Matematik 1, 1968–69

Børge Jessen

Forelæsningsnoter til Mat 1x

Matematik 1

er delt i to dele. Mat 1x omfatter fortrinsvis algebra med geometriske anvendelser. Mat 1y omfatter fortrinsvis analyse med geometriske (og enkelte fysiske) anvendelser.

Til Mat 1x, 1968-69 benyttes følgende noter:

Pakke 10 betegnet:

Mat 1, 1964-65. Elementer vektorregning.

Nærværende Pakke 11, der omfatter

Pakke 13 betegnet

Mat 1, 1968-69. Lineær algebra. 1. del.

Pakke 14 betegnet

Mat 1, 1968-69. Lineær algebra. 2. del.

Yderligere noter vil komme i årets løb.

Indledning.

I matematikens udvikling har perioder af ekspansion stedse været fulgt af perioder af konsolidering og systematisering. Kun gennem stadig forenkling har det været muligt at beherske et stadig mere omfattende stof. I de sidste hundred år har store bestræbelser været rettet mod at finde frem til matematikens fundamentale strukturer. I kim findes disse i den klassiske matematiks begrebsverden. Ved at behandle den klassiske matematiks objekter som specielle tilfælde af almene strukturer har man opnået en hidtil ukendt unifikation af matematikken.

I den forelæggende fremstilling forudsættes den elementære matematik bekendt. Forskellige emner af elementær karakter vil dog blive taget op til fornyet behandling. Den fristende tanke, at give en samlet systematisk behandling af matematikens grundlæggende discipliner, har måttet vige for praktiske hensyn. Opgaven har været i et kursus af overkommeligt omfang på en gang at lægge en grund for videregående matematiske studier og at give en nogenlunde afrundet behandling af de for anvendelserne vigtigste emner. Hovedvægten har måttet lægges på de klassiske discipliner, men det er tilstræbt at fremstille disse i lys af den moderne matematiks begreber. Ved behandlingen af grundlæggende spørgsmål er tilstræbt en høj grad af nøjagtighed; ved behandlingen af eksempler og af emner, der kun medtages af hensyn til anvendelserne, er fremstillingen ofte mere summarisk.

Litteratur.

Af det store udvalg af bøger vedrørende de i Mat 1x behandlede emner anføres her blot nogle enkelte.

Angelo Margaris: First order mathematical logic.
(Blaisdell, 1967.)

Felix Hausdorff: Mengenlehre.
(Walter de Gruyter & Co., 1927.)

Paul Halmos: Naive set theory.
(Van Nostrand, 1960.)

Patrick Suppes: Axiomatic set theory.
(Van Nostrand, 1960.)

G. T. Kneebone: Mathematical logic and the foundations of mathematics.
(Van Nostrand, 1963.)

B. L. van der Waerden: Algebra I.
(Springer, 1960.)

W. H. Greub: Linear algebra.
(Springer, 1963.)

G. E. Shilov: An introduction to the theory of linear spaces.
(Prentice-Hall, 1965.)

Det greske alfabet.

Alfa	A	α	
Beta	B	β	
Gamma	Γ	γ	
Delta	Δ	δ	
Epsilon	E	ε	
Zeta	Z	ζ	
Eta	H	η	
Theta	Θ	θ	ϑ
Jota	I	ι	
Kappa	K	κ	
Lamda	Λ	λ	
My	M	μ	
Ny	N	ν	
Ksi	Ξ	ξ	
Omikron	O	o	
Pi	Π	π	
Rho	P	ρ	
Sigma	Σ	σ	ς
Tau	T	τ	
Upsilon	Y	υ	
Fi	Φ	φ	
Khi	X	χ	
Psi	Ψ	ψ	
Omega	Ω	ω	

Sammen med a b c d
benyttes ofte α β γ δ

Sammen med x y z
benyttes ofte ξ η ζ

§1. Matematisk logik.

Matematisk logik er logik udtrykt i formelsprog efter matematisk forbillede. Som grundlægger af den matematiske logik regner man George Boole (1815-64). Den har udviklet sig til en omfattende disciplin i nær tilknytning til studiet af matematikens grundlag. Vi indskrænker os her til at give en præcisering af det logiske tegnsprog i den form vi vil benytte det.

Udsagnskalkylen. Ved et udsagn vil vi forstå et matematisk udsagn, d.v.s. et udsagn om matematiske objekter, som kan være sandt eller falskt, men ikke begge dele; vi siger, at det er tilskrevet en sandhedsværdi, nemlig „sandt" eller „falskt", forkortet s og f.

En matematisk teori er en samling af sande udsagn. Når et udsagn fremsættes i en matematisk teori er meningen, med mindre andet siges, at udsagnet enten vides at være sandt eller skal vises at være sandt.

I det følgende betegnes uspecificerede udsagn ved bogstaver eller ved symboler sammensat af bogstaver og de logiske tegn.

Af udsagn dannes nye udsagn på følgende måder:

$\neg p$, der læses „non p" eller „ikke p";

$p \wedge q$, der læses „p og q";

$p \vee q$, der læses „p eller q";

$p \Rightarrow q$, der læses „hvis p så q";

$p \Leftrightarrow q$, der læses „p hvis og kun hvis q".

Disse sammensatte udsagn kaldes negation, konjunktion, disjunktion, implikation, biimplikation. Udsagnenes betydning fremgår af deres sand-

hedstabeller:

p	$\neg p$
s	f
f	s

p	q	$p \wedge q$	$p \vee q$	$p \Rightarrow q$	$p \Leftrightarrow q$
s	s	s	s	s	s
s	f	f	s	f	f
f	s	f	s	s	f
f	f	f	f	s	s

.

To ikke specificerede udsagn kaldes <u>ækvivalente</u>, hvis de, uanset hvilke udsagn man indsætter for de optrædende bogstaver, enten begge er sande eller begge er falske. Til angivelse af ækvivalens benyttes tegnet $\sim$.

Således er $\neg(\neg p) \sim p$ og $p \Rightarrow q \sim (\neg p) \vee q$ og $p \Leftrightarrow q \sim (p \Rightarrow q) \wedge (q \Rightarrow p)$. Endvidere er $(p \wedge q) \wedge r \sim p \wedge (q \wedge r)$ og $(p \vee q) \vee r \sim p \vee (q \vee r)$, så at man kan udelade parenteserne og tale om udsagnene $p \wedge q \wedge r$ og $p \vee q \vee r$. Når $p_1, \ldots, p_n$ er udsagn, kan man herefter også tale om udsagnene $p_1 \wedge \ldots \wedge p_n$ og $p_1 \vee \ldots \vee p_n$.

Af særlig interesse er <u>dualitetslovene</u>

$$\neg(p \wedge q) \sim (\neg p) \vee (\neg q) \quad \text{og} \quad \neg(p \vee q) \sim (\neg p) \wedge (\neg q).$$

<u>Prædikatkalkylen.</u> Et <u>prædikat</u> eller et <u>åbent udsagn</u> er en konstruktion, der har samme struktur som et udsagn, men hvori der indgår en eller flere variable; når man for de variable indsætter bestemte objekter, forvandles prædikatet hi et udsagn (hvis sandhedsværdi i almindelighed vil afhænge af, hvilke objekter der indsættes i stedet for de variable).

Af prædikater dannes nye prædikater med anvendelse af tegnene $\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow$ på samme måde som for udsagn.

Af prædikater dannes endvidere udsagn eller nye prædikater ved brug af kvantorer, nemlig alkvantoren $\forall$, der læses „for alle", og eksistenskvantoren $\exists$, der læses „der eksisterer et ... så ...".

Ud fra et prædikat $p(x)$ med een variabel x, der kan gennemløbe en mængde M af objekter, dannes to udsagn

$$\forall x \in M : p(x) \qquad \text{og} \qquad \exists x \in M : p(x),$$

af hvilke det første er sandt, hvis $p(x)$ er sandt for alle x fra M, og ellers falskt, medens det andet er sandt, hvis $p(x)$ er sandt for mindst et x fra M, og ellers falskt. Der gælder dualitetslovene

$$\neg(\forall x \in M : p(x)) \sim \exists x \in M : \neg p(x) \text{ og } \neg(\exists x \in M : p(x)) \sim \forall x \in M : \neg p(x).$$

Ud fra et prædikat $p(x,y)$ med to variable x og y, der kan gennemløbe mængderne M og N, kan f. eks. dannes prædikaterne

$$\forall x \in M : p(x,y) \qquad \text{og} \qquad \exists y \in N : p(x,y)$$

og udsagnene

$$\forall y \in N \; \forall x \in M : p(x,y) \qquad \text{og} \qquad \forall x \in M \; \exists y \in N : p(x,y).$$

De variable, der er forsynet med en kvantor, kaldes bundne, de øvrige frie. Når alle de variable bindes, fås et udsagn; bindes kun nogle af de variable, fås et prædikat i de frie variable.

Man overbeviser sig umiddelbart om, at flere på hinanden følgende kvantorer af samme art kan ombyttes. Derimod kan kvantorer af forskellig art i almindelighed ikke ombyttes. Negationen af et udsagn eller et prædikat dannet med flere på hin-

anden følgende kvantorer omskrives ved at man anvender dualitetslovene på en kvantor ad gangen.

Anvendelsen af det logiske tegnsprog. Ved en skriftlig fremstilling af matematikken foretrækker man i reglen det smidige sædvanlige sprog for det logiske tegnsprog, som dog, når det skal læses, kræver en omsætning til sædvanligt sprog. Derimod finder det logiske tegnsprog udstrakt anvendelse i tilslutning til mundtlig fremstilling.

Ved anvendelsen tillader man sig, ligesom ved brugen af det egentlige matematiske tegnsprog, ofte friheder, som det ikke lønner sig at forsøge at afgrænse.

§2. Mængdelære.

Mængdelæren er grundlæggende i vore dages matematik. Som selvstændig disciplin er den grundlagt af Georg Cantor (1845-1918) i en række afhandlinger fra årene 1874-97. Vi skal ikke her gå ind på de dybereliggende afsnit af den almene mængdelære, men kun omtale dens tegnsprog og dens simpleste begreber.

Mængdebegrebet. Ved en mængde vil vi i det følgende forstå en velafgrænset samling af matematiske objekter; disse kaldes mængdens elementer. At x er element af mængden M, skrives $x \in M$ eller $M \ni x$; at x ikke er element af mængden M, skrives $x \notin M$ eller $M \not\ni x$. Man ser, at $x \notin M$ blot er en anden skrivemåde for $\neg(x \in M)$. En mængde er selv et matematisk objekt og kan som sådant være element af andre mængder. En mængde kaldes ofte et rum; dens elementer kaldes da punkter.

En endelig mængde kan angives ved at man i en krøllet parentes opremser dens elementer. Der er herved intet i vejen for, at samme element skrives flere gange, og rækkefølgen er ligegyldig. Således betegner $\{1,3,2,5,2\}$ og $\{1,5,2,3\}$ den samme mængde, nemlig den, hvis elementer er tallene 1, 2, 3, 5 og ikke andre objekter, og hvis x er et matematisk objekt betegner $\{x\}$ mængden med det ene element x.

For nogle mængder benyttes faste betegnelser:

$\emptyset$ er den tomme mængde;

$\mathbb{N}$ er mængden af alle naturlige, d.v.s. hele, positive tal;

$\mathbb{N}_0$ er mængden af alle ikke-negative hele tal;

$\mathbb{Z}$ er mængden af alle hele tal;

$\mathbb{Q}$ er mængden af alle rationale tal;
$\mathbb{Q}_+$, $\mathbb{Q}_-$ er mængden af alle {positive, negative} rationale tal;
$\mathbb{R}$ er mængden af alle reelle tal;
$\mathbb{R}_+$, $\mathbb{R}_-$ er mængden af alle {positive, negative} reelle tal;
$\mathbb{C}$ er mængden af alle komplekse tal;
$\mathbb{U}$ er mængden af alle komplekse tal med numerisk værdi 1.

En mængde A kaldes <u>delmængde</u> af mængden B og man skriver $A \subseteq B$ eller $B \supseteq A$, hvis hvert element af A også er element af B. Mængden A kaldes <u>ægte delmængde</u> af mængden B og man skriver $A \subset B$ eller $B \supset A$, hvis A er delmængde af B og $A \neq B$. Den tomme mængde $\emptyset$ er delmængde af enhver mængde.

Mængden af delmængder af en mængde M, altså den mængde, hvis elementer er delmængderne af M, betegnes i det følgende $\mathbb{P}(M)$.

Ofte vil der være givet en fast mængde M, hvorom undersøgelserne drejer sig. Mængden M kaldes da <u>grundmængden</u> eller <u>universalmængden</u>. Af sproglige grunde er det hensigtsmæssigt i et sådant tilfælde at benytte benævnelsen mængde forbeholdt for delmængder af M og for andre mængder at benytte et synonym. F. eks. kan man kalde en delmængde af $\mathbb{P}(M)$ et <u>system</u> af delmængder af M eller blot et mængdesystem.

Hvis der til hvert element i af en mængde I (der ikke behøver at være delmængde af M) er knyttet et element x_i af M, udgør disse elementer en delmængde af M, der betegnes $\{x_i \mid i \in I\}$. Mængden I kaldes <u>indexmængden</u>. Ved brug af denne betegnelse forlanges ikke,

at de til to forskellige indices svarende elementer er forskellige. Hvis I består af tallene $1, \dots, n$, er det mængden $\{x_1, \dots, x_n\}$. Hvis $I = \mathbb{N}$, benyttes også betegnelsen $\{x_1, x_2, \dots\}$.

En delmængde A af M kan være karakteriseret ved en eller flere egenskaber, der udskiller elementerne af A blandt elementerne af M. Det er i reglen bekvemt at formulere de egenskaber, der karakteriserer elementerne af A, ved et prædikat $p(x)$, således at A som elementer har netop de elementer x af M, for hvilke $p(x)$ er sandt. Vi skriver da

$$A = \{x \in M \mid p(x)\} \quad \text{eller} \quad A = \{x \mid p(x)\},$$

idet den sidste skrivemåde kan benyttes, når det af sammenhængen fremgår, hvilken mængde M, der er grundmængde.

Mængdealgebra. For delmængder af en grundmængde M defineres fællesmængden $A \cap B$, foreningsmængden $A \cup B$, og overskudsmængden $A \setminus B$ af A over B, eller komplementet af B i A, ved formlerne

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$
$$A \cup B = \{x \mid x \in A \vee x \in B\}$$
$$A \setminus B = \{x \mid x \in A \wedge x \notin B\}.$$

Komplementet $M \setminus A$ af en delmængde A af M i M kaldes kort komplementærmængden for A og betegnes også $\sim A$ eller $\complement A$. Man bemærker, at $\sim(\sim A) = A$, $\sim M = \emptyset$, $\sim \emptyset = M$, og at der for vilkårlige delmængder af M gælder $A \setminus B = A \cap (\sim B)$. Hvis $A \cap B = \emptyset$, kaldes A og B disjunkte.

Man ser, at $(A \cap B) \cap C = A \cap (B \cap C)$ og $(A \cup B) \cup C = A \cup (B \cup C)$, så at man kan udelade parenteserne og tale om mængderne $A \cap B \cap C$ og $A \cup B \cup C$. For vilkårlige

mængder $A_1, \ldots, A_n$ kan man herefter også tale om fællesmængden $A_1 \cap \ldots \cap A_n$ og foreningsmængden $A_1 \cup \ldots \cup A_n$, der kort betegnes $\bigcap_{i=1}^{n} A_i$ og $\bigcup_{i=1}^{n} A_i$.

Alment kan vi, hvis der til hvert element i af en indexmængde I er knyttet en delmængde A_i af M, definere fællesmængden $\cap\{A_i \mid i \in I\}$ og foreningsmængden $\cup\{A_i \mid i \in I\}$ ved formlerne

$$\cap\{A_i \mid i \in I\} = \{x \mid \forall i \in I : x \in A_i\}$$

$$\cup\{A_i \mid i \in I\} = \{x \mid \exists i \in I : x \in A_i\}.$$

De to mængder betegnes også $\bigcap_{i \in I} A_i$ og $\bigcup_{i \in I} A_i$. Hvis $I = \mathbb{N}$ anvendes også betegnelserne $A_1 \cap A_2 \cap \ldots$ og $A_1 \cup A_2 \cup \ldots$ eller $\bigcap_{i=1}^{\infty} A_i$ og $\bigcup_{i=1}^{\infty} A_i$.

Der gælder <u>dualitetslovene</u>

$$A \setminus \bigcap_{i \in I} A_i = \bigcup_{i \in I} (A \setminus A_i)$$

$$A \setminus \bigcup_{i \in I} A_i = \bigcap_{i \in I} (A \setminus A_i).$$

Et system $\{A_i \mid i \in I\}$ af delmængder af M siges at <u>overdække</u> en delmængde A af M, eller at udgøre en <u>overdækning</u> af A, hvis $A \subseteq \cup\{A_i \mid i \in I\}$. Hvis $A = \cup\{A_i \mid i \in I\}$ og mængderne i systemet er parvis disjunkte og ingen af dem er den tomme mængde $\emptyset$, kaldes overdækningen en <u>klassedeling</u> af A.

Den betragtede grundmængde har kun virkelig betydning i forbindelse med begrebet komplementærmængde. De øvrige begreber: fællesmængde, foreningsmængde, overskudsmængde, er uafhængige af hvilken grundmængde indeholdende de pågældende mængder man vælger.

Produktmængder. Lad X og Y være to mængder. Ved produktet $X \times Y$ forstås mængden af alle ordnede par (x,y), hvor $x \in X$ og $y \in Y$. Man kalder elementerne x og y koordinaterne af (x,y) eller projektionerne af (x,y) på X og Y; undertiden kalder x abscissen og y ordinaten af (x,y).

Hvis $A \subseteq X$ og $B \subseteq Y$, er $A \times B$ en delmængde af $X \times Y$ (men $X \times Y$ har naturligvis, undtagen i trivielle tilfælde, mange andre delmængder end disse).

For tre mængder X, Y, Z kan vi danne produktmængderne $(X \times Y) \times Z$ og $X \times (Y \times Z)$. Den første består af alle ordnede par $((x,y),z)$, den anden af alle ordnede par $(x,(y,z))$. Da disse svarer til de ordnede sæt (x,y,z), kan vi regne $(X \times Y) \times Z$ og $X \times (Y \times Z)$ for den samme mængde, som vi betegner $X \times Y \times Z$, og som består af alle ordnede sæt (x,y,z), hvor $x \in X$, $y \in Y$, $z \in Z$. For vilkårlige mængder $X_1, \ldots, X_n$ kan vi danne mængden $X_1 \times \ldots \times X_n$ bestående af alle ordnede sæt $(x_1, \ldots, x_n)$, hvor $x_1 \in X_1, \ldots, x_n \in X_n$.

Hvis alle X_i er samme mængde X, betegnes produktet $X \times \ldots \times X$ med X^n. Mængden X^n består altså af alle ordnede sæt $(x_1, \ldots, x_n)$, hvor $x_1, \ldots, x_n \in X$.

Mængden $\mathbb{R}^n$ kaldes det n-dimensionale reelle talrum. For $n = 1, 2, 3$ optræder $\mathbb{R}^n$ i den aritmetiske beskrivelse af en ret linie, en plan, eller rummet, der baseres på indførelsen af koordinater. Analogt kaldes mængden $\mathbb{C}^n$ det n-dimensionale komplekse talrum.

Numerable mængder. At M er en endelig mængde med n elementer betyder, at elementerne i M kan nummereres ved hjælp af afsnittet $\{1, \dots, n\}$ af den naturlige talrække. Man får M skrevet på formen $M = \{x_1, \dots, x_n\}$, hvor $x_i \neq x_j$ for $i \neq j$. Til de endelige mængder regnes også $\emptyset$.

En mængde M kaldes numerabel eller tællelig, hvis elementerne i M kan nummereres ved hjælp af hele den naturlige talrække $\mathbb{N} = \{1, 2, \dots\}$, altså hvis M kan skrives på formen $M = \{x_1, x_2, \dots\} = \{x_n \mid n \in \mathbb{N}\}$, hvor $x_i \neq x_j$ for $i \neq j$.

Det kunde synes rimeligt under benævnelsen numerabel mængde at medtage de endelige mængder (og undertiden ser man denne sprogbrug anvendt), men vi vil her bruge udtrykket i den anførte betydning.

(1) Enhver uendelig mængde M har en numerabel delmængde.

Lad x_1 være et element af M. Da M er uendelig, er $M \setminus \{x_1\}$ ikke tom. Lad x_2 være et element af $M \setminus \{x_1\}$. Da M er uendelig, er $M \setminus \{x_1, x_2\}$ ikke tom. Således fortsættes, og vi får derved i M valgt en numerabel delmængde $\{x_1, x_2, \dots\}$.

(2) Enhver delmængde af en numerabel mængde M er endelig eller numerabel.

Lad $M = \{x_1, x_2, \dots\}$ og lad A være en delmængde af M. Vi noterer elementerne i A i den rækkefølge vi møder dem i M og konstaterer, at $A = \{x_{p_1}, \dots, x_{p_n}\}$, hvor $p_1 < \dots < p_n$, eller $A = \{x_{p_1}, x_{p_2}, \dots\}$, hvor $p_1 < p_2 < \dots$.

(3) Foreningsmængden af endeligt eller numerabelt mange endelige eller numerable mængder er endelig

eller numerabel.

Lad mængderne være $M_1 = \{x_{11}, x_{12}, \dots\}$, $M_2 = \{x_{21}, x_{22}, \dots\}$, ... [hvor vi har afstået fra i betegnelserne at give udtryk for, om de enkelte mængder er endelige eller numerable og om der er endeligt eller numerabelt mange mængder] og lad $M = M_1 \cup M_2 \cup \dots$. Da er $M = \{x_{11}, x_{12}, x_{21}, x_{13}, x_{22}, x_{31}, \dots\}$ [hvor pladser, til hvilke der ikke svarer noget element, naturligvis skal forbigås]. Idet vi stryger gentagelser, får vi M skrevet på formen $M = \{x_1, \dots, x_n\}$ eller $\{x_1, x_2, \dots\}$, hvor $x_i \neq x_j$ for $i \neq j$.

(4) Hvis $X_1, \dots, X_n$ er numerable mængder, er også produktmængden $X_1 \times \dots \times X_n$ numerabel.

For $n = 2$ følger det af, at $X_1 \times X_2$ er foreningsmængden af de numerabelt mange mængder $\{(x_1, x_2) \mid x_1 \in X_1\}$, $x_2 \in X_2$, som hver er numerabel. Ved induktion ses herefter, at det gælder for $n > 2$.

Som eksempler nævnes:
$\mathbb{Z}$ er numerabel. Thi $\mathbb{Z} = \{0\} \cup \{1, 2, \dots\} \cup \{-1, -2, \dots\}$.
$\mathbb{Q}$ er numerabel. Thi $\mathbb{Q} = M_1 \cup M_2 \cup \dots$, hvor M_n er mængden $\left\{\frac{z}{n} \mid z \in \mathbb{Z}\right\}$, som er numerabel.
Følgelig er også $\mathbb{Z}^n$ og $\mathbb{Q}^n$ numerable for ethvert $n \in \mathbb{N}$.
Det vil senere blive vist, at $\mathbb{R}$ ikke er numerabel. Følgelig er $\mathbb{R}^n$, $\mathbb{C}$, $\mathbb{C}^n$ heller ikke numerable.

§3. Relationer. Afbildninger eller funktioner.

Relationer. Lad X og Y være to mængder. Ved en relation fra X til Y forstås en delmængde R af produktmængden $X \times Y$. For vilkårlige elementer $x \in X$ og $y \in Y$ siger vi, at x står i relationen R til y, såfremt $(x,y) \in R$. I denne sammenhæng benyttes i stedet for $(x,y) \in R$ også skrivemåden xRy.

Relationer betegnes ofte ved særlige tegn i stedet for ved bogstaver.

Ud fra relationen R fra X til Y dannes en relation R^{-1} fra Y til X, kaldet den omvendte relation til R, idet delmængden R^{-1} af produktmængden $Y \times X$ defineres som mængden af ordnede par (y,x), for hvilke $(x,y) \in R$. Man ser, at de to udsagn xRy og $yR^{-1}x$ er ensbetydige.

Er specielt X og Y samme mængde M, kaldes en relation fra X til Y en relation i M. En relation i M er altså en delmængde R af M^2.

En relation R i en mængde M kaldes refleksiv, hvis der for ethvert $x \in M$ gælder xRx. Den kaldes symmetrisk, hvis der for vilkårlige $x, y \in M$ gælder $xRy \Rightarrow yRx$, altså hvis $R^{-1} = R$. Den kaldes asymmetrisk, hvis der for vilkårlige $x, y \in M$ gælder $xRy \wedge x \neq y \Rightarrow \neg yRx$, man overbeviser sig let om, at dette kommer ud på et med, at der for vilkårlige $x, y \in M$ gælder $xRy \wedge yRx \Rightarrow x = y$. Den kaldes transitiv, hvis der for vilkårlige $x, y, z \in M$ gælder $xRy \wedge yRz \Rightarrow xRz$.

Ækvivalensrelation. En relation $\sim$ i en mængde M kaldes en ækvivalensrelation, hvis den er refleksiv, symmetrisk, og transitiv, altså hvis der for vilkårlige elementer af M gælder

(1) $x \sim x$

(2) $x \sim y \Rightarrow y \sim x$

(3) $x \sim y \wedge y \sim z \Rightarrow x \sim z$.

Begrebet ækvivalensrelation står på følgende måde i forbindelse med begrebet klassedeling:

Lad $\{A_i \mid i \in I\}$ være et system af delmængder af M, der udgør en klassedeling af M. Ved fastsættelsen $x \sim y$, når x og y tilhører samme klasse A_i, er da defineret en ækvivalensrelation i M. Dette er klart.

Enhver ækvivalensrelation $\sim$ i M fremkommer på denne måde ud fra netop een klassedeling. For at indse dette danner man for hvert $x \in M$ mængden $A_x = \{y \in M \mid x \sim y\}$. Man viser nu let, at systemet $\{A_x \mid x \in M\}$ udgør en klassedeling af M, at $\sim$ netop er den til denne klassedeling hørende ækvivalensrelation, og at $\sim$ ikke hører til nogen anden klassedeling af M.

Klasserne (delmængderne) ved den til en ækvivalensrelation hørende klassedeling kaldes ækvivalensklasser, og mængden af ækvivalensklasser kaldes kvotientmængden for ækvivalensrelationen.

Ordningsrelation. En relation $\prec$ i en mængde M kaldes en ordningsrelation, hvis den er refleksiv, asymmetrisk, og transitiv, altså hvis

(1) $x \preccurlyeq x$

(2) $x \prec y \wedge y \preccurlyeq x \Rightarrow x = y$

(3) $x \preccurlyeq y \wedge y \preccurlyeq z \Rightarrow x \preccurlyeq z$.

Når $\preccurlyeq$ er en ordningsrelation i M, skrives i stedet for $x \preccurlyeq y \wedge x \neq y$ også $x \prec y$. I stedet for $x \preccurlyeq y$ og $x \prec y$ skrives også $y \succcurlyeq x$ og $y \succ x$, d.v.s. $\succcurlyeq$ og $\succ$ benyttes som betegnelser for de omvendte relationer til $\preccurlyeq$ og $\prec$. Bemærk, at $\neg(x \prec x)$ og at $x \prec y \wedge y \prec z \Rightarrow x \prec z$.

En ordningsrelation kaldes <u>total</u>, hvis der for vilkårlige indbyrdes forskellige $x, y \in M$ gælder $x \prec y$ eller $y \prec x$.

En mængde M udstyret med en ordningsrelation $\preccurlyeq$ kaldes en <u>ordnet mængde</u>; mængden siges at være <u>organiseret</u> ved relationen $\preccurlyeq$; er ordningsrelationen total kaldes mængden <u>totalt ordnet</u>. Ønsker man i benævnelsen for en ordnet mængde at anføre ordningsrelationens navn, taler man om den ordnede mængde $(M, \preccurlyeq)$.

Når $x \preccurlyeq y$, siger man, at x <u>går foran</u> y eller at y <u>følger efter</u> x; for at undgå misforståelser kan man hilfore: i vid forstand. Når $x \prec y$ siger man, at x går foran y eller at y følger efter x i streng forstand. At $x \preccurlyeq y \preccurlyeq z$ (d.v.s. $x \preccurlyeq y \wedge y \preccurlyeq z$) udtrykkes ved at sige, at y ligger <u>mellem</u> x og z, eller at y ligger mellem z og x.

En delmængde A af M siges at have x som <u>første element</u>, hvis $x \in A$ og x går foran ethvert element af A; den siges at have x som <u>sidste element</u>, hvis $x \in A$ og x følger efter ethvert element af A. Er A en delmængde af M, siges et element $x \in M$ at være <u>majorant</u> for A, hvis x følger efter ethvert element af A; et ele-

ment $x \in M$ siges at være minorant for A, hvis x går foran ethvert element af A. En mængde A kaldes majoriseret, hvis den har en majorant; den kaldes minoriseret, hvis den har en minorant. Hvis der i mængden af majoranter findes et første element, kaldes dette element supremum for A og betegnes $\sup A$; hvis der i mængden af minoranter findes et sidste element, kaldes dette element infimum for A og betegnes $\inf A$.

I mængden $\mathbb{R}$ af reelle tal er $\leqslant$ en total ordningsrelation. Den foran omtalte terminologi benyttes her med visse varianter. I stedet for majorant for en talmængde siger man overtal, i stedet for minorant undertal, i stedet for majoriseret siger man opad begrænset, i stedet for minoriseret nedad begrænset.

Om $(\mathbb{R}, \leqslant)$ gælder den fundamentale sætning:

For enhver ikke tom opad begrænset delmængde af $\mathbb{R}$ findes et supremum, altså et mindste overtal; for enhver ikke tom nedad begrænset delmængde af $\mathbb{R}$ findes et infimum, altså et største undertal.

Afbildninger eller funktioner. Ved en afbildning af en mængde X ind i en mængde Y, eller en funktion fra X til Y, forstås en tilordning, hvorved der til hvert element $x \in X$ svarer et bestemt element $y \in Y$.

En afbildning betegnes i reglen ved et enkelt bog-

stav, undertiden ved en ordforkortelse. At f er en afbildning af X ind i Y skrives

$$f: X \to Y \quad \text{eller} \quad X \xrightarrow{f} Y.$$

Mængden X kaldes afbildningens definitionsmængde og mængden Y dens dispositionsmængde. Det til et element $x \in X$ svarende element af Y betegnes $f(x)$. Det kaldes billedet af x ved f eller den til x hørende funktionsværdi. At $f(x)$ svarer til x skrives hyppigt

$$x \longmapsto f(x).$$

En afbildning $f: X \to Y$ omtales ofte som afbildningen $f(x)$ eller $y = f(x)$, idet $x \in X$ kaldes den uafhængige variable og $y \in Y$ den afhængige variable.

I tilfælde af en endelig mængde X kan en afbildning angives ved en tabel:

$$f = \begin{pmatrix} x_1 & \dots & x_n \\ f(x_1) & \dots & f(x_n) \end{pmatrix}.$$

For en vilkårlig delmængde A af X udgør billederne af alle $x \in A$ en delmængde af Y, der kaldes billedet af A ved f og betegnes $f(A)$, altså

$$f(A) = \{ f(x) \mid x \in A \}.$$

Den særlige brug af tegnet f i forbindelsen $f(A)$ er en praktisk konvention og bør ikke føre til misforståelser. Billedet $f(X)$ kaldes billedmængden eller værdimængden for f.

Ved grafen for en afbildning $f: X \to Y$ forstås delmængden $\{(x, f(x)) \mid x \in X\}$ af $X \times Y$. En delmængde R af $X \times Y$ er åbenbart grafen for en afbildning af X ind i Y, hvis og kun hvis der for ethvert $x \in X$ findes

et og kun eet $y \in Y$, for hvilket $(x,y) \in R$. Begrebet afbildning indordnes herigennem under begrebet relation, idet afbildninger af X ind i Y modsvarer denne specielle type af relationer fra X til Y.

En afbildning $f: X \to Y$ kaldes <u>surjektiv</u> eller en afbildning af X <u>på</u> Y, hvis $f(X) = Y$. Den kaldes <u>injektiv</u>, hvis der for vilkårlige indbyrdes forskellige $x_1, x_2 \in X$ gælder $f(x_1) \neq f(x_2)$. Den kaldes <u>bijektiv</u>, hvis den er både surjektiv og injektiv, altså hvis ethvert $y \in Y$ er billede af et og kun eet $x \in X$. Man ser, at afbildningen $f: X \to Y$ er bijektiv, hvis og kun hvis det om dens graf $R = \{(x, f(x)) \mid x \in X\}$, opfattet som relation fra X til Y, gælder, at den omvendte relation R^{-1} modsvarer en afbildning af Y ind i X; denne afbildning kaldes den <u>omvendte afbildning</u> til f og betegnes f^{-1}; den er naturligvis også bijektiv, og der gælder $(f^{-1})^{-1} = f$.

Er $A \subseteq X$ og er $f: X \to Y$ og $g: A \to Y$ afbildninger, siges g at være en <u>restriktion</u> (indskrænkning) af f, og f en <u>ekstention</u> (udvidelse) af g, hvis $g(x) = f(x)$ for ethvert $x \in A$. Nærmere bestemt kaldes g i dette tilfælde restriktionen af f til A. Den betegnes $f|A$.

Er $f: X \to Y$ en afbildning og er y et element af Y, kaldes ethvert element x af X, for hvilket $f(x) = y$, et <u>originalelement</u> for y ved f. Et element $y \in Y$ kan have intet, eet, eller flere originalelementer. For en vilkårlig delmængde B af Y udgør samtlige originalelementer for alle $y \in B$ en delmængde af X, der

kaldes <u>originalmængden</u> for B ved f og betegnes $f^{-1}(B)$, altså

$$f^{-1}(B) = \{x \in X \mid f(x) \in B\}.$$

Bemærk, at denne betegnelse bruges uanset om f er bijektiv eller ej. Hvis f er bijektiv, så at den omvendte afbildning $f^{-1}: Y \to X$ eksisterer, er originalmængden $f^{-1}(B)$ lig med billedet af B ved f^{-1}. Ved indførelsen af betegnelsen $f^{-1}(B)$ for originalmængden er vi altså ikke kommet i strid med betegnelsesmåden for billedet af en mængde. Bemærk, at $f^{-1}(Y) = X$, og at der for en vilkårlig delmængde A af X gælder $f^{-1}(f(A)) \supseteq A$.

Vælges specielt for B en mængde $\{y\}$ bestående af ét element, bliver originalmængden $f^{-1}(\{y\})$ mængden bestående af samtlige originalelementer for y. Man bemærker, at de fra $\emptyset$ forskellige af disse mængder $f^{-1}(\{y\})$ udgør en klassedeling af X. [Den tilsvarende ækvivalensrelation $\sim$ er bestemt ved, at $x_1 \sim x_2 \iff f(x_1) = f(x_2)$.]

I visse sammenhænge spiller betragtningen af originalmængder en større rolle end betragtningen af billedmængder. Vi fremhæver følgende regler, som kort kan udtrykkes ved at sige, at de fundamentale mængdeoperationer bevares ved overgang til originalmængder:

$$f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2) \qquad f^{-1}\Big(\bigcap_{i \in I} B_i\Big) = \bigcap_{i \in I} f^{-1}(B_i)$$

$$f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2) \qquad f^{-1}\Big(\bigcup_{i \in I} B_i\Big) = \bigcup_{i \in I} f^{-1}(B_i)$$

$$f^{-1}(B_1 \setminus B_2) = f^{-1}(B_1) \setminus f^{-1}(B_2).$$

[For billedmængder gælder $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$, $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$, $f(A_1 \setminus A_2) \subseteq f(A_1)$, men i almindelighed ikke $f(A_1 \cap A_2) = f(A_1) \cap f(A_2)$ og $f(A_1 \setminus A_2) = f(A_1) \setminus f(A_2)$.]

Lad X, Y, Z være mængder og lad $f: X \to Y$ og $g: Y \to Z$ være afbildninger. Den <u>sammensatte afbildning</u> $g \circ f: X \to Z$ defineres da som den afbildning, hvorved der til hvert element $x \in X$ svarer elementet $g(f(x))$ i Z, altså

$$x \longmapsto g \circ f(x) = g(f(x)).$$

For sammensætning af afbildninger gælder den <u>associative regel</u>: Hvis X, Y, Z, U er mængder og $f: X \to Y$, $g: Y \to Z$, $h: Z \to U$ er afbildninger, er

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

Thi $h \circ (g \circ f)$ og $(h \circ g) \circ f$ er afbildninger af X ind i U, og begge har for ethvert $x \in X$ værdien $h(g(f(x)))$. Man kan derfor udelade parenteserne og simpelthen skrive $h \circ g \circ f$.

Lad $f: X \to Y$ og $g: Y \to Z$ være afbildninger. Da gælder: Hvis f og g begge er surjektive, er $g \circ f$ surjektiv. Hvis f og g begge er injektive, er $g \circ f$ injektiv. Hvis f og g begge er bijektive, er $g \circ f$ bijektiv, og da er $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Endvidere gælder: Hvis $g \circ f$ er injektiv, er f injektiv (men ikke nødvendigvis g). Hvis $g \circ f$ er surjektiv, er g surjektiv (men ikke nødvendigvis f).

Blandt afbildningerne af en mængde X ind i sig selv fremhæves den <u>identiske</u> afbildning id_X,

ved hvilken hvert element $x \in X$ svarer til sig selv: $x \longmapsto x$. Hvis A er en delmængde af X, kaldes restriktionen af id_X til A for inklusionsafbildningen fra A til X.

For enhver bijektiv afbildning $f: X \to Y$ gælder $f^{-1} \circ f = id_X$ og $f \circ f^{-1} = id_Y$.

Ækvipotens. Hvis X og Y er mængder og der findes en bijektiv afbildning af X på Y, og dermed også en bijektiv afbildning af Y på X, kaldes X og Y ækvipotente eller de siges at have samme mægtighed.

De endelige mængder med n elementer kan karakteriseres som de mængder, der er ækvipotente med afsnittet $\{1, \ldots, n\}$ af den naturlige talrække, de numerable mængder som de mængder, der er ækvipotente med hele den naturlige talrække $\mathbb{N} = \{1, 2, \ldots\}$. Mængder, der er ækvipotente med $\mathbb{R}$ siges at have kontinuets mægtighed.

Medens en endelig mængde ikke er ækvipotent med nogen ægte delmængde, gælder om uendelige mængder:

Enhver uendelig mængde er ækvipotent med en ægte delmængde, for eksempel med enhver mængde, der fremgår af den ved at udelade et element.

Bevis. Lad M være en uendelig mængde og a et af dens elementer. Vi vælger i M en numerabel delmængde $D = \{x_1, x_2, \ldots\}$, hvor $x_1 = a$ og $x_i \neq x_j$ for $i \neq j$. Sættes nu $f(x_i) = x_{i+1}$ for alle $i \in \mathbb{N}$, og $f(x) = x$ når $x \in M \setminus D$, er f en bijektiv afbildning af M på $M \setminus \{a\}$. [I et hotel med uendelig mange værelser kan der, selv om alle er belagt, altid skaffes plads til en ny gæst.]

§4. Kompositioner.

Kompositioner i en mængde. Ved en kompositionforstås en funktion f fra en produktmængde $X \times Y$ til en mængde Z, altså en afbildning, hvorved der til hvert ordnet par (x, y) af et element $x \in X$ og et element $y \in Y$ svarer et bestemt element $z \in Z$. I denne sammenhæng benyttes i stedet for $z = f(x,y)$ også skrivemåden $z = x f y$.

I tilfælde af endelige mængder X og Y kan en komposition $f: X \times Y \to Z$ angives ved en tabel med dobbelt indgang, idet man i indgangssøjlen anbringer elementerne af X og i indgangsrækken elementerne af Y og i det ved elementerne $x \in X$, $y \in Y$ bestemte felt anbringer $f(x,y)$.

Når X, Y, Z er samme mængde M, så at talen er om en funktion $f: M \times M \to M$, kaldes kompositionen en komposition indenfor mængden M eller blot en komposition i mængden M. Vi betragter foreløbig kun sådanne kompositioner.

Normalt betegnes kompositioner med tegn som $+, \cdot, \cap, \cup$, etc. Ved betragtning af ikke specificerede kompositioner benytter man tegn som $\top$ og $*$, der ikke har nogen speciel matematisk betydning.

En mængde M udstyret med en eller flere kompositioner $\top, *, \ldots$ siges at være organiseret ved disse. Ønsker man i benævnelsen at anføre kompositionerne, taler man om den organiserede mængde $(M, \top, *, \ldots)$. Blandt de således ved kompositioner organiserede mængder skal vi i det følgende be-

bragte de fundamentale algebraiske strukturer: gruppe, ring, legeme.

En komposition $*$ i en mængde M siges at have elementet $e \in M$ til neutralt element, hvis

$$e * a = a * e = a$$

for alle $a \in M$. En komposition kan højst have ét neutralt element. Thi hvis e_1 og e_2 begge er neutrale, gælder både $e_1 * e_2 = e_1$ og $e_1 * e_2 = e_2$.

Kompositionen $*$ kaldes associativ, hvis der for vilkårlige $a, b, c \in M$ gælder

$$(a * b) * c = a * (b * c).$$

Man kan da udelade parenteserne og i stedet for $(a*b)*c$ og $a*(b*c)$ skrive $a*b*c$. For vilkårlige $a_1, \ldots, a_n \in M$ kan man tale om $a_1 * \cdots * a_n$, idet alle de lovmåder, der kan fastsættes ved forskellig anbringelse af parenteser, giver samme resultat.

To elementer $a, b \in M$ siges at kommutere ved kompositionen $*$, hvis

$$a * b = b * a.$$

Kompositionen kaldes kommutativ, hvis to vilkårlige elementer $a, b \in M$ kommuterer. Hvis kompositionen er både kommutativ og associativ, er $a_1 * \cdots * a_n = a_{p_1} * \cdots * a_{p_n}$, når $p_1, \ldots, p_n$ er tallene $1, \ldots, n$ i en anden rækkefølge.

I tilfælde af en endelig mængde M viser kommutativitet sig ved at kompositionstabellen er symmetrisk

om hoveddiagonalen, når elementerne af M skrives i samme rækkefølge i indgangssøjlen og indgangsrækken.

Hvis kompositionen $*$ har et neutralt element e, siges et element $a \in M$ at have elementet b som <u>inverst</u> element ved $*$, hvis

$$a * b = b * a = e.$$

Hvis komposition'en er associativ, har et element $a \in M$ højst ét inverst. Thi hvis b_1 og b_2 begge er inverse til a gælder både $b_1 * a * b_2 = b_1 * e = b_1$ og $b_1 * a * b_2 = e * b_2 = b_2$. Hvis elementet a har et inverst, kaldes a <u>invertibelt</u>. Det inverse element b er da også invertibelt, idet det har a til inverst. Det neutrale element e er invertibelt, idet det har sig selv til inverst.

Et element $a \in M$ kaldes <u>involutorisk</u>, hvis $a * a = e$, d.v.s. hvis det har sig selv til inverst.

Når $\top$ og $*$ er kompositioner i en mængde M, siges $*$ at være <u>distributiv</u> med hensyn til $\top$, hvis der for vilkårlige $a, b, c \in M$ gælder

$$a * (b \top c) = (a * b) \top (a * c)$$

$$(a \top b) * c = (a * c) \top (b * c).$$

[Hvis $*$ er kommutativ, er det naturligvis nok at forlange den første regel opfyldt.]

Lad $(M, \top, *, \ldots)$ være en mængde organiseret ved kompositioner. En delmængde L af M kaldes <u>stabil</u> overfor kompositionerne $\top, *, \ldots$, hvis der for vilkårlige $a, b \in L$ gælder $a \top b \in L$, $a * b \in L$, ...

Når L er stabil, er der ved $(a,b) \mapsto a \top b$, $(a,b) \mapsto a * b$, ... , idet man indskrænker sig til at betragte elementer $a, b \in L$, defineret kompositioner i L, som det er praktisk også at betegne $\top, *, \ldots$. En stabil delmængde L bliver herved til den organiserede mængde $(L, \top, *, \ldots)$. Man siger, at organisationen af M inducerer en tilsvarende organisation af L.

Additiv og multiplikativ skrivemåde. Vi får kun anledning til at betragte associative kompositioner. For associative kompositioner benyttes i langt de fleste tilfælde enten den additive skrivemåde, d.v.s. kompositionen betegnes $+$, og $a+b$ kaldes summen af a og b, eller den multiplikative skrivemåde, d.v.s. kompositionen betegnes $\cdot$ (og tegnet udelades ofte), og $a \cdot b$ kaldes produktet af a og b. Den additive skrivemåde benyttes kun, når kompositionen tillige er kommutativ; den multiplikative skrivemåde bruges både for kommutative og ikke kommutative kompositioner.

I tilfælde af additiv skrivemåde betegnes et neutralt element i reglen med o eller 0 (eller lign.) og kaldes nulelementet, og et inverst element betegnes $-a$ og kaldes også det modsatte element til a. En sum $a+\ldots+a$ af n ens addender betegnes na. Hvis der findes et neutralt element o, skrives $0a = o$, og hvis a har et modsat element $-a$ skrives i stedet for $n(-a)$ også $(-n)a$. Hvis a

har et modsat element kaldes $(-a)+b = b+(-a)$ <u>differensen</u> af b og a og skrives også $-a+b$ eller $b-a$.

I tilfælde af multiplikativ skrivemåde betegnes et neutralt element i reglen med e eller 1 (eller lign.) og kaldes <u>et elementet</u>, og et inverst element betegnes a^{-1} og kaldes det <u>reciproke</u> element til a. Et produkt $a \cdots a$ af n ens faktorer betegnes a^n. Hvis der findes et neutralt element e skrives $a^0 = e$, og hvis a har et inverst element a^{-1} skrives i stedet for $(a^{-1})^n$ også a^{-n}. Hvis multiplikationen tillige er kommutativ og a har et inverst element kaldes $a^{-1}b = ba^{-1}$ <u>kvotienten</u> af b og a og skrives også $\frac{b}{a}$.

<u>Homomorfi, isomorfi, endomorfi, automorfi.</u>

Lad $(M, \top, *, \cdots)$ og $(\hat{M}, \hat{\top}, \hat{*}, \cdots)$ være to mængder organiseret ved lige mange kompositioner. Ved en <u>homomorf afbildning</u> eller kort en <u>homomorfi</u> af M ind i $\hat{M}$ forstås en afbildning $\varphi: M \to \hat{M}$, for hvilken der for vilkårlige $a, b \in M$ gælder

$$\varphi(a \top b) = \varphi(a) \hat{\top} \varphi(b), \quad \varphi(a * b) = \varphi(a) \hat{*} \varphi(b), \quad \cdots.$$

En homomorf afbildning $\varphi: M \to \hat{M}$ kaldes <u>isomorf</u> eller en <u>isomorfi</u>, hvis φ er bijektiv; da er den omvendte afbildning $\varphi^{-1}: \hat{M} \to M$ også en isomorfi.

De to organiserede mængder $(M, \top, *, \cdots)$ og $(\hat{M}, \hat{\top}, \hat{*}, \cdots)$ kaldes <u>isomorfe</u>, hvis der findes en isomorf afbildning $\varphi: M \to \hat{M}$. Man kan udtrykke dette ved at sige, at de to organiserede mængder har nøjagtigt samme struktur, så at forskellen kun ligger i, at det er forskellige mængder der bærer strukturen. Man udtrykker det ofte ved at sige,

at $(M, \top, *, \dots)$ og $(\hat{M}, \hat{\top}, \hat{*}, \dots)$ er forskellige eksemplarer af den samme struktur.

Hvis specielt $(\hat{M}, \hat{\top}, \hat{*}, \dots) = (M, \top, *, \dots)$, så at der kun er tale om een organiseret mængde $(M, \top, *, \dots)$, benyttes i stedet for ordene homomorf, homomorfi, isomorf, isomorfi ordene endomorf, endomorfi, automorf, automorfi. En endomorf afbildning eller en endomorfi i M er altså en afbildning $\varphi: M \to M$, for hvilken der for vilkårlige $a, b \in M$ gælder

$$\varphi(a \top b) = \varphi(a) \top \varphi(b), \quad \varphi(a * b) = \varphi(a) * \varphi(b), \quad \dots.$$

En endomorf afbildning $\varphi: M \to M$ kaldes automorf eller en automorfi, hvis φ er bijektiv.

Den i det foregående indførte terminologi finder analog anvendelse, når talen er om en mængde M organiseret på anden måde end netop ved kompositioner inden for mængden; for eksempel kan der i organisationen indgå kompositioner $f: M \times M \to Z$, hvor Z er en fra M forskellig mængde, eller kompositioner $f: X \times M \to M$, hvor X er en fra M forskellig mængde. I teorien for vektorrum og metriske rum, som vil blive udførligt behandlet, møder vi typiske eksempler af denne art. I mange tilfælde har man dog særlige navne for de pågældende begreber. Eksempelvis i tilfælde af mængder organiseret ved ordningsrelationer:

Hvis $(M, \preceq)$ og $(\hat{M}, \hat{\preceq})$ er ordnede mængder, og $\varphi: M \to \hat{M}$ er en afbildning, for hvilken der for vilkårlige $a, b \in M$ gælder $a \preceq b \Rightarrow \varphi(a) \hat{\preceq} \varphi(b)$, taler man

ikke om en homomorf afbildning, men man siger, at afbildningen er <u>monotont voksende</u> eller stigende. Hvis $a \preceq b \Rightarrow \varphi(a) \hat{\preceq} \varphi(b)$ siges den at være <u>monotont aftagende</u> eller dalende. Hvis $a \prec b \Rightarrow \varphi(a) \hat{\prec} \varphi(b)$ siges den at være <u>ordenstro</u> eller <u>strengt voksende</u>. Hvis $a \prec b \Rightarrow \varphi(a) \hat{\succ} \varphi(b)$ siges den at være <u>strengt aftagende</u>.

§5. Grupper. Transformationer. Permutationer.

Grupper. Ved en gruppe forstås en mængde G organiseret ved een komposition, som opfylder følgende betingelser: (1) Kompositionen er associativ; (2) der findes et neutralt element; (3) ethvert element af G har et inverst. En komposition med disse egenskaber kaldes kort en gruppekomposition.

Idet vi benytter den multiplikative skrivemåde, kan definitionen udtrykkes således:

En gruppe $(G,\cdot)$ er en mængde G organiseret ved een komposition $\cdot$, der opfylder følgende betingelser:

(1) for vilkårlige elementer $a,b,c \in G$ gælder $(ab)c = a(bc)$;

(2) der findes et element $e \in G$, gruppens etelement, for hvilket $ea = ae = a$ for alle $a \in G$;

(3) ethvert element $a \in G$ har et inverst element a^{-1}, for hvilket $aa^{-1} = a^{-1}a = e$.

Hvis G er endelig, kaldes antallet af elementer i G gruppens orden.

En gruppe kan bestå af etelementet alene. I en mængde bestående af eet element findes kun een komposition, og mængden er med denne komposition en gruppe.

Når $(G,\cdot)$ er en gruppe, har for vilkårlige $a,b \in G$ hver af ligningerne $ax = b$ og $ya = b$ een løsning, nemlig henholdsvis $x = a^{-1}b$ og $y = ba^{-1}$. Thi disse elementer ses at være løsninger til ligningerne, og

ligningerne kan åbenbart ikke have andre løsninger [af $ax = b$ følger nemlig $x = ex = (a^{-1}a)x = a^{-1}(ax) = a^{-1}b$ og af $ya = b$ følger $y = ye = y(aa^{-1}) = (ya)a^{-1} = ba^{-1}$].

Hvis H er en stabil delmængde af G, har det mening at tale om $(H, \cdot)$. Man ser umiddelbart, at $(H, \cdot)$ er en gruppe, hvis og kun hvis $e \in H$ og der for ethvert $a \in H$ gælder $a^{-1} \in H$. En sådan gruppe kaldes en <u>undergruppe</u> af $(G, \cdot)$.

Lad $(M, \cdot)$ være en mængde med en komposition, som er associativ, og for hvilken der findes et neutralt element e. Da har hver af ligningerne $ax = b$ og $ya = e$ en løsning, forsåvidt a er invertibelt, nemlig henholdsvis $x = a^{-1}b$ og $y = ba^{-1}$. Endvidere gælder, at <u>mængden G af invertible elementer er stabil</u>, og at $(G, \cdot)$ <u>er en gruppe</u>. For at indse dette bemærker vi: Hvis a og b er invertible, er ab invertibelt; thi $b^{-1}a^{-1}$ er åbenbart inverst til ab. Altså er G stabil, og det har mening at tale om $(G, \cdot)$. Endvidere er e invertibelt, idet e har sig selv til inverst, og hvis a er invertibelt er a^{-1} invertibelt, idet a^{-1} har a til inverst. Herefter er det klart, at $(G, \cdot)$ er en gruppe.

En gruppe med kommutativ komposition kaldes <u>kommutativ</u> eller <u>abelsk</u> (efter N. H. Abel). Idet vi benytter den additive skrivemåde, altså betegner gruppen $(G, +)$, er løsningen til ligningen $a + x = b$ differensen $x = b - a$.

Transformationer. Lad M være en vilkårlig mængde, og lad G være mængden af alle bijektive afbildninger af M på sig selv. Da er G med sammensætningen $\circ$ som komposition åbenbart en gruppe. Det neutrale element e i $(G,\circ)$ er den identiske afbildning id_M og det inverse element hø et element $f \in G$ er den omvendte afbildning f^{-1}. [Disse betegnelser svarer til, at vi betragter skrivemåden $g \circ f$ som multiplikativ.] De bijektive afbildninger af M på sig selv kaldes transformationer eller permutationer af M, og gruppen $(G,\circ)$ kaldes den fulde transformationsgruppe eller permutationsgruppe for M. Ordet transformation bruges især, når M er uendelig, ordet permutation især, når M er endelig. En undergruppe af $(G,\circ)$ kaldes en transformationsgruppe eller permutationsgruppe i M.

Lad M og $\hat{M}$ være mængder, og antag, at der findes en bijektiv afbildning $\varphi: M \to \hat{M}$, altså at M og $\hat{M}$ er ækvipotente. Lad $(G,\circ)$ og $(\hat{G},\circ)$ være den fulde transformationsgruppe for henholdsvis M og $\hat{M}$. For ethvert $f \in G$ er da $\hat{f} = \varphi \circ f \circ \varphi^{-1}$ en transformation i $\hat{M}$, altså $\hat{f} \in \hat{G}$. Man ser umiddelbart, at den ved $f \mapsto \hat{f} = \varphi \circ f \circ \varphi^{-1}$ bestemte afbildning af G ind i $\hat{G}$ er bijektiv, og at den er en isomorfi. Strukturen af den fulde transformationsgruppe for to ækvipotente mængder er således den samme.

I tilfælde af en uendelig mængde M har man i almindelighed ikke anledning til at betragte den

fulde transformationsgruppe $(G, \circ)$, men kun udvalgte undergrupper af den. I det sædvanlige rum er således mængden af flytninger en transformationsgruppe; ligeledes mængden af parallelforskydninger.

Derimod spiller den fulde permutationsgruppe for en endelig mængde med n elementer en betydningsfuld rolle i mange forbindelser, og vi vil derfor give den en mere indgående behandling.

Permutationer i en mængde med n elementer:
Lad M være en endelig mængde med n elementer. Det er hensigtsmæssigt at give dem navne, og vi vælger at benævne dem $1, \ldots, n$, således at M simpelthen bliver mængden $\{1, \ldots, n\}$. Det er iøvrigt netop dette tilfælde man oftest har anledning til at betragte. Den fulde permutationsgruppe for $M = \{1, \ldots, n\}$ kaldes den symmetriske gruppe af graden n og betegnes S_n.

Et element f af S_n angives ved en tabel

$$f = \begin{bmatrix} x_1 & \cdots & x_n \\ y_1 & \cdots & y_n \end{bmatrix},$$

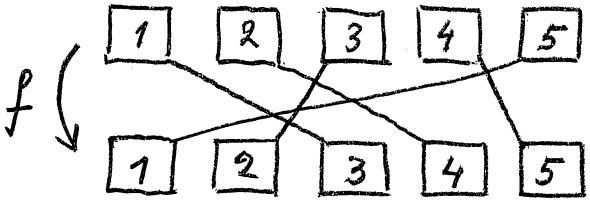
hvor der i første række står tallene $1, \ldots, n$ i en eller anden rækkefølge og i anden række de tilsvarende funktionsværdier $y_1 = f(x_1), \ldots, y_n = f(x_n)$. Betingelsen for, at en sådan tabel bestemmer en permutation, er naturligvis, at der også i anden række står tallene $1, \ldots, n$ i en eller anden rækkefølge. Man kan for givet f vælge rækkefølgen i den ene eller den anden af de to rækker efter behag. De forskellige tabeller, der fremstiller samme permutation f, be-

står af de samme tal, blot i forskellig rækkefølge.

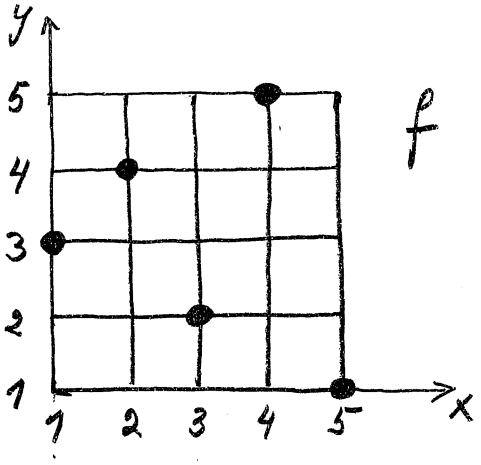
Eksempelvis er for $n=5$ en permutation f bestemt ved

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 4 & 3 & 5 & 1 \\ 4 & 5 & 2 & 1 & 3 \end{bmatrix} = \begin{bmatrix} 5 & 3 & 1 & 2 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{bmatrix}.$$

Man kan også benytte grafiske afbildninger. Den anførte permutation kan således fremstilles på følgende måder:



eller



I den anden fremstilling har vi simpelthen tegnet grafen for f, idet $M \times M$ repræsenteres ved mængden af gitterpunkter i kvadratnettet.

Vælger man specielt i tabellen for en permutation $f \in S_n$ som første række $(1, \ldots, n)$, bliver anden række $(f(1), \ldots, f(n))$. Et sådant ordnet talsat bestående af tallene $1, \ldots, n$ i en eller anden rækkefølge er det man i den elementære kombinatorik kalder en permutation af elementerne $1, \ldots, n$. Af sådanne findes som bekendt $n!$. Den symmetriske gruppe S_n har således ordenen $n!$.

For $n=1$ indeholder S_n kun ét element, nemlig den identiske afbildning.

For $n=2$ består S_n af to elementer $e = \begin{bmatrix} 1 & 2 \\ 1 & 2 \end{bmatrix}$ og $a = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$, og strukturen af S_2 er angivet ved at $a \circ a = e$, idet det er overflødigt at anføre de trivielle relationer $e \circ e = e$, $e \circ a = a \circ e = a$. [I øvrigt er dette, som man

umiddelbart ser, den eneste mulige struktur af en gruppe med to elementer.] Man ser, at S_2 er kommutativ.

For $n=3$ består S_n af seks elementer. Idet vi betegner dem

$$① = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix} \quad ② = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \quad ③ = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

$$④ = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix} \quad ⑤ = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \quad ⑥ = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix},$$

er kompositionstabellen følgende:

	①	②	③	④	⑤	⑥
①	①	②	③	④	⑤	⑥
②	②	③	①	⑤	⑥	④
③	③	①	②	⑥	④	⑤
④	④	⑥	⑤	①	③	②
⑤	⑤	④	⑥	②	①	③
⑥	⑥	⑤	④	③	②	①

	f
g	g∘f

.

Man ser, at S_3 ikke er kommutativ (tabellen er ikke symmetrisk om hoveddiagonalen).

Da S_n for $n>3$ indeholder undergrupper isomorfe med S_3, nemlig dem der fås ved kun at betragte de permutationer, ved hvilke alle pånær tre bestemte af tallene $1,\dots,n$ går over i sig selv, er S_n ikke kommutativ for $n \geq 3$.

I det følgende betragtes S_n for et vilkårligt $n \geq 2$. For et vilkårligt $f = \begin{bmatrix} x_1 & \dots & x_n \\ y_1 & \dots & y_n \end{bmatrix}$ vil produktet

$$\operatorname{sign} f = \prod_{1 \leq i < j \leq n} \frac{x_j - x_i}{y_j - y_i}$$

være uafhængigt af hvilken fremstilling vi benytter

for f. Thi i en anden fremstilling optræder jo de samme søjler, blot i en anden rækkefølge, men den faktor i produktet, der hidrører fra to søjler, ændres ikke ved at søjlernes placering i forhold til hinanden skifter, idet det blot betyder, at tæller og nævner begge multipliceres med -1. Man ser, at

$$|\operatorname{sign} f| = \prod_{1 \leq i < j \leq n} \frac{|x_j - x_i|}{|y_j - y_i|} = 1.$$

Thi tællerproduktet og nævnerproduktet er begge $= 1^{n-1} 2^{n-2} \cdots (n-1)^1$. Man har altså $\operatorname{sign} f = 1$ eller $\operatorname{sign} f = -1$. Tallet $\operatorname{sign} f$ kaldes <u>fortegnet</u> for permutationen f. Man ser, at det er 1 eller -1 efterhånden som der i produktet, der definerer det, optræder et lige eller et ulige antal negative faktorer. En negativ faktor $\frac{x_j - x_i}{y_j - y_i}$ siges at svare til en <u>inversion</u> i f, og antallet af inversioner betegnes $I(f)$. Vi har altså

$$\operatorname{sign} f = (-1)^{I(f)}.$$

En permutation med fortegnet 1, altså med lige inversionstal $I(f)$, kaldes en <u>lige permutation</u>. En permutation med fortegnet -1, altså med ulige inversionstal $I(f)$, kaldes en <u>ulige permutation</u>. Man finder hurtigst inversionstallet $I(f)$ ud fra fremstillingen $f = \begin{bmatrix} 1 & \cdots & n \\ f(1) & \cdots & f(n) \end{bmatrix}$, idet man de blot skal optælle, hvor ofte det i anden række indtræffer, at et mindre tal står efter et større. Ud fra grafen for f findes $I(f)$ ved at man tæller alle forbindelseslinier mellem grafens punkter og tæller, hvormange der har negativ hældningskoefficient.

For den identiske permutation e er $I(e)=0$, altså $\operatorname{sign} e = 1$, så at e er en lige permutation.

I S_2 er således $\begin{bmatrix}1&2\\1&2\end{bmatrix}$ lige, medens $\begin{bmatrix}1&2\\2&1\end{bmatrix}$ åbenbart er ulige. I S_3 er $\begin{bmatrix}1&2&3\\1&2&3\end{bmatrix}, \begin{bmatrix}1&2&3\\2&3&1\end{bmatrix}, \begin{bmatrix}1&2&3\\3&1&2\end{bmatrix}$ lige, medens $\begin{bmatrix}1&2&3\\1&3&2\end{bmatrix}, \begin{bmatrix}1&2&3\\2&1&3\end{bmatrix}, \begin{bmatrix}1&2&3\\3&2&1\end{bmatrix}$ er ulige.

For vilkårlige permutationer $f, g \in S_n$ gælder

$$\boxed{\operatorname{sign}(g\circ f) = \operatorname{sign} f \cdot \operatorname{sign} g}.$$

Anderledes udtrykt: Ved sammensætning af to lige permutationer eller to ulige permutationer fås en lige permutation, ved sammensætning af en lige og en ulige permutation fås en ulige permutation.

Med multiplikation som komposition er mængden $\{1,-1\}$ åbenbart en gruppe. Sætningen kan også udtrykkes ved at sige, at $\operatorname{sign}: S_n \to \{1,-1\}$ er en homomorf afbildning af $(S_n,\circ)$ ind i $(\{1,-1\},\cdot)$.

Bevis. Vi vælger for f og g fremstillinger

$$f=\begin{bmatrix}x_1 & \cdots & x_n\\ y_1 & \cdots & y_n\end{bmatrix} \quad \text{og} \quad g=\begin{bmatrix}y_1 & \cdots & y_n\\ z_1 & \cdots & z_n\end{bmatrix},$$

således at den anden række i f er lig med den første række i g. Da er

$$g\circ f = \begin{bmatrix}x_1 & \cdots & x_n\\ z_1 & \cdots & z_n\end{bmatrix},$$

og formlen følger af, at

$$\prod_{1\le i<j\le n}\frac{x_j-x_i}{z_j-z_i} = \prod_{1\le i<j\le n}\frac{x_j-x_i}{y_j-y_i}\cdot\prod_{1\le i<j\le n}\frac{y_j-y_i}{z_j-z_i}. \qquad \square$$

Da e er lige, følger af formlen, at den inverse

permutation f^{-1} til en permutation f har samme fortegn som f, altså at f og f^{-1} enten begge er lige eller begge er ulige.

Ved en <u>transposition</u> forstås en permutation, der kan skrives på formen

$$t = \begin{bmatrix} i & j & \cdots \\ j & i & \cdots \end{bmatrix},$$

hvor prikkerne angiver søjler, i hvilke der står det samme på begge pladser. Vi har altså $t(i) = j$, $t(j) = i$, medens $t(k) = k$ for alle $k \neq i, j$. Kort udtrykt består transpositionen i <u>ombytning</u> af i og j. <u>Enhver transposition har fortegnet</u> -1, <u>er altså en ulige permutation</u>. Thi i det produkt, der tjener til definition af sign t, optræder hidrørende fra søjlerne $\begin{bmatrix} i \\ j \end{bmatrix}$ og $\begin{bmatrix} j \\ i \end{bmatrix}$ faktoren $\frac{j-i}{i-j} = -1$, hidrørende fra søjlerne $\begin{bmatrix} i \\ j \end{bmatrix}$ og $\begin{bmatrix} j \\ i \end{bmatrix}$ taget sammen med en søjle $\begin{bmatrix} k \\ k \end{bmatrix}$ faktorerne $\frac{k-i}{k-j}$ og $\frac{k-j}{k-i}$, hvis produkt er 1, og hidrørende fra alle andre par af to søjler en faktor 1. Altså er sign $t = -1$. Der er i S_n ialt $\binom{n}{2} = \frac{n(n-1)}{2}$ transpositioner. En transposition er åbenbart <u>involutorisk</u>.

<u>Enhver permutation</u> $f \in S_n$ <u>kan dannes ved sammensætning af transpositioner</u>, d.v.s. den kan skrives på formen

$$f = t_p \circ \cdots \circ t_1,$$

hvor $t_1, \ldots, t_p$ er transpositioner. [Et tomt udtryk skal naturligvis betegne den identiske permutation e; iøvrigt kan e også fremstilles ved

ikke tomme udtryk, f. eks. ved $e = t \circ t$, hvor t er en vilkårlig transposition.]

Bevis. Vi fører beviset ved induktion efter n. For S_2 er udsagnet evident. Antag det rigtigt for S_{n-1} (hvor $n \geq 3$), og betragt en permutation $f \in S_n$. Hvis $f(n) = n$, er $f' = \begin{bmatrix} 1 & \cdots & n-1 \\ f(1) & \cdots & f(n-1) \end{bmatrix}$ en permutation i S_{n-1}, og f' kan altså dannes ved sammensætning af transpositioner $t' = \begin{bmatrix} i & j & \cdots \\ j & i & \cdots \end{bmatrix}$ i S_{n-1}. Ved sammensætning af de tilsvarende transpositioner $t = \begin{bmatrix} i & j & \cdots & n \\ j & i & \cdots & n \end{bmatrix}$ i S_n (i samme rækkefølge) fås f. Hvis $f(n) = m < n$, betragter vi transpositionen $t = \begin{bmatrix} n & m & \cdots \\ m & n & \cdots \end{bmatrix}$ i S_n og danner $t \circ f$. Man ser, at $t \circ f(n) = n$. Efter det lige beviste kan $t \circ f$ altså skrives på formen $t_q \circ \cdots \circ t_1$, hvor $t_1, \ldots, t_q$ er transpositioner. Men så er $f = t \circ t_q \circ \cdots \circ t_1$. □

Når $f = t_p \circ \cdots \circ t_1$, er $\operatorname{sign} f = (-1)^p$. Vi ser altså:

Når en permutation f er dannet ved sammensætning af transpositioner, er disses antal lige eller ulige, eftersom f er lige eller ulige.

En transposition kan specielt bestå i en ombytning af naboer, d.v.s. af to elementer i, j, hvor $|i - j| = 1$. Der er i S_n ialt $n-1$ sådanne transpositioner.

Enhver permutation kan dannes ved sammensætning af transpositioner, der hver består i en ombytning af naboer.

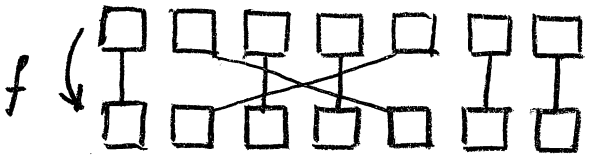
Bevis. Det er tilstrækkeligt at vise, at enhver transposition $t = \begin{bmatrix} i & j & \cdots \\ j & i & \cdots \end{bmatrix}$ kan dannes på denne måde. Vi kan antage $j = i+k$, hvor $k \geq 2$. Man ser, at

$$t = t_1 \circ t_2 \circ \cdots \circ t_k \circ \cdots \circ t_2 \circ t_1,$$

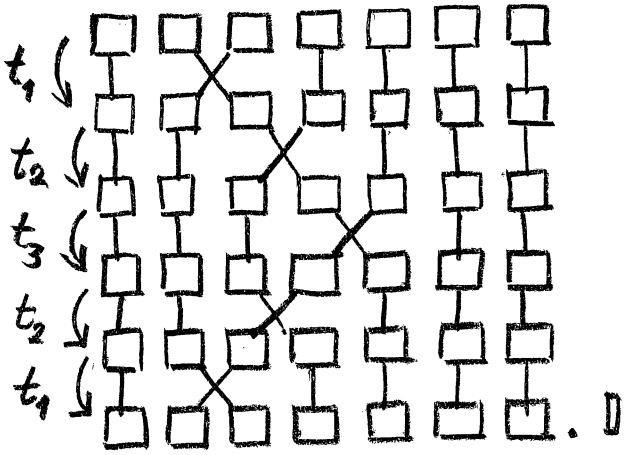
hvor

$$t_1 = \begin{bmatrix} i & i+1 & \cdots \\ i+1 & i & \cdots \end{bmatrix}, \quad t_2 = \begin{bmatrix} i+1 & i+2 & \cdots \\ i+2 & i+1 & \cdots \end{bmatrix}, \cdots, t_k = \begin{bmatrix} i+k-1 & i+k & \cdots \\ i+k & i+k-1 & \cdots \end{bmatrix}.$$

Beviset kan illustreres ved følgende diagram:



$f = t_1 \circ t_2 \circ t_3 \circ t_2 \circ t_1$



. □

Der findes i S_n lige mange lige og ulige permutationer, altså $\frac{1}{2}n!$ af hver slags.

Bevis. Lad $f_1, \cdots, f_N$ være alle de lige permutationer, og lad g være en bestemt ulige permutation. Da er permutationerne $g \circ f_1, \cdots, g \circ f_N$ parvis forskellige ulige permutationer. Enhver ulige permutation h er med blandt disse; thi da g^{-1} er ulige, er $g^{-1} \circ h$ lige, altså lig med et f_s, og følgelig er $h = g \circ f_s$. □

Mængden A_n af lige permutationer i S_n er en undergruppe i S_n. Thi vi har vist, at $f, g \in A_n$ medfører $g \circ f \in A_n$, at $e \in A_n$, og at $f \in A_n$ medfører $f^{-1} \in A_n$.

Denne gruppe A_n kaldes den <u>alternerende gruppe af graden</u> n.

Vi gik ud fra en endelig mængde M og valgte at kalde dens elementer $1, \dots, n$, således at M blev mængden $\{1, \dots, n\}$. Definitionen af fortegnet for en permutation i M beroede på denne nummerering. Af sætningen om, at en permutation er lige eller ulige, eftersom den kan sammensættes af et lige eller et ulige antal transpositioner, fremgår imidlertid, at fortegnet for en permutation i M må være uafhængigt af, hvilken af de $n!$ mulige nummereringer af M man vælger. Inddelingen af permutationerne i den fulde permutationsgruppe $(G, \circ)$ for en endelig mængde M i lige og ulige permutationer er således uafhængig af nummereringen.

<u>Øvelse</u>. For $n \geq 2$ betegner vi, når p er et af tallene $2, \dots, n$, som en p-<u>cykel</u> i S_n en permutation, der kan skrives på formen

$$c = \begin{pmatrix} i_1 & i_2 & \cdots & i_{p-1} & i_p & \cdots \\ i_2 & i_3 & \cdots & i_p & i_1 & \cdots \end{pmatrix},$$

hvor prikkerne efter den p^{te} søjle angiver søjler, i hvilke der står det samme på begge pladser. Man ser, at en 2-cykel er det samme som en transposition. Man indser let, at <u>enhver p-cykel har fortegnet</u> $(-1)^{p-1}$; den er altså ulige eller lige eftersom p er lige eller ulige. I reglen anvender man den forenklede skrivemåde

$$c = (i_1 \cdots i_p).$$

Man bemærker, at c ikke ændres ved cyklisk for-

skydning af $i_1, \ldots, i_p$, d.v.s. $(i_1 \cdots i_p) = (i_2 \cdots i_p\ i_1) = \cdots = (i_p\ i_1 \cdots i_{p-1})$, og at $c^{-1} = (i_p \cdots i_1)$. Man indser endvidere, at to cykler $(i_1 \cdots i_p)$ og $(j_1 \cdots j_q)$, hvor $\{i_1, \ldots, i_p\}$ og $\{j_1, \ldots, j_q\}$ er disjunkte, kommuterer. Enhver permutation $f \in S_n$ kan på en og, bortset fra cyklernes rækkefølge, kun på een måde dannes ved sammensætning af cykler, for hvilke de tilsvarende delmængder af $\{1, \ldots, n\}$ er parvis disjunkte. [Som tidligere skal et tomt udtryk betegne den identiske permutation e.] Fortegnet for permutationen er $(-1)^s$, hvor s er antallet af cykler i fremstillingen med lige elementtal p.

Eksempelvis finder man for permutationen

$$f = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 6 & 1 & 3 & 5 & 2 & 7 \end{bmatrix} = \begin{bmatrix} 1 & 4 & 3 & 2 & 6 & 5 & 7 \\ 4 & 3 & 1 & 6 & 2 & 5 & 7 \end{bmatrix}$$

fremstillingen

$$f = (1\ 4\ 3) \circ (2\ 6).$$

Gruppeteorien udvikledes i løbet af 18-hundredtallet, længe — til henimod 1880 — næsten udelukkende som en teori om transformationsgrupper (A.-L. Cauchy, É. Galois, C. Jordan). Det almene gruppebegreb går dog tilbage til 1854 (A. Cayley). Ved overgangen 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 undergruppe af den fulde transformationsgruppe $(\Gamma, \circ)$ for mængden G. For at indse dette bemærker man,

at hvis a er et element af G, defineres ved $x \mapsto ax$, $x \in G$, en bijektiv afbildning $\tau_a : G \to G$. Ved $a \mapsto \tau_a$, $a \in G$, defineres således en afbildning $\varphi : G \to \Gamma$. Man eftervise nu let, at φ er injektiv, at $\varphi(G)$ er stabil overfor $\circ$, at $(\varphi(G), \circ)$ er en undergruppe af $(\Gamma, \circ)$, og at φ, betragtet som en afbildning af G på $\varphi(G)$, er en isomorfi.

Opgaver. 1. Udregn $\begin{bmatrix}1&2&3\\2&3&1\end{bmatrix} \circ \begin{bmatrix}1&2&3\\2&3&1\end{bmatrix}$, $\begin{bmatrix}1&2&3\\2&3&1\end{bmatrix}^{-1}$, $\begin{bmatrix}1&2&3&4&5\\2&3&1&5&4\end{bmatrix} \circ \begin{bmatrix}1&2&3&4&5\\3&5&4&1&2\end{bmatrix}$, $\begin{bmatrix}1&2&3&4&5&6\\2&4&6&1&3&5\end{bmatrix}^{-1}$.

2. Find fortegnet for følgende permutationer i S_5: $\begin{bmatrix}1&2&3&4&5\\5&4&3&2&1\end{bmatrix}$ og $\begin{bmatrix}1&2&3&4&5\\2&3&4&5&1\end{bmatrix}$.

3. Bestem antallet af permutationer i S_n, ved hvilke intet element af $\{1, \dots, n\}$ afbildes i sig selv.

4. Find samtlige undergrupper i S_3.

5. Vis, at permutationerne

$$f_1 = \begin{bmatrix}1&2&3&4\\1&2&3&4\end{bmatrix},\ f_2 = \begin{bmatrix}1&2&3&4\\3&2&1&4\end{bmatrix},\ f_3 = \begin{bmatrix}1&2&3&4\\1&4&3&2\end{bmatrix},\ f_4 = \begin{bmatrix}1&2&3&4\\3&4&1&2\end{bmatrix}$$

danner en gruppe.

6. Fremstil hver af permutationerne

$$\begin{bmatrix}1&2&3&4&5\\2&3&4&5&1\end{bmatrix} \quad \text{og} \quad \begin{bmatrix}1&2&3&4&5\\3&4&1&5&2\end{bmatrix}$$

som sammensætning af transpositioner.

7. Vis, at enhver permutation i S_n kan dannes ved sammensætning af transpositioner af formen

$$\begin{bmatrix}1&k&\dots\\k&1&\dots\end{bmatrix}, \quad k = 2, \dots, n.$$

8. Opstil en nødvendig og tilstrækkelig betingelse

for, at to transpositioner $\begin{pmatrix} i & j & \dots \\ j & i & \dots \end{pmatrix}$ og $\begin{pmatrix} k & l & \dots \\ l & k & \dots \end{pmatrix}$ i S_n kommuterer.

9. Vis, at et element $f \in S_n$ er involutorisk, hvis og kun hvis det kan skrives på formen

$$f = \begin{pmatrix} i_1 & j_1 & \dots \\ j_1 & i_1 & \dots \end{pmatrix} \circ \dots \circ \begin{pmatrix} i_p & j_p & \dots \\ j_p & i_p & \dots \end{pmatrix},$$

hvor transpositionerne opfylder den betingelse, at $\{i_u, j_u\}$ og $\{i_v, j_v\}$ er disjunkte, når $u, v \in \{1, \dots, p\}$ og $u \neq v$. Benyt dette til at bestemme antallet af involutoriske elementer i S_n.

*10. Bevis, at hvis T er en delmængde af S_n bestående af færre end $n-1$ transpositioner, er det ikke muligt at danne enhver permutation i S_n ved sammensætning af elementer fra T.

11. Opskriv permutationerne $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 7 & 3 & 8 & 5 & 1 & 6 \end{pmatrix}$ og $(1\,3\,5) \circ (1\,2\,4\,8) \circ (7\,1\,3\,5) \circ (2\,4\,8)$ i S_8 som sammensætning af cykler, for hvilke de tilsvarende delmængder af $\{1, \dots, 8\}$ er disjunkte.

12. Find fortegnet af permutationen

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 6 & 2 & 4 & 1 & 3 & 5 & 7 \end{pmatrix},$$

dels ved at tælle inversionerne, dels ved at skrive den som sammensætning af cykler, for hvilke de tilsvarende delmængder af $\{1, \dots, 8\}$ er disjunkte.

*13. Vis, at enhver lige permutation i S_n kan dannes ved sammensætning af 3-cykler af formen $(1\,2\,k)$, hvor $3 \leqslant k \leqslant n$.

14. Opskriv kompositionstabellen for den alternerende gruppe af graden 4.

*15. Et velkendt legetøj består i en lille kvadratisk æske, hvori er anbragt 15 kvadratiske brikker med numrene 1 til 15, som vist på figur 1. Man kan nu puffe en af brikkerne 12 og 15 ind i det tomme felt, derefter atter en af de brikker, der støder op til det således fremkomne tomme felt, ind i dette, etc. Man skal på denne måde frembringe forskellige ongåede stillinger af brikkerne, f. eks. den på figur 2 viste.

Vis, at den på figur 3 angåede stilling af brikkerne kan opnås, hvis og kun hvis

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ a & b & c & d & e & f & g & h & i & j & k & l & m & n & o \end{pmatrix}$$

er en lige permutation.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Figur 1

6	7	8	9
5	14	15	10
4	13	12	11
3	2	1	

Figur 2

a	b	c	d
e	f	g	h
i	j	k	l
m	n	o	

Figur 3

§6. Ringe og legemer.

Ringe og legemer. Ved en ring forstås en mængde M organiseret ved to kompositioner $+$ og $\cdot$, der opfylder følgende betingelser: (1) additionen $+$ er en kommutativ gruppekomposition; (2) multiplikationen $\cdot$ er associativ; (3) multiplikationen er distributiv med hensyn til additionen.

Udførligt lyder definitionen således:

En ring $(M,+,\cdot)$ er en mængde M organiseret ved to kompositioner $+$ og $\cdot$, der opfylder følgende betingelser:

(1a) for vilkårlige elementer $a,b,c \in M$ gælder $(a+b)+c = a+(b+c)$ og for vilkårlige elementer $a,b \in M$ gælder $a+b = b+a$;

(1b) der findes et element o, ringens nulelement, for hvilket $a+o = a$ for alle $a \in M$;

(1c) ethvert element $a \in M$ har et modsat element $-a$, for hvilket $a+(-a) = o$;

(2) for vilkårlige elementer $a,b,c \in M$ gælder $(ab)c = a(bc)$;

(3) for vilkårlige elementer $a,b,c \in M$ gælder $a(b+c) = ab+ac$ og $(a+b)c = ac+bc$.

En ring kan bestå af nulelementet alene. En mængde bestående af eet element organiseret ved sin eneste komposition betragtet både som addition og multiplikation er med disse kompositioner en ring.

I en ring $(M,+,\cdot)$ spiller nulelementet en særlig rolle også i forhold til multiplikationen, idet der for ethvert $a \in M$ gælder

$$oa = ao = o.$$

Vælges et element $b \in M$, f.eks. $b = o$, har vi nemlig $b + o = b$, altså $(b+o)a = ba$, og dermed $ba + oa = ba$, hvoraf $oa = o$, og analogt $o + b = b$, altså $a(o+b) = ab$, og dermed $ao + ab = ab$, hvoraf $ao = o$.

Et produkt ab er altså o, hvis mindst en af faktorerne er o. Derimod gælder det omvendte ikke i almindelighed. Hvis det omvendte gælder, altså hvis et produkt ab kun er o, når mindst en af faktorerne er o, siger man at nulreglen gælder i M. Nulreglen kan også udtrykkes ved at sige, at $ab \neq o$, når $a \neq o$ og $b \neq o$; nulreglens gyldighed kommer altså ud på, at mængden $M \setminus \{o\}$ er stabil overfor multiplikationen.

Et eventuelt neutralt element e ved multiplikationen kaldes ringens ét-element. I det trivielle tilfælde $M = \{o\}$ er nulelementet tillige ét-element. I ethvert andet tilfælde er et eventuelt ét-element e sikkert $\neq o$ og nulelementet har intet reciprokt element. Ved et invertibelt element i en ring med ét-element mener man et invertibelt element med hensyn til multiplikationen.

Ved et legeme forstås en ring $M \neq \{o\}$, der har et ét-element og i hvilken ethvert fra o forskelligt element er invertibelt.

Udførligt lyder definitionen således:

Et legeme $(M, +, \cdot)$ er en ring, der opfylder følgende betingelser:

(4a) *der findes et element* $e \neq 0$, *legemets etelement, for hvilket* $ea = ae = a$ *for alle* $a \in M$;

(4b) *ethvert element* $a \in M \setminus \{0\}$ *har et reciprokt element* a^{-1}, *for hvilket* $aa^{-1} = a^{-1}a = e$.

I et legeme gælder nulreglen. Thi af $ab = 0$ og $a \neq 0$ følger $b = a^{-1}0 = 0$, og af $ab = 0$ og $b \neq 0$ følger $a = 0b^{-1} = 0$.

Hvis $(M, +, \cdot)$ er en ring, eller specielt et legeme, kaldes den kommutative gruppe $(M, +)$ ringens eller legemets additive gruppe. Hvis $(M, +, \cdot)$ er et legeme, er $(M \setminus \{0\}, \cdot)$ en gruppe; den kaldes legemets multiplikative gruppe.

En ring eller et legeme med kommutativ multiplikation kaldes en *kommutativ ring* eller et *kommutativt legeme*. Med den sædvanlige betydning af $+$ og $\cdot$ er $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ kommutative legemer, $\mathbb{Z}$ en ring med etelement, medens mængden $\{2z \mid z \in \mathbb{Z}\}$ af lige tal er en ring uden etelement. I teorien for *matricer* og *lineare afbildninger* møder vi ikke kommutative ringe af fundamental betydning. Af ikke kommutative legemer vil vi nedenfor omtale kvaternionlegemet.

I stedet for ordet legeme benyttes også ordet *divisionsring* eller *skævlegeme*, og ordet legeme forbeholdes da de kommutative legemer.

De fra regning med tallene velkendte algebraiske regler (vedrørende multiplikation af summer, etc.) gælder i vilkårlige ringe og legemer, med de nødvendige modifikationer i tilfælde af, at multiplikationen ikke er kommutativ. Vi indskrænker os til for en

vilkårlig ring at eftervise reglerne

$$(-a)b = -ab, \qquad a(-b) = -ab$$

(hvoraf naturligvis følger $(-a)(-b) = -a(-b) = -(-ab) = ab$). Den første regel fremgår af, at $ab + (-a)b = (a + (-a))b = 0b = 0$, den anden af, at $ab + a(-b) = a(b + (-b)) = a0 = 0$.

Er $(M, +, \cdot)$ en ring, og er H en delmængde af M, der er stabil overfor begge kompositioner $+$ og $\cdot$, har det mening at tale om $(H, +, \cdot)$. Man ser umiddelbart, at $(H, +, \cdot)$ er en ring, hvis og kun hvis $0 \in H$ og der for ethvert $a \in H$ gælder $-a \in H$. En sådan ring kaldes en <u>delring</u> af $(M, +, \cdot)$. Er $(M, +, \cdot)$ et legeme, vil en delring $(H, +, \cdot)$ være et legeme, hvis og kun hvis $e \in H$ og der for ethvert $a \in H \setminus \{0\}$ gælder $a^{-1} \in H$. Et sådant legeme $(H, +, \cdot)$ kaldes et <u>dellegeme</u> af $(M, +, \cdot)$.

<u>Funktionsringe.</u> Lad $\mathcal{E}$ være en vilkårlig ikke tom mængde og $(M, +, \cdot)$ en ring, og lad $\mathcal{F}$ betegne mængden af alle funktioner $f: \mathcal{E} \to M$. I $\mathcal{F}$ indfører vi to kompositioner, der også betegnes $+$ og $\cdot$, idet vi for vilkårlige $f, g \in \mathcal{F}$ og ethvert $x \in \mathcal{E}$ sætter

$$(f+g)(x) = f(x) + g(x), \qquad (fg)(x) = f(x)\,g(x).$$

Da er $(\mathcal{F}, +, \cdot)$ åbenbart en ring. Dens nulelement er funktionen 0 (den funktion, der for ethvert $x \in \mathcal{E}$ har værdien 0). For ethvert $x \in \mathcal{E}$ er afbildningen $f \mapsto f(x)$ en homomorf afbildning af $(\mathcal{F}, +, \cdot)$ på $(M, +, \cdot)$. Hvis $\mathcal{E}$ kun består af et element, er $\mathcal{F}$ og M altså isomorfe. Hvis nulreglen ikke gælder i M, gælder den naturligvis heller ikke i $\mathcal{F}$. Men selv om nulreglen gælder i M, vil den ikke gælde i $\mathcal{F}$,

når blot $M \neq \{0\}$ og $\mathfrak{E}$ indeholder mere end eet element. Thi vælges et element $a \neq 0$ i M og to forskellige elementer y og z i $\mathfrak{E}$, ser man, at de to funktioner f og g, der defineres ved

$$f(x) = \begin{cases} a & \text{for } x = y \\ 0 & \text{for } x \neq y \end{cases} \quad \text{og} \quad g(x) = \begin{cases} a & \text{for } x = z \\ 0 & \text{for } x \neq z \end{cases}$$

begge er $\neq$ funktionen 0, og dog er $fg = 0$.

Ringen $(\mathfrak{F}, +, \cdot)$ kaldes den fulde funktionsring over $\mathfrak{E}$ hørende til M og enhver delring af den en funktionsring over $\mathfrak{E}$ hørende til M.

Det er klart, at $\mathfrak{F}$ er kommutativ, hvis M er kommutativ.

Man ser, at $\mathfrak{F}$ kun er et legeme i det trivielle tilfælde, hvor M er et legeme og $\mathfrak{E}$ består af netop eet element.

Ordnede ringe og legemer. Ved en ordnet ring $(M, +, \cdot, \leqslant)$ forstås en kommutativ ring udstyret med en total ordningsrelation $\leqslant$, der opfylder betingelserne

$$a \leqslant b \Rightarrow a + c \leqslant b + c \quad \text{for ethvert } c$$

$$a \leqslant b \Rightarrow ac \leqslant bc \quad \text{for ethvert } c \geqslant 0.$$

Er ringen et legeme, taler man om et ordnet legeme.

Med den sædvanlige betydning af $\leqslant$ er $\mathbb{Z}$ og $\{2z \mid z \in \mathbb{Z}\}$ ordnede ringe og $\mathbb{Q}$ og $\mathbb{R}$ ordnede legemer.

I en ordnet ring siges et element $a \neq 0$ at være positivt, hvis $a > 0$, og negativt, hvis $a < 0$. Man viser let, at hvis a er positivt, er $-a$ negativt, og omvendt. Endvidere, at summen af to positive elementer er positiv, summen af to negative elementer negativ, at produktet af to positive eller to negative elementer er posi-

tivt, og at produktet af et positivt og et negativt element er negativt. Heraf følger specielt, at nulreglen gælder i enhver ordnet ring. Endvidere, at hvis $M \neq \{0\}$, må et eventuelt etelement e være positivt (da $e = ee$). I en ordnet ring defineres $|a|$ som a hvis a er positivt, som 0 hvis $a = 0$, og som $-a$ hvis a er negativt. De fra regning med tallene velkendte regler for regning med uligheder og med numeriske værdier gælder i en vilkårlig ordnet ring.

Det bemærkes, at det ikke er muligt i $\mathbb{C}$ at vælge en ordningsrelation $\leqslant$, således at $(\mathbb{C}, +, \cdot, \leqslant)$ bliver et ordnet legeme.

Teorien for ringe og legemer udvikledes i anden halvdel af 18-hundredtallet i tilknytning til funktionsteori og talteori (L. Kronecker, R. Dedekind, D. Hilbert). Den almene teori er udviklet i dette århundrede (E. Steinitz, E. Noether).

§7. Reelle tal. Komplekse tal. Kvaternioner.

De reelle tal. Idet vi sammenfatter det foran om de reelle tal sagte konstaterer vi:

De reelle tals legeme $(\mathbb{R}, +, \cdot, \leqslant)$ er et ordnet legeme med følgende egenskab: enhver ikke tom opad begrænset delmængde af $\mathbb{R}$ har et supremum; enhver ikke tom nedad begrænset delmængde af $\mathbb{R}$ har et infimum.

Hermed er de reelle tal karakteriseret, idet der gælder: Hvis $(\mathbb{R}', +', \cdot', \leqslant')$ og $(\mathbb{R}'', +'', \cdot'', \leqslant'')$ er ordnede legemer med den anførte egenskab, eksisterer en og kun een isomorf afbildning af $(\mathbb{R}', +', \cdot')$ på $(\mathbb{R}'', +'', \cdot'')$; denne afbildning er ordenstro.

Der gælder altså ikke blot, at $(\mathbb{R}', +', \cdot', \leqslant')$ og $(\mathbb{R}'', +'', \cdot'', \leqslant'')$ er eksemplarer af samme struktur, men endda, at hvert element af $\mathbb{R}'$ har sit bestemte tilsvarende i $\mathbb{R}''$.

Ud fra de naturlige tal kan man konstruere de reelle tal. Konstruktionen kan udføres på forskellige måder. Ved forskellige konstruktioner bliver det faktisk forskellige mængder, der kommer til at bære strukturen. I kraft af ovenstående kan man imidlertid, når konstruktionen først er udført, glemme den igen, og i fortsætningen blot fasthælde, at $(\mathbb{R}, +, \cdot, \leqslant)$ i den anførte forstand er et bestemt matematisk objekt.

Matematikken har sit udgangspunkt i studiet af tallene og de geometriske figurer. Medens den

babylonske matematik (begyndende omkr. -1800) var aritmetisk betonet, første opdagelsen af eksistensen af inkommensurable liniestykker, den tilskrives Pythagoras, til at grækerne skød geometrien i forgrunden. Den almene, af Eudoxos grundlagte, størrelseslære, som vi finder i Euklids elementer (omkr. -300) indeholder dog væsentlige træk af en teori for de positive reelle tal. De negative tal fik først rent almindeligt indpas. Med udviklingen af algebraen i 15-hundredtallet og med P. Fermats og R. Descartes' grundlæggelse af den analytiske geometri i første halvdel af 16-hundredtallet kom tallene igen i forgrunden og vejen var banet for analysen (differential- og integralregningen) som fik sin færdige form med I. Newton og G.W. Leibniz i sidste halvdel af 16-hundredtallet. Under den fortsatte udvikling i 17- og 18-hundretallet spillede spørgsmålet om matematikens grundlag kun en underordnet rolle. En strengt gennemført teori for de reelle tal blev først udført i anden halvdel af 18-hundredtallet af K. Weierstrass, G. Cantor, Ch. Méray, R. Dedekind. Samtidig indså man, at geometrien kunde underordnes aritmetikken, idet den kunde opbygges som en rent aritmetisk konstruktion. Tænker man fx. på planens geometri, går man simpelthen ud fra den analytiske geometris formelapparat, idet man vender sagen på hovedet og definerer et punkt som et ordnet par (x,y) af to reelle tal, en ret linie som mængden af løsninger (x,y) til en ligning $ax+by+c=0$, hvor $(a,b)\neq(0,0)$,

afstanden mellem to punkter (x_1, y_1) og (x_2, y_2) som $\sqrt{(x_2-x_1)^2+(y_2-y_1)^2}$, etc. Herefter fik matematikken sit grundlag i den naturlige talrække; af L. Kronecker udtrykt således: „De naturlige tal har Vorherre skabt; alt andet er menneskevark". Den naturlige talrække blev karaktemiseret af G. Peano. Om hele spørgsmålet om matematikens grundlag gælder, at det må ses i sammenhæng med den matematiske logik.

Vi vil på dette sted se bort fra en nærmere behandling af geometriens grundlag. En direkte behandling af dette emne er væsentligt mere kompliceret end behandlingen af algebraens grundlag. Vi henholder os til, at geometrien som anført kan indordnes under aritmetikken, og forudsætter i det følgende den elementære geometri bekendt. Forbindelsen med aritmetikken virker begge veje: dels gennem den analytiske behandling af geometriske opgaver, dels ved at den geometriske beskrivelse anvendes til anskueliggørelse af opgaver i analysen. Når man, som det ofte sker, anvender et geometrisk ræsonnement ved behandlingen af en rent analytisk opgave, bør man naturligvis gøre sig klart, at det kunde omsættes i en strengt aritmetisk form.

I forbindelse med de reelle tal anvender vi den velkendte sprogbrug, hvorefter $\mathbb{R}$ tænkes som en tallinie orienteret mod højre.

Som intervaller betegnes delmængder af $\mathbb{R}$ af de fire typer:

$$[a,b] = \{x \mid a \leqslant x \leqslant b\} \quad \text{afsluttet interval}$$

$$\left.\begin{aligned} [a,b[&= \{x \mid a \leqslant x < b\} \\ ]a,b] &= \{x \mid a < x \leqslant b\} \end{aligned}\right\} \text{halvåbent interval}$$

$$]a,b[= \{x \mid a < x < b\} \quad \text{åbent interval.}$$

Herved er antaget $a<b$. Punktet a er venstre endepunkt og punktet b højre endepunkt for intervallet. Lejlighedsvis er det bekvemt at regne en mængde bestående af eet punkt som et afsluttet interval med sammenfaldende endepunkter. En talmængde kaldes begrænset, hvis den er delmængde af et interval. Tallet $b-a$ kaldes længden af intervallet.

Som halvlinier betegnes delmængder af $\mathbb{R}$ af de fire typer:

$$\left.\begin{aligned}]-\infty,a] &= \{x \mid x \leqslant a\} \quad \text{afsluttet} \\ ]-\infty,a[&= \{x \mid x < a\} \quad \text{åben} \end{aligned}\right\} \text{venstre halvlinie}$$

$$\left.\begin{aligned} [a,+\infty[&= \{x \mid x \geqslant a\} \quad \text{afsluttet} \\ ]a,+\infty[&= \{x \mid x > a\} \quad \text{åben} \end{aligned}\right\} \text{højre halvlinie.}$$

Punktet a er endepunkt for halvlinien. Lejlighedsvis kaldes også halvlinier og hele $\mathbb{R}$, der også skrives $]-\infty,+\infty[$, intervaller; intervaller i den strenge betydning af ordet må da kendetegnes som begrænsede intervaller. At en delmængde A af $\mathbb{R}$ er opad begrænset med overtal a betyder, at $A \subseteq]-\infty,a]$; at A er nedad begrænset med undertal a betyder, at $A \subseteq [a,+\infty[$.

De komplekse tal. For en andengradsligning $x^2+ax+b=0$ med koefficienter $a,b \in \mathbb{R}$ fører løsningsformlen $x = -\frac{1}{2}a \pm \sqrt{\frac{1}{4}a^2-b}$ i tilfældet $\frac{1}{4}a^2-b<0$ til udtryk af formen $\alpha+\beta\sqrt{-1}$, hvor $\alpha,\beta \in \mathbb{R}$. Allerede i 15-hundred-

tallet begyndte man at operere med sådanne imaginære tal, og i løbet af 16- og 17-hundredtallet vandt de almindeligt indpas i matematiken. En tilfredsstillende fremstilling af teorien for disse tal blev dog først givet af C. Wessel (1797) og R. Argand (1806) på geometrisk grundlag og af W. R. Hamilton (1837) på aritmetisk grundlag. Betegnelsen i for den imaginære enhed $\sqrt{-1}$ går tilbage til L. Euler; med C. F. Gauss blev den en standardbetegnelse.

[Caspar Wessel (1745-1818) var en brodersønnesøn af Tordenskjold. Han virkede på fortjenstfuld måde som geodæt ved Videnskabernes Selskabs opmåling af Danmark. Broderen Johan Herman Wessel skrev om ham: „Han tegner landkort og læser loven, han er så flittig som jeg er doven".]

Efter Hamilton indføres de komplekse tal som mængden $\mathbb{R}^2$ af ordnede par af reelle tal med kompositionerne

$$(x_1, x_2) + (y_1, y_2) = (x_1 + x_2, y_1 + y_2),$$

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1 - x_2 y_2, x_1 y_2 + x_2 y_1).$$

[Disse definitioner er netop dem man føres til, når man rent formelt adderer og multiplicerer udtrykkene $x_1 + x_2\sqrt{-1}$ og $y_1 + y_2\sqrt{-1}$ og skriver resultatet på formen $z_1 + z_2\sqrt{-1}$.]

Vi vil først gøre rede for, at $\mathbb{R}^2$ med disse kompositioner er et kommutativt legeme.

Det ses umiddelbart, at $(\mathbb{R}^2, +)$ er en kommutativ gruppe. Nulelementet er $(0,0)$ og det modsatte element til et element (x_1, x_2) er $(-x_1, -x_2)$. Det ses endvidere straks, at multiplikationen er kommutativ, den er også associativ, thi

$$[(x_1,x_2)(y_1,y_2)](z_1,z_2) = (x_1y_1 - x_2y_2, x_1y_2 + x_2y_1)(z_1,z_2)$$
$$= ([x_1y_1 - x_2y_2]z_1 - [x_1y_2 + x_2y_1]z_2, [x_1y_1 - x_2y_2]z_2 + [x_1y_2 + x_2y_1]z_1)$$

og

$$(x_1,x_2)[(y_1,y_2)(z_1,z_2)] = (x_1,x_2)(y_1z_1 - y_2z_2, y_1z_2 + y_2z_1)$$
$$= (x_1[y_1z_1 - y_2z_2] - x_2[y_1z_2 + y_2z_1], x_1[y_1z_2 + y_2z_1] + x_2[y_1z_1 - y_2z_2])$$

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 element ved multiplikationen, d.v.s. etelement, mangler vi at godtgøre, at der til et vilkårligt element $(a_1,a_2) \neq (0,0)$ findes et reciprokt, altså et element (x_1,x_2), således at $(a_1,a_2)(x_1,x_2) = (1,0)$, d.v.s.

$$a_1x_1 - a_2x_2 = 1$$
$$a_2x_1 + a_1x_2 = 0;$$

for $(a_1,a_2) \neq (0,0)$ har dette ligningssystem virkelig en løsning, nemlig

$$(x_1,x_2) = \left(\frac{a_1}{a_1^2+a_2^2}, \frac{-a_2}{a_1^2+a_2^2}\right).$$

Vi betragter dernæst kompositionerne anvendt på elementer af delmængden $\hat{\mathbb{R}} = \{(x,0) \mid x \in \mathbb{R}\}$ af $\mathbb{R}^2$. Vi finder

$$(x,0) + (y,0) = (x+y,0), \qquad (x,0)\cdot(y,0) = (xy,0).$$

Man ser, at mængden $\hat{\mathbb{R}}$ er stabil overfor kompositionerne, og at afbildningen $x \mapsto (x,0)$ er en isomorf afbildning af $(\mathbb{R},+,\cdot)$ på $(\hat{\mathbb{R}},+,\cdot)$, således at $(\hat{\mathbb{R}},+,\cdot)$ blot er et nyt eksemplar af de reelle tals legeme.

Betegner vi endelig med i elementet $(0,1)$, har vi dels $i^2 = (-1,0) = -(1,0)$, dels er for et vilkårligt element (x_1,x_2)

$$(x_1,x_2) = (x_1,0) + i(x_2,0).$$

Hvis omvendt $(x_1,x_2) = (y_1,0) + i(y_2,0)$, er naturligvis $x_1=y_1, x_2=y_2$.

Idet vi opsummerer det væsentlige, har vi fundet:

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 een fremstilling af formen

$$z = z_1 + i z_2, \quad z_1, z_2 \in \mathbb{R}.$$

For ethvert sådant legeme er afbildningen $z \mapsto (z_1,z_2)$ en isomorf afbildning af $(\mathbb{C},+,\cdot)$ på det ovenfor konstruerede legeme $(\mathbb{R}^2,+,\cdot)$. To vilkårlige legemer $(\mathbb{C}',+',\cdot')$ og $(\mathbb{C}'',+'',\cdot'')$ af den anførte art er derfor isomorfe. Et legeme $(\mathbb{C},+,\cdot)$ af den anførte art kaldes et eksemplar af de komplekse tals legeme; dets elementer kaldes komplekse tal. De elementer, for hvilke $z_2\neq 0$, kaldes imaginære; de for hvilke tillige $z_1=0$, kaldes rent imaginære. Efter eksistensbevisets afslutning er der ingen fordel ved specielt at tænke på det under beviset konstruerede eksemplar.

De reelle tal z_1 og z_2 kaldes realdelen og imaginærdelen af $z=z_1+iz_2$ (strengt taget er det iz_2, der burde kaldes imaginærdelen) og betegnes ofte $\mathrm{Re}\,z$ og $\mathrm{Im}\,z$, og det komplekse tal $\overline{z} = z_1 - iz_2$ kaldes det konjugerede tal til z. Afbildningen $z\mapsto\overline{z}$ er åbenbart en bijektiv afbildning af $\mathbb{C}$ på sig selv, ved hvilken ethvert element af $\mathbb{R}$ afbildes på sig selv. For vilkårlige komplekse tal $z=z_1+iz_2$ og $w=w_1+iw_2$ gælder

$$\overline{z+w} = \overline{z} + \overline{w}, \qquad \overline{zw} = \overline{z}\cdot\overline{w}.$$

Afbildningen $z \mapsto \overline{z}$ er altså en <u>automorf afbildning</u> af $(\mathbb{C}, +, \cdot)$ på sig selv.

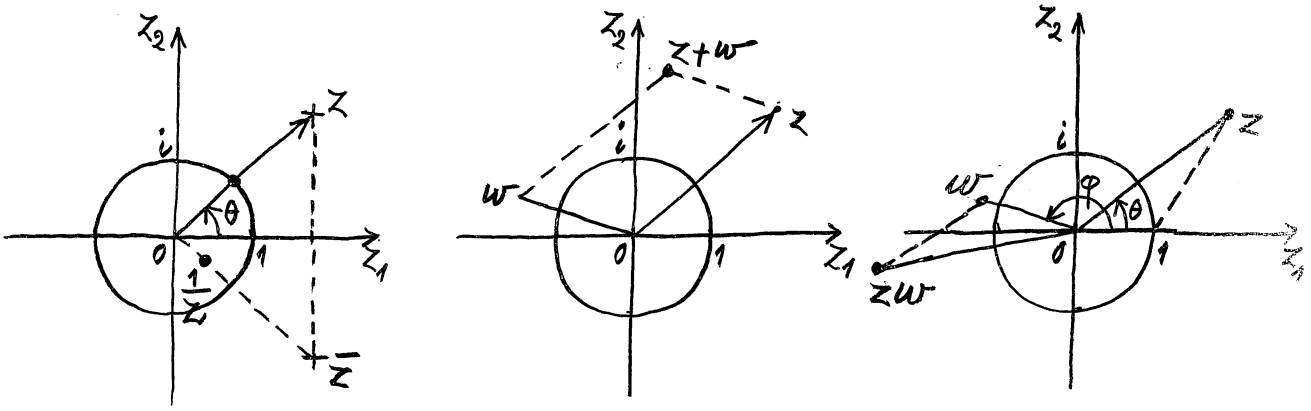
Medens der i $(\mathbb{R}, +, \cdot)$ kun findes een automorfi, nemlig den identiske afbildning, findes altså i $(\mathbb{C}, +, \cdot)$ to automorfier, der fører ethvert element af $\mathbb{R}$ over i sig selv, nemlig den identiske afbildning og afbildningen $z \mapsto \overline{z}$. Der findes ikke flere. Thi hvis φ er en sådan automorfi, må gælde $(\varphi(i))^2 = \varphi(i^2) = \varphi(-1) = -1$. Som man let konstaterer, er imidlertid i og $-i$ de eneste elementer i $\mathbb{C}$, hvis kvadrat er -1. Altså må gælde $\varphi(i) = i$ eller $\varphi(i) = -i$. I det første tilfælde finder vi for ethvert $z = z_1 + i z_2$, at $\varphi(z) = \varphi(z_1) + \varphi(i)\varphi(z_2) = z_1 + i z_2$, så at φ er den identiske afbildning. I det andet tilfælde finder vi for ethvert $z = z_1 + i z_2$, at $\varphi(z) = \varphi(z_1) + \varphi(i)\varphi(z_2) = z_1 - i z_2$, så at φ er afbildningen $z \mapsto \overline{z}$.

For et vilkårligt komplekst tal $z = z_1 + i z_2$ har vi $z\overline{z} = (z_1 + i z_2)(z_1 - i z_2) = z_1^2 + z_2^2$. Det ikke negative reelle tal $|z| = \sqrt{z\overline{z}} = \sqrt{z_1^2 + z_2^2}$ kaldes den <u>numeriske værdi</u> eller <u>modulus</u> af z. Man bemærker, at for $z \neq 0$ er $\frac{1}{z} = \frac{\overline{z}}{|z|^2}$.

Indfører man i planen sædvanlige retvinklede koordinater, bliver $\mathbb{R}^2$ og dermed $\mathbb{C}$ afbildet bijektivt på planen, idet $z = z_1 + i z_2$ afbildes i punktet (z_1, z_2). Planen kaldes i denne forbindelse <u>den komplekse talplan</u>, og z_1-aksen og z_2-aksen den reelle og den imaginære akse. Et komplekst tal bliver repræsenteret ved et punkt z i planen, eller om man vil ved vektoren $\overrightarrow{0z}$. Konjugering svarer til spejling i den reelle akse. Den numeriske værdi $|z|$ er længden af vektoren $\overrightarrow{0z}$. Additionen af komplekse tal

svarer til vektoraddition. Man ser derfor straks, at der for vilkårlige komplekse tal z og w gælder

$$|z+w| \leqslant |z| + |w|.$$



Benytter man polære koordinater, fås fremstillingen

$$z = |z|\cos\theta + i|z|\sin\theta = |z|(\cos\theta + i\sin\theta).$$

Vinklen θ kaldes et <u>argument</u> af z. For $z=0$ kan θ vælges vilkårligt. For $z\neq 0$ er θ kun bestemt modulo 2π, d.v.s. hvis θ er et argument er samtlige argumenter bestemt ved $\theta + p2\pi$, $p \in \mathbb{Z}$. Mængden af argumenter for et komplekst tal z betegnes $\arg z$; dog benyttes $\arg z$ også som betegnelse for enhver af værdierne. For $z\neq 0$ findes netop ét argument i halvåbent interval $[-\pi, \pi[$; det kaldes <u>hovedværdien</u> og betegnes $\operatorname{Arg} z$. (Man ser også ofte hovedværdien defineret som det argument, der hører til intervallet $[0, 2\pi[$.)
For $z\neq 0$ kaldes tallet $\frac{z}{|z|} = \cos\theta + i\sin\theta$ <u>fortegnet</u> af z. Man ser, at de komplekse fortegn udgør enhedscirklen $U = \{z \mid |z| = 1\}$. Ved hjælp af fremstillingen i polære koordinater udtrykkes multiplikationen på simpel måde. Hvis

$$z = |z|(\cos\theta + i\sin\theta), \qquad w = |w|(\cos\varphi + i\sin\varphi),$$

finder vi nemlig

$$\begin{aligned} zw &= |z||w|\left[\cos\theta\cos\varphi - \sin\theta\sin\varphi + i(\cos\theta\sin\varphi + \sin\theta\cos\varphi)\right] \\ &= |z||w|\left[\cos(\theta+\varphi) + i\sin(\theta+\varphi)\right]. \end{aligned}$$

Vi har altså

$$|zw| = |z||w| \quad \text{og} \quad \arg zw = \arg z + \arg w,$$

hvor meningen med den sidste ligning er, at summen af et vilkårligt argument for z og et vilkårligt argument for w er et argument for zw. [Den første ligning følger naturligvis også direkte af at $|zw| = \sqrt{zw\,\overline{zw}} = \sqrt{z\bar{z}}\sqrt{w\bar{w}}$.] Specielt har vi for $z \neq 0$

$$\frac{1}{z} = \frac{1}{|z|}(\cos\theta - i\sin\theta), \text{ d.v.s. } \left|\frac{1}{z}\right| = \frac{1}{|z|} \text{ og } \arg\frac{1}{z} = -\arg z.$$

Kvaternionerne. På baggrund af den overordentlige betydning af de komplekse tal var det nærliggende at spørge, om det er muligt på tilsvarende måde at organisere $\mathbb{R}^n$ for vilkårligt n som et legeme. W. R. Hamilton opdagede (1843), at dette kan gøres for $n=4$, når man giver afkald på multiplikationens kommutativitet. De Hamiltonske kvaternioner har fundet interessante anvendelser inden for geometri og fysik. Det er senere bevist (G. Frobenius 1878), at der udover de reelle tal ($n=1$), de komplekse tal ($n=2$) og kvaternionerne ($n=4$) ikke findes legemer af den omhandlede art.

Som heuristisk udgangspunkt for indførelsen af kvaternionerne kan man betragte symboler af formen

$$x_0 + x_1 i + x_2 j + x_3 k, \qquad x_0, x_1, x_2, x_3 \in \mathbb{R},$$

med tre "imaginære enheder" i, j, k. Et sådant udtryk kaldes en kvaternion med koordinaterne x_0, x_1, x_2, x_3. Addition af kvaternioner indføres nu naturligt som koordinatvis addition, d.v.s. ved

$$(x_0 + x_1 i + x_2 j + x_3 k) + (y_0 + y_1 i + y_2 j + y_3 k)$$
$$= (x_0 + y_0) + (x_1 + y_1) i + (x_2 + y_2) j + (x_3 + y_3) k.$$

Vil man også definere multiplikationen som formel

multiplikation, ser man (idet man naturligt vil forlange, at elementerne af $\mathbb{R}$ skal kommutere med i, j, k) at man får brug for at fastsætte en multiplikationstabel for i, j, k. Hamilton så, at man får et interessant resultat ved at benytte tabellen

	i	j	k
i	-1	k	$-j$
j	$-k$	-1	i
k	j	$-i$	-1

altså

$$\begin{aligned} i^2 = j^2 = k^2 &= -1 \\ jk = i &= -kj \\ ki = j &= -ik \\ ij = k &= -ji. \end{aligned}$$

Det svarer til, at man som produkt af to kvaternioner benytter

$$(x_0 + x_1 i + x_2 j + x_3 k) \cdot (y_0 + y_1 i + y_2 j + y_3 k) = z_0 + z_1 i + z_2 j + z_3 k,$$

hvor

$$\begin{cases} z_0 = x_0 y_0 - x_1 y_1 - x_2 y_2 - x_3 y_3 \\ z_1 = x_0 y_1 + x_1 y_0 + x_2 y_3 - x_3 y_2 \\ z_2 = x_0 y_2 - x_1 y_3 + x_2 y_0 + x_3 y_1 \\ z_3 = x_0 y_3 + x_1 y_2 - x_2 y_1 + x_3 y_0. \end{cases}$$

Denne heuristiske betragtning erstattes nu med en eksakt indførelse, idet man går frem på samme måde som ovenfor ved indførelsen af de komplekse tal. Vi indfører i $\mathbb{R}^4$ to kompositioner ved fastsættelserne

$$(x_0, x_1, x_2, x_3) + (y_0, y_1, y_2, y_3) = (x_0 + y_0, x_1 + y_1, x_2 + y_2, x_3 + y_3)$$

$$(x_0, x_1, x_2, x_3) \cdot (y_0, y_1, y_2, y_3) = (z_0, z_1, z_2, z_3),$$

hvor z_0, z_1, z_2, z_3 er defineret ved ovenstående udtryk. Da er $(\mathbb{R}^4, +)$ åbenbart en kommutativ gruppe. Nulelementet er $(0,0,0,0)$, og det modsatte element til elementet (x_0, x_1, x_2, x_3) er $(-x_0, -x_1, -x_2, -x_3)$. Man efterregner umiddelbart, at multiplikationen er associativ og at den er distributiv med hensyn til additionen. Altså er $(\mathbb{R}^4, +, \cdot)$ en ring. Man

ser, at elementet $(1,0,0,0)$ er neutralt overfor multiplikationen, altså et element i ringen. For at vise, at ringen er et legeme, mangler vi blot at vise, at ethvert element (a_0,a_1,a_2,a_3) har et reciprokt. Ved udregning ser man, at elementet

$$(x_0,x_1,x_2,x_3)=\left(\frac{a_0}{a_0^2+a_1^2+a_2^2+a_3^2},\frac{-a_1}{a_0^2+a_1^2+a_2^2+a_3^2},\frac{-a_2}{a_0^2+a_1^2+a_2^2+a_3^2},\frac{-a_3}{a_0^2+a_1^2+a_2^2+a_3^2}\right)$$

er reciprokt til (a_0,a_1,a_2,a_3), idet både $(a_0,a_1,a_2,a_3)(x_0,x_1,x_2,x_3)$ og $(x_0,x_1,x_2,x_3)(a_0,a_1,a_2,a_3)$ er $(1,0,0,0)$.

Man ser, at delmængden $\hat{\mathbb{R}}=\{(x,0,0,0)\mid x\in\mathbb{R}\}$ er stabil overfor kompositionerne, og at afbildningen $x\mapsto(x,0,0,0)$ af $\mathbb{R}$ på $\hat{\mathbb{R}}$ er en isomorfi, så at $(\hat{\mathbb{R}},+,\cdot)$ er et eksemplar af de reelle tals legeme. Man ser endvidere, at ethvert element af $\hat{\mathbb{R}}$ kommuterer med ethvert element af $\mathbb{R}^4$. Sættes nu

$$i=(0,1,0,0)$$
$$j=(0,0,1,0)$$
$$k=(0,0,0,1),$$

har vi dels

$$i^2=j^2=k^2=-(1,0,0,0)$$
$$jk=i=-kj$$
$$ki=j=-ik$$
$$ij=k=-ji,$$

dels er for ethvert element (x_0,x_1,x_2,x_3)

$$(x_0,x_1,x_2,x_3)$$
$$=(x_0,0,0,0)+(x_1,0,0,0)i+(x_2,0,0,0)j+(x_3,0,0,0)k.$$

Hvis omvendt $(x_0,x_1,x_2,x_3)=(y_0,0,0,0)+(y_1,0,0,0)i+(y_2,0,0,0)j+(y_3,0,0,0)k$, er altså $x_0=y_0, x_1=y_1, x_2=y_2, x_3=y_3$.

Hermed har vi fundet:

Der findes et ikke kommutativt legeme $(\mathbb{K},+,\cdot)$, der indeholder et eksemplar $(\mathbb{R},+,\cdot)$ af de reelle tals legeme, hvis elementer kommuterer med alle elementer af $\mathbb{K}$, og

tre elementer i, j, k, der multipliceres efter tabellen ovenfor, således at ethvert $x \in \mathbb{K}$ har en og kun een fremstilling af formen

$$x = x_0 + x_1 i + x_2 j + x_3 k, \qquad x_0, x_1, x_2, x_3 \in \mathbb{R}.$$

Ethvert sådant legeme er åbenbart isomorft med det konstruerede legeme $(\mathbb{R}^4, +, \cdot)$; et sådant legeme kaldes et eksemplar af kvaternionlegemet og dets elementer kaldes kvaternioner.

Det reelle tal x_0 kaldes realdelen eller skalardelen og $x_1 i + x_2 j + x_3 k$ vektordelen af kvaternionen $x = x_0 + x_1 i + x_2 j + x_3 k$, og $\overline{x} = x_0 - x_1 i - x_2 j - x_3 k$ kaldes den konjugerede kvaternion til x. Man har $x\overline{x} = x_0^2 + x_1^2 + x_2^2 + x_3^2$. Det ikke-negative reelle tal $|x| = \sqrt{x\overline{x}} = \sqrt{x_0^2 + x_1^2 + x_2^2 + x_3^2}$ kaldes den numeriske værdi af kvaternionen x.

Opgaver. 1. Vis, at et legeme, der indeholder et eksemplar af $\mathbb{R}$, hvis elementer kommuterer med alle legemets elementer, som indeholder tre elementer i, j, k, for hvilke

$$i^2 = j^2 = k^2 = ijk = -1,$$

og i hvilket ethvert element x har en og kun een fremstilling

$$x = x_0 + x_1 i + x_2 j + x_3 k, \qquad x_0, x_1, x_2, x_3 \in \mathbb{R},$$

er et eksemplar af kvaternionlegemet.

2. Find alle løsninger i $\mathbb{K}$ til ligningen $x^2 = -1$.