at

$\hat{F}(T \rightarrow L)$ med denne addition som komposition er en kommutativ gruppe.

Dens neutrale element er den konstante funktion bestemt ved $t \rightarrow 0$ for $t \in T$, og det til ϕ modsatte element er funktionen bestemt ved $t \rightarrow -\phi(t)$ for $t \in T$. For $\phi \in \hat{F}(T \rightarrow L)$ og $\lambda \in L$ forstås ved $\lambda\phi$ den ved

$$t \mapsto \lambda\phi(t) \quad \text{for } t \in T$$

bestemte funktion tilhørende $\hat{F}(T \rightarrow L)$. Det er indlysende, at med den således definerede komposition $L \times \hat{F}(T \rightarrow L) \rightarrow L$ er kravene VR6-10 opfyldt, så at

$$(\hat{F}(T \rightarrow L), +, L)$$

er et vektorrum.

Af særlig betydning er de tilfælde, hvor T er en endelig mængde. Er n antallet af dens elementer, betegnes disse med $1, \dots, n$, og elementerne i $\hat{F}(T \rightarrow L)$ kan da skrives som n -sæt $(x_1, \dots, x_n)$ med elementer fra L . Her er altså $\hat{F}(T \rightarrow L) = L^n$, vektorrummets betegnelse bliver $(L^n, +, L)$ og kompositionerne

$$\begin{aligned} (x_1, \dots, x_n) + (y_1, \dots, y_n) &= (x_1 + y_1, \dots, x_n + y_n), \\ \lambda(x_1, \dots, x_n) &= (\lambda x_1, \dots, \lambda x_n). \end{aligned}$$

For $n = 1$ fås selve legemet L som et vektorrum over sig selv. Dets elementer skal da fortolkes som både skalarer og vektorer.

Andre for analysen vigtige tilfælde fås for $T = \mathbb{N}$. Elementerne i $\hat{F}(T \rightarrow L)$ er da følgerne $(x_1, x_2, \dots)$ af elementer fra L . Kompositionerne bliver

$$\begin{aligned} (x_1, x_2, \dots) + (y_1, y_2, \dots) &= (x_1 + y_1, x_2 + y_2, \dots) \\ \lambda(x_1, x_2, \dots) &= (\lambda x_1, \lambda x_2, \dots) \end{aligned}$$

Dette følgerum over L betegnes med $(L^{\mathbb{N}}, +, L)$

I det følgende vil vi nøjes med at undersøge vektorrum over tallegemer, dvs. dellegemer af de komplekse tals legeme $(\mathbb{C}, +, \cdot)$ med sædvanlig addition og multiplikation som kompositioner. Et

tallegeme $(L, +, \cdot)$ udgøres altså af en delmængde L af $\mathbb{C}$, som indeholder mindst ét fra 0 forskelligt tal, og for hvilken det gælder, at når λ og μ tilhører L , vil $\lambda + \mu$, $\lambda - \mu$, $\lambda\mu$ og, såfremt $\mu \neq 0$, også λ/μ tilhøre L . Heraf kan sluttet, at ethvert tallegeme $(L, +, \cdot)$ indeholder de rationale tals legeme $(\mathbb{Q}, +, \cdot)$ som dellegeme. Er nemlig λ et fra 0 forskelligt tal i L , vil $\lambda/\lambda = 1$, altså også $1 + 1 = 2$, $2 + 1 = 3, \dots$, altså alle tal $n \in \mathbb{N}$, endvidere $1 - 1 = 0$ og $0 - n$ for $n \in \mathbb{N}$, altså alle tal $p \in \mathbb{Z}$, og endelig p/n for $p \in \mathbb{Z}$ og $n \in \mathbb{N}$, altså alle rationale tal tilhøre L .

Lad $(V, +, L)$ være et vektorrum over et tallegeme L . I VR10 og de udledte regler kan da skrives 1 i stedet for ε og 0 i stedet for o . For $n \in \mathbb{N}$ og $v \in V$ haves ifølge VR8 og VR10

$$\begin{aligned} n\underline{v} &= (1 + 1 + \dots + 1)\underline{v} = 1\underline{v} + 1\underline{v} + \dots + 1\underline{v} \\ &= \underline{v} + \underline{v} + \dots + \underline{v} \end{aligned}$$

med n summander. Dette viser, at $n\underline{v}$ er den n -te "potens" af $\underline{v}$ i gruppen $(V, +)$. Idet $0\underline{v} = \underline{0}$, som vist ovenfor, er $0\underline{v}$ det neutrale element, altså den 0-te "potens" af $\underline{v}$ i $(V, +)$. Af $(-n)\underline{v} = -(n\underline{v})$ for $n \in \mathbb{N}$ sluttet, at $(-n)\underline{v}$ er den $-n$ -te "potens" af $\underline{v}$ i $(V, +)$. Specielt haves $(-1)\underline{v} = -(1\underline{v}) = -\underline{v}$.

Linearkombinationer.

Lad $(V, +, L)$ være et vektorrum. Er $\underline{v}_1, \dots, \underline{v}_p$ vilkårlige vektorer i V og $\lambda_1, \dots, \lambda_p$ vilkårlige tal i L , vil også

$$\underline{v} = \lambda_1 \underline{v}_1 + \dots + \lambda_p \underline{v}_p = \sum_{i=1}^p \lambda_i \underline{v}_i$$

være en vektor i V , som kaldes en linearkombination af vektorerne $\underline{v}_1, \dots, \underline{v}_p$. Er to eller flere af vektorerne $\underline{v}_1, \dots, \underline{v}_p$ ens, kan de pågældende led ifølge VR9 sammenfattes til ét. Forekommer nulvektoren $\underline{0}$ blandt vektorerne $\underline{v}_1, \dots, \underline{v}_p$ eller 0 blandt tallene

$\lambda_1, \dots, \lambda_p$, kan de pågældende led udelades. I disse tilfælde kan $\underline{v}$ altså skrives som en linearkombination af færre vektorer. På den anden side kan man altid tilføje $\underline{0}$ med en vilkårlig talkoefficient og andre vektorer med koefficienten 0.

Produktet af en linearkombination med en skalar kan ifølge VR9 og VR7 skrives som en linearkombination af de samme vektorer. Summen af to linearkombinationer kan skrives som linearkombination af de vektorer, der forekommer i de givne. Det samme gælder for differensen af to linearkombinationer, hvilket ses ved hjælp af omskrivningen $\underline{u} - \underline{v} = \underline{u} + (-1)\underline{v}$.

Underrum.

Lad $(V, +, L)$ være et vektorrum. En ikke tom delmængde U af V kaldes et underrum eller delrum af det, hvis den er et vektorrum med restriktionerne til $U \times U$ og $L \times U$ af det givne vektorrums kompositioner. Nødvendige betingelser for, at en delmængde U af V er et underrum, er øjensynlig

$$\text{UR1. } \forall_U \underline{u}, \underline{v} : \underline{u} + \underline{v} \in U,$$

$$\text{UR2. } \forall_L \lambda \forall_U \underline{v} : \lambda \underline{v} \in U,$$

idet disse jo udsiger, at de nævnte restriktioner er henholdsvis en komposition i U og en komposition fra $L \times U$ til U . Disse betingelser er også tilstrækkelige. Er nemlig $\underline{u}$ en vilkårlig vektor i U , vil $-\underline{u} = (-1)\underline{u} \in U$ ifølge UR2, hvorpå $\underline{0} = \underline{u} + (-\underline{u}) \in U$ følger af UR1. Heraf fremgår, at VR1, VR4, VR5 og VR6 er opfyldt for U . De resterende krav til et vektorrum er regneregler, som er selvfølgelig gyldige for vektorerne i U , da de er det for alle vektorer i V .

UR1-2 ses let at være ensbetydende med

$$\text{UR. } \forall_L \lambda, \mu \forall_U \underline{u}, \underline{v} : \lambda \underline{u} + \mu \underline{v} \in U.$$

En delmængde U af V er altså et underrum, hvis alle linearkombinationer af vilkærlig mange vektorer i U tilhører U .

Det ses umiddelbart, at $\{0\}$ og V er underrum af vektorrummet $(V, +, L)$.

Et underrum af et underrum af $(V, +, L)$ er også et underrum af $(V, +, L)$.

Ved hjælp af UR ses, at fællesmængden for vilkårlig (endelig eller uendelig) mange underrum af et vektorrum er ligelædes et underrum af dette.

Lad der være givet et vektorrum $(V, +, L)$ og en ikke tom delmængde M af V . Der findes mindst et underrum, som indeholder M , nemlig V . Fællesmængden for alle underrum, som indeholder M , er det "mindste" sådanne underrum i den forstand, at det er indeholdt i ethvert andet. Dette underrum, som betegnes $V(M)$, kan også bestemmes på en anden måde. Hvert underrum, som indeholder M , vil indeholde hver linearkombination af endelig mange vektorer tilhørende M . Mængden U af alle disse linearkombinationer er altså en delmængde af $V(M)$. På den anden side indeholder U øjensynlig vektorerne i M og er et underrum; thi idet summen af to linearkombinationer af vektorer tilhørende M såvel som produktet af en skalar og en linearkombination af vektorer tilhørende M igen kan skrives som linearkombination af vektorer i M , er UR1-2 opfyldt. Følgelig gælder $V(M) \subseteq U$, altså $V(M) = U$. Man kalder $V(M)$ det af M frembragte underrum af $(V, +, L)$.

Er M specielt en mængde bestående af endelig mange vektorer, kan hver linearkombination af nogle af dem skrives som en linearkombination af dem alle, idet de eventuelt manglende kan tilføjes med faktoren 0. Det af en endelig delmængde M frembragte underrum består altså af alle linearkombinationer af samtlige vektorer til-

hørende M .

Det geometriske vektorrum $(V_3, +, \mathbb{R})$ har foruden $\{0\}$ og sig selv to slags underrum. Et underrum af den ene slags udgøres af alle geometriske vektorer, som, afsat fra samme punkt, ligger på en linie. Det frembringes af en hvilken som helst egentlig vektor parallel med linien. Et underrum af den anden slags udgøres af alle geometriske vektorer, som, afsat fra samme punkt, ligger i en plan. Det frembringes af hvilke som helst to egentlige vektorer, som er parallelle med planen, men ikke indbyrdes parallelle. Det er let at se, at der ikke kan findes andre underrum.

Funktionsrum $(\hat{F}(T \rightarrow L), +, L)$ har i almindelighed mange forskellige underrum. Der anføres nogle eksempler.

De funktioner $\varphi: T \rightarrow L$, som på en opgiven delmængde T' af T er konstant lig 0, udgør et underrum i $(\hat{F}(T \rightarrow L), +, L)$. Erstattes 0 med et andet tal i L , fås ikke noget underrum.

En funktion $\varphi: T \rightarrow L$, siges at være begrænset, når der findes et positivt tal k , således at $|\varphi(t)| \leq k$ for $t \in T$. De funktioner $\varphi: T \rightarrow L$, som hver for sig er begrænset, udgør et underrum i $(\hat{F}(T \rightarrow L), +, L)$. Derimod er mængden af funktioner, som er begrænset ved et og samme tal $k > 0$, ikke noget underrum.

Er T et topologisk, specielt et metrisk, rum, og tænkes tallegemet L forsynet med den sædvanlige metrik, $\text{dist}(\lambda, \mu) = |\mu - \lambda|$, vil mængden $\hat{C}(T \rightarrow L)$ af de kontinuerte funktioner $\varphi: T \rightarrow L$ være et underrum i $(\hat{F}(T \rightarrow L), +, L)$.

Lad $T \subseteq \mathbb{R}$ være et interval og $L = \mathbb{R}$. For hvert naturligt tal p er da mængden $\hat{D}^p(T \rightarrow \mathbb{R})$ af de i T definerede reelle funktioner, som er p gange differentiable, et underrum i $(\hat{F}(T \rightarrow \mathbb{R}), +, L)$. Det samme gælder for mængden $\hat{C}^p(T \rightarrow \mathbb{R})$ af funktioner, som er p gange

kontinuert differentiable (dvs. har en kontinuert p -te afledet). Mængden af vilkårlig ofte differentiable funktioner er ligeledes et underrum. Tilsvarende gælder for funktioner $\varphi: T \rightarrow \mathbb{C}$.

Et eksempel på et underrum i følgerummet $(\mathbb{R}^{\mathbb{N}}, +, \mathbb{R})$ er mængden af alle konvergente følger. Et underrum i dette er mængden af alle følger, der konvergerer mod 0, og et underrum heraf er mængden af alle følger $(x_1, x_2, \dots)$, for hvilke den uendelige række $x_1 + x_2 + \dots$ er konvergent. Tilsvarende gælder for $(\mathbb{C}^{\mathbb{N}}, +, \mathbb{C})$.

Underrummene i talrummene $(L^n, +, L)$ vil blive behandlet i de følgende paragraffer.

Lineær afhængighed og uafhængighed.

Lad $(V, +, L)$ være et vektorrum. Et sæt $(\underline{v}_1, \dots, \underline{v}_p)$ af endelig mange vektorer fra V kaldes lineært afhængigt, hvis der findes skalarer $\lambda_1, \dots, \lambda_p$, som ikke alle er 0, således at

$$\lambda_1 \underline{v}_1 + \dots + \lambda_p \underline{v}_p = \underline{0}.$$

Hvis der ikke findes sådanne skalarer, med andre ord, hvis ligningen kun er tilfredsstillet, når $\lambda_1 = \dots = \lambda_p = 0$, siges sættet at være lineært uafhængigt. En ligning af ovenstående form kaldes en lineær relation mellem de p vektorer; den kaldes egentlig, hvis ikke alle koefficienter $\lambda_1, \dots, \lambda_p$ er 0. Vektorerne $\underline{v}_1, \dots, \underline{v}_p$ er altså lineært afhængige eller lineært uafhængige, ^{består} efter som der består en eller ikke nogen egentlig lineær relation imellem dem.

At én vektor $\underline{v}$ er lineært afhængig, altså at der findes en skalar $\lambda \neq 0$, således at $\lambda \underline{v} = \underline{0}$, er ensbetydende med, at $\underline{v} = \underline{0}$.

Når et delset af et vektorsæt er lineært afhængigt, er hele

sættet lineært afhængigt; thi i en egentlig lineær relation mellem en del af vektorerne kan sættets øvrige vektorer tilføjes med koefficienten 0. Ensbetydende hermed er: Hvert delsat af et lineært uafhængigt sæt er lineært uafhængigt.

Et vektorsæt, hvori nulvektoren forekommer, er altså lineært afhængigt. Det samme gælder for et vektorsæt, hvori der forekommer to ens vektorer. Når talen er om lineær afhængighed, må følgelig vektorsættet $(\underline{v}_1, \dots, \underline{v}_p)$ ikke sammenblandes med mængden $\{\underline{v}_1, \dots, \underline{v}_p\}$ bestående af dets indbyrdes forskellige vektorer.

Lad J være en endelig indexmængde. En indiceret mængde $(\underline{v}_i)_{i \in J}$ af vektorer i V siges at være lineært afhængig, hvis der findes et lineært afhængigt endeligt delsat, og lineært uafhængigt, hvis ethvert endeligt delsat er lineært uafhængigt.

Vektorer $\underline{v}_1, \dots, \underline{v}_p$ er lineært afhængige, hvis og kun hvis mindst en af dem kan fremstilles som en linearkombination af de øvrige.

Bevis: Betingelsen er nødvendig. Er nemlig

$$\lambda_1 \underline{v}_1 + \dots + \lambda_p \underline{v}_p = \underline{0}$$

en egentlig lineær relation mellem vektorerne, altså f.eks. $\lambda_1 \neq 0$, fås ved additionen af $-\lambda_1 \underline{v}_1$ på begge sider og påfølgende multiplikation med $-1/\lambda_1$

$$\underline{v}_1 = \left(-\frac{\lambda_2}{\lambda_1}\right) \underline{v}_2 + \dots + \left(-\frac{\lambda_p}{\lambda_1}\right) \underline{v}_p.$$

Betingelsen er også tilstrækkelig. Er nemlig f.eks.

$$\underline{v}_1 = \mu_2 \underline{v}_2 + \dots + \mu_p \underline{v}_p,$$

fås ved addition af $-\underline{v}_1 = (-1)\underline{v}_1$ på begge sider

$$(-1)\underline{v}_1 + \mu_2 \underline{v}_2 + \dots + \mu_p \underline{v}_p = \underline{0},$$

og dette er en egentlig lineær relation mellem vektorerne.

Herefter er to vektorer lineært afhængige, hvis og kun hvis en af dem er et skalært multiplum af den anden. Dette udtrykkes

ofte ved at sige, at den pågældende vektor er proportional med den anden.

Hvis en vektor $\underline{v}$ kan fremstilles som linearkombination af vektorer $\underline{v}_1, \dots, \underline{v}_p$, vil fremstillingens koefficienter være entydigt bestemte, hvis og kun hvis $\underline{v}_1, \dots, \underline{v}_p$ er lineært uafhængige.

Bevis: Lad

$$\underline{v} = \lambda_1 \underline{v}_1 + \dots + \lambda_p \underline{v}_p, \quad \underline{v} = \mu_1 \underline{v}_1 + \dots + \mu_p \underline{v}_p$$

være fremstillinger af $\underline{v}$. Ved subtraktion fås

$$(\mu_1 - \lambda_1) \underline{v}_1 + \dots + (\mu_p - \lambda_p) \underline{v}_p = \underline{0}.$$

Er $\underline{v}_1, \dots, \underline{v}_p$ lineært uafhængige, kan man heraf slutte, at $\mu_1 - \lambda_1 = \dots = \mu_p - \lambda_p = 0$, altså at de to fremstillinger stemmer overens. Dette viser, at betingelsen er tilstrækkelig. Findes der en egentlig lineær relation

$$\underline{0} = \nu_1 \underline{v}_1 + \dots + \nu_p \underline{v}_p,$$

fås ved at addere den til en fremstilling af $\underline{v}$ en ny fremstilling, forskellig fra den forrige. Dette viser, at betingelsen er nødvendig.

Som eksempler nævnes følgende:

To (tre) geometriske vektorer er lineært afhængige, hvis og kun hvis de, afsat fra samme punkt, ligger på samme linie (i samme plan). Hvilkesomhelst fire geometriske vektorer er lineært afhængige.

Vektorerne

$$\underline{v}_1 = (1, 0, 0, \dots, 0),$$

$$\underline{v}_2 = (0, 1, 0, \dots, 0),$$

$$\vdots \quad \quad \quad \vdots$$

$$\underline{v}_n = (0, 0, 0, \dots, 1)$$

i talrummet $(L^n, +, L)$ er lineært uafhængige, idet

$$\lambda_1 \underline{v}_1 + \dots + \lambda_n \underline{v}_n = (\lambda_1, \dots, \lambda_n)$$

kun er lig $(0, \dots, 0)$, når $\lambda_1 = \dots = \lambda_n = 0$.

Konstanten 1 og funktionerne $\cos$ og $\sin$ er tre lineært uafhængige vektorer i $(\hat{F}(\mathbb{R} \rightarrow \mathbb{R}), +, \mathbb{R})$. Er nemlig λ, μ, ν reelle tal, for hvilke

$$\forall_{\mathbb{R}} t : \lambda + \mu \cos t + \nu \sin t = 0,$$

fås ved at indsætte $t = 0$ og $t = \pi$ henholdsvis $\lambda + \mu = 0$ og $\lambda - \mu = 0$, altså $\lambda = \mu = 0$, og derefter ved at indsætte f.eks. $t = \frac{1}{2}\pi$, at også $\nu = 0$.

Potenserne t^p , $p = 0, 1, \dots$, udgør et uendeligt, lineært uafhængigt sæt i vektorrummet $(\hat{F}(T \rightarrow \mathbb{C}), +, \mathbb{C})$ eller $(\hat{F}(T \rightarrow \mathbb{R}), +, \mathbb{R})$, når T er en uendelig delmængde af henholdsvis $\mathbb{C}$ eller $\mathbb{R}$. En linearkombination af endelig mange potenser er nemlig et polynomium, og hvis ikke alle koefficienter er 0, vil det kun have endelig mange rødder og følgelig ikke være 0 for alle $t \in T$.

Rang, dimension, basis.

Lad $(V, +, L)$ være et vilkårligt vektorrum og M en ikke tom delmængde af V . Der foreligger da to muligheder. Enten findes der for hvert naturligt tal p et sæt af mindst p lineært uafhængige vektorer i M . I dette tilfælde siges M at have rang uendelig, og man skriver

$$\text{rg } M = \infty.$$

Eller antallet af vektorer i lineært uafhængige delmængder af M er opad begrænset. Det største af disse antal er et helt tal $r \geq 0$, for hvilket det gælder, at der findes r lineært uafhængige vektorer i M , medens hvilkensomhelst $r + 1$ vektorer i M er lineært afhængige. Man siger da, at M har rang r og skriver

$$\text{rg } M = r.$$

Hvert sæt af r lineært uafhængige vektorer fra M kaldes et maximalsæt for M . At $r = 0$, er ensbetydende med, at $M = \{0\}$.

Er mængden M et vektorrum, altså et underrum U i $(V, +, L)$, specielt hele V , kaldes dens rang for vektorrummets dimension og betegnes $\dim(U, +, L)$ eller ofte kort $\dim U$.

Et vektorrum bestående af én vektor, som så må være nulvektor, og kun et sådant, har dimensionen 0.

Lad M være en vektormængde af endelig rang r i et vektorrum $(V, +, L)$, og lad $(\underline{v}_1, \dots, \underline{v}_r)$ være et maximalsæt i M . Da kan hver vektor $\underline{v}$ i M på en og kun én måde fremstilles som linearkombination af $\underline{v}_1, \dots, \underline{v}_r$.

Bevis: De $r + 1$ vektorer $\underline{v}_1, \dots, \underline{v}_r, \underline{v}$ er lineært afhængige. I en egentlig lineær relation mellem dem kan koefficienten til $\underline{v}$ ikke være 0, da der ellers ville bestå en egentlig lineær relation mellem $\underline{v}_1, \dots, \underline{v}_r$ i strid med, at disse vektorer er lineært uafhængige. Følgelig kan $\underline{v}$ fremstilles som en linearkombination af $\underline{v}_1, \dots, \underline{v}_r$. At fremstillingen er entydig bestemt, fremgår af en tidligere sætning.

Anvendes dette specielt på $M = V$, hvor V er et endelig-dimensionalt vektorrum, fås:

Hvert maximalsæt i et endelig-dimensionalt vektorrum frembringer dette rum.

For hvert underrum U i et vektorrum $(V, +, L)$ gælder

$$\dim U \leq \dim V,$$

og hvis $\dim V$ er endelig, består lighed kun for $U = V$.

Bevis: Hvis $\dim V = \infty$ er intet at bevise. Hvis $\dim V = n$ er endelig, kan der i delmængden U af V ikke findes lineært uaf-

hængige sæt bestående af flere end n vektorer. Heraf følger ulighedens gyldighed. Er $\dim U = \dim V = n$, vil et maximalsæt i U til lige være maximalsæt i V . Ifølge den foregående sætning er da både U og V det af et sådant sæt frembragte underrum, altså $U = V$.

Hvis $V = \infty$, kan man af $\dim U = \dim V$ for et underrum $U \subseteq V$ ikke slutte, at $U = V$. Som eksempel kan nævnes, at mængden af reelle talfølger, som konvergerer mod 0, er et uendelig-dimensionalt, ægte underrum i følgerummet $(\mathbb{R}^{\mathbb{N}}, +, \cdot)$.

Ved en basis for et vektorrum $(V, +, L)$ forstås en indiceret mængde af vektorer fra V , som er lineært uafhængig og frembringer V .

Hvert endelig-dimensionalt vektorrum har baser, nemlig maximalsættene, idet et sådant, som vist ovenfor, frembringer rummet og ifølge definition er lineært uafhængigt. Det er oplagt, at antallet af vektorer i en basis er højst lig rummets dimension. Det vil frørgå af nedenstående udskiftningssætning, at det altid er lig med dimensionen, altså at hver basis er et maximalsæt.

Også hvert uendelig-dimensionalt vektorrum har baser. Dette vil imidlertid ikke blive bevist her.

At et sæt $(e_1, \dots, e_p)$ af endelig mange vektorer i et vektorrum $(V, +, L)$ er en basis, er ensbetydende med, at hver vektor i V på en og kun én måde kan fremstilles som en linearkombination af $e_1, \dots, e_p$. Dette er en umiddelbar følge af sætningen om entydigheden af en vektors fremstilling som linearkombination (side III, 1, 11).

En uendelig indiceret mængde $(\underline{v}_i), i \in J$, af vektorer i et vektorrum $(V, +, L)$ er en basis, hvis og kun hvis hver vektor i V har en og kun én fremstilling som linearkombination af endelig

mange vektorer $\underline{v}_i$ med fra 0 forskellige koefficienter.

Som allerede antydnet, følger vigtige egenskaber ved baser af følgende "udskiftningssætning" (H. Grassmann, 1844, E. Steinitz, 1910):

Lad $(V, +, L)$ være et vilkårligt vektorrum, $\underline{v}_1, \dots, \underline{v}_q$ vektorer i V og U det af disse frembragte underrum. Lad endvidere $\underline{u}_1, \dots, \underline{u}_p$ være lineært uafhængige vektorer i U . Da er $p \leq q$, og der findes $q - p$ blandt vektorerne $\underline{v}_1, \dots, \underline{v}_q$, som sammen med $\underline{u}_1, \dots, \underline{u}_p$ frembringer U .

Bevis: Ifølge forudsætning er $\underline{u}_1$ som vektor i U en linearkombination af $\underline{v}_1, \dots, \underline{v}_q$. I denne må mindst én af disse vektorer optræde med fra 0 forskellig koefficient, da $\underline{u}_1$ som lineært uafhængig vektor er forskellig fra $\underline{0}$. Man kan tænke sig vektorerne $\underline{v}_i$ nummeret således, at $\underline{v}_1$ har en koefficient forskellig fra 0. Da kan $\underline{v}_1$ fremstilles som en linearkombination af $\underline{u}_1, \underline{v}_2, \dots, \underline{v}_q$. Men dette medfører, at hver vektor $\underline{x} \in U$ er en linearkombination af disse vektorer; thi ifølge forudsætning er $\underline{x}$ en linearkombination af $\underline{v}_1, \dots, \underline{v}_q$, og i denne kan vektoren $\underline{v}_1$ erstattes med den nævnte linearkombination af $\underline{u}_1, \underline{v}_2, \dots, \underline{v}_q$. I sættet $(\underline{v}_1, \dots, \underline{v}_q)$ kan følgende $\underline{v}_1$ erstattes med $\underline{u}_1$, uden at det mister egenskaben at frembringe U . Specielt er altså $\underline{u}_2$ en linearkombination af $\underline{u}_1, \underline{v}_2, \dots, \underline{v}_q$. I denne må mindst én af vektorerne $\underline{v}_2, \dots, \underline{v}_q$ optræde med fra 0 forskellig koefficient, da $\underline{u}_1$ og $\underline{u}_2$ er lineært uafhængige. Lad nummereringen af vektorerne være valgt således, at det gælder for $\underline{v}_2$. Da kan $\underline{v}_2$ fremstilles som linearkombination af $\underline{u}_1, \underline{u}_2, \underline{v}_3, \dots, \underline{v}_q$, og man ser som før, at disse vektorer frembringer U . På denne måde fortsættes. Var nu $p > q$, ville man få vektorerne $\underline{v}_1, \dots, \underline{v}_q$ erstattet med $\underline{u}_1, \dots, \underline{u}_q$, og de resterende

vektorer $\underline{u}_{q+1}, \dots, \underline{u}_p$ ville være linearkombinationer af $\underline{u}_1, \dots, \underline{u}_q$, hvilket er umuligt, da $\underline{u}_1, \dots, \underline{u}_p$ er lineært uafhængige. Dermed er sætningen bevist.

En umiddelbar følge af sætningen er:

Dimensionen af et vektorrum, som frembringes af et sæt af q vektorer, er højst q ; thi antallet af vektorer i et lineært uafhængigt sæt er højst q .

Ved hjælp heraf fås:

Antallet af vektorer i en basis for et endelig-dimensionalt vektorrum er lig med rummets dimension. Da en basis frembringer rummet, kan dettes dimension ikke være større end antallet af vektorer i den. Men dimensionen kan heller ikke være mindre, da vektorerne er lineært uafhængige.

Sammen med et tidligere resultat giver dette:

Et sæt af vektorer i et endelig-dimensionalt vektorrum er en basis, hvis og kun hvis det er et maximalsæt.

For hver delmængde M af et vektorrum $(V, +, L)$ gælder

$$\text{rg } M = \dim V(M).$$

Bevis: Er $\text{rg } M = \infty$, haves øjensynlig også $\dim V(M) = \infty$. Er $\text{rg } M = r$ endelig og $(\underline{v}_1, \dots, \underline{v}_r)$ et maximalsæt i M , kan hver vektor i M fremstilles som en linearkombination af $\underline{v}_1, \dots, \underline{v}_r$. Det samme gælder da for hver vektor i $V(M)$, da den jo er linearkombination af vektorer tilhørende M . Sættet $(\underline{v}_1, \dots, \underline{v}_r)$ frembringer altså $V(M)$, og idet det er lineært uafhængigt, er det en basis for $V(M)$. Ifølge den foregående sætning er antallet r af vektorer da lig med $\dim V(M)$ som påstået.

Hvert lineært uafhængigt sæt $(\underline{u}_1, \dots, \underline{u}_p)$ i et n -dimensionalt vektorrum $(V, +, L)$ kan, når $p < n$, suppleres til en basis for V

ved tilføjelse af passende vektorer $\underline{u}_{p+1}, \dots, \underline{u}_n$ fra V .

Bevis: Lad $(\underline{v}_1, \dots, \underline{v}_n)$ være en basis for V . Erstatte visse p af dens vektorer med $\underline{u}_1, \dots, \underline{u}_p$, fås ifølge udskiftningssætningen et sæt af n vektorer, som frembringer V . Ifølge den foregående sætning er dette sæts rang lig med dimensionen n af V . Sættet er altså lineært uafhængigt og dermed en basis for V .

Eksempler.

1) Det geometriske vektorrum $(V_3, +, \mathbb{R})$ har dimension 3. Hvert sæt af 3 vektorer, som afsat fra samme punkt ikke ligger i samme plan, er en basis for V_3 . Underrummene kan altså kun have dimensionerne 0, 1, 2 eller 3. Det eneste 0-dimensionale underrum er $\{\underline{0}\}$. Hvert 1-dimensionalt underrum har som basis en vektor $\underline{e}_1 \neq \underline{0}$ og består af alle vektorer $\lambda_1 \underline{e}_1, \lambda_1 \in \mathbb{R}$, altså af alle vektorer, som afsat fra samme punkt ligger på linien parallel med $\underline{e}_1$ gennem punktet. Hvert 2-dimensionalt underrum har en basis bestående af to vektorer $\underline{e}_1$ og $\underline{e}_2$, som afsat fra samme punkt ikke ligger på samme linie. Det består af alle vektorer $\lambda_1 \underline{e}_1 + \lambda_2 \underline{e}_2, \lambda_1, \lambda_2 \in \mathbb{R}$, altså af alle vektorer, som afsat fra samme punkt ligger i planen parallel med $\underline{e}_1$ og $\underline{e}_2$ gennem punktet. Det eneste 3-dimensionale underrum er V_3 selv. Dermed er alle underrum af V_3 bestemt.

2) Vektorerne

$$\underline{e}_1 = (1, 0, 0, \dots, 0, 0)$$

$$\underline{e}_2 = (0, 1, 0, \dots, 0, 0)$$

$$\vdots \quad \quad \quad \vdots$$

$$\underline{e}_{n-1} = (0, 0, 0, \dots, 1, 0)$$

$$\underline{e}_n = (0, 0, 0, \dots, 0, 1)$$

i talrummet $(\mathbb{L}^n, +, \mathbb{L})$ er, som vist tidligere, lineært uafhængige,

og hver vektor $(v_1, \dots, v_n) \in L^n$ kan fremstilles som linearkombination af dem:

$$(v_1, \dots, v_n) = v_1 \underline{e}_1 + \dots + v_n \underline{e}_n.$$

Dette viser, at sættet $(\underline{e}_1, \dots, \underline{e}_n)$ er en basis, og derved at rummet har dimensionen n . Det kaldes derfor det n -dimensionale talrum over L , for $L = \mathbb{R}$ og $L = \mathbb{C}$ også kort det n -dimensionale reelle, henholdsvis komplekse talrum.

3) I følgerummet $(L^{\mathbb{N}}, +, L)$ er

$$\underline{e}_1 = (1, 0, 0, \dots)$$

$$\underline{e}_2 = (0, 1, 0, \dots)$$

$$\vdots \quad \quad \quad \vdots$$

lineært uafhængige. Men disse følger danner ikke nogen basis, idet f.eks. følgen $(1, 1, 1, \dots)$ ikke kan fremstilles som en linearkombination af endelig mange af dem.

4) Polynomierne af højst n -te grad (herunder "nulpolynomiet", dvs. konstanten 0, som ikke tilskrives nogen grad) med komplekse koefficienter danner et underrum $\hat{P}_n$ i vektorrummet $(\hat{P}(\mathbb{C} \rightarrow \mathbb{C}), +, \mathbb{C})$. Dette underrum frembringes af potenserne t^ν , $\nu = 0, 1, \dots, n$, og da disse, som omtalt tidligere, er lineært uafhængige, danner de en basis for det. Dimensionen af $\hat{P}_n$ er altså $n + 1$.

Lad der være givet $n + 1$ indbyrdes forskellige komplekse tal $t_0, t_1, \dots, t_n$. For $\mu = 0, 1, \dots, n$ er

$$f_\mu(t) = (t - t_0) \dots (t - t_{\mu-1})(t - t_{\mu+1}) \dots (t - t_n)$$

et polynomium af n -te grad, ^{og} for alle $\mu, \nu = 0, 1, \dots, n$ gælder

$$f_\mu(t_\nu) = \begin{cases} f_\mu(t_\mu) \neq 0 & \text{for } \nu = \mu \\ 0 & \text{for } \nu \neq \mu. \end{cases}$$

Heraf kan slutes, at de $n + 1$ polynomier f_μ er lineært uafhængige og dermed danner en basis for $\hat{P}_n$. Er nemlig $c_0, c_1, \dots, c_n$ komplekse tal, således at

$$\forall t : c_0 f_0(t) + c_1 f_1(t) + \dots + c_n f_n(t) = 0,$$

fås ved at sætte $t = t_\nu$ for $\nu = 0, 1, \dots, n$, at $c_\nu f_\nu(t_\nu) = 0$, altså $c_\nu = 0$.

Til hvert polynomium g af højst n -te grad findes der altså et og kun ét sæt af komplekse tal $a_0, a_1, \dots, a_n$, således at

$$\forall t : g(t) = \sum_{\mu=0}^n a_\mu f_\mu(t).$$

Ved at sætte $t = t_\nu$ for $\nu = 0, 1, \dots, n$ fås $g(t_\nu) = a_\nu f_\nu(t_\nu)$.

Der gælder altså for alle $t \in \mathbb{C}$

$$g(t) = \sum_{\mu=0}^n \frac{g(t_\mu) f_\mu(t)}{f_\mu(t_\mu)}.$$

Denne ligning, der kaldes Lagranges interpolationsformel, udtrykker et polynomium g af højst n -te grad ved de værdier $g(t_\mu)$, som det antager for $n + 1$ givne, indbyrdes forskellige værdier $t_0, t_1, \dots, t_n$ af den variable. Da

$$\sum_{\mu=0}^n \frac{b_\mu f_\mu(t)}{f_\mu(t_\mu)}$$

for vilkårligt opgivne tal $b_0, b_1, \dots, b_n$ er et polynomium g af højst n -te grad, for hvilket $g(t_\mu) = b_\mu$, har man: Der findes netop ét polynomium af højst n -te grad, som for $n + 1$ givne, indbyrdes forskellige værdier af den variable antager givne værdier.

Lad f være et polynomium af $(n + 1)$ -te grad med højeste koeficient 1 og indbyrdes forskellige rødder $t_0, t_1, \dots, t_n$, altså

$$f(t) = (t - t_0)(t - t_1) \dots (t - t_n),$$

og lad g være et polynomium af højst n -te grad. Med ovenstående betegnelser fås da for $t \neq t_\mu$, $\mu = 0, 1, \dots, n$,

$$\frac{g(t)}{f(t)} = \sum_{\mu=0}^n \frac{g(t_{\mu})}{f'_{\mu}(t_{\mu})(t - t_{\mu})}.$$

Man ser, at hver brudde rational funktion, hvor nævneren har indbyrdes forskellige rødder t_{μ} , og tællerens grad er mindre end nævnerens, har en og kun én fremstilling som linearkombination af funktionerne $1/(t - t_{\mu})$. En sådan fremstilling kaldes en dekomposition. (Om generaliseringen til tilfældet, hvor nævneren har multiple rødder se øvelse 22).

Alt, hvad ovenfor er sagt om polynomier med komplekse koefficienter og af en kompleks variabel, gælder ordret for polynomier med reelle koefficienter af en reel variabel.

Koordinater.

Lad $(V, +, L)$ være et vektorrum med den endelige dimension n , og lad der være valgt en basis $(\underline{e}_1, \dots, \underline{e}_n)$. Hver vektor $\underline{x} \in V$ har da en og kun én fremstilling af formen

$$\underline{x} = x_1 \underline{e}_1 + \dots + x_n \underline{e}_n,$$

hvor $(x_1, \dots, x_n)$ er et talsæt tilhørende L^n . Det kaldes koordinatsættet for vektoren $\underline{x}$ med hensyn til basen eller koordinatsystemet $(\underline{e}_1, \dots, \underline{e}_n)$. Tallet x_i kaldes vektorens i -te koordinat. Idet der til hvert talsæt $(x_1, \dots, x_n) \in L^n$ findes netop én vektor, hvis koordinatsæt det er, nemlig $x_1 \underline{e}_1 + \dots + x_n \underline{e}_n$, fås en bijektiv afbildning k af V på L^n ved til hver vektor $\underline{x}$ at lade svare dens koordinatsæt:

$$k(\underline{x}) = (x_1, \dots, x_n).$$

Idet der for to vektorer

$$\underline{x} = x_1 \underline{e}_1 + \dots + x_n \underline{e}_n, \quad \underline{y} = y_1 \underline{e}_1 + \dots + y_n \underline{e}_n$$

gælder

$$(1) \quad \underline{x} + \underline{y} = (x_1 + y_1)\underline{e}_1 + \dots + (x_n + y_n)\underline{e}_n,$$

altså

$$k(\underline{x} + \underline{y}) = k(\underline{x}) + k(\underline{y}),$$

er $k: V \rightarrow L^n$ en isomorf afbildning af gruppen $(V, +)$ på gruppen $(L^n, +)$. Endvidere gælder for

$$\underline{x} = x_1\underline{e}_1 + \dots + x_n\underline{e}_n$$

og $\lambda \in L$, at

$$(2) \quad \lambda \underline{x} = \lambda x_1 \underline{e}_1 + \dots + \lambda x_n \underline{e}_n,$$

altså

$$k(\lambda \underline{x}) = \lambda k(\underline{x}).$$

En bijektiv afbildning f af et vektorrum $(V, +, L)$ på et vektorrum $(W, +, L)$ over det samme legeme L , således at

$$f(\underline{x} + \underline{y}) = f(\underline{x}) + f(\underline{y}), \quad f(\lambda \underline{x}) = \lambda f(\underline{x})$$

for alle $\underline{x}, \underline{y} \in V$ og alle $\lambda \in L$, kaldes en isomorf afbildning. Hvis der findes en isomorf afbildning af et vektorrum $(V, +, L)$ på et vektorrum $(W, +, L)$, siges $(V, +, L)$ at være isomorft med $(W, +, L)$. Ovenstående kan derfor formuleres således:

Hvert n-dimensional vektorrum $(V, +, L)$ over et tallegeme L er isomorft med talrummet $(L^n, +, L)$. Til hvert valg af en basis for V svarer der en isomorfi, nemlig "koordinatafbildningen" k af V på L^n .

Som følge af (1) og (2) vil lineære regninger med vektorer fra V afspejle sig i ganske tilsvarende regninger med deres koordinatsæt med hensyn til en basis: Koordinatsættet for en linearkombination af visse vektorer er lig den tilsvarende linearkombination af disses koordinatsæt. Lineært afhængige (uafhængige) vektorer i V har lineært afhængige (uafhængige) koordinatsæt.

Eksempel.

Lad $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$ være en basis for det geometriske vektorrum $(V_3, +, \cdot)$, og lad der være valgt et punkt O i rummet. Sættet $(O; \underline{e}_1, \underline{e}_2, \underline{e}_3)$ kaldes et parallelkoordinatsystem. Afsættes vektorerne $\underline{e}_1, \underline{e}_2, \underline{e}_3$ fra O , vil hver af dem bestemme en orienteret linie gennem O , der kaldes heholdsvi første, anden og tredje koordinatakse eller kort 1-aksen, 2-aksen og 3-aksen. De ved O og parrene $(\underline{e}_2, \underline{e}_3)$, $(\underline{e}_3, \underline{e}_1)$ og $(\underline{e}_1, \underline{e}_2)$ bestemte planer, 23-planen, 31-planen og 12-planen, kaldes koordinatplaner.

For en vilkårlig vektor $\underline{v} \in V_3$ har man

$$\underline{v} = v_1 \underline{e}_1 + v_2 \underline{e}_2 + v_3 \underline{e}_3,$$

hvor (v_1, v_2, v_3) er vektorens koordinatsæt. Afsættes $\underline{v}$ fra O til punktet P , så at $\underline{v} = \overrightarrow{OP}$, kan denne fremstilling af $\underline{v}$ som en sum af vektorer $v_1 \underline{e}_1$, $v_2 \underline{e}_2$ og $v_3 \underline{e}_3$, der er henholdsvis parallelle med 1-, 2- og 3-aksen, fås geometrisk på følgende måde. Gennem P lægges de tre planer, der hver er parallel med sin koordinatplan. Hver af disse planer skærer én af koordinataksene. Lad skæringspunkterne være P_1 på 1-aksen, P_2 på 2-aksen og P_3 på 3-aksen. Skæringslinien mellem de to planer gennem P , som er parallelle med 23-planen og 31-planen, er parallel med 3-aksen og skærer 12-planen i et punkt P_{12} . Man har da

$$\overrightarrow{OP} = \overrightarrow{OP_1} + \overrightarrow{P_1P_{12}} + \overrightarrow{P_{12}P} = \overrightarrow{OP_1} + \overrightarrow{OP_2} + \overrightarrow{OP_3},$$

altså

$$\overrightarrow{OP_1} = v_1 \underline{e}_1, \quad \overrightarrow{OP_2} = v_2 \underline{e}_2, \quad \overrightarrow{OP_3} = v_3 \underline{e}_3.$$

Er X et vilkårligt punkt i rummet, forstås ved koordinatsættet for punktet X koordinatsættet for stedvektoren $\overrightarrow{OX}$.

En linie l tænkes bestemt ved et punkt A på den og en vektor $\underline{v} \neq \underline{0}$ parallel med den. Er $\underline{a} = \overrightarrow{OA}$ stedvektoren til A og $\underline{x} = \overrightarrow{OX}$

stedvektoren til et vilkårligt punkt X , vil

$$\underline{x} = \underline{a} + t\underline{v}, \quad t \in \mathbb{R},$$

være en parameterfremstilling for linien, idet $t \rightarrow \underline{a} + t\underline{v}$ er en bijektiv afbildning af $\mathbb{R}$ på mængden af stedvektorer til punkterne på l . Med betegnelserne (a_1, a_2, a_3) , (v_1, v_2, v_3) og (x_1, x_2, x_3) for koordinatsættene for henholdsvis $\underline{a}$, $\underline{v}$ og $\underline{x}$ er parameterfremstillingen ensbetydende med

$$x_1 = a_1 + tv_1,$$

$$x_2 = a_2 + tv_2, \quad t \in \mathbb{R}.$$

$$x_3 = a_3 + tv_3,$$

Det bemærkes, at $(A; \underline{v})$ er et parallelkoordinatsystem på linien l , i hvilket vektoren $\overrightarrow{AX}$ og dermed punktet X på l har koordinatsættet (t) .

En plan π tænkes bestemt ved, at den går gennem et givet punkt A med stedvektoren $\underline{a} = \overrightarrow{OA}$ og er parallel med to givne lineært uafhængige vektorer $\underline{v}_1$ og $\underline{v}_2$. Betegner $\underline{x}$ igen stedvektoren $\overrightarrow{OX}$ til et vilkårligt punkt X , vil

$$\underline{x} = \underline{a} + t_1\underline{v}_1 + t_2\underline{v}_2, \quad (t_1, t_2) \in \mathbb{R}^2,$$

være en parameterfremstilling for π , idet $(t_1, t_2) \rightarrow \underline{a} + t_1\underline{v}_1 + t_2\underline{v}_2$ er en bijektiv afbildning af $\mathbb{R}^2$ på mængden af stedvektorer til punkterne i π . Med betegnelserne (a_1, a_2, a_3) , (v_{11}, v_{12}, v_{13}) , (v_{21}, v_{22}, v_{23}) og (x_1, x_2, x_3) for koordinatsættene for henholdsvis $\underline{a}$, $\underline{v}_1$, $\underline{v}_2$ og $\underline{x}$ er parameterfremstillingen ensbetydende med

$$x_1 = a_1 + t_1v_{11} + t_2v_{21},$$

$$x_2 = a_2 + t_1v_{12} + t_2v_{22}, \quad (t_1, t_2) \in \mathbb{R}^2.$$

$$x_3 = a_3 + t_1v_{13} + t_2v_{23},$$

$(A; \underline{v}_1, \underline{v}_2)$ er et parallelkoordinatsystem i planen π , i hvilket vektoren $\overrightarrow{AX}$ og dermed punktet X i π har koordinatsættet (t_1, t_2) .

Sum og direkte sum af underrum.

Lad $(V, +, L)$ være et vilkårligt vektorrum og M' og M'' delmængder af V . Mængden af alle vektorer, som hver er sum af en vektor tilhørende M' og en vektor tilhørende M'' , kaldes de to delmængders sum og betegnes med $M' + M''$:

$$M' + M'' = \{\underline{u}' + \underline{u}'' \mid \underline{u}' \in M' \wedge \underline{u}'' \in M''\}.$$

Hvis en af mængderne M' eller M'' er tom, er $M' + M''$ også tom.

Herved er der defineret en komposition i mængden af alle delmængder af V . Det er klart, at den er kommutativ og associativ, idet vektoradditionen har disse egenskaber. Der findes et neutralt element, nemlig $\underline{0}$. Men en mængde M' , der indeholder mindst to vektorer har ikke nogen "modsat" mængde; thi for hver ikke tom mængde M'' vil $M' + M''$ indeholde mindst to vektorer. Forkortningsreglen gælder heller ikke.

For to underrum U' og U'' af $(V, +, L)$ er $U' + U''$ det mindste underrum, der indeholder dem begge, altså

$$U' + U'' = V(U' \cup U'').$$

Bevis: $V(U' \cup U'')$ er mængden af alle linearkombinationer af endelig mange vektorer tilhørende $U' \cup U''$. For $\underline{u}' \in U'$ og $\underline{u}'' \in U''$ er $\underline{u}' + \underline{u}''$ en sådan linearkombination. Dette viser, at $U' + U'' \subseteq V(U' \cup U'')$. På den anden side er $U' + U''$ et underrum; thi for $\lambda, \mu \in L$, $\underline{u}', \underline{v}' \in U'$, $\underline{u}'', \underline{v}'' \in U''$ har man $\lambda(\underline{u}' + \underline{u}'') + \mu(\underline{v}' + \underline{v}'') = (\lambda\underline{u}' + \mu\underline{v}') + (\lambda\underline{u}'' + \mu\underline{v}'') \in U' + U''$, hvilket viser, at UR (side III, 1, 6) er opfyldt for $U' + U''$.
Idet

$$\left. \begin{array}{l} U' = U' + \{\underline{0}\} \\ U'' = \{\underline{0}\} + U'' \end{array} \right\} \subseteq U' + U'',$$

og $V(U' \cup U'')$ er fællesmængden for alle underrum, som indeholder U' og U'' , kan man slutte, at $V(U' \cup U'') \subseteq U' + U''$, og dermed at $U' + U'' = V(U' \cup U'')$ som påstået.

For endelig-dimensionale underrum U' og U'' af $(V, +, L)$ gælder dimensionsformlen (H. Grassmann, 1844)

$$\dim(U' + U'') + \dim(U' \cap U'') = \dim U' + \dim U''.$$

Bevis: Der indføres betegnelserne

$$\dim U' = p, \quad \dim U'' = q, \quad \dim(U' \cap U'') = r.$$

I $U' \cap U''$ vælges en basis $\underline{e}_1, \dots, \underline{e}_r$. Denne suppleres til en basis

$$\underline{e}_1, \dots, \underline{e}_r, \underline{e}'_{r+1}, \dots, \underline{e}'_p$$

for U' og til en basis

$$\underline{e}_1, \dots, \underline{e}_r, \underline{e}''_{r+1}, \dots, \underline{e}''_q$$

for U'' . (Hvis $r = 0$, menes hermed, at der vælges en basis

$\underline{e}'_1, \dots, \underline{e}'_p$ for U' og en basis $\underline{e}''_1, \dots, \underline{e}''_q$ for U'' .) Hver vektor i

$U' + U''$ kan da fremstilles som en linearkombination af de $p + q - r$ vektorer

$$(*) \quad \underline{e}_1, \dots, \underline{e}_r, \underline{e}'_{r+1}, \dots, \underline{e}'_p, \underline{e}''_{r+1}, \dots, \underline{e}''_q.$$

Disse vektorer er lineært uafhængige. Lad nemlig

$$\lambda_1 \underline{e}_1 + \dots + \lambda_r \underline{e}_r + \lambda'_{r+1} \underline{e}'_{r+1} + \dots + \lambda'_p \underline{e}'_p + \lambda''_{r+1} \underline{e}''_{r+1} + \dots + \lambda''_q \underline{e}''_q = \underline{0}$$

være en lineær relation mellem dem. Den udsiger, at vektoren

$$-\lambda''_{r+1} \underline{e}''_{r+1} - \dots - \lambda''_q \underline{e}''_q,$$

som jo tilhører U'' , også må tilhøre U' , altså $U' \cap U''$. Den er

følgelig lig $\underline{0}$; hvis $r = 0$, og en linearkombination af $\underline{e}_1, \dots, \underline{e}_r$,

hvis $r > 0$. Der må altså bestå en lineær relation af formen

$$\mu_1 \underline{e}_1 + \dots + \mu_r \underline{e}_r + \lambda''_{r+1} \underline{e}''_{r+1} + \dots + \lambda''_q \underline{e}''_q = \underline{0},$$

hvor leddene med $\underline{e}_1, \dots, \underline{e}_r$ falder bort, hvis $r = 0$. Da de indgående vektorer er lineært uafhængige, kan man heraf slutte, at

$\lambda_{r+1}'' = \dots = \lambda_q'' = 0$. Derefter følger af den foregående ligning, at $\lambda_1 = \dots = \lambda_r = \lambda_{r+1}' = \dots = \lambda_p' = 0$, idet $\underline{e}_1, \dots, \underline{e}_r, \underline{e}_{r+1}', \dots, \underline{e}_1'$ er lineært uafhængige. Dermed er vist, at vektorerne (*) er lineært uafhængige, og da de frembringer $U' + U''$, danner de en basis for dette underrum. Dettets dimension er følgelig $p + q - r$, som påstået.

Et underrum U i et vektorrum $(V, +, L)$ siges at være direkte sum af underrummene $U' \subseteq U$ og $U'' \subseteq U$, hvis hver vektor i U har en og kun én fremstilling af formen $\underline{u}' + \underline{u}''$, $\underline{u}' \in U'$, $\underline{u}'' \in U''$. Man har da naturligvis $U = U' + U''$. Ønsker man at fremhæve, at summen er direkte, skriver man

$$U = U' \oplus U''.$$

Hver af de følgende betingelser, hvoraf den første er selve definitionen, er nødvendig og tilstrækkelig for, at summen af to underrum U' og U'' er direkte:

1°. For $\underline{u}', \underline{v}' \in U'$, $\underline{u}'', \underline{v}'' \in U''$ gælder

$$\underline{u}' + \underline{u}'' = \underline{v}' + \underline{v}'' \Rightarrow \underline{u}' = \underline{v}' \wedge \underline{u}'' = \underline{v}''.$$

2°. For $\underline{u}' \in U'$, $\underline{u}'' \in U''$ gælder

$$\underline{u}' + \underline{u}'' = 0 \Rightarrow \underline{u}' = \underline{u}'' = \underline{0}.$$

3°. $U' \cap U'' = \{\underline{0}\}.$

Bevis: Hvis 1° er opfyldt, fås 2° for $\underline{v}' = \underline{v}'' = \underline{0}$. Omvendt, hvis 2° er opfyldt, fås under forudsætningerne i 1°, at

$$(\underline{u}' - \underline{v}') + (\underline{u}'' - \underline{v}'') = \underline{0},$$

altså $\underline{u}' - \underline{v}' = \underline{u}'' - \underline{v}'' = \underline{0}$, idet $\underline{u}' - \underline{v}' \in U'$ og $\underline{u}'' - \underline{v}'' \in U''$.

Dette viser, at 1° og 2° er ensbetydende. Hvis 2° er opfyldt, kan man af $\underline{u} \in U' \cap U''$ slutte, at $\underline{u} = \underline{0}$, idet $\underline{u} + (-\underline{u}) = \underline{0}$ og $\underline{u} \in U'$, $-\underline{u} \in U''$. Dette viser, at 2° medfører 3°. Omvendt, hvis

3° er opfyldt, kan man af $\underline{u}' \in U'$, $\underline{u}'' \in U''$ og $\underline{u}' + \underline{u}'' = \underline{0}$ slutte, at $\underline{u}' = -\underline{u}'' = \underline{0}$, idet jo $\underline{u}' = -\underline{u}'' \in U' \cap U''$. Dermed er påstanden bevist.

Er U' og U'' endelig-dimensionale, viser dimensionsformlen, at 3° , og dermed også 1° og 2° , er ensbetydende med

$$4^\circ \quad \dim(U' + U'') = \dim U' + \dim U''.$$

Hvis det for to underrum U' og U'' i et vektorrum $(V, +, L)$ gælder, at

$$V = U' \oplus U'',$$

siges de at være komplementære. Hver vektor $\underline{u} \in V$ kan da på en og kun én måde skrives

$$\underline{u} = \underline{u}' + \underline{u}'', \quad \underline{u}' \in U', \quad \underline{u}'' \in U''.$$

Vektoren $\underline{u}'$ kaldes komponenten af $\underline{u}$ efter U' med hensyn til U'' eller også projektionen af $\underline{u}$ på U' langs U'' , og tilsvarende for $\underline{u}''$.

Spørgsmålet, om der til hvert underrum U' i et vektorrum $(V, +, L)$ findes et komplementært, kan let besvares bekræftende, hvis V har endelig dimension n . Man vælger en basis $\underline{e}_1, \dots, \underline{e}_p$, $p = \dim U'$, for U' og supplerer den med vektorer $\underline{e}_{p+1}, \dots, \underline{e}_n$ til en basis for V . Sættes

$$U'' = V(\underline{e}_{p+1}, \dots, \underline{e}_n),$$

haves øjensynlig $U' + U'' = V$, altså $\dim(U' + U'') = n$, og da $\dim U' = p$, $\dim U'' = n - p$, giver 4°

$$V = U' \oplus U''.$$

Til et givet underrum U' findes der i almindelighed uendelig mange komplementære.

Tilsvarende gælder for uendelig-dimensionale vektorrum. Men dette vil ikke blive bevist her.

Idet additionen af delmængder af et vektorrum er associativ og kommutativ, er summen af flere end to mængder uafhængige af den orden, i hvilken additionerne foretages og af mængdernes rækkefølge. Specielt kan altså sådanne summer skrives uden parenteser.

Er $U^{(1)}, \dots, U^{(p)}$ underrum af et vektorrum $(V, +, L)$, vil

$$U = U^{(1)} + \dots + U^{(p)}$$

være mængden af vektorer

$$\underline{u} = \underline{u}^{(1)} + \dots + \underline{u}^{(p)}, \quad \underline{u}^{(1)} \in U^{(1)}, \dots, \underline{u}^{(p)} \in U^{(p)}.$$

Har hver vektor $\underline{u} \in U$ netop én sådan fremstilling, siges summen at være direkte, og man skriver

$$U = U^{(1)} \oplus \dots \oplus U^{(p)}.$$

En tilstrækkelig (og selvfølgelig også nødvendig) betingelse herfor er, at $\underline{0}$ kun har én sådan fremstilling, altså at

$$\underline{u}^{(1)} + \dots + \underline{u}^{(p)} = \underline{0}, \quad \underline{u}^{(1)} \in U^{(1)}, \dots, \underline{u}^{(p)} \in U^{(p)},$$

medfører $\underline{u}^{(1)} = \dots = \underline{u}^{(p)} = \underline{0}$. Dette ses på tilsvarende måde som i tilfældet $p = 2$.

For endelig-dimensionale underrum $U^{(1)}, \dots, U^{(p)}$ af et vektorrum $(V, +, L)$ er

$$\dim(U^{(1)} + \dots + U^{(p)}) \leq \dim U^{(1)} + \dots + \dim U^{(p)}.$$

Lighedstegnet gælder, hvis og kun hvis summen af $U^{(1)}, \dots, U^{(p)}$ er direkte. (Se øvelse 30).

Som første eksempel betragtes det geometriske vektorrum $(V_3, +, \mathbb{R})$. Vektorerne tænkes afsat fra samme punkt. Endimensionale underrum kaldes her kort for linier og todimensionale for planer (gående gennem det pågældende punkt). Summen af to forskellige linier er den plan, de bestemmer. Summen er direkte. Summen af tre forskellige linier, der ikke ligger i samme plan, er rummet. Summen er direkte. Ligger de i samme plan, er summen denne plan og

ikke direkte. Summen af en plan og en linie, som ikke ligger i den, er rumret. Summen er direkte, linien og planen altså komplementære. Ligger linien i planen, er denne summen, men ikke direkte sum. To forskellige planers sum er rummet og aldrig direkte.

Som andet eksempel betragtes vektorrummet $(\hat{P}_n(\mathbb{C} \rightarrow \mathbb{C}), +, \cdot)$ af alle polynomier af højst n -te grad. Lad der være givet et polynomium $d(t)$ af graden δ , $1 \leq \delta \leq n$. Mængden af alle med $d(t)$ delelige polynomier i $\hat{P}_n$, altså alle polynomier af formen $q(t)d(t)$, hvor $q(t)$ er et polynomium af højst $(n - \delta)$ -te grad, er øjensynlig et underrum U' i $\hat{P}_n$. Polynomierne $d(t) = t^0 d(t), td(t), \dots, t^{n-\delta} d(t)$ danner en basis for det. De frembringer nemlig U' og er lineært uafhængige; thi en linearkombination af dem har formen $q(t)d(t)$, hvor $q(t)$ er et polynomium, og af $q(t)d(t) = 0$ for alle t følger, at $q(t)$ er nulpolynomiet, da $d(t) \neq 0$ for uendelig mange værdier af t . Dimensionen af U' er følgelig $n - \delta + 1$. Desuden betragtes underrummet $U'' = \hat{P}_{\delta-1}$ bestående af alle polynomier af højst $(\delta - 1)$ -te grad. Dette har dimensionen δ . Nu har U' og U'' kun nulpolynomiet fælles, idet hvert fra dette forskelligt polynomium i U' har mindst graden δ . U' og U'' danner altså direkte sum, og idet $\dim(U' \oplus U'') = \dim U' + \dim U'' = n + 1 = \dim \hat{P}_n$, har vi $\hat{P}_n = U' \oplus U''$, dvs. de to underrum er komplementære. Heraf sluttes, at hvert polynomium $p(t)$ har en og kun én fremstilling af formen $p(t) = q(t)d(t) + r(t)$, hvor $q(t)$ og $r(t)$ er polynomier, og graden af $r(t)$ er mindre end graden af $d(t)$. (Division med rest af $p(t)$ med $d(t)$.)

Normerede vektorrum.

Undertiden er det ønskeligt at kunne tilskrive hver vektor $\underline{v}$ i et vektorrum $(V, +, L)$ over et tallegeme L en "længde" $\|\underline{v}\|$, der har lignende egenskaber som en geometrisk vektors sædvanlige længde. Man ønsker altså en funktion $\underline{v} \rightarrow \|\underline{v}\|$ fra V til $\mathbb{R}$, som opfylder visse krav. Det har vist sig at være hensigtsmæssigt at stille de følgende, som øjensynlig er opfyldt for geometriske vektorers længder:

$$N1. \quad \forall \underline{v} : \underline{v} \neq \underline{0} \Rightarrow \|\underline{v}\| > 0.$$

$$N2. \quad \forall \underline{v} \forall \lambda : \|\lambda \underline{v}\| = |\lambda| \|\underline{v}\|.$$

$$N3. \quad \forall \underline{u}, \underline{v} : \|\underline{u} + \underline{v}\| \leq \|\underline{u}\| + \|\underline{v}\|.$$

Af N2 sluttes, at

$$\|\underline{0}\| = \|\underline{00}\| = 0, \quad \|-\underline{v}\| = \|(-1)\underline{v}\| = \|\underline{v}\|.$$

En funktion $\|\cdot\|$ fra V til $\mathbb{R}$ med egenskaberne N1, N2, N3 kaldes en norm i $(V, +, L)$, og vektorrummet sammen med en bestemt norm kaldes et normeret vektorrum. Et sådant kan betegnes $(V, +, L, \|\cdot\|)$.

Ved til hvert tal i L at lade svare dets absolutte værdi fås en norm i det endimensionale talrum $(L, +, L)$. Dette således normerede vektorrum betegnes sædvanligvis kort med L . Det underforstås altså (om fornødent), at L er organiseret som normeret vektorrum med den absolutte værdi som norm.

Et normeret vektorrum $(V, +, L, \|\cdot\|)$ bliver til et metrisk rum ved afstandsdefinitionen

$$\text{dist}(\underline{u}, \underline{v}) = \|\underline{v} - \underline{u}\|.$$

Ved hjælp af N1-3 og de anførte konsekvenser fås nemlig for $\underline{u}, \underline{v}, \underline{w} \in V$.

$$\begin{aligned}
\text{dist}(\underline{v}, \underline{v}) &= \|\underline{v} - \underline{v}\| = 0, \\
\text{dist}(\underline{u}, \underline{v}) &= \|\underline{v} - \underline{u}\| > 0 \quad \text{for } \underline{u} \neq \underline{v}, \\
\text{dist}(\underline{v}, \underline{u}) &= \|\underline{u} - \underline{v}\| = \|\underline{v} - \underline{u}\| = \text{dist}(\underline{v}, \underline{u}), \\
\text{dist}(\underline{u}, \underline{w}) &= \|\underline{w} - \underline{u}\| = \|\underline{w} - \underline{v} + \underline{v} - \underline{u}\| \\
&\leq \|\underline{w} - \underline{v}\| + \|\underline{v} - \underline{u}\| \\
&= \text{dist}(\underline{u}, \underline{v}) + \text{dist}(\underline{v}, \underline{w}).
\end{aligned}$$

Ved den indførte afstandsfunktion bestemmes en topologi i V , og man kan tale om kontinuerte afbildninger af det normerede vektorrum ind i et topologisk (specielt metrisk) rum, f.eks. ind i $\mathbb{R}$. Normen selv bliver herved en (endda ligelig) kontinuert funktion fra V til $\mathbb{R}$. Man har nemlig ifølge N3 for $\underline{u}, \underline{v} \in V$

$$\|\underline{v} - \underline{u}\| + \|\underline{u}\| \geq \|\underline{v}\|, \quad \|\underline{u} - \underline{v}\| + \|\underline{v}\| \geq \|\underline{u}\|,$$

altså

$$\left. \begin{aligned} \|\underline{v}\| - \|\underline{u}\| \\ \|\underline{u}\| - \|\underline{v}\| \end{aligned} \right\} \leq \|\underline{v} - \underline{u}\| = \text{dist}(\underline{u}, \underline{v}),$$

altså

$$|\|\underline{v}\| - \|\underline{u}\|| \leq \text{dist}(\underline{u}, \underline{v}).$$

For hvert positivt tal ε er således $|\|\underline{v}\| - \|\underline{u}\|| < \varepsilon$, når blot $\text{dist}(\underline{u}, \underline{v}) < \varepsilon$.

Eksempler.

I talrummet $(L^n, +, L)$ bestående af alle talsæt

$$\underline{x} = (x_1, \dots, x_n), \quad x_i \in L \text{ for } i = 1, \dots, n,$$

vil

$$\|\underline{x}\|_1 = |x_1| + \dots + |x_n|$$

være en norm; thi N1 og N2 er øjensynlig opfyldt, og at N3 gælder, sluttet af

$$|x_i + y_i| \leq |x_i| + |y_i|$$

for $x_i, y_i \in L$, $i = 1, \dots, n$.

I samme vektorrum er også

$$\|\underline{x}\|_{\infty} = \max \{|x_1|, \dots, |x_n|\}$$

en norm. At N1 og N2 er opfyldt er ligeledes klart, og at N3 gælder, sluttet af, at man ifølge ovenstående ulighed for hvert $i = 1, \dots, n$ har

$$|x_i + y_i| \leq \max\{|x_1|, \dots, |x_n|\} + \max\{|y_1|, \dots, |y_n|\}.$$

En tredje, hyppig anvendt norm i $(L^n, +, L)$ defineres ved

$$\|\underline{x}\|_2 = (|x_1|^2 + \dots + |x_n|^2)^{\frac{1}{2}}$$

Også her er det klart, at N1 og N2 er opfyldt. At N3 gælder, vil fremgå af et senere, mere alment resultat.

Motiveringen for betegnelsen $\|\cdot\|_p$, $p = 1, 2, \infty$ for disse normer er følgende: Man kan vise, at

$$\|\underline{x}\|_p = (|x_1|^p + \dots + |x_n|^p)^{1/p}$$

for hvert reelt tal $p \geq 1$ er en norm, den såkaldte p -norm, i $(L^n, +, L)$, og at $\|\underline{x}\|_p$ for hvert fast $\underline{x}$ konvergerer mod $\|\underline{x}\|_{\infty}$, når p går mod uendelig. For normerne $\|\cdot\|_p$ kaldes N3 Minkowskis ulighed.

I et vilkårligt n -dimensionalt vektorrum $(V, +, L)$ kan man indføre normer ved at vælge en basis $(\underline{e}_1, \dots, \underline{e}_n)$ og for $\underline{x} = x_1 \underline{e}_1 + \dots + x_n \underline{e}_n$ definere $\|\underline{x}\|_p$, specielt $\|\underline{x}\|_{\infty}$, ved ovenstående udtryk. På grund af friheden ved valg af basis findes for hvert p uendelig mange p -normer i et givet vektorrum.

Disse begreber finder især anvendelse på vektorrum over de reelle eller de komplekse tals legeme.

Normer, der er analoge med de omtalte kan også defineres i visse uendelig-dimensionale funktionsrum. Vi vil her betragte vektorrummet $(\hat{C}([a, b] \rightarrow \mathbb{R}), +, \mathbb{R})$ af alle på et afsluttet interval

$[a,b] \subset \mathbb{R}$, $a < b$, definerede kontinuerte ^{reelle} funktioner. (Det følgende gælder ordret også for $(\hat{C}([a,b] \rightarrow \mathbb{C}), +, \cdot)$, altså vektorrummet bestående af de på $[a,b]$ kontinuerte funktioner med komplekse værdier.)

For $\varphi \in \hat{C}([a,b] \rightarrow \mathbb{R})$ defineres

$$\begin{aligned}\|\varphi\|_1 &= \int_a^b |\varphi(t)| dt, \\ \|\varphi\|_2 &= \left(\int_a^b |\varphi(t)|^2 dt \right)^{\frac{1}{2}}, \\ \|\varphi\|_\infty &= \sup\{|\varphi(t)| \mid t \in [a,b]\}.\end{aligned}$$

I stedet for sup kan der også skrives max, idet den kontinuerte funktion $|\varphi|$ har et maximum på det afsluttede og begrænsede interval $[a,b]$.

At $\|\varphi\|_1$ og $\|\varphi\|_\infty$ er normer, ses som i det endelig-dimensionale tilfælde med benyttelse af

$$|\varphi(t) + \psi(t)| \leq |\varphi(t)| + |\psi(t)|$$

for $\varphi, \psi \in \hat{C}([a,b] \rightarrow \mathbb{R})$ og $t \in [a,b]$. At $\|\varphi\|_2$ opfylder N1 og N2 er også let at se, og at N3 er gyldig i dette tilfælde vil fremgå af et senere resultat.

Vektorrum med indre produkt.

I det geometriske vektorrum $(V_3, +, \cdot, \mathbb{R})$ har man foruden de kompositioner, som indgår i definitionen på vektorrum, det skalære produkt, altså en komposition fra $V_3 \times V_3$ til $\mathbb{R}$. Også dette begreb generaliseres. Vi skal her kun betragte vektorrum over de reelle eller de komplekse tals legeme. Den følgende definition er formuleret for det komplekse tilfælde. Overstregningen af et bogstav, som står for et komplekst tal, betyder overgang til det komplekst konjugerede tal. Definitionen i det reelle tilfælde er den samme,

idet overstregningerne dog kan bortfalde.

Ved et indre produkt i et vektorrum $(V, +, \dot{\mathbb{C}})$ (eller $(V, +, \dot{\mathbb{R}})$), forstås en komposition fra $V \times V$ til $\dot{\mathbb{C}}$ (eller $\dot{\mathbb{R}}$), $(\underline{u}, \underline{v}) \rightarrow \underline{u} \cdot \underline{v}$, for hvilken der gælder:

$$\text{IP1. } \forall \underline{u}, \underline{v} : \underline{v} \cdot \underline{u} = \overline{\underline{u} \cdot \underline{v}}.$$

$$\text{IP2. } \forall \underline{u}, \underline{v}, \underline{w} : (\underline{u} + \underline{v}) \cdot \underline{w} = \underline{u} \cdot \underline{w} + \underline{v} \cdot \underline{w}.$$

$$\text{IP3. } \forall \underline{u}, \underline{v} \forall \dot{\mathbb{C}}\lambda : (\lambda \underline{u} \cdot \underline{v}) = \lambda(\underline{u} \cdot \underline{v}).$$

$$\text{IP4. } \forall \underline{v} : \underline{v} \neq \underline{0} \Rightarrow \underline{v} \cdot \underline{v} > 0.$$

I det reelle tilfælde, hvor overstregningen i IP1 bortfalder og $\dot{\mathbb{R}}$ træder i stedet for $\dot{\mathbb{C}}$ i IP3, er dette velkendte egenskaber ved geometriske vektorers skalære produkt.

Egenskaben IP1 betegnes ofte som Hermiteisk symmetri (Ch. Hermite, 1822-1901). Ved hjælp af denne fås af IP2 for $\underline{u}, \underline{v}, \underline{w} \in V$

$$\begin{aligned} \underline{w} \cdot (\underline{u} + \underline{v}) &= \overline{(\underline{u} + \underline{v}) \cdot \underline{w}} = \overline{\underline{u} \cdot \underline{w} + \underline{v} \cdot \underline{w}} \\ &= \overline{\underline{u} \cdot \underline{w}} + \overline{\underline{v} \cdot \underline{w}} = \underline{w} \cdot \underline{u} + \underline{w} \cdot \underline{v} \end{aligned}$$

og af IP3 for $\underline{u}, \underline{v} \in V$ og $\mu \in \dot{\mathbb{C}}$ (eller $\dot{\mathbb{R}}$)

$$\underline{u} \cdot (\mu \underline{v}) = \overline{(\mu \underline{v}) \cdot \underline{u}} = \overline{\mu(\underline{v} \cdot \underline{u})} = \overline{\mu}(\overline{\underline{v} \cdot \underline{u}}) = \overline{\mu}(\underline{u} \cdot \underline{v}).$$

Af dette med $\mu = 0$, $\underline{v} = \underline{0}$ og IP3 med $\lambda = 0$, $\underline{u} = \underline{0}$ sluttes

$$\underline{u} = \underline{0} \vee \underline{v} = \underline{0} \Rightarrow \underline{u} \cdot \underline{v} = 0.$$

I et vektorrum $(V, +, \dot{\mathbb{C}})$ (eller $(V, +, \dot{\mathbb{R}})$) med indre produkt defineres en norm ved

$$\|\underline{v}\| = (\underline{v} \cdot \underline{v})^{\frac{1}{2}}.$$

Egenskaben N1 ved en norm er sikret gennem IP4, og da

$$\|\lambda \underline{v}\| = (\lambda \underline{v} \cdot \lambda \underline{v})^{\frac{1}{2}} = (\lambda \overline{\lambda} \underline{v} \cdot \underline{v})^{\frac{1}{2}} = |\lambda| (\underline{v} \cdot \underline{v})^{\frac{1}{2}} = |\lambda| \|\underline{v}\|,$$

er N2 opfyldt.

Ved beviset for N3 benyttes en generalisation af Cauchy-Schwarz' ulighed:

$$\forall \underline{u}, \underline{v} : |\underline{u} \cdot \underline{v}| \leq (\underline{u} \cdot \underline{u})^{\frac{1}{2}} (\underline{v} \cdot \underline{v})^{\frac{1}{2}}.$$

For $\underline{u} \cdot \underline{v} = 0$ er den øjensynlig rigtig. Det kan herefter antages, at $\underline{u} \cdot \underline{v} \neq 0$, så at $\underline{u} \neq \underline{0}$ og $\underline{v} \neq \underline{0}$. For $\lambda, \mu \in \mathbb{C}$ gælder

$$\begin{aligned} & (\lambda \underline{u} - \mu \underline{v}) \cdot (\lambda \underline{u} - \mu \underline{v}) \\ &= \lambda \bar{\lambda} \underline{u} \cdot \underline{u} - \lambda \bar{\mu} \underline{u} \cdot \underline{v} - \bar{\lambda} \mu \underline{v} \cdot \underline{u} + \mu \bar{\mu} \underline{v} \cdot \underline{v} \\ &= \lambda \bar{\lambda} \underline{u} \cdot \underline{u} - 2 \operatorname{Re}(\lambda \bar{\mu} \underline{u} \cdot \underline{v}) + \mu \bar{\mu} \underline{v} \cdot \underline{v} \geq 0 \end{aligned}$$

med betegnelsen Re for reel del, idet

$$\bar{\lambda} \mu \underline{v} \cdot \underline{u} = \overline{\lambda \bar{\mu} \underline{u} \cdot \underline{v}}.$$

Sættes her $\lambda = (\underline{v} \cdot \underline{v})^{\frac{1}{2}} |\underline{u} \cdot \underline{v}| / (\underline{u} \cdot \underline{v})$ og $\mu = (\underline{u} \cdot \underline{u})^{\frac{1}{2}}$, fås, da μ er reel,

$$(\underline{u} \cdot \underline{u})(\underline{v} \cdot \underline{v}) - 2(\underline{u} \cdot \underline{u})^{\frac{1}{2}} (\underline{v} \cdot \underline{v})^{\frac{1}{2}} |\underline{u} \cdot \underline{v}| + (\underline{u} \cdot \underline{u})(\underline{v} \cdot \underline{v}) \geq 0,$$

hvoraf den ønskede ulighed fremgår ved division med $(\underline{u} \cdot \underline{u})^{\frac{1}{2}} (\underline{v} \cdot \underline{v})^{\frac{1}{2}}$.

Vi bemærker, at lighedstegnet i uligheden gælder, hvis og kun hvis $\underline{u}$ og $\underline{v}$ er lineært afhængige. Ved indsættelse af f.eks. $\underline{u} = \nu \underline{v}$ i ulighedens to sider fås nemlig samme resultat, og ud fra lighedstegnets gyldighed sluttes i tilfældet $\underline{u} \cdot \underline{v} = 0$, at $\underline{u} = \underline{0}$ eller $\underline{v} = \underline{0}$, i tilfældet $\underline{u} \cdot \underline{v} \neq 0$, at $\lambda \underline{u} - \mu \underline{v} = \underline{0}$ med de ovenfor anførte værdier for λ og μ .

At N3 gælder for $\|\underline{v}\| = (\underline{v} \cdot \underline{v})^{\frac{1}{2}}$, aflæses nu af

$$\begin{aligned} \|\underline{u} + \underline{v}\|^2 &= (\underline{u} + \underline{v}) \cdot (\underline{u} + \underline{v}) = \underline{u} \cdot \underline{u} + 2 \operatorname{Re}(\underline{u} \cdot \underline{v}) + \underline{v} \cdot \underline{v} \\ &\leq \underline{u} \cdot \underline{u} + 2|\underline{u} \cdot \underline{v}| + \underline{v} \cdot \underline{v} \\ &\leq \underline{u} \cdot \underline{u} + 2(\underline{u} \cdot \underline{u})^{\frac{1}{2}} (\underline{v} \cdot \underline{v})^{\frac{1}{2}} + \underline{v} \cdot \underline{v} \\ &= ((\underline{u} \cdot \underline{u})^{\frac{1}{2}} + (\underline{v} \cdot \underline{v})^{\frac{1}{2}})^2 = (\|\underline{u}\| + \|\underline{v}\|)^2. \end{aligned}$$

Det sidste af tegnene $\leq$ står for $=$, netop når $\underline{u}$ og $\underline{v}$ er lineært afhængige. Er $\underline{v} \neq \underline{0}$ og $\underline{u} = \nu \underline{v}$, fås som betingelse for, at også det første $\leq$ kan erstattes med $=$, at $\operatorname{Re} \nu = |\nu|$, dvs. at ν er reel og ikke negativ.

Lighedstegn i N3, altså i

$$\|\underline{u} + \underline{v}\| \leq \|\underline{u}\| + \|\underline{v}\|,$$

gælder derfor her, hvis og kun hvis en af vektorerne $\underline{u}$ og $\underline{v}$ frem-

går af den anden ved multiplikation med et reelt tal $\nu \geq 0$.

Eksempler.

Det ses umiddelbart, at der ved

$$\underline{x} \cdot \underline{y} = x_1 \bar{y}_1 + \dots + x_n \bar{y}_n$$

defineres et indre produkt i det komplekse talrum $(\mathbb{C}^n, +, \cdot)$ og også i det reelle talrum $(\mathbb{R}^n, +, \cdot)$, hvor overstregningerne dog er overflødige. Den til dette indre produkt hørende norm $\|\underline{x}\| = (\underline{x} \cdot \underline{x})^{\frac{1}{2}}$ stemmer overens med den ovenfor (side III, 1, 32) indførte funktion $\|\underline{x}\|_2$, og derne er altså en norm, som påstået. De to talrum med dette indre produkt betegnes $l_2(n, \mathbb{C})$ og $l_2(n, \mathbb{R})$.

Der kan også defineres andre indre produkter i de to talrum, f.eks. ved for faste positive tal $\gamma_1, \dots, \gamma_n$ at sætte

$$\underline{x} \cdot \underline{y} = \gamma_1 x_1 \bar{y}_1 + \dots + \gamma_n x_n \bar{y}_n.$$

I et vilkårligt vektorrum $(V, +, \cdot)$ eller $(V, +, \cdot)$ af endelig dimension n kan defineres et indre produkt ved at vælge en basis og for vektorer $\underline{u}$ og $\underline{v}$ med koordinatsættene $(u_1, \dots, u_n)$ og $(v_1, \dots, v_n)$ med hensyn til denne at sætte f.eks.

$$\underline{u} \cdot \underline{v} = u_1 \bar{v}_1 + \dots + u_n \bar{v}_n.$$

Vælger man i det geometriske vektorrum en basis bestående af tre parvis vinkelrette enhedsvektorer, fås på denne måde to vektorers skalarprodukt.

I følgerummet $(\mathbb{C}^{\mathbb{N}}, +, \cdot)$ eller $(\mathbb{R}^{\mathbb{N}}, +, \cdot)$ er mængden af følger $\underline{x} = (x_1, x_2, \dots)$, for hvilke den uendelige række

$$|x_1|^2 + |x_2|^2 + \dots$$

er konvergent, et underrum $l_2(\mathbb{C})$, henholdsvis $l_2(\mathbb{R})$. Af konvergens af rækkerne $\sum |x_i|^2$ og $\sum |y_i|^2$ følger nemlig konvergens af $\sum |x_i + y_i|^2$, idet der for vilkårlige komplekse tal x og y gælder

$$2|xy| = |x|^2 + |y|^2 - (|x| - |y|)^2 \leq |x|^2 + |y|^2$$

og følgelig

$$|x + y|^2 \leq |x|^2 + |y|^2 + 2|xy| \leq 2(|x|^2 + |y|^2).$$

Af den første af disse uligheder sluttet endvidere, at rækken $\sum x_i \bar{y}_i$ er absolut konvergent. Sættes

$$\underline{x} \cdot \underline{y} = x_1 \bar{y}_1 + x_2 \bar{y}_2 + \dots$$

for vektorer $\underline{x} = (x_1, x_2, \dots)$ og $\underline{y} = (y_1, y_2, \dots)$ tilhørende $l_2(\mathbb{C})$ eller $l_2(\mathbb{R})$, fås et indre produkt i $l_2(\mathbb{C})$ eller $l_2(\mathbb{R})$. (Disse to vektorrum er eksempler på Hilbert rum, hvorved forstås fuldstændige uendelig-dimensionale vektorrum med indre produkt over de komplekse eller de reelle tals legeme.)

I funktionsrummet $(\hat{C}([a, b] \rightarrow \mathbb{C}), +, \cdot)$ eller $(\hat{C}([a, b] \rightarrow \mathbb{R}), +, \cdot)$ bestående af de på et afsluttet interval $[a, b] \subset \mathbb{R}$ definerede og kontinuerte funktioner med henholdsvis komplekse eller reelle værdier defineres ved

$$\varphi \cdot \psi = \int_a^b \varphi(t) \overline{\psi(t)} dt,$$

hvor $\varphi, \psi \in \hat{C}([a, b] \rightarrow \mathbb{C})$ eller $\varphi, \psi \in \hat{C}([a, b] \rightarrow \mathbb{R})$, et indre produkt. De betragtede vektorrum med dette indre produkt betegnes kort $\hat{C}_2([a, b] \rightarrow \mathbb{C})$ og $\hat{C}_2([a, b] \rightarrow \mathbb{R})$.

I det følgende betragtes et vilkårligt komplekst eller reelt vektorrum med et indre produkt. Det betegnes med $(V, +, L, \cdot)$, hvor altså $L = \mathbb{C}$ eller $L = \mathbb{R}$. Den ved det indre produkt bestemte norm betegnes $\| \cdot \|$.

En vektor $\underline{y} \in V$, for hvilken $\| \underline{y} \| = 1$, kaldes en normeret vektor eller enhedsvektor. Hver vektor $\underline{y} \neq \underline{0}$ kan "normeres" på netop én måde ved multiplikation med et positivt reelt tal, nemlig $1/\| \underline{y} \|$.

En vektor $\underline{u}$ siges at være ortogonal (i det komplekse til-

fælde også unitær-ortogonal) til en vektor $\underline{v}$, hvis

$$\underline{u} \cdot \underline{v} = 0.$$

Da $\underline{v} \cdot \underline{u} = \overline{\underline{u} \cdot \underline{v}}$ og $\underline{u} \cdot \underline{v}$ er samtidig 0 eller ikke 0, er ortogonalitet en symmetrisk relation i V . Nulvektoren $\underline{0}$ er ortogonal til hver vektor i V , og den er den eneste vektor, der er ortogonal til sig selv. I stedet for $\underline{u} \cdot \underline{v} = 0$ skrives også

$$\underline{u} \perp \underline{v}.$$

(I det geometriske vektorrum med skalarproduktet som indre produkt er $\underline{u} \perp \underline{v}$ for $\underline{u} \neq \underline{0}$ og $\underline{v} \neq \underline{0}$ ensbetydende med, at vektorerne $\underline{u}$ og $\underline{v}$ er vinkelrette på hinanden.)

For vilkårlige vektorer $\underline{u}, \underline{v}$ i et vektorrum med indre produkt gælder "Pythagoras' sætning":

$$\underline{u} \perp \underline{v} \Rightarrow \|\underline{u}\|^2 + \|\underline{v}\|^2 = \|\underline{u} + \underline{v}\|^2.$$

Dette sluttes af

$$\begin{aligned} \|\underline{u} + \underline{v}\|^2 &= (\underline{u} + \underline{v}) \cdot (\underline{u} + \underline{v}) = \underline{u} \cdot \underline{u} + \underline{v} \cdot \underline{v} + \underline{u} \cdot \underline{v} + \underline{v} \cdot \underline{u} \\ &= \|\underline{u}\|^2 + \|\underline{v}\|^2 + \underline{u} \cdot \underline{v} + \overline{\underline{u} \cdot \underline{v}}. \end{aligned}$$

(Heraf ses tillige, at i reelle vektorrum gælder også den omvendte sætning.) Ved induktion fås, at der for parvis ortogonale vektorer $\underline{u}_1, \dots, \underline{u}_p$ i et vektorrum med indre produkt gælder

$$\|\underline{u}_1 + \dots + \underline{u}_p\|^2 = \|\underline{u}_1\|^2 + \dots + \|\underline{u}_p\|^2.$$

To delmængder M og N af V siges at være ortogonale, og man skriver

$$M \perp N,$$

hvis

$$\forall \underline{u} \in M \forall \underline{v} \in N : \underline{u} \perp \underline{v}.$$

Er $M \neq \emptyset$ en delmængde af V , vil mængden

$$M^\perp = \{\underline{v} \in V \mid \forall \underline{w} \in M : \underline{v} \perp \underline{w}\}$$

af vektorer, som hver er ortogonal til samtlige vektorer i M ,

være et underrum af V ; thi af

$$\forall \underline{M}^{\perp} : \underline{u} \cdot \underline{w} = 0 \quad \wedge \quad \underline{v} \cdot \underline{w} = 0$$

sluttes ved hjælp af IP2-3, at

$$\forall \underline{L}^{\perp}, \mu \quad \forall \underline{M}^{\perp} : (\lambda \underline{u} + \mu \underline{v}) \cdot \underline{w} = 0.$$

$M^{\perp}$ kaldes det maksimale til M ortogonale underrum. Man har specielt $\{\underline{0}\}^{\perp} = V$ og $V^{\perp} = \{\underline{0}\}$.

Det maksimale til $M^{\perp}$ ortogonale underrum $M^{\perp\perp}$ indeholder M og dermed det af M frembragte underrum $V(M)$. Der gælder altså

$$V(M) \subseteq M^{\perp\perp},$$

specielt for et underrum U af V

$$U \subseteq U^{\perp\perp}.$$

Har vektorrummet endelig dimension, gælder lighedstegnet for hvert underrum, hvilket bevises nedenfor. I uendelig-dimensionale vektorrum behøver dette ikke at være tilfældet (jfr. øv.50)

Fra 0 forskellige, parvis ortogonale vektorer $\underline{u}_1, \dots, \underline{u}_r$ i et vektorrum med indre produkt er lineært uafhængige; thi af

$$\lambda_1 \underline{u}_1 + \dots + \lambda_{\rho-1} \underline{u}_{\rho-1} + \dots + \lambda_r \underline{u}_r = \underline{0}$$

fås for hvert $\rho = 1, \dots, r$ ved indre multiplikation med $\underline{u}_{\rho}$

$$\lambda_{\rho} \underline{u}_{\rho} \cdot \underline{u}_{\rho} = 0,$$

altså $\lambda_{\rho} = 0$, da $\underline{u}_{\rho} \neq \underline{0}$.

En indexeret mængde $(\underline{u}_{\iota})$, $\iota \in J$, af vektorer i et vektorrum med indre produkt siges at være et ortonormeret eller ortonormalt system, hvis alle dens vektorer er normerede og hvilke som helst to af dem, svarende til forskellige indices, er ortogonale, altså hvis

$$\forall J^{\iota}, \kappa : \underline{u}_{\iota} \cdot \underline{u}_{\kappa} = \begin{cases} 1 & \text{for } \iota = \kappa \\ 0 & \text{for } \iota \neq \kappa \end{cases}$$

Idet et ortonormalt system er lineært uafhængigt, er det en basis, dersom det frembringer hele vektorrummet. Det kaldes da en orto-

normeret eller ortonormal basis.

Ved undersøgelse af vektorrum med indre produkt er det ofte fordelagtigt at benytte ortonormale baser (i det geometriske vektorrum sædvanlige retvinklede koordinater). Hvert endelig-dimensionalt (men ikke hvert uendelig-dimensionalt) vektorrum med indre produkt har ortonormale baser, hvilket vil fremgå af den følgende ortonormaliseringssætning (J.P. Gram, 1879, E. Schmidt, 1907):

Lad der i et vektorrum med indre produkt være givet et endeligt eller numerabelt, lineært uafhængigt vektorsæt $(\underline{v}_\nu)$, $\nu \in J$, hvor $J = \{1, \dots, p\}$ eller $J = \mathbb{N}$. Da findes et ortonormalt sæt $(\underline{u}_\nu)$, $\nu \in J$, således at sættene $(\underline{v}_1, \dots, \underline{v}_\rho)$ og $(\underline{u}_1, \dots, \underline{u}_\rho)$ for hvert $\rho \in J$ frembringer det samme underrum.

Bevis: Med U_ρ , $\rho \in J$, betegnes det af $(\underline{v}_1, \dots, \underline{v}_\rho)$ frembragte underrum. Antag, at vi for et $r \in J$ har et ortonormalt sæt $(\underline{u}_1, \dots, \underline{u}_r)$, der frembringer U_r . Under forudsætning af at $r + 1 \in J$, vil vi søge at udvide til et ortonormalt sæt $(\underline{u}_1, \dots, \underline{u}_r, \underline{u}_{r+1})$, der frembringer U_{r+1} . Vektoren $\underline{v}_{r+1}$ kan ikke tilhøre U_r , idet $\underline{v}_1, \dots, \underline{v}_r, \underline{v}_{r+1}$ er lineært uafhængige. Heraf sluttes, at $\underline{u}_1, \dots, \underline{u}_r, \underline{v}_{r+1}$ er lineært uafhængige og følgelig bringer U_{r+1} idet dette underrum har dimensionen $r+1$. Her kan nu $\underline{v}_{r+1}$ erstattes med en vilkårlig vektor $\underline{w}_{r+1}$ af formen

$$\underline{w}_{r+1} = \underline{v}_{r+1} + \lambda_1 \underline{u}_1 + \dots + \lambda_r \underline{u}_r$$

med koefficienter $\lambda_1, \dots, \lambda_r$ fra L , idet $\underline{v}_{r+1}$ er en linearkombination af $\underline{u}_1, \dots, \underline{u}_r, \underline{w}_{r+1}$. Vi søger sådanne koefficienter $\lambda_1, \dots, \lambda_r$, at $\underline{w}_{r+1}$ bliver ortogonal til $\underline{u}_1, \dots, \underline{u}_r$. Dette vil være tilfældet, hvis (og kun hvis) der for $\rho = 1, \dots, r$ gælder

$$\underline{w}_{r+1} \cdot \underline{u}_\rho = \underline{v}_{r+1} \cdot \underline{u}_\rho + \lambda_\rho = 0,$$

altså

$$\lambda_\rho = -\underline{v}_{r+1} \cdot \underline{u}_\rho.$$

Da $\underline{u}_1, \dots, \underline{u}_r, \underline{v}_{r+1}$ er lineært uafhængige, er den således bestemte vektor $\underline{w}_{r+1} \neq \underline{0}$ og kan normeres. Sættes $\underline{u}_{r+1} = \underline{w}_{r+1} / \|\underline{w}_{r+1}\|$, vil $(\underline{u}_1, \dots, \underline{u}_{r+1})$ være et ortonormalt sæt, som frembringer U_{r+1} .

Idet $\underline{v}_1 \neq \underline{0}$, vil sættet bestående af $\underline{u}_1 = \underline{v}_1 / \|\underline{v}_1\|$ være ortonormalt og frembringe U_1 . Bestemmes nu successivt $\underline{u}_2, \underline{u}_3, \dots$ på den ovenfor angivne måde: $\underline{u}_2$ ved normering af

$$\underline{w}_2 = \underline{v}_2 - (\underline{v}_2 \cdot \underline{u}_1) \underline{u}_1,$$

dernæst $\underline{u}_3$ ved normering af

$$\underline{w}_3 = \underline{v}_3 - (\underline{v}_3 \cdot \underline{u}_1) \underline{u}_1 - (\underline{v}_3 \cdot \underline{u}_2) \underline{u}_2,$$

osv., fås et ortonormalt sæt $(\underline{u}_i)$, $i \in J$, med den ønskede egenskab, $(\underline{u}_1, \dots, \underline{u}_\rho)$ frembringer U_ρ for hvert $\rho \in J$. Metoden kaldes Gram-Schmidts ortonormalisering.

Er det givne vektorsæt $(\underline{v}_1, \underline{v}_2, \dots)$ en basis for det betragtede vektorrum, vil også $(\underline{u}_1, \underline{u}_2, \dots)$ være en basis. Man har altså:

Hvert vektorrum med indre produkt, som har endelig dimension eller en numerabel basis, har ortonormale baser.

I det følgende betragtes et vektorrum $(V, +, \cdot, \cdot)$ eller $(V, +, \cdot, \cdot)$ med indre produkt og den endelige dimension n .

For hvert underum U af V gælder

$$U \oplus U^\perp = V.$$

Bevis: Det er klart, at $U \cap U^\perp = \{\underline{0}\}$, altså at summen $U + U^\perp$ er direkte, idet $\underline{0}$ er den eneste vektor, der er ortogonal til sig selv. Der gælder følgelig

$$\dim(U \oplus U^\perp) = \dim U + \dim U^\perp \leq n.$$

Sættes $\dim U = p$, er det altså tilstrækkeligt at vise, at $\dim U^\perp \geq n - p$. En basis $(\underline{e}_1, \dots, \underline{e}_p)$ for U suppleres med vektorer $\underline{e}_{p+1}, \dots, \underline{e}_n$ til en basis $(\underline{e}_1, \dots, \underline{e}_n)$ for V , og denne ortonormaliseres. Derved fås en ortonormal basis $(\underline{f}_1, \dots, \underline{f}_n)$ for V , hvor $(\underline{f}_1, \dots, \underline{f}_p)$ frembringer U . De $n - p$ vektorer $\underline{f}_{p+1}, \dots, \underline{f}_n$ tilhører $U^\perp$, idet hver af dem er ortogonal til vektorerne $\underline{f}_1, \dots, \underline{f}_p$ og dermed til det af disse frembragte underrum U . Da $U^\perp$ således indeholder $n - p$ lineært uafhængige vektorer, er $\dim U^\perp \geq n - p$, som påstået.

Vi bemærker, at $U^\perp$ er det eneste underrum, som er både ortogonalt til U og komplementært til U . $U^\perp$ kaldes derfor det ortogonale komplement til U .

For vilkårlige underrum U og U' af et vektorrum V med indre produkt (gerne af uendelig dimension) gælder nemlig

$$(*) \quad U \perp U' \wedge U + U' = V \Rightarrow U' = U^\perp,$$

thi af $U \perp U'$ følger $U' \subseteq U^\perp$, og skrives en vektor $\underline{v} \in U^\perp$ på formen $\underline{v} = \underline{u} + \underline{u}'$, $\underline{u} \in U$, $\underline{u}' \in U'$, haves dels $\underline{v} - \underline{u}' = \underline{u}$, dels $\underline{v} - \underline{u}' \perp \underline{u}$, følgelig $\underline{v} - \underline{u}' = \underline{0}$ og dermed $\underline{v} = \underline{u}' \in U'$, hvilket viser $U^\perp \subseteq U'$.

(Også når V har uendelig dimension, siges et underrum U' at være ortogonalt komplement til et underrum U , hvis $U \perp U'$ og $U + U' = V$. Ifølge $(*)$ kan et underrum U ikke have andre ortogonale komplement end $U^\perp$. Når $\dim V = \infty$, kan det imidlertid forekomme, at et underrum slet ikke har noget ortogonalt komplement, jfr. øvelse 50.)

Det er nu klart, at vi for hvert underrum U af et endelig dimensionalt vektorrum med indre produkt har

$$U = U^{\perp\perp},$$

thi U er jo ortogonalt og komplementært til $U^\perp$.

Lad der være givet et underrum U af det n -dimensionale vektorrum V med indre produkt. Hver vektor $\underline{v} \in V$ har da en og kun én fremstilling af formen

$$\underline{v} = \underline{v}' + \underline{v}'', \quad \underline{v}' \in U, \underline{v}'' \in U^\perp.$$

Vektoren $\underline{v}'$, altså projektionen af $\underline{v}$ på U langs $U^\perp$, kaldes ortogonalprojektionen af $\underline{v}$ på U . Den kan også karakteriseres som den vektor $\underline{u} \in U$, hvis afstand fra $\underline{v}$ er mindst:

$$\|\underline{v} - \underline{v}'\| = \min_{\underline{u} \in U} \|\underline{v} - \underline{u}\|.$$

For hver vektor $\underline{u} \in U$ er nemlig $\underline{v} - \underline{v}' \perp \underline{v}' - \underline{u} \in U$, følgelig

$$\begin{aligned} \|\underline{v} - \underline{u}\|^2 &= \|\underline{v} - \underline{v}' + \underline{v}' - \underline{u}\|^2 \\ &= \|\underline{v} - \underline{v}'\|^2 + \|\underline{v}' - \underline{u}\|^2 \geq \|\underline{v} - \underline{v}'\|^2, \end{aligned}$$

hvor lighedstegnet gælder, hvis og kun hvis $\underline{u} = \underline{v}'$.

Af $\underline{v} = \underline{v}' + \underline{v}''$ og $\underline{v}' \perp \underline{v}''$ fås

$$\|\underline{v}\|^2 = \|\underline{v}'\|^2 + \|\underline{v}''\|^2$$

og dermed

$$\|\underline{v}'\| \leq \|\underline{v}\|,$$

hvor lighedstegnet gælder, hvis og kun hvis $\underline{v}'' = \underline{0}$, altså $\underline{v} \in U$.

Kender man en ortonormal basis $(\underline{e}_1, \dots, \underline{e}_p)$ for U , kan man finde ortogonalprojektionen

$$\underline{v}' = \lambda_1 \underline{e}_1 + \dots + \lambda_p \underline{e}_p$$

af $\underline{v}$ ved at bestemme $\lambda_1, \dots, \lambda_p$ således, at $\underline{v} - \underline{v}'$ bliver ortogonal til $\underline{e}_1, \dots, \underline{e}_p$. Ligningerne

$$(\underline{v} - \lambda_1 \underline{e}_1 - \dots - \lambda_p \underline{e}_p) \cdot \underline{e}_i = 0, \quad i = 1, \dots, p,$$

er opfyldte, hvis og kun hvis $\lambda_i = \underline{v} \cdot \underline{e}_i$, hvilket giver

$$\underline{v}' = (\underline{v} \cdot \underline{e}_1) \underline{e}_1 + \dots + (\underline{v} \cdot \underline{e}_p) \underline{e}_p.$$

For $\|\underline{v}'\|^2$ finder man

$$\underline{v}' \cdot \underline{v}' = \sum_{i,j=1}^p [(\underline{v} \cdot \underline{e}_i) \underline{e}_i] \cdot [(\underline{v} \cdot \underline{e}_j) \underline{e}_j]$$

$$= \sum_{i,j=1}^p (\underline{v} \cdot \underline{e}_i) \overline{(\underline{v} \cdot \underline{e}_j)} \underline{e}_i \cdot \underline{e}_j = \sum_{i=1}^p |\underline{v} \cdot \underline{e}_i|^2.$$

Uligheden $\|\underline{v}'\| \leq \|\underline{v}\|$ giver nu Bessels ulighed (efter F.W. Bessel, der 1828 beviste den tilsvarende ulighed for et specielt funktionsrum):

For hvert ortonormalt sæt $(\underline{e}_1, \dots, \underline{e}_p)$ og hver vektor $\underline{v}$ i et endelig-dimensionalt vektorrum med indre produkt gælder

$$|\underline{v} \cdot \underline{e}_1|^2 + \dots + |\underline{v} \cdot \underline{e}_p|^2 \leq \|\underline{v}\|^2.$$

Lighedstegnet gælder, hvis og kun hvis $\underline{v}$ tilhører det af $(\underline{e}_1, \dots, \underline{e}_p)$ frembragte underrum U , specielt for hver vektor $\underline{v}$, hvis $U = V$. I dette tilfælde fås Parsevals ligning (efter M.A. Parseval, der i 1806 beviste en analog ligning for et specielt funktionsrum):

For hver ortonormal basis $(\underline{e}_1, \dots, \underline{e}_n)$ og hver vektor $\underline{v}$ i et n -dimensionalt vektorrum med indre produkt gælder

$$|\underline{v} \cdot \underline{e}_1|^2 + \dots + |\underline{v} \cdot \underline{e}_n|^2 = \|\underline{v}\|^2.$$

Idet her $\underline{v}' = \underline{v}$, er

$$\underline{v} = (\underline{v} \cdot \underline{e}_1) \underline{e}_1 + \dots + (\underline{v} \cdot \underline{e}_n) \underline{e}_n,$$

dvs. de indre produkter $v_i = \underline{v} \cdot \underline{e}_i$ er koordinaterne for $\underline{v}$ med hensyn til den ortonormale basis. Parsevals ligning er altså ikke andet end en generalisation

$$\|\underline{v}\|^2 = |v_1|^2 + \dots + |v_n|^2$$

af det geometriske vektorrums "afstandsformel". Også skalarproduktets udtryk i sædvanlige retvinklede koordinater kan generaliseres:

For vektorer $\underline{u}$ og $\underline{v}$ i et n -dimensionalt vektorrum med indre produkt haves

$$\underline{u} \cdot \underline{v} = u_1 \bar{v}_1 + \dots + u_n \bar{v}_n,$$

hvor $(u_1, \dots, u_n)$ og $(v_1, \dots, v_n)$ er koordinatsættene for $\underline{u}$ og $\underline{v}$ med hensyn til en ortonormal basis $(e_1, \dots, e_n)$.

Dette fremgår af følgende regning:

$$\begin{aligned} \underline{u} \cdot \underline{v} &= \left(\sum_{i=1}^n u_i \underline{e}_i \right) \cdot \left(\sum_{j=1}^n v_j \underline{e}_j \right) \\ &= \sum_{i,j=1}^n (u_i \underline{e}_i) \cdot (v_j \underline{e}_j) = \sum_{i,j=1}^n u_i \bar{v}_j (\underline{e}_i \cdot \underline{e}_j) = \sum_{i=1}^n u_i \bar{v}_i. \end{aligned}$$

I reelle vektorrum med indre produkt defineres en vinkel ϑ , $0 \leq \vartheta \leq \pi$, mellem to vektorer $\underline{u} \neq \underline{0}$ og $\underline{v} \neq \underline{0}$ ved

$$\vartheta = \text{Arccos} \frac{\underline{u} \cdot \underline{v}}{\|\underline{u}\| \|\underline{v}\|},$$

hvilket er muligt på grund af Cauchy-Schwarz' ulighed. Vinklerne ϑ_i mellem en vektor $\underline{v} \neq \underline{0}$ og vektorerne $\underline{e}_i$, $i = 1, \dots, n$, i en ortonormal basis kaldes vektorens retningsvinkler med hensyn til denne basis. Vektorens koordinater v_i kan da skrives

$$v_i = \|\underline{v}\| \cos \vartheta_i, \quad i = 1, \dots, n,$$

og "afstandsformlen" giver relationen

$$\cos^2 \vartheta_1 + \dots + \cos^2 \vartheta_n = 1$$

mellem vektorens "retningscosinusser".

Endelig-dimensionale reelle vektorrum med indre produkt kaldes ofte euklidiske rum, for komplekse bruges navnet unitære rum.

Øvelser til kap. III, § 1.

1. Vis, at VR10 ikke følger af de øvrige krav, der er stillet til et vektorrum. (F.eks. kan man for geometriske vektorer i planen erstatte det sædvanlige produkt $\lambda \underline{v}$ af et reelt tal λ og en vektor $\underline{v}$ med dettes projektion på en fast linie.)
2. Undersøg hvilke af følgende delmængder af $\hat{F}(\hat{C} \rightarrow \hat{C})$, der er underrum i $(\hat{F}(\hat{C} \rightarrow \hat{C}), +, \hat{C})$:
Mængden af alle polynomier med komplekse koefficienter, mængden af alle polynomier af en given grad $m > 0$, mængden af alle polynomier af højst m -te grad (herunder nulpolynomiet).
Mængden af alle funktioner $f: \hat{C} \rightarrow \hat{C}$, der opfylder betingelsen $zf(i) = f(-i)$, henholdsvis $\forall z : f(z) = f(1-z)$.
3. Undersøg, om de monotone (dvs. de aldrig aftagende og de aldrig voksende) funktioner defineret på et interval I udgør et underrum i $(\hat{F}(I \rightarrow \hat{R}), +, \hat{R})$.
4. Vektorerne $(1, 0, 0, 0, \dots)$, $(0, 1, 0, 0, \dots)$, $(0, 0, 1, 0, \dots)$, ... frembringer et underrum i rummet $(\hat{R}^{\hat{N}}, +, \hat{R})$ af alle reelle talfølger. Hvorledes kan det ses på en talfølge, om den tilhører dette underrum?
5. Undersøg, om vektorerne i de følgende vektorsæt tilhørende de angivne vektorrum er lineært afhængige, og fremstil i bekræftende fald en af dem som en linearkombination af de øvrige:
 - a) $(-1, 1), (2, 2), (0, 3)$ i $(\hat{R}^2, +, \hat{R})$.
 - b) $(i, 1), (1+i, 0), (0, 1-i)$ i $(\hat{C}^2, +, \hat{C})$.
 - c) $(1, 1, 1), (0, 2, 2), (0, 1, 3)$ i $(\hat{R}^3, +, \hat{R})$.

d) $(1,0,1,0)$, $(0,1,0,1)$, $(1,-1,1,-1)$, $(0,0,1,1)$ i $(\mathbb{R}^4, +, \mathbb{R})$!

6. For hvilke tal t er

a) vektorerne $(1,t)$ og $(t,1)$ i $(\mathbb{R}^2, +, \mathbb{R})$,

b) vektorerne $(1,t,0)$, $(t,0,1)$ og $(0,1,t)$ i $(\mathbb{R}^3, +, \mathbb{R})$,

c) de samme vektorer i $(\mathbb{C}^3, +, \mathbb{C})$

lineært afhængige?

7. Angiv en betingelse, som tallene a_{ij} , $i = 1, \dots, n$, $j = i, \dots, n$, $i < j$, opfylder, hvis og kun hvis vektorerne

$$(a_{11}, 0, 0, \dots, 0),$$

$$(a_{12}, a_{22}, 0, \dots, 0),$$

$$\vdots$$

$$(a_{1n}, a_{2n}, a_{3n}, \dots, a_{nn})$$

i vektorrummet $(L^n, +, L)$ er lineært uafhængige.

8. Vis, at hvis vektorerne $\underline{v}_1, \underline{v}_2, \dots, \underline{v}_p$ i et vektorrum $(V, +, L)$ er lineært uafhængige, vil også vektorerne $\underline{v}_1 + a\underline{v}_2, \underline{v}_2, \dots, \underline{v}_p$, hvor a betegner et tal fra L , være lineært uafhængige.

9. Gælder det, at når tre vektorer $\underline{u}, \underline{v}, \underline{w}$ i et vektorrum er lineært uafhængige, vil også vektorerne $\underline{v} + \underline{w}, \underline{w} + \underline{u}, \underline{u} + \underline{v}$ være lineært uafhængige? Gælder det omvendte?

10. Vis, at to vektorer (x_1, x_2) og (y_1, y_2) i $(L^2, +, L)$ er lineært afhængige, hvis og kun hvis $x_1 y_2 - x_2 y_1 = 0$.

11. For ethvert positivt reelt tal a betragtes funktionen bestemt ved $t \rightarrow a^t$ for $t \in \mathbb{R}$. Vis, at denne mængde af funktioner tilhørende vektorrummet $\hat{F}(\mathbb{R} \rightarrow \mathbb{R}), +, \mathbb{R})$ er lineært uafhængig.

12. Angiv rangen og alle maximalsæt for mængden $\{(1,1), (1,-1), (-1,1), (-1,-1)\}$ af vektorer i $(\mathbb{R}^2, +, \mathbb{R})$.
13. Bestem rangen af mængden $\{(-2,4,0), (0,3,1), (2,-1,1)\}$ af vektorer i $(\mathbb{R}^3, +, \mathbb{R})$, og angiv et maximalsæt. Undersøg, om det af disse vektorer frembragte underrum indeholder vektorerne $(1,0,0)$ og $(2,2,2)$.
14. For hvert reelt tal ϕ og hvert reelt tal $a \geq 0$ bestemmes en funktion ved $t \rightarrow a \cos(t - \phi)$ for $t \in \mathbb{R}$. Vis, at mængden af sådanne funktioner er et underrum i $\hat{F}(\mathbb{R} \rightarrow \mathbb{R}, +, \mathbb{R})$, og angiv en basis for dette underrum.
15. Bestem dimensionen af det underrum i $\hat{F}(\mathbb{R} \rightarrow \mathbb{R}, +, \mathbb{R})$, som frembringes af funktionerne $t \rightarrow 1, \cos t, \sin t, \cos^2 t, \cos t \sin t, \sin^2 t$ for $t \in \mathbb{R}$, og angiv en basis for det.
16. Angiv en basis for $(\mathbb{R}^4, +, \mathbb{R})$, som indeholder vektorerne $(3,0,1,2)$ og $(-1,2,0,-1)$.
17. Bestem dimensionen af vektorrummet $(\mathbb{C}^n, +, \mathbb{R})$ og angiv en basis for det. (Betragt først tilfældet $n = 1$.)
18. Vis, at vektorrummet $(\mathbb{R}, +, \mathbb{Q})$ har uendelig dimension. (Benyt, at mængden $\mathbb{Q}$ af rationale tal er numerabel, eller denne opgaves sidste resultat.)
- Hvad betyder det for det reelle tal a , at 1 og a er lineært uafhængige i dette vektorrum?
- Vis, at 1, $\sqrt{2}$, $\sqrt{3}$ er lineært uafhængige i $(\mathbb{R}, +, \mathbb{Q})$.
- Vis, at $\log p_1, \dots, \log p_n$, hvor $p_1, \dots, p_n$ er indbyrdes forskellige primtal, er lineært uafhængige i $(\mathbb{R}, +, \mathbb{Q})$. (Bemærk,

at hvis vektorer i et vektorrum over $\mathbb{Q}$ er lineært afhængige, består der en egentlig lineær relation med heltallige koefficienter mellem dem.)

19*. En reel funktion f defineret på intervallet $I =$

$\{x \in \mathbb{R} \mid 0 \leq x \leq 1\}$ kaldes stykkevis lineær, hvis der findes en inddeling af I , $0 = t_0 < t_1 < \dots < t_n = 1$, og polynomier $a_i x + b_i$ af højst 1. grad, $i = 1, 2, \dots, n$, hvor

$$a_i t_i + b_i = a_{i+1} t_i + b_{i+1}, \quad i = 1, \dots, n-1,$$

således at

$$f(x) = a_i x + b_i \quad \text{for } t_{i-1} \leq x \leq t_i, \quad i = 1, \dots, n.$$

Vis, at mængden $\hat{F}_{sl} = \hat{F}_{sl}(I \rightarrow \mathbb{R})$ af stykkevis lineære funktioner defineret på I er et underrum i vektorrummet $\hat{F}(I \rightarrow \mathbb{R}, +, \cdot)$ af alle reelle funktioner på I .

For hvert t , $0 \leq t < 1$, er funktionen g_t , hvor

$$g_t(x) = \begin{cases} 0 & \text{for } 0 \leq x \leq t, \\ x - t & \text{for } t \leq x \leq 1, \end{cases}$$

en stykkevis lineær funktion på I . Vis, at disse funktioner g_t , $0 \leq t < 1$, sammen med den konstante funktion $g_1 = 1$ danner en basis for $\hat{F}_{sl}$. (Benyt ved påvisningen af, at hver funktion f tilhørende $\hat{F}_{sl}$ kan skrives som linearkombination af endelig mange af funktionerne g_t , $0 \leq t \leq 1$, induktion efter antallet af knæk for f .)

For hvert t , $0 \leq t < 1$, er funktionen h_t , hvor

$$h_t(x) = |x - t| \quad \text{for } 0 \leq x \leq 1,$$

ligeledes en stykkevis lineær funktion på I . Vis (under benyttelse af det allerede fundne) at også funktionerne h_t , $0 \leq t \leq 1$, danner en basis for $\hat{F}_{sl}$. (Med andre ord vil da være vist, at enhver stykkevis lineær funktion f på $[0, 1]$ har en

og kun én fremstilling

$$f(x) = c_0 |x - t_0| + c_1 |x - t_1| + \dots + c_n |x - t_n|$$

for $0 \leq x \leq 1$,

hvor $0 = t_0 < t_1 < \dots < t_n = 1$, og $c_1, \dots, c_{n-1}$ alle er forskellige fra 0.)

20. Bestem polynomiet g af højst tredje grad således, at $g(-1) = 3$, $g(0) = 1$, $g(2) = -1$ og $g(4) = 2$.

21*. Bevis ved hjælp af Lagranges interpolationsformel, at der for vilkårlige, indbyrdes forskellige komplekse tal $t_0, t_1, \dots, t_n$ og de angivne hele tal m gælder

$$\sum_{\mu=0}^n \frac{t_{\mu}^m}{f'_{\mu}(t_{\mu})} = \begin{cases} 0 & \text{for } 0 \leq m \leq n-1 \\ 1 & \text{for } m = n, \end{cases}$$

hvor

$$f_{\mu}(t) = (t - t_0) \dots (t - t_{\mu-1})(t - t_{\mu+1}) \dots (t - t_n).$$

22*. Der antages givet et naturligt tal n , naturlige tal

$m_0, m_1, \dots, m_r$, således at

$$m_0 + m_1 + \dots + m_r = n + 1,$$

samt $r + 1$ indbyrdes forskellige komplekse tal $t_0, t_1, \dots, t_r$.

Polynomiet

$$f(t) = (t - t_0)^{m_0} (t - t_1)^{m_1} \dots (t - t_r)^{m_r}$$

er da af graden $n + 1$. Med $f_{\rho\mu}$, $\rho = 0, 1, \dots, r$, $\mu = 1, 2, \dots, m_{\rho}$,

betegnes det polynomium, som for $t \neq t_{\rho}$, $\rho = 0, 1, \dots, r$, er bestemt ved

$$f_{\rho\mu}(t) = f(t) (t - t_{\rho})^{-\mu}.$$

Disse $n + 1$ polynomier er alle af højst n -te grad.

Vis, at de danner en basis for $\hat{P}_n(\mathbb{C} \rightarrow \mathbb{C})$. (Benyt f.eks., at hvis et tal er m -dobbel rod i et polynomium, vil det være $(m-1)$ -dobbel rod i polynomiets afledede.)

Slut heraf, at hver brudde rational funktion g/f , hvor g er et polynomium af højst n -te grad, har en og kun én dekomposition af formen

$$\frac{g(t)}{f(t)} = \sum_{\rho=0}^r \sum_{\mu=1}^{m_{\rho}} a_{\rho\mu} (t - t_{\rho})^{-\mu},$$

hvor $a_{\rho\mu} \in \mathbb{C}$.

Bevis, at der for givne komplekse tal $b_{\rho\mu}$, $\rho = 0, 1, \dots, r$, $\mu = 1, 2, \dots, m_{\rho}$, findes netop ét polynomium g af højst n -te grad, for hvilket

$$D^{\mu} g(t_{\rho}) = b_{\rho\mu},$$

(for hvilket altså værdien og de $m_{\rho} - 1$ første afledede i hvert t_{ρ} er foreskrevet). Betragt specielt tilfældet $r = 0$, $m_0 = n + 1$ (Taylors formel for polynomier).

23. I vektorrummet $(V_3, +, \mathbb{R})$ af de geometriske vektorer er givet fra O forskellige vektorer $\underline{a}, \underline{b}, \underline{c}, \underline{d}, \underline{e}$. Det forudsættes, at $\underline{b}, \underline{c}, \underline{d}, \underline{e}$ er parallelle med samme plan, at $\underline{a}$ ikke er parallel med denne plan, at $\underline{b} \neq \underline{c}$, og at $\underline{d}$ og $\underline{e}$ er indbyrdes vinkelrette enhedsvektorer. Alle vektorer tænkes afsat fra samme punkt. Giv geometriske beskrivelser af følgende delmængder af V_3 :

$$M_1 = \{\lambda \underline{a} \mid \lambda \in \mathbb{R}\},$$

$$M_2 = \{\mu \underline{b} \mid \mu \in [0, \infty[\},$$

$$M_3 = \{\nu \underline{c} \mid \nu \in [0, 1] \},$$

$$M_4 = \{\rho \underline{d} + \sigma \underline{e} \mid \rho^2 + \sigma^2 \leq 1 \},$$

$$M_1 + M_1, M_1 + M_2, M_1 + M_2 + M_3, M_3 + M_4, M_2 + M_3 + M_4, M_4 + M_4.$$

24. Lad M, M', M'' være delmængder af et vektorrum. Mængderne $M \cap (M' + M'')$ og $(M \cap M') + (M \cap M'')$ stemmer almindeligvis

ikke overens. Vis dette ved angivelse af et eksempel, og undersøg, om en inklusion mellem de to mængder er almengyldig.

25. Idet U , U' og U'' betegner endelig-dimensionale underrum af et vektorrum, skal man vise

$$U' \subseteq U'' \wedge U \cap U' = U \cap U'' \wedge U + U' = U + U'' \Rightarrow U' = U''.$$

26. Hvilke direkte summer kan der dannes af underrummene

$$U = V((1,1,1,1)),$$

$$U' = V((0,1,0,-1), (1,2,1,0)),$$

$$U'' = V((-1,0,1,0), (1,1,0,0))$$

i talrummet $(L^4, +, L)$?

27. En funktion $f: \mathbb{R} \rightarrow \mathbb{R}$ kaldes lige, hvis

$$\forall_{\mathbb{R}} t : f(-t) = f(t),$$

og ulige, hvis

$$\forall_{\mathbb{R}} t : f(-t) = -f(t).$$

Vis, at mængden af lige funktioner og mængden af ulige funktioner er underrum i $(\hat{F}(\mathbb{R} \rightarrow \mathbb{R}), +, \mathbb{R})$, og at de er komplementære.

28. Angiv en basis for et komplementært underrum U'' til underrummet $U' = V((3, -2, 1))$ i $(L^3, +, L)$. Find derefter projektionen af vektoren $(2, 2, 2)$ på U' langs med det fundne underrum U'' .

29. Vis, at et fra $\{0\}$ og V forskelligt underrum i et endelig-dimensionalt vektorrum $(V, +, L)$ altid har uendelig mange komplementære.

30. Vis, at for endelig-dimensionale underrum $U^{(1)}, \dots, U^{(p)}$ af

et vektorrum er

$$\dim(U^{(1)} + \dots + U^{(p)}) \leq \dim U^{(1)} + \dots + \dim U^{(p)},$$

samt at lighedstegnet gælder, hvis og kun hvis summen af $U^{(1)}, \dots, U^{(p)}$ er direkte. (Vælg en basis i hvert af under-
rummene $U^{(1)}, \dots, U^{(p)}$.)

31. Vis, at summen $U + U' + U''$ af tre underrum af et vektor-
rum er direkte, hvis og kun hvis

$$U \cap (U' + U'') = U' \cap (U + U'') = U'' \cap (U + U') = \{\underline{0}\}.$$

- 32*. Lad U være et underrum i et vektorrum $(V, +, L)$. En vektor $\underline{v}' \in V$ siges at være kongruent modulo U med en vektor $\underline{v} \in V$, hvis $\underline{v}' - \underline{v} \in U$, og man skriver da $\underline{v}' \equiv \underline{v} \pmod{U}$. Vis, at den herved definerede relation i V er en ækvivalensrelation, som harmonerer med vektorrummets kompositionsforskrifter, dvs.

$$\begin{aligned} \underline{v}'_1 \equiv \underline{v}_1 \quad \wedge \quad \underline{v}'_2 \equiv \underline{v}_2 &\Rightarrow \underline{v}'_1 + \underline{v}'_2 \equiv \underline{v}_1 + \underline{v}_2, \\ \underline{v}' \equiv \underline{v} &\Rightarrow \lambda \underline{v}' \equiv \lambda \underline{v}. \end{aligned}$$

Definer kompositionsforskrifter i mængden V/U af ækvivalensklasser, således at dette "kvotientrum" bliver et vektorrum $(V/U, +, L)$. (Jfr. AG II, §1.)

Giv en geometrisk beskrivelse af relationen, ækvivalensklasserne og kompositionsforskrifterne for disse i det tilfælde, hvor U er et endimensionalt underrum i vektorrummet $(V_2, +, \vec{R})$ af geometriske vektorer i en plan. (Alle vektorer tænkes afsat fra samme punkt.) Angiv en isomorfi mellem $(V_2/U, +, \vec{R})$ og et vilkårligt til U komplementært underrum af $(V_2, +, \vec{R})$.

- 33*. Idet U og U' er komplementære underrum i et vektorrum $(V, +, L)$ skal man angive en isomorfi mellem U' og kvotientrummet $(V/U, +, L)$. (Se øvelse 32.)

34. Beskriv "enhedskuglerne" $\{\underline{x} \mid \|\underline{x}\|_p = 1\}$ for $p = 1, 2, \infty$ i talrummene $(\mathbb{R}^2, +, \mathbb{R})$ og $(\mathbb{R}^3, +, \mathbb{R})$.

35. Vis, at den i $(\mathbb{R}^2, +, \mathbb{R})$ ved

$$(x_1, x_2) \rightarrow (|x_1|^{\frac{1}{2}} + |x_2|^{\frac{1}{2}})^2$$

definerede funktion ikke er en norm.

36. Bestem samtlige normer i det endimensionale talrum $(L, +, L)$.

37. I det todimensionale talrum $(\mathbb{Q}^2, +, \mathbb{Q})$ over de rationale tals legeme defineres en norm ved

$$\|(x_1, x_2)\| = (x_1^2 + x_2^2)^{\frac{1}{2}}.$$

Angiv et endimensionalt underrum, som ikke indeholder nogen vektor med norm 1.

38. Vis, at der for hver vektor $(x_1, \dots, x_n)$ i talrummet $(\mathbb{R}^n, +, \mathbb{R})$ gælder

$$\begin{aligned} \|\underline{x}\|_{\infty} &\leq \|\underline{x}\|_2 \leq \|\underline{x}\|_1, \\ n^{-\frac{1}{2}} \|\underline{x}\|_1 &\leq \|\underline{x}\|_2 \leq n^{\frac{1}{2}} \|\underline{x}\|_{\infty}. \end{aligned}$$

*Undersøg, hvilke lignende uligheder der gælder mellem normerne $\|\varphi\|_1$, $\|\varphi\|_2$ og $\|\varphi\|_{\infty}$ i vektorrummet $(\hat{C}([a, b] \rightarrow \mathbb{R}), +, \mathbb{R})$.

39. Vis, at der ved

$$\|\varphi\|_{\infty}^{(1)} = \sup_{t \in [a, b]} |\varphi(t)| + \sup_{t \in [a, b]} |D\varphi(t)|$$

for $\varphi \in \hat{C}^1([a, b] \rightarrow \mathbb{R})$ defineres en norm i vektorrummet $(\hat{C}^1([a, b] \rightarrow \mathbb{R}), +, \mathbb{R})$ bestående af de på intervallet $[a, b]$ definerede og kontinuert differentiable reelle funktioner.

40. Vis, at for to lineært afhængige vektorer $\underline{u}$ og $\underline{v}$ i et normeret vektorrum gælder lighedstegnet i N3, altså i

$$\|\underline{u} + \underline{v}\| \leq \|\underline{u}\| + \|\underline{v}\|,$$

da og kun da, hvis en af vektorerne fremgår af den anden.

ved multiplikation med et reelt tal $v \geq 0$.

Giv et eksempel på, at lighedstegn i N_3 kan indtræffe for lineært uafhængige vektorer $\underline{u}$ og $\underline{v}$. (Benyt normen $\|\cdot\|_1$ i $(\mathbb{R}^2, +, \mathbb{R})$.)

41. Undersøg, om der i $(\mathbb{R}^2, +, \mathbb{R})$ defineres et indre produkt ved, at man til $(\underline{x}, \underline{y})$, hvor $\underline{x} = (x_1, x_2)$ og $\underline{y} = (y_1, y_2)$, lader svare

$$(1) \quad x_1 y_2 + x_2 y_1,$$

$$(2) \quad x_1 y_1 + x_1 y_2 + x_2 y_1 + x_2 y_2,$$

$$(3) \quad 2x_1 y_1 - x_1 y_2 - x_2 y_1 + 2x_2 y_2.$$

42. Vis, at der for vilkårlige vektorer $\underline{u}$ og $\underline{v}$ i et reelt vektorrum med indre produkt gælder

$$\underline{u} \perp \underline{v} \iff \|\underline{u} + \underline{v}\| = \|\underline{u} - \underline{v}\|.$$

Hvilken elementargeometrisk sætning udtrykkes herved i det tilfælde, hvor $\underline{u}$ og $\underline{v}$ er lineært uafhængige geometriske vektorer?

43. Vis, at der for vilkårlige vektorer $\underline{u}$ og $\underline{v}$ i et komplekst vektorrum med indre produkt gælder

$$\underline{u} \perp \underline{v} \iff \forall \lambda, \mu : \|\lambda \underline{u} + \mu \underline{v}\|^2 = \|\lambda \underline{u}\|^2 + \|\mu \underline{v}\|^2.$$

44. Vis, at der for vilkårlige vektorer $\underline{u}$ og $\underline{v}$ i et vektorrum med indre produkt gælder

$$\|\underline{u} + \underline{v}\|^2 + \|\underline{u} - \underline{v}\|^2 = 2\|\underline{u}\|^2 + 2\|\underline{v}\|^2.$$

Hvilken elementargeometrisk sætning udtrykkes herved i det tilfælde, hvor $\underline{u}$ og $\underline{v}$ er lineært uafhængige vektorer i vektorrummet $(V_3, +, \mathbb{R}, \cdot)$ af geometriske vektorer med skalarproduktet som indre produkt?

Vis, at ingen af normerne $\|\cdot\|_1$ og $\|\cdot\|_\infty$ i $(\mathbb{R}^2, +, \mathbb{R})$ udspringer af et indre produkt.

$$\int_0^1 \varphi(t) dt = 0,$$

som ortogonalt komplement i $\hat{C}_2([0,1] \rightarrow \mathbb{R})$ har underrummet af de på intervallet $[0,1]$ konstante reelle funktioner.

* Mængden af funktioner $\psi \in \hat{C}([-1,1] \rightarrow \mathbb{R})$, for hvilke

$$\int_0^1 \psi(t) dt = 0,$$

er et underrum U af $\hat{C}_2([-1,1] \rightarrow \mathbb{R})$. Vis, at $U^\perp = \{0\}$, og begrund herved, at U ikke har noget ortogonalt komplement.

51. Mængden af lige funktioner tilhørende $\hat{C}([-1,1] \rightarrow \mathbb{R})$ er et underrum U af $\hat{C}_2([-1,1] \rightarrow \mathbb{R})$. Vis, at U har et ortogonalt komplement, og angiv dette.

52. Vis, at der for hvilket som helst underrum U_1 og U_2 af et vektorrum med indre produkt gælder

$$(U_1 + U_2)^\perp = U_1^\perp \cap U_2^\perp.$$

Undersøg, om også ligningen

$$(U_1 \cap U_2)^\perp = U_1^\perp + U_2^\perp$$

er almengyldig, når vektorrummet er endelig-dimensionalt,

* og når det er uendelig-dimensionalt (jfr. øv. 50 og 51).

53. Vis, at funktionerne

$$1, \cos t, \sin t, \cos 2t, \sin 2t, \dots, \quad t \in [-\pi, \pi],$$

er parvis ortogonale i $\hat{C}_2([-\pi, \pi] \rightarrow \mathbb{R})$ såvel som i

$\hat{C}_2([-\pi, \pi] \rightarrow \mathbb{C})$, og dan ved normering af funktionerne et ortonormalsystem.

Vis, at man ved normering af funktionerne

$$\dots, e^{-i2t}, e^{-it}, 1, e^{it}, e^{i2t}, \dots \quad t \in [-\pi, \pi],$$

ligeledes får et ortonormalsystem i $\hat{C}_2([-\pi, \pi] \rightarrow \mathbb{C})$. Frembringer dette samme underrum som det forrige?

54. I vektorrummet $(\hat{P}([-1,1] \rightarrow \mathbb{R}), +, \mathbb{R})$ bestående af de reelle polynomiers restriktioner til intervallet $[-1,1]$ defineres et indre produkt ved

$$p \cdot q = \int_{-1}^1 p(t)q(t)dt.$$

Find ved ortonormalisering en ortonormal basis for det af $1, t, t^2$ udspændte underrum bestående af polynomierne af højst anden grad.

* Vis, at funktionerne

$$\varphi_n(t) = (n + \frac{1}{2})^{\frac{1}{2}} P_n(t), \quad n = 0, 1, 2, \dots,$$

hvor

$$P_n(t) = (2^n n!)^{-1} D^n(t^2 - 1)^n$$

er de såkaldte Legendre-polynomier, danner en ortonormal basis for det betragtede vektorrum. (Begynd med at vise, at $P_n(t)$ er ortogonal til alle polynomier af højst $(n-1)$ -te grad.)

- 55.** Der er givet en reel funktion $w(t)$, som er defineret, kontinuert og positiv i det åbne interval $]a, b[$, hvor $-\infty \leq a < b \leq \infty$, og for hvilken integralerne

$$\int_a^b w(t)|t|^n dt, \quad n = 0, 1, 2, \dots,$$

alle er konvergente. I vektorrummet $(\hat{P}(]a, b[\rightarrow \mathbb{R}, +, \mathbb{R})$ bestående af de reelle polynomiers restriktioner til intervallet $]a, b[$ defineres et indre produkt ved

$$p \cdot q = \int_a^b w(t)p(t)q(t)dt.$$

- 1) Vis, at dette vektorrum med indre produkt har en og kun én ortonormal basis $(\varphi_0, \varphi_1, \dots)$, således at φ_n for hvert

$n = 0, 1, \dots$ er et polynomium af n -te grad, hvori t^n har en positiv koefficient.

2) Vis, at polynomiet φ_n har n forskellige reelle rødder, som alle ligger i intervallet $]a, b[$. (Benyt, at der findes polynomier af $(n-1)$ -te grad, som har $n-1$ foreskrevne rødder.)

3) De til visse specielle "vægtfunktioner" w hørende ortonormale sæt af polynomier spiller en fremtrædende rolle i analysen og dens anvendelser.

α) For $a = -1$, $b = 1$, $w(t) = 1$ fås de ovenfor (øv. 54) omtalte polynomier, som fremgår ved normering af Legendre-polynomierne $P_n(t)$.

β) For $a = -1$, $b = 1$, $w(t) = (1-t^2)^{-\frac{1}{2}}$ fås

$$\varphi_0(t) = \pi^{-\frac{1}{2}}, \quad \varphi_n(t) = \left(\frac{1}{2}\pi\right)^{-\frac{1}{2}} T_n(t), \quad n = 1, 2, \dots,$$

hvor

$$T_n(t) = \cos(n \operatorname{Arccos} t), \quad n = 0, 1, 2, \dots$$

er de såkaldte Chebyshev-polynomier.

γ) For $a = 0$, $b = \infty$, $w(t) = e^{-t}$ fås

$$\varphi_n(t) = (-1)^n n!^{-1} L_n(t),$$

hvor

$$L_n(t) = e^t D^n(t^n e^{-t}), \quad n = 0, 1, 2, \dots$$

er de såkaldte Laguerre-polynomier.

δ) For $a = -\infty$, $b = \infty$, $w(t) = e^{-t^2}$ fås

$$\varphi_n(t) = (2^n n! \sqrt{\pi})^{-\frac{1}{2}} H_n(t), \quad n = 0, 1, 2, \dots$$

hvor

$$H_n(t) = (-1)^n e^{t^2} D^n e^{-t^2}, \quad n = 0, 1, 2, \dots$$

er de såkaldte Hermite-polynomier.

Eftervis, at disse polynomifølger er ortonormale sæt hørende til de angivne vægtfunktioner.

§ 2. Lineære afbildninger og matricer.

Definition af lineær afbildning. Billedrum. Kerne.

Lad der være givet to (ikke nødvendigvis forskellige) vektorrum $(U, +, L)$ og $(V, +, L)$ over det samme tallegeme L . (De to additioner plejer man at betegne på samme måde, skønt de jo er kompositioner i forskellige mængder.)

En afbildning $f: U \rightarrow V$ siges at være en homomorf afbildning af $(U, +, L)$ ind i $(V, +, L)$, hvis den opfylder betingelserne

$$LA1. \quad \forall_U \underline{u}_1, \underline{u}_2 : f(\underline{u}_1 + \underline{u}_2) = f(\underline{u}_1) + f(\underline{u}_2),$$

$$LA2. \quad \forall_L \lambda \quad \forall_U \underline{u} : f(\lambda \underline{u}) = \lambda f(\underline{u}),$$

som tilsammen er ensbetydende med

$$LA. \quad \forall_L \lambda_1, \lambda_2 \quad \forall_U \underline{u}_1, \underline{u}_2 : f(\lambda_1 \underline{u}_1 + \lambda_2 \underline{u}_2) = \lambda_1 f(\underline{u}_1) + \lambda_2 f(\underline{u}_2)$$

Homomorfe afbildninger af vektorrum kaldes i reglen lineære afbildninger, også tensorer eller, især når det drejer sig om uendelig-dimensionale vektorrum, lineære operatorer.

Ved enhver lineær afbildning $f: U \rightarrow V$ er

$$f(\underline{0}) = \underline{0},$$

billedet af nulvektoren i U er nulvektoren i V . (Man plejer at bruge samme betegnelse for de to nulvektorer; når der er fare for misforståelser, kan man skrive $\underline{0}_U$ og $\underline{0}_V$.) Påstanden følger f.eks. af LA2 med $\lambda = 0$, $\underline{u} = \underline{0}$:

$$f(\underline{0}) = f(0\underline{0}) = 0f(\underline{0}) = \underline{0}.$$

Den konstante afbildning, der til hver vektor i U lader svare nulvektoren i V , er øjensynlig lineær. Den kaldes nulafbildningen og betegnes hyppigt med 0 . Man skriver da $0(\underline{u}) = \underline{0}$ for $\underline{u} \in U$.

Af LA sluttet ved induktion, at der for hver lineær afbildning f , vilkårlige vektorer $\underline{u}_1, \dots, \underline{u}_p$ i U og vilkårlige skalarer $\lambda_1, \dots, \lambda_p$ gælder

$$f(\lambda_1 \underline{u}_1 + \dots + \lambda_p \underline{u}_p) = \lambda_1 f(\underline{u}_1) + \dots + \lambda_p f(\underline{u}_p).$$

Ved en lineær afbildning svarer altså til en linearkombination af vektorer den "samme" linearkombination af deres billedvektorer. Idet $f(\underline{0}) = \underline{0}$, kan heraf sluttet, at billedvektorerne til vektorer, mellem hvilke der består en egentlig lineær relation, tilfredsstiller den samme relation, følgelig:

Ved enhver lineær afbildning afbildes lineært afhængige vektorer på lineært afhængige vektorer.

Med andre ord:

Hvis vektorer ved en lineær afbildning har lineært uafhængige billedvektorer, er de selv lineært uafhængige.

Derimod kan lineært uafhængige vektorer have lineært afhængige billedvektorer. Dette vil f.eks. være tilfældet ved nulafbildningen.

Ved hver lineær afbildning $f: (U, +, L) \rightarrow (V, +, L)$ er billedet $f(U')$ af et underrum U' af U et underrum af V , og der gælder $\dim f(U') \leq \dim U'$.

Bevis: Er $\underline{v}_1, \underline{v}_2 \in f(U')$, altså $\underline{v}_1 = f(\underline{u}_1)$, $\underline{v}_2 = f(\underline{u}_2)$, hvor $\underline{u}_1, \underline{u}_2 \in U'$, gælder for $\lambda_1, \lambda_2 \in L$

$\lambda_1 \underline{v}_1 + \lambda_2 \underline{v}_2 = \lambda_1 f(\underline{u}_1) + \lambda_2 f(\underline{u}_2) = f(\lambda_1 \underline{u}_1 + \lambda_2 \underline{u}_2) \in f(U')$, idet $\lambda_1 \underline{u}_1 + \lambda_2 \underline{u}_2 \in U'$. Dette viser, at UR (side III, 1, 6) er opfyldt for $f(U')$. Dermed er den første påstand bevist. Den anden følger af, at hvis der findes p lineært uafhængige vektorer i $f(U')$, må der ifølge den foregående sætning også findes p lineært uafhængige vektorer i U' .

Specielt er billedet $f(U)$ af hele rummet U et underrum af V , hvis dimension er højst lig med dimensionen af U . Det kaldes billedrummet ved f . Dets dimension kaldes også den lineære afbildnings rang.

Originalmængden

$$f^{-1}(\underline{0}) = \{\underline{u} \in U \mid f(\underline{u}) = \underline{0}\}$$

til nulvektoren i V ved en lineær afbildning $f:(U,+,L) \rightarrow (V,+,L)$ kaldes den lineære afbildnings kerne og betegnes med K_f eller kort K , når det er klart, hvilken afbildning talen er om. (Idet LA1 udsiger, at en lineær afbildning er en homomorfi af gruppen $(U,+)$ ind i gruppen $(V,+)$, er denne definition på kerne i overensstemmelse med den tidligere.)

Kernen K for en lineær afbildning $f:(U,+,L) \rightarrow (V,+,L)$ er et underrum af U .

Bevis: Er $\underline{u}_1, \underline{u}_2 \in K$, altså $f(\underline{u}_1) = f(\underline{u}_2) = \underline{0}$, fås for $\lambda_1, \lambda_2 \in L$

$$f(\lambda_1 \underline{u}_1 + \lambda_2 \underline{u}_2) = \lambda_1 f(\underline{u}_1) + \lambda_2 f(\underline{u}_2) = \underline{0},$$

altså $\lambda_1 \underline{u}_1 + \lambda_2 \underline{u}_2 \in K$.

Kernen K kaldes også den lineære afbildnings nulrum.

Lad $\underline{v}_0$ være en vektor i V . Originalmængden

$$f^{-1}(\underline{v}_0) = \{\underline{u} \in U \mid f(\underline{u}) = \underline{v}_0\}$$

er tom, hvis $\underline{v}_0$ ikke tilhører billedrummet $f(U)$. Antag, at $\underline{v}_0 \in f(U)$, altså at der findes en vektor $\underline{u}_0 \in U$, for hvilken $f(\underline{u}_0) = \underline{v}_0$. For hver vektor $\underline{u} \in f^{-1}(\underline{v}_0)$ gælder da

$$f(\underline{u} - \underline{u}_0) = f(\underline{u}) - f(\underline{u}_0) = \underline{v}_0 - \underline{v}_0 = \underline{0},$$

dvs. $\underline{u} - \underline{u}_0 \in K$. Vektoren $\underline{u}$ fås altså af $\underline{u}_0$ ved at addere en vek-

tor tilhørende K . Dette kan også skrives $\underline{u} \in \{\underline{u}_0\} + K$ eller (uden fare for misforståelser)

$$\underline{u} \in \underline{u}_0 + K.$$

Vi har altså

$$f^{-1}(\underline{v}_0) \subseteq \underline{u}_0 + K.$$

Omvendt, er $\underline{u}_0 + \underline{k}$, $\underline{k} \in K$, en vilkårlig vektor tilhørende $\underline{u}_0 + K$, fås

$$f(\underline{u}_0 + \underline{k}) = f(\underline{u}_0) + f(\underline{k}) = \underline{v}_0 + \underline{0} = \underline{v}_0,$$

hvilket viser, at

$$\underline{u}_0 + \underline{k} \in f^{-1}(\underline{v}_0).$$

Vi har altså også

$$\underline{u}_0 + K \subseteq f^{-1}(\underline{v}_0).$$

Dermed er bevist:

For hver vektor $\underline{v}_0$ i billedrummet $f(U)$ ved en lineær afbildning $f:(U,+,L) \rightarrow (V,+,L)$ gælder

$$f^{-1}(\underline{v}_0) = \{\underline{u}_0 + \underline{k} \mid \underline{k} \in K\} = \underline{u}_0 + K,$$

hvor $\underline{u}_0$ er en af vektorerne i $f^{-1}(\underline{v}_0)$ og K er afbildningens kerne.

Dette udsiger, at man af én løsning $\underline{u}_0$ til ligningen $f(\underline{u}) = \underline{v}_0$ igen får en løsning ved at addere en vilkårlig vektor i kernen, og at man på denne måde kan få alle løsninger.

Kernen K kan opfattes som en undergruppe af gruppen $(U,+)$ og $\underline{u}_0 + K$ følgelig som en sideklasse til K . Tilsvarende gælder for et vilkårligt underrum U' af U . En delmængde af et vektorrum U af formen $\underline{u}_0 + U'$, hvor U' er et underrum, vil blive kaldt et sideunderrum eller kort et siderum til underrummet U' . To forskellige siderum til U' er disjunkte og siges også at være parallelle. Hver vektor i U er indeholdt i netop ét siderum til U' .

Den beviste sætning kan herefter gengives således: For hver vektor $\underline{v}_0 \in f(U)$ er løsningsmængden for ligningen $f(\underline{u}) = \underline{v}_0$ et siderum til kernen for f .

Det fremgår af sætningen, at $f^{-1}(\underline{v})$ for hver vektor $\underline{v} \in f(U)$ kun består af én vektor, hvis og kun hvis kernen K kun består af én vektor, som så må være $\underline{0}$. Altså:

En lineær afbildning $f:(U,+,L) \rightarrow (V,+,L)$ er injektiv, hvis og kun hvis der for kernen K gælder $K = \{\underline{0}\}$.

Om injektive lineære afbildninger gælder følgende sætning:

For en injektiv lineær afbildning $f:(U,+,L) \rightarrow (V,+,L)$ er den inverse $f^{-1}:f(U) \rightarrow U$ ligeledes lineær; lineært uafhængige vektorer afbildes ved f på lineært uafhængige vektorer, og for hvert underrum U' af U gælder $\dim f(U') = \dim U'$.

Bevis: For vilkårlige vektorer $\underline{v}_1 = f(\underline{u}_1)$ og $\underline{v}_2 = f(\underline{u}_2)$ i $f(U)$ og vilkårlige skalarer $\lambda_1, \lambda_2 \in L$ gælder

$$\lambda_1 \underline{v}_1 + \lambda_2 \underline{v}_2 = \lambda_1 f(\underline{u}_1) + \lambda_2 f(\underline{u}_2) = f(\lambda_1 \underline{u}_1 + \lambda_2 \underline{u}_2)$$

og dermed

$$f^{-1}(\lambda_1 \underline{v}_1 + \lambda_2 \underline{v}_2) = \lambda_1 \underline{u}_1 + \lambda_2 \underline{u}_2 = \lambda_1 f^{-1}(\underline{v}_1) + \lambda_2 f^{-1}(\underline{v}_2).$$

Dette viser, at f^{-1} er lineær. At lineært uafhængige vektorer i U afbildes på lineært uafhængige vektorer i $f(U) \subseteq V$, følger nu af, at de førstnævnte er billeder af de sidstnævnte ved den lineære afbildning f^{-1} (jfr. side 2.). At der for hvert underrum U' af U gælder $\dim f(U') = \dim U'$ er herefter indlysende.

En nødvendig betingelse for, at en lineær afbildning $f:(U,+,L) \rightarrow (V,+,L)$ er surjektiv, altså at $f(U) = V$, er øjensynlig $\dim f(U) = \dim V$. Hvis V er endelig-dimensional, er betingelsen også tilstrækkelig. Det følger umiddelbart af en tidligere

sætning (side III, 1, 13). Vi har altså:

En lineær afbildning f af et vektorrum $(U, +, L)$ ind i et endelig-dimensionalt vektorrum $(V, +, L)$ er surjektiv, hvis og kun hvis $\dim f(U) = \dim V$.

Eksempler.

1) En afbildning f af det geometriske vektorrum $(V_3, +, \mathbb{R})$ ind i sig selv defineres ved for en given vektor $\underline{a} \neq \underline{0}$ at sætte

$$f(\underline{u}) = \underline{a} \times \underline{u}, \quad \underline{u} \in V_3.$$

At f er lineær, følger af velkendte egenskaber ved vektorproduktet. Alle billedvektorer $\underline{v} = \underline{a} \times \underline{u}$ er vinkelrette på $\underline{a}$, og omvendt er hver vektor $\underline{v} \perp \underline{a}$ billede af en vektor $\underline{u}$, nemlig af $\underline{0}$, hvis $\underline{v} = \underline{0}$, og af én af de to på $\underline{a}$ og $\underline{v}$ vinkelrette vektorer med længden $\|\underline{v}\|/\|\underline{a}\|$, hvis $\underline{v} \neq \underline{0}$. Billedrummet består altså af alle på $\underline{a}$ vinkelrette vektorer. Tænkes alle vektorer afsat fra samme punkt O , kan man sige, at $f(V_3)$ er den på $\underline{a}$ vinkelrette plan gennem O . Kernen K består af de vektorer $\underline{u}$, for hvilke $\underline{a} \times \underline{u} = \underline{0}$, altså af vektorerne parallelle med $\underline{a}$, så at $K = \{t\underline{a} \mid t \in \mathbb{R}\}$. Afsattes vektorerne fra O , kan K siges at være den ved $\underline{a}$ bestemte linie gennem O . For en vektor $\underline{v}_0 = f(\underline{u}_0) \in f(V_3)$, som altså er vinkelret på $\underline{a}$, har ligningen $f(\underline{u}) = \underline{v}_0$, dvs.

$$\underline{a} \times \underline{u} = \underline{v}_0,$$

som løsningsmængde siderummet

$$\{\underline{u}_0 + t\underline{a} \mid t \in \mathbb{R}\}.$$

Afsattes vektorerne fra O , kan dette fortolkes som en parameterfremstilling for den med $\underline{a}$ parallelle linie gennem endepunktet af $\underline{u}_0$.

2) Lad der være givet to naturlige tal m og n samt mn tal a_{ij} , $i = 1, \dots, m$, $j = 1, \dots, n$, tilhørende et tallegeme L . Ved til talsættet $\underline{x} = (x_1, \dots, x_n) \in L^n$ at lade svare talsættet $\underline{y} = (y_1, \dots, y_m) \in L^m$ bestemt ved

$$y_1 = a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n$$

$$y_2 = a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n$$

$$\vdots \qquad \qquad \qquad \vdots$$

$$y_m = a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n$$

eller kort

$$y_i = \sum_{j=1}^n a_{ij}x_j, \quad i = 1, \dots, m,$$

fås en lineær afbildning $f: (L^n, +, L) \rightarrow (L^m, +, L)$. Det er nemlig klart, at der til $\lambda \underline{x}$, $\lambda \in L$, svarer $\lambda \underline{y}$, og hvis der til $\underline{x}' = (x'_1, \dots, x'_n)$ svarer $\underline{y}' = (y'_1, \dots, y'_m)$, vil der til $\underline{x} + \underline{x}'$ svare $\underline{y} + \underline{y}'$.

Tallene a_{ij} , ved hvilke den lineære afbildning f er bestemt, opstilles i et rektangulært skema, en såkaldt matrix,

$$\begin{pmatrix} a_{11} & a_{12} & \cdot & \cdot & \cdot & a_{1n} \\ a_{21} & a_{22} & \cdot & \cdot & \cdot & a_{2n} \\ \cdot & \cdot & & & & \cdot \\ \cdot & \cdot & & & & \cdot \\ a_{m1} & a_{m2} & \cdot & \cdot & \cdot & a_{mn} \end{pmatrix}.$$

Den har m "rækker" og n "søjler". For at angive dette taler man om en $(m \times n)$ -matrix. "Elementet" a_{ij} står i den i -te række og den j -te søjle; den første indeks angiver altså rækkenummeret, den anden søjlenummeret. Hver søjle er et talsæt tilhørende L^n , skrevet som en $(m \times 1)$ -matrix, hver række et talsæt tilhørende L^m .

Talsættet $\underline{y} = f(\underline{x})$ er linearkombinationen af matrixens søjler med koefficienterne $x_1, \dots, x_n$. Billedrummet $f(L^n)$ er det af søjlerne frembragte underrum af $(L^m, +, L)$. Kernen for f er mængden af de talsæt $\underline{x} = (x_1, \dots, x_n)$, som tilfredsstiller det homogene lineære ligningssystem

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= 0 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= 0 \\ \vdots & \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= 0. \end{aligned}$$

Et sådant systems løsningsmængde er altså et underrum af $(L^n, +, L)$. Originalmængden $f^{-1}(\underline{b})$ til et talsæt $\underline{b} = (b_1, \dots, b_m) \in L^m$ er løsningsmængden til det inhomogene lineære ligningssystem

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= b_2 \\ \vdots & \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n &= b_m. \end{aligned}$$

Hvis $\underline{b}$ ikke tilhører billedrummet $f(L^n)$, er løsningsmængden tom. Hvis $\underline{b} \in f(L^n)$, er løsningsmængden et siderum til kernen K_f . Man får da samtlige løsninger ved til én af dem at addere løsningerne til det homogene system. Dette viser, at hvis et lineært ligningssystem overhovedet har løsninger, har det enten én, nemlig når kernen for f er nuldimensional, eller uendelig mange.

3) Lad $(U, +, \dot{\mathbb{R}})$ betegne vektorrummet bestående af alle konvergente reelle talfølger $(x_1, x_2, \dots)$. Ved

$$(x_1, x_2, \dots) \rightarrow \lim_{i \rightarrow \infty} x_i$$

defineres en afbildning $f: U \rightarrow \dot{\mathbb{R}}$. Denne er en lineær afbild-

ning af $(\mathbb{U}, +, \mathbb{R})$ på $(\mathbb{R}, +, \mathbb{R})$, hvilket følger umiddelbart af regnereglerne for konvergente talfølger. Den er surjektiv, da hvert reelt tal er grænseværdi for en talfølge. Kernen for f består af alle talfølger, som konvergerer mod 0. Originalmængden $f^{-1}(b)$ til et reelt tal b består af alle reelle talfølger, som konvergerer mod b . Alle sådanne talfølger fås ved til én af dem at addere samtlige følger med grænseværdien 0.

4) En afbildning f af mængden $\hat{C}^1(I \rightarrow \mathbb{R})$ af de i et interval $I \subseteq \mathbb{R}$ kontinuert differentiable reelle funktioner ind i mængden $\hat{C}(I \rightarrow \mathbb{R})$ af de i samme interval kontinuerte funktioner fås ved til hver funktion φ tilhørende den første mængde at lade svare dens afledede $D\varphi$. Af velkendte differentiationsregler sluttes, at f er en lineær afbildning af $(\hat{C}^1(I \rightarrow \mathbb{R}), +, \mathbb{R})$ ind i $(\hat{C}(I \rightarrow \mathbb{R}), +, \mathbb{R})$.

Kernen for f er mængden af funktioner φ , for hvilke $D\varphi = 0$, altså det endimensionale underrum af $\hat{C}^1(I \rightarrow \mathbb{R})$, som består af de i I konstante funktioner. Originalmængden $f^{-1}(\psi)$ til en funktion $\psi \in \hat{C}(I \rightarrow \mathbb{R})$ består af stamfunktionerne til ψ . Alle disse fås ved til én af dem at addere samtlige konstanter. Idet hver i I kontinuert funktion har en stamfunktion, er f surjektiv.

5) Lad der være givet tre funktioner $\alpha_0, \alpha_1, \alpha_2 \in \hat{C}(I \rightarrow \mathbb{R})$, hvor $I \subseteq \mathbb{R}$ er et interval. En afbildning f af mængden $\hat{C}^2(I \rightarrow \mathbb{R})$ af de i intervallet I to gange kontinuert differentiable reelle funktioner φ ind i $\hat{C}(I \rightarrow \mathbb{R})$ defineres ved

$$\varphi \rightarrow \alpha_0 \varphi + \alpha_1 D\varphi + \alpha_2 D^2\varphi.$$

Ved hjælp af differentiationsregler ses, at f er en lineær afbildning af $(\hat{C}^2(I \rightarrow \mathbb{R}), +, \mathbb{R})$ ind i $(\hat{C}(I \rightarrow \mathbb{R}), +, \mathbb{R})$. Den kaldes en lineær differentialoperator af anden orden.

Kernen for f er mængden af løsninger φ til den homogene lineære differentiaalligning

$$\alpha_0 \varphi + \alpha_1 D\varphi + \alpha_2 D^2 \varphi = 0.$$

Originalmængden $f^{-1}(\beta)$ til en given funktion $\beta \in \hat{C}(I \rightarrow \mathbb{R})$ består af løsningerne φ til den inhomogene lineære differentiaalligning

$$\alpha_0 \varphi + \alpha_1 D\varphi + \alpha_2 D^2 \varphi = \beta.$$

Er der en løsning, fås samtlige ved til én af dem at addere alle løsninger til den homogene ligning.

Under forudsætning af, at $\alpha_2(t) \neq 0$ for alle $t \in I$, kan man bevise, at der til givne reelle tal $t_0 \in I$, c og c' findes netop én løsning φ til den sidst opskrevne differentiaalligning, for hvilken $\varphi(t_0) = c$ og $D\varphi(t_0) = c'$. Idet dette gælder for enhver opgiven funktion $\beta \in \hat{C}(I \rightarrow \mathbb{R})$, sluttet, at f er surjektiv. Endvidere følger, at kernen, altså løsningsmængden for den homogene differentiaalligning, er et todimensionalt underrum af $\hat{C}^2(I \rightarrow \mathbb{R})$. Er nemlig φ_0 og φ_1 de løsninger til den homogene ligning, for hvilke

$$\begin{aligned} \varphi_0(t_0) &= 1, & D\varphi_0(t_0) &= 0, \\ \varphi_1(t_0) &= 0, & D\varphi_1(t_0) &= 1, \end{aligned}$$

vil $\varphi = c\varphi_0 + c'\varphi_1$ være løsningen, for hvilken $\varphi(t_0) = c$ og $D\varphi(t_0) = c'$. Dette viser, at φ_0, φ_1 frembringer kernen. De to funktioner er også lineært uafhængige, idet man for $\lambda_0, \lambda_1 \in \mathbb{R}$ af

$$\forall t \in I : \lambda_0 \varphi_0(t) + \lambda_1 \varphi_1(t) = 0$$

kan slutte, at

$$\forall t \in I : \lambda_0 D\varphi_0(t) + \lambda_1 D\varphi_1(t) = 0,$$

og, ved at sætte $t = t_0$ i de to ligninger, at $\lambda_0 = 0$ og $\lambda_1 = 0$.

Er $(U, +, L)$ et vilkårligt vektorrum, bestemmes for hvert tal $\alpha \in L$ ved

$$\underline{u} \rightarrow \alpha \underline{u}, \quad \underline{u} \in U,$$

en lineær afbildning af vektorrummet ind i sig selv. For $\alpha = 0$ er den nulafbildningen. For $\alpha \neq 0$ er den bijektiv og kaldes en homoteti eller også multiplikation med multiplikatoren α . For $\alpha = 1$ fås den identiske afbildning e af U .

Lad U' og U'' være komplementære underrum af et vektorrum $(U, +, L)$, dvs.

$$U = U' \oplus U''.$$

Ved til hver vektor $\underline{u} \in U$ at lade svare dens projektion $\underline{u}'$ på U' langs U'' (jfr. side III,1,27) fås en afbildning $p': U \rightarrow U'$. Den er lineær; thi er

$$\underline{u}_1 = \underline{u}'_1 + \underline{u}''_1, \quad \underline{u}_2 = \underline{u}'_2 + \underline{u}''_2$$

opspaltningerne af vektorer $\underline{u}_1, \underline{u}_2 \in U$ i komponenter efter U' og U'' , vil der for $\lambda_1, \lambda_2 \in L$ gælde

$$\lambda_1 \underline{u}_1 + \lambda_2 \underline{u}_2 = (\lambda_1 \underline{u}'_1 + \lambda_2 \underline{u}'_2) + (\lambda_1 \underline{u}''_1 + \lambda_2 \underline{u}''_2),$$

hvor

$$\lambda_1 \underline{u}'_1 + \lambda_2 \underline{u}'_2 \in U', \quad \lambda_1 \underline{u}''_1 + \lambda_2 \underline{u}''_2 \in U'',$$

og dette viser, at

$$p'(\lambda_1 \underline{u}_1 + \lambda_2 \underline{u}_2) = \lambda_1 p'(\underline{u}_1) + \lambda_2 p'(\underline{u}_2).$$

Billedrummet $p'(U)$ er U' , idet $p'(\underline{u})$ for hver vektor $\underline{u} \in U$ ifølge definition tilhører U' , og hver vektor $\underline{u}' \in U'$ er billedvektor, nemlig af sig selv. Kernen for p' er mængden af vektorer $\underline{0} + \underline{u}''$, $\underline{u}'' \in U''$, altså U'' .

Afbildningen p' kaldes parallelprojektion på U' langs U'' . Tilsvarende defineres parallelprojektion på U'' langs U' .

Lad f være en lineær afbildning af et vektorrum $(U, +, L)$ ind i et vektorrum $(V, +, L)$. Lad U' være et til kernen K komplementært underrum af U . (Et sådant findes i hvert fald, når U har

endelig dimension; jfr. side III,1,27.) Er $\underline{u} = \underline{k} + \underline{u}'$ opspaltningen af en vilkårlig vektor $\underline{u} \in U$ i komponenter efter K og U' , fås

$$f(\underline{u}) = f(\underline{k}) + f(\underline{u}') = f(\underline{u}') .$$

Dette viser, at hver vektor $f(\underline{u})$ i billedrummet $f(U)$ tillige er billede af en vektor $\underline{u}' \in U'$, altså at $f(U) = f(U')$. Nu har restriktionen $f:U' \rightarrow V$ af f til U' kernen $\{\underline{0}\}$, idet $K \cap U' = \{\underline{0}\}$. Denne restriktion er følgelig injektiv, hvilket medfører, at $\dim f(U') = \dim U'$ (jfr. side III, 2, 5). Forudsættes, at U har den endelige dimension n , har man endvidere

$$\dim K + \dim U' = n ,$$

idet $K \oplus U' = U$ (jfr. side III,1,27). Dermed er bevist:

Ved hver lineær afbildning f af et vektorrum $(U,+,L)$ af endelig dimension n ind i et vektorrum $(V,+,L)$ består mellem kernens og billedrummets dimension relationen

$$\dim K + \dim f(U) = n .$$

Kvotientrum.

Lad U være et underrum i et vektorrum $(V,+,L)$. En vektor $\underline{v}' \in V$ siges at være kongruent modulo U med en vektor $\underline{v} \in V$, hvis $\underline{v}' - \underline{v} \in U$; man skriver da $\underline{v}' \equiv \underline{v} \pmod{U}$, eller blot $\underline{v}' \equiv \underline{v}$. Ved benyttelse af, at U er et underrum, vises let, at den herved definerede relation i V er en ækvivalensrelation. Det fremgår af definitionen, at ækvivalensklasserne er sideklasserne til U ; ækvivalensklassen, som indeholder en vektor $\underline{v} \in V$, er sideklassen $\underline{v} + U$. Mængden af ækvivalensklasser betegnes V/U .

Den indførte ækvivalensrelation harmonerer med vektorrummets

kompositionsforskrifter i den betydning, at

$$\begin{aligned}\underline{v}_1' \equiv \underline{v}_1 \wedge \underline{v}_2' \equiv \underline{v}_2 &\Rightarrow \underline{v}_1' + \underline{v}_2' \equiv \underline{v}_1 + \underline{v}_2, \\ \underline{v}' \equiv \underline{v} &\Rightarrow \lambda \underline{v}' \equiv \lambda \underline{v};\end{aligned}$$

dette viser let ved benyttelse af, at U er et underrum. Af den første af disse formler fremgår, at summen af en vilkårlig repræsentant fra klassen $\underline{v}_1 + U$ og en vilkårlig repræsentant fra klassen $\underline{v}_2 + U$ altid vil tilhøre klassen $(\underline{v}_1 + \underline{v}_2) + U$. Af den anden formel fremgår, at produktet af en skalar $\lambda \in L$ og en vilkårlig repræsentant fra klassen $\underline{v} + U$ altid vil tilhøre klassen $\lambda \underline{v} + U$. Dette viser, at der ved

$$(1) \quad (\underline{v}_1 + U) + (\underline{v}_2 + U) = (\underline{v}_1 + \underline{v}_2) + U$$

defineres en indre komposition i V/U , betegnet $+$ og kaldet addition, og at der ved

$$(2) \quad \lambda(\underline{v} + U) = \lambda \underline{v} + U$$

defineres en komposition fra $L \times V/U$ til V/U , kaldet multiplikation. Det eftervises uden besvær, at V/U herved er organiseret som et vektorrum $(V/U, +, L)$ over L , kaldet kvotientrummet af $(V, +, L)$ over (eller med hensyn til) underrummet U . Nulvektoren i kvotientrummet er klassen $\underline{0} + U = U$, den modsatte til $\underline{v} + U$ er $-\underline{v} + U$. For $V = U$ bliver kvotientrummet et vektorrum kun indeholdende nulvektoren, for $U = \{\underline{0}\}$ bliver kvotientrummet isomorft med $(V, +, L)$.

Lad afbildningen $\pi: V \rightarrow V/U$ være defineret ved $\pi(\underline{v}) = \underline{v} + U$. Afbildningen, som oplagt er surjektiv, kaldes den kanoniske projektion af V på V/U . Af (1) fremgår, at

$$\begin{aligned}\pi(\underline{v}_1 + \underline{v}_2) &= (\underline{v}_1 + \underline{v}_2) + U = (\underline{v}_1 + U) + (\underline{v}_2 + U) \\ &= \pi(\underline{v}_1) + \pi(\underline{v}_2),\end{aligned}$$

og af (2) fremgår, at

$$\begin{aligned}\pi(\lambda \underline{v}) &= \lambda \underline{v} + U = \lambda(\underline{v} + U) \\ &= \lambda \pi(\underline{v}) ,\end{aligned}$$

hvilket viser, at den kanoniske projektion er lineær. Kernen for π er netop underrummet U ; er V af endelig dimension, gælder følgelig (smlgn, III.2.12a)

$$\boxed{\dim U + \dim V/U = \dim V}$$

Lad nu f være en surjektiv lineær afbildning af et vektorrum $(V, +, L)$ på et vektorrum $(W, +, L)$, og lad K være kernen. For vilkårlige vektorer $\underline{v}_1, \underline{v}_2 \in V$ er da $f(\underline{v}_1) = f(\underline{v}_2)$ ensbetydende med $\underline{v}_1 - \underline{v}_2 \in K$. Heraf fremgår, at der ved $\underline{v} + K \rightarrow f(\underline{v})$ defineres en afbildning Φ af V/K ind i W , og at denne afbildning er bijektiv. Den er endvidere lineær; thi

$$\begin{aligned}\Phi((\underline{v}_1 + K) + (\underline{v}_2 + K)) &= \Phi((\underline{v}_1 + \underline{v}_2) + K) \\ &= f(\underline{v}_1 + \underline{v}_2) = f(\underline{v}_1) + f(\underline{v}_2) \\ &= \Phi(\underline{v}_1 + K) + \Phi(\underline{v}_2 + K) ,\end{aligned}$$

og

$$\begin{aligned}\Phi(\lambda(\underline{v} + K)) &= \Phi(\lambda \underline{v} + K) \\ &= f(\lambda \underline{v}) = \lambda f(\underline{v}) \\ &= \lambda \Phi(\underline{v} + K) .\end{aligned}$$

Hermed er godtgjort, at hvis $f: (V, +, L) \rightarrow (W, +, L)$ er en surjektiv lineær afbildning med kerne K , så er kvotientrummet $(V/K, +, L)$ isomorft med $(W, +, L)$; afbildningen Φ givet ved $\Phi(\underline{v} + K) = f(\underline{v})$ er en isomorfi af $(V/K, +, L)$ på $(W, +, L)$.

Som en konsekvens af denne sætning fås, at er U et under-

rum i et vektorrum $(V, +, L)$, så er kvotientrummet $(V/U, +, L)$ isomorft med ethvert til U komplementært underrum i V. Thi er U' et til U komplementært underrum, og betegner p projektionen af V på U' langs U , d.v.s. $p(\underline{u} + \underline{u}') = p(\underline{u}')$ for $\underline{u} \in U$, $\underline{u}' \in U'$, så er p en surjektiv lineær afbildning af V på U' med U som kerne.

Lineære afbildningers bestemmelse ved matricer.

Lad $(U, +, L)$ være et vektorrum af den endelige dimension n og $(\underline{e}_1, \dots, \underline{e}_n)$ en basis for det, og lad $(V, +, L)$ være et vilkårligt vektorrum. For vilkårligt opgivne vektorer $\underline{v}_1, \dots, \underline{v}_n \in V$ findes da en og kun én lineær afbildning $f: (U, +, L) \rightarrow (V, +, L)$, således at $f(\underline{e}_i) = \underline{v}_i$ for $i = 1, \dots, n$.

Bevis: At der ikke kan findes mere end én sådan afbildning, ses på følgende måde: Er $\underline{u}$ en vilkårlig vektor i U og $(u_1, \dots, u_n)$ dens koordinatsæt med hensyn til den givne basis, må der for en afbildning f af den forlangte art gælde

$$\begin{aligned}
 f(\underline{u}) &= f(u_1 \underline{e}_1 + \dots + u_n \underline{e}_n) \\
 &= u_1 f(\underline{e}_1) + \dots + u_n f(\underline{e}_n) \\
 &= u_1 \underline{v}_1 + \dots + u_n \underline{v}_n.
 \end{aligned}$$

Den eneste afbildning af U ind i V , som kan komme i betragtning, bestemmes altså ved

$$\underline{u} = u_1 \underline{e}_1 + \dots + u_n \underline{e}_n \mapsto u_1 \underline{v}_1 + \dots + u_n \underline{v}_n.$$

På den anden side ses det let, at den således definerede afbildning f er lineær, og idet koordinatsættet for $\underline{e}_i$ er $(0, \dots, 0, 1, 0, \dots, 0)$, hvor 1 står på den i -te plads, fås $f(\underline{e}_i) = \underline{v}_i$. Dermed er sætningen bevist.

Dimensionen af billedrummet ved f er lig med rangen af vektorsættet $(\underline{v}_1, \dots, \underline{v}_n)$, idet $f(U)$ jo består af alle linearkombinationer af disse vektorer, dvs. er det af $\underline{v}_1, \dots, \underline{v}_n$ frembragte underrum. For enhver lineær afbildning f af det n -dimensionale vektorrum $(U, +, L)$ med basen $(\underline{e}_1, \dots, \underline{e}_n)$ gælder altså

$$\dim f(U) = \text{rg}(f(\underline{e}_1), \dots, f(\underline{e}_n)).$$

Dette tal kaldes også den lineære afbildnings rang.

Det forudsættes nu, at $(V, +, L)$ også har endelig dimension. Lad denne være m , og lad der være valgt en basis $(\underline{f}_1, \dots, \underline{f}_m)$ for V . Billedvektorerne $\underline{v}_i = f(\underline{e}_i)$ ved en lineær afbildning $f: U \rightarrow V$ kan da på en og kun én måde skrives som linearkombinationer af $\underline{f}_1, \dots, \underline{f}_m$:

$$\begin{aligned}
 f(\underline{e}_1) &= a_{11} \underline{f}_1 + a_{21} \underline{f}_2 + \dots + a_{m1} \underline{f}_m \\
 f(\underline{e}_2) &= a_{12} \underline{f}_1 + a_{22} \underline{f}_2 + \dots + a_{m2} \underline{f}_m \\
 &\vdots \\
 f(\underline{e}_n) &= a_{1n} \underline{f}_1 + a_{2n} \underline{f}_2 + \dots + a_{mn} \underline{f}_m
 \end{aligned}$$

eller kort

$$(*) \quad f(\underline{e}_j) = \sum_{i=1}^m a_{ij} \underline{f}_i, \quad j = 1, \dots, n.$$

De mn tal a_{ij} , som optræder her, opstilles i form af en $(m \times n)$ -matrix (se side III, 2, 7)

$$\begin{pmatrix} a_{11} & a_{12} & \cdot & \cdot & \cdot & a_{1n} \\ a_{21} & a_{22} & \cdot & \cdot & \cdot & a_{2n} \\ \cdot & \cdot & & & & \cdot \\ \cdot & \cdot & & & & \cdot \\ \cdot & \cdot & & & & \cdot \\ a_{m1} & a_{m2} & \cdot & \cdot & \cdot & a_{mn} \end{pmatrix} = (a_{ij})_{i=1, \dots, m; j=1, \dots, n},$$

hvis søjler er koordinatsættene i koordinatsystemet $(\underline{f}_1, \dots, \underline{f}_m)$ af billedvektorerne $f(\underline{e}_1), \dots, f(\underline{e}_n)$.

Af den ovenfor beviste sætning fremgår, at der omvendt til hver $(m \times n)$ -matrix $(a_{ij})_{i=1, \dots, m; j=1, \dots, n}$ efter valg af baser $(\underline{e}_1, \dots, \underline{e}_n)$ og $(\underline{f}_1, \dots, \underline{f}_m)$ for U og V hører en bestemt lineær afbildning f af U ind i V , nemlig den, ved hvilken billedvektorerne af $\underline{e}_1, \dots, \underline{e}_n$ er givet ved (*).

Er $\underline{u} = u_1 \underline{e}_1 + \dots + u_n \underline{e}_n$ en vilkårlig vektor i U fås for billedvektoren $\underline{v} = f(\underline{u})$ ved hjælp af (*)

$$\begin{aligned} \underline{v} = f(\underline{u}) &= f\left(\sum_{j=1}^n u_j \underline{e}_j\right) = \sum_{j=1}^n u_j f(\underline{e}_j) \\ &= \sum_{j=1}^n u_j \sum_{i=1}^m a_{ij} \underline{f}_i \\ &= \sum_{i=1}^m \left(\sum_{j=1}^n a_{ij} u_j\right) \underline{f}_i. \end{aligned}$$

Heraf ses, at den i -te koordinat v_i for $\underline{v}$ med hensyn til koordinatsystemet $(\underline{f}_1, \dots, \underline{f}_m)$ er

$$v_i = \sum_{j=1}^n a_{ij} u_j, \quad i = 1, \dots, m.$$

Koordinatsættet $(v_1, \dots, v_m)$ for billedvektoren $\underline{v} = f(\underline{u})$ af en vektor $\underline{u}$ med koordinatsættet $(u_1, \dots, u_n)$ bestemmes altså ved

$$\begin{aligned} v_1 &= a_{11}u_1 + a_{12}u_2 + \dots + a_{1n}u_n \\ v_2 &= a_{21}u_1 + a_{22}u_2 + \dots + a_{2n}u_n \\ &\vdots \\ v_m &= a_{m1}u_1 + a_{m2}u_2 + \dots + a_{mn}u_n. \end{aligned}$$

Disse resultater kan sammenfattes på følgende måde:

Lad $(U, +, L)$ være et n -dimensionalt og $(V, +, L)$ et m -dimensionalt vektorrum, og lad der være valgt en basis $(\underline{e}_1, \dots, \underline{e}_n)$ for U og en basis $(\underline{f}_1, \dots, \underline{f}_m)$ for V . Der består da en enentydig korrespondance mellem de lineære afbildninger $f: (U, +, L) \rightarrow (V, +, L)$ og $(m \times n)$ -matricerne $(a_{ij})_{i=1, \dots, m; j=1, \dots, n}$ med elementer fra L , således at søjlerne i matricen svarende til en afbildning f er koordinatsættene med hensyn til koordinatsystemet $(\underline{f}_1, \dots, \underline{f}_m)$ for billedvektorerne $f(\underline{e}_j)$ af basisvektorerne $\underline{e}_1, \dots, \underline{e}_n$:

$$f(\underline{e}_j) = \sum_{i=1}^m a_{ij} \underline{f}_i, \quad j = 1, \dots, n.$$

Koordinatsættet $(v_1, \dots, v_m)$ for billedvektoren $\underline{v} = f(\underline{u})$ af en vektor $\underline{u}$ med koordinatsættet $(u_1, \dots, u_n)$ er bestemt ved

$$v_i = \sum_{j=1}^n a_{ij} u_j, \quad i = 1, \dots, m.$$

Er specielt $U = L^n$ og $V = L^m$, og vælges som basisvektorer for U n -sættene $\underline{e}_j = (0, \dots, 0, 1, 0, \dots, 0)$, hvor 1 står på den j -te plads, og som basisvektorer $\underline{f}_i$ de analoge m -sæt, ses heraf, at enhver lineær afbildning $f: (L^n, +, L) \rightarrow (L^m, +, L)$ kan fremstilles

på den tidligere angivne måde (side III, 2, 7, eks. 2).

Dimensionen af billedrummet $f(U)$ er som nævnt lig med rangen af vektorsættet $(f(\underline{e}_1), \dots, f(\underline{e}_n))$, dvs. maximaltallet af lineært uafhængige blandt disse vektorer, og dette tal er lig med maximaltallet af lineært uafhængige blandt vektorernes koordinatsæt (jfr. side III, 1, 21). Idet disse koordinatsæt er søjlerne i den til afbildningen hørende matrix, drejer det sig altså om maximaltallet af lineært uafhængige blandt søjlerne (hvorved disse skal betragtes som vektorer i L^m). Idet dette tal kaldes matrixens søjlerang, får vi med benyttelse af tidligere sætninger (side III, 2, 12 og 5):

For billedrummet ved og kernen for en lineær afbildning f af et n -dimensionalt vektorrum $(U, +, L)$ ind i et m -dimensionalt vektorrum $(V, +, L)$ gælder

$$\dim f(U) = r, \quad \dim K = n - r,$$

hvor r betegner søjlerangen af den $(m \times n)$ -matrix, der efter valg af baser for U og V hører til afbildningen.

Afbildningen f er injektiv, hvis og kun hvis $r = n$.

Regning med lineære afbildninger.

Af lineære afbildninger kan på flere måder dannes andre lineære afbildninger.

Er $f: (U, +, L) \rightarrow (V, +, L)$ en lineær afbildning og α et tal i L , bestemmes der ved

$$\underline{u} \rightarrow \alpha f(\underline{u}), \quad \underline{u} \in U,$$

en afbildning af U ind i V , som øjensynlig også er lineær. Den betegnes αf . Som eksempel nævnes, at en homoteti af $(U, +, L)$ med

multiplikatoren α kan betegnes αe , hvor e er den identiske afbildning af U .

Er $f_i: (U, +, L) \rightarrow (V, +, L)$, $i = 1, 2$, lineære afbildninger, bestemmes der ved

$$\underline{u} \rightarrow f_1(\underline{u}) + f_2(\underline{u}), \quad \underline{u} \in U,$$

en afbildning af U ind i V , som øjensynlig også er lineær. Den betegnes $f_1 + f_2$. Som eksempel nævnes: Er U' og U'' underrum af U , således at $U' \oplus U'' = U$, har man for parallelprojektionerne p' på U' langs U'' og p'' på U'' langs U'

$$p' + p'' = e,$$

hvor e er den identiske afbildning af U .

Idet mængden af lineære afbildninger (homomorfier) $f: (U, +, L) \rightarrow (V, +, L)$ betegnes $\text{Hom}(U, V)$, er der defineret en komposition $L \times \text{Hom}(U, V) \rightarrow \text{Hom}(U, V)$, betegnet som multiplikation, og en komposition i $\text{Hom}(U, V)$, betegnet som addition. Det ses let, at $\text{Hom}(U, V)$ med disse kompositioner er et vektorrum. Dets nulvektor er nulafbildningen.

Det forudsættes nu, at U og V er endelig-dimensionale med dimensionerne n og m , og det antages, at der er valgt baser for U og V . Er da

$$(a_{ij})_{i=1, \dots, m; j=1, \dots, n}$$

eller kort $(a_{ij})_{m,n}$ den til en lineær afbildning f hørende $(m \times n)$ -matrix og $\alpha \in L$, vil der til afbildningen αf høre matricen $(\alpha a_{ij})_{m,n}$. Denne fremgår altså af den oprindelige ved, at hvert element multipliceres med α . Man definerer

$$\alpha(a_{ij})_{m,n} = (a_{ij})_{m,n} \alpha = (\alpha a_{ij})_{m,n}.$$

Er $(a_{ij}^{(1)})_{m,n}$ og $(a_{ij}^{(2)})_{m,n}$ de til lineære afbildninger f_1 og f_2 hørende matricer, vil der til afbildningen $f_1 + f_2$ høre matricen $(a_{ij}^{(1)} + a_{ij}^{(2)})_{m,n}$. Denne fremgår af de givne ved, at tilsvarende

elementer i disse adderes. Man definerer

$$(a_{ij}^{(1)})_{m,n} + (a_{ij}^{(2)})_{m,n} = (a_{ij}^{(1)} + a_{ij}^{(2)})_{m,n}.$$

Organiseret ved disse kompositioner er mængden $M_{m,n}(L)$ af alle $(m \times n)$ -matricer med elementer fra L et vektorrum over L . Dets nulvektor er "nulmatricen", hvis elementer alle er 0. Det har dimensionen mn , idet de mn matricer, som hver har ét element lig 1 og de øvrige lig 0, danner en basis.

Ved til hver lineær afbildning af U ind i V at lade svare den tilhørende matrix, fås en bijektiv lineær afbildning, dvs. en isomorf afbildning (se side III, 1, 21) af $\text{Hom}(U,V)$ på $M_{m,n}(L)$.

Er $(U,+,L)$, $(V,+,L)$ og $(W,+,L)$ vektorrum over det samme tallegeme L , og er $f:(U,+,L) \rightarrow (V,+,L)$ og $g:(V,+,L) \rightarrow (W,+,L)$ lineære afbildninger, vil også afbildningen $g \circ f:(U,+,L) \rightarrow (W,+,L)$ være lineær.

Bevis: For $\underline{u}_1, \underline{u}_2 \in U$ og $\lambda_1, \lambda_2 \in L$ gælder

$$\begin{aligned} g(f(\lambda_1 \underline{u}_1 + \lambda_2 \underline{u}_2)) &= g(\lambda_1 f(\underline{u}_1) + \lambda_2 f(\underline{u}_2)) \\ &= \lambda_1 g(f(\underline{u}_1)) + \lambda_2 g(f(\underline{u}_2)). \end{aligned}$$

Har de tre vektorrum $(U,+,L)$, $(V,+,L)$ og $(W,+,L)$ de endelige dimensioner n , m og l , og er der valgt baser $(\underline{e}_1, \dots, \underline{e}_n)$, $(\underline{f}_1, \dots, \underline{f}_m)$ og $(\underline{g}_1, \dots, \underline{g}_l)$ for dem, hører der til en lineær afbildning $f:(U,+,L) \rightarrow (V,+,L)$ en $(m \times n)$ -matrix $(a_{ij})_{m,n}$ og til en lineær afbildning $g:(V,+,L) \rightarrow (W,+,L)$ en $(l \times m)$ -matrix $(b_{hi})_{l,m}$. Man har da

$$f(\underline{e}_j) = \sum_{i=1}^m a_{ij} \underline{f}_i, \quad j = 1, \dots, n,$$

$$g(\underline{f}_i) = \sum_{h=1}^l b_{hi} g_h, \quad i = 1, \dots, m,$$

følgelig

$$\begin{aligned} g(f(\underline{e}_j)) &= \sum_{i=1}^m a_{ij} g(\underline{f}_i) \\ &= \sum_{h=1}^l \left(\sum_{i=1}^m b_{hi} a_{ij} \right) g_h, \quad j = 1, \dots, n. \end{aligned}$$

Heraf ses, at den til g af hørende $(l \times n)$ -matrix $(c_{hj})_{l,n}$ har elementerne

$$c_{hj} = \sum_{i=1}^m b_{hi} a_{ij}, \quad h = 1, \dots, l; j = 1, \dots, n.$$

Denne matrix kaldes produktet af matricerne $(b_{hi})_{l,m}$ og $(a_{ij})_{m,n}$, og man skriver

$$(c_{hj})_{l,n} = (b_{hi})_{l,m} (a_{ij})_{m,n}.$$

Det bemærkes, at den første faktor har lige så mange søjler, som den anden har rækker; kun når dette er tilfældet, defineres produktet. Produktmatrixens element c_{hj} i h -te række og j -te søjle fås ved at multiplicere hvert element i den første faktors h -te række med det "tilsvarende placerede" element i den anden faktors j -te søjle og addere disse produkter.

For sammensætning af lineære afbildninger

$$f : (U, +, L) \rightarrow (V, +, L) \quad f' : (U, +, L) \rightarrow (V, +, L) ,$$

$$g : (V, +, L) \rightarrow (W, +, L) , \quad g' : (V, +, L) \rightarrow (W, +, L)$$

gælder

$$g \circ (f + f') = g \circ f + g \circ f' , \quad (g + g') \circ f = g \circ f + g' \circ f ,$$

$$\lambda(g \circ f) = (\lambda g) \circ f = g \circ (\lambda f) , \quad \lambda \in L .$$

For hvert $\underline{u} \in U$ har man nemlig

$$g((f + f')(\underline{u})) = g(f(\underline{u}) + f'(\underline{u})) = g(f(\underline{u})) + g(f'(\underline{u})) ,$$

$$(g + g')(f(\underline{u})) = g(f(\underline{u})) + g'(f(\underline{u})) ,$$

$$\lambda g(f(\underline{u})) = (\lambda g)(f(\underline{u})) = g(\lambda f(\underline{u})) .$$

I vektorrummet $\text{Hom}(U, U)$ af alle lineære afbildninger af $(U, +, L)$ ind i sig selv er $\circ$ en komposition. Ovenstående regler viser, at $(\text{Hom}(U, U), +, L, \circ)$ er en algebra. Den har et etelement, nemlig den identiske afbildning af U , og er associativ, men, hvis $\dim U > 1$, ikke kommutativ. Man kalder den endomorfialgebraen for vektorrummet $(U, +, L)$ eller, idet lineære afbildninger, især af uendelig-dimensionale vektorrum, også betegnes som lineære operatorer, vektorrummets operatoralgebra.

Matrixregning.

De indførte regneoperationer for matricer finder også anvendelse uden for teorien for lineære afbildninger. De tages derfor som grundlag for en regning med matricer.

I det følgende betragtes matricer med vilkårlige tal tilhø-

rende et tallegeme L som elementer. Foruden de allerede benyttede betegnelser

$$\begin{pmatrix} a_{11} & \cdot & \cdot & \cdot & a_{1n} \\ \vdots & & & & \vdots \\ a_{m1} & \cdot & \cdot & \cdot & a_{mn} \end{pmatrix} = (a_{ij})_{i=1, \dots, m; j=1, \dots, n} = (a_{ij})_{m,n}$$

for en $(m \times n)$ -matrix plejer man som betegnelse at bruge et enkelt bogstav, i det følgende for tydelighedens skyld dobbelt understreget, f.eks. $\underline{\underline{A}}$ eller $\underline{\underline{A}}_{m,n}$, hvis det er nødvendigt at angive rækketal m og søjletal n .

I stedet for en (1×1) -matrix (a_{11}) kan man i reglen uden fare for misforståelser skrive tallet a_{11} .

Det er ofte hensigtsmæssigt at opfatte et talsæt $(a_1, \dots, a_n)$ som en rækkematrix, dvs. en $(1 \times n)$ -matrix, eller som en søjlematrix, dvs. en $(n \times 1)$ -matrix. Vi skriver da henholdsvis

$$\underline{\underline{a}}_{-} = (a_1 \ \dots \ a_n), \quad \underline{\underline{a}}_{|} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

Den i -te række i en matrix $\underline{\underline{A}} = (a_{ij})_{m,n}$, opfattet som $(1 \times n)$ -matrix, vil blive betegnet $\underline{\underline{a}}_{i-}$ og den j -te søjle, opfattet som $(m \times 1)$ -matrix, $\underline{\underline{a}}_{|j}$.

Nulmatricerne, dvs. de matricer, hvis elementer alle er 0, betegnes $\underline{\underline{0}}$ eller, hvis angivelse af "typen" er nødvendig, $\underline{\underline{0}}_{m,n}$.

En matrix med lige mange rækker og søjler siges at være kvadratisk.

For hvert naturligt tal n defineres $(n \times n)$ -enhedsmatricen ved

$$\underline{\underline{E}} = \underline{\underline{E}}_{n,n} = \begin{pmatrix} 1 & 0 & \dots & \dots & \dots & 0 & 0 \\ 0 & 1 & \dots & \dots & \dots & 0 & 0 \\ \vdots & \vdots & & & & \vdots & \vdots \\ \vdots & \vdots & & & & \vdots & \vdots \\ 0 & 0 & \dots & \dots & \dots & 1 & 0 \\ 0 & 0 & \dots & \dots & \dots & 0 & 1 \end{pmatrix}$$

Ved hjælp af det såkaldte Kroneckersymbol

$$\delta_{\iota\kappa} = \begin{cases} 1 & \text{for } \iota = \kappa \\ 0 & \text{for } \iota \neq \kappa \end{cases}, \quad \iota, \kappa \in J,$$

hvor J betegner en vilkårlig indeksmængde, kan man også skrive

$$\underline{\underline{E}} = \underline{\underline{E}}_{n,n} = (\delta_{ij})_{i,j=1,\dots,n} = (\delta_{ij})_{n,n}.$$

Elementerne a_{ii} , $i = 1, \dots, n$, i en kvadratisk matrix kaldes dens hoveddiagonalelementer eller kort diagonalelementer. En $(n \times n)$ -matrix $(a_{ij})_{n,n}$, hvor alle elementer "over hoveddiagonalen" er 0, altså $a_{ij} = 0$ for $i < j$, kaldes en nedre trekantsmatrix. Tilsvarende kaldes $(a_{ij})_{n,n}$ en øvre trekantsmatrix, hvis $a_{ij} = 0$ for $i > j$. Endelig forstås ved en diagonalmatrix en kvadratisk matrix $(a_{ij})_{n,n}$, hvor alle elementer uden for hoveddiagonalen er 0, altså $a_{ij} = 0$ for $i \neq j$. En diagonalmatrix med diagonalelementerne $a_1, \dots, a_n$ betegnes undertiden $(a_1, \dots, a_n)_{\text{diag}}$.

Er $\underline{\underline{A}} = (a_{ij})_{m,n}$ en vilkårlig matrix og $\alpha \in L$, defineres som omtalt produktet af α og $\underline{\underline{A}}$ ved

$$\alpha \underline{\underline{A}} = \underline{\underline{A}} \alpha = (\alpha a_{ij})_{m,n}.$$

Er $\underline{\underline{A}} = (a_{ij})_{m,n}$ og $\underline{\underline{B}} = (b_{ij})_{m,n}$ to matricer af samme type, defineres som omtalt summen af $\underline{\underline{A}}$ og $\underline{\underline{B}}$ ved

$$\underline{\underline{A}} + \underline{\underline{B}} = (a_{ij} + b_{ij})_{m,n}.$$

For to matricer af forskellig type defineres ikke nogen sum.

Hvad angår regneregler, er det tilstrækkeligt at bemærke,

at for givne m og n er mængden $M_{m,n}(L)$ af $(m \times n)$ -matricer med disse kompositioner et vektorrum.

Er $\underline{\underline{A}} = (a_{ij})_{m,n}$ og $\underline{\underline{B}} = (b_{jk})_{n,p}$ to matricer, hvor den førstes søjletal er lig med den andens rækketal, defineres produktmatricen $\underline{\underline{AB}}$ som $(m \times p)$ -matricen

$$\underline{\underline{AB}} = \left(\sum_{j=1}^n a_{ij} b_{jk} \right)_{i=1, \dots, m; k=1, \dots, p}.$$

For andre par af matricer defineres ikke nogen produktmatrix.

Hvis produktet $\underline{\underline{AB}}$ kan dannes, vil $\underline{\underline{BA}}$ almindeligvis ikke kunne dannes. Alene af denne grund kan der ikke være tale om kommutativitet. Men selv om begge produktmatricer er definerede, ja selv om $\underline{\underline{A}}$ og $\underline{\underline{B}}$ er kvadratiske matricer med samme rækketal, gælder almindeligvis $\underline{\underline{AB}} \neq \underline{\underline{BA}}$.

Matrixmultiplikationen er associativ i den forstand, at når $\underline{\underline{A}} = (a_{ij})$ er en $(m \times n)$ -matrix, $\underline{\underline{B}} = (b_{jk})$ en $(n \times p)$ -matrix og $\underline{\underline{C}} = (c_{kl})$ en $(p \times q)$ -matrix, kan $(\underline{\underline{AB}})\underline{\underline{C}}$ og $\underline{\underline{A}}(\underline{\underline{BC}})$ dannes, og der gælder

$$(\underline{\underline{AB}})\underline{\underline{C}} = \underline{\underline{A}}(\underline{\underline{BC}}).$$

Dette kan slutes af, at sammensætning af lineære afbildninger er associativ. Men det følger også af

$$\sum_{k=1}^p \left(\sum_{j=1}^n a_{ij} b_{jk} \right) c_{kl} = \sum_{j=1}^n a_{ij} \sum_{k=1}^p b_{jk} c_{kl},$$

idet venstre og højre side er elementet i den i -te række og l -te søjle af henholdsvis $(\underline{\underline{AB}})\underline{\underline{C}}$ og $\underline{\underline{A}}(\underline{\underline{BC}})$. Produkter af flere end to matricer kan altså skrives uden parenteser.

Når $\underline{\underline{AB}}$ er defineret og $\alpha \in L$, gælder

$$(\alpha \underline{\underline{A}})\underline{\underline{B}} = \underline{\underline{A}}(\alpha \underline{\underline{B}}) = \alpha(\underline{\underline{AB}}).$$

Matrixmultiplikationen er distributiv med hensyn til additionen i den forstand, at når $\underline{A} = (a_{ij})$ er en $(m \times n)$ -matrix og $\underline{B} = (b_{jk})$ og $\underline{C} = (c_{jk})$ er $(n \times p)$ -matricer, kan $\underline{A}(\underline{B} + \underline{C})$ og $\underline{AB} + \underline{AC}$ dannes, og der gælder

$$\underline{A}(\underline{B} + \underline{C}) = \underline{AB} + \underline{AC}.$$

Dette følger af

$$\sum_{j=1}^n a_{ij}(b_{jk} + c_{jk}) = \sum_{j=1}^n a_{ij}b_{jk} + \sum_{j=1}^n a_{ij}c_{jk}.$$

Tilsvarende ses, at der gælder

$$(\underline{B} + \underline{C})\underline{D} = \underline{BD} + \underline{CD},$$

når $\underline{D}$ er en $(p \times q)$ -matrix.

For multiplikationen af en $(m \times n)$ -matrix $\underline{A}$ med nulmatricer gælder

$$\underline{0}_{1,m} \underline{A}_{m,n} = \underline{0}_{1,n}, \quad \underline{A}_{m,n} \underline{0}_{n,p} = \underline{0}_{m,p}.$$

For multiplikationen af en $(m \times n)$ -matrix $\underline{A} = (a_{ij})$ med enhedsmatricer gælder

$$\underline{E}_{m,m} \underline{A}_{m,n} = \underline{A}_{m,n} \underline{E}_{n,n} = \underline{A}_{m,n}.$$

Dette følger af

$$\sum_{j=1}^m \delta_{ij} a_{jk} = \sum_{j=1}^m a_{ij} \delta_{jk} = a_{ik}.$$

Idet der for en enhedsmatrix $\underline{E}$ og $\alpha \in L$ gælder

$$\alpha \underline{E} = (\alpha, \dots, \alpha)_{\text{diag}},$$

har man for hver matrix $\underline{A}$

$$\alpha \underline{A} = \alpha \underline{E} \underline{A} = (\alpha, \dots, \alpha)_{\text{diag}} \underline{A}.$$

For et givet naturligt tal n betragtes nu mængden $M_{n,n}(L)$ af $(n \times n)$ -matricer. For hvert par af sådanne matricer er såvel summen som produktet defineret og tilhører $M_{n,n}(L)$. Additionen og

multiplikationen er altså kompositioner i $M_{n,n}(L)$, og af de viste regler fremgår, at der foreligger en (ikke kommutativ) ring. Den kaldes matrixringen af graden n over L . For additionen er $\underline{0}$ neutralt element, for multiplikationen er $\underline{E}$ neutralt element, og der kan ikke findes andre.

For hver $(n \times n)$ -matrix $\underline{A}$ defineres potenserne

$$\underline{A}^p = \begin{cases} \underline{E} & \text{for } p = 0 \\ \underbrace{\underline{A}\underline{A} \dots \underline{A}}_{(p \text{ faktorer})} & \text{for } p \in \mathbb{N}. \end{cases}$$

Da gælder for ikke-negative hele tal potensreglerne

$$\underline{A}^p \underline{A}^q = \underline{A}^{p+q}, \quad (\underline{A}^p)^q = \underline{A}^{pq},$$

og dersom $\underline{A}$ og $\underline{B}$ er ombyttelige $(n \times n)$ -matricer, dvs. dersom $\underline{AB} = \underline{BA}$, også

$$\underline{A}^p \underline{B}^p = (\underline{AB})^p.$$

Idet matrixmultiplikationen er associativ, findes der til en $(n \times n)$ -matrix $\underline{A}$ højst én (med hensyn til multiplikationen) invers, dvs. der findes højst én $(n \times n)$ -matrix $\underline{X}$, for hvilken

$$\underline{AX} = \underline{XA} = \underline{E}.$$

Hvis der findes en, siges $\underline{A}$ at være regulær eller invertibel, og den inverse matrix betegnes $\underline{A}^{-1}$. For en regulær matrix $\underline{A}$ og dens inverse gælder altså

$$\underline{AA}^{-1} = \underline{A}^{-1}\underline{A} = \underline{E}.$$

Heraf ses, at den inverse til en regulær matrix ligeledes er regulær, og at der gælder

$$(\underline{A}^{-1})^{-1} = \underline{A}.$$

Det er klart, at $\underline{E}$ er regulær. Er $\underline{A}$ og $\underline{B}$ regulære $(n \times n)$ -matricer, vil også $\underline{AB}$ være regulær med den inverse

$$(\underline{AB})^{-1} = \underline{B}^{-1}\underline{A}^{-1};$$

thi

$$\underline{\underline{A}}\underline{\underline{B}}\underline{\underline{B}}^{-1} \underline{\underline{A}}^{-1} = \underline{\underline{A}}\underline{\underline{E}}\underline{\underline{A}}^{-1} = \underline{\underline{A}}\underline{\underline{A}}^{-1} = \underline{\underline{E}},$$

$$\underline{\underline{B}}^{-1} \underline{\underline{A}}^{-1} \underline{\underline{A}}\underline{\underline{B}} = \underline{\underline{B}}^{-1} \underline{\underline{E}}\underline{\underline{B}} = \underline{\underline{B}}^{-1} \underline{\underline{B}} = \underline{\underline{E}}.$$

Matrixmultiplikationen er altså en komposition i mængden af regulære $(n \times n)$ -matricer, og det fremgår af det sagte, at de regulære $(n \times n)$ -matricer med elementer fra L danner en gruppe med multiplikationen som komposition. Den kaldes den generelle lineære gruppe af graden n over tallegemet L og betegnes $GL(n, L)$.

Af sætninger om grupper sluttes, at de ovenfor nævnte potensregler gælder for regulære matricer med vilkårlige hele eksponenter, og at

$$(\underline{\underline{A}}_1 \underline{\underline{A}}_2 \dots \underline{\underline{A}}_p)^{-1} = \underline{\underline{A}}_p^{-1} \dots \underline{\underline{A}}_2^{-1} \underline{\underline{A}}_1^{-1}$$

for vilkårlige regulære matricer $\underline{\underline{A}}_1, \dots, \underline{\underline{A}}_p$.

Er $\underline{\underline{A}}$ en regulær $(n \times n)$ -matrix, $\underline{\underline{B}}$ en $(n \times p)$ -matrix og $\underline{\underline{C}}$ en $(m \times n)$ -matrix, findes der en og kun én $(n \times p)$ -matrix $\underline{\underline{X}}$, som tilfredsstiller ligningen

$$\underline{\underline{A}} \underline{\underline{X}} = \underline{\underline{B}},$$

og en og kun én $(m \times n)$ -matrix $\underline{\underline{Y}}$, som tilfredsstiller ligningen

$$\underline{\underline{Y}} \underline{\underline{A}} = \underline{\underline{C}}.$$

Multipliseres nemlig den første ligning fra venstre og den anden fra højre med $\underline{\underline{A}}^{-1}$, ses, at de eneste matricer, der kan være løsninger til disse matrixligninger, er

$$\underline{\underline{X}} = \underline{\underline{A}}^{-1} \underline{\underline{B}}, \quad \underline{\underline{Y}} = \underline{\underline{C}} \underline{\underline{A}}^{-1}.$$

Indsættelse viser, at de virkelig tilfredsstiller ligningerne.

Skriver man for eksempel ligningen $\underline{\underline{A}} \underline{\underline{X}} = \underline{\underline{B}}$ elementvis, ser man, at det drejer sig om et lineært ligningssystem bestående af np ligninger og med de np elementer af $\underline{\underline{X}}$ som ubekendte. For $p = 1$ er

$$\underline{B} = \underline{b}_j = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}, \quad \underline{X} = \underline{x}_j = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

søjlematricer, og matrixligningen

$$\underline{A} \underline{x}_j = \underline{b}_j$$

er ensbetydende med et ligningssystem

$$\begin{array}{ccccccc} a_{11}x_1 & + & \cdots & + & a_{1n}x_n & = & b_1 \\ \vdots & & & & \vdots & & \vdots \\ a_{n1}x_1 & + & \cdots & + & a_{nn}x_n & = & b_n \end{array}$$

med lige mange ligninger og ubekendte. Ovenstående sætning udsiger, at hvis "koefficientmatricen" $\underline{A}$ er regulær, har ligningssystemet for hver søjle $\underline{b}_j$ en og kun én løsning $\underline{x}_j = \underline{A}^{-1} \underline{b}_j$. Dette resultat er imidlertid uden betydning for bestemmelsen af løsningen til et forelagt ligningssystem, sålænge man ikke råder over metoder til afgørelse af, om en kvadratisk matrix er regulær, og til bestemmelse af den inverse til en regulær matrix. (Ifølge den inverses definition kommer beregningen af den ud på løsning af et lineært ligningssystem med n^2 ubekendte.) Sådanne metoder vil blive omtalt senere. Her vil der ved hjælp af sætninger om lineære afbildninger blive opstillet en nødvendig og tilstrækkelig betingelse for, at en kvadratisk matrix er regulær:

En $(n \times n)$ -matrix $\underline{A}$ er regulær, hvis og kun hvis dens søjler $\underline{a}_1, \dots, \underline{a}_n$ er lineært uafhængige talsæt, dvs. hvis dens søjlerang er n .

En tilstrækkelig betingelse for, at en $(n \times n)$ -matrix $\underline{A}$ har søjlerangen n og dermed er regulær, er allerede, at der findes en $(n \times n)$ -matrix $\underline{X}$, for hvilken $\underline{A} \underline{X} = \underline{E}$, eller en $(n \times n)$ -matrix $\underline{Y}$, for hvilken $\underline{Y} \underline{A} = \underline{E}$.

Bevis: I talrummet $(L^n, +, L)$ vælges som basissæt $(1, 0, \dots, 0)$, $(0, 1, \dots, 0)$, $\dots$, $(0, 0, \dots, 1)$. Til hver $(n \times n)$ -matrix $\underline{A}$ hører da den lineære afbildning f af $(L^n, +, L)$ ind i sig selv, der til sættet $\underline{x}_i$ lader svare sættet $\underline{A} \underline{x}_i$. Specielt hører til enhedsmatricen $\underline{E}$ den identiske afbildning e , idet dens søjler netop er basissættene.

Antag, at søjlerne i $\underline{A}$ er lineært uafhængige. Afbildningen f har da rangen n og billedrummet $f(L^n)$ dimensionen n . Men idet $f(L^n) \subseteq L^n$, medfører dette $f(L^n) = L^n$, altså at f er surjektiv. Endvidere følger, at kernens dimension er 0 (jfr. side III, 2, 12), og dermed, at f er injektiv. Der eksisterer altså en invers afbildning $f^{-1}: L^n \rightarrow L^n$. Denne er lineær og følgelig bestemt ved en $(n \times n)$ -matrix $\underline{X}$. Idet $f \circ f^{-1} = f^{-1} \circ f = e$, gælder for denne $\underline{A} \underline{X} = \underline{X} \underline{A} = \underline{E}$, hvilket viser, at $\underline{A}$ er regulær.

Antag, at der findes en $(n \times n)$ -matrix $\underline{X}$, for hvilken $\underline{A} \underline{X} = \underline{E}$. Betegner f og g de ved $\underline{A}$ og $\underline{X}$ bestemte afbildninger, er $f \circ g = e$. Da $f \circ g$ er surjektiv, må også f være surjektiv; f har altså rangen n , hvorfor også søjlerangen for $\underline{A}$ er n .

Antages, at der findes en $(n \times n)$ -matrix $\underline{Y}$, for hvilken $\underline{Y} \underline{A} = \underline{E}$, og betegnes med h og f de ved $\underline{Y}$ og $\underline{A}$ bestemte afbildninger, er $h \circ f = e$. Da $h \circ f$ er injektiv, må også f være injektiv; kernen for f har altså dimensionen 0, hvorfor $\dim f(L^n)$ og dermed søjlerangen for $\underline{A}$ er $n - 0 = n$.

Dermed er sætningen bevist. Vi bemærker:

For $(n \times n)$ -matricer $\underline{A}$ og $\underline{B}$ gælder, at blot $\underline{A} \underline{B} = \underline{E}$, så er $\underline{A}$ og $\underline{B}$ regulære og hinandens inverse,

$$\underline{A} \underline{B} = \underline{E} \Rightarrow \underline{A} \underline{B} = \underline{B} \underline{A} = \underline{E}.$$

Thi af $\underline{A} \underline{B} = \underline{E}$ sluttes, at $\underline{A}$ er regulær. Ifølge den forrige sætning har ligningen $\underline{A} \underline{X} = \underline{E}$ da kun én løsning, hvorfor $\underline{B} = \underline{A}^{-1}$.

Foruden de omtalte måder at danne nye matricer ud fra givne er den såkaldte transponering af en matrix af betydning. Den består i, at man skriver rækkerne i en matrix $\underline{\underline{A}}$ i samme orden som søjler og sammenfatter disse til en ny matrix. Denne kaldes den transponerede af $\underline{\underline{A}}$ og betegnes med $\underline{\underline{A}}'$. Er $\underline{\underline{A}}$ en $(m \times n)$ -matrix, vil $\underline{\underline{A}}'$ være en $(n \times m)$ -matrix. Den transponerede til en rækkematrix er en søjlematrix, og omvendt.

Med betegnelserne

$$\underline{\underline{A}} = (a_{ij})_{i=1, \dots, m; j=1, \dots, n}, \quad \underline{\underline{A}}' = (a'_{kl})_{k=1, \dots, n; l=1, \dots, m}$$

har man

$$a'_{kl} = a_{lk}.$$

Det er indlysende, at

$$(\underline{\underline{A}}')' = \underline{\underline{A}},$$

at der for hvert tal $\lambda \in L$ gælder

$$(\lambda \underline{\underline{A}})' = \lambda \underline{\underline{A}}'$$

og at

$$(\underline{\underline{A}} + \underline{\underline{B}})' = \underline{\underline{A}}' + \underline{\underline{B}}',$$

når $\underline{\underline{A}}$ og $\underline{\underline{B}}$ er af samme type.

Er $\underline{\underline{A}} = (a_{ij})$ en $(m \times n)$ -matrix og $\underline{\underline{B}} = (b_{jk})$ en $(n \times p)$ -matrix, altså $\underline{\underline{A}}'$ en $(n \times m)$ -matrix og $\underline{\underline{B}}'$ en $(p \times n)$ -matrix, kan produkterne $\underline{\underline{A}} \underline{\underline{B}}$ og $\underline{\underline{B}}' \underline{\underline{A}}'$ dannes, og der gælder

$$(\underline{\underline{A}} \underline{\underline{B}})' = \underline{\underline{B}}' \underline{\underline{A}}',$$

dvs. den transponerede af et produkt af to matricer er lig med produktet af de transponerede matricer taget i omvendt orden.

Med betegnelserne $\underline{\underline{A}}' = (a'_{ji})$ og $\underline{\underline{B}}' = (b'_{kj})$ fås nemlig for elementet i den k -te række og den i -te søjle af matricen $\underline{\underline{B}}' \underline{\underline{A}}'$

$$\sum_{j=1}^n b'_{kj} a'_{ji} = \sum_{j=1}^n a_{ij} b_{jk},$$

altså elementet i den i -te række og den k -te søjle af matricen $\underline{\underline{A}} \underline{\underline{B}}$.

Idet $\underline{\underline{E}}' = \underline{\underline{E}}$, fås for en regulær kvadratisk matrix $\underline{\underline{A}}$ af ligningerne $\underline{\underline{A}} \underline{\underline{A}}^{-1} = \underline{\underline{E}}$ og $\underline{\underline{A}}^{-1} \underline{\underline{A}} = \underline{\underline{E}}$, at

$$(\underline{\underline{A}}^{-1})' \underline{\underline{A}}' = \underline{\underline{E}}, \quad \underline{\underline{A}}' (\underline{\underline{A}}^{-1})' = \underline{\underline{E}}.$$

Heraf slutes:

Er $\underline{\underline{A}}$ en regulær kvadratisk matrix, vil også dens transponerede $\underline{\underline{A}}'$ være regulær, og der gælder

$$(\underline{\underline{A}}')^{-1} = (\underline{\underline{A}}^{-1})'.$$

Idet søjlerne i $\underline{\underline{A}}'$ er rækkerne i $\underline{\underline{A}}$, har man som modstykke til en tidligere sætning: En kvadratisk matrix er regulær, hvis og kun hvis dens rækker er lineært uafhængige.

En kvadratisk matrix $\underline{\underline{A}} = (a_{ij})_{n,n}$ siges at være symmetrisk, hvis

$$\underline{\underline{A}}' = \underline{\underline{A}},$$

altså hvis $a_{ij} = a_{ji}$ for $i, j = 1, \dots, n$.

Enhver (1×1) -matrix er selvfølgelig symmetrisk.

En kvadratisk matrix $\underline{\underline{A}} = (a_{ij})_{n,n}$ siges at være skævsymmetrisk eller antisymmetrisk, hvis

$$\underline{\underline{A}}' = -\underline{\underline{A}},$$

altså hvis $a_{ij} = -a_{ji}$ for $i, j = 1, \dots, n$. I en skævsymmetrisk matrix er $a_{ii} = 0$ for $i = 1, \dots, n$.

Man har undertiden anledning til at benytte matricer, hvis elementer ikke er tal, men visse andre størrelser, for hvilke passende kompositioner er definerede.

Bestemmelsen af et produkt $\underline{\underline{A}} \underline{\underline{B}}$ af en $(m \times n)$ -matrix $\underline{\underline{A}}$ og en $(n \times p)$ -matrix $\underline{\underline{B}}$ kan ofte gøres mere overskuelig ved at opdele disse matricer i delmatricer, såkaldte blokke. Er $m_1, \dots, m_M$, $n_1, \dots, n_N$, $p_1, \dots, p_P$ naturlige tal, for hvilke

$m_1 + \dots + m_M = m$, $n_1 + \dots + n_N = n$, $p_1 + \dots + p_P = p$, kan man skrive A og B som "blokmatricer":

$$\underline{\underline{A}} = \begin{matrix} & \begin{matrix} n_1 & n_2 & & n_N \end{matrix} \\ \begin{pmatrix} \underline{\underline{A}}_{11} & \underline{\underline{A}}_{12} & \cdots & \underline{\underline{A}}_{1N} \\ \underline{\underline{A}}_{21} & \underline{\underline{A}}_{22} & \cdots & \underline{\underline{A}}_{2N} \\ \vdots & \vdots & & \vdots \\ \underline{\underline{A}}_{M1} & \underline{\underline{A}}_{M2} & \cdots & \underline{\underline{A}}_{MN} \end{pmatrix} & \begin{matrix} m_1 \\ m_2 \\ \\ m_M \end{matrix} \end{matrix}$$

$$\underline{\underline{B}} = \begin{matrix} & \begin{matrix} p_1 & p_2 & & p_P \end{matrix} \\ \begin{pmatrix} \underline{\underline{B}}_{11} & \underline{\underline{B}}_{12} & \cdots & \underline{\underline{B}}_{1P} \\ \underline{\underline{B}}_{21} & \underline{\underline{B}}_{22} & \cdots & \underline{\underline{B}}_{2P} \\ \vdots & \vdots & & \vdots \\ \underline{\underline{B}}_{N1} & \underline{\underline{B}}_{N2} & \cdots & \underline{\underline{B}}_{NP} \end{pmatrix} & \begin{matrix} n_1 \\ n_2 \\ \\ n_N \end{matrix} \end{matrix}$$

hvor blokkenes række- og søjletal er angivet henholdsvis til højre og foroven. Blokken $\underline{\underline{A}}_{\alpha\beta}$ er $(m_\alpha \times n_\beta)$ -matricen bestående af de elementer af $\underline{\underline{A}}$, som står i rækkerne med numre fra $m_1 + \dots + m_{\alpha-1} + 1$ til $m_1 + \dots + m_\alpha$ og i søjlerne med numre fra $n_1 + \dots + n_{\beta-1} + 1$ til $n_1 + \dots + n_\beta$, og blokken $\underline{\underline{B}}_{\beta\gamma}$ er $(n_\beta \times p_\gamma)$ -matricen bestående af de elementer af $\underline{\underline{B}}$, som står i rækkerne med numre fra $n_1 + \dots + n_{\beta-1} + 1$ til $n_1 + \dots + n_\beta$ og søjlerne med numre fra $p_1 + \dots + p_{\gamma-1} + 1$ til $p_1 + \dots + p_\gamma$. Produktmatricen $\underline{\underline{A}} \underline{\underline{B}}$ kan da skrives som en blokmatrix

$$\underline{\underline{A}} \underline{\underline{B}} = \begin{matrix} & \begin{matrix} p_1 & p_2 & & & p_p \end{matrix} \\ \begin{matrix} m_1 \\ m_2 \\ \vdots \\ m_M \end{matrix} & \begin{pmatrix} \underline{\underline{C}}_{11} & \underline{\underline{C}}_{12} & \cdot & \cdot & \cdot & \underline{\underline{C}}_{1p} \\ \underline{\underline{C}}_{21} & \underline{\underline{C}}_{22} & \cdot & \cdot & \cdot & \underline{\underline{C}}_{2p} \\ \vdots & \vdots & & & & \vdots \\ \underline{\underline{C}}_{M1} & \underline{\underline{C}}_{M2} & \cdot & \cdot & \cdot & \underline{\underline{C}}_{Mp} \end{pmatrix} \end{matrix}$$

og her er

$$\underline{\underline{C}}_{\alpha\gamma} = \sum_{\beta=1}^N \underline{\underline{A}}_{\alpha\beta} \underline{\underline{B}}_{\beta\gamma}.$$

Produktet fås altså i form af en blokmatrix ved at multiplicere de to blokmatricer, som om deres blokke var tal. Rækkefølgen af faktorerne i de enkelte produkter er her væsentlig.

Rigtigheden heraf kan indses på følgende måde: Med de sædvanlige betegnelser $\underline{\underline{A}} = (a_{ij})$, $\underline{\underline{B}} = (b_{jk})$ er

$$\sum_{j=1}^n a_{ij} b_{jk}$$

det element af $\underline{\underline{A}} \underline{\underline{B}}$, som står i den i -te række og den k -te søjle. Ved den angivne blokinddeling af $\underline{\underline{A}} \underline{\underline{B}}$ vil c_{ik} tilhøre én af blokkene, $\underline{\underline{C}}_{\alpha\beta}$. Elementerne a_{ij} , $j = 1, \dots, n_1$, udgør da en række i blokken $\underline{\underline{A}}_{\alpha 1}$, elementerne a_{ij} , $j = n_1 + 1, \dots, n_1 + n_2$, udgør den tilsvarende række i $\underline{\underline{A}}_{\alpha 2}$, de n_3 følgende elementer den tilsvarende række i $\underline{\underline{A}}_{\alpha 3}$, osv. De n_1 første af elementerne b_{jk} , $j = 1, \dots, n$, udgør en søjle i $\underline{\underline{B}}_{1\beta}$, de næste n_2 den tilsvarende søjle i $\underline{\underline{B}}_{2\beta}$, osv. Ovenstående sum spaltes nu i N summer, den første bestående af de n_1 første led, den anden af de n_2 næste led, den tredje af de n_3 derpå følgende led, osv. Den første af disse summer er da et element i produktet $\underline{\underline{A}}_{\alpha 1} \underline{\underline{B}}_{1\beta}$, den anden sum det tilsvarende element i $\underline{\underline{A}}_{\alpha 2} \underline{\underline{B}}_{2\beta}$, den tredje det tilsvarende element i $\underline{\underline{A}}_{\alpha 3} \underline{\underline{B}}_{3\beta}$, osv. Dette viser, at

$$C_{\alpha\beta} = A_{\alpha 1} B_{1\beta} + A_{\alpha 2} B_{2\beta} + \dots + A_{\alpha N} B_{N\beta}, \text{ som påstået.}$$

Man har også anledning til at betragte vektormatricer, dvs. matricer, hvis elementer er vektorer tilhørende et vektorrum $(V, +, L)$.

Det er klart, hvad man vil forstå ved produktet af en sådan matrix med et tal fra L , og endvidere, hvad man vil forstå ved summen af to vektormatricer af samme type. Af de i vektorrum gyldige regneregler sluttes, at for givne $m, n \in \mathbb{N}$ danner $(m \times n)$ -matricerne, hvis elementer er vektorer fra $(V, +, L)$, et vektorrum over L .

Definitionen på produktet af en $(m \times n)$ -matrix $\underline{A}$ og en $(n \times p)$ -matrix $\underline{B}$ kan uden videre overføres til det tilfælde, hvor én af faktorerne er en vektormatrix. Produktet bliver da en vektormatrix, og denne kan igen multipliceres fra venstre eller højre med en talmatrix af passende type. Man kan sige, at et produkt af flere tal- og vektormatricer kan dannes, når de nødvendige betingelser vedrørende række- og søjleantal er opfyldt og højst én af matricerne er en vektormatrix. Den associative lov er også gyldig her, idet den regning, ved hvilken den blev bevist for talmatricer (side III, 2, 22), med benyttelse af regnereglerne for vektorrum kan gennemføres på samme måde, når elementerne i én af de tre matricer er vektorer.

Begrebet "transponeret matrix" bruges også ved vektormatricer, og der gælder $(\underline{AB})' = \underline{B}' \underline{A}'$, også når én af matricerne $\underline{A}$ og $\underline{B}$ er en vektormatrix.

Begreberne "regulær matrix" og "invers matrix" defineres ikke for vektormatricer.

Er $\underline{v}_1, \dots, \underline{v}_p$ vektorer fra $(V, +, L)$, kan deres linearkombination med koefficienter $\lambda_1, \dots, \lambda_p$ fra L på to måder skrives som matrixprodukt, nemlig

$$\lambda_1 \underline{v}_1 + \dots + \lambda_p \underline{v}_p = (\lambda_1 \dots \lambda_p) \begin{pmatrix} \underline{v}_1 \\ \vdots \\ \underline{v}_p \end{pmatrix}.$$

og transponeret

$$\lambda_1 \underline{v}_1 + \dots + \lambda_p \underline{v}_p = (\underline{v}_1 \dots \underline{v}_p) \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_p \end{pmatrix}.$$

Her skal venstre side i begge ligninger opfattes som (1×1) -vektormatrix.

Er vektorerne $\underline{v}_1, \dots, \underline{v}_p$ lineært uafhængige, kan man af ligningen

$$(\lambda_1 \dots \lambda_p) \begin{pmatrix} \underline{v}_1 \\ \vdots \\ \underline{v}_p \end{pmatrix} = (\mu_1 \dots \mu_p) \begin{pmatrix} \underline{v}_1 \\ \vdots \\ \underline{v}_p \end{pmatrix}$$

eller den dermed ensbetydende

$$(\underline{v}_1 \dots \underline{v}_p) \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_p \end{pmatrix} = (\underline{v}_1 \dots \underline{v}_p) \begin{pmatrix} \mu_1 \\ \vdots \\ \mu_p \end{pmatrix}$$

slutte, at

$$(\lambda_1 \dots \lambda_p) = (\mu_1 \dots \mu_p).$$

Dette er bare en anden måde at udtrykke på, at koefficienterne i en vektors fremstilling som linearkombination af lineært uafhængige vektorer er entydigt bestemte.

Lineære afbildningers matrixligninger. Koordinattransformation.

Vi betragter igen en lineær afbildning f af et n -dimensionalt vektorrum $(U, +, L)$ ind i et m -dimensionalt vektorrum $(V, +, L)$. Er $(\underline{e}_1, \dots, \underline{e}_n)$ en basis for U og $(\underline{f}_1, \dots, \underline{f}_m)$ en basis for V , findes der som omtalt tidligere (side III, 2, 15) en $(m \times n)$ -matrix $\underline{A} = (a_{ij})$ med elementer fra L , således at

$$f(\underline{e}_j) = \sum_{i=1}^m a_{ij} \underline{f}_i, \quad j = 1, \dots, n.$$

Disse ligninger, som kan sammenfattes til matrixligningen

$$(f(\underline{e}_1) \dots f(\underline{e}_n)) = (\underline{f}_1 \dots \underline{f}_m) \underline{A},$$

udsiger, at søjlerne i $\underline{A}$ er koordinatsættene med hensyn til $(\underline{f}_1, \dots, \underline{f}_m)$ af billedvektorerne $f(\underline{e}_1), \dots, f(\underline{e}_n)$.

Betegner $\underline{u}_|$ det som søjle skrevne koordinatsæt for en vektor $\underline{u} \in U$ med hensyn til $(\underline{e}_1, \dots, \underline{e}_n)$ og $\underline{v}_|$ det som søjle skrevne koordinatsæt for billedvektoren

$$\underline{v} = f(\underline{u}) = u_1 f(\underline{e}_1) + \dots + u_n f(\underline{e}_n),$$

gælder matrixligningerne

$$\begin{aligned} \underline{u} &= (\underline{e}_1 \dots \underline{e}_n) \underline{u}_|, \\ \underline{v} &= (\underline{f}_1 \dots \underline{f}_m) \underline{v}_| \\ &= (f(\underline{e}_1) \dots f(\underline{e}_n)) \underline{u}_|, \end{aligned}$$

hvor de venstre sider skal opfattes som (1×1) -matricer.

Af den sidste ligning fås ved indsættelse

$$(\underline{f}_1 \dots \underline{f}_m) \underline{v}_| = (\underline{f}_1 \dots \underline{f}_m) \underline{A} \underline{u}_|.$$

Idet $\underline{f}_1, \dots, \underline{f}_m$ er lineært uafhængige, kan man heraf slutte

$$\underline{v}_| = \underline{A} \underline{u}_|.$$

Denne ligning er ikke andet end en sammenfatning af de tidligere (side III, 2, 15) fundne ligninger

$$v_i = \sum_{j=1}^n a_{ij} u_j, \quad i = 1, \dots, m.$$

Den udsiger, at man ved multiplikation af matricen $\underline{A}$ med en vilkårlig søjle $\underline{u}_j$ får koordinatsøjlen $\underline{v}_j$ for billedvektoren af vektoren $\underline{u}$ med koordinatsøjlen $\underline{u}_j$. Vi bemærker, at $\underline{A}$ er den eneste matrix med denne egenskab. Er nemlig $\tilde{\underline{A}}$ en $(m \times n)$ -matrix, og betegnes med $\delta_{=j}$ den j -te søjle i enhedsmatricen $\underline{E}_{n,n}$, altså koordinatsøjlen for $\underline{e}_j$ med hensyn til $(\underline{e}_1, \dots, \underline{e}_n)$, bliver $\tilde{\underline{A}} \delta_{=j}$ den j -te søjle i $\tilde{\underline{A}}$; er derfor $\tilde{\underline{A}} \delta_{=j}$ koordinatsøjlen for $f(\underline{e}_j)$ med hensyn til $(\underline{f}_1, \dots, \underline{f}_m)$, sluttet, at den j -te søjle af $\tilde{\underline{A}}$ stemmer overens med den j -te søjle af $\underline{A}$.

Ligningen

$$\underline{v}_j = \underline{A} \underline{u}_j$$

kaldes den lineære afbildnings matrixligning med hensyn til baserne $(\underline{e}_1, \dots, \underline{e}_n)$ og $(\underline{f}_1, \dots, \underline{f}_m)$.

Er $(W, +, L)$ et tredie vektorrum med den endelige dimension l , $(\underline{g}_1, \dots, \underline{g}_l)$ en basis for det og $g: V \rightarrow W$ en lineær afbildning, vil dennes matrixligning med hensyn til $(\underline{f}_1, \dots, \underline{f}_m)$ og $(\underline{g}_1, \dots, \underline{g}_l)$ have formen

$$\underline{w}_j = \underline{B} \underline{v}_j,$$

hvor $\underline{B}$ er en $(l \times m)$ -matrix med elementer fra L . Sættes heri $\underline{v}_j = \underline{A} \underline{u}_j$, fås matrixligningen

$$\underline{w}_j = \underline{B} \underline{A} \underline{u}_j$$

for den sammensatte afbildning $g \circ f: U \rightarrow W$ med hensyn til baserne $(\underline{e}_1, \dots, \underline{e}_n)$ og $(\underline{g}_1, \dots, \underline{g}_l)$.

Den lineære afbildning $f: U \rightarrow V$ med matrixligningen $\underline{v}_j = \underline{A} \underline{u}_j$ er bijektiv, hvis og kun hvis U og V har samme dimension $n = m$ og $\underline{A}$ er regulær. Er dette tilfældet, fås

$$\underline{u}_j = \underline{A}^{-1} \underline{v}_j$$

som matrixligning for den inverse afbildning $f^{-1}: V \rightarrow U$ med hensyn til baserne $(\underline{f}_1, \dots, \underline{f}_m)$ og $(\underline{e}_1, \dots, \underline{e}_n)$.

Ved opstillingen af en matrixligning for en lineær afbildning af et vektorrum U ind i sig selv vil man i reglen henhøre billedvektorerne til den samme basis som originalvektorerne. Man kan imidlertid også i dette tilfælde bruge to forskellige baser. Vi skal benytte os af denne mulighed til at besvare det vigtige spørgsmål, hvilken sammenhæng der består mellem koordinatsættene for en og samme vektor med hensyn til to forskellige baser.

Lad der i det n -dimensionale vektorrum $(U, +, L)$ være valgt to baser, den "oprindelige" $(\underline{e}_1, \dots, \underline{e}_n)$ og den "nye" $(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n)$, og lad $\underline{u}_|$ og $\hat{\underline{u}}_|$ betegne koordinatsøjlerne for en vektor $\underline{u} \in U$ med hensyn til disse to baser. Den søgte relation mellem $\underline{u}_|$ og $\hat{\underline{u}}_|$ er da matrixligningen for den identiske afbildning e_U af U med hensyn til baserne $(\underline{e}_1, \dots, \underline{e}_n)$ og $(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n)$, idet vektoren $\underline{u}$ henføres til den oprindelige eller den nye basis, efter som den betragtes som originalvektor eller billedvektor $e_U(\underline{u}) = \underline{u}$. Der gælder altså

$$\hat{\underline{u}}_| = \underline{\underline{S}} \underline{u}_| ,$$

hvor $\underline{\underline{S}}$ er en $(n \times n)$ -matrix, som er regulær, idet e_U er bijektiv. Søjlerne i $\underline{\underline{S}}$ er koordinatsættene for billedvektorerne af $\underline{e}_1, \dots, \underline{e}_n$, altså af selve disse vektorer, med hensyn til basen $(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n)$,

$$(\underline{e}_1 \dots \underline{e}_n) = (\hat{\underline{e}}_1 \dots \hat{\underline{e}}_n) \underline{\underline{S}}.$$

Overgangen fra koordinaterne med hensyn til basen $(\underline{e}_1, \dots, \underline{e}_n)$ til koordinaterne med hensyn til basen $(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n)$ kaldes en koordinattransformation og den tilhørende matrix $\underline{\underline{S}}$ koordinattransformationsmatricen. Hver regulær $(n \times n)$ -matrix kan forekomme som en sådan; thi vælges basen $(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n)$ og en regulær $(n \times n)$ -matrix $\underline{\underline{S}}$ vilkårligt, vil der ved den sidst opskrevne matrixligning bestemmes en basis $(\underline{e}_1, \dots, \underline{e}_n)$, således at $\underline{\underline{S}}$ er koordinattransformationsmatricen for overgangen fra denne basis til $(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n)$.

Koordinattransformationsmatricen $\underline{\underline{S}}$ kendes, når de oprindelige basisvektorer er givet som linearkombinationer af de nye. Ofte vil

det omvendte være tilfældet. Idet

$$(\hat{e}_1 \dots \hat{e}_n) = (e_1 \dots e_n) \underline{\underline{S}}^{-1},$$

vil dette sige, at man kender matricen $\underline{\underline{S}}^{-1}$, og $\underline{\underline{S}}$ må da bestemmes som dennes inverse.

Vi betragter igen en lineær afbildning f af et n -dimensionalt vektorrum $(U, +, L)$ ind i et m -dimensionalt $(V, +, L)$. Lad

$$\underline{\underline{v}} = \underline{\underline{A}} \underline{\underline{u}}$$

være afbildningens matrixligning med hensyn til basen $(e_1, \dots, e_n)$ for U og basen $(f_1, \dots, f_m)$ for V . Vælges der nye baser $(\hat{e}_1, \dots, \hat{e}_n)$ og $(\hat{f}_1, \dots, \hat{f}_m)$, vil afbildningen f i almindelighed få en anden matrixligning. Denne kan bestemmes på følgende måde: Mellem koordinatsættene $\underline{\underline{u}}$ og $\hat{\underline{\underline{u}}}$ for en vektor $u \in U$ med hensyn til den oprindelige og den nye basis for U består relationen

$$\hat{\underline{\underline{u}}} = \underline{\underline{S}} \underline{\underline{u}},$$

hvor $\underline{\underline{S}}$ er koordinattransformationsmatricen. Tilsvarende har man for koordinatsættene for en vektor $v \in V$

$$\hat{\underline{\underline{v}}} = \underline{\underline{T}} \underline{\underline{v}},$$

hvor $\underline{\underline{T}}$ er den til koordinattransformationen i V hørende koordinattransformationsmatrix. Af de tre opskrevne ligninger fås ved elimination af $\underline{\underline{u}}$ og $\underline{\underline{v}}$

$$\hat{\underline{\underline{v}}} = \underline{\underline{T}} \underline{\underline{A}} \underline{\underline{S}}^{-1} \hat{\underline{\underline{u}}},$$

og dette er afbildningens matrixligning med hensyn til de nye baser.

Mellem matricerne $\underline{\underline{A}}$ og $\hat{\underline{\underline{A}}}$, som hører til afbildningen, efter som de oprindelige eller de nye baser benyttes, består altså relationen

$$\hat{\underline{\underline{A}}} = \underline{\underline{T}} \underline{\underline{A}} \underline{\underline{S}}^{-1}.$$

(Dette kan også slttes af, at f kan skrives $e_V \circ f \circ e_U^{-1}$, hvor e_U og

e_U betegner de identiske afbildninger af U og V . Henføres nemlig e_U til baserne $(\underline{e}_1, \dots, \underline{e}_n)$ og $(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n)$, f til baserne $(\underline{e}_1, \dots, \underline{e}_n)$ og $(\underline{f}_1, \dots, \underline{f}_m)$ og e_V til baserne $(\underline{f}_1, \dots, \underline{f}_m)$ og $(\hat{\underline{f}}_1, \dots, \hat{\underline{f}}_m)$, fås for den sammensatte afbildning $e_V \cdot f \cdot e_U^{-1} = f$ henført til baserne $(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n)$ og $(\hat{\underline{f}}_1, \dots, \hat{\underline{f}}_m)$ matricen $\underline{\underline{A}} \underline{\underline{S}}^{-1}$.

Matricerne $\underline{\underline{A}}$ og $\hat{\underline{\underline{A}}}$ har samme søjlerang, idet denne for begge er lig med afbildningens rang, dvs. billeddrummets dimension.

Ved passende valg af de nye baser kan opnås, at $\hat{\underline{\underline{A}}}$ antager en særlig simpel "normalform". Lad r betegne afbildningens rang. Man vælger en basis $(\hat{\underline{e}}_{r+1}, \dots, \hat{\underline{e}}_n)$ for afbildningens kerne K og supplerer den (hvis $r > 0$) til en basis $(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n)$ for U . Vektorsættet $(f(\hat{\underline{e}}_1), \dots, f(\hat{\underline{e}}_n))$ har rangen r . Da

$$f(\hat{\underline{e}}_{r+1}) = \dots = f(\hat{\underline{e}}_n) = \underline{0},$$

må $f(\underline{e}_1), \dots, f(\underline{e}_r)$ være lineært uafhængige. Vælges disse vektorer (i denne orden) som de r første vektorer i en basis $(\underline{f}_1, \dots, \underline{f}_m)$ for V , fås

$$\hat{\underline{\underline{A}}} = \begin{pmatrix} \underline{\underline{E}}_{r,r} & \underline{\underline{O}}_{r,n-r} \\ \underline{\underline{O}}_{m-r,r} & \underline{\underline{O}}_{m-r,n-r} \end{pmatrix},$$

idet søjlerne i $\hat{\underline{\underline{A}}}$ jo er koordinatsættene for vektorerne

$$f(\hat{\underline{e}}_1) = \hat{\underline{f}}_1, \dots, f(\hat{\underline{e}}_r) = \hat{\underline{f}}_r, f(\hat{\underline{e}}_{r+1}) = \underline{0}, \dots, f(\hat{\underline{e}}_n) = \underline{0}.$$

Denne matrix betegnes i det følgende med $\underline{\underline{E}}_{m,n}^{(r)}$. (Er $r = 0$, $r = m$ eller $r = n$, falder naturligvis nogle af blokkene bort.)

Rangen af en matrix.

Af disse resultater kan udledes vigtige sætninger om søjlerangen af matricer med elementer fra et tallegeme L .

Er $\underline{A}$ en $(m \times n)$ -matrix, $\underline{P}$ en regulær $(m \times m)$ -matrix og $\underline{Q}$ en regulær $(n \times n)$ -matrix, da har matrixerne $\underline{A}$ og $\underline{P} \underline{A} \underline{Q}$ samme søjlerang.

Bevis: Man fortolker $\underline{A}$ som matrix hørende til en lineær afbildning af et n -dimensionalt vektorrum $(U, +, L)$ ind i et m -dimensionalt vektorrum $(V, +, L)$ med hensyn til valgte baser i disse rum. Anvendes koordinattransformationer i U og V med henholdsvis $\underline{S} = \underline{Q}^{-1}$ og $\underline{T} = \underline{P}$ som koordinattransformationsmatrixer, fås $\underline{P} \underline{A} \underline{Q}$ som matrix hørende til den samme afbildning.

Idet man ved rækkerangen af en matrix forstår maximaltallet af lineært uafhængige blandt dens rækker, gælder:

For hver matrix $\underline{A} \in M_{m,n}(L)$ stemmer søjlerang og rækkerang overens. Den fælles værdi kaldes matrixens rang og betegnes med $\text{rg } \underline{A}$.

Bevis: Lad $\underline{P}$ og $\underline{Q}$ være regulære matrixer, for hvilke

$$\underline{P} \underline{A} \underline{Q} = \underline{E}_{m,n}^{(r)}.$$

Eksistensen indses, idet $\underline{A}$ fortolkes som matrix hørende til en lineær afbildning f ; overgangen til $\underline{E}_{m,n}^{(r)}$ sker da ved, at f henføres til nye baser (jfr. side 38). Ved transponering fås

$$\underline{Q}' \underline{A}' \underline{P}' = \underline{E}_{m,n}^{(r)'} = \underline{E}_{n,m}^{(r)}.$$

Idet $\underline{P}'$ og $\underline{Q}'$ er regulære, har $\underline{A}'$ samme søjlerang som $\underline{E}_{n,m}^{(r)}$, ligesom $\underline{A}$ har samme søjlerang som $\underline{E}_{m,n}^{(r)}$. Men $\underline{E}_{m,n}^{(r)}$ og $\underline{E}_{n,m}^{(r)}$ har øjensynlig samme søjlerang, nemlig r . Følgelig har $\underline{A}$ og $\underline{A}'$ samme søjlerang, og da søjlerangen af $\underline{A}'$ er rækkerangen af $\underline{A}$, er påstanden hermed bevist.

En matrix, som fremkommer ved udeladelse af rækker og/eller søjler af en matrix $\underline{A}$, kaldes en delmatrix af $\underline{A}$.

Rangen af en fra nulmatricen forskellig matrix $\underline{A} \in M_{m,n}(L)$

er det største blandt de naturlige tal p , for hvilke der findes en regulær $(p \times p)$ -delmatrix af $\underline{A}$.

Bevis: Først bemærkes at rangen af en matrix ikke kan formindskes, når der tilføjes rækker (eller søjler). De søjler af $\underline{A}$, der indeholder en regulær $(p \times p)$ -delmatrix, er følgelig lineært uafhængige. Dette viser, at $\text{rg } \underline{A} \geq p$, når der findes en sådan delmatrix. På den anden side har $\underline{A}$ en regulær $(r \times r)$ -delmatrix, når $\text{rg } \underline{A} = r$. Der findes nemlig r lineært uafhængige rækker i $\underline{A}$. Disse udgør en delmatrix, hvis rang også er r , og som altså indeholder r lineært uafhængige søjler. Delmatricen bestående af disse søjler er af den forlangte art. Dermed er sætningen bevist.

Lineære afbildninger af normerede vektorrum.

I det følgende står L for de reelle eller de komplekse tals legeme. Lad $(U, +, L, \| \cdot \|_U)$ og $(V, +, L, \| \cdot \|_V)$ være normerede vektorrum. De er da metriske rum med distancerne

$$\text{dist}_U(\underline{u}_1, \underline{u}_2) = \|\underline{u}_2 - \underline{u}_1\|_U, \quad \text{dist}_V(\underline{v}_1, \underline{v}_2) = \|\underline{v}_2 - \underline{v}_1\|_V$$

(jf. side III, 1.30-31). Vi betragter lineære afbildninger f af U ind i V .

Det kan hende, at der findes en normbevarende lineær afbildning $f: U \rightarrow V$, for hvilken altså

$$\forall \underline{u} \in U : \|f(\underline{u})\|_V = \|\underline{u}\|_U.$$

Idet der da for $\underline{u}_1, \underline{u}_2 \in U$ gælder

$$\|f(\underline{u}_2) - f(\underline{u}_1)\|_V = \|f(\underline{u}_2 - \underline{u}_1)\|_V = \|\underline{u}_2 - \underline{u}_1\|_U,$$

er den en isometrisk, altså specielt injektiv, afbildning af U på et underrum af V . Er en sådan afbildning surjektiv, vil dens

inverse være en lineær isometrisk afbildning af V på U . De to normerede vektorrum er da isomorfe.

Homotetien af U med faktoren -1 er en lineær isometrisk afbildning af $(U, +, L, \| \cdot \|_U)$ på sig selv, idet

$$\| -\underline{u} \|_U = \| \underline{u} \|_U .$$

I almindelighed findes der, bortset fra identiteten, ikke andre.

En vigtig klasse af lineære afbildninger af et normeret vektorrum ind i et normeret vektorrum udgøres af de såkaldte begrænsede. En lineær afbildning

$$f: (U, +, L, \| \cdot \|_U) \rightarrow (V, +, L, \| \cdot \|_V)$$

siges at være begrænset, hvis der findes et tal $M \geq 0$ således, at

$$\forall \underline{u} : \| f(\underline{u}) \|_V \leq M \| \underline{u} \|_U .$$

Dette medfører

$$\sup \{ \| f(\underline{u}) \|_V \mid \| \underline{u} \|_U \leq 1 \} \leq M ,$$

altså at funktionen $\| f(\underline{u}) \|_V$ er begrænset, med majorant M , på "enhedskuglen" $\| \underline{u} \|_U \leq 1$. Omvendt, hvis dette er tilfældet, er den lineære afbildning f begrænset; thi for $\underline{u} \neq \underline{0}$ har man da

$$\left\| f \left(\frac{\underline{u}}{\| \underline{u} \|_U} \right) \right\|_V \leq M ,$$

altså (ifølge N2, side III, 1,30)

$$\| f(\underline{u}) \|_V \leq M \| \underline{u} \|_U ,$$

og denne ulighed er også opfyldt for $\underline{u} = \underline{0}$.

Idet rummene U og V som angivet ovenfor er metriske rum, kan man tale om kontinuerte afbildninger f af U ind i V . At f er kon-

tinuert i $\underline{u}_0$ betyder, at der til hvert $\varepsilon > 0$ findes et $\delta > 0$, således at der for $\underline{u} \in U$ gælder

$$\|\underline{u} - \underline{u}_0\|_U \leq \delta \Rightarrow \|f(\underline{u}) - f(\underline{u}_0)\|_V \leq \varepsilon .$$

Idet $f(\underline{u}) - f(\underline{u}_0) = f(\underline{u} - \underline{u}_0)$, er det tilstrækkeligt at kræve dette opfyldt for $\underline{u}_0 = \underline{0}$. Hvis en lineær afbildning $f: U \rightarrow V$ er kontinuert i $\underline{0}$, er den altså kontinuert (endda ligelig) i hele rummet U .

En lineær afbildning af et normeret vektorrum ind i et normeret vektorrum er begrænset, hvis og kun hvis den er kontinuert.

Bevis: Hvis $f: U \rightarrow V$ er kontinuert, findes der til $\varepsilon = 1$ et $\delta > 0$ således, at der for $\underline{u} \in U$ gælder

$$\|\underline{u}\|_U \leq \delta \Rightarrow \|f(\underline{u})\|_V \leq 1 ,$$

altså

$$\|\underline{u}\|_U \leq 1 \Rightarrow \|\delta \underline{u}\|_U \leq \delta \Rightarrow \|f(\delta \underline{u})\|_V \leq 1 \Rightarrow \|f(\underline{u})\|_V \leq \frac{1}{\delta} .$$

Dette viser, at f er begrænset.

Hvis f er begrænset, hvis der altså eksisterer et $M \geq 0$ således, at der for $\underline{u} \in U$ gælder

$$\|f(\underline{u})\|_V \leq M \|\underline{u}\|_U ,$$

har vi for hvert $\varepsilon > 0$

$$\|\underline{u}\|_U \leq \frac{\varepsilon}{M} \Rightarrow \|f(\underline{u})\|_V \leq \varepsilon .$$

Dette viser, at f er kontinuert i $\underline{0}$, altså i hele U .

Alle lineære afbildninger af et endelig-dimensionalt normeret vektorrum ind i et normeret vektorrum er kontinuerte. Ved beviset herfor får vi brug for følgende sætning. (Den har som

simpel konsekvens, at forskellige normer i et endelig-dimensionalt vektorrum gør dette til ækvivalente metriske rum, altså til rum med samme topologi (jf. MA 8.17.1-2). For uendelig-dimensionale vektorrum gælder ikke noget tilsvarende.)

Lad $(U, +, L, \| \cdot \|_U)$ være et normeret vektorrum af den endelige dimension n og $(\underline{e}_1, \dots, \underline{e}_n)$ en basis for det. Ved for

$$\underline{u} = u_1 \underline{e}_1 + \dots + u_n \underline{e}_n \in U$$

at sætte

$$\|\underline{u}\|_1 = |u_1| + \dots + |u_n|$$

defineres en norm $\| \cdot \|_1$ i U . Der findes da tal $k, K \in \mathbb{R}_+$, således at der for $u \in U$ gælder

$$k\|\underline{u}\|_1 \leq \|\underline{u}\|_U \leq K\|\underline{u}\|_1 .$$

Bevis: Ved gentagen anvendelse af N2 og N3 (side III, 1, 30) fås

$$\|u_1 \underline{e}_1 + \dots + u_n \underline{e}_n\|_U \leq |u_1| \|\underline{e}_1\|_U + \dots + |u_n| \|\underline{e}_n\|_U ,$$

og heraf følger den højre af de påståede uligheder med

$$K = \max \{ \|\underline{e}_1\|_U, \dots, \|\underline{e}_n\|_U \} .$$

For at bevise den venstre ulighed betragter vi den ved

$$(u_1, \dots, u_n) \rightarrow \|u_1 \underline{e}_1 + \dots + u_n \underline{e}_n\|_U$$

bestemte funktion $\varphi: L^n \rightarrow \mathbb{R}$. Den er kontinuert hvis L^n og $\mathbb{R}$ forsynes med de sædvanlige metrikker. For $(a_1, \dots, a_n) \in L^n$ og $(u_1, \dots, u_n) \in L^n$ gælder nemlig ifølge det allerede viste

$$\begin{aligned}
& | \|u_1 e_1 + \dots + u_n e_n\|_U - \|a_1 e_1 + \dots + a_n e_n\|_U | \\
& \leq \| (u_1 e_1 + \dots + u_n e_n) - (a_1 e_1 + \dots + a_n e_n) \|_U \\
& = \| (u_1 - a_1) e_1 + \dots + (u_n - a_n) e_n \|_U \\
& \leq K(|u_1 - a_1| + \dots + |u_n - a_n|) \\
& \leq nK(|u_1 - a_1|^2 + \dots + |u_n - a_n|^2)^{\frac{1}{2}} .
\end{aligned}$$

Idet mængden

$$E = \{(u_1, \dots, u_n) \mid |u_1| + \dots + |u_n| = 1\} \subseteq L^n$$

er begrænset og afsluttet, altså kompakt, har restriktionen af φ til E et minimum k , som må være positivt, idet φ er positiv på E (jf. MA 11.9.1 og 11.12.2). For

$$\underline{u} = u_1 e_1 + \dots + u_n e_n \neq \underline{0}$$

sluttes heraf, idet

$$\frac{1}{|u_1| + \dots + |u_n|} (u_1, \dots, u_n) \in E ,$$

at

$$\left\| \frac{\underline{u}}{\|\underline{u}\|_1} \right\|_U \geq k ,$$

altså

$$k \|\underline{u}\|_1 \leq \|\underline{u}\|_U .$$

Da dette også gælder for $\underline{u} = \underline{0}$, er sætningen hermed bevist.

Enhver lineær afbildning af et endelig-dimensionalt normeret vektorrum ind i et normeret vektorrum er begrænset, altså kontinuert.

Bevis: Med ovenstående betegnelser antages, at $(U, +, L, \| \cdot \|_U)$ har dimensionen n , og at der er valgt en basis $(\underline{e}_1, \dots, \underline{e}_n)$ for U . Lad f være en lineær afbildning af U ind i V . For

$$\underline{u} = u_1 \underline{e}_1 + \dots + u_n \underline{e}_n$$

fås da ved hjælp af den foregående sætning

$$\begin{aligned} \|f(\underline{u})\|_V &= \|f(u_1 \underline{e}_1 + \dots + u_n \underline{e}_n)\|_V \\ &= \|u_1 f(\underline{e}_1) + \dots + u_n f(\underline{e}_n)\|_V \\ &\leq |u_1| \|f(\underline{e}_1)\|_V + \dots + |u_n| \|f(\underline{e}_n)\|_V \\ &\leq K' \|\underline{u}\|_1 \leq \frac{K'}{k} \|\underline{u}\|_U, \end{aligned}$$

hvor

$$K' = \max \{ \|f(\underline{e}_1)\|_V, \dots, \|f(\underline{e}_n)\|_V \}.$$

Heraf aflæses, at f er begrænset.

For lineære afbildninger af uendelig-dimensionale vektorrum gælder sætningen ikke.

Vi beviser endnu en sætning om afbildninger af reelle normerede vektorrum, som undertiden finder anvendelse:

Hvis en afbildning f af et normeret vektorrum $(U, +, \dot{R}, \| \cdot \|_U)$ ind i et normeret vektorrum $(V, +, \dot{R}, \| \cdot \|_V)$ er kontinuert i 0 og en homomorfi af gruppen $(U, +)$ ind i gruppen $(V, +)$, da er den lineær.

Bevis: Det er givet, at der for $\underline{u}_1, \underline{u}_2 \in U$ gælder

$$f(\underline{u}_1 + \underline{u}_2) = f(\underline{u}_1) + f(\underline{u}_2)$$

og at der til hvert $\varepsilon > 0$ findes et $\delta > 0$, således at

$$\|\underline{u}\|_U \leq \delta \Rightarrow \|f(\underline{u})\|_V \leq \varepsilon.$$

Det skal vises, at der for $\underline{u} \in U$ og $\lambda \in \mathbb{R}$ gælder

$$f(\lambda \underline{u}) = \lambda f(\underline{u}) .$$

Idet $p\underline{u}$ for $p \in \mathbb{Z}$ er den "p-te potens" af $\underline{u}$ i gruppen $(U, +)$ og f er en homomorfi af denne har vi

$$f(p\underline{u}) = pf(\underline{u}) , \quad p \in \mathbb{Z} .$$

For $q \in \mathbb{N}$ gælder derfor

$$qf\left(\frac{p}{q}\underline{u}\right) = pqf\left(\frac{1}{q}\underline{u}\right) = pf(\underline{u}) ,$$

altså

$$f\left(\frac{p}{q}\underline{u}\right) = \frac{p}{q}f(\underline{u}) .$$

Påstanden er altså rigtig for rationale λ . Lad nu $\underline{u} \in U$ og $\lambda \in \mathbb{R}$ være vilkårligt givne. For hvert rationalt tal ρ gælder da

$$\begin{aligned} \|f(\lambda \underline{u}) - \lambda f(\underline{u})\|_V &= \|f(\lambda \underline{u}) - f(\rho \underline{u}) + \rho f(\underline{u}) - \lambda f(\underline{u})\|_V \\ &= \|f((\lambda - \rho)\underline{u}) + (\rho - \lambda)f(\underline{u})\|_V \\ &\leq \|f((\lambda - \rho)\underline{u})\|_V + |\lambda - \rho| \|f(\underline{u})\|_V . \end{aligned}$$

Til hvert $\varepsilon > 0$ findes nu et $\rho \in \mathbb{Q}$ så nær ved λ , at

$$\|(\lambda - \rho)\underline{u}\|_U = |\lambda - \rho| \|\underline{u}\|_U \leq \delta$$

og

$$|\lambda - \rho| \|f(\underline{u})\|_V \leq \varepsilon .$$

Man får da

$$0 \leq \|f(\lambda \underline{u}) - \lambda f(\underline{u})\|_V < 2\varepsilon .$$

Idet dette (med faste $\underline{u}$ og λ) gælder for hvert $\varepsilon > 0$, må vi have

$$\|f(\lambda \underline{u}) - \lambda f(\underline{u})\|_V = 0 ,$$

altså (N1, side III, 1, 30)

$$f(\lambda \underline{u}) = \lambda f(\underline{u}) ,$$

som påstået.

Som specielt tilfælde ($n = 1$, $U = V = \mathbb{R}$ med normen $|\cdot|$) fremhæves:

De eneste funktioner $f: \mathbb{R} \rightarrow \mathbb{R}$, som er kontinuerte i 0 og opfylder "Cauchys funktionalligning"

$$\forall_{\mathbb{R}} x, y : f(x + y) = f(x) + f(y) ,$$

er funktionerne $f(x) = cx$, hvor c er en konstant.

Det bemærkes, at tilsvarende ikke gælder for de komplekse tals legeme; funktionen $f(x) = \bar{x}$, $x \in \mathbb{C}$, opfylder sætningens forudsætninger, men er ikke lineær.

Endelig nævnes uden bevis, at der findes funktioner $f: \mathbb{R} \rightarrow \mathbb{R}$, som tilfredsstiller Cauchys funktionalligning, og som ikke er kontinuerte i noget $x \in \mathbb{R}$.

Lineære afbildninger af vektorrum med indre produkt.

Lad $(U, +, L, \cdot)$ og $(V, +, L, *)$, hvor $L = \mathbb{C}$ eller $L = \mathbb{R}$, være to vektorrum med indre produkt. Man kan da betragte lineære afbildninger f af U ind i V , ved hvilke det indre produkt bevares, dvs. for hvilke

$$\forall_{U} \underline{u}_1, \underline{u}_2 : f(\underline{u}_1) * f(\underline{u}_2) = \underline{u}_1 \cdot \underline{u}_2 .$$

For de ved de indre produkter bestemte normer

$$\|\underline{u}\|_U = (\underline{u} \cdot \underline{u})^{\frac{1}{2}} , \quad \|\underline{v}\|_V = (\underline{v} * \underline{v})^{\frac{1}{2}}$$

gælder da

$$\|f(\underline{u})\|_V = \|\underline{u}\|_U .$$

En sådan afbildning er følgelig isometrisk og dermed injektiv. Endvidere vil der til ortogonale vektorer svare ortogonale vektorer, til et ortonormeret system et orthonormeret system. Hvis en sådan afbildning f er surjektiv, er den inverse af samme art. Afbildningen siges da at være unitær i tilfældet $L = \mathbb{C}$ og ortogonal i tilfældet $L = \mathbb{R}$. Hvis en sådan eksisterer, er de to vektorrum med indre produkt isomorfe. Det er klart, at sammensætningerne af to unitære (ortogonale) afbildninger er igen unitær (ortogonal).

Har de to vektorrum U og V samme endelige dimension n , findes der unitære (ortogonale) afbildninger $f: U \rightarrow V$. Vælger man nemlig ortonormerede baser $(\underline{e}_1, \dots, \underline{e}_n)$ og $(\underline{f}_1, \dots, \underline{f}_n)$ for henholdsvis U og V , vil den lineære afbildning $f: U \rightarrow V$ bestemt ved, at $f(\underline{e}_i) = \underline{f}_i$ for $i = 1, \dots, n$, være unitær (ortogonal), da de to indre produkter jo har samme koordinatudtryk med hensyn til de ortonormerede baser (jf. side III, 1, 44-45), og en vektor i U og dens billedvektor har samme koordinatsæt.

Specielt gælder, at to vektorrum med indre produkt, der fås ved i samme endelig-dimensionale vektorrum at indføre to forskellige indre produkter, altid er isomorfe.

I det følgende betragtes lineære afbildninger af et vektorrum med indre produkt $(V, +, L, \cdot)$ ind i sig selv, kort omtalt som lineære afbildninger af $(V, +, L, \cdot)$. Det forudsættes, at V har den endelige dimension n . (Begrebsdannelser, der svarer til de nedenfor omtalte, for afbildninger af uendelig-dimensionale

vektorrum med indre produkt, specielt Hilbert rum, spiller ganske vist en betydningsfuld rolle i den matematiske analyse, men overførelsen til det uendelig-dimensionale tilfælde er ikke helt simpel og kan ikke gennemføres her.)

Med henblik på en anvendelse nedenfor bemærkes, at det indre produkt af to vektorer $\underline{u}$ og $\underline{v}$ i V , som med hensyn til en ortonormeret basis har koordinatsættene $(u_1, \dots, u_n)$ og $(v_1, \dots, v_n)$, kan skrives

$$\underline{u} \cdot \underline{v} = (u_1 \dots u_n) \begin{pmatrix} \bar{v}_1 \\ \vdots \\ \bar{v}_n \end{pmatrix} = \underline{u} \cdot \underline{\bar{v}} \quad ,$$

hvor overstregning som sædvanlig betyder overgang til det konjugeret komplekse tal og bortfalder i tilfældet $L = \mathbb{R}$.

Når der i det følgende tales om den matrix, der med hensyn til en valgt basis for vektorrummet V hører til en lineær afbildning V , menes matricen, der fås ved at henhøre såvel original- som billedvektorerne til denne basis.

Til hver lineær afbildning f af $(V, +, L, \cdot)$ findes der netop én lineær afbildning f^* af $(V, +, L, \cdot)$, for hvilken

$$\forall \underline{u}, \underline{v} : f(\underline{u}) \cdot \underline{v} = \underline{u} \cdot f^*(\underline{v}) \quad .$$

Denne afbildning f^* kaldes den til f adjungerede.

Bevis: Lad $(\underline{e}_1, \dots, \underline{e}_n)$ være en ortonormeret basis for V , og lad $\underline{A}$ være den matrix, der med hensyn til denne basis hører til f . For

$$\underline{u} = u_1 \underline{e}_1 + \dots + u_n \underline{e}_n, \quad \underline{v} = v_1 \underline{e}_1 + \dots + v_n \underline{e}_n$$

gælder da

$$f(\underline{u}) \cdot \underline{v} = \underline{u} \underline{A}' \underline{\bar{v}} ,$$

idet $\underline{A} \underline{u}_j$ er koordinatsøjlen, og følgelig $\underline{u} \underline{A}'$ koordinatrækken for $f(\underline{u})$. En lineær afbildning g af V med tilhørende matrix $\underline{B}$ vil altså tilfredsstille det til f^* stillede krav, hvis og kun hvis der for alle $\underline{u}$ og $\underline{v}$ i V gælder

$$\underline{u} \underline{A}' \underline{\bar{v}} = \underline{u} \underline{B} \underline{\bar{v}} ,$$

altså

$$\underline{u} (\underline{B} - \underline{A}') \underline{\bar{v}} = 0 .$$

Man ser let, at dette er opfyldt for alle rækker $\underline{u}$, hvis og kun hvis

$$(\underline{B} - \underline{A}') \underline{\bar{v}} = \underline{0} ,$$

og dette for alle søjler $\underline{v}_j$, dvs. alle søjler $\underline{\bar{v}}_j$, hvis og kun hvis $\underline{B} = \underline{A}'$, altså

$$\underline{B} = \underline{A}' .$$

Den lineære afbildning f^* der med hensyn til den valgte basis er bestemt ved matricen $\underline{A}'$, og kun denne, opfylder altså de stillede krav.

Af beviset fremgår:

Hvis der til en lineær afbildning f af $(V, +, L, \cdot)$ med hensyn til en ortonormeret basis hører matricen $\underline{A}$, vil der til den adjungerede afbildning f^* høre den "adjungerede" matrix

$$\underline{A}^* = \underline{A}' ,$$

altså i tilfældet $L = \mathbb{R}$ den transponerede $\underline{A}'$.

For hver lineær afbildning af $(V, +, L, \cdot)$ gælder

$$f^{**} = f ;$$

thi for $\underline{u}, \underline{v} \in V$ har man

$$f^*(\underline{u}) \cdot \underline{v} = \overline{\underline{v} \cdot f^*(\underline{u})} = \overline{f(\underline{v}) \cdot \underline{u}} = \underline{u} \cdot f(\underline{v}) .$$

For lineære afbildninger f og g af $(V, +, L, \cdot)$ og $\lambda \in L$ gælder

$$(f + g)^* = f^* + g^*$$

$$(\lambda f)^* = \bar{\lambda} f^*,$$

$$(g \circ f)^* = f^* \circ g^*$$

og, hvis f er bijektiv,

$$(f^{-1})^* = (f^*)^{-1} .$$

Disse regler kan sluttet af, at de tilsvarende relationer øjensynlig er gyldige for de matricer, der med hensyn til en ortonormeret basis til afbildningerne. Men de følger også let direkte af definitionen på adjungeret afbildning. For $\underline{u}, \underline{v} \in V$ har man nemlig

$$\begin{aligned} (f + g)(\underline{u}) \cdot \underline{v} &= f(\underline{u}) \cdot \underline{v} + g(\underline{u}) \cdot \underline{v} \\ &= \underline{u} \cdot f^*(\underline{v}) + \underline{u} \cdot g^*(\underline{v}) = \underline{u} \cdot (f^* + g^*)(\underline{v}) , \\ \lambda f(\underline{u}) \cdot \underline{v} &= \lambda \underline{u} \cdot f^*(\underline{v}) = \underline{u} \cdot \bar{\lambda} f^*(\underline{v}) , \\ g(f(\underline{u})) \cdot \underline{v} &= f(\underline{u}) \cdot g^*(\underline{v}) = \underline{u} \cdot f^*(g^*(\underline{v})) \end{aligned}$$

og, hvis f er bijektiv

$$f^{-1}(\underline{u}) \cdot \underline{v} = f^{-1}(\underline{u}) \cdot f^*((f^*)^{-1}(\underline{v})) = \underline{u} \cdot (f^*)^{-1}(\underline{v}) .$$

Et underrum U af et vektorrum $(V, +, L)$ siges at være invariant ved en lineær afbildning $f : V \rightarrow V$, hvis det ved f afbildes ind i sig selv, altså hvis

$$f(U) \subseteq U.$$

Underrummene $\{\underline{0}\}$ og V er invariante ved enhver afbildning f . Endvidere er kernen K_f invariant. Almindeligvis findes også andre invariante underrum.

Om den adjungerede til en lineær afbildning af et vektorrum med indre produkt gælder:

Hvis et underrum U af $(V, +, L, \cdot)$ er invariant ved en lineær afbildning $f : V \rightarrow V$, vil dets ortogonale komplement $U^\perp$ være invariant ved den adjungerede afbildning f^* .

Bevis: Idet $f(\underline{u}) \in U$ for $\underline{u} \in U$, gælder for hvert $\underline{v} \in U^\perp$

$$\underline{u} \cdot f^*(\underline{v}) = f(\underline{u}) \cdot \underline{v} = 0.$$

Dette viser, at $f^*(\underline{v})$ er ortogonal til hver vektor $\underline{u} \in U$ og tilhører følgelig $U^\perp$, som påstået.

En lineær afbildning f af $(V, +, L, \cdot)$ siges at være normal, hvis den er ombyttelig med sin adjungerede, hvis altså

$$f^* \circ f = f \circ f^*.$$

Er $\underline{A}$ matricen, der med hensyn til en ortonormeret basis hører til f , er dette ensbetydende med

$$\underline{\bar{A}}' \underline{A} = \underline{A} \underline{\bar{A}}'.$$

Er $\underline{A}$ en diagonalmatrix, vil også $\underline{\bar{A}}$ være en. Da hvilket-somhelst to $(n \times n)$ -diagonalmatricer er ombyttelige, er altså

afbildningen f normal, dersom der findes en ortonormeret basis, med hensyn til hvilken dens matrix er en diagonalmatrix. (Vi skal vise senere, at der i tilfældet $L = \mathbb{C}$ også gælder det omvendte.) Heraf fremgår specielt, at hver homoteti er normal.

Er f en normal afbildning og $\underline{u}, \underline{v} \in V$, har man

$$f(\underline{u}) \cdot f(\underline{v}) = \underline{u} \cdot f^*(f(\underline{v})) = \underline{u} \cdot f(f^*(\underline{v})) = f^*(\underline{u}) \cdot f^*(\underline{v}) .$$

For $\underline{v} = \underline{u}$ slutes heraf, at $f(\underline{u}) = 0 \iff f^*(\underline{u}) = 0$, altså at f og f^* har samme kerne K . Da K er invariant ved f og f^* , er som vist ovenfor også kernens ortogonale komplement $K^\perp$ invariant ved f og f^* . Restriktionerne af f og f^* til $K^\perp$ (som er bijektive, da $K \cap K^\perp = \{0\}$) er adjungerede til hinanden og selvfølgelig ombyttelige. Vi har altså:

Er f en normal afbildning af $(V, +, L, \cdot)$ og K dens kerne, vil dennes ortogonale komplement $K^\perp$ være invariant ved f , og restriktionen af f til $K^\perp$ vil være normal.

I almindelighed er hverken summen eller sammensætningen af to normale afbildninger normal. Men det bekræftes let, at multiplikation af en normal afbildning med en skalar fører til en normal afbildning, og at den inverse til en bijektiv normal afbildning er normal.

Med henblik på en senere anvendelse bemærkes yderligere:

Er f en normal afbildning af $(V, +, L, \cdot)$ og e den identiske afbildning af V , da er $f - \lambda e$ for hvert $\lambda \in L$ normal.

Da $e^* = e$, følger dette af

$$(f^* - \bar{\lambda}e) \circ (f - \lambda e) = f^* \circ f - \bar{\lambda}f - \lambda f^* + \bar{\lambda}\lambda e ,$$

$$(f - \lambda e) \circ (f^* - \bar{\lambda}e) = f \circ f^* - \lambda f^* - \bar{\lambda}f + \lambda\bar{\lambda}e .$$

En lineær afbildning af $(V, +, L, \cdot)$, for hvilken

$$f^* = f,$$

altså

$$\forall \underline{u}, \underline{v} : f(\underline{u}) \cdot \underline{v} = \underline{u} \cdot f(\underline{v}) ,$$

siges at være selvadjungeret. I tilfældet $L = \mathbb{C}$ siges også Hermiteisk symmetrisk eller kort Hermiteisk, i tilfældet $L = \mathbb{R}$ også symmetrisk. (Det bemærkes, at man i teorien for uendelig-dimensionale vektorrum med indre produkt tillægger "Hermiteisk symmetrisk" en noget mere omfattende betydning end "selvadjungeret". I stedet for "Hermiteisk symmetrisk" bruges ofte "symmetrisk" også i det komplekse tilfælde. Dette kan imidlertid give anledning til forvekslinger.)

Det er klart, at hver selvadjungeret afbildning er normal.

For en lineær afbildnings matrix $\underline{\underline{A}}$ med hensyn til en ortonormeret basis gælder

$$\overline{\underline{\underline{A}}}^t = \underline{\underline{A}} ,$$

hvis og kun hvis afbildningen er selvadjungeret. For matricen $\underline{\underline{A}}$ betyder dette, at diagonalelementerne er reelle, og elementer, der står symmetrisk med hensyn til hoveddiagonalen, er konjugeret komplekse. En matrix $\underline{\underline{A}}$, der opfylder denne ligning, kaldes Hermiteisk symmetrisk eller Hermiteisk. I tilfældet $L = \mathbb{R}$ er dette ensbetydende med, at matricen er symmetrisk, dvs. lig med sin transponerede.

Er $\underline{\underline{A}}$ en reel diagonalmatrix, gælder øjensynlig $\overline{\underline{\underline{A}}}^t = \underline{\underline{A}}$. Afbildningen f er altså selvadjungeret, dersom der findes en ortonormeret basis, med hensyn til hvilken dens matrix er en reel

diagonalmatrix. (Vi skal vise senere, at det omvendte også gælder.) Heraf fremgår, at hver homoteti med reel multiplikator er selvadjungeret. Endvidere følger, at ortogonalprojektionen p af V på et underrum U , dvs. paralelprojektion langs $U^\perp$ (jfr. side III,1,43 og 2,11), er selvadjungeret. Vælges nemlig en ortonormeret basis for U og suppleres denne til en ortonormeret basis for V (hvilket er muligt ifølge ortonormaliseringssætningen, side III,1,40), vil den til p hørende matrix være en diagonalmatrix, hvis diagonalelementer er lig 1 eller 0.

Ifølge et tidligere resultat gælder:

Hvis et underrum U af $(V, +, L, \cdot)$ er invariant ved en selvadjungeret afbildning f af V , er også det ortogonale komplement $U^\perp$ invariant ved f .

Summen af to selvadjungerede afbildninger af $(V, +, L, \cdot)$ er selvadjungeret. Det samme gælder om afbildningen der fås ved at multiplicere en selvadjungeret afbildning med en reel skalar (reel, hvad enten $L = \mathbb{R}$ eller $L = \mathbb{C}$). Heraf sluttes, at de symmetriske afbildninger af et vektorrum V over de reelle tals legeme udgør et underrum i vektorrummet $(\text{Hom}(V, V), +, \mathbb{R})$ af alle lineære afbildninger af V .

Sammensætningen $g \circ f$ af to selvadjungerede afbildninger f og g af V er i almindelighed ikke selvadjungeret. Men hvis f og g er ombyttelige, er det tilfældet, idet da

$$(g \circ f)^* = f^* \circ g^* = f \circ g = g \circ f.$$

For hver lineær afbildning f af $(V, +, L, \cdot)$ er $f + f^*$ selvadjungeret.

En lineær afbildning f af $(V, +, L, \cdot)$, for hvilken

$$f^* = -f,$$

altså

$$\forall \underline{u}, \underline{v} : f(\underline{u}) \cdot \underline{v} = -\underline{u} \cdot f(\underline{v}) ,$$

kaldes anti-Hermitesk, i tilfældet $L = \mathbb{R}$ også antisymmetrisk. Nødvendig og tilstrækkelig for, at en afbildning har denne egenskab, er, at dens matrix $\underline{A}$ med hensyn til en ortonormeret basis tilfredsstiller

$$\underline{A}' = -\underline{A} .$$

Matricen kaldes da anti-Hermitesk. I tilfældet $L = \mathbb{R}$ er dette ensbetydende med, at matricen er antisymmetrisk, altså modsat sin transponerede.

De antisymmetriske afbildninger af et vektorrum $(V, +, \mathbb{R})$ udgør et underrum i $(\text{Hom}(V, V), +, \mathbb{R})$.

For hver lineær afbildning f af $(V, +, L, \cdot)$ er $f - f^*$ anti-Hermitesk. Idet

$$f = \frac{1}{2}(f + f^*) + \frac{1}{2}(f - f^*) ,$$

kan hver lineær afbildning fremstilles som sum af en Hermitesk og en anti-Hermitesk. Det ses let, at dette kun kan ske på én måde.

Som eksempel på en antisymmetrisk afbildning nævnes afbildningen f af det sædvanlige geometriske vektorrum bestemt ved

$$f(\underline{u}) = \underline{a} \times \underline{u} ,$$

hvor $\underline{a}$ er en given vektor. For alle $\underline{u}$ og $\underline{v}$ i rummet har man

nemlig

$$f(\underline{u}) \cdot \underline{v} = \underline{a} \times \underline{u} \cdot \underline{v} = [\underline{a} \underline{u} \underline{v}] = -[\underline{u} \underline{a} \underline{v}] = \underline{u} \cdot (-\underline{a} \times \underline{v}) = \underline{u} \cdot (-f(\underline{v})) .$$

Endelig betragtes lineære afbildninger af $(V, +, L, \cdot)$, ved hvilke det indre produkt, og dermed normen, bevares. Som allerede nævnt er en sådan afbildning f injektiv. Billedrummet har altså samme dimension n som V (jf. side III, 2, 5) og må derfor som under- rum af V stemme overens med V . Heraf følger, at f er bijektiv, altså unitær (ortogonal). Idet f således er en transformation af V , taler man også om en unitær (ortogonal) transformation.

Der findes netop én unitær (ortogonal) transformation af V , ved hvilken en valgt ortonormeret basis afbildes på en vilkårligt given ortonormeret basis.

Er f en unitær (ortogonal) afbildning af V , gælder for $\underline{u}, \underline{v} \in V$

$$f(\underline{u}) \cdot \underline{v} = f(\underline{u}) \cdot f(f^{-1}(\underline{v})) = \underline{u} \cdot f^{-1}(\underline{v}) ,$$

hvilket viser, at

$$f^* = f^{-1} .$$

Omvendt, hvis den adjungerede til en bijektiv lineær afbildning f af V stemmer overens med den inverse, har man for $\underline{u}, \underline{v} \in V$

$$f(\underline{u}) \cdot f(\underline{v}) = \underline{u} \cdot f^*(f(\underline{v})) = \underline{u} \cdot \underline{v} ,$$

altså at f er unitær (ortogonal).

Idet f og f^{-1} er ombyttelige, er de unitære (ortogonale) afbildninger af V normale.

For en lineær afbildnings matrix $\underline{A}$ med hensyn til en orto-

normeret basis for V gælder

$$\bar{\underline{A}}' \underline{A} = \underline{E} ,$$

hvis og kun hvis afbildningen er unitær (ortogonal). Matricen $\underline{A}$ er da regulær. Ligningen er ensbetydende med, at søjlerne i $\underline{A}$ danner et ortonormeret system i talrummet L^n med det indre produkt

$$(u_1, \dots, u_n) \cdot (v_1, \dots, v_n) = u_1 \bar{v}_1 + \dots + u_n \bar{v}_n .$$

Idet matrixligningen medfører

$$\underline{A} \bar{\underline{A}}' = \underline{E} ,$$

danner også rækkerne i $\underline{A}$ et ortonormeret system. En sådan matrix kaldes i det komplekse tilfælde for unitær og i det reelle, hvor ligningen udsiger, at den transponerede $\underline{A}'$ er lig med den inverse $\underline{A}^{-1}$, for ortogonal. Idet $\bar{\underline{A}}'' = \underline{A}$, følger af den sidste matrixligning, at den inverse til en unitær (ortogonal) matrix også er unitær (ortogonal).

Koordinattransformationsmatricen hørende til overgangen fra en ortonormeret basis $(\underline{e}_1, \dots, \underline{e}_n)$ for V til en ortonormeret basis $(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n)$ for V er unitær (ortogonal). Dette følger af, at matrixens søjler som koordinatsæt for vektorerne i et ortonormeret system $(\underline{e}_1, \dots, \underline{e}_n)$ med hensyn til en ortonormeret basis $(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n)$ må danne et ortonormeret sæt i L^n (jf. side III, 1, 44-45 og III, 2, 36). Omvendt gælder, at hvis koordinattransformationsmatricen er unitær (ortogonal) og en af baserne er ortonormeret, er den anden det også.

Hvis en lineær afbildnings matrix med hensyn til en orto-

normeret basis er en diagonalmatrix $(a_{11}, \dots, a_{nn})_{\text{diag}}$, vil den være unitær (ortogonal), hvis og kun hvis $\bar{a}_{ii}a_{ii} = 1$, $i = 1, \dots, n$, altså hvis og kun hvis diagonalelementerne har den absolutte værdi 1, i det reelle tilfælde, hvis og kun hvis de har værdierne 1 og -1. (Af en allerede nævnt sætning om normale afbildninger fremgår, at der til hver unitær afbildning af et vektorrum $(V, +, \mathbb{C}, \cdot)$ over de komplekse tals legeme findes en ortonormeret basis, med hensyn til hvilken afbildningens matrix er en diagonalmatrix. For ortogonale afbildninger af vektorrum over de reelle tals legeme gælder dette almindeligvis ikke.)

Af definitionen på unitær (ortogonal) afbildning slutes:
Er et underrum U af V invariant ved en unitær (ortogonal) afbildning f af V , vil restriktionen af f til U være en unitær (ortogonal) afbildning af U , og det ortogonale komplement $U^\perp$ til U vil også være invariant ved f .

Summen af to unitære (ortogonale) afbildninger af V er i almindelighed ikke unitær (ortogonal). Afbildningen, der fås ved at multiplicere en unitær (ortogonal) med en skalar λ , er unitær (ortogonal), hvis og kun hvis $|\lambda| = 1$ ($\lambda = \pm 1$).

Af definitionen slutes umiddelbart, at sammensætningen af to unitære (ortogonale) afbildninger og den inverse til en unitær (ortogonal) afbildning af V atter er unitær (ortogonal). De unitære afbildninger af et vektorrum $(V, +, \mathbb{C}, \cdot)$ over de komplekse tals legeme danner altså en transformationsgruppe, der kaldes vektorrummets unitære gruppe. Tilsvarende danner de ortogonale afbildninger af et vektorrum $(V, +, \mathbb{R}, \cdot)$ over de reelle tals legeme en transformationsgruppe, der kaldes vektorrummets

ortogonale gruppe. Hver af disse grupper er undergrupper i det pågældende vektorrums generelle lineære gruppe, dvs. gruppen af alle lineære transformationer (bijektive lineære afbildninger) af vektorrummet.

Vælges en ortonormeret basis for vektorrummet $(V, +, L, \cdot)$, fås en isomorf afbildning af rummets unitære (ortogonale) gruppe på mængden af unitære (ortogonale) $(n \times n)$ -matricer med matrixmultiplikation som komposition ved til hver afbildning i gruppen at lade svare den tilhørende matrix (jf. side III, 2, 15). De unitære $(n \times n)$ -matricer danner altså en gruppe, betegnet $U(n, \mathbb{C})$, der kaldes den unitære gruppe af graden n , og de reelle ortogonale $(n \times n)$ -matricer en gruppe, betegnet $O(n, \mathbb{R})$, der kaldes den reelle ortogonale gruppe af graden n . Dette bekræftes også let ved matrixregning. (At legemerne $\mathbb{C}$ og $\mathbb{R}$ indgår i gruppernes betegnelser, hvilket i betragtning af definitionerne synes overflødigt, skyldes, at analoge grupper også kan defineres for andre legemer.) $U(n, \mathbb{C})$ er en undergruppe af den generelle lineære gruppe $GL(n, \mathbb{C})$, og $O(n, \mathbb{R})$ er en undergruppe af $GL(n, \mathbb{R})$ (jf. side III, 2, 25).

De ortogonale grupper for 2- og 3-dimensionale reelle vektorrum med indre produkt er isomorfe med grupperne af de isometrier af henholdsvis en sædvanlig plan og det sædvanlige rum, som lader et valgt punkt fast.

Øvelser til kap. III, § 2.

1. Der er givet to lineært uafhængige geometriske vektorer $\underline{a}$ og $\underline{b}$. Vis, at den ved

$$\underline{u} \rightarrow \underline{a} \cdot \underline{u}$$

bestemte afbildning af det geometriske vektorrum V_3 ind i $\mathbb{R}$ samt de ved

$$\underline{u} \rightarrow \underline{u} + \underline{a} \times \underline{u}$$

og

$$\underline{u} \rightarrow (\underline{a} \cdot \underline{u})\underline{b} + (\underline{b} \cdot \underline{u})\underline{a}$$

bestemte afbildninger af V_3 ind i sig selv er lineære, og angiv i hvert af tilfældene billedrum og kerne.

2. Ved til talsættet $(x_1, x_2, x_3) \in \mathbb{R}^3$ at lade svare talsættet $(y_1, y_2) \in \mathbb{R}^2$ bestemt ved

$$y_1 = 2x_1 - x_2 + x_3$$

$$y_2 = x_1 + x_3$$

defineres en lineær afbildning af $(\mathbb{R}^3, +, \mathbb{R})$ ind i $(\mathbb{R}^2, +, \mathbb{R})$.

Bestem billedrum og kerne, og diskuter det lineære lignings-system

$$2x_1 - x_2 + x_3 = b_1$$

$$x_1 + x_3 = b_2$$

for vilkårligt givne $b_1, b_2 \in \mathbb{R}$.

Gennemfør det tilsvarende for den ved

$$y_1 = 2x_1 + x_2$$

$$y_2 = -x_1$$

$$y_3 = x_1 + x_2$$

bestemte lineære afbildning af $(\mathbb{R}^2, +, \mathbb{R})$ ind i $(\mathbb{R}^3, +, \mathbb{R})$.

3. Bestem samtlige lineære afbildninger $f: (\mathbb{R}, +, \mathbb{R}) \rightarrow (\mathbb{R}, +, \mathbb{R})$, samtlige lineære afbildninger $f: (\mathbb{R}^n, +, \mathbb{R}) \rightarrow (\mathbb{R}, +, \mathbb{R})$ og endelig samtlige lineære afbildninger $f: (\mathbb{R}^n, +, \mathbb{R}) \rightarrow (\mathbb{R}^m, +, \mathbb{R})$.

4. Idet $f_1, f_2, \dots, f_m$ er lineære afbildninger af et vektorrum $(U, +, L)$ ind i det endimensionale talrum $(L, +, L)$, skal man vise, at den ved

$$\underline{u} \rightarrow (f_1(\underline{u}), f_2(\underline{u}), \dots, f_m(\underline{u})), \quad \underline{u} \in U,$$

bestemte afbildning $f: (U, +, L) \rightarrow (L^m, +, L)$ er lineær, samt udtrykke kernen K_f ved kernerne $K_{f_1}, K_{f_2}, \dots, K_{f_m}$.

5. En lineær afbildning f af vektorrummet $(\mathbb{R}^{\mathbb{N}}, +, \mathbb{R})$ af alle reelle talfølger ind i sig selv defineres ved

$$(u_1, u_2, \dots) \rightarrow (v_1, v_2, \dots),$$

hvor

$$v_n = \frac{1}{n} (u_1 + \dots + u_n), \quad n = 1, 2, \dots$$

Vis, at f er bijektiv, og angiv den omvendte afbildning.

*Vis, at underrummet U bestående af alle konvergente reelle

talfølger ved f går over i et ægte underrum af sig selv:

$f(U) \subset U$. (Dette går ud på at vise, at hvis følgen

$(u_1, u_2, \dots)$ er konvergent, vil også $(v_1, v_2, \dots)$ være konvergent (med samme grænseværdi), og at det omvendte ikke gælder generelt.)

6. Idet t_0 er et fast tal tilhørende et interval $I \subseteq \mathbb{R}$, skal man vise, at der ved

$$\varphi \rightarrow \varphi(t_0)$$

defineres en lineær afbildning $f: (\hat{F}(I, \mathbb{R}), +, \mathbb{R}) \rightarrow (\mathbb{R}, +, \mathbb{R})$ af

vektorrummet bestående af de i I definerede reelle funktioner på det endimensionale talrum $(\mathbb{R}, +, \mathbb{R})$. Angiv afbildningens

kerne, find et til kernen komplementært underrum og verificer, at restriktionen af f til dette underrum er injektiv og har samme billedrum som f .

7. Vis, at der ved

$$\varphi \rightarrow \int_a^b \varphi(t) dt$$

defineres en lineær afbildning $f: (\hat{C}([a, b] \rightarrow \mathbb{R}), +, \mathbb{R}) \rightarrow (\mathbb{R}, +, \mathbb{R})$ af vektorrummet bestående af de på det afsluttede interval $[a, b] \subset \mathbb{R}$, $a < b$, kontinuerte reelle funktioner ind i talrummet $(\mathbb{R}, +, \mathbb{R})$. Find et til afbildningens kerne komplementært underrum og verificer, at restriktionen af f til dette underrum er injektiv og har samme billedrum som f .

8. Idet t_0 er et fast tal tilhørende et interval $I \subseteq \mathbb{R}$, skal man vise, at man ved til hver kontinuert reel funktion φ defineret på I at tilordne funktionen bestemt ved

$$\int_{t_0}^t \varphi(u) du, \quad t \in I$$

får en lineær afbildning $f: (\hat{C}(I \rightarrow \mathbb{R}), +, \mathbb{R}) \rightarrow (\hat{C}(I \rightarrow \mathbb{R}), +, \mathbb{R})$. Angiv billedrum og kerne for f .

For et om 0 symmetrisk interval I og $t_0 = 0$ skal man bestemme billedrummene svarende til underrummene af lige, henholdsvis ulige kontinuerte funktioner på I .

• For $I = [-\pi, \pi]$, $t_0 = 0$ skal man angive en basis for $f(U)$, hvor U er underrummet frembragt af funktionerne $1, \cos t, \sin t, \cos 2t, \sin 2t, \dots$, $t \in [-\pi, \pi]$.

Vis endelig, at når I er et afsluttet interval, og $\hat{C}(I \rightarrow \mathbb{R})$ forsynes med den til normen $\|\varphi\|_\infty = \sup \{|\varphi(t)| \mid t \in I\}$ svarende metrik, da vil den lineære afbildning f være (ligeligt) kontinuert.

9. For vektorrummet $(V_2, +, \cdot)$ af geometriske vektorer i en given plan vælges en basis $(\underline{e}_1, \underline{e}_2)$. (Alle vektorer afsættes fra et fast punkt 0; tegn $\underline{e}_1$ og $\underline{e}_2$ som vektorer af forskellig længde, ikke vinkelrette på hinanden.)

Konstruer den til en vilkårlig vektor $\underline{u} \in V_2$ hørende billedvektor ved den lineære afbildning $f: (V_2, +, \cdot) \rightarrow (V_2, +, \cdot)$ bestemt ved

- a) $f(\underline{e}_1) = \underline{e}_1, \quad f(\underline{e}_2) = -\underline{e}_2,$
b) $f(\underline{e}_1) = \underline{e}_2, \quad f(\underline{e}_2) = \underline{e}_1,$
c) $f(\underline{e}_1) = \underline{e}_1 - \underline{e}_2, \quad f(\underline{e}_2) = \underline{e}_2 - \underline{e}_1.$

Bestem i hvert tilfælde billedrum og kerne, samt mængden $\{\underline{u} \in V_2 \mid f(\underline{u}) = \underline{u}\}$ af vektorer, der afbildes i sig selv.

10. Vis, at de lineære afbildninger f_1, f_2 og f_3 af vektorrummet $(V_2, +, \cdot)$ ind i sig selv bestemt ved

$$\begin{aligned} f_1(\underline{e}_1) &= \underline{e}_2, & f_1(\underline{e}_2) &= -\underline{e}_1, \\ f_2(\underline{e}_1) &= -\underline{e}_1, & f_2(\underline{e}_2) &= -\underline{e}_2, \\ f_3(\underline{e}_1) &= -\underline{e}_2, & f_3(\underline{e}_2) &= \underline{e}_1, \end{aligned}$$

hvor $(\underline{e}_1, \underline{e}_2)$ er en basis for $(V_2, +, \cdot)$, sammen med den identiske afbildning af V_2 danner en transformationsgruppe.

11. Opskriv matricerne hørende til de i øvelserne 9. og 10. betragtede lineære afbildninger af $(V_2, +, \cdot)$ ind i sig selv, idet basen $(\underline{e}_1, \underline{e}_2)$ benyttes også for billedvektorer. Angiv koordinaterne til billedet af $3\underline{e}_1 + 2\underline{e}_2$ ved hver af afbildningerne.

12. Rumfigurer gengives som bekendt ofte på papiret, idet man tegner et billede, som kan tænkes fremkommet ved en parallelprojektion. Hvorledes gengives vektoren $\underline{v}$ med koordinatsættet $(2, \frac{1}{2}, -1)$ med hensyn til en basis $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$ for de geometriske vektorer, når billederne af $\underline{e}_1$, $\underline{e}_2$ og $\underline{e}_3$ er kendt?

13. Idet $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$ er en basis for et vektorrum $(U, +, L)$ og $(\underline{f}_1, \underline{f}_2)$ en basis for et vektorrum $(V, +, L)$, skal man angive koordinatfremstillingen for den lineære afbildning $f: (U, +, L) \rightarrow (V, +, L)$ bestemt ved

$$f(\underline{e}_1) = \underline{f}_1, \quad f(\underline{e}_2) = \underline{f}_2, \quad f(\underline{e}_3) = \underline{f}_1 + \underline{f}_2,$$

finde kernen K_f samt $f^{-1}(\underline{f}_1 + \underline{f}_2)$.

14. Lad $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$ være en ortonormal basis for det geometriske vektorrum $(V_3, +, \mathbb{R})$, og lad $\underline{e}_1$, $\underline{e}_2$ og $\underline{e}_3$ være i højrestilling. For en given vektor $\underline{a}$ med koordinatsættet $(\underline{a}_1, \underline{a}_2, \underline{a}_3)$ betragtes den lineære afbildning af $(V_3, +, \mathbb{R})$ ind i sig selv bestemt ved $\underline{u} \rightarrow \underline{a} \times \underline{u}$, $\underline{u} \in V_3$. Find den tilhørende matrix, idet vektorer og billedvektorer henføres til basen $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$.

Angiv en nødvendig og tilstrækkelig betingelse for, at det lineære ligningssystem

$$\begin{aligned} -a_3x_2 + a_2x_3 &= b_1 \\ a_3x_1 - a_1x_3 &= b_2 \\ -a_2x_1 + a_1x_2 &= b_3, \end{aligned}$$

hvor $a_1, a_2, a_3 \neq 0, 0, 0$ og b_1, b_2, b_3 er reelle tal, har en løsning, og bestem i bekræftende fald samtlige løsninger.

15. Lad $(\underline{e}_1, \underline{e}_2)$ være en ortonormal basis for vektorrummet $(V_2, +, \mathbb{R})$ af geometriske vektorer i en given plan, og lad f og g være de lineære afbildninger af $(V_2, +, \mathbb{R})$ ind i sig selv bestemt ved

$$f(\underline{e}_1) = \underline{e}_2, \quad f(\underline{e}_2) = -\underline{e}_1,$$

$$g(\underline{e}_1) = 2\underline{e}_1, \quad g(\underline{e}_2) = \underline{e}_2,$$

medens e er den identiske afbildning af V_2 . Find (evt. med støtte i regninger med matricer) geometriske beskrivelser af følgende afbildninger: $(\sqrt{2})^{-1}(f + e)$, $\frac{1}{2}(g + e)$, $g - e$, $(g - e) \circ f \circ (g - e)$, $f \circ g \circ f^{-1}$.

16. Udregn alle produkter med to faktorer, som kan dannes af matricerne

$$\underline{A} = \begin{pmatrix} 2 & 1 \\ -1 & 0 \\ 3 & 2 \end{pmatrix}, \quad \underline{B} = \begin{pmatrix} -1 & -2 \\ 3 & 3 \end{pmatrix}, \quad \underline{C} = \begin{pmatrix} 1 & -1 & 1 \end{pmatrix}, \quad \underline{D} = \begin{pmatrix} 3 \\ 1 \end{pmatrix}.$$

17. Dan matrixprodukterne

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} (b_1 \quad \dots \quad b_n) \quad \text{og} \quad (b_1 \quad \dots \quad b_n) \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

18. Multipliser en vilkårlig $(m \times n)$ -matrix med en diagonalmatrix 1) fra venstre, 2) fra højre.

19. Hvad kan siges om produktet af to $(n \times n)$ -matricer, der begge er øvre trekantsmatricer?

20. Er $\underline{A} = (a_{ij})$ en $(m \times m)$ -matrix, forstås ved dens spor (engelsk og fransk "trace") tallet

$$\text{tr } \underline{A} = \sum_{i=1}^m a_{ii}.$$

Vis, at der for hver $(m \times n)$ -matrix $\underline{B}$ og hver $(n \times m)$ -matrix $\underline{C}$ gælder

$$\text{tr}(\underline{B} \underline{C}) = \text{tr}(\underline{C} \underline{B}).$$

21. Reducer

$$\sum_{i=1}^n \sum_{j=1}^n \delta_{ij} \delta_{ji}, \quad \sum_{i=1}^n \sum_{j=1}^n (\delta_{ij} \delta_{kl} - \delta_{ik} \delta_{jl}) \delta_{ij}.$$

22.* For et vilkårligt tal x og et positivt helt tal p defineres

$$\binom{x}{p} = \frac{x(x-1)\dots(x-p+1)}{1 \cdot 2 \cdot \dots \cdot p}; \quad \binom{x}{0} = 1$$

Vis, at der for $((n+1) \times (n+1))$ -matricen

$$\underline{A} = \left((-1)^j \binom{j}{i} \right)_{i,j=0,\dots,n}$$

gælder $\underline{A}^2 = \underline{E}$.

23. Idet $\underline{A}$ er en given $(n \times n)$ -matrix med elementer fra tallegeme-
 man L , skal vise, at der findes tal $\lambda_0, \lambda_1, \dots, \lambda_n \in L$, som
 ikke alle er 0, således at

$$\lambda_0 \underline{E} + \lambda_1 \underline{A} + \lambda_2 \underline{A}^2 + \dots + \lambda_n \underline{A}^{n^2} = \underline{0}.$$

24. Beregn matrixprodukterne $\underline{E}_{\alpha\beta} \underline{A}$ og $\underline{A} \underline{E}_{\alpha\beta}$, hvor $\underline{A}$ er en vil-
 kårlig $(n \times n)$ -matrix, medens $\underline{E}_{\alpha\beta}$ betegner den $(n \times n)$ -ma-
 trix, hvor elementet i α -te række og β -te søjle er 1, alle
 øvrige elementer 0.

Bestem samtlige $(n \times n)$ -matricer, som hver er ombyttelig
 med alle $(n \times n)$ -matricer, altså samtlige matricer $\underline{A} \in M_{n,n}$
 hvor

$$\forall_{M_{n,n}} \underline{X} : \underline{A} \underline{X} = \underline{X} \underline{A}.$$

25. Vis, at matrixadditionen og matrixmultiplikationen er kom-
 positioner i mængden af (2×2) -matricer $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $a, b \in \mathbb{R}$,
 og vis, at mængden med disse kompositioner er isomorf med
 de komplekse tals legeme $(\mathbb{C}, +, \cdot)$.

26. Angiv en nødvendig og tilstrækkelig betingelse for, at en
 diagonalmatrix er regulær. Hvorledes bestemmes den inverse,
 når betingelsen er opfyldt?

27. Udregn matrixproduktet $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$, hvor a, b, c, d betegner vilkårlige tal fra L .

Find en nødvendig og tilstrækkelig betingelse for, at en

(2×2) -matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ er regulær, og angiv i bekræftende fald dens inverse.

28. Beregn samtlige potenser $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^n$, $n \in \mathbb{Z}$, og $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n$, $n \in \mathbb{Z}$, og angiv ordenen af de to undergrupper af $GL(2, L)$, der udgøres af disse potenser.

29. Idet $\underline{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, medens vi sætter $\underline{A}^p = \begin{pmatrix} a_p & b_p \\ c_p & d_p \end{pmatrix}$ for

hvert $p \in \mathbb{N}$, skal man opstille rekursionsformler til bestemmelse af a_p, b_p, c_p, d_p (dvs. formler som tillader beregning af disse tal, når a, b, c, d og $a_{p-1}, b_{p-1}, c_{p-1}, d_{p-1}$ kendes).

Find derefter a_p, b_p, c_p, d_p udtrykt ved p, a, b, d , når det er givet, at $c = 0$.

Bestem samtlige reelle matricer $\underline{A} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, som tilfredsstiller ligningen $\underline{A}^p = \underline{A}$, hvor $p \in \mathbb{N}$ er givet.

30. Idet $\underline{A}$ er en vilkårlig (2×2) -matrix, skal man vise, at der ikke findes nogen (2×2) -matrix $\underline{X}$, som tilfredsstiller ligningen

$$\underline{A} \underline{X} - \underline{X} \underline{A} = \underline{E}.$$

31. Vis, at for enhver matrix $\underline{A}$ vil $\underline{A} \underline{A}'$ være symmetrisk. Vis, at når $\underline{A}$ er en vilkårlig $(m \times n)$ -matrix og $\underline{B}$ en (skæv)symmetrisk $(n \times n)$ -matrix, da vil $\underline{A} \underline{B} \underline{A}'$ være (skæv)symmetrisk. Idet $\underline{B}$ er en symmetrisk, $\underline{C}$ en skævsymmetrisk $(n \times n)$ -matrix, skal man undersøge, om matricerne $\underline{B} \underline{C} + \underline{C} \underline{B}$ og $\underline{B} \underline{C} - \underline{C} \underline{B}$ er symmetriske eller skævsymmetriske.

Vis, at hver kvadratisk matrix på en og kun én måde kan fremstilles som en sum af en symmetrisk og en skævsymmetrisk matrix.

32. Vis, at når en symmetrisk (skævsymmetrisk) matrix er regulær, vil den inverse matrix ligeledes være symmetrisk (skævsymmetrisk). Vis, at ingen skævsymmetrisk (3×3) -matrix er regulær.

33. Om en blokmatrix af formen $\begin{pmatrix} \underline{A} & \underline{B} \\ \underline{0} & \underline{C} \end{pmatrix}$ forudsættes, at blokkene $\underline{A}$ og $\underline{C}$ er kvadratiske. Vis, at matricen er regulær, hvis og kun hvis $\underline{A}$ og $\underline{C}$ er regulære, og angiv i bekræftende fald den inverse i form af en tilsvarende blokmatrix.

34. Idet $(U, +, \mathbb{R})$ er et todimensionalt og $(V, +, \mathbb{R})$ et tredimensionalt vektorrum, hvori er valgt baser $(\underline{e}_1, \underline{e}_2)$ og $(\underline{f}_1, \underline{f}_2, \underline{f}_3)$, er en lineær afbildning $f: (U, +, \mathbb{R}) \rightarrow (V, +, \mathbb{R})$ givet ved matrixligningen

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ -4 & 0 \\ 1 & 3 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

Bestem matrixligningerne for samtlige lineære afbildninger $g: (V, +, \mathbb{R}) \rightarrow (U, +, \mathbb{R})$ med den egenskab, at $g \circ f$ er den identiske afbildning af U .

35. Vi betragter vektorrummet $(\hat{P}_n(\mathbb{R} \rightarrow \mathbb{R}), +, \mathbb{R})$ af alle reelle polynomier af højst n -te grad.

Ved til hvert polynomium

$$p(t) = p_0 + p_1 t + p_2 t^2 + \dots + p_n t^n, \quad t \in \mathbb{R},$$

at lade svare dets differentialkvotient fås en lineær afbildning $D: \hat{P}_n \rightarrow \hat{P}_n$. Angiv afbildningens kerne og billedrum.

med $D(\hat{P}_n)$. Find afbildningens matrix, idet der som basis benyttes $(1, t, t^2, \dots, t^n)$. Angiv kernen og billedrummet ved afbildningen D^2 , og bekræft ved matrixregning, at D^2 er afbildningen, der til hvert polynomium $p(t)$ lader svare dets anden afledede.

Idet h er et givet reelt tal, defineres ved $F_h(p(t)) = p(t+h)$ en afbildning $F_h: \hat{P}_n \rightarrow \hat{P}_n$. Vis, at F_h er en bijektiv lineær afbildning, og find dens matrix i den nævnte basis. (Begynd med at bestemme de til basispolynomierne svarende polynomier.)

Vis, at polynomierne

$$t^{(0)} = 1, \quad t^{(i)} = t(t-h)(t-2h)\dots(t-(i-1)h), \quad i = 1, \dots, n,$$

danner en basis for $\hat{P}_n$. Angiv matrixerne hørende til den øjensynligt lineære afbildning $\Delta_h: \hat{P}_n \rightarrow \hat{P}_n$ bestemt ved $\Delta_h(p(t)) = p(t+h) - p(t)$ og til afbildningen F_h , når denne basis benyttes. Vis, at der, når $h \neq 0$, for ethvert polynomium $q(t) \in \hat{P}_{n-1}$ findes et polynomium $p(t) \in \hat{P}_n$, som tilfredsstiller "differensligningen"

$$\forall_R t : \Delta_h(p(t)) = p(t+h) - p(t) = q(t),$$

og angiv, hvorledes samtlige løsninger $p(t) \in \hat{P}_n$ bestemmes ud fra en vilkårlig.

36. Lad f være en afbildning af en mængde $A \subseteq \mathbb{R}^n$ ind i $\mathbb{R}^m$ med koordinatfunktioner $f_1, \dots, f_m$:

$$(y_1, \dots, y_m) = f(x_1, \dots, x_n) \iff y_i = f_i(x_1, \dots, x_n), \\ i = 1, \dots, m.$$

Vi forudsætter, at f er differentiabel i et indre punkt $(a_1, \dots, a_n) \in A$, hvilket er ensbetydende med, at $f_1, \dots, f_m$ alle er differentiable i punktet. Ved funktionalmatrixen for afbildningen f i punktet $(a_1, \dots, a_n)$ forstås $(m \times n)$ -

matricen

$$\left(\frac{\partial y_i}{\partial x_j} \right)_{i=1, \dots, m; j=1, \dots, n},$$

hvor de partielle afledede alle er taget i $(a_1, \dots, a_n)$.

Lad endvidere g være en afbildning af en mængde B ,

$f(A) \subseteq B \subseteq \mathbb{R}^m$, ind i $\mathbb{R}^1$ med koordinatfunktioner $g_1, \dots, g_l$:

$$(z_1, \dots, z_l) = g(y_1, \dots, y_m) \iff z_h = g_h(y_1, \dots, y_m),$$

$$h = 1, \dots, l.$$

Vi forudsætter, at $(b_1, \dots, b_m) = f(a_1, \dots, a_n)$ er indre punkt

i B , og at g er differentiabel i dette punkt. Den sammensatte

afbildning $g \circ f: A \rightarrow \mathbb{R}^1$ er da differentiabel i $(a_1, \dots, a_n)$.

Vis, at funktionalmatricen for $g \circ f$ i $(a_1, \dots, a_n)$ er lig ma-

trixproduktet af funktionalmatricen for g i $(b_1, \dots, b_m) =$

$f(a_1, \dots, a_n)$ og funktionalmatricen for f i $(a_1, \dots, a_n)$:

$$\left(\frac{\partial z_h}{\partial x_j} \right)_{1, n} = \left(\frac{\partial z_h}{\partial y_i} \right)_{1, m} \left(\frac{\partial y_i}{\partial x_j} \right)_{m, n}.$$

37. I et tredimensionalt vektorrum $(V, +, L)$ er givet en basis

$(\underline{e}_1, \underline{e}_2, \underline{e}_3)$. Vis, at de tre vektorer

$$\hat{\underline{e}}_1 = \underline{e}_1 + a\underline{e}_2 + b\underline{e}_3, \quad \hat{\underline{e}}_2 = \underline{e}_2 + c\underline{e}_3, \quad \hat{\underline{e}}_3 = \underline{e}_3,$$

hvor a, b, c er givne tal fra L , danner en basis.

Find koordinaterne til en vilkårlig vektor $\underline{v}$ med hensyn til

basen $(\hat{\underline{e}}_1, \hat{\underline{e}}_2, \hat{\underline{e}}_3)$ udtrykt ved dens koordinater med hensyn til

$(\underline{e}_1, \underline{e}_2, \underline{e}_3)$. Find også omvendt de sidstnævnte koordinater udtrykt ved de førstnævnte.

38. Lad $(0; \underline{e}_1, \underline{e}_2)$ og $(0; \hat{\underline{e}}_1, \hat{\underline{e}}_2)$ være to parallelkoordinatsystemer i en plan E_2 , således at

$$\hat{\underline{e}}_1 = \underline{e}_1 + \underline{e}_2, \quad \hat{\underline{e}}_2 = \underline{e}_1 - \underline{e}_2.$$

Find $\underline{e}_1$ og $\underline{e}_2$ som linearkombinationer af $\hat{\underline{e}}_1$ og $\hat{\underline{e}}_2$.

En linie har i koordinatsystemet $(0; \underline{e}_1, \underline{e}_2)$ parameterfremstillingen

$$x_1 = 3 - t, \quad x_2 = -2 + 2t, \quad t \in \mathbb{R}.$$

Omregn denne til koordinatsystemet $(0; \hat{\underline{e}}_1, \hat{\underline{e}}_2)$.

Lad Q betegne punktet med koordinatsættet $(3, -4)$ i systemet $(0; \underline{e}_1, \underline{e}_2)$. Angiv liniens parameterfremstilling i koordinatsystemet $(Q; \hat{\underline{e}}_1, \hat{\underline{e}}_2)$.

39. I rummet $\mathbb{E}_3$ er valgt et koordinatsystem $(0; \underline{e}_1, \underline{e}_2, \underline{e}_3)$. To planer har i dette koordinatsystem parameterfremstillingerne

$$\begin{aligned} x_1 &= 2 + s' & y_1 &= 3 + 2t' \\ x_2 &= s' - s'' & y_2 &= 1 + 2t'' \\ x_3 &= -1 - s'' & y_3 &= 1 - 2t' + 2t''. \end{aligned}$$

Vis, at det er samme plan, der fremstilles. Til et punkt i denne plan svarer altså såvel et parameterpar (s', s'') i den første som et parameterpar (t', t'') i den anden parameterfremstilling. Find t' og t'' udtrykt ved s' og s'' .

40. En lineær afbildning af et tredimensionalt vektorrum $(U, +, L)$, hvori der er valgt en basis $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$, ind i et todimensionalt vektorrum $(V, +, L)$, hvori der er valgt en basis $(\underline{f}_1, \underline{f}_2)$, er med hensyn til de nævnte baser givet ved matrixligningen

$$\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} = \begin{pmatrix} a & 0 & a \\ 1 & a-1 & a \end{pmatrix} \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix},$$

hvor a er et givet tal tilhørende L . Angiv for hver værdi af a afbildningens rang r . Bestem dernæst nye baser i de to rum, således at den til afbildningen hørende matrix antager normalformen med $(r \times r)$ -enhedsmatricen i øverste venstre hjørne og nuller på alle andre pladser. Angiv også de tilsvarende regulære koordinattransformationsmatricer $\underline{S}$ og $\underline{T}$.

og gennemfør en kontrol ved at udregne $\underline{T} \underline{A} \underline{S}^{-1}$, hvor $\underline{A}$ er ovenstående (2×3) -matrix.

41. I mængden $M_{m,n}(L)$ af $(m \times n)$ -matricer med elementer fra tallegemet L defineres en relation ved at fastsætte, at $\underline{A}$ står i relationen til $\underline{B}$, hvis der findes en regulær $(m \times m)$ -matrix $\underline{P}$ og en regulær $(n \times n)$ -matrix $\underline{Q}$, således at $\underline{P} \underline{A} \underline{Q} = \underline{B}$.
Vis, at der foreligger en ækvivalensrelation, og angiv antallet af ækvivalensklasser.

42. Vis, at matricen

$$\begin{pmatrix} a_1 \\ \vdots \\ a_m \end{pmatrix} (b_1 \ \dots \ b_n),$$

hvor $a_1, \dots, a_m, b_1, \dots, b_n \in L$, har rangen 0 eller 1. Vis omvendt, at hver matrix med elementer fra L , hvis rang er 0 eller 1, kan skrives som produkt af en søjlematrix og en rækkematrix.

43. Om en lineær afbildning f af et n -dimensionalt vektorrum $(U, +, L)$ ind i sig selv forudsættes, at hver vektor $\underline{u} \neq \underline{0}$ er egenvektor, dvs. til hver vektor $\underline{u} \neq \underline{0}$ svarer et tal $\lambda(\underline{u}) \in L$, den til $\underline{u}$ hørende egenværdi, således at $f(\underline{u}) = \lambda(\underline{u})\underline{u}$. Vis, at $\lambda(\underline{u})$ ikke kan afhænge af $\underline{u}$, altså at f er en homoteti eller nulafbildningen, og angiv afbildningens matrixfremstilling med hensyn til en vilkårlig basis.

52. Lad $(V, +, \dot{R}, \cdot)$ være et 2-dimensionalt vektorrum med indre produkt, lad f være en lineær afbildning af $(V, +, \dot{R}, \cdot)$, og lad

$$\underline{\underline{A}} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

være den til f hørende matrix med hensyn til en ortonormal basis. Vis, at f er normal, hvis og kun hvis $b = c$, eller $b = -c$ og $a = d$. Vis, at hvis f er normal, og $ad \neq b^2$, så er f regulær.

53. Lad f være en bijektiv selvadjungeret afbildning af et endelig-dimensionalt vektorrum $(V, +, L, \cdot)$ med indre produkt. Vis, at f^{-1} er selvadjungeret.

54. Lad f være en involutorisk unitar (ortogonal) afbildning af et endelig-dimensionalt vektorrum $(V, +, L, \cdot)$ med indre produkt. Vis, at f er selvadjungeret.

55. Lad f være en anti-symmetrisk afbildning af det 3-dimensionale geometriske vektorrum $(V_3, +, \dot{R}, \cdot)$. Vis, at der findes en vektor $\underline{v} \in V_3$, således at $f(\underline{x}) = \underline{v} \times \underline{x}$ for alle $\underline{x} \in V_3$.

56. Lad $(V, +, \dot{R}, \cdot)$ være et n -dimensionalt vektorrum med indre produkt, hvori der er valgt en ortonormal basis. Vis, at der for enhver ortogonal transformation f af $(V, +, \dot{R}, \cdot)$ gælder

$$|\operatorname{tr} \underline{\underline{A}}| \leq n,$$

hvor $\operatorname{tr} \underline{\underline{A}}$ betegner sporet af den til f hørende matrix $\underline{\underline{A}}$

med hensyn til den valgte basis. Bestem endvidere samtlige ortogonale transformationer f for hvilke

$$|\operatorname{tr} \underline{\underline{A}}| = n.$$

(Ved sporet af $\underline{\underline{A}}$ forstås som bekendt summen af $\underline{\underline{A}}$'s diagonalelementer.)

57. Lad $(V, +, L, \cdot)$ være et endelig-dimensionalt vektorrum med indre produkt, og lad f være en normal afbildning af $(V, +, L, \cdot)$ med kerne K . Vis, at $f(V) = K^\perp$. Vis, at for hvert $n \in \mathbb{N}$ har f^n samme rang som f .
58. Lad f være en idempotent selvadjungeret afbildning af et endelig dimensionalt vektorrum $(V, +, L, \cdot)$ med indre produkt. Vis, at f er orthogonalprojektion på underrummet $f(V)$.

§ 3a. Løsning af lineære ligningssystemer.

Skal man bestemme de eventuelle løsninger $(x_1, x_2, \dots, x_n) \in L^n$ til et forelagt lineært ligningssystem

$$\begin{array}{ccccccc} a_{11}x_1 & + & a_{12}x_2 & + & \dots & + & a_{1n}x_n = b_1 \\ a_{21}x_1 & + & a_{22}x_2 & + & \dots & + & a_{2n}x_n = b_2 \\ a_{31}x_1 & + & a_{32}x_2 & + & \dots & + & a_{3n}x_n = b_3 \\ \vdots & & \vdots & & & & \vdots \\ \vdots & & \vdots & & & & \vdots \\ a_{m1}x_1 & + & a_{m2}x_2 & + & \dots & + & a_{mn}x_n = b_m, \end{array}$$

hvor alle koefficienter a_{ij} er givne tal tilhørende et tallegeme L , ligesom alle b_i tilhører L , vil det i reglen være det letteste først at skaffe sig et nyt ligningssystem med samme løsninger, af formen

$$\begin{array}{ccccccc} c_{11}x'_1 & + & c_{12}x'_2 & + & \dots & + & c_{1r}x'_r + c_{1,r+1}x'_{r+1} + \dots + c_{1n}x'_n = d_1 \\ c_{22}x'_2 & + & \dots & + & c_{2r}x'_r + c_{2,r+1}x'_{r+1} + \dots + c_{2n}x'_n = d_2 \\ & & & & \vdots & & \vdots \\ & & & & \vdots & & \vdots \\ & & & & \vdots & & \vdots \\ c_{rr}x'_r & + & c_{r,r+1}x'_{r+1} & + & \dots & + & c_{rn}x'_n = d_r \\ 0x'_r & + & 0x'_{r+1} & + & \dots & + & 0x'_n = d_{r+1} \\ \vdots & & \vdots & & & & \vdots \\ 0x'_r & + & 0x'_{r+1} & + & \dots & + & 0x'_n = d_m, \end{array}$$

hvor $c_{11}, c_{22}, \dots, c_{rr}$ alle er forskellige fra 0; her står $x'_1, x'_2, \dots, x'_n$ for de oprindelige ubekendte, blot måske i en ny rækkefølge; eventuelt er $r = n$ eller $r = m$.

At ethvert lineært ligningssystem, hvor koefficienterne a_{ij} ikke alle er 0, kan reduceres til den nævnte form, indses således:

Det kan antages, at $a_{11} \neq 0$; ellers foretages blot en pas-

sende omordning af ligninger eller af ubekendte med tilhørende koefficienter. Findes der nu koefficienter $a_{i1} \neq 0$ med $2 \leq i \leq m$, går man over til et nyt ligningssystem ved til den i^{te} ligning, $i = 2, \dots, m$, at addere den første ligning multipliceret med $-a_{i1}/a_{11}$; det er klart, at enhver løsning til det gamle ligningssystem er løsning til det nye; at også det omvendte er tilfældet, fremgår straks, når man bemærker, at det gamle ligningssystem kan fås ud fra det nye ved til den i^{te} ligning, $i = 2, \dots, m$, at addere den første ligning multipliceret med a_{i1}/a_{11} . Herefter er a_{11} den eneste fra 0 forskellige koefficient til x_1 .

Har ligningssystemet nu ikke allerede den ønskede form, vil opgaven dog være reduceret til at omforme et lineært ligningssystem med $m - 1$ ligninger og $n - 1$ ubekendte, nemlig de $m - 1$ sidste ligninger i de ubekendte $x_2, \dots, x_n$. Kan nemlig disse ligninger bringes på den tilstræbte form, mangler der blot, at man fører en eventuel omordning af $x_2, \dots, x_n$ med også i den første ligning.

At ethvert lineært ligningssystem, hvor koefficienterne a_{ij} ikke alle er 0, kan reduceres til den ønskede form, følger da ved induktion. Dennes "start" sikres ved, at lineære ligningssystemer med kun én ligning eller én ubekendt let bringes på reduceret form.

Ved den praktiske udførelse af reduktionen af et forelagt lineært ligningssystem foretages første skridt som under beviset ovenfor, hvorved opnås, at i første koefficientsøjle alene den øverste koefficient er forskellig fra 0. Har ligningssystemet nu ikke allerede den ønskede form, omordnes om fornødent de $m - 1$ sidste ligninger eller de $n - 1$ sidste ubekendte med tilhørende koefficienter (i samtlige ligninger), således at man får en koef-

ficient $c_{22} \neq 0$; findes der nu i anden koefficientsøjle under c_{22} koefficienter forskellige fra 0, bortskaffes disse, idet man til de pågældende ligninger adderer anden ligning multipliceret med passende konstanter. Efter dette andet skridt i udførelsen af reduktionen følger om nødvendigt et tilsvarende tredje skridt med sigte på tredje koordinatsøjle, osv.

Er nu et lineært ligningssystem omdannet til et ensbetydende af den ønskede form, volder bestemmelsen af de eventuelle løsninger ingen vanskeligheder:

I tilfælde af, at $r < m$ og $d_{r+1}, \dots, d_m$ ikke alle er 0, er der åbenbart ingen løsninger. Er $r < m$ og $d_{r+1}, \dots, d_m$ alle 0, kan de sidste $m - r$ ligninger i det reducerede ligningssystem bortkastes.

Har ligningssystemet nu formen

$$\begin{array}{rcll} c_{11}x'_1 + \dots + c_{1,r-1}x'_{r-1} + & c_{1r}x'_r & = & d_1 \\ & \vdots & & \vdots \\ & \vdots & & \vdots \\ c_{r-1,r-1}x'_{r-1} + c_{r-1,r}x'_r & = & d_{r-1} \\ & c_{rr}x'_r & = & d_r, \end{array}$$

hvor $c_{11}, \dots, c_{r-1,r-1}, c_{rr}$ alle er forskellige fra 0, er der netop én løsning; de ubekendte $x'_r, x'_{r-1}, \dots, x'_1$ kan bestemmes successivt.

Er ligningssystemet derimod af formen

$$\begin{array}{ccccccc}
 c_{11}x'_1 + \dots + c_{1,r-1}x'_{r-1} + & c_{1r}x'_r + \dots + & c_{1n}x'_n = d_1 \\
 & \vdots & \vdots \\
 & \ddots & \vdots \\
 & c_{r-1,r-1}x'_{r-1} + c_{r-1,r}x'_r + \dots + c_{r-1,n}x'_n = d_{r-1} \\
 & & c_{rr}x'_r + \dots + c_{rn}x'_n = d_r,
 \end{array}$$

hvor $c_{11}, \dots, c_{r-1,r-1}, c_{rr}$ alle er forskellige fra 0 og $r < n$, da findes der for vilkårlige $t_1, \dots, t_{n-r} \in L$ netop én løsning $(x'_1, \dots, x'_n)$ med $x'_{r+1} = t_1, \dots, x'_n = t_{n-r}$; de øvrige ubekendte $x'_r, x'_{r-1}, \dots, x'_1$ kan bestemmes successivt; herved fås samtlige løsninger på formen

$$\begin{array}{lcl}
 x'_1 & = k_1 + l_{11}t_1 + \dots + l_{1,n-r}t_{n-r} \\
 \vdots & \vdots & \vdots \\
 x'_r & = k_r + l_{r1}t_1 + \dots + l_{r,n-r}t_{n-r} & t_1, \dots, t_{n-r} \in L, \\
 x'_{r+1} & = t_1 \\
 \vdots & \ddots & \\
 x'_n & = t_{n-r},
 \end{array}$$

eller

$$\begin{pmatrix} x'_1 \\ \vdots \\ x'_r \\ x'_{r+1} \\ \vdots \\ x'_n \end{pmatrix} = \begin{pmatrix} k_1 \\ \vdots \\ k_r \\ 0 \\ \vdots \\ 0 \end{pmatrix} + t_1 \begin{pmatrix} l_{11} \\ \vdots \\ l_{r1} \\ \delta_{11} \\ \vdots \\ \delta_{n-r,1} \end{pmatrix} + \dots + t_{n-r} \begin{pmatrix} l_{1,n-r} \\ \vdots \\ l_{r,n-r} \\ \delta_{1,n-r} \\ \vdots \\ \delta_{n-r,n-r} \end{pmatrix}.$$

Vi bemærker, at medmindre løsningsmængden er tom, er den, som vi på forhånd vidste (III,2,8), et siderum i det n -dimensionale talrum $(L^n, +, L)$. Siderummets dimension er $n - r$; thi for $r = n$ er der netop én løsning, og for $r < n$ er de $n - r$ koefficientsøjler til $t_1, \dots, t_{n-r}$ i udtrykket for løsningsmængden lineært uafhængige. Det tal r , der fremkommer ved reduktion af et lineært ligningssystem, er følgelig koefficientmatricens rang (jfr. III,2, side 8 og 16).

Øvelser om lineære ligningssystemer.

1. Find eventuelle løsninger $(x_1, x_2, x_3) \in \mathbb{R}^3$ til ligningssystemet

$$\begin{aligned}x_1 + x_2 + 2x_3 &= 3 \\2x_1 - x_2 + 4x_3 &= 0 \\x_1 + 3x_2 - 2x_3 &= 3 \\-3x_1 - 2x_2 + x_3 &= 0.\end{aligned}$$

2. Find eventuelle løsninger $(x_1, x_2, x_3, x_4) \in \mathbb{R}^4$ til ligningssystemet

$$\begin{aligned}x_1 - x_2 + 2x_3 + x_4 &= 1 \\-4x_1 - 5x_2 + 7x_3 - 7x_4 &= -7 \\2x_1 + x_2 - x_3 + 3x_4 &= 3 \\-x_1 - 5x_2 + 8x_3 - 3x_4 &= -3.\end{aligned}$$

3. Afgør for hvert af de følgende tre lineære ligningssystemer med samme venstre side, om det har løsninger $(x_1, x_2, x_3) \in \mathbb{R}^3$, og angiv i bekræftende fald disse:

$$\begin{array}{rclcl} -2x_1 & + & 2x_3 & = & 0 & = & 1 & = & 2 \\ 4x_1 + 3x_2 & - & x_3 & = & 0 & = & 0 & = & 2 \\ & & x_2 + x_3 & = & 0 & = & 0 & = & 2. \end{array}$$

4. I et parallelkoordinatsystem $(0; \underline{e}_1, \underline{e}_2, \underline{e}_3)$ i rummet er to planer givet ved ligningerne

$$x_1 + x_2 - x_3 = 0, \quad 2x_1 - x_2 + 3x_3 = 9.$$

Find en parameterfremstilling for planernes skæringslinje.

Øvelser om lineære ligningssystemer. (fortsat)

5. I et vektorrum $(V, +, L)$ med basis $(\underline{e}_1, \underline{e}_2, \underline{e}_3, \underline{e}_4)$ er fire vektorer givet ved koordinatsættene

$$(0, 1, 3, -1), \quad (1, 2, 1, 2), \quad (3, -5, -4, -1), \quad (-4, 1, 6, 1).$$

Undersøg, om vektorerne er lineært afhængige eller lineært uafhængige.

6. En lineær afbildning $f: (\mathbb{R}^4, +, \mathbb{R}) \rightarrow (\mathbb{R}^3, +, \mathbb{R})$ er givet ved

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} 2 & -1 & 1 & 3 \\ 0 & 1 & 1 & -1 \\ 1 & 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}.$$

Bestem afbildningens kerne K_f og angiv en basis for denne.

Angiv også en basis for billedrummet $f(\mathbb{R}^4)$.

7. Bestem en basis for det underrum i $(\mathbb{R}^4, +, \mathbb{R})$, som udgøres af løsningerne til ligningssystemet

$$x_1 + x_2 - x_3 - x_4 = 0$$

$$x_1 - x_2 + x_3 - x_4 = 0,$$

og angiv samtlige løsninger.

Angiv også samtlige løsninger til ligningssystemet

$$x_1 + x_2 - x_3 - x_4 = 2$$

$$x_1 - x_2 + x_3 - x_4 = 0.$$

8. Find de (reelle) tal a , for hvilke ligningssystemet

$$x + 2y + z = a$$

$$3x + 4y + 2z = a - 3$$

$$-4x + 2y + z = 2$$

Har en løsning $(x, y, z) \in \mathbb{R}^3$, og angiv for hvert sådant tal a samtlige løsninger til ligningssystemet.

§ 4. Volumen og determinanter.Definition af volumenmål.

Et parallelogram ABCD i planen er på nær parallelforskydning bestemt ved de to geometriske vektorer $\underline{u}_1 = \vec{AB}$ og $\underline{u}_2 = \vec{AD}$, der siges at udspænde det. Parallelogrammets areal er en reel funktion F af vektorerne $\underline{u}_1$ og $\underline{u}_2$. Simple geometriske sætninger viser, at der for vilkårlige vektorer $\underline{u}_1, \underline{u}_2$, vilkårlige reelle tal λ_1, λ_2 og vilkårlige reelle tal $\lambda \geq 0$ gælder

$$(1) \quad F(\underline{u}_1, \underline{u}_2 + \lambda_1 \underline{u}_1) = F(\underline{u}_1 + \lambda_2 \underline{u}_2, \underline{u}_2) = F(\underline{u}_1, \underline{u}_2),$$

$$(2) \quad F(\lambda \underline{u}_1, \underline{u}_2) = F(\underline{u}_1, \lambda \underline{u}_2) = \lambda F(\underline{u}_1, \underline{u}_2).$$

Det har vist sig at være hensigtsmæssigt, at skelne mellem de af vektorparrene $(\underline{u}_1, \underline{u}_2)$ og $(\underline{u}_2, \underline{u}_1)$ udspændte parallelogrammer. Til et par $(\underline{u}_1, \underline{u}_2)$ af lineært uafhængige vektorer lader man svare omløbsretningen bestemt ved den korteste drejning, der fører den første vektors retning over i den andens. Er der valgt en orientering af planen, altså en omløbsretning, som regnes som den positive, tilskrives det af $(\underline{u}_1, \underline{u}_2)$ udspændte parallelogram positivt eller negativt areal, efter som den ved $(\underline{u}_1, \underline{u}_2)$ bestemte omløbsretning stemmer overens med eller er modsat planens orientering. Man har da

$$F(\underline{u}_2, \underline{u}_1) = -F(\underline{u}_1, \underline{u}_2),$$

og man ser let, at (2) nu er gyldig for alle reelle tal λ .

I det sædvanlige rum udspænder tre geometriske vektorer $\underline{u}_1, \underline{u}_2, \underline{u}_3$ et paralleløpipedum. Dettets volumen er lig med den absolute værdi af rumproduktet $[\underline{u}_1, \underline{u}_2, \underline{u}_3]$. Selve rumproduktet er volumenet regnet med fortegn. Hvis $\underline{u}_1, \underline{u}_2, \underline{u}_3$ er lineært uafhængige, er det positivt eller negativt, efter som $\underline{u}_1, \underline{u}_2, \underline{u}_3$ taget i denne orden er i højre- eller venstrestilling. At orientere rummet vil sige at vælge mellem højreskruing og venstreskruing og regne de valgte som den positive. Sædvanligvis vælges højreskru-

ning. Dette valg indgår i vektorproduktets og dermed i rumproduktets definition. Man tilskriver altså et parallelepipedum udspændt af vektorsættet $(\underline{u}_1, \underline{u}_2, \underline{u}_3)$ positivt eller negativt volumen, efter som den ved sættet bestemte skruning, den korteste drejning, der fører retningen af $\underline{u}_1$ over i retningen af $\underline{u}_2$, sammen med forskydning i retningen af $\underline{u}_3$, stemmer overens med eller er modsat rummets orientering.

AF rumproduktets egenskaber eller også direkte slutes, at der for funktionen $F(\underline{u}_1, \underline{u}_2, \underline{u}_3) = [\underline{u}_1 \underline{u}_2 \underline{u}_3]$ gælder de til (1) og (2) analoge ligninger, (2) for alle reelle tal λ . Endvidere ses, at $F(\underline{u}_1, \underline{u}_2, \underline{u}_3)$ skifter fortegn ved ombytning af to af vektorerne $\underline{u}_1, \underline{u}_2, \underline{u}_3$.

Det følgende går ud på at generalisere volumenbegrebet til vilkårlige endeligdimensionale vektorrum.

Lad $(V, +, L)$ være et vektorrum af den endelige dimension n . En funktion $F: V^n \rightarrow L$ kaldes et volumenmål i V , hvis den opfylder følgende betingelser:

VOL1: For hvert sæt $(\underline{u}_1, \dots, \underline{u}_n) \in V^n$, hvert $\lambda \in L$ og $i, j = 1, \dots, n$, $i \neq j$, gælder

$$F(\underline{u}_1, \dots, \underline{u}_i + \lambda \underline{u}_j, \dots, \underline{u}_j, \dots, \underline{u}_n) = F(\underline{u}_1, \dots, \underline{u}_i, \dots, \underline{u}_j, \dots, \underline{u}_n).$$

VOL2: For hvert sæt $(\underline{u}_1, \dots, \underline{u}_n) \in V^n$, hvert $\lambda \in L$ og $i = 1, \dots, n$ gælder

$$F(\underline{u}_1, \dots, \lambda \underline{u}_i, \dots, \underline{u}_n) = \lambda F(\underline{u}_1, \dots, \underline{u}_i, \dots, \underline{u}_n).$$

VOL3: Der findes et sæt $(\underline{u}_1, \dots, \underline{u}_n) \in V^n$, for hvilket

$$F(\underline{u}_1, \dots, \underline{u}_n) \neq 0.$$

At der for hvert vektorrum findes en funktion, der opfylder kravene, er ikke oplagt og vil blive bevist nedenfor. Vi begynder med at drage konklusioner af VOL1-2.

Volumenmål og alternarende n-linearformer.

I det følgende forudsættes, at $F: V^n \rightarrow L$ er en funktion, der opfylder VOL1-2. For vilkårlige vektorer $\underline{u}_i, \underline{u}_i', \underline{u}_i'', i = 1, \dots, n$, fra V gælder da:

(I) $F(\underline{u}_1, \dots, \underline{u}_i, \dots, \underline{u}_n)$ ændres ikke, når der til $\underline{u}_i$ adderes en vilkårlig linearkombination af de øvrige vektorer $\underline{u}_1, \dots, \underline{u}_{i-1}, \underline{u}_{i+1}, \dots, \underline{u}_n$.

Bevis: Ifølge VOL1 kan linearkombinationens led ét efter ét adderes til $\underline{u}_i$, uden at værdien af F ændres.

(II) $F(\underline{u}_1, \dots, \underline{u}_{i-1}, \underline{0}, \underline{u}_{i+1}, \dots, \underline{u}_n) = 0$.

Bevis: Ifølge VOL2 for $\lambda = 0$ har man

$$\begin{aligned} F(\underline{u}_1, \dots, \underline{0}, \dots, \underline{u}_n) &= F(\underline{u}_1, \dots, 0\underline{0}, \dots, \underline{u}_n) \\ &= 0F(\underline{u}_1, \dots, \underline{0}, \dots, \underline{u}_n) = 0. \end{aligned}$$

(III) Hvis sættet $(\underline{u}_1, \dots, \underline{u}_n)$ er lineært afhængigt, er

$$F(\underline{u}_1, \dots, \underline{u}_n) = 0.$$

Bevis: Forudsætningen er ensbetydende med, at en af vektorerne, $\underline{u}_i$, er en linearkombination af de øvrige. Ifølge (I) kan denne linearkombination trækkes fra $\underline{u}_i$, uden at værdien af F ændres. Da $\underline{u}_i$ herefter er erstattet med $\underline{0}$, følger påstanden af (II).

Som specielt tilfælde fremhæves:

(III') Hvis to af vektorerne $\underline{u}_1, \dots, \underline{u}_n$ stemmer overens, er

$$F(\underline{u}_1, \dots, \underline{u}_n) = 0.$$

(IV) For hver permutation p af $\{1, \dots, n\}$ gælder

$$F(\underline{u}_{p(1)}, \dots, \underline{u}_{p(n)}) = \text{sgn } p \cdot F(\underline{u}_1, \dots, \underline{u}_n).$$

Bevis: Idet hver permutation kan sammensættes af transpositioner, og en sådan har fortegnet -1 , er det tilstrækkeligt at

vise, at $F(\underline{u}_1, \dots, \underline{u}_n)$ skifter fortegn, når to af vektorerne, $\underline{u}_i$ og $\underline{u}_j$, $i < j$, ombyttes. Ved at anvende VOL1 tre gange og dernæst VOL2 fås

$$\begin{aligned} F(\dots, \underline{u}_j, \dots, \underline{u}_i, \dots) &= F(\dots, \underline{u}_j - \underline{u}_i, \dots, \underline{u}_i, \dots) \\ &= F(\dots, \underline{u}_j - \underline{u}_i, \dots, \underline{u}_i + (\underline{u}_j - \underline{u}_i), \dots) \\ &= F(\dots, \underline{u}_j - \underline{u}_i, \dots, \underline{u}_j, \dots) \\ &= F(\dots, (\underline{u}_j - \underline{u}_i) - \underline{u}_j, \dots, \underline{u}_j, \dots) \\ &= F(\dots, -\underline{u}_i, \dots, \underline{u}_j, \dots) \\ &= -F(\dots, \underline{u}_i, \dots, \underline{u}_j, \dots) . \end{aligned}$$

$$\begin{aligned} (V) \quad &F(\underline{u}_1, \dots, \underline{u}_i' + \underline{u}_i'', \dots, \underline{u}_n) \\ &= F(\underline{u}_1, \dots, \underline{u}_i', \dots, \underline{u}_n) + F(\underline{u}_1, \dots, \underline{u}_i'', \dots, \underline{u}_n) . \end{aligned}$$

Bevis: Er $\underline{u}_1, \dots, \underline{u}_{i-1}, \underline{u}_{i+1}, \dots, \underline{u}_n$ lineært afhængige, følger påstanden af (III). Er disse vektorer lineært uafhængige, suppleres de med en vektor $\underline{e}$ til en basis for vektorrummet V . Man har da fremstillinger

$$\underline{u}_i' = \lambda' \underline{e} + \dots , \quad \underline{u}_i'' = \lambda'' \underline{e} + \dots ,$$

hvor $\lambda', \lambda'' \in L$, og hvor prikkerne står for linearkombinationer af $\underline{u}_1, \dots, \underline{u}_{i-1}, \underline{u}_{i+1}, \dots, \underline{u}_n$. Efter indsættelse for $\underline{u}_i'$ og $\underline{u}_i''$ kan disse linearkombinationer ifølge (I) trækkes fra uden ændring af de pågældende værdier af F . Påstanden reduceres derved til

$$\begin{aligned} &F(\underline{u}_1, \dots, \lambda' \underline{e} + \lambda'' \underline{e}, \dots, \underline{u}_n) \\ &= F(\underline{u}_1, \dots, \lambda' \underline{e}, \dots, \underline{u}_n) + F(\underline{u}_1, \dots, \lambda'' \underline{e}, \dots, \underline{u}_n) . \end{aligned}$$

og at dette er rigtigt, følger af VOL2, idet man på venstre side kan sætte $\lambda' + \lambda''$ og i leddene på højre side henholdsvis λ' og λ'' uden for F .

Tilsammen udsiger (V) og VOL2, at $F(\underline{u}_1, \dots, \underline{u}_n)$ for faste $\underline{u}_1, \dots, \underline{u}_{i-1}, \underline{u}_{i+1}, \dots, \underline{u}_n$ er en linearform defineret på V med $\underline{u}_i$ som variabel vektor. Man kalder en funktion af et givet antal p af vektorvariable og med værdier i L , altså en funktion $G: V^p \rightarrow L$,

en multilinearform eller, når man vil fremhæve antallet af variable vektorer, en p-linearform (for $p = 2$ bilinearform), hvis den, betragtet som funktion af hver af vektorerne for sig, er en linearform på V . En multilinearform $G(\underline{u}_1, \dots, \underline{u}_p)$, som har værdien 0, når to af vektorerne $\underline{u}_1, \dots, \underline{u}_p$ stemmer overens, siges at være alternerende. Idet (III') gælder for funktionerne, der opfylder VOL 1-2, er disse alternerende n -linearformer.

Der gælder også det omvendte, dvs. en funktion $F: V^n \rightarrow L$, for hvilken (V), VOL2 og (III') gælder, opfylder også VOL1. For en sådan funktion har man nemlig

$$\begin{aligned} & F(\underline{u}_1, \dots, \underline{u}_i + \lambda \underline{u}_j, \dots, \underline{u}_j, \dots, \underline{u}_n) \\ &= F(\underline{u}_1, \dots, \underline{u}_i, \dots, \underline{u}_j, \dots, \underline{u}_n) + F(\underline{u}_1, \dots, \lambda \underline{u}_j, \dots, \underline{u}_j, \dots, \underline{u}_n) \\ &= F(\underline{u}_1, \dots, \underline{u}_i, \dots, \underline{u}_j, \dots, \underline{u}_n) + \lambda F(\underline{u}_1, \dots, \underline{u}_j, \dots, \underline{u}_j, \dots, \underline{u}_n) \\ &= F(\underline{u}_1, \dots, \underline{u}_i, \dots, \underline{u}_j, \dots, \underline{u}_n) . \end{aligned}$$

Tager vi VOL3 i betragtning, har vi altså vist:

Volumenmålene i et n -dimensionalt vektorrum $(V, +, L)$ er identiske med de fra konstanten 0 forskellige alternerende n -linearformer på V .

Definition af determinant.

Lad der være givet en $(n \times n)$ -matrix $\underline{A} = (a_{ij})$, $a_{ij} \in L$. For et vilkårligt sæt $(\underline{u}_1, \dots, \underline{u}_n)$ af vektorer i V betragtes de n linearkombinationer

$$\underline{v}_j = \sum_{i=1}^n a_{ij} \underline{u}_i, \quad j = 1, \dots, n.$$

Disse danner et nyt sæt

$$(\underline{v}_1 \dots \underline{v}_n) = (\underline{u}_1 \dots \underline{u}_n) \underline{A}.$$

Er $F: V^n \rightarrow L$ en n -linearform, fås ved gentagen anvendelse af (V) og VOL2

$$\begin{aligned}
 F(\underline{v}_1, \dots, \underline{v}_n) &= F\left(\sum_{i_1=1}^n a_{i_1} \underline{u}_{i_1}, \dots, \sum_{i_n=1}^n a_{i_n} \underline{u}_{i_n}\right) \\
 &= \sum_{i_1=1}^n \dots \sum_{i_n=1}^n a_{i_1} \dots a_{i_n} F(\underline{u}_{i_1}, \dots, \underline{u}_{i_n}) .
 \end{aligned}$$

Forudsættes nu, at F er alternerende, forsvinder alle de led i den n -dobbelte sum, hvor (mindst) to af mærkerne $i_1, \dots, i_n$ har samme værdi, idet den sidste faktor da er 0 ifølge (III'). Det er altså tilstrækkeligt at udstrække summationen over de mærkesæt $(i_1, \dots, i_n)$, som består af indbyrdes forskellige numre, dvs. over alle permutationer $\begin{pmatrix} 1 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix}$ af $\{1, \dots, n\}$. Tager man (IV) i betragtning, får man altså

$$F(\underline{v}_1, \dots, \underline{v}_n) = \sum_{p \in S_n} \text{sgn } p \, a_{p(1)1} \dots a_{p(n)n} F(\underline{u}_1, \dots, \underline{u}_n) ,$$

hvor p betegner en permutation af $\{1, \dots, n\}$ og S_n den symmetriske gruppe af graden n .

Ligningen viser, at $F(\underline{v}_1, \dots, \underline{v}_n)$ fås af $F(\underline{u}_1, \dots, \underline{u}_n)$ ved multiplikation med et tal, som kun afhænger af matricen $\underline{A}$. Det kaldes denne talmatrixes determinant og betegnes

$$\det \underline{A} = \det(\underline{a}_{|1}, \dots, \underline{a}_{|n}) = \begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} ,$$

hvor $\underline{a}_{|1}, \dots, \underline{a}_{|n}$ er søjlerne i $\underline{A}$. Determinanten er altså defineret ved

$$\det \underline{A} = \sum_{p \in S_n} \text{sgn } p \, a_{p(1)1} \dots a_{p(n)n}$$

(G.W. Leibniz, 1678). Summen på højre side har $n!$ led. Hvert af disse er et med et vist fortegn forsynet produkt af n af matrixens elementer, nemlig ét fra hver søjle, således at også hver række er repræsenteret netop én gang.

Herefter kan den ovenfor fundne egenskab ved en alternerende n -linearform F formuleres således:

(VI) Er $(\underline{u}_1, \dots, \underline{u}_n)$ et vilkårligt n -sæt af vektorer i det n -dimensionale vektorrum $(V, +, L)$ og $\underline{A} = (a_{ij})$ en vilkårlig $(n \times n)$ -matrix med elementer fra L , gælder for det ved matrixligningen

$$(\underline{v}_1 \dots \underline{v}_n) = (\underline{u}_1 \dots \underline{u}_n) \underline{A}$$

bestemte vektorsæt $(\underline{v}_1, \dots, \underline{v}_n)$

$$F(\underline{v}_1, \dots, \underline{v}_n) = \det \underline{A} F(\underline{u}_1, \dots, \underline{u}_n) .$$

Af determinanternes egenskaber fremhæves foreløbig to, som følger umiddelbart af definitionen:

1° En kvadratisk matrix $\underline{A}$ og dens transponerede $\underline{A}'$ har samme determinant:

$$\det \underline{A}' = \det \underline{A} .$$

Bevis: Ifølge definition er

$$\det \underline{A}' = \sum_{q \in S_n} \text{sgn } q \, a_{1q(1)} \cdots a_{nq(n)} .$$

Da faktorernes orden i de enkelte led er ligegyldig, kan de ordnes efter søjlenumret. Rækkenumrene vil da optræde i den orden, der bestemmes ved den til q inverse permutation $p = q^{-1}$. Man kan altså skrive

$$\det \underline{A}' = \sum_{q \in S_n} \text{sgn } q \, a_{p(1)1} \cdots a_{p(n)n} .$$

Men da q og $q^{-1} = p$ har samme fortegn, og da $p = q^{-1}$ gennemløber hele gruppen S_n , når q gør det, er summen på højre side lig med $\det \underline{A}$.

2° Determinanten af en øvre eller nedre trekantsmatrix er lig med produktet af elementerne i hoveddiagonalen.

Bevis: Ifølge 1° er det tilstrækkeligt at betragte en øvre trekantsmatrix $\underline{A} = (a_{ij})$, hvor altså $a_{ij} = 0$ for $i > j$. Ved hver fra den identiske forskellig permutation p af $\{1, \dots, n\}$ findes der mindst ét nummer j , således at $p(j) > j$, nemlig det laveste, for hvilket $p(j) \neq j$. Hvert led af determinanten, som svarer til en fra den identiske forskellig permutation, indeholder således mindst én faktor $a_{p(j)j}$, der er lig 0. For determinanten fås altså $a_{11}a_{22}\dots a_{nn}$ som påstået.

Volumenmålets entydighed og eksistens.

I et n -dimensionalt vektorrum $(V, +, L)$ findes et og kun ét volumenmål, som for en given basis for V antager en given værdi $k \neq 0$. (H. Grassmann, 1844, K. Weierstrass, 1864.)

Bevis: Lad $(\underline{e}_1, \dots, \underline{e}_n)$ være den givne basis og $(\underline{u}_1, \dots, \underline{u}_n)$ et vilkårligt n -sæt af vektorer. Med $\underline{U}$ betegnes $(n \times n)$ -matricen, hvis søjler $\underline{u}_1, \dots, \underline{u}_n$ er koordinatsættene for $\underline{u}_1, \dots, \underline{u}_n$ med hensyn til basen $(\underline{e}_1, \dots, \underline{e}_n)$. Hvis der findes et volumenmål F , som opfylder det stillede krav, må dets værdi for $(\underline{u}_1, \dots, \underline{u}_n)$ ifølge (VI) være

$$F(\underline{u}_1, \dots, \underline{u}_n) = \det \underline{U} F(\underline{e}_1, \dots, \underline{e}_n) = k \det \underline{U}.$$

Dette viser, at hvis der overhovedet findes et sådant volumenmål, kan det kun være den ved

$$(\underline{u}_1, \dots, \underline{u}_n) \rightarrow k \det \underline{U}$$

bestemte funktion $G: V^n \rightarrow L$.

Påstanden om eksistensen går herefter ud på, at den således definerede funktion G faktisk er et volumenmål, hvis værdi for $(\underline{e}_1, \dots, \underline{e}_n)$ er k . Da $\det \underline{E} = 1$ ifølge 2°, er

$$G(\underline{e}_1, \dots, \underline{e}_n) = k \det \underline{E} = k,$$

altså det sidste krav og, idet $k \neq 0$, også VOL 3 opfyldt. Det er derfor tilstrækkeligt at vise, at G er en alternerende n -linearform.

I hvert af de $n!$ led af $\det \underline{U}$ findes, som nævnt, netop én faktor, der er element i den j -te søjle $\underline{u}|_j$ af $\underline{U}$. Man kan altså skrive

$$\det \underline{U} = u_{1j} U_{1j} + \dots + u_{nj} U_{nj},$$

hvor koefficienterne $U_{1j}, \dots, U_{nj}$ kun afhænger af elementerne i søjlerne $\underline{u}|_1, \dots, \underline{u}|_{j-1}, \underline{u}|_{j+1}, \dots, \underline{u}|_n$. Idet $\underline{u}|_j$ er koordinatsættet for $\underline{u}_j$, viser dette, at

$$G(\underline{u}_1, \dots, \underline{u}_n) = k \det \underline{U}$$

for faste $\underline{u}_1, \dots, \underline{u}_{j-1}, \underline{u}_{j+1}, \dots, \underline{u}_n$ er en linearform som funktion af $\underline{u}_j$.

At vise, at G er alternerende, kommer ud på at vise, at $\det \underline{U} = 0$, når to søjler $\underline{u}|_i$ og $\underline{u}|_j$, $i < j$, stemmer overens. For de to givne naturlige tal i og j , $1 \leq i < j \leq n$, inddeles permutationerne af $\{1, \dots, n\}$ i to klasser. I den første, S'_n , regnes de permutationer p , for hvilke $p(i) < p(j)$, og til den anden, S''_n , de permutationer q , for hvilke $q(i) > q(j)$. Ved $p \rightarrow q = p \circ \begin{pmatrix} i & j \\ j & i \end{pmatrix}$ bestemmes en enentydig korrespondance mellem S'_n og S''_n , hvor permutationer p og q , der svarer til hinanden, har modsat fortegn. Man kan derfor skrive

$$\det \underline{U} = \sum_{p \in S'_n} \text{sgn } p (u_{p(1)1} \dots u_{p(n)n} - u_{q(1)1} \dots u_{q(n)n}),$$

hvor $q = p \cdot \begin{pmatrix} i & j \\ j & i \end{pmatrix}$. Nu er

$$\begin{aligned} & u_{q(1)}1 \cdots u_{q(i)}i \cdots u_{q(j)}j \cdots u_{q(n)}n \\ &= u_{p(1)}1 \cdots u_{p(j)}i \cdots u_{p(i)}j \cdots u_{p(n)}n \\ &= u_{p(1)}1 \cdots u_{p(i)}i \cdots u_{p(j)}j \cdots u_{p(n)}n, \end{aligned}$$

idet $u_{p(j)}i = u_{p(j)}j$ og $u_{p(i)}j = u_{p(i)}i$. Alle led i ovenstående sum er altså lig 0.

Dermed er sætningen bevist.

Uden forudsætningen $k \neq 0$ havde vi fået resultatet:

I et n-dimensionalt vektorrum $(V, +, L)$ findes en og kun én alternerende n-linearform, som for en given basis for V antager en given værdi k .

En alternerende n-linearform, der antager værdien 0 blot for én basis, må derfor være identisk 0. Som modstykke til III har vi således:

Er F et volumenmål i et n-dimensionalt vektorrum, da er $F(\underline{u}_1, \dots, \underline{u}_n) \neq 0$ for ethvert lineært uafhængigt sæt $(\underline{u}_1, \dots, \underline{u}_n)$.

Volumenmålene i et n-dimensionalt vektorrum er da de funktioner $F: V^n \rightarrow L$, som, efter valg af en vilkårlig basis

$(\underline{e}_1, \dots, \underline{e}_n)$ for rummet, kan skrives

$$F(\underline{u}_1, \dots, \underline{u}_n) = k \det \underline{U},$$

hvor $(\underline{u}_1, \dots, \underline{u}_n)$ og $\underline{U}$ er sammenknyttet ved

$$(\underline{u}_1, \dots, \underline{u}_n) = (\underline{e}_1, \dots, \underline{e}_n) \underline{U},$$

medens k er en konstant $\neq 0$. Der er således uendelig mange volumenmål, men de er indbyrdes proportionale.

Sætninger om determinanter.

Determinanten af en $(n \times n)$ -matrix $\underline{A}$, betragtet som funktion af sættet $(\underline{a}_1, \dots, \underline{a}_n)$ af søjlerne i $\underline{A}$, er det volumenmål i talrummet $(L^n, +, L)$, som antager værdien 1 for sættet af enhedsmatricens søjler. Af egenskaber ved volumenmål fås altså egenskaber ved matrixers determinanter. Ifølge den ovenfor beviste sætning 1°, hvorefter $\det \underline{A}' = \det \underline{A}$, kan matrixens rækker træde i stedet for søjlerne. Man får således:

3° En kvadratisk matrices determinant forbliver uændret, når der til en af matrixens søjler (rækker) adderes en linearkombination af de andre søjler (rækker).

4° Multipliseres én af søjlerne (rækkerne) i en kvadratisk matrix med et tal, vil matrixens determinant multipliceres med samme tal.

Det bemærkes, at dette for en $(n \times n)$ -matrix $\underline{A}$ og et tal λ medfører

$$\det(\lambda \underline{A}) = \lambda^n \det \underline{A}.$$

5° Er én af søjlerne (rækkerne) i en kvadratisk matrix $\underline{A}$ en sum af to søjler (rækker),

$$\underline{a}_{|i} = \underline{a}_{|i}^{\prime} + \underline{a}_{|i}^{\prime\prime} \quad (\underline{a}_{i-} = \underline{a}_{i-}^{\prime} + \underline{a}_{i-}^{\prime\prime}),$$

vil matrixens determinant være summen af determinanterne hørende til de to matricer, der fremgår af $\underline{A}$ ved at erstatte den i-te søjle (række) med henholdsvis $\underline{a}_{|i}^{\prime}$ ($\underline{a}_{i-}^{\prime}$) og $\underline{a}_{|i}^{\prime\prime}$ ($\underline{a}_{i-}^{\prime\prime}$).

Tilsammen udsiger 4° og 5°, at determinanten, betragtet som funktion af en enkelt søjle (række), er en linearform.

6° Hvis søjlerne (rækkerne) i en kvadratisk matrix er lineært afhængige, specielt hvis en af søjlerne (rækkerne) er nulsøjlen (nulrækken) eller to af søjlerne (rækkerne) stemmer overens, er matrixens determinant lig 0.

Endvidere gælder multiplikationssætningen for determinanter:

7° Determinanten af et produkt af to $(n \times n)$ -matricer er lig med produktet af de to matricers determinanter.

Bevis: Lad $\underline{A}$ og $\underline{B}$ være vilkårlige $(n \times n)$ -matricer med elementer fra tallegemet L . Med F betegnes det volumenmål i talrummet $(L^n, +, L)$, som for en valgt basis $(\underline{e}_1, \dots, \underline{e}_n)$ antager værdien 1. Sættes

$$(\underline{u}_1 \dots \underline{u}_n) = (\underline{e}_1 \dots \underline{e}_n) \underline{A},$$

$$(\underline{v}_1 \dots \underline{v}_n) = (\underline{u}_1 \dots \underline{u}_n) \underline{B},$$

fås ved gentagen anvendelse af (VI)

$$F(\underline{v}_1, \dots, \underline{v}_n) = F(\underline{u}_1, \dots, \underline{u}_n) \det \underline{B} = \det \underline{A} \det \underline{B}.$$

Idet

$$(\underline{v}_1 \dots \underline{v}_n) = (\underline{e}_1 \dots \underline{e}_n) \underline{AB},$$

fås også

$$F(\underline{v}_1, \dots, \underline{v}_n) = \det(\underline{AB}) ,$$

hvilket viser, at

$$\det(\underline{AB}) = \det \underline{A} \det \underline{B} .$$

Er $\underline{A}$ en regulær matrix, slutes af $\underline{AA}^{-1} = \underline{E}$ og $\det \underline{E} = 1$, at

$$\det \underline{A} \det \underline{A}^{-1} = 1 ,$$

altså:

8° Indbyrdes inverse regulære matrixer har indbyrdes reciproke determinanter.

Heraf aflæses endvidere, at en regulær matrices determinant er forskellig fra 0. Sammen med 6° giver dette:

9° En kvadratisk matrix er regulær, hvis og kun hvis dens determinant er forskellig fra 0.

Lad $\underline{A}$ være en vilkårlig (ikke nødvendigvis kvadratisk) talmatrix. Determinanten af en $(p \times p)$ -delmatrix af $\underline{A}$ kaldes en underdeterminant af p-te orden af $\underline{A}$.

En tidligere sætning (side III, 2, 38-39) og 9° giver følgende sætning om rangen af en matrix:

Rangen r af en matrix, som ikke er nulmatrix, er det største af de naturlige tal p, for hvilke matrixen har en fra 0 forskellig underdeterminant af p-te orden.

For en ortogonal matrix, dvs. en kvadratisk matrix $\underline{A}$, for hvilken $\underline{A}'\underline{A} = \underline{E}$, har man

$$(\det \underline{A})^2 = \det \underline{A} \det \underline{A} = \det(\underline{A}'\underline{A}) = 1 ,$$

altså: Determinanten af en ortogonal matrix er 1 eller -1.

For en unitær matrix, dvs. en kvadratisk matrix $\underline{A}$, for hvilken $\overline{\underline{A}}' \underline{A} = \underline{E}$, har man

$$|\det \underline{A}|^2 = \overline{\det \underline{A}} \det \underline{A} = \det \overline{\underline{A}}' \det \underline{A} = \det(\overline{\underline{A}}' \underline{A}) = 1,$$

altså: Determinanten af en unitær matrix har den absolutte værdi 1.

Determinants udvikling. Bestemmelse af invers matrix.

Lad $\underline{A} = (a_{ij})$ være en $(n \times n)$ -matrix med elementer fra et tallegeme. Er K og M ikke-tomme delmængder af mængden $N = \{1, 2, \dots, n\}$, betegnes med $\underline{A}_{K,M}$ den delmatrix af $\underline{A}$, hvis rækkenumre og søjlenumre er elementerne i K hhv. M . To sådanne delmatrixer $\underline{A}_{K_1, M_1}$ og $\underline{A}_{K_2, M_2}$ siges at være komplementære, der M både mængderne K_1 og K_2 , og mængderne M_1 og M_2 er komplementære delmængder af N .

Lad nu I og J være fast valgte ikke-tomme komplementære delmængder af N ,

$$I = \{i_1, i_2, \dots, i_k\}, \quad i_1 < i_2 < \dots < i_k,$$

$$J = \{j_1, j_2, \dots, j_l\}, \quad j_1 < j_2 < \dots < j_l.$$

Sættes

$$P = \{\pi \in S_n \mid \pi(i_1) < \dots < \pi(i_k) \wedge \pi(j_1) < \dots < \pi(j_l)\},$$

gælder Laplace's udvikling:

$$(1) \quad \det \underline{A} = \sum_{\pi \in P} \operatorname{sgn} \pi \det \underline{A}_{I, \pi(I)} \det \underline{A}_{J, \pi(J)},$$

hvor

$$\operatorname{sgn} \pi = (-1)^{i_1 + \dots + i_k + \pi(i_1) + \dots + \pi(i_k)}$$

$$(2) \quad = (-1)^{j_1 + \dots + j_l + \pi(j_1) + \dots + \pi(j_l)}.$$

Formlen (1) viser, at $\det \underline{A}$ kan udregnes som en sum af produkter af formen $\pm \det \underline{A}_{I,K_1} \det \underline{A}_{J,K_2}$, hvor $\underline{A}_{I,K_1}$ og $\underline{A}_{J,K_2}$ er komplementære kvadratiske delmatricer af $\underline{A}$ med rækkenumre i I hhv. J ; det er klart, at hvert af de $\binom{n}{k}$ sådanne par af delmatricer giver netop ét bidrag til summen.

Det bemærkes, at (1) anvendt på $\underline{A}'$ giver

$$\det \underline{A} = \sum_{\pi \in P} \operatorname{sgn} \pi \det \underline{A}_{\pi(I), I} \det \underline{A}_{\pi(J), J},$$

idet en kvadratisk matrix har samme determinant som den transponerede matrix.

Bevis for (1).

For $\underline{a}_j = (a_{1j}, a_{2j}, \dots, a_{nj}) \in L^n$, $j = 1, 2, \dots, n$, sættes

$$G(\underline{a}_1, \underline{a}_2, \dots, \underline{a}_n) = \sum_{\pi \in P} \operatorname{sgn} \pi \det \underline{A}_{I, \pi(I)} \det \underline{A}_{J, \pi(J)},$$

hvor $\underline{A}$ er matricen $(a_{ij})_{i=1,2,\dots,n; j=1,2,\dots,n}$. Det påstås, at G er et volumenmål med $G(\underline{e}_1, \underline{e}_2, \dots, \underline{e}_n) = 1$, hvor $\underline{e}_1 = (1, 0, \dots, 0)$, $\underline{e}_2 = (0, 1, 0, \dots, 0)$, $\dots$, $\underline{e}_n = (0, \dots, 0, 1)$. Da det på forhånd vides, at den ved

$$F(\underline{a}_1, \underline{a}_2, \dots, \underline{a}_n) = \det \underline{A}$$

definerede afbildning F er det eneste volumenmål i $(L^n, +, L)$, som på sættet $(\underline{e}_1, \underline{e}_2, \dots, \underline{e}_n)$ antager værdien 1, vil (1) hermed være bevist.

Ifølge kendte sætninger om determinanter er for hvert $\pi \in P$ den ved

$$G_\pi(\underline{a}_1, \underline{a}_2, \dots, \underline{a}_n) = \operatorname{sgn} \pi \det \underline{A}_{I, \pi(I)} \det \underline{A}_{J, \pi(J)}$$

definerede afbildning G_π en n -linearform. Da summen af endelig

mange n -linearformer oplagt er en n -linearform sluttes, at G er en n -linearform.

Det skal herefter vises, at G er alternerende. Lad i sættet $(\underline{a}_1, \underline{a}_2, \dots, \underline{a}_n)$ vektoren $\underline{a}_r$ være identisk med vektoren $\underline{a}_s$, hvor $r < s$. Er $\pi \in P$ en permutation med $r \in \pi(I)$ og $s \in \pi(I)$, eller $r \in \pi(J)$ og $s \in \pi(J)$, fås $\text{sgn } \pi \det \underline{A}_{\pi(I)} \det \underline{A}_{\pi(J)} = 0$, thi determinanten af en matrix med to ens søjler er 0. De øvrige permutationer i P deles i to klasser Q' og Q'' , hvor Q' indeholder de $\pi' \in P$ for hvilke $r \in \pi'(I)$ og $s \in \pi'(J)$, og Q'' indeholder de $\pi'' \in P$ for hvilke $r \in \pi''(J)$ og $s \in \pi''(I)$. Idet der for enhver delmængde M af $N = \{1, 2, \dots, n\}$ med k elementer findes netop et $\pi \in P$ med $\pi(I) = M$, og dermed $\pi(J) = N \setminus M$, findes til hvert $\pi' \in Q'$ et og kun ét $\pi'' \in Q''$ med

$$(3) \quad \begin{aligned} \pi''(I) &= (\pi'(I) \setminus \{r\}) \cup \{s\}, \\ \pi''(J) &= (\pi'(J) \setminus \{s\}) \cup \{r\}, \end{aligned}$$

og den herved definerede afbildning af Q' ind i Q'' er bijektiv. Vi får følgelig

$$\begin{aligned} &G(\underline{a}_1, \underline{a}_2, \dots, \underline{a}_n) \\ &= \sum_{\pi' \in Q'} (\text{sgn } \pi' \det \underline{A}_{\pi'(I)} \det \underline{A}_{\pi'(J)} + \\ &\quad \text{sgn } \pi'' \det \underline{A}_{\pi''(I)} \det \underline{A}_{\pi''(J)}) , \end{aligned}$$

hvor for hvert $\pi' \in Q'$ permutationen π'' er det ved (3) bestemte element af Q'' . Det er derfor tilstrækkeligt at vise, at

$$\begin{aligned} &\text{sgn } \pi'' \det \underline{A}_{\pi''(I)} \det \underline{A}_{\pi''(J)} \\ &= -\text{sgn } \pi' \det \underline{A}_{\pi'(I)} \det \underline{A}_{\pi'(J)} \end{aligned}$$

for ethvert $\pi' \in Q'$.

Vi bemærker først, at er π_1 en vilkårlig permutation i P , t en transposition, som ombytter to elementer af $\pi_1(I)$, og sættes $\pi_2 = t \circ \pi_1$, gælder

$$\begin{aligned} & \operatorname{sgn} \pi_1 \det \underline{A}_{I, \pi_1}(I) \det \underline{A}_{J, \pi_1}(J) \\ &= \operatorname{sgn} \pi_2 \det \underline{A}_{I, \pi_2}(I) \det \underline{A}_{J, \pi_2}(J); \end{aligned}$$

thi $\operatorname{sgn} \pi_2 = -\operatorname{sgn} \pi_1$, $\underline{A}_{J, \pi_2}(J) = \underline{A}_{J, \pi_1}(J)$, $\det \underline{A}_{I, \pi_2}(I) = -\det \underline{A}_{I, \pi_1}(I)$, idet $\underline{A}_{I, \pi_2}(I)$ fremgår af $\underline{A}_{I, \pi_1}(I)$ ved ombytning af to søjler. Tilsvarende gælder, hvis t ombytter to elementer af $\pi_1(J)$.

Det er klart, at sættet $(\pi''(i_1), \dots, \pi''(i_k))$ fremgår af sættet $(\pi'(i_1), \dots, \pi'(i_k))$ ved først at fjerne elementet r , dernæst rykke de af de efterfølgende elementer, som er $< s$, én position til venstre, og endelig indføje s på den herved ledigblevne position. Tilsvarende fremgår sættet $(\pi''(j_1), \dots, \pi''(j_l))$ af sættet $(\pi'(j_1), \dots, \pi'(j_l))$ ved først at fjerne elementet s , dernæst rykke de af de foranstående elementer, som er $> r$, én position til højre, og endelig indføje r på den herved ledigblevne position. Sammensættes derfor π'' successivt fra venstre, dels med transpositioner, som ombytter s med naboen til venstre i sættet $(\pi''(i_1), \dots, \pi''(i_k))$, indtil s er placeret i den position, som indtages af elementet r i sættet $(\pi'(i_1), \dots, \pi'(i_k))$, og dels med transpositioner, som ombytter r med naboen til højre i sættet $(\pi''(j_1), \dots, \pi''(j_l))$, indtil r er placeret i den position, som indtages af elementet s i sættet $(\pi'(j_1), \dots, \pi'(j_l))$, fås som resultat permutationen $\pi = \begin{pmatrix} r & s \\ s & r \end{pmatrix} \circ \pi'$. Ved gentagen anvendelse af bemærkningen ovenfor ses, at

$$\begin{aligned} & \operatorname{sgn} \pi'' \det \underline{A}_{\underline{I}, \pi''(I)} \det \underline{A}_{\underline{J}, \pi''(J)} \\ &= \operatorname{sgn} \pi \det \underline{A}_{\underline{I}, \pi(I)} \det \underline{A}_{\underline{J}, \pi(J)}. \end{aligned}$$

Endvidere har vi åbenbart $\operatorname{sgn} \pi = -\operatorname{sgn} \pi'$, samt

$\det \underline{A}_{\underline{I}, \pi(I)} = \det \underline{A}_{\underline{I}, \pi'(I)}$ og $\det \underline{A}_{\underline{J}, \pi(J)} = \det \underline{A}_{\underline{J}, \pi'(J)}$, thi $\underline{a}|_r = \underline{a}|_s$ i $\underline{A}$. Dette giver ved indsættelse det ønskede.

Vi mangler herefter blot at vise, at

$$\sum_{\pi \in P} \operatorname{sgn} \pi \det \underline{E}_{\underline{I}, \pi(I)} \det \underline{E}_{\underline{J}, \pi(J)} = 1.$$

Betegner e den identiske permutation, fås åbenbart

$$\operatorname{sgn} e \det \underline{E}_{\underline{I}, e(I)} \det \underline{E}_{\underline{J}, e(J)} = 1.$$

Alle øvrige bidrag til summen er imidlertid 0; thi er

$\pi \in P \setminus \{e\}$, findes et $i \in I$ med $\pi(i) \notin I$, og dermed en 0-søjle i $\underline{E}_{\underline{I}, \pi(I)}$.

Bevis for (2).

Det påstås, at $\pi \in P$ kan fremstilles som sammensætning af

$$\sum_{\nu=1}^k (\pi(i_\nu) + i_\nu - 2\nu)$$

transpositioner. Da dette tal er kongruent modulo 2 med

$$\sum_{\nu=1}^k (\pi(i_\nu) + i_\nu),$$

og da det åbenbart er tilstrækkeligt at vise rigtigheden af det første lighedstegn, følger (2) heraf. - I sættet $(1, 2, \dots, n)$ kan $\pi(i_1)$ føres til første position, mens alle øvrige elementer bevarer deres indbyrdes rækkefølge, ved $\pi(i_1)-1$ ombytninger. Derefter kan $\pi(i_2)$ føres til anden position ved $\pi(i_2)-2$ ombytninger, etc. Herved fås efter ialt

$$\sum_{\nu=1}^k (\pi(i_\nu) - \nu)$$

ombytninger $\pi(i_\nu)$ på ν -te position for $\nu = 1, 2, \dots, k$. Idet resten af elementerne har bevaret deres indbyrdes rækkefølge, har sættet herefter udseendet

$$(\pi(i_1), \pi(i_2), \dots, \pi(i_k), \pi(j_1), \pi(j_2), \dots, \pi(j_e)).$$

I dette sæt kan nu $\pi(i_k)$ ved i_k -k ombytninger føres til den i_k -te position, dernæst $\pi(i_{k-1})$ ved $i_{k-1}-(k-1)$ ombytninger til den i_{k-1} -te position, etc. Herved fås efter ialt

$$\sum_{\nu=1}^k (i_\nu - \nu)$$

ombytninger elementerne $\pi(i_\nu)$ på i_ν -te position for $\nu = 1, 2, \dots, k$. Da de øvrige elementer har bevaret deres indbyrdes rækkefølge, har vi også $\pi(j_\mu)$ på j_μ -te position, $\mu = 1, 2, \dots, l$. Vi har altså efter ialt

$$\sum_{\nu=1}^k (\pi(i_\nu) - \nu) + \sum_{\nu=1}^k (i_\nu - \nu) = \sum_{\nu=1}^k (\pi(i_\nu) + i_\nu - 2\nu)$$

ombytninger fået sættet $(1, 2, \dots, n)$ ført over i sættet $(\pi(1), \pi(2), \dots, \pi(n))$. Heraf fremgår, at permutationen π som påstået kan sammensættes af dette antal transpositioner.

Et vigtigt specielt tilfælde af Laplace's udvikling fås ved at vælge et fast $i \in \{1, 2, \dots, n\}$ og sætte

$$I = \{i\}, \quad J = \{1, \dots, i-1, i+1, \dots, n\}.$$

Vi får da

$$P = \{\pi \in S_n \mid \pi(1) < \dots < \pi(i-1) < \pi(i+1) < \dots < \pi(n)\},$$

og, for $\pi \in P$,

$$\text{sgn } \pi = (-1)^{i+\pi(i)}.$$

Idet vi med $\underline{A}_{\neq k; \neq l}$ betegner den delmatrix af $\underline{A}$, som fås ved i $\underline{A}$ at slette k -te række og l -te søjle, får vi endvidere

$$\underline{\underline{A}}_{I, \pi(I)} = (a_{i, \pi(i)})$$

og

$$\underline{\underline{A}}_{J, \pi(J)} = \underline{\underline{A}}_{\cancel{I}; \cancel{\pi(I)}},$$

hvor $(a_{i, \pi(i)})$ er en (1×1) -matrix. Ved indsættelse i (1) får vi derefter

$$\det \underline{\underline{A}} = \sum_{j=1}^n (-1)^{i+j} a_{ij} \det \underline{\underline{A}}_{\cancel{I}; \cancel{J}}.$$

Udtrykket $(-1)^{i+j} \det \underline{\underline{A}}_{\cancel{I}; \cancel{J}}$ kaldes komplementet til elementet a_{ij} , og betegnes A_{ij} . Vi får da

$$(4) \quad \det \underline{\underline{A}} = \sum_{j=1}^n a_{ij} A_{ij}.$$

Denne fremstilling af $\det \underline{\underline{A}}$ kaldes determinantens udvikling efter den i-te række. Ved anvendelse af (4) på $\underline{\underline{A}}'$ fås, idet $\det \underline{\underline{A}}' = \det \underline{\underline{A}}$, determinantens udvikling efter den j-te søjle,

$$(5) \quad \det \underline{\underline{A}} = \sum_{i=1}^n a_{ij} A_{ij}.$$

Erstattes i $\underline{\underline{A}}$ elementerne i den j-te søjle med elementerne i den k-te, hvor $k \neq j$, og udvikles determinanten af den herved fremkomne matrix efter den j-te søjle, fås

$$0 = \sum_{i=1}^n a_{ik} A_{ij},$$

idet determinanten af en matrix med to ens søjler er 0.

Sammenholdes dette med (5) ses, at der gælder

$$(A_{ij})'(a_{ij}) = (A_{ij})'\underline{\underline{A}} = (\det \underline{\underline{A}})\underline{\underline{E}}.$$

Er $\underline{\underline{A}}$ regulær, altså $\det \underline{\underline{A}} \neq 0$, fås

$$\left(\frac{A_{ij}}{\det \underline{\underline{A}}} \right)' \underline{\underline{A}} = \underline{\underline{E}},$$

hvoraf sluttes, at

$$\underline{\underline{A}}^{-1} = \left(\frac{A_{ij}}{\det \underline{\underline{A}}} \right)' .$$

Vi har dermed:

Den inverse til en regulær matrix $\underline{\underline{A}}$ er den transponerede af den matrix, der fås ved at erstatte hvert element i $\underline{\underline{A}}$ med sit komplement divideret med $\det \underline{\underline{A}}$.

Eksempel.

Som eksempel udregnes den såkaldte Vandermonde determinant (N.Vandermonde, 1779, A.Cauchy, 1815)

$$D_n(a_1, \dots, a_n) = \begin{vmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-2} & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{n-2} & a_2^{n-1} \\ \cdot & \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & \cdot & & \cdot & \cdot \\ 1 & a_n & a_n^2 & \dots & a_n^{n-2} & a_n^{n-1} \end{vmatrix}$$

hvor $a_1, \dots, a_n$ er vilkårlige tal. Der gælder

$$D_n(a_1, \dots, a_n) = \prod_{\substack{i, j=1 \\ i < j}}^n (a_j - a_i).$$

Beviset føres ved induktion. Man finder $D_2 = a_2 - a_1$. Antag, at ligningen er rigtig for $n-1 \geq 2$ i stedet for n . Adderes i D_n den $(n-1)$ -te søjle efter multiplikation med $-a_1$ til den sidste, dernæst den $(n-2)$ -te søjle efter multiplikation med $-a_1$ til den

(n-1)-te, ..., den første søjle efter multiplikation med $-a_1$ til den anden, fås ved derefter at udvikle efter den første række

$$\begin{aligned}
 & D_n(a_1, \dots, a_n) \\
 &= \begin{vmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & a_2 - a_1 & a_2(a_2 - a_1) & \dots & a_2^{n-3}(a_2 - a_1) & a_2^{n-2}(a_2 - a_1) \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 1 & a_n - a_1 & a_n(a_n - a_1) & \dots & a_n^{n-3}(a_n - a_1) & a_n^{n-2}(a_n - a_1) \end{vmatrix} \\
 &= \begin{vmatrix} a_2 - a_1 & a_2(a_2 - a_1) & \dots & a_2^{n-3}(a_2 - a_1) & a_2^{n-2}(a_2 - a_1) \\ \vdots & \vdots & & \vdots & \vdots \\ a_n - a_1 & a_n(a_n - a_1) & \dots & a_n^{n-3}(a_n - a_1) & a_n^{n-2}(a_n - a_1) \end{vmatrix} \\
 &= \left(\prod_{j=2}^n (a_j - a_1) \right) D_{n-1}(a_2, \dots, a_n).
 \end{aligned}$$

Ved hjælp af induktionsantagelsen fås da det ønskede resultat.

Differentiation af determinant.

En determinant $\det(u_{ij})$ af en reel $(n \times n)$ -matrix kan opfattes som en funktion $\det: \mathbb{R}^{n^2} \rightarrow \mathbb{R}$ med de n^2 elementer u_{ij} som variable. Som funktion af hver af disse variable u_{ij} for sig er den et førstegradspolynomium, hvor koefficienten til u_{ij} er U_{ij} . For den partielle afledede med hensyn til u_{ij} har man altså

$$\frac{\partial(\det \underline{U})}{\partial u_{ij}} = U_{ij}.$$

Antag, at elementerne u_{ij} i matricen $\underline{U}$ er differentiable funktioner $u_{ij}: J \rightarrow \mathbb{R}$, hvor $J \subseteq \mathbb{R}$ betegner et interval. Idet D betegner differentiation med hensyn til den variable $t \in J$, fås

$$\begin{aligned}
 D \det \underline{U} &= \sum_{i,j=1}^n U_{ij} Du_{ij} \\
 &= \sum_{j=1}^n \sum_{i=1}^n U_{ij} Du_{ij} \\
 &= \sum_{j=1}^n \det(\underline{u}_1, \dots, \underline{u}_{j-1}, Du_{ij}, \underline{u}_{j+1}, \dots, \underline{u}_n).
 \end{aligned}$$

Determinantens afledede er altså summen af determinanterne af de matricer, der fremgår af $\underline{U}$ ved, at én søjle ad gangen erstattes med sin afledede.

Orientering af vektorrum.

Lad $(\underline{u}_1, \dots, \underline{u}_n)$ og $(\underline{v}_1, \dots, \underline{v}_n)$ være lineært uafhængige sæt i et n -dimensionalt vektorrum $(V, +, \cdot)$ over de reelle tals legeme. Idet F er et volumenmål i V , siges $(\underline{u}_1, \dots, \underline{u}_n)$ og $(\underline{v}_1, \dots, \underline{v}_n)$ at være ens orienterede eller modsat orienterede efter som $F(\underline{u}_1, \dots, \underline{u}_n)$ og $F(\underline{v}_1, \dots, \underline{v}_n)$ har samme eller modsat fortegn; da alle volumenmål er indbyrdes proportionale, er definitionen uafhængig af det valgte volumenmål F . Herved inddeles mængden af lineært uafhængige n -sæt af vektorer i V , d.v.s. mængden af baser for V , i to klasser. At orientere V vil sige at udmærke en bestemt af de to klasser; vektorrummet V siges da at være orienteret ved den pågældende klasse. Man kan tale om, at V er orienteret ved et lineært uafhængigt u -sæt $(\underline{u}_1, \dots, \underline{u}_n)$, hvorved menes, at V er orienteret ved den klasse, som indeholder $(\underline{u}_1, \dots, \underline{u}_n)$. Er V orienteret, siges sættene i den udmærkede klasse at være positive eller positivt orienterede, sættene i den anden klasse siges at være negative eller negativt orienterede.

To baser $(\underline{e}_1, \dots, \underline{e}_n)$ og $(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n)$ er ens eller modsat orienterede efter som den tilhørende koordinattransformationsmatrix $\underline{\underline{S}}$ har positiv eller negativ determinant. Thi af

$$(\underline{e}_1 \dots \underline{e}_n) = (\hat{\underline{e}}_1 \dots \hat{\underline{e}}_n) \underline{\underline{S}}$$

følger

$$F(\underline{e}_1, \dots, \underline{e}_n) = \det \underline{\underline{S}} F(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n)$$

for ethvert volumenmål F .

Ved valg af en basis i et orienteret vektorrum vil man oftest vælge en positivt orienteret basis. Ved valg af et volumenmål vælges gerne et, der er positivt på de positive sæt; er der allerede valgt en positiv basis $(\underline{e}_1, \dots, \underline{e}_n)$, vælges gerne det volumenmål F for hvilket $F(\underline{e}_1, \dots, \underline{e}_n) = 1$.

Hvis vektorrummet er forsynet med et indre produkt, $(\underline{e}_1, \dots, \underline{e}_n)$ er en positiv ortonormal basis, og F er bestemt ved at $F(\underline{e}_1, \dots, \underline{e}_n) = 1$, så gælder $F(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n) = 1$ for enhver positiv ortonormal basis $(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n)$. Betegner vi nemlig med $\underline{\underline{S}}$ den tilhørende koordinattransformationsmatrix, har vi som ovenfor

$$(*) \quad F(\underline{e}_1, \dots, \underline{e}_n) = \det \underline{\underline{S}} F(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n).$$

Matricen $\underline{\underline{S}}$ er åbenbart ortogonal, hvormed $|\det \underline{\underline{S}}| = 1$ (jf. side 12). Idet $(\underline{e}_1, \dots, \underline{e}_n)$ og $(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_n)$ er ens orienterede, har vi endvidere $\det \underline{\underline{S}} > 0$, og dermed $\det \underline{\underline{S}} = 1$. Påstanden følger da ved indsætning i (*).

Når der tales om volumenmålet i et orienteret vektorrum med indre produkt, menes det, der har værdien 1 for de positive ortonormale baser.

Er (U, U') et ordnet par af komplementære underrum af et n -dimensionalt orienteret vektorrum $(V, +, \hat{R})$, siges orienteringen af U og U' at være sammenhørende, hvis en positiv basis for U efterfulgt af en positiv basis for U' giver en positiv basis for V .

Dette finder hyppig anvendelse, når V er forsynet med et indre produkt, U er en hyperplan, d.v.s. et underrum af dimension $n-1$, og U' dennes ortogonale komplement, altså dens normal. Er V orienteret, hører der altså til hver orientering af U en orientering af normalen. Den således orienterede normal kaldes den orienterede hyperplans positive normal (jf. definitionen af vektorproduktet af to vektorer i det tredimensionale geometriske vektorrum).

Volumen og lineære afbildninger.

Lad $(\underline{u}_1, \dots, \underline{u}_n)$ være et n -sæt af vektorer i et n -dimensionalt vektorrum $(V, +, \hat{R})$, og lad delmængden P af V være defineret ved

$$P = \left\{ \sum_{i=1}^n t_i \underline{u}_i \mid 0 \leq t_i \leq 1, \quad i = 1, \dots, n \right\}.$$

Knytter vi til P sættet $(\underline{u}_1, \dots, \underline{u}_n)$, vil vi kalde P et orienteret parallellotop, og vi vil da sige, at P er udspændt af sættet $(\underline{u}_1, \dots, \underline{u}_n)$.

Er nu F et volumenmål i V , kan vi tilskrive ethvert orienteret parallellotop P et volumenmåltal ("volumen"), nemlig tallet $F(\underline{u}_1, \dots, \underline{u}_n)$, hvor P er udspændt af sættet $(\underline{u}_1, \dots, \underline{u}_n)$. Herved fås den ønskede generalisation af begreberne "areal af parallelogram" og "volumen af parallellepipedum" til vilkårlige endelig-dimensionale vektorrum over $\hat{R}$ (jf. side 2).

Lad $(U, +, \cdot)$ og $(V, +, \cdot)$ være to n -dimensionale vektorrum og f en lineær afbildning af U på V . Er $(\underline{e}_1, \dots, \underline{e}_n)$ en basis for U , og vælges $(\underline{f}_1, \dots, \underline{f}_n)$, hvor $\underline{f}_i = f(\underline{e}_i)$, som basis for V , vil tilsvarende vektorer $\underline{u}$ og $\underline{v} = f(\underline{u})$ i de to vektorrum have ens koordinatsæt. Er $(\underline{u}_1, \dots, \underline{u}_n)$ et n -sæt af vektorer i U , $(\underline{v}_1, \dots, \underline{v}_n)$ sættet af billedvektorer og $\underline{U}$ matricen, hvis søjler er koordinatsættene for vektorerne $\underline{u}_i$, har vi altså

$$(\underline{u}_1 \dots \underline{u}_n) = (\underline{e}_1 \dots \underline{e}_n) \underline{U}$$

og

$$(\underline{v}_1 \dots \underline{v}_n) = (\underline{f}_1 \dots \underline{f}_n) \underline{U}.$$

For et volumenmål F i U og et volumenmål G i V fås følgelig

$$F(\underline{u}_1, \dots, \underline{u}_n) = \det \underline{U} F(\underline{e}_1, \dots, \underline{e}_n)$$

og

$$G(\underline{v}_1, \dots, \underline{v}_n) = \det \underline{U} G(\underline{f}_1, \dots, \underline{f}_n),$$

hvormed

$$(*) \quad G(\underline{v}_1, \dots, \underline{v}_n) = \frac{G(\underline{f}_1, \dots, \underline{f}_n)}{F(\underline{e}_1, \dots, \underline{e}_n)} F(\underline{u}_1, \dots, \underline{u}_n).$$

Idet vi ved billedet af det orienterede parallellotop udspændt af sættet $(\underline{u}_1, \dots, \underline{u}_n)$ forstår det orienterede parallellotop udspændt af sættet $(f(\underline{u}_1), \dots, f(\underline{u}_n))$, følger af (*), at forholdet mellem volumenet af et orienteret parallellotops billede og volumenet af selve parallellotopet er uafhængigt af det betragtede parallellotop. Heraf sluttet videre, at forholdet mellem volumenerne af to orienterede parallellotoper i U er lig med forholdet mellem volumenerne af de to billedparallellotoper; man kan udtrykke dette ved at sige, at volumenforholdet er invariant ved lineære afbildninger.

Er specielt $U = V$, altså f en lineær afbildning af U på sig selv, og $F = G$, kan vi slutte

$$\frac{G(\underline{f}_1, \dots, \underline{f}_n)}{F(\underline{e}_1, \dots, \underline{e}_n)} = \frac{F(\underline{f}_1, \dots, \underline{f}_n)}{F(\underline{e}_1, \dots, \underline{e}_n)} = \det \underline{A},$$

hvor $\underline{A}$ er matricen hørende til f med hensyn til basen $(\underline{e}_1, \dots, \underline{e}_n)$.

Thi af

$$(\underline{f}_1 \ \dots \ \underline{f}_n) = (\underline{e}_1 \ \dots \ \underline{e}_n) \underline{A}$$

følger

$$(**) \quad F(\underline{f}_1, \dots, \underline{f}_n) = \det \underline{A} \ F(\underline{e}_1, \dots, \underline{e}_n).$$

Indsættes i (*) fås

$$F(\underline{v}_1, \dots, \underline{v}_n) = \det \underline{A} \ F(\underline{u}_1, \dots, \underline{u}_n).$$

Forholdet mellem volumenet af et orienteret parallellotops bilde og volumenet af selve parallellotopet er altså ikke alene uafhængigt af det betragtede parallellotop, men også af det betragtede volumenmål. Endvidere er det klart, at forholdet er uafhængigt af den valgte basis, - hvilket iøvrigt kan bekræftes ved anvendelse af 7° og 8°, idet matricen $\underline{A}$ ved koordinatskifte erstattes med en matrix af formen $\underline{S} \underline{A} \underline{S}^{-1}$. Tallet $\det \underline{A}$ kaldes afbildningens determinant eller dens volumenfaktor. Af (**) aflæses, at baserne $(\underline{e}_1, \dots, \underline{e}_n)$ og $(\underline{f}_1, \dots, \underline{f}_n)$ bestemmer samme eller modsat orientering af U efter som $\det \underline{A}$ er positiv eller negativ; dette kan udtrykkes ved at sige, at afbildningen bevarer eller skifter vektorrummets orientering efter som volumenfaktoren er positiv eller negativ.

Som tidligere omtalt (side III,2,25) danner de regulære $(n \times n)$ -matricer med elementer fra $\mathbb{R}$ en gruppe med matrixmultiplikation som komposition. Gruppen kaldes den generelle lineære gruppe af grad n over $\mathbb{R}$, og betegnes $GL(n, \mathbb{R})$. Man overbeviser sig let om, at de matricer, hvis determinant er positiv, danner en undergruppe $GL^+(n, \mathbb{R})$, samt at de matricer, hvis determinant er 1, danner en undergruppe $SL(n, \mathbb{R})$; gruppen $SL(n, \mathbb{R})$ kaldes den specielle lineære gruppe af grad n over $\mathbb{R}$. Er $(U, +, \mathbb{R})$ et n -dimensionalt vektorrum, og vælges i U en basis, så fås en isomorfi mellem gruppen af bijektive lineære afbildninger af U på sig selv og $GL(n, \mathbb{R})$ ved til en lineær afbildning at lade svare den tilhørende matrix med hensyn til den valgte basis. Ved denne isomorfi svarer til gruppen $GL^+(n, \mathbb{R})$ gruppen af lineære afbildninger med positiv volumenfaktor, de såkaldte orienteringsbevarende afbildninger. Til gruppen $SL(n, \mathbb{R})$ svarer gruppen af lineære afbildninger med volumenfaktor 1, de såkaldte volumentro afbildninger.

§ 11. Determinanter og lineære ligningssystemer.

Løsningerne til vilkårlige lineære ligningssystemer kan angives ved hjælp af determinanter.

Lad $(V_m, +, L)$ være et m -dimensionalt vektorrum, $\underline{a}_1, \dots, \underline{a}_m$ lineært uafhængige vektorer og $\underline{b}$ en vilkårlig vektor i V_m . Idet $(\underline{a}_1, \dots, \underline{a}_m)$ er en basis for V_m , har ligningen

$$x_1 \underline{a}_1 + \dots + x_m \underline{a}_m = \underline{b}$$

en og kun een løsning $(x_1, \dots, x_m) \in L^m$. Er F et volumenmål i V_m , fås ved hjælp af VOL 1-2 (side III, 10, 10)

$$\begin{aligned} F(\underline{a}_1, \dots, \underline{a}_{i-1}, \underline{b}, \underline{a}_{i+1}, \dots, \underline{a}_m) \\ &= F(\underline{a}_1, \dots, \underline{a}_{i-1}, x_1 \underline{a}_1 + \dots + x_m \underline{a}_m, \underline{a}_{i+1}, \dots, \underline{a}_m) \\ &= F(\underline{a}_1, \dots, \underline{a}_{i-1}, x_i \underline{a}_i, \underline{a}_{i+1}, \dots, \underline{a}_m) \\ &= x_i F(\underline{a}_1, \dots, \underline{a}_{i-1}, \underline{a}_i, \underline{a}_{i+1}, \dots, \underline{a}_m). \end{aligned}$$

Idet $F(\underline{a}_1, \dots, \underline{a}_m) \neq 0$, giver dette for ligningens løsning

$$x_i = \frac{F(\underline{a}_1, \dots, \underline{a}_{i-1}, \underline{b}, \underline{a}_{i+1}, \dots, \underline{a}_m)}{F(\underline{a}_1, \dots, \underline{a}_{i-1}, \underline{a}_i, \underline{a}_{i+1}, \dots, \underline{a}_m)}, \quad i = 1, \dots, m.$$

Anvendes dette specielt på talrummet $(L^m, +, L)$, fås for et lineært ligningssystem

$$\begin{array}{rcl} a_{11}x_1 + \dots + a_{1m}x_m & = & b_1 \\ \vdots & & \vdots \\ a_{m1}x_1 + \dots + a_{mm}x_m & = & b_m \end{array}$$

med en regulær $(m \times m)$ -koefficientmatrix $\underline{A}$ løsningen

$$x_i = \frac{\det(\underline{a}_{|1}, \dots, \underline{a}_{|i-1}, \underline{b}, \underline{a}_{|i+1}, \dots, \underline{a}_{|m})}{\det \underline{A}}, \quad i = 1, \dots, m.$$

Den i -te ubekendte er altså en brøk, hvis nævner er koefficientmatrixens determinant, og hvis tæller er determinanten hørende til matricen, som fås ved i koefficientmatricen at erstatte den

i-te søjle med søjlen bestående af ligningernes højre sider.

De fundne udtryk for de ubekendte kaldes Cramers formler.

For et vilkårligt lineært ligningssystem

$$\begin{array}{rcl} a_{11}x_1 + \dots + a_{1n}x_n & = & b_1 \\ \vdots & & \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n & = & b_m \end{array}$$

kan opgaven at finde de eventuelle løsninger føres tilbage til det ovenfor behandlede specielle tilfælde. En nødvendig og tilstrækkelig betingelse for eksistensen af løsninger er øjensynlig, at søjlen $\underline{b}_1$ tilhører det af koefficientmatricens søjler $\underline{a}_{|1}, \dots, \underline{a}_{|n}$ udspændte underrum i L^m , og dette er ensbetydende med, at rangen af sættet $(\underline{a}_{|1}, \dots, \underline{a}_{|n})$ ikke forøges, når $\underline{b}_1$ tilføjes:

$$\text{rg}(\underline{a}_{|1}, \dots, \underline{a}_{|n}, \underline{b}_1) = \text{rg}(\underline{a}_{|1}, \dots, \underline{a}_{|n}).$$

Der foreligger altså i første række opgaven at bestemme rangen af en vilkårlig matrix. Herom gælder:

Lad $\underline{A}$ være en fra nulmatricen forskellig $(m \times n)$ -matrix med elementer fra tallegemet L . Da er $\text{rg } \underline{A}$ lig med det største positive hele tal p , for hvilket der findes en fra 0 forskellig underdeterminant af p -te orden i $\underline{A}$.

Bevis: Man betragter en $(p \times p)$ -delmatrix af $\underline{A}$, hvis determinant er forskellig fra 0. Dens p søjler er da lineært uafhængige. Disse søjler er enten tillige søjler i $\underline{A}$ (nemlig hvis $p = m$) eller dele af søjler i $\underline{A}$ (nemlig hvis $p < m$). De pågældende p søjler i $\underline{A}$ må da også være lineært uafhængige; thi lineært afhængige søjler forbliver lineært afhængige, når der slettes rækker i dem. Dette viser, at der for rangen r af $\underline{A}$ må gælde $r \geq p$. For at bevise den omvendte ulighed benyttes, at

en matrices rækkerang er lig med dens søjlerang. I en delmatrix af $\underline{A}$, som udgøres af r lineært uafhængige rækker, må der altså findes r lineært uafhængige søjler. Disse udgør en regulær $(r \times r)$ -delmatrix af $\underline{A}$, og da dens determinant er forskellig fra 0, må $p \geq r$, altså $p = r$, som påstået.

Koefficientmatricen $\underline{A}$ for ligningssystemet har altså en fra 0 forskellig underdeterminant af ordenen r . For overskuelighedens skyld antages at søjlerne, og dermed de ubekendte, er nummereret således, at denne underdeterminant er indeholdt i de r første søjler. Endvidere antages, at rækkerne er nummereret, altså ligningerne ordnet således, at underdeterminanten er indeholdt i de r første rækker. Dette kommer ud på antagelsen, at

$$\begin{vmatrix} a_{11} & \cdots & a_{1r} \\ \vdots & & \vdots \\ a_{r1} & \cdots & a_{rr} \end{vmatrix} \neq 0.$$

De r første af ligningerne skrives da

$$\begin{array}{ccccccc} a_{11}x_1 + \cdots + a_{1r}x_r & = & b_1 & - & a_{1,r+1}x_{r+1} & - \cdots & - a_{1n}x_n \\ \vdots & & \vdots & & \vdots & & \vdots \\ a_{r1}x_1 + \cdots + a_{rr}x_r & = & b_r & - & a_{r,r+1}x_{r+1} & - \cdots & - a_{rn}x_n. \end{array}$$

For vilkårligt opgivne værdier af $x_{r+1}, \dots, x_n$ har dette ligningssystem en og kun een løsning $(x_1, \dots, x_r)$, som ifølge Cramers formler er givet ved

$$x_i = \frac{\det(\hat{a}_{|1}, \dots, \hat{a}_{|i-1}, \hat{b}_{|i}, -\hat{a}_{|i,r+1}x_{r+1} - \cdots - \hat{a}_{|i,n}x_n, \hat{a}_{|i+1}, \dots, \hat{a}_{|r})}{\det(\hat{a}_{|1}, \dots, \hat{a}_{|r})}$$

for $i = 1, \dots, r$. Her betegner $\hat{a}_{|1}, \dots, \hat{a}_{|n}$ de til de r første elementer afkortede søjler $\underline{a}_{|1}, \dots, \underline{a}_{|n}$ i koefficientmatricen $\underline{A}$ og $\hat{b}_{|i}$ den tilsvarende afkortede søjle $\underline{b}_{|i}$ af de højre sider i

det oprindelige ligningssystem. De fundne værdier for $x_1, \dots, x_r$ sammen med de opgivne $x_{r+1}, \dots, x_n$ tilfredsstiller det oprindelige ligningssystem's r første ligninger. Det skal vises, at de også tilfredsstiller de øvrige $m-r$.

Da de r første rækker i $\underline{A}$ er lineært uafhængige, vil de r første rækker i den, med ligningernes højre sider udvidede matrix $(\underline{A} \ \underline{b}_|)$ også være lineært uafhængige. Nu har denne matrix ifølge forudsætning den samme rang r som $\underline{A}$. Følgelig er dens $m-r$ sidste rækker linearkombinationer af de r første. Men dette betyder, at man kan få hver af de $m-r$ sidste ligninger ved at addere de med passende tal fra L multiplicerede r første ligninger. Hvert talsæt $(x_1, \dots, x_n)$, som tilfredsstiller de r første ligninger, vil følgelig også tilfredsstille de øvrige. Dermed er den fremsatte påstand bevist.

Sammenfattende kan altså siges:

Et lineært ligningssystem $\underline{A}\underline{x}_| = \underline{b}_|$, hvor $\underline{A}$ er en given $(m \times n)$ -matrix, $\underline{b}_|$ en given $(m \times 1)$ -matrix og $\underline{x}_|$ en $(n \times 1)$ -matrix, hvis elementer er de ubekendte, har mindst een løsning $(x_1, \dots, x_n)$, hvis og kun hvis

$$r = \text{rg } \underline{A} = \text{rg}(\underline{A} \ \underline{b}_|).$$

Er denne betingelse opfyldt, har systemet de samme løsninger som et delsystem bestående af r ligninger udvalgt således, at dets $(r \times n)$ -koefficientmatrix $\hat{\underline{A}}$ har en fra 0 forskellig underdeterminant af r -te orden. Samtlige løsninger fås da ved at tildele de $n-r$ ubekendte, hvis tilhørende søjler i $\hat{\underline{A}}$ ikke optræder i underdeterminanten, vilkårlige værdier og dernæst at bestemme de resterende r ubekendte ved hjælp af Cramers formler.

Betingelsen for et systems løsbarhed kan bringes på en anden, tit hensigtsmæssig form. Lad

$$k_1 \underline{a}_{1-} + \dots + k_m \underline{a}_{m-} = \underline{0-}$$

være en lineær relation mellem rækkerne $\underline{a}_{1-}, \dots, \underline{a}_{m-}$ i koefficientmatricen $\underline{A}$. Antages nu, at systemet har en løsning $(x_1, \dots, x_n)$, og multipliceres den første ligning med $k_1, \dots$, den m -te ligning med k_m , fås ved påfølgende addition af ligningerne

$$0x_1 + \dots + 0x_n = k_1 b_1 + \dots + k_m b_m.$$

Dette viser, at følgende er en nødvendig betingelse for, at systemet har en løsning: Enhver lineær relation, der består mellem linearformerne på ligningernes venstre sider, tilfredsstilles også af de højre sider. Denne betingelse er også tilstrækkelig, hvilket ses således: Et delsystem bestående af r ligninger med lineært uafhængige venstre sider (koefficientrækker) har i hvert fald mindst en løsning. Lad disse ligningers koefficientrækker f.eks. være $\underline{a}_{1-}, \dots, \underline{a}_{r-}$. Hver af de øvrige ligningers koefficientrække er da en linearkombination af disse, og dens højre side er, hvis betingelsen er opfyldt, den samme linearkombination af $b_1, \dots, b_r$. Hver af de øvrige ligninger kan altså fås som en linearkombination af de r valgte, og vil derfor tilfredsstilles af disses løsninger.

For at undersøge de (side III, 11, 3) fundne løsninger nærmere, omskrives udtrykket for x_i ved at benytte, at determinanten i tælleren, hvis i -te søjle er en sum af $n-r+1$ søjler, kan skrives som en sum af lige så mange determinanter. Dette giver

$$x_i = k_i + \sum_{j=1}^{n-r} c_{ij} x_{r+j}, \quad i = 1, \dots, r,$$

hvor

$$K_i = \frac{\det(\hat{\underline{a}}_1, \dots, \hat{\underline{a}}_{i-1}, \hat{\underline{b}}, \hat{\underline{a}}_{i+1}, \dots, \hat{\underline{a}}_r)}{\det(\hat{\underline{a}}_1, \dots, \hat{\underline{a}}_r)}$$

$$c_{ij} = - \frac{\det(\hat{\underline{a}}_1, \dots, \hat{\underline{a}}_{i-1}, \hat{\underline{a}}_{r+j}, \hat{\underline{a}}_{i+1}, \dots, \hat{\underline{a}}_r)}{\det(\hat{\underline{a}}_1, \dots, \hat{\underline{a}}_r)}.$$

Indføres desuden betegnelserne

$$t_j = x_{r+j} \quad j = 1, \dots, n-r,$$

kan løsningerne skrives

$$\begin{aligned} x_1 &= k_1 + c_{11}t_1 + c_{12}t_2 + \dots + c_{1,n-r}t_{n-r} \\ &\vdots \\ x_r &= k_r + c_{r1}t_1 + c_{r2}t_2 + \dots + c_{r,n-r}t_{n-r} \\ x_{r+1} &= t_1 \\ &\vdots \\ x_n &= t_{n-r} \end{aligned}$$

hvor $t_1, \dots, t_{n-r}$ er parametre, der uafhængigt af hinanden kan gennemløbe L . Dette skrives kortere

$$\underline{x}_i = \underline{k}_i + \underline{c}_{i1}t_1 + \dots + \underline{c}_{i,n-r}t_{n-r}, \quad (t_1, \dots, t_{n-r}) \in L^{n-r},$$

hvor der er sæt

$$\underline{k}_i = \begin{pmatrix} k_1 \\ \vdots \\ k_r \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \underline{c}_{ij} = \begin{pmatrix} c_{1j} \\ \vdots \\ c_{rj} \\ \delta_{1j} \\ \vdots \\ \delta_{n-r,j} \end{pmatrix}, \quad j = 1, \dots, n-r.$$

De $n-r$ søjler $\underline{c}_{ij}$ er lineært uafhængige, da deres $n-r$ sidste rækker udgør $((n-r) \times (n-r))$ -enhedsmatricen. Det ses på ny, at mængden af løsninger er et sideunderrum til et $(n-r)$ -dimensionalt underum i L^n . Søjlen $\underline{k}_i$ er en løsning til det givne ligningssystem, nemlig den, der fremkommer for $t_1 = \dots = t_{n-r} = 0$, og $\underline{c}_{i1}, \dots, \underline{c}_{i,n-r}$ danner en basis for løsningsrummet for det tilsvarende homogene system.

Øvelser til kap. III, §4.

1. I en plan er valgt et begyndelsespunkt O for stedvektorer samt et arealmål F . Idet der er givet to lineært uafhængige vektorer $\underline{a}$ og $\underline{b}$ samt et reelt tal c , betegnes med A , B og C mængden af punkter i planen, hvis stedvektorer $\underline{x}$ tilfredsstiller henholdsvis ligningen

$$F(\underline{a}, \underline{x}) = c, \quad F(\underline{b}, \underline{x}) = c \quad \text{og} \quad F(\underline{a}, \underline{x}) + F(\underline{b}, \underline{x}) = c.$$

Beskriv mængderne A , B og C , og angiv, hvorledes C kan konstrueres, når A og B kendes.

2. I rummet er valgt et volumenmål F . Idet A , B , C og D er hjørner i et tetraeder, skal man vise, at

$$-F(\vec{AB}, \vec{AC}, \vec{AD}) = F(\vec{AB}, \vec{CD}, \vec{PQ}),$$

hvor P er et vilkårligt punkt på linien gennem A og B , og Q et vilkårligt punkt på linien gennem C og D .

3. Udregn den til matricen

$$\begin{pmatrix} 0 & 0 & \dots & 0 & c_1 \\ 0 & 0 & \dots & c_2 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & c_{n-1} & \dots & 0 & 0 \\ c_n & 0 & \dots & 0 & 0 \end{pmatrix}.$$

hørende determinant.

4. Udregn determinanterne

$$\begin{vmatrix} 3 & 0 & 2 & -2 \\ 5 & -1 & 0 & 3 \\ 1 & 2 & 0 & 1 \\ 2 & 4 & -1 & -2 \end{vmatrix}, \quad \begin{vmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{vmatrix}.$$

5. Udregn determinanten

$$\begin{vmatrix} 1 & 2 & 3 & \dots & n \\ n+1 & n+2 & n+3 & \dots & 2n \\ 2n+1 & 2n+2 & 2n+3 & \dots & 3n \\ \vdots & \vdots & \vdots & & \vdots \\ (n-1)n+1 & (n-1)n+2 & (n-1)n+3 & \dots & n^2 \end{vmatrix}.$$

6. I en $(n \times n)$ -matrix er alle elementer i hoveddiagonalen lig med tallet a , og elementerne uden for hoveddiagonalen er alle lig med tallet b . Udregn matrixens determinant. (Begynd f.eks. med at addere de $n-1$ sidste rækker til den første.)

7. Vis, at determinanten for en skævsymmetrisk $(n \times n)$ -matrix er 0, når n er ulige.

8. Vis, at

$$\begin{vmatrix} 0 & a_{12} & a_{13} & a_{14} \\ -a_{12} & 0 & a_{23} & a_{24} \\ -a_{13} & -a_{23} & 0 & a_{34} \\ -a_{14} & -a_{24} & -a_{34} & 0 \end{vmatrix} = (a_{12}a_{34} - a_{13}a_{24} + a_{14}a_{23})^2.$$

9. Udregn determinanten

$$\begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_1 & a_0 \\ -1 & x & 0 & \dots & 0 & 0 \\ 0 & -1 & x & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & x & 0 \\ 0 & 0 & 0 & \dots & -1 & x \end{vmatrix},$$

hvor $a_0, \dots, a_n$ og x er vilkårlige tal.

10. Beregn den inverse til hver af matricerne

$$\begin{pmatrix} 2 & -1 & 0 \\ -3 & 2 & -1 \\ 0 & 1 & 3 \end{pmatrix}, \quad \begin{pmatrix} 2 & 1 & 2 \\ 1 & 2 & 3 \\ 4 & 1 & 2 \end{pmatrix}.$$

11. Vis, at den inverse til en regulær trekantsmatrix igen er en trekantsmatrix, og angiv dennes elementer i hoveddiagonalen.
12. Bestem, under forudsætning af at $c_1, c_2, \dots, c_n$ alle er forskellige fra 0, den inverse til matricen i øvelse 3.
13. I et tredimensionalt vektorrum $(V, +, L)$ benyttes en basis $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$. Bestem de værdier $a \in L$, for hvilke den ved matrixligningen

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \begin{pmatrix} a+1 & 0 & a \\ 1 & a & 1 \\ -1 & -a & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$$

givne lineære afbildning af $(V, +, L)$ ind i sig selv er bijektiv, og find for sådanne a den omvendte afbildnings matrixligning.

14. Vis, at hvis en $(n \times n)$ -matrix (u_{ij}) har rangen $n-1$, vil matricen (U_{ij}) , hvor U_{ij} er komplementet til u_{ij} , have rangen 1. Hvad kan der siges om $\text{rg}(U_{ij})$, når $\text{rg}(u_{ij}) < n-1$?
15. Lad F være et volumenmål i et m -dimensionalt vektorrum $(V, +, L)$ og $(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_m)$ et $(m+1)$ -sæt af vektorer i V med rangen m .

Vis, at ligningen $\sum_{i=0}^m x_i \underline{a}_i = 0$ tilfredsstilles af

$x_i = (-1)^i F(\underline{a}_0, \dots, \underline{a}_{i-1}, \underline{a}_{i+1}, \dots, \underline{a}_m)$, $i = 0, 1, \dots, m$,
og angiv samtlige løsninger $(x_0, x_1, \dots, x_m)$.

Benyt dette til at løse et homogent lineært ligningssystem bestående af m ligninger med $m + 1$ ubekendte, hvis koefficientmatrix har rangen m .

16. Vis, at der findes netop ét reelt polynomium af højst anden grad

$$p(x) = a_0 + a_1 x + a_2 x^2,$$

som for givne indbyrdes forskellige reelle tal x_1, x_2, x_3 antager givne værdier y_1, y_2, y_3 :

$$p(x_1) = y_1, \quad p(x_2) = y_2, \quad p(x_3) = y_3,$$

og anfør udtryk for koefficienterne.

Generaliser til polynomier af højst n -te grad.

17. Tre linier i en plan er givet ved lineære ligninger i henhold til et parallelkoordinatsystem. Opstil ved hjælp af determinanter nødvendige og tilstrækkelige betingelser for, at linierne har et og kun ét punkt fælles.

Løs den tilsvarende opgave for fire planer i rummet.

18. To linier i rummet har i et parallelkoordinatsystem parameterfremstillingerne

$$\begin{aligned} x_1 &= a_1 + su_1 & y_1 &= b_1 + tv_1 \\ x_2 &= a_2 + su_2, \quad s \in \mathbb{R}, & y_2 &= b_2 + tv_2, \quad t \in \mathbb{R}. \\ x_3 &= a_3 + su_3 & y_3 &= b_3 + tv_3 \end{aligned}$$

Angiv ved hjælp af determinanter nødvendige og tilstrækkelige betingelser for, at linierne skærer hinanden, samt under forudsætning af, at disse betingelser er opfyldt, udtryk for skæringspunktets koordinater.

19. Lad

$$a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = b_1$$

$$a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = b_2$$

$$a_{31}x_1 + a_{32}x_2 + a_{33}x_3 = b_3$$

være ligninger i et parallelkoordinatsystem for tre planer i rummet. Med r betegnes rangen af koefficientmatricen (a_{ij}) og med r' rangen af den matrix, der fås ved at tilføje de højre sider b_i som sidste søjle. Angiv de talpar (r, r') , som kan forekomme, og beskriv i hvert af disse tilfælde planernes indbyrdes beliggenhed. (Antag først, at $b_1 = b_2 = b_3 = 0$.)

20. Find rangen af matricen

$$\begin{pmatrix} i & 1+i & 2 & 2-i \\ 2+i & 3 & 3-2i & 2-3i \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

Angiv et maximalsæt af rækker (søjler) og udtryk de øvrige rækker (søjler) som linearkombinationer af disse.

21. Find for hvert talpar (a, b) samtlige løsninger til ligningssystemet

$$ax_1 - bx_2 + ax_3 - bx_4 = -1$$

$$ax_1 + bx_2 - ax_3 + bx_4 = 1$$

$$ax_1 + bx_2 + ax_3 - bx_4 = 0$$

$$ax_1 + bx_2 + ax_3 + bx_4 = 1.$$

§ 5. Egenværdiproblemet. Normalformer.

Invariante underrum.

Lad $(V, +, L)$ være et vilkårligt vektorrum og V' et underrum af V . Vi betragter en lineær afbildning $f: V' \rightarrow V$. Et underrum U af V' siges at være invariant (eller stabilt) ved f , hvis

$$f(U) \subseteq U .$$

Det er klart, at $U = \{0\}$ og kernen $\text{Ker } f$ ved f opfylder dette krav.

Eksempler:

1) Lad $(V', +, L) = (V, +, L)$ være et vilkårligt vektorrum, og lad $f: V \rightarrow V$ være homotetien med multiplikatoren $\alpha \in L$, altså $f(\underline{u}) = \alpha \underline{u}$ for $\underline{u} \in V$. Da er ethvert underrum af V invariant ved f .

2) Lad $(V', +, L) = (V, +, L)$, og antag, at V er direkte sum af to underrum U_1 og U_2 , altså

$$V = U_1 \oplus U_2 .$$

Lad f være parallelprojektion af V på U_1 langs U_2 (jf. side III, 2, 11). Da er underrummet U_1 invariant ved f , da det er kernen ved f , og U_2 er invariant, idet restriktionen af f til U_2 er den identiske afbildning.

3) Lad $(V, +, L)$ være vektorrummet $(\hat{C}(\mathbb{R} \rightarrow \mathbb{R}), +, \mathbb{R})$ bestående af de på $\mathbb{R}$ definerede kontinuerte reelle funktioner og $(V', +, L)$ underrummet $(\hat{C}^1(\mathbb{R} \rightarrow \mathbb{R}), +, \mathbb{R})$ bestående af de kontinuert differentiable blandt disse funktioner. Ved den lineære afbildning $D: V' \rightarrow V$, der til hver funktion $\varphi \in U$ lader svare den afledede

$D\phi \in V$, er bl.a. følgende underrum af V' invariante: det uendelig-dimensionale bestående af alle reelle polynomier, det $(n + 1)$ -dimensionale bestående af alle reelle polynomier af højst n -te grad, det endimensionale frembragt af funktionen e^{at} , hvor a er et givet tal, det uendelig-dimensionale, frembragt af alle funktioner e^{at} , $a \in \mathbb{R}$, det todimensionale frembragt af $\cos$ og $\sin$. Derimod er det endimensionale underrum frembragt af $\cos$ ikke invariant ved D , men det er invariant ved D^2 .

4) Ved drejningen med drejningsvinkel $\frac{1}{2}\pi$ af det todimensionale vektorrum bestående af de geometriske vektorer i en plan er $\{0\}$ og hele vektorrummet de eneste invariante underrum.

Vi betragter igen lineære afbildninger af et underrum V' af et vilkårligt vektorrum V ind i V . Er underrummene U_1 og U_2 af V' invariante ved en sådan afbildning f , vil også $U_1 \cap U_2$ og $U_1 + U_2$ være invariante ved f . For $\underline{u} \in U_1 \cap U_2$ gælder nemlig

$$f(\underline{u}) \in f(U_1) \cap f(U_2) \subseteq U_1 \cap U_2$$

og for $\underline{u}_1 \in U_1$, $\underline{u}_2 \in U_2$

$$f(\underline{u}_1 + \underline{u}_2) = f(\underline{u}_1) + f(\underline{u}_2) \in f(U_1) + f(U_2) \subseteq U_1 + U_2 .$$

Er et underrum U af V' invariant ved de lineære afbildninger f og g af V' ind i V , vil det også være invariant ved αf , hvor $\alpha \in L$, og ved $f + g$, idet

$$\alpha f(U) \subseteq \alpha U \subseteq U ,$$

$$(f + g)(U) \subseteq f(U) + g(U) \subseteq U + U = U .$$

Endelig bemærkes, at hvis et underrum U af $(V, +, L)$ er invariant ved lineære afbildninger f og g af V ind i V , vil det også være invariant ved $g \circ f$.

Lad nu $(V', +, L) = (V, +, L)$ være et vektorrum af den endelige dimension n , og lad f være en lineær afbildning af V ind i V . Efter valg af en basis for V hører der til f en $(n \times n)$ -matrix $\underline{A}$. Hvis et underrum $U_1 \subset V$ af dimension p , $0 < p < n$, er invariant ved f , kan man ved passende valg af basis opnå, at matricen $\underline{A}$ får en $((n - p) \times p)$ -nulmatrix som delmatrix. Vælger man nemlig en basis $(\underline{e}_1, \dots, \underline{e}_p)$ for U_1 og supplerer til en basis $(\underline{e}_1, \dots, \underline{e}_n)$ for V , vil vektorerne i U_1 netop være de vektorer, hvis $n - p$ sidste koordinater er 0. Idet U_1 er invariant ved f , gælder dette for vektorerne $f(\underline{e}_1), \dots, f(\underline{e}_p)$, hvis koordinatsæt er de p første søjler i $\underline{A}$. Heraf sluttes, at $\underline{A}$ må have formen

$$\underline{A} = \begin{pmatrix} \underline{A}_{11} & \underline{A}_{12} \\ \underline{0} & \underline{A}_{22} \end{pmatrix}.$$

Her er $\underline{A}_{11}$ den $(p \times p)$ -matrix, som med hensyn til basen $(\underline{e}_1, \dots, \underline{e}_p)$ hører til restriktionen af f til U_1 .

Er også et til U_1 komplementært underrum U_2 invariant ved f , kan $\underline{e}_{p+1}, \dots, \underline{e}_n$ vælges således, at de danner en basis for U_2 . Matricen antager da formen

$$\underline{A} = \begin{pmatrix} \underline{A}_{11} & \underline{0} \\ \underline{0} & \underline{A}_{22} \end{pmatrix},$$

hvor $((n - p) \times (n - p))$ -matricen $\underline{A}_{22}$ hører til restriktionen af f til U_2 .

Det fremgår heraf, at invariante underrum er af betydning, når det drejer sig om at finde en simpel matrixligning for en given lineær afbildning af et endelig-dimensionalt vektorrum ind i sig selv.

Egenvektorer og egenverdier.

Lad $(V, +, L)$ være et vilkårligt vektorrum og V' et under-
rum af V . Lad endvidere f betegne en lineær afbildning af V' ind
i V . Det kan hændes, at der findes ved f invariante underrum U
med den egenskab, at restriktionen af f til U er en homoteti. Så-
danne underrum er af særlig betydning ved en nærmere undersøgel-
se af f . I det følgende undersøges bl.a. spørgsmålet om eksi-
stensens af sådanne underrum.

Et tal $\lambda \in L$ siges at være en egenverdi for afbildningen
 $f: V' \rightarrow V$, hvis der findes en vektor $\underline{u} \in V'$, således at

$$\underline{u} \neq \underline{0} \wedge f(\underline{u}) = \lambda \underline{u} .$$

Enhver sådan vektor $\underline{u}$ kaldes en til egenverdien λ hørende egen-
vektor.

Sammen med $\underline{0}$ udgør de til en egenverdi λ for f hørende
egenvektorer et underrum i V' . Restriktionen af f til dette er
homotetien med multiplikatoren λ .

Den sidste påstand er oplagt. Den første bekræftes let di-
rekte. Men den følger også umiddelbart af, at egenvektorerne til
 λ netop er de fra $\underline{0}$ forskellige vektorer i kernen

$$K_{\lambda} = \text{Ker}(f - \lambda e)$$

ved den lineære afbildning $f - \lambda e: V' \rightarrow V$, hvor e betegner den
identiske afbildning af V' .

Et tal $\lambda \in L$ er altså egenverdi, hvis og kun hvis afbild-
ningen $f - \lambda e$ ikke er injektiv. Specielt er $\underline{0}$ egenverdi, hvis og
kun hvis f selv ^{ikke} er injektiv.

For hvert $\lambda \in L$ kaldes kernen K_λ ved $f - \lambda e$ for det til λ hørende egenrum og dets dimension $\dim K_\lambda$ for egenværdimultipliciteten af λ . Denne betegnes også $\text{em } \lambda$. At λ er egenværdi for f er ensbetydende med $\text{em } \lambda > 0$.

Eksempler:

1) Homotetien med multiplikatoren α af et vektorrum V af dimension større end 0 har α som eneste egenværdi og det tilhørende egenrum er V selv.

2) Er $V = U_1 \oplus U_2$ og f parallelprojektion af V på U_1 langs U_2 , vil 1 være egenværdi med U_1 som tilhørende egenrum, og 0 vil være egenværdi med U_2 som tilhørende egenrum. Det ses let, at der ikke findes andre egenværdier.

3) Ved den i eksempel 3 (side III, 5, 1-2) betragtede afbildning $D: \hat{C}^1(\mathbb{R} \rightarrow \mathbb{R}) \rightarrow \hat{C}(\mathbb{R} \rightarrow \mathbb{R})$ udgør funktionerne $ce^{\lambda t}$, $c \in \mathbb{R}$, det til λ hørende egenrum, idet disse funktioner netop er løsningerne til differentialligningen $D\phi = \lambda\phi$. Hvert reelt tal λ har således egenværdimultipliciteten 1.

4) Lad $(V, +, \mathbb{R})$ være underrummet af $(\hat{C}(\mathbb{R} \rightarrow \mathbb{R}), +, \mathbb{R})$ bestående af de på $\mathbb{R}$ kontinuerte funktioner med perioden 2π , og lad V' bestå af de to gange kontinuert differentiable blandt disse funktioner. Ved til hver funktion $\phi \in V'$ at lade svare dens anden afledede $D^2\phi$ defineres en lineær afbildning af V' ind i V . For at bestemme dennes egenværdier og "egenfunktioner" løses differentialligningen $D^2\phi = \lambda\phi$ for et vilkårligt givet reelt tal λ . For $\lambda > 0$ er de fra 0 forskellige løsninger ikke periodiske og tilhører derfor ikke V' . Man kan altså antage $\lambda \leq 0$. Sættes $\lambda = -k^2$, hvor $k \geq 0$, kan løsningerne skrives

$$\varphi(t) = c_1 + c_2 t \quad \text{for } k = 0,$$

$$\varphi(t) = c_1 \cos kt + c_2 \sin kt \quad \text{for } k > 0,$$

hvor c_1 og c_2 er arbitrære reelle konstanter. Blandt løsninger-
ne for $k = 0$ er kun konstanterne $\varphi(t) = c_1$ periodiske med pe-
rioden 2π . Idet disse danner et endimensionalt underrum, er
 $\lambda = 0$ egenværdi med multipliciteten 1 og de fra 0 forskellige
konstanter som egenfunktioner. Løsningerne for $k > 0$ er perio-
diske med perioden 2π , hvis og kun hvis k er et naturligt tal.
Tallene $\lambda = -k^2$, $k \in \mathbb{N}$, og kun disse, er altså fra 0 forskel-
lige egenværdier. Egenrummet hørende til $\lambda = -k^2$, $k \in \mathbb{N}$, har
dimensionen 2, idet $\cos kt$ og $\sin kt$ er lineært uafhængige.

Egenvektorer hørende til indbyrdes forskellige egenværdier
for en lineær afbildning f af et underrum V' af vektorrummet
 $(V, +, L)$ ind i V er lineært uafhængige.

Bevis: Beviset føres ved induktion efter antallet p af
betragtede egenværdier. For $p = 1$ er påstanden klar, idet hver
egenvektor er forskellig fra $\underline{0}$. Antag at påstanden er rigtig for
 $p - 1$ egenværdier, og lad $\lambda_1, \dots, \lambda_p$ være indbyrdes forskellige
egenværdier for f og $\underline{u}_1, \dots, \underline{u}_p$ egenvektorer hørende til henholds-
vis $\lambda_1, \dots, \lambda_p$. Er

$$\alpha_1 \underline{u}_1 + \dots + \alpha_{p-1} \underline{u}_{p-1} + \alpha_p \underline{u}_p = \underline{0}$$

en lineær relation mellem disse vektorer, fås

$$\begin{aligned} & f(\alpha_1 \underline{u}_1 + \dots + \alpha_{p-1} \underline{u}_{p-1} + \alpha_p \underline{u}_p) \\ &= \alpha_1 \lambda_1 \underline{u}_1 + \dots + \alpha_{p-1} \lambda_{p-1} \underline{u}_{p-1} + \alpha_p \lambda_p \underline{u}_p = \underline{0}. \end{aligned}$$

Multipliseres den givne relation med λ_p og subtraheres den der-

efter fra den sidste, fås

$$\alpha_1(\lambda_1 - \lambda_p)\underline{u}_1 + \dots + \alpha_{p-1}(\lambda_{p-1} - \lambda_p)\underline{u}_{p-1} = \underline{0}.$$

Ifølge induktionsantagelsen kan heraf sluttes, at

$$\alpha_i(\lambda_i - \lambda_p) = 0 \quad \text{for } i = 1, \dots, p-1,$$

altså, da $\lambda_i - \lambda_p \neq 0$, at

$$\alpha_i = 0 \quad \text{for } i = 1, \dots, p-1.$$

Af den givne relation og $\underline{u}_p \neq \underline{0}$ følger, at også $\alpha_p = 0$. Dermed er sætningen bevist.

Summen af egenrum $K_{\lambda_1}, \dots, K_{\lambda_p}$ hørende til indbyrdes forskellige egenverdier $\lambda_1, \dots, \lambda_p$ for en lineær afbildning f af et underrum V' af vektorrummet $(V, +, L)$ ind i V er direkte.

Bevis: Påstanden er ensbetydende med, at man af

$$\underline{v}_1 + \dots + \underline{v}_p = \underline{0}, \quad \underline{v}_i \in K_{\lambda_i}, \quad i = 1, \dots, p,$$

kan slutte, at $\underline{v}_1 = \dots = \underline{v}_p = \underline{0}$. Fandtes der fra $\underline{0}$ forskellige blandt vektorerne $\underline{v}_i$, måtte de ifølge den foregående sætning være lineært uafhængige og kunne følgelig ikke have summen $\underline{0}$.

Om egenverdiens og egenrums forhold ved regning med lineære afbildninger gælder nogle simple sætninger. For det til et $\lambda \in L$ hørende egenrum for en lineær afbildning f benyttes nu den udførlige betegnelse $\text{Ker}(f - \lambda e)$.

Er $f: V' \rightarrow V$, hvor $V' \subseteq V$ en lineær afbildning og $\alpha \neq 0$ et tal fra L , har afbildningerne f og αf de samme egenrum, og der

gælder for $\lambda \in L$

$$\text{Ker}(f - \lambda e) = \text{Ker}(\alpha f - \alpha \lambda e) .$$

Er $f:V' \rightarrow V$ og $g:V' \rightarrow V$ lineære afbildninger, og er $\underline{u}$ egenvektor for f til egenværdien λ og egenvektor for g til egenværdien μ , vil $\underline{u}$ være egenvektor for $f + g$ til egenværdien $\lambda + \mu$. Der gælder altså for $\lambda, \mu \in L$

$$\text{Ker}(f - \lambda e) \cap \text{Ker}(g - \mu e) \subseteq \text{Ker}(f + g - (\lambda + \mu)e) .$$

Er f og g lineære afbildninger af V ind i sig selv, og er $\underline{u}$ egenvektor for f til egenværdien λ og egenvektor for g til egenværdien μ , vil $\underline{u}$ være egenvektor for $g \circ f$ til egenværdien $\mu\lambda$. Der gælder altså

$$\text{Ker}(f - \lambda e) \cap \text{Ker}(g - \mu e) \subseteq \text{Ker}(g \circ f - \mu\lambda e) .$$

For $f = g$ fås specielt

$$\text{Ker}(f - \lambda e) \subseteq \text{Ker}(f^2 - \lambda^2 e)$$

og ved induktion

$$\text{Ker}(f - \lambda e) \subseteq \text{Ker}(f^2 - \lambda^2 e) \subseteq \dots \subseteq \text{Ker}(f^p - \lambda^p e)$$

for $p \in \mathbb{N}$. Er λ egenværdi for f , er altså λ^p egenværdi for f^p med mindst samme multiplicitet.

Er $f:V \rightarrow V$ en bijektiv lineær afbildning og λ en egenværdi for f , altså $\lambda \neq 0$, kan af $f(\underline{u}) = \lambda \underline{u}$ sluttet, at $f^{-1}(\underline{u}) = (1/\lambda)\underline{u}$, og omvendt. Dette viser, at der for $\lambda \in L$ gælder

$$\text{Ker}(f - \lambda e) = \text{Ker}(f^{-1} - \frac{1}{\lambda}e) .$$

Er λ egenværdi for f , vil altså $1/\lambda$ være egenværdi med samme multiplicitet for f^{-1} .

Ovenstående sætninger benyttes til at bestemme egenverdierne for visse typer af lineære afbildninger af et vektorrum ind i sig selv.

En lineær afbildning $f: V \rightarrow V$ kaldes nilpotent, hvis der findes et $p \in \mathbb{N}$ således, at

$$f^p = 0 ,$$

hvor 0 her står for nulafbildningen, som til hver vektor i V lader svare nulvektoren. Under forudsætning af, at $\dim V > 0$, er nulafbildningen ikke injektiv, og f kan da heller ikke være injektiv. Tallet 0 er altså egenværdi for f , og det tilhørende egenrum, altså kernen ved f , er et (mindst endimensionalt) ægte underrum af V , medmindre f er nulafbildningen. Idet λ^p for enhver egenværdi λ for f er egenværdi for nulafbildningen, altså lig 0, har f ikke andre egenverdier end 0.

Lad $f: V \rightarrow V$ være en idempotent lineær afbildning, for hvilken altså

$$f^2 = f .$$

For hver egenværdi λ og tilhørende egenvektor $\underline{u}$ har man da $\lambda^2 \underline{u} = \lambda \underline{u}$, altså $\lambda^2 = \lambda$. Kun 0 og 1 kan altså være egenverdier for f . Om de tilhørende egenrum K_0 og K_1 påstås, at

$$K_0 \oplus K_1 = V .$$

Da summen af K_0 og K_1 vides at være direkte, er det tilstrækkeligt at vise, at hver vektor $\underline{v} \in V$ er sum af en vektor i K_0 og en vektor i K_1 . En sådan fremstilling er

$$\underline{v} = (e - f)(\underline{v}) + f(\underline{v}) .$$

Man har nemlig

$$f((e - f)(\underline{v})) = (f - f^2)(\underline{v}) = \underline{0} ,$$

altså $(e - f)(\underline{v}) \in K_0$, og

$$f(f(\underline{v})) = f(\underline{v}) ,$$

altså $f(\underline{v}) \in K_1$. Heraf ses, at $f(\underline{v})$ er parallelprojektion af $\underline{v}$ på K_1 langs K_0 .

Idet hver parallelprojektion er idempotent, er hermed vist, at de idempotente lineære afbildninger af et vektorrum ind i sig selv er præcis parallelprojektionerne på et underrum langs et til dette komplementært (herunder nulafbildningen og den identiske afbildning).

Lad $f: V \rightarrow V$ være en involutorisk lineær afbildning, for hvilken altså $f^2 = e$ og

$$f^2 = e .$$

For hver egenværdi λ har man da $\lambda^2 = 1$, altså $\lambda = 1$ eller $\lambda = -1$. For de tilhørende egenrum gælder

$$K_1 \oplus K_{-1} = V .$$

Dette sluttes af fremstillingen

$$\underline{v} = \frac{1}{2}(e + f)(\underline{v}) + \frac{1}{2}(e - f)(\underline{v})$$

af en vilkårlig vektor $\underline{v} \in V$. Sættes $\underline{v}' = \frac{1}{2}(e + f)(\underline{v})$ og $\underline{v}'' = \frac{1}{2}(e - f)(\underline{v})$, fås nemlig $f(\underline{v}') = \underline{v}'$ og $f(\underline{v}'') = -\underline{v}''$.

Billedvektoren $f(\underline{v})$ af en vektor $\underline{v} \in V$ fås ved at bibeholde komponenten af $\underline{v}$ efter K_1 og erstatte komponenten efter K_{-1} med den modsatte vektor. Enhver involutorisk lineær afbildning af et vektorrum ind i sig selv er altså en "(skrå) spejling" i

et (ægte) underrum parallel med et til dette komplementært underrum. Omvendt er enhver sådan spejling involutorisk.

Vi betragter nu en lineær afbildning f af et vektorrum $(V, +, L)$ af endelig dimension n ind i sig selv. Da summen af egenrum hørende til indbyrdes forskellige egenverdier er direkte, og da denne sum er underrum af V , kan der kun findes endelig mange egenrum. Summen af deres dimensioner kan nemlig højst være n . Betegner $\lambda_1, \dots, \lambda_p$ de indbyrdes forskellige egenverdier, gælder altså

$$\dim \lambda_1 + \dots + \dim \lambda_p \leq n.$$

Af særlig betydning er tilfældet, hvor der gælder lighed. For egenrummene $K_1, \dots, K_p$ hørende til henholdsvis $\lambda_1, \dots, \lambda_p$ har man da

$$K_1 \oplus \dots \oplus K_p = V.$$

Idet restriktionen af f til K_i , $i = 1, \dots, p$, er homotetien med multiplikatoren λ_i , kan afbildningen i dette tilfælde beskrives på følgende måde. For en vilkårlig vektor $\underline{u} \in V$ sættes

$$\underline{u} = \underline{u}_1 + \dots + \underline{u}_p, \quad \underline{u}_i \in K_i.$$

Man får da

$$\begin{aligned} f(\underline{u}) &= f(\underline{u}_1) + \dots + f(\underline{u}_p) \\ &= \lambda_1 \underline{u}_1 + \dots + \lambda_p \underline{u}_p. \end{aligned}$$

Lad pr_i betegne parallelprojektion af V på K_i langs

$$K'_i = K_1 \oplus \dots \oplus K_{i-1} \oplus K_{i+1} \oplus \dots \oplus K_p.$$

Da er

$$\text{pr}_i \underline{u} = \underline{u}_i ,$$

og afbildningen kan skrives

$$(*) \quad f = \lambda_1 \text{pr}_1 + \dots + \lambda_p \text{pr}_p .$$

Man ser let, at der for afbildningerne $\text{pr}_i, i = 1, \dots, p$, gælder

$$\text{pr}_j \circ \text{pr}_i = \begin{cases} \text{pr}_i & \text{for } j = i , \\ 0 & \text{for } j \neq i . \end{cases}$$

Mængden $\{\lambda_1, \dots, \lambda_p\}$ af egenverdier for afbildningen f kaldes dens spektrum og $(*)$ dens spektralfremstilling. (For afbildninger af uendelig-dimensionale vektorrum er definitionerne på spektrum og spektralfremstilling mere kompliceret.)

Idempotente og involutoriske afbildninger har ifølge ovenstående spektralfremstillinger, medens dette, bortset fra nulafbildningen, ikke gælder for nilpotente.

Regulær-ækvivalens.

Vi betragter igen lineære afbildninger af et vektorrum $(V, +, L)$ af endelig dimension n ind i sig selv. Efter valg af en basis $(\underline{e}_1, \dots, \underline{e}_n)$ for V hører der til en sådan afbildning f en (og kun én) $(n \times n)$ -matrix $\underline{A}$, således at der for koordinatsøjlen $\underline{u}_|$ for en vilkårlig vektor $\underline{u} \in V$ og koordinatsøjlen $\underline{v}_|$ for billevektoren $\underline{v} = f(\underline{u})$ gælder

$$\underline{v}_| = \underline{A} \underline{u}_| .$$

Med hensyn til en ny basis

$$(\hat{e}_1, \dots, \hat{e}_n) = (\underline{e}_1, \dots, \underline{e}_n) \underline{S}^{-1},$$

hvor $\underline{S}$ er en vilkårlig regulær $(n \times n)$ -matrix, hører til samme afbildning af matricen $\underline{S} \underline{A} \underline{S}^{-1}$ (jf. side III, 2, 37). Dette giver anledning til den følgende definition (hvor $M_{n,n,L}$ betegner mængden af $(n \times n)$ -matricer med elementer fra L):

En matrix $\underline{B} \in (M_{n,n,L})$ siges at være regulær-ækvivalent (eller ligedannet) i $(M_{n,n,L})$ med en matrix $\underline{A} \in (M_{n,n,L})$, hvis der findes en regulær matrix $\underline{S} \in (M_{n,n,L})$, således at

$$\underline{B} = \underline{S} \underline{A} \underline{S}^{-1}.$$

Den herved definerede relation i mængden af $(n \times n)$ -matricer med elementer fra L er en ækvivalensrelation. Den er nemlig refleksiv, idet $\underline{A} = \underline{E} \underline{A} \underline{E}^{-1}$, symmetrisk, idet $\underline{B} = \underline{S} \underline{A} \underline{S}^{-1}$ medfører $\underline{A} = \underline{S}^{-1} \underline{B} (\underline{S}^{-1})^{-1}$, og transitiv, idet $\underline{B} = \underline{S} \underline{A} \underline{S}^{-1}$ og $\underline{C} = \underline{T} \underline{B} \underline{T}^{-1}$ medfører

$$\underline{C} = \underline{T} \underline{S} \underline{A} \underline{S}^{-1} \underline{T}^{-1} = (\underline{T} \underline{S}) \underline{A} (\underline{T} \underline{S})^{-1}.$$

At to matricer $\underline{A}$ og $\underline{B}$ er regulær-ækvivalente betyder, at de med hensyn til hver sin passende valgt basis hører til samme lineære afbildning af V ind i V . Sådanne afbildningers egenskaber må altså give sig til kende ved de egenskaber ved matricer, der er fælles for regulær-ækvivalente. Man søger derfor i hver klasse af indbyrdes regulær-ækvivalente matricer en særlig simpel repræsentant, en "normalform", af hvilken afbildningens egenskaber let kan aflæses. Den tilsvarende opgave for lineære afbildninger af et vektorrum ind i et andet blev løst tidligere (side III, 2, 37-38) med et særdeles simpelt resultat. Ved at disponere over

to baser, nemlig en for hvert af de to vektorrum, blev der fundet en normalform, der er fuldstændig bestemt ved afbildningens rang (og de to vektorrums dimensioner). Ved en nærmere undersøgelse af lineære afbildninger af et vektorrum ind i sig selv henføres imidlertid original- og billedvektorer til samme basis, som sket ovenfor. Relationer mellem original- og billedvektorer ved sådanne afbildninger, som f.eks. eksistensen af egenrum, vil nemlig kun da afspejle sig i egenskaber ved de tilhørende matrixer. At der således kun kan disponeres over én basis, medfører, at der for hvert dimensionstal findes uendelig mange ækvivalensklasser og altså normalformer.

Karakteristisk polynomium.

Lad f være en lineær afbildning af et n -dimensionalt vektorrum $(V, +, L)$ ind i sig selv, og lad $\underline{A}$ være matrixen, der med hensyn til en valgt basis for V hører til f . Et tal $\lambda \in L$ er egen værdi for f , hvis og kun hvis afbildningen $f - \lambda e$ ikke er injektiv. Idet der til denne afbildning hører matrixen $\underline{A} - \lambda \underline{E}$, er dette ensbetydende med, at denne matrix ikke er regulær, altså med

$$\det(\underline{A} - \lambda \underline{E}) = 0 .$$

Betegner t en kompleks variabel, vil $\det(\underline{A} - t \underline{E})$ ifølge determinantens definition være et polynomium af grad n , hvis koefficienter tilhører L . Skrives

$$\det(\underline{A} - t \underline{E}) = c_0 + c_1 t + \dots + c_n t^n ,$$

ses, at

$$c_0 = \det \underline{A} , \quad c_n = (-1)^n .$$

Dette polynomium kaldes det karakteristiske polynomium (også reduktionsdeterminanten) for matricen $\underline{A}$ og dets rødder dennes karakteristiske rødder. Idet der for hver regulær $(n \times n)$ -matrix $\underline{S}$ gælder

$$\underline{S}\underline{A}\underline{S}^{-1} - t\underline{E} = \underline{S}(\underline{A} - t\underline{E})\underline{S}^{-1} ,$$

sluttes af multiplikationssætningen for determinanter, at regulær-ækvivalente matricer har samme karakteristiske polynomium. Man kan derfor tale om den lineære afbildnings karakteristiske polynomium og rødder. Herefter kan siges:

Egenværdierne for en lineær afbildning f af et n -dimensionalt vektorrum $(V, +, L)$ ind i sig selv er præcis de karakteristiske rødder for f , der tilhører L .

Lad λ være en egenværdi for f . Det til λ hørende egenrum er $\text{Ker}(f - \lambda e)$. Koordinatsættene $\underline{u}_i$ for dets vektorer med hensyn til basen, for hvilken afbildningens matrix er $\underline{A}$, er altså løsninger til det homogene lineære ligningssystem

$$(\underline{A} - \lambda\underline{E})\underline{u}_i = \underline{0}_i .$$

Da løsningsrummet har dimensionen $n - \text{rg}(\underline{A} - \lambda\underline{E})$, gælder

$$em \lambda = \dim(\text{Ker}(f - \lambda e)) = n - \text{rg}(\underline{A} - \lambda\underline{E}) .$$

(Denne ligning kan også opretholdes, når $\lambda \in L$ ikke er egenværdi, idet $\underline{A} - \lambda\underline{E}$ da er regulær, har altså rang n .)

Antallet p af indbyrdes forskellige egenværdier $\lambda_1, \dots, \lambda_p$ for afbildningen f er højst n , da et n -te grads polynomium højst kan have n forskellige rødder. Men der gælder endda

$$em \lambda_1 + \dots + em \lambda_p \leq n .$$

Venstre side er nemlig lig med summen af egenrummenes dimensioner, altså lig med dimensionen af egenrummenes sum, da denne sum er direkte. Uligheden følger derfor af, at egenrummenes direkte sum er et underrum af V .

Det til λ_i , $i = 1, \dots, p$, hørende egenrum betegnes kort K_i . Endvidere sættes

$$m_i = \dim K_i$$

samt

$$m = m_1 + \dots + m_p.$$

Der vælges m vektorer $\underline{e}_1, \dots, \underline{e}_m \in V$ således, at de første m_1 danner en basis for K_1 , de næste m_2 en basis for K_2 , ..., de sidste m_p en basis for K_p . Disse m vektorer er lineært uafhængige, da egenrummenes sum er direkte. De kan altså (om fornødent) suppleres til en basis $(\underline{e}_1, \dots, \underline{e}_n)$ for V . Idet $\underline{e}_i$ for $i = 1, \dots, m_1$ er egenvektor til λ_1 , altså $f(\underline{e}_i) = \lambda_1 \underline{e}_i$, for $i = m_1+1, \dots, m_1+m_2$ egenvektor til λ_2 , altså $f(\underline{e}_i) = \lambda_2 \underline{e}_i$ osv., får den til f hørende matrix ved dette basisvalg følgende udseende:

$$\underline{A} = \begin{pmatrix} \lambda_1 & & & 0 & a_{1,m+1} & \dots & a_{1n} \\ & \ddots & & & & & \\ & & \lambda_1 & & & & \\ \vdots & & & \ddots & & & \\ \vdots & & & & \lambda_p & & \\ \vdots & & & & & \ddots & \\ 0 & & & & & & \lambda_p & a_{m,m+1} & \dots & a_{mn} \\ 0 & & & & & & 0 & a_{m+1,m+1} & \dots & a_{m+1,n} \\ \vdots & & & & & & & \vdots & & \vdots \\ \vdots & & & & & & & \vdots & & \vdots \\ 0 & & & & & & 0 & a_{n,m+1} & \dots & a_{nn} \end{pmatrix}$$

$(m \times m)$ -delmatricen i øverste venstre hjørne er en diagonalmatrix, hvis diagonalelementer er egenværdierne, hver taget så mange gange, som dens egenværdimultiplicitet angiver; og $((m-n) \times m)$ -matricen i nederste venstre hjørne er en nulmatrix.

Matricen $\underline{A} - t\underline{E}$ fås ved at subtrahere t fra alle diagonalelementer i $\underline{A}$. Udvikles $\det(\underline{A} - t\underline{E})$ efter første søjle, dernæst den fremkommende determinant af $(n-1)$ -te orden efter første søjle osv., fås efter m skridt

$$\det(\underline{A} - t\underline{E}) = (\lambda_1 - t)^{m_1} \dots (\lambda_p - t)^{m_p} Q(t),$$

hvor $Q(t)$ er et polynomium af grad $n - m$ (nemlig det karakteristiske polynomium for $((n-m) \times (n-m))$ -delmatricen af $\underline{A}$ i nederste højre hjørne). Heraf ses, at λ_i , $i = 1, \dots, p$, er mindst m_i -dobbel rod i $\det(\underline{A} - t\underline{E})$. Betegnes "rodmultipliciteten" af λ_i med $rm \lambda_i$, gælder altså for hver egenværdi λ_i

$$1 \leq em \lambda_i \leq rm \lambda_i.$$

Det fremgår af ovenstående, at hvis der findes en basis for V , som består af egenvektorer for f , altså hvis

$$em \lambda_1 + \dots + em \lambda_p = n,$$

vil afbildningens matrix med hensyn til denne basis være en diagonalmatrix, hvis diagonalelementer er egenværdierne, hver taget med så mange gange som egenværdimultipliciteten angiver. På den anden side er det klart, at hvis der findes en basis, med hensyn til hvilken f har en diagonalmatrix, er basens vektorer egenvektorer med diagonalelementerne som egenværdier, og summen af egenrummenes dimensioner er n . Dette tilfælde foreligger, hvis og kun hvis afbildningen f har en spektralfremstilling. Vi kan

altså slutte:

En lineær afbildning $f: V \rightarrow V$, til hvilken der med hensyn til en basis for V hører matricen $\underline{A}$, har en spektralfremstilling, hvis og kun hvis $\underline{A}$ er regulær-ækvivalent med en diagonalmatrix. Ovenstående resultater fører til følgende kriterium herfor:

En matrix $\underline{A} \in (M_{n,n}, L)$ er regulær-ækvivalent i $(M_{n,n}, L)$ med en diagonalmatrix, hvis og kun hvis der for dens indbyrdes forskellige karakteristiske rødder λ_i , $i = 1, \dots, p$, gælder

$$\lambda_i \in L, \quad \text{rm } \lambda_i = n - \text{rg}(\underline{A} - \lambda_i \underline{E}),$$

$$\text{rm } \lambda_1 + \dots + \text{rm } \lambda_p = n,$$

specielt, hvis $\underline{A}$ har n indbyrdes forskellige karakteristiske rødder tilhørende L .

Hvis en klasse af regulær-ækvivalente matricer indeholder en diagonalmatrix, er denne entydig bestemt på nær diagonalelementernes rækkefølge, idet disse jo er de karakteristiske rødder, hver taget i et antal svarende til multipliciteten. Nu er diagonalmatricer, der kun adskiller sig ved diagonalelementernes rækkefølge, regulær-ækvivalente, nemlig ved koordinattransformationer, ved hvilke basisvektorerne permuteres. Man kan derfor fastsætte en rækkefølge for de karakteristiske rødder og vælge den pågældende diagonalmatrix som repræsentant for klassen. Som normalform for den tilhørende lineære afbildning matrixligning fås da

$$\underline{v}| = (\lambda_1, \dots, \lambda_1, \dots, \lambda_p, \dots, \lambda_p)_{\text{diag}} \underline{u}|.$$

Vedrørende lineære afbildninger, som ikke har nogen spektralfremstilling - hvis tilhørende matricer altså ikke er regulær-ækvivalente med diagonalmatricer - vil vi foreløbig nøjes med følgende bemærkninger.

Ifølge den såkaldte algebraens fundamentalsætning (der ikke vil blive bevist her) har hvert komplekst polynomium $p(t)$ af grad $n \geq 1$ mindst én kompleks rod t_1 . Idet der da gælder

$$p(t) = (t - t_1)p_1(t) ,$$

hvor $p_1(t)$ er et polynomium af grad $n - 1$, inderes let ved induktion, at $p(t)$ kan skrives

$$p(t) = c_n(t - t_1)(t - t_2)\dots(t - t_n) ,$$

hvor $c_n \neq 0$ er koefficienten til t^n . Dette viser, at $p(t)$ har n rødder, hvis rodmultipliciteter har summen n .

For endelig-dimensionale vektorrum over de komplekse tals legeme kan heraf sluttes, at hver lineær afbildning af et sådant rum ind i sig selv har mindst én egenværdi. Men om egenværdimultipliciteten kan i almindelighed ikke siges mere end, at den er mindst 1. Som eksemple, der viser dette, nævnes en (nilpotent) lineær afbildning af et tredimensionalt vektorrum (over et vilkårligt tallegeme), der med hensyn til en valgt basis har matricen

$$\underline{A} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} .$$

Det karakteristiske polynomium er $-t^3$, har altså roden 0 med $\text{rm } 0 = 3$. Men da $\text{rg}(\underline{A} - 0\underline{E}) = \text{rg } \underline{A} = 2$, er $\text{em } 0 = 1$.

Idet hvert reelt polynomium af ulige grad har en reel rod, har hver lineær afbildning af et vektorrum af ulige dimension over de reelle tals legeme mindst én egenværdi. Derimod tillader hvert vektorrum af lige dimension (> 0) over de reelle tals legeme lineære afbildninger uden egenværdier. Som eksempel i det todimensionale tilfælde nævnes en afbildning med matricen $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Det karakteristiske polynomium er $t^2 + 1$ og har altså ingen reelle rødder.

Det er undertiden nyttigt at have eksplicite udtryk for koefficienterne $c_0, c_1, \dots, c_{n-1}$ i det karakteristiske polynomium for en matrix $\underline{A} = (a_{ij})$.

Den j -te søjle i matricen $\underline{A} - t\underline{E}$ kan skrives som en sum af to søjler, nemlig

$$\underline{a}_{|j} + (-t\underline{\delta}_{|j}),$$

hvor $\underline{a}_{|j}$ og $\underline{\delta}_{|j}$ betegner de j -te søjler i henholdsvis $\underline{A}$ og $\underline{E}$. Benyttes dette for $j = 1$, ses, at $\det(\underline{A} - t\underline{E})$ kan skrives som en sum af to determinanter, hvoraf den ene har $\underline{a}_{|1}$ og den anden $-t\underline{\delta}_{|1}$ som første søjle, medens de ellers har de samme søjler $\underline{a}_{|j} + (-t\underline{\delta}_{|j})$, $j = 2, \dots, n$. Dernæst skrives hver af de to fremkomne determinanter som sum af en med $\underline{a}_{|2}$ som anden søjle og en med $-t\underline{\delta}_{|2}$ som anden søjle, og således fortsættes. Man får da det karakteristiske polynomium fremstillet som en sum af ialt 2^n determinanter, som fremgår af det $\underline{A}$ ved at erstatte en del af søjlerne (specielt ingen eller alle) med de tilsvarende søjler i $-t\underline{E}$. Forekommer i en sådan determinant netop p søjler fra $\underline{A}$, altså $n - p$ søjler fra $-t\underline{E}$, kan faktoren $(-t)^{n-p}$ sættes udenfor, og den determinant, som denne er multipliceret med, fremgår af det $\underline{A}$ ved at erstatte $n - p$ søjler med de tilsvarende søjler

i $\underline{\underline{E}}$. Koefficienten c_{n-p} til t^{n-p} er altså $(-1)^{n-p}$ multipliceret med summen af alle $\binom{n}{n-p} = \binom{n}{p}$ determinanter af den sidstnævnte art. Ved at udvikle successivt efter de $n - p$ søjler fra $\underline{\underline{E}}$ ses, at disse determinanter stemmer overens med hovedunderdeterminanterne af p -te orden i matricen $\underline{\underline{A}}$. (Ved en sådan forstås determinanten af en delmatrix af $\underline{\underline{A}}$, der fås ved at slette søjler og rækker med de samme numre.) Der gælder altså for $p = 1, \dots, n$

$$c_{n-p} = (-1)^{n-p} \sum_{1 \leq i_1 < \dots < i_p \leq n} \begin{vmatrix} a_{i_1 i_1} & \dots & a_{i_1 i_p} \\ \vdots & & \vdots \\ a_{i_p i_1} & \dots & a_{i_p i_p} \end{vmatrix} .$$

For $p = n$ har man, som allerede nævnt,

$$c_0 = \det \underline{\underline{A}}$$

og for $p = 1$

$$c_{n-1} = (-1)^{n-1} \sum_{i=1}^n a_{ii} = (-1)^{n-1} \operatorname{tr} \underline{\underline{A}} ,$$

hvor altså summen af elementerne i hoveddiagonalen af matricen $\underline{\underline{A}}$, denne matrices spor, er betegnet $\operatorname{tr} \underline{\underline{A}}$.

Da regulær-ækvivalente matricer har samme karakteristiske polynomium, kan man slutte, at for to sådanne matricer har summen af hovedunderdeterminanterne af en given orden p den samme værdi. Specielt gælder: Regulær-ækvivalente matricer har samme determinant og samme spor.

Ifølge algebraens fundamentalsætning kan det karakteristiske polynomium skrives

$$\det(\underline{A} - t\underline{E}) = (t_1 - t)(t_2 - t)\dots(t_n - t) ,$$

hvor $t_1, \dots, t_n$ betegner de karakteristiske rødder, hver taget så mange gange, som rodmultipliciteten angiver. Idet dette gælder for alle $t \in \mathbb{C}$, fås ved udregning af højre side og sammenligning af tilsvarende koefficienter, at c_{n-p} for hvert $p = 1, \dots, n$ er $(-1)^{n-p}$ gange summen af alle de produkter af p blandt tallene $t_1, \dots, t_n$, hvis faktorer har indbyrdes forskellige mærketal. Vi kan altså skrive

$$c_{n-p} = (-1)^{n-p} \sum_{1 \leq i_1 < \dots < i_p \leq n} t_{i_1} \dots t_{i_p} ,$$

hvor summen udstrækkes over alle $\binom{n}{p}$ kombinationer af p mærker udtaget blandt $1, \dots, n$. Betragtet som funktion af n variable $t_1, \dots, t_n$ er denne sum den såkaldte p -te elementarsymmetriske funktion .) Specielt fås for $p = n$

$$\det \underline{A} = t_1 \dots t_n ,$$

og for $p = 1$

$$\text{tr } \underline{A} = t_1 + \dots + t_n .$$

Egenværdiproblemet for normale afbildninger.

Lad $(V, +, \mathbb{C}, \cdot)$ være et vektorrum med indre produkt over de komplekse tals legeme med $\dim V = n$. Blandt de lineære afbildninger af et sådant vektorrum ind i sig selv udmærker de normale (jf. side III,2,52) sig ved at have spektralfremstillinger med parvis ortogonale egenrum. Ved beviset herfor benyttes algebraens fundamentalsætning samt følgende to egenskaber ved normale afbildninger, der blev vist tidligere (side III,2,53):

Er f en normal afbildning og e den identiske afbildning,

vil $f - \lambda e$ for hvert $\lambda \in \mathbb{C}$ være normal.

Ved en normal afbildning f er kernens ortogonale komplement invariant, og restriktionen af f til dette er normal.

Til en lineær afbildning f af et vektorrum $(V, +, \mathbb{C}, \cdot)$ med indre produkt og endelig dimension $n > 0$ findes en ortonormeret basis bestående af egenvektorer, hvis og kun hvis f er normal.

Bevis: Først vises ved induktion efter n , at betingelsen er tilstrækkelig. For $n = 1$ er intet at bevise, idet et endimensionalt vektorrum er egenrum for hver af sine lineære afbildninger. En vilkårlig af rummets to enhedsvektorer opfylder altså kravet. Vi antager, at påstanden er rigtig for alle dimensionstal mindre end et givet $n \in \mathbb{N}$. Lad $f: V \rightarrow V$, hvor $\dim V = n$, være en normal afbildning. Ifølge algebraens fundamentalsætning har den en egenverdi λ_1 . Lad K_1 være det tilhørende egenrum, altså kernen ved $f - \lambda_1 e$. Da også denne afbildning er normal, er $K_1^\perp$ invariant ved den. Endvidere er restriktionen af $f - \lambda_1 e$ og følgelig også restriktionen af $(f - \lambda_1 e) + \lambda_1 e = f$ til $K_1^\perp$ normal. Ifølge induktionsantagelsen findes der en ortonormeret basis for $K_1^\perp$, der består af egenvektorer for restriktionen af f . Disse vektorer er da også egenvektorer for f . Idet

$$K_1 \oplus K_1^\perp = V,$$

vil de sammen med vektorerne i en ortonormeret basis for K_1 danne en ortonormeret basis for V , som består af egenvektorer.

Nødvendigheden følger af, at en lineær afbildning af V er normal, dersom der findes en ortonormeret basis, med hensyn til hvilken dens matrix er en diagonalmatrix (side III, 2, 52-53).

Hermed er sætningen bevist.

Det fremgår af den, at enhver normal afbildning af $(V, +, \dot{\mathbb{C}}, \cdot)$ har parvis ortogonale egenrum, hvis direkte sum er V , og den har følgelig en spektralfremstilling ved ortogonalprojektioner.

Det er hensigtsmæssigt (lige som tidligere, (side III, 2, 48 og følgende)) at henhøre lineære afbildninger af vektorrum med indre produkt til ortonormale baser. To matricer $\underline{\underline{A}}, \underline{\underline{B}} \in (M_{n,n}, \dot{\mathbb{C}})$ hører til samme afbildning f med hensyn til hver sin ortonormerede basis, hvis og kun hvis der findes en unitær matrix $\underline{\underline{U}}$ (for hvilken altså $\underline{\underline{U}}' \underline{\underline{U}} = \underline{\underline{E}}$), således at

$$\underline{\underline{B}} = \underline{\underline{U}} \underline{\underline{A}} \underline{\underline{U}}^{-1} = \underline{\underline{U}} \underline{\underline{A}} \underline{\underline{U}}'$$

(jf. side III, 2, 58). I så fald siges $\underline{\underline{A}}$ at være unitær-ækvivalent med $\underline{\underline{B}}$. At der foreligger en ækvivalensrelation, ses som ved den regulær-ækvivalens med benyttelse af, at $\sqrt{}$ inverse til en unitær matrix og produktet af to unitære matricer er unitære. Unitær-ækvivalente matricer er naturligvis regulær-ækvivalente. Hver klasse af unitær-ækvivalente er altså indeholdt i en klasse af regulær-ækvivalente.

En lineær afbildning f af $(V, +, \dot{\mathbb{C}}, \cdot)$ er normal, hvis og kun hvis matricen $\underline{\underline{A}}$, der hører til den med hensyn til en ortonormeret basis, er "normal", dvs. hvis og kun hvis $\underline{\underline{A}}' \underline{\underline{A}} = \underline{\underline{A}} \underline{\underline{A}}'$ (jf. side III, 2, 52). Hvis en af to unitær-ækvivalente matricer er normal, er den anden altså ligeledes normal. (Dette bekræftes også let ved matrixregning.)

Ovenstående sætning om normale afbildninger giver herefter følgende sætning om matricer:

En matrix $\underline{A} \in (M_{n,n}, \mathbb{C})$ er unitær-ækvivalent med en diagonal matrix, hvis og kun hvis den er normal, dvs. hvis og kun hvis $\underline{A}'\underline{A} = \underline{A}\underline{A}'$.

Normale afbildninger af et n -dimensionalt vektorrum $(V, +, \dot{R}, \cdot)$ med indre produkt over de reelle tals legeme behøver ikke at have spektralfremstillinger, end ikke egenverdier. Men der gælder som i det komplekse tilfælde: Egenrum hørende til indbyrdes forskellige egenverdier er parvis ortogonale.

I beviset herfor benyttes ikke, at det drejer sig om et vektorrum over $\dot{R}$. Lad altså f være en normal afbildning af et endelig-dimensionalt vektorrum $(V, +, L, \cdot)$ med indre produkt, og lad λ og μ være to forskellige egenverdier for f . Vi skal vise, at

$$f(\underline{u}) = \lambda \underline{u} \wedge f(\underline{v}) = \mu \underline{v} \Rightarrow \underline{u} \cdot \underline{v} = 0.$$

Idet afbildningen $f - \mu e$ er normal, medfører $(f - \mu e)(\underline{v}) = \underline{0}$, at $(f^* - \bar{\mu}e)(\underline{v}) = \underline{0}$ (jf. side III, 2, 53), altså at $f(\underline{v}) = \bar{\mu}\underline{v}$. Vi har derfor

$$\lambda \underline{u} \cdot \underline{v} = f(\underline{u}) \cdot \underline{v} = \underline{u} \cdot f^*(\underline{v}) = \underline{u} \cdot (\bar{\mu}\underline{v}) = \bar{\mu} \underline{u} \cdot \underline{v}.$$

Da $\lambda \neq \bar{\mu}$, følger heraf $\underline{u} \cdot \underline{v} = 0$, som påstået.

Overgangen fra en ortonormeret basis for $(V, +, \dot{R}, \cdot)$ til en anden sker ved hjælp af en reel ortogonal matrix (jf. side III, 2, 58). To matricer $\underline{A}, \underline{B} \in (M_{n,n}, \dot{R})$ hører til samme lineære afbildning med hensyn til hver sin ortonormerede basis, hvis og kun hvis der findes en ortogonal matrix $\underline{U}$, således at

$$\underline{B} = \underline{U}\underline{A}\underline{U}^{-1} = \underline{U}\underline{A}\underline{U}'.$$

I så fald siges A at være ortogonal-ækvivalent med B. At der foreligger en ækvivalensrelation følger af, at de ortogonale $(n \times n)$ -matricer danner en gruppe.

Af en bemærkning ovenfor fremgår, at ikke alle reelle normale matricer er ortogonal-ækvivalente med diagonalmatricer.

Egenværdiproblemet for unitær^e og ortogonale afbildninger.

Vi betragter igen først det komplekse tilfælde, altså en unitær afbildning f af et vektorrum $(V, +, \cdot, \cdot)$ af dimension n ind i sig selv (jf. side III, 2, 57). Idet det indre produkt, og dermed normen, bevares ved f , må der for hver egenværdi λ og tilhørende egenvektor $\underline{u}$ gælde

$$\|f(\underline{u})\| = \|\lambda \underline{u}\| = |\lambda| \|\underline{u}\| = \|\underline{u}\|.$$

Da $\underline{u} \neq \underline{0}$, følger heraf $|\lambda| = 1$. Tages i betragtning, at en unitær afbildning er normal,^{ses,} at f har en spektralfremstilling med parvis ortogonale egenrum og egenværdier, der alle har absolut værdi 1.

Med hensyn til en ortonormeret basis hører til en lineær afbildning f en unitær matrix, altså en matrix A, for hvilken $\overline{\underline{A}}' \underline{A} = \underline{E}$, hvis og kun hvis f er unitær. Da en diagonalmatrix, hvis diagonalelementer har absolut værdi 1, øjensynlig er unitær, har vi ialt:

En lineær afbildning f af et n -dimensionalt vektorrum $(V, +, \cdot, \cdot)$ er unitær, hvis og kun hvis der findes en ortonormeret basis bestående af egenvektorer og alle egenværdier har absolut værdi 1.

En matrix $\underline{A} \in (M_{n,n}, \mathbb{C})$ er unitær, hvis og kun hvis den er unitær-ækvivalent med en diagonalmatrix, hvis diagonalelementer har absolut værdi 1.

Vi betragter nu ortogonale afbildninger af et n -dimensionalt vektorrum $(V, +, \cdot)$ på sig selv. Vi har tidligere (side III, 2, 59) bemærket, at hvis U er et invariant underrum ved en sådan afbildning f , vil også $U^\perp$ være invariant ved f , og restriktionerne af f til disse underrum vil være ortogonale. Hvis en ortogonal afbildning f har et egenrum, vil altså dettes ortogonale komplement være invariant ved f .

Efter valg af en ortonormeret basis hører der til en ortogonal afbildning f en ortogonal matrix, altså en matrix $\underline{A}$, for hvilken $\underline{A}'\underline{A} = \underline{E}$, og omvendt. Idet en ortogonal matrix kan opfattes som en reel unitær matrix, har alle dens karakteristiske rødder absolut værdi 1. Kun 1 og -1 kan altså være reelle karakteristiske rødder og dermed egenværdier. (Dette følger også umiddelbart af, at en ortogonal afbildning er normbevarende.) Det karakteristiske polynomium for $\underline{A}$ har reelle koefficienter. Hvis det har en ikke-reel rod α , vil altså også $\bar{\alpha}$ være rod og med samme rodmultiplicitet. Da $\alpha\bar{\alpha} = 1$ for hver sådan rod, er produktet af de ikke-reelle rødder lig 1. Da endvidere produktet af alle karakteristiske rødder er lig med $\det \underline{A} = \pm 1$, kan vi heraf slutte, at rodmultipliciteten af -1 er lige (specielt 0) eller ulige efter som $\det \underline{A} = 1$ eller $\det \underline{A} = -1$. Endvidere bemærkes, at der for ulige n altid eksisterer en reel karakteristisk rod.

Idet man kalder en ortogonal afbildning for egentlig ortogonal, hvis dens determinant er lig 1, og for uegentlig ortogonal,

hvis dens determinant er lig -1 , kan man sammenfatte de fundne resultater således:

Enhver uegentlig ortogonal afbildning af et endelig-dimensionalt vektorrum $(V, +, \dot{R}, \cdot)$ på sig selv har egenværdien -1 . Enhver egentlig ortogonal afbildning af et vektorrum $(V, +, \dot{R}, \cdot)$ af ulige dimension på sig selv har egenværdien 1 .

Der gælder endvidere i alle tilfælde

$$em\ 1 = rm\ 1, \quad em\ -1 = rm\ -1.$$

Dette kan indses på følgende måde: Lad K_1 og K_{-1} være de til 1 og -1 hørende egenrum og $m_1 = \dim K_1$ og $m_{-1} = \dim K_{-1}$ deres dimensioner. Endvidere sættes

$$U = (K_1 \oplus K_{-1})^\perp.$$

Vælges ortonormerede baser for K_1, K_{-1} og U , vil disse basers vektorer tilsammen udgøre en ortonormeret basis for V . Den til den ortogonale afbildning f hørende matrix vil da have formen

$$\underline{A} = \begin{pmatrix} \underline{E}_{m_1, m_1} & \underline{0} & \underline{0} \\ \underline{0} & -\underline{E}_{m_{-1}, m_{-1}} & \underline{0} \\ \underline{0} & \underline{0} & \hat{\underline{A}} \end{pmatrix},$$

hvor $\hat{\underline{A}}$ er matricen hørende til restriktionen af f til U . For det karakteristiske polynomium fås da

$$\det(\underline{A} - t\underline{E}) = (1 - t)^{m_1} (-1 - t)^{m_{-1}} \det(\hat{\underline{A}} - t\underline{E}).$$

Hvis 1 eller -1 var rod i $\det(\hat{\underline{A}} - t\underline{E})$, ville restriktionen af f til U have en egenværdi. De tilhørende egenvektorer ville også

være egenvektorer for f og måtte derfor tilhøre K_1 eller K_{-1} , hvilket er umuligt. Polynomiet $\det(\hat{\underline{A}} - t\underline{E})$ har altså hverken roden 1 eller roden -1, og heraf følger påstanden.

Vi betragter specielt det todimensionale og det tredimensionale geometriske vektorrum. Idet vektorerne tænkes afsat fra samme punkt 0, kan de ortogonale afbildninger fortolkes som de kongruenser af planen henholdsvis rummet, ved hvilke 0 er fixpunkt.

At en (2×2) -matrix $\underline{A} = (\alpha_{ij})$ er ortogonal, er ensbetydende med

$$a_{11}^2 + a_{21}^2 = 1, a_{12}^2 + a_{22}^2 = 1, a_{11}a_{12} + a_{21}a_{22} = 0.$$

Af den første ligning ses, at der findes netop ét $\alpha \in [0, 2\pi[$, for hvilket

$$a_{11} = \cos \alpha, \quad a_{21} = \sin \alpha.$$

Af de to øvrige ligninger sluttes, at

$$\underline{A} = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \quad \text{eller} \quad \underline{A} = \begin{pmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{pmatrix}.$$

Det første tilfælde, hvor $\det \underline{A} = 1$, svarer til en egentlig kongruens, nemlig drejningen om 0 med drejningsvinklen α . Egenverdier findes kun for $\alpha = 0$ og $\alpha = \pi$, nemlig henholdsvis 1 med $\text{em } 1 = 2$ og -1 med $\text{em } -1 = 2$. Det andet tilfælde, hvor $\det \underline{A} = -1$, svarer til en uegentlig kongruens. Af det generelle resultat ovenfor (eller af, at det karakteristiske polynomium er $t^2 - 1$) sluttes, at -1 og 1 er egenverdier for hvert α . Vektorerne

med koordinatparrene $(-\sin \frac{1}{2}\alpha, \cos \frac{1}{2}\alpha)$ og $(\cos \frac{1}{2}\alpha, \sin \frac{1}{2}\alpha)$ er normerede egenvektorer til henholdsvis -1 og 1 . Afbildningen er involutorisk, nemlig en spejling i linien, der danner vinklen $\frac{1}{2}\alpha$ med den første koordinatakse.

Ifølge ovenstående generelle resultater har en kongruens f med fixpunkt O af det sædvanlige rum egenværdien 1 , hvis den er egentlig, og egenværdien -1 , hvis den er uegentlig. Lad d betegne linien (eller en af linierne) gennem O , der indeholder en egenvektor til 1 , hvis f er egentlig, en egenvektor til -1 , hvis f er uegentlig. I begge tilfælde er normalplanen til d gennem O invariant, og restriktionen af f til den er en kongruens. Denne må være egentlig i begge tilfælde, da dens determinant multipliceret med den pågældende egenværdi er lig med determinanten for f . Heraf sluttet, at enhver egentlig kongruens med fixpunkt O er en drejning om en akse d , og at enhver uegentlig kongruens med fixpunkt O er en drejspejling, dvs. sammensat (i en eller anden orden) af en drejning om en linie d og en spejling i dennes normalplan gennem O .

Egenværdiproblemet for selvadjungerede afbildninger.

Enhver selvadjungeret eller Hermiteske symmetrisk afbildning f af et n -dimensionalt vektorrum $(V, +, \cdot, \cdot)$ ind i sig selv, som ifølge definition (side III, 2, 54) stemmer overens med sin adjungerede, er normal og har følgelig en spektralfremstilling med parvis ortogonale egenrum.

Med hensyn til en ortonormeret basis hører til en lineær afbildning f en Hermiteske symmetrisk matrix, altså en matrix $\underline{\underline{A}}$, for hvilken $\underline{\underline{A}}' = \underline{\underline{A}}$, hvis og kun hvis f er Hermiteske symmetrisk.

Idet diagonalelementerne i en sådan matrix er reelle og enhver reel diagonalmatrix er Hermitesk symmetrisk, har vi:

En lineær afbildning f af et n -dimensionalt vektorrum $(V, +, \cdot, \cdot)$ er Hermitesk symmetrisk, hvis og kun hvis der findes en ortonormeret basis bestående af egenvektorer, og alle egen-værdier er reelle.

En matrix $\underline{A} \in (M_{n,n}, \mathbb{C})$ er Hermitesk symmetrisk, hvis og kun hvis den er unitær-ækvivalent med en reel diagonalmatrix.

Som en følge heraf fremhæves, at det karakteristiske polynomium for en Hermitesk symmetrisk matrix har lutter reelle rødder og altså (jf. side III,5,22) reelle koefficienter.

For symmetriske afbildninger af et endelig-dimensionalt vektorrum med indre produkt over de reelle tals legeme gælder tilsvarende sætninger. De kan dog ikke sluttes uden videre af resultaterne i det komplekse tilfælde. En reel symmetrisk matrix $\underline{A}$ er ganske vist Hermitesk symmetrisk, og der findes følgelig en unitær matrix $\underline{U}$ således, at $\underline{U}\underline{A}\underline{U}^{-1}$ er en reel diagonalmatrix. Men at denne matrix $\underline{U}$ kan vælges reel, altså ortogonal, er ikke klart på forhånd. Vi kan imidlertid slutte på følgende måde.

Lad f være en symmetrisk afbildning af det n -dimensionale vektorrum $(V, +, \cdot, \cdot)$ ind i sig selv. Afbildningens matrix $\underline{A}$ med hensyn til en ortonormeret basis er reel og symmetrisk, altså Hermitesk symmetrisk. Dens karakteristiske polynomium har ifølge ovenstående reelle rødder. Afbildningen f har altså mindst én egen-værdi λ_1 . Er K_1 det tilhørende egenrum, vil dets ortogonale komplement være invariant ved f (jf. side III,2,55), og restriktionen af f til $K_1^\perp$ vil være symmetrisk. Som for normale afbild-

ninger i det komplekse tilfælde (side III,5,23) kan man nu ved induktion efter n slutte, at der findes en ortonormeret basis bestående af egenvektorer for f . Da endvidere en lineær afbildning af V , der med hensyn til en ortonormeret basis har en symmetrisk matrix, er symmetrisk, gælder:

En lineær afbildning f af et n -dimensionalt vektorrum $(V, +, \dot{R}, \cdot)$ ind i sig selv er symmetrisk, hvis og kun hvis der findes en ortonormeret basis bestående af egenvektorer.

En matrix $\underline{A} \in (M_{n,n}, \dot{R})$ er symmetrisk, hvis og kun hvis den i $(M_{n,n}, \dot{R})$ er ortogonal-ækvivalent med en diagonalmatrix.

22. En lineær afbildning af et 4-dimensionalt vektorrum

$(V, +, \mathbb{R})$ ind i sig selv er givet ved sin matrixligning med hensyn til en basis:

$$\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}.$$

Find afbildningens egenverdier.

23. En lineær afbildning f af et tredimensionalt vektorrum

$(V, +, \mathbb{R})$ ind i sig selv er bestemt ved

$$f(\underline{e}_1) = 2\underline{e}_3, \quad f(\underline{e}_2) = \underline{e}_1 + 3\underline{e}_3, \quad f(\underline{e}_3) = \underline{e}_2,$$

hvor $\{\underline{e}_1, \underline{e}_2, \underline{e}_3\}$ er en basis for V . Find egenverdierne samt en basis for hvert af de tilhørende egenrum. Undersøg, om man ved passende valg af basis kan opnå, at den til f svarende matrix bliver en diagonalmatrix.

24. En lineær afbildning f af et to-dimensionalt vektorrum

$(U, +, \mathbb{R})$ ind i sig selv er givet ved matrixligningen

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} \cosh \alpha & \sinh \alpha \\ \sinh \alpha & \cosh \alpha \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix},$$

med hensyn til en basis. α er et reelt tal. Bestem afbildningens egenverdier og egenvektorer og vis, at man ved basis-skifte kan opnå, at den til f svarende matrix bliver en diagonalmatrix.

Undersøg ligeledes en lineær afbildning g af et to-dimensionalt vektorrum $(V, +, \mathbb{C})$ ind i sig selv givet ved

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}.$$

44. Find egenverdier og egenvektorer for den lineære afbildning af vektorrummet $(\mathcal{P}(\mathbb{R} \rightarrow \mathbb{R}), +, \mathbb{R})$ af alle reelle polynomier ind i sig selv, hvor til hvert polynomium $p(t)$, $t \in \mathbb{R}$, svarer $t Dp(t)$, $t \in \mathbb{R}$.
45. En lineær afbildning f af et todimensionalt vektorrum $(V, +, L)$ ind i sig selv er bestemt ved $f(\underline{e}_1) = \underline{e}_2$, $f(\underline{e}_2) = \underline{e}_1$, hvor $(\underline{e}_1, \underline{e}_2)$ er en basis. Find afbildningens invariante underrum, egenvektorer og egenverdier.
- * En lineær afbildning f af et tredimensionalt vektorrum $(V, +, L)$ ind i sig selv er bestemt ved $f(\underline{e}_1) = \underline{e}_2$, $f(\underline{e}_2) = \underline{e}_3$, $f(\underline{e}_3) = \underline{e}_1$, hvor $(\underline{e}_1, \underline{e}_2, \underline{e}_3)$ er en basis. Find afbildningens invariante underrum, egenvektorer og egenverdier.
46. Om to lineære afbildninger f og g af et vektorrum $(V, +, L)$ ind i sig selv forudsættes, at de er ombyttelige, dvs. at $f \circ g = g \circ f$. Vis, at hvert egenrum ved en af afbildningerne er invariant ved den anden.
47. Med $(V, +, \mathbb{R})$ betegnes vektorrummet $(\mathcal{C}([0, \pi] \rightarrow \mathbb{R}), +, \mathbb{R})$ af alle på intervallet $[0, \pi]$ kontinuerte reelle funktioner, medens U er underrummet bestående af de to gange kontinuert differentiable funktioner $\varphi \in V$, for hvilke $\varphi(0) = \varphi(\pi) = 0$. Bestem egenverdier og tilhørende egenfunktioner for den lineære afbildning af $(U, +, \mathbb{R})$ ind i $(V, +, \mathbb{R})$, hvor til hver funktion $\varphi \in U$ svarer dens anden afledede $D^2\varphi$.
48. Givet en oversigt over alle idempotente og alle involutoriske lineære afbildninger af det geometriske vektorrum $(V_3, +, \mathbb{R})$ ind i sig selv, og beskriv de forskellige typer geometrisk.

49. Vis, at hvis f er en idempotent lineær afbildning af et vilkårligt vektorrum ind i sig selv, vil $g = 2f - e$ være involutorisk, og vis, at hver involutorisk lineær afbildning kan fås på denne måde.

Giv en geometrisk beskrivelse af forbindelsen mellem afbildningerne f og g , når vektorrummet er det geometriske vektorrum $(V_3, +, \mathbb{R})$.

50. Lad $(\underline{e}_1, \underline{e}_2)$ være en basis for det todimensionale geometriske vektorrum $(V_2, +, \mathbb{R})$ bestående af vektorerne i en plan. Idet alle vektorer tænkes afsat fra samme punkt, forudsættes om en lineær afbildning f af $(V_2, +, \mathbb{R})$ ind i sig selv, at billedvektorerne $f(\underline{e}_1)$ og $f(\underline{e}_2)$ begge falder i det indre af det mindste af de to vinkelrum, der bestemmes af $\underline{e}_1$ og $\underline{e}_2$. Vis, at f har to forskellige egenverdier. (Nødvendigt og tilstrækkeligt for, at en (2×2) -matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ikke er regulær, er $ad - bc = 0$, jfr. øv. 27.)

51. Vis, at Legendre polynomierne

$$P_n(t) = (2^n n!)^{-1} D^n(t^2 - 1)^n, \quad n=0,1,2,\dots,$$

er egenfunktioner for den lineære differentialoperator

$$(t^2 - 1)D^2 + 2tD,$$

der til hver funktion $\varphi(t) \in \hat{C}^2(\mathbb{R} \rightarrow \mathbb{R})$ lader svare funktionen $(t^2 - 1)D^2\varphi(t) + 2tD\varphi(t) \in \hat{C}(\mathbb{R} \rightarrow \mathbb{R})$, og angiv de til-

hørende egenverdier. (Differentier identiteten

$$(t^2 - 1) D(t^2 - 1)^n = 2nt(t^2 - 1)^n$$

$n+1$ gange ved benyttelse af Leibniz' formel

$$D^p(uv) = \sum_{i=0}^p \binom{p}{i} D^i(u) D^{p-i}(v)$$

for den p -te afledede af et produkt af to funktioner.) Gør rede for, at Legendre-polynomierne danner en basis for vektorrummet $(\hat{P}(\mathbb{R} \rightarrow \mathbb{R}), +, \mathbb{R})$ af reelle polynomier, og vis derpå, at der ikke er andre polynomier end de med Legendre polynomier proportionale, som er egenfunktioner for den betragtede differentialoperator.

§ 12. Bilineære og kvadratiske former.

Lad der være givet to vektorrum $(U, +, L)$ og $(V, +, L)$ over samme tallegeme L . En funktion $B: U \times V$ ind i L siges at være en bilinearform, hvis $B(\underline{u}, \underline{v})$ for hver fast vektor $\underline{v} \in V$ er en linearform på U , og for hver fast vektor $\underline{u} \in U$ er en linearform på V , eller med andre ord, hvis der gælder

$$B(\underline{u}_1 + \underline{u}_2, \underline{v}) = B(\underline{u}_1, \underline{v}) + B(\underline{u}_2, \underline{v})$$

$$B(\lambda \underline{u}, \underline{v}) = \lambda B(\underline{u}, \underline{v})$$

$$B(\underline{u}, \underline{v}_1 + \underline{v}_2) = B(\underline{u}, \underline{v}_1) + B(\underline{u}, \underline{v}_2).$$

$$B(\underline{u}, \mu \underline{v}) = \mu B(\underline{u}, \underline{v}).$$

Hvis man adderer to bilinearformer på $U \times V$ får man åbenbart igen en bilinearform på $U \times V$, og på samme måde går det, dersom man multiplicerer en bilinearform med en skalar fra L . Man ser altså, at bilinearformerne på $U \times V$ udgør et vektorrum over L .

Dersom U' og V' er underrum i henholdsvis U og V , vil restriktionen af en bilinearform B til $U' \times V'$ åbenbart være en bilinearform på $U' \times V'$, idet de ovenfor opskrevne betingelsesligninger jo specielt gælder for underrummene.

Det antages nu, at $(U, +, L)$ og $(V, +, L)$ har de endelige dimensioner m og n . Lad der være valgt baser $(\underline{e}_1, \dots, \underline{e}_m)$ og $(\underline{f}_1, \dots, \underline{f}_n)$ i henholdsvis U og V . Idet

$$\underline{u} = u_1 \underline{e}_1 + \dots + u_m \underline{e}_m,$$

$$\underline{v} = v_1 \underline{f}_1 + \dots + v_n \underline{f}_n,$$

får man ved en gentagen anvendelse af de ovenfor opskrevne linearitetsbetingelser, at

$$B(\underline{u}, \underline{v}) = \sum_{i=1}^m \sum_{j=1}^n u_i v_j B(\underline{e}_i, \underline{f}_j).$$

Sættes

$$B(\underline{e}_i, \underline{f}_j) = b_{ij}, \quad (b_{i,j})_{i=1, \dots, m; j=1, \dots, n} = \underline{\underline{B}}$$

kan formelen kort skrives som matrixligningen

$$B(\underline{u}, \underline{v}) = \underline{\underline{u}} \underline{\underline{B}} \underline{\underline{v}}.$$

Heraf ses, at en bilinearform er fuldstændig bestemt ved de værdier, som den antager for de mn par $(\underline{e}_i, \underline{f}_j)$ af basisvektorer, idet disse værdier bestemmer $(m \times n)$ -matricen $\underline{\underline{B}}$. Omvendt vil der for en vilkårlig opgiven $(m \times n)$ -matrix $B = (b_{ij})$, $b_{ij} \in L$, ved ovenstående matrixligning defineres en bilinearform B over L på $U \times V$, for hvilken $B(\underline{e}_i, \underline{f}_j) = b_{ij}$. Og man ser, at vektorrummet af bilinearformer på $U \times V$ over L bliver isomorft med vektorrummet af $(m \times n)$ -matricer $\underline{\underline{B}}$ over L .

Man bemærker også, at for en fastholdt vektor $\underline{v} \in V$ er $B(\underline{u}, \underline{v})$ netop den linearform på vektorrummet U , hvis koefficientsæt (skrevet som søjle) er $\underline{\underline{B}} \underline{\underline{v}}$, og tilsvarende, at for en fastholdt vektor $\underline{u} \in U$ er $B(\underline{u}, \underline{v})$ netop den linearform på vektorrummet V , hvis koefficientsæt (skrevet som række) er $\underline{\underline{u}} \underline{\underline{B}}$.

For at undersøge, hvorledes matricen $\underline{\underline{B}}$ ændres ved overgangen til nye baser $(\hat{\underline{e}}_1, \dots, \hat{\underline{e}}_m)$ og $(\hat{\underline{f}}_1, \dots, \hat{\underline{f}}_n)$ i U og V , antages koordinattransformationsformlerne løst med hensyn til de oprindelige koordinater. De kan da skrives

$$\underline{\underline{u}} = \underline{\underline{S}} \underline{\underline{\hat{u}}}, \quad \underline{\underline{v}} = \underline{\underline{T}} \underline{\underline{\hat{v}}},$$

hvor $\underline{\underline{\hat{u}}}$ og $\underline{\underline{\hat{v}}}$ er de nye koordinatsæt for $\underline{u}$ og $\underline{v}$ og hvor $\underline{\underline{S}}$ er en regulær $(m \times m)$ -matrix og $\underline{\underline{T}}$ en regulær $(n \times n)$ -matrix. Ved transponering af den første ligning fås $\underline{\underline{u}} = \underline{\underline{\hat{u}}} \underline{\underline{S}}'$, og derfor

$$B(\underline{u}, \underline{v}) = \underline{\underline{u}} \underline{\underline{B}} \underline{\underline{v}} = \underline{\underline{\hat{u}}} \underline{\underline{S}}' \underline{\underline{B}} \underline{\underline{T}} \underline{\underline{\hat{v}}}.$$

Heraf ser man, at den matrix, som ved de nye baser hører til bilinearformen bliver

$$\hat{\underline{\underline{B}}} = \underline{\underline{S}}' \underline{\underline{B}} \underline{\underline{T}}.$$

Man bør bemærke, at denne formel for ændringen af en bilinear-forms matrix ved basisskifte er en væsentlig anden end formelen for ændringer af en lineær afbildnings matrix ved basisskifte: Dersom B er matrix for en lineær afbildning $\underline{u}_i = \underline{B}\underline{v}_i$ af V ind i U , så vil de samme basisskifter som ovenfor give en matrix $\underline{S}^{-1}\underline{B}\underline{T}$ for den lineære afbildning (se AG III, 2, 37, hvor dog $\underline{S}$ og $\underline{T}$ har en anden betydning end her).

Ved rangen af bilinearformen $B(u,v)$ forstår man rangen af matricen $\underline{B}$, idet man bemærker, at denne rang er uafhængig af de anvendte baser for U og V , thi matricerne $\underline{S}$ (og dermed $\underline{S}'$) og $\underline{T}$ er jo regulære kvadratiske matricer, så at $\underline{B}$ og $\hat{\underline{B}}$ har samme rang.

I alt det følgende vil vi antage, at $(U,+,L)$ og $(V,+,L)$ er det samme vektorrum, betegnet $(V,+,L)$, og bilinearformerne defineret på $V \times V$ vil vi kort kalde for bilinearformer på V . Af tidligere betragtede eksempler på sådanne kan nævnes dels volumenmålet (arealmålet) i et 2-dimensionalt vektorrum, og dels det indre produkt i et vektorrum over det reelle tallegeme.

Man kalder en sådan bilinearform symmetrisk, dersom

$$B(\underline{u},\underline{v}) = B(\underline{v},\underline{u})$$

for alle vektorer $\underline{u}, \underline{v} \in V$. Man kalder en sådan bilinearform antisymmetrisk (skøvsymmetrisk) eller alternerende, dersom

$$B(\underline{u},\underline{v}) = -B(\underline{v},\underline{u})$$

for alle vektorer $\underline{u}, \underline{v} \in V$; den sidste ligning medfører specielt, at $B(\underline{v},\underline{v}) = 0$ for alle $\underline{v} \in V$ i overensstemmelse med en tidligere definition af "alternerende multilinearform".

Dersom V er endeligdimensional, kan $B(\underline{u},\underline{v})$ efter valg af en basis angives ved sin matrix $\underline{B}$. Da en (1×1) -matrix er lig

sin transponerede, bliver

$$B(\underline{u}, \underline{v}) = \underline{u} \underline{B} \underline{v} = \underline{v} \underline{B}' \underline{u},$$

hvoraf man ser, at $B(\underline{u}, \underline{v})$ er symmetrisk netop når $\underline{B} = \underline{B}'$, d.v.s. netop når $\underline{B}$ er symmetrisk, og at $B(\underline{u}, \underline{v})$ er antisymmetrisk netop når $\underline{B} = -\underline{B}'$, d.v.s. netop når $\underline{B}$ er antisymmetrisk.

Enhver bilinearform $B(\underline{u}, \underline{v})$ på et vektorrum V kan på en og een måde skrives som sum af en symmetrisk og en antisymmetrisk bilinearform, nemlig henholdsvis $B_s(\underline{u}, \underline{v}) = \frac{1}{2}(B(\underline{u}, \underline{v}) + B(\underline{v}, \underline{u}))$ og $B_a(\underline{u}, \underline{v}) = \frac{1}{2}(B(\underline{u}, \underline{v}) - B(\underline{v}, \underline{u}))$. Thi man ser umiddelbart, at disse er henholdsvis symmetrisk og antisymmetrisk og har summen $B(\underline{u}, \underline{v})$; fremstillingen er entydig, for hvis $B_{s_1} + B_{a_1} = B_{s_2} + B_{a_2}$ får man $B_{s_1} - B_{s_2} = B_{a_2} - B_{a_1}$, og denne bilinearform skal altså være både symmetrisk og antisymmetrisk, hvilket kun er opfyldt af nulformen. For endeligdimensionale vektorrum ses dette at være i overensstemmelse med at en kvadratisk matrix $\underline{B}$ på en og kun een måde kan skrives som sum af en symmetrisk og en antisymmetrisk matrix, nemlig henholdsvis $\underline{B}_s = \frac{1}{2}(\underline{B} + \underline{B}')$ og $\underline{B}_a = \frac{1}{2}(\underline{B} - \underline{B}')$.

Ved den til en bilinearform $B(\underline{u}, \underline{v})$ hørende kvadratiske form forstår vi funktionen $B(\underline{v}, \underline{v})$, som afbilder V ind i L , eller med andre ord: den kvadratiske form er bilinearformens restriktion til diagonalen i $V \times V$. Når B er spaltet i symmetrisk og antisymmetrisk del $B = B_s + B_a$, bliver den kvadratiske form $B(\underline{v}, \underline{v}) = B_s(\underline{v}, \underline{v}) + B_a(\underline{v}, \underline{v}) = B_s(\underline{v}, \underline{v})$ og den er altså bestemt alene ved B_s ; men på den anden side er $B_s(\underline{u}, \underline{v})$ bestemt entydigt ved den kvadratiske form, altså ved sin restriktion til diagonalen i $V \times V$, thi ved at benytte linearitetsbetingelserne og at B_s er symmetrisk, finder man, at

$$B_s(\underline{u} + \underline{v}, \underline{u} + \underline{v}) - B_s(\underline{u} - \underline{v}, \underline{u} - \underline{v}) = 4 B_s(\underline{u}, \underline{v}).$$

Vi har altså, at enhver kvadratisk form $B(\underline{v}, \underline{v})$ hører til en klasse af bilinearformer $B(\underline{u}, \underline{v})$, og enhver sådan klasse indeholder netop een symmetrisk repræsentant.

Ved den nærmere undersøgelse af kvadratiske former i det følgende vil vi derfor kun betragte symmetriske bilinearformer $B(\underline{u}, \underline{v})$.

Eksempel: Dersom $(V, +, L) = (\mathbb{R}^2, +, \mathbb{R})$ og

$$\underline{B} = \begin{pmatrix} 3 & 6 \\ 2 & 0 \end{pmatrix}$$

så er den tilsvarende bilinearform $B(\underline{u}, \underline{v}) = 3u_1v_1 + 6u_1v_2 + 2u_2v_1$ og den kvadratiske form $B(\underline{v}, \underline{v}) = 3v_1^2 + 8v_1v_2$, og den symmetriske matrix for denne og for den tilsvarende symmetriske bilinearform er

$$\underline{B}_s = \begin{pmatrix} 3 & 4 \\ 4 & 0 \end{pmatrix}.$$

Når V er endeligdimensional, så er efter valg af en basis $\underline{v} = v_1\underline{e}_1 + \dots + v_n\underline{e}_n$, og $B(\underline{v}, \underline{v}) = \underline{v} \underline{B} \underline{v}$ bliver åbenbart en sum af led $b_{ij}v_i v_j$, altså et homogent andengradspolynomium i koordinaterne, og omvendt ser man, at ethvert sådant polynomium åbenbart kan skrives på formen $\underline{v} \underline{B} \underline{v}$ med en passende koefficientmatrix $\underline{B}$. Derfor: I et endeligdimensionalt vektorrum, hvori der er valgt en basis, er mængden af kvadratiske former $B(\underline{v}, \underline{v})$ identisk med mængden af homogene andengradspolynomier i koordinaterne for $\underline{v}$.

To vektorer $\underline{u}$ og $\underline{v}$ siges at være konjugerede med hensyn til den symmetriske bilinearform B , dersom $B(\underline{u}, \underline{v}) = 0$. Da $B(\underline{u}, \underline{v}) = B(\underline{v}, \underline{u})$ er dette en symmetrisk relation i V (og talemåden " $\underline{u}$ og $\underline{v}$ er konjugerede" er altså berettiget).

Mængden af de med hensyn til en vis bilinearform til en givne vektor $\underline{u}_0$ konjugerede vektorer betegnes $K(\underline{u}_0)$, (eller $K_B(\underline{u}_0)$) hvis man vil fremhæve, at det er med hensyn til bilinearformen B). Da $K(\underline{u}_0)$ netop er kernen ved den lineære afbildning $B(\underline{u}_0, \underline{v})$, $\underline{v} \in V$ af V ind i L , må $K(\underline{u}_0)$ være et underrum i V .

Er der givet en mængde M af vektorer i V , så vil de vektorer $\underline{v}$, som med hensyn til en vis bilinearform er konjugerede med samtlige vektorer $\underline{u} \in M$ udgøre et underrum, nemlig

$$K(M) = \bigcap_{\underline{u} \in M} K(\underline{u}),$$

og dette kaldes det fuldstændige til M konjugerede underrum med hensyn til den givne linearform. Man ser, at K er en operation, der afbilder mængden af delmængder af V ind i mængden af delmængder af V . Man har

$$(1) \quad M \subseteq K \circ K(M),$$

thi blandt de vektorer, som er konjugerede med $K(M)$ findes jo specielt vektorerne i M . Endvidere vil åbenbart

$$(2) \quad M_1 \subseteq M_2 \Rightarrow K(M_1) \supseteq K(M_2).$$

Af (1) og (2) fås $K(M) \supseteq K \circ K \circ K(M)$, medens man ved at indsætte $K(M)$ i stedet for M i (1) får, at $K(M) \subseteq K \circ K \circ K(M)$, så at

$$(3) \quad K(M) = K \circ K \circ K(M).$$

Heraf ser man, at man har inklusionskæderne $M \subseteq K^{\circ 2}(M) = K^{\circ 4}(M) = \dots$ og $K(M) = K^{\circ 3}(M) = K^{\circ 5}(M) = \dots$, og at operationen $K^{\circ 2}$ er idempotent. Specielt ser man ved at benytte (1) og (3), at for enhver mængde M_1 , hvor $M \subseteq M_1 \subseteq K^{\circ 2}(M)$, bliver $K(M_1) = K(M)$; da $K^{\circ 2}(M)$ er et vektorrum, vil det af M frembragte underrum $V(M)$ (som er det mindste vektorrum, der indeholder M) være en sådan mængde M_1 , og vi har derfor

$$(4) \quad K(M) = K(V(M)).$$

Man kalder to underrum for konjugerede underrum med hensyn til

bilinearformen, hvis enhver vektor i det ene er konjugeret med enhver vektor i det andet, og så gælder øjensynlig, at hvert af to konjugerede underrum er indeholdt i det andets fuldstændige konjugerede underrum.

Ved nulrummet $N = N_B$ for en bilinearform B defineret på vektorrummet $(V, +, L)$ forstår man $K(V)$. For ethvert $M \subseteq V$ har man $N \subseteq K(M)$. Man kan også beskrive N som mængden af de vektorer $\underline{u}_0$, for hvilke $B(\underline{u}_0, \underline{v})$ - betragtet som linearform i $\underline{v}$ - er nulformen.

En vektor $\underline{v}$ kan være selvkonjugeret, altså opfylde $B(\underline{v}, \underline{v}) = 0$. Selvkonjugerede vektorer kaldes også isotrope for bilinearformen (eller for den kvadratiske form). Enhver vektor tilhørende nulrummet N_B er åbenbart isotrop for B , men der kan også findes andre. Mængden af isotrope vektorer er ikke i almindelighed noget underrum.

Når V er endeligdimensional, $\dim V = n$, kan vi præcisere resultaterne. Vi skal her benytte sætningen: Lad $\underline{Ax} = \underline{0}$ være et lineært homogent ligningssystem over legemet L , således at koef-
ficientmatricen $\underline{A}$ er en $(m \times n)$ -matrix, og $\underline{x}$ er en $(n \times 1)$ -søjle
af ubekendte (en vektor i $(L^n, +, L)$), og $\underline{0}$ er en $(m \times 1)$ -nulsøjle,
så vil løsningsvektorerne $\underline{x}$ udgøre et underrum af dimension $n-r$
indenfor $(L^n, +, L)$, idet $r = \text{rg } \underline{A}$. Denne sætning står implicit formuleret i AG III, § 11.

Nulrummet N er mængden af vektorer $\underline{v}$, for hvilke $B(\underline{u}, \underline{v}) = \underline{u} \cdot \underline{Bv} = 0$ for alle $\underline{u}$, og det ses netop at være mængden af $\underline{v}$, for hvilke $\underline{Bv} = \underline{0}$, og af den ovennævnte sætning ser man, at $\dim N = n - \text{rg } \underline{B}$. Dersom nulrummet kun består af nulvektoren siges bilinearformen at være regulær eller ikke-udartet, og dette indtræffer altså netop når $\text{rg } \underline{B} = n$. Dersom $\text{rg } \underline{B} < n$ vil nul-

rummet bestå af mere end nulvektoren, og så siges bilinearformen at være singular eller udartet.

Vi kan for V vælge en basis ved først at vælge $n-r$ basiselementer $\underline{e}_{r+1}, \dots, \underline{e}_n$ for nulrummet, og så supplere dem med elementer $\underline{e}_1, \dots, \underline{e}_r$ til en basis for hele V . I matricen $\underline{B}$ er $b_{ij} = B(\underline{e}_i, \underline{e}_j)$, og man ser, at med den valgte basis får $\underline{B}$ udseendet

$$\underline{B} = \begin{pmatrix} \underline{B}_{r,r} & \underline{0}_{r,n-r} \\ \underline{0}_{n-r,r} & \underline{0}_{n-r,n-r} \end{pmatrix}$$

med 0 overalt undtagen i det øvre venstre hjørne, hvor $\underline{B}_{r,r}$ er en $(r \times r)$ -matrix, og dennes rang er r , da jo $\text{rg } \underline{B} = r$.

Lad nu M_1 være en delmængde af V , vi vil betragte $K(M_1)$. Det er ovenfor vist, at $K(V(M_1)) = K(M_1)$, og da nulrummet er konjugeret med alle vektorer, er endda $K(M_1) = K(V(M_1, N))$. Vi sætter $V(M_1, N) = M$, og vil så undersøge $K(M)$, hvor altså M er et underrum som indeholder nulrummet. Vi sætter $\dim M = n-s$, hvor $n-s \geq n-r = \dim N$, så at $s \leq r$.

Ved det foregående valg af basis kunne vi, efter først at have valgt $\underline{e}_{r+1}, \dots, \underline{e}_n$ som basis for nulrummet, supplere med $r-s$ elementer $\underline{e}_{s+1}, \dots, \underline{e}_r$ til en basis for M , og så endelig supplere til en basis for hele V . Nødvendigt og tilstrækkeligt for at $\underline{v}$ er konjugeret med M er, at $B(\underline{e}_j, \underline{v}) = 0$ for samtlige basisvektorer $\underline{e}_j$ for M , altså at

$$\underline{e}_{j-} \underline{B} \underline{v} = 0 \quad \text{for } j = s+1, \dots, n.$$

Her er $\underline{e}_{j-}$ en rækkematrix med 1 på den j 'te plads og 0 på de øvrige pladser. Disse $n-s$ matrixligninger kan samles i en matrixligning $\underline{R} \underline{B} \underline{v} = \underline{0}$, hvor $\underline{R}$ består af de nævnte rækker, og altså er en $((n-s) \times n)$ -matrix

$$\underline{R} = \begin{pmatrix} \underline{0}_{n-s,s} & \underline{E}_{n-s,n-s} \end{pmatrix},$$

(sammensat af en nulmatrix og en enhedsmatrix).

Ifølge den nævnte sætning om ligningssystemer bliver nu $\dim K(M) = n - \operatorname{rg}(\underline{R} \ \underline{B})$. Da $\underline{R}$ består af de underste $n-s$ rækker af en $(n \times n)$ -enhedsmatrix, vil $\underline{R} \ \underline{B}$ bestå af de underste $n-s$ rækker af $(n \times n)$ -matricen $\underline{B}$, og af den angivne form for $\underline{B}$ ser man, at $\underline{R} \ \underline{B}$ indeholder de underste $r-s$ rækker af $\underline{B}_{r,r}$, og har 0 på alle de øvrige pladser. Disse $r-s$ rækker er lineært uafhængige (da $\operatorname{rg} \underline{B}_{r,r} = r$), så at $\operatorname{rg}(\underline{R} \ \underline{B}) = r-s$. Vi har dermed fundet, at $\dim K(M) = n-(r-s)$, og $\dim M + \dim K(M) = (n-s)+(n-r+s) = n+(n-r) = \dim V + \dim N$, uafhængigt af M . Hvis man i den sidste formel erstatter M med $K(M)$, får man at $\dim K \circ K(M) = \dim M$, og da $M \subseteq K \circ K(M)$ bliver $M = K \circ K(M)$. For en regulær bilinearform bliver $\dim M + \dim K(M) = \dim V$, og at man så i almindelighed finder $\dim M + \dim K(M) = \dim V + \dim N$ kan forekomme ret naturligt, da N er indeholdt i både M og $K(M)$; man skal ikke lægge for meget i denne betragtning (smlgn. øv. 18).

Lad os sammenfatte resultatet: Hvis man i et endeligdimensionalt vektorrum V har et underrum M som indeholder nulrummet N , så er $\dim M + \dim K(M) = \dim V + \dim N$, og endvidere er $K \circ K(M) = M$; hvis man har en vilkårlig vektormængde M_1 , så er $K \circ K(M_1)$ lig det af M_1 og N frembragte underrum $V(M_1, N)$, og endvidere er $\dim V \leq \operatorname{rg} M_1 + \dim K(M_1) \leq \dim V + \dim N$. (Den sidste ulighed følger af at $\operatorname{rg} M_1 \leq \dim V(M_1, N) \leq \operatorname{rg} M_1 + \dim N$).

Vi har foran set, at man ved et specielt valg af basis kunne opnå et simplere udseende af matricen $\underline{B}$. Vi vil nu vise, at man endda kan vælge basis således, at $\underline{B}$ bliver en diagonalmatrix. Da elementerne i $\underline{B}$ er $b_{ij} = B(\underline{e}_i, \underline{e}_j)$, er dette åbenbart ensbetydende med at vise, at man kan vælge basisvektorerne indbyrdes konjugerede.

For enhver symmetrisk bilinearform B på et n -dimensionalt vektorrum $(V, +, L)$ findes der mindst én basis $(\underline{e}_1, \dots, \underline{e}_n)$ bestående af vektorer, som er parvis konjugerede med hensyn til B , dvs. for hvilken matricen $\underline{B}$ er symmetrisk.

For $n = 1$ gælder påstanden, da en $(1 \ 1)$ -matrix altid er symmetrisk. Sætningen bevises nu ved induktion, idet vi for at vise den gyldig for vektorrummet V vil antage den gyldig for alle vektorrum U , hvor $\dim U = \dim V - 1$. Hvis $B(\underline{v}, \underline{v})$ er nulformen, så er B en nulmatrix, og altså diagonalmatrix. Hvis $B(\underline{v}, \underline{v})$ ikke er nulformen findes en vektor $\underline{e}_1$, således at $B(\underline{e}_1, \underline{e}_1) \neq 0$, og derfor $\underline{e}_1 \notin K(\underline{e}_1)$, og specielt $\underline{e}_1 \notin N$. Vi har $\dim V(\underline{e}_1, N) = \dim N + 1$, og derfor $\dim K(\underline{e}_1) = \dim V + \dim N - (\dim N + 1) = \dim V - 1$. Restriktionen af $B(\underline{u}, \underline{v})$ til $K(\underline{e}_1) \times K(\underline{e}_1)$ er en symmetrisk bilinearform, og ifølge induktionsforudsætningen findes der i $K(\underline{e}_1)$ en basis $(\underline{e}_2, \underline{e}_3, \dots)$, for hvilken $B(\underline{e}_i, \underline{e}_j) = 0$ for $i \neq j$; $i, j = 2, 3, \dots$. Endvidere er $B(\underline{e}_1, \underline{e}_j) = 0$ for $j = 2, 3, \dots$ da $\underline{e}_j \in K(\underline{e}_1)$. Og $\underline{e}_1, \underline{e}_2, \underline{e}_3, \dots$ er en basis for hele V , thi da $\underline{e}_1 \notin K(\underline{e}_1)$ er $\dim V(\underline{e}_1, K(\underline{e}_1)) > \dim K(\underline{e}_1) = \dim V - 1$, så at $\dim V(\underline{e}_1, K(\underline{e}_1)) = \dim V$. Dermed er sætningen bevist.

Vi har foran (side 2) fundet, hvorledes en bilinearforms matrix ændres ved basisskifte; i den nu foreliggende situation er $B(\underline{u}, \underline{v})$ en symmetrisk bilinearform, og $\underline{u}$ og $\underline{v}$ ligger begge i det samme vektorrum, således at begges koordinatsæt ændres ved den samme matrix $\underline{T}$; basisskiftet bevirker altså, at den symmetriske matrix $\underline{B}$ overføres i matricen $\underline{T}' \underline{B} \underline{T}$ (som også er symmetrisk).

Den foregående sætning kan så udtrykkes som en sætning om matricer: Til enhver symmetrisk $(n \times n)$ -matrix $\underline{B}$ med elementer fra et tallegeme L findes der en regulær $(n \times n)$ -matrix $\underline{T}$ med

elementer fra L , således at $\underline{T}' \underline{B} \underline{T}$ er en diagonalmatrix.

Denne diagonalmatrix vides at have samme rang r som $\underline{B}$. Følgelig er netop r blandt de n diagonalelementer forskellige fra 0. Det er klart, at de nye basisvektorer kan nummereres således, at dette gælder for de første r diagonalelementer.

Hvis man betragter de to specielle tilfælde, hvor L er henholdsvis de komplekse tals legeme $\mathbb{C}$ og de reelle tals legeme $\mathbb{R}$, er det muligt at opnå skarpere resultater:

Hvis $(V, +, \cdot)$ er et n -dimensionalt vektorrum over de komplekse tals legeme, og B er en symmetrisk bilinearform af rang r på V , så kan vi ifølge det forrige finde en basis, således at $\underline{B}$ har

$$b_{ii} = B(\underline{e}_i, \underline{e}_i) \neq 0 \quad \text{for } i = 1, \dots, r,$$

medens alle øvrige b_{ij} er 0. Der findes komplekse tal $\beta_1, \dots, \beta_r$, således at $\beta_i^2 b_{ii} = 1$ for $i = 1, \dots, r$. Vektorsættet

$(\beta_1 \underline{e}_1, \dots, \beta_r \underline{e}_r, \underline{e}_{r+1}, \dots, \underline{e}_n)$ er da en ny basis, og da $B(\beta_i \underline{e}_i, \beta_i \underline{e}_i) = \beta_i^2 b_{ii} = 1$, vil den tilhørende matrix være en diagonalmatrix, hvis første r diagonalelementer er 1, medens alle øvrige elementer er 0. For bilinearformen fås i dette koordinatsystem

$$B(\underline{u}, \underline{v}) = u_1 v_1 + \dots + u_r v_r.$$

Ved passende valg af basis kan altså enhver kompleks symmetrisk bilinearform af rang r bringes på denne "normalform".

Udtrykt som et matrixresultat bliver sætningen:

Til enhver symmetrisk $(n \times n)$ -matrix $\underline{B}$ af komplekse tal findes der mindst een regulær $(n \times n)$ -matrix $\underline{T}$ af komplekse tal, således at

$$\underline{T}' \underline{B} \underline{T} = \begin{pmatrix} \underline{E}_{r,r} & \underline{O}_{r,n-r} \\ \underline{O}_{n-r,r} & \underline{O}_{n-r,n-r} \end{pmatrix},$$

d.v.s. lig en $(n \times n)$ -matrix, der har en $(r \times r)$ -enhedsmatrix i øvre

venstre hjørne, og 0 på alle øvrige pladser.

For reelle symmetriske bilinearformer får man analoge resultater; de bliver knap så simple, men mere nuancerede:

Når $(V, +, \cdot)$ er et n -dimensionalt vektorrum over de reelle tals legeme, og B er en bilinearform med symmetrisk matrix $\underline{B}$, hvor

$$b_{ii} = B(\underline{e}_i, \underline{e}_i) \neq 0 \quad \text{for } i = 1, \dots, r,$$

medens alle øvrige b_{ij} er 0, så findes der reelle tal $\beta_1, \dots, \beta_r$, således at $\beta_i^2 |b_{ii}| = 1$ for $i = 1, \dots, r$. Vektorsættet

$(\beta_1 \underline{e}_1, \dots, \beta_r \underline{e}_r, \underline{e}_{r+1}, \dots, \underline{e}_n)$ er da en ny basis, og da $B(\beta_i \underline{e}_i, \beta_j \underline{e}_j) = \beta_i \beta_j b_{ij} = \pm 1$, vil den tilhørende matrix være en diagonalmatrix, hvis første r diagonalelementer er $+1$ eller -1 , medens alle øvrige elementer er 0. Ved omnummerering af basisvektorerne kan man altid opnå, at de første diagonalelementer $b_{11}, \dots, b_{pp}$ bliver $+1$ (hvor $p \geq 0$), medens de påfølgende $b_{p+1,p+1}, \dots, b_{rr}$ bliver -1 (hvor $p \leq r$), og sluttelig kommer diagonalelementerne $b_{r+1,r+1}, \dots, b_{nn}$ (hvor $r = \text{rg } \underline{B} \leq N$), som er lig 0. For bilinearformen fås i dette koordinatsystem

$$B(\underline{u}, \underline{v}) = u_1 v_1 + \dots + u_p v_p - u_{p+1} v_{p+1} - \dots - u_r v_r.$$

Ved passende valg af basis kan altså enhver reel symmetrisk bilinearform af rang r bringes på en sådan form.

I almindelighed vil der være uendelig mange koordinatsystemer i hvilke en given bilinearform har en sådan fremstilling. Dette fremgår bl.a. af, at der i beviset (side 10) allerede var en overordentlig stor frihed i valget af det første basiselement $\underline{e}_1$ (og vi skal også senere i denne § se, at vi kan stille stærke yderligere krav til basisvektorerne). Men vi skal vise, at ligesom tallet $r = \text{rg } \underline{B}$ for en given bilinearform B er uafhængigt af basisvalget, så er også for en given bilinearform

antallet p af plusled i fremstillingen uafhængigt af basisvalget (og dermed altså også antallet $r-p$ af minusled), således at man kan sige, at disse antal er af koordinatsystemet uafhængige "invarianter" for bilinearformen (Sylvester's trægthedssætning; Sylvester 1814-1893).

For den tilsvarende kvadratiske form får vi fremstillingen

$$B(\underline{y}, \underline{y}) = v_1^2 + \dots + v_p^2 - v_{p+1}^2 - \dots - v_r^2.$$

På underrummet P frembragt af de første p basisvektorer er restriktionen af $B(\underline{y}, \underline{y})$ lig $v_1^2 + \dots + v_p^2$, og derfor $B(\underline{y}, \underline{y}) \geq 0$ og kun lig 0 for $\underline{y} = \underline{0}$ (formen er "positiv definit" på dette underrum). På underrummet S frembragt af de sidste $n-p$ basisvektorer er restriktionen af $B(\underline{y}, \underline{y})$ lig $-v_{p+1}^2 - \dots - v_r^2$, og derfor $B(\underline{y}, \underline{y}) \leq 0$ (formen er "negativ semidefinit" på dette underrum; den kan evt. antage værdien 0 for egentlige vektorer, nemlig for vektorer fra nulrummet). For et andet basisvalg kunne vi få p' plusled og tilsvarende underrum P' og S' , på hvilke restriktionen af $B(\underline{y}, \underline{y})$ er hhv. positiv definit og negativ semidefinit. Da åbenbart $B(\underline{y}, \underline{y}) = 0$ for $\underline{y} \in P' \cap S'$ bliver $P' \cap S' = \{\underline{0}\}$, og derfor

$\dim(P' + S') = \dim P' + \dim S' - \dim(P' \cap S') = p' + (n-p) - 0$, og da dimensionen af et underrum højst kan være n , får vi $p' \leq p$; analogt fås $p \leq p'$, og derfor $p = p'$, hvormed Sylvester's sætning er bevist.

Et underrum, på hvilket restriktionen af en kvadratisk form er positiv definit (altså ≥ 0 og kun lig 0 for $\underline{y} = \underline{0}$), kaldes et positivitetsunderrum for formen. Dersom man i det forrige bevis (de sidste fem linier) i stedet for P' benyttede et vilkårligt positivitetsunderrum, fandt man, at dets dimension var mindre end eller lig p . Et underrum, på hvilket restriktionen

af en kvadratisk form er negativ definit (altså ≤ 0 og kun lig 0 for $\underline{y} = \underline{0}$), kaldes et negativitetsunderrum for formen. Ved i stedet for $B(\underline{y}, \underline{y})$ at betragte $-B(\underline{y}, \underline{y})$ finder man, at dimensionen af et vilkårligt negativitetsunderrum er mindre end eller lig antallet $r-p$ af minusled i fremstillingen ovenfor.

Tallet p kan derfor uafhængigt af koordinatsystemet karakteriseres som den maximale dimension for et positivitetsunderrum for den kvadratiske form; det kaldes også for formens positivitetsindex, og betegnes $\text{ind}_+ B$. Tallet $q = r-p$ kan uafhængigt af koordinatsystemet karakteriseres som den maximale dimension for et negativitetsunderrum for den kvadratiske form; det kaldes også for formens negativitetsindex, og betegnes $\text{ind}_- B$. Resultatet af det foregående kan derfor formuleres som følger:

Til enhver symmetrisk bilinearform B på et n -dimensionalt vektorrum over de reelle tals legeme findes der baser, i hvilke

$$B(\underline{u}, \underline{v}) = u_1 v_1 + \dots + u_p v_p - u_{p+1} v_{p+1} - \dots - u_{p+q} v_{p+q}.$$

For alle sådanne baser er tallene p og q de samme, nemlig hhv. formens positivitetsindex $\text{ind}_+ B$ og dens negativitetsindex $\text{ind}_- B$, og $p+q$ er formens rang $\text{rg } B$.

Og som resultat om matricer: Til enhver reel symmetrisk matrix B findes der reelle regulære matricer T , således at $T' B T$ er en diagonalmatrix, hvis diagonalelementer er $+1$, -1 eller 0 . For alle disse matricer T har $T' B T$ det samme antal elementer $+1$ og det samme antal elementer -1 , og summen af disse to antal er lig rangen af B .

Eksempel: Lad $B(\underline{y}, \underline{y})$ være en kvadratisk form med matricen

$$\underline{B} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

på et 3-dimensionalt vektorrum over et tallegeme; man ser, at

$r = \text{rg} \underline{B} = 2$, og at $B(\underline{v}, \underline{v}) = v_1^2 - v_2^2$; nulrummet N er mængden af vektorer $(0, 0, t)$. Dersom tallegemet er $\mathbb{C}$, kan man erstatte $\underline{e}_2$ med $i\underline{e}_2$, og derved bringe $B(\underline{v}, \underline{v})$ på normalformen $B(\underline{v}, \underline{v}) = v_1^2 + v_2^2$. Dersom tallegemet er $\mathbb{R}$, er dette ikke muligt, og som "normalform" har man $v_1^2 - v_2^2$; har man så $\text{ind}_+ B = 1$; udover $\{0\}$, som er både positivitetsrum og negativitetsrum, er positivitetsunderrummene de 1-dimensionale vektorrum, der består af alle multipla af en fast vektor $(a_0, b_0, 0)$, hvor $|a_0| > |b_0|$, og et negativitetsrum vil tilsvarende bestå af alle multipla af en fast vektor $(a_0, b_0, 0)$, hvor $|a_0| < |b_0|$.

De fundne resultater kan udnyttes på en måde, som bliver af betydning for det senere.

Lad $(V, +, L)$ være et vektorrum over et tallegeme L , og lad H være mængden af funktioner $F: V \rightarrow L$. Vi vil sige, at F_1 er lineær-ækvivalent (eller kort "ækvivalent") med F_2 (idet begge tilhører H), såfremt der findes en lineær bijektiv afbildning f af V ind på V , således at $F_2(\underline{v}) = F_1(f(\underline{v}))$ for alle $\underline{v}$ (eksempel: på $(\mathbb{R}, +, \mathbb{R})$ er $\sin 3x$ lineær-ækvivalent med $\sin x$).

Denne relation er virkelig en ækvivalensrelation. Lad os et øjeblik kort betegne mængden af lineære bijektive afbildninger f af V ind på V for G ; da vil ¹⁾ identiteten tilhøre G , hvilket medfører, at relationen er reflektiv, ²⁾ hvis $f \in G$ vil $f^{-1} \in G$ hvilket medfører at relationen er symmetrisk, og ³⁾ hvis $f \in G$ og $g \in G$ vil $g \circ f$ tilhøre G hvilket medfører at relationen er transitiv. Man bemærker i øvrigt, at ¹⁾, ²⁾ og ³⁾ netop udtrykker, at $(G, \circ)$ er en gruppe. Ved denne relation vil H altså blive opdelt i ækvivalensklasser.

Såfremt F_1 er lineær på $(V, +, L)$, vil alle dens ækvivalente være lineære på $(V, +, L)$, da jo så $F_2(\underline{v}) = F_1 \circ f(\underline{v})$ er lineær.

Såfremt $F_1(\underline{v})$ er en kvadratisk form på $(V, +, L)$, vil alle dens ækvivalente være kvadratiske former på $(V, +, L)$. Thi at $F_1(\underline{v})$ er en kvadratisk form betyder jo, at $F_1(\underline{v}) = B(\underline{v}, \underline{v})$, hvor $B(\underline{u}, \underline{v})$ er en symmetrisk bilinearform på $V \times V$, og betragter man nu $B(f(\underline{u}), f(\underline{v}))$ er denne åbenbart lineær i $\underline{u}$ og lineær i $\underline{v}$, altså en bilinearform, og endvidere symmetrisk (den ændres ikke når $\underline{u}$ og $\underline{v}$ ombyttes), og $F_1(f(\underline{v})) = B(f(\underline{v}), f(\underline{v}))$ er da en kvadratisk form på V . I øvrigt siger man også, at $B_1(\underline{u}, \underline{v})$ og $B_2(\underline{u}, \underline{v})$ er lineær-ækvivalente, og når $B_2(\underline{u}, \underline{v}) = B_1(f(\underline{u}), f(\underline{v}))$ for et $f \in G$.

For endelig-dimensionale vektorrum $(V, +, L)$ kan man få præcisere resultater.

Mængden af linearformer (lineære afbildninger af $(V, +, L)$ ind i L) på et n -dimensionalt vektorrum udgør netop to ækvivalensklasser, den ene bestående af nulformen alene, og den anden af alle øvrige linearformer.

At nulformen udgør en klasse for sig er klart, og vi skal blot vise, at to vilkårlige andre linearformer er ækvivalente. Lad $F_1(\underline{v})$ være en egentlig linearform; vi kan vælge en basis således at $F_1(\underline{v}) = v_1 = \underline{k}_1 - \underline{v}_1$, hvor $\underline{k}_1 = (1, 0, \dots, 0)$; så er $F_2(\underline{v})$ af formen $\underline{k}_2 - \underline{v}_1$. Vi søger en afbildning $f(\underline{v})$, på matrixform $\underline{v}_1 \rightarrow \underline{A}\underline{v}_1$ med en regulær matrix $\underline{A}$, således at $F_2(\underline{v}) = F_1(f(\underline{v}))$ eller på matrixform $\underline{k}_2 - \underline{v}_1 = \underline{k}_1 - \underline{A}\underline{v}_1$, d.v.s. vi søger $\underline{A}$ så $\underline{k}_2 = \underline{k}_1 - \underline{A}$; men højresiden heri er netop den første række i $\underline{A}$, så vi skal blot tage $\underline{k}_2$ (der ikke består af lutter 0) som første række i en regulær matrix, hvilket altid er muligt.

De kvadratiske former (og dermed de symmetriske bilinearformer) på et n -dimensionalt vektorrum over de komplekse tal udgør $n+1$ ækvivalensklasser, idet to former er lineær-ækvivalente hvis og kun hvis de er af samme rang. Som repræsentant for klas-

sen med rang r kan man tage formen $v_1^2 + \dots + v_r^2$ (henholdsvis $u_1 v_1 + \dots + u_r v_r$).

Thi lad i et vist koordinatsystem formen have matricen $\underline{B}$. En lineær bijektiv afbildning af vektorrummet på sig selv kan i koordinaterne udtrykkes ved at $\underline{v} \mapsto \underline{A}\underline{v}$, hvor $\underline{A}$ er en regulær matrix, og indsætter man $f(\underline{v})$ for $\underline{v}$ i formen, vil formens matrix blive $\underline{A}' \underline{B} \underline{A}$. Ifølge de foregående resultater kan man derved få ført formen over i en og kun én af de anførte repræsentanter (nemlig den med $r = \text{rg } B$). Da $0 \leq r \leq n$ ses, at der er $n+1$ ækvivalensklasser (af hvilke den med $r = 0$ kun består af nulformen).

De kvadratiske former (og dermed de symmetriske bilinearformer) på et n -dimensionalt vektorrum over de reelle tal udgør $(n+1)(n+2)/2$ ækvivalensklasser, idet to former er lineær-ækvivalente hvis og kun hvis de har samme negativitetsindex. Som repræsentant for klassen med indices p, q kan man tage formen $v_1^2 + \dots + v_p^2 - v_{p+1}^2 - \dots - v_{p+q}^2$ (henholdsvis $u_1 v_1 + \dots$ o.s.v.).

Dette følger på ganske samme måde som det foregående af de tidligere resultater. At antallet af par p, q af ikke-negative hele tal med $p+q \leq n$ har den i sætningen anførte værdi, fremgår ved optælling. Tallene p og q kaldes som tidligere anført invariant for formen, og de bestemmer altså dens klasse.

De positiv definite kvadratiske former er karakteriseret ved at $(p, q) = (n, 0)$, og de udgør altså én klasse. Ligelødes udgør de negativ definite former én klasse. De positiv semidefinite udgør $(n+1)$ klasser (af hvilke nulklassen er en og klassen af definite en anden), karakteriseret ved at $q = 0$, og tilsvarende for de negativ semidefinite. For de kvadratiske former i de øvrige klasser vil værdiområdet bestå af alle reelle tal.

I et euklidisk rum, d.v.s. et reelt endeligdimensionalt vektorrum $(V, +, \dot{\mathbb{R}})$ med indre produkt $\underline{u} \cdot \underline{v}$ vil som nævnt det indre produkt være et eksempel på en bilinearform. Det ved det indre produkt definerede normkvadrat $\|\underline{v}\|^2$ er en positiv definit kvadratisk form, og for en ortonormal basis bliver formens matrix en enhedsmatrix. Oriogonal bliver det samme som konjugeret, og formens nulrum består kun af nulvektoren. Omvendt ser man, at dersom man i et endeligdimensionalt vektorrum har en positiv definit kvadratisk form, så kan man sætte formens værdi lig $\|\underline{v}\|^2$, og får derved gjort rummet til et euklidisk rum med et indre produkt, som er den til formen svarende bilinearform. Og resultatet om at en positiv definit form er ækvivalent med en form, hvis matrix er en enhedsmatrix, beviser endnu engang, at man i et euklidisk rum kan vælge en ortonormal basis.

Vi skal nu vise en sætning om en bilinearform på et euklidisk rum, og den kan altså egentlig siges at omhandle et vektorrum på hvilket man har to bilinearformer, men det bliver væsentligt, at den til den ene af dem svarende kvadratiske form, nemlig $\|\underline{v}\|^2$, er positiv definit.

For enhver symmetrisk bilinearform B på et n -dimensionalt euklidisk rum $(V, +, \dot{\mathbb{R}})$ findes der mindst én ortonormal basis bestående af vektorer, som er parvis konjugerede med hensyn til B , d.v.s. for hvilken matricen B er en diagonalmatrix.

Sætningen betyder for de euklidiske rum en skærpelse af sætningen side 10. At der eventuelt kan findes flere baser med den søgte egenskab er klart, f.eks. vil jo for $B(\underline{u}, \underline{v}) = \underline{u} \cdot \underline{v}$ enhver ortonormal basis have egenskaben.

For $n = 1$ gælder påstanden, da en (1×1) -matrix altid er en diagonalmatrix. Sætningen bevises nu ved induktion, idet vi for at vise den gyldig for vektorrummet V vil antage den gyldig

for alle vektorrum U , hvor $\dim U = \dim V - 1$, og erindrer, at i et euklidisk rum V vil ethvert underrum U være euklidisk, idet man som indre produkt tager restriktionen af det indre produkt på V .

Som basisvektor $\underline{e}_1$ udtager vi nu blandt de normerede vektorer $\underline{w}$ en, for hvilken $B(\underline{w}, \underline{w})$ er maximal. En sådan forefindes, thi i et eller andet ortonormalt koordinatsystem (hvad der jo findes i det euklidiske rum) er de normerede vektorer karakteriserede ved at $w_1^2 + \dots + w_n^2 = 1$, så at deres koordinatsæt udgør en kompakt mængde i koordinatrummet $\mathbb{R}^n$, og i denne mængde vil der forefindes et talsæt $(w_1, \dots, w_n)$, for hvilket den i $\mathbb{R}^n$ kontinuerede funktion $\sum b_{ij} w_i w_j = B(\underline{w}, \underline{w})$ er maximal. Vi skal om lidt godtgøre, at $\underline{e}_1 \perp \underline{v}$ medfører $B(\underline{e}_1, \underline{v}) = 0$, og så kan beviset let fuldføres, thi $\dim(\underline{e}_1^\perp) = \dim V - 1$, og ifølge induktionsforudsætningen vil der i $\underline{e}_1^\perp$ findes en ortonormal basis $(\underline{e}_2, \underline{e}_3, \dots)$ for hvilken $B(\underline{e}_i, \underline{e}_j) = 0$, $i \neq j$; $i, j = 2, 3, \dots$; suppleret med $\underline{e}_1$ bliver det en ortonormal basis for V , og da også $B(\underline{e}_1, \underline{e}_j) = 0$ for $j = 2, 3, \dots$ er dens vektorer parvis konjugerede med hensyn til B .

For enhver vektor $\underline{u}$ gælder $B(\underline{u}, \underline{u}) \leq \|\underline{u}\|^2 B(\underline{e}_1, \underline{e}_1)$; thi for $\underline{u} = \underline{0}$ er det klart, og for en egentlig vektor $\underline{u}$ vil $\underline{w} = \underline{u}/\|\underline{u}\|$ være normeret, og derfor $B(\underline{u}, \underline{u}) = \|\underline{u}\|^2 B(\underline{w}, \underline{w}) \leq \|\underline{u}\|^2 B(\underline{e}_1, \underline{e}_1)$. Uligheden anvendes nu på $\underline{u} = \underline{e}_1 + \underline{v}$, idet vi antager $\underline{e}_1 \perp \underline{v}$, og vi finder

$$B(\underline{e}_1 + \underline{v}, \underline{e}_1 + \underline{v}) \leq \|\underline{e}_1 + \underline{v}\|^2 B(\underline{e}_1, \underline{e}_1) = (1 + \|\underline{v}\|^2) B(\underline{e}_1, \underline{e}_1);$$

da

$$B(\underline{e}_1 + \underline{v}, \underline{e}_1 + \underline{v}) = B(\underline{e}_1, \underline{e}_1) + B(\underline{v}, \underline{v}) + 2B(\underline{e}_1, \underline{v}),$$

fås ved subtraktion

$$2B(\underline{e}_1, \underline{v}) \leq \|\underline{v}\|^2 B(\underline{e}_1, \underline{e}_1) - B(\underline{v}, \underline{v}) = \phi(\underline{v}).$$

Erstattes $\underline{v}$ med $-\underline{v}$ vil venstre side skifte fortegn og højre side være uændret, så $|2B(\underline{e}_1, \underline{v})| \leq \varphi(\underline{v})$, og erstattes $\underline{v}$ med $\lambda \underline{v}$ fås $|2B(\underline{e}_1, \lambda \underline{v})| = 2|\lambda| |B(\underline{e}_1, \underline{v})| \leq \varphi(\lambda \underline{v}) = \lambda^2 \varphi(\underline{v})$, hvorefter for $\lambda \neq 0$ fås $2|B(\underline{e}_1, \underline{v})| \leq |\lambda| \varphi(\underline{v})$, og da man heri kan vælge λ vilkårlig nær 0 fås $B(\underline{e}_1, \underline{v}) = 0$, hvormed sætningens bevis er fuldført.

Vi skal nu vise, at der er nær forbindelse mellem den her beviste sætning og tidligere resultater om egenverdier og egenvektorer for en lineær afbildning af et vektorrum ind i sig selv (AG III, §2, 40-48a): Lad $(V, +, \cdot)$ være et n -dimensionalt vektorrum, hvori der er valgt en basis, og lad $f: \underline{v} \mapsto \underline{Av}$ være en lineær afbildning af V ind i sig selv; her er $\underline{A}$ en $(n \times n)$ -matrix, og til den hører der en reduktionsdeterminant $\det(\underline{A} - \lambda \underline{E})$, som udregnet bliver et polynomium af n 'te grad i λ , det karakteristiske polynomium for A . Rødderne i det karakteristiske polynomium er netop de tal λ , for hvilke $\text{rg}(\underline{A} - \lambda \underline{E}) < n$, og det er også netop egenverdierne for den lineære afbildning, og for enhver egenverdi λ er $n - \text{rg}(\underline{A} - \lambda \underline{E})$ lig egenverdiens geometriske multiplisitet, d.v.s. dimensionen af underrummet af de tilsvarende egenvektorer.

Lad der på et n -dimensionalt euklidisk rum være givet en symmetrisk bilinearform B , som for en vis ortonormal basis har matricen $\underline{B}$. Hvis man skifter til en ny ortonormal basis for hvilken bilinearformens matrix er en diagonalmatrix, (hvilket er muligt ifølge forrige sætning), da vil diagonalelementerne i denne netop være rødderne i det karakteristiske polynomium for $\underline{B}$, endda i den ("algebraiske") forstand, at

$$\det(\underline{B} - \lambda \underline{E}) = (\lambda_1 - \lambda) \cdots (\lambda_n - \lambda),$$

hvor $\lambda_1, \dots, \lambda_n$ er diagonalelementerne i diagonalmatricen.

Beviset følger nedenfor. Sætningen viser specielt, at selvom der er flere (og hyppigt mange) ortonormale baser, i hvilke bilinearformens matrix er en diagonalmatrix, så er diagonalmatrixens elementer bestemt entydigt (pånær rækkefølgen), da det karakteristiske polynomium jo højst på een måde kan skrives som produkt af linearfaktorer. Da endvidere enhver symmetrisk matrix kan opfattes som matrix for en kvadratisk form, viser sætningen det (langtfra trivielle) resultat, at for enhver symmetrisk $(n \times n)$ -matrix $\underline{B}$ over $\mathbb{R}$ vil det karakteristiske polynomium $\det(\underline{B} - \lambda \underline{E})$ have n reelle rødder; f.eks. vil reduktionsdeterminanterne

$$\begin{vmatrix} 0-\lambda & 1 \\ 1 & 0-\lambda \end{vmatrix}, \quad \begin{vmatrix} 0-\lambda & 1 \\ -1 & 0-\lambda \end{vmatrix} \quad \text{og} \quad \begin{vmatrix} 2-\lambda & 4 \\ 1 & 2-\lambda \end{vmatrix} \quad \text{være henholdsvis}$$

$K_1(\lambda) = \lambda^2 - 1$ (som har to reelle rødder, matrixen er symmetrisk), $K_2(\lambda) = \lambda^2 + 1$ (som ikke har nogen reelle rødder, matrixen er ikke symmetrisk) og $K_3(\lambda) = \lambda^2 - 4\lambda$ (som har to reelle rødder, selvom matrixen er ikke-symmetrisk, hvilket naturligvis er meget vel foreneligt).

Bevis: Basisskiftet kan udtrykkes ved en regulær matrix $\underline{T}$, således at hvis en vektor i den oprindelige basis har koordinatsættet $\underline{v}_i$, så vil den i den nye basis have koordinatsættet $\underline{T} \underline{v}_i$. Den kvadratiske form, som i den oprindelige basis havde matrixen $\underline{B}$, vil i den nye basis have matrixen $\underline{T}' \underline{B} \underline{T}$, og her er altså $\underline{T}$ således at der er fremkommet en diagonalmatrix

$$\underline{T}' \underline{B} \underline{T} = \underline{A} = \begin{pmatrix} \lambda_1 & \dots & 0 \\ & \ddots & \\ 0 & \dots & \lambda_n \end{pmatrix}.$$

Men samtidig betød $\underline{T}$ jo et skifte fra en ortonormal basis til en ortonormal basis, og da den kvadratiske form $\underline{y} \cdot \underline{y}$ for enhver

ortonormal basis er lig $v_1^2 + \dots + v_n^2$, hvis matrix er $\underline{\underline{E}}$, så er $\underline{\underline{T}}' \underline{\underline{E}} \underline{\underline{T}} = \underline{\underline{E}}$, hvorefter fås $(\det \underline{\underline{T}})^2 = 1$. Så er

$$\det(\underline{\underline{B}} - \lambda \underline{\underline{E}}) = \det(\underline{\underline{T}}'(\underline{\underline{B}} - \lambda \underline{\underline{E}})\underline{\underline{T}}) = \det(\underline{\underline{A}} - \lambda \underline{\underline{E}}),$$

hvilket er lig

$$\det \begin{pmatrix} \lambda_1 - \lambda & & 0 \\ & \ddots & \\ 0 & & \lambda_n - \lambda \end{pmatrix} = (\lambda_1 - \lambda) \cdot \dots \cdot (\lambda_n - \lambda),$$

hvormed sætningen er bevist.

Lad der på et n-dimensionalt euklidisk rum være givet en bilinearform B. Der eksisterer en og kun en lineær afbildning $\underline{v} \rightarrow f(\underline{v})$ af rummet ind i sig selv, således at $B(\underline{u}, \underline{v}) = \underline{u} \cdot f(\underline{v})$ for alle $\underline{u}$ og $\underline{v}$. Dersom B er symmetrisk gælder også $B(\underline{u}, \underline{v}) = f(\underline{u}) \cdot \underline{v}$, og f kaldes den til bilinearformen svarende symmetriske tensor. Thi lad os vælge en vilkårlig ortonormal basis $\underline{e}_1, \dots, \underline{e}_n$; i denne vil bilinearformen have en matrix $\underline{\underline{B}}$, og den pågældende afbildning f vil i koordinaterne kunne angives ved at $\underline{v}_i \rightarrow \underline{\underline{B}} \underline{v}_i$. For dels ser man umiddelbart, at $B(\underline{u}, \underline{v}) = \underline{u} \cdot (\underline{\underline{B}} \underline{v}_i)$ kan fortolkes som det skalære produkt af vektoren med koordinatrækken $\underline{u}$ og vektoren med koordinatsøjlen $(\underline{\underline{B}} \underline{v}_i)$, og dels ser man, at hvis $B(\underline{u}, \underline{v}) = \underline{u} \cdot f(\underline{v})$, hvor $f(\underline{v})$ er givet som $\underline{v}_i \rightarrow \underline{\underline{C}} \underline{v}_i$ med en $(n \times n)$ -matrix $\underline{\underline{C}}$, så vil $\underline{u} = \underline{e}_i$, $\underline{v} = \underline{e}_j$ give $c_{ij} = B(\underline{e}_i, \underline{e}_j) = b_{ij}$, så at $\underline{\underline{C}} = \underline{\underline{B}}$. For et symmetrisk B er $B(\underline{u}, \underline{v}) = B(\underline{v}, \underline{u}) = \underline{v} \cdot f(\underline{u})$.

Lad der på et n-dimensionalt euklidisk rum være givet en symmetrisk bilinearform B, og lad $(\underline{e}_1, \dots, \underline{e}_n)$ være en ortonormal basis, ved hvilken B har en diagonalmatrix $\underline{\underline{A}}$ med diagonalelementerne $\lambda_1, \dots, \lambda_n$. Da gælder, at ved den til bilinearformen svarende symmetriske tensor er $\underline{e}_i$ egenvektor for egenværdien λ_i , $i = 1, \dots, n$.

Beviset er umiddelbart, hvis vi benytter den pågældende basis, for så er den symmetriske tensor givet ved at $\underline{v}_i \rightarrow \underline{\underline{A}} \underline{v}_i$, som di-

rekte viser, at $\underline{e}_i \rightarrow \lambda_i \underline{e}_i$.

Enhver rod λ^* i reduktionsdeterminanten er egenværdi, og vi kan definere dens "algebraiske multiplicitet" a-mlt λ^* som det antal gange den optræder som diagonalelement i $\underline{\Lambda}$, hvilket ifølge det foregående er det samme som det antal gange faktoren $(\lambda^* - \lambda)$ findes i det karakteristiske polynomium. Da de tilsvarende basisvektorer er indbyrdes ortogonale egenvektorer for λ^* , vil den geometriske multiplicitet g-mlt λ^* for egenværdien λ^* ved den symmetriske tensor være større end eller lig a-mlt λ^* . Hvis man summerer over de forskellige egenværdier er $\sum$ a-mlt $\lambda^* = n$, og da desuden $\sum$ g-mlt $\lambda^* \leq n$ (se AG III, § 2, 45), ser vi, at for enhver egenværdi λ^* for en symmetrisk tensor i et euklidisk rum er den algebraiske multiplicitet a-mlt λ^* lig den geometriske multiplicitet g-mlt λ^* .

Endvidere ses, at egenvektorer hørende til forskellige egenværdier for den symmetriske tensor er ortogonale. Dette kan også let ses direkte, thi hvis $f(\underline{u}) = \lambda \underline{u}$ og $f(\underline{v}) = \mu \underline{v}$, fås ved at benytte symmetriligningen $\underline{u} \cdot f(\underline{v}) = f(\underline{u}) \cdot \underline{v}$ at $\underline{u} \cdot \mu \underline{v} = \lambda \underline{u} \cdot \underline{v}$, eller $(\mu - \lambda) \underline{u} \cdot \underline{v} = 0$, hvilket viser påstanden.

Man ser, hvorledes de foregående resultater kan benyttes til den praktiske løsning af opgaven : Givet en symmetrisk bilinearform i et euklidisk rum, bestem en ortonormal basis i hvilken bilinearformens matrix er en diagonalmatrix $\underline{\Lambda}$. Thi man kan først tage bilinearformens matrix $\underline{B}$ i et vilkårligt ortonormalt system, så udregne det karakteristiske polynomium $\det(\underline{B} - \lambda \underline{E})$, og finde rødderne i dette, idet vi ved, at der er n reelle rødder; dermed har vi diagonalelementerne i $\underline{\Lambda}$. For en rod λ^* udtages blandt egenvektorerne for λ^* ved afbildningen $\underline{w}_i \rightarrow \underline{B} \underline{w}_i$ (i den valgte basis) så mange ortonormale som muligt, og ved at gøre dette

for de forekommende værdier af λ^* har man opnået en basis af den søgte art.

Af metoden fremgår, at hvis det karakteristiske polynomium har n forskellige rødder, så er basisvektorerne entydigt bestemt, dog på nær deres fortegn. Hvis der derimod er "multiple rødder", så har rummene af de tilsvarende egenvektorer dimension større end 1, og så er der uendelig mange muligheder for valg af ortonormal basis i dem.

Endvidere får man sætningen: Hvis f er en lineær afbildning af et n -dimensionalt vektorrum $(V, +, \cdot)$ ind i sig selv, og den i et vist koordinatsystem er givet ved $\underline{v}_i \rightarrow \underline{B} \underline{v}_i$, hvor $\underline{B}$ er en symmetrisk matrix, så findes der n lineært uafhængige egenvektorer. Den er indlysende af det foregående, idet vi jo blot kan indføre den euklidiske metrik i koordinatrummet. Uden forudsætning om at $\underline{B}$ er symmetrisk gælder sætningen ikke; f.eks. vil i en sædvanlig euklidisk plan afbildningen med matricen.

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

betyde en drejning om begyndelsespunktet, og der findes ingen egenvektorer. Omvendt er det klart, at dersom der findes n lineært uafhængige egenvektorer, så kan man benytte dem som basis, hvorved afbildningens matrix bliver en diagonalmatrix (og altså symmetrisk).

Lad der være givet en ikke-udartet symmetrisk bilinearform B på det n -dimensionale vektorrum $(V, +, \cdot)$. Vi har tidligere betragtet lineære bijektive afbildninger af rummet på sig selv, hvorved B overførtes i dermed ækvivalente bilinearformer. Vi skal nu specielt undersøge de lineære bijektive afbildninger, ved hvilke B overføres i sig selv. Som tidligere omtalt er en symmetrisk

bilinearform bestemt ved den tilhørende kvadratiske form $K(\underline{y}) = B(\underline{y}, \underline{y})$, og vi skal altså betragte afbildninger $\underline{y} \rightarrow f(\underline{y})$, for hvilke $K(\underline{y}) = K(f(\underline{y}))$. Geometrisk kan afbildningerne anskueliggøres ved at niveaufaderne $K^{-1}(a)$ for den kvadratiske form skal afbildes ind på sig selv. Afbildningerne af den betragtede art kaldes ortogonale med hensyn til den kvadratiske form (eller med hensyn til bilinearformen).

Man ser, at ¹⁾ identiteten er en afbildning af den betragtede art, ²⁾ hvis f er det, så er f^{-1} det også og ³⁾ hvis f og g er det, så er $g \circ f$ det også. Dermed er vist, at afbildningerne udgør en gruppe, en undergruppe i den "generelle lineære gruppe" af alle lineære bijektive afbildninger af vektorrummet på sig selv. Gruppen kaldes den til den kvadratiske form $B(\underline{y}, \underline{y})$ (på det n -dimensionale reelle rum) hørende ortogonale gruppe, og kan betegnes $O(n, \mathbb{R}, B)$.

Lad os betragte forholdene i et koordinatsystem: Bilinearformen har en symmetrisk matrix $\underline{B}$, og den lineære afbildning $\underline{y} \rightarrow f(\underline{y})$ af vektorrummet på sig selv udtrykkes ved $\underline{y}_i \rightarrow \sum_j \underline{S}_{ij} \underline{y}_j$, hvor $\underline{S}$ er en regulær matrix, og så kan ortogonalitetsbetingelsen $B(f(\underline{u}), f(\underline{v})) = B(\underline{u}, \underline{v})$ skrives som $\underline{u} \underline{S}' \underline{B} \underline{S} \underline{v} = \underline{u} \underline{B} \underline{v}$. Hvoraf ses, at de brugbare afbildningers matricer $\underline{S}$ netop er de regulære $n \times n$ -matricer, som for det givne $\underline{B}$ opfylder ortogonalitetsbetingelsen

$$(0) \quad \underline{S}' \underline{B} \underline{S} = \underline{B}.$$

Og ifølge det foregående resultat vil mængden af disse matricer med matrixmultiplikation udgøre en gruppe.

Til lineær-ækvivalente kvadratiske former hører isomorfe ortogonale grupper. Thi ækvivalente kvadratiske former kan jo ved valg af passende (forskellige) baser udtrykkes ved den samme matrix $\underline{B}$ (f.eks. diagonalmatricen svarende til ækvivalensklassen),

og de tilsvarende ortogonale grupper bliver derfor isomorfe med gruppen af matricer $\underline{S}$, som opfylder ortogonalitetsligningen (0). For et givet dimensionstal n kunne man derfor få ligeså mange væsentlig forskellige ortogonale grupper, som antallet af ækvivalensklasser af ikke-udartede kvadratiske former (dette antal er $n + 1$), dog ser man umiddelbart, at f.eks. klassen af positiv definite former og klassen af negativ definite former har isomorfe ortogonale grupper. Men man kan for forskellige klasser få ortogonale grupper af væsentlig forskellig struktur (eksempel senere).

For bilinearformen B på det n -dimensionale vektorrum over $\mathbb{R}$ er det ifølge de tidligere resultater muligt at bestemme en basis, $\underline{e}_1, \dots, \underline{e}_n$, for hvilken $B(\underline{e}_i, \underline{e}_j) = \begin{cases} 1 & i=j \\ 0 & i \neq j \end{cases}$, medens $B(\underline{e}_i, \underline{e}_j) = 0$ for $i \neq j$. En sådan basis betegner man som ortonormal basis med hensyn til bilinearformen (eller med hensyn til den tilhørende kvadratiske form). Ved en ortogonal afbildning, hvor $\underline{v} \rightarrow \hat{\underline{v}}$ er ifølge afbildningens definition $B(\underline{v}, \underline{w}) = B(\hat{\underline{v}}, \hat{\underline{w}})$, og alment $B(\underline{u}, \underline{v}) = B(\hat{\underline{u}}, \hat{\underline{v}})$. Man ser heraf, at en afbildning, som er ortogonal med hensyn til B fører en ortonormal basis for B over i en ortonormal basis for B .

Det ovenstående generaliserer det tidligere indførte begreb ortonormal basis i et euklidisk rum, idet en sådan er i den nye forstand ortonormal med hensyn til det indre produkt. Den tilsvarende kvadratiske form er afstandskvadratet $\|\underline{v}\|^2$, og de tilsvarende ortogonale afbildninger er netop de afstandsbevarende lineære afbildninger (med fastholdt begyndelsespunkt); niveaufladerne, som går over i sig selv ved afbildningerne, er kuglefladerne $\|\underline{v}\|^2 = a$. Afstandskvadratet er en positiv definit kvadratisk form, og i en ortonormal basis bliver matricen $\underline{B}$ netop en enhedsmatrix $\underline{E}$. Ortogonalitetsligningen (0) viser så, at i en ortonormal basis for et euklidisk rum er matricerne $\underline{S}$ for de ortogonale afbildninger karakteriseret ved

at $\underline{S}'\underline{S} = \underline{E}$, d.v.s. at matrixens transponerede er lig dens reciproke (dette resultat er en passant nævnt i s.22, hvor der jo netop var tale om ortogonale afbildninger af et euklidisk rum).

Lad os igen i det almindelige tilfælde antage, at vi har valgt en ortonormal basis, og betragte matrixen $\underline{S}$; denne kaldes så kort for en ortogonal matrix. Ved i ortogonalitetsligningen (0) at tage determinanterne og benytte, at $\det \underline{B} \neq 0$, findes, at $(\det \underline{S})^2 = 1$, altså at $\det \underline{S} = +1$ eller $\det \underline{S} = -1$. Begge muligheder kan forekomme (man ser f.eks. let, at hvis man i en matrix $\underline{S}$ der opfylder ligningen (0) skifter fortegn i en enkelt række, så vil den nye matrix også opfylde (0), men dens determinant har skiftet fortegn). De ortogonale afbildninger hvis determinant er +1 kaldes de "egentlig ortogonale afbildninger", og udgør åbenbart en undergruppe, den egentlig ortogonale gruppe $O^+(n, \mathbb{R}, B)$ i gruppen $O(n, \mathbb{R}, B)$. Undergruppens index er 2, og sideklassen udgøres af de ortogonale afbildninger, hvis determinant er -1, de "uegentlig ortogonale afbildninger". Definitionerne er uafhængige af basisvalget, thi determinanten for en lineær vektorfunktion er jo uafhængig af basis. Specielt kalder man i det euklidiske rum de egentlig ortogonale afbildninger for drejninger (om begyndelsespunktet), og de uegentlig ortogonale afbildninger for spejlinger (om en hyperplan gennem begyndelsespunktet).

Tilfældet $n = 2$: For en positiv definit form kan man benytte formen som afstandskvadrat, og får derved et 2-dimensionalt euklidisk rum. Matrixen $\underline{S}$ skal opfylde ligningen $\underline{S}'\underline{S} = \underline{E}$; ved at opskrive betingelsesligningerne for dens elementer og løse, finder man som parameterfremstilling for $\underline{S}$

$$\underline{S} = \begin{pmatrix} \cos t & -\sin t \\ \pm \sin t & \pm \cos t \end{pmatrix}, \quad 0 \leq t < 2\pi;$$

heri vil de øverste fortegn give de egentlig ortogonale afbildninger, og de underste giver de uegentlig ortogonale. For en indefinit form vil $\underline{B}$ i en ortonormal basis have diagonalelementerne $+1$ og -1 ; som par amøderfremstilling for $\underline{S}$ finder man i dette tilfælde

$$\underline{S} = \begin{pmatrix} + \cosh t & + \sinh t \\ + \sinh t & + \cosh t \end{pmatrix}, \quad -\infty < t < \infty;$$

heri vil samme fortegn i de to rækker give de egentlig ortogonale afbildninger, medens modsat fortegn giver de uegentlige. Strukturen af de ortogonale grupper er væsentlig forskellig i de to tilfælde, f.eks. kan man se, at der i den første gruppe findes uendelig mange elementer af endelig grad (for t lig et rationalt multiplum af 2π), medens der i den anden gruppe kun findes et par trivielle elementer af endelig grad (Smlgn. iøvrigt AG II, 2, øv. 26-27).

Nogle trykfejl i AG III, § 12

Side	2, linie	2 f.o.		tilføj	=
	4,	2 f.o.	står $= \underline{v}_1$	læs	$= \underline{v}_-$
	9,	15 f.o.	" øv.18).	"	øv.15, der viser, at M og K(M) ikke altid udspænder V)
	10,	4 f.o.	" symmetrisk	læs	diagonalmatrix
	10,	6 f.o.	" symmetrisk	"	diagonalmatrix
	10,	9 f.o.	" B	"	$\underline{B}$
	13,	5 f.o.	" 1893	"	1897
	15,	5 f.o.	" har man	"	man har
	16,	9 f.o.	" og når	"	når
	17,	1 f.n.	tilføj: disse former kaldes <u>indefinite</u>		
	27,	7-11 f.n.	erstattes af : I det sædvanlige 3-di- mensionale euklidiske rum kan man som eksempel på en egentlig og en u- egentlig ortogonal afbildning tage hhv. en drejning (om begyndelsespunkt- et 0) og en spejling (i en plan gen- nem 0).		
øv.23		1	står $B(\underline{u}, \underline{v})$	læs	$B(\underline{v}, \underline{v})$
øv.24		1	" øv.20	"	øv. 23
øv.25		1	" øv. 20	"	øv. 23
øv.33		4	" $\underline{u}_-$	"	$\underline{u}_1$
øv.35		4-5	læs: kan samles i par af reciprokke, eller er +1 eller -1 (som er selv- reciprokke).		
øv.36		6	står $\underline{u} \underline{H} \underline{v}_1$	læs	$\underline{u} \underline{H} \underline{v}_1$

Øvelser til kap. III, § 12.

1. For en bilinearform B defineret i de vilkårlige vektorrum $(U, +, L)$ og $(V, +, L)$ defineres nulrummet i V som mængden af de vektorer $\underline{v} \in V$, for hvilke $B(\underline{u}, \underline{v}) = 0$ for alle $\underline{u} \in U$. Tilsvarende defineres nulrummet i U .

Opskriv den i $\mathbb{R}^3 \times \mathbb{R}^4$ definerede bilinearform

$$u_1 v_1 + 4u_2 v_1 + 2u_3 v_1 + 3u_1 v_2 - 2u_2 v_3 - u_3 v_3 + u_1 v_4$$

på matrixform, og angiv dens rang. Find parameterfremstillinger for dens nulrum i $\mathbb{R}^3$ og $\mathbb{R}^4$.

2. Lad $(U, +, \mathbb{C})$ være vektorrummet bestående af alle komplekse talfølger $\underline{u} = (u_1, u_2, \dots)$, for hvilke rækken $u_1 + u_2 + \dots$ er absolut konvergent, og lad $(V, +, \mathbb{C})$ være vektorrummet bestående af alle begrænsede komplekse talfølger $\underline{v} = (v_1, v_2, \dots)$. For $\underline{u} \in U$ og $\underline{v} \in V$ er da rækken

$$B(\underline{u}, \underline{v}) = u_1 v_1 + u_2 v_2 + \dots$$

konvergent og definerer en bilinearform i $U \times V$.

Hvilke talfølger udgør nulrummene i U og V ?

3. Lad $(U, +, \mathbb{R})$ og $(V, +, \mathbb{R})$ være vektorrummene af alle reelle kontinuerte funktioner, der er definerede henholdsvis i intervallet $[a, b]$ og i intervallet $[c, d]$. Er der givet en i $[a, b] \times [c, d]$ defineret og kontinuert reel funktion $K(x, y)$, vil

$$B(f, g) = \int_a^b \int_c^d K(x, y) f(x) g(y) dx dy, \quad f \in U, g \in V,$$

være en bilinearform i $U \times V$.

Hvad kan der siges om Fourierrækkerne for de funktioner, som udgør nulrummene, når $a = c = -\pi$, $b = d = \pi$ og $K(x, y) = \sin(2x - y)$?

4. Vis, at en bilinearform defineret i to endelig-dimensionale vektorrum er et produkt af en linearform i U og en linearform i V , hvis og kun hvis dens rang er 1 eller 0.

5. Bilinearformerne på et vektorrum $(V, +, L)$ udgør et nyt vektorrum $(W, +, L)$.

Gør rede for at de symmetriske bilinearformer på $(V, +, L)$ danner et underrum i W , og at det samme gælder for de antisymmetriske bilinearformer, og at W er den direkte sum af de to nævnte underrum. Angiv dimensionerne af W og af de to underrum.

6. I et todimensionalt vektorrum $(V_2, +, L)$ er hvert arealmål en antisymmetrisk bilinearform af rangen 2. Findes der andre antisymmetriske bilinearformer i et sådant vektorrum?

Hvilke værdier kan rangen af en antisymmetrisk bilinearform i et tredimensionalt vektorrum $(V_3, +, L)$ antage? Er F et volumenmål og $\underline{a}$ en fast valgt vektor i V_3 , vil $F(\underline{a}, \underline{u}, \underline{v})$ være en antisymmetrisk bilinearform i V_3 . Kan hver antisymmetrisk bilinearform i V_3 fås på denne måde?

7. Bestem de symmetriske bilinearformer i $(\mathbb{R}^3, +, \mathbb{R})$, hvis tilhørende kvadratiske former er

$$\begin{aligned} v_1 v_2 - v_3^2, & \quad v_2 v_3 + v_3 v_1 + v_1 v_2, \\ (v_1 + v_2 + v_3)^2, & \quad (v_1 + 2v_2)(3v_1 - v_3), \end{aligned}$$

og angiv for hver af dem rangen og den tilhørende symmetriske matrix.

Bestem endvidere for hver af de fundne bilinearformer det fuldstændige konjugerede underrum til det af vektorerne $(1, -1, 0)$ og $(0, 0, 1)$ udspændte underrum.

8. Bevis følgende sætning: En kvadratisk form i et endelig-dimensionalt vektorrum over de komplekse tals legeme er et produkt af to fra nulformen forskellige, ikke-proportionale linearformer, hvis og kun hvis dens rang er 2, og den er kvadrattet på en fra nulformen forskellig linearform, hvis og kun hvis dens rang er 1.

Opstil en tilsvarende sætning for kvadratiske former i vektorrummet over de reelle tals legeme.

9. Man betragter et endeligdimensionalt vektorrum over de reelle tal, og en på vektorrummet defineret kvadratisk form. Vis, at mængden af de med hensyn til formen isotrope vektorer er et underrum, hvis og kun hvis formen er semidefinit (eller definit).

10. Bestem en basis for vektorrummet $(\mathbb{C}^2, +, \cdot)$, med hensyn til hvilken bilinearformen

$$u_1 v_1 - i u_1 v_2 - i u_2 v_1$$

antager normalformen.

Angiv derefter en basis for vektorrummet $(\mathbb{C}^3, +, \cdot)$, med hensyn til hvilken bilinearformen

$$- 2u_2 v_2 + 2iu_2 v_3 + 2iu_3 v_2$$

antager normalformen.

11. Bestem en basis for vektorrummet $(\mathbb{R}^4, +, \cdot)$, med hensyn til hvilken den kvadratiske form

$$v_1^2 + 4v_1 v_4 - 2v_2 v_3 + 2v_2 v_4 + 2v_3 v_4 + 4v_4^2$$

antager normalformen.

12. Lad $(V, +, \cdot)$ være et vilkårligt vektorrum over de reelle tals

legeme og B en bilinearform på V .

Vis, at hvis vektorerne $\underline{v}_1, \dots, \underline{v}_s$ er parvis konjugerede og $B(\underline{v}_1, \underline{v}_1) > 0, \dots, B(\underline{v}_s, \underline{v}_s) > 0$, vil disse vektorer være lineært uafhængige, og det af dem udspændte underrum vil være et positivitetsrum for B .

13. Lad B være en symmetrisk bilinearform med positivitetsindex 1 på et vektorrum $(V, +, \mathbb{R})$. Vis, at der for to vektorer $\underline{u}$ og $\underline{v}$, for hvilke $B(\underline{u}, \underline{u}) > 0$ og $B(\underline{v}, \underline{v}) > 0$, gælder uligheden

$$B(\underline{u}, \underline{v})^2 \leq B(\underline{u}, \underline{u}) B(\underline{v}, \underline{v}).$$

(Betragt $B(\lambda \underline{u} + \mu \underline{v}, \lambda \underline{u} + \mu \underline{v})$, $\lambda, \mu \in \mathbb{R}$.)

14. Lad $\underline{B}$ være en reel, symmetrisk og regulær $(n \times n)$ -matrix. Med B og B^{-1} betegnes de to bilinearformer på talrummet $(\mathbb{R}^n, +; \mathbb{R})$, hvis matricer er $\underline{B}$ og $\underline{B}^{-1}$. Vis, at hvis søjlerne $\underline{u}_i$ og $\underline{v}_i$ er konjugerede med hensyn til B , vil $\underline{B}\underline{u}_i$ og $\underline{B}\underline{v}_i$ være konjugerede med hensyn til B^{-1} . Vis at de til B og B^{-1} hørende kvadratiske former har samme positivitets- og negativitetsindices.

15. Lad $B(\underline{u}, \underline{v})$ være en symmetrisk bilinearform på $(\mathbb{R}^n, +, \mathbb{R})$. Nulpunktet betegnes N og mængden af isotrope vektorer betegnes I . Vis, at det af $\underline{u}$ og $K(\underline{u})$ frembragte vektorrum $V(\underline{u}, K(\underline{u}))$ er et ægte underrum i $\mathbb{R}^n$ hvis og kun hvis $\underline{u} \in I \setminus N$.

16. Lad $\underline{M}$ være en vilkårlig reel $(m \times n)$ -matrix. Vis, at den kvadratiske form med $(n \times n)$ -matricen $\underline{M}'\underline{M}$ er positiv semidefinit, og at den er positiv definit, når og kun når $\text{rg } \underline{M} = n$. Vis, at der til hver reel symmetrisk $(n \times n)$ -matrix $\underline{B}$, hvis tilhørende kvadratiske form er positiv definit, findes en reel regulær $(n \times n)$ -matrix $\underline{M}$, således at $\underline{M}'\underline{M} = \underline{B}$.

17. På $(\mathbb{R}^n, +, \mathbb{R})$ er givet en kvadratisk form hvis matrix $\underline{B}$ består af lutter 1, undtagen i diagonalen, hvor der står lutter 0. Best em formens positivitetsindex og dens negativitetsindex.
18. Angiv nødvendige og tilstrækkelige betingelser, som de reelle tal a, b, c må opfylde, for at den reelle kvadratiske form med matrixen $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ er positiv(negativ)definit. Undersøg, om der findes reelle tal a, b, c , således at den reelle kvadratiske form med matrixen.

$$\begin{pmatrix} a & b & c \\ b & c & a \\ c & a & b \end{pmatrix}$$

er positiv definit.

19. Om en reel funktion f defineret på en åben delmængde Ω af $\mathbb{R}^n$ forudsættes, at den har kontinuerte partielle afledede $D_{ij}f$, $i, j = 1, \dots, n$, af anden orden. Lad $\underline{a} = (a_1, \dots, a_n)$ være et punkt i Ω , for hvilket funktionens første differential er nulformen, altså

$$df(\underline{a}, d\underline{x}) = \sum_{i=1}^n D_i f(\underline{a}) dx_i = 0$$

for alle $d\underline{x} = (dx_1, \dots, dx_n) \in \mathbb{R}^n$. Bevis følgende: En nødvendig betingelse for, at f har et lokalt minimum (maximum) i $\underline{a}$ er, at det andet differential

$$d^2f(\underline{a}, d\underline{x}) = \sum_{i,j=1}^n D_{ij}f(\underline{a}) dx_i dx_j$$

er en positiv (negativ) semidefinit kvadratisk form. En tilstrækkelig betingelse er, at denne kvadratiske form er positiv (negativ) definit.

20. Vis, at matricen hørende til en positiv definit kvadratisk form har positiv determinant. Angiv i almindelighed fortegnet for determinanten af matricen hørende til en kvadratisk form, udtrykt ved formens invarianter.

Vis, at hvis $\underline{B}$ er matrix for en positiv definit kvadratisk form defineret på $\mathbb{R}^n$, så er alle hovedunderdeterminanter i $\underline{B}$ positive. (En hovedunderdeterminant er determinanten for en undermatrix, som er udtaget symmetrisk om hoveddiagonalen). Vis omvendt, at dersom blot de n hovedunderdeterminanter, der dannes af den første rækker og søjler i $\underline{B}$, ($m = 1, 2, \dots, n$), er positive, så er den tilsvarende kvadratiske form positiv definit (og altså samtlige hovedunderdeterminanter positive).

21. Lad M være en mængde af reelle kontinuerte funktioner f på $(\mathbb{R}^n, +, \mathbb{R})$ (med den sædvanlige topologi), og således at M ved den i teksten definerede lineær-ækvivalens bliver delt i endelig mange ækvivalensklasser. Vis, at dersom $(M, +, \mathbb{R})$ er et vektorrum, så er der for hvert f højst 4 muligheder for værdiområdet, og angiv disse.

22. Idet $(V, +, L)$ er et vektorrum over tallegemet L , og H er mængden af funktioner, der afbilder V ind i L , skal man bestemme samtlige ækvivalensklasser i H (ved den side 15 definerede lineær-ækvivalens), som indeholder netop een funktion F . Giv for $(V, +, L) = (\mathbb{R}, +, \mathbb{R})$ et eksempel på en ækvivalensklasse, som indeholder netop 2 funktioner F .

23. Lad $B(\underline{u}, \underline{v})$ være en positiv definit kvadratisk form på vektorrummet $(V, +, \mathbb{R})$ (af endelig eller uendelig dimension), og lad $\underline{v}_1, \dots, \underline{v}_s$ være vektorer fra V . Man sætter $B(\underline{v}_i, \underline{v}_j) = b_{ij}$, $i, j = 1, \dots, s$. Vis, at $\det(b_{ij}) \geq 0$, og at der her gælder lighedstegn hvis og kun hvis $\underline{v}_1, \dots, \underline{v}_s$ er lineært afhængige (Grams's sætning; J.P.Gram 1850-1916, dansk).

24. Vis ved hjælp af Gram's sætning (øv. 20), at rækkerne i en reel $(m \times n)$ -matrix $\underline{A}$ er lineært afhængige, hvis og kun hvis $\det(\underline{AA}') = 0$.

25. Vis ved hjælp af Gram's sætning (øv. 20), at funktionerne $1, \cos t, \sin t, \cos 2t, \sin 2t, \dots, \cos pt, \sin pt$ på intervallet $[-\pi, \pi]$ er lineært uafhængige.

26. Lad α betegne en reel voksende funktion defineret på et interval $[a, b]$. Ved denne funktions i'te moment forstås tallet

$$c_i = \int_a^b t^i d\alpha(t), \quad i = 0, 1, \dots$$

Vis, at der gælder ulighederne

$$c_{2i-1}^2 \leq c_{2i-2} c_{2i}, \quad i = 1, 2, \dots$$

Vis endvidere, at der for determinanterne

$$D_k = \det(c_{i+j}), \quad i, j = 0, 1, \dots, k-1; \quad k=1, 2, \dots$$

gælder følgende: Enten er $D_k > 0$ for alle k , eller der findes et naturligt tal m , således at $D_k > 0$ for $k < m$ og $D_k = 0$ for $k \geq m$. Det sidstnævnte tilfælde indtræffer, hvis og kun hvis funktionen α kun antager endelig mange forskellige værdier (er stykkevis konstant).

27. Bestem positivitetsindex og negativitetsindex for formen

$$3v_1^2 + 3v_2^2 + 2v_1v_2 + 2v_2v_3 \text{ på } (\mathbb{R}^3, +, \mathbb{R}).$$

28. I et todimensionalt vektorrum over $\mathbb{R}$ har man i et givet koordinatsystem $B_1(\underline{u}, \underline{v}) = u_1v_1 + u_2v_2$ og $B_2(\underline{u}, \underline{v}) = u_1v_2 + u_2v_1$;

bestem en ny basis $(\underline{e}_1, \underline{e}_2)$, således at $B_1(\underline{e}_1, \underline{e}_2) = B_2(\underline{e}_1, \underline{e}_2) = 0$.

Vis, at hvis $B_1(\underline{u}, \underline{v}) = u_1v_1 - u_2v_2$ og $B_2(\underline{u}, \underline{v}) = u_1v_2 + u_2v_1$, så findes der ikke nogen basis $(\underline{e}_1, \underline{e}_2)$ for hvilken $B_1(\underline{e}_1, \underline{e}_2) = B_2(\underline{e}_1, \underline{e}_2) = 0$.

29. På det 2-dimensionale euklidiske rum er givet to kvadratiske former, der i et ortonormalt koordinatsystem hedder $B_1(\underline{v}, \underline{v}) = 5v_1^2 + 7v_2^2 - 2\sqrt{3}v_1v_2$, $B_2(\underline{v}, \underline{v}) = v_1^2 - v_2^2 + 2\sqrt{3}v_1v_2$; Bestem en ny ortonormal basis, således at matricen for B_1 bringes på diagonalform; vis, at ved enhver sådan vil matricen for B_2 også være bragt på diagonalform.
30. Lad $\underline{s}_1, \dots, \underline{s}_n$ betegne søjlerne i matricen $\underline{S}$; hvad er den geometriske betydning af elementerne i søjlen $\underline{s}_j$? Angiv et sæt betingelser for disse søjler's elementer, som er nødvendige og tilstrækkelige for at $\underline{S}$ er en ortogonal matrix i det n -dimensionale euklidiske rum. Eftersom, at når disse betingelser er opfyldt af søjlerne i $\underline{S}$, så er de analoge betingelser opfyldt af rækkerne i $\underline{S}$.
- Lad $\underline{s}_j$ og $\underline{s}_k$ være to forskellige søjler i $\underline{S}$; elementerne i dem betegnes henholdsvis $(a_1, \dots, a_n)$ og $(b_1, \dots, b_n)$; vi sætter det komplekse tal $c_m = a_m + ib_m$, $m = 1, \dots, n$. Vis, at når $\underline{S}$ er en ortogonal matrix i det euklidiske rum, så er $c_1^2 + \dots + c_n^2 = 0$ og endvidere $|c_1|^2 + \dots + |c_n|^2 = 2$, og at dersom omvendt $\underline{s}_j$ og $\underline{s}_k$ opfylder disse betingelser, så findes der i det euklidiske rum en ortogonal matrix $\underline{S}$, i hvilken de er søjler. Er der to eller tre betingelsesligninger for søjleparret?
31. I et euklidisk n -dimensionalt rum med ortonormal basis er givet en kvadratisk form $\underline{x} \underline{A} \underline{x}$; vis, at hvis og kun hvis $\text{tr}(\underline{A}) = 0$ er det muligt ved en ortogonal afbildning at føre formen over i en form, hvis matrix har lutter 0 i diagonalen.

32. I det euklidiske 3-dimensionale rum er givet en kvadratisk form med matricen

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 4 \\ 3 & 4 & 5 \end{pmatrix}$$

Bestem en ortogonal afbildning i det euklidiske rum, som fører formens matrix over i en diagonalmatrix, og bestem denne.

33. Lad $\underline{A}$ være en regulær $(n \times n)$ -matrix, n ulige, og lad $\underline{u}$ og $\underline{v}$ være vektorer i $(\mathbb{R}^n, +, \mathbb{R})$. Idet $B(\underline{u}, \underline{v})$ betegner værdien af $(n+1) \times (n+1)$ -determinanten

$$\det \begin{pmatrix} \underline{u} & - & \underline{A} \\ 0 & & \underline{v} \end{pmatrix},$$

skal man vise, at $B(\underline{u}, \underline{v})$ er en bilinearform, og bestemme elementerne i dens matrix $\underline{B}$. Vis, at $B(\underline{u}, \underline{v}) = \underline{u} \underline{A} \underline{v}$, hvis og kun hvis $\underline{A}$ er en egentlig ortogonal matrix i det n -dimensionale euklidiske rum.

34. Findes der nogen (ægte eller uægte) undergruppe U i gruppen $GL(n, \mathbb{R})$ af lineære bijektive afbildninger af et n -dimensionalt euklidisk rum på sig selv, således at den ortogonale gruppe $O(n, \mathbb{R}, \underline{u}, \underline{v})$ er normal ægte undergruppe i U ?
35. Lad $\underline{S}$ være en med hensyn til en regulær bilinearform på $(\mathbb{R}^n, +, \mathbb{R})$ ortogonal matrix. Vis, at $\det(\underline{S} - \lambda \underline{E}) = \pm \det(\underline{E} - \lambda \underline{S}')$, og udled heraf, at rødderne (reelle eller komplekse) i det karakteristiske polynomium for $\underline{S}$ kan samles i par af reciprokke, idet der dog for n ulige desuden er en rod $+1$ eller -1 . Betragt som eksempel tilfældet $n = 2$.

36. Lad V være et n -dimensionalt unitært rum (AG, III, 1, 37-45).

Ved en Hermite'sk form ($H(\underline{u}, \underline{v})$) forstås en funktion, som afbilder $V \times V$ ind i $\mathbb{C}$, og således at $H(\underline{u}, \underline{v})$ for fastholdt $\underline{v}$ er lineær i $\underline{u}$, og således at $H(\underline{v}, \underline{u}) = \overline{H(\underline{u}, \underline{v})}$. Ved dens matrix for en given basis forstås en matrix $\underline{H}$ således at $H(\underline{u}, \underline{v}) = \underline{u} \underline{H} \overline{\underline{v}}$.

Vis, at matricen $\underline{H}$ er "Hermite'sk", d.v.s. at for alle dens elementer gælder $h_{ij} = \overline{h_{ji}}$ (og specielt er diagonalleddene reelle).

Hvorledes ændres $\underline{H}$ ved basisskifte?

Vis, ved generalisation af beviserne S.18-22 sætningerne:

- 1) For enhver Hermite'sk form på et unitært rum findes mindst en ortonormal basis, for hvilken matricen $\underline{H}$ er en diagonal-matrix,
- 2) For enhver Hermite'sk matrix $\underline{H}$ vil det karakteristiske polynomium $\det(\underline{H} - \lambda \underline{E})$ have n reelle rødder.

37. (Fortsættelse af 36) Ved en unitær matrix $\underline{U}$ forstås en matrix, som er således, at $\underline{x}_i = \underline{U} \hat{x}_i$ angiver forbindelsen mellem koordinaterne for vektoren $\underline{x}$ i to forskellige ortonormale baser for et unitært rum ($\underline{U}$ er altså det, som for et unitært rum svarer til en ortogonal matrix i et euklidisk rum). Vis, at betingelsen for at $\underline{U}$ er en unitær matrix er, at $\underline{U}^{-1} = \overline{\underline{U}}'$. Hvad kan siges om værdien af $\det \underline{U}$? Vis (smlgn. øv. 35), at rødderne (reelle eller komplekse) i det karakteristiske polynomium for en unitær matrix $\underline{U}$ kan samles i par af reciprokke eller er +1 eller -1 (som er selvreciprokke).

Vis, at en unitær 2×2 -matrix kan skrives på formen

$$e^{iv} \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}, \quad v \in \mathbb{R}; a, b \in \mathbb{C}; \|(a, b)\| = 1.$$

38. Der er givet et n -dimensionelt vektorrum $(V, +, \mathbb{R})$, hvori der er valgt en basis. Lad $B(\underline{x}, \underline{x})$ være en positiv definit kvadratisk form, og lad $B_1(\underline{x}, \underline{x})$ være formen $B(\underline{x}, \underline{x}) + L(\underline{x})^2$, hvor $L(\underline{x})$ er en egentlig linearform.

Bevis, at for formernes symmetriske matricer, hhv. $\underline{B}$ og $\underline{B}_1$, gælder $\det \underline{B} < \det \underline{B}_1$ (man kan f. eks. undervejs benytte en basis $\hat{e}_1, \dots$, i hvilken $L(\underline{x}) = \hat{x}_1$).

AG III,1,10¹⁴ $\underline{v}_1, \dots, \underline{v}_p$ ", læs: " $\underline{v}_1, \dots, \underline{v}_p$, $p > 1$ ".AG III,1,14₂"hver vektor i $\underline{v}$ ", læs: "hver fra $\underline{0}$ forskellig vektor i V ".AG III,1,31³Læs: " $\text{dist}(\underline{v}, \underline{u}) = \|\underline{u} - \underline{v}\| = \|\underline{v} - \underline{u}\| = \text{dist}(\underline{u}, \underline{v})$ ".AG III,2,33₆Der skal ikke være understregning af λ_1 og λ_p .AG III,2,38¹⁵ $(\underline{f}_1, \dots, \underline{f}_m)$ ", læs $(\hat{\underline{f}}_1, \dots, \hat{\underline{f}}_m)$ ".AG III,2,ø.v.8¹³

"afsluttet interval", læs: "afsluttet, begrænset interval".

AG III,4,3¹

"alternarende", læs: "alternerende".

AG III,4,5₅
$$\sum_{j=1}^n, \text{ læs: } \sum_{i=1}^n.$$
AG III,4,6¹ a_{i_1} ", læs: " $a_{i_1 1}$ ".

AG III, 4, 3¹

"alternarende", læs: "alternerende".

AG III, 4, 5₅

$$\sum_{j=1}^n, \text{ læs: } \sum_{i=1}^n.$$

AG III, 4, 6¹" a_{i_1} ", læs: " $a_{i_1, 1}$ ".AG III, 4, 11¹

Indføj som et ekstra punkt mellem 6° og 7°: "Ombyttes to søjler (rækker) i en kvadratisk matrix, vil matrixens determinant skifte fortegn."

AG III, 4, 13₉

"ifølge determinantens definition", læs: "ifølge VI (side 7)".

AG III, 4, 14₃" $\hat{u}_j$ ", læs: " $\hat{u}_{j-1}$ ".AG III, 4, 14₁

Tilføj: "Her er venstre side lig med

$$\begin{aligned} & F(\hat{u}_1, \dots, \hat{u}_{j-1}, \underline{e}_i, \hat{u}_{j+1}, \dots, \hat{u}_n) \\ & = F(\underline{u}_1, \dots, \underline{u}_{j-1}, \underline{e}_i, \underline{u}_{j+1}, \dots, \underline{u}_n) = U_{ij}. \end{aligned}$$

AG III, 4, 16₇

I øverste højre hjørne af determinanten rettes " a_1^{n-2} " til " a_1^{n-1} ".

AG III, 4, 3v. 15²" $(m+1)$ -sæt", " $(m+1)$ -sæt".

Rettelser til AG III, 1.

4, linie 7

 $"L \times \hat{F}(T \rightarrow L) \rightarrow L"$, læs: $"L \times \hat{F}(T \rightarrow L) \rightarrow \hat{F}(T \rightarrow L)"$.

14, linie 5

 $"\text{Hvis } V = \infty"$, læs: $"\text{Hvis } \dim V = \infty"$.

18, linie 2 f.n.

 $"C_0, C_1, \dots, C_K"$, læs: $"C_0, C_1, \dots, C_n"$.

20, linie 1 f.n.

 $"y = y_1 e_1 + \dots + y_{n-n} e_{n-n}"$, læs: $"\underline{y} = y_1 \underline{e}_1 + \dots + y_{n-n} \underline{e}_{n-n}"$.

24, linie 11

 $"\underline{0}"$, læs: $"\{\underline{0}\}"$.

26, linie 9 f.n.

 $"\underline{u}' + \underline{u} = 0"$, læs: $"\underline{u}' + \underline{u} = \underline{0}"$.

30, linie 1 f.n.

 $"\underline{w} \quad V"$, læs: $"\underline{w} \in V"$.

34, linie 7

 $"(\lambda \underline{u} \cdot \underline{v})"$, læs: $"(\lambda \underline{u}) \cdot \underline{v}"$.

39, linie 15 og 17

 $"0"$, læs: $"\underline{0}"$.

Øv. 7, linie 2

 $"i < j"$, læs: $"i \leq j"$.

Øv. 14 og 15

 $"\hat{F}(\hat{R} \rightarrow \hat{R}, +, \hat{R})"$, læs: $"(\hat{F}(\hat{R} \rightarrow \hat{R}), +, \hat{R})"$.