Matematik 221, 1985

Anders Thorup

Algebra

Håndskrevne noter

NAIV MÆNGDELÆRE

1. Zermelo–Fraenkel's axiomer
2. Ækvipotens
3. Zorn's Lemma
4. Velordning
5. Ækvivalens af eksistens-axiomerne
6. Den transfinite talrække
7. Ordinaltal og kardinaltal. Uendelighedsaxiomet

MODULER

1. Modulbegrebet
2. Undermodul. Kvotientmodul
3. Noether's isomorfisætninger
4. Direkte sum af moduler. Basis
5. Simple moduler
6. Moduler af endelig længde

MODULER OVER KOMMUTATIVE RINGE. DETERMINANT (Det)

1. Moduler over kommutative ringe
2. Alternerende n-lineære afbildninger. Determinant
3. Determinantsætninger
4. Udviklinger. Cramer's formel
5. Rang og dimension

MODULER OVER HOVEDIDEALOMRÅDER (PID)

1. Frie moduler. Rang og dimension
2. Torsionsfri moduler
3. Matricer over hovedidealområder
4. Basissætningen
5. Endomorfier i vektorrum

OPGAVER (mærket side 1–5, 32–40)

NAIV MÆNGDELÆRE

1. Zermelo-Fraenkel's axiomer. 1.0: Indledning. 1.1: Identitetsprincippet. 1.2: Specifikationsaxiomet. Russell's paradox. 1.3: Par-axiomet. 1.4: Sum-axiomet. 1.5: Potens-axiomet. 1.6: Udskiftnings-axiomet. 1.7: Eksistens-axiomet. Den tomme mængde. 1.8: Uendeligheds-axiomet. 1.9: De grundlæggende begreber. 1.10: Om mængdelære. 1.11: Udvalgs-axiomet.

2. Ækvipotens. 2.1: Lemma. 2.2: Ækvipotens. 2.3: Bernstein's ækvivalenssætning. 2.4: Cantor's sætning. 2.5-7: Tællelige mængder. 2.8-9: Kontinuets mægtighed. 2.10: $A \times A \approx A$, $A \times \mathbb{N} \approx A$.

3. Zorn's lemma. 3.1: Induktiv ordning. 3.2: Zorn's lemma. 3.3-4: Udvalgs-axiomet medfører Zorn's lemma.

4. Velordning. 4.1: Afsnit. 4.2-4: Velordnede mængder. 4.5: Velordningssætning. 4.6: Induktionssætningen. 4.7: Rekursionssætning. 4.8: Sammenligningssætninger. 4.9: Den mindste ikke-tallelige velordnede mængde. 4.10: $X \approx Y \times \mathbb{N}$, $X \times \mathbb{N} \approx \mathbb{N}$.

5. Ækvivalens af eksistensaxiomerne. 5.1: Udvalgs-axiomet. Zorn's lemma. Velordningssætningen. Maksimalitetsprincippet. Sammenligningssætningen. 5.2-5: Zorn's lemma og de andre.

6. Den transfinite talrække. 6.1-4: Endelige og transfinite ordinaltal. 6.5: Ordinaltallet for en velordnet mængde. 6.6-8: Kardinaltal. 6.9-11: Aritmetik. 6.12: $\alpha+\beta = \alpha\cdot\beta = \max\{\alpha,\beta\}$.

7. Ordinaltal og kardinaltal. Uendelighedsaxiomet. 7.0: Indledning. 7.1-3: Ordinaltal. 7.4: Induktionsprincip. 7.5-13: Sammenligning af ordinaltal. 7.14-17: Kardinaltal. 7.18-21: Naturlige tal. 7.22: Endelige mængder. 7.23: Skuffeprincip. 7.24-26: Uendelighedsaxiomet. 7.27: Numerable valg.

NAIV MÆNGDELÆRE

1. Zermelo - Fraenkel's axiomer.

1.0 Hvad er en mængde? Vi har alle en intuitiv forenmelse af hvad en mængde er. Det er en samling af ting, en klasse af objekter, en gruppe af individer, et aggregat af bestanddele, ... I disse beskrivelser er indeholdt, at vi kan tale om, at noget er indlemmet i samlingen, er med i klassen, tilhører gruppen, er en del af aggregatet, ... I mængdebegrebet ligger altså en afgrænsning af hvad der er element i en given mængde, og hvad der ikke er. Men hvad er egentlig definitionen på en mængde? På den ene side har vi en række samlinger, som vi med sikkerhed synes er mængder. Hvem vil f.eks. ikke som mængde acceptere samlingen af de fem spørgsmålstegn herunder

? ? ? ? ? ?

På den anden side har vi visse samlinger, som vi nødig vil acceptere som mængder, f.eks. samlingen af alle mængder, idet acceptan af sådanne samlinger som mængder fører til paradoxer.

Spørgsmålet "Hvad er en mængde?" er således ikke uinteressant. Overraskende nok er der endnu ingen, der har kunnet besvare det tilfredsstillende!

1.1. Lad os antage, at vi har mødt en matematiker, som hævder at have besvaret spørgsmålet, og dermed

har en såkaldt model for mængdelæren. Inden vi hører svaret, gør vi opmærksom på, at svaret skal opfylde en række krav, før vi synes at det er tilfredsstillende.

Først og fremmest vil vi kræve, at når A er en mængde, så er det et veldefineret udsagn at sige, at "a er element i A". Er dette opfyldt, skriver vi

$$a \in A,$$

og vi siger også, at a tilhører A eller at A har a som element eller at A omfatter elementet a. Videre kræver vi, at der gælder det såkaldte IDENTITETSPRINCIP. To mængder er identiske, hvis og kun hvis de har de samme elementer.

Er A og B mængder (i denne model), vil vi sige, at A er en delmængde af B eller at A er indeholdt i B, og vi skriver

$$A \subseteq B \qquad (\text{eller } B \supseteq A),$$

hvis ethvert element i A er element i B. Identitetsprincippet udsiger altså, at der gælder

$$(A \subseteq B \wedge B \subseteq A) \Rightarrow A = B.$$

A er en ægte delmængde ($A \subset B$), hvis $A \subseteq B$ og $A \neq B$.

De øvrige krav formuleres nedenfor i form af såkaldte axiomer.

1.2. SPECIFIKATIONS-AXIOMET. Hvis $p(x)$ er et udsagn med én fri variabel x [et såkaldt prædikat] og A er en mængde, så eksisterer der en mængde, hvis elementer netop er de elementer $a \in A$, for hvilke $p(a)$ gælder.

Af identitetsprincippet følger, at der er netop én mængde med disse egenskaber. Vi betegner den

$$\{x \in A \mid p(x)\}.$$

Det er øjensynlig en delmængde af A.

BEMÆRKNING 1. Vi kræver ikke, at der til hvert prædikat $p(x)$ findes en mængde, der som elementer har ethvert x for hvilket $p(x)$ gælder. Findes der imidlertid for et givet prædikat $p(x)$ en sådan mængde E, ser vi at mængden

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

som elementer har præcis de x, for hvilke $p(x)$ gælder. I så fald siger vi, at prædikatet $p(x)$ er mængdebestemmende, og mængden ovenfor betegner vi

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

Vi siger, at den er specificeret ved prædikatet $p(x)$.

BEMÆRKNING 2. Vi kræver ikke, at elementerne i en mængde ikke selv er mængder. Tværtimod spiller som bekendt mængder af mængder en betydelig rolle i matematik (og det er faktisk enklest og ikke nogen indskrænkning at antage, at hvert element i en mængde selv er en mængde).

Vi kan sagtens forestille os mængder A og B, så at vi har både $B \subseteq A$ og $B \in A$. Specielt kræver vi ikke, at en mængde ikke må være element i sig selv [men vi har selvfølgelig svært ved at forestille os en mængde, der er element i sig selv].

Er A en given mængde, kan vi betragte mængden

$$B = \{x \in A \mid x \notin x\}.$$

Mængden B er en delmængde af A, men B er ikke element i A, thi var $B \in A$ ville vi få modstriden

$$B \in B \iff B \notin B.$$

Heraf fås: For hver mængde A findes en mængde B (endda en delmængde af A), som ikke er element i A. Specielt fås:

RUSSELL'S PARADOX. Ingen mængde kan have

alle mængder som elementer.
Anderledes udtrykt: Prædikatet "x er en mængde" er ikke mængdebestemmende.

1.3. PAR-AXIOMET. Til to mængder A og B eksisterer altid en mængde, der som elementer har både A og B.

Af Specifikationsaxiomet følger så, at der findes en mængde, hvis elementer netop er A og B. Vi betegner den $\{A,B\}$ og kalder den det uordnede par bestående af A og B. Den specificeres ved

$$\{A,B\} = \{x \mid x=A \vee x=B\}.$$

Hvis $A=B$, skriver vi blot $\{A\}$ for $\{A,A\}$, altså

$$\{A\} = \{x \mid x=A\}.$$

1.4. SUM-AXIOMET. Til hver mængde $\mathcal{C}$ af mængder eksisterer en mængde, der som elementer har ethvert element, der er element i en af de mængder, der tilhører $\mathcal{C}$.

Af specifikationsaxiomet følger så, at der findes en mængde, hvis elementer netop er de elementer, der tilhører en af mængderne i $\mathcal{C}$. Vi kalder den foreningsmængden af mængderne i $\mathcal{C}$, og vi betegner den $\cup\mathcal{C}$ eller $\cup_{X\in\mathcal{C}} X$. Den specificeres ved

$$\cup\mathcal{C} = \{x \mid \exists X : X\in\mathcal{C} \wedge x\in X\}.$$

Er $\mathcal{C}=\{A,B\}$ skriver vi også $A\cup B$ for foreningsmængden $\cup\{A,B\}$.

BEMÆRKNING 1. Gentagen anvendelse af Sumaxiomet og Paraxiomet tillader til endelig mange givne

mængder $A_1, \ldots, A_n$ at definere mængden $\{A_1, \cdots, A_n\}$, hvis elementer netop er de givne endelig mange mængder.

BEMÆRKNING 2. Vi har ikke behov for et axiom for at definere fællesmængde: Hvis $\mathcal{C}$ er en mængde af mængder og der findes elementer i $\mathcal{C}$, specificeres fællesmængden $\cap\mathcal{C}$ ved:

$$\cap\mathcal{C} = \{x \mid \forall X : X \in \mathcal{C} \Rightarrow x \in X\}.$$

[Hvorfor er forudsætningen om at der findes elementer i $\mathcal{C}$ nødvendig?]. Er $\mathcal{C} = \{A, B\}$, skrives $A \cap B := \cap\{A, B\}$. Er intet x element heri, kaldes A og B disjunkte. Overskudsmængde $A \setminus B$ specificeres ved

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

1.5. POTENSAXIOMET. Til hver mængde A eksisterer der en mængde, der som elementer har enhver delmængde af A.

Af specifikationsaksiomet følger så, at der findes en mængde, hvis elementer netop er delmængderne af A. Vi kalder den A's potensmængde ("mængden af delmængder"), og vi betegner den $\mathcal{P}(A)$. Den specificeres ved

$$\mathcal{P}(A) = \{x \mid x \subseteq A\}.$$

1.6. UDSKIFTNINGSAXIOMET. Hvis $p(x, y)$ er et udsagn med to frie variable x, y og A er en mængde, således at der for hvert element a i A findes en mængde, der som elementer har ethvert y for hvilket $p(a, y)$ gælder, så eksisterer en mængde, der som elementer har ethvert y for hvilket der eksisterer et element a i A så at $p(a, y)$ gælder.

Anderledes udtrykt: Hvis der for hvert element a i mængden A gælder, at prædikatet $p(a, y)$ er mængdebestemmende, så er også prædikatet "$\exists a : a \in A \wedge p(a, y)$" mængdebestemmende.

1.7. De foregående axiomer har udtalt sig om, at der under visse forudsætninger (om visse mængder) eksisterer nye mængder (med visse ønskede egenskaber). Vigtigt er derfor også

EKSISTENS-AXIOMET. Der eksisterer en mængde.

Heraf følger, at predikatet "$x \neq x$" er mængdebestemmende. Den specificerede mængde kaldes den tomme mængde og betegnes $\emptyset$. Den er karakteriseret ved at intet x er element i $\emptyset$.

Ud fra den tomme mængde $\emptyset$ kan vi indse eksistensen af yderligere en række mængder. F.eks. er $\{\emptyset\}$ en mængde (jfr. 1.3), og den har et element (nemlig $\emptyset$) og den er derfor forskellig fra $\emptyset$, som ingen elementer har. Tilsvarende ser vi at mængden $\{\emptyset, \{\emptyset\}\}$ er forskellig fra både $\emptyset$ og $\{\emptyset\}$. Bemærk, at vi har

$$\emptyset \in \{\emptyset\} \quad \text{og} \quad \emptyset \subseteq \{\emptyset\}.$$

BEMÆRKNING. Af Russell's Paradox 1.2 og Bemærkning 1.4.1 følger, at der må være uendelig mange mængder.

1.8. Af de foregående axiomer følger som nævnt, at der er uendelig mange mængder. Men det sikrer ikke, at der eksisterer en mængde med uendelig mange elementer. For at sikre en sådan eksistens (i en præcis betydning) kræver vi

UENDELIGHEDS-AXIOMET. Der eksisterer en ikke-tom mængde $\mathcal{N}$ af mængder, således at der for hvert $a \in \mathcal{N}$ findes et element $b \in \mathcal{N}$ med $a \subset b$.

1.9 Ovenstående er de 8 krav, vi stiller til et svar på spørgsmålet "Hvad er en mængde?". Efter at have formuleret disse axiomer opdager vi imidlertid, at vi slet ikke behøver at kende svaret. Alene ud-fra axiomerne kan vi udlede de begreber og sætninger, vi kender fra den elementære mængdelære. Uden at gå i detaljer nævner vi:

(1) Til to mængder A og B findes en mængde $A \times B$, kaldet det <u>cartesiske produkt</u>, hvis elementer er ordnede par (a,b), $a \in A$, $b \in B$.

(2) En <u>relation</u> R er en mængde, der er delmængde af et cartesisk produkt $A \times B$ for passende mængder A og B. Relationens <u>domæne</u> er mængden

$$\operatorname{dom} R := \{ x \mid \exists y : (y,x) \in R \}$$

og dens <u>billede</u> (eller værdimængde) er

$$\operatorname{ran} R := \{ y \mid \exists x : (y,x) \in R \}$$

[ran for "range"].

For hver relation R er også den <u>inverse</u>

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

en relation, og er S endnu en relation, er også den <u>sammensatte</u>

$$S \circ R := \{ (x,z) \mid \exists y : (x,y) \in S \wedge (y,z) \in R \}$$

en relation.

(3) En <u>afbildning</u> er en relation f, som opfylder:

$$\forall x,y,z : (y,x) \in f \wedge (z,x) \in f \Rightarrow y = z.$$

For hvert element $x \in \operatorname{dom} f$ findes altså netop ét element y, så at $(y,x) \in f$. Det kaldes <u>f's værdi i x</u> og betegnes $y = f(x)$.

(4) En afbildning f siges at være en <u>afbildning fra A til B</u>, og vi skriver

$$f : A \to B,$$

hvis $\mathrm{dom} f = A$ og $\mathrm{ran} f \subseteq B$. Mængden af afbildninger $f: A \to B$ betegnes B^A [Hvorfor er det en mængde?]. For hver mængde A er den <u>identiske afbildning</u> Id_A eller 1_A bestemt ved

$$Id_A = \{ (x,y) \in A \times A \mid x = y \}$$

Er $A \subseteq B$ en delmængde, kan den identiske afbildning Id_A opfattes som en afbildning (kaldet <u>inklusions-afbildningen</u>) $: A \to B$.

(5) En afbildning $f: A \to B$ er <u>injektiv</u>, hvis der for alle elementer a_1 og a_2 i A gælder

$$f(a_1) = f(a_2) \Rightarrow a_1 = a_2,$$

den er <u>surjektiv</u>, hvis der for alle elementer b i B gælder

$$\exists a : a \in A \wedge f(a) = b$$

og den er <u>bijektiv</u>, hvis den er både injektiv er surjektiv. I så fald er f^{-1} en afbildning $: B \to A$.

(6) Er $f: A \to B$ en afbildning, defineres for hver delmængde $A' \subseteq A$ <u>billedet af A'</u> ved

$$f(A') := \{ y \in B \mid \exists x : x \in A' \wedge f(x) = y \}.$$

Billedet betegnes også

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

For hver delmængde $B' \subseteq B$ defineres <u>urbilledet</u> eller <u>originalmængden</u> for B' ved

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

(Er $B' = \{b\}$, hvor $b \in B$, skrives ofte $f^{-1}(b)$ for $f^{-1}(\{b\})$.)

(7) Er $f: A \to B$ en afbildning, defineres for hver delmængde $A' \subseteq A$ <u>restriktionen til A'</u> ved

$$f|A' = \{ (x,y) \mid x \in A' \wedge y = f(x) \}.$$

(8) Er $f: A \to B$ og $g: B \to C$ afbildninger, så er også den

sammensatte relation en afbildning

$$g \circ f : A \to C. \quad (\text{med } g \circ f(x) = g(f(x)),\ x \in A).$$

(9). En afbildning $F : I \to \mathcal{C}$, hvor $\mathcal{C}$ er en mængde af mængder, kaldes også en <u>familie af mængder</u>, og mængden I kaldes familiens <u>indexmængde</u>. Afbildningen F's værdi i et element $i \in I$ betegnes ofte F_i, og vi skriver $F = (F_i)_{i \in I}$. Afbildningens billede, altså ran F, er mængden

$$\{ F_i \mid i \in I \}$$

og denne mængdes foreningsmængde (jfr. sumaksiomet) betegnes

$$\bigcup_{i \in I} F_i \quad \text{eller} \quad \bigcup \{ F_i \mid i \in I \}.$$

Er U denne foreningsmængde, defineres <u>produktmængden</u> af familien F ved

$$\underset{i \in I}{X} F_i := \{ x \mid x \in U^I \wedge \forall i \in I : x(i) \in F_i \}$$

For hvert index j ($j : j \in I$) er <u>den j-te projektion</u> defineret ved

$$pr_j := \{ (x, y) \mid x \in \underset{i \in I}{X} F_i \wedge y = x(i) \}$$

Det er en afbildning

$$pr_j : \underset{i \in I}{X} F_i \to F_j$$

(10) Endelig indses v.hj.a Uendelighedsaxiomet, at der eksisterer en mængde $\mathbb{N}$, som opfylder de krav vi stiller til mængden af naturlige tal, jfr. Talsystemets Opbygning. Og så kan vi jo opfatte vores sædvanlige talsystem, som noget der findes i denne teori.

Bemærk, at vi for afbildninger med domæne $\mathbb{N}$ bruger sædvanlige notationer: $f : \mathbb{N} \to A$ skrives ofte $f = (f_1, f_2, \dots)$, og for familier $F : \mathbb{N} \to \mathcal{C}$ skrives

$$\{F_1, F_2, \dots\} := \{ F_i \mid i \in \mathbb{N} \},\ F_1 \cup F_2 \cup \dots := \bigcup_{i \in \mathbb{N}} F_i \text{ og}$$

$$F_1 \times F_2 \times \dots := \underset{i \in \mathbb{N}}{X} F_i .$$

1.10. Mængdelære kan datere sin fødsel til 1874, hvor Georg Cantor som den første betragtede samlinger af reelle tal, som ikke apriori var "angivet ved en opskrift". I sidste del af 1800-tallet udvikledes mængdelære ud fra det synspunkt, at den var en del af logikken, at dens principper kan udledes af de logiske principper. Dette synspunkt blev anfægtet, da Bertrand Russell formulerede sit paradox i 1903.

Den første axiomatiske opbygning af mængdelære skyldes Ernst Zermelo i 1908. At Zermelo's axiomer yderligere burde suppleres en lille smule blev klarlagt i årene derefter, af bl.a. Abraham Fraenkel i 1922, og de axiomer vi har skitseret er essentielt Zermelo-Fraenkel's axiomer (ZF-axiomerne). Det skal dog understreges, at den stringente opbygning af en sådan axiomatisk mængdelære kræver en nøjere præcision af hvad (matematisk) logik er.

1.11. Udover ZF-axiomerne kan man stille yderligere krav: Er A en mængde, kan man for hver ikke-tom delmængde $X \subseteq A$ vælge et element $x \in A$, så at

$$x \in X.$$

Men axiomerne sikrer ikke, at der eksisterer en afbildning, der til hver ikke-tom delmængde $X \subseteq A$ tilordner et sådant udvalgt element $x \in X$. En sådan afbildning kaldes en udvalgsfunktion på A. Mere præcist er en udvalgsfunktion på A en afbildning

$$u : \mathcal{P}(A) \setminus \{\emptyset\} \longrightarrow A,$$

således at der for hvert element $X \in \mathcal{P}(A) \setminus \{\emptyset\}$ (dvs for hver ikke-tom delmængde $X \subseteq A$) gælder

$$u(X) \in X.$$

UDVALGS-AXIOMET. Til enhver mængde A eksisterer der en udvalgsfunktion på A.

Som nævnt er der endnu ikke fundet en "definition af mængder", som opfylder ZF-axiomerne. Man ved ikke engang om axiomsystemet er konsistent (inkonsistens ville betyde, at der findes sætninger, som ved brug af axiomerne kan både bevises og modbevises). Derimod er det vist af Kurt Gödel i 1938, at der findes sætninger, "formuleret inden for denne teori", som hverken kan bevises eller modbevises ved brug af axiomerne.

Samme år viste Gödel, at hvis ZF-systemet er konsistent, så fås også et konsistent system ved til ZF-axiomerne at tilføje udvalgsaksiomet.

I 1963 viste Paul Cohen, at udvalgsaxiomet ikke kan udledes af ZF-axiomerne, og man ved nu, at såfremt ZF-systemet er konsistent, så får man et konsistent system både hvis man til ZF-axiomerne tilføjer udvalgsaxiomet og hvis man til ZF-axiomerne tilføjer udvalgsaxiomets negation (f.eks. i den konkrete form: Der findes ingen udvalgsfunktion på $\mathbb{R}$).

I det følgende vælger vi at acceptere udvalgs-axiomet, men vi vil dog med et

(u) i margenen fremhæve de resultater, hvor udvalgsaxiomet - eller en form deraf - er en nødvendig forudsætning.

2. Ækvipotens.

2.1 LEMMA. Lad $f: A \to B$ være en afbildning. Da gælder:

(i) f er surjektiv, hvis og kun hvis der findes en afbildning $g: B \to A$, så at $f \circ g = 1_B$.

(ii) Hvis $A \neq \emptyset$, så er f injektiv, hvis og kun hvis der findes en afbildning $g: B \to A$, så at $g \circ f = 1_A$

(iii) f er bijektiv, hvis og kun hvis der findes en afbildning $g: B \to A$, så at $f \circ g = 1_B$ og $g \circ f = 1_A$.

I bekræftende fald er $g = f^{-1}$!

BEVIS. (i) "kun hvis": Her er det nødvendigt at bruge udvalgsaxiomet. Lad G være afbildningen bestemt ved

$$G(b) = f^{-1}(b), \quad b \in B.$$

Hver værdi er en delmængde $G(b) \subseteq A$, og da f er surjektiv, er $G(b) \neq \emptyset$ for alle $b \in B$. Følgelig er G en afbildning $: B \to \mathcal{P}(A) \setminus \{\emptyset\}$. Lad $u: \mathcal{P}(A) \setminus \{\emptyset\} \to A$ være en udvalgsfunktion på A. Da kan $g = u \circ G: B \to A$ bruges.

Resten af argumenterne for lemmaet er en øvelse i elementær mængdelære. Udvalgsaxiomet er ikke nødvendigt □

2.2. DEFINITION. To mængder A og B siges at have samme mægtighed eller at være ækvipotente, og vi skriver

$$A \approx B,$$

hvis der findes en bijektiv afbildning $: A \to B$.

Hvis der blot findes en injektiv afbildning $: A \to B$ skriver vi

$$A \lesssim B. \quad (\text{eller } B \gtrsim A.)$$

A siges at have mindre mægtighed end B, og vi skriver

$$A < B \quad (\text{eller } B > A),$$

hvis der findes en injektiv afbildning $: A \to B$ og ingen afbildninger $: A \to B$ er bijektive, altså

$$A < B \iff A \lesssim B \wedge A \not\approx B.$$

(11) BEMÆRKNING. Af Lemma 2.1 (i) og (ii) følger, når $A \neq \emptyset$, at der findes en injektiv afbildning $: A \to B$, hvis og kun hvis der findes en surjektiv afbildning $: B \to A$.

2.3. SÆTNING. For vilkårlige mængder A, B og C gælder:

(1) $A \approx A$

$A \approx B \Rightarrow B \approx A$

$A \approx B \wedge B \approx C \Rightarrow A \approx C$

(2) $A \lesssim A$

$A \lesssim B \wedge B \lesssim C \Rightarrow A \lesssim C$

$A \lesssim B \wedge B \lesssim A \Rightarrow A \approx B$

(3) $A \not< A$

$A < B \wedge B < C \Rightarrow A < C.$

BEVIS. Det sidste udsagn i (3) er en konsekvens af det sidste udsagn i (2) [Hvorfor?] (og de øvrige udsagn er trivielle). At det sidste udsagn i (2) er opfyldt, er indholdet i

BERNSTEINS ÆKVIVALENS-SÆTNING. Hvis der findes en injektiv afbildning $f: A \to B$ og en injektiv afbildning $g: B \to A$, så findes også en bijektiv afbildning $: A \to B$.

BEVIS. Der findes delmængder $Q \subseteq A$, som opfylder

$$(*)\quad Q \supseteq A \setminus g(B) \quad \text{og} \quad g \circ f(Q) \subseteq Q$$

f. eks. $Q = A$. Lad C være fællesmængden af alle sådanne delmængder, altså $C = \bigcap \{Q \mid Q \subseteq A \wedge Q \supseteq A \setminus g(B) \wedge g \circ f(Q) \subseteq Q\}$.

Det er klart, at også C har egenskaben $(*)$, så vi har

(0) $A \setminus C \subseteq g(B)$

(1) $g \circ f(C) \subseteq C$. Endvidere er

(2) $C \cap g(B) \subseteq gf(C)$,

thi $(A \setminus g(B)) \cup g \circ f(C)$ vil øjensynlig opfylde (*), og følgelig er $C \subseteq (A \setminus g(B)) \cup g \circ f(C)$, og dét er netop påstanden.

Da g er injektiv, følger det af (0), at der for hvert element $x \in A \setminus C$ findes netop et element $y \in B$, så at $g(y) = x$. Idet vi betegner dette element $y = g^{-1}(x)$ defineres $h: A \to B$ ved

$$h(x) := \begin{cases} f(x), & \text{hvis } x \in C \\ g^{-1}(x), & \text{hvis } x \in A \setminus C. \end{cases}$$

<u>h er injektiv</u>: Antag nemlig, at vi for $a_1, a_2 \in A$ har $h(a_1) = h(a_2)$. Hvis $\{a_1, a_2\} \subseteq C$, følger $a_1 = a_2$, da f er injektiv. Hvis $\{a_1, a_2\} \subseteq A \setminus C$, følger $a_1 = a_2$, da vi jo så har $a_i = g(h(a_i))$. Og var f.eks. $a_1 \in C$ og $a_2 \in A \setminus C$, så ville $a_2 = gh(a_2) = gh(a_1) = gf(a_1)$ være i modstrid med (1), da $a_2 \notin C$, $a_1 \in C$.
<u>h er surjektiv</u>: Lad $b \in B$. Hvis $g(b) \in A \setminus C$, så er $b = h(g(b))$, og hvis $g(b) \in C$, så er ifølge (2): $g(b) = gf(c)$, med $c \in C$. Da g er injektiv, følger $b = f(c) = h(c)$ ▨

(21) BEMÆRKNING. Vi beviser senere, at vilkårlige to mængder A og B altid kan sammenlignes, altså at der gælder: $A < B$ eller $A \approx B$ eller $B < A$.

2.4. CANTOR'S SÆTNING. (i) For enhver mængde A er

$$A < \mathcal{P}(A).$$

(ii) Lad $\underline{2}$ betegne mængden $\{0,1\}$. Da er for enhver mængde A

$$\mathcal{P}(A) \approx \underline{2}^A.$$

BEVIS. <u>(i)</u>: Afbildningen $x \mapsto \{x\}$, $x \in A$, er øjensynlig en injektiv afbildning $: A \to \mathcal{P}(A)$, så vi har $A \lesssim \mathcal{P}(A)$, og skal altså vise, at der ikke findes bijektive afbildninger $: A \to \mathcal{P}(A)$. Vi viser, at der ikke findes surjektive afbildninger $: A \to \mathcal{P}(A)$. Til en given afbildning $\psi: A \to \mathcal{P}(A)$ kan vi betragte mængden

$$Y := \{ x \in A \mid x \notin \psi(x) \},$$

som jo er en delmængde af A. Vi har altså $Y \in \mathcal{P}(A)$, men

$$Y \notin \psi(A),$$

thi var $Y = \psi(a)$, med $a \in A$, ville vi få modstriden

$$a \in Y \iff a \notin \psi(a) \iff a \notin Y.$$

(ii): Mængden $\underline{2}^A$ er mængden af alle afbildninger

$$\chi : A \to \{0,1\}.$$

Og disse afbildninger er netop de karakteristiske funktioner for delmængderne af A, idet den karakteristiske funktion for delmængden $B \subseteq A$ er afbildningen χ_B defineret ved

$$\chi_B(x) = \begin{cases} 1, & \text{hvis } x \in B \\ 0, & \text{hvis } x \in A \setminus B. \end{cases}$$

Ved $B \mapsto \chi_B$ defineres således en bijektiv afbildning: $\mathcal{P}(A) \to \underline{2}^A$, med $\chi \mapsto \chi^{-1}(1)$ som invers ▨

2.5. DEFINITION. Vi vil kalde en mængde A for <u>tællelig</u>, hvis A er tom eller der findes en surjektiv afbildning $\varphi : \mathbb{N} \to A$.

En afbildning $\varphi : \mathbb{N} \to A$ er en følge $\varphi = (\varphi_1, \varphi_2, \dots)$ med værdier i A. En ikke-tom mængde A er altså tællelig, hvis der findes en sådan følge, hvori ethvert element element fra A bliver "talt med", dvs optræder i følgen.

Af Bemærkning 2.2 fremgår umiddelbart, at en mængde A er tællelig, hvis og kun hvis $A \lesssim \mathbb{N}$ (Og hertil er det faktisk ikke nødvendigt at indrage udvalgsaxiomet). Det følger derfor af Cantor's sætning, at mængden $\mathcal{P}(\mathbb{N})$ <u>ikke</u> er tællelig.

En mængde A kaldes <u>numerabel</u>, hvis den er ækvipotent med $\mathbb{N}$, og <u>endelig</u>, hvis den er tom eller ækvipotent med et afsnit

$$\mathbb{N}_{\leq n} = \{1, \dots, n\}$$

af $\mathbb{N}$. Er det sidste tilfældet, er n elementantallet i A.

Vedrørende egenskaber ved endelige mængder henvises til kapitlet om Naturlige tal. Med blandt disse egenskaber regnes også følgende:

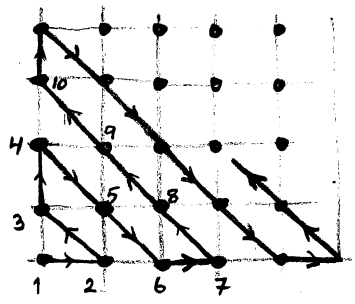
(1) En mængde A er tællelig, hvis og kun hvis den er endelig eller numerabel.

(U) (2) En mængde A er uendelig (dvs ikke endelig), hvis og kun hvis $\mathbb{N} \lesssim A$.

(U) (3) En mængde A er uendelig, hvis og kun hvis A er ækvipotent med en af sine ægte delmængder.

2.6. SÆTNING. Produktmængden $\mathbb{N}\times\mathbb{N}$ er numerabel. Med andre ord: $\mathbb{N} \sim \mathbb{N}\times\mathbb{N}$.

BEVIS. Nummerering af elementerne i $\mathbb{N}\times\mathbb{N}$ efter følgende skema:



giver en bijektiv afbildning: $\mathbb{N} \to \mathbb{N}\times\mathbb{N}$ □

(U) KOROLLAR 1. En tællelig forening af tællelige mængder er igen tællelig.

BEVIS. Lad $A = \bigcup_{i\in I} A_i$ være foreningsmængden, hvor altså indexmængden I er tællelig og hver mængde A_i er tællelig. Vi kan antage, at hver mængde A_i er $\neq \emptyset$ (ellers erstattes I med mængden $\{i \mid A_i \neq \emptyset\}$), og at $I \neq \emptyset$. Vælg en surjektiv afbildning $\varphi: \mathbb{N} \to I$ og for hvert $n \in \mathbb{N}$ en surjektiv afbildning $\psi_n: \mathbb{N} \to A_{\varphi(n)}$, da defineres ved

$$\Phi(n,m) = \psi_n(m)$$

en surjektiv afbildning : $\mathbb{N}\times\mathbb{N} \to A$. Brug nu sætningen □

KOROLLAR 2. Betragt for en mængde A de to mængder:
$\mathcal{E}(A)$ bestående af alle endelige sæt af elementer fra A
og
$\mathcal{F}(A)$ bestående af alle følger : $\mathbb{N} \to A$, der er konstante fra et vist trin.
Da gælder:
(1) $\mathcal{F}(A) \lesssim \mathcal{E}(A)$
(2) Hvis A har mindst 2 elementer, er $\mathcal{F}(A) \sim \mathcal{E}(A)$.
(3) Hvis A er $\neq \emptyset$ og tællelig, er $\mathcal{E}(A)$ numerabel.

BEVIS. Et n-sæt i A er en afbildning : $\{1,\cdots,n\} \to A$, hvor $n \in \mathbb{N}$, og mængden af n-sæt er produktet $A\times\cdots\times A = A^n$. Mængden $\mathcal{E}(A)$ af endelige sæt er altså foreningen
$$\mathcal{E}(A) = A \cup A^2 \cup A^3 \cup \cdots$$

(1): For hver følge $(y_1, y_2, \cdots)$ i $\mathcal{F}(A)$ findes $n \in \mathbb{N}$, så at $y_{n-1} \neq y_n = y_{n+1} = y_{n+2} = \cdots$, og $(y_1, y_2, \cdots) \longmapsto (y_1, \cdots, y_n)$ er en injektiv afbildning : $\mathcal{F}(A) \to \mathcal{E}(A)$.
(2): Vælg 2 forskellige elementer $a, b \in A$. Ved
$$(x_1, \cdots, x_m) \longmapsto \begin{cases} (x_1, \cdots, x_m, a, a, a, \cdots), & \text{hvis } x_m \neq a \\ (x_1, \cdots, x_m, b, b, b, \cdots), & \text{hvis } x_m = a \end{cases}$$
defineres en injektiv afbildning : $\mathcal{E}(A) \to \mathcal{F}(A)$. Brug nu Bernstein's ækvivalenssætning.
(3): Ved brug af sætningen følger først, at $A^n = A^{n-1}\times A$ er tællelig og dernæst, at $\mathcal{E}(A)$ er tællelig. Og åbenbart uendelig □

2.7. EKSEMPLER. (1) Mængderne $\mathbb{Z}$ og $\mathbb{Q}$ er numerable.
(2) Mængden $\mathbb{R}$ er ikke tællelig.
(3) Mængden af reelle algebraiske tal er numerabel.
(4) Der eksisterer et reelt tal, der er transcendent.
VINK. (1): Det er let at angive en bijektiv afbild-

ning : $\mathbb{N} \to \mathbb{Z}$. Og der findes som bekendt en surjektiv afbildning : $\mathbb{Z} \times \mathbb{N} \to \mathbb{Q}$.

(2): Dette skyldes Cantor (1873). Det er nok at vise, at enhedsintervallet $[0,1[\subseteq \mathbb{R}$ ikke er tælleligt, altså at en afbildning $f: \mathbb{N} \to [0,1[$ ikke kan være surjektiv. Elementerne $\xi \in [0,1[$ kan udvikles i decimalbrøker

$$\xi = 0, x_1 x_2 x_3 \cdots \qquad x_n \in \{0,1,\cdots,8,9\},$$

entydigt, hvis vi udelukker decimalbrøker, der "ender med luttet 9-taller". Til en given afbildning $f: \mathbb{N} \to [0,1[$ angiver vi et tal $\alpha \in [0,1[$, så at $\alpha \notin f(\mathbb{N})$, på følgende måde:

$$\alpha = 0, a_1 a_2 a_3 \cdots$$

hvor a_n er bestemt ved at $a_n = 0$ hvis det n-te ciffer i $f(n)$ er $\neq 0$, og $a_n = 1$, hvis det n-te ciffer i $f(n)$ er $= 0$. Da vil α's decimaler afvige fra $f(n)$'s for hvert n, og følgelig er $\alpha \notin \{f(1), f(2), \cdots\}$.

(3): Et reelt tal ξ kaldes algebraisk, hvis der findes et polynomium $p(X) = q_n X^n + \cdots + q_1 X + q_0$, med koefficienter $q_i \in \mathbb{Q}$, $i = 0, \cdots, n$ og $q_n \neq 0$, hvori ξ er rod (d: $p(\xi) = 0$). Mængden af "rationale" polynomier betegnes $\mathbb{Q}[X]$. Vi kan opfatte polynomier $q_0 + q_1 X + \cdots + q_n X^n \in \mathbb{Q}[X]$ som følger $(q_0, q_1, \cdots, q_n, 0, 0, \cdots)$ af rationale tal, der er $= 0$ fra et vist trin. Af korollar 2.6.2 følger, at mængden $\mathbb{Q}[X]$ er numerabel, og da hvert polynomium $p \neq 0$ i $\mathbb{Q}[X]$ kun kan have endelig mange rødder i $\mathbb{R}$ følger påstanden af Korollar 2.6.1.

(4): Et reelt tal ξ kaldes transcendent, hvis det ikke er algebraisk. Påstanden er derfor en konsekvens af (2) og (3).

2.8. DEFINITION. En mængde, der er ækvipotent med $\mathbb{R}$, siges også at have kontinuets mægtighed. Cantor formodede, at der gælder den såkaldte
KONTINUUMS HYPOTESE. Enhver mængde af reelle tal, som ikke er tællelig, har kontinuets mægtighed.

Under antagelse af at ZF-axiomerne udgør et konsistent system viste Gödel i 1938 at hypotesen ikke kunne modbevises, og Cohen har vist i 1963 at hypotesen heller ikke kan bevises, og at ZF-axiomerne + udvalgsaxiomet + kontinuumshypotesen udgør et konsistent system (stadig under forudsætning af ZF-systemets konsistens).

2.9. EKSEMPLER. Følgende mængder: (1) $\mathcal{P}(\mathbb{N})$ (2) $\underline{2}^{\mathbb{N}}$ (3) $\mathbb{N}^{\mathbb{N}}$ (4) $\mathbb{R}^n$, $n \in \mathbb{N}$ har alle kontinuets mægtighed. Vi har altså

$$\mathcal{P}(\mathbb{N}) \approx \underline{2}^{\mathbb{N}} \approx \mathbb{N}^{\mathbb{N}} \approx \mathbb{R}^n \approx \mathbb{R} \quad (n \in \mathbb{N}).$$

VINK. (1): $\mathcal{P}(\mathbb{N}) \approx \underline{2}^{\mathbb{N}}$ ifølge Cantors sætning 2.4 (ii).
(2): At $\underline{2}^{\mathbb{N}} \approx \mathbb{R}$ indses ved at udvikle reelle tal i dual-bøker.
(3): $\mathbb{N}^{\mathbb{N}} \approx \mathbb{R}$, thi da $\mathbb{N}^{\mathbb{N}} \subseteq \mathcal{P}(\mathbb{N} \times \mathbb{N})$, og $\mathbb{N} \times \mathbb{N} \approx \mathbb{N}$ har vi $\mathbb{N}^{\mathbb{N}} \lesssim \mathcal{P}(\mathbb{N}) \approx \underline{2}^{\mathbb{N}} \lesssim \mathbb{N}^{\mathbb{N}}$, hvoraf $\mathbb{N}^{\mathbb{N}} \approx \underline{2}^{\mathbb{N}} \approx \mathbb{R}$.
(4): For $n = 2$ har vi $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} \simeq \mathbb{N}^{\mathbb{N}} \times \mathbb{N}^{\mathbb{N}} \simeq (\mathbb{N} \times \mathbb{N})^{\mathbb{N}} \approx \mathbb{N}^{\mathbb{N}} \approx \mathbb{R}$. Det almindelige tilfælde følger heraf ved induktion.

(U) 2.10. BEMÆRKNING. Man kan vise, at der for hver uendelig mængde A gælder:

$$A \times A \approx A \quad (\text{hvoraf specielt: } A \times \mathbb{N} \approx A)$$

3. Zorn's lemma.

3.1. DEFINITION. En partielt ordnet mængde $(X,<)$ kaldes induktivt ordnet, hvis enhver totalt ordnet delmængde af X har en majorant i X.

BEMÆRKNING. Da den tomme mængde $\emptyset$ er en totalt ordnet delmængde af enhver partielt ordnet delmængde, følger det specielt, at en induktivt ordnet mængde er $\neq \emptyset$.

(U) 3.2. ZORN'S LEMMA. Lad $(X,<)$ være en partielt ordnet mængde. Hvis X er induktivt ordnet, så eksisterer der i X et maksimalt element.

BEMÆRKNING. Zorn's lemma er et eksistensudsagn: Det udtaler sig om, at der under visse forudsætninger eksisterer noget. Zorn's lemma (og beslægtede eksistensudsagn) spiller en stor rolle i mange grene af matematikken. Vi kan kun bevise Zorn's lemma ved at inddrage udvalgsaksiomet (og vi beviser senere, at Zorn's lemma er ækvivalent med udvalgsaksiomet).

3.3. Lad $(X,<)$ være en partielt ordnet mængde. I det følgende betegner vi for hver delmængde $A \subseteq X$ med M_A mængden af ægte majoranter for A, altså

$$M_A = \{ x \in X \mid \forall a \in A : a < x \}.$$

Lad u være en udvalgsfunktion på X. Ved en u-kæde i X forstås en delmængde $K \subseteq X$ som opfylder følgende 2 betingelser:

(u1): K er en totalt ordnet delmængde af X.

(u2): Hvis en delmængde $A \subseteq K$ opfylder, at $M_A \cap K \neq \emptyset$, så er

$$u(M_A) \in K$$

og

$$u(M_A) \leqslant k \text{ for alle } k \in M_A \cap K.$$

SÆTNING 1. Lad $K \subseteq X$ være en u-kæde, og antag, at $M_K \neq \emptyset$. Da er også $K \cup \{u(M_K)\}$ en u-kæde i X.
BEVIS. □.

LEMMA. Lad k og l være elementer i X, og antag, at der findes en u-kæde, som indeholder k og en u-kæde, som indeholder l, men ikke k. Da er $l < k$.
BEVIS. Ifølge antagelsen findes u-kæder $K, L \subseteq X$, så at $k \in K \setminus L$, $l \in L$. Betragt nu delmængden

$$A := \{a \in K \cap L \mid a < k\}.$$

Det er nok at vise, at $M_A \cap L = \emptyset$, thi så er specielt $l \notin M_A$, og da L er totalt ordnet og $L \supseteq A$, følger heraf, at der findes et $a \in A$, så at $l \leqslant a$, og så er $l \leqslant a < k$.

Idet beviset føres indirekte, antages, at $M_A \cap L \neq \emptyset$. Specielt er altså $M_A \neq \emptyset$, og vi kan betragte elementet

$$m := u(M_A).$$

Da L er en u-kæde, og $M_A \cap L \neq \emptyset$, ser vi, at

$$m \in L.$$

På den anden side er $A \subseteq K$ og $k \in M_A \cap K$. Da K er en u-kæde følger det, at

$$m \in K,$$

og at $m \leqslant k$. Nu var $m \in L$ og $k \notin L$, så $m \neq k$, og følgelig gælder der endda

$$m < k.$$

Men så er $m \in A$ i modstrid med at $m = u(M_A) \in M_A$ ⊠

SÆTNING 2. En vilkårlig foreningsmængde $K = \bigcup K_j$ af u-kæder K_j er selv en u-kæde.

BEVIS. Vi skal eftervise de to betingelser.

(u1): Lad $k, l \in K = \bigcup K_j$. Hvis intet K_j indeholder både k og l følger det af lemma'et, at vi har $l < k$ og $k < l$. Altså findes et K_j, som indeholder både k og l, og da K_j er totalt ordnet, gælder følgelig $k < l$ eller $l \leqslant k$.

(u2): Lad $A \subseteq K$ være en delmængde så at $M_A \cap K \neq \varnothing$, og sæt $k_0 := u(M_A)$. Vi skal vise, at

(1) $k_0 \in K$

og

(2) $k_0 \leqslant k$ for alle $k \in M_A \cap K$.

Lad k være et element i $M_A \cap K$, [sådanne findes, da $M_A \cap K \neq \varnothing$], og vælg en u-kæde K_j, så at $k \in K_j$.

Nu er

$$A \subseteq K_j ,$$

thi ellers fandtes $a \in A \subseteq K$, så $a \notin K_j$, og af lemmaet ville så følge $k < a$, i modstrid med at $k \in M_A$.

Da K_j er en u-kæde, og $k \in M_A \cap K_j$, slutter vi, at $k_0 = u(M_A) \in K_j \subseteq K$, hvoraf (1), og at $k_0 \leqslant k$, hvoraf (2), da k var et vilkårligt element i $M_A \cap K$ ▨

3.4. Vi kan nu bevise Zorn's lemma, eller mere præcist følgende:

SÆTNING. Udvalgsaksiomet medfører Zorn's lemma.

BEVIS. Lad $(X, <)$ være induktivt ordnet, og lad u være en udvalgsfunktion på X. Lad K være foreningsmængden af alle u-kæder. Da er K selv en u-kæde ifølge Sætning 3.3.2, og den omfatter alle u-kæder. Af Sætning 3.3.1 følger derfor, at $M_K = \varnothing$. Da K er totalt ordnet, og derfor har majoranter, må hver af disse være maksimalt element ▨

4. Velordning.

4.1. DEFINITION. Lad $(X,<)$ være en partielt ordnet mængde. Ved et *afsnit i X* forstås en delmængde $A \subseteq X$, som opfylder, at der for alle $a, x \in X$ gælder

$$x < a \wedge a \in A \Rightarrow x \in A.$$

Afsnittet $A \subseteq X$ kaldes *ægte*, hvis $A \subset X$.

For hvert element $b \in X$ er ögensynlig

$$X_{<b} := \{ x \in X \mid x < b \}$$

et ægte afsnit af X. Afsnit af X, der har denne form (med et passende $b \in X$) kaldes *elementbestemte*.

4.2. DEFINITION. En partielt ordnet mængde $(X,<)$ kaldes *velordnet* (og relationen $<$ kaldes en *velordning*), hvis enhver ikke-tom delmænde af X har et første element. Betingelsen er altså, at der i enhver ikke-tom delmængde $S \subseteq X$ findes et element $s_0 \in S$, så at der for alle elementer $s \in S$ gælder $s_0 \leq s$.

SÆTNING. En partielt ordnet mængde $(X,<)$ er velordnet, hvis og kun hvis X er totalt ordnet og hvert ægte afsnit af X er elementbestemt.

BEVIS. "hvis": Lad $S \subseteq X$ være en ikke-tom delmængde, og lad A være mængden af ægte minoranter for S, dvs

$$A = \{ a \in X \mid \forall s \in S : a < s \}.$$

Det er klart, at A er et afsnit i X, og da $S \neq \emptyset$ er A et ægte afsnit i X og dermed af formen

$$A = X_{<b},$$

med et passende $b \in X$.

Nu gælder

(*) $b \leq s$ for alle $s \in S$,

thi da X er totalt ordnet ville der i modsat fald findes et element $s \in S$, så at $s < b$, og så ville $s \in X_{<b} = A$ være en modstrid. Endvidere er

$b \in S$,

thi ellers ville der i (*) gælde $b < s$ for alle $s \in S$, og så er $b \in A = X_{<b}$ en modstrid.

"kun hvis": At X er totalt ordnet indses ved for givne $x, y \in X$, hvor $x \not\leq y$, at betragte delmængden $\{x, y\} \subseteq X$. Det første element heri kan ikke være x, og så må det være y, og så er $y \leq x$.

Lad nu $A \subset X$ være et ægte afsnit og lad s være det første element i komplementermængden $X \setminus A$. Det påstås, at

$$A = X_{<s}.$$

Hvis $x < s$, har vi $x \in A$, hvoraf $X_{<s} \subseteq A$. Er omvendt $a \in A$, så er $a < s$, thi da vi har vist, at X er totalt ordnet ville der imodsat fald gælde

$s \leq a$ og $s \in X \setminus A$,

i modstrid med at A var et afsnit ▨

4.3. OBSERVATIONER. (1) Den tomme mængde $\emptyset$ er velordnet.

(2) Enhver delmængde af en velordnet mængde er selv velordnet.

(3) Enhver ikke-tom velordnet mængde har et første element.

(4) Til hvert element a i en velordnet mængde X, som ikke er sidste element i X, findes et umiddelbart

efterfølgende, dvs et element $a^+ \in X$, som opfylder

$$a < a^+ \quad \text{og} \quad a < x \Rightarrow a^+ \leq x.$$

4.4. BEMÆRKNING. Enhver endelig totalt ordnet mængde X er velordnet. Er der n elementer i X kan de nummereres, så at vi har

$$x_1 < x_2 < x_3 < \cdots < x_n.$$

Det vigtigste eksempel på en velordnet mængde er mængden $\mathbb{N}$ af naturlige tal med sædvanlig ordning:

$$1 < 2 < 3 < \cdots.$$

Men vi kan let konstruere større velordnede mængder: F.eks. kan vi udvide $\mathbb{N}$ med et element ω og vi kan udvide ordningen til $\mathbb{N} \cup \{\omega\}$ ved fastsættelsen $n < \omega$, når $n \in \mathbb{N}$. Herved fås

$$1 < 2 < 3 < \cdots < \omega.$$

Og her kan vi yderligere tilføje et ω_1 med $\omega < \omega_1$:

$$1 < 2 < 3 < \cdots < \omega < \omega_1$$

osv, eller endda tilføje en hel følge:

$$1 < 2 < 3 < \cdots < \omega < \omega_1 < \omega_2 < \omega_3 < \cdots$$

og også hertil kan vi tilføje et element, endda en hel følge af elementer, osv. Og vi kan gentage det nummerabelt mange gange (!) og til resultatet kan vi yderligere tilføje ....

Omvendt er det klart, at enhver velordnet mængde X har en "begyndelse", der ligner ovenstående: Under forudsætning af at elementerne "ikke slipper op" kan vi sætte x_1 = første element i X, x_2 = første element i $X \setminus \{x_1\}$, x_3 = første element i $X \setminus \{x_1, x_2\}$, ..., ω = første element i $X \setminus \{x_1, x_2, \cdots\}$, ω_1 = første element i $X \setminus \{x_1, x_2, \cdots; \omega\}$ osv.

4.5. Som nævnt ovenfor er der ingen grænse for hvor "store" velordnede mængder "man kan forestille sig". På den anden side er det klart, at de velordnede mængder vi har opbygget ovenfor alle er nummerable. Så meget mere overraskende er følgende resultat, der også kaldes:

(W) VELORDNINGSSÆTNINGEN. Enhver mængde X kan velordnes.

BEVIS. Vi betragter par $(K,<)$ bestående af en delmængde $K \subseteq X$ og en velordning $<$ på K. For sådanne par $(K,<)$ og $(K',<')$ skriver vi

$$(K',<') \subset (K,<),$$

hvis $(K',<')$ er et ægte afsnit i $(K,<)$, dvs hvis K' er et ægte afsnit i K (mht ordningen $<$), og der for alle $x, y \in K'$ gælder: $x <' y \Rightarrow x < y$.

Det er klart, at der herved defineres en partiel ordning af disse par, og det er nok at vise, at der findes et par $(K,<)$, der er maksimalt m.h.t. til ordningen $\subset$. Er nemlig $(K,<)$ maksimalt, må vi have $K = X$ (og så er $(X,<)$ velordnet), thi ellers fandtes et element $\omega \in X \setminus K$, og så kunne vi udvide K ved tilføjelse af elementet ω: $\tilde{K} := K \cup \{\omega\}$, og vi kunne udvide ordningen til en ordning $<$ i $\tilde{K}$ ved fastsættelsen $x < \omega$ når $x \in K$. Det er klart, at $(\tilde{K},<)$ er velordnet, og da $K = \tilde{K}_{<\omega}$, har vi $(K,<) \subset (\tilde{K},<)$ i modstrid med at $(K,<)$ var maksimalt.

For at eftervise eksistensen af et maksimalt par er det ifølge Zorn's lemma nok at vise, at disse par er induktivt ordnede ved $\subset$. Lad derfor $(K_\iota, <_\iota)$ være en mængde af sådanne par, der er totalt ordnet ved $\subset$.

Lad $K = \bigcup K_j \subseteq X$ være foreningsmængden, og betragt heri relationen $<$ defineret ved

$$x < y \iff \exists j : x \in K_j \wedge y \in K_j \wedge x <_j y.$$

Herom er det nok at vise:

1° Relationen $<$ er en ordensrelation i K

2° $(K, <)$ er velordnet

3° For hvert j er K_j et afsnit i K

4° For $x, y \in K_j$ gælder $x <_j y \Rightarrow x < y$,

thi så er $(K, <)$ majorant for hvert $(K_j, <_j)$.

1°: Relationen er åbenbart irrefleksiv, så vi skal vise, at den er transitiv: Antag, at $x, y, z \in K$, at $x < y$ og at $y < z$. Vælg j, så at $x, y \in K_j$ og $x <_j y$, og vælg i, så at $y, z \in K_i$, $y <_i z$. Lad $(K_\ell, <_\ell)$ være det største (mht $\subseteq$) af de to par $(K_i, <_i)$ og $(K_j, <_j)$. Da har vi $x, y, z \in K_\ell$, og af $x <_i y$ og $y <_j z$ følger $x <_\ell y$ og $y <_\ell z$. Og så er $x <_\ell z$, og dermed $x < z$.

2°: Lad $S \subseteq K$ være en ikke-tom delmængde, vælg et j, så at $K_j \cap S \neq \emptyset$, og lad s_0 være det mindste (mht $<_j$) element i $K_j \cap S$. Vi skal vise for hvert $s \in S$, at

$$s_0 \leqslant s.$$

Hvis $s \in K_j$, har vi $s \in K_j \cap S$, og så er $s_0 \leqslant_j s$ og dermed $s_0 \leqslant s$. Hvis $s \notin K_j$, vælger vi i, så at $s \in K_i$. Da $s \in K_i \setminus K_j$, er $K_i \not\subseteq K_j$, og så må $(K_j, <_j)$ være et afsnit i $(K_i, <_i)$. Da $s \in K_i \setminus K_j$, gælder for hvert $x \in K_j$, at $x <_i s$. Specielt er $s_0 <_i s$ og dermed $s_0 < s$.

3°: Lad $a \in K_j$, lad $x \in K$ og antag $x < a$. Vi skal vise, at $x \in K_j$. Da $x < a$ findes et i, så at $x, a \in K_i$ og $x <_i a$. Hvis $K_i \subseteq K_j$ er påstanden klar. I modsat fald er K_j et afsnit i K_i og af $x <_i a \in K_j$ følger så $x \in K_j$.

4°: Er trivielt udfra definitionen af $<$. ▨

4.6 INDUKTIONS-SÆTNINGEN (TRANSFINIT INDUKTION). Lad $(X, <)$ være en velordnet mængde, og lad $S \subseteq X$ være en delmængde. Hvis der for alle elementer $x \in X$ gælder:

$$(*) \quad X_{<x} \subseteq S \Rightarrow x \in S,$$

så er $S = X$.

IDÉ. Er x_1 det første element i X, så er $X_{<x_1} = \emptyset$. Da $\emptyset \subseteq S$, sikrer (*), at $x_1 \in S$. Er x_2 efterfølgeren til x_1, så er $X_{<x_2} = \{x_1\}$. Da vi har vist, at $\{x_1\} \subseteq S$, sikrer (*), at $x_2 \in S$. Er x_3 efterfølgeren til x_2, har vi $X_{<x_3} = \{x_1, x_2\}$. Da vi har vist, at $\{x_1, x_2\} \subseteq S$, sikrer (*), at $x_3 \in S$. Og således fortsættes: Er ω det mindste element, der er $>$ ethvert x_n, er $X_{<\omega} = \{x_1, x_2, \dots\}$. Da vi ved, at $\{x_1, x_2, \dots\} \subseteq S$, sikrer (*), at $\omega \in S$. Osv. Heldigvis er det stringente bevis kortere.

BEVIS. Var $S \subset X$ kunne vi betragte det første element a i $X \setminus S$. Her er $X_{<a} \subseteq S$, og så er (*) i modstrid med at $a \notin S$ ▨

4.7. REKURSIONS-SÆTNINGEN. (DEFINITION VED TRANSFINIT REKURSION). Lad $(X, <)$ være en velordnet mængde og lad der være givet en forskrift Φ, som til hver afbildning g, hvis domæne er et ægte afsnit af X, knytter en mængde $\Phi(g)$. Da findes der en og kun én afbildning f med domæne X, så at

$$(+) \quad f(x) = \Phi(f|X_{<x}) \text{ for alle } x \in X.$$

DEFINITION. Denne entydigt bestemte afbildning f siges at være <u>rekursivt bestemt</u> ved (+)

BEMÆRKNING. Vi tænker på $\Phi(g)$'erne som "elementer", men forudsætter ikke, at der findes en mængde, som har ethvert $\Phi(g)$ som element. Det er således en ikke-trivial konsekvens af sætningen, at der eksi-

sterer en mængde (nemlig $\operatorname{ran} f$), der har ethvert $f(x) = \phi(f|X_{<x})$ som element.

EKSEMPEL. I den velordnede mængde $(\mathbb{N}, <)$ er de ægte afsnit af formen $\mathbb{N}_{<n^+} = \{1, 2, \cdots, n\}$ eller $\mathbb{N}_1 = \varnothing$ og en afbildning g, hvis domæne er et sådant afsnit, er et n-tuppel $g = (g_1, \cdots, g_n)$ eller "det tomme tuppel" $g = \varnothing$. En forskrift ϕ knytter altså til hvert sådant tuppel et element

$$\phi(g_1, \cdots, g_n), \quad \text{samt til } g = \varnothing \text{ et element } \phi(\varnothing),$$

Rekursionssætningen udsiger altså, at der findes netop én afbildning $f = (f_1, f_2, \cdots)$ med domæne $\mathbb{N}$, således at

$$(+) \quad f_1 = \phi(\varnothing), \quad f_{n+1} = \phi(f_1, \cdots, f_n) \text{ for alle } n \in \mathbb{N}.$$

Hvis forskriften ϕ er bestemt ud fra en forskrift φ, der til hver mængde Y knytter en mængde $\varphi(Y)$, og en udvalgt mængde A, ved at

$$\phi(\varnothing) = A, \quad \phi(g_1, \cdots, g_n) = \varphi(g_n)$$

giver sætningen afbildningen $f = (f_1, f_2, \cdots)$ rekursivt bestemt ved

$$(+) \quad f_1 = A, \quad f_{n+1} = \varphi(f_n).$$

Er f.eks. φ bestemt ved $\varphi(Y) = \mathcal{P}(Y)$, får vi den rekursive definition af $\mathcal{P}^n(A)$, $n \in \mathbb{N}$, og samtidig <u>eksistensen</u> af mængden $\{A, \mathcal{P}(A), \mathcal{P}^2(A), \cdots\}$ (og dermed også eksistensen af foreningsmængden $A \cup \mathcal{P}(A) \cup \mathcal{P}^2(A) \cup \cdots$).

BEVIS FOR REKURSIONS-SÆTNINGEN. <u>Entydighed</u>: Lad f_1 og f_2 være være afbildninger, som opfylder det stillede krav. Vi bruger transfinit induktion på mængden

$$S = \{x \in X \mid f_1(x) = f_2(x)\}.$$

Antag altså, at $x \in X$, og at $X_{<x} \subseteq S$. Da er $f_1(y) = f_2(y)$ for alle $y \in X_{<x}$ og følgelig er $f_1|X_{<x} = f_2|X_{<x}$. Men så er $f_1(x) = \phi(f_1|X_{<x}) = \phi(f_2|X_{<x}) = f_2(x)$.

Eksistens: Lad os et øjeblik kalde en afbildning g for ϕ-rekursiv, hvis dens domæne er et afsnit i X og hvis der gælder

$$g(x) = \phi(g|X_{<x}) \text{ for alle } x \in \mathrm{dom}\, g.$$

Vi skal bevise, at der findes en ϕ-rekursiv afbildning, hvis domæne er hele X.

Vi bemærker først, at den allerede beviste entydighed sikrer, at der for et givet afsnit $A \subseteq X$ højst findes én ϕ-rekursiv afbildning, der har domæne A. Heraf følger, at hvis der for et givet $x \in X$ findes ϕ-rekursive afbildninger g og h, så at $x \in \mathrm{dom}\, g$ og $x \in \mathrm{dom}\, h$, så er $g(x) = h(x)$, thi restriktionerne $g|X_{\leq x}$ og $h|X_{\leq x}$ er ligeledes ϕ-rekursive afbildninger med domæne $X_{\leq x}$, så $g|X_{\leq x} = h|X_{\leq x}$ og derfor er specielt $g(x) = h(x)$.

Lad nu $B \subseteq X$ være foreningsmængden af de afsnit, der er domæne for en ϕ-rekursiv afbildning. Vi ønsker, at definere en afbildning f med domæne B ved for hvert $x \in B$ at definere værdien $y = f(x)$ ved: Der eksisterer en ϕ-rekursiv afbildning g med $x \in \mathrm{dom}\, g$ og $y = g(x)$. For hvert element $x \in B$ er der netop et sådant element y. For at der herved defineres en afbildning, må vi imidlertid sikre, at der findes en mængde, der indeholder alle sådanne y'er. Men det følger af Udskiftningsaxiomet, da vi jo lige har set, at for ethvert element $x \in B$ er det fremhævede udsagn mængdebestemmende (det bestemmer en mængde med ét element).

Mængden B er en foreningsmængde af afsnit

og derfor selv et afsnit. Afbildningen f har domæne B, og hvis $x \in B$ findes en ϕ-rekursiv afbildning g med $x \in \mathrm{dom}\, g$, og så er $f(z) = g(z)$ for alle $z \in \mathrm{dom}\, g$. Specielt er

$$f(x) = g(x) = \phi(g|X_{<x}) = \phi(f|X_{<x}),$$

og afbildningen f er derfor ϕ-rekursiv.

For afsnittet B må der gælde $B = X$, thi i modsat fald havde B formen $B = X_{<a}$, med $a \in X$, og så kunne vi udvide f ved definitionen

$$\bar{f}(a) = \phi(f)$$

til en ϕ-rekursiv afbildning $\bar{f}$ med domæne $X_{\leq a} \supset B$, i modstrid med at ethvert domæne for en ϕ-rekursiv afbildning er $\subseteq B$. Afbildningen f er således en ϕ-rekursiv afbildning med domæne X ▨

4.8. SÆTNING. Lad $(X, <)$ og $(Y, <)$ være velordnede mængder. Da findes højst én afbildning $f: X \to Y$, som afbilder $(X, <)$ ordensisomorft på et afsnit af Y. Hvis ingen sådan afbildning findes, da eksisterer der en afbildning $g: Y \to X$, som afbilder $(Y, <)$ ordensisomorft på et ægte afsnit af X.

BEVIS. At $f: X \to Y$ afbilder $(X, <)$ ordensisomorft på et afsnit af Y er ensbetydende med at

$$(*) \quad Y_{<f(x)} = f(X_{<x}) \quad \text{for alle } x \in X.$$

Men det er jo en rekursiv bestemmelse af afbildningen f. Mere præcist: Lad os med $\lightning$ betegne en mængde, der ikke er element i Y (jfr. Bemærkning 1.2.2) og betragt følgende forskrift ϕ:

For hver afbildning g, hvis domæne er et ægte afsnit af X, sætter vi

$$\phi(g) = \begin{cases} y, & \text{hvis } g \text{ afbilder domæ } g \text{ ordensisomorft} \\ & \text{på afsnittet } Y_{<y} \text{ af } Y. \\ \lightning & \text{ellers.} \end{cases}$$

Hvis $f: X \to Y$ afbilder X ordensisomorft på et afsnit af Y, følger det af $(\neq)$, at f er ϕ-rekursiv. Heraf følger entydigheden.

Omvendt kan vi altid betragte den ved ovenstående forskrift ϕ rekursivt bestemte afbildning f. Da vi altid har $\phi(g) \in Y$ eller $\phi(g) = \lightning$, er f en afbildning $f: X \to Y \cup \{\lightning\}$. Hvis der for et element $x \in X$ gælder $f(x) \in Y$, ser vi af forskriften, at

$$Y_{<f(x)} = f(X_{<x}).$$

Tilfælde 1°: For alle $x \in X$ gælder $f(x) \in Y$. Af det foregående følger, at f så afbilder X ordensisomorft på et afsnit af Y.

Tilfælde 2°: Der eksisterer $x \in X$ med $f(x) = \lightning$. Lad $a \in X$ være det første sådanne element. Af det foregående følger, at $f_0 := f/X_{<a}$ afbilder $X_{<a}$ ordens-isomorft på et afsnit af Y. Men dette afsnit må være hele Y, thi ellers havde det formen $Y_{<b}$, $b \in Y$, og så er $\phi(f_0) = b$ og dermed $f(a) = \phi(f/X_{<a}) = \phi(f_0) = b \in Y$, i modstrid med at $f(a) = \lightning \notin Y$.

Og nu definerer f_0^{-1} en ordensisomorfi af Y på afsnittet $X_{<a}$ af X ▨

KOROLLAR 1. SAMMENLIGNINGSSÆTNING FOR VELORDNEDE MÆNGDER. Lad $(X,<)$ og $(Y,<)$ være velordnede mængder. Da indtræffer netop én af følgende muligheder:

1° $(X,<)$ er ordensisomorf med et ægte afsnit af $(Y,<)$

2° $(X,<)$ er ordensisomorf med $(Y,<)$

3° $(Y,<)$ er ordensisomorf med et ægte afsnit af $(X,<)$.

BEVIS. Af Sætningen følger, at der altid indtræffer en af de tre muligheder. Af entydigheden i sætningen følger lit, at der højst kan indtræffe én af de tre muligheder □

(u) KOROLLAR 2. SAMMENLIGNINGSSÆTNING FOR MÆNGDER. Lad X og Y være mængder. Da indtræffer netop én af følgende muligheder:

1° $X < Y$

2° $X \simeq Y$

3° $Y < X$.

BEVIS. De to mængder X og Y kan velordnes (Velordningssætningen). Af Korollar 1 følger derfor specielt, at $X \lesssim Y$ eller $Y \lesssim X$. Og heraf følger påstanden, jfr. Sætning 2.3 ▨

4.9. EKSEMPEL. Der findes en ikke-tællelig mængde (jfr. 2.5 eller Eksempel 2.7.(2)) og dermed ifølge velordningssætningen en ikke-tællelig velordnet mængde $(\Omega,<)$. Tilføjes om fornødent et sidste element til Ω kan vi antage, at der findes elementer $w \in \Omega$ så at afsnittet $\Omega_{<w}$ er ikke-tælleligt. Lad w_1 være det mindste af disse elementer. Da er $\Omega_1 := \Omega_{<w_1}$ en <u>ikke-tællelig velordnet mængde, hvori ethvert ægte afsnit er tælleligt</u>. Af Sammenligningssætningen følger, at enhver ikke-tællelig velordnet mængde indeholder Ω_1 som et afsnit.

Bemærk, at Ω_1 ikke har et sidste element, men at enhver følge $x_1, x_2, \dots$ i Ω_1 er opad begrænset. Thi $U = \bigcup_{n \in \mathbb{N}} (\Omega_1)_{\leq x_n}$ er et afsnit, og en tællelig forening

af tællelige mængder, og dermed selv tællelig (Korollar 2.6.1). Men så er $U \subset \Omega_1$, og derfor af formen $U = (\Omega_1)_{<b}$, med $b \in \Omega_1$, og så er specielt $x_n < b$ for alle n.

(U) 4.10. SÆTNING. Enhver uendelig mængde X er ækvipotent med en mængde af formen $Y \times \mathbb{N}$.

BEVIS. Da X er uendelig, har X en numerabel delmængde. Idet vi først velordner komplementærmængden (Velordningssætningen) og dernæst tilføjer den numerable delmængde, fås en velordning $<$ i X, så at intet element i X er sidste element. Vi kan derfor definere en afbildning $\varepsilon : X \to X$ ved $\varepsilon(x) := x^+$ (det umiddelbart følgende til x, jfr. Observation 4.3 (4)). Lad Y betegne komplementærmængden

$$Y := X \setminus \varepsilon(X).$$

Vi påstår, at $f(y,n) := \varepsilon^{n-1}(y)$ definerer en bijektiv afbildning $f : Y \times \mathbb{N} \to X$. Den er <u>injektiv</u>, thi er $f(y,n) = f(y',n')$, kan vi antage, at $n' = n+p$, $p \geq 0$, og så er $f(y',n') = \varepsilon^{n'-1}(y') = \varepsilon^{n-1}(\varepsilon^p(y')) = \varepsilon^{n-1}(y)$. Da ε, og dermed også potensen ε^{n-1}, er injektiv, må vi have $\varepsilon^p(y') = y$. Da $y \notin \varepsilon(X)$, må vi have $p = 0$, altså $y' = y$ og $n' = n$. Og den er <u>surjektiv</u>, thi ellers kunne vi betragte det første x, der ikke tilhører billedmængden. Vi har $x \notin Y$ (thi ellers var $x = f(x,1)$), og dermed $x = \varepsilon(z)$, $z \in X$. Her er $z < x$, så vi kan skrive $z = f(y,n)$ og dermed $x = \varepsilon(z) = \varepsilon f(y,n) = f(y,n+1)$, i modstrid med at x ikke tilhørte billedmængden ▨

(U) KOROLLAR. For enhver uendelig mængde X er $X \times \mathbb{N}$ ækvipotent med X.

BEVIS. Ifølge Sætning 2.6 er

$$X \times \mathbb{N} \bar{\sim} Y \times \mathbb{N} \times \mathbb{N} \bar{\sim} Y \times \mathbb{N} \bar{\sim} X \quad \square$$

5. Ækvivalens af eksistensaxiomerne.

5.1. Vi har i det foregående mødt følgende eksistensudsagn:

UDVALGSAXIOMET (U). For enhver mængde A eksisterer der en udvalgsfunktion u på A.

ZORN'S LEMMA (Z). I enhver partielt ordnet mængde $(X, <)$, der er induktivt ordnet, eksisterer der et maksimalt element.

VELORDNINGSSÆTNINGEN (V). For enhver mængde M eksisterer der en relation $<$ i M så at $(M, <)$ er velordnet.

Til denne gruppe eksistensudsagn medregnes ofte:
MAKSIMALITETSPRINCIPPET (M). I enhver partielt ordnet mængde $(Y, <)$ eksisterer der en totalt ordnet delmængde K, så at intet element i $Y \setminus K$ er sammenligneligt med alle elementer i K.
Bemærk: En ækvivalent formulering er øjensynlig: I enhver partielt ordnet mængde $(Y, <)$ eksisterer en totalt ordnet delmængde K, der er maksimal blandt de totalt ordnede delmængder.

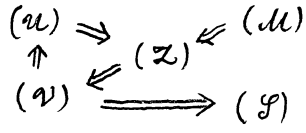
SAMMENLIGNINGSSÆTNINGEN (S). For vilkårlige givne mængder X og Y eksisterer der enten en injektiv afbildning $: X \to Y$ eller en injektiv afbildning $: Y \to X$.

5.2. HOVEDRESULTAT. Under forudsætning af ZF-axiomerne er de fem ovennævnte eksistensudsagn ækvivalente, dvs ethvert af dem medfører de fire andre.

OVERSIGT. At (U) ⇒ (Z) så vi i Sætning 3.4. At (Z) ⇒ (V) så vi i beviset for Velordningssætningen 4.5. At (V) ⇒ (F) så vi i Korollar 4.8.2. Det er klart, at (F) ⇒ (U), thi udfra en velordning $<$ på mængden A kan vi definere en udvalgsfunktion u på A ved

$$u(X) := (\text{første element i } X), \quad \text{for } \emptyset \neq X \subseteq A.$$

Det er ligeledes klart, at (M) ⇒ (Z): Lad nemlig $(X,<)$ være induktivt ordnet. Ifølge (M) kan vi betragte en delmængde $K \subseteq X$, maksimal blandt de totalt ordnede delmængder af X. Da X var induktivt ordnet, har K en majorant. Og denne må være maksimalt element i X, da K ellers ville have ægte majoranter, i modstrid med maksimaliteten af K. Vi har altså



At (F) ⇒ (V) vises senere, jfr. 7.17, så der resterer (f.eks.):

5.3. BEVIS FOR (Z) ⇒ (M). Lad $(Y,<)$ være partielt ordnet. Vi betragter mængden $\mathfrak{X}$ af totalt ordnede delmængder $K \subseteq Y$. Mængden $\mathfrak{X}$ er partielt ordnet ved sædvanlig inklusion $\subset$, og vi skal vise, at der i $(\mathfrak{X}, \subset)$ eksisterer et maksimalt element. Da vi antager (Z), er det nok at vise, at $(\mathfrak{X}, \subset)$ er induktivt ordnet. Lad derfor $\mathcal{A} = \{K_i \mid i \in I\}$ være en totalt ordnet delmængde af $\mathfrak{X}$. Vi påstår, at foreningsmængden $K := \bigcup K_i$ er majorant for $\mathcal{A}$. Da vi øjensynlig har $K_i \subseteq K$ for alle i, skal vi blot vise, at $K \in \mathfrak{X}$, dvs at K er en totalt ordnet delmængde af Y. Lad $x, y \in K = \bigcup_i K_i$, da findes $i, j \in I$, så at $x \in K_i$ og $y \in K_j$. Da $\mathcal{A}$ var totalt ordnet, kan vi antage, at $K_i \subseteq K_j$, og så er både x og y elementer i K_j og derfor sammenlignelige, da K_j var totalt ordnet ▨

5.4 Som illustration af anvendeligheden af Zorn's lemma vil vi her direkte vise $(Z) \Rightarrow (U)$ og $(Z) \Rightarrow (S)$.

BEVIS FOR $(Z) \Rightarrow (U)$. En udvalgsfunktion på en mængde A er en afbildning $u : \mathcal{P}(A) \setminus \{\emptyset\} \to A$, som opfylder

$(*)$ $u(X) \in X$ for alle X med $\emptyset \subset X \subseteq A$.

I det følgende betragtes partielle udvalgsfunktioner på A, dvs par $(\mathcal{D}, u)$ bestående af en delmængde $\mathcal{D} \subseteq \mathcal{P}(A) \setminus \{\emptyset\}$ og en afbildning $u : \mathcal{D} \to A$, som opfylder $(*)$ for alle $X \in \mathcal{D}$. Vi skal vise vise, at der eksisterer en partiel udvalgsfunktion $(\mathcal{D}, u)$, hvis domæne $\mathcal{D}$ er hele $\mathcal{P}(A) \setminus \{\emptyset\}$.

Mængden $\mathfrak{X}$ af partielle udvalgsfunktioner ordnes ved definitionen

$$(\mathcal{D}, u) < (\mathcal{D}', u') \overset{DEF}{\iff} \mathcal{D} \subset \mathcal{D}' \wedge u'/\mathcal{D} = u.$$

Et maksimalt element $(\mathcal{D}, u)$ i $\mathfrak{X}$ må have $\mathcal{D} = \mathcal{P}(A) \setminus \{\emptyset\}$, thi i modsat fald findes en ikke-tom delmængde $B \subseteq A$ med $B \notin \mathcal{D}$, og vælges et element $b \in B$ kan vi udvide u til en afbildning $\tilde{u}$ med domæne $\tilde{\mathcal{D}} = \mathcal{D} \cup \{B\}$ ved definitionen

$$\tilde{u}(X) = \begin{cases} u(X), & \text{hvis } X \in \mathcal{D} \\ b, & \text{hvis } X = B, \end{cases}$$

Det er klart, at $(\tilde{\mathcal{D}}, \tilde{u}) \in \mathfrak{X}$, men så er $(\mathcal{D}, u) < (\tilde{\mathcal{D}}, \tilde{u})$ i modstrid med maksimaliteten af $(\mathcal{D}, u)$.

Da vi antager (Z), er det nok at vise, at $(\mathfrak{X}, <)$ er induktivt ordnet. Er $\{(\mathcal{D}_i, u_i) \mid i \in I\}$ en totalt ordnet delmængde kan vi betragte $\mathcal{D} = \bigcup_i \mathcal{D}_i$ og herpå definere $u : \mathcal{D} \to A$ ved $u(X) = u_i(X)$, når $X \in \mathcal{D}_i$. Det er let at se, at der herved defineres en partiel udvalgsfunktion $(\mathcal{D}, u)$, og at

$$(\mathcal{D}_i, u_i) \leqslant (\mathcal{D}, u) \text{ for alle } i \in I \quad \square$$

BEVIS FOR $(\mathcal{Z}) \Rightarrow (\mathcal{S})$. Lad X og Y være mængder og betragt mængden af injektive afbildninger med dom $\subseteq X$ og ran $\subseteq Y$. Vi kan tænke på disse afbildninger som par (A, f) bestående af en delmængde $A \subseteq X$ og en injektiv afbildning $f : A \to Y$. Vi kan ordne disse afbildninger ved definitionen

$$(A, f) < (B, g) \overset{\text{DEF}}{\Leftrightarrow} A \subset B \wedge g/A = f.$$

For et maksimalt element (A, f) blandt disse afbildninger har vi <u>enten</u> $A = X$ (og så er f en injektiv afbildning $: X \to Y$) <u>eller</u> $f(A) = Y$ (og så er f^{-1} en injektiv afbildning $: Y \to X$). Var nemlig både $A \subset X$ og $f(A) \subset Y$, så kunne finde $a \in X \setminus A$ og $b \in Y \setminus f(A)$ og definere $g : A \cup \{a\} \to Y$ ved $g(a) = b$ og $g/A = f$. Det er klart, at g er injektiv og at $(A, f) < (A \cup \{a\}, g)$ og dét er i modstrid med maksimaliteten af (A, f).

Da vi antager $(\mathcal{Z})$ er det nok at vise, at den betragtede mængde af injektive afbildninger er induktivt ordnet. Og dette følger ganske som i beviset for den foregående sætning □

(PL) ## 6. Den transfinite talrække.

6.1. I det følgende er det bekvemt at tænke sig valgt en velordnet mængde Ω så stor, at alle i praksis forekommende mængder har mindre mægtighed end Ω.

BEMÆRKNING. Teoretisk er et sådant valg naturligvis en umulighed, thi ifølge definitionen kan Ω ikke forekomme i praksis. På den anden side behøver vi i praksis kun at behandle en given mængde af mængder, og så kan vi ifølge Sumaxiomet 1.4 finde en mængde X, hvori enhver af de givne mængder er delmængde. Hertil kan vi finde en mængde Y af større mægtighed end X (f.eks. $Y = \mathcal{P}(X)$, jfr. Cantor's Sætning 2.4, eller $Y = X \cup \mathcal{P}(X) \cup \mathcal{P}(\mathcal{P}(X)) \cup \cdots$). Vi kan velordne Y (Velordningssætningen 4.5) og bruge denne mængde som Ω. Har vi to kandidater for Ω følger det af Sammenligningssætningen 4.8.1, at den ene er ordensisomorf med et afsnit af den anden, så heller ikke dette kan genere os i praksis.

6.2. Vi kan antage, at ethvert ægte afsnit i Ω har mindre mægtighed end Ω, thi var dette ikke tilfældet, kunne vi erstatte Ω med $\Omega_{<\infty}$, hvor ∞ er det første element i Ω så at afsnittet $\Omega_{<\infty}$ er ækvipotent med Ω.

DEFINITION. Elementerne i Ω kaldes <u>ordinaltal</u>.

6.3. Af antagelsen følger specielt, at der ikke er noget sidste element i Ω. For hvert ordinaltal $\lambda \in \Omega$

kan vi altså betragte det efterfølgende ordinaltal λ^+ (jfr. Observation 4.3 (4)).

NOTATION. Det første element i Ω betegnes 0. Vi betegner

$$0^+ =: 1, \quad 1^+ =: 2, \quad 2^+ =: 3, \quad \cdots$$

Med denne notation kan vi opfatte de naturlige tal (med 0 medregnet) som elementer i Ω, dvs som ordinaltal. Efterfølgeren af et naturligt tal n er den sædvanlige efterfølger $n^+ = n+1$. Bemærk, at afsnittet

$$\Omega_{<n} = \{0, 1, \cdots, n-1\}$$

har præcis n elementer.

6.4. DEFINITION. De naturlige tal (0 medregnet) kaldes også de endelige ordinaltal. De ikke-endelige ordinaltal siges at være transfinite. Det første transfinite ordinaltal betegnes ω. Bemærk, at afsnittet

$$\Omega_{<\omega} = \{0, 1, 2, 3, \cdots\}$$

præcis består af de naturlige tal.

6.5. Ifølge Sammenligningssætningen 4.8.1 er "enhver" velordnet mængde $(M, <)$ ordensisomorf med et ægte afsnit $\Omega_{<\lambda}$ af Ω, og λ er entydigt bestemt.

DEFINITION. Ordinaltallet $\lambda \in \Omega$ kaldes ordinaltallet for den velordnede mængde $(M, <)$ og betegnes

$$\lambda := \mathrm{ord}(M, <)$$

(eller blot $\mathrm{ord}(M)$, hvis ordningen $<$ i M er underforstået).

OBSERVATION. For velordnede mængder $(M,<)$ og $(N,<)$ har vi øjensynlig

$$\text{ord}\, N < \text{ord}\, M,$$

netop når $(N,<)$ er ordensisomorf med et ægte afsnit af $(M,<)$.

EKSEMPLER. For en endelig totalt ordnet (og dermed velordnet) mængde $(M,<)$ med n elementer, har vi $\text{ord}\, M = n$.

For mængden $\mathbb{N}$ af naturlige tal (med sædvanlig ordning) har vi $\text{ord}\, \mathbb{N} = \omega$.

Udvides $\mathbb{N}$ med et element ∞, der er $>$ alle naturlige tal fås en velordnet mængde $\bar{\mathbb{N}}$ med $\text{ord}\, \bar{\mathbb{N}} = \omega^+$.

6.6. DEFINITION. Et element $\alpha \in \Omega$ kaldes et <u>kardinaltal</u>, hvis afsnittet $\Omega_{<\alpha}$ ikke er ækvipotent med noget afsnit $\Omega_{<\beta}$, hvor $\beta < \alpha$. Betingelsen er altså, at der for hvert ordinaltal $\beta < \alpha$ gælder $\Omega_{<\beta} < \Omega_{<\alpha}$.

OBSERVATION. Som delmængde af den velordnede mængde Ω udgør kardinaltallene selv en velordnet mængde.

De endelige ordinaltal er øjensynlig kardinaltal. Det første ikke-endelige kardinaltal betegnes

$$\aleph_0$$

(tegnet $\aleph$, der er det første bogstav i det hebraiske alfabet, læses: "alef").
Det første kardinaltal, der er $> \aleph_0$, betegnes $\aleph_1$.
Det første kardinaltal, der er $> \aleph_1$, betegnes $\aleph_2$, o.s.v.
Det første kardinaltal, der er $> \aleph_n$, for alle na-

tuerlige tal n, betegnes $\aleph_\omega$, o.s.v. De første kardinaltal er altså

$$0, 1, 2, \dots, \aleph_0, \aleph_1, \aleph_2, \dots, \aleph_\omega, \aleph_{\omega+}, \aleph_{\omega++}, \dots$$

BEMÆRKNING. Ordinaltallet ω er et kardinaltal, thi $\Omega_{<\omega}$ er en uendelig mængde, og for hvert ordinaltal $n < \omega$ er $\Omega_{<n}$ en endelig mængde (med n elementer). Derimod er ω^+ ikke et kardinaltal, thi afsnittet $\Omega_{<\omega+} = \{0, 1, 2, \dots, \omega\}$ er ligemægtig ækvipotent med afsnittet $\Omega_{<\omega} = \{0, 1, 2, \dots\}$. Tilsvarende er ordinaltallene ω^{++}, ω^{+++}, ω^{++++}, ... ikke kardinaltal. Heller ikke det mindste ordinaltal $\tilde{\omega}$ større end alle disse er et kardinaltal, thi afsnittet $\Omega_{<\tilde{\omega}} = \{0, 1, 2, \dots, \omega, \omega^+, \omega^{++}, \dots\}$ er ækvipotent med $\Omega_{<\omega}$.

Det er klart, at $\aleph_0 = \omega$. Derimod kan vi ikke "tælle til" $\aleph_1$ i ordinalrækken, thi kunne vi det, ville $\Omega_{<\aleph_1}$ være ækvipotent med $\Omega_{<\omega}$ i modstrid med $\omega < \aleph_1$. Kardinaltal $> \aleph_0$ er altså "utællelige".

6.7. Ifølge Velordningssætningen 4.5 kan enhver mængde velordnes. "Enhver" mængde A er derfor ækvipotent med et ægte afsnit $\Omega_{<\alpha}$ af Ω.

DEFINITION. Det mindste ordinaltal $\alpha \in \Omega$, således at A er ækvipotent med afsnittet $\Omega_{<\alpha}$, kaldes kardinaltallet for mængden A og betegnes

$$\alpha = \mathrm{card}(A) \left(= \#A = |A|\right).$$

BEMÆRKNING. Det er klart, at $\mathrm{card}(A)$ er et kardinaltal.

OBSERVATION. For "vilkårlige" mængder A og B gælder:

$$A \approx B \iff \mathrm{card}(A) = \mathrm{card}(B)$$

$$A < B \iff \mathrm{card}(A) < \mathrm{card}(B).$$

6.8. EKSEMPLER. En mængde A er endelig, netop når $n := \mathrm{card}(A)$ er et naturligt tal (0 medregnet), og tallet n er elementantallet i A i den forstand, at A er ækvipotent med $\Omega_{<n} = \{0, 1, \cdots, n-1\}$.

For mængden $\mathbb{N}$ finder vi

$$\mathrm{card}(\mathbb{N}) = \aleph_0.$$

En mængde A er således numerabel, netop når $\mathrm{card}(A) = \aleph_0$, og en mængde B er tællelig, netop når $\mathrm{card}(B) \leqslant \aleph_0$.

Af resultaterne i 2.6 og 2.7 fremgår, at

$$\mathrm{card}(\mathbb{N}\times\mathbb{N}) = \mathrm{card}(\mathbb{Z}) = \mathrm{card}(\mathbb{Q}) = \aleph_0$$

og at

$$\mathrm{card}(\mathbb{R}) > \aleph_0.$$

Kardinaltallet $\mathrm{card}(\mathbb{R})$ betegnes også $\aleph$. Af uligheden ovenfor følger, at

$$\aleph_0 < \aleph,$$

og dermed, at

$$\aleph_1 \leqslant \aleph.$$

Kontinuumshypotesen (jfr. 2.8) udsiger, at $\aleph = \aleph_1$, men dette kan som nævnt hverken bevises eller modbevises ud fra ZF-axiomerne.

6.9. Ud fra operationer med mængder kan vi definere tilsvarende operationer med kardinaltallene.

Er α og β kardinaltal, defineres <u>summen</u> $\alpha+\beta$, <u>produktet</u> $\alpha\cdot\beta$ og <u>potensen</u> β^α på følgende måde:

Vælg mængder A og B, så at

$$\boxed{\alpha = \operatorname{card}(A)\ ,\quad \beta = \operatorname{card}(B)}$$

og sæt

$$\boxed{\begin{aligned} \alpha+\beta &= \operatorname{card}(A\cup B)\ , \quad A,B \text{ forudsættes her disjunkte}\\ \alpha\cdot\beta &= \operatorname{card}(A\times B)\\ \beta^\alpha &= \operatorname{card}(B^A)\end{aligned}}$$

Det er lit at se, at disse kompositioner er veldefinerede, dvs at kardinaltallene på højre-siden er uafhængige af valgene af A og B. Og så følger dit, at disse ligninger gælder for "vilkårlige" mængder A og B.

6.10. For disse kompositioner blandt kardinaltallene gælder de fleste af de regneregler, vi kender fra de sædvanlige tal. Lad os som eksempel vise <u>potensreglerne</u>:

0. $\alpha^1 = \alpha$

1. $\gamma^{\alpha+\beta} = \gamma^\alpha\cdot\gamma^\beta$

2. $\gamma^{\alpha\cdot\beta} = (\gamma^\alpha)^\beta$

3. $(\beta\cdot\gamma)^\alpha = \beta^\alpha\cdot\gamma^\alpha$

Vi har $1 = \operatorname{card}\{0\}$, og vælger mængder A, B, C (med A og B disjunkte for 1. potensregel) så at $\alpha = \operatorname{card}(A)$, $\beta = \operatorname{card}(B)$, $\gamma = \operatorname{card}(C)$. Afbildningerne

$$\begin{aligned} A^{\{0\}} &\to A & f &\longmapsto f(0)\\ C^{A\cup B} &\to C^A\times C^B & g &\longmapsto (g/A\ \ g/B)\\ (C^A)^B &\to C^{A\times B} & h &\longmapsto [(a,b)\mapsto h(b)(a)]\\ B^A\times C^A &\to (B\times C)^A & (k,\ell) &\longmapsto [a\mapsto (k(a),\ell(a))]\end{aligned}$$

er da bijektive, og heraf følger påstandene.

6.11. Cantor's sætning 2.4 udsiger, at der for "enhver" mængde A gælder

$$\operatorname{card}(A) < \operatorname{card}(\mathcal{P}(A)) = 2^{\operatorname{card}(A)}$$

Specielt gælder altså $\alpha < 2^\alpha$ for ethvert kardinaltal α.

EKSEMPEL. Ifølge resultatet i 2.9 er

$$\operatorname{card}(\mathcal{P}(\mathbb{N})) = 2^{\aleph_0} = \aleph.$$

Kontinuumshypotesen udsiger altså, at $2^{\aleph_0} = \aleph_1$.

6.12. For endelige kardinaltal er kompositionerne de sædvanlige kompositioner af naturlige tal. For transfinite kardinaltal simplificeres aritmetikken af følgende:

SÆTNING. Lad α og β være kardinaltal $\neq 0$, hvoraf et forudsættes transfinit. Da er

$$\alpha + \beta = \alpha \cdot \beta = \max\{\alpha, \beta\}.$$

BEVIS. Vi kan antage $\beta \leqslant \alpha$, altså at $\max\{\alpha, \beta\} = \alpha$. Det er klart, at $\alpha \leqslant \alpha + \beta$. At $\alpha + \beta \leqslant \alpha \cdot \beta$ ses også lit (for $\beta = 1$ er det dog nødvendigt at udnytte, at α er uendeligt). Da vi trivielt har $\alpha \cdot \beta \leqslant \alpha \cdot \alpha$, er det derfor nok at vise, at

$$\alpha \cdot \alpha \leqslant \alpha \quad , \text{ når } \alpha \text{ er transfinit.}$$

Var dette ikke opfyldt, kunne vi, da kardinaltallene er velordnede, betragte det første transfinite kardinaltal α, for hvilket

$$\alpha < \alpha \cdot \alpha.$$

Her er $\alpha = \operatorname{card}(\Omega_{<\alpha})$ og $\alpha \cdot \alpha = \operatorname{card}(\Omega_{<\alpha} \times \Omega_{<\alpha})$.

Produktmængden $\Omega_{<\alpha} \times \Omega_{<\alpha}$ ordner vi ved at skrive

$(\lambda_1, \lambda_2) < (\mu_1, \mu_2)$, når

$$\max\{\lambda_1, \lambda_2\} < \max\{\mu_1, \mu_2\}$$

eller $\max\{\lambda_1, \lambda_2\} = \max\{\mu_1, \mu_2\}$ og $\lambda_1 < \mu_1$

eller $\max\{\lambda_1, \lambda_2\} = \max\{\mu_1, \mu_2\}$ og $\lambda_1 = \mu_1$ og $\lambda_2 < \mu_2$.

Det er klart, at der herved definerer en velordning i $\Omega_{<\alpha} \times \Omega_{<\alpha}$. Det er udelukket, at $\Omega_{<\alpha} \times \Omega_{<\alpha}$ er ordensisomorf med et afsnit af $\Omega_{<\alpha}$, idet vi jo så ville få $\alpha \cdot \alpha = \operatorname{card}(\Omega_{<\alpha} \times \Omega_{<\alpha}) \leq \operatorname{card} \Omega_{<\alpha} = \alpha$ i modstrid med at $\alpha < \alpha \cdot \alpha$. Af Sammenligningssætningen 4.8.1 følger derfor, at $\Omega_{<\alpha}$ er ordensisomorf med et ægte afsnit $W \subseteq \Omega_{<\alpha} \times \Omega_{<\alpha}$. Der findes altså $\mu_1, \mu_2 \in \Omega_{<\alpha}$, så at $W = \{(\lambda_1, \lambda_2) \mid (\lambda_1, \lambda_2) < (\mu_1, \mu_2)\}$. Da α er et transfinit kardinaltal er der intet sidste element i $\Omega_{<\alpha}$. Der findes derfor et ordinaltal $\beta < \alpha$, så at $\max\{\mu_1, \mu_2\} < \beta$, og så følger det, at vi for hvert element $(\lambda_1, \lambda_2) \in W$ har $\lambda_1 < \beta$ og $\lambda_2 < \beta$. Altså er $W \subseteq \Omega_{<\beta} \times \Omega_{<\beta}$. Sættes $\gamma = \operatorname{card}(\Omega_{<\beta})$, har vi $\gamma \leq \beta$ og ifølge det foregående $\Omega_{<\alpha} \sim W \subseteq \Omega_{<\beta} \times \Omega_{<\beta}$, og dermed

$$\alpha \leq \gamma \cdot \gamma \quad , \quad \gamma < \alpha.$$

Men dette er en modstrid, thi hvis γ var endelig kunne vi slutte at også α var endelig, og var γ transfinit sikrer valget af α, at $\gamma \cdot \gamma \leq \gamma$ og så fås $\alpha < \alpha$ ▨

KOROLLAR. For et transfinit kardinaltal α gælder $\alpha^\alpha = 2^\alpha$.

BEVIS. $2^\alpha \leq \alpha^\alpha \leq (2^\alpha)^\alpha = 2^{\alpha \cdot \alpha} = 2^\alpha$ ▨

7. Ordinaltal og kardinaltal. Uendelighedsaxiomet.

7.0. INDLEDNING. Vi vil her vise nogle resultater om mængder, idet vi af ZF-axiomerne kun forudsætter de første 7 og altså hverken Uendelighedsaxiomet 1.8 eller Udvalgsaxiomet 1.11. Som vi skal se, kan vi alene på dette grundlag definere ordinaltal og kardinaltal (og vi kan altså specielt gøre dette uden at vi behøver at vælge en "utænkelig" mængde Ω af ordinaltal). Som nævnt i 1.9 (10) sikrer Uendelighedsaxiomet, at der findes en mængde, som vi kan opfatte som mængden $\mathbb{N}$ af naturlige tal. Vi vil præcisere, hvorledes dette skal forstås.. Samtidig får vi løst et lille problem: For at definere, hvad det vil sige, at mængde er endelig, jfr. Definition 2.5, har vi måttet indrage de naturlige tal $\mathbb{N}$, så specielt har vi måttet antage, at der eksisterer en uendelig mængde.

Til sidst fremhæver vi nogle (svækkede) varianter af udvalgsaxiomet.

7.1. DEFINITION. Et <u>ordinaltal</u> er en mængde v af mængder, således at følgende betingelser er opfyldt:

(ord 1): For hvert element $x \in v$ er $x \notin x$.

(ord 2): For hvert element $x \in v$ er $x \subseteq v$.

(ord 3): Elementerne i v er velordnet ved $\subset$ (sædvanlig inklusion).

OBSERVATION. For et ordinaltal v gælder $v \notin v$ og for hvert element $x \in v$ gælder $x \subset v$,
thi af (ord 1) fås

$$v \in v \Rightarrow v \notin v,$$

hvoraf $v \notin v$, og er $x \in v$, ses af (ord 2), at $x \subseteq v$, og her er endda $x \subset v$, idet jo $x \in v \setminus x$ ifølge (ord 1).

7.2. SÆTNING. Lad v være et ordinaltal, lad $x \in v$ og lad $y \in x$. Da er $y \in v$ og $y \subset x$.

BEVIS. Da $y \in x \subseteq v$, er $y \in v$. Da elementerne i v ifølge (ord 3) specielt er totalt ordnede ved $\subseteq$, gælder enten $y \subset x$ eller $x \subseteq y$. Og det sidste er udelukket, da vi jo så ville have $y \in x \subseteq y$ og dermed $y \in y$, hvilket er i modstrid med (ord 1), da $y \in v$ ▨

KOROLLAR. (1) For ethvert ordinaltal $v \neq \varnothing$ gælder, at $\varnothing$ er det første element i v.

(2) Hvis v er et ordinaltal, så er også $v^+ = v \cup \{v\}$ et ordinaltal, og $v \subset v^+$.

(3) Hvis v er et ordinaltal, så er hvert element $x \in v$ selv et ordinaltal.

BEVIS. (1): Da v er velordnet og ikke-tom, har v et første element x. Af sætningen (og definitionen på første

element) følger, at intet y kan være element i x. Og så er $x = \emptyset$.

(2): Det er klart, at v er sidste element i $v^+ = v \cup \{v\}$, jfr (Ord 2), og det er nu trivielt at eftervise, at v^+ opfylder betingelserne. At $v \subset v^+$ betyder, at $v \notin v$, og det har vi jo også set.

(3): Lad $x \in v$, da er $x \subseteq v$. Da v er velordnet, er også delmængden x velordnet. Videre gælder for $y \in x$, at $y \notin y$ (idet $y \in v$) og at $y \subseteq x$ (idet endda $y \subset x$), ifølge Sætningen □

7.3. EKSEMPLER. Den tomme mængde $\emptyset$ er et ordinaltal (trivielt). Mængden $\emptyset^+ = \emptyset \cup \{\emptyset\} = \{\emptyset\}$ er et ordinaltal. Mængden $\{\emptyset\}^+ = \{\emptyset, \{\emptyset\}\}$ er et ordinaltal. Mængden $\{\emptyset, \{\emptyset\}\}^+ = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ er et ordinaltal. Osv.

SÆTNING. Lad $(M, <)$ være en velordnet mængde og lad f være afbildningen med domæne M bestemt rekursivt ved

$$f(x) = \operatorname{ran} f/M_{<x}, \quad x \in M.$$

Lad V betegne billedmængden $V := \operatorname{ran} f$. Da er V et ordinaltal, og afbildningen f er en ordensisomorfi

$$f : (M, <) \xrightarrow{\sim} (V, \subset).$$

BEVIS. For alle $x \in M$ gælder

$$f(x) \notin f(x),$$

thi i modsat fald kunne vi betragte det første element $x_0 \in M$ for hvilket $f(x_0) \in f(x_0)$. At $f(x_0) \in f(x_0) = \operatorname{ran} f/M_{<x_0}$ betyder, at der eksisterer $x < x_0$, så at $f(x_0) = f(x)$. Men da $x < x_0$, er $f(x) \notin f(x)$ i modstrid med $f(x) = f(x_0) \notin f(x_0) = f(x)$.

Videre gælder for alle $x \in M$, at $f(x) = \operatorname{ran} f/M_{<x} \subseteq \operatorname{ran} f$, altså

$$f(x) \subseteq V.$$

Elementerne i billedmængden V opfylder altså (ord1) og (ord2). Det er derfor nok at vise, at f er en ordensisomorfi : $(M,<) \to (V,\subset)$, idet $(V,\subset)$ så må være velordnet. Ifølge definitionen på V er f en surjektiv afbildning : $M \to V$, så vi skal vise, at f er (strengt) ordenstro.

Antag derfor, at vi for elementer $x, y \in M$ har $x < y$. Da er $M_{<x} \subset M_{<y}$ og følgelig er

$$f(x) = \operatorname{ran} f/M_{<x} \subseteq \operatorname{ran} f/M_{<y} = f(y),$$

og $f(x) = f(y)$ er udelukket, thi da $x \in M_{<y}$ ville vi i så fald have $f(x) \in \operatorname{ran} f/M_{<y} = f(y) = f(x)$ i modstrid med at $f(x) \notin f(x)$. Altså er

$$f(x) \subset f(y) \quad \blacksquare$$

7.4. INDUKTIONSPRINCIP FOR ORDINALTAL. Lad $p(x)$ være et predikat. Hvis der for ethvert ordinaltal v gælder:

$$\big(\forall x \in v : p(x)\big) \Rightarrow p(v),$$

så er $p(v)$ sandt for ethvert ordinaltal v.

BEVIS. Et givet ordinaltal v er ifølge Korollar 7.2 (2) element i et ordinaltal V (f.eks. $V = v^+$). Det er derfor nok at vise, at $p(v)$ er sandt for ethvert element $v \in V$, og da $(V,\subset)$ er velordnet, kan vi ved transfinit induktion antage, at $p(w)$ er sandt for alle elementer $w \in V$ med $w \subset v$. Men så er ifølge Sætning 7.2 specielt $p(x)$ sandt for hvert element $x \in v$ $\blacksquare$

7.5. SÆTNING. Lad v være et ordinaltal. For hvert ordinaltal u gælder da, at hvis $v \notin u$, så er $u \in v$.

BEVIS. Ifølge induktionsprincippet kan vi antage, at påstanden gælder for alle elementer $x \in v$.

Lad u være et ordinaltal med $v \notin u$. Lad v_0 være det første element i $v \setminus u$. Da er

(1) $\quad v_0 \in v \quad$ og $\quad v_0 \notin u$.

Endvidere er

(2) $\quad v_0 \subseteq u$,

thi er $z \in v_0$, så er $z \in v_0 \subseteq v$ og $z \subset v_0$, så valgt af v_0 sikrer, at $z \in u$.

Det er nok at vise, at $u = v_0$. I det beviset føres indirekte, antages, at $u \neq v_0$. Ifølge (2) gælder så, at $u \notin v_0$. Ganske som ovenfor kan vi da betragte det første element u_0 i $u \setminus v_0$, og vi får

(3) $\quad u_0 \in u$, $u_0 \notin v_0$ og $u_0 \subseteq v_0$.

Ifølge (1) er $v_0 \notin u$ og ifølge (3) er $u_0 \in u$. Vi må derfor have $v_0 \neq u_0$, og dermed $u_0 \subset v_0$ ifølge (3). Specielt er altså

(4) $\quad v_0 \notin u_0$.

På den anden side var $v_0 \in v$, så af (4) og induktionsantagelsen følger, at $u_0 \in v_0$. Og det er i modstrid med (3) ▨

7.6. SAMMENLIGNINGSSÆTNING FOR ORDINALTAL. Lad u og v være ordinaltal. Da indtræffer netop én af mulighederne

$$u \subset v, \quad u = v, \quad v \subset u.$$

Endvidere er følgende betingelser ækvivalente:

(i) $\quad u \subset v$.

(ii) $\quad u \in v$

(iii) $\quad u$ er et ægte afsnit i den velordnede mængde $(v, \subset)$.

BEVIS. Det er klart, at der højst kan indtræffe én af mulighederne. Og er $v \notin u$, så er $u \in v$ ifølge Sætning 7.5, og dermed $u \subset v$.

(i) $\Rightarrow$ (ii): Er $u \subset v$, så er specielt $v \notin u$, og følgelig er $u \in v$ ifølge Sætning 7.5.

(ii) $\Rightarrow$ (iii): Vi viser, at u er det ægte afsnit

$$u = v_{\subset u} = \{ x \in v \mid x \subset u \}.$$

i v. At $u \subseteq v_{\subset u}$ er indholdt af Sætning 7.2, og er omvendt $x \in v_{\subset u}$, så er x et ordinaltal (Korollar 7.2 (3)), så af $x \subset u$ følger $x \in u$, idet vi jo har vist, at (i) $\Rightarrow$ (ii).

(iii) $\Rightarrow$ (i): Trivielt ▨

BEMÆRKNING. Det følger, at i induktionsprincippet 7.4 er induktionsantagelsen, at $p(x)$ er sandt for ethvert ordinaltal $x \subset v$.

7.7. KOROLLAR. Lad u og v være ordinaltal. Da er $u \subseteq v$, hvis og kun hvis $u^+ \subseteq v^+$.

BEVIS. "hvis": Af $u \in u^+ \subseteq v^+ = v \cup \{v\}$ følger, at vi enten har $u = v$ eller $u \in v$ og dermed $u \subseteq v$, og altså i begge tilfælde $u \subseteq v$.

"kun hvis": Er $u = v$, så er $u^+ = v^+$, og er $u \subset v$, så er $u \in v$ og følgelig $u^+ = u \cup \{u\} \subseteq v \subseteq v^+$. ▨

7.8. KOROLLAR. Lad u og v være ordinaltal. Lad f være en ordensbevarende afbildning

$$f: (u, \subset) \to (v, \subset).$$

Da er $u \subseteq v$, og for alle $x \in u$ gælder $x \subseteq f(x)$.

BEVIS. Vi viser først, at der for hvert $x \in u$ gælder

(*) $x \subseteq f(x)$

Da $(u, \subset)$ er velordnet, kan vi antage, at (*) gælder for alle elementer $y \in u$ med $y \subset x$. Er $z \in x$, så er $z \in u$ og $z \subset x$, og følgelig er

$$z \subseteq f(z) \subset f(x),$$

da f er ordenstro. Og af $z \subset f(x)$ følger $z \in f(x)$.

Af $f(x) \in v$ følger $f(x) \subset v$, så af (*) følger, at $x \subset v$. Og så er $x \in v$.

Heraf ses, at $u \subseteq v$ ▨

7.9. KOROLLAR. Enhver mængde af ordinaltal er velordnet (ved $\subset$).

BEVIS. Det er nok at vise, at enhver ikke-tom mængde S af ordinaltal har et første element.

Vælg et element $v_0 \in S$. Hvis $v_0 \cap S = \emptyset$, så gælder for hvert element $v \in S$, at $v \notin v_0$. Og så følger det, at $v_0 \subseteq v$. I dette tilfælde er altså v_0 første element i S.

Hvis $v_0 \cap S \neq \emptyset$, kan vi (da v_0 er velordnet) betragte det første element v_1 i $v_0 \cap S$. Da $v_1 \in v_0$, er $v_1 \subset v_0$. Lad nu $v \in S$. Hvis $v \in v_0$, så er $v \in v_0 \cap S$ og dermed $v_1 \subseteq v$, og hvis $v \notin v_0$, så er $v_0 \subseteq v$ og dermed $v_1 \subset v_0 \subseteq v$. Følgelig er v_1 første element i S ▨

7.10. KOROLLAR. Lad $\mathcal{V}$ være en mængde af ordinaltal. Da er også foreningsmængden $V := \bigcup \mathcal{V}$ et ordinaltal.

BEVIS. Lad $x \in V$. Da findes et element $v \in \mathcal{V}$, så at $x \in v$. Da v er et ordinaltal, gælder:

(1) $x \notin x$, (2) $x \subseteq v \subseteq V$

(3) x er et ordinaltal.

Af (1) og (2) fremgår (ord1) og (ord2), og af (3) fremgår, at V er en mængde af ordinaltal. Følgelig er V velordnet ifølge Korollar 7.9, dvs at også (ord3) er opfyldt ▨

7.11. BURALI-FORTI'S PARADOX. Der findes ikke en mængde, hvori ethvert ordinaltal er element.

BEVIS. Fandtes nemlig en sådan mængde kunne vi ifølge Specifikationsaxiomet betragte mængden Ω af alle ordinaltal. Af Observation 7.1, Korollar 7.3.(2) og Korollar 7.9 følger, at Ω er et ordinaltal. Men så er $\Omega \in \Omega$ i modstrid med Observation 7.1 ▨

OBSERVATION. Hvis $q(x)$ er et prædikat således at der findes et ordinaltal v_0, så at $q(v_0)$ gælder, så findes også et første ordinaltal v_1, så at $q(v)$ gælder, thi ordinaltallene $v \subseteq v_0$ udgør en mængde (nemlig mængden v_0^+), så heriblandt findes (Korollar 7.9) et første element v_1, så at $q(v_1)$ gælder. Hvis w er et ordinaltal, så at $q(w)$ gælder, så er enten $w \subseteq v_0$, og dermed $v_1 \subseteq w$ ifølge valget af v_1, eller $w \notin v_0$, og så er $v_0 \subset w$ og dermed også $v_1 \subseteq w$.

BEMÆRKNING. Det er naturligt at udtrykke dette ved at sige, at ordinaltallene er velordnede (ved inklusion). Det første ordinaltal er ordinaltallet $\varnothing$. Der er intet sidste ordinaltal, thi for hvert ordinaltal v er $v \subset v^+$.

7.12. Lad $(M, <)$ være en velordnet mængde. Af Sætning 6.3

følger, at $(M,<)$ er ordensisomorf med et ordinaltal v. Og af Korollar 7.8 følger, at $(M,<)$ ikke kan være ordensisomorf med andre ordinaltal, thi er $(M,<)$ ordensisomorf med ordinaltallet w, så får vi en ordensisomorfi : $(W,\subset) \xrightarrow{\sim} (M,<) \xrightarrow{\sim} (V,\subset)$, hvoraf $w = v$.

DEFINITION. Det entydigt bestemte ordinaltal, der er ordensisomorft med den velordnede mængde $(M,<)$ kaldes <u>ordinaltallet</u> for $(M,<)$ og betegnes $\mathrm{ord}(M,<)$ (eller blot $\mathrm{ord}(M)$, hvis ordningen i M er underforstået.)

SÆTNING. Lad $(M,<)$ og $(N,<)$ være velordnede mængder. Da er $\mathrm{ord}(N,<) \leq \mathrm{ord}(M,<)$, hvis og kun hvis der findes en ordenstro afbildning : $(N,<) \to (M,<)$. Endvidere er $\mathrm{ord}(N,<) \subset \mathrm{ord}(M,<)$, hvis og kun hvis $(N,<)$ er ordensisomorf med et ægte afsnit af $(M,<)$.

BEVIS. Brug Korollar 7.8 (og 7.6) □

7.13. En velordnet mængde er ifølge det foregående ordensisomorf med et ordinaltal og dermed specielt ækvipotent med et ordinaltal. Omvendt er det klart, at en mængde M kan velordnes, hvis den er ækvipotent med et ordinaltal v, thi ved en bijektiv afbildning $f : M \to v$ kan vi overføre velordningen $\subset$ i v til en velordning $<$ i M (defineret ved: $x < y$, hvis $f(x) \subset f(y)$).

SÆTNING. Lad A være en mængde. Da findes en mængde, hvori ethvert ordinaltal $v \lesssim A$ er element.

BEVIS. At $v \lesssim A$ betyder som bekendt, at der findes en injektiv afbildning : $v \to A$. Og det gælder

netop når der findes et par $(M,<)$ bestående af en delmængde $M \subseteq A$ og en velordning $<$ i M, så at

$$v = ord(M,<).$$

Da disse par $(M,<)$ udgør en mængde $\mathcal{V}$ (nemlig en delmængde $\mathcal{V} \subseteq \mathcal{P}(A) \times \mathcal{P}(A \times A)$), følger påstanden af Udskiftningsaxiomet 1.6 ved at betragte predikatet

$$a \in \mathcal{V} \wedge ord(a) = y. \quad \blacksquare$$

KOROLLAR. For enhver mængde A findes et ordinaltal w, som ikke kan afbildes injektivt ind i A.
BEVIS. Den i sætningen nævnte mængde kan ifølge Paradoxet 7.11 ikke omfatte alle ordinaltal. $\blacksquare$

7.14. DEFINITION. En mængde α kaldes et <u>kardinaltal</u>, hvis α er et ordinaltal, og hvis der for hvert ordinaltal $u \subset \alpha$ gælder $u < \alpha$ (altså at u ikke er ækvipotent med α).

OBSERVATION 1. Kardinaltallene er velordnede (ved $\subset$) og den tomme mængde $\varnothing$ er det første kardinaltal. thi kardinaltallene er specielt ordinaltal, og $\varnothing$ er øjensynlig et kardinaltal.

OBSERVATION 2. Ethvert ordinaltal v er ækvipotent med et kardinaltal,
nemlig med det første blandt de ordinaltal, der er ækvipotente med v.

OBSERVATION 3. For ethvert ordinaltal v findes et kardinaltal α, så at $v \subset \alpha$,
thi ifølge korollar 7.13 findes et ordinaltal og dermed også et kardinaltal α, der ikke kan afbildes injektivt ind i v. Specielt er $\alpha \subseteq v$ udelukket, og så må vi have $v \subset \alpha$.

OBSERVATION 4. Kardinaltallene udgør ikke en mængde,
thi i modsat fald kunne vi betragte foreningsmængden af alle kardinaltal, og denne mængde ville ifølge Observation 3 omfatte ethvert ordinaltal i modstrid med Paradoxet 7.11.

7.15. DEFINITION. Lad A være en mængde. Ved <u>kardinaltallet</u> for A forstås mængden

$$\operatorname{card} A = \{ v \mid v \text{ er et ordinaltal og } v < A \}.$$

BEMÆRKNING. Af Sætning 7.8 følger, at prædikatet "v er et ordinaltal og $v < A$" er mængdebestemmende, så $\operatorname{card}(A)$ er en veldefineret mængde. At denne mængde er et kardinaltal, er indholdet af følgende:

SÆTNING. For enhver mængde A er $\operatorname{card}(A)$ et kardinaltal.
BEVIS. Lad os først vise, at $\alpha := \operatorname{card}(A)$ er et ordinaltal. Da elementerne i α er ordinaltal, gælder (ord 1) ifølge Observation 7.1, og (ord 3) ifølge Korollar 7.9. For at vise (ord 2) skal vi vise for hvert element $v \in \alpha$, at $v \subseteq \alpha$. Lad derfor $x \in v$. Da er x et ordinaltal, og $x \subset v$. Af $x \subseteq v$ og $v < A$ følger imidlertid $x < A$ (Bernstein's ækvivalenssætning 2.3). Og så er $x \in \alpha$.

Hvis α ikke var et ordinaltal, ville der findes et ordinaltal $v \subset \alpha$, med $\alpha \bar{\sim} v$. Af $v \subset \alpha$ følger $v \in \alpha$ og dermed $v < A$. Da $\alpha \bar{\sim} v$, følger så at også $\alpha < A$. Men så er $\alpha \in \alpha$ i modstrid med at α var et ordinaltal ▨

7.16. SÆTNING. For en mængde A er følgende betingelser ækvivalente:

(i) A kan velordnes.

(ii) A er ækvipotent med et ordinaltal.

(iii) $\mathrm{card}(A) \lesssim A$

(iv) $A \approx \mathrm{card}(A)$

(v) $A \lesssim \mathrm{card}(A)$

(vi) A er ækvipotent med en delmængde af et ordinaltal.

BEVIS. (i) $\Rightarrow$ (ii) ifølge Sætning 7.3.

(ii) $\Rightarrow$ (iii): Antag, at $\nu \approx A$, hvor ν er et ordinaltal. Da er $\nu < A$ udelukket, så $\nu \notin \mathrm{card}(A)$. Men så er $\mathrm{card}(A) \subseteq \nu \approx A$, og dermed $\mathrm{card}(A) \lesssim A$.

(iii) $\Rightarrow$ (iv): Da $\mathrm{card}(A) \notin \mathrm{card}(A)$, er $\mathrm{card}A < A$ udelukket.

(iv) $\Rightarrow$ (v) er trivielt. (v) $\Rightarrow$ (vi) er trivielt.

(vi) $\Rightarrow$ (i): trivielt, da et ordinaltal er velordnet (ved $\subset$). ▨

7.17. For mængder A og B er det klart, at vi har:

$$A \lesssim B \Rightarrow \mathrm{card}(A) \subseteq \mathrm{card}(B),$$

$$A \approx B \Rightarrow \mathrm{card}(A) = \mathrm{card}(B).$$

Vi kan ikke umiddelbart slutte de omvendte implikationer. Herom gælder:

SÆTNING. Hvert af følgende udsagn er ækvivalent med udvalgsaxiomet:

(i) Enhver mængde A kan velordnes.

(ii) Enhver mængde A er ækvipotent med sit kardinaltal $\mathrm{card}(A)$.

(iii) Enhver mængde A kan sammenlignes med sit kardinaltal $\mathrm{card}(A)$.

(iv) Vilkårlige to mængder A og B kan sammenlignes.

(v) For vilkårlige to mængder A og B gælder:

$$\mathrm{card}(A) = \mathrm{card}(B) \Rightarrow A \approx B.$$

BEVIS. (i) er velordningssætningen og derfor ækvivalent med udvalgsaxiomet. Ifølge den foregående sætning er (i), (ii) og (iii) ækvivalente. Det er derfor nok at vise,

at (ii) $\Rightarrow$ (iv) $\Rightarrow$ (iii) og (ii) $\Leftrightarrow$ (v).

(ii) $\Rightarrow$ (iv): Sættes $\alpha = \mathrm{card}(A)$ og $\beta = \mathrm{card}(B)$, er $A \sim \alpha$ og $B \sim \beta$. Det er derfor nok at vise, at α og β kan sammenlignes. Og det følger af at α og β er ordinaltal.

(iv) $\Rightarrow$ (iii) er klart.

(ii) $\Rightarrow$ (v): Af $A \sim \mathrm{card}(A) = \mathrm{card}(B) \sim B$ fås $A \sim B$.

(v) $\Rightarrow$ (ii): Da $\mathrm{card}(A)$ er et kardinaltal, er $\mathrm{card}(A) = \mathrm{card}\big(\mathrm{card}(A)\big)$. Og heraf fås $A \sim \mathrm{card}(A)$ ▨

BEMÆRKNING. Antages udvalgsaxiomet følger det, at spørgsmål om mægtighed mellem mængder spejles i simple relationer mellem de tilsvarende kardinaltal. Og ud fra "mængdeoperationerne" kan man definere "kompositioner" blandt kardinaltallene. Er α og β kardinaltal, defineres f.eks.

produktet ved $\alpha \cdot \beta := \mathrm{card}(\alpha \times \beta)$,

potensen ved $\exp_\alpha(\beta) := \mathrm{card}(\alpha^\beta)$

[α^β betegner som bekendt mængden af afbildninger: $\beta \to \alpha$]

og summen ved $\alpha + \beta := \mathrm{card}(\alpha \vee \beta)$.

[$\alpha \vee \beta$ betegner her den disjunkte forening af α og β; er $(F_i)_{i \in I}$ en familie af mængder, kan den disjunkte forening defineres som delmængden af $\left(\bigcup_{i \in I} F_i\right) \times I$ bestående af de par (x,i) for hvilke $x \in F_i$].

Vi vil ikke her gå nærmere ind på de regneregler, der gælder for disse kompositioner.

7.18. DEFINITION. En mængde n kaldes et naturligt tal, hvis n er et ordinaltal, og hvis der desuden gælder:

(ord 3°): Elementerne i n er velordnet ved $\supseteq$.

BEMÆRKNING. Under ét udsiger betingelserne (ord 3) og (ord 3°), at mht inklusion $\subseteq$ har enhver ikke-tom delmængde $S \subseteq n$ et første element og et sidste element.

OBSERVATION 1. De naturlige tal er velordnede (ved $\subset$) og den tomme mængde $\varnothing$ er det første naturlige tal, thi de naturlige tal er specielt ordinaltal, og $\varnothing$ er øjensynlig et naturligt tal.

OBSERVATION 2. For hvert naturligt tal n er også n^+ et naturligt tal, thi $n^+ = n \cup \{n\}$ er et ordinaltal med n som sidste element.

OBSERVATION 3. Er n et naturligt tal, så er hvert element $x \in n$ selv et naturligt tal, og hvert ordinaltal $v \subseteq n$ er et naturligt tal, thi den første påstand følger af den anden, og den anden følger af at betingelsen (ord 3°) nedarves fra n til delmængden v.

OBSERVATION 4. For hvert naturligt tal $n \neq \varnothing$ er $\varnothing$ det første element i n, og $n = m^+$, hvor m er det sidste element i n, thi den første påstand gælder generelt for ordinaltal $\neq \varnothing$, og den sidste gælder øjensynlig for ordinaltal, der har et sidste element. Og det har n ifølge (ord 3°).

7.19. Svarende til at de naturlige tal er velordnede gælder princippet om transfinit induktion, der for de naturlige tal også kaldes <u>princippet om fuldstændig induktion</u>

Vi noterer også følgende specielle
INDUKTIONSPRINCIP FOR NATURLIGE TAL. Lad $p(x)$ være et prædikat. Hvis $p(\emptyset)$ er sandt, og hvis der for hvert naturligt tal n gælder:

$$p(n) \Rightarrow p(n^+),$$

så er $p(n)$ sandt for ethvert naturligt tal n.
BEVIS. I modsat fald kunne vi betragte det første naturlige tal n, for hvilket $p(n)$ er falsk. Da vi har antaget $p(\emptyset)$, er $n \neq \emptyset$, og så har n formen $n = m^+$ med et naturligt tal m. Her er $m \subset n$, så valget af n sikrer $p(m)$. Men så gælder også $p(m^+)$, dvs $p(n)$, i modstrid med at $p(n)$ var falsk ▨

7.20. SÆTNING. Lad n være et naturligt tal og lad u være et ordinaltal. Lad f være en ordenstro afbildning

$$f : (u, \subset) \to (n, \subset).$$

Da er $u \subseteq n$ og for alle $x \in u$ er $x \subseteq f(x)$. Ordinaltallet u er selv et naturligt tal, og hvis $u = n$, så er f den identiske afbildning.
BEVIS. Den første påstand er indeholdt i korollar 7.9. Da u er et ordinaltal, følger af $u \subseteq n$, at u er et naturligt tal. Hvis $u = n$, og f ikke var den identiske afbildning kunne vi betragte det sidste element $y \in n$, så at $y \subset f(y)$. Valget af y sikrer så, at $f(f(y)) = f(y)$, og da f er ordenstro, får vi modstriden $f(y) \subset f(f(y)) = f(y)$ ▨

KOROLLAR. Lad n være et naturligt tal og lad $A \subset n$ være en ægte delmængde. Da er A ækvipotent med et naturligt tal $\subset n$.
BEVIS. Som delmængde af den velordnede mængde n er A selv velordnet, så med $u := \mathrm{ord}(A)$ har vi en ordensisomorfi $(u, \subset) \to (A, \subset)$. Sammensættes med inklusionsafbild-

mingen $A \to n$ fås en ordenstro afbildning : $u \to n$, som ikke er surjektiv, da A var en ægte delmængde af n. Nu er A ækvipotent med u og ifølge sætningen er u et naturligt tal og $u \subset n$ ▨

7.21. SÆTNING. Lad n være et naturligt tal. Da er n et kardinaltal og hver injektiv afbildning $f: n \to n$ er surjektiv (og dermed bijektiv).

BEVIS. Den første påstand er en konsekvens af den anden, thi er v et ordinaltal, der ikke er et kardinaltal, findes en bijektiv afbildning : $v \to u$, hvor $u \subset v$, og så fås ved sammensætning en injektiv afbildning : $v \to u \hookrightarrow v$, der ikke er surjektiv.

Var den anden påstand gal, kunne vi betragte det mindste naturlige tal n, for hvilket der findes en afbildning $f: n \to n$, der er injektiv, men ikke surjektiv. Da f er injektiv, er n ækvipotent med billedmængden $A \subseteq n$, og da f ikke er surjektiv, er A en ægte delmængde af n, og følgelig er (Korollar 7.20) A ækvipotent med et naturligt tal $u \subset n$. Da u er ækvipotent med n findes en afbildning : $u \to u$, der er injektiv, men ikke surjektiv, og da $u \subset n$, er det i modstrid med valget af n ▨

7.22. DEFINITION. En ordning $<$ i en mængde A kaldes endelig, hvis enhver ikke-tom delmængde $S \subseteq A$ har et første element og et sidste element (mht $<$).

En mængde A kaldes endelig, hvis der eksisterer en endelig ordning i A.

OBSERVATION. Et ordinaltal n er et naturligt tal netop når ordningen $\subset$ i n er endelig,

thi betingelserne (ord 3) og (ord 3°) udsiger netop at $\subset$ er en endelig ordning.

SÆTNING. For en mængde A er følgende betingelser ækvivalente:
(i) A er en endelig mængde
(ii) A er ækvipotent med et naturligt tal.
(iii) $\mathrm{card}(A)$ er et naturligt tal.
BEVIS. (i) $\Rightarrow$ (ii): Lad $<$ være en endelig ordning i A. Da er $(A,<)$ specielt velordnet, så $(A,<)$ er ordensisomorf med $(n,\subset)$, hvor $n = \mathrm{ord}(A,<)$. Det følger, at ordningen $\subset$ i n er endelig, så n er et naturligt tal, ækvipotent med A.
(ii) $\Rightarrow$ (i): Ved en bijektiv afbildning $A \to n$ svarer ordningen $\subset$ i n til en ordning $<$ i A, og hvis $\subset$ er endelig, bliver $<$ endelig.
(ii) $\Rightarrow$ (iii): Antag $A \bar{\sim} n$, hvor n er et naturligt tal. Da er $A \bar{\sim} \mathrm{card}(A)$ (Sætning 7.16), og da $\mathrm{card}(A) \subseteq n$, er $\mathrm{card}(A)$ et naturligt tal [i øvrigt er $\mathrm{card}(A) = n$ ifølge Sætning 7.21)]
(iii) $\Rightarrow$ (ii): Da påstanden er triviel, hvis $\mathrm{card}(A) = \varnothing$, kan vi antage, at $n := \mathrm{card}(A) \neq \varnothing$, og dermed (Observation 4), at $\mathrm{card}(A) = m^+$, hvor m er et naturligt tal. Da $m \in m^+ = \mathrm{card}(A)$, er $m < A$, så der findes en injektiv afbildning $g: m \to A$. Da $m < A$, kan g ikke være surjektiv, så vi kan udvide g til en injektiv afbildning $: m^+ \to A$. Men så er A specielt sammenlignelig med $m^+ = \mathrm{card}(A)$ og dermed ækvipotent med $\mathrm{card}(A)$ ifølge Sætning 7.16 ▨

7.23. DIRICHLET'S SKUFFEPRINCIP.

(1) Lad A være en endelig mængde. Da er enhver injektiv afbildning $: A \to A$ surjektiv.

(2) Lad $f: B \to A$ være en afbildning, der er injektiv, men ikke surjektiv. Hvis A er endelig, så er $\mathrm{card}(B) \subset \mathrm{card}(A)$.

(3). Lad $f: B \to A$ være en afbildning. Hvis A er endelig, og $\mathrm{card}(A) \subset \mathrm{card}(B)$, så er f ikke injektiv.

BEMÆRKNING. Udsagnet (3), der er en ofte anvendt version af skuffeprincippet, er kun medtaget af formelle grunde i denne formulering. Det gælder øjensynlig uden antagelse af at A er endelig, thi var f injektiv, ville $B \lesssim A$, og så er $\mathrm{card}(B) \subseteq \mathrm{card}(A)$ i modstrid med antagelsen.
Det er også klart, at (1) følger af (2), så det er nok at give et

BEVIS FOR (2). Da A er endelig, er A ækvipotent med et naturligt tal n, så vi kan antage, at $A = n = \mathrm{card}(A)$ (Sætning 7.21). Da B er ækvipotent med billedmængden ved den injektive afbildning f, kan vi antage, at $B \subset n$ er en ægte delmængde. Af Korollar 7.20 følger, at B er ækvipotent med et naturligt tal $u \subset n$. Men så er $u = \mathrm{card}(B)$ ifølge Sætning 7.21. Altså $\mathrm{card}(B) = u \subset n = \mathrm{card}(A)$ ▨

7.24. BEMÆRKNING. Antages det, at der findes en mængde hvori ethvert naturligt tal er element, kan vi ifølge Specifikationsaxiomet betragte mængden $\tilde{\mathbb{N}}$ af naturlige tal. Af det foregående følger:
(1) Mængden $\tilde{\mathbb{N}}$ er velordnet ved ordningen $\subset$. Det første element i $\tilde{\mathbb{N}}$ er den tomme mængde $\varnothing$ (7.18.1)
(2) For hvert element $n \in \tilde{\mathbb{N}}$ er også $n^+ \in \tilde{\mathbb{N}}$. Hvert element $m \neq \varnothing$ i $\tilde{\mathbb{N}}$ har formen $m = n^+$, hvor $n \in \tilde{\mathbb{N}}$ (7.18.2 og 4).
(3) Den ved $\varepsilon(n) := n^+$ definerede afbildning $\varepsilon: \tilde{\mathbb{N}} \to \tilde{\mathbb{N}}$ er injektiv, og $\varnothing \notin \varepsilon(\mathbb{N})$ (7.7)
(4) Hvis en delmængde $S \subseteq \tilde{\mathbb{N}}$ opfylder: $\varnothing \in S$ og $\varepsilon(S) \subseteq S$, så er $S = \tilde{\mathbb{N}}$ (7.19).

Af (3) og (4) fremgår specielt, at $(\tilde{\mathbb{N}}, \varnothing, \varepsilon)$ er et såkaldt Peano-tripel (jfr. kapitlet "Naturlige tal" i Talsystemets opbygning).

7.25 Om ovenstående antagelse gælder yderligere følgende:

SÆTNING. Følgende eksistensudsagn er ækvivalente:

(i) Der eksisterer en ikke-tom partielt ordnet mængde $(S, <)$ uden sidste element.

(ii) Der eksisterer en ikke-tom mængde $\mathcal{N}$ af mængder, så at der for hvert $a \in \mathcal{N}$ findes $b \in \mathcal{N}$ med $a \subset b$.

(iii) Der eksister en mængde $\mathcal{M}$ af mængder, så at

$$\emptyset \in \mathcal{M} \quad \text{og} \quad a \in \mathcal{M} \Rightarrow a \cup \{a\} \in \mathcal{M}.$$

(iv) Der eksisterer et naturligt tripel (N, n_1, ε).

(v) Der eksisterer et Peano-tripel (Q, q_1, φ).

(vi) Der eksisterer et par (P, f) bestående af en mængde P og en afbildning $f: P \to P$, der er injektiv og ikke surjektiv.

(vii) Der eksister en mængde U, der ikke er endelig.

(viii) Der eksisterer et ordinaltal u, der ikke er et naturligt tal.

(ix) Der eksisterer en mængde, hvori ethvert naturligt tal er element.

BEMÆRKNINGER. Udsagnet (ii) er Uendelighedsaxiomet 1.8. I stedet for dette kan altså vælges ethvert af de øvrige udsagn. Men udsagnet (ii) er i en vis forstand det enkleste, idet der i formuleringen kun indgår det primitive begreb "element i", og ikke nogen af de begreber, der er introduceret i forbindelse med de øvrige ZF-axiomer. [Angående definitionen af naturligt tripel og Peano-tripel henvises i øvrigt til kapitlet "Naturlige tal" i Talsystemets opbygning].

Antages (ix) eksisterer ifølge Bemærkning 7.24 mængden $\tilde{\mathbb{N}}$ af naturlige tal. Det er ikke svært at vise, at $\tilde{\mathbb{N}}$ (med $\emptyset$ som udvalgt element og $n \mapsto n^+$ som afbildning: $\tilde{\mathbb{N}} \to \tilde{\mathbb{N}}$) opfylder de krav der stilles i (i) - (viii).

Vi vil dog her givet et cyklisk bevis for ækvivalensen efter følgende skema:

$$(i) \Rightarrow (ii) \Rightarrow (iii) \Rightarrow (ix) \Rightarrow (iv) \Rightarrow (v) \Rightarrow (vi) \Rightarrow (vii) \Rightarrow (viii) \Rightarrow (i).$$

BEVIS. (i) $\Rightarrow$ (ii): Mængden $\mathcal{N}$ af delmængder $X \subseteq S$ af formen $X = S_{\leqslant a}$, $a \in S$, vil opfylde kravet.

(ii) $\Rightarrow$ (iii): Ifølge Sætning 7.13 (og Specifikationsaxiomet) kan vi betragte mængden $\mathcal{M}$ af de naturlige tal n, for hvilke der findes en ordenstro afbildning $: (n, \subset) \to (\mathcal{N}, \subset)$. Det er klart, at $\emptyset \in \mathcal{M}$, så vi vil vise, at når $n \in \mathcal{M}$, så er også $n^+ \in \mathcal{M}$. Vi antager altså, at $f : (n, \subset) \to (\mathcal{N}, \subset)$ er ordenstro, og skal vise, at der findes en ordenstro afbildning $: (n^+, \subset) \to (\mathcal{N}, \subset)$. Hvis $n = \emptyset$, så har $n^+ = \{\emptyset\}$ ét element, og påstanden følger af at $\mathcal{N} \neq \emptyset$. Hvis $n \neq \emptyset$, så kan vi i n betragte det sidste element $=: p$. Sættes $a = f(p) \in \mathcal{N}$ findes ifølge antagelsen $b \in \mathcal{N}$ med $a \subset b$. Vi har $n^+ = n \cup \{n\}$, og ved definitionen $\tilde{f}(n) = b$ udvides ojensynlig $f : n \to \mathcal{N}$, til en ordenstro afbildning $\tilde{f} : (n^+, \subset) \to (\mathcal{N}, \subset)$.

(iii) $\Rightarrow$ (ix): Ifølge Induktionsprincippet 7.19 er ethvert naturligt tal element i $\mathcal{M}$.

(ix) $\Rightarrow$ (iv): Ifølge Bemærkning 7.19 kan vi betragte $(\tilde{\mathbb{N}}, \emptyset, \varepsilon)$, hvor $\tilde{\mathbb{N}}$ er mængden af naturlige tal og $\varepsilon(n) = n^+$. Da $\tilde{\mathbb{N}}$ er velordnet med $\emptyset$ som første element følger det af Rekursionssætningen 4.7 (jfr. Eksempel 4.7), at $(\tilde{\mathbb{N}}, \emptyset, \varepsilon)$ er et naturligt tripel.

(iv) $\Rightarrow$ (v): (N, n_1, ε) er et Peano-tripel, jfr. "Naturlige tal".

(v) $\Rightarrow$ (vi): φ er injektiv og ikke surjektiv, da $q_1 \notin \varphi(P)$.

(vi) $\Rightarrow$ (vii): P er ikke endelig ifølge Skuffe-princippet 7.23 (1).

(vii) $\Rightarrow$ (viii): $\mathrm{card}(U)$ er et ordinaltal, der ikke er et naturligt tal (Sætning 7.22).

(viii) $\Rightarrow$ (i): Da ordningen $\subset$ i u ikke er endelig, har u en ikke-tom delmængde uden sidste element. ▨

7.26. Vi har nu begrundet, hvorledes Uendelighedsaxiomet 1.8 (eller en af de ækvivalente former nævnt i Sætning 7.25) ikke alene tillader at vise eksistensen af mængde, hvis elementer har de egenskaber, vi synes, at sædvanlige naturlige tal bør have, men at axiomet faktisk tillader os at udvælge en ganske bestemt sådan mængde, nemlig mængden $\tilde{\mathbb{N}}$. Elementerne i $\tilde{\mathbb{N}}$ kaldes også de <u>endelige ordinaltal</u>. Bemærk, at mængden $\tilde{\mathbb{N}}$ selv er et ordinaltal, jfr Observation 7.18.1 og 3. Når vi tænker på $\tilde{\mathbb{N}}$ som ordinaltal, skrives ofte

$$\omega := \tilde{\mathbb{N}}$$

Ordinaltallet ω er ikke endeligt (Observation 7.1), og det er endda det første blandt de ikke-endelige, jfr Sammenligningssætning 7.6. Da mængden $\tilde{\mathbb{N}}$ ikke er endelig (Dirichlet's Skuffeprincip og Bemærkning 7.24(3)) er ordinaltallet ω endda et kardinaltal. Opfattet sådan betegnes det også $\aleph_0$, altså

$$\tilde{\mathbb{N}} = \omega = \aleph_0.$$

Af Observation 7.14.1 og 3 følger, at der findes et mindste kardinaltal $\aleph_1 \supset \aleph_0$, et mindste kardinaltal $\aleph_2 \supset \aleph_1$, osv. Nu kan vi (rekursion) definere kardinaltal $\aleph_n$, $n \in \tilde{\mathbb{N}}$ og indse eksistensen af et mindste kardinaltal $\aleph_\omega \supset \aleph_n$ for alle $n \in \tilde{\mathbb{N}}$. Osv.

BEMÆRKNING. Kardinaltallet $\aleph_1$ har øjensynlig som velordnet mængde den i Eksempel 4.9 nævnte egenskab. Det er således ikke nødvendigt at indrage udvalgsaxiomet for at indse eksistensen af en sådan mængde.

7.27. Sædvanligvis antages i matematik, at Uendelighedsaxiomet 1.8 gælder. Vi har så til rådighed mængden $\tilde{\mathbb{N}}$ af naturlige tal og kan herudfra opbygge talsystemet og dit grundlag, hvorpå (næsten) al matematik hviler. Vi behøver ikke at tænke på naturlige tal som specielle mængder, vi skriver

$$0 := \varnothing,\quad 1 := 0^+,\quad 2 := 1^+,\quad 3 := 2^+ \quad \text{osv},$$

og for naturlige tal n, m

$$n < m,$$

i stedet for $n \subset m$.

Det er lidt en smagssag, hvorvidt tallet 0 medregnes som naturligt tal. I overensstemmelse med den notation, som hyppigst anvendes skriver vi i hvert fald

$$\mathbb{N} := \tilde{\mathbb{N}} \setminus \{0\}.$$

Udvalgsaxiomet (U) 1.11 spiller derimod en mere tvivlsom rolle. Man må imidlertid gøre sig klart, at man også i mere uskyldige (tællelige) situationer kan have brug for at foretage valg ved hjælp af en afbildning. Herom gælder:

SÆTNING. Antag at ZF-axiomerne (incl. uendelighedsaxiomet) gælder, og betragt følgende eksistensudsagn:

<u>Afhængige valg (A)</u>: Lad X være en ikke-tom mængde med en relation R, som opfylder, at der for hvert $x \in X$ findes $x' \in X$ med $x R x'$. Da findes en afbildning $f : \tilde{\mathbb{N}} \to X$ således at $f_n \, R \, f_{n^+}$ for alle $n \in \tilde{\mathbb{N}}$.

<u>Numerable valg (B)</u>: Lad $(Y_n)_{n \in \tilde{\mathbb{N}}}$ være en familie af ikke-tomme mængder. Da findes en afbildning $g : \tilde{\mathbb{N}} \to \bigcup_{n \in \tilde{\mathbb{N}}} Y_n$, således at $g_n \in Y_n$ for alle $n \in \tilde{\mathbb{N}}$.

<u>Numerable delmængder (C)</u>: Lad Z være en ikke-endelig mængde. Da findes en injektiv afbildning $h : \tilde{\mathbb{N}} \to Z$.

Dirichlet's princip (𝔇): Lad U være en ikke-endelig mængde. Da findes en afbildning $\varphi: U \to U$ som er injektiv, men ikke surjektiv.

Der gælder da, at

$$(\mathfrak{U}) \Rightarrow (\mathfrak{A}) \Rightarrow (\mathfrak{B}) \Rightarrow (\mathfrak{C}) \Leftrightarrow (\mathfrak{D}).$$

BEMÆRKNING 1. Det fremgår, at disse udsagn er svækkede former af udvalgsaxiomet ($\mathfrak{U}$): Dersom ($\mathfrak{U}$) antages, gælder også ($\mathfrak{A}$), ($\mathfrak{B}$), ($\mathfrak{C}$) og ($\mathfrak{D}$). Men det fremhæves, at ingen af disse udsagn kan bevises alene ud fra ZF-axiomerne. Det er sædvane i matematiske beviser ikke at fremhæve, at udsagnet ($\mathfrak{A}$) (eller ($\mathfrak{B}$) eller ($\mathfrak{C}$)) indgår. I den forstand optræder altså ($\mathfrak{A}$) som et axiom på linie med ZF-axiomerne.

BEMÆRKNING 2. Dirichlet's skuffeprincip (jfr. 7.23 (1)), som vi jo har bevist, udsiger, at hvis der findes en injektiv, ikke-surjektiv afbildning $U \to U$ så er U ikke endelig. Udsagnet ($\mathfrak{D}$) er altså, at det omvendte også gælder.

BEVIS FOR SÆTNINGEN. ($\mathfrak{U}$) $\Rightarrow$ ($\mathfrak{A}$): Lad u være en udvalgsfunktion på X. I følge antagelsen er

$$x \longmapsto \varphi(x) := u(\{x' \in X \mid x R x'\})$$

en veldefineret afbildning $\varphi: X \to X$. Sættes $x_0 = u(X)$, kan vi induktivt definere $f: \tilde{\mathbb{N}} \to X$ ved $f(0) = x_0$, $f(n^+) = \varphi(f(n))$. Og øjensynlig er $f(n)\, R\, f(n^+)$ for alle $n \in \tilde{\mathbb{N}}$.

($\mathfrak{A}$) $\Rightarrow$ ($\mathfrak{B}$): Lad X være mængden af par (A, g) bestående af ægte afsnit $A \subset \tilde{\mathbb{N}}$ og en afbildning $g: A \to \bigcup_n Y_n$ som opfylder $g(i) \in Y_i$ for $i \in A$.

Definerer i X relationen R ved

$$(A, g)\ R\ (B, h) \Leftrightarrow A \subset B \wedge h/A = g$$

er det let at se, at den i ($\mathfrak{A}$) nævnte betingelse

er opfyldt. Der findes derfor en afbildning $: \tilde{\mathbb{N}} \to X$

$$n \longmapsto (A_n, g_n)$$

så at

$$A_n \subset A_{n^+} \quad \text{og} \quad g_{n^+} / A_n = g_n \,, \quad n \in \tilde{\mathbb{N}}.$$

Af dit første følger let (induktion), at $n \in A_{n^+}$ for alle n, og så defineres ved

$$n \longmapsto g_{n^+}(n)$$

en afbildning $g : \tilde{\mathbb{N}} \to \bigcup_i Y_i$ som opfylder dit ønskede.

(B) $\Rightarrow$ (C): Da Z ikke er endelig findes for hvert $n \in \tilde{\mathbb{N}}$ injektive afbildninger $: n \to Z$. Det følger, at vi kan finde en afbildning $: n \longmapsto h_n$, så at h_n er en injektiv afbildning $h_n : \tilde{\mathbb{N}}_{<n} = n \to Z$ for hvert $n \in \tilde{\mathbb{N}}$. Herudfra er det nemt rekursivt at definere en injektiv afbildning $: \tilde{\mathbb{N}} \to Z$ som ønsket.

(C) $\Rightarrow$ (D): Vi kan tænke på U som en disjunkt forening $U = \tilde{\mathbb{N}} \cup W$. Afbildningen $\varphi : U \to U$ bestemt ved

$$\varphi(u) = \begin{cases} u^+ & \text{når } u \in \tilde{\mathbb{N}} \\ u & \text{når } u \in W \end{cases}$$

opfylder da dit ønskede.

(D) $\Rightarrow$ (C): Vælg $\varphi : Z \to Z$, injektiv og ikke surjektiv og vælg $z_0 \in Z \setminus \varphi(Z)$. Afbildningen $h : \tilde{\mathbb{N}} \to Z$ defineret induktivt ved $h(0) = z_0$, $h(n^+) = \varphi(h(n))$ opfylder da dit ønskede. □

MODULER

1. Modulbegrebet. 1.1-2: Definitioner. 1.3: $\mathbb{Z}$-moduler. 1.4: venstre- og højre. 1.5: Nulmodulen. 1.6: Λ_s og Λ_d. 1.7: Λ_s^n. 1.8: $\mathrm{Mat}_{m,p}(\Lambda)$. 1.9: Homotetier. 1.10: Λ-homomorfi og endomorfi. 1.11: $\mathrm{Hom}_\Lambda(\Lambda_s^m, \Lambda_s^p)$.

2. Undermodul. Kvotientmodul. 2.1-2: Definitioner. 2.3: Udvidelsessætning. 2.4: Isomorfisætning. 2.5: Triviel undermodul. 2.6: Venstreideal. 2.7-8: Undermodul frembragt af delmængde. Cyklisk undermodul. 2.9-10: Annullator.

3. Noether's isomorfisætninger. 3.1-2: Noether's anden isomorfisætning. 3.3: Noether's første isomorfisætning.

4. Direkte sum af moduler. Basis. 4.1-5: Direkte sum. 4.6-8: Komplement til undermodul. 4.9-10: Frembringersystem. Frit system. Basis. 4.11: Fri modul. 4.12: Homomorfier fra en fri modul. 4.13: Observation. 4.14: Sætning. 4.15: Sætning om fri kvotient. 4.16: Uendelige systemer. 4.17: Konstruktion af fri modul. 4.18: Minimalt frembringersystem. Maksimalt frit system. 4.19-21: Baser i vektorrum.

5. Simple moduler. 5.1: Definition. 5.2: Karakterisering af simpel modul. 5.3: Karakterisering af skævlegeme. 5.4: Simple $\mathbb{Z}$-moduler. 5.5: Maksimal undermodul. 5.6: Simpel kvotient.

6. Moduler af endelig længde. 6.1: Kæder i en modul. 6.2: Eksempler. 6.3: Jordan's sætning. 6.4: Hölder's sætning. Schreier's forfiningssætning. Zassenhaus' lemma. 6.5-11: Moduler af endelig længde. 6.12-16: Ringe af endelig længde. 6.17: Baser i vektorrum.

MODULER

I det følgende betegner Λ en ring, med nul-element og et-element betegnet hhv 0 og 1.

1. Modulbegrebet.

1.1. DEFINITION. En <u>Λ-modul</u> $(M,+,\Lambda)$ er en mængde M forsynet med en (indre) komposition : $M\times M\to M$ kaldet <u>addition</u> og betegnet $(x,y)\mapsto x+y$ og en ydre komposition : $\Lambda\times M\to M$ kaldet <u>multiplikation</u> og betegnet $(\lambda,x)\mapsto \lambda x$, således at følgende er opfyldt:

(a) Med hensyn til addition er M en kommutativ gruppe.

(m) Multiplikationen harmonerer med additionen i den forstand at der gælder:

$$\begin{cases} (i) & \lambda(x+y) = \lambda x + \lambda y \\ (ii) & (\lambda+\mu)x = \lambda x + \mu x \\ (iii) & (\lambda\mu)x = \lambda(\mu x) \\ (iv) & 1x = x \end{cases} \qquad \begin{matrix} x,y\in M \\ \lambda,\mu\in\Lambda \end{matrix}$$

Den kommutative gruppe $(M,+)$ kaldes modulens additive gruppe. Dens neutrale element kaldes modulens <u>nul-element</u> og betegnes 0_M eller blot 0. Det inverse mht addition af et element $x\in M$ er dit <u>modsatte</u> element $-x$. Kravene til additionen i M kan udtrykkes ved ligningerne

$$(a)\begin{cases} x+y = y+x \\ x+(y+z) = (x+y)+z \\ x+0 = x \\ x+(-x) = 0 \end{cases} \qquad x,y,z\in M$$

Den kommutative gruppe $(M,+)$ siges også at være <u>orga-</u>

seret (via multiplikationen $\cdot : \Lambda \times M \to M$) som modul over Λ.

OBSERVATION I en Λ-modul M gælder

$$0x = 0_M = \lambda 0_M, \qquad (-\lambda)x = -(\lambda x) = \lambda(-x)$$

$\lambda \in \Lambda$, $x \in M$,

ganske som (det formelt tilsvarende) for ringe.

1.2. TERMINOLOGI. Hvis ringen Λ er et legeme (f.eks. $\mathbb{R}$ eller $\mathbb{C}$) ses det, at de krav vi har stillet til de to kompositioner i en Λ-modul $(M,+,\Lambda)$ netop er (ækvivalente med) de krav, der stilles til et vektorrum. (et reelt vektorrum er altså det samme som en $\mathbb{R}$-modul).

I overensstemmelse hermed vil vi også i den generelle situation for en modul M over en vilkårlig ring Λ kalde elementerne i Λ for skalarer og af og til elementerne i M for vektorer. Betegnelsen vektorrum (mere præcist: Λ-vektorrum) vil vi dog kun benytte for Λ-moduler, når Λ er et skæv-legeme.

1.3. $\mathbb{Z}$-MODULER. Lad $(M,+)$ være en kommutativ gruppe. Vi kan da definere produktet af en "skalar" $p \in \mathbb{Z}$ og en "vektor" $x \in M$ ved

$$px = (p\text{'te potens af } x).$$

At der herved defineres en $\mathbb{Z}$-modul, dvs at betingelserne (i), (ii), (iii) og (iv) er opfyldt, er netop indholdt af potensreglerne.

En kommutativ gruppe $(M,+)$ kan altså opfattes som en $\mathbb{Z}$-modul $(M,+,\mathbb{Z})$. Det er iøvrigt klart, at at ovenstående multiplikation $\cdot : \mathbb{Z} \times M \to M$ er den eneste via hvilken $(M,+)$ kan organiseres som $\mathbb{Z}$-modul, thi er $(n,x) \mapsto n \cdot x$ en sådan multiplikation fås af 1.1 (ii) og (iv), når f.eks. $n > 0$, at

$$n \cdot x = (1+\cdots+1)\cdot x = 1\cdot x + \cdots + 1 \cdot x = x + \cdots + x = nx.$$

1.4. DEFINITION. En modul $(M,+,\Lambda)$ således som defineret ovenfor kaldes også en <u>venstre-modul</u>. I modsætning hertil defineres en <u>højre-modul</u> $(M,+,\Lambda)$ som en mængde M med to kompositioner

$$M\times M \to M \quad \text{betegnet} \quad (x,y)\mapsto x+y \quad \text{og}$$
$$\Lambda\times M \to M \quad \text{betegnet} \quad (\lambda,x)\mapsto \lambda x$$

som opfylder de 8 krav ovenfor, bortset fra at multiplikations betingelsen (iii) erstattes af

$$(iii)^{op} \qquad (\lambda\mu)x = \mu(\lambda x), \quad \lambda,\mu\in\Lambda,\ x\in M.$$

Hvis ringen Λ er kommutativ, er dette ækvivalent med (iii), Over en kommutativ ring er venstre- og højre-moduler altså det samme.

BEMÆRKNING. For en højre-modul $(M,+,\Lambda)$ er det sædvane at betegne produktet af en skalar $\lambda\in\Lambda$ og en vektor $x\in M$ med $x\lambda$ [og altså ikke λx]. Herved får betingelsen $(iii)^{op}$ den mere håndterbare form

$$(iii)^{op} \qquad x(\lambda\mu) = (x\lambda)\mu \quad , \quad \lambda,\mu\in M,\ x\in M.$$

1.5. NUL-MODULEN er den Λ-modul, som kun har ét element (som altså må være nul-elementet). Den betegnes ofte (0) [eller blot 0, hvis misforståelser er udelukket].

1.6. Λ SOM Λ-MODUL. Ringen Λ kan opfattes som Λ-modul, idet <u>addition</u> i modulen Λ er addition i ringen Λ og <u>multiplikation</u> af en skalar $\lambda\in\Lambda$ med en vektor $x\in\Lambda$ er produktet λx i ringen Λ. At de 8 krav er opfyldt følger umiddelbart af kravene til en ring.

Når det ønskes præciseret, at Λ opfattes som (venstre-) modul over sig selv bruges betegnelsen Λ_s (s for sinistra = venstre).

Tilsvarende kan Λ opfattes som en højre-Λ-modul Λ_d (d for dextra = højre), idet multiplikation af en skalar $\lambda \in \Lambda$ med en vektor $x \in \Lambda$ her er produktet $x\lambda$ i ringen Λ.

1.7. n-SÆT. Produktmængden $\Lambda^n = \Lambda \times \cdots \times \Lambda$ af n-sæt

$$x = (x_1, \cdots, x_n) \quad , \quad x_\nu \in \Lambda$$

opfattes som Λ-modul med "koordinatvise kompositioner", dvs

$$(x_1, \cdots, x_n) + (y_1, \cdots, y_n) = (x_1+y_1, \cdots, x_n+y_n)$$

$$\lambda (x_1, \cdots, x_n) = (\lambda x_1, \cdots, \lambda x_n).$$

Opfattet således som (venstre-) Λ-modul skrives $\Lambda^n = \Lambda_s^n$.

Tilsvarende kan Λ^n opfattes som højre-modul Λ_d^n idet multiplikation af en skalar $\lambda \in \Lambda$ med en vektor $x = (x_1, \cdots, x_n) \in \Lambda_d^n$ her er

$$(x_1, \cdots, x_n)\lambda = (x_1\lambda, \cdots, x_n\lambda).$$

1.8. MATRICER. For givne $n, p \in \mathbb{N}$ kan vi betragte mængden $Mat_{n,p}(\Lambda)$ af $(n \times p)$-matricer

$$\alpha = \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1p} \\ \vdots & & \\ \alpha_{n1} & \cdots & \alpha_{np} \end{pmatrix} \qquad \alpha_{ij} \in \Lambda, \ i = 1, \cdots, n, \ j = 1, \cdots, p.$$

Matricen er kvadratisk, hvis $n = p$ [og vi skriver $Mat_n = Mat_{n,n}$]

For matricer $\alpha, \beta \in Mat_{n,p}(\Lambda)$ (af samme størrelse) er <u>summen</u> $\alpha + \beta \in Mat_{n,p}(\Lambda)$ defineret ved

$$(\alpha + \beta)_{ij} = \alpha_{ij} + \beta_{ij}$$

og er $\alpha \in Mat_{n,p}(\Lambda)$ og $\gamma \in Mat_{p,r}(\Lambda)$ er <u>produktet</u> $\alpha\gamma \in Mat_{n,r}(\Lambda)$ defineret ved

$$(\alpha\gamma)_{ij} = \sum_{k=1}^{p} \alpha_{ik}\gamma_{kj}.$$

For de herved udførte kompositioner af matricer gælder regneregler ganske svarende til hvad der gælder for reelle matricer. De vigtigste af disse regler kan sammenfattes således:

Mængden $Mat_n(\Lambda)$ af kvadratiske $n \times n$-matricer er en ring. Mængden $Mat_{n,p}(\Lambda)$ af $n \times p$-matricer er en venstre-$Mat_n(\Lambda)$-modul og en højre-$Mat_p(\Lambda)$-modul.

BEMÆRKNING. Et n-sæt $x \in \Lambda^n$ kan opfattes som en søjlematrix: $x \in Mat_{n,1}(\Lambda)$ og som en rækkematrix: $x \in Mat_{1,n}(\Lambda)$. Følgelig kan Λ^n opfattes som venstre-$Mat_n(\Lambda)$-modul og som højre-$Mat_n(\Lambda)$-modul.

1.9. DEFINITION. Lad M være en Λ-modul. For hver fast skalar $\lambda \in \Lambda$ kan vi betragte den ved

$$x \mapsto \lambda x$$

definerede afbildning: $M \to M$. Den kaldes <u>homotheti med faktor λ</u> og den betegnes $\lambda_M : M \to M$. Betingelsen 1.1 (i) udsiger, at λ_M er en homomorfi: $(M,+) \to (M,+)$, altså at λ_M er en endomorfi i $(M,+)$. Vi har altså $\lambda_M \in End(M)$, og kan derfor betragte $\lambda \mapsto \lambda_M$ som en afbildning:

$$\Lambda \longrightarrow End(M)$$

Det ses nu, at de øvrige betingelser (ii), (iii) og (iv)

netop udsiger, at denne afbildning er en ringhomomorfi. Den kaldes den til Λ-modulen M hørende repræsentation af Λ.

Er der omvendt givet en kommutativ gruppe $(M,+)$ og en ringhomomorfi

$$\rho : \Lambda \to End(M)$$

følger det let, at M ved definitionen

$$\lambda x = \rho(\lambda)(x)$$

organiseres som en Λ-modul.

BEMÆRKNING. Er $(M,+,\Lambda)$ en højre-Λ-modul kan vi ligeledes betragte afbildningen

$$\rho : \Lambda \to End(M)$$

defineret ved $\lambda \mapsto \lambda_M$, hvor $\lambda_M(x) = x\lambda$. Det følger, at ρ i dette tilfælde er en anti-ringhomomorfi, dvs

$$(\lambda+\mu)_M = \lambda_M + \mu_M, \quad (\lambda\mu)_M = \mu_M \circ \lambda_M, \quad 1_M = \text{identiteten}.$$

Idet Λ^{op} betegner den til Λ hørende modsatte ring kan vi derfor opfatte ρ som en ringhomomorfi

$$\Lambda^{op} \to End(M).$$

En højre-Λ-modul er følgelig det samme som en venstre-Λ^{op}-modul.

1.10. DEFINITION. En afbildning $f : M \to N$ mellem Λ-moduler M og N kaldes en (Λ-)homomorfi eller en (Λ-)lineær afbildning, hvis den bevarer strukturen i den forstand, at

$$f(x+y) = f(x) + f(y)$$
$$f(\lambda x) = \lambda f(x) \qquad x, y \in M,\ \lambda \in \Lambda.$$

Ved kernen for homomorfien $f : M \to N$ forstås originalmængden $f^{-1}(0)$. Da f specielt er en gruppehomomorfi : $(M,+) \to (N,+)$, er f injektiv,

netop når kernen er $f^{-1}(0) = \{0\}$.

En bijektiv Λ-homomorfi $f: M \to N$ kaldes også en <u>Λ-isomorfi</u>. For en sådan er også den inverse afbildning en Λ-isomorfi $f^{-1}: N \to M$.

En Λ-homomorfi $f: M \to M$ af modulen ind i sig selv kaldes også en <u>Λ-endomorfi</u>, og hvis den er bijektiv også en <u>Λ-automorfi</u>.

Det er klart, at sammensætning af Λ-homomorfier $f: M \to N$ og $g: N \to P$ er en Λ-homomorfi $g \circ f: M \to P$. Endvidere er for hver Λ-modul M den identiske afbildning $1_M = Id_M: x \mapsto x$ en Λ-homomorfi $: M \to M$. Ydertigere gælder for Λ-homomorfier $f, g: M \to N$, at også summen $f+g$, dvs afbildningen

$$f+g : x \mapsto f(x) + g(x)$$

er en Λ-homomorfi $: M \to N$.

NOTATION. For Λ-moduler M, N betegnes med

$\mathrm{Hom}_\Lambda(M,N)$ mængden af Λ-homomorfier $: M \to N$, med

$\mathrm{End}_\Lambda(M)$ mængden af Λ-endomorfier $: M \to M$ og med

$\mathrm{Aut}_\Lambda(M)$ mængden af Λ-automorfier $: M \to M$.

OBSERVATION. $(\mathrm{Hom}_\Lambda(M,N), +)$ er en kommutativ gruppe [nemlig en undergruppe i gruppen $\mathrm{Afb}(M,N)$ af alle afbildninger af M ind i den kommutative gruppe N]

$(\mathrm{End}_\Lambda(M), +, \circ)$ er en ring [nemlig en delring af ringen $\mathrm{End}(M)$ af additive endomorfier i $(M,+)$]

$(\mathrm{Aut}_\Lambda(M), \circ)$ er en gruppe [nemlig en undergruppe af den fulde automorfigruppe for M].

Gruppen $Aut_\Lambda(M)$ er åbenbart gruppen af invertible elementer i $End(M)$.

1.11. SÆTNING. *Λ-homomorfierne $\Lambda_s^m \longrightarrow \Lambda_s^p$ er netop afbildningerne af formen*

$$x \longmapsto x\alpha$$

med en matrix $\alpha \in Mat_{m,p}(\Lambda)$, hvor vi opfatter elementer i Λ_s^m og Λ_s^p som rækkematricer.

BEVIS. At en afbildning af den anførte form $x \longmapsto x\alpha$ er Λ-lineær, dvs at $(x+y)\alpha = x\alpha + y\alpha$, $(\lambda x)\alpha = \lambda(x\alpha)$, følger af regnereglerne for matrixkompositionerne. Lad omvendt $f: \Lambda_s^m \to \Lambda_s^p$ være Λ-lineær. Indføres m-sættene

$$\delta_\mu = (0, \dots, 1, \dots, 0) \in \Lambda_s^m,$$

hvor $1 \in \Lambda$ står på den μ'te plads, $\mu = 1, \dots, m$, kan vi for et vilkårligt $x = (x_1, \dots, x_m) \in \Lambda_s^m$ med de indførte kompositioner i Λ_s^m skrive

$$x = x_1\delta_1 + \cdots + x_m\delta_m$$

Sættes $f(\delta_\mu) = (\alpha_{\mu 1}, \dots, \alpha_{\mu p}) \in \Lambda_s^p$ finder vi, da f er lineær:

$$\begin{aligned} f(x) &= f(x_1\delta_1 + \cdots + x_m\delta_m) \\ &= x_1 f(\delta_1) + \cdots + x_m f(\delta_m) \\ &= x_1(\alpha_{11}, \dots, \alpha_{1p}) + \cdots + x_m(\alpha_{m1}, \dots, \alpha_{mp}) \\ &= (x_1\alpha_{11} + \cdots + x_m\alpha_{m1}, \dots, x_1\alpha_{1p} + \cdots + x_m\alpha_{mp}) \\ &= (x_1, \dots, x_m)\begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1p} \\ \vdots & & \\ \alpha_{m1} & & \alpha_{mp} \end{pmatrix} = x\alpha \quad \blacksquare \end{aligned}$$

BEMÆRKNING. Den i sætningen beskrevne bijektive afbildning: $Mat_{m,p}(\Lambda) \longrightarrow Hom_\Lambda(\Lambda_s^m, \Lambda_s^p)$ bevarer addition og er altså en gruppeisomorfi. Men multiplikation af matricer svarer til sammensætning af afbildninger i <u>den modsatte rækkefølge</u>. Specielt ses for $m = p$, at

$$Mat_m(\Lambda) \longrightarrow End_\Lambda(\Lambda_s^m)$$

er en anti-isomorfi af ringe. For $m = 1$ fås en anti-isomorfi af ringe: $\Lambda \xrightarrow{\sim} End_\Lambda(\Lambda_s)$.

2. Undermodul. Kvotientmodul.

2.1. DEFINITION. Lad M være en Λ-modul. En delmængde $N \subseteq M$ kaldes en undermodul, hvis N er stabil over for addition og multiplikation og hvis N med de inducerede kompositioner $N \times N \to N$ og $\Lambda \times N \to N$ er en Λ-modul.

Det ses let, at enhver ikke-tom, stabil delmængde N af M er en Λ-modul.

Det er klart, at for en undermodul $N \subseteq M$ er inklusionsafbildningen $: N \hookrightarrow M$ en Λ-homomorfi.

2.2. DEFINITION. Lad M være en Λ-modul. Ved en kongruensrelation i M forstås en ækvivalensrelation $\equiv$ i M, som harmonerer med additionen (i den sædvanlige forstand:

$$x \equiv x' \wedge y \equiv y' \Rightarrow x+y \equiv x'+y')$$

og med multiplikationen i den forstand, at

$$x \equiv x' \Rightarrow \lambda x \equiv \lambda x'.$$

Der er en bijektiv forbindelse mellem kongruensrelationer i M og undermoduler i M, ved hvilken der til undermodulen $N \subseteq M$ svarer kongruensrelationen $\underset{N}{\equiv}$ ("kongruens modulo N") defineret ved

$$x \underset{N}{\equiv} x' \Leftrightarrow x'-x \in N.$$

Den tilhørende kvotient betegnes også M/N, og den kan organiseres til en Λ-modul, således, at der gælder

$$\overline{x} + \overline{y} = \overline{x+y} \qquad \lambda \in \Lambda$$
$$\lambda\overline{x} = \overline{\lambda x}, \qquad x, y \in M.$$

Her betegner O som sædvanlig den kanoniske afbildning ind i kvotienten $O: M \to M/N$; denne afbildning er altså en Λ-homomorfi. Modulen M/N kaldes en <u>kvotientmodul</u> af M.

2.3. Vi får nu på velkendt måde:
UDVIDELSESSÆTNING. <u>Enhver Λ-homomorfi $f: M \to P$, som forsvinder på undermodulen $N \subseteq M$, kan entydigt udvides til en Λ-homomorfi $\tilde{f}: M/N \to P$.</u> Dette betyder, at der findes netop én Λ-homomorfi $\tilde{f}: M/N \to P$, så at $\tilde{f} \circ O = f$

$$\begin{array}{ccc} M & \xrightarrow{O} & M/N \\ {\scriptstyle f}\downarrow & \swarrow_{\tilde{f}} & \\ P & & \end{array}$$

Afbildningen $\tilde{f}: M/N \to P$ siges at være <u>induceret</u> af $f: M \to P$.

2.4. Kernen for en Λ-homomorfi $f: M \to P$ er øjensynlig en undermodul i M, og billedet $f(M)$ er en undermodul i P. Herom gælder
ISOMORFISÆTNING. <u>Den inducerede Λ-homomorfi $: M/f^{-1}(0) \to P$ giver en isomorfi $\tilde{f}: M/f^{-1}(0) \to f(M)$ af kvotienten $M/f^{-1}(0)$ på billedet $f(M)$.</u>

$$\begin{array}{ccc} M & \xrightarrow{O} & M/f^{-1}(0) \\ \downarrow & & \vdots\ \tilde{f} \\ P & \longleftarrow & f(M) \end{array}$$

BEMÆRK, at Isomorfisætningen anvendt på en surjektiv Λ-homomorfi $f: M \to P$ giver en isomorfi:

$$M/f^{-1}(0) \xrightarrow{\sim} P.$$

2.5. Enhver modul M har de <u>trivielle</u> undermoduler (0) (bestående alene af modulens nul-element) og M (bestående af alle elementer i M). For de tilhørende kvotienter fås:

$$M/(0) \simeq M \qquad M/M \simeq (0).$$

2.6. DEFINITION. Undermodulerne i Λ-modulen Λ_s kaldes <u>venstreidealer</u> i ringen Λ. Det er klart, at en delmængde $I \subseteq \Lambda$ er et venstreideal, netop når der gælder:

$$0 \in I,$$
$$\alpha \in I \wedge \beta \in I \Rightarrow \alpha + \beta \in I,$$
$$\lambda \in \Lambda \wedge \alpha \in I \Rightarrow \lambda\alpha \in I.$$

2.7. Enhver fællesmængde af undermoduler i en modul M er øjensynlig selv en undermodul. Heraf følger, at der for en given delmængde $S \subseteq M$ findes en mindste undermodul, som omfatter S, nemlig fællesmængden af alle undermoduler, der omfatter S. Den betegnes ΛS, og den kan beskrives således:

0) Hvis $S = \varnothing$, så er $\Lambda S = (0) \subseteq M$.

1) Hvis S består af ét element, $S = \{e\}$, så er $\Lambda S = \{\lambda e \mid \lambda \in \Lambda\}$. Som betegnelse bruges også
$$\Lambda e := \{\lambda e \mid \lambda \in \Lambda\} \subseteq M.$$

2) Hvis S er endelig, $S = \{e_1, \dots, e_n\}$, så er $\Lambda S = \{\lambda_1 e_1 + \dots + \lambda_n e_n \mid \lambda_1, \dots, \lambda_n \in \Lambda\}$. Som betegnelse bruges
$$\Lambda e_1 + \dots + \Lambda e_n := \{\lambda_1 e_1 + \dots + \lambda_n e_n \mid \lambda_1, \dots, \lambda_n \in \Lambda\}.$$

3) Hvis S er vilkårlig, består ΛS af de elementer $x \in M$ der er linearkombinationer
$$x = \lambda_1 s_1 + \dots + \lambda_k s_k, \quad \lambda_1, \dots, \lambda_k \in \Lambda$$
af endelig mange elementer $s_1, \dots, s_k \in S$.

2.8. DEFINITION. Lad M være en Λ-modul. Hvis der for en delmængde $S \subseteq M$ gælder $\Lambda S = M$, siges M at være <u>frembragt</u> af S.

Hvis M kan frembringes af en mængde med ét element, siges M at være en <u>cyklisk</u> modul. Betingelsen er altså, at der findes et element $e \in M$, så at

$$\Lambda e = M.$$

2.9. DEFINITION. Lad M være en Λ-modul og betragt et element $e \in M$. Et element $\alpha \in \Lambda$ siges at <u>annullere</u> e, hvis $\alpha e = 0$, og mængden af sådanne elementer $\alpha \in \Lambda$ kaldes <u>annullatoren</u> for e og betegnes $\mathrm{Ann}\, e$, altså

$$\mathrm{Ann}\, e = \{\alpha \in \Lambda \mid \alpha e = 0\}.$$

Ved $\lambda \mapsto \lambda e$ defineres øjensynlig en Λ-homomorfi:

$$\Lambda_s \longrightarrow M.$$

Kernen, dvs $\mathrm{Ann}\, e$, er derfor et venstreideal $\subseteq \Lambda$ og billedet er undermodulen $\Lambda e \subseteq M$, der kaldes den cykliske undermodul frembragt af elementet e. Isomorfisætningen giver altså en isomorfi

$$\Lambda_s / \mathrm{Ann}\, e \xrightarrow{\sim} \Lambda e.$$

SÆTNING. En Λ-modul M er cyklisk, hvis og kun hvis den er isomorf med en kvotient Λ_s / I, hvor I er et venstreideal.

BEVIS. □

2.10. DEFINITION. Lad M være en Λ-modul. Mængden af de $\alpha \in \Lambda$, som <u>annullerer</u> M, dvs annullerer hvert element i M, kaldes <u>annullatoren</u> for M og betegnes $\mathrm{Ann}\, M$.

Det ses, at $\lambda \in \mathrm{Ann}\, M$, netop når homotetien $\lambda_M : x \mapsto \lambda x$ er nul-afbildningen. Annullatoren for M er således kerne for ringhomomorfien $: \Lambda \longrightarrow \mathrm{End}(M)$, og den er derfor et ideal i ringen Λ.

3. Noethers isomorfisætninger.

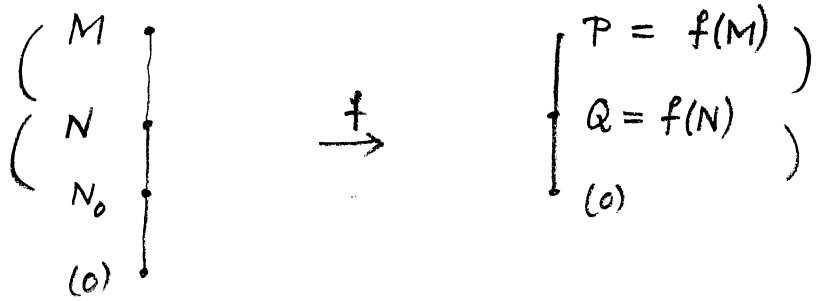
3.1. For en Λ-homomorfi $f: M \to P$ ser vi let, at billedet $f(N)$ af en undermodul N i M er en undermodul i P, og at originalmængden $f^{-1}(Q)$ af en undermodul Q i P er en undermodul i M.

NOETHERS ANDEN ISOMORFISÆTNING. *Lad $f: M \to P$ være en surjektiv Λ-homomorfi, og lad $N_0 \subseteq M$ være kernen for f. Ved $N \mapsto f(N)$ og $Q \mapsto f^{-1}(Q)$ defineres da en bijektiv forbindelse*

$$\{\text{undermoduler } N \text{ i } M \mid N \supseteq N_0\} \rightleftarrows \{\text{undermoduler } Q \text{ i } P\}.$$

Denne forbindelse bevarer inklusionen $\subseteq$, og der gælder

$$f(N) \cong N/N_0 \quad \text{og} \quad P/f(N) \cong M/N.$$



Bevis. For en undermodul Q i P har vi åbenbart $f^{-1}(Q) \supseteq N_0$, og da f er en surjektiv afbildning, gælder $f(f^{-1}(Q)) = Q$. For at vise, at forbindelsen er bijektiv, skal vi altså vise, at der for en undermodul N i M, med $N \supseteq N_0$, gælder

$$f^{-1}(f(N)) = N.$$

Her er "$\supseteq$" klart, og omvendt, hvis $x \in f^{-1}(f(N))$, kan vi skrive $f(x) = f(n)$, hvor $n \in N$, og

har altså $f(x-n) = f(x) - f(n) = 0$. Det følger, at $x - n \in \operatorname{Ker} f = N_0 \subseteq N$, men så er også

$$x = n + (x-n) \in N.$$

Af den generelle isomorfisætning følger de to isomorfier let, – den første fordi f definerer en surjektiv afbildning $: N \to f(N)$, der klart har kernen N_0, den anden fordi den sammensatte surjektive afbildning

$$M \xrightarrow{f} P \xrightarrow{0} P/f(N)$$

har kernen $f^{-1}(f(N)) = N$. ▨

3.2. Specielt kan f være den kanoniske homomorfi $0 : M \to M/N_0$, hvor $N_0 \subseteq M$ er en givet undermodul. Hvis $N \supseteq N_0$ er en undermodul i M, kan vi identificere billedet $\textcircled{N} \subseteq M/N_0$ med N/N_0:

$$N/N_0 \subseteq M/N_0,$$

og vi får isomorfien

$$M/N \xrightarrow{\sim} (M/N_0)/(N/N_0)$$

3.3. Hvis N_1 og N_2 er undermoduler i Λ-modulen M, ses det let, at <u>fællesmængden</u> $N_1 \cap N_2$ er en undermodul. Videre er det let at se, at <u>summen</u> $N_1 + N_2$, defineret ved

$$N_1 + N_2 = \{ n_1 + n_2 \mid n_1 \in N_1 \wedge n_2 \in N_2 \},$$

er en undermodul, endda den mindste undermodul i M, som indeholder både N_1 og N_2. Vi har

$$N_1 \cap N_2 \subseteq \left\{ \begin{matrix} N_1 \\ N_2 \end{matrix} \right\} \subseteq N_1 + N_2,$$

og den gælder

NOETHERS FØRSTE ISOMORFISÆTNING. <u>Lad N_1 og N_2</u>

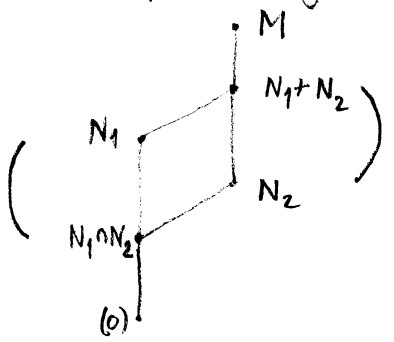
være undermoduler i Λ-modulen M. Der findes en naturlig isomorfi

$$N_1 / N_1 \cap N_2 \xrightarrow{\sim} N_1 + N_2 / N_2$$

Bevis. Vi har $N_1 \subseteq N_1 + N_2$, og vi betragter den sammensatte homomorfi

$$N_1 \xrightarrow{i} N_1 + N_2 \xrightarrow{k} N_1 + N_2 / N_2 .$$

Denne homomorfi er surjektiv, thi hvert element i $N_1 + N_2 / N_2$ er af formen $\overline{(n_1 + n_2)} = \overline{(n_1)} = k \circ i (n_1)$. Da kernen for denne homomorfi åbenbart er $N_1 \cap N_2$, følger påstanden af den generelle isomorfisætning. ▨



4. Direkte sum af moduler. Basis.

4.1. DEFINITION. Lad M være en Λ-modul. Ved <u>summen</u> af undermoduler $N_1, \dots, N_n$ i M forstås delmængden

$$N_1 + \cdots + N_n := \{ x_1 + \cdots + x_n \mid x_i \in N_i,\ i = 1, \dots, n \}.$$

Summen er øjensynlig selv en undermodul, endda den mindste, som indeholder alle N_i, $i = 1, \dots, n$.

At M <u>er sum</u> af undermodulerne $N_1, \dots, N_n$ betyder, at der for hvert $x \in M$ findes en fremstilling

$$x = x_1 + \cdots + x_n, \quad x_i \in N_i,\ i = 1, \dots, n$$

4.2. DEFINITION. Lad M være en Λ-modul. Undermoduler $N_1, \dots, N_n$ i M kaldes da <u>uafhængige</u> eller siges at <u>danne direkte sum</u>, hvis der af

$$x_1 + \cdots + x_n = 0, \quad x_i \in N_i,\ i = 1, \dots, n$$

følger, at $x_1 = \cdots = x_n = 0$.

Betingelsen er øjensynlig ækvivalent med at der for elementer $x \in N_1 + \cdots + N_n$ gælder, at fremstillingen

$$x = x_1 + \cdots + x_n, \quad x_i \in N_i,\ i = 1, \dots, n,$$

er entydig.

4.3. DEFINITION. Lad M være en Λ-modul. Vi siger da, at M <u>er direkte sum af undermodulerne</u> $N_1, \dots, N_n$, hvis disse undermoduler er uafhængige og deres sum er hele M.

Betingelsen udsiger, at hvert element $x \in M$ har en og kun én fremstilling

$$x = x_1 + \cdots + x_n, \quad x_i \in N_i,\ i = 1, \dots, n.$$

OBSERVATION. To undermoduler N_1 og N_2 i M er uafhængige, netop når $N_1 \cap N_2 = (0)$,
thi ligningen $x_1 + x_2 = 0$, $x_1 \in N_1$, $x_2 \in N_2$ svarer til ligningen $x + (-x) = 0$, $x \in N_1 \cap N_2$.

Det følger, at M er direkte sum af undermoduler N_1 og N_2, netop når $N_1 + N_2 = M$ og $N_1 \cap N_2 = (0)$.

SÆTNING. Antag, at Λ-modulen M er direkte sum af undermodulerne $N_1, \cdots, N_n$. Lad der være givet homomorfier $f_i : N_i \to P$, $i = 1, \cdots, n$, ind i en Λ-modul P. Da findes en og kun én homomorfi $f : M \to P$, så at $f/N_i = f_i$, $i = 1, \cdots, n$.

BEVIS. Entydighed: Lad $f : M \to P$ være en homomorfi, der opfylder det stillede krav. Da M er sum af undermodulerne $N_1, \cdots, N_n$ har hvert $x \in M$ en fremstilling

$$(*) \quad x = x_1 + \cdots + x_n, \quad x_i \in N_i, \quad i = 1, \cdots, n,$$

og så finder vi $f(x) = f(x_1 + \cdots + x_n) = f(x_1) + \cdots + f(x_n) = f_1(x_1) + \cdots + f_n(x_n)$, altså

$$(**) \quad f(x) = f_1(x_1) + \cdots + f_n(x_n).$$

Heraf følger entydigheden.

Eksistens: Da undermodulerne $N_1, \cdots, N_n$ er uafhængige, er fremstillingen $(*)$ entydig. Vi kan derfor ved ligningen $(**)$ definere en afbildning $f : M \to P$, og det er nu let at vise, at f er en homomorfi og at $f/N_i = f_i$, $i = 1, \cdots, n$. □

4.4. Betragt nu vilkårlige Λ-moduler $M_1, \cdots, M_n$. Produktmængden $M_1 \times \cdots \times M_n$ består da af n-sæt x, hvor der på den i-te plads står et element x_i i den i-te modul M_i, $i = 1, \cdots, n$. Vi vil oftest skrive disse n-sæt som søjler, og vi organiserer dem som Λ-modul ved kompositionerne

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix} \quad \text{og} \quad \lambda \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix}, \quad \lambda \in \Lambda.$$

Opfattet som Λ-modul betegnes produktmængden sædvanligvis $M_1 \oplus \cdots \oplus M_n$.

For hvert $i = 1, \ldots, n$ er den <u>i-te projektion</u>, dvs afbildningen

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \longmapsto x_i$$

øjensynlig en surjektiv homomorfi : $M_1 \oplus \cdots \oplus M_n \longrightarrow M_i$.

For hvert $i = 1, \ldots, n$ definerer vi den <u>i-te injektion</u> som afbildningen

$$y \longmapsto \begin{pmatrix} 0 \\ \vdots \\ y \\ \vdots \\ 0 \end{pmatrix}, \quad y \in M_i.$$

Det er let at se, at denne afbildning er en injektiv homomorfi : $M_i \longrightarrow M_1 \oplus \cdots \oplus M_n$. Hvis misforståelser er udelukket, vil vi oftist identificere modulen M_i med sit billede ved denne homomorfi, og altså opfatte M_i som undermodulen

$$M_i \subseteq M_1 \oplus \cdots \oplus M_n$$

bestående af de søjler, der har 0'er på alle andre pladser end den i-te.

Opfattet således som undermoduler, får vi den entydige fremstilling

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ x_2 \\ \vdots \\ 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ x_n \end{pmatrix}, \quad \begin{pmatrix} 0 \\ \vdots \\ x_i \\ \vdots \\ 0 \end{pmatrix} \in M_i,$$

Modulen $M_1 \oplus \cdots \oplus M_n$ er således den direkte sum af de givne moduler $M_1, \ldots, M_n$ opfattet som undermoduler i $M_1 \oplus \cdots \oplus M_n$.

DEFINITION. Modulen $M_1 \oplus \cdots \oplus M_n$ kaldes <u>den (ydre) direkte sum</u> af de givne moduler $M_1, \ldots, M_n$.

4.5. Lad $N_1, \dots, N_n$ være undermoduler i en given Λ-modul M. Vi kan da betragte den ydre direkte sum $N_1 \oplus \cdots \oplus N_n$. Ved

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \longmapsto x_1 + \cdots + x_n \in M$$

defineres øjensynlig en homomorfi : $N_1 \oplus \cdots \oplus N_n \to M$.

Af definitionerne 4.1, 4.2 og 4.3 fås umiddelbart følgende

OBSERVATION. Homomorfien $N_1 \oplus \cdots \oplus N_n \to M$ er

(1) surjektiv, netop når M er sum af undermodulerne $N_1, \dots, N_n$,

(2) injektiv, netop når undermodulerne $N_1, \dots, N_n$ er uafhængige og

(3) bijektiv, netop når M er direkte sum af undermodulerne $N_1, \dots, N_n$.

Det følger, at M er direkte sum af undermodulerne $N_1, \dots, N_n$, netop når homomorfien er en isomorfi :

$$N_1 \oplus \cdots \oplus N_n \xrightarrow{\sim} M.$$

At dette er tilfældet udtrykkes sædvanligvis ved at skrive

$$N_1 \oplus \cdots \oplus N_n = M \quad (\text{eller } M = N_1 \oplus \cdots \oplus N_n).$$

4.6. For to undermoduler N_1 og N_2 i en Λ-modul M følger det, at vi har

$$M = N_1 \oplus N_2,$$

netop når

$$M = N_1 + N_2 \quad \text{og} \quad N_1 \cap N_2 = (0).$$

DEFINITION. Lad M være en Λ-modul og lad $N \subseteq M$ være en undermodul. En undermodul $K \subseteq M$ kaldes da et <u>komplement</u> til N, hvis $M = N \oplus K$.

SÆTNING. En undermodul $K \subseteq M$ er et komplement til $N \subseteq M$, hvis og kun hvis den sammensatte homomorfi

$$K \hookrightarrow M \to M/N$$

er en isomorfi.

BEVIS. Kernen for homomorfien består af de elementer $k \in K$, for hvilke $\overline{k} = 0$ i M/N, dvs $k \in N$. Kernen er derfor $N \cap K$, så homomorfien er injektiv, netop når $N \cap K = (0)$. Billedet ved homomorfien er undermodulen bestående af ækvivalensklasserne $\overline{k}$, $k \in K$, og denne undermodul svarer ifølge Noethers 2. isomorfisætning til en undermodul $\supseteq N$ i M. Denne undermodul er $N+K$, thi vi har $N+K \supseteq N$, og for $n \in N$ og $k \in K$ har vi $\overline{n+k} = \overline{k}$ i M/N. Homomorfien er derfor surjektiv, netop når $M = N+K$. Heraf følger påstanden □

4.7. EKSEMPLER. (1) Den trivielle undermodul (0) [resp. M] har M [resp. (0)] som (det eneste) komplement.

(2) En undermodul kan godt have flere komplementer. Et 1-dimensionalt undervrum i et 2-dimensionalt vektorrum har således som komplement ethvert andet 1-dimensionalt undervrum.

(3) Til en given undermodul behøver der ikke at findes komplementer. I $\mathbb{Z}$-modulen $\mathbb{Z}$ må et komplement til $N = \mathbb{Z}n$, $n \geq 0$ have formen $K = \mathbb{Z}k$, $k \geq 0$. Da $kn \in \mathbb{Z}n \cap \mathbb{Z}k = (0)$, må vi have $n = 0$ (og dermed $N = (0)$) eller $k = 0$ (og dermed $\mathbb{Z} = N+K = N$). Det er således kun de trivielle undermoduler $N = (0)$ og $N = \mathbb{Z}$, der har komplementer.

4.8. DEFINITION. Lad M være en Λ-modul. En undermodul $N \subseteq M$ siges at være <u>direkte sumand</u> i M, hvis der findes et komplement til N, dvs en undermodul $K \subseteq M$, så

$$M = N \oplus K.$$

SÆTNING. Lad N være en undermodul i M, lad $i : N \hookrightarrow M$ være inklusionsafbildningen (dvs $i(x) = x$, $x \in N$) og lad

$p : M \to M/N$ være den kanoniske homomorfi (dvs $p(x) = \overline{x}$, $x \in M$). Da er følgende betingelser ækvivalente:

(i) Undermodulen N er direkte sumand i M.

(ii) Der eksisterer en homomorfi $r : M \to N$, så at $r \circ i = 1_N$.

(iii) Der eksisterer en homomorfi $s : M/N \to M$, så at $p \circ s = 1_{M/N}$.

BEVIS. Antag først, at K er et komplement til N. Hvert element $x \in M$ har da en entydig fremstilling

$$x = n + k, \quad n \in N, \ k \in K,$$

så vi kan definere afbildningen $r : M \to N$ ved $r(x) = n$. Det er klart, at r er en homomorfi og at $r(n) = n$, når $n \in N$. Altså er $r \circ i = 1_N$, så vi har vist, at (i) $\Rightarrow$ (ii). Videre følger dit (jfr. Sætning 4.6), at hvert element $X \in M/N$ har formen $X = \overline{k}$, med et entydigt bestemt $k \in K$, så vi kan definere afbildningen $s : M/N \to M$ ved $s(X) = k$. Det er klart, at s er en homomorfi og at $\overline{s(x)} = X$, når $X \in M/N$. Altså er $p \circ s = 1_{M/N}$, så vi har vist, at (i) $\Rightarrow$ (iii).

(ii) $\Rightarrow$ (i): Her gælder, at kernen $K := r^{-1}(0)$ er et komplement til N. Er nemlig $n \in N \cap K$, så er $n = r(n) = 0$. Følgelig er $N \cap K = (0)$. Videre har vi fremstillingen

$$x = r(x) + (x - r(x))$$

og her er $r(x) \in N$ og $r(x - r(x)) = r(x) - r(r(x)) = r(x) - r(x) = 0$, dvs $x - r(x) \in K$. Følgelig er $M = N + K$.

(iii) $\Rightarrow$ (i): Her gælder, at billedet $K := s(M/N)$ er et komplement til N. Er nemlig $n \in N \cap K$, så findes $X \in M/N$, så at $n = s(X)$, og så er $0 = \overline{n} = p(n) = ps(X) = X$, dvs $X = 0$ og dermed $n = 0$. Følgelig er $N \cap K = 0$. Videre har vi

$$x = (x - s(\overline{x})) + s(\overline{x}),$$

og her er $p(x - s(\overline{x})) = \overline{x} - ps(\overline{x}) = \overline{x} - \overline{x} = 0$, dvs $x - s(\overline{x}) \in N$ og $s(\overline{x}) \in K$. Følgelig er $M = N + K$. ▨

4.9. DEFINITION. Lad M være en Λ-modul. Et sæt $(v_1, \dots v_n)$ af elementer i M kaldes et <u>frembringersystem</u> for M, hvis hvert element $x \in M$ har en fremstilling som en linearkombination

$$x = \lambda_1 v_1 + \dots + \lambda_n v_n \ , \quad \lambda_i \in \Lambda, \ i = 1, \dots, n.$$

Sættet kaldes et <u>fit system</u> eller et <u>lineært uafhængigt system</u> i M, hvis der af

$$0 = \lambda_1 v_1 + \dots + \lambda_n v_n \ , \quad \lambda_1, \dots, \lambda_n \in \Lambda,$$

følger, at $\lambda_1 = \dots = \lambda_n = 0$.

Sættet kaldes en <u>fri basis</u> for M, hvis det både er et frembringersystem og et frit system.

BEMÆRKNINGER. Sættet $(v_1, \dots, v_n)$ er ögensynlig et frembringersystem for M, netop når delmængden $\{v_1, \dots, v_n\} \subseteq M$ frembringer M.

Et enkelt element $v \in M$ udgör et frit system i M, netop når der af

$$\lambda v = 0 \ , \quad \lambda \in \Lambda,$$

følger, at $\lambda = 0$. Et sådant element $v \in M$ kaldes også et <u>fit element</u> i M.

En ligning

$$\lambda_1 v_1 + \dots + \lambda_n v_n = 0$$

kaldes også en <u>lineær relation</u> mellem v_i'erne. At et sæt $(v_1, \dots, v_n)$ er et frit system betyder således, at den eneste lineære relation mellem v_i'erne er den trivielle, hvor alle koefficienterne er nul. At sættet ikke er frit, dvs et <u>lineært afhængigt</u> system betyder, at der findes en ikke-triviel lineær relation mellem v_i'erne, dvs en relation, hvori mindst én af koefficienterne er forskellig fra 0.

4.10. OBSERVATION. Sammenlignes med definitionerne 4.1, 4.2 og 4.3, ser vi, at sættet $(v_1, \dots, v_n)$ er et frembringersystem, netop når M er sum af undermodulerne

$\Lambda v_1, \dots, \Lambda v_n$, dvs når

$$M = \Lambda v_1 + \cdots + \Lambda v_n .$$

Sættet er et frit system, netop når undermodulerne $\Lambda v_1, \dots, \Lambda v_n$ er uafhængige og hvert v_i er et fritelement. Sættet er en fri basis, netop når

$$M = \Lambda v_1 \oplus \cdots \oplus \Lambda v_n \text{, og hvert } v_i \text{ er et fritelement.}$$

BEMÆRKNING. Det er sædvane at kalde et sæt $(v_1, \dots, v_n)$ i M for en <u>basis</u> for M, hvis

$$M = \Lambda v_1 \oplus \cdots \oplus \Lambda v_n \text{ og } v_i \neq 0,\ i = 1, \dots, n.$$

En fri basis er således en basis, hvis elementer er frie.

4.11. DEFINITION. En Λ-modul M i hvilken der findes en fri basis $(v_1, \dots, v_n)$ kaldes også en <u>fri</u> modul

BEMÆRKNING. Vi vil senere udvide denne definition til at omfatte moduler i hvilke der findes "uendelige" fri baser.

EKSEMPEL. Et-elementet $1 \in \Lambda$ er en fri basis for Λ-modulen Λ_S, idet hvert $\lambda \in \Lambda_S = \Lambda$ har den entydige fremstilling $\lambda = \lambda 1$. Mere generelt gælder for $n \in \mathbb{N}$, at søjlerne

$$\delta_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \quad \delta_2 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \quad \dots, \quad \delta_n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

er en fri basis for Λ-modulen Λ_S^n (opfattet som søjler). Dette følger af fremstillingen

$$\begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} = \lambda_1 \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \lambda_2 \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix} + \cdots + \lambda_n \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = \lambda_1 \delta_1 + \lambda_2 \delta_2 + \cdots + \lambda_n \delta_n .$$

Sættet $(\delta_1, \dots, \delta_n)$ kaldes også den <u>kanoniske basis</u> for Λ_S^n.

4.12. SÆTNING. Antag, at Λ-modulen M har en fri basis $(u_1, \dots, u_n)$. Lad der være givet elementer $v_1, \dots, v_n$ i en Λ-modul P. Da findes en og kun én homomorfi $f: M \to P$, så at $f(u_i) = v_i$, $i = 1, \dots, n$.

BEVIS. Resultatet vises enten analogt med beviset for Sætning 4.3 eller som et korollar til Sætning 4.3 □

4.13. Lad $(v_1, \dots, v_n)$ være et sæt af elementer i en Λ-modul M. Ved

$$\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_n \end{pmatrix} \longmapsto \lambda_1 v_1 + \dots + \lambda_n v_n$$

defineres øjensynlig en homomorfi: $\Lambda_s^n \to M$. Det er for øvrigt den entydigt bestemte homomorfi: $\Lambda_s^n \to M$, som opfylder $\delta_i \mapsto v_i$, $i = 1, \dots, n$, jfr. Sætning 4.12.

Af definitionen 4.9 fås umiddelbart følgende

OBSERVATION. Homomorfien: $\Lambda_s^n \to M$ er

(1) surjektiv, netop når $(v_1, \dots, v_n)$ er et frembringersystem,
(2) injektiv, netop når $(v_1, \dots, v_m)$ er et frit system, og
(3) bijektiv, netop når $(v_1, \dots, v_n)$ er en fri basis.

Det følger, at $(v_1, \dots, v_n)$ er en fri basis for M, netop når homomorfien er en isomorfi:

$$\Lambda_s^n \xrightarrow{\sim} M.$$

4.14. SÆTNING. Lad $f: M \to P$ være en surjektiv Λ-homomorfi med kerne $N \subseteq M$. Lad $(u_1, \dots, u_m)$ være et sæt i N, lad $(w_1, \dots, w_p)$ være et sæt i P, og vælg $v_j \in M$ med $f(v_j) = w_j$, $j = 1, \dots, p$. Da gælder:

Er $(u_1, \dots, u_m)$ et frembringersystem (resp. et frit system, resp. en fri basis) i N og er $(w_1, \dots, w_p)$ et frembringersystem (resp. et frit system, resp. en fri basis) i P, så er $(u_1, \dots, u_m, v_1, \dots, v_p)$ et frembringersystem (resp. et frit system, resp. en fri basis) i M.

BEVIS. (1) "frembringersystem": For $x \in M$ er $f(x) = \lambda_1 w_1 + \cdots + \lambda_p w_p$ med $\lambda_j \in \Lambda$. Valget af v_j sikrer, at $x - \lambda_1 v_1 - \cdots - \lambda_p v_p$ tilhører kernen $f^{-1}(0) = N$, og så er $x - \lambda_1 v_1 - \cdots - \lambda_p v_p = \mu_1 u_1 + \cdots + \mu_m u_m$ med $\mu_i \in \Lambda$. Heraf fås den ønskede fremstilling af x.
(2) "frit system": Antag, at $0 = \mu_1 u_1 + \cdots + \mu_m u_m + \lambda_1 v_1 + \cdots + \lambda_p v_p$. Anvendes homomorfien f fås ligningen $0 = \lambda_1 w_1 + \cdots + \lambda_p v_p$. Følgelig er $\lambda_1 = \cdots = \lambda_p = 0$. Den første ligning kan nu skrives $0 = \mu_1 u_1 + \cdots + \mu_m u_m$, og så er også $\mu_1 = \cdots = \mu_m = 0$.
(3) "fri basis": Er naturligvis en konsekvens af (1) og (2) ▨

BEMÆRKNING. For en given undermodul N i en Λ-modul M anvendes sætningen ofte på den kanoniske homomorfi: $M \to M/N$. Det følger, at hvis undermodulen N og kvotientmodulen M/N er fri moduler, så er også M en fri modul.

4.15. SÆTNING. Lad M være en Λ-modul og lad $N \subseteq M$ være en undermodul. Hvis kvotienten M/N er en fri modul, så er N direkte sumand i M.
BEVIS. Lad $(u_1, \ldots, u_k)$ være en fri basis for kvotienten M/N og lad $p: M \to M/N$ være den kanoniske afbildning. Vi eftervise betingelsen 4.8 (iii). Vælg elementer $v_i \in M$, så at $p(v_i) = u_i$. Der findes da (Sætning 4.12, "eksistensen") en homomorfi $s: M/N \to M$, så at

$$s(u_i) = v_i \quad , \; i = 1, \ldots, n.$$

For den sammensatte homomorfi $p \circ s: M/N \to M/N$ fås derfor

$$p \circ s(u_i) = p(v_i) = u_i \quad , \; i = 1, \ldots, n,$$

og så er (Sætning 4.12, "entydigheden") $p \circ s = 1_{M/N}$ ▨

4.16. DEFINITION. Lad M være en Λ-modul. En familie $(v_i)_{i\in I}$ af elementer i M, med mængden I som indexmængde, kaldes et <u>frembringersystem</u> for M, hvis hvert element $x\in M$ kan skrives som en lineærkombination af endelig mange elementer fra familien, dvs hvis der for hvert $x\in M$ findes en endelig delmængde $\{i_1,\dots,i_k\}\subseteq I$ og koefficienter $\lambda_1,\dots,\lambda_k$ så at

$$(*)\quad x = \lambda_1 v_{i_1} + \cdots + \lambda_k v_{i_k}.$$

Familien kaldes et <u>frit system</u> eller et <u>lineært uafhængigt system i M</u>, hvis enhver endelig delfamilie udgør et frit system, dvs hvis der for enhver endelig delmængde $\{i_1,\dots,i_k\}\subseteq I$ (med forskellige elementer $i_1,\dots,i_k$) gælder, at af

$$(0)\quad 0 = \lambda_1 v_{i_1} + \cdots + \lambda_k v_{i_k},\quad \lambda_1,\dots,\lambda_k\in\Lambda,$$

følger, at $\lambda_1 = \cdots = \lambda_k = 0$.

Familien kaldes en <u>fri basis</u> for M, hvis den er både et frembringersystem og et frit system.

BEMÆRKNINGER. Familien $(v_i)_{i\in I}$ er øjensynlig et frembringersystem for M, netop når delmængden $\{v_i \mid i\in I\}\subseteq M$ frembringer M.

I en ligning af formen (*) eller (0), kan man til højresiden tilføje led af formen λe_i, når blot $\lambda = 0$. Heraf følger bl.a., at ovennævnte definition stemmer overens med Definition 4.9, når indexmængden er den endelige mængde $I = \{1,\dots,n\}$. Også for en generel indexmængde I kan det være bekvemt at tilføje sådanne led, og tilføjer vi $\lambda_i v_i$, med $\lambda_i = 0$ for hvert $i \neq i_1,\dots,i_k$, kan (*) skrives

$$(*)\quad x = \sum_{i\in I} \lambda_i v_i$$

(hvor vi har sat $\lambda_{i_1} = \lambda_1, \ldots, \lambda_{i_k} = \lambda_k$). Summen på højre-siden er altså en endelig sum, i den forstand, at kun endelig mange af dens led er $\neq 0$.

4.17. DEFINITION. En Λ-modul M, i hvilken der findes en fri basis, kaldes en fri modul.

KONSTRUKTION. Lad I være en vilkårlig mængde.

Mængden Λ^I af alle afbildninger $\varphi: I \to \Lambda$ organiseres på oplagt måde som en Λ-modul, idet vi for afbildninger $\varphi, \psi: I \to \Lambda$ definer summen som afbildningen

$$i \longmapsto \varphi(i) + \psi(i), \text{ dvs } \quad (\varphi + \psi)(i) = \varphi(i) + \psi(i)$$

og produktet $\lambda\varphi$, $\lambda \in \Lambda$, som afbildningen

$$i \longmapsto \lambda\varphi(i), \text{ dvs } \quad (\lambda\varphi)(i) = \lambda \cdot \varphi(i).$$

Delmængden af Λ^I bestående af de afbildninger $\varphi: I \to \Lambda$, for hvilke $\varphi(i) \neq 0$ kun gælder for endelig mange indices $i \in I$, betegnes $\Lambda^{\oplus I}$ eller $\Lambda^{(I)}$. Det er let at se, at $\Lambda^{\oplus I} \subseteq \Lambda^I$ er en undermodul.

For hvert index $j \in I$ kan vi betragte den ved

$$\delta_j(i) = \begin{cases} 1 & \text{hvis } j = i \\ 0 & \text{hvis } j \neq i \end{cases}$$

definerede afbildning $\delta_j: I \to \Lambda$. Det er klart, at $\delta_j \in \Lambda^{\oplus I}$. Der gælder nu, at familien $(\delta_i)_{i \in I}$ er en fri basis for Λ-modulen $\Lambda^{\oplus I}$.

Dette følger af, at ligningen

$$\varphi = \lambda_1 \delta_{i_1} + \cdots + \lambda_k \delta_{i_k}$$

(der udtrykker, at to afbildninger $: I \to \Lambda$ er den samme, dvs antager ens værdi for hvert $i \in I$), når $i_1, \ldots, i_k$ er forskellige elementer i I, udsiger, at

$$\varphi(i) = \begin{cases} \lambda_1 & \text{hvis } i = i_1 \\ \vdots & \\ \lambda_k & \text{hvis } i = i_k \\ 0 & \text{hvis } i \neq i_1, \ldots, i_k. \end{cases}$$

Når $\varphi \in \Lambda^{\oplus I}$ er altså

$$\varphi = \sum_{i \in I} \varphi(i)\, \delta_i$$

den entydige fremstilling af φ som endelig linearkombination af elementer i familien $(\delta_i)_{i \in I}$. Familien $(\delta_i)_{i \in I}$ kaldes også den kanoniske basis for $\Lambda^{\oplus I}$, og $\Lambda^{\oplus I}$ siges at være den fri modul konstrueret med mængden I som fri basis (idet jo elementerne $i \in I$ svarer til basiselementer δ_i i den fri basis).

4.18. DEFINITION. Lad M være en Λ-modul og $(v_i)_{i \in I}$ være en familie af elementer i M. Familien kaldes et minimalt frembringersystem, hvis den er et frembringersystem og ingen ægte delfamilie er et frembringersystem. Familien kaldes et maksimalt frit system, hvis den er et frit system og ikke er ægte delfamilie af noget større frit system.

BEMÆRKNING. Et frembringersystem for M er ligesyntig minimalt, netop når "det holder op med at være et frembringersystem, når der fjernes et (vilkårligt) element fra systemet".
Et frit system er ligesyntig maksimalt, netop når "det holder op med at være et frit system, når der tilføjes et (vilkårligt) element fra M til systemet".

4.19. SÆTNING. Antag, at ringen Λ er et skævlegeme. Lad M være en Λ-modul, dvs et vektorrum over Λ, og lad $(v_i)_{i\in I}$ være en familie i M. Da er følgende betingelser ækvivalente:
(i) Familien er et minimalt frembringersystem for M.
(ii) Familien er et maksimalt frit system i M.
(iii) Familien er en (fri) basis for M.

OBSERVATION. Da alle elementer $\lambda \neq 0$ i Λ er invertible, er enhver vektor $v \neq 0$ fri, idet der af $\lambda v = 0$, $\lambda \neq 0$, følger $0 = \lambda^{-1}\lambda v = 1v = v$. Enhver basis for M er således en fri basis.

BEVIS. <u>(i) ⇒ (iii):</u> Da vi specielt har antaget, at familien er et frembringersystem, mangler vi at vise, at familien er et frit system. Var dette ikke tilfældet, ville der findes en ikke-triviel lineær relation mellem endelig mange vektorer $v_{i_0}, v_{i_1}, \dots, v_{i_k}$ i familien:

$$0 = \lambda_0 v_{i_0} + \lambda_1 v_{i_1} + \cdots + \lambda_k v_{i_k},$$

hvor mindst en af koefficienterne $\lambda_i \in \Lambda$ er $\neq 0$. Vi kan antage, at f.eks. $\lambda_0 \neq 0$. Multipliceres ligningen med λ_0^{-1}, fås en ligning af formen

$$(*) \quad v_{i_0} = \mu_1 v_{i_1} + \cdots + \mu_k v_{i_k} \quad (\text{hvor } \mu_j = -\lambda_0^{-1}\lambda_j \in \Lambda).$$

Men så er også familien $(v_i)_{i\in I\setminus\{i_0\}}$ et frembringersystem, thi enhver vektor x er en linearkombination af endelig mange af vektorerne $(v_i)_{i\in I}$, og hvis v_{i_0} forekommer i denne, kan vi indsætte $(*)$ og herved få en fremstilling af x som linearkombination af vektorerne $(v_i)_{i\in I\setminus\{i_0\}}$. Og det er i modstrid med at frembringersystemet var minimalt.

<u>(iii) ⇒ (i):</u> Da vi specielt har antaget, at familien er et frembringersystem, mangler vi at vise, at dette er minimalt. Var dette ikke tilfældet, ville en af vektorerne, f.eks. v_{i_0} være overflødig i familien, dvs opfylde, at

også familien $(v_i)_{i\in I\setminus\{i_0\}}$ er et frembringersystem. Specielt ville så v_{i_0} være en linearkombination

$$v_{i_0} = \lambda_1 v_{i_1} + \cdots + \lambda_k v_{i_k},$$

hvor $i_1, \ldots, i_k \in I\setminus\{i_0\}$. Men denne ligning kan opfattes som en ikke-triviel lineær relation mellem vektorerne $v_{i_0}, v_{i_1}, \ldots, v_{i_k}$. Og det er i modstrid med at familien også var et frit system.

(ii) ⇒ (iii): Da vi specielt har antaget, at familien er et frit system, mangler vi at vise, at familien er et frembringersystem. Lad $x \in M$. Tilføjes x til familien, er det udvidede system ikke længere frit. Der findes altså en ikke-triviel lineær relation mellem endelig mange af vektorerne $(v_i)_{i\in I}$ og x. I denne relation må x forekomme med en koefficient $\lambda \neq 0$, da vi jo har antaget, at der blandt vektorerne $(v_i)_{i\in I}$ kun findes den trivielle relation. Relationen har derfor formen

$$0 = \lambda x + \lambda_1 v_{i_1} + \cdots + \lambda_k v_{i_k},$$

hvor $\lambda \neq 0$. Multipliceres med λ^{-1} fås en ligning af formen

$$x = \mu_1 v_{i_1} + \cdots + \mu_k v_{i_k} \quad (\text{hvor } \mu_j = -\lambda^{-1}\lambda_j \in \Lambda).$$

Men så er x en linearkombination af endelig mange vektor i familien $(v_i)_{i\in I}$. Og familien er følgelig et frembringersystem.

(iii) ⇒ (ii): Da vi specielt har antaget, at familien er et frit system, mangler vi at vise, at dette er maksimalt. Lad $x \in M$. Da findes en fremstilling

$$x = \lambda_1 v_{i_1} + \cdots + \lambda_k v_{i_k}.$$

Men denne ligning kan opfattes som en ikke-triviel lineær relation mellem endelig mange af vektorerne $(v_i)_{i\in I}$ og x. For hver vektor x er således familien bestående af $(v_i)_{i\in I}$ og x ikke et frit system. Og følgelig er det givne frie system $(v_i)_{i\in I}$ maksimalt ▨

4.20. SÆTNING. Antag, at ringen Λ er et skævlegeme. Lad M være en Λ-modul, dvs et vektorrum over Λ. Da gælder:
(a) M er en fri modul, dvs der findes en basis for M.
(b) Alle baser for M har samme kardinaltal.

BEMÆRKNING. At to baser $(v_i)_{i\in I}$ og $(u_j)_{j\in J}$ har samme kardinaltal betyder, at indexmængderne I og J er ækvipotente.

I beviserne (for både (a) og (b)) er det naturligt at betragte to tilfælde hver for sig:

Tilfælde 1°: Der findes et endeligt frembringersystem for M

Tilfælde 2°: Der findes ingen endelige frembringersystemer for M.

Vi vil først senere bevise påstanden (b) i tilfælde 1°. (Påstanden er for øvrigt velkendt, i hvert fald for reelle vektorrum. Kardinaltallet for en basis er som bekendt vektorrummets dimension). De resterende påstande er under brug af Sætning 4.19 en umiddelbar følge af nedenstående observation og to lemma'er.

OBSERVATION. Hvis der i en modul M over en vilkårlig ring Λ findes et endeligt frembringersystem, så findes også et minimalt frembringersystem,
thi fra det endelige frembringersystem kan vi successivt fjerne eventuelt overflødige elementer, og så fås efter endelig mange skridt et minimalt frembringersystem.

LEMMA 1. Lad M være en modul over en vilkårlig ring Λ. Da findes en delmængde af M, som er et maksimalt fit system.

BEVIS. De delmængder $S \subseteq M$, der er fri systemer, udgør med sædvanlig inklusion $\subset$ som ordning en partielt ordnet mængde. Ifølge Zorn's lemma

er det nok at vise, at denne mængde er induktivt ordnet. Lad altså S_j, $j \in J$ være en totalt ordnet mængde af delmængder $S_j \subseteq M$, der er fri systemer. Vi påstår, at foreningsmængden $S := \bigcup_J S_j$ er en majorant. Det er klart, at hvert $S_j \subseteq S$, så vi skal vise, at også S er et frit system. Betragt derfor en lineær relation

$$(*) \quad 0 = \lambda_1 s_1 + \cdots + \lambda_k s_k$$

mellem endelig mange forskellige elementer $s_1, \cdots, s_k \in S$. Da $S = \bigcup S_j$ findes for hvert $i = 1, \cdots, k$ et j_i, så at $s_i \in S_{j_i}$. Da S_j'erne var totalt ordnede vil en af de endelig mange mængder $S_{j_1}, \cdots, S_{j_k}$, f.eks. S_{j_1}, omfatte de øvrige S_{j_i}'er. Følgelig er $s_i \in S_{j_1}$, $i = 1, \cdots, k$, og så er (*) en lineær relation mellem endelig mange forskellige elementer i S_{j_1}. Og så er koefficienterne $\lambda_1 = \cdots = \lambda_k = 0$, da S_{j_1} var et frit system ▨

LEMMA 2. Lad M være en modul over en vilkårlig ring Λ, lad $(v_i)_{i \in I}$ være et minimalt frembringersystem og lad $(u_j)_{j \in J}$ være et vilkårligt frembringersystem. Da gælder:

1° Hvis J er endelig, så er også I endelig.

2° Hvis J er uendelig, så er $\operatorname{Card} I \leq \operatorname{Card} J$, dvs der findes en injektiv afbildning: $I \to J$.

BEVIS. Da $(v_i)_{i \in I}$ er et frembringersystem, kan hvert element i M skrives som linearkombination af endelig mange elementer v_i. Specielt kan vi for hvert $j \in J$ vælge en endelig delmængde $I_j \subseteq I$, så at

(*) u_j er en linearkombination af v_i'er med $i \in I_j$.

Da $(u_j)_{j \in J}$ er et frembringersystem, kan hvert element x i M skrives som linearkombination af endelig mange u_j'er,

og heri kan vi (jfr. (*)) erstatte hvert u_j med en linearkombination af v_i'er med $i \in I_j$. Specielt fås herved en fremstilling af x som linearkombination af endelig mange v_i'er med $i \in \bigcup_J I_j$. Følgelig er delfamilien $(v_i)_{i \in \bigcup I_j}$ et frembringersystem, og da det givne frembringersystem $(v_i)_{i \in I}$ var minimalt, må vi have

$$\bigcup_{j \in J} I_j = I.$$

1°: Hvis mængden J er endelig, er I derfor en endelig foreningsmængde af endelige mængder, og dermed endelig.
2°: Hvis mængden J er uendelig, vælger vi for hvert $j \in J$ en surjektiv afbildning af $\mathbb{N}$ på den endelige mængde I_j. Herudfra fås klart en surjektiv afbildning: $J \times \mathbb{N} \longrightarrow \bigcup_{j \in J} I_j = I$, og så findes som bekendt også en injektiv afbildning: $I \to J \times \mathbb{N}$. For en uendelig mængde J er det imidlertid velkendt, at $J \times \mathbb{N}$ er ækvipotent med J. Idet vi derfor kan sammensætte med en bijektiv afbildning: $J \times \mathbb{N} \to J$, får vi en injektiv afbildning: $I \to J$ ▨

4.21. Bemærk forskellen på konklusionerne i de to tilfælde i Lemma 4.20.2. Hvis der findes et minimalt frembringersystem med uendelig mange elementer, kan vi slutte, at alle minimale frembringersystemer er ækvipotente. Hvis der findes et minimalt frembringersystem med endelig mange elementer, kan vi slutte, at alle minimale frembringersystemer er endelige, men <u>ikke</u>, at de har samme elementantal.

EKSEMPEL. Som $\mathbb{Z}$-modul er $\mathbb{Z}$ fri med 1 som fri basis. Sættet med 1 som eneste element er altså et minimalt frembringersystem. Af ligningen $x = x \cdot 3 - x \cdot 2$, $x \in \mathbb{Z}$ fremgår, at også sættet $(3,2)$ er et frembringersystem. Og det er ligeledes også minimalt.

5. Simple moduler.

5.1. DEFINITION. En Λ-modul S kaldes en <u>simpel modul</u>, hvis den har præcis 2 undermoduler.

OBSERVATION. Nul-modulen 0 har kun én undermodul, og den er derfor ikke simpel. Enhver modul $S \neq 0$ har altid mindst 2 undermoduler, nemlig de triviele (0) og S. At en sådan modul S er simpel betyder altså, at disse er de eneste undermoduler i S.

5.2. SÆTNING. For en Λ-modul S er følgende betingelser ækvivalente:

(i) S er en simpel modul.

(ii) $S \neq 0$, og for hvert element $e \neq 0$ i S er $\Lambda e = S$.

(iii) S er isomorf med en kvotientmodul Λ/I, hvor $I \subset \Lambda$ er et maksimalt venstre-ideal.

BEMÆRKNING. Et maksimalt venstre-ideal er et venstre-ideal M i Λ, der er maksimalt blandt venstre-idealer $\subset \Lambda$ (og specielt selv opfylder $M \subset \Lambda$).

BEVIS. <u>(i) $\Rightarrow$ (ii)</u>: At $S \neq 0$ har vi observeret, og er $e \neq 0$, så er $\Lambda e \subseteq S$ en undermodul. Vi har $\Lambda e \neq (0)$, da $e \in \Lambda e$, og følgelig er $\Lambda e = S$.
<u>(ii) $\Rightarrow$ (i)</u>: Vi skal vise, at enhver undermodul $N \subseteq S$ er triviel. Hvis $N = (0)$, er dette klart, og hvis $N \neq (0)$, findes et element $e \neq 0$ i N. Og så er $\Lambda e \subseteq N \subseteq S$ og dermed $(\Lambda e =)\ N = S$.
<u>(i) $\Leftrightarrow$ (iii)</u>: Hvis S er simpel, er S cyklisk ifølge det viste, og dermed isomorf med en kvotientmodul Λ/I, hvor $I \subseteq \Lambda$ er et venstre-ideal. Vi kan derfor antage, at S er en kvotientmodul Λ/I. Ifølge Noethers 2. isomorfisætning er der så en bijektiv forbindelse mellem undermoduler $\subseteq S = \Lambda/I$ og undermoduler $N \subseteq \Lambda$ (dvs venstre-idealer $N \subseteq \Lambda$), som opfylder:

$$I \subseteq N \subseteq \Lambda.$$

Modulen $S = \Lambda/I$ er derfor simpel netop hvis der er præcis 2 venstre-idealer N, der opfylder denne betingelse. Og det gælder netop hvis $I \subseteq \Lambda$ er et maksimalt venstre-ideal ▨

5.3. SÆTNING. Lad Λ være en ring. Da er Λ, som modul over sig selv, en simpel Λ-modul, hvis og kun hvis ringen Λ er et skævlegeme.

BEVIS. Vi udnytter betingelsen i Sætning 5.2 (ii).

"hvis": Et skævlegeme er $\neq 0$, så $1 \neq 0$, og hvis $e \neq 0$ i Λ, så er e invertibel, og for hvert $\lambda \in \Lambda$ gælder følgelig $\lambda = \lambda e^{-1} e \in \Lambda e$. Altså er $\Lambda e = \Lambda$.

"kun hvis": En simpel modul er $\neq 0$, så $\Lambda \neq 0$. Vi skal vise, at hvert element $e \neq 0$ i Λ er invertibelt. Da $e \neq 0$, er $\Lambda e = \Lambda$, så der findes et element $e' \in \Lambda$, så at $e'e = 1$. Her må vi have $e' \neq 0$, og tilsvarende findes derfor et element $e'' \in \Lambda$, så et $e''e' = 1$. Nu er $e'' = e''.1 = e''(e'e) = (e''e')e = 1e = e$, altså $e'' = e$, og dermed ialt

$$e'e = ee' = 1.$$

Elementet e er derfor invertibelt (med e' som invers) ▨

KOROLLAR. Lad Λ være et skævlegeme. Enhver cyklisk modul $\neq 0$ er da simpel (og isomorf med Λ).

BEVIS. En cyklisk modul $\neq 0$ er isomorf med en kvotient Λ/I, hvor $I \subset \Lambda$ er et venstre-ideal. Da Λ kun har trivielle venstre-idealer, må $I = (0)$ ▨

5.4. EKSEMPEL. De simple kommutative grupper, dvs de simple $\mathbb{Z}$-moduler, er de endelige cykliske grupper af primtals orden, thi maksimalidealerne i den kommutative ring $\mathbb{Z}$ er som bekendt idealerne $\mathbb{Z}p$, hvor p er et primtal, og $\mathbb{Z}/\mathbb{Z}p$ har orden p.

5.5. SÆTNING. Lad M være en Λ-modul $\neq 0$, og antag, at der i M findes et endeligt frembringersystem $(v_1, \cdots, v_n)$. Da findes i M en maksimal undermodul.

BEVIS. Vi skal vise, at der i M findes en undermodul, der er maksimal blandt undermodulerne $\subset M$ (ordnet ved sædvanlig inklusion). Der findes undermoduler $\subset M$, thi da vi har antaget $M \neq 0$, er $(0) \subset M$. Ifølge Zorn's lemma er det nok at vise, at mængden af sådanne undermoduler er induktivt ordnet. Lad altså N_j, $j \in J$, være en ikke-tom, totalt ordnet mængde af sådanne undermoduler. Vi påstår, at foreningsmængden $N := \bigcup_J N_j$ er en majorant. Da $N_j \subseteq N$ for alle j, skal vi vise, at N er en undermodul og at $N \subset M$.

Lad $x, y \in N = \bigcup N_j$, da findes $i, j \in J$, så at $x \in N_i$ og $y \in N_j$. Da N_j'erne var totalt ordnede, kan vi antage f.eks. at $N_i \subseteq N_j$, og så er både x og y elementer i N_j. Men så er også

$$x + y \ , \quad \lambda x, (\lambda \in \Lambda) \text{ og nul-elementet } 0$$

elementer i N_j og dermed også i N.

Videre er $N \subset M$, thi ellers var hver frembringer $v_i \in N = \bigcup_J N_j$ og så ville der findes j_i, $i = 1, \cdots, n$, så at $v_i \in N_{j_i}$. Da N_j'erne var totalt ordnede, vil en af modulerne $N_{j_1}, \cdots, N_{j_n}$, f.eks. N_{j_1} omfatte de øvrige. Men så er $v_1, \cdots, v_n \in N_{j_1}$ og dermed

$$M = \Lambda v_1 + \cdots + \Lambda v_n \subseteq N_{j_1},$$

i modstrid med at $N_{j_1} \subset M$ ▨

Sætningen kan specielt anvendes på $M = \Lambda$ (som modul over sig selv), der jo er frembragt af elementet 1. Det følger, at når $1 \neq 0$, så findes der maksimale venstre-idealer i Λ. Vi fremhæver specielt følgende

KOROLLAR. I en kommutativ ring $\neq 0$ findes maksimalidealer.

5.6. Lad M være en Λ-modul. En undermodul N af M er øjensynlig en maximal undermodul i M netop når der er præcis 2 undermoduler P, som opfylder

$$N \subseteq P \subseteq M$$

[og disse 2 må så være $P = N$ og $P = M$]. Af Noethers 2. isomorfisætning følger, at dette gælder netop når kvotienten M/N er en simpel modul.

Sætning 5.5 kan derfor omformuleres til følgende:

KOROLLAR. Enhver endeligt frembragt Λ-modul $M \neq 0$ har en simpel kvotient ▨

EKSEMPEL. Ringen $\mathbb{Z}$ har ingen simple undermoduler. Af Eksempel 5.4 fremgår nemlig specielt, at de simple $\mathbb{Z}$-moduler er endelige, og blandt undermodulerne i $\mathbb{Z}$ (nødvendigvis af formen $\mathbb{Z}n$) er øjensynlig (0) den eneste endelige, og den er ikke simpel.

6. Moduler af endelig længde.

6.1. DEFINITION. Lad M være en Λ-modul. En endelig følge $(M_\nu)_{\nu=0,\dots,n}$ af undermoduler i M, således at

$$(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{n-1} \subseteq M_n = M$$

kaldes en <u>kæde</u> i M. Tallet n kaldes <u>kædens længde</u>. Kvotientmodulerne $M_{\nu+1}/M_\nu$, $\nu = 0, \dots, n-1$ kaldes <u>kædens kvotienter</u> (eller <u>faktorer</u>). Antallet af kvotienter er altså kædens længde. En kæde siges at have <u>gentagelser</u>, hvis der for et ν gælder $M_\nu = M_{\nu+1}$. Dette er ensbetydende med at der for den tilsvarende kvotient gælder $M_{\nu+1}/M_\nu = (0)$.

En kæde $(N_\nu)_{\nu=0,\dots,n}$ i M siges at være en <u>forfining</u> af kæden $(M_\mu)_{\mu=0,\dots,m}$ i M, hvis der findes $0 \leqslant \nu_0 < \nu_1 < \cdots < \nu_m \leqslant n$, således at

$$N_{\nu_i} = M_i \,, \quad i = 0, \dots, m.$$

Dette betyder, at vi kan tænke på kæden (N_ν) som fremkommet ud fra kæden (M_μ) ved at der mellem M_μ og $M_{\mu+1}$ er indskudt visse N'er:

$$\left(M_\mu =\right) N_{\nu_\mu} \subseteq N_{\nu_\mu+1} \subseteq N_{\nu_\mu+2} \subseteq \cdots \subseteq N_{\nu_{\mu+1}} \left(= M_{\mu+1}\right)$$

En kæde $(M_\mu)_{\mu=0,\dots,m}$ kan <u>trivielt forfines</u> ved at gentage visse af M_μ'erne.

En kæde (M_μ), hvori alle kvotienterne er simple moduler kaldes en <u>Jordan-Hölder kæde</u> i M. Undermodulerne i en kvotient $M_{\mu+1}/M_\mu$ svarer til undermoduler N, så at $M_\mu \subseteq N \subseteq M_{\mu+1}$. Det følger heraf, at en kæde (M_μ) i M er en Jordan-Hölderkæde, hvis og kun hvis den er uden gentagelser og kun trivielt kan forfines.

6.2. Eksempler. En kæde i et vektorrum V over et legeme L er en følge af underrum

$$(0) = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_n = V.$$

De simple L-moduler er modulerne isomorfe med L_s, altså de 1-dimensionale vektorrum. At kæden er en Jordan-Hölder kæde betyder altså at $\dim V_1 = 1$, $\dim V_2/V_1 = 1, \ldots, \dim V_n/V_{n-1} = 1$, hvilket ifølge dimensionsformlen er ensbetydende med at

$$\dim V_1 = 1, \dim V_2 = 2, \ldots, \dim V_n = n.$$

Der findes således kun Jordan-Hölderkæder i endeligdimensionale vektorrum, og alle Jordan-Hölderkæder i et sådant vektorrum V har den samme længde, nemlig $\dim V$.

En $\mathbb{Z}$-modul er blot en kommutativ gruppe M, og en kæde i M er en følge af undergrupper

$$(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M.$$

De simple $\mathbb{Z}$-moduler er grupper, hvis orden er et primtal p (nødvendigvis isomorfe med $\mathbb{Z}/p$). At kæden er en Jordan-Hölder kæde betyder altså, at indeks

$$|M_1|, |M_2 : M_1|, \ldots, |M_n : M|$$

alle er primtal. Ifølge indekssætningen (Lagrange's formel) er $|M_2| = |M_2 : M_1||M_1|$, $|M_3| = |M_3 : M_2||M_2| = |M_3 : M_2||M_2 : M_1||M_1|$, $\ldots$, $|M| = |M_n| = |M_n : M_{n-1}| \cdots |M_2 : M_1||M_1|$.

Hvis (M_μ) er en Jordan-Hölderkæde i M, er

$$|M| = |M_n : M_{n-1}| \cdots |M_2 : M_1||M_1|$$

en primopløsning af $|M|$. Specielt er altså M en endelig gruppe, og n er antallet af primfaktorer i $|M|$.

Kæden

$$(0) \subseteq 12\mathbb{Z} \subseteq 6\mathbb{Z} \subseteq \mathbb{Z}$$

i $\mathbb{Z}$ er ikke en Jordan-Hölderkæde. Dens kvotienter

er (på isomorfi nær): $\mathbb{Z}$, $\mathbb{Z}/2$, $\mathbb{Z}/6$.

6.3. I analogi med de foregående eksempler gælder for moduler over en vilkårlig ring
JORDANS SÆTNING. *To vilkårlige Jordan-Hölderkæder i en Λ-modul M har samme længde.*
Denne sætning er en følge af Hölders sætning, som vi nu formulerer.

6.4. DEFINITION. To kæder $(M_\mu)_{\mu=0,\dots,m}$ og $(N_\nu)_{\nu=0,\dots,n}$ i Λ-modulen M kaldes *ækvivalente*, hvis de (på nær isomorfi og permutation) har de samme kvotienter. Dette betyder altså, at $m=n$ og at der findes en permutation $i: \{0,\dots,m-1\} \longrightarrow \{0,\dots,m-1\}$, således at $M_{\mu+1}/M_\mu$ er isomorf med $N_{i\mu+1}/N_{i\mu}$. To ækvivalente kæder i M har specielt samme længde.

HÖLDERS SÆTNING. *To vilkårlige Jordan-Hölderkæder i en Λ-modul M er ækvivalente.*
Denne sætning følger af

SCHREIERS FORFININGSSÆTNING. *To vilkårlige kæder i en Λ-modul M har ækvivalente forfininger.*
Det er klart, at forfiningssætningen medfører Hölders sætning, idet en Jordan-Hölderkæde kun har triviele forfininger.
Bevis for forfiningssætningen. Lad de to kæder i M være $(M_\mu)_{\mu=0,\dots,m}$ og $(N_\nu)_{\nu=0,\dots,n}$. Ved hjælp af kæden (N_ν) indskyder vi nu mellem M_μ og $M_{\mu+1}$ en hel række undermoduler og vi får herved en for-

fining af kæden (M_μ): Vi sætter

$$M_{\mu\nu} = (M_{\mu+1} \cap N_\nu) + M_\mu \,, \quad \mu = 0, \cdots, m-1;\ \nu = 0, \cdots, n.$$

Vi har $M_\mu = M_{\mu 0} \subseteq M_{\mu 1} \subseteq \cdots \subseteq M_{\mu,n-1} \subseteq M_{\mu n} = M_{\mu+1}$;
Af kæden (M_μ) får vi således en forfining

$$(0) = M_0 \subseteq M_{01} \subseteq \cdots \subseteq M_{0,n-1} \subseteq M_1 \subseteq M_{11} \subseteq \cdots \subseteq \cdots \subseteq M_{m-1,n-1} \subseteq M_m.$$

Denne kæde har længden mn og dens kvotienter er

$$M_{\mu,\nu+1} / M_{\mu,\nu} \,, \quad \mu = 0, \cdots, m-1;\ \nu = 0, \cdots, n-1.$$

Tilsvarende sætter vi

$$N_{\nu\mu} = (M_\mu \cap N_{\nu+1}) + N_\nu \,,$$

og vi får en forfining af kæden (N_ν), af længden nm og med kvotienterne

$$N_{\nu,\mu+1} / N_{\nu,\mu} \,, \quad \nu = 0, \cdots, n-1;\ \mu = 0, \cdots, m-1.$$

For at vise, at de to forfininger er ækvivalente, viser vi, at der for alle ν, μ gælder

$$M_{\mu,\nu+1} / M_{\mu,\nu} \simeq N_{\nu,\mu+1} / N_{\nu,\mu}$$

altså

$$\frac{(M_{\mu+1} \cap N_{\nu+1}) + M_\mu}{(M_{\mu+1} \cap N_\nu) + M_\mu} \simeq \frac{(M_{\mu+1} \cap N_{\nu+1}) + N_\nu}{(M_\mu \cap N_{\nu+1}) + N_\nu}$$

Denne påstand involverer de fire undermoduler $M_\mu \subseteq M_{\mu+1}$ og $N_\nu \subseteq N_{\nu+1}$. Påstanden kaldes

ZASSENHAUS' LEMMA. *Lad der i Λ-modulen M være givet fire undermoduler $M' \subseteq M''$ og $N' \subseteq N''$. Da findes en isomorfi*

$$\frac{(M'' \cap N'') + M'}{(M'' \cap N') + M'} \simeq \frac{(M'' \cap N'') + N'}{(M' \cap N'') + N'}.$$

Bevis for lemmaet. Ved sammensætning får vi en homomorfi

$$M'' \cap N'' \hookrightarrow (M'' \cap N'') + M' \to \frac{(M'' \cap N'') + M'}{(M'' \cap N') + M'}.$$

Denne homomorfi er klart surjektiv, og dens kerne er $(M'' \cap N'') \cap [(M'' \cap N') + M'] = (M'' \cap N') + (M' \cap N'')$. Vi får derfor en isomorfi

$$\frac{M'' \cap N''}{(M'' \cap N') + (M' \cap N'')} \xrightarrow{\sim} \frac{(M'' \cap N'') + M'}{(M'' \cap N') + M'}$$

Påstanden fås nu ved at ombytte M'erne med N'erne ▨

Hermed er beviset for sætningerne fuldført.

6.5. En Λ-modul M, i hvilken der findes en Jordan-Hölder kæde, kaldes en <u>Jordan-Hölder modul</u> eller en modul af <u>endelig længde</u>. <u>Længden</u> af en sådan modul M kan ifølge Jordans sætning defineres som længden af en vilkårlig Jordan-Hölderkæde i M. Denne længde betegnes $\operatorname{long}(M)$.

Nul-modulen har længde 0. Den eneste kæde uden gentagelser er $M_0 = (0)$. Modulerne af længde 1 er de simple Λ-moduler.

6.6. En simpel anvendelse af forfinings sætningen giver følgende

KOROLLAR. <u>I en Jordan-Hölder modul M kan enhver kæde uden gentagelser forfines til en Jordan-Hölder kæde.</u> □

Specielt har enhver kæde uden gentagelser en længde $\leqslant \operatorname{long} M$.

6.7 SÆTNING. *Lad N være en undermodul i Λ-modulen M. M er da en Jordan-Hölder modul, hvis og kun hvis både N og M/N er Jordan-Hölder moduler. Er dette tilfældet, gælder*

$$\operatorname{long} M = \operatorname{long} N + \operatorname{long} M/N.$$

Bevis. I følge Noethers anden isomorfisætning er der en entydig forbindelse mellem kæder i M/N og følger

$$(*) \quad N = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_m = M,$$

endda på en sådan måde, at kvotienterne for kæden i M/N er isomorfe med kvotienterne $M_{\mu+1}/M_\mu$. Jordan-Hölder kæder i M/N svarer altså til følger (*), der er uden gentagelser, og som kun trivielt kan forfines.

"hvis", så findes en Jordan-Hölder kæde

$$(0) = N_0 \subset N_1 \subset \cdots \subset N_n = N$$

i endelmodulen N, og en Jordan-Hölderkæde i M/N svarende til en følge

$$N = M_0 \subset M_1 \subset \cdots \subset M_m = M$$

med simple kvotienter. Vi får nu i M en Jordan-Hölder kæde

$$(0) = N_0 \subset \cdots \subset N_{n-1} \subset N \subset M_1 \subset \cdots \subset M_m = M.$$

(og vi ser, at dens længde er $n+m$).

"kun hvis". Vi kan antage, at $(0) \subset N \subset M$. Hvis M er en Jordan-Hölder modul, kan kæden $(0) \subset N \subset M$ forfines til en Jordan-Hölder kæde:

$$(0) = N_0 \subset \cdots \subset N_{n-1} \subset N \subset M_1 \subset \cdots \subset M_m = M.$$

Her er $(0) = N_0 \subset \cdots \subset N_{n-1} \subset N$ en Jordan-Hölder kæde i N og af følgen $N \subset M_1 \subset \cdots \subset M_m = M$ får vi som nævnt en Jordan-Hölderkæde i M/N. ▨

6.8. KOROLLAR. Lad der i modulen M være givet en kæde

$$(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M,$$

med kvotienterne $Q_\nu = M_\nu / M_{\nu-1}$, $\nu = 1, \cdots, n$. Da er M en Jordan-Hölder modul, hvis og kun hvis alle kvotienterne Q_ν er Jordan-Hölder moduler. Er dette tilfældet, gælder

$$\operatorname{long} M = \operatorname{long} Q_1 + \cdots + \operatorname{long} Q_n.$$

Følger af sætningen ved induktion. ▨

6.9. KOROLLAR Lad der være givet en direkte sum $M = N_1 \oplus \cdots \oplus N_n$. Da er M en Jordan-Hölder modul, hvis og kun hvis hver af modulerne N_ν er Jordan-Hölder moduler. Er dette tilfældet, gælder

$$\operatorname{long} N_1 \oplus \cdots \oplus N_n = \operatorname{long} N_1 + \cdots + \operatorname{long} N_n,$$

thi i M har vi kæden

$$(0) \subseteq N_1 \subseteq N_1 \oplus N_2 \subseteq \cdots \subseteq N_1 \oplus \cdots \oplus N_n = M \quad ▨$$

6.10. KOROLLAR. Lad N_1 og N_2 være undermoduler i Λ-modulen M, og antag, at de er Jordan-Hölder moduler. Da er også $N_1 \cap N_2$ og $N_1 + N_2$ Jordan-Hölder moduler, og

$$\operatorname{long}(N_1 \cap N_2) + \operatorname{long}(N_1 + N_2) = \operatorname{long} N_1 + \operatorname{long} N_2$$

Dette følger ved gentagen anvendelse af sætning 6.7. i forbindelse med Noethers første isomorfi

$$N_1 + N_2 / N_1 \simeq N_2 / N_1 \cap N_2.$$

6.11. LEMMA. Lad $(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ være en kæde, hvis kvotienter $M_\nu / M_{\nu-1}$ er cykliske, og vælg for hvert $\nu = 1, \cdots, n$ et element $v_\nu \in M_\nu$, hvis ækvivalensklasse $\overline{(v_\nu)} \in M_\nu / M_{\nu-1}$ frembringer $M_\nu / M_{\nu-1}$. Da er $(v_1, \cdots, v_n)$ et frembringersystem for M.

BEVIS. Induktivt kan vi antage, at $(v_1, \cdots, v_{n-1})$ er et frembringersystem for M_{n-1}. Og så følger påstanden af Sætning 4.14 ▨

Da en simpel modul er cyklisk fås følgende

KOROLLAR. En Jordan-Hölder modul er endeligt frembragt. ▨

BEMÆRKNING. Er $(v_1 \cdots, v_n)$ et frembringersystem i en modul M defineres omvendt ved $M_\nu = \Lambda v_1 + \cdots + \Lambda v_\nu$ en kæde $(0) = M_0 \subseteq \cdots \subseteq M_n = M$, hvis kvotienter $M_\nu / M_{\nu-1}$ er cykliske, thi i $M_\nu / M_{\nu-1}$ gælder

$$\overline{(\lambda_1 v_1 + \cdots + \lambda_\nu v_\nu)} = \overline{(\lambda_\nu v_\nu)} = \lambda_\nu \overline{(v_\nu)},$$

hvoraf følger, at $\overline{(v_\nu)}$ frembringer $M_\nu / M_{\nu-1}$.

6.12. DEFINITION. Ringen Λ siges at have endelig længde, hvis Λ-modulen Λ_s har endelig længde (altså hvis Λ_s er en Jordan-Hölder modul). En ring af endelig længde siges mere præcist at have endelig venstrelængde. Tilsvarende kunne vi nemlig have betragtet højre-modulen Λ_d. Hvis denne højremodul har endelig længde, siger vi, at Λ har endelig højrelængde. Kæden i Λ-modulen Λ_s svarer til følgen

$$(0) = \mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_n = \Lambda$$

af venstreidealer i Λ, hvorimod kæden i højremodulen Λ_d svarer til følgen af højreidealer i Λ.

6.13. EKSEMPEL. Hvis ringen Λ er et skævlegeme, så er Λ_s en simpel Λ-modul (Sætning 5.3). Følgelig har Λ den endelige venstrelængde $\operatorname{long} \Lambda_s = 1$. Tilsvarende er også $\operatorname{long} \Lambda_d = 1$. Man kan vise, at matrixringen $\operatorname{Mat}_n(\Lambda)$ i så fald har længden n (både venstre- og højre-).

6.14. EKSEMPEL. En ring A, som indeholder et legeme L som delring kan specielt også opfattes som vektorrum over L, idet multiplikation af $a \in A$ med en skalar $\lambda \in L$ defineres som ringproduktet $\lambda \cdot a \in A$. Venstreidealerne i ringen A er specielt underrum i vektorrummet. Hvis vektorrummet A er endelig dimensionalt, så har ringen A endelig længde, endda

$$\text{long } A_s \leqslant \dim_L A.$$

Specielt følger det, at enhver delring $A \subseteq \text{Mat}_n(L)$, som indeholder skalarmatricerne $\begin{pmatrix} \lambda & & \\ & \ddots & \\ & & \lambda \end{pmatrix}$, $\lambda \in L$, har endelig længde og at

$$\text{long } A_s \leqslant n^2 \quad \text{og} \quad \text{long } A_d \leqslant n^2.$$

6.15. EKSEMPEL. Man kan vise, at den for ringen $A = \begin{pmatrix} \mathbb{C} & \mathbb{C} \\ 0 & \mathbb{R} \end{pmatrix}$ bestående af 2×2-matricer $\begin{pmatrix} z & v \\ 0 & w \end{pmatrix}$, $z, v \in \mathbb{C}$, $w \in \mathbb{R}$, gælder

$$\text{long } A_s = 3 \qquad \text{long } A_d = 4.$$

Bemærk, at $\dim_{\mathbb{R}}(A) = 5$.

For den tilsvarende definerede ring $B = \begin{pmatrix} \mathbb{C} & \mathbb{C} \\ 0 & \mathbb{Q} \end{pmatrix}$ kan man vise, at $\text{long } B_s = 3$ og at B_d <u>ikke</u> har endelig længde.

6.16. SÆTNING. Hvis Λ er en ring af endelig længde, så har enhver endeligt frembragt Λ-modul endelig længde.

BEVIS. Da M er endeligt frembragt, findes en surjektiv homomorfi: $\Lambda_s^n \to M$, og følgelig er M isomorf med en kvotient af Λ_s^n. Da Λ_s har endelig længde, har Λ_s^n endelig længde (Korollar 6.9) og så har også kvotienten endelig længde (Sætning 6.7) ▨

6.17. Vi har tidligere v.hj.a. vektorrum givet eksempler på Jordan-Hölder moduler. Omvendt giver den nu udviklede teori let de klassiske sætninger om baser i vektorrum:

SÆTNING. Antag, at ringen Λ er et skævlegeme. Lad V være en Λ-modul (dvs et vektorrum over Λ), der er endeligt frembragt. Da gælder:

(1) V har endelig længde.

(2) V er en fri Λ-modul og alle baser for V har $\operatorname{long} V$ elementer.

BEVIS. Da Λ er et skævlegeme, er Λ, som modul over sig selv, en simpel modul. Vi har altså $\operatorname{long} \Lambda = 1$, og (1) følger derfor af den foregående sætning.

Ud fra et endeligt frembringersystem kan vi ligefrem udtage et minimalt frembringersystem, og det er som bekendt en fri basis. Følgelig er V en fri modul. Lad $(u_1, \dots, u_r)$ være en basis for V. Da $(u_1, \dots, u_r)$ er et frembringersystem, er $\Lambda u_1 + \cdots + \Lambda u_r = V$, så vi kan betragte kæden

$$(*) \quad (0) = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_r = V,$$

hvor

$$V_i = \Lambda u_1 + \cdots + \Lambda u_i \text{ , altså } V_i = V_{i-1} + \Lambda u_i, \; i = 1, \dots, r.$$

Kvotienten V_i / V_{i-1} er cyklisk, frembragt af $\overline{(u_i)}$, og dermed isomorf med en kvotient af den simple modul Λ. Da $\overline{(u_i)} \neq 0$ (!), er $V_i / V_{i-1} \neq 0$, og V_i / V_{i-1} er derfor en simpel modul. Men så er $(*)$ en Jordan-Hölder kæde i V, og følgelig er $r = \operatorname{long} V$ ▨

BEMÆRKNING. Et endeligt frembragt vektorrum V siges også at være endelig dimensionalt og dets længde kaldes også vektorrummets dimension og betegnes

$$\dim V = \operatorname{long} V.$$

MODULER OVER KOMMUTATIVE RINGE. DETERMINANT.

1. Moduler over kommutative ringe. 1.0-8: Observationer.

2. Alternerende n-lineære afbildninger. Determinant. 2.1-2: Definition. 2.3: Sætning. 2.4: Observation. 2.5: Motivation. 2.6: Definition af determinant. Sætning. 2.7: $\det: \mathrm{Mat}_n(R) \to R$.

3. Determinantsætninger. 3.1: Determinant af transponeret matrix. 3.2-3: Determinant af "øvre" blokmatrix. 3.4: Determinant som alternerende n-lineær afbildning. 3.5: Determinant af produkt.

4. Udviklinger. Cramers formel. 4.1: Komplement. 4.2-3: Udvikling af determinant efter søjle og efter række. 4.4: Komplementmatrix. Formler. 4.5: $\alpha\tilde{\alpha} = \tilde{\alpha}\alpha = \det(\alpha)$. 4.6: Invertibel matrix. 4.7: Cramers formel. 4.8: GL_n og SL_n.

5. Rang og dimension. 5.1: $\mathrm{Hom}_R(R^p, R^n) = \mathrm{Mat}_{n,p}(R)$. 5.2: Bijektive homomorfier: $R^n \to R^n$. 5.3: Injektive homomorfier: $R^p \to R^n$. 5.4-6. Rang og dimension. 5.7: Underdeterminant. Søjleregulær matrix. 5.8: Ligningen $\alpha x = 0$, når α er søjleregulær. 5.9: Injektive homomorfier: $R^p \to R^n$. 5.10: Surjektive homomorfier: $R^p \to R^n$.

MODULER OVER KOMMUTATIVE RINGE. DETERMINANT.

I det følgende betegner R en kommutativ ring.

1. Moduler over kommutative ringe.

1.0. Generelle resultater om moduler gælder naturligvis specielt for moduler over en kommutativ ring R. I det følgende anføres nogle observationer, der er specielle for kommutative ringe.

1.1. Der er ingen forskel på venstre- og højremoduler over R. For en R-modul M skriver vi $\lambda x = x\lambda$ for produktet af modulelementet $x \in M$ med skalaren $\lambda \in \Lambda$.

1.2. Homotetierne i en R-modul M er R-lineære afbildninger, thi for $\alpha, \lambda \in R$ og $x \in M$ har vi $\alpha_M(\lambda x) = \lambda\, \alpha_M(x)$, idet jo $\alpha_M(\lambda x) = \alpha(\lambda x) = (\alpha\lambda)x = (\lambda\alpha)x = \lambda(\alpha x) = \lambda \alpha_M(x)$.

1.3. For moduler M, N er den kommutative gruppe $\mathrm{Hom}_R(M,N)$ af R-homomorfier $f: M \to N$ igen en R-modul, idet produktet λf af en sådan homomorfi f med en skalar $\lambda \in R$ defineres som afbildningen

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

Bemærk, at $\lambda f = \lambda_N \circ f = f \circ \lambda_M$.

1.4. Specielt er for en R-modul M ringen $\mathrm{End}_R(M)$ igen en R-modul, og den omfatter delringen bestående af homotetierne. For $f \in \mathrm{End}_R(M)$ og $\lambda \in R$ har vi

$$\lambda_M \circ f = f \circ \lambda_M \ (= \lambda f).$$

Homotetierne tilhører altså endda centret i ringen $End_R(M)$.

1.5. R-homomorfierne $f: R^p \to R^n$ er netop afbildningerne af formen

$$x \longmapsto \alpha x \ , \quad x \in R^p$$

med en matrix $\alpha \in Mat_{n,p}(R)$. Her fortolkes $x \in R^p$ som en søjle, og de p søjler i matricen α er billederne ved f af den kanoniske basis $\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}, \dots, \begin{pmatrix}0\\\vdots\\0\\1\end{pmatrix}$ for R^p.

[Bemærk, at der ikke er grund til at skelne R^p_s fra R^p_d. Vi skriver blot R^p for denne R-modul].

1.6. Den i 1.5 beskrevne bijektive afbildning:

$$Hom_R(R^p, R^n) \xrightarrow{\sim} Mat_{n,p}(R)$$

er en isomorfi af R-moduler. Yderligere svarer sammensætning af afbildninger til produkt af matricer.

I tilfældet $n = p$ fås en ring-isomorfi:

$$End_R(R^n) \xrightarrow{\sim} Mat_n(R).$$

Herved svarer homotetier i R^n til skalarmatricer $\begin{pmatrix}\lambda & & 0\\ & \ddots & \\ 0 & & \lambda\end{pmatrix}$ i $Mat_n(R)$.

1.7. Hvis skalaren $\alpha \in R$ annullerer elementet e i modulen M, vil α annullere hele undermodulen Re, thi så er $\alpha(\lambda e) = \lambda \alpha e = 0$. Det følger, at vi for en cyklisk modul $M = R/\mathfrak{a}$, hvor $\mathfrak{a}$ er et ideal i R (bemærk, at idealerne i R netop er undermodulerne i R-modulen R), har

$$Ann(R/\mathfrak{a}) = \mathfrak{a}.$$

1.8. Hvis skalaren $\alpha \in R$ annullerer elementerne $e_1, \dots, e_n$ i modulen M, vil α også annullere undermodulen $Re_1 + \dots + Re_n \subseteq M$.

2. Alternerende n-lineære afbildninger. Determinant.

2.1. DEFINITION. Lad $N_1, \dots, N_n, M$ være R-moduler. Ved en *multi-lineær* afbildning

$$\varphi : N_1 \times \cdots \times N_n \to M$$

forstås en afbildning som er lineær i hver variabel, dvs opfylder

$$\varphi(\dots, x_i' + x_i'', \dots) = \varphi(\dots, x_i', \dots) + \varphi(\dots, x_i'', \dots)$$

$$\varphi(\dots, \lambda x_i, \dots) = \lambda\, \varphi(\dots, x_i, \dots)$$

[hvor $(\cdots$ og $\dots)$ står for $(x_1, \dots, x_{i-1}$ og $x_{i+1}, \dots, x_n)$]

for alle $x_j \in N_j$, $j \neq i$ og $x_i', x_i'', x_i \in N_i$ og $\lambda \in R$.

Ønskes antallet n af variable fremhævet, taler man om en *n-lineær* afbildning. For $n = 1, 2$ og 3 bruges også benævnelserne *lineær*, *bilineær* og *trilineær*.

2.2. DEFINITION. Lad N og M være R-moduler. En n-lineær afbildning

$$\varphi : N^n \to M \qquad \left(N^n = \overbrace{N \times \cdots \times N}^{n}\right)$$

kaldes *alternerende*, hvis $\varphi(x_1, \dots, x_n) = 0$ for ethvert sæt $(x_1, \dots, x_n) \in N^n$, hvor 2 af koordinaterne er ens, dvs hvis der findes $i < j$ så at $x_i = x_j$.

2.3. SÆTNING. Lad $\varphi : N^n \to M$ være en alternerende n-lineær afbildning og lad $\sigma \in S_n$ være en permutation. Da gælder for hvert sæt $(x_1, \dots, x_n) \in N^n$, at

$$\varphi(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \operatorname{sign}(\sigma)\, \varphi(x_1, \dots, x_n).$$

BEVIS. Som bekendt kan σ fremstilles som produkt af transpositioner og $\operatorname{sign}(\sigma) = (-1)^m$, hvor m er antallet af transpositioner i en sådan fremstilling. Det er følgelig nok at vise ligningen i tilfældet hvor σ er en transposition $\sigma = (i,j)$ (der ombytter i og j). Idet vi undlader at skrive de variable på pladserne $\neq i,j$ finder vi

$$0 = \varphi(x_i + x_j, x_i + x_j) = \varphi(x_i, x_i) + \varphi(x_i, x_j) + \varphi(x_j, x_i) + \varphi(x_j, x_j)$$
$$= \varphi(x_i, x_j) + \varphi(x_j, x_i),$$

og dét er netop påstanden ▨

BEMÆRKNING. En n-lineær afbildning $\varphi: N^n \to M$ som opfylder ligningen ovenfor kaldes <u>anti-symmetrisk</u>. Hvis 2 er invertibel i R, dvs hvis $1_R + 1_R$ er et invertibelt element i R, gælder omvendt, at en anti-symmetrisk n-lineær afbildning er alternerende, thi er i $(x_1, \dots, x_n)$ $x_i = x_j = x$ $(i \neq j)$, så følger af antisymmetrien, at

$$\varphi(x,x) = -\varphi(x,x)$$

og dermed at

$$0 = \varphi(x,x) + \varphi(x,x) = (1_R + 1_R)\,\varphi(x,x)$$

og multiplikation med den inverse til $1_R + 1_R$ giver så at

$$0 = \varphi(x,x).$$

2.4. OBSERVATION. En alternerende n-lineær afbildning $\varphi: N^n \to M$ er specielt lineær i den i-te variabel og bevarer derfor linearkombinationer i den i-te variabel. Det følger umiddelbart, at der gælder

$$\varphi(x_1, \dots, x_i + \sum_{j \neq i} \lambda_j x_j, \dots, x_n) = \varphi(x_1, \dots, x_i, \dots, x_n).$$

["Værdien ændres ikke dersom man til én af de

variable adderes en linearkombination af de øvrige."]

2.5. MOTIVATION. Lad $\varphi: N^n \to M$ være en alternerende n-linear afbildning og lad $x = (x_1, \dots, x_n) \in N^n$. Lad $y = (y_1, \dots, y_n)$ være endnu et sæt og antag at hvert y_i er en linearkombination af $x_1, \dots, x_n$. Af multi-linearitetet følger da at φ's værdi på $y = (y_1, \dots, y_n)$ kan udtrykkes ved φ's værdi på $x = (x_1, \dots, x_n)$ og sæt, der fremgår heraf ved permutation. Lidt mere præcist:

Skriv for $j = 1, \dots, n$ y_j som linearkombination af $x_1, \dots, x_n$ og anbring koefficienterne som j-te søjle i $n \times n$ matricen α. Vi har altså

$$y_j = \sum_{i=1}^{n} \alpha_{ij} x_i \quad , \quad j = 1, \dots, n,$$

dvs med oplagt matrixmultiplikation

$$(y_1, \dots, y_n) = (x_1, \dots, x_n) \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{n1} & \cdots & \alpha_{nn} \end{pmatrix},$$

eller kort:

$$y = x\alpha \quad , \quad x \in N^n \quad \alpha \in \mathrm{Mat}_n(R),$$

og finder

$$\varphi(y) = \varphi(y_1, \dots, y_n) = \varphi\Big(\sum_{\sigma_1=1}^{n} \alpha_{\sigma_1 1} x_{\sigma_1}, \dots, \sum_{\sigma_n=1}^{n} \alpha_{\sigma_n n} x_{\sigma_n}\Big),$$

hvor vi har brugt forskellige summationsindices i de n summer. Multilinearitetet giver

$$\varphi(y) = \sum_{\sigma_1=1}^{n} \alpha_{\sigma_1 1} \sum_{\sigma_2=1}^{n} \alpha_{\sigma_2 2} \cdots \sum_{\sigma_n=1}^{n} \alpha_{\sigma_n n}\, \varphi(x_{\sigma_1}, \dots, x_{\sigma_n})$$

eller som multibel sum

$$\varphi(y) = \sum_{(\sigma_1, \dots, \sigma_n)} \alpha_{\sigma_1 1} \cdots \alpha_{\sigma_n n}\, \varphi(x_{\sigma_1}, \dots, x_{\sigma_n}),$$

hvor der summeres over alle $\sigma_1, \dots, \sigma_n$ med $1 \le \sigma_k \le n$.

Et sådant sæt $(\sigma_1, \dots, \sigma_n)$ af tal kan opfattes som en afbildning $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$. Da φ er alternerende, kan $\varphi(x_{\sigma_1}, \dots, x_{\sigma_n})$ kun være $\neq 0$, når σ_i'erne er forskellige, dvs når $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ er injektiv (og dermed bijektiv). Disse afbildninger er netop permutationerne $\sigma \in S_n$, så vi får

$$\varphi(y) = \sum_{\sigma \in S_n} \alpha_{\sigma_1 1} \cdots \alpha_{\sigma_n n} \varphi(x_{\sigma_1}, \dots, x_{\sigma_n}).$$

Af Sætning 2.3 fås endelig

$$\varphi(y) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \alpha_{\sigma_1 1} \cdots \alpha_{\sigma_n n} \varphi(x_1, \dots, x_n).$$

2.6 DEFINITION. Lad $\alpha \in \mathrm{Mat}_n(R)$ være en kvadratisk matrix. Ved <u>determinanten</u> af α forstås elementet

$$\det(\alpha) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \alpha_{\sigma_1 1} \cdots \alpha_{\sigma_n n} \in R.$$

SÆTNING. Lad $\varphi : N^n \to M$ være en n-lineær alternerende afbildning, lad $x = (x_1, \dots, x_n) \in N^n$ og lad $\alpha \in \mathrm{Mat}_n(R)$. Da er

$$\varphi(x\alpha) = \det(\alpha)\varphi(x).$$

BEVIS. Dette var resultatet i 2.5 ▨

BEMÆRKNING. Dette er måske kønnest at skrive ligningen på formen $\varphi(x\alpha) = \varphi(x)\det(\alpha)$, hvor skalaren $\det(\alpha)$ er skrevet til højre for modulelementet $\varphi(x)$.

2.7. BEMÆRKNING. Determinanten er en afbildning

$$\det : \mathrm{Mat}_n(R) \to R.$$

Forskellige værdier af n giver naturligvis forskellige afbildninger, men det fører sædvanligvis ikke til misforståelser at lade det betegne enhver af disse afbildninger.

3. Determinantsætninger.

3.1. SÆTNING. For den transponerede matrix α^t til en matrix $\alpha \in Mat_n(R)$ gælder

$$\boxed{det(\alpha^t) = det(\alpha).}$$

BEVIS. Den transponerede matrix α^t er bestemt ved $\alpha^t{}_{ij} = \alpha_{ji}$, så ifølge definitionen er

$$det(\alpha^t) = \sum_{\sigma \in S_n} sign(\sigma)\, \alpha_{1\sigma_1} \cdots \alpha_{n\sigma_n}$$

Når σ gennemløber gruppen S_n vil også σ^{-1} gennemløbe S_n, og da $sign(\sigma^{-1}) = sign(\sigma)$ får vi

$$det(\alpha^t) = \sum_{\sigma \in S_n} sign(\sigma)\, \alpha_{1\sigma^{-1}(1)} \cdots \alpha_{n\sigma^{-1}(n)}$$

Faktorerne i produktet $\alpha_{1\sigma^{-1}(1)} \cdots \alpha_{n\sigma^{-1}(n)}$ er netop de α_{ij}, hvor $i = \sigma(j)$. Idet vi frit kan omordne faktorerne, følger det, at

$$\alpha_{1\sigma^{-1}(1)} \cdots \alpha_{n\sigma^{-1}(n)} = \alpha_{\sigma(1)1} \cdots \alpha_{\sigma(n)n} \quad (= \alpha_{\sigma_1 1} \cdots \alpha_{\sigma_n n}),$$

og så er øjensynlig

$$det(\alpha^t) = det(\alpha) \quad \blacksquare$$

3.2. SÆTNING. Determinanten af en kvadratisk blokmatrix

$$\alpha = \left(\begin{array}{c|c} \beta & \gamma \\ \hline 0 & \delta \end{array}\right),$$

hvor $\beta \in Mat_p(R)$ og $\delta \in Mat_q(R)$ er kvadratiske matricer, $\gamma \in Mat_{p,q}(R)$ og 0 betegner nul-matricen $0 \in Mat_{q,p}(R)$, er:

$$\boxed{det\begin{pmatrix} \beta & \gamma \\ 0 & \delta \end{pmatrix} = det(\beta)\, det(\delta).}$$

BEVIS. Vi klasse-deler mængden $\{1, \cdots, n\}$ $(n = p+q)$ i de 2 delmængder $P = \{1, \cdots, p\}$ og $Q = \{p+1, \cdots, p+q\}$.

I summen

$$det(\alpha) = \sum_{\sigma \in S_n} sign(\sigma)\, \alpha_{\sigma_1 1} \cdots \alpha_{\sigma_n n}$$

behøver vi kun at summere over permutationer $\sigma \in S_n$ som opfylder $\sigma(P) \subseteq P$, thi hvis $\sigma \in S_n$ ikke opfylder dette, så findes $j \leq p$ med $\sigma_j > p$ og så vil det tilsvarende led

$$\operatorname{sign}(\sigma)\, \alpha_{\sigma_1 1} \cdots \alpha_{\sigma_m n}$$

indeholde faktoren $\alpha_{\sigma_j j}$, som er $= 0$ ifølge forudsætningen.

Permutationerne $\sigma \in S_n$ med $\sigma(P) \subseteq P$ må opfylde $\sigma(P) = P$ og $\sigma(Q) = Q$, og de kan derfor entydigt skrives $\sigma = \sigma' \circ \sigma''$, hvor σ' svarer til en permutation af P, dvs $\sigma \in S_p$, og σ'' svarer til en permutation af Q og dermed til en permutation $\sigma'' \in S_q$. Med disse identifikationer finder vi $\operatorname{sign}(\sigma) = \operatorname{sign}(\sigma')\operatorname{sign}(\sigma'')$ og dermed for det tilsvarende led:

$$\operatorname{sign}(\sigma)\, \alpha_{\sigma_1 1} \cdots \alpha_{\sigma_p p} \cdots \alpha_{\sigma_m n}$$

$$= \operatorname{sign}(\sigma')\, \beta_{\sigma'_1 1} \cdots \beta_{\sigma'_p p} \cdot \operatorname{sign}(\sigma'')\, \delta_{\sigma''_1 1} \cdots \delta_{\sigma''_q q}.$$

Og så følger påstanden ▨

3.3. KOROLLAR. Determinanten af en (kvadratisk) "øvre" blokmatrix

$$\begin{pmatrix} \beta_1 & \cdots & \cdots \\ & \beta_2 & \cdots \\ 0 & & \beta_s \end{pmatrix}$$

med kvadratiske matricer $\beta_1, \ldots, \beta_s$ langs diagonalen er

$$\det \begin{pmatrix} \beta_1 & \cdots & \cdots \\ & \beta_2 & \cdots \\ 0 & & \beta_s \end{pmatrix} = \det(\beta_1) \cdots \det(\beta_s).$$

BEVIS. Følger umiddelbart ved induktion efter s ▨

BEMÆRKNING. Af Sætning 3.1 fås nu et tilsvarende resultat om "nedre" blokmatricer.

SPECIELT. Determinanten af en øvre trekantsmatrix $\begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ er $\boxed{\det \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} = \lambda_1 \cdots \lambda_n}$.

Determinanten af en diagonalmatrix $\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$ er $\boxed{\det \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} = \lambda_1 \cdots \lambda_n}$.

Determinanten af enhedsmatricen $1_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ er $\boxed{\det \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = 1}$.

3.4. En matrix $\alpha \in \mathrm{Mat}_n(R)$ kan opfattes som et n-sæt $\alpha = (\alpha_1, \ldots, \alpha_n)$ bestående af matricens n-søjler (hvor altså hvert $\alpha_i \in R^n$.) Determinanten kan altså opfattes som en afbildning $\det : R^n \times \cdots \times R^n \to R$.

SÆTNING. Som funktion af matricens søjler er determinanten en alternerende n-lineær afbildning

$$\det : R^n \times \cdots \times R^n \to R.$$

BEVIS. For at vise, at afbildningen er n-lineær, skal vi for hvert $k = 1, \ldots, n$ vise, at afbildningen

$$x \longmapsto \det(\alpha_1, \ldots, x, \ldots, \alpha_n), \quad x \in R^n,$$

(hvor $x = (x_1, \ldots, x_n)$ er placeret som k-te søjle og de øvrige søjler $\alpha_j \in R^n$, $j \neq k$, er konstante) er lineær. Vi har

$$\det(\alpha_1, \ldots, x, \ldots, \alpha_n) = \sum_{\sigma \in S_n} \mathrm{sign}(\sigma)\, \alpha_{\sigma_1 1} \cdots x_{\sigma_j j} \cdots \alpha_{\sigma_n n}$$

Samler vi her for $i = 1, \ldots, n$ de led i hvilke faktoren x_i forekommer, får vi

$$\det(\alpha_1, \ldots, x, \ldots, \alpha_n) = A_1 x_1 + \cdots + A_n x_n,$$

hvor $A_i \in R$ kun afhænger af α_j, $j \neq k$. Heraf fremgår lineariteten.

For at vise, at afbildningen $\det$ er alternerende betragtes $\det(\alpha_1, \ldots, x, \ldots, x, \ldots, \alpha_n)$, hvor $x \in R^n$

er placeret som k-te og ℓ-te søjle ($k<\ell$). Vi har

$$\det(\alpha_1,\dots,x,\dots,x,\dots,\alpha_n)=\sum_{\sigma\in S_n}\operatorname{sign}(\sigma)\alpha_{\sigma_1,1}\cdots x_{\sigma_k}\cdots x_{\sigma_\ell}\cdots\alpha_{\sigma_n n}=\sum_{\sigma}\lambda_\sigma$$

hvor $\lambda_\sigma\in R$ betegner leddet svarende til $\sigma\in S_n$.

Er $S'\subset S_n$ delmængden bestående permutationer σ med $\sigma_k<\sigma_\ell$, består komplementærmængden $S''=S_n\setminus S'$ af permutationer $\tau\in S_n$ med $\tau_k>\tau_\ell$. I det (k,ℓ) betegner transpositionen, der ombytter k og ℓ, ses det at S'' består at permutationerne

$$\sigma\circ(k,\ell)\ ,\ \sigma\in S'.$$

Vi kan følgelig skrive

$$\begin{aligned}\det&=\sum_{\sigma\in S_n}\lambda_\sigma=\sum_{\sigma\in S'}\lambda_\sigma+\sum_{\tau\in S''}\lambda_\tau\\&=\sum_{\sigma\in S'}\lambda_\sigma+\sum_{\sigma\in S'}\lambda_{\sigma\circ(k,\ell)}\\&=\sum_{\sigma\in S'}\left(\lambda_\sigma+\lambda_{\sigma\circ(k,\ell)}\right).\end{aligned}$$

Her er

$$\begin{aligned}\lambda_{\sigma\circ(k,\ell)}&=\operatorname{sign}\left(\sigma\circ(k,\ell)\right)\alpha_{\sigma_1,1}\cdots x_{\sigma_\ell}\cdots x_{\sigma_k}\cdots\alpha_{\sigma_n n}\\&=-\operatorname{sign}(\sigma)\,\alpha_{\sigma_1,1}\cdots x_{\sigma_k}\cdots x_{\sigma_\ell}\cdots\alpha_{\sigma_n n}\\&=-\lambda_\sigma\end{aligned}$$

og følgelig er $\det=0$ ▨

3.5. Af Sætning 3.4 følger, at generelle resultater om alternerende n-lineære afbildninger (jfr. 2.3-6) kan anvendes på determinanten opfattet som funktion af matricens søjler. Af Sætning 3.1 fremgår, at det samme gælder dersom determinanten opfattes som funktion af matricens rækker.

SÆTNING. For produktet $\beta\alpha$ af kvadratiske matricer $\alpha,\beta\in\operatorname{Mat}_n(R)$ gælder $\boxed{\det(\beta\alpha)=\det(\beta)\det(\alpha).}$

BEVIS. Opfattes β som sættet $\beta = (\beta_1, \cdots, \beta_n)$ bestående af de n søjler i β kan vi med notationen fra 2.5 betragte sættet

$$(\gamma_1, \cdots, \gamma_n) = (\beta_1, \cdots, \beta_n)\alpha.$$

Opfattet som matrix $\gamma = (\gamma_1, \cdots, \gamma_n)$ gælder øjensynlig $\gamma = \beta\alpha$. Påstanden følger derfor af Sætning 2.6 ▨

4. Udviklinger. Cramers formel.

4.1. Lad $\alpha \in Mat_n(R)$ være en kvadratisk matrix med søjlerne $\alpha_1, \ldots, \alpha_n$, lad $x \in R^n$ og lad

$$(\alpha_1, \ldots, \overset{k}{\underset{\downarrow}{x}}, \ldots, \alpha_n)$$

betegne den matrix der fremgår af α ved at erstatte k-te søjle med søjlen x. Som nævnt i 3.4 har vi da

$$(*) \quad \det(\alpha_1, \ldots, \overset{k}{\underset{\downarrow}{x}}, \ldots, \alpha_n) = A_{k1}x_1 + \cdots + A_{kn}x_n,$$

hvor koefficienterne $A_{ki} \in R$ kun afhænger af matricen α (endda kun af søjlerne α_j, $j \neq k$)

DEFINITION. Elementet $A_{ki} \in R$ kaldes <u>komplementet</u> til den (i,k)-te plads i matricen α.

4.2. Idet $\delta_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}$ er den i-te søjle i enhedsmatricen, hvor altså $1 \in R$ er placeret på den i-te plads, får vi ved at indsætte $x = \delta_i$ i (*) ovenfor, at

$$\det(\alpha_1, \ldots, \overset{k}{\underset{\downarrow}{\delta_i}}, \ldots, \alpha_n) = A_{ki}$$

Flyttes her den k-te søjle i matricen, dvs δ_i, hen som første søjle er der anvendt en k-cykel. Da en k-cykel har fortegnet $(-1)^{k-1}$ følger det af Sætning 2.3 (og 3.5), at

$$\det(\delta_i, \alpha_1, \ldots, \alpha_{k-1}, \alpha_{k+1}, \ldots, \alpha_n) = (-1)^{k-1}A_{ki}$$

Flytter vi her den i-te række i matricen hen som første række får vi en matrix β, der tilsvarende har determinant

$$\det\beta = (-1)^{i-1}(-1)^{k-1}A_{ik} = (-1)^{i+k}A_{ki}.$$

Matricen β har imidlertid formen

$$\beta = \begin{pmatrix} 1 & & \\ 0 & & \\ \vdots & & \alpha_{\not i,\not k} \\ 0 & & \end{pmatrix}$$

hvor $\alpha_{\not i,\not k}$ betegner den $(n-1)\times(n-1)$ matrix der fremgår af α ved at slette i-te række og k-te søjle. Af Sætning 3.2 følger derfor, at vi har $\det\beta = \det(\alpha_{\not i,\not k})$, og dermed følgende:

SÆTNING. Komplementet A_{ki} til den (i,k)-te plads i matricen α er

$$\boxed{A_{ki} = (-1)^{k+i}\det(\alpha_{\not i,\not k}).}$$

BEMÆRKNING. Indsættes dette i ligningen 4.1 (*) får vi

$$\det(\alpha_1,\dots,\overset{k}{\overset{\downarrow}{x}},\dots,\alpha_n) = \sum_{i=1}^{n}(-1)^{k+i}\det(\alpha_{\not i,\not k})\,x_i,$$

der også kaldes <u>udvikling</u> af determinanten efter k-te søjle.

4.3. Idet vi med $\alpha^1,\dots,\alpha^n$ betegner de n rækker i matricen α får vi af Sætning 3.1, at for $y\in R^n$ gælder

$$\det\begin{pmatrix}\alpha^1\\ \vdots\\ y \leftarrow k\\ \vdots\\ \alpha^n\end{pmatrix} = B_{k1}y_1+\cdots+B_{kn}y_n$$

hvor B_{ki} er komplementet til den (i,k)-te plads i matricen α^t. Af den foregående Sætning (og Sætning 3.1) følger, at $B_{ki} = A_{ik}$. Vi har derfor

$$(*)^t \qquad \det\begin{pmatrix}\alpha^1\\ \vdots\\ y \leftarrow k\\ \vdots\\ \alpha^n\end{pmatrix} = y_1A_{1k}+\cdots+y_nA_{nk},$$

og dermed en tilsvarende udvikling af determinanten efter k-te række.

4.4. DEFINITION. Lad $\alpha \in Mat_n(R)$. Den matrix i $Mat_n(R)$, der på den (k,i)-te plads har komplementtal til den (i,k)-te plads i α, kaldes komplementmatricen til α. I det følgende vil vi betegne komplementmatricen til en kvadratisk matrix α med $\tilde{\alpha}$. Vi har altså

$$\tilde{\alpha}_{ij} = A_{ij} = (-1)^{i+j} \det(\alpha_{\hat{j},\hat{i}}).$$

Bemærk, at der i definitionen er indeholdt en form for transponering: Den i-te søjle i $\tilde{\alpha}$ (betegnet $\tilde{\alpha}_i$) indeholder komplementerne til i-te række i α og den j-te række i $\tilde{\alpha}$ (betegnet $\tilde{\alpha}^j$) indeholder komplementerne til j-te søjle i α.

Ved indsættelse i 4.1 (*) og 4.3 $(*)^t$ fås umiddelbart følgende

FORMLER. For en matrix $\alpha \in Mat_n(R)$ gælder

$$(*) \qquad \boxed{\det(\alpha_1, \dots, x, \dots, \alpha_n) = \tilde{\alpha}^k x,}$$

hvor $x \in R^n$ er placeret som k-te søjle, og

$$(*)^t \qquad \boxed{\det \begin{pmatrix} \alpha^1 \\ \vdots \\ y \\ \vdots \\ \alpha^n \end{pmatrix} = y \tilde{\alpha}_k,}$$

hvor $y \in R^n$ er placeret som k-te række.

4.5. SÆTNING. For en matrix $\alpha \in Mat_n(R)$ gælder

$$\boxed{\alpha \tilde{\alpha} = \tilde{\alpha} \alpha = \det(\alpha) 1,}$$

hvor $\det(\alpha) 1$ betegner den diagonalmatrix der har $\det(\alpha)$ overalt i diagonalen.

BEVIS. Elementet på plads (i,j) i produktmatricen $\tilde{\alpha}\alpha$ er (i-te række i $\tilde{\alpha}$)$\cdot$(j-te søjle i α), altså $\tilde{\alpha}^i\alpha_j$. Af formel 4.4 (*) følger, at

$$\tilde{\alpha}^i\alpha_j = \det(\alpha_1, \ldots, \overset{i}{\overset{\downarrow}{\alpha_j}}, \ldots, \alpha_n)$$

Matricen $(\alpha_1, \ldots, \overset{i}{\overset{\downarrow}{\alpha_j}}, \ldots, \alpha_n)$ har to ens søjler, hvis $i \neq j$, og dermed determinant $= 0$. Er derimod $i = j$, er matricen $= \alpha$, og dens determinant er altså $= \det(\alpha)$. Vi har følgelig

$$\tilde{\alpha}^i\alpha_j = \det(\alpha)\,\delta_{ij} \qquad \left(\delta_{ij} = \begin{cases} 0 & i \neq j \\ 1 & i = j \end{cases}\right)$$

og det er netop ligningen $\tilde{\alpha}\alpha = \det(\alpha)1$. Tilsvarende følger ligningen $\alpha\tilde{\alpha} = \det(\alpha)1$ af Formel 4.4 $(*)^t$ ▨

4.6 KOROLLAR. En matrix $\alpha \in \mathrm{Mat}_n(R)$ er invertibel i ringen $\mathrm{Mat}_n(R)$, hvis og kun hvis dens determinant $\det(\alpha)$ er invertibel i ringen R. I bekræftende fald er den inverse matrix α^{-1} givet ved $\alpha^{-1} = [\det(\alpha)]^{-1}\tilde{\alpha}$, hvor $\tilde{\alpha}$ betegner komplementmatricen til α.

BEVIS. "<u>hvis</u>": Er $\det(\alpha)$ invertibel, kan vi betragte matricen $\beta = [\det(\alpha)]^{-1}\tilde{\alpha} = \tilde{\alpha}[\det(\alpha)]^{-1}$. Af sætningen følger umiddelbart, at $\alpha\beta = \beta\alpha = 1$, og dermed at α er invertibel med $\alpha^{-1} = \beta$.

"<u>kun hvis</u>": Er α invertibel i $\mathrm{Mat}_n(R)$ så findes en matrix $\beta \in \mathrm{Mat}_n(R)$ med $\beta\alpha = \alpha\beta = 1$. Det følger, at

$$1 = \det(1) = \det(\alpha\beta) = \det(\alpha)\det(\beta),$$

og heraf ses, at $\det(\alpha)$ er invertibel i den kommutative ring R (med $\det(\alpha)^{-1} = \det(\beta)$) ▨

TILFØJELSE. En matrix $\alpha \in \mathrm{Mat}_n(R)$ er invertibel, hvis der findes en matrix $\beta \in \mathrm{Mat}_n(R)$, som opfylder blot den ene af betingelserne $\alpha\beta = 1$ og $\beta\alpha = 1$, thi hver af betingelserne medfører, at $\det(\alpha)\det(\beta) = 1$ og dermed, at $\det(\alpha) \in R$ er invertibel.

4.7. Hvis matricen $\alpha \in Mat_n(R)$ er invertibel, har ligningen

$$\alpha x = b,$$

hvor $a, x \in R^n$ opfattes som søjler, for hver værdi $b \in R^n$ en og kun én løsning $x \in R^n$, thi multiplikation med α^{-1} (fra venstre) giver ligningen

$$x = \alpha^{-1} b$$

og omvendt følger den oprindelige ligning heraf ved multiplikation med α.

Vi har $\alpha^{-1} = det(\alpha)^{-1} \tilde{\alpha}$, altså

$$x = det(\alpha)^{-1} \tilde{\alpha} b$$

og altså for $i = 1, \cdots, n$:

$$x_i = det(\alpha)^{-1} \tilde{\alpha}^i b.$$

Indsættelse i Formel 4.4 (*) giver $\tilde{\alpha}^i b = det(\alpha_1, \cdots, \overset{i}{\underset{\downarrow}{b}}, \cdots, \alpha_n)$ og dermed

CRAMER'S FORMEL. Løsningen $x \in R^n$ til ligningen $\alpha x = b$, hvor $det(\alpha)$ er invertibel, er bestemt ved

$$\boxed{x_i = \frac{det(\alpha_1, \cdots, \overset{i}{\underset{\downarrow}{b}}, \cdots, \alpha_n)}{det(\alpha_1, \cdots, \alpha_i, \cdots, \alpha_n)}}, \quad i = 1, \cdots, n.$$

4.8. DEFINITION. Gruppen af invertible elementer i ringen $Mat_n(R)$ kaldes den <u>generelle lineære gruppe</u> (over R) og den betegnes $GL_n(R)$. Ifølge Korollar 4.6 består den af de matricer $\alpha \in Mat_n(R)$ for hvilke $det(\alpha) \in R^*$. Vi kan øjensynlig opfatte determinanten som en gruppehomomorfi

$$det : GL_n(R) \to R^*.$$

Kernen heraf, der består af de matricer der har determinant 1, er altså en normal undergruppe i $GL_n(R)$. Den kaldes den <u>specielle lineære gruppe</u> (over R) og den betegnes

$$SL_n(R) \subseteq GL_n(R).$$

5. Rang og dimension.

5.1. De lineære afbildninger $R^p \to R^n$ er som bekendt netop afbildningerne af formen

$$x \longmapsto \alpha x,$$

hvor $x \in R^p$ opfattes som en søjle og $\alpha \in Mat_{n,p}(R)$ er en $(n \times p)$-matrix. Idet

$$\delta_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \ \ldots, \ \delta_p = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

er den kanoniske (fri) basis for R^p finder vi

$$\alpha_j := \alpha \delta_j = j\text{-te søjle i } \alpha.$$

Søjlerne i matricen α er altså billederne af elementerne i den kanoniske basis for R^p.

I tilfældet $p = n$ får vi altså beskrevet endomorfierne i R^n ved kvadratiske matricer $\alpha \in Mat_n(R)$.

5.2. SÆTNING. For en kvadratisk matrix $\alpha \in Mat_n(R)$ er følgende betingelser ekvivalente:

(i) Afbildningen $x \longmapsto \alpha x$ er surjektiv: $R^n \to R^n$.

(ii) Determinanten $\det(\alpha)$ er invertibel i R.

(iii) Matricen α er invertibel i $Mat_n(R)$

(iv) Afbildningen $x \longmapsto \alpha x$ er bijektiv: $R^n \to R^n$.

BEVIS. At (ii) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (iv) følger af overvejelserne i 4.6-7, og det er klart, at (iv) $\Rightarrow$ (i).

Er omvendt $x \longmapsto \alpha x$ surjektiv, kan vi løse hver af ligningerne

$$\alpha\beta_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \ \ldots, \ \alpha\beta_n = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \quad \text{med } \beta_j \in R^n.$$

Betegner $\beta \in Mat_n(R)$ matricen $\beta = (\beta_1, \ldots, \beta_n)$, kan lig-

ningerne sammenfattes til matrixligningen

$$\alpha\beta = 1,$$

og hvaf følger (som nævnt i 4.6), at $\det(\alpha)$ er invertibel ▨

5.3. SÆTNING. For en kvadratisk matrix $\alpha \in Mat_n(R)$ er følgende betingelser ækvivalente:

(i) Afbildningen $x \mapsto \alpha x$ er injektiv: $R^n \to R^n$

(ii) Determinanten $\det(\alpha)$ er regulær i ringen R

(iii) Matricen α er regulær i ringen $Mat_n(R)$.

BEVIS. (i) ⇒ (ii): Dette er en konsekvens af en efterfølgende mere generel sætning (Sætning 5.8).

(ii) ⇒ (iii): Antag, at vi for en matrix $\beta \in Mat_n(R)$ har

$$\alpha\beta = 0 \quad \text{(nul-matrix)}.$$

Multiplikation med komplementmatricen $\tilde{\alpha}$ fra venstre giver da (jfr. Sætning 4.5), at

$$\det(\alpha)\,\beta = 0.$$

For hvert element β_{ij} har vi altså $\det(\alpha)\beta_{ij} = 0$, og da vi har antaget, at $\det(\alpha) \in R$ er regulær, følger det, at $\beta_{ij} = 0 \in R$. Altså er $\beta = 0$ (nul-matrix).

Tilsvarende følger af $\beta\alpha = 0$, at $\beta = 0$. Og følgelig er α regulær i $Mat_n(R)$.

(iii) ⇒ (i): Antag, at $\alpha x = 0 \in R^n$, $x \in R^n$. For matricen $(x, 0, \cdots, 0)$, hvor første søjle er $x \in R^n$ og de øvrige søjler er $0 \in R^n$, har vi $\alpha(x, 0, \cdots, 0) = (0, \cdots, 0)$ (nul-matrix).

Da vi har antaget, at $\alpha \in Mat_n(R)$ er regulær følger, at $(x, 0, \cdots, 0)$ er nul-matricen. Specielt er første søjle $x = 0 \in R^n$.

Følgelig er afbildningen $x \mapsto \alpha x$ injektiv: $R^n \to R^n$. □

5.4. KOROLLAR. Hvis der findes en injektiv lineær afbildning: $R^p \to R^n$ og ringen R ikke er nulringen, så er $p \leq n$.

BEVIS. En lineær afbildning: $R^p \to R^n$ har formen $x \mapsto \alpha x$ med en matrix $\alpha \in Mat_{n,p}(R)$. Er afbildningen injektiv og er $n < p$, får vi ved sammensætning med den injektive lineære afbildning: $R^n \hookrightarrow R^p$ en injektiv afbildning: $R^p \to R^p$ af formen $x \mapsto \beta x$, hvor matricen $\beta \in Mat_p(R)$ fremgår af α ved at tilføje $p-n$ rækker, der alle er $= 0$. Af sætningen [mere præcist: af (i) $\Rightarrow$ (ii), som vi endnu ikke har bevist] følger nu, at $\det(\beta)$ er regulær i R. Da vi øjensynlig har $\det(\beta) = 0$, kan dette kun være tilfældet, når $1 = 0$, dvs når R er nulringen $\square$

BEMÆRKNING. Af korollaret følger specielt, at hvis M er en endeligt frembragt fri R-modul (og $R \neq 0$), så er elementantallet i en fri basis for M entydigt bestemt ved M, thi er $M \simeq R^n$ og $M \simeq R^p$ får vi $R^p \simeq R^n$ og dermed både $p \leq n$ og $n \leq p$.

Det fremhæves, at dette resultat afgørende forudsætter, at ringen R er kommutativ. Der findes en (ikke-kommutativ) ring Λ, der tillader en Λ-isomorfi: $\Lambda_s \xrightarrow{\sim} \Lambda_s^2$.

5.5. DEFINITION. Lad M være en R-modul. Ved <u>dimensionen</u> af M, betegnet $\dim M$, vil vi forstå det mindste antal elementer i et frembringersystem for M [vi sætter $\dim M = \infty$, hvis M ikke er endeligt frembragt]. Ved <u>rangen</u> af M, betegnet $\operatorname{rg} M$, vil vi forstå det største antal elementer i et frit system i M [vi sætter $\operatorname{rg} M = \infty$, hvis der i M findes vilkårligt store frie systemer].

BEMÆRKNING. En fri basis for en modul er på en gang et frembringersystem og et frit system. Følgelig gælder trivielt for en fri R-modul F, at $\dim F \leq \operatorname{rg} F$. Her gælder endda "=", idet vi mere generelt har følgende:

5.6. SÆTNING. Lad M være en R-modul ($R \neq 0$). Da er

$$\operatorname{rg} M \leq \dim M.$$

Hvis M er endeligt frembragt, så er M fri, hvis og kun hvis $\operatorname{rg} M = \dim M$.

BEVIS. Uligheden er triviel, hvis M ikke er endeligt frembragt. Det er derfor nok at vise, at hvis $v_1, \dots, v_n$ er et frembringersystem og $u_1, \dots, u_p$ er et frit system, så er $p \leq n$.

Frembringersystemet svarer til en surjektiv afbildning $v: R^n \to M$ og det frie system svarer til en injektiv afbildning $u: R^p \to M$. Da v er surjektiv, kan vi finde elementer $\alpha_1, \dots, \alpha_p \in R^n$ med $v(\alpha_j) = u_j$. Betegner $\alpha: R^p \to R^n$ den tilhørende lineære afbildning, har vi $v \circ \alpha = u : R^p \to M$. Da u er injektiv, er også α injektiv, og så følger $p \leq n$ af Korollar 5.4.

Hvis M er fri, gælder også den omvendte ulighed, og dermed "=". Er omvendt $\operatorname{rg} M = \dim M < \infty$, kan u og v som ovenfor bestemmes med $n = p$. Her er α injektiv, og altså $\det(\alpha)$ regulær i R (Sætning 5.3). Af $\alpha \tilde{\alpha} = \det(\alpha) 1$ følger nu, at også $\tilde{\alpha}$ (dvs $y \mapsto \tilde{\alpha} y$) er injektiv. Da $\det(\alpha) v = v \circ \det(\alpha) = v \circ \alpha \circ \tilde{\alpha} = u \circ \tilde{\alpha}$ er injektiv, er også v injektiv. Følgelig er v bijektiv, og altså $v_1, \dots, v_n$ en fri basis for M ▨

5.7. DEFINITION. Lad $\alpha \in Mat_{n,p}(R)$ være en matrix med n rækker og p søjler. Ved en $\underline{(q \times q)\text{-underdeterminant}}$ i α forstås determinanten af en delmatrix af α fremkommet ved at slette $n-q$ rækker og $p-q$ søjler. (Dette er naturligvis kun muligt, når $1 \leqslant q \leqslant \min\{n,p\}$).

(1×1)-underdeterminanterne er elementerne α_{ij}. For en kvadratisk matrix $\alpha \in Mat_n(R)$ er determinanten den eneste $(n\times n)$-underdeterminant i α.

Lad $\alpha \in Mat_{n,p}(R)$. Vi vil kalde α $\underline{\underline{\text{søjlesingulær}}}$, hvis der findes et element $a \in R$ så at

$$a \neq 0 \quad \text{og} \quad a\Delta = 0$$

for enhver $(p\times p)$-underdeterminant Δ i α. Er dette ikke opfyldt, vil vi kalde α $\underline{\underline{\text{søjleregulær}}}$.

OBSERVATION 1. Hvis der findes en søjlesingulær matrix kan R ikke være nul-ringen, thi specielt forudsættes, at der findes et element $\neq 0$ i R.

OBSERVATION 2. Hvis $n < p$ (og $R \neq 0$), så er enhver matrix $\alpha \in Mat_{n,p}(R)$ søjlesingulær, thi i dette tilfælde findes ingen $(p\times p)$-underdeterminanter i α.

OBSERVATION 3. En kvadratisk matrix $\alpha \in Mat_n(R)$ $(n=p)$ er søjleregulær, netop når $\det(\alpha)$ er et regulært element i R.

OBSERVATION 4. Hvis R er et integritetsområde, så er en matrix $\alpha \in Mat_{n,p}(R)$ søjlesingulær, netop når alle $(p\times p)$-underdeterminanter i α er $=0$.

5.8. SÆTNING. Hvis $\alpha \in Mat_{n,p}(R)$ er søjlesingulær, så har ligningen $\alpha x = 0$, $x \in R^p$, en løsning $x \neq 0$.

BEVIS. Vi kan antage, at $n \geq p$, thi er $n < p$ kan vi til α tilføje $p-n$ rækker, der alle er $= 0$. Den herved fremkomne $(p \times p)$-matrix $\hat{\alpha}$ er stadig søjlesingulær (idet $\det(\hat{\alpha}) = 0$), og ligningerne $\alpha x = 0$ og $\hat{\alpha} x = 0$ har de samme løsninger $x \in R^p$.

Betragt nu det største tal $q \geq 0$, så at der findes q søjler i α, som udgør en søjleregulær matrix. Vi kan uden indskrænkning antage, at matricen $(\alpha_1, \ldots, \alpha_q)$ bestående af de q første søjler i α er søjleregulær. I følge forudsætningen om α er $q < p$, og valget af q sikrer, at dersom vi tilføjer ydeligere en søjle, f.eks. α_{q+1}, så får vi en søjlesingulær matrix $(\alpha_1, \ldots, \alpha_q, \alpha_{q+1})$. Vi kan antage, at $q+1 = p$, thi er $y \in R^{q+1}$ en løsning til $(\alpha_1, \ldots, \alpha_{q+1})\, y = 0$, så definerer vi ved

$$x = \begin{pmatrix} y_1 \\ \vdots \\ y_{q+1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

en løsning til $\alpha x = 0$.

Da $\alpha \in \mathrm{Mat}_{n,p}(R)$ er søjlesingulær, findes $a \neq 0$ i R så at

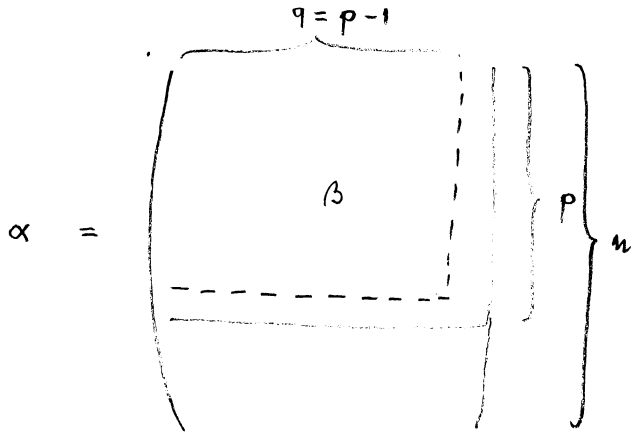
$$(*) \qquad \Delta a = 0$$

for enhver $(p \times p)$-underdeterminant Δ i α. Da vi har antaget, at matricen $(\alpha_1, \ldots, \alpha_{p-1})$ bestående af de første $q = p-1$ søjler ikke er søjlesingulær, findes heri en $(p-1) \times (p-1)$-underdeterminant δ, så at

$$(**) \qquad \delta a \neq 0.$$

Vi kan uden indskrænkning antage, at δ er determinanten af delmatricen bestående af de første $p-1$ rækker i $(\alpha_1, \ldots, \alpha_{p-1})$. Er β $(p \times p)$-matricen bestående af de første p rækker i α har vi derfor

$$\delta = \det(\beta_{\ast,\ast}).$$



De p rækker i matricen β er de p første rækker $\alpha^1, \dots, \alpha^p$ i matricen α. Komplementerne til den p-te række i β er den p-te søjle $\tilde{\beta}_p$ i komplementmatricen $\tilde{\beta}$. Af Formel 4.4 følger nu, at vi for en vilkårlig række α^i, $i = 1, \dots, n$ i α har

$$\alpha^i \tilde{\beta}_p = \det \begin{pmatrix} \alpha^1 \\ \vdots \\ \alpha^{p-1} \\ \alpha^i \end{pmatrix} = \begin{cases} 0 & \text{hvis } i < p \\ (p \times p)\text{-underdeterminant} \\ \text{i } \alpha, \text{ hvis } p \leq i \leq n. \end{cases}$$

Sættes $x = \tilde{\beta}_p a \in R^p$ følger det derfor af (*), at vi har $\alpha^i x = 0$, $i = 1, \dots, n$, altså

$$\alpha x = 0.$$

På den anden side er $x_p = \tilde{\beta}_{pp} a = \det(\beta_{p,p}) a = \delta a \neq 0$ ifølge (**), og specielt altså

$$x \neq 0 \quad \square$$

BEMÆRKNING. Som nævnt i Observation 5.7.3 giver denne sætning den manglende implikation (i) $\Rightarrow$ (ii) i Sætning 5.3. Lidt mere generelt fås følgende:

5.9. SÆTNING. For en matrix $\alpha \in \mathrm{Mat}_{n,p}(R)$ er følgende betingelser ækvivalente:

(i) Afbildningen $x \mapsto \alpha x$ er injektiv: $R^p \to R^n$

(ii) Søjlerne i α udgør et frit system i R^n.

(iii) Matricen α er søjleregulær.

BEVIS. For $x \in R^p$ har vi

$$\alpha x = \alpha_1 x_1 + \cdots + \alpha_p x_p .$$

Altså er søjlerne et frit system i R^n, hvis og kun hvis ligningen $\alpha x = 0$, $x \in R^p$, kun har løsningen $x = 0$, og følgelig gælder <u>(i) $\Leftrightarrow$ (ii)</u>.
At <u>(i) $\Rightarrow$ (iii)</u> er indholdet af Sætning 5.8.
<u>(iii) $\Rightarrow$ (i)</u>: Antag, at $\alpha x = 0$. Da gælder for hver række α^i i α, at $\alpha^i x = 0$, og følgelig gælder for hver delmatrix β bestående af p rækker af α, at $\beta x = 0$. Multipliceres her fra venstre med komplementmatricen $\tilde{\beta}$ fås (Sætning 4.5):

$$0 = \tilde{\beta}\beta x = \det(\beta)\, x .$$

For hvert $j = 1, \cdots, p$ har vi altså $\Delta x_j = 0$ for hver $(p \times p)$-underdeterminant $\Delta = \det(\beta)$ af α. Da α antages søjleregulær, følger heraf $x_j = 0$, $j = 1, \cdots, p$. Altså er $x = 0$ ▨

BEMÆRKNING. Det følger, at det i beviset for Sætning 5.8 benyttede tal q kan beskrives som det største antal af matricens søjler, der udgør et frit system. Det kaldes også matricens <u>søjlerang</u>. Hvis R er et integritetsområde, er søjlerangen af matricen $\alpha \in \mathrm{Mat}_{n,p}(R)$ det største tal q, for hvilket der i α findes en $(q \times q)$-underdeterminant $\neq 0$ (jfr. Observation 5.4.4.).

Det fremgår, at der under denne forudsætning gælder, at matricens <u>rækkerang</u> (dvs søjlerangen af den transponerede matrix) stemmer overens med søjlerangen.
Det bemærkes, at et tilsvarende resultat ikke gælder for vilkårlige ringe R.

5.10. SÆTNING. For en matrix $\alpha \in Mat_{n,p}(R)$ er følgende betingelser ækvivalente:

(i) Afbildningen $x \mapsto \alpha x$ er surjektiv: $R^p \to R^n$

(ii) Søjlerne i α udgør et frembringersystem i R^n.

(iii) Elementet $1 \in R$ er en R-linearkombination af $(n \times n)$-underdeterminanter i α.

BEVIS. Af $\alpha x = \alpha_1 x_1 + \cdots + \alpha_p x_p$ fås (i) $\Leftrightarrow$ (ii).

(i) $\Rightarrow$ (iii): For hver matrix γ og $q = 1, 2, \ldots$ betegner vi med

$$\mathcal{O}\ell_q(\gamma) \subseteq R$$

idealet frembragt af $(q \times q)$-underdeterminanterne i γ. Søjlerne i et matrixprodukt $\alpha\beta$ er linearkombinationer af søjlerne i α. Da determinanten er multilinear (og alternerende) følger det, at enhver $(q \times q)$-underdeterminant i $\alpha\beta$ er en linearkombination af $(q \times q)$-underdeterminanter i α, og heraf følger videre, at

$$\mathcal{O}\ell_q(\alpha\beta) \subseteq \mathcal{O}\ell_q(\alpha).$$

Antages, at $x \mapsto \alpha x$ er surjektiv: $R^p \to R^n$, kan vi for hver af søjlerne $\delta_1, \ldots, \delta_n$ i enhedsmatricen $1_n = (\delta_1, \ldots, \delta_n) \in Mat_n(R)$ finde en søjle $\beta_i \in R^p$ med $\alpha\beta_i = \delta_i$. For matricen $\beta = (\beta_1, \ldots, \beta_n) \in Mat_{p,n}(R)$ har vi altså $\alpha\beta = 1_n$, og så er

$$1 \in \mathcal{O}\ell_n(1_n) = \mathcal{O}\ell_n(\alpha\beta) \subseteq \mathcal{O}\ell_n(\alpha),$$

hvoraf påstanden.

(iii) $\Rightarrow$ (i): Vi kan antage, at $R \neq 0$. Af (iii) følger så specielt, at $n \leq p$. Lad os et øjeblik for en given række $y \in R^p$ og en given delmængde $J \subseteq \{1, \ldots, p\}$ med n elementer med

$$[J, y] \in Mat_n(R)$$

betegne den matrix, der fremgår af α ved at erstatte første række α^1 med y og dernæst betragte delmatri-

cen bestående af søjler med index i J. For en række α^i i α finder vi

$$(*) \qquad \det[J, \alpha^i] = \begin{cases} (n\times n)\text{-underdeterminant i } \alpha, \text{ når } i = 1 \\ 0, \text{ når } i > 1, \end{cases}$$

idet matricen i det sidste tilfælde har 2 ens rækker. På den anden side viser udvikling efter første række i matricen $[J, y]$, at det $[J, y]$ er en linearkombination af y_j, $j \in J$, med koefficienter, der kun afhænger af matricen α. Vi kan specielt skrive

$$\det[J, y] = y_1 A_{1,J} + \cdots + y_p A_{p,J},$$

med koefficienter $A_{i,J} \in R$, der kun afhænger af α og den givne delmængde J. Er $A_J \in R^p$ søjlen bestående af disse koefficienter, kan ligningen skrives

$$(**) \qquad \det[J, y] = y A_J.$$

Ifølge antagelsen er $1 \in R$ en R-linearkombination af $(n\times n)$-underdeterminanter i α, og denne relation kan med den indførte notation skrives

$$1 = \sum_J \lambda_J \det[J, \alpha^1].\,, \quad \lambda_J \in R,$$

hvor der summeres over alle delmængder $J \subseteq \{1, \ldots, p\}$ med n elementer. Sættes

$$w = \sum_J \lambda_J A_J \in R^p,$$

kan relationen ifølge $(**)$ skrives

$$\alpha^1 w = 1.$$

Af $(*)$ og $(**)$ følger videre, at vi har

$$\alpha^i w = 0, \quad \text{når } i > 1.$$

Altså er

$$\alpha w = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in R^n$$

Tilsvarende kan vi for hver af de øvrige søjler $\delta_2, \ldots, \delta_n$ i enhedsmatricen $1_n \in \mathrm{Mat}_n(R)$ løse ligningen

$$\alpha w_i = \delta_i,$$

og så er $x \mapsto \alpha x$ øjensynlig surjektiv : $R^p \to R^n$ ▨

MODULER OVER HOVEDIDEALOMRÅDER

1. Frie moduler. Rang og dimension. 1.1-2: Sætning om undermodul i en endeligt frembragt fri modul. Dimension af undermodul.

2. Torsionsfrie moduler. 2.1: Definition af torsionsfri. 2.2: Observationer. 2.3: Sætning om endeligt frembragte torsionsfri moduler. 2.4: Definition af torsion. 2.5: Lemma. Sætning.

3. Matricer over hovedidealområder. 3.1-2: Elementære operationer. 3.3-4: Specielle operationer. 3.5: Lemma. 3.6: Elementardivisorsætningen. 3.7: Korollar om SL_p. 3.8: Tilfældet, hvor der findes en numerisk funktion.

4. Basissætningen. 4.1: Lemma. 4.2: Basissætningen. 4.3: Bemærkning. 4.4: Korollar om minimal annullator. 4.5: Eksempel $R = \mathbb{Z}$. 4.6: Sætning om endelig længde af cyklisk modul. 4.7: Sætning om karakterisering af endeligt frembragte torsionsmoduler. 4.8-10. Primære elementer. Primær basis. 4.11: Definition af karakteristisk element. 4.12-14: Sætninger om karakteristisk element. 4.15: Eksempel: $R = \mathbb{Z}$. 4.16: Sætning om karakteristisk element for $R^n/\alpha(R^n)$.

5. Endomorfier i vektorrum. 5.1: Jordan's normalform. 5.2: Matricer hørende til endomorfier. 5.3-10: Oversættelse til $L[X]$-moduler. 5.11: $L[X]$-moduler af endelig længde. 5.12: Minimalt polynomium. 5.13: Karakteristisk polynomium. 5.14: Hamilton-Cayley's sætning. 5.15: Egenværdi og egenvektor. 5.16: Hovedsætning. 5.17: Komplekse endomorfier. 5.18: Reelle endomorfier.

MODULER OVER HOVEDIDEALOMRÅDER

I det følgende betegner R et hovedidealområde. [Et hovedidealområde hedder på engelsk 'Principal Ideal Domain (PID)']. Ringen R er altså et kommutativt integritetsområde hvori ethvert ideal er et hovedideal. For hovedidealet frembragt af $\lambda \in R$ skriver vi $R\lambda = (\lambda)$.

1. Frie moduler. Rang og dimension.

1.1. Lad M være en R-modul. Ved rangen af M, betegnet $\operatorname{rg} M$, forstås som bekendt det største antal elementer, der kan være i et frit system fra M (Findes vilkårligt store (endelige) frie systemer, sættes $\operatorname{rg} M = \infty$).
Ved dimensionen af M, betegnet $\dim M$, forstår vi som bekendt det mindste antal elementer, der frembringer M (Er M ikke endeligt frembragt, sættes $\dim M = \infty$).

Som bekendt gælder generelt for R-moduler, at

$$\operatorname{rg} M \leqslant \dim M.$$

For en fri modul F gælder $\operatorname{rg} F = \dim F$ og dette tal er det fælles elementantal i alle frie baser for F.

1.2. SÆTNING. Lad F være en endeligt frembragt fri R-modul. Da er enhver undermodul $N \subseteq F$ en endeligt frembragt fri modul, og $\operatorname{rg} N \leqslant \operatorname{rg} F$.

BEVIS. Påstanden vises ved induktion efter $n = \operatorname{rg} F$. Hvis $n = 0$, så er $F = (0)$ (Vi vedtager, at den tomme mængde er en basis for nul-modulen), og påstanden er triviel. Hvis $n = 1$, kan vi antage, at $F = R$. En under-

modul $N \subseteq R$ er altså et ideal i R. Da R er et hovedidealområde, er N af formen $N = Ra$, $a \in R$. Hvis $a = 0$, så er $N = (0)$ fri af rang 0, og hvis $a \neq 0$, så er $N = Ra$ fri af rang 1 (med a som fri basis).

I induktionsskridtet betragtes en fri modul F af rang $n+1$ og en undermodul $N \subseteq F$, og det antages, at sætningen gælder for frie moduler af rang n. Vi kan antage, at $F = R^{n+1}$, og vi betragter den R-lineære afbildning $: R^{n+1} \to R^n$ bestemt ved

$$\begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_n \end{pmatrix} \longmapsto \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

Kernen K for denne afbildning består af $(n+1)$-sæt $\begin{pmatrix} \lambda \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, hvor $\lambda \in R$, og K er derfor fri af rang 1 (med basis $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$).

Lad $\bar{N} \subseteq R^n$ betegne billedet af undermodulen $N \subseteq R^{n+1}$. Ved restriktion fås en surjektiv R-lineær afbildning $: N \to \bar{N}$, hvis kerne er $N_0 = N \cap K$. Ifølge det allerede viste er $N_0 \subseteq K$ fri af rang ≤ 1 og ifølge induktionsantagelsen er $\bar{N} \subseteq R^n$ fri af rang $\leq n$, og så følger som bekendt, at N er fri af rang $= \operatorname{rg} N_0 + \operatorname{rg} \bar{N} \leq 1 + n = n+1$. ▨

KOROLLAR. Lad M være en endeligt frembragt R-modul. Da er enhver undermodul $N \subseteq M$ endeligt frembragt, og $\dim N \leq \dim M$.

BEVIS. Vælg et frembringersystem $(e_1, \ldots, e_d)$ for M med $d = \dim M$, og betragt den tilhørende surjektive R-lineære afbildning $f : R^d \to M$. Originalmængden $f^{-1}(N)$ er da en undermodul i R^d, og altså ifølge sætningen fri af en rang n, med $n \leq d$. Følgelig er $f^{-1}(N)$ isomorf med R^n og ved sammensætning fås en surjektiv R-lineær afbildning

$$R^n \xrightarrow{\sim} f^{-1}(N) \xrightarrow{f} f(f^{-1}(N)) = N.$$

Men så kan N frembringes af n elementer, og derfor er

$$\dim N \leqslant n \leqslant d \quad \blacksquare$$

2. Torsionsfri moduler.

Vi minder om, at R stadig er et hovedidealområde.

2.1. DEFINITION. Et fit element x i en R-modul M kaldes også torsionsfrit. Som bekendt betyder det, at der for $\lambda \neq 0$ i R gælder $\lambda x \neq 0$. En R-modul M kaldes torsionsfri, hvis alle elementer $x \neq 0$ i M er torsionsfri. Betingelsen er altså, at vi for $\lambda \in R$ og $x \in M$ kun har $\lambda x = 0$, når $\lambda = 0$ eller $x = 0$.

2.2. OBSERVATIONER. (1) En undermodul af en torsionsfri modul er selv torsionsfri.

(2) En endeligt frembragt fri R-modul F er torsionsfri, thi er $e_1, \dots, e_n$ en fri basis, og er $\lambda \in R \setminus \{0\}$ og $x \in M$ med $\lambda x = 0$, så kan vi skrive $x = \lambda_1 e_1 + \cdots + \lambda_n e_n$, og af $0 = \lambda x = \lambda\lambda_1 e_1 + \cdots + \lambda\lambda_n e_n$ følger $\lambda\lambda_i = 0$ og dermed $\lambda_i = 0$ (da nulreglen gælder i R), $i = 1, \dots, n$, og så er $x = 0$.

EKSEMPEL. Ethvert vektorrum V over et legeme L af karakteristik 0 (dvs $L \supseteq \mathbb{Z}$) er torsionsfrit som $\mathbb{Z}$-modul, thi af $nv = 0$, $n \in \mathbb{Z} \setminus \{0\}$ følger $v = \frac{1}{n}(nv) = 0$ idet jo $\frac{1}{n} \in L$.

2.3. SÆTNING. Lad M være en endeligt frembragt torsionsfri modul over R. Da er M en fri modul.

BEVIS. Vi viser, at ethvert frembringersystem $e_1, \dots, e_d \in M$ med det mindst mulige antal elementer, dvs $d = \dim M$, er en fri basis. Lad $M' \subseteq M$ være undermodulen frembragt af $e_1, \dots, e_{d-1}$, altså

$$M' = Re_1 + \cdots + Re_{d-1}.$$

Her er $\dim M' = d-1$, thi ellers kunne M' frembringes af færre end $d-1$ elementer, og så ville disse elementer suppleret med e_d være et frembringersystem for M med færre end d elementer.

Idet beviset føres ved induktion efter d, kan vi antage, at $e_1, \dots, e_{d-1}$ er en fri basis for M'. Hvis $e_1, \dots, e_d$ ikke var et frit system, ville der findes en egentlig lineær relation

$$(*) \quad \lambda_1 e_1 + \dots + \lambda_{d-1} e_{d-1} + \lambda_d e_d = 0, \quad \lambda_1, \dots, \lambda_{d-1}, \lambda_d \in R$$

Her gælder om koefficienten λ_d, at

$$\lambda_d \neq 0,$$

thi ellers ville $(*)$ være en egentlig relation mellem $e_1, \dots, e_{d-1}$.

Af $(*)$ følger, at $\lambda_d e_d \in M'$. Da vi trivielt har $\lambda_d e_i \in M'$, $i = 1, \dots, d-1$, slutter vi, at

$$\lambda_d M \subseteq M'.$$

Nu er $x \mapsto \lambda_d x$ en R-lineær afbildning, med billede $\lambda_d M \subseteq M'$. Da $\dim M' = d-1$ følger det af Korollar 1.4, at $\dim(\lambda_d M) \leq d-1$. På den anden side er $x \mapsto \lambda_d x$ en injektiv homomorfi, da $\lambda_d \neq 0$ og M er torsionsfri, og så er M isomorf med billedet $\lambda_d M$, i modstrid med at $\dim M = d$ ▨

BEMÆRK. Forudsætningen om at M er endeligt frembragt er nødvendig. F.eks. er R's brøklegeme $K \supseteq R$ som R-modul torsionsfri og af rang 1 (hvorfor?), og heraf følger lit, at K kun kan være fri som R-modul, når $R = K$, dvs når R er et legeme.

2.4. DEFINITION. Lad M være en R-modul. Et element $x \in M$ kaldes et <u>torsionselement</u>, hvis det ikke er torsionsfrit, dvs hvis der findes $\mu \in R$, $\mu \neq 0$, så at $\mu x = 0$. Mængden af torsionselementer i M kaldes <u>torsionsundermodulen</u> i M og betegnes M_{tor}. M er <u>torsionsmodul</u>, hvis $M_{tor} = M$.

BEMÆRKNING. Delmængden $M_{tor} \subseteq M$ af torsionselementer er en undermodul, thi $0 \in M_{tor}$, da $1 \cdot 0 = 0$, og er $x \in M_{tor}$ med $\mu x = 0$, $\mu \in R \setminus \{0\}$, så er også $\mu(\lambda x) = \lambda \mu x = 0$, og dermed $\lambda x \in M_{tor}$, $\lambda \in R$, og er også $y \in M_{tor}$ med $\gamma y = 0$, $\gamma \in R \setminus \{0\}$, så er $\mu\gamma(x+y) = \gamma\mu x + \mu\gamma y = 0$, og her er $\mu\gamma \neq 0$, og altså $x + y \in M_{tor}$.

2.5. LEMMA. Lad M være en R-modul. Da er kvotienten M/M_{tor} en torsionsfri R-modul.

BEVIS. Lad $X \in M/M_{tor}$, og antag, at $\lambda X = 0$, med $\lambda \in R \setminus \{0\}$. Lad $x \in M$ være en repræsentant for X. Da er i M/M_{tor}:

$$0 = \lambda X = \lambda \textcircled{x} = \textcircled{\lambda x},$$

og følgelig er $\lambda x \in M_{tor}$ og altså et torsionselement i M. Der findes derfor $\mu \in R \setminus \{0\}$, så at $\mu\lambda x = 0$. Da $\mu\lambda \neq 0$ følger heraf, at også $x \in M_{tor}$, og så er $X = \textcircled{x} = 0$ i M/M_{tor} □

SÆTNING. Lad M være en endeligt frembragt R-modul. Da er torsionsundermodulen M_{tor} direkte sumand i M og ethvert komplement til M_{tor} er en fri R-modul af rang $\operatorname{rg} M$.

BEVIS. Da M er endeligt frembragt er også kvotienten M/M_{tor} endeligt frembragt, og da den er torsionsfri ifølge lemmaet, er den fri ifølge Sætning 2.3. Heraf følger, at M_{tor} er direkte sumand i M. Et komplement K afbildes ved den kanoniske homomorfi $: M \to M/M_{tor}$

isomorft på M/M_{tor}. Følgelig er K fri af rang $n := rg\,K = rg(M/M_{tor})$. Det er klart, at der for undermodulen $K \subseteq M$ gælder $rg\,K \leq rg\,M$.

Omvendt vil ethvert frit system i M med p elementer frembringe en fri undermodul $F \subseteq M$ af rang p. Da F er torsionsfri (Observation 2.2.(2)) er $F \cap M_{tor} = (0)$, så ved den kanoniske homomorfi $M \to M/M_{tor}$ afbildes F isomorft på en undermodul i M/M_{tor}. Men så er $p = rg\,F \leq rg\,M/M_{tor} = rg\,K$, og følgelig er $rg\,M \leq rg\,K$ ▨

3. Matricer over hovedidealområder

3.1. Lad $\alpha \in Mat_{n,p}(R)$ være en matrix med de p søjler $\alpha_1, \ldots, \alpha_p$. At omforme α med en <u>elementær søjleoperation</u> betyder, at man til én af søjlerne i α addérer et multiplum af en af de øvrige, altså at man for passende $j \neq k$ erstatter j-te søjle α_j med $\alpha_j + \lambda\alpha_k$, $\lambda \in R$.

EKSEMPEL. Successive søjleoperationer omformer:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

og når $\varepsilon \in R$ er invertibel:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & \varepsilon \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} \varepsilon & \varepsilon \\ 1-\varepsilon^{-1} & 1 \end{pmatrix} \mapsto \begin{pmatrix} \varepsilon & 0 \\ 1-\varepsilon^{-1} & \varepsilon^{-1} \end{pmatrix} \mapsto \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}.$$

OBSERVATION. Med elementære søjleoperationer kan man:

(1) Multiplicere en søjle med et invertibelt element $\varepsilon \in R$ (specielt med -1), når samtidig en anden søjle multipliceres med ε^{-1}, og

(2) Permutere søjlerne, når samtidig én af søjlerne multipliceres med permutationens fortegn,

thi (2) reduceres let til tilfældet hvor permutationen er en transposition og så vedrører (1) og (2) kun to søjler og det er essentielt de 2 omformninger behandlet i eksemplet ovenfor.

BEMÆRKNING. Tilsvarende resultater gælder naturligvis for <u>elementære rækkeoperationer</u>.

3.2. Idet $\delta_1, \ldots, \delta_p \in R^p$ betegner de p søjler i enhedsmatricen

$$1 = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in Mat_p(R),$$

har vi

$$(\alpha_1, \dots, \underset{\downarrow j}{\alpha_j + \lambda\alpha_k}, \dots, \alpha_p) = (\alpha_1, \dots, \alpha_p)\,(\delta_1, \dots, \underset{\downarrow j}{\delta_j + \lambda\delta_k}, \dots, \delta_p).$$

Den elementære søjleoperation beskrevet i 3.1 kan altså udføres ved at multiplicere matricen $\alpha \in Mat_{n,p}(R)$ fra højre med matricen

$$(\delta_1, \dots, \delta_j + \lambda\delta_k, \dots, \delta_p) = \begin{pmatrix} 1 & & \overset{\downarrow j}{\lambda} & & \\ & \ddots & \vdots & & \\ & & 1 & & \\ & 0 & & \ddots & \\ & & & & 1 \end{pmatrix} \leftarrow k$$

hvor $j, k \in \{1, \dots, p\}$, $j \neq k$, og $\lambda \in R$. En sådan matrix siges at være en <u>elementær</u> matrix. Den "inverse" søjleoperation fås øjensynlig ved at erstatte λ med $-\lambda$. Heraf følger, at en elementær matrix er invertibel og at den inverse matrix igen er elementær.

Successive søjleoperationer på en matrix $\alpha \in Mat_{n,p}(R)$ kan altså udføres ved at multiplicere α fra højre med et endeligt produkt af elementære matricer i $Mat_p(R)$. Det fremgår, at mængden af sådanne endelige produkter af elementære matricer udgør en undergruppe i $GL_p(R)$. Vi kalder den den <u>elementære</u> undergruppe i $GL_p(R)$, og vi betegner den

$$E_p(R).$$

EKSEMPEL. Søjleoperationerne fra Eksempel 3.1 svarer til identiteterne

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

og (for $\varepsilon \in R^*$)

$$\begin{pmatrix} 1 & \varepsilon \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1-\varepsilon^{-1} & 1 \end{pmatrix}\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \varepsilon - 1 & 1 \end{pmatrix} = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}.$$

Disse matricer tilhører altså gruppen $E_2(R)$.

BEMÆRKNING. Tilsvarende kan naturligvis elementære rækkeoperationer på matricen $\alpha \in Mat_{n,p}(R)$ udføres

ved at multiplicere α fra venstre med en matrix i den elementære gruppe $E_n(R)$.

3.3. Til de elementære søjleoperationer nævnt i 3.1 vil vi her føje den <u>specielle søjleoperation</u> der består i for givne

$$\lambda_1, \lambda_2, \mu_1, \mu_2 \in R \quad \text{med} \quad \lambda_1\mu_2 - \lambda_2\mu_1 = 1$$

at erstatte $\alpha = (\alpha_1, \alpha_2, \cdots, \alpha_p)$ med $(\lambda_1\alpha_1 + \lambda_2\alpha_2, \mu_1\alpha_1 + \mu_2\alpha_2, \cdots, \alpha_p)$.

Denne specielle søjleoperation udføres øjensynlig ved at multiplicere $(n \times p)$-matricen α fra højre med den <u>speciele</u> $(p \times p)$-matrix

$$\begin{pmatrix} \lambda_1 & \mu_1 & & \\ \lambda_2 & \mu_2 & & \\ & & 1 & \\ & & & \ddots \\ & & & & 1 \end{pmatrix} \qquad \lambda_1\mu_2 - \lambda_2\mu_1 = 1$$

OBSERVATION. De speciele søjleoperationer berører kun de to første søjler i matricen α. Da vi ved hjælp af elementære søjleoperationer kan permutere søjlerne, jfr. Observation 1, kan vi hermed lave operationer svarende til de speciele på vilkårlige to givne søjler i α.

BEMÆRKNING. Tilsvarende kan en <u>speciel rækkeoperation</u> udføres ved at multiplicere α fra venstre med en speciel $(n \times n)$-matrix.

3.4. En elementær matrix er specielt en (øvre eller nedre) trekantsmatrix med 1'er i diagonalen og den har derfor determinant $= 1$. Det følger, at den elementære undergruppe $E_p(R)$ er en undergruppe

$$E_p(R) \subseteq SL_p(R)$$

i den speciele lineære gruppe (bestående af $(p \times p)$-matricer med determinant 1). En speciel (2×2)-matrix $\begin{pmatrix} \lambda_1 & \mu_1 \\ \lambda_2 & \mu_2 \end{pmatrix}$ har ifølge definitionen determinant $\lambda_1\mu_2 - \lambda_2\mu_1 = 1$.

Heraf følger, at enhver speciel matrix har determinant 1 [samt at den "inverse" til en speciel operation igen er en speciel operation svarende til matricen

$$\begin{pmatrix} \lambda_1 & \mu_1 \\ \lambda_2 & \mu_2 \end{pmatrix}^{-1} = \begin{pmatrix} \mu_2 & -\mu_1 \\ -\lambda_2 & \lambda_1 \end{pmatrix} \ ]$$

Specielt følger dit, at elementære og speciælle operationer anvendt på en kvadratisk matrix ikke ændre matricens determinant.

3.5. LEMMA. Lad R være et hovedidealområde og lad $\alpha_1, \alpha_2 \in R$. Da kan (1×2)-matricen (α_1, α_2) med en speciel søjleoperation omformes til $(\delta, 0)$, hvor δ er en største fælles divisor for α_1 og α_2.

BEVIS. En største fælles divisor δ er en frembringer for (hoved-)idealet $R\alpha_1 + R\alpha_2$. Vi har altså dels

$$\delta = \lambda_1\alpha_1 + \lambda_2\alpha_2 \quad \text{med} \quad \lambda_1, \lambda_2 \in R$$

dels

$$\alpha_1 = \mu_1\delta \ , \quad \alpha_2 = \mu_2\delta \quad \text{med} \quad \mu_1, \mu_2 \in R.$$

Vi kan antage $\delta \neq 0$, og får derfor

$$1 = \lambda_1\mu_1 + \lambda_2\mu_2 \ , \quad \mu_2\alpha_1 = \mu_1\alpha_2$$

og så er

$$\begin{pmatrix} \lambda_1 & -\mu_2 \\ \lambda_2 & \mu_1 \end{pmatrix} \text{ speciel og } (\alpha_1, \alpha_2)\begin{pmatrix} \lambda_1 & -\mu_2 \\ \lambda_2 & \mu_1 \end{pmatrix} = (\delta, 0). \ \blacksquare$$

3.6. ELEMENTARDIVISORSÆTNINGEN. Lad R være et hovedidealområde. Da kan enhver matrix $\alpha \in Mat_{n,p}(R)$ ved hjælp af elementære og specielle (række- og søjle-) operationer omformes til en matrix af normalformen

$$\begin{pmatrix} \delta_1 & & \\ & \ddots & \\ & & \delta_r \\ & & \end{pmatrix},$$

hvor $\delta_1 | \delta_2, \cdots, \delta_{r-1} | \delta_r$, $\delta_r \neq 0$ (og hvor matricens øvrige elementer alle er 0).

BEVIS. Hvis α er nul-matricen, har α selv normalformen (med $r=0$). Antag derfor, at $\alpha \neq 0$. Efter en eventuel permutation af rækker og søjler kan vi antage, at $\alpha_{11} \neq 0$.

1. skridt: Hvis der blandt elementerne i første række findes et α_{1j}, der ikke er deleligt med α_{11}, så er største fælles divisor for α_{11} og α_{1j} en ægte divisor i α_{11} (dvs ikke associeret med α_{11}). Anvendes Lemma 1 ses, at vi så ved søjleoperationer kan omforme α til en matrix α' hvori α'_{11} er ægte divisor i α_{11}. En tilsvarende reduktion kan opnås (ved rækkeoperationer), hvis et element i første søjle ikke er deleligt med α_{11}. Dette kan kun gentages endelig mange gange, idet vi jo ikke kan have en uendelig følge $\alpha_{11}, \alpha_{11}', \alpha_{11}'', \cdots, \alpha_{11}^{(m)}, \cdots$, hvori $\alpha_{11}^{(m)}$ er ægte divisor i $\alpha_{11}^{(m-1)}$. Når processen ikke kan gentages, har vi omformet α til en matrix β, hvor β_{11} er divisor i α_{11} og hvor alle elementer β_{1j} i første række og alle elementer i β_{i1} i første søjle er multipla af β_{11}. Subtraheres et passende multiplum af første søjle fra den j-te søjle, $j = 2, \cdots, p$ kan vi opnå $\beta_{1j} = 0$ og tilsvarende $\beta_{i1} = 0$, $i = 2, \cdots, n$.

2. skridt: Hvis der i den omformede matrix β findes et element β_{ij}, $i \geq 2$, $j \geq 2$, der ikke er deleligt med β_{11}, kan vi addere j-te søjle til første søjle. Herved

ændres β_{11} ikke (idet jo $\beta_{1j} = 0$), og nu står der i første søjle et element (nemlig β_{ij}), der ikke er deleligt med β_{11}, og så gentager vi 1. skridt med denne matrix.

Af samme grund som ovenfor ses, at denne reduktion kun kan foretages endelig mange gange. Når processen stopper, er α omformet til en matrix δ, hvor $\delta_{11} \neq 0$, $\delta_{1j} = 0$, $\delta_{i1} = 0$, δ_{ij} er delelig med δ_{11}, $i \geq 2$, $j \geq 2$.

3. skridt: Den omformede matrix har nu formen

$$\delta = \begin{pmatrix} \delta_1 & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & & \\ 0 & & & \end{pmatrix} \Bigg\} n-1 \qquad \text{hvor } \delta_1 = \delta_{11} \neq 0,$$

($p-1$ søjler)

og hvor $(n-1) \times (p-1)$-matricen har formen $\delta_1 \alpha_1$ med en $(n-1) \times (p-1)$-matrix α_1. Et oplagt induktionsargument anvendt på matricen α_1 giver nu den ønskede omformning af α ▨

3.7. KOROLLAR. Lad R være et hovedidealområde. Da kan enhver matrix $\alpha \in SL_p(R)$ (dvs kvadratisk, med determinant 1) skrives som et endeligt produkt af matricer, der er elementære eller specielle.

BEVIS. Ifølge sætningen ($n = p$) findes specielt matricer σ, τ, der er endelige produkter af elementære eller specielle matricer, så at $\sigma\alpha\tau$ er en diagonalmatrix

$$\sigma\alpha\tau = \begin{pmatrix} \delta_1 & & 0 \\ & \delta_2 & \\ 0 & & \ddots \end{pmatrix}.$$

Da omformningen ikke ændrer determinanten, har denne matrix determinant 1. Følgelig er $\tau = p$ og $\delta_1 \cdots \delta_p = 1$. Heraf følger, at hvert δ_j er en enhed i R, og så

kan vi (eventuelt efter yderligere elementære søjleoperationer) antage, at $\delta_2 = \cdots = \delta_p = 1$. Men så er jo også $\delta_1 = 1$, og $\alpha = \sigma^{-1}\tau^{-1}$ er nu en fremstilling af den ønskede art ▨

3.8. Hvis der for et integritetsområde R findes en funktion $\nu : R \to \mathbb{Z}$, som er nedad begrænset og opfylder, at der for alle $\alpha, \in R$, $\beta \neq 0$, findes et $\lambda \in R$ med

$$\nu(\alpha - \lambda\beta) < \nu(\beta),$$

så er som bekendt R et hovedidealområde.

For sådanne hovedidealområder gælder, at de specielle (række- og søjle-) operationer kan erstattes af elementære operationer. Denne skærpelse af Sætning 3.6 kaldes også:

ELEMENTARDIVISORSÆTNINGEN. Lad R være et hovedidealområde og antag, at der i R findes en funktion $\nu : R \to \mathbb{Z}$ med egenskaberne ovenfor. Da kan enhver matrix $\alpha \in \mathrm{Mat}_{m,p}(R)$ ved hjælp af elementære (række- og søjle-) operationer omformes til en matrix

$$\begin{pmatrix} \delta_1 & & \\ & \ddots & \\ & & \delta_r \end{pmatrix},$$

hvor $\delta_1 | \delta_2, \ldots, \delta_{r-1} | \delta_r$, $\delta_r \neq 0$.

BEVIS. Det er øjensynlig nok at vise, at den specielle søjleoperation anvendt i Lemma 3.5 kan erstattes af gentagne elementære søjleoperationer. Og det er netop det der foretages i Euklid's velkendte algoritme. □

KOROLLAR. Under forudsætningerne om R ovenfor gælder, at enhver matrix $\alpha \in SL_p(R)$ kan skrives som et endeligt produkt af elementære matricer.

BEVIS □

Korollaret udtrykker, at den elementære undergruppe $E_p(R)$ er hele gruppen $SL_p(R)$. Alternativt kan siges, at de elementære matricer er et frembringersystem for gruppen $SL_p(R)$ [under de angivne forudsætninger om R]. For $p=2$ ser vi specielt, at gruppen $SL_2(R)$ er frembragt af matricerne $\begin{pmatrix}1&\lambda\\0&1\end{pmatrix}$ og $\begin{pmatrix}1&0\\\lambda&1\end{pmatrix}$, $\lambda\in R$. Idet

$$\begin{pmatrix}1&0\\\lambda&1\end{pmatrix}=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}1&-\lambda\\0&1\end{pmatrix}\begin{pmatrix}0&1\\-1&0\end{pmatrix}=\begin{pmatrix}0&-1\\1&0\end{pmatrix}\begin{pmatrix}1&-\lambda\\0&1\end{pmatrix}\begin{pmatrix}0&-1\\1&0\end{pmatrix}^{-1},$$

kan vi alternativt som frembringere bruge matricerne $\begin{pmatrix}1&\lambda\\0&1\end{pmatrix}$, $\lambda\in R$ og $\begin{pmatrix}0&-1\\1&0\end{pmatrix}$.

EKSEMPEL. For $R=\mathbb{Z}$ har funktionen $q\mapsto|q|$ som bekendt den 3.8 nævnte egenskab. Sætningen og korollaret gælder altså for matricer med hele koefficienter. Da vi yderligere har

$$\begin{pmatrix}1&q\\0&1\end{pmatrix}=\begin{pmatrix}1&1\\0&1\end{pmatrix}^q,\quad q\in\mathbb{Z},$$

følger det, at gruppen $SL_2(\mathbb{Z})$ er frembragt af de to matricer $\begin{pmatrix}1&1\\0&1\end{pmatrix}$ og $\begin{pmatrix}0&-1\\1&0\end{pmatrix}$.

4. Basissætningen.

Vi minder om at R stadig er et hovedidealområde.

4.1. LEMMA. *Lad F være en endeligt frembragt fri modul af rang n og lad $N \subseteq F$ være en undermodul. Da findes en fri basis $(v_1, \dots, v_n)$ for F og skalarer $\delta_1 | \delta_2, \dots, \delta_{p-1} | \delta_p$, med $p \leq n$, så at $(\delta_1 v_1, \dots, \delta_p v_p)$ er en fri basis for N.*

BEVIS. Lad $(u_1, \dots, u_n)$ være en fri basis for F. Ifølge Sætning 1.2 er undermodulen $N \subseteq F$ fri af en rang $p \leq n$, så vi kan vælge en fri basis $(w_1, \dots, w_p)$ for N. Da $(u_1, \dots, u_n)$ er en basis for F findes en relation

$$(w_1, \dots, w_p) = (u_1, \dots, u_n)\alpha, \qquad \alpha \in \mathrm{Mat}_{n,p}(R),$$

hvor j-te søjle i α består af de koefficienter, der optræder når w_j skrives som R-linearkombination af $u_1, \dots, u_n$. Ifølge Elementardivisorsætningen 3.6 findes specielt invertible matricer $\sigma \in GL_n(R)$, $\tau \in GL_p(R)$, så at $\sigma\alpha\tau$ har formen

$$\sigma\alpha\tau = \begin{pmatrix} \delta_1 & & \\ & \ddots & \\ & & \delta_r \\ & & \end{pmatrix}, \quad \delta_1 | \delta_2, \dots, \delta_{r-1} | \delta_r.$$

Da $\sigma \in GL_n(R)$ er invertibel, følger det, at også sættet $(v_1, \dots, v_n) := (u_1, \dots, u_n)\sigma^{-1}$ er en fri basis for F. Tilsvarende er $(w_1, \dots, w_p)\tau$ en fri basis for N. Og denne nye basis for N er

$$\begin{aligned}(w_1, \dots, w_p)\tau &= (u_1, \dots, u_n)\alpha\tau = (u_1, \dots, u_n)\sigma^{-1}\sigma\alpha\tau \\ &= (v_1, \dots, v_n)\sigma\alpha\tau \\ &= (\delta_1 v_1, \dots, \delta_r v_r, 0, \dots, 0).\end{aligned}$$

Her må vi have $r = p$ (altså ingen 0'er), og $(v_1, \dots, v_n)$ er derfor den søgte basis ▨

4.2. BASISSÆTNINGEN. *Enhver endeligt frembragt R-modul M har en basis $(e_1, \dots, e_n)$, endda med $\mathrm{Ann}(e_1) \supseteq \dots \supseteq \mathrm{Ann}(e_n)$.*

BEMÆRKNING. Vi minder om at elementer $e_1, \dots, e_n \in M$ er en basis, netop hvis M er direkte sum af de cykliske moduler $Re_1, \dots, Re_n$:

$$M = Re_1 \oplus \dots \oplus Re_n, \quad e_i \neq 0.$$

Disse cykliske moduler har formen $R/(\delta_i)$, hvor (hoved-) idealet (δ_i) er annullatoren for Re_i. Ekvivalent kan Basissætningen derfor formuleres:
Enhver endeligt frembragt R-modul er isomorf med en direkte sum

$$R/(\delta_1) \oplus \dots \oplus R/(\delta_n),$$

endda med $\delta_1 \mid \delta_2, \dots, \delta_{n-1} \mid \delta_n$ og δ_1 ikke en enhed.

BEVIS FOR BASISSÆTNINGEN. Da M er endeligt frembragt, findes for passende n (f.eks. $n = \dim M$) en fri modul F af rang n og en surjektiv homomorfi $F \to M$. Er N kernen for denne homomorfi, så er $M \simeq F/N$. Ifølge Lemma 4.1 findes en basis for F, altså en isomorfi

$$F \simeq R \oplus \dots \oplus R$$

så at undermodulen N herved svarer til

$$N \simeq R\delta_1 \oplus \dots \oplus R\delta_p, \quad \delta_1 \mid \delta_2, \dots, \delta_{p-1} \mid \delta_p.$$

Tilføjes eventuelt $\delta_{p+1} = \dots = \delta_n = 0$, kan vi skrive

$$N \simeq R\delta_1 \oplus \dots \oplus R\delta_n,$$

og så er åbenbart

$$M \simeq F/N \simeq R/R\delta_1 \oplus \dots \oplus R/R\delta_n.$$

Og fjernes her de eventuelle cykliske moduler, som er $= (0)$ [svarende til δ_j'er, som er enheder i R], har vi den ønskede fremstilling. ∎

4.3. BEMÆRKNING. Hvis en modul M har en basis $e_1, \dots, e_n$:

$$M = Re_1 \oplus \dots \oplus Re_n$$

svarende til en isomorfi:

$$M \simeq R/(\delta_1) \oplus \dots \oplus R/(\delta_n)$$

med $(\delta_i) = \operatorname{Ann} e_i$, så er e_i torsionsfrit netop når $\delta_i = 0$, og altså et torsionselement, netop når $\delta_i \neq 0$. Er M en torsionsfri modul er det sidste udelukket, og basen er derfor en fri basis. Specielt følger det, at Basissætningen indeholder Sætning 2.3 som specialtilfælde.

I det almindelige tilfælde kan vi ordne elementerne $e_1, \dots, e_n$ således at $e_1, \dots, e_p$ er torsionselementer og $e_{p+1}, \dots, e_n$ er torsionsfri, svarende til at $\delta_1, \dots, \delta_p$ er $\neq 0$ og $\delta_{p+1}, \dots, \delta_n$ er $= 0$ $(0 \leqslant p \leqslant n)$. For de tilsvarende undermoduler

$$N = Re_1 \oplus \dots \oplus Re_p, \qquad K = Re_{p+1} \oplus \dots \oplus Re_n.$$

har vi $M = N \oplus K$. Undermodulen K er øjensynlig fri, og undermodulen N er netop torsionsundermodulen M_{tor}. Det er nemlig klart, at $N \subseteq M_{tor}$, idet f.eks. $\delta_1 \cdots \delta_p$ annullerer alle elementer i N, og er omvendt $x \in M_{tor}$, så findes $\lambda \neq 0$ i R med $\lambda x = 0$. Skrives $x = n + k$, $n \in N$, $k \in K$ får vi $0 = \lambda x = \lambda n + \lambda k$, og heraf følger $\lambda k = 0$. Da K er torsionsfri, er $k = 0$, og altså $x = n \in N$.

Af Sætning 2.5 fremgår nu, at antallet af torsionsfri elementer i basen, dvs rangen af K, faktisk er rangen af M. Specielt er dette antal entydigt bestemt. Et tilsvarende resultat gælder ikke for antallet af torsionselementer i en basis.

4.4. I det følgende vil vi specielt interessere os for endeligt frembragte torsionsmoduler M. For en sådan giver Basissætningen en basis $e_1, \dots, e_n$, hvor

$$R \supset \operatorname{Ann}(e_1) \supseteq \dots \supseteq \operatorname{Ann}(e_n) \supset (0)$$

svarende til en isomorfi

$$M \simeq R/(\delta_1) \oplus \cdots \oplus R/(\delta_n),$$

hvor $(\delta_i) = \mathrm{Ann}(e_i)$ og altså $\delta_1 \mid \delta_2, \ldots, \delta_{n-1} \mid \delta_n$, $\delta_n \neq 0$. Det er klart, at der for hvert element $x \in M$ gælder

$$\mathrm{Ann}(M) \subseteq \mathrm{Ann}(x).$$

Specielt er altså $\mathrm{Ann}(M) \subseteq \mathrm{Ann}(e_n) = (\delta_n)$. Da $\delta_i \mid \delta_n$, $i \leq n$ følger omvendt at, at δ_n annullerer ethvert e_i, og dermed også enhver linearkombination af e_i'erne og altså hele M. Vi har derfor $(\delta_n) \subseteq \mathrm{Ann}(M)$, og altså

$$\mathrm{Ann}(M) = \mathrm{Ann}(e_n).$$

KOROLLAR. Lad M være en endelig frembragt torsionsmodul. Da findes et element $e \in M$, så at

$$\mathrm{Ann}(M) = \mathrm{Ann}(e) \quad \square$$

DEFINITION. Ligningen $\mathrm{Ann}(M) = \mathrm{Ann}(e)$ er ígensynlig ensbetydende med at der gælder $\mathrm{Ann}(e) \subseteq \mathrm{Ann}(x)$ for alle $x \in M$. Et sådant element siges også at have <u>minimal annullator</u>. En frembringer for (hoved-)idealet $\mathrm{Ann}(M)$ kaldes også et <u>minimalt element</u> for M.

4.5 EKSEMPEL. En endelig kommutativ gruppe M er som $\mathbb{Z}$-modul naturligvis en endeligt frembragt torsionsmodul, og Basissætningen giver for en sådan gruppe en isomorfi:

$$M \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z}$$

af M på en direkte sum af endelige cykliske grupper (endda med $d_1 \mid d_2, \ldots, d_{n-1} \mid d_n$). For $x \in M$ er ordenen af x netop den positive frembringer for idealet $\mathrm{Ann}(x) \in M$. Korollaret udsiger altså, at der findes et element $e \in M$, hvis orden er et multiplum af enhver anden "elementorden". Bemærk, at denne orden, som jo er minimalt element for M, er <u>maksimal</u> (m.h.t. $<$ og $\mid$) blandt alle "elementordener".

4.6. SÆTNING. For hvert $\mu \neq 0$ i R er den cykliske modul $R/(\mu)$ en Jordan-Hölder modul, hvis længde er antallet r af primfaktorer i en primopløsning $\mu = \pi_1 \cdots \pi_r$.

BEVIS. Hvis δ er divisor i μ: $\mu'\delta = \mu$, så er

$$R\mu \subseteq R\delta \subseteq R.$$

Af Noethers 2. isomorfisætning følger at $R\delta$ svarer til en undermodul $M' \simeq R\delta/R\mu$ i $M = R/R\mu$ med $M/M' \simeq R/R\delta$. Vi har øjensynlig en surjektiv homomorfi: $R \to M' = R\delta/R\mu$ defineret ved $\lambda \mapsto \lambda\overline{0} = \overline{\lambda\delta}$ og den har kernen $R\mu'$, thi da μ og dermed μ' er $\neq 0$, er $\lambda\delta \in R\mu = R\mu'\delta$, hvis og kun hvis $\lambda \in R\mu'$.

Af $\mu = \mu'\delta$ får vi således i $M = R/(\mu)$ en kæde

$$(0) \subseteq M' \subseteq M \quad \text{med } M' \simeq R/(\mu') \text{ og } M/M' \simeq R/(\delta).$$

Ved induktion fås af $\mu = \pi_1 \cdots \pi_r$ en kæde af længde r i $M = R/(\mu)$ med kvotienterne $R/(\pi_i)$. Er π_i'erne primelementer, så er (π_i)'erne maximalidealer og kvotienterne $R/(\pi_i)$ altså simple moduler. Og så er $r = \operatorname{long} M$ ▨

4.7. LEMMA. Lad $(0) = M_0 \subseteq \cdots \subseteq M_k = M$ være en kæde, og antag at μ_i annullerer M_i/M_{i-1}, $i = 1, \ldots, k$. Da vil $\mu = \mu_1 \cdots \mu_k$ annullere M.

BEVIS. Lad $x \in M$. Da μ_k annullerer M/M_{k-1}, er $\mu_k\overline{x} = \overline{0}$, altså $\mu_k x \in M_{k-1}$. Induktivt fås derfor

$$\mu x = \mu_1 \cdots \mu_{k-1}(\mu_k x) = 0 \quad ▨$$

SÆTNING. Betragt for en R-modul M følgende betingelser:

(i) M er en endeligt frembragt torsionsmodul.

(ii) Der findes kæde: (*) $(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_k = M$, med kvotienter $M_i/M_{i-1} \simeq R/(\mu_i)$, med $\mu_i \neq 0$, $i = 1, \ldots, k$.

(iii) M er endeligt frembragt, og der findes en skalar $\mu \neq 0$, der annullerer M.

(iv). M har endelig længde.

Da gælder: (i) $\Leftrightarrow$ (ii) $\Leftrightarrow$ (iii) $\Rightarrow$ (iv).

Hvis R ikke er et legeme, er (iv) ækvivalent med de andre.

BEVIS. (i) ⇒ (ii): Da M er endeligt frembragt findes en kæde (*) med cykliske kvotienter $M_i/M_{i-1} \simeq R/(\mu_i)$. Da M er en torsionsmodul er også M_i/M_{i-1} en torsionsmodul, og så er $\mu_i \neq 0$.
(ii) ⇒ (iii): Omvendt sikrer en kæde (*), at M er endeligt frembragt, og som μ kan vi ifølge lemmaet bruge $\mu = \mu_1 \cdots \mu_K$.
(iii) ⇒ (i): Er trivielt.
(ii) ⇒ (iv): Følger umiddelbart af Sætning 4.6.
(iv) ⇒ (ii), når R ikke er et legeme: I en Jordan-Hölder kæde

$$(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_K = M$$

er kvotienterne simple, dvs $M_i/M_{i-1} \simeq R/(\mu_i)$, hvor $(\mu_i) \subseteq R$ er et maksimalideal. Da R ikke er et legeme, er $\mu_i \neq 0$. ▨

4.8. DEFINITION. Lad $\pi \in R$ være et primelement. Et element x i en R-modul M kaldes π-primært, hvis der findes et naturligt tal n, så at

$$\pi^n x = 0.$$

Modulen M kaldes π-primær, hvis alle dens elementer er π-primære. [Et element i en modul kaldes primært, hvis det er π-primært for et passende primelement π. Tilsvarende er en modul primær, hvis den er π-primær for et passende π]

OBSERVATION. Hvis M er en π-primær modul, så er alle M's undermoduler og kvotientmoduler ligeledes π-primære.

4.9. SÆTNING. Lad M være en R-modul og antag, at $\mu \in R \setminus \{0\}$ annullerer M. Lad

$$\mu = \varepsilon \pi_1^{n_1} \cdots \pi_r^{n_r}$$

være en primopløsning af μ [hvor altså ε er en en-

hed og primelementerne π_i og π_j ikke er associerede, når $i \neq j$). Sæt

$$M_i = \{ x \in M \mid \pi_i^{n_i} x = 0 \}.$$

Da er M_i en π_i-primær undermodul af M og enhver primær undermodul af M er indeholdt i et af M_i'erne. Endvidere er M direkte sum af M_i'erne:

$$M = M_1 \oplus \cdots \oplus M_r.$$

BEVIS. At hvert M_i er en undermodul følger f.eks. af at M_i er kernen for den R-lineære afbildning $x \mapsto \pi_i^{n_i} x$. Det er klart, at M_i er π_i-primær.

Lad $x \in M$ være et π-primært element, og sæt $\operatorname{Ann} x = (\alpha)$. Med passende n er $\pi^n x = 0$, så α er divisor i π^n. Følgelig er α associeret med en potens af π, så vi kan antage, at $\operatorname{Ann} x = (\pi^n)$. Da $\mu x = 0$, er π^n divisor i $\mu = \varepsilon \pi_1^{n_1} \cdots \pi_r^{n_r}$. Idet vi kan antage, at $x \neq 0$, og dermed at $n \geq 1$, følger det, at π er associeret med et π_i og at $n \leq n_i$. Men så er $\operatorname{Ann} x = (\pi^n) = (\pi_i^n)$ og dermed

$$\pi_i^{n_i} x = \pi_i^{n_i - n} \pi_i^n x = 0,$$

og altså $x \in M_i$.

Vi mangler at vise, at M er direkte sum af M_i'erne: Skriv

$$\mu = \mu_i \pi_i^{n_i}, \quad \text{hvor } \mu_i = \frac{\mu}{\pi_i^{n_i}} = \varepsilon \pi_1^{n_1} \cdots \pi_{i-1}^{n_{i-1}} \pi_{i+1}^{n_{i+1}} \cdots \pi_r^{n_r}.$$

Da er μ_i'erne primiske, så der findes $\lambda_1, \ldots, \lambda_r \in R$, så at

$$1 = \lambda_1 \mu_1 + \cdots + \lambda_r \mu_r.$$

For hvert $x \in M$ har vi da fremstillingen

$$x = \lambda_1 \mu_1 x + \cdots + \lambda_r \mu_r x.$$

Her er $\pi_i^{n_i}(\lambda_i \mu_i x) = 0$, da $\pi_i^{n_i} \mu_i = \mu$ og $\mu x = 0$, så fremstillingen viser, at $M = M_1 + \cdots + M_r$.

Og summen er direkte. Lad nemlig

$$0 = x_1 + \cdots + x_r \,, \quad \text{hvor } x_i \in M_i \,, \; i = 1, \cdots, r.$$

Når $j \neq i$ er $\pi_j^{n_j}$ divisor i μ_i og følgelig er

$$\mu_i x_j = 0 \quad \text{når } i \neq j.$$

Og så er

$$x_i = \sum_j \lambda_j \mu_j x_i = \lambda_i \mu_i x_i = \sum_j \lambda_i \mu_i x_j = \lambda_i \mu_i 0 = 0 \; \blacksquare$$

4.10. PRIMÆR-BASIS-SÆTNINGEN. Enhver endeligt frembragt torsionsmodul M over R har en primær-basis, dvs en basis, hvis elementer er primære.

BEVIS. Da M er en endeligt frembragt torsionsmodul, findes et $\mu \neq 0$, der annullerer M. Af sætningen fås nu en dekomposition $M = M_1 \oplus \cdots \oplus M_r$, hvor M_i er en π_i-primær undermodul. Vælg nu ifølge Basissætningen i hvert M_i en basis (nødvendigvis bestående af π_i-primære elementer). Da udgør de valgte elementer en primær-basis for M $\blacksquare$

BEMÆRKNING. Basissætningen 4.2 udsiger, at enhver endeligt frembragt torsionsmodul er en direkte sum af cykliske moduler, dvs moduler isomorfe med $R/(\alpha)$, hvor $\alpha \in R \setminus \{0\}$. Af Primærbasissætningen følger, at de cykliske moduler kan vælges primære, dvs isomorfe med $R/(\pi^n)$, hvor $\pi \in R$ er et primelement. Hvis $\mu = \pi_1^{n_1} \cdots \pi_r^{n_r}$ annullerer modulen kan de endda vælges isomorfe med $R/(\pi_i^n)$, hvor $n \leq n_i$.

4.11. Er M en endelig frembragt torsionsmodul, findes ifølge Sætning 4.7 en Jordan-Hölder kæde

$$(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_k = M.$$

Ifølge Hölders Sætning afhænger de simple kvotienter M_i/M_{i-1}, $i = 1, \cdots, k$ på nær isomorfi og rækkefølge kun af modulen M (og ikke af den valgte kæde). Idealerne Ann M_i/M_{i-1}, $i = 1, \cdots, k$ afhænger derfor (bortset fra rækkefølgen) kun af M. Skrives for hvert $i = 1, \cdots, k$ Ann $M_i/M_{i-1} = (\pi_i)$ følger det, at elementet

$$\chi = \pi_1 \cdots \pi_k$$

på nær association er entydigt bestemt ved M.

DEFINITION. Elementet $\chi = \pi_1 \cdots \pi_k$ og dets associerede kaldes <u>karakteristiske elementer</u> for den endeligt frembragte torsionsmodul M.

BEMÆRKNING. Simple moduler er cykliske, så at M_i/M_{i-1} har annullator (π_i) betyder, at M_i/M_{i-1} er isomorf med $R/(\pi_i)$. Da M_i/M_{i-1} er simpel, er (π_i) et maksimalideal, og da $\pi_i \neq 0$, er π_i et primelement, og $\chi = \pi_1 \cdots \pi_k$ er derfor en primoplösning af det karakteristiske element χ for M.

4.12. SÆTNING. Lad $C = R/(\mu)$ være en cyklisk R-modul, hvor $\mu \neq 0$. Da er μ karakteristisk element for C.

BEVIS. Lad $\mu = \pi_1 \cdots \pi_n$ være en primoplösning af μ. Af (beviset for) Sætning 4.6 fremgår, at C har en Jordan-Hölder kæde med kvotienter $R/(\pi_i)$, $i = 1, \cdots, n$. Og så er $\pi_1 \cdots \pi_n$ karakteristisk element for C ▨

4.13. SÆTNING. Lad M være en endeligt frembragt torsionsmodul over R. Hvis χ' er karakteristisk element for en undermodul $M' \subseteq M$ og χ'' er karakteristisk element for kvotienten M/M', så er $\chi' \cdot \chi''$ karakteristisk element for M.

BEVIS. Gauske som beviset for at $\text{long}M' + \text{long}M/M' = \text{long}M$ □

KOROLLAR. Lad M være en endeligt frembragt torsionsmodul. (1) Hvis $(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_k = M$ er en kæde i M og χ_i er karakteristisk for kvotienten M_i/M_{i-1}, $i = 1, \cdots, k$, så er $\chi = \chi_1 \cdots \chi_k$ karakteristisk element for M.
(2) Hvis $M = M_1 \oplus \cdots \oplus M_k$, og χ_i er karakteristisk element for M_i, $i = 1, \cdots, k$, så er $\chi = \chi_1 \cdots \chi_k$ karakteristisk element for M.
BEVIS. □

4.14. SÆTNING. Lad M være en endeligt frembragt torsionsmodul over R, og lad χ være karakteristisk element for M. Da vil χ annullere M. Lad $\alpha \in R$ være minimalt element for M, dvs $(\alpha) = \text{Ann}(M)$. Da er α divisor i χ, og α og χ har de samme primdivisorer.
BEVIS. At χ annullerer M fås umiddelbart af definitionen og Lemma 4.7. Altså er $\chi \in \text{Ann}(M) = (\alpha)$, dvs α er divisor i χ. Specielt er hver primdivisor i α (dvs hvert primelement, der er divisor i α) også divisor i χ. Er omvendt $\chi = \pi_1 \cdots \pi_k$, så er hver primdivisor i χ associeret med et af π_i'erne. Her er $(\pi_i) = \text{Ann}\, M_i/M_{i-1}$ annullator for en kvotient i en Jordan-Hölder for M, og da α annullerer M og dermed også M_i/M_{i-1}, er $\alpha \in (\pi_i)$, dvs π_i er divisor i α ▨

4.15. EKSEMPEL. Lad M være en endelig kommutativ gruppe. Ud fra en Jordan-Hölder kæde

$$(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_k = M$$

hvor $M_i/M_{i-1} \simeq \mathbb{Z}/(p_i)$, p_i et primtal, bestemmes det karakteristiske element for M som $\chi = p_1 \cdots p_k$, jfr.

Definition 4.11. På den anden side gælder ifølge Lagrange's index-sætning

$$|M| = |M_{K-1}|\,|M_K/M_{K-1}| = \cdots = |M_1|\,|M_2/M_1| \cdots |M_K/M_{K-1}|$$
$$= p_1 \cdot p_2 \cdots p_K .$$

Ordenen $|M|$ er altså karakteristisk element for M. Lad α være den maksimale elementorden for M, jfr. Eksempel 4.5. Af Sætning 4.14 fås nu dels, at α er divisor i $|M|$ (og dermed at enhver elementorden er divisor i $|M|$, men det er jo et velkendt korollar til Lagrange's index-sætning), dels følgende RESULTAT: For hver primdivisor p i $|M|$ har M et element af orden p.
Vi har nemlig p/α, $p\lambda = \alpha$, og hvis $e \in M$ har orden α, så har λe øjensynlig orden p.

4.16. SÆTNING. Lad $\alpha \in \mathrm{Mat}_n(R)$ være en kvadratisk matrix, sæt $F = R^n$ og lad $N \subseteq F$ betegne undermodulen frembragt af søjlerne $\alpha_1, \cdots, \alpha_n$ i α. Da er følgende betingelser ækvivalente:
(i) Kvotientmodulen F/N er en endeligt frembragt torsionsmodul.
(ii) Matricen $\alpha = (\alpha_1, \cdots, \alpha_n)$ har determinant $\neq 0$.
(iii) Søjlerne $\alpha_1, \cdots, \alpha_n$ er en fri basis for N.
Er disse betingelser opfyldt, så er $\det(\alpha)$ karakteristisk element for F/N.

BEVIS. Opfattes α som den lineære afbildning $F \to F$ bestemt ved $x \mapsto \alpha x$, er søjlerne $\alpha_1, \cdots, \alpha_n$ billederne af den kanoniske basis for F og $N = \alpha(F)$. Betingelsen (iii) er derfor ækvivalent med at $\alpha : F \to F$ er injektiv.
(ii) $\Leftrightarrow$ (iii) er nu et generelt resultat om determinanter, idet R specielt er et integritetsområde.

(i) ⇒ (ii): Vælg $\mu \neq 0$, som annullerer $F/\alpha(F)$, jfr. Sætning 4.7. Er $e_1, \cdots, e_n$ den kanoniske basis for $F = R^n$, er altså $\mu(e_i) = 0$ i $F/\alpha(F)$, så der findes $\beta_i \in F$ med $\mu e_i = \alpha(\beta_i)$, $i = 1, \cdots, n$. Er $\beta : F \to F$ bestemt ved matricen $\beta = (\beta_1, \cdots, \beta_n)$ er altså

$$\alpha\beta = \begin{pmatrix} \mu & & 0 \\ & \ddots & \\ 0 & & \mu \end{pmatrix}.$$

Heraf fås $\det(\alpha)\det(\beta) = \mu^n \neq 0$, så specielt er $\det(\alpha) \neq 0$.

(iii) ⇒ (i): Ifølge Lemma 4.1 findes en fri basis $(v_1, \cdots, v_n)$ for F, og skalarer $\delta_1, \cdots, \delta_p \in R$, så at $(\delta_1 v_1, \cdots, \delta_p v_p)$ er en fri basis for N. Her er specielt $\delta_i \neq 0$, $i = 1, \cdots, p$, og da N ifølge forudsætningen specielt har rang n, er $n = p$. Det følger nu, at $F/N \simeq R/(\delta_1) \oplus \cdots \oplus R/(\delta_n)$, og specielt, at N er en endeligt frembragt torsionsmodul.

For at vise sætningens sidste påstand bruges elementerne bestemt i "(iii) ⇒ (i)". Af Sætning 4.12 og Korollar 4.13 følger, at $\chi = \delta_1 \cdots \delta_n$ er karakteristisk element for F/N. Idet $(e_1, \cdots, e_n)$ og $(\alpha_1, \cdots, \alpha_n)$ er baser for $F = R^n$ og N har vi "basisskift-matricer" $\sigma, \tau \in GL_n(R)$ bestemt ved

$$(e_1, \cdots, e_n) = (v_1, \cdots, v_n)\sigma \quad \text{og} \quad (\alpha_1, \cdots, \alpha_n) = (\delta_1 v_1, \cdots, \delta_n v_n)\tau.$$

Idet v betegner matricen med søjlerne $v_1, \cdots, v_n$ og δ betegner diagonalmatricen med $\delta_1, \cdots, \delta_n$ i diagonalen (og 1 betegner enhedsmatricen) kan ligningerne skrives

$$1 = v\sigma \quad \text{og} \quad \alpha = v\delta\tau$$

Heraf fås $\alpha = v\delta\tau = \sigma^{-1}\delta\tau$ og dermed

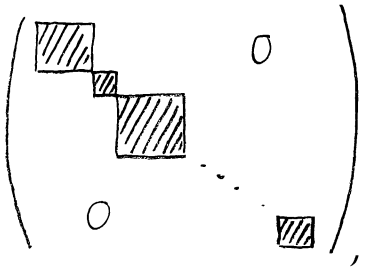
$$\det(\alpha) = \det(\sigma^{-1})\det(\delta)\det(\tau) = \det(\sigma^{-1}\tau)\chi.$$

Da $\det(\sigma^{-1}\tau)$ er en enhed, er $\det(\alpha)$ associeret med χ, og følgelig er også $\det(\alpha)$ karakteristisk element for F/N ▨

EKSEMPEL. Når $R = \mathbb{Z}$ gælder under sætningens betingelser, at F/N er en endelig kommutativ gruppe af orden $|F/N| = |\det(\alpha)|$, jfr. Eksempel 4.15.

5. Endomorfier i vektorrum.

5.1. JORDAN'S NORMALFORM. Lad V være et endeligt dimensionalt vektorrum over $\mathbb{C}$ og lad $\varphi : V \to V$ være en $\mathbb{C}$-lineær endomorfi. Da findes en basis for V, hvori φ beskrives ved en Jordan-matrix, dvs en blokmatrix



hvor de kvadratiske blokke langs diagonalen har formen

$$\begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & 1 & \\ & & \lambda & \ddots \\ & & & 1 \\ 0 & & & \lambda \end{pmatrix}, \qquad \lambda \in \mathbb{C}.$$

BEMÆRKNING. De simpleste sådanne blokke er 1×1-matricen (λ), 2×2-matricen $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ og 3×3-matricen $\begin{pmatrix} \lambda & 1 & 0 \\ 0 & \lambda & 1 \\ 0 & 0 & \lambda \end{pmatrix}$

5.2. I det følgende viser vi, at sætningen om Jordan's normalform er en konsekvens af Basissætningen (4.2 og 4.10). Vi betragter vektorrum V over et vilkårligt legeme L og minder om at polynomiumsringen $L[X]$ er et hovedidealområde.

Lad $\varphi : V \to V$ være en L-lineær endomorfi.

Er $(e_1, \dots, e_n)$ en given basis for V, kan hver vektor $v \in V$ skrives

$$(*) \qquad v = v_1 e_1 + \cdots + v_n e_n$$

med entydigt bestemte koefficienter $v_i \in L$, $i = 1, \dots, n$.

Sættet bestående af de n koefficienter en vektorens koordinatsæt m.h.t. den givne basis. Vi vil altid skrive det som søjle, og vi betegner det

$$\underline{\underline{v}} = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \in L^n$$

Bemærk, at sammenhængen mellem vektoren v og dens koordinatsæt $\underline{\underline{v}}$, dvs ligningen (*), bekvemt kan skrives

$$(**) \quad v = (e_1, \dots, e_n)\,\underline{\underline{v}} \qquad [\text{kort: } v = e\,\underline{\underline{v}}]$$

Ved matricen hørende til endomorfien φ m.h.t. den givne basis forstås den matrix $\underline{\underline{\Phi}} \in \mathrm{Mat}_n(L)$, hvori den i-te søjle $\underline{\underline{\Phi}}_i$ er koordinatsættet for billedet $\varphi(e_i)$ af den i-te basisvektor. Vi har altså

$$\varphi(e_i) = (e_1, \dots, e_n)\,\underline{\underline{\Phi}}_i, \quad i = 1, \dots, n, \quad \text{dvs}$$

$$(\varphi(e_1), \dots, \varphi(e_n)) = (e_1, \dots, e_n)\,\underline{\underline{\Phi}}. \qquad [\text{kort: } \varphi(e) = e\,\underline{\underline{\Phi}}]$$

Heraf følger, at matricen $\underline{\underline{\Phi}}$ beskriver endomorfien $\varphi: V \to V$ i den forstand, at der for enhver vektor $v \in V$ gælder

$$\boxed{\underline{\varphi(v)} = \underline{\underline{\Phi}}\,\underline{\underline{v}},}$$

thi da φ er lineær og derfor bevarer linearkombinationer fås: $\varphi(v) = \varphi\big((e_1, \dots, e_n)\,\underline{\underline{v}}\big) = (\varphi(e_1), \dots, \varphi(e_n))\,\underline{\underline{v}}$
$= [(e_1, \dots, e_n)\,\underline{\underline{\Phi}}]\,\underline{\underline{v}} = (e_1, \dots, e_n)\,[\underline{\underline{\Phi}}\,\underline{\underline{v}}]$.

Bemærk, at i betegnelserne $\underline{\underline{v}}$ og $\underline{\underline{\Phi}}$ er den givne basis $(e_1, \dots, e_n)$ underforstået. Hvis der for en matrix $\alpha \in \mathrm{Mat}_n(L)$ eksisterer en basis for V m.h.t. hvilken $\underline{\underline{\Phi}} = \alpha$, siger vi, at φ kan <u>beskrives</u> ved α eller at α <u>hører til</u> φ

OBSERVATION. Hvis der til endomorfien $\varphi: V \to V$ m.h.t. en given basis $(e_1, \dots, e_n)$ hører matricen $\underline{\underline{\Phi}} \in \mathrm{Mat}_n(L)$, så er de øvrige matricer, der hører til φ, netop

de matricer, der er regulær-ækvivalente med $\underline{\varphi}$, dvs har formen

$$\sigma^{-1}\underline{\varphi}\,\sigma \qquad \text{med } \sigma \in GL_n(L).$$

5.3. OVERSÆTTELSE. Par (V,φ) bestående af et vektorrum V over L og en L-lineær endomorfi $\varphi: V \to V$ svarer bijektivt til moduler V over polynomiumsringen $L[X]$, v.hj. af følgende "oversættelse":

Polynomiumsringen $L[X]$ omfatter L som delringen $L \subseteq L[X]$ bestående af konstanter. En $L[X]$-modul V kan derfor specielt opfattes som L-modul, dvs som vektorrum over L (som sådan kaldes det også modulens underliggende vektorrum). Videre er homotetien $X_V : V \to V$, dvs afbildningen $v \mapsto X.v$ en $L[X]$-lineær afbildning og dermed specielt en L-lineær endomorfi i det underliggende vektorrum.

Er der omvendt givet en L-lineær endomorfi φ i et vektorrum V, så kan V entydigt organiseres som $L[X]$-modul med V som underliggende vektorrum og med $X_V = \varphi$. For en sådan struktur på V må vi jo have $X.v = \varphi(v)$ og $X^n.v = \varphi^n(v)$ (induktivt: $X^{n+1}.v = X^n.(X.v) = X^n.(\varphi(v)) = \varphi^n(\varphi(v)) = \varphi^{n+1}(v)$) og dermed generelt:

$$(*)\quad \left(a_0 + a_1 X + \cdots + a_m X^m\right).v = a_0 v + a_1 \varphi(v) + \cdots + a_m \varphi^m(v).$$

Og omvendt definerer denne ligning en sådan struktur på V som $L[X]$-modul. Vi betegner denne $L[X]$-modul (V,φ), eller blot V, når misforståelser er udelukket.

5.4. OBSERVATION 1. Undermodulerne i $L[X]$-modulen (V,φ) er netop de undervektorrum $W \subseteq V$, som er φ-invariante,

thi en undergruppe $W \subseteq V$ er et φ-invariant underrum, netop når

(1) $aw \in W$ og $\varphi(w) \in W$, for alle $a \in L$, $w \in W$,

og en $L[X]$-undermodul, netop når

(2) $f.w \in W$, for alle $f = a_0 + a_1 X + \cdots + a_m X^m \in L[X]$, $w \in W$.

Da $L \subseteq L[X]$ og $\varphi(w) = X.w$ er det klart, at (2) $\Rightarrow$ (1). Omvendt følger det let af ligningen (*) ovenfor, at (1) $\Rightarrow$ (2).

OBSERVATION 2. Er U og V vektorrum over L med endomorfier $\psi: U \to U$ og $\varphi: V \to V$, så er en afbildning

$$\sigma : U \longrightarrow V$$

en $L[X]$-lineær afbildning : $(U, \psi) \to (V, \varphi)$, netop når den er L-lineær og $\sigma \circ \psi = \varphi \circ \sigma$.
Dette indses ganske som ovenfor, idet $\sigma(\psi(u)) = \varphi(\sigma(u))$ blot udtrykker, at $\sigma(X.u) = X.\sigma(u)$, $u \in U$.

5.5. DEFINITION. Hvis en $L[X]$-modul V er endelig dimensional (som vektorrum) siges matricerne hørende til endomorfien $X_V = \varphi$ også at <u>høre til</u> modulen V eller at kunne <u>beskrive</u> modulen V.

SÆTNING. Endeligdimensionale $L[X]$-moduler V og W er isomorfe, hvis og kun hvis de kan beskrives ved regulærækvivalente matricer (og dermed også ved samme matrix).
BEVIS. "<u>kun hvis</u>": Sæt $X_V = \varphi$, $X_W = \psi$. Lad $\sigma: V \to W$ være en $L[X]$-isomorfi. Da er σ en L-isomorfi og $\sigma \circ \varphi = \psi \circ \sigma$. Lad $(e_1, \cdots, e_m)$ være en basis for V og lad $\alpha \in Mat_m(L)$ være den tilhørende matrix for φ, dvs

$$(*) \quad (\varphi(e_1), \cdots, \varphi(e_m)) = (e_1, \cdots, e_m)\,\alpha$$

Sæt $e_i' = \sigma(e_i)$, $i = 1, \cdots, n$, og anvend afbildningen

σ på de to sider af (*). Da $\sigma(\varphi(e_i)) = \psi(\sigma(e_i)) = \psi(e_i')$ fås

$$(\psi(e_1'), \dots, \psi(e_n')) = (e_1', \dots, e_n')\alpha.$$

Da σ er en L-isomorfi, er $(e_1', \dots, e_n')$ en basis for W, og den fundne ligning udsiger netop at α er matricen hørende til ψ m.h.t. denne basis.

"hvis": Hvis φ og ψ kan beskrives ved regulærækvivalente matricer, kan de (jfr. Observation 5.2) også beskrives ved samme matrix. Antag derfor at matricen $\alpha \in \mathrm{Mat}_n(L)$ beskriver φ m.h.t. basen $(e_1, \dots, e_n)$ for V og beskriver ψ m.h.t. basen $(e_1', \dots, e_n')$ for W. Da er

$$(\varphi(e_1), \dots, \varphi(e_n)) = (e_1, \dots, e_n)\alpha$$

$$(\psi(e_1'), \dots, \psi(e_n')) = (e_1', \dots, e_n')\alpha.$$

Lad $\sigma : V \to W$ være L-isomorfien bestemt ved $\sigma(e_i) = e_i'$, $i = 1, \dots, n$. Da finder vi

$$\sigma(\varphi(e_i)) = \sigma((e_1, \dots, e_n)\alpha_i) = (e_1', \dots, e_n')\alpha_i$$

$$= \psi(e_i') = \psi(\sigma(e_i))$$

Ligningen $\sigma(\varphi(v)) = \psi(\sigma(v))$ gælder altså når $v = e_i$ er en basisvektor og dermed for enhver vektor $v \in V$. Og så er $\sigma : V \to W$ en $L[X]$-lineær isomorfi. ▨

5,6. EKSEMPEL 1. Lad $f = X^n + a_{n-1}X^{n-1} + \dots + a_0 \in L[X]$ være et normeret polynomium. En $L[X]$-modul V er isomorf med kvotientmodulen $L[X]/(f)$, hvis og kun hvis den kan beskrives ved matricen

$$\begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & -a_2 \\ 0 & 0 & 1 & \dots & 0 & -a_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}.$$

Thi ifølge Struktursætningen for polynomiumskvotienter udgør ækvivalensklasserne

$$e_0 := \boxed{1}\,,\ e_1 := \boxed{X}\,,\ \cdots\,,\ e_{n-1} := \boxed{X^{n-1}}$$

en L-basis for kvotienten $V = L[X]/(f)$. Vi finder

$$X.e_0 = X\boxed{1} = \boxed{X} = e_1$$

$$X.e_1 = X.\boxed{X} = \boxed{X^2} = e_2$$

$$\vdots$$

$$X.e_{n-1} = X\boxed{X^{n-1}} = \boxed{X^n} = \boxed{-a_0 - a_1X - \cdots - a_{n-1}X^{n-1}}$$

$$= -a_0\boxed{1} - a_1\boxed{X} - \ldots - a_{n-1}\boxed{X^{n-1}}$$

$$= -a_0e_0 - a_1e_1 - \cdots - a_{n-1}e_{n-1}\,,$$

og det betyder netop, at X_V m.h.t. basen $(e_0, \cdots, e_{n-1})$ beskrives ved den angivne matrix.

5.7. EKSEMPEL. Lad $\lambda \in L$ og lad $n \in \mathbb{N}$. En $L[X]$-modul V er isomorf med kvotientmodulen $L[X]/((X-\lambda)^n)$, hvis og kun hvis den kan beskrives ved $n \times n$-matricen

$$\begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & 1 & \\ & & \ddots & \ddots \\ & & & 1 \\ 0 & & & \lambda \end{pmatrix}.$$

Thi blandt polynomierne $(X-\lambda)^i$, $i = 0, \cdots, n-1$, findes netop ét af enhver grad $\leq n-1$. Heraf følger, at disse polynomier udgør en basis for vektorrummet af polynomier af grad $\leq n-1$, og dermed at deres ækvivalensklasser

$$e_0 := \boxed{1}\,,\ e_1 := \boxed{X-\lambda}\,,\ \cdots\,,\ e_{n-1} := \boxed{(X-\lambda)^{n-1}}$$

udgør en L-basis for kvotienten $V = L[X]/((X-\lambda)^n)$. Vi finder

$$(X-\lambda).e_i = (X-\lambda).\boxed{(X-\lambda)^i} = \boxed{(X-\lambda)^{i+1}} = \begin{cases} e_{i+1} & \text{når } i < n-1 \\ 0 & \text{når } i = n-1 \end{cases}$$

og dermed

$$X.e_i = \lambda e_i + (X-\lambda)e_i = \begin{cases} \lambda e_i + e_{i+1}, & \text{når } i < n-1 \\ \lambda e_{n-1}, & \text{når } i = n-1. \end{cases}$$

Og det betyder netop, at X_V m.h.t. basen $(e_{n-1}, \dots, e_1, e_0)$ beskrives ved den angivne matrix.

5.8. SÆTNING. Lad V være en $L[X]$-modul, endelig dimensional som vektorrum, og lad $\varphi := X_V$ være den tilhørende endomorfi i vektorrummet V. Lad $W \subseteq V$ være en $L[X]$-undermodul. Hvis undermodulen W kan beskrives ved matricen α og kvotientmodulen V/W kan beskrives ved matricen γ, så kan modulen V beskrives ved en blokmatrix af formen

$$\left(\begin{array}{c|c} \alpha & \beta \\ \hline 0 & \gamma \end{array}\right)$$

BEVIS. Lad $\varphi_0 := X_W$ betegne φ's restriktion til det φ-invariante underrum W, og lad $\psi := X_{V/W}$ betegne den tilhørende endomorfi i kvotienten V/W. Antag, at α beskriver φ_0 m.h.t. basen $(e_1, \dots, e_r)$ for W og at γ beskriver ψ m.h.t. basen $(e_1', \dots, e_s')$ for V/W. Vælg vektorer $e_{r+1}, \dots, e_{r+s}$ i V, hvis ækvivalensklasser (mod W) er

$$\overline{e_{r+i}} = e_i', \quad i = 1, \dots, s.$$

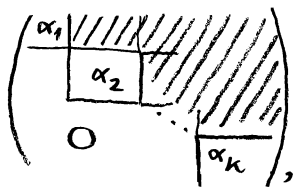
Da er $(e_1, \dots, e_r, e_{r+1}, \dots, e_{r+s})$ en basis for V, og heri beskrives φ ved en matrix af den angivne form □

BEMÆRKNING 1. Omvendt ses, at hvis en $L[X]$-modul V m.h.t. en basis $(e_1, \dots, e_n)$ beskrives ved en blokmatrix af formen

$$\left(\begin{array}{c|c} \alpha & \beta \\ \hline 0 & \gamma \end{array}\right),$$

hvor α er en $r \times r$-matrix, så er underrummet W frembragt af de første r basisvektorer φ-invariant, og α beskriver $L[X]$-undermodulen W og γ beskriver kvotientmodulen V/W.

BEMÆRKNING 2. Ved induktion ses, at det at søge en endomorfi $\varphi : V \to V$ beskrevet ved en blokmatrix af formen

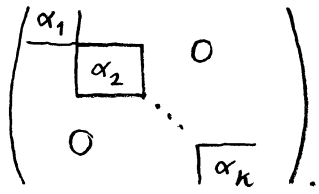


hvor $\alpha_1, \ldots, \alpha_k$ er kvadratiske blokke langs diagonalen, svarer til at søge kæder

$$(0) = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_k = V$$

af φ-invariante underrum, dvs undermoduler i (V, φ), således at α_i hører til kvotienten V_i / V_{i-1}, $i = 1, \ldots, k$.

5.9. SÆTNING. Lad $V_1, \ldots, V_k$ være $L[X]$-moduler, så at matricen α_i hører til V_i, $i = 1, \ldots, k$. Da kan den direkte sum $V = V_1 \oplus \cdots \oplus V_k$ beskrives ved blokmatricen



BEVIS. Ganske som 5.8 □

5.10. DEFINITION. Lad φ være en endomorfi i vektorrummet V og lad (V, φ) betegne den tilhørende $L[X]$-modul. Af definitionen 5.3 (*) fremgår, at for et polynomium

$$f = a_0 + a_1 X + \cdots + a_n X^n \in L[X]$$

er homoteti med f afbildningen

$$v \longmapsto f.v = a_0 v + a_1 \varphi(v) + \cdots + a_n \varphi^n(v).$$

Denne afbildning er således endomorfien

$$a_0 1_V + a_1 \varphi + \cdots + a_n \varphi^n \in End_L(V).$$

Den siges at fremkomme ved <u>indsættelse</u> af φ i polynomiet f, og den betegnes $f(\varphi)$.

Det ses, at $f \in L[X]$ annullerer $L[X]$-modulen (V, φ), netop når $f(\varphi) = 0 \in End_L(V)$. Er dette tilfældet siges endomorfien φ at <u>være rod</u> i polynomiet f.

5.11. SÆTNING. Lad φ være en endomorfi i et vektorrum V. Da er følgende betingelser ækvivalente:

(i) Vektorrummet V er endelig dimensionalt.

(ii) $L[X]$-modulen (V, φ) har endelig længde.

(iii) $L[X]$-modulen (V, φ) er endeligt frembragt, og der findes et polynomium $f \neq 0$ i $L[X]$ hvori φ er rod.

BEVIS. <u>(i) ⇒ (ii)</u>, thi undermodulerne i (V, φ) er specielt underrum i V, og følgelig er $\text{long}(V, \varphi) \leq \dim V$.

<u>(ii) ⇒ (i)</u>: Hvis (V, φ) har endelig længde, findes i V en kæde

$$(0) = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_k = V$$

bestående af $L[X]$-undermoduler V_i, således at kvotienterne V_i / V_{i-1} er simple $L[X]$-moduler. Det er derfor nok at vise påstanden for en simpel $L[X]$-modul. Og en simpel $L[X]$-modul er isomorf med en kvotientmodul $L[X]/\mathfrak{M}$, hvor $\mathfrak{M} \subseteq L[X]$ er et maksimalideal. Specielt er $\mathfrak{M} \neq (0)$, og så er $\mathfrak{M}$ et hovedideal frembragt af et normeret polynomium. Af Struktursætningen for polynomiumskvotient

følger derfor, at kvotienten er endelig dimensional som vektorrum over L.

(ii) $\Leftrightarrow$ (iii): At φ er rod i et polynomium $f \in L[X]$ betyder, at f annullerer $L[X]$-modulen (V, φ). Påstanden følger derfor af generelle resultater om torsionsmoduler (Sætning 4.7).

5.12. Lad i det følgende φ betegne en endomorfi i et endelig dimensionalt vektorrum V. Polynomierne i $L[X]$, der har φ som rod, udgør da et ideal, nemlig annullatoren for $L[X]$-modulen (V, φ). Ifølge Sætning 5.11 er dette ideal $\neq (0)$, og det er derfor et hovedideal frembragt af et polynomium $\neq 0$. Blandt frembringerne findes netop ét normeret polynomium.

DEFINITION. Det normerede polynomium i $L[X]$, der frembringer idealet af polynomier, hvori φ er rod, kaldes det <u>minimale polynomium</u> for endomorfien φ og betegnes f_φ.

Definitionen udsiger altså at $f_\varphi \in L[X]$ er et normeret polynomium med φ som rod og at f_φ er divisor i ethvert polynomium, der har φ som rod.

OBSERVATION. Det minimale polynomium f_φ er det normerede minimale element for $L[X]$-modulen (V, φ).

5.13. Lad α være en matrix hørende til endomorfien φ. Matricen $X1 - \alpha$ har da koefficienter i $L[X]$ ($X1$ betegner matricen $X\begin{pmatrix}1&0\\0&1\end{pmatrix} = \begin{pmatrix}X&0\\0&X\end{pmatrix}$) og dens determinant

$$\chi_\alpha := \det(X1 - \alpha)$$

er derfor et polynomium, øjensynlig normeret. Det er,

eventuelt bortset fra fortegnet ± 1, det sædvanlige karakteristiske polynomium for matricen α. Hvis også matricen β hører til φ, så er $\beta = \sigma^{-1}\alpha\sigma$, hvor matricen σ er invertibel, jfr. Observation 5.2. Det følger, at $\det(\sigma^{-1})\det(\sigma) = \det(1) = 1$, og da matricen $X1$ kommuterer med enhver matrix, har vi $X1 - \beta = \sigma^{-1}(X1)\sigma - \beta$ $= \sigma^{-1}(X1)\sigma - \sigma^{-1}\alpha\sigma = \sigma^{-1}(X1-\alpha)\sigma$ og altså

$$\chi_\beta = \det(X1-\beta) = \det(\sigma^{-1})\det(X1-\alpha)\det(\sigma) = \chi_\alpha.$$

Matricen β har derfor samme karakteristiske polynomium for α. Følgende er derfor en

DEFINITION. Det normerede polynomium $\det(X1-\alpha) \in L[X]$ defineret ud fra en matrix α hørende til φ kaldes det <u>karakteristiske polynomium</u> for endomorfien φ og betegnes χ_φ.

SÆTNING. Det karakteristiske polynomium χ_φ er karakteristisk element for $L[X]$-modulen (V,φ).

BEVIS. Som $L[X]$-modul har V en kæde af undermoduler

$$(0) = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_k = V,$$

så at kvotienterne V_i/V_{i-1} er cykliske $L[X]$-moduler, $i = 1, \cdots, k$. Hvis matricen α_i hører til V_i/V_{i-1}, så hører til V en blokmatrix α af formen

$$\alpha = \begin{pmatrix} \alpha_1 & \text{////} \\ & \ddots \\ 0 & \alpha_k \end{pmatrix}$$

(jfr. Bemærkning 5.8.2) og her har vi øjensynlig $\chi_\alpha = \chi_{\alpha_1} \cdots \chi_{\alpha_k}$. På den anden side gælder ifølge Korollar 4.13(1), at hvis χ_i er karakteristisk element for V_i/V_{i-1}, så er $\chi_1 \cdots \chi_k$ karakteristisk element for V. Det er derfor nok at vise sætningen under forudsætning af at V er cyklisk som $L[X]$-modul, og der-

med isomorf med $L[X]/(f)$, hvor f er et normeret polynomium

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in L[X].$$

Her kan V beskrives ved den i Eksempel 5.6.1 angivne matrix α. På den anden side er f karakteristisk element for V ifølge Sætning 4.12. Det er derfor nok at vise, at $\chi_\alpha = \det(X1 - \alpha) = f$, altså at

$$\det \begin{pmatrix} X & 0 & 0 & \cdots & 0 & a_0 \\ -1 & X & 0 & & 0 & a_1 \\ 0 & -1 & X & & 0 & a_2 \\ \vdots & & \ddots & & & \vdots \\ & & & & X & \vdots \\ 0 & 0 & & & -1 & X+a_{n-1} \end{pmatrix} = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

og det ses let ved induktion efter n ved at udvikle determinanten efter første række ▨

5.14. HAMILTON-CAYLEY'S SÆTNING. Endomorfien φ er rod i sit karakteristiske polynomium χ_φ. Det minimale polynomium f_φ er divisor i χ_φ og de to polynomier har de samme primdivisorer.

BEVIS. Uden brug af den foregående sætning er dette netop indholdet af Sætning 4.14 ▨

OBSERVATION. Det karakteristiske polynomium χ_φ har øjensynlig gradtal $\dim V$, idet φ beskrives ved en $n \times n$-matrix, hvor $n = \dim V$. Det minimale polynomium har derfor grad $\leqslant \dim V$.

EKSEMPEL. $n \times n$-matricen $\begin{pmatrix} \lambda & 1 & 0 \\ & \ddots & 1 \\ 0 & & \lambda \end{pmatrix}$, $\lambda \in L$ beskriver øjensynlig homotetien $v \mapsto \lambda v$. Den karakteristiske polynomium er $(X-\lambda)^n$ og det minimale polynomium er øjensynlig $X - \lambda$.

$n \times n$ matricen $\alpha = \begin{pmatrix} \lambda & 1 & 0 \\ & \ddots & 1 \\ 0 & & \lambda \end{pmatrix}$, $\lambda \in L$ har også karakte-

ristisk polynomium $(X-\lambda)^n$, så det minimale polynomium er divisor heri. Vi finder

$$\alpha-\lambda = \begin{pmatrix} 0 & 1 & & 0 \\ & 0 & 1 & \\ & & 0 & \ddots \\ & & & 1 \\ 0 & & & 0 \end{pmatrix} \qquad (\alpha-\lambda)^i = \begin{pmatrix} 0 & \cdots & 0 & 1 & \cdots & 0 \\ & & & 0 & 1 & \\ & & & & & \ddots \\ & & & & & 1 \\ & & 0 & & & \vdots \\ & & & & & 0 \end{pmatrix} \quad i < n$$

(med i 0'er før 1 i første række). Indsættelse af α i $(X-\lambda)^i$ giver derfor kun 0, når $i \geq n$. Det minimale polynomium er derfor netop $(X-\lambda)^n$.

5.15. Et element $\lambda \in L$ kaldes som bekendt en <u>egenværdi</u> for φ, hvis der i V findes en til λ hørende <u>egenvektor</u> $v \neq 0$, dvs en vektor $v \in V$, $v \neq 0$, således at

$$\varphi(v) = \lambda v.$$

Opfattes V som $L[X]$-modul, er betingelsen ækvivalent med

$$\operatorname{Ann} v = (X-\lambda),$$

thi at $\operatorname{Ann} v \supseteq (X-\lambda)$ er ensbetydende med at $X-\lambda$ annullerer v, dvs $\varphi(v) - \lambda v = 0$, og da $(X-\lambda) \subseteq L[X]$ er et maximalideal, gælder der her "=", netop når $v \neq 0$.

SÆTNING. For et element $\lambda \in L$ er følgende betingelser ækvivalente:
(i) λ er egenværdi for endomorfien φ.
(ii) λ er rod i det minimale polynomium f_φ.
(iii) λ er rod i det karakteristiske polynomium χ_φ.

BEVIS. Et polynomium f i $L[X]$ har som bekendt $\lambda \in L$ som rod netop når (det irreducible førstegradspolynom) $X-\lambda$ er divisor i f. Af Hamilton-Cayley's sætning 5.14 følger derfor straks, at <u>(ii) $\Leftrightarrow$ (iii)</u>.

<u>(i) $\Rightarrow$ (ii)</u>: Antag, at $v \neq 0$ er egenvektor hørende til λ, altså at $\operatorname{Ann} v = (X-\lambda)$. Da f_φ annullerer enhver vektor, er $f_\varphi \in (X-\lambda)$, så $X-\lambda$ er divisor i f_φ.

<u>(ii) $\Rightarrow$ (i)</u>: Hvis $X-\lambda$ er divisor i f_φ, kan vi skrive

$f_\varphi = (x-\lambda)g$, hvor $g \in L[x]$. Specielt ses, at $g \notin (f_\varphi)$, og da (f_φ) er annullator for $L[x]$-modulen V findes derfor en vektor $w \in V$, så at $v := g.w \neq 0$. Og da

$$(x-\lambda).v = (x-\lambda)g.w = f_\varphi.w = 0,$$

er v en egenvektor hørende til φ ▨

5.16. HOVEDSÆTNING. For en endomorfi φ i et endelig dimensionalt vektorrum V over L er følgende betingelser ækvivalente:

(i) Endomorfien φ kan beskrives ved en Jordan-matrix (jfr. 5.1).

(ii) Endomorfien φ kan beskrives ved en øvre trekantsmatrix.

(iii) Det karakteristiske polynomium χ_φ er et produkt

$$\chi_\varphi = (x-\lambda_1)\cdots(x-\lambda_n), \quad \lambda_i \in L$$

af førstegradspolynomier.

(iv) Det minimale polynomium f_φ er et produkt

$$f_\varphi = (x-\lambda_1)\cdots(x-\lambda_s), \quad \lambda_i \in L$$

af førstegradspolynomier.

BEVIS. <u>(i) ⇒ (ii)</u>; thi en Jordan-matrix er specielt en øvre trekantsmatrix.

<u>(ii) ⇒ (iii)</u>, thi det karakteristiske polynomium for en øvre trekantsmatrix er ligesyldig $(x-\lambda_1)\cdots(x-\lambda_n)$, hvor $\lambda_1, \cdots, \lambda_n$ er elementerne i diagonalen.

<u>(iii) ⇒ (iv)</u> ifølge Hamilton-Cayley's sætning 5.14.

<u>(iv) ⇒ (i)</u>: Af sætningen om primær-basis (Bemærkning 4.10) følger, at V som $L[x]$-modul er en direkte sum

$$V = V_1 \oplus \cdots \oplus V_k,$$

hvor undermodulerne V_j er cykliske og isomorfe med moduler af formen $L[x]/(p^n)$, hvor $p \in L[x]$ er et primelement, dvs et irreducibelt polynomium, som vi kan antage er normeret. Da f_φ annullerer V og dermed hver af undermodulerne V_j, er p^n divisor i f_φ.

Af forudsætningen om f_φ følger derfor, at $p = X - \lambda$, med $\lambda \in \{\lambda_1, \dots, \lambda_s\}$. Hver af undermodulerne V_j er derfor isomorf med en modul af formen $L[X]/((X-\lambda)^n)$. Af Eksempel 5.7 følger derfor, at hvert V_j kan beskrives ved en matrix af formen

$$\begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix},$$

og så kan den direkte sum $V = V_1 \oplus \cdots \oplus V_k$ beskrives ved en Jordan-matrix (jfr. Sætning 5.9) ▨

TILFØJELSE. Endomorfien φ kan beskrives ved en diagonalmatrix, hvis og kun hvis det minimale polynomium f_φ er et produkt

$$f_\varphi = (X-\lambda_1)\cdots(X-\lambda_s), \quad \lambda_i \in L$$

af forskellige førstegradspolynomier.

BEVIS. "<u>hvis</u>": Med betegnelserne fra beviset ovenfor er V_j isomorf med en modul af formen $L[X]/(p^n)$, hvor p^n er divisor i f_φ og $p = X - \lambda$. Men så må vi have $n = 1$, og hvert V_j beskrives derfor ved en 1×1-matrix.

"<u>kun hvis</u>": Hvis α er en diagonalmatrix og $\lambda_1, \dots, \lambda_s \in L$ betegner de forskellige elementer i diagonalen så er produktet $(\alpha - \lambda_1)\cdots(\alpha - \lambda_s)$ lig med nulmatricen [idet diagonal-matricer som bekendt multipliceres ved at multiplicere tilsvarende diagonalelementer]. Hvis endomorfien φ kan beskrives ved α, er φ derfor rod i polynomiet $(X-\lambda_1)\cdots(X-\lambda_s)$ og det minimale polynomium f_φ er derfor divisor heri ▨

5.17. Algebraens fundamentalsætning udsiger som bekendt, at hvert normeret polynomium $f \in \mathbb{C}[X]$ kan skrives som produkt

$$f = (X-\lambda_1)\cdots(X-\lambda_s), \quad \lambda_i \in \mathbb{C}.$$

For $L = \mathbb{C}$ indeholder Hovedsætningen derfor sætningen om Jordans normalform (Sætning 5.1).

For normerede polynomier f med reelle koefficienter, $f \in \mathbb{R}[X]$, medfører algebraens fundamentalsætning, at f kan skrives som et produkt

$$(*) \qquad f = p_1 \cdots p_t ,$$

hvor de reelle polynomier p_j enten er førstegradspolynomier $p_j = (X - \lambda)$, $\lambda \in \mathbb{R}$ eller andengradspolynomier $p_j = (X-a)^2 + b^2$, $a \in \mathbb{R}$, $b \in \mathbb{R} \setminus \{0\}$ (uden reelle rødder).

I $\mathbb{C}[X]$ har vi nemlig fremstillingen

$$(**) \qquad f = (X - \lambda_1) \cdots (X - \lambda_s) , \quad \lambda_i \in \mathbb{C}.$$

og heraf fås ved kompleks konjugering (idet jo $\bar{f} = f$):

$$f = (X - \bar{\lambda}_1) \cdots (X - \bar{\lambda}_s) .$$

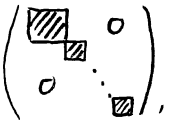
Da fremstillingen (**) er entydig bortset fra permutation af faktorerne, ses, at for hver ikke-reel faktor $X - \lambda$, $\lambda = a + ib$, $a \in \mathbb{R}$, $b \in \mathbb{R} \setminus \{0\}$ i (**) forekommer også faktoren $X - \bar{\lambda}$ i (**), endda det samme antal gange. De ikke-reelle faktorer i (**) kan derfor to og to multipliceres sammen til

$$(X - \lambda)(X - \bar{\lambda}) = (X - a - ib)(X - a + ib) = (X-a)^2 + b^2 ,$$

og så fås fremstillingen (*).

Det følger, at de normerede, irreducible polynomier (dvs primelementer) i $\mathbb{R}[X]$ er polynomierne $X - \lambda$, $\lambda \in \mathbb{R}$ og $(X-a)^2 + b^2$, $a \in \mathbb{R}$, $b \in \mathbb{R} \setminus \{0\}$.

5.18. SÆTNING. *Lad V være et endeligdimensionalt vektorrum over $\mathbb{R}$ og lad $\varphi : V \to V$ være en $\mathbb{R}$-lineær endomorfi. Da kan φ beskrives ved en blokmatrix*



hvor de kvadratiske blokke langs diagonalen har formen

(1) $\begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}$, hvor $\lambda \in \mathbb{R}$, eller (2) $\begin{pmatrix} \alpha & \varepsilon & & 0 \\ & \alpha & \ddots & \\ & & \ddots & \varepsilon \\ 0 & & & \alpha \end{pmatrix}$

hvor $\alpha = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $a \in \mathbb{R}$, $b \in \mathbb{R} \setminus \{0\}$ og $\varepsilon = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ er 2×2-matricer.

BEVIS. I følge sætningen om primær-basis er V som $\mathbb{R}[X]$-modul en direkte sum af moduler af formen $\mathbb{R}[X]/(p^n)$, hvor p er et primelement i $\mathbb{R}[X]$. Det er derfor nok at vise for et sådant primelement p, som vi kan antage er normeret, at $\mathbb{R}[X]$-modulen $V = \mathbb{R}[X]/(p^n)$ kan beskrives ved en matrix af en af de anførte to typer. Hvis $p = X - \lambda$, $\lambda \in \mathbb{R}$, har vi vist det i Eksempel 5.7. Antag derfor, at $p = (X-a)^2 + b^2$, $a \in \mathbb{R}$, $b \in \mathbb{R} \setminus \{0\}$. Blandt de $2n$ polynomier $\frac{1}{b^i} p^i$, $\frac{1}{b^i} \frac{X-a}{b} p^i$, $i = 0, \dots, n-1$, findes netop ét af hver grad $\leq 2n-1$, og disse polynomier udgør derfor en basis for vektorrummet af polynomier af grad $\leq 2n-1$. Da polynomiet p^n har grad $2n$, vil deres ækvivalensklasser

$$e_{2i} := \left(\frac{1}{b^i} p^i\right), \quad e_{2i+1} := \left(\frac{1}{b^i} \frac{X-a}{b} p^i\right) \quad i = 0, \dots, n-1$$

derfor udgøre en $\mathbb{R}$-basis for kvotientten $V = \mathbb{R}[X]/(p^n)$.

Vi finder

$$\frac{X-a}{b} \cdot e_{2i} = e_{2i+1} \qquad i = 0, \dots, n-1, \text{ og dermed}$$

$$(X-a) \cdot e_{2i+1} = \frac{(X-a)^2}{b} \cdot e_{2i} = \frac{p}{b} \cdot e_{2i} - b e_{2i} = \begin{cases} e_{2i+2} - b e_{2i}, & i = 0, \dots, n-2 \\ -b e_{2n-2} & i = n-1 \end{cases}$$

og det betyder netop, at X_V m.h.t. basen $(e_{2n-1}, \dots, e_1, e_0)$ beskrives ved en matrix af den anden type. ▨

("Mængder")

1. Prædikatet

$$p(x): \quad \exists y \left(y \in x \wedge \forall z \left(z \in x \Rightarrow z = y \right) \right)$$

læses sædvanligvis "x er en singleton". Er det ri-meligt?
Vis, at prædikatet $p(x)$ ikke er mængdebestemmende.

2. For at definere ordnet par og kartesisk produkt har vi strengt taget brug for en forskrift, der til vilkårlige mængder a og b knytter (a,b) (det ordnede par) så at følgende gælder:
(a,b) er en mængde.
For mængder a, b, c, d gælder: $(a,b) = (c,d) \Leftrightarrow a = c \wedge b = d$.
For mængder A og B er prædikatet $\exists a \exists b \, (a \in A \wedge b \in B \wedge x = (a,b))$ mængdebestemmende (den specificerede mængde er så $A \times B$).
Vis, at med definitionen

$$(a,b) := \{ \{a\}, \{a,b\} \}$$

er dette krav opfyldt (med $A \times B \subseteq \mathcal{P}(\mathcal{P}(A \cup B))$).
Vis, at en relation kan defineres som en mængde, hvis elementer er ordnede par.

3. "Definition". En "mængde" er en endelig streng bestående af symbolerne "$\varnothing$", "{", "}" og ",", opbygget rekursivt ved betingelserne: $\varnothing$ er en "mængde"; Hvis $A_1, \ldots, A_n$ er "mængder", er også $\{A_1, \ldots, A_n\}$ en "mængde" (idet dog to "mængder", der har de samme "elementer" identificeres). Overvej, at ZF-axiomerne på nær uendelighedsaxiomet gælder.

4. "Definition". En "mængde" er en mængde, og a "$\in$" b betyder, at $\varnothing \subset a \subseteq b$. Overvej, at ZF-axiomerne på nær specifikationsaxiomet gælder.

Algebra 1984 — Opgaver ("Mængder") — 2*

1. Vis for afbildninger $f: A \to B$ og $g: C \to A$ følgende:
   (i) f er injektiv $\wedge$ g er injektiv $\Rightarrow$ $f \circ g$ er injektiv.
   (ii) f er surjektiv $\wedge$ g er surjektiv $\Rightarrow$ $f \circ g$ er surjektiv.
   (iii) $g \circ f$ er injektiv $\Rightarrow$ f er injektiv.
   (iv) $g \circ f$ er surjektiv $\Rightarrow$ g er surjektiv.

2. Bevis påstandene i "Mængder", Lemma 2.1.

3. Vis for afbildninger $f: A \to B$ og $g: B \to A$ følgende:
   (i) $g \circ f = Id_A$ $\wedge$ g injektiv $\Rightarrow$ g og f er bijektive og $g = f^{-1}$
   (ii) $g \circ f = Id_A$ $\wedge$ f surjektiv $\Rightarrow$ g og f er bijektive og $g = f^{-1}$

4. For en afbildning $f: A \to B$ betegner vi med f^{-1} den ved $Y \longmapsto f^{-1}(Y)$ bestemte afbildning $f^{-1}: \mathcal{P}(B) \to \mathcal{P}(A)$. Vis:
   (i) f er injektiv $\Leftrightarrow$ f^{-1} er surjektiv
   (ii) f er surjektiv $\Leftrightarrow$ f^{-1} er injektiv.

5. Vis, at sammensætning af relationer ("Mængder", 1.9 (2)) er associativ.

6. Lad M betegne relationen "er mor til" [xMy betyder altså, at x er mor til y]. Definér tilsvarende: F = "er far til", S = "er søn af", D = "er datter af", B = "er barn af", G = "er gift med".
   (i) Oversæt relationerne $B \circ B$, $F \circ B^{-1}$, $G \circ S$.
   (ii) Udtryk relationerne "er onkel til" og "er tipoldemor til".
   (iii) Hvad betyder udsagnene $x\, B \circ B^{-1}\, x$ og $x\, B^{-1} \circ B\, x$.

7. Lad P, L og C betegne mængden af punkter, linier og cirkler i en plan. Lad $R \subseteq P \times L$ være relationen bestemt ved $p\,R\,l \Leftrightarrow p \in l$. Definer tilsvarende relationen S = "er tangent til". Hvornår gælder $p\,R\,S\,c$ for $p \in P$, $c \in C$?

Algebra 1984 Opgaver 3
("Mængder")

1. Lad $f: A \to B$ være en afbildning. Vis følgende:
   (i) Er $A' \subseteq A$, så er $A' \subseteq f^{-1}(f(A'))$
   (ii) Er $B' \subseteq B$, så er $f(f^{-1}(B')) \subseteq B'$. Hvis f er surjektiv, gælder $f(f^{-1}(B')) = B'$.
   (iii) Er $B', B'' \subseteq B$, så er
   $f^{-1}(B' \cap B'') = f^{-1}(B') \cap f^{-1}(B'')$, $f^{-1}(B' \cup B'') = f^{-1}(B') \cup f^{-1}(B'')$.
   $f^{-1}(B' \setminus B'') = f^{-1}(B') \setminus f^{-1}(B'')$.
   (iv) Er $A', A'' \subseteq A$, så er
   $f(A' \cup A'') = f(A') \cup f(A'')$ og $f(A' \cap A'') \subseteq f(A') \cap f(A'')$
   (gælder "=" altid i den sidste inklusion?).

2. Beskriv følgende familie af delmængder af $\mathbb{R}^2$:
   (i) $A_\lambda = \{(x,y) \mid (x-\lambda)^2 + y^2 = 1\}$, $\lambda \in \mathbb{R}$.
   (ii) $B_\lambda = \{(x,y) \mid x^2 - 2\lambda y + y^2 \leq 1\}$, $\lambda \in \mathbb{R}$.
   Angiv familiens foreningsmængde og fællesmængde.

3. Lad $(B_i)_{i \in I}$ være en familie af mængder, med $I \neq \emptyset$.
   (i) Vis, at der for enhver mængde C gælder:
   $$C \setminus \bigcup_{i \in I} B_i = \bigcap_{i \in I} (C \setminus B_i) \quad \text{og} \quad C \setminus \bigcap_{i \in I} B_i = \bigcup_{i \in I} (C \setminus B_i)$$
   (ii) Vis, at der for enhver afbildning $f: A \to B$, med $B_i \subseteq B$ for alle $i \in I$, gælder:
   $$f^{-1}\left(\bigcup_{i \in I} B_i\right) = \bigcup_{i \in I} f^{-1}(B_i), \quad f^{-1}\left(\bigcap_{i \in I} B_i\right) = \bigcap_{i \in I} f^{-1}(B_i).$$

4. Lad A være en mængde. Findes der afbildninger: $\emptyset \to A$? Hvor mange? Findes der afbildninger: $A \to \emptyset$? Hvor mange?

Algebra 1984

Opgaver 4
("Mængder")

1. Bestem for mængder A, B og C bijektive afbildninger
   (i) $A^{B \cup C} \approx A^B \times A^C$ [når $B \cap C = \varnothing$]
   (ii) $A^{B \times C} \approx (A^B)^C$
   (iii) $(A \times B)^C \approx A^C \times B^C$.

2. Vis v.hj.a. følgende konstruktion, at for en given familie $(F_i)_{i \in I}$ af mængder kan hver mængde F_i erstattes med en ækvipotent mængde F_i', så at mængderne $(F_i')_{i \in I}$ er parvis disjunkte (dvs opfylder: $i \neq j \Rightarrow F_i' \cap F_j' = \varnothing$):
   Konstruktion: $F_i' = \{ (x, k) \in \bigcup_{j \in I} F_j \times I \mid k = i \wedge x \in F_i \}$.

3. (i) Gennemfør de enkelte skridt i beviset for Bernstein's ækvivalenssætning "Mængder" 2.3.
   (ii) Vis, at den dér forekommende mængde C kan beskrives ud fra $A_0 := A \setminus g(B)$ som
   $$C = A_0 \cup A_1 \cup A_2 \cup \ldots \quad , \quad A_n = (g \circ f)^n (A_0).$$
   (iii) Gør denne beskrivelse de enkelte skridt lettere?

4. Lad A være en mængde og lad a, b være to forskellige elementer i A. Angiv en bijektiv afbildning: $\mathcal{E}(A) \to \mathcal{F}(A)$, jfr. "Mængder", 2.6.2. [Vink: Brug eventuelt beviset for Bernstein's ækvivalenssætning].

5. Lad $X \subseteq \mathbb{R}$ være en delmængde, som indeholder et intval. (af længde > 0). Vis, at X er ækvipotent med $\mathbb{R}$.

6. Lad $\mathcal{C}$ være en mængde af parvis disjunkte åbne cirkelskiver i $\mathbb{R}^2$. Vis, at $\mathcal{C}$ er tællelig.

7. Vis, at $\mathbb{R}^{\mathbb{N}}$ er ækvipotent med $\mathbb{R}$.

8. Vis, at $\mathbb{R} < \mathbb{R}^{\mathbb{R}}$.

Algebra 1984 Opgaver 5
("Mængder")

1. Lad $\mathcal{C}$ betegne mængden af kontinuerte afbildninger $f: \mathbb{R} \to \mathbb{R}$. Vis, at $\mathcal{C}$ er ækvipotent med $\mathbb{R}$. [gør rede for, at $\mathcal{C} \subseteq \mathbb{R}^{\mathbb{R}}$ og at restriktion definerer en afbildning: $\mathbb{R}^{\mathbb{R}} \to \mathbb{R}^{\mathbb{Q}}$. Vis, at den sammensatte afbildning: $\mathcal{C} \hookrightarrow \mathbb{R}^{\mathbb{R}} \to \mathbb{R}^{\mathbb{Q}}$ er injektiv].

2. Der findes en afbildning $\psi: \mathbb{R} \to \mathbb{R}$ med følgende egenskab: For enhver kontinuert afbildning $f: \mathbb{R} \to \mathbb{R}$ eksisterer der et tal $t \in \mathbb{R}$, så at $f(t) = \psi(t)$. Vis denne påstand. [Vink: Definér ud fra en bijektiv afbildning: $\Psi: \mathbb{R} \tilde{\to} \mathcal{C}$ (jfr. opgave 1) ψ ved $\psi(t) = \Psi(t)(t)$].

3. Lad M være en mængde og lad χ_1, χ_2 være de karakteristiske funktioner for to delmængder $A_1, A_2 \subseteq M$. Udtryk ved χ_1, χ_2 de karakteristiske funktioner for $M \setminus A_1$, $A_1 \cap A_2$, $A_1 \cup A_2$, $A_1 \setminus A_2$.

4. (i) Lad P betegne mængden af polynomier $p = a_0 + a_1 X + \cdots + a_m X^m$ med hele koefficienter (d: $a_i \in \mathbb{Z}$). Vis, at følgende fører til en effektiv numerering af elementerne i P: Delmængden

$$P_n = \{ a_0 + a_1 X + \cdots + a_m X^n \mid |a_0| + \cdots + |a_m| \leq n \}$$

er endelig. Vi kan opfatte P_n som delmængde $P_n \subseteq \mathbb{Z}^{n+1}$, og som sådan er P_n totalt ordnet med leksikografisk ordning. P_0 består af ét polynomium p_0 = nulpolynomiet. Føj hertil polynomierne i P_1 i rækkefølge (drop gentagelser), føj hertil polynomierne i P_2 o.s.v.

(ii) Lad A betegne mængden af algebraiske tal i intervallet $[0,1[$. Vis, at hvert tal $\xi \in A$ er rod i et polynomium p_i fra $P = \{p_0, p_1, \cdots\}$, med $p_i \neq p_0$. Vis, at følgende fører til en nummerering af A: Tag først, ordnet efter størrelse, de $\xi \in A$, der er rødder i p_1, dernæst dem der er rødder i p_2 (drop gentagelser) osv.

(iii) Cantor's argument producerer et transcendent tal ξ ud fra det foregående. Bestem ξ med 4 decimaler.

Algebra 1985 — Opgaver 32 ("Mængder")

1. Lad u være en udvalgsfunktion på en partielt ordnet mængde X.
   (i) Bevis Sætning 3.3.1 i "Mængder".
   (ii) Vis, at hvis K og L er forskellige u-kæder i X, så er enten L et ægte afsnit af K (dvs $L = K_{<k}$ med passende $k \in K$) eller K er et ægte afsnit af L [Kig nærmere på beviset for Lemma 3.3 i "Mængder"]
   (iii) Vis, at en delmængde $K \subseteq X$ er en u-kæde, hvis og kun hvis K er en velordnet delmængde og for alle $k \in K$ er $u(M_{K<k}) = k$.

2. Vis, at mængden $\{n - \frac{1}{m} \mid n, m \in \mathbb{N}\}$ er en velordnet delmængde af $(\mathbb{Q}, <)$.

3. (i) Lad X og Y være velordnede mængder. Vis, at produktet $X \times Y$ med leksikografisk ordning $[(x_1, y_1) < (x_2, y_2) \overset{DEF}{\Leftrightarrow} (x_1 < x_2) \vee (x_1 = x_2 \wedge y_1 < y_2)]$ er velordnet.
   (ii) Generaliser til et endeligt produkt $X_1 \times \cdots \times X_m$.
   (iii) Hvad med et numerabelt produkt $X_1 \times X_2 \times \cdots$
   (iv) Kan mængden af (endelige dansk) sætninger velordnes?

4. Lad R være en kommutativ ring, som ikke er nulringen.
   (i) Vis, at der i R findes et maksimalideal.
   (ii) Vis, at der i R findes et minimalt primideal [Er du sikker på, at der overhovedet findes primidealer i R?]
   (iii) Spørgsmål (ii) er lettest at besvare, hvis nulreglen gælder. Hvorfor?

5. Lad R betegne produktringen $R = \mathbb{R}^{\mathbb{N}} = \mathbb{R} \times \mathbb{R} \times \cdots$ af alle reelle talfølger $(\varphi_1, \varphi_2, \cdots)$.
   (i) Vis, at for hvert $a \in \mathbb{N}$ er delmængden $I_a := \{(\varphi_1, \varphi_2, \cdots) \mid \varphi_a = 0\}$ et maksimal-ideal i R, og angiv kvotienten R/I_a.
   (ii) Vis, at delmængden $J_\infty := \{(\varphi_1, \varphi_2, \cdots) \mid \varphi_m = 0$ fra et vist trin$\}$ er et ideal i R.
   (iii) Vis, at ethvert maksimalideal i R, som er $\neq I_a$ for alle $a \in \mathbb{N}$, vil $\supseteq J_\infty$.
   (iv) Vis, at der i R findes maksimalidealer $\mathfrak{m}$ med $\mathfrak{m} \supseteq J_\infty$. Kan du beskrive sådan et maksimalideal?

1. Lad N være en Λ-modul og lad $\mathfrak{a} \subseteq \Lambda$ være et ideal, så at $\mathfrak{a} \subseteq \mathrm{Ann}(N)$. Vis, at N "på fornuftig måde" er en $\Lambda/\mathfrak{a}$ - modul.

2. For en Λ-modul M og et ideal $\mathfrak{a} \subseteq \Lambda$ skrives
$$\mathfrak{a}M = \{ \alpha_1 x_1 + \cdots + \alpha_n x_n \mid n \in \mathbb{N},\ \alpha_1, \ldots, \alpha_n \in \mathfrak{a},\ x_1, \ldots, x_n \in M \}.$$
(i) Vis, at $\mathfrak{a}M$ er en undermodul i M.
(ii) Vis, at kvotientmodulen $M/\mathfrak{a}M$ på fornuftig måde er en $\Lambda/\mathfrak{a}$-modul.
(iii) Bestem en isomorfi af $\Lambda/\mathfrak{a}$-moduler : $\Lambda_s^n / \mathfrak{a}\Lambda_s^n \xrightarrow{\sim} (\Lambda/\mathfrak{a})_s^n$.

3. Lad I være et venstreideal i Λ, og sæt $\tilde{\Lambda} = \{ \lambda \in \Lambda \mid I\lambda \subseteq I \}$.
(i) Vis, at $\tilde{\Lambda} \subseteq \Lambda$ er en delring.
(ii) Vis, at $I \subseteq \tilde{\Lambda}$ og at I er et (tosidet) ideal i $\tilde{\Lambda}$.
(iii) Find en anti-ring isomorfi : $\tilde{\Lambda}/I \xrightarrow{\sim} \mathrm{End}_\Lambda(\Lambda_s/I)$.

4. (i) Lad $\alpha_1, \ldots, \alpha_m$ være elementer i Λ_s^n opfattet som rækker, og lad $\alpha = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_m \end{pmatrix} \in \mathrm{Mat}_m(\Lambda)$ være matricen bestående af disse rækker. Lad $\lambda = (\lambda_1, \ldots, \lambda_m)$ være en række bestående af skalarer $\lambda_i \in \Lambda$. Vis, at $\lambda\alpha = \lambda_1\alpha_1 + \cdots + \lambda_m\alpha_m$.
(ii) Lad $N \subseteq \Lambda_s^n$ være en undermodul. Vis, at delmængden $I_N \subseteq \mathrm{Mat}_n(\Lambda)$ bestående af de matricer, hvis rækker alle tilhører N, er et venstreideal i $\mathrm{Mat}_n(\Lambda)$.
(iii) Vis, at alle venstreidealer i $\mathrm{Mat}_n(\Lambda)$ er af formen I_N med en passende (entydigt bestemt) undermodul $N \subseteq \Lambda_s^n$.

5. For hvilke $\begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{Z}^2$ er undermodulen $\mathbb{Z}\begin{pmatrix} a \\ b \end{pmatrix} \subseteq \mathbb{Z}^2$ direkte summand.

6. (i) Sæt $M = \mathbb{Z}^{\mathbb{N}} = \mathbb{Z} \times \mathbb{Z} \times \cdots$. Vis, at
$$(\varphi_1, \varphi_2, \cdots) \longmapsto ((\varphi_1, \varphi_3, \cdots), (\varphi_2, \varphi_4, \cdots))$$
definerer en isomorfi af $\mathbb{Z}$-moduler : $M \xrightarrow{\sim} M \oplus M$.
(ii) Sæt $\Lambda = \mathrm{End}_{\mathbb{Z}}(M)$. Vis, at der findes en isomorfi : $\Lambda_s \xrightarrow{\sim} \Lambda_s^2$.
(iii) Vis, at for alle n, m er $\Lambda_s^n \simeq \Lambda_s^m$.

Algebra 1985

Opgaver 34
("Moduler").

1. Lad S og T være simple moduler.
(i) Vis, at hvis en Λ-homomorfi $f: S \to T$ ikke er nulhomomorfien, så er f en isomorfi [Betragt f's kerne og billede].
(ii) Vis, at ringen $End_\Lambda(S)$ er et skævlegeme (Schur's lemma).

2. Vis, at $\bigcap \{I \mid I \subseteq \Lambda$ er et maksimalt venstreideal$\}$
$= \bigcap \{Ann\, S \mid S$ er en simpel Λ-modul$\}$.

3. Lad M være en kommutativ gruppe og lad $\Lambda \subseteq End(M)$ være en delring. Hvordan organiseres M fornuftigt som Λ-modul. Hvad betyder det, at M er simpel som Λ-modul.

4. Lad V være et vektorrum af dimension n over et skævlegeme D, med basis $e_1, \dots, e_n$ og skriv $S = V$ for V opfattet som modul over $\Lambda = End_D(V)$.
(i) Vis, at S er en simpel Λ-modul.
(ii) Vis, at $\varphi \mapsto (\varphi(e_1), \dots, \varphi(e_n))$ er en bijektiv afbildning
$$End_D(V) \xrightarrow{\sim} V \oplus \cdots \oplus V,$$
og at denne afbildning er en Λ-isomorfi
$$\Lambda_S \xrightarrow{\sim} S \oplus \cdots \oplus S.$$
(iii) Vis, at ringen $\Lambda = End_D(V)$ har længde n.
(iv) Vis, at enhver simpel Λ-modul T er isomorf med S [Vælg surjektiv homomorfi : $S^n \simeq \Lambda_S \to T$. Restriktionen til en af summanderne er en homomorfi $\neq 0 : S \to T$].

5. For fast $n \in \mathbb{N}$ betragtes $M = \mathbb{Z}/\mathbb{Z}n$. For hver divisor d i n er $\mathbb{Z}n \subseteq \mathbb{Z}d$ og $\mathbb{Z}d$ svarer således til en undermodul, som vi betegner $M(d) \subseteq M$.
(i) Vis, at når $e \mid d$, $d = ef$, så er $M(d) \subseteq M(e)$, og bestem en isomorfi $\mathbb{Z}/f\mathbb{Z} \xrightarrow{\sim} M(e)/M(d)$.
(ii) Bestem når d og d' er divisorer i n : $M(d) \cap M(d')$ og $M(d) + M(d')$.
(iii) For $n = 24$ har de to kæder $(0) = M(24) \subseteq M(6) \subseteq M(2) \subseteq M$ og $(0) = M(24) \subseteq M(3) \subseteq M$ ækvivalente forfininger. Angiv disse.

Algebra 1985 — Opgaver 35

("Moduler")

1. Lad Λ være en ring af endelig (venstre-) længde d. Vis, at $\operatorname{long}(\mathrm{Mat}_n(\Lambda)) = nd$ [Udnyt f.eks. en beskrivelse af venstreidealer i $\mathrm{Mat}_n(\Lambda)$ ved undermoduler i Λ_Λ^n].

2. (i) Sæt $A = \begin{pmatrix} \mathbb{C} & \mathbb{C} \\ 0 & \mathbb{R} \end{pmatrix}$ og vis: $\operatorname{long} A_\Lambda = 3$, $\operatorname{long} A_A = 4$.

(ii) Sæt $B = \begin{pmatrix} \mathbb{C} & \mathbb{C} \\ 0 & \mathbb{Q} \end{pmatrix}$ og vis: $\operatorname{long} B_\Lambda = 3$, $\operatorname{long} B_B = \infty$.

3. (i) Lad $n = n_1 \cdots n_r$ være en opløsning af $n \in \mathbb{N}$. Konstruer en kæde af længde r i $M = \mathbb{Z}/\mathbb{Z}n$, hvis kvotienter er $\mathbb{Z}/n_\nu\mathbb{Z}$, $\nu = 1, \dots, r$.

(ii) De simple $\mathbb{Z}$-moduler er som bekendt $\mathbb{Z}/\mathbb{Z}p$, hvor p er et primtal. Vis, at en endelig kommutativ gruppe er en Jordan-Hölder modul (over $\mathbb{Z}$), og vis, at Jordan-Hölder's sætning medfører sætningen om eksistens og entydighed af primopløsninger.

4. (i) Lad F være en fri Λ-modul med fri basis $(e_1, \dots, e_n)$. Vis, at for hvert ideal $\mathfrak{a} \subseteq \Lambda$ har $F/\mathfrak{a}F$ som $\Lambda/\mathfrak{a}$-modul en fri basis med n elementer.

(ii) Lad R være en kommutativ ring, lad $\mathfrak{m} \subset R$ være et maksimalideal (og altså $R/\mathfrak{m}$ et legeme). Lad F være en fri R-modul. Vis, at der for hver fri R-modul F med fri basis $e_1, \dots, e_m$ gælder $n = \dim_{R/\mathfrak{m}} F/\mathfrak{m}F$.

(iii) Bevis, at der for en kommutativ ring $R \neq 0$ gælder:
$$R^n \simeq R^m \Rightarrow n = m.$$

5. Lad Λ være en endelig ring af karakteristik p, hvor p er et primtal. Vis, at $|\Lambda|$ er en potens af p.

6. Lad R være en kommutativ ring. Polynomiumsringen $R[x]$ kan opfattes som R-modul. Vis, at den er fri og angiv en basis.

1. Betragt for idealer $I, J \subseteq R$ kvotientmodulerne R/I og R/J.
(i) Vis, at hvis der findes en injektiv homomorfi: $R/I \to R/J$ så er $I \supseteq J$.
(ii) Vis, at hvis der findes en surjektiv homomorfi: $R/I \to R/J$, så er $I \subseteq J$.
(iii) Vis, at R/I og R/J kun er isomorfe R-moduler, når $I = J$.

2. Betragt for elementer $a_1, \dots, a_n \in R$ "van der Monde determinanten"

$$D(a_1, \dots, a_n) = \det \begin{pmatrix} 1 & 1 & & 1 \\ a_1 & a_2 & \cdots & a_n \\ \vdots & \vdots & & \vdots \\ a_1^{n-1} & a_2^{n-1} & & a_n^{n-1} \end{pmatrix}$$

Vis, at $D(a_1, \dots, a_n) = \prod_{j>i} (a_j - a_i)$ [Skaf 0'er i øverste række (på nær på 1. pladsen), og find $D = 1 \cdot \det((n-1)\times(n-1)\text{-matrix})$. Heri er j-te søjle et multiplum af $a_j - a_1$, $j > 1$. Find herved $D = \left(\prod_{j>1}(a_j - a)\right) \cdot \det((n-1)\times(n-1)\text{-matrix})$ og omform denne matrix ved rækkeoperationer til en "$(n-1)\times(n-1)$ van der Monde matrix"].

3. Betragt en kvadratisk matrix $\beta \in \mathrm{Mat}_n(R)$ med søjler betegnet $x_1, \dots, x_p, y_1, \dots, y_q$ $(p+q = n)$. For hver delmængde $P \subseteq \{1, \dots, n\}$ med p elementer betegnes med x^P den $(p \times p)$-delmatrix af $(x_1, \dots, x_p)$, der hører til rækker med index i P. Determinanten $\det\beta$ er en sum af led af formen $\pm x_{1\sigma_1} \cdots x_{p\sigma_p} y_{1\tau_1} \cdots y_{q\tau_q}$ hvor $\sigma_1, \dots, \sigma_p, \tau_1, \dots, \tau_q$ er forskellige tal i $\{1, \dots, n\}$. Vi kan følgelig skrive

$$\det\beta = \sum x_{1\sigma_1} \cdots x_{p\sigma_p} A_{\sigma_1, \dots, \sigma_p},$$

hvor $A_{\sigma_1, \dots, \sigma_p}$ kun afhænger søjlerne $y_1, \dots, y_q$.
(i) Sæt $\{\sigma_1, \dots, \sigma_p\} = P = \{i_1, \dots, i_p\}$, hvor $1 \le i_1 < \cdots < i_p \le n$ og lad σ være permutationen i P bestemt ved $\sigma(i_\nu) = \sigma_\nu$, $\nu = 1, \dots, p$.
Vis, at $A_{\sigma_1, \dots, \sigma_p} = \mathrm{sign}(\sigma) A_{i_1, \dots, i_p}$
[vink: overvej, at led, der indeholder $x_{1\sigma_1} \cdots x_{p\sigma_p}$ kan fås udfra led, der indeholder $x_{1i_1} \cdots x_{pi_p}$ ved en permutation af søjlerne]
Slut heraf, at

$$\det\beta = \sum_{|P|=p} \det x^P A_{i_1 \cdots i_p} \qquad P = \{i_1, \dots, i_p\},\ i_1 < \cdots < i_p$$

(ii) Vis formlen

$$\det\beta = \sum_{|P|=p} \mathrm{sign}\, P \,(\det x^P)(\det y^{CP}) \qquad \begin{pmatrix} \text{og angiv fortegnet} \\ \text{sign } P \end{pmatrix}$$

Algebra 1985

Opgaver 37

("Det").

1. Gør rede for at matricen $\begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix} \in Mat_2(\mathbb{Z})$ definerer en isomorfi $(\mathbb{Z}/6)^2 \to (\mathbb{Z}/6)^2$, og angiv den inverse afbildning.

2. (i) Vis, at matricen $\sigma = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \in Mat_2(\mathbb{F}_2)$ er invertibel og altså definerer en bijektiv (lineær) afbildning: $\mathbb{F}_2^3 \to \mathbb{F}_2^3$.
(ii) Der er 8 elementer i mængden $\mathbb{F}_2^3$. Skriv permutationen σ som sammensætning af disjunkte cykler.
(iii) Angiv ordenen af σ. Hvad er fortegnet $\operatorname{sign}(\sigma)$.

3. Lad $\lambda \in R$. Vis, at matricen $\begin{pmatrix} 1 & 1 & \lambda \\ \lambda & 1 & 0 \end{pmatrix}$ definerer en surjektiv lineær afbildning: $R^3 \to R^2$.

4. For $R = \mathbb{Z}/6$ betragtes matricen $\alpha = (\bar{2}, \bar{3})$.
(i) Vis, at α definerer en surjektiv homomorfi: $R^2 \to R$.
(ii) Vis, at α har søjlerang 0 og at billedet $\alpha(R^2)$ har rang 1.
(iii) Vis, at α har rækkerang 1

5. Lad R være et integritetsområde, og lad $\alpha \in Mat_{n,p}(R)$.
(i) Vis, at søjlerang og rækkerang af α er samme tal og beskriv dette tal.
(ii) Vis, at rangen af billedet $\operatorname{rg}(\alpha(R^p))$ er matricens søjlerang.

6. Lad M være en R-modul og lad $v_1, \ldots, v_n \in M$ være et frembringersystem. Lad M' være undermodulen frembragt af elementer $u_1, \ldots, u_m \in R$ bestemt ved $(u_1, \ldots, u_m) = (v_1, \ldots, v_n)\alpha$.
(i) Vis, at der for alle $x \in M$ gælder $\det(\alpha)x \in M'$.
(ii) Vis, at $\det(\alpha) \in \operatorname{Ann}(M/M')$.

7. Lad F være et endeligt legeme med q elementer.
(i) Bestem antallet af injektive lineære afbildninger: $F^p \to F^n$.
(ii) Vis, at gruppen $GL_n(F)$ er endelig og bestem ordenen af $GL_n(F)$ og $SL_n(F)$.

Algebra 1985

Opgaver 38*
("PID")

1. Betragt en cyklisk R-modul $M = R/(\alpha)$, hvor $\alpha \neq 0$.
(i) Vis, at enhver undermodul $C \subseteq M$ er cyklisk og at $\mathrm{Ann}\, C = (\delta)$, med $\delta \mid \alpha$.
(ii) Vis, at der for hver divisor $\delta \mid \alpha$ findes netop én undermodul C i M med $\mathrm{Ann}(C) = (\delta)$.

2. Lad e være et torsionselement i R-modulen M, således at $\mathrm{Ann}\, e = (\alpha)$, $\alpha \neq 0$. Bestem $\mathrm{Ann}\, \lambda e$ for $\lambda \in R$.

3. Successive række- og søjleoperationer på en matrix $\alpha \in \mathrm{Mat}_{n,p}(R)$ styres bekvemt på følgende måde:
I de kolonner skrives øverst matricen $1_n \in \mathrm{Mat}_n(R)$, matricen $\alpha \in \mathrm{Mat}_{n,p}(R)$ og matricen $1_p \in \mathrm{Mat}_p(R)$. Hver rækkeoperation udføres på begge matricer i 1. og 2. kolonne og hver søjleoperation udføres på begge matricer i 2. og 3. kolonne. Når α efter endelig mange skridt er omformet til en matrix δ står der i 1. kolonne en matrix $\sigma \in \mathrm{Mat}_n(R)$ og i 3. kolonne en matrix $\tau \in \mathrm{Mat}_p(R)$.
(i) Vis, at $\sigma \alpha \tau = \delta$.
(ii) Vis, at $\{ x \in R^p \mid \alpha x = b \} = \{ \tau y \mid y \in R^p \wedge \delta y = \sigma b \}$
(iii) Bestem den fuldstændige løsning $(x, y, z) \in \mathbb{Z}^3$ til

$$\begin{aligned} x + 2y + 3z &= 2 \\ 4x + 5y + 6z &= -1. \end{aligned}$$

4. For en matrix $\alpha \in \mathrm{Mat}_{n,p}(R)$ og $q = 0, 1, \ldots$ betegnes med $\mathcal{O}_q(\alpha) \subseteq R$ idealet frembragt af $(q \times q)$-underdeterminanterne i α.
(i) Vis når $\sigma \in GL_n(R)$ og $\tau \in GL_p(R)$ at $\mathcal{O}_q(\sigma \alpha \tau) = \mathcal{O}_q(\alpha)$.
(ii) Bestem når $\sigma \alpha \tau = \begin{pmatrix} \delta_1 & & & \\ & \ddots & & \\ & & \delta_r & \\ 0 & & & 0 \end{pmatrix}$, $\delta_1 \mid \delta_2 \mid \ldots \mid \delta_n \neq 0$, idealerne $\mathcal{O}_q(\alpha)$, og vis, at $\delta_1, \delta_2, \ldots$ (på nær association) kan bestemmes udfra $\mathcal{O}_q(\alpha)$, $q = 0, 1, \ldots$ og dermed ud fra α.

Algebra 1985 Opgaver 39
("PID").

1. Lad π være et irreducibelt element i R. For en R-modul M sættes ${}_\pi M = \{x \mid \pi x = 0\}$ = kernen for homotetien π_M, og $\pi M = \{\pi x \mid x \in M\}$ = billedet ved homotetien π_M.

(i) Vis, at ${}_\pi M$ og $M/\pi M$ er vektorrum over legemet $R/(\pi)$.

(ii) Vis, at hvis M er en endeligt frembragt torsionsmodul, så er $\dim_{R/(\pi)} {}_\pi M = \dim_{R/(\pi)} M/\pi M$.

[Vink: Benyt, at $\dim_{R/(\pi)} = \text{long}_R$ og at M har endelig længde]

(iii) Lad $(e_1, \cdots, e_n)$ være en primærbasis for en endeligt frembragt torsionsmodul, og lad a_π betegne antallet af π-primære blandt e_i'erne. Vis, at

$$a_\pi = \dim_{R/\pi} M/\pi M$$

Lad $a_{\pi,n}$ betegne antallet af e_i'er for hvilke $\operatorname{Ann} e_i = (\pi^n)$. Vis, at

$$\dim_{R/(\pi)} \pi^{k-1}M/\pi^k M = \sum_{n \geq k} a_{\pi,n}.$$

2. Lad φ være en endomorfi i et endeligt dimensionalt komplekst vektorrum V. Lad α være en Jordan matrix hørende til φ (i en passende basis). Matricen α består altså af kvadratiske blokke langs diagonalen af formen.

$$n\left\{\begin{pmatrix} \lambda & 1 & & 0 \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix}\right.$$

Vis, hvorledes antallet $a_{\lambda,n}$ af sådanne blokke i α kan bestemmes ud fra tallene $\dim_{\mathbb{C}} (\varphi - \lambda)^k(V)$, $k = 0, 1, 2, \cdots$

3. (i) Lad $\alpha \in GL_2(\mathbb{R})$ have formen $\alpha = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ med $(a,b) \neq (0,0)$. Vis, at der findes $r > 0$ og $v \in \mathbb{R}$ så at der gælder $\alpha = r\begin{pmatrix} \cos v & -\sin v \\ \sin v & \cos v \end{pmatrix}$, og vis, at $t \mapsto f(t) = [1-t+rt.]\begin{pmatrix} \cos vt & -\sin vt \\ \sin vt & \cos vt \end{pmatrix}$ definerer en kontinuert afbildning $f: [0,1] \to GL_2(\mathbb{R})$ med $f(0) = 1_2$, $f(1) = \alpha$.

(ii) Find en tilsvarende kontinuert afbildning når $\alpha = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$, $\lambda\mu > 0$.

(iii) Vis, at der for enhver matrix $\alpha \in GL_n^+(\mathbb{R})$ (dvs $\det \alpha > 0$) findes en kontinuert afbildning $f: [0,1] \to GL_n(\mathbb{R})$ med $f(0) = 1_n$, $f(1) = \alpha$.

Algebra 1985

Opgaver 40
("PID")

1. I $\mathbb{Z}^2$ betragtes undergruppen H frembragt af $\binom{2}{3}$ og $\binom{3}{-2}$. Vis, at kvotienten $\mathbb{Z}^2/H$ er en endelig gruppe og prøv at bestemme dens orden.

2. Lad $\mathbb{Z}[\xi]$ være en kvadratisk talring. Vis, at hvert ideal i $\mathbb{Z}[\xi]$ kan frembringes af 2 elementer [Vink: dit relevante hovedidealområde er $R = \mathbb{Z}$].

3. Lad G være en endelig kommutativ gruppe og lad $e = e(G)$ betegne den maximale elementorden i G. Vis, at e er divisor i $|G|$, og at $e(G) = |G|$, hvis og kun hvis G er cyklisk.

4. Lad L være et legeme og lad $G \subseteq L^*$ være en endelig gruppe. Vis, at G er cyklisk [Vink: Kig på rødder i polynomiet $X^e - 1 \in L[X]$, hvor $e = e(G)$].

5. Lad $\alpha = (\alpha_1, \ldots, \alpha_n)$ være en basis for $\mathbb{R}^n$ og betragt "polytopet" $P(\alpha) = \{ \lambda_1\alpha_1 + \cdots + \lambda_n\alpha_n \mid 0 \leq \lambda_i < 1, i = 1, \ldots, n \}$. Vis, at hvis vektorerne $\alpha_1, \ldots, \alpha_n$ er gitterpunkter ($\ni \in \mathbb{Z}^n$), så er antallet af gitterpunkter i $P(\alpha)$ netop $|\det(\alpha)|$.

6. Letter resultatet i Sætning 4.16 besvarelsen af opgave 1

7. I den kvadratiske talring $\mathbb{Z}[\sqrt{-5}]$ betragtes idealet $m = (3, 1 - \sqrt{-5})$. Vis, at m er et **maksimalideal** og bestem kvotienten $\mathbb{Z}[\sqrt{-5}]/m$ [Vink: Vis, at $\mathbb{Z}3 + \mathbb{Z}(1 - \sqrt{-5})$ er et ideal i $\mathbb{Z}[\sqrt{-5}]$, og følgelig $= m$, og bestem $|\mathbb{Z}[\sqrt{-5}]/m|$.

8. Vis, at matricerne $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$ og $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ frembringer gruppen $SL_2(\mathbb{Z}[i])$.