NAIV MÆNGDELÆRE

1. Zermelo–Fraenkel's axiomer.

(1.0) Hvad er en mængde? Vi har alle en intuitiv fornemmelse 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 tre spørgsmåltegn herunder

????

På den anden side har vi visse samlinger, som vi nødig vil acceptere som mængder, f.eks. samlingen af alle mængder, idet accepten 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 mængdeteori. 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

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

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

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

Mængden A er en *ægte* delmængde af mængden B, og vi skriver $A \subset B$, hvis $A \subseteq B$ og der findes et element b i B, så at b ikke tilhører A.

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 denne egenskab. 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 både har $B \subseteq A$ og $B \in A$. Specielt kræver vi ikke, at en mængde ikke må være element i sig selv (men det er nu ikke nemt at forestille sig 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

$$B \in B \quad \Leftrightarrow \quad B \notin B.$$

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 $\mathcal{C}$.*

Vi kalder den *foreningsmængden* af mængderne i $\mathcal{C}$, og vi betegner den $\cup\mathcal{C}$eller $\bigcup_{X\in\mathcal{C}} X$. 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 $\{A_1, \ldots, A_n\}$, 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 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 $A \cap B := \bigcap\{A, B\}$. 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) Potens–axiomet. *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) Udskiftnings–axiomet. *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 der 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 prædikatet "$x \neq x$" 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

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

Af Russell's paradox 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 udfra axiomerne kan vi udlede de begreber og sætninger, vi kender fra den elementære mængdelære. Uden at gå i detaljer nævner vi:

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

(1.9.2) En *relation* R er en mængde, der er delmængde af et cartesisk produkt $A \times B$ for passende mængder A og B. Relationens *venstre–domæne* er mængden

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

og dens *højre-domæne* er mængden

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

For hver relation R er også den *inverse*

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

en relation, og er S endnu en relation, så er også den *sammensatte*

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

en relation.

(1.9.3) En *afbildning* er en relation f, som opfylder:

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

Afbildningens højre–domæne kaldes også dens *domæne* eller *definitionsmængde* og betegnes $\mathbf{dom} f$. For hvert element $x \in \mathbf{dom} f$ findes altså netop et element y, så at $(y, x) \in f$. Det kaldes f's *værdi* i x og betegnes $y =: f(x)$.

(1.9.4) En afbildning f siges at være en *afbildning fra A til B* , og vi skriver

$$f : A \to B,$$

hvis $\mathbf{dom} f = A$ og $\mathbf{dom}_l f \subseteq B$. Mængden af afbildninger $f : A \to B$ betegnes B^A [Hvorfor er det en mængde?]. For hver mængde A er den *identiske afbildning* Id_A (eller 1_A) bestemt ved

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

Er $A \subseteq B$ en delmængde, kan den identiske afbildning Id_A opfattes som en afbildning (kaldet *inklusionsafbildningen*) : $A \to B$.

(1.9.5) En afbildning $f : A \to B$ er *injektiv* , 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 *surjektiv* , hvis der for alle elementer b i B gælder

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

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

(1.9.6) Er $f : A \to B$ en afbildning, defineres for hver delmængde $A' \subseteq A$ *billedet* eller *billedmængden* af A' 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 *urbilledet* eller *originalmængden* 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 $f^{-1}(\{b\})$.

(1.9.7) Er $f : A \to B$ en afbildning, defineres for hver delmængde $A' \subseteq A$ en afbildning $f|A' : A' \to B$, kaldet *restriktionen* til A', ved

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

(1.9.8) Er $f : A \to B$ og $g : B \to C$ afbildninger, så er også den sammensatte relation en afbildning

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

Af og til udelades tegnet '$\circ$', således at den sammensatte afbildning blot skrives $gf : A \to C$.

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

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

og denne mængdes foreningsmængde (jfr. Sum-aksiomet) betegens

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

Er U denne foreningsmængde, defineres *produktmængden* af familien F ved

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

For hvert index j i indexmængden I er den j-te *projektion* defineret ved

$$pr_j := \{(y, x) \mid x \in \prod_{i\in I} F_i \ \wedge \ y = x(j)\}.$$

Projektionen er en afbildning

$$pr_j : \prod_{i\in I} F_i \to F_j.$$

(1.9.10) Endelig indses v.hj.a. Uendelighedsaxiomet, at der eksisterer en mængde $\mathbf{N}$, 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 $\mathbf{N}$ bruger sædvanlige notationer: For en afbildning $f : \mathbf{N} \to A$ skrives ofte $f = (f_1, f_2, ...)$, og for en familie af mængder $F : \mathbf{N} \to \mathcal{C}$ skrives ofte

$$\begin{aligned} \{F_1, F_2, \dots\} &:= \{F_i \mid i \in \mathbf{N}\}, \\ F_1 \cup F_2 \cup \dots &:= \bigcup_{i\in\mathbf{N}} F_i \quad \text{og} \\ F_1 \times F_2 \times \dots &:= \prod_{i\in\mathbf{N}} F_i. \end{aligned}$$

(1.10) Mængdelære kan datere sin fødsel til 1874, hvor Georg Cantor som den første betragtede samlinger af reelle tal, som ikke a priori var "angivet ved en opskrift". I sidste del af 1800-tallet udvikledes mængdelære ud fra det synspunkt, at den var en del af logikken, således at dens principper kunne 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 klargjort 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 $X \subseteq A$ finde 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

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

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

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

At forudsætte eksistensen af sådanne afbildninger betyder til ZF-axiomerne at tilføje:

Udvalgs–axiomet. *Til enhver mængde A eksisterer der en udvalgsfunktion på A.*

Det fremhæves, at Udvalgsaxiomet ikke er nødvendigt for at vi kan vælge elementer i ikke tomme mængder. Det er kun nødvendigt for at sikre, at der findes afbildninger, der "foretager sådanne valg for os".

(1.12) 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 Poul 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

hvadenten man til ZF-axiomerne tilføjer udvalgsaxiomet eller tilføjer dets negation (f.eks. i den konkrete form: Der findes ingen udvalgsfunktion på mængden $\mathbf{R}$ af reelle tal).

I det følgende vælger vi at acceptere udvalgsaxiomet.

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 Udvalgs-axiomet. 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 $G : B \to \mathcal{P}(A) \setminus \{\emptyset\}$. 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. Det er ikke nødvendigt at bruge Udvalgs–axiomet ♡

(2.2) Definition. To mængder A og B siges at have *samme mægtighed* eller at være *ækvipotente*, og vi skriver

$$A \simeq B,$$

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

Hvis der blot findes en injektiv afbildning : $A \to B$, siges A at have *højst samme mægtighed som* B, og vi skriver

$$A \preceq B \qquad (\text{eller } B \succeq A).$$

Mængden A siges at have (strengt) *mindre mægtighed* end mængden B, og vi skriver

$$A \prec B, \qquad (\text{eller } B \succ A),$$

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

$$A \prec B \quad \Longleftrightarrow \quad A \preceq B \wedge A \not\simeq B.$$

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:*

$$(1)\qquad \begin{cases} A \simeq A \\ A \simeq B \Rightarrow B \simeq A \\ A \simeq B \wedge B \simeq C \Rightarrow A \simeq C \end{cases}$$

$$(2)\qquad \begin{cases} A \preceq A \\ A \preceq B \wedge B \preceq C \Rightarrow A \preceq C \\ A \preceq B \wedge B \preceq A \Rightarrow A \simeq B \end{cases}$$

$$(3)\qquad \begin{cases} A \not\prec A \\ A \prec B \wedge B \prec C \Rightarrow A \prec C. \end{cases}$$

Bevis. Det sidste udsagn i (3) er en konsekvens af det sidste udsagn i (2) (og de øvrige udsagn er trivielle). At det sidste udsagn i (2) er opfyldt, er indholdet i:

Bernstein's Ækvivalenssætning. *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. Da f er injektiv, kan vi for hvert $b \in f(A)$ med $f^{-1}(b)$ betegne det entydigt bestemte element $a \in A$ for hvilket $f(a) = b$. Tilsvarende definerer vi $g^{-1}(a) \in B$ for $a \in g(B)$. Idéen i beviset er, at vi splitter mængden A i to delmængder A_0 og $A \setminus A_0$, og definerer afbildningen $h : A \to B$ som f på A_0 og som g^{-1} på $A \setminus A_0$. For at dette har mening, må $A \setminus A_0$ være en delmængde af $g(B)$, og ved et 'snedigt' valg af A_0 sikres, at h er en bijektiv afbildning.

Udfra hvert element $a \in A$ kan vi definere følgende "urbilled-algoritme":
Hvis $a \in g(B)$, så sættes $b := g^{-1}(a)$, ellers stoppes.
Hvis $b \in f(A)$, så sættes $a' := f^{-1}(b)$, ellers stoppes.
Hvis $a' \in g(B)$, så sættes $b' := g^{-1}(a')$, ellers stoppes.
Hvis $b' \in f(A)$, så sættes $a'' := f^{-1}(b')$, ellers stoppes.
$\vdots$
Lad nu $A_0 \subseteq A$ betegne delmængden bestående af de elementer $a \in A$, for hvilke algoritmen **stopper** med et element i mængden A. [Alternative muligheder er at algoritmen stopper med et element i B eller at den slet ikke stopper.] Når $a \in A \setminus A_0$ gælder specielt, at $a \in g(B)$, idet jo algoritmen udfra a ellers ville stoppe med $a \in A$ (uden overhovedet at komme igang). Vi kan derfor definere en afbildning $h : A \to B$ ved

$$h(x) = \begin{cases} f(x), & \text{hvis} \quad x \in A_0 \\ g^{-1}(x), & \text{hvis} \quad x \in A \setminus A_0\,. \end{cases}$$

Vi påstår, at $h : A \to B$ er bijektiv.
h **er injektiv:** Antag, at to elementer $a_1, a_2 \in A$ har samme værdi b ved afbildningen h, altså at $h(a_1) = h(a_2) = b$. Hvis begge elementer tilhører A_0, så er $f(a_1) = f(a_2)$, og vi får $a_1 = a_2$, da f er injektiv. Hvis begge elementer tilhører $A \setminus A_0$, så er

$g^{-1}(a_1) = g^{-1}(a_2)$, og vi får $a_1 = g(g^{-1}(a_1)) = g(g^{-1}(a_2)) = a_2$. Og de to elementer kan ikke tilhøre hver sin af mængderne A_0 og $A \setminus A_0$. Var nemlig f.eks. $a_1 \in A \setminus A_0$ og $a_2 \in A_0$, så var $g^{-1}(a_1) = b = f(a_2)$ og algoritmen udfra a_1 ville altså føre til b og dernæst til a_2. Idet $a_2 \in A_0$ vil algoritmen udfra a_2 stoppe med et element fra A, og den vil derfor også stoppe udfra a_1 med det samme element fra A. Men det er i modstrid med at $a_1 \notin A_0$.
h **er surjektiv:** Lad $b \in B$, og sæt $a := g(b) \in A$. Algoritmen udfra a fører altså først til b. Hvis $a \notin A_0$, så er $b = g^{-1}(a) = h(a)$. Og hvis $a \in A_0$, så kan algoritmen ikke stoppe med elementet b fra B, så der findes specielt et element $a' \in A$ med $f(a') = b$. Algoritmen udfra a fører altså til b og dernæst til a'. Da $a \in A_0$ stopper algoritmen udfra a med et element i A og udfra a' stopper den derfor med det samme element i A. Altså er også $a' \in A_0$, og derfor er $b = f(a') = h(a')$. I begge tilfælde er altså $b \in h(A)$♠

Bemærkning. I ovenstående bevis har vi defineret en delmængde A_0 af A ved at se på en algoritme. Det er ikke helt i overensstemmelse med ZF–axiomerne, der ikke umiddelbart tillader at specificere delmængder ved prædikater, der indeholder tre prikker (...). Det er værd at bemærke, at sætningen kan bevises stringent udfra axiomerne, endda uden brug af Uendeligheds–axiomet.

Stringent Bevis. Analyserer vi beviset ovenfor, ser vi, at vi om A_0 kun har brugt, at det er en af de delmængder Q af A, som opfylder følgende betingelser:

(1) $A \setminus Q \subseteq g(B)$ [Brugt ved definitionen af h]
(2) $gf(Q) \subseteq Q$ [Brugt ved injektiviteten af h]
(3) $g^{-1}(Q) \subseteq f(Q)$ [Brugt ved surjektiviteten af h]

Det er derfor nok at indse, at der **findes** delmængder Q af A, som opfylder disse betingelser. Det er klart, at der findes delmængder Q, som opfylder (1) og (2), f.eks. $Q = A$. Betingelsen (1) er øjensynlig ækvivalent med

$$A \setminus g(B) \subseteq Q.$$

Definerer vi delmængden A_0 som fællesmængden af alle de delmængder, som opfylder (1) og (2), så er altså

$$A_0 := \bigcap \{Q \in \mathcal{P}(A) \mid A \setminus g(B) \subseteq Q \ \wedge \ gf(Q) \subseteq Q\},$$

og det følger, at også A_0 har egenskaberne (1) og (2). Det er nu let at se, at også delmængden $(A \setminus g(B)) \cup gf(A_0)$ har egenskaberne (1) og (2), og definitionen på A_0 sikrer derfor, at $A_0 \subseteq (A \setminus g(B)) \cup gf(A_0)$. Heraf sluttes let, at A_0 også har egenskaben (3) ♡

Bemærkning. Vi beviser senere, at vilkårlige to mængder A og B altid kan sammenlignes, altså at der gælder: $A \prec B$ eller $A \simeq B$ eller $B \prec A$.

(2.4) Cantor's Sætning.

(i) *For enhver mængde A er*

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

(ii) *Lad* $\mathbf{2}$ *betegne mængden* $\{0,1\}$. *For enhver mængde* A *er da*

$$\mathcal{P}(A) \simeq \mathbf{2}^A.$$

Bevis. **(i):** Afbildningen $x \mapsto \{x\}, \quad x \in A$, er øjensynlig en injektiv afbildning $: A \to \mathcal{P}(A)$, så vi har $A \preceq \mathcal{P}(A)$, og skal altså vise, at der ikke findes bijektive afbildninger $: A \to \mathcal{P}(A)$. Vi viser, at ingen afbildning $: A \to \mathcal{P}(A)$ kan være surjektiv. 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

$$a \in Y \quad \Longleftrightarrow \quad a \notin \psi(a) \quad \Longleftrightarrow \quad a \notin Y.$$

(ii): Mængden $\mathbf{2}^A$ 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

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

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

(2.5) Definition. Vi vil kalde en mængde A for *tællelig*, hvis A er tom eller der findes en surjektiv afbildning $\phi : \mathbf{N} \to A$.

En afbildning $\phi : \mathbf{N} \to A$ er en følge $\phi = (\phi_1, \phi_2, ...)$ med værdier i A. En ikke-tom mængde A er altså tællelig, hvis der findes en sådan følge, hvori ethvert 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 $A \preceq \mathbf{N}$ (og hertil er det faktisk ikke nødvendigt at indrage Udvalgs-axiomet). Det følger derfor af Cantor's sætning, at mængden $\mathcal{P}(\mathbf{N})$ **ikke** er tællelig.

En mængde A kaldes *numerabel*, hvis den er ækvipotent med $\mathbf{N}$, og *endelig*, hvis den er tom eller ækvipotent med et afsnit

$$\mathbf{N}_{\leq n} := \{1, ..., n\}$$

af $\mathbf{N}$. Er det sidste tilfældet, er n elementantallet i A og vi skriver ofte $|A| := n$.

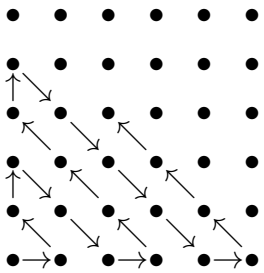
Vedrørende egenskaber ved endelige mængder henvises til kapitlet om Naturlige tal. Med blandt disse egenskaber regnes også følgende:

(1) *En mængde A er tællelig, hvis og kun hvis den er endelig eller numerabel.*
(2) *En mængde A er uendelig (dvs. ikke endelig), hvis og kun hvis $\mathbf{N} \preceq A$.*
(3) *En mængde A er uendelig, hvis og kun hvis A er ækvipotent med en af sine ægte delmængder.*

(2.6) Sætning. *Produktmængden $\mathbf{N} \times \mathbf{N}$ er numerabel. Anderledes udtrykt:*

$$\mathbf{N} \times \mathbf{N} \simeq \mathbf{N}.$$

Bevis. Nummerering af elementerne i $\mathbf{N} \times \mathbf{N}$ efter følgende skema:



giver en bijektiv afbildning : $\mathbf{N} \to \mathbf{N} \times \mathbf{N}$♡

Korollar 1. *En tællelig forening af tællelig 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 $\phi : \mathbf{N} \to I$ og for hvert $n \in \mathbf{N}$ en surjektiv afbildning $\psi_n : \mathbf{N} \to A_{\phi(n)}$, da defineres ved

$$\Psi(n, m) := \psi_n(m)$$

en surjektiv afbildning $\Psi : \mathbf{N} \times \mathbf{N} \to A$. 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: $\mathbf{N} \to A$, der er konstante fra et vist trin.
Da gælder:

(1) *$\mathcal{F}(A) \preceq \mathcal{E}(A)$.*
(2) *Hvis A har mindst 2 elementer, så er $\mathcal{F}(A) \simeq \mathcal{E}(A)$.*
(3) *Hvis A er $\neq \emptyset$ og tællelig, så er $\mathcal{E}(A)$ numerabel.*

Bevis. Et n-sæt i A er en afbildning : $\{1, ..., n\} \to A$, hvor $n \in \mathbf{N}$, 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 $(y_1, y_2, \dots)$ i $\mathcal{F}(A)$ findes $n \in \mathbf{N}$, så at $y_{n-1} \neq y_n = y_{n+1} = y_{n+2} = \dots$, og $(y_1, y_2, \dots) \mapsto (y_1, \dots, y_n)$ er en injektiv afbildning : $\mathcal{F}(A) \to \mathcal{E}(A)$.
(2): Vælg 2 forskellige elementer $a, b \in A$. Ved

$$(x_1, \dots, x_n) \mapsto \begin{cases} (x_1, \dots, x_n, a, a, a, \dots), & \text{hvis} \quad x_n \neq a \\ (x_1, \dots, x_n, b, b, b, \dots), & \text{hvis} \quad x_n = a \end{cases}$$

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 $\mathcal{E}(A)$ er øjensynlig uendelig♡

(2.7) Eksempler.

(1) *Mængderne* $\mathbf{Z}$ *og* $\mathbf{Q}$ *er numerable.*
(2) *Mængden* $\mathbf{R}$ *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 afbildning : $\mathbf{N} \to \mathbf{Z}$. Og afbildningen $(a, s) \mapsto a/s$ er som bekendt en surjektiv afbildning : $\mathbf{Z} \times \mathbf{N} \to \mathbf{Q}$.
(2): Dette skyldes Cantor (1873). Det er nok at vise, at enhedsintervallet $[0, 1[\subseteq \mathbf{R}$ ikke er tælleligt, altså at en afbildning $f : \mathbf{N} \to [0, 1[$ ikke kan være surjektiv. Elementerne $\xi \in [0, 1[$ kan udvikles i decimalbrøker

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

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

$$\alpha = 0, \alpha_1 \alpha_2 \alpha_3 \dots ,$$

hvor α_n er bestemt ved at $\alpha_n = 0$ hvis det n-te ciffer i $f(n)$ er $\neq 0$, og $\alpha_n = 1$, hvis det n-te ciffer i $f(n)$ er $= 0$. For hvert $n \in \mathbf{N}$ vil da α's decimaler på den n-te plads afvige fra $f(n)$'s, og følgelig er $\alpha \notin \{f(1), f(2), \dots\}$.
(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 $q_i \in \mathbf{Q}$, $i = 0, \dots, n$ og $q_n \neq 0$, hvori ξ er rod (dvs. $p(\xi) = 0$). Mængden af sådanne polynomier betegnes $\mathbf{Q}[X]$. Vi kan opfatte polynomier $q_0 + q_1 X + \cdots + q_n X^n \in \mathbf{Q}[X]$ som følger $(q_0, q_1, \dots, q_n, 0, 0, \dots)$ af

rationale tal, der er $= 0$ fra et vist trin. Af Korollar 2 (2.6) følger, at mængden $\mathbf{Q}[X]$ er numerabel, og da hvert polynomium $p \neq 0$ i $\mathbf{Q}[X]$ kun kan have endelig mange rødder i $\mathbf{R}$, følger påstanden af Korollar 1 (2.6).
(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 $\mathbf{R}$, 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 hypotensen ikke kunne modbevises, og Cohen har vist i 1963, at hypotesen heller ikke kan bevises, og at ZF-axiomerne + udvalgs-axiomet + kontinumshypotesen udgør et konsistent system (stadig under forudsætning af ZF-systemets konsistens).

(2.9) Eksempler. *Følgende mængder:*

$$(1)\quad \mathcal{P}(\mathbf{N}) \qquad (2)\quad \mathbf{2}^{\mathbf{N}} \qquad (3)\quad \mathbf{N}^{\mathbf{N}} \qquad (4)\quad \mathbf{R}^n, \quad \textit{for } n \in \mathbf{N}$$

har alle kontinuets mægtighed. Vi har altså

$$\mathcal{P}(\mathbf{N}) \simeq \mathbf{2}^{\mathbf{N}} \simeq \mathbf{N}^{\mathbf{N}} \simeq \mathbf{R}^n \simeq \mathbf{R} \quad (n \in \mathbf{N}).$$

Vink. **(1):** $\mathcal{P}(\mathbf{N}) \simeq \mathbf{2}^{\mathbf{N}}$ ifølge Cantor's sætning (2.4) (ii).
(2): At $\mathbf{2}^{\mathbf{N}} \simeq \mathbf{R}$ indses ved at udvikle reelle tal i dual-brøker.
(3): $\mathbf{N}^{\mathbf{N}} \simeq \mathbf{R}$, thi da $\mathbf{N}^{\mathbf{N}} \subseteq \mathcal{P}(\mathbf{N} \times \mathbf{N})$, og $\mathbf{N} \times \mathbf{N} \simeq \mathbf{N}$, har vi $\mathbf{N}^{\mathbf{N}} \preceq \mathcal{P}(\mathbf{N}) \simeq \mathbf{2}^{\mathbf{N}} \preceq \mathbf{N}^{\mathbf{N}}$, hvoraf $\mathbf{N}^{\mathbf{N}} \simeq \mathbf{2}^{\mathbf{N}} \simeq \mathbf{R}$.
(4): For $n = 2$ har vi $\mathbf{R}^2 \simeq \mathbf{R} \times \mathbf{R} \simeq \mathbf{N}^{\mathbf{N}} \times \mathbf{N}^{\mathbf{N}} \simeq (\mathbf{N} \times \mathbf{N})^{\mathbf{N}} \simeq \mathbf{N}^{\mathbf{N}} \simeq \mathbf{R}$. Det almindelige tilfælde følger heraf ved induktion.

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

$$A \times A \simeq A \qquad (\text{hvoraf specielt:} \quad A \times \mathbf{N} \simeq A).$$

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 $\neq \emptyset$.

(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 Udvalgs–axiomet (og vi beviser senere, at Zorn's lemma er ækvivalent med Udvalgs–aksiomet).

(3.3) Definition. Lad $(X, <)$ være en partielt ordnet mængde. I det følgende betegner vi for hver delmængde $A \subseteq X$ med $\mathcal{M}_A$ mængden af *ægte majoranter* for A, altså

$$\mathcal{M}_A = \{x \in X \mid \forall a \in A : a < x\} \ .$$

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 $\mathcal{M}_A \cap K \neq \emptyset$, så er

$$\begin{aligned} &u(\mathcal{M}_A) \in K \qquad \text{og} \\ &u(\mathcal{M}_A) \leq k \quad \text{for alle} \quad k \in \mathcal{M}_A \cap K \ . \end{aligned}$$

Sætning 1. *Lad $K \subseteq X$ være en u-kæde, og antag, at $\mathcal{M}_K \neq \emptyset$. Da er også $K \cup \{u(\mathcal{M}_K)\}$ en u-kæde i X.*

Bevis. Sættes $\tilde{k} := u(\mathcal{M}_K)$ og $\tilde{K} := K \cup \{\tilde{k}\}$, skal vi vise, at $\tilde{K}$ er en u-kæde, dvs. at $\tilde{K}$ opfylder betingelserne (u1) og (u2).
(u1): Det tilføjede element $\tilde{k}$ er valgt blandt de ægte majoranter for K, og det er derfor $>$ end alle elementer i K. Da K er totalt ordnet, følger det, at også $\tilde{K}$ er totalt ordnet, og at $\tilde{k}$ er sidste element i $\tilde{K}$.
(u2): Lad $A \subseteq \tilde{K}$ være en delmængde, så at $\mathcal{M}_A \cap \tilde{K} \neq \emptyset$. Vi kan da finde et element k_0 i $\mathcal{M}_A \cap \tilde{K}$. Da $k_0 \in \tilde{K}$ og $\tilde{k}$ var sidste element i $\tilde{K}$ ifølge det allerede viste, får

vi uligheden $k_0 \leq \tilde{k}$, og da $k_0 \in \mathcal{M}_A$, medfører denne ulighed, at også $\tilde{k} \in \mathcal{M}_A$. Specielt er altså $\tilde{k} \notin A$, og heraf følger, at vi har $A \subseteq K$. Der er nu to tilfælde:

1°: $\mathcal{M}_A \cap K \neq \emptyset$. I dette tilfælde følger påstanden let af, at betingelsen (u2) gælder for K.

2°: $\mathcal{M}_A \cap K = \emptyset$. I dette tilfælde er $\mathcal{M}_A = \mathcal{M}_K$, thi "$\supseteq$" følger af, at $A \subseteq K$, og "$\subseteq$" betyder, at der for hvert $x \in \mathcal{M}_A$ og hvert $k \in K$ gælder: $k < x$, og dette indses således: Da $k \in K$, har vi $k \notin \mathcal{M}_A$, og heraf følger, da K er totalt ordnet, at der findes et $a \in A$, så at $k \leq a$. For dette a har vi $a < x$, da $x \in \mathcal{M}_A$. Og så har vi $k \leq a < x$, som påstået.
Nu er øjensynlig

$$u(\mathcal{M}_A) = u(\mathcal{M}_K) = \tilde{k} \in \tilde{K},$$

og videre gælder der, at

$$u(\mathcal{M}_A) \leq k \text{ for alle } k \in \mathcal{M}_A \cap \tilde{K},$$

idet fællesmængden $\mathcal{M}_A \cap \tilde{K} = \mathcal{M}_K \cap \tilde{K}$ kun indeholder det ene element $u(\mathcal{M}_K) = u(\mathcal{M}_A)$ ♠

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 $k \in K \setminus L$ og $l \in L$. Betragt nu delmængden

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

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

Idet beviset føres indirekte, antages, at $\mathcal{M}_A \cap L \neq \emptyset$. Specielt er altså $\mathcal{M}_A \neq \emptyset$, og vi kan betragte elementet

$$m := u(\mathcal{M}_A) .$$

Da L er en u-kæde, og $\mathcal{M}_A \cap L \neq \emptyset$, ser vi, at

$$m \in L .$$

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

$$m \in K ,$$

og at $m \leq k$. 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 $m = u(\mathcal{M}_A) \in \mathcal{M}_A$ ♠

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 $l \leq k$.

(u2): Lad $A \subseteq K$ være en delmængde så at $\mathcal{M}_A \cap K \neq \emptyset$ og sæt $k_0 := u(\mathcal{M}_A)$. Vi skal vise, at

$$\begin{array}{ll} (1) & k_0 \in K \\ \text{og} & \\ (2) & k_0 \leq k \quad \text{for alle} \quad k \in \mathcal{M}_A \cap K \ . \end{array}$$

Lad k være et element i $\mathcal{M}_A \cap K$, [sådanne findes, da $\mathcal{M}_A \cap K \neq \emptyset$], 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 $k \in \mathcal{M}_A$. Da K_j er en u-kæde, og $k \in \mathcal{M}_A \cap K_j$, slutter vi, at $k_0 = u(\mathcal{M}_A) \in K_j \subseteq K$, hvoraf (1), og at $k_0 \leq k$, hvoraf (2), da k var et vilkårligt element i $\mathcal{M}_A \cap K$♠

(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 $\mathcal{M}_K = \emptyset$. 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* af X forstås en delmængde $A \subseteq X$, som opfylder, at der for alle $a, x \in X$ gælder:

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

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

For hvert element $b \in X$ er øjensynlig delmængden:

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

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

(4.2) Definition. En partielt ordnet mængde $(X, <)$ kaldes *velordnet* (og relationen $<$ i X kaldes en *velordning*), hvis enhver ikke-tom delmængde 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, at $s_0 \leq s$.

(4.3) Lemma. *Lad $(X, <)$ være en velordnet mængde. Da gælder:*

(1) *Ordningen $<$ er total.*
(2) *Hvis a er element i et ægte afsnit A af X og b er et element i komplementærmængden $X \setminus A$, så er $a < b$.*
(3) *Hvis A er et ægte afsnit og c er det første element i komplementærmængden $X \setminus A$, så er $A = X_{<c}$. Specielt er hvert ægte afsnit elementbestemt.*

Bevis. **(1)**: At X er totalt ordnet indses ved at bemærke, at for givne $x, y \in X$ vil det første element i mængden $\{x, y\}$, som jo er det ene af x og y, gå forud for det andet element i denne mængde.
(2): Da X er totalt ordnet ifølge (1), ville der i modsat fald gælde, at $b \leq a$, og så er $b \notin A$ i modstrid med, at A er et afsnit.
(3): At '$\subseteq$' gælder betyder, at for alle $a \in A$ er $a < c$, og det gælder ifølge (2). Og omvendt, hvis $a \notin A$, så sikrer valget af c, at $c \leq a$, og så er $a \notin X_{<c}$ ♠

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) I en velordnet mængde X har hvert element a, som ikke er sidste element i X, en *umiddelbar efterfølger*, dvs. et element $a^+ \in X$, som opfylder:

$$a < a^+ \qquad \text{og} \qquad a < x \implies a^+ \leq x \quad \text{for alle } x \in X.$$

(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 $\mathbf{N}$ af naturlige tal med sædvanlig ordning:

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

Men vi kan let konstruere større velordnede mængder: F.eks. kan vi udvide $\mathbf{N}$ med et element ω og vi kan udvide ordningen i $\mathbf{N}$ til en ordning i $\mathbf{N} \cup \{\omega\}$ ved fastsættelsen: $n < \omega$, når $n \in \mathbf{N}$. 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 numerabelt mange gange, og til resultatet kan vi yderliger tilføje $\ldots$. 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 jo sætte $x_1 :=$ første element i X, vi kan sætte $x_2 :=$ første element i $X \backslash \{x_1\}$, sætte $x_3 :=$ første element i $X \backslash \{x_1, x_2\}, \ldots$, sætte $\omega :=$ første element i $X \backslash \{x_1, x_2, x_3, \ldots\}$, sætte $\omega_1 :=$ første element i $X \backslash \{x_1, x_2, x_3, \ldots, \omega\}$ osv.

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

Velordningssætningen. *Enhver mængde X kan velordnes.*

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

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

hvis $(K', <')$ er et ægte afsnit af $(K, <)$, dvs. hvis K' er et ægte afsnit af 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 mht. ordningen $\subset$. Er nemlig $(K,<)$ et maksimalt par, så må vi have $K = X$ (og så er $(X,<)$ velordnet), thi ellers fandtes et element $\omega \in X\backslash K$, og så kunne vi udvide K til $\tilde{K} := K \cup \{\omega\}$ og vi kunne udvide ordningen $<$ i K 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 parret $(K,<)$ var maksimalt.

For at eftervise eksistensen af et maksimalt par er det ifølge Zorn's lemma nok at vise, at parrene er induktivt ordnede ved $\subset$. Lad derfor $(K_j,<_j)$, hvor $j \in J$, være en mængde af sådanne par, der er totalt ordnet ved $\subset$, lad $K := \bigcup K_j$ være foreningsmængden og betragt heri relationen $<$ defineret ved:

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

Herom er det nok at vise:

(1) Relationen $<$ er en ordensrelation i K,
(2) Parret $(K,<)$ er velordnet,
(3) For hvert j er K_j et afsnit af K,
(4) For $x,y \in K_j$ gælder: $x <_j y \implies x < y$,

thi så er parret $(K,<)$ majorant for mængden af par $(K_j,<_j)$.

(1): Relationen er øjensynlig irreflexiv, så vi skal vise, at den er transitiv. Antag, at x,y,z er elementer i K, så at $x < y$ og $y < z$. Vælg j, så at $x,y \in K_j$ og $x <_j y$, og vælg i, så at $y,z \in K_i$ og $y <_i z$. Lad $(K_l,<_l)$ være det største (mht. $\subset$) af de to par $(K_j,<_j)$ og $(K_i,<_i)$. Da har vi $x,y,z \in K_l$, og af $x <_j y$ og $y <_i z$ følger, at $x <_l y$ og $y <_l z$. Da $<_l$ er transitiv, slutter vi, at $x <_l z$, og af definitionen følger nu, at $x < z$.

(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 første (mht. $<_j$) element i $K_j \cap S$. Vi skal vise for hvert $s \in S$, at

$$(*) \qquad s_0 \leq s.$$

Hvis $s \in K_j$, så har vi $s \in K_j \cap S$ og valget af s_0 sikrer derfor, at $s_0 \leq_j s$, og så følger $(*)$ af definitionen på $<$. Hvis $s \notin K_j$, så vælger vi i, så at $s \in K_i$. Da $s \in K_i\backslash K_j$, er $K_i \not\subseteq K_j$, og da parrene var totalt ordnede, må $(K_j,<_j)$ følgelig være et afsnit af $(K_i,<_i)$. Da $s \in K_i\backslash K_j$, gælder ifølge Lemma (4.3)(2) for hvert x i K_j, at $x <_i s$. Specielt er $s_0 <_i s$, og så følger $(*)$ af definitionen på $<$.

(3): Lad $a \in K_j$, lad $x \in K$ og antag, at $x < a$. 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 $K_i \subseteq K_j$, så er påstanden klar, og i modsat fald er K_j et afsnit i K_i og af $x <_i a$ og $a \in K_j$ følger påstanden ligeledes.

(4): Er trivielt ud fra definitionen af $<$.

Hermed er Velordningssætningen bevist ♠

(4.6) Sætning om Transfinit Induktion. *Lad $(X,<)$ være en velordnet mængde og lad $S \subseteq X$ være en delmængde. Hvis der for alle elementer x i X gælder:*

$$(*) \qquad X_{<x} \subseteq S \implies x \in S,$$

så er $S = X$.

Bevisidé. 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 den umiddelbare efterfølger 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 den umiddelbare efterfølger til x_2, så er $X_{<x_3} = \{x_1, x_2\}$. Da vi har vist, at $\{x_1, x_2\} \subseteq S$, sikrer $(*)$, at $x_3 \in S$. Og således fortsættes: Er ω det mindste elment, der er $>$ ethvert x_n, så 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 for Induktions-sætningen. Var $S \subset X$, så kunne vi betragte det første element a i komplementærmængden $X \setminus S$. Her er øjensynlig $X_{<a} \subseteq S$, og så er $(*)$ i modstrid med at $a \notin S$ ♠

(4.7) Sætning om Transfinit Rekursions. *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*

$$(\dagger) \qquad f(x) = \Phi(f|X_{<x}) \quad \textit{for alle } x \in X.$$

Definition. Den entydigt bestemte afbildning f siges at være *rekursivt bestemt* ved $(\dagger)$.

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-triviel og vigtig konsekvens af Rekursions-sætningen, at der eksisterer en mængde (nemlig billedmængden for afbildningen f), hvori ethvert $\Phi(f|X_{<x})$ er element.

Eksempel. I den velordnende mængde $(\mathbf{N},<)$ er de ægte afsnit af formen $\mathbf{N}_1 = \emptyset$ eller $\mathbf{N}_{<n^+} = \{1, 2, \dots, n\}$, og en afbildning g, hvis domæne er et sådant afsnit, er det 'tomme' sæt $g = \emptyset$ eller et n-sæt $g = (g_1, \dots, g_n)$. En forskrift Φ knytter altså her til hvert n-sæt et element:

$$\Phi(g_1 \dots, g_n), \quad \text{samt til } g = \emptyset \text{ et element } \Phi(\emptyset).$$

Rekursions-sætningen udsiger altså, at der findes netop én afbildning $f = (f_1, f_2, \dots)$ med domæne $\mathbf{N}$, således at

$$(\dagger) \qquad f_1 = \Phi(\emptyset) \quad \text{og } f_{n+1} = \Phi(f_1, \dots, f_n) \text{ for alle } n \in \mathbf{N}.$$

Hvis forskriften Φ er bestemt ud fra en udvalgt mængde A og en forskrift φ, der til hver mængde Y knytter en mængde $\varphi(Y)$, på følgende måde:

$$\Phi(\emptyset) = A \quad \text{og} \quad \Phi(g_1, \dots, g_n) = \varphi(g_n),$$

så giver Rekursions-sætningen en entydig afbildning $f = (f_1, f_2, \dots)$ bestemt ved

$$(\dagger) \qquad f_1 = A \quad \text{og } f_{n+1} = \varphi(f_n) \text{ for alle } n \in \mathbf{N}.$$

Er f.eks. φ bestemt ved $\varphi(Y) := \mathcal{P}(Y)$, får vi den rekursive definition af mængderne $\mathcal{P}^n(A)$ for alle $n \in \mathbf{N}$, og samtidig eksistensen af mængden $\{A, \mathcal{P}(A), \mathcal{P}^2(A), \dots\}$, og dermed også eksistensen af foreningsmængden:

$$A \cup \mathcal{P}(A) \cup \mathcal{P}^2(A) \cup \cdots .$$

Bevis for Rekursions-sætningen. **Entydighed**: Lad f_1 og f_2 være afbildninger, som opfylder det stillede krav. Vi bruger transfinit induktion (4.6) på mængden

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

Antag altså, at $x \in X$ og at $X_{<x} \subseteq S$. Vi skal vise, at $x \in S$. Vi har, at $f_1(y) = f_2(y)$ for alle $y \in X_{<x}$, og følgelig er

$$f_1|X_{<x} = f_2|X_{<x}.$$

Og så er $f_1(x) = \Phi(f_1|X_{<x}) = \Phi(f_2|X_{<x}) = f_2(x)$. Altså er $x \in S$.
Eksistens: Lad os et øjeblik kalde en afbildning g for Φ-rekursiv, hvis dens domæne er et afsnit af X og der gælder:

$$g(x) = \Phi(g|X_{<x}) \quad \text{for alle } x \in \operatorname{dom} g.$$

Vi skal altså vise, 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 af X højst findes én Φ-rekursiv afbildning med domæne A. Heraf følger, at hvis der for et givet $x \in X$ findes Φ-rekursive afbildninger g og h, så at $x \in \operatorname{dom} g$ og $x \in \operatorname{dom} h$, så er $g(x) = h(x)$, thi restriktionerne $g|X_{\leq x}$ og $h|X_{\leq x}$ er øjensynlig Φ-rekursive afbildninger med domæne $X_{\leq x}$, så vi har, at $g|X_{\leq x} = h|X_{\leq x}$ og derfor specielt, at $g(x) = h(x)$.

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 følgende prædikat:

Der eksisterer en Φ-rekursiv afbildning g, så at $x \in \operatorname{dom} g$ og $y = g(x)$.

For hvert element $x \in B$ er der netop ét 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 Udskiftnings–axiomet (1.6), da vi jo lige har set, at for ethvert element $x \in B$ er prædikatet mængdebestemmende (det bestemmer en mængde med ét element).

Mængden B er en foreningsmængde af afsnit af X. Heraf følger klart, at B selv er et afsnit af X. Afbildningen f har domæne B, og hvis $x \in B$, så findes en Φ-rekursiv afbildning g med $x \in \operatorname{dom} g$, og så er $f(z) = g(z)$ for alle $z \in \operatorname{dom} g$ ifølge definitionen af f. Specielt er

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

og afbildningen f er derfor Φ-rekursiv.

For afsnittet B af X må der gælde, at $B = X$, thi i modsat fald havde B ifølge Lemma (4.3)(3) formen $B = X_{<c}$ med $c \in X$, og så kunne vi udvide afbildningen f ved definitionen:

$$\bar{f}(c) := \Phi(f)$$

til en Φ-rekursiv afbildning $\bar{f}$ med domæne $X_{\leq c} = X_{<c} \cup \{c\} \supset B$, i modstrid med at ethvert domæne for en Φ-rekursiv afbildning er delmængde af B. Afbildningen f er således en Φ-rekursiv afbildning med domæne X, som ønsket ♠

(4.8) Sætning. *Lad $(X, <)$ og $(Y, <)$ være velordnede mængder. Der findes da højst én afbildning $f : X \to Y$, som afbilder $(X, <)$ ordens-isomorft på et afsnit af Y. Hvis ingen sådan afbildning findes, da findes der en afbildning $g : Y \to X$, som afbilder $(Y, <)$ ordens-isomorft på et ægte afsnit af X.*

Bevis. At $f : X \to Y$ afbilder $(X, <)$ ordens-isomorft på et afsnit af Y er klart ensbetydende med, at der gælder:

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

Men (†) er jo en rekursiv bestemmelse af afbildningen f. Mere præcist: Lad os med $\diamondsuit$ 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

$$\Phi(g) := \begin{cases} y, & \text{hvis } g \text{ afbilder } \operatorname{dom} g \text{ ordens-isomorft} \\ & \text{på afsnittet } Y_{<y} \text{ af } Y. \\ \diamondsuit & \text{ellers.} \end{cases}$$

Hvis $f : X \to Y$ afbilder X ordens-isomorft på et afsnit af Y, så følger det af (†), 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 $\Phi(g) = \diamondsuit$, er f en afbildning $f : X \to Y \cup \{\diamondsuit\}$. Hvis der for et element $x \in X$ gælder, at $f(x) \in Y$, så ser vi af forskriften, at

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

Vi betragter nu to muligheder:
Tilfælde 1: For alle $x \in X$ gælder, at $f(x) \in Y$. Af det foregående følger, at afbildningen f så afbilder X ordens-isomorft på et afsnit af Y.
Tilfælde 2: Der eksisterer elementer $x \in X$ med $f(x) = \diamondsuit$. Lad $a \in X$ være det første sådannne element. Af det foregående følger så, at afbildningen $f_0 := f|X_{<a}$ så afbilder $X_{<a}$ ordens-isomorft på et afsnit af Y. Men dette afsnit må være hele Y, thi ellers havde det formen $Y_{<b}$, hvor $b \in Y$, 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 $f(a) = \diamondsuit \notin Y$. Det er nu klart, at den inverse f_0^{-1} er en ordens-isomorfi af Y på afsnittet $X_{<a}$ af X ♠

Af Sætningen få en række korollarer:
Sammenlignings-sætning for velordnede mængder. *Lad $(X, <)$ og $(Y, <)$ være velordnede mængder. Da indtræffer netop én af følgende muligheder:*

1° $(X, <)$ *er ordens-isomorf med et ægte afsnit af* $(Y, <)$.
2° $(X, <)$ *er ordens-isomorf med* $(Y, <)$.
3° $(Y, <)$ *er ordens-isomorf med et ægte afsnit af* $(X, <)$.

Bevis. Af Sætningen følger, at der altid indtræffer en af de tre muligheder. Af entydigheden i Sætningen følger let, at der højst kan indtræffe én af de tre muligheder ♡

Sammenlignings-sætning for mængder. *Lad X og Y være mængder. Da indtræffer netop én af følgende muligheder:*

1° $X \prec Y$.
2° $X \simeq Y$.
3° $Y \prec X$.

Bevis. De to mængder X og Y kan velordnes ifølge Velordnings-sætningen (4.5). Af Sammenlignings-sætningen for velordnede mængder følger derfor specielt, at der gælder: $X \preceq Y$ eller $Y \preceq X$. Og heraf følger påstanden, jfr. Sætning (2.3) ♡

(4.9) Eksempel. Der findes en ikke-tællelig, velordnet mængde, jfr. Eksempel (2.7)(2) eller Cantor's sætning (2.4)(1). Ifølge Velordnings-sætningen (4.5) findes derfor en ikke-tællelig, velordnet mængde $(\Omega, <)$. Tilføjes om fornødent et sidste element til Ω, kan vi antage, at der findes elementer $\omega \in \Omega$, således at afsnittet $\Omega_{<\omega}$ er ikke-tælleligt. Lad ω_1 være det første af sådanne elementer i Ω og betrag afsnittet $\Omega_1 := \Omega_{<\omega_1}$. Det er klart, at Ω_1 er et eksempel på en ikke-tællelig, velordnet mængde, hvori ethvert ægte afsnit er tælleligt. Af sammenlignings-sætningen for velordnede mængder 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 $(x_1, x_2, \dots)$ af elementer i Ω_1 er opad begrænset. Foreningsmængden $U := \bigcup_{n \in \mathbf{N}} (\Omega_1)_{\leq x_n}$ er nemlig

klart et afsnit i Ω_1 og også en tællelig forening af tællelige mængder, og dermed selv tællelig ifølge Korollar (2.6)(1). Følgelig er $U \subset \Omega_1$ et ægte afsnit og dermed af formen $U = (\Omega_1)_{<b}$ med et element $b \in \Omega_1$. Specielt er altså $x_n < b$ for alle $n \in \mathbf{N}$.

(4.10) Sætning. *Enhver uendelig mængde X er ækvipotent med en mængde af formen $Y \times \mathbf{N}$.*

Bevis. Da X er uendelig, har X en numerabel delmængde. Idet vi først velordner komplemæntærmængden til denne numerable delmængde og dernæst tilføjer den numerable delmængde, fås en velordning $<$ i X, så at intet element i X er sidste element. Hvert element x i X har derfor et umiddelbart følgende x^+, jfr. Observation (4.2), og $x \mapsto x^+$ definerer en afbildning $\varepsilon : X \to X$. Lad Y betegne komplementærmængden:

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

Vi påstår, at $f(y,n) := \varepsilon^{n-1}(y)$ (hvor $\varepsilon^0(y) := y$) definerer en bijektiv afbildning $f : Y \times \mathbf{N} \to X$. Afbildningen er **injektiv**, thi er $f(y,n) = f(y',n')$, kan vi antage, at $n' = n + p$, hvor $p \geq 0$, og så er

$$\varepsilon^{n-1}(\varepsilon^p(y')) = \varepsilon^{n'-1}(y') = f(y',n') = f(y,n) = \varepsilon^{n-1}(y).$$

Da ε, og dermed også potensen ε^{n-1}, øjensynlig er en injektiv afbildning, må vi have $\varepsilon^p(y') = y$, og da $y \notin \varepsilon(X)$, følger det, at $p = 0$, og altså, at $y' = y$ og $n' = n$.
Og afbildningen er **surjektiv**, thi ellers kunne vi betragte den første element x, der ikke tilhører billedmængden for f. Vi har $x \notin Y$ (thi ellers var $x = f(x,1)$), og følgelig er $x = \varepsilon(z) = z^+$, hvor $z \in X$. Det er klart, $z < z^+ = x$, så valget af x sikrer, at z tilhører billedmængden for f. Vi har altså $z = f(y,n)$, hvor $y \in Y$ og $n \in \mathbf{N}$, og så er $x = \varepsilon(f(y,n)) = f(y,n+1)$ i modstrid med, at x ikke tilhørte billedmængden for f ♠

Korollar. *For enhver uendelig mængde X gælder, at $X \times \mathbf{N}$ er ækvipotent med X.*

Bevis. Vælg en mængde Y, så at $X \simeq Y \times \mathbf{N}$. Da gælder ifølge Sætning (2.6), at

$$X \times \mathbf{N} \simeq Y \times \mathbf{N} \times \mathbf{N} \simeq Y \times \mathbf{N} \simeq X \text{ ♠}$$

5. Ækvivalens af eksistens-axiomerne.

(5.1) Vi har i det foregående mødt en række eksistensudsagn:
Udvalgs–axiomet ($\mathcal{U}$). *For enhver mængde A eksisterer der en udvalgsfunktion på A.*

Zorn's lemma ($\mathcal{Z}$). *I enhver partielt ordnet mængde $(X, <)$, der er induktivt ordnet, eksisterer der et maksimalt element.*

Velordnings-sætningen ($\mathcal{V}$). *For enhver mængde M eksisterer der en relation $<$ i M, så at $(M, <)$ er velordnet.*

Til denne gruppe eksistensudsagn medregnes ofte følgende:
Maksimalitetsprincippet ($\mathcal{M}$). *I enhver partielt ordnet mængde $(Y, <)$ eksisterer der en totalt ordnet delmængde K, så at intet element i komplementærmængden $Y \setminus K$ er sammenligneligt med alle elementer i K.*

Sammenlignings-sætningen ($\mathcal{S}$). *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 5 ovennævnte eksistensudsagn ækvivalente, dvs. ethvert af dem medfører de 4 andre.*

Bevis-oversigt. At $(\mathcal{U}) \Rightarrow (\mathcal{Z})$ så vi i Sætning (3.4). At $(\mathcal{Z}) \Rightarrow (\mathcal{V})$ så vi i beviset for Velordnings-sætningen (4.5). At $(\mathcal{V}) \Rightarrow (\mathcal{S})$ så vi i Korollar (4.8)(2). Det er klart, at $(\mathcal{V}) \Rightarrow (\mathcal{U})$, thi udfra en velordning $<$ på mængden A kan vi definere en udvalgsfunktion u på A ved

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

Det er ligeledes klart, at $(\mathcal{M}) \Rightarrow (\mathcal{Z})$, thi er $(X, <)$ induktivt ordnet og og er $K \subseteq X$ en delmængde med den i $(\mathcal{M})$ nævnte egenskab, så har K en majorant, da X er induktivt ordnet og K er totalt ordnet, og en sådan majorant må være et maksimalt element i X, thi ellers havde K også en ægte majorant, dvs. en majorant i $X \setminus K$, i modstrid at intet element i $X \setminus K$ er sammenligneligt med alle elementer i K.

Vi har således vist, at

$$\begin{array}{ccccc} (\mathcal{M}) & \to & (\mathcal{Z}) & & \\ & \nearrow & \downarrow & & \\ (\mathcal{U}) & \leftarrow & (\mathcal{V}) & \to & (\mathcal{S})\,. \end{array}$$

Beviset kan derfor fuldføres f.eks. ved at vise, at $(\mathcal{S}) \Rightarrow (\mathcal{V})$ og $(\mathcal{Z}) \Rightarrow (\mathcal{M})$. Det første viser vi senere, i (7.17), det andet viser vi herunder.

(5.3) Bemærkning. Ovenstående eksistens-udsagn kan bruges i mange områder af matematik. Ved de fleste anvendelser er det mest hensigtsmæssigt at bruge Zorn's lemma, og herunder viser vi et par typiske eksempler på anvendelser af Zorn's lemma.

(5.4) Bevis for $(\mathcal{Z}) \Rightarrow (\mathcal{M})$. Lad $(Y, <)$ være en partielt ordnet mængde. Vi betragter mængden X af totalt ordende delmængder K af Y, partielt ordnet ved sædvanlig inklusion $\subset$. Det er klart, at en delmængde med den i $(\mathcal{M})$ nævnte egenskab netop er et maksimalt element i $(X, \subset)$. Da vi antager, at $(\mathcal{Z})$ gælder, er det nok at vise, at $(X, \subset)$ er induktivt ordnet. Lad derfor (K_i), hvor $i \in I$, være en totalt ordnet delmængde af X. Vi påstår, at foreningsmængden $K := \bigcup_i K_i$ er majorant for mængden af K_i'er. Da vi øjensynlig har, at $K_i \subseteq K$ for alle i, skal vi blot vise, at $K \in X$, dvs. at K er en totalt ordnet delmængde af Y. Er altså $x, y \in K$, skal vi vise, at x og y er sammenlignelige. Vi har $x \in K_i$ og $y \in K_j$, og da K_l'erne er totalt ordnede, kan vi antage, at $K_i \subseteq K_j$, og så er både x og y elementer i K_j, og de er derfor sammenlignelige, da K_j er en totalt ordnet delmængde af Y ♠

(5.5) Bevis for $(\mathcal{Z}) \Rightarrow (\mathcal{U})$. En udvalgsfunktion på mængden A er som bekendt en afbildning $u : \mathcal{P}(A) \setminus \{\emptyset\} \to A$, som opfylder følgende betingelse:

$$(*) \qquad u(X) \in X$$

for alle delmængder X med $\emptyset \subset X \subseteq A$.

I det følgende betragter vi *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 betingelsen $(*)$ for alle $X \in \mathcal{D}$. Vi skal vise, at der eksisterer en partiel udvalgsfunktion $(\mathcal{D}, u)$, hvis domæne $\mathcal{D}$ er hele $\mathcal{P}(A) \setminus \{\emptyset\}$. Mængden $\mathcal{X}$ af partielle udvalgsfunktioner ordnes ved definitionen:

$$(\mathcal{D}, u) \prec (\mathcal{D}', u') \overset{\text{DEF}}{\iff} \mathcal{D} \subseteq \mathcal{D}' \wedge u'|\mathcal{D} = u.$$

For et maksimalt element $(\mathcal{D}, u)$ i mængden $\mathcal{X}$ må vi have, at $\mathcal{D} = \mathcal{P}(A) \setminus \{\emptyset\}$, 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 afbildningen u til en afbildning $\bar{u}$ med domæne $\bar{\mathcal{D}} := \mathcal{D} \cup \{B\}$ ved definitionen:

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

Det er klart, at $(\bar{\mathcal{D}}, \bar{u})$ er en partiel udvalgsfunktion, men så er $(\mathcal{D}, u) \prec (\bar{\mathcal{D}}, \bar{u})$ i modstrid med maksimaliteten af $(\mathcal{D}, u)$.

Da vi antager, at $(\mathcal{Z})$ gælder, er det følgelig nok at vise, at $(\mathcal{X}, \prec)$ er induktivt ordnet. Er $(\mathcal{D}_i, u_i)$, hvor $i \in I$, en totalt ordnet delmængde af $\mathcal{X}$, så kan vi betragte foreningsmængden $\mathcal{D} := \bigcup_i \mathcal{D}_i$. Hvis $X \in \mathcal{D}$, så er $X \in \mathcal{D}_i$ for et index i, og hvis også $X \in \mathcal{D}_j$, så er $u_i(X) = u_j(X)$, da $(\mathcal{D}_i, u_i)$'erne er totalt ordnede ved relationen

$\prec$. Vi kan følgelig definere en afbildning $u : \mathcal{D} \to A$ ved at sætte $u(X) := u_i(X)$, når $X \in \mathcal{D}_i$. Det er let at se, at der herved defineres en partiel udvalgsfunktion $(\mathcal{D}, u)$, og at der gælder:

$$(\mathcal{D}_i, u_i) \preceq (\mathcal{D}, u) \quad \text{for alle } i.$$

Følgelig er $(\mathcal{D}, u)$ en majorant i $\mathcal{X}$ for mængden af $(\mathcal{D}_i, u_i)$'er, som ønsket ♠

(5.6) Bevis for $(\mathcal{Z}) \Rightarrow (\mathcal{S})$. Lad X og Y være mængder og betragt mængden af par (A, f) bestående af en delmængde $A \subseteq X$ og en injektiv afbildning $f : A \to Y$. Vi kan ordne disse par ved definitionen:

$$(A, f) \prec (B, g) \overset{\text{DEF}}{\iff} A \subset B \wedge g|A = f.$$

For et maksimalt par (A, f) blandt disse par har vi enten, at $A = X$, og så er f en injektiv afbildning : $X \to Y$, eller, at $f(A) = Y$, og så er f^{-1} en injektiv afbildning : $Y \to X$. Var nemlig både $A \subset X$ og $f(A) \subset Y$, så kunne vi finde $a \in X \backslash A$ og $b \in Y \backslash f(A)$ og definere en afbildning $g : A \cup \{a\} \to Y$ ved $g|A = f$ og $g(a) = b$. Det er klart, at afbildningen g er injektiv og at $(A, f) \prec (A \cup \{a\}, g)$, og det er i modstrid med maksimaliteten af (A, f).

Da vi antager, at $(\mathcal{Z})$ gælder, er det følgelig nok at vise, at mængden af par (A, f) med ordningen $\prec$ er induktivt ordnet. Dette følger ganske som i det foregående bevis ♡

6. Den transfinite talrække.

(6.1) I det følgende er det bekvemt at tænke sig valgt en velordent 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 Sum–axiomet (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. $Y = \mathcal{P}(X)$ ifølge Cantor's sætning (2.4)(1) eller $Y = X \cup \mathcal{P}(X) \cup \mathcal{P}(\mathcal{P}(X)) \cup \cdots$, jfr. Eksempel (4.7). Vi kan velordne Y ifølge Velordnings-sætningen (4.5) og bruge denne mængde som Ω. Har vi to kandidater til Ω, følger det af Sammenlignings-sætningen for velordnede mængder (4.8), at den ene er ordens-isomorf med et afsnit af den anden, så heller ikke dette vil genere os i praksis.

(6.2) Vi kan yderligere antage, at ethvert ægte afsnit i Ω har mindre mægtighed end Ω, thi var dette ikke tilfældet, kunne vi erstatte Ω med afsnittet $\Omega_{<\infty}$, hvor $\infty \in \Omega$ er det første element, således at afsnittet $\Omega_{<\infty}$ har samme mægtighed som Ω.

Definition. Elementerne i den velordnede mængde Ω 'defineret' ovenfor kaldes *ordinaltal*.

(6.3) Af antagelsen om Ω følger specielt, at der ikke er noget sidste element i Ω. Hvert ordinaltal $\lambda \in \Omega$ har altså en umiddelbar efterfølger λ^+, jfr. Observation (4.2)(2).

Notation. Det første element i Ω betegnes 0. Endvidere sætter vi

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

Med denne notation kan vi opfatte de naturlige tal, hvortil vi her medregner 0, som elementer i Ω, dvs. som ordinaltal. Efterfølgeren af et naturlig tal n er den sædvanlige efterfølger $n^+ = n + 1$.

(6.4) Definition. De naturlige tal, hvortil vi her medregner 0, kaldes også de *endelige ordinaltal*. De ikke-endelige ordinaltal kaldes også *transfinite ordinaltal*. Det første transfinite ordinaltal betegnes ω.

Bemærk, at for et naturligt tal n har afsnittet

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

af Ω præcis n elementer. For ordinaltallet ω består afsnittet

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

præcis af de naturlige tal.

(6.5) Definition. Ifølge Sammenlignings-sætningen for velordnede mængder (4.8) er 'enhver i praksis forekommende' velordnet mængde $(V, <)$ ordens-isomorf med et ægte afsnit $\Omega_{<\lambda}$ af Ω, og $\lambda \in \Omega$ er entydigt bestemt ved den velordnede mængde $(V, <)$. Ordinaltallet λ kaldes *ordinaltallet* for den velordnede mængde $(V, <)$ og betegnes $\mathrm{Ord}(V, <)$, eller blot $\mathrm{Ord}\, V$, hvis ordningen $<$ i V er underforstået.

Observation. For velordnede mængder $(V, <)$ og $(W, <)$ har vi øjensynlig, at $\mathrm{Ord}(V, <) < \mathrm{Ord}(W, <)$, netop når $(V, <)$ er ordens-isomorf med et ægte afsnit af $(W, <)$.

Eksempler. (1) For en endelig, totalt ordnet (og dermed velordnet) mængde $(M, <)$ har vi $\mathrm{Ord}\, M = n$, hvor n er antallet af elementer i M.
(2) For mængden $\mathbf{N}$ af naturlige tal med sædvanlig ordning har vi $\mathrm{Ord}\, \mathbf{N} = \omega$.
(3) Udvides $\mathbf{N}$ med et element ∞, så at $n < \infty$ for alle naturlige tal n, får vi en velordnet mængde $\bar{\mathbf{N}}$ med $\mathrm{Ord}\, \bar{\mathbf{N}} = \omega^+$.

(6.6) Et element $\alpha \in \Omega$ kaldes et *kardinaltal*, hvis afsnittet $\Omega_{<\alpha}$ af Ω ikke er ækvipotent med noget afsnit $\Omega_{<\beta}$, hvor $\beta < \alpha$. Betingelsen er altså, at der for hvert ordinaltal $\beta < \alpha$ gælder, at $\Omega_{<\beta} \prec \Omega_{<\alpha}$.

Observation. Kardinaltallene er altså specielle ordinaltal. Som delmængde af den velordnede mængde Ω udgør kardinaltallene selv en velordnet mængde.

Notation. De endelige ordinaltal er øjensynlig kardinaltal. De naturlige tal er således både kardinaltal og ordinaltal.

Det første ikke-endelige kardinaltal betegnes $\aleph_0$ [tegnet $\aleph$, der er det første bogstav i det hebræiske alfabet læses: 'alef']. Det første kardinaltal, der følger efter $\aleph_0$, betegnes $\aleph_1$. Det første kardinaltal, der følger efter $\aleph_1$, betegnes $\aleph_2$ osv. Det første kardinaltal, der følger efter $\aleph_n$ for alle naturlige tal n, betegnes $\aleph_\omega$ osv. De første kardinaltal er altså følgende:

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

Bemærkning. Ordinaltallet ω er et kardinaltal, thi afsnittet $\Omega_{<\omega}$ er en uendelig mængde og for hvert ordinaltal $n < \omega$ er afsnittet $\Omega_{<n}$ en endelig mængde (med n elementer). Derimod er ordinaltallet ω^+ ikke et kardinaltal, thi afsnittet

$\Omega_{<\omega^+} = \{0, 1, 2, \ldots, \omega\}$ er øjensynlig ækvipotent med afsnittet $\Omega_{<\omega} = \{0, 1, 2, \ldots\}$. Tilsvarende er ordinaltallene:

$$\omega^{++}, \omega^{+++}, \omega^{++++}, \ldots$$

ikke ordinaltal. Heller ikke det første ordinaltal $\tilde{\omega}$, der følger efter alle disse, er et kardinaltal, thi afsnittet:

$$\Omega_{<\tilde{\omega}} = \{0, 1, 2, 3, \ldots, \omega, \omega^+, \omega^{++}, \omega^{+++}, \ldots\}$$

er øjensynlig numerabelt og derfor ækvipotent med afsnittet $\Omega_{<\omega}$

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

(6.7) Ifølge Velordnings-sætningen (4.5) kan enhver mængde velordnes. 'Enhver' mængde A er derfor ækvipotent med et ægte afsnit $\Omega_{<\alpha}$ af Ω.

Definition. Det første ordinaltal α, således at mængden A er ækvipotent med afsnittet $\Omega_{<\alpha}$ kaldes *kardinaltallet for mængden* A og betegnes

$$\operatorname{Card} A$$

[Andre almindelige betegnelser for kardinaltallet for mængden A er $|A|$ og $\#A$.] Det er klart, at $\operatorname{Card} A$ er et kardinaltal.

Observation. For 'vilkårllige' mængder A og B gælder:

$$A \simeq B \iff \operatorname{Card}(A) = \operatorname{Card}(B),$$
$$A \prec B \iff \operatorname{Card}(A) < \operatorname{Card}(B).$$

(6.8) Eksempler. (1) En mængde A er endelig, netop når kardinaltallet $n := \operatorname{Card} A$ er et naturligt tal (med 0 medregnet) og tallet n er så elementantallet i A i den forstand, at A er ækvipotent med $\Omega_{<n} = \{0, 1, \ldots, n-1\}$.
(2) For mængden $\mathbf{N}$ af naturlige tal har vi øjensynlig, at $\operatorname{Card} \mathbf{N} = \aleph_0$. En mængde A er således numerabel, netop når $\operatorname{Card} A = \aleph_0$, og tællelig, netop når $\operatorname{Card} A \leq \aleph_0$.
(3) Af resultaterne i (2.6) og (2.7) fremgår, at

$$\operatorname{Card}(\mathbf{N} \times \mathbf{N}) = \operatorname{Card} \mathbf{Z} = \operatorname{Card} \mathbf{Q} = \aleph_0 \quad \text{og} \quad \operatorname{Card} \mathbf{R} > \aleph_0.$$

Kardinaltallet $\operatorname{Card} \mathbf{R}$ betegnes også $\aleph$. Af uligheden ovenfor følger, at $\aleph_0 < \aleph$ og dermed, at

$$\aleph_1 \leq \aleph.$$

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

(6.9) Udfra operationer med mængder kan vi definere tilsvarende operationer med kardinaltallene. Er α og β kardinaltal, defineres *summen* $\alpha + \beta$, *produktet* $\alpha \cdot \beta$ og *potensen* β^α på følgende måde: Vælg mængder A og B så at

$$\alpha = \operatorname{Card} A \quad \text{og} \quad \beta = \operatorname{Card} B$$

og sæt

$$\begin{aligned} \alpha + \beta &:= \operatorname{Card}(A \cup B), \\ \alpha \cdot \beta &:= \operatorname{Card}(A \times B), \\ \beta^\alpha &:= \operatorname{Card}(B^A), \end{aligned}$$

hvor vi for summen forudsætter, at mængderne A og B er disjunkte. Det er let at se, at disse kompositioner er veldefinerede, dvs. at kardinaltallene på højre-siden er uafhængige af valgene af A og B. Og derefter følger det, at ligningerne ovenfor gælder for 'vilkårlige' mængder A og B.

(6.10) For kompositionerne af kardinaltal gælder de fleste af de regneregler, vi kender fra de sædvanlig naturlige tal. Lad os som eksempel vise *potensreglerne*:

$$\begin{aligned} &0. && \alpha^1 = \alpha \\ &1. && \gamma^{\alpha+\beta} = \gamma^\alpha \cdot \gamma^\beta \\ &2. && \gamma^{\alpha\cdot\beta} = (\gamma^\alpha)^\beta \\ &3. && (\beta \cdot \gamma)^\alpha = \beta^\alpha \cdot \gamma^\alpha \end{aligned}$$

Bevis for Potensreglerne. Vi har, at $1 = \operatorname{Card}\{0\}$ og vælger mængder A, B og C (med A og B disjunkte for den 1. potensregel), således at $\alpha = \operatorname{Card} A$, $\beta = \operatorname{Card} B$ og $\gamma = \operatorname{Card} C$. Afbildningerne:

$$\begin{aligned} A^{\{0\}} \to A, &\quad \text{givet ved: } f \mapsto f(0), \\ C^{A\cup B} \to C^A \times C^B, &\quad \text{givet ved: } g \mapsto (g|A, g|B), \\ (C^A)^B \to C^{A\times B}, &\quad \text{givet ved: } h \mapsto [(a,b) \mapsto h(b)(a)], \\ B^A \times C^A \to (B \times C)^A, &\quad \text{givet ved: } (k,l) \mapsto [a \mapsto (k(a), l(a))], \end{aligned}$$

er da bijektive, og heraf følger reglerne ♡

EKSEMPEL. Ifølge resultatet i (2.9) er

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

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

(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 forskellige fra 0, hvoraf et forudsættes transfinit. Da gælder:*

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

Bevis. Vi kan f.eks. antage, at $\beta \leq \alpha$ og altså at $\alpha = \max\{\alpha, \beta\}$. Specielt er altså α transfinit. Det er klart, at $\alpha \leq \alpha + \beta$. At $\alpha + \beta \leq \alpha \cdot \beta$ ses også let (for $\beta = 1$ er det dog nødvendigt at udnytte, at α er transfinit). Da $\beta \leq \alpha$, har vi trivielt, at $\alpha \cdot \beta \leq \alpha \cdot \alpha$. Følgelig er det nok at vise, at

$$\alpha \cdot \alpha \leq \alpha \qquad \text{når } \alpha \text{ er transfinit.}$$

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 $\alpha \cdot \alpha = \operatorname{Card}(\Omega_{<\alpha} \times \Omega_{<\alpha})$. I produktmængden $\Omega_{<\alpha} \times \Omega_{<\alpha}$ defineres en relation $<$ på følgende måde:

$$\begin{aligned}(\lambda_1, \lambda_2) < (\mu_1, \mu_2) \iff & \\ & \max\{\lambda_1, \lambda_2\} < \max\{\mu_1, \mu_2\} \quad \textbf{eller} \\ & \max\{\lambda_1, \lambda_2\} = \max\{\mu_1, \mu_2\} \text{ og } \lambda_1 < \mu_1 \quad \textbf{eller} \\ & \max\{\lambda_1, \lambda_2\} = \max\{\mu_1, \mu_2\} \text{ og } \lambda_1 = \mu_1 \text{ og } \lambda_2 < \mu_2.\end{aligned}$$

Det er klart, at der herved defineres en velordning af produktmængden $\Omega_{<\alpha} \times \Omega_{<\alpha}$. Det er udelukket, at $\Omega_{<\alpha} \times \Omega_{<\alpha}$ er ordens-isomorf med et afsnit at $\Omega_{<\alpha}$, idet vi jo så ville få, at

$$\alpha \cdot \alpha = \operatorname{Card}(\Omega_{<\alpha} \times \Omega_{<\alpha}) \leq \operatorname{Card}\Omega_{<\alpha} = \alpha,$$

i modstrid med antagelsen om, at $\alpha < \alpha \cdot \alpha$. Af Sammenlignings-sætningen for velordnede mængder (4.8) følger derfor, at $\Omega_{<\alpha}$ er ordens-isomorf med et ægte afsnit W af $\Omega_{<\alpha} \times \Omega_{<\alpha}$. Der findes altså ordinaltal $\mu_1, \mu_2 \in \Omega_{<\alpha}$, så at afsnittet W består af de par (λ_1, λ_2), for hvilke $(\lambda_1, \lambda_2) < (\mu_1, \mu_2)$. Da α er et transfinit kardinaltal, er der intet sidste element i $\Omega_{<\alpha}$. Der findes derfor et ordinaltal $\beta \in \Omega_{<\alpha}$, så at $\max\{\mu_1, \mu_2\} < \beta$, og så følger det, at vi for hvert par (λ_1, λ_2) i W har, at $\lambda_1 < \beta$ og

$\lambda_2 < \beta$. Altså er $W \subseteq \Omega_{<\beta} \times \Omega_{<\beta}$. Vi sætter $\gamma := \operatorname{Card} \Omega_{<\beta}$. Da $\beta < \alpha$ og α er et kardinaltal, er $\gamma < \alpha$ og ifølge det foregående er $\Omega_{<\alpha}$ ækvipotent med delmængden W af $\Omega_{<\beta} \times \Omega_{<\beta}$. Følgelig har vi, at

$$\alpha \leq \gamma \cdot \gamma \quad \text{og} \quad \gamma < \alpha.$$

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

KOROLLAR. *For ethvert transfinit kardinaltal α gælder, at $\alpha^\alpha = 2^\alpha$.*

Bevis. Under brug af Sætningen finder vi:

$$2^\alpha \leq \alpha^\alpha \leq (2^\alpha)^\alpha = 2^{\alpha \cdot \alpha} = 2^\alpha \spadesuit$$

BEMÆRKNING. Sætningen indeholder øjensynlig Korollar (4.10) (og Sætning (2.6)) som specialtilfælde.

STRUKTURER

1. Indledning.

(1.1) Grundlæggende i al matematik er mængde- og afbildningsbegrebet. Mængder forekommer imidlertid yderst sjældent isolerede; de vil, afhængigt af situationen, være forsynet med en vis *struktur*. Vi kan **ikke** gennerelt definere, hvad det vil sige, at en mængde således er *struktureret*, men vi kan løst sige, at en struktur på en mængde består i, at der udover mængden er "givet noget", som "opfylder visse betingelser". Det vil sædvanligvis være klart hvad der menes med, at to mængder har strukturer af samme *type*.

(1.2) Eksempler på Strukturtyper.

(1) **Ordnede mængder**. Strukturen på en mængde M er her en relation $<$ i M, dvs. en delmængde af $M \times M$, som opfylder visse velkendte betingelser.
(2) **Metriske rum**. Strukturen på en mængde M er her en afbildning $dist : M \times M \to \mathbf{R}$, som opfylder visse velkendte betingelser.
(3) **Komplekse, normerede vektorrum**. Strukturen på en mængde M består her af tre afbildninger:

$$\begin{aligned} M \times M &\to M \quad \text{(vektoraddition)} \\ \mathbf{C} \times M &\to M \quad \text{(multiplikation med skalar)} \\ M &\to \mathbf{R} \quad \text{(normen)}, \end{aligned}$$

som opfylder visse betingelser.

(1.3) Man kan angive, at en mængde er struktureret, ved efter betegenelsen for mængden at anføre symboler for den givne struktur. I eksemplerne ovenfor kan vi således skrive $(M, <)$ for en ordnet mængde, $(M, dist)$ for et metrisk rum, og $(M, +, \mathbf{C}, \| \quad \|)$ for et komplekst, normeret vektorrum.

(1.4) En matematisk teori vil ofte omfatte studiet af mængder med strukturer af en given fast type. I en sådan teori vil der for mængder $(M, \$)$ og $(N, £)$ med strukturer af den givne type være visse afbildninger

$$f : M \to N,$$

der kan siges, at "have noget at gøre med strukturen" eller at "harmonere med strukturen" eller at "bevare (eller respektere) strukturen". Når det for en bestemt

strukturtype er **præciseret**, hvilke afbildninger der i en sådan forstand er relevante, kan disse afbildninger kaldes *homomorfier*. For en homomorfi $f : M \to N$ skrives også

$$f : (M, \$) \to (N, £).$$

Ved denne sprogbrug er det altid underforstået, at sammensætning af to homomorfier igen er en homomorfi, og at den identiske afbildning $x \mapsto x$ af M på sig selv er en homomorfi $Id_M : (M, \$) \to (M, \$)$.

En homomorfi $f : (M, \$) \to (N, £)$, der er bijektiv og således at den inverse afbildning $f^{-1} : N \to M$ også er en homomorfi : $(N, £) \to (M; \$)$, kaldes en *isomorfi*. At en homomorfi $f : (M, \$) \to (N, £)$ er en isomorfi, angives ofte ved at skrive

$$f : (M, \$) \xrightarrow{\approx} (N, £).$$

Hvis der findes en sådan isomorfi, siges $(M, \$)$ og $(N, £)$ at være *isomorfe*. Herfor kan skrives

$$(M, \$) \approx (N, £).$$

En homomorfi $f : (M, \$) \to (M, \$)$ af $(M, \$)$ ind i sig selv kaldes også en *endomorfi*. En endomorfi, der er en isomorfi, kaldes også en *automorfi*.

Observation. En homomorfi $f : (M, \$) \to (N, £)$ er en isomorfi, hvis og kun hvis der findes en homomorfi $g : (N, £) \to (M, \$)$, så at

$$g \circ f = Id_M \quad \text{og} \quad f \circ g = Id_N,$$

thi af de to ligninger følger, at f er en bijektiv afbildning med g som den inverse.

(1.5) Det skal understreges, at vi for en given strukturtype **ikke** i (1.4) har **defineret**, hvad en homomorfi (og dermed en isomorfi, ...) er. Når vi taler om homomorfier, skal det altid være præciseret, hvilke afbildninger, der er så interessante, at de fortjener denne betegnelse. For en bestemt strukturtype vil der ofte være flere lige gode valg. For ordnede mængder vil det forekomme ret naturligt, at homomorfierne er de afbildninger

$$f : (M, <) \to (N, <)$$

som opfylder: $x < y \Rightarrow f(x) < f(y)$. For metriske rum er situationen ikke så entydig. Vi kan betragte afbildninger

$$f : (M, dist) \to (N, dist),$$

som er afstandsbevarende, eller (svagt) afstandsformindskende, eller blot kontinuente. Ved de to første valg bliver isomorfierne de såkaldte isometrier, ved det sidste valg bliver de homeomorfierne.

(1.6) I det følgende behandles de fundamentale *algebraiske strukturer* afledt af kompositioner og relationer.

2. Kompositioner.

(2.1) Definition. En *komposition* $*$ i en mængde M er som bekendt en afbildning

$$* : M \times M \to M.$$

Billedet i M af $(a, b) \in M \times M$ ved denne afbildning betegnes sædvanligvis $a * b$. Det kaldes *kompositet* af a med b [læses: "a stjerne b" eller "a komponeret med b"]. For et fast $a \in M$ er

$$l_a : x \mapsto a * x$$

en afbildning $l_a : M \to M$. Den kaldes *venstrekomposition med* a.

Tilsvarende er *højrekomposition med* a givet ved $r_a : x \mapsto x * a$.

Mængden M med en given komposition $*$ betegnes kort $(M, *)$.

(2.2) Definition. I en mængde med en komposition $(M, *)$ siges en delmængde $S \subseteq M$ at være *stabil*, dersom

$$x \in S \wedge y \in S \implies x * y \in S.$$

Er dette tilfældet, definerer kompositionen $*$ ved *restriktion* en komposition i S, kaldet den *inducerede* komposition.

(2.3) Definitioner. Lad $(M, *)$ være en mængde med en komposition. Elementer $x, y \in M$ siges at *kommmutere*, hvis

$$x * y = y * x.$$

Gælder dette for alle $x, y \in M$, kaldes kompositionen *kommutativ*. Den kaldes *associativ*, hvis der for alle $x, y, z \in M$ gælder:

$$(x * y) * z = x * (y * z).$$

Et element $e \in M$ kaldes *neutralt element*, hvis der for alle $x \in M$ gælder:

$$e * x = x * e = x.$$

Et element $a \in M$ kaldes *regulært*, hvis der for alle $x, y \in M$ gælder:

$$a * x = a * y \implies x = y \qquad \text{og} \qquad x * a = y * a \implies x = y.$$

Et element $a \in M$ kaldes *invertibelt*, hvis der for hvert element $b \in M$ gælder, at hver af de to ligninger

$$a * x = b \quad \text{og} \quad z * a = b$$

har en og kun én løsning i M.

Hvis alle elementer er regulære, siges *forkortningsreglen* at gælde.

BEMÆRKNING. At et element $a \in M$ er regulært (resp. invertibelt) betyder, at venstrekomposition $x \mapsto a * x$ og højrekomposition $x \mapsto x * a$ er injektive (resp. bijektive) afbildninger : $M \to M$.

(2.4) DEFINITIONER. En *semigruppe* $(M, *)$ er en mængde med en associativ komposition. Et *monoid* $(M, *)$ er en semigruppe med et neutralt element. En *gruppe* $(M, *)$ er et monoid, hvori alle elementer er invertible.

OBSERVATIONER. En komposition kan højst have ét neutralt element. I et monoid $(M, *)$ betegnes det neutrale element ofte e_M. I et monoid $(M, *)$ er et element a invertibelt, netop hvis der findes et element $a' \in M$, således at

$$a * a' = a' * a = e_M.$$

Elementet a' er i så fald entydigt bestemt. Det kaldes det *inverse* til a, og det betegnes a^{-1}.

Det følger, at en mængde M med en komposition $*$ er en gruppe, hvis der findes et element $e \in M$, og for hvert element $x \in M$ et element $x^{-1} \in M$, så at ligningerne

$$(x * y) * z = x * (y * z)$$
$$e * x = x * e = x$$
$$x * x^{-1} = x^{-1} * x = e$$

gælder for alle $x, y, z \in M$.

SÆTNING. *Lad $(M, *)$ være et monoid. Hvis a og b er invertible elementer, så er også $a * b$ invertibelt, og*

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

De invertible elementer i M udgør en stabil delmængde, som med den inducerede komposition er en gruppe.

Bevis. ♡

(2.5) EKSEMPEL. Lad X være en mængde, og lad $End(X)$ betegne mængden af alle afbildninger : $X \to X$ af mængden ind i sig selv. Vi kan opfatte sammensætning som en komposition $\circ$ i mængden $End(X)$. Da sammensætning af afbildninger som bekendt er associativ, og da den identiske afbildning

$$Id_X : x \mapsto x$$

øjensynlig er neutralt element, er $(End(X), \circ)$ et monoid. Gruppen af invertible elementer heri består netop af de bijektive afbildninger : $X \to X$. Denne gruppe betegnes også $Aut(X)$.

(2.6) NOTATION. I en mængde med en komposition $(M, *)$ er det ofte hensigtsmæssigt at bruge kompositionstegnet i forbindelse med delmængder. Er A, B delmængder af M, betegner vi således med $A * B$ delmængden

$$A * B := \{a * b \mid a \in A \wedge b \in B\}.$$

Tilsvarende sættes for $a \in M$ og $B \subseteq M$

$$a * B := \{a * b \mid b \in B\},$$

og, hvis $(M, *)$ er en gruppe,

$$B^{-1} := \{b^{-1} \mid b \in B\} \qquad \text{og}$$
$$a * B * a^{-1} := \{a * b * a^{-1} \mid b \in B\}.$$

(2.7) DEFINITION. Lad $*$ være en komposition i mængden M og lad $*'$ være en komposition i mængden M'. En afbildning $f : M \to M'$ siges da at være en *homomorfi*

$$f : (M, *) \to (M', *'),$$

hvis der for alle $x, y \in M$ gælder

$$f(x * y) = f(x) *' f(y).$$

En bijektiv homomorfi $f : (M, *) \to (M, *')$ kaldes også en *isomorfi*. For en sådan er den inverse afbildning f^{-1} en homomorfi

$$f^{-1} : (M', *') \to (M, *).$$

En homomorfi $f : (M, *) \to (M, *)$ kaldes også en *endomorfi* i $(M, *)$.

OBSERVATION. For en *gruppehomomorfi*, dvs. en homomorfi $f : (M, *) \to (M', *')$ mellem grupper $(M, *)$ og $(M', *')$ gælder

$$f(e_M) = e_{M'} \quad \text{og} \quad f(x^{-1}) = f(x)^{-1} \quad \text{for alle } x \in M,$$

BEMÆRKNING. For en homomorfi $f : (M, *) \to (M', *')$ mellem monoider $(M, *)$ og $(M', *')$ gælder ikke i almindelighed, at

$$f(e_M) = e_{M'}.$$

Er denne betingelse opfyldt, kaldes homomorfien en *monoidhomomorfi*.

(2.8) Vi vil ofte møde mængder M, i hvilke der er givet to (eller flere) kompositioner. I en sådan situation må man naturligvis præcisere, på hvilken af kompositionerne de foregående definitioner anvendes. Er $(M, \perp, *)$ en mængde med kompositioner $\perp$ og $*$, kan en delmængde $S \subseteq M$ være stabil under $\perp$, og stabil under $*$. Er den stabil under begge kompositioner kaldes den *stabil* i $(M, \perp, *)$. Den kan i så fald selv opfattes som en mængde med inducerede kompositioner $(S, \perp, *)$.

Er tilsvarende $(M', \perp', *')$ en mængde med to kompositioner, kan en afbildning $f : M \to M'$ være en homomorfi $f : (M, \perp) \to (M', \perp')$ eller en homomorfi $f : (M, *) \to (M', *')$. Er begge dele opfyldt, siges f at være en *homomorfi*

$$f : (M, \perp, *) \to (M', \perp', *').$$

DEFINITION. I en mængde M med kompositioner $\perp$ og $*$ siges $*$ at være *distributiv* mht. $\perp$, hvis der for alle $x, y, z \in M$ gælder:

$$x * (y \perp z) = (x * y) \perp (x * z) \quad \text{og} \quad (x \perp y) * z = (x * z) \perp (y * z)\,.$$

(2.9) NOTATION. En komposition i en mængde kan naturligvis betegnes med et hvilketsomhelst symbol. (Andre almindeligt brugte tegn er $\circ, \times, \cup, \cap, \vee, \wedge$). Vi vil ofte skrive kompositioner *multiplikativt*, dvs. bruge tegnet $\cdot$ for kompositionen. Kompositet $a \cdot b$ kaldes da *produktet*, og heri udelader vi oftest kompositionstegnet og skriver ab for $a \cdot b$. Et eventuelt neutralt element kan også kaldes et *et-element* og betegnes 1. Betingelsen er:

$$1x = x1 = x.$$

Visse kommutative kompositioner vil vi dog skrive *additivt*, dvs. vi vil bruge tegnet $+$ for kompositionen. Kompositet $a + b$ kaldes da *summen*. Et eventuelt neutralt element kan kaldes et *nul-element* og betegnes 0. Betingelsen er:

$$0 + x = x.$$

Et eventuelt inverst element til x kaldes da det *modsatte* til x og betegnes $-x$. Betingelsen er:

$$x + (-x) = 0.$$

Er $(M, *)$ en kommutativ semigruppe og $I \neq \emptyset$ en endelig mængde, kan vi for en afbildning $a : I \to M$ definere elementet

$$\underset{i\in I}{*}\, a_i \qquad [\text{additivt: } \sum_{i\in I} a_i\,, \qquad \text{multiplikativt: } \prod_{i\in I} a_i]$$

som kompositet af elementerne a_i, $i \in I$ [Overvej dette!]. Har M et neutralt element e, er det hensigtmæssigt at tillægge dette kompositum værdien e, når $I = \emptyset$.

(2.10) Definition. En *ring* $(\Lambda, +, \cdot)$ er en mængde Λ med kompositioner $+$ og $\cdot$ således at

(1) $(\Lambda, +)$ er en kommutativ gruppe.
(2) $(\Lambda, \cdot)$ er et monoid.
(3) $\cdot$ er distributiv mht. $+$.

Nul-elementet i $(\Lambda, +)$ er ringens *nul-element* 0_Λ, og et-elementet i $(\Lambda, \cdot)$ er ringens *et-element* 1_Λ.

Gentagne anvendelser af den distributive lov giver, for et endeligt produkt af endelige summer,

$$(a_1+a_2+\cdots)(b_1+b_2+\cdots)(c_1+c_2+\cdots)\cdots = \sum a_i b_j c_k \cdots\ .$$

En *ringhomomorfi* $f : (\Lambda, +, \cdot) \to (\Gamma, +, \cdot)$ er en afbildning $f : \Lambda \to \Gamma$ mellem ringe, som opfylder

$$\begin{aligned} f(x+y) &= f(x) + f(y), \\ f(xy) &= f(x)f(y), \\ f(1_\Lambda) &= 1_\Gamma\,. \end{aligned}$$

(2.11) Definition. Lad $(G, \cdot)$ være en gruppe. En delmængde $H \subseteq G$ kaldes da en *undergruppe*, hvis den er stabil, og med den inducerede komposition selv er en gruppe. Det følger, at inklusionsafbildningen i så fald er en gruppehomomorfi $: (H, \cdot) \hookrightarrow (G, \cdot)$.

Observation. En delmængde H af en gruppe $(G, \cdot)$ er en undergruppe, netop når der gælder:

$$\begin{gathered} x \in H \wedge y \in H \implies xy \in H, \\ e_G \in H, \\ x \in H \implies x^{-1} \in H. \end{gathered}$$

(2.12) Definition. Lad $(\Lambda, +, \cdot)$ være en ring. En delmængde $\triangle \subseteq \Lambda$ kaldes da en *delring*, hvis den er stabil, og med de inducerede kompositioner selv er en ring med samme et-element som Λ. Den sidste betingelse er nødvendig for at sikre, at inklusionsafbildningen er en ringhomomorfi $: (\triangle, +, \cdot) \hookrightarrow (\Lambda, +, \cdot)$.

3. Relationer.

(3.1) Definition. En *relation* R i en mængde M er som bekendt en delmængde

$$R \subseteq M \times M.$$

Udsagnet $(x, y) \in R$ skrives sædvanligvis

$$xRy,$$

og dets negation skrives $x \not R y$.

(3.2) Definitioner. En relation R i en mængde M kaldes *refleksiv*, hvis der for alle $x \in M$ gælder:

$$xRx,$$

og *irreflexiv*, hvis der for alle $x \in M$ gælder:

$$x \not R x\,.$$

Den kaldes *symmetrisk*, hvis der for alle $x, y \in M$ gælder:

$$xRy \implies yRx,$$

og *asymmetrisk*, hvis der for alle $x, y \in M$ gælder:

$$xRy \wedge yRx \implies x = y.$$

Den kaldes *transitiv*, hvis der for alle $x, y, z \in M$ gælder:

$$xRy \wedge yRz \implies xRz.$$

Den kaldes *total*, hvis der for alle $x, y \in M$ gælder:

$$x = y \ \vee \ xRy \ \vee \ yRx.$$

(3.3) Definition. Lad R være en relation i mængden M og lad R' være en relation i mængden M'. En afbildning $f : M \to M'$ siges da at *respektere relationerne*, eller at være en *homomorfi*

$$f : (M, R) \to (M', R'),$$

hvis der for alle $x, y \in M$ gælder: $xRy \implies f(x)R'f(y)$. Er der kun givet en relation R i M siges en afbildning $f : M \to M'$ at *respektere relationen*, hvis der for alle $x, y \in M$ gælder:

$$xRy \implies f(x) = f(y).$$

(3.4) Definition. En transitiv relation R i en mængde M kaldes en *pre-ordning*. Den kaldes en *ordning*, hvis den desuden er asymmetrisk. Som betegnelse for en ordning bruges ofte et af tegnene $\prec$ [læses: "går forud for"] og $\succ$ [læses: "følger efter"]. Til hver ordning $\prec$ hører en reflexiv ordning $\underset{=}{\prec}$ defineret ved

$$x \underset{=}{\prec} y \overset{\text{DEF}}{\iff} x \prec y \vee x = y,$$

og en irrefleksiv ordning $\underset{\neq}{\prec}$ defineret ved

$$x \underset{\neq}{\prec} y \overset{\text{DEF}}{\iff} x \prec y \wedge x \neq y.$$

Vi vil **reservere** tegnene $\leq, \subseteq, \geq, \supseteq$ (resp. $<, \subset, >, \supset$) som betegnelse for ordninger, som er refleksive (resp. irrefleksive).

En *ordnet mængde* $(M, \prec)$ er en mængde M med en given ordning $\prec$. Hvis relationen $\prec$ er total, kaldes $(M, \prec)$ *totalt ordnet*. Er relationen $\prec$ ikke nødvendigvis total, siges $(M, \prec)$ også at være *partielt ordnet*.

For ordnede mængder $(M, \prec)$ og $(M', \prec')$ siges en afbildning $f : M \to M'$, som respekterer ordningerne, også at være en *ordenstro* afbildning eller en *ordenshomomorfi*

$$f : (M, \prec) \to (M', \prec').$$

En ordning $\prec$ i mængden M nedarves umidelbart til enhver delmængde $N \subseteq M$. Med denne *inducerede* ordning i N er inklusionsafbildningen ordenstro : $(N, \prec) \hookrightarrow (M, \prec)$.

Observation. En relation R, som er transitiv og irrefleksiv, er også asymmetrisk (og altså en ordning).

(3.5) Definition. I en ordnet mængde $(M, \prec)$ siget et element a at være *minimalt*, hvis der for alle $x \in M$ gælder:

$$x \prec a \implies x = a,$$

og at være *første element*, hvis der for alle $y \in M$ gælder:

$$a \underset{=}{\prec} y.$$

Tilsvarende defineres *maksimalt element* og *sidste element*.

BEMÆRK. "Minimalt" betyder, at ingen elementer går ægte forud, "første element" betyder, at alle elementer følger efter. De to definitioner stemmer kun overens for totalt ordnede mængder. I almindelighed kan der godt være flere minimale elementer (men højst ét første element).

(3.6) DEFINITION. Lad $(M, \prec)$ være en ordnet mængde, og lad $N \subseteq M$ være en delmængde. Et element $a \in M$ kaldes en *majorant* for N, hvis der for alle $y \in N$ gælder $y \underset{=}{\prec} a$. Et element $b \in M$, der er første element i delmængden af majoranter for N, kaldes også *supremum* for N. Herfor skrives

$$b = sup\, N.$$

Tilsvarende defineres *minorant*, *infimum* og $inf\, N$.

Hvis der findes majoranter for N, siges N at være *opad begrænset*. Er der også minoranter, kaldes N *begrænset*.

(3.7) DEFINITION. En ordnet mængde $(M, \prec)$ kaldes *velordnet*, hvis enhver ikke-tom delmængde af M har et første element.

(3.8) DEFINITION. En relation R i en mængde M kaldes en *ækvivalensrelation*, hvis den er refleksiv, symmetrisk og transitiv. *Ækvivalensklasserne* er da de delmængder af M, der har formen

$$\{x \in M \mid xRa\} \quad , \text{ med } a \in M.$$

De udgør en *klassedeling* af M, dvs. en mængde af ikke-tomme, parvis disjunkte delmængder, hvis foreningsmængde er M.

Mængden af ækvivalensklasser kaldes *kvotienten* (eller *kvotientmængden*) af M mht. R og betegnes M/R [læses: "M over R" eller "M modulo R"].

En ækvivalensklasse X kan altså opfattes dels som en delmængde $X \subseteq M$, dels som et element i den nye mængde M/R. Hvis $x \in X$, siges x at være en *repræsentant* for X.

Idet vi for hvert $x \in M$ med $\boxed{x}$ [læses: "x kvadrat"] betegner ækvivalensklassen, der indeholder x, altså

$$\boxed{x} = \{x' \mid x'Rx\},$$

defineres ved $x \mapsto \boxed{x}$ en surjektiv afbildning

$$\boxed{} : M \to M/R,$$

kaldet den *kanoniske afbildning*. At elementet $x \in M$ er repræsentant for ækvivalensklassen X betyder således, at $\boxed{x} = X$. Bemærk, at

$$\boxed{x} = \boxed{y} \iff xRy.$$

Elementet $\boxed{x} \in M/R$ kan også betegnes: x mod R.

(3.9) SPROGBRUG. Lad der være givet en afbildning $\varphi : M \to \bar{M}$. En afbildning $\bar{f} : \bar{M} \to P$ siges da at *udvide* afbildningen $f : M \to P$ mht. φ, hvis $\bar{f} \circ \varphi = f$.

I diagramform:

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & \bar{M} \\ {\scriptstyle f}\big\downarrow & & \\ P & & \end{array}$$

Hvis det er underforstået hvilken afbildning : $M \to \bar{M}$, der er givet, siger vi blot, at $\bar{f}$ er en *udvidelse* f.

(3.10) Med denne sprogbrug gælder følgende trivielle:

UDVIDELSESSÆTNING FOR MÆNGDER. *Lad R være en ækvivalensrelation i M, og lad $\boxed{\ } : M \to M/R$ være den kanoniske afbildning ind i kvotienten. Enhver afbildning $f : M \to P$, som respekterer ækvivalensrelationen R, kan da entydigt udvides til en afbildning $\bar{f} : M/R \to P$ fra kvotienten. I diagramform:*

$$\begin{array}{ccc} M & \xrightarrow{\boxed{\ }} & M/R \\ {\scriptstyle f}\big\downarrow & & \\ P & & \end{array}$$

Bevis. At $\bar{f}$ er en udvidelse af f betyder, at $\bar{f} \circ \boxed{\ } = f$, altså at

$$\bar{f}(\boxed{x}) = f(x) \quad \text{for alle } x \in M.$$

Heraf følger påstanden let, da hvert element $X \in M/R$ har formen $X = \boxed{x}$ ♡

DEFINITION. Den entydigt bestemte udvidelse siges også at være *induceret* af f.

(3.11) DEFINITION. Lad $f : M \to P$ være en afbildning. *Billedet* ved f er da billedmængden

$$f(M) := \{f(x) \mid x \in M\},$$

og den *til f hørende relation* er relationen $\underset{f}{\sim}$ defineret ved

$$x' \underset{f}{\sim} x \overset{\text{DEF}}{\iff} f(x') = f(x).$$

Det er klart, at afbildningen f respekterer relationen $\underset{f}{\sim}$.

ISOMORFISÆTNING FOR MÆNGDER. *Lad $f : M \to P$ være en afbildning. Da er billedet en delmængde af P, og relationen $\underset{f}{\sim}$ er en ækvivalensrelation i M. Den inducerede afbildning er en bijektion $\bar{f} : M/\underset{f}{\sim} \xrightarrow{\sim} f(M)$ af kvotienten på billedet.*

Bevis. Relationen $\underset{f}{\sim}$ er øjensynlig en ækvivalensrelation, så ifølge Udvidelsessætningen (3.10) inducerer f en afbildning $\bar{f} : M/\underset{f}{\sim} \to P$. Billedmængden herfor er netop $f(M)$, så vi kan opfatte $\bar{f}$ som en surjektiv afbildning

$$\bar{f} : M/\underset{f}{\sim} \to f(M),$$

og skal vise, at den er injektiv. Lad X og Y være elementer i kvotienten $M/\underset{f}{\sim}$, således at $\bar{f}(X) = \bar{f}(Y)$. Vælges repræsentanter x for X og y for Y har vi

$$f(x) = \bar{f}(\boxed{x}) = \bar{f}(X) = \bar{f}(Y) = \bar{f}(\boxed{y}) = f(y),$$

men så er $x \underset{f}{\sim} y$, og altså $X = \boxed{x} = \boxed{y} = Y$♠

BEMÆRKNING. Idet vi med $\iota : f(M) \hookrightarrow P$ betegner inklusionsafbildningen, er den givne afbildning en sammensætning $f = \iota \circ \bar{f} \circ \square$ af en surjektiv afbildning $\square$, en bijektiv afbildning $\bar{f}$ og en injektiv afbildning ι. I diagramform:

$$\begin{array}{ccc} M & \xrightarrow{f} & P \\ \square\downarrow & & \uparrow\iota \\ M/\underset{f}{\sim} & \xrightarrow{\bar{f}} & f(M) \end{array}$$

4. Harmoniske relationer.

(4.1) DEFINITION. Lad M være en mængde med en komposition $*$ og en relation R. Relationen siges da at *harmonere med højrekomposition*, hvis der for alle elementer $x, y, a \in M$ gælder

$$x\,R\,y \implies x{*}a\,R\,y{*}a,$$

og at *harmonere med venstrekomposition*, hvis der for alle $x, y, a \in M$ gælder

$$x\,R\,y \implies a{*}x\,R\,a{*}y.$$

Er begge dele opfyldt, siges relationen R at *harmonere med kompositionen* $*$, eller at være en *harmonisk relation* i $(M, *)$.

BEMÆRKNING. Betingelserne udsiger, at højrekomposition $x \mapsto x * a$ og venstrekomposition $x \mapsto a * x$ for ethvert element a er homomorfier : $(M, R) \to (M, R)$

OBSERVATION. Hvis en harmonisk relation R i $(M, *)$ er transitiv, så gælder for alle $x, x', y, y' \in M$, at $x\,R\,x' \wedge y\,R\,y' \implies x * y\,R\,x' * y'$.

(4.2) OBSERVATION. En relation R i en **gruppe** $(G, \cdot)$ (multiplikativt skrevet, med neutralt element e), som harmonerer med venstremultiplikation, er helt bestemt ved delmængden $\{z \in G \mid e\,R\,z\}$, idet vi har

$$x\,R\,y \iff x^{-1}y \in \{z \in G \mid e\,R\,z\}.$$

Omvendt gælder følgende:

SÆTNING. *Lad $(G, \cdot)$ være en gruppe med neutralt element e. For hver delmængde $N \subseteq G$ defineres da ved*

$$x\,R_N\,y \overset{DEF}{\iff} x^{-1}y \in N$$

en relation R_N i G, som harmonerer med venstremultiplikation, og for hvilken

$$\{z \in G \mid e\,R_N\,z\} = N.$$

Om relationen R_N gælder yderligere:

(1) *R_N er harmonisk $\iff a^{-1}Na \subseteq N$ for alle $a \in G$.*
(2) *R_N er refleksiv $\iff e \in N$.*
(3) *R_N er irrefleksiv $\iff e \notin N$.*
(4) *R_N er symmetrisk $\iff N^{-1} \subseteq N$.*
(5) *R_N er asymmetrisk $\iff N \cap N^{-1} \subseteq \{e\}$.*
(6) *R_N er transitiv $\iff N \cdot N \subseteq N$ (dvs. N er stabil).*
(7) *R_N er total $\iff G = \{e\} \cup N \cup N^{-1}$.*

Bevis. Den første påstand følger af at

$$(ax)^{-1}(ay) = x^{-1}a^{-1}ay = x^{-1}y.$$

(1),"⇒": Vi skal vise for $a \in G$ og $z \in N$, at $a^{-1}za \in N$. Da $z \in N$, har vi $e\,R_N\,z$, og da R_N harmonerer med højremultiplikation, følger heraf $ea\,R_N\,za$, altså

$$a^{-1}za = (ea)^{-1}(za) \in N.$$

(1),"⇐": Vi skal vise, at R_N harmonerer med højremultiplikation. Antag derfor, at $x\,R_N\,y$, og lad $a \in G$. Da er $(xa)^{-1}(ya) = a^{-1}(x^{-1}y)a \in N$, thi $x^{-1}y \in N$ og $a^{-1}Na \subseteq N$.

De øvrige påstande vises analogt ♡

Bemærkninger. Ud fra en delmængde $N \subseteq G$ kan vi analogt ved

$$x\,R_N^h\,y \overset{DEF}{\iff} yx^{-1} \in N$$

definere en relation R_N^h, som harmonerer med højremultiplikation. Det er let at se, at R_N og R_N^h er den samme relation, netop når betingelsen (1) er opfyldt.

Vi kan yderligere ved at betragte produkterne $y^{-1}x$ og xy^{-1} definere endnu to relationer. Hvis både (1) og (4) er opfyldt, bliver disse 4 relationer ens, idet udsagnene

$$x^{-1}y \in N, \quad yx^{-1} \in N, \quad y^{-1}x \in N \quad \text{og} \quad xy^{-1} \in N$$

så er ensbetydende.

Notation. I en kommutativ gruppe er betingelsen (4.2)(1) altid opfyldt. Vi fremhæver, at for en delmængde N i en kommutativ, additivt skrevet gruppe $(G, +)$, er relationen R_N bestemt ved

$$x\,R_N\,y \overset{DEF}{\iff} y - x \in N,$$

og at denne relation altid er harmonisk. De øvrige betingelser har udseendet:

(2) R_N er refleksiv $\iff 0 \in N$.
(3) R_N er irrefleksiv $\iff 0 \notin N$.
(4) R_N er symmetrisk $\iff -N \subseteq N$.
(5) R_N er asymmetrisk $\iff N \cap (-N) \subseteq \{0\}$.
(6) R_N er transitiv $\iff N + N \subseteq N$.
(7) R_N er total $\iff G = \{0\} \cup N \cup (-N)$.

Tilføjelse. Er der i den kommutative gruppe $(G, +)$ givet endnu en komposition $*$, der er distributiv mht. $+$, gælder:

(8) R_N harmonerer med $* \iff a * N \subseteq N$ for alle $a \in G$.

Bevis. Som de foregående. Det er nødvendigt at udnytte, at

$$a * 0 = 0 * a = 0, \quad a * (-x) = -(a * x), \quad (-x) * a = -(x * a)\,♡$$

5. Harmoniske ordninger.

(5.1) DEFINITION. En *ordnet gruppe* $(G, \cdot, <)$ er en mængde G forsynet med en komposition $\cdot$ og en relation $<$ således at

(1) $(G, \cdot)$ er en gruppe.
(2) $(G, <)$ er en totalt, irrefleksivt ordnet mængde.
(3) Relationen $<$ harmonerer med kompositionen $\cdot$.

Den sidste betingelse udsiger, at der for alle $x, y, a \in G$ gælder:

$$x < y \implies xa < ya \wedge ax < ay\,.$$

Vi vil her udelukkende beskæftige os med kommutative (additivt skrevne) ordnede grupper $(G, +, <)$. For en sådan udsiger betingelsen (3), at

$$x < y \implies x + a < y + a.$$

Af transitiviteten følger, at vi kan "addere uligheder":

$$x \leq y \wedge a \leq b \implies x + a \leq y + b.$$

(5.2) DEFINITION. Et element a i en kommutativ, ordnet gruppe $(G, +, <)$ kaldes *positivt*, hvis $0 < a$. Delmængden bestående af positive elementer betegnes

$$G_+ := \{a \in G \mid 0 < a\}.$$

Vi har øjensynlig

$$x < y \iff y - x \in G_+.$$

Af betingelserne (3), (6) og (7) i Sætning (4.2) følger, at vi har $0 \notin G_+$, at G_+ er stabil og at der for hvert element $x \neq 0$ i G gælder, at $x \in G_+$ eller $-x \in G_+$. Endvidere følger det, at vi omvendt har:

SÆTNING. *Lad $(G, +)$ være en kommutativ gruppe, og lad $P \subseteq G$ være en stabil delmængde, således at $0 \notin P$ og således at der for hvert element $x \neq 0$ i G gælder, at $x \in P$ eller $-x \in P$. Da defineres ved*

$$x < y \overset{DEF}{\iff} y - x \in P$$

en relation $<$ i G således at $(G, +, <)$ er en ordnet gruppe.

bevis. ♠

(5.3) DEFINITION. Lad a være element i en kommutativ ordnet gruppe $(G, +, <)$. Ved *absolutværdien* af a, betegnet $|a|$, forstås det største af elementerne a og $-a$.

Vi har:

$$|a| \geq 0, \quad \text{med "=" kun når } a = 0.$$
$$|-a| = |a|.$$
$$|a+b| \leq |a| + |b|. \quad \text{(Trekantsuligheden).}$$

Af ulighederne $\left.\begin{matrix} a \\ -a \end{matrix}\right\} \leq |a|$ og $\left.\begin{matrix} b \\ -b \end{matrix}\right\} \leq |b|$ fås nemlig ved addition, at $\left.\begin{matrix} a+b \\ -a-b \end{matrix}\right\} \leq |a|+|b|$, og det er netop trekantsuligheden.

Heraf følger let, at

$$||a| - |b|| \leq |a - b|.$$

(5.4) DEFINITION. En *ordnet ring* $(\Lambda, +, \cdot, <)$ er en mængde Λ med to kompositioner $+$ og $\cdot$ og en relation $<$ således at

(1) $(\Lambda, +, \cdot)$ er en ring.
(2) $(\Lambda, <)$ er en totalt, irrefleksivt ordnet mængde.
(3) Relationen $<$ harmonerer med additionen $+$ og med multiplikation med positive elementer.

Den sidste betingelse udsiger, at der for alle $x, y, a \in \Lambda$ gælder:

$$x < y \implies x + a < y + a$$
$$x < y \wedge 0 < a \implies xa < ya \wedge ax < ay\,.$$

Da $(\Lambda, +, <)$ specielt er en ordnet gruppe, følger af det foregående, at delmængden

$$\Lambda_+ := \{a \in \Lambda \mid 0 < a\}$$

bestående af *positive* elementer i Λ bestemmer ordningen, idet

$$x < y \iff y - x \in \Lambda_+\,,$$

og at Λ_+ mht. addition har egenskaberne nævnt i (5.2). Yderligere er Λ_+ stabil under multiplikation, thi af $0 < a$ og $0 < b$ følger $0 = a \cdot 0 < ab$. Omvendt har vi:

SÆTNING. *Lad $(\Lambda, +, \cdot)$ være en ring, og lad $P \subseteq \Lambda$ være en stabil (mht. $+$ **og** $\cdot$) delmængde, således at $0 \notin P$ og således at der for hvert $x \neq 0$ i Λ gælder, at $x \in P$ eller $-x \in P$. Da defineres ved*

$$x < y \overset{DEF}{\iff} y - x \in P$$

en relation $<$ i Λ således at $(\Lambda, +, \cdot, <)$ er en ordnet ring med $\Lambda_+ = P$.

Bevis. Det skal blot vises, at relationen harmonerer med multiplikation med positive elementer, og det følger let af, at P er stabil under multiplikation ♡

OBSERVATION. For absolutværdien gælder, at $|xy| = |x||y|$. Endvidere er $0_\Lambda < 1_\Lambda$ (med mindre Λ er nulringen).

6. Kongruensrelation og kvotient.

(6.1) DEFINITION. Lad $(M, *)$ være en mængde med en komposition. En ækvivalensrelation $\sim$ i M, der harmonerer med kompositionen $*$, kaldes også en *kongruensrelation* i $(M, *)$. En relation $\sim$ i M er altså en kongruensrelation, hvis den er refleksiv, symmetrisk og transitiv, samt opfylder:

$$x' \sim x \ \wedge \ y' \sim y \implies x' * y' \sim x * y\,.$$

Er $\sim$ en kongruensrelation i $(M, *)$, kan vi i kvotientmængden $M/\!\sim$ definere en komposition $\tilde{*}$ på følgende måde: Lad X og Y være ækvivalensklasser, og vælg en repræsentant x for X og en repræsentant y for Y. *Kompositet* $X\tilde{*}Y$ af ækvivalensklasserne X og Y er da ækvivalensklassen

$$X\tilde{*}Y := \boxed{x * y}\,,$$

der indeholder kompositet af repræsentanterne. At dette er **veldefineret**, altså at ækvivalensklassen $\boxed{x * y}$ ikke afhænger af de foretagne vælg, følger af betingelsen ovenfor.

Den således definerede komposition $\tilde{*}$ i kvotientmængden kaldes den *inducerede komposition*. Den betegnes sædvanligvis med samme symbol som den givne komposition i M. Kvotientmængden $M/\!\sim$ med den inducerede komposition $*$ kaldes også *kvotienten* af $(M, *)$, og skrives

$$(M/\!\sim, *) = (M, *)/\!\sim.$$

(6.2) Er $\sim$ en kongruensrelation i $(M, *)$, følger det af definitionen på den inducerede komposition, at vi for alle $x, y \in M$ har

$$\boxed{x * y} = \boxed{x} * \boxed{y}\,.$$

Dette betyder imidlertid, at den kanoniske afbildning $x \mapsto \boxed{x}$ er en homomorfi

$$\boxed{\ }\colon (M, *) \to (M/\!\sim, *)\,.$$

Den kaldes også den *kanoniske homomorfi*.

OBSERVATION. Da den kanoniske homomorfi

$$\boxed{\ }\colon (M, *) \to (M/\!\sim, *)$$

er en surjektiv homomorfi, vil en lang række egenskaber ved $(M,*)$ nedarves til kvotienten $(M/\!\sim,*)$. Som eksempler på sådanne egenskaber kan nævnes kommutativitet, associativitet, eksistens af neutralt element og eksistens af inverst element.

Lad os f.eks. vise, at associativitet nedarves: Lad X, Y og Z være elementer i kvotienten, og vælg repræsentanter: $X = \boxed{x}$, $Y = \boxed{y}$, $Z = \boxed{z}$. Under brug af definitionen på kompositionen i kvotientmængden finder vi så:

$$(X * Y) * Z = \boxed{x * y} * Z = \boxed{(x * y) * z} \qquad \text{og}$$
$$X * (Y * Z) = X * \boxed{y * z} = \boxed{x * (y * z)}.$$

Af $(x * y) * z = x * (y * z)$ følger derfor, at

$$(X * Y) * Z = X * (Y * Z)$$

som påstået.

(6.3) Udvidelsessætning for mængder med komposition. *Lad $\sim$ være en kongruensrelation i $(M,*)$, og lad $\square : (M,*) \to (M/\!\sim,*)$ være den kanoniske homomorfi ind i kvotienten. Enhver homomorfi $f : (M,*) \to (P,*)$, som respekterer relationen $\sim$, kan entydigt udvides til en homomorfi $\bar{f} : (M/\!\sim,*) \to (P,*)$ fra kvotienten. I diagramform:*

$$\bar{f} \circ \square = f\,.$$

$$\begin{array}{ccc} (M,*) & \xrightarrow{\ \square\ } & (M/\!\sim,*) \\ {\scriptstyle f}\big\downarrow & \swarrow & \\ (P,*) & & \end{array}$$

Bevis. Ifølge Udvidelsessætning (3.10) skal det blot vises, at den inducerede afbildning $\bar{f} : M/\!\sim \to P$ er en homomorfi, og det følger let af definitionerne ♡

(6.4) For en homomorfi $f : (M,*) \to (P,*)$ kan vi, jfr. (3.11), betragte dels billedet $f(M)$, dels den til f hørende ækvivalensrelation

$$x' \underset{f}{\sim} x \overset{DEF}{\iff} f(x') = f(x).$$

Isomorfisætning for mængder med komposition. *Lad $f : (M,*) \to (P,*)$ være en homomorfi. Da er billedet $f(M)$ en stabil delmængde i $(P,*)$, og relationen $\underset{f}{\sim}$ er en kongruensrelation i $(M,*)$. Den inducerede homomorfi er en isomorfi*

$$\bar{f} : (M/\underset{f}{\sim},*) \xrightarrow{\ \sim\ } (f(M),*)$$

af kvotienten på billedet.

Bevis. Følger af Isomorfisætning (3.11) ♡

BEMÆRKNING. Homomorfien f er således en sammensætning $f = \iota \circ \bar{f} \circ \square$ af en surjektiv homomorfi $\square : M \to M/\underset{f}{\sim}$, en isomorfi $\bar{f} : M/\underset{f}{\sim} \xrightarrow{\sim} f(M)$, og den injektive inklusionshomomorfi $\iota : f(M) \hookrightarrow P$.

(6.5) DEFINITION. Lad $(G, \cdot)$ være en gruppe. En *normal undergruppe* N i G er da en undergruppe N, således at $aNa^{-1} \subseteq N$ for alle $a \in G$.

SÆTNING. *Lad $(G, \cdot)$ være en gruppe. Kongruensrelationerne i $(G, \cdot)$ er da netop relationerne $\underset{N}{\equiv}$ definerede ved*

$$x \underset{N}{\equiv} y \overset{DEF}{\iff} x^{-1}y \in N,$$

hvor $N \subseteq G$ er en normal undergruppe.

Bevis. Af (4.2) følger, at relationerne i $(G, \cdot)$, der harmonerer med venstremultiplikation, netop er relationerne R_N definerede ved

$$x \, R_N \, y \overset{DEF}{\iff} x^{-1} \in N,$$

hvor $N \subseteq G$ er en delmængde. Af betingelserne (1), (2), (4) og (6) i Sætning (4.2) aflæses umiddelbart, at R_N er en kongruensrelation i $(G, \cdot)$, netop når delmængden N er en normal undergruppe i G ♠

(6.6) DEFINITION. Lad N være en normal undergruppe i en gruppe $(G, \cdot)$. Kongruensrelationen $\underset{N}{\equiv}$ defineret ovenfor kaldes da *kongruens modulo N*. Da den kanoniske homomorfi $\square : (G, \cdot) \to (G/\underset{N}{\equiv}, \cdot)$ er surjektiv, følger det let, at kvotienten med den inducerede komposition $\cdot$ igen er en gruppe. Den kaldes *kvotientgruppen* af G mht. N og betegnes G/N.

Elementerne i kvotienten G/N er ækvivalensklasserne ved $\underset{N}{\equiv}$. Det er øjensynlig delmængderne i G af formen

$$xN, \quad \text{hvor } x \in G\,.$$

De kaldes også *sideklasser modulo N*. Det neutrale element i kvotienten G/N er sideklassen $eN = N$.

(6.7) DEFINITION. For en gruppehomomorfi $f : (G, \cdot) \to (H, \cdot)$ gælder som bekendt, at $f(e_G) = e_H$ og at $f(x^{-1}) = f(x)^{-1}$ for alle x i G. Det følger let, at en gruppehomomorfi $f : (G, \cdot) \to (H, \cdot)$ respekterer relationen $\underset{N}{\equiv}$, netop når

$$f(z) = e_H \quad \text{for alle} \quad z \in N\,.$$

Er dette opfyldt, siges homomorfien f at *forsvinde på* N.

Af Udvidelsessætning (6.3) får vi nu – med de nye betegnelser – følgende:

UDVIDELSESSÆTNING FOR GRUPPER. *Lad N være en normal undergruppe i en gruppe $(G,\cdot)$, og lad $\square : (G,\cdot) \to (G/N,\cdot)$ være den kanoniske homomorfi ind i kvotienten. Enhver gruppehomomorfi $f : (G,\cdot) \to (H,\cdot)$, der forsvinder på N, kan da entydigt udvides til en homomorfi $\bar{f} : (G/N,\cdot) \to (H,\cdot)$ fra kvotienten.*

Bevis. ♠

(6.8) DEFINITION. For en gruppehomomorfi $f : (G,\cdot) \to (H,\cdot)$ defineres *kernen* som originalmængden

$$f^{-1}(e_H) = \{z \in G \mid f(z) = e_H\}$$

til det neutrale element e_H i H. Det er klart, at homomorfien f forsvinder på sin kerne.

ISOMORFISÆTNING FOR GRUPPER. *Lad $f : (G,\cdot) \to (H,\cdot)$ være en gruppehomomorfi. Da er billedet $f(G)$ en undergruppe i $(H,\cdot)$ og kernen $f^{-1}(e_H)$ er en normal undergruppe i $(G,\cdot)$. Den inducerede homomorfi fra kvotienten er en isomorfi $\bar{f} : (G/f^{-1}(e_H),\cdot) \xrightarrow{\sim} (f(G),\cdot)$ af kvotienten på billedet.*

Bevis. Vi har $e_H = f(e_G)$ og $f(x)^{-1} = f(x^{-1})$ for alle $x \in G$. Heraf følger let, at den stabile delmængde $f(G)$ er en undergruppe i H. For den til f hørende ækvivalensrelation $\underset{f}{\sim}$, jfr. (6.4), har vi nu

$$e_G \underset{f}{\sim} z \iff f(e_G) = z \iff z \in f^{-1}(e_H)\,.$$

Da $\underset{f}{\sim}$ er en kongruensrelation, er $f^{-1}(e_H)$ følgelig en normal undergruppe [Dette kan naturligvis også let vises direkte] og $\underset{f}{\sim}$ er relationen "kongruens modulo $f^{-1}(e_H)$". Den sidste påstand følger nu af Isomorfisætning (6.4) ♠

BEMÆRKNING. Homomorfien f er således en sammensætning $f = \iota \circ \bar{f} \circ \square$ af en surjektiv homomorfi $\square$, en isomorfi $\bar{f}$ og en injektiv homomorfi ι.

OBSERVATION. En gruppehomomorfi $f : (G,\cdot) \to (H,\cdot)$ er injektiv, netop når kernen $f^{-1}(e_H)$ kun består af det neutrale element e_G i G,

thi vi har

$$f(x) = f(y) \iff x^{-1}y \in f^{-1}(e_H)\,.$$

NOTATION. Vi fremhæver, at i en kommutativ, additivt skrevet gruppe $(G,+)$ er alle undergrupper normale. Kongruensrelationerne i $(G,+)$ er netop relationerne af formen

$$x \underset{N}{\equiv} y \overset{DEF}{\iff} y - x \in N,$$

hvor $N \subseteq G$ er en undergruppe. Sideklasserne er her delmængderne af formen

$$x + N, \quad \text{med} \quad x \in G\,.$$

(6.9) DEFINITION. Lad $(M, \perp, *)$ være en mængde med to kompositioner $\perp$ og $*$. En ækvivalensrelation $\sim$, der harmonerer med begge kompositioner, siges også at være en *kongruensrelation* i $(M, \perp, *)$. Kompositionerne $\perp$ og $*$ inducerer da i kvotientmængden $M/\!\sim$ kompositioner betegnet $\tilde{\perp}$ og $\tilde{*}$, og den kanoniske afbildning $x \mapsto \boxed{x}$ er en surjektiv homomorfi

$$\boxed{} : (M, \perp, *) \to (M/\!\sim, \tilde{\perp}, \tilde{*})\,.$$

Vi får øjensynlig en UDVIDELSESSÆTNING og en ISOMORFISÆTNING for mængder med to kompositioner ved at anvende de tilsvarende sætninger (6.3) og (6.4) på hver af de to kompositioner.

(6.10) DEFINITION. Lad $(\Lambda, +, \cdot)$ være en ring. Ved et *ideal* i Λ forstås en delmængde $\mathcal{A} \subseteq \Lambda$, der er en undergruppe i den additive gruppe $(\Lambda, +)$ og således, at $\lambda \cdot \mathcal{A} \subseteq \mathcal{A}$ og $\mathcal{A} \cdot \lambda \subseteq \mathcal{A}$ for alle $\lambda \in \Lambda$.

SÆTNING. *Lad $(\Lambda, +, \cdot)$ være en ring. Kongruensrelationerne i $(\Lambda, +, \cdot)$ er da netop relationerne*

$$x \underset{\mathcal{A}}{\equiv} y \overset{DEF}{\iff} y - x \in \mathcal{A},$$

hvor $\mathcal{A} \subseteq \Lambda$ er et ideal.

Bevis. Ganske som beviset for Sætning (6.5), idet også (4.2)(8) inddrages ♡

(6.11) DEFINITION. Lad $\mathcal{A}$ være et ideal i en ring $(\Lambda, +, \cdot)$. Kongruensrelationen $\underset{\mathcal{A}}{\equiv}$ defineret ovenfor kaldes da *kongruens modulo $\mathcal{A}$*. Da den kanoniske afbildning er en surjektiv homomorfi $\boxed{} : (\Lambda, +, \cdot) \to (\Lambda/\underset{\mathcal{A}}{\equiv}, +, \cdot)$, følger det let, at kvotienten, med de inducerede kompositioner $+$ og $\cdot$, igen er en ring. Den kaldes *kvotientringen* af Λ mht. idealet $\mathcal{A}$ og betegnes $\Lambda/\mathcal{A}$.

Elementerne i kvotienten $\Lambda/\mathcal{A}$ er ækvivalensklasser ved relationen $\underset{\mathcal{A}}{\equiv}$, dvs. delmængderne af Λ af formen

$$\lambda + \mathcal{A}, \quad \text{med} \quad \lambda \in \Lambda\,.$$

De kaldes også *sideklasser modulo $\mathcal{A}$*. Nul-elementet og et-elementet i kvotienten $\Lambda/\mathcal{A}$ er sideklasserne

$$0 + \mathcal{A} = \mathcal{A} \qquad \text{og} \qquad 1 + \mathcal{A}\,.$$

(6.12) Idet en ringhomomorfi $f : (\Lambda, +, \cdot) \to (\Gamma, +, \cdot)$ siges at *forsvinde* på delmængden $\mathcal{A} \subseteq \Lambda$, hvis

$$f(x) = 0 \quad \text{for alle} \quad x \in \mathcal{A}\,,$$

får vi følgende:

UDVIDELSESSÆTNING FOR RINGE. *Lad $\mathcal{A}$ være et ideal i en ring $(\Lambda, +, \cdot)$, og lad $\square : (\Lambda, +, \cdot) \to (\Lambda/\mathcal{A}, +, \cdot)$ være den kanoniske homomorfi ind i kvotienten. Enhver ringhomomorfi $f : (\Lambda, +, \cdot) \to (\Gamma, +, \cdot)$, der forsvinder på $\mathcal{A}$, kan da entydigt udvides til en homomorfi $\bar{f} : (\Lambda/\mathcal{A}, +, \cdot) \to (\Gamma, +, \cdot)$ fra kvotienten.*

Bevis. Ganske som beviset for Udvidelsessætning for grupper ♠

(6.13) DEFINITION. For en ringhomomorfi $f : (\Lambda, +, \cdot) \to (\Gamma, +, \cdot)$ defineres *kernen* som originalmængden $f^{-1}(0)$ af nul-elementet i Γ.

ISOMORFISÆTNING FOR RINGE. *Lad $f : (\Lambda, +, \cdot) \to (\Gamma, +, \cdot)$ være en ringhomomorfi. Da er billedet $f(\Lambda)$ en delring i $(\Gamma, +, \cdot)$ og kernen $f^{-1}(0)$ er et ideal i Λ. Den inducerede homomorfi fra kvotienten er en isomorfi $\bar{f} : (\Lambda/f^{-1}(0), +, \cdot) \xrightarrow{\sim} (f(\Lambda), +, \cdot)$ af kvotienten på billedet.*

Bevis. Ganske som beviset for Isomorfisætning for grupper (6.8) ♡

GRUPPER

1. Gruppebegrebet.

(1.1) DEFINITION. En *gruppe* $(G, \cdot)$ er en mængde G med en komposition : $G \times G \to G$, betegnet $(x, y) \mapsto x \cdot y$, der er associativ, har et neutralt element og opfylder, at hvert element i G er invertibelt. Betegnes det *neutrale element* e, og det til elementet $x \in G$ hørende *inverse* x^{-1}, kan betingelserne udtrykkes ved ligningerne:

$$\begin{aligned} (x \cdot y) \cdot z &= x \cdot (y \cdot z) \\ e \cdot x = x \cdot e &= x \qquad \text{for alle } x, y, z \in G \\ x^{-1} \cdot x = x \cdot x^{-1} &= e \end{aligned}$$

En gruppe $(G, \cdot)$ kaldes *kommutativ* eller *abelsk*, hvis kompositionen er kommutativ, dvs. hvis

$$x \cdot y = y \cdot x \quad \text{for alle } x, y \in G.$$

Elementantallet i en gruppe kaldes også gruppens *orden*.

(1.2) NOTATION. Som betegnelse for en komposition i en gruppe kan anvendes ethvert bekvemt symbol. Det er sædvane i betegnelserne ikke at skelne parret bestående af mængden og kompositionen fra mængden. Man taler således om gruppen G, idet det så er underforstået hvilken komposition i mængden G, der er tale om.

I ovenstående definitioner er kompositionen skrevet *multiplikativt*, dvs. at kompositionstegnet er en '$\cdot$', som vi endda oftest udelader i det følgende. Det neutrale element i gruppen G kan så betegnes e_G eller blot e eller eventuelt 1. En kommutativ gruppe kan skrives *additivt*, dvs. at kompositionen betegnes $(x, y) \mapsto x + y$. Det neutrale element betegnes i så fald 0, og det inverse til x betegnes $-x$ og kaldes det *modsatte* til x.

EKSEMPEL. De hele tal udgør en kommutativ gruppe $(\mathbf{Z}, +)$.

(1.3) DEFINITION. En afbildning $f : H \to G$ mellem grupper $(H, \cdot)$ og $(G, \cdot)$ kaldes en *(gruppe-) homomorfi*, hvis

$$f(xy) = f(x)f(y), \quad \text{for alle } x, y \in H.$$

Heraf følger let, at der så gælder

$$f(e_H) = e_G \ \text{ og } \ f(x^{-1}) = f(x)^{-1}, \quad \text{for alle } x \in H.$$

Ved *kernen* for en gruppehomomorfi $f : H \to G$ forstås originalmængden $f^{-1}(e_G)$. Det er let at se, at f er injektiv, netop når kernen er $f^{-1}(e_G) = \{e_H\}$.

Det er klart, at sammensætning af homomorfier $f : H \to G$ og $g : K \to H$ er en homomorfi $f \circ g : K \to G$, og at den identiske afbildning $x \mapsto x$ er en gruppehomomorfi $Id_G : G \to G$.

En bijektiv homomorfi $f : H \to G$ kaldes også en *isomorfi* (og ofte skriver vi herfor $f : H \xrightarrow{\sim} G$). For en sådan er også den inverse afbildning en isomorfi $f^{-1} : G \xrightarrow{\sim} H$.

En homomorfi $f : G \to G$ kaldes en *endomorfi* i G, og hvis den er bijektiv også en *automorfi*.

(1.4) Definition. Ved en *undergruppe* i en gruppe G forstås en delmængde $H \subseteq G$, som er stabil og med sin inducerede komposition selv er en gruppe. Det følger, at inklusionsafbildningen $x \mapsto x,\ x \in H$, så er en homomorfi : $H \to G$.

De *trivielle undergrupper* i G er delmængderne $\{e\}$ og G.

Observation. En delmængde $H \subseteq G$ er en undergruppe, netop når

$$\begin{aligned} x, y \in H &\Rightarrow xy \in H, \\ e \in H &\qquad \text{og} \\ x \in H &\Rightarrow x^{-1} \in H. \end{aligned}$$

For gruppen $(\mathbf{Z}, +)$ gælder som bekendt den såkaldte:

Hovedidealsætning. *Undergrupperne i* $(\mathbf{Z}, +)$ *er netop delmængderne af formen*

$$H = \mathbf{Z}n = \{pn \mid p \in \mathbf{Z}\},\ \textit{hvor } n \geq 0.$$

Tallet n *er entydigt bestemt ved undergruppen* H*, nemlig som* $n = 0$*, hvis* $H = \{0\}$*, og* $n =$ *mindste positive tal i* H*, hvis* $H \neq \{0\}$♠

(1.5) Definition. Lad H være en undergruppe i gruppen G. Den ved

$$x \sim y \overset{\text{DEF}}{\iff} x^{-1}y \in H$$

definerede relation $\sim$ i G ses da let at være en ækvivalensrelation. Den kaldes *venstreækvivalens modulo* H. Ækvivalensklasserne kaldes *(venstre-) sideklasser* modulo H, og antallet af sideklasser kaldes undergruppens *index* i G og betegnes $|G{:}H|$. Den tilhørende kvotientmængde, dvs. mængden af sideklasser, betegnes G/H. Antallet af elementer i G/H er altså

$$|G/H| = |G{:}H|.$$

Sideklassen, der indeholder et givet element $a \in G$, er øjensynlig delmængden

$$aH := \{ah \mid h \in H\}.$$

Da $x \mapsto ax$ definerer en bijektiv afbildning : $H \to aH$ (med den inverse afbildning $y \mapsto a^{-1}y$), har alle sideklasser samme elementantal som H. Da sideklasserne udgør en klassedeling af G med $|G : H|$ klasser, får vi derfor umiddelbart:

LAGRANGE'S INDEX–SÆTNING. *For en undergruppe H i en gruppe G gælder:*

$$|G| = |G{:}H| \cdot |H| \spadesuit$$

BEMÆRKNING. For en undergruppe H i G kan vi analogt ved

$$x \underset{\text{h}}{\sim} y \overset{\text{DEF}}{\iff} yx^{-1} \in H$$

definere *højreækvivalens* modulo H, og tilsvarende *højresideklasser* af formen

$$Ha := \{ha \mid h \in H\}, \quad a \in G$$

[Huskeregel: $H\text{ø}$ er en **Høj**re-sideklasse]. Mængden af højresideklasser betegnes $H\backslash G$. For en højresideklasse $X \subseteq G$ er mængden $X^{-1} := \{x^{-1} \mid x \in X\}$ en venstresideklasse. Det følger, at $X \mapsto X^{-1}$ er en bijektiv afbildning : $H\backslash G \tilde{\to} G/H$. Vi har altså specielt

$$|H\backslash G| = |G/H| = |G{:}H|.$$

(1.6) DEFINITION. Ved en *normal undergruppe* i en gruppe G forstås en undergruppe $N \subseteq G$, således at der for alle $a \in G$ gælder:

$$aNa^{-1} \subseteq N.$$

OBSERVATION. De trivielle undergrupper er normale. I en kommutativ gruppe er alle undergrupper normale.

Hvis undergruppen $N \subseteq G$ er normal, er det let at se, at venstre- og højreækvivalens er samme ækvivalensrelation. Den kaldes også *kongruens modulo N* og den betegnes $\underset{N}{\equiv}$. I denne situation kan vi i mængden G/N af sideklasser definere en komposition på følgende måde: Lad X og Y være sideklasser, og vælg repræsentanter: x for X og y for Y, altså

$$X = \boxed{x}, \quad Y = \boxed{y}, \qquad \text{og sæt}$$
$$X \cdot Y := \boxed{x \cdot y}.$$

Som sædvanlig betegner $\boxed{z}$ ækvivalensklassen, der indeholder z.

Det er let at vise, at ækvivalensklassen på højresiden ikke afhænger af de foretagne valg af repræsentanter, og at vi derfor får en veldefineret komposition i mængden

G/N. Da den *kanoniske* afbildning $x \mapsto \boxed{x}$ øjensynlig er en surjektiv homomorfi $: (G, \cdot) \to (G/N, \cdot)$, følger det let, at $(G/N, \cdot)$ er en gruppe. Den kaldes også *kvotientgruppen* af G mht. den normale undergruppe N.

Følgende sætninger om grupper følger let af de tilsvarende sætninger om mængder:

UDVIDELSESSÆTNING. *Lad $N \subseteq G$ være en normal undergruppe. En gruppehomomorfi $f : G \to K$, der forsvinder på N (dvs. opfylder: $x \in N \Rightarrow f(x) = e_K$), kan da entydigt udvides til en homomorfi $\bar{f} : G/N \to K$ fra kvotienten* ♡

Homomorfien $\bar{f}$ siges at være *induceret* af f.

ISOMORFISÆTNING. *Lad $f : G \to K$ være en gruppehomomorfi. Da er kernen $f^{-1}(e_K)$ en normal undergruppe i G, billedet $f(G)$ er en undergruppe i K og f inducerer en isomorfi $\bar{f} : G/f^{-1}(e_K) \tilde{\to} f(G)$ af kvotienten på billedet* ♡

(1.7) Til et element a i en gruppe G kan vi betragte potenserne a^p, $p \in \mathbf{Z}$. Ifølge første potensregel er afbildningen $: p \mapsto a^p$ en gruppehomomorfi $: (\mathbf{Z}, +) \to (G, \cdot)$.

DEFINITION. Billedet ved homomorfien $: p \mapsto a^p$ kaldes *undergruppen frembragt af* a og betegnes $\langle a \rangle$, altså

$$\langle a \rangle := \{ \ldots, a^{-2}, a^{-1}, e, a, a^2, \ldots \}.$$

Det er øjensynlig den mindste undergruppe, som indeholder a. Kernen for denne homomorfi er en undergruppe i $\mathbf{Z}$, altså ifølge Sætning (1.4) af formen $\mathbf{Z}n$, hvor $n \geq 0$ er entydigt bestemt.

Hvis $n > 0$, siges elementet $a \in G$ at have *orden* n. Hvis $n = 0$, siges elementet $a \in G$ at *have uendelig orden.*

Af beskrivelsen i Sætning (1.4) og af Isomorfisætning (1.6) fås nu umiddelbart følgende:

RESULTAT. *Elementet $a \in G$ har uendelig orden, netop når*

$$a^m \neq e \text{ for alle } m \in \mathbf{N}.$$

I bekræftende fald er $p \mapsto a^p$ en injektiv homomorfi, og $\langle a \rangle$ er isomorf med $\mathbf{Z}$. Specielt har $\langle a \rangle$ uendelig orden.

Elementet $a \in G$ har orden n, netop når n er det mindste tal, så at $a^n = e$. I bekræftende fald er $\langle a \rangle$ isomorf med kvotientgruppen $\mathbf{Z}/\mathbf{Z}n$. Specielt har $\langle a \rangle$ orden $|\mathbf{Z}/n\mathbf{Z}| = n$ og

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}.$$

OBSERVATION. Undergruppen $\langle a \rangle$ har samme orden som elementet a.

KOROLLAR TIL LAGRANGE'S INDEX-SÆTNING. *Et element a i en endelig gruppe G har en orden, som er divisor i G's orden, og der gælder $a^{|G|} = e$.*

Bevis. Er n ordenen af a, har vi $|\langle a\rangle| = n$. Sættes $d = |G{:}\langle a\rangle|$ har vi derfor $|G| = |G{:}\langle a\rangle| \cdot |\langle a\rangle| = dn$, så n er divisor i $|G|$. Videre er $a^{|G|} = a^{nd} = (a^n)^d = e^d = e$♠

(1.8) Definition. En gruppe $(G, \cdot)$ kaldes *cyklisk*, hvis der findes et element $a \in G$, så at $G = \langle a\rangle$. Et sådant element kaldes også en *frembringer* for G.

Observation. En gruppe $(G, \cdot)$ er cyklisk, netop hvis der findes en surjektiv homomorfi: $(\mathbf{Z}, +) \to (G, \cdot)$. De cykliske grupper er altså isomorfe med $\mathbf{Z}$ eller med $\mathbf{Z}/\mathbf{Z}n$, $n \geq 1$. Specielt er de kommutative.

Sætning. *Lad $(G, \cdot)$ være en cyklisk gruppe. Enhver undergruppe og enhver kvotientgruppe af G er da ligeledes cyklisk.*

Bevis. Lad $f : \mathbf{Z} \to G$ være en surjektiv homomorfi. For en kvotient G/N af G fås ved sammensætning : $\mathbf{Z} \to G \to G/N$ en surjektiv homomorfi, og så er G/N cyklisk. For en undergruppe H af G fås ved restriktion en homomorfi : $f^{-1}(H) \to H$, der er surjektiv, da f var surjektiv. Her er $f^{-1}(H) \subseteq \mathbf{Z}$ en undergruppe, og dermed af formen $f^{-1}(H) = \mathbf{Z}n$, og så er sammensætningen $p \mapsto pn \mapsto f(pn)$ en surjektiv homomorfi : $\mathbf{Z} \to \mathbf{Z}n = f^{-1}(H) \to H$♠

(1.9) Definition. I en gruppe $(G, \cdot)$ defineres en modsat komposition $\overset{op}{\cdot}$ ved

$$x \overset{op}{\cdot} y := y \cdot x.$$

Det er let at se, at $(G, \overset{op}{\cdot})$ igen er en gruppe. Den kaldes G's *modsatte gruppe* og betegnes G^{op}. Hvis G er kommutativ, er $G^{op} = G$.

En afbildning $f : H \to G$ mellem grupper H og G kaldes en *anti-homomorfi*, hvis $f(xy) = f(y)f(x)$. Det ses, at dette gælder, netop når f er en homomorfi : $H \to G^{op}$.

2. Permutationer.

(2.1) DEFINITION. Lad X være en mængde. En bijektiv afbildning $\sigma : X \to X$, af X ind i sig selv, kaldes en *automorfi* eller en *transformation* eller (især når X er endelig) en *permutation* i X. Med sammensætning som komposition udgør disse bijektive afbildninger en gruppe, kaldet den *fulde automorfi-* (eller *transformations-* eller *permutations-) gruppe* for X. Vi vil generelt betegne denne gruppe

$$Aut(X).$$

Vi vil ofte skrive kompositionen multiplikativt, og altså omtale sammensætning som produkt. Det neutrale element i $Aut(X)$ er den identiske afbildning $1_X = Id_X : x \mapsto x$.

For mængden $\{1, \ldots, n\}$ bruges også betegnelsen

$$S_n := Aut(\{1, \ldots, n\}).$$

Denne gruppe kaldes også den *symmetriske gruppe af grad n*. Den har øjensynlig orden

$$|S_n| = n!\,.$$

OBSERVATION. Lad $\varphi : X \to Y$ være en bijektiv afbildning. Den ved $\sigma \mapsto \varphi \circ \sigma \circ \varphi^{-1}$ definerede afbildning:

$$Aut(X) \to Aut(Y)$$

er da en bijektiv gruppehomomorfi, altså en isomorfi. Ækvipotente mængder har derfor isomorfe automorfigrupper. Specielt er automorfigruppen for en endelig mængde X isomorf med S_n, hvor $n = |X|$.

(2.2) DEFINITION. Lad σ være en permutation i X. Et element $x \in X$ kaldes *fixelement* for σ, hvis $\sigma(x) = x$. Mængden af fixelementer for σ betegnes X^σ. Permutationer σ og τ i X kaldes *disjunkte*, når $X^\sigma \cup X^\tau = X$, dvs. når komplementærmængderne $X \setminus X^\sigma$ og $X \setminus X^\tau$ er disjunkte.

OBSERVATION. Disjunkte permutationer σ og τ kommuterer, dvs. opfylder, at $\sigma\tau(x) = \tau\sigma(x)$ for alle $x \in X$.

Er nemlig $x \in X \setminus X^\sigma$, fås $\sigma(x) \in X \setminus X^\sigma$ (da σ er injektiv), og da $X \setminus X^\sigma \subseteq X^\tau$ får vi $\sigma\tau(x) = \sigma(x) = \tau\sigma(x)$. Tilsvarende følger påstanden, når $x \in X \setminus X^\tau$, og den er helt triviel, når $x \in X^\sigma \cap X^\tau$.

(2.3) DEFINITION. En permutation $\tau : X \to X$ kaldes en *p-cykel* eller en *cykel af længde p* (hvor $p \geq 2$), hvis der findes p forskellige elementer $x_1, \ldots, x_p \in X$, således at

$$\tau(x_1) = x_2, \quad \tau(x_2) = x_3, \ \ldots\ , \tau(x_{p-1}) = x_p, \quad \tau(x_p) = x_1 \quad \text{og}$$
$$\tau(x) = x, \text{ når } x \notin \{x_1, \ldots, x_p\}.$$

Delmængden $\{x_1, \ldots, x_p\} \subseteq X$ kaldes cyklens *bane*. Den består netop af de elementer, der ikke er fix-elementer for cyklen.

OBSERVATION. En p-cykel $\tau : X \to X$ har orden p i gruppen $Aut(X)$,

thi øjensynlig er $\tau^p = 1_X$, og da $\tau^i(x_1) = x_{1+i}, \quad 1 \leq i < p$ er $\tau^i \neq 1_X$ for $1 \leq i < p$.

NOTATION. Den ovenfor beskrevne p-cykel τ betegnes (hvis misforståelser er udelukket):

$$\tau =: (x_1, \ldots, x_p).$$

Bemærk, at ethvert element i banen kan optræde på førstepladsen, idet vi har

$$\tau = (x_1, x_2, \ldots, x_p) = (x_i, x_{i+1}, \ldots, x_p, x_1, \ldots, x_{i-1}).$$

En cykel af længde 2 kaldes også en *transposition*. En transposition $\tau = (x_1, x_2)$ ombytter altså x_1 og x_2 og "fixer" de øvrige elementer i X.

(2.4) CYKELSÆTNING. *Enhver permutation σ i en endelig mængde X kan skrives som en sammensætning af disjunkte cykler, og bortset fra rækkefølgen af faktorerne er fremstillingen entydig.*

BEMÆRKNING. Her medregnes fremstillingen af den identiske permutation som et "tomt produkt".

Bevis. Ved fuldstændig induktion efter elementantallet i mængden $B_\sigma := X \setminus X^\sigma$ vises, at σ kan skrives som et produkt af disjunkte cykler, hvis baner "udgør" B_σ.

Lad $x_1 \in B_\sigma$. Overvej, at der findes yderligere elementer $x_2, \ldots, x_p \in B_\sigma$, $p \geq 2$, så at $x_2 = \sigma(x_1), \ldots, x_p = \sigma(x_{p-1}), x_1 = \sigma(x_p)$. Overvej, at vi med p-cyklen $\tau := (x_1, \ldots, x_p)$ har

$$B_{\tau^{-1}\sigma} = B_\sigma \setminus \{x_1, \ldots, x_p\}.$$

Ifølge induktionsantagelsen kan $\tau^{-1}\sigma$ derfor skrives som et produkt $\tau_1 \cdots \tau_r$ af disjunkte cykler $\tau_1, \ldots, \tau_r$, der specielt også er disjunkte med τ, og så er

$$\sigma = \tau\tau_1 \cdots \tau_r$$

den ønskede fremstilling♡

(2.5) FORMLER. *For disjunkte cykler $(x_1, \ldots, x_p), (y_1, \ldots, y_q)$, og $a \notin \{x_1, x_2\}$ gælder:*

(1) $$(x_1, \ldots, x_p) = (x_1, x_p)(x_1, x_{p-1}) \cdots (x_1, x_2).$$

(2) $$(x_1, x_2) = (a, x_1)(a, x_2)(a, x_1).$$

(3) $$(x_1, x_i) = (x_1, x_{i-1})(x_{i-1}, x_i)(x_1, x_{i-1}), \quad 2 \leq i \leq p.$$

(4) $$(x_1, x_i)(x_1, \ldots, x_p) = (x_1, \ldots, x_{i-1})(x_i, \ldots, x_p), \quad 2 < i < p.$$

(5) $$(x_1, y_1)(x_1, \ldots, x_p)(y_1, \ldots, y_q) = (x_1, \ldots, x_p, y_1, \ldots, y_q).$$

Bevis. Sammensæt selv♡

BEMÆRKNING. Det er ofte hensigtsmæssigt for et givet element $x_1 \in X$ at lade (x_1) betegne den identiske permutation. I denne forstand er identiteten altså en 1-cykel. Overvej, at Formel (4) [resp.(5)] bevarer sin gyldighed i "grænsetilfældene" $2 = i$ og $i = p$ [resp. $p = 1$ eller $q = 1$].

SÆTNING. *Lad X være en endelig mængde. Da gælder:*

(1) *Enhver permutation σ i X kan fremstilles som en sammensætning af transpositioner.*
(2) *Er $a \in X$ et givet element, kan der i fremstillingen vælges transpositioner af formen (a, x), $x \in X \setminus \{a\}$.*
(3) *Er $X = \{x_1, \ldots, x_n\}$ en nummerering af elementerne i X, kan der i fremstillingen vælges transpositioner af formen (x_i, x_{i+1}), $i = 1, \ldots, n-1$ ("ombytning af naboer").*

Bevis. **(1)**: Ifølge Cykelsætning (2.4) er det nok at betragte en cykel, og for en sådan får vi fremstillingen af Formel (1).
(2): Ifølge (1) er det nok at betragte en transposition, og for en sådan får vi fremstillingen af Formel (2).
(3): Ifølge (2) er det nok at betragte en transposition af formen (x_1, x_i), og for en sådan får vi fremstillingen induktivt af Formel (3)♠

(2.6) DEFINITION. Lad σ være en permutation i den endelige mængde X, og lad os for hvert $p \in \mathbf{N}$ med $m_p = m_p(\sigma)$ betegne antallet af p-cykler, der forekommer i fremstillingen af σ som produkt af disjunkte cykler. Tallet

$$Z(\sigma) := \sum m_p(p-1)$$

vil vi kalde *transpositionstallet* for σ, og tallet

$$\operatorname{sign}(\sigma) := (-1)^{Z(\sigma)} \in \{1, -1\}$$

kaldes *fortegnet* for σ.

OBSERVATION 1. En permutation σ i en endelig mængde kan skrives som et produkt af $Z(\sigma)$ transpositioner,

thi $Z(\sigma)$ er netop antallet af transpositioner, der fremkommmer, når man i fremstillingen af σ som produkt af disjunkte cykler skriver hver p-cykel som produkt af $p-1$ transpositioner, jfr. Formel (2.5)(1).

BEMÆRKNING. Fremstillingen af en permutation σ som produkt af transpositioner er ikke entydig. Man kan vise, at $Z(\sigma)$ er det mindste antal transpositioner, der er nødvendige i en sådan fremstilling.

OBSERVATION 2. En p-cykel har fortegnet $(-1)^{p-1}$, thi transpositionstallet er $Z = p-1$.

(2.7) LEMMA. *For en permutation σ og en transposition τ i en endelig mængde X gælder:*

$$Z(\tau\sigma) = Z(\sigma) \pm 1.$$

Bevis. For at bestemme transpositionstallet for $\tau\sigma$ vil vi ud fra fremstillingen af σ som produkt af disjunkte cykler finde den tilsvarende fremstilling af $\tau\sigma$. Idet vi medregner σ's fixpunkter som 1-cykler, udgør banerne for σ's cykler en klassedeling af X. De to elementer, der ombyttes ved transpositionen τ ligger derfor enten i samme bane eller i hver sin bane, og det er klart, at de resterende cykler fra σ indgår uændret i fremstilling af $\tau\sigma$. Vi kan derfor dele op i følgende to tilfælde:
Tilfælde 1°: Vi kan antage, at $\sigma = (x_1, \ldots, x_p)$, $\tau = (x_1, x_i)$, $2 \leq i \leq p$. Formel (2.5)(4) giver da den ønskede fremstilling af $\tau\sigma$. Vi ser, at

$$Z(\tau\sigma) = (i-1-1) + (p-i) = (p-1) - 1 = Z(\sigma) - 1.$$

Tilfælde 2°: Vi kan antage, at $\sigma = (x_1, \ldots, x_p)(y_1, \ldots, y_q)$, $\tau = (x_1, y_1)$. Formel (2.5)(5) giver den ønskede fremstilling af $\tau\sigma$. Vi ser, at

$$Z(\tau\sigma) = p + q - 1 = (p-1) + (q-1) + 1 = Z(\sigma) + 1\spadesuit$$

SÆTNING. *For en endelig mængde X er fortegnet en gruppehomomorfi*

$$\text{sign} : Aut(X) \to (\{\pm 1\}, \cdot).$$

En transposition har fortegnet -1.

Bevis. Lad $\sigma, \tau \in Aut(X)$. Hvis τ er en transposition, får vi

$$\text{sign}(\tau\sigma) = (-1)^{Z(\tau\sigma)} = (-1)^{Z(\sigma)\pm 1} = (-1) \cdot (-1)^{Z(\sigma)} = (-1) \cdot \text{sign}(\sigma).$$

I det almindelige tilfælde kan τ skrives som produkt af $z = Z(\tau)$ transpositioner, så gentagen anvendelse af det viste giver

$$\text{sign}(\tau\sigma) = (-1)^z \text{sign}(\sigma) = \text{sign}(\tau) \cdot \text{sign}(\sigma).$$

Den sidste påstand er triviel, jfr. Observation 2 (2.6)♠

(2.8) DEFINITION. En permutation σ i den endelige mængde X kaldes *lige* eller *ulige* eftersom transpositionstallet $Z(\sigma)$ er lige eller ulige.

De lige permutationer er bestemt ved at de har fortegnet 1. De udgør derfor kernen for homomorfien sign : $Aut(X) \to (\{\pm 1\}, \cdot)$ og danner altså specielt en normal undergruppe i $Aut(X)$. Hvis X har mere end 1 element (således at der findes transpositioner i X), så er homomorfien sign : $Aut(X) \to \{\pm 1\}$ surjektiv. Undergruppen af lige permutationer har derfor index 2 i $Aut(X)$. Der er altså lige mange lige og ulige permutationer.

Hvis $X = \{1, \ldots, n\}$, således at $Aut(X) = S_n$ er den symmetriske gruppe af grad n, kaldes undergruppen af lige permutationer også den *alternerende gruppe af grad* n, og den betegnes A_n.

Hvis $n \geq 2$, har vi

$$|S_n : A_n| = 2, \quad S_n/A_n \xrightarrow{\sim} \{\pm 1\}, \quad |A_n| = \frac{1}{2}n!\,.$$

Er derimod $n = 1$, har vi $S_1 = A_1 = \{1\}$.

(2.9) Observation. Er en permutation σ fremstillet som en sammensætning af transpositioner, så er den lige elle ulige, eftersom antallet af faktorer er lige eller ulige,

thi er a antallet af faktorer, har vi $\text{sign}(\sigma) = (-1)^a$.

Sætning. *Lad X være en endelig mængde.*

(1) *Enhver lige permutation i X kan fremstilles som sammensætning af 3-cykler.*
(2) *Er $a, b \in X$ to givne elementer, kan der i fremstillingen vælges 3-cykler af formen $(a, b, x), x \in X \setminus \{a, b\}$.*
(3) *Er $X = \{x_1, \ldots, x_n\}$ en nummerering af elementerne i X, kan der i fremstillingen vælges 3-cykler af formen $(x_i, x_{i+1}, x_{i+2}), \quad i = 1, \ldots, n-2$ ("cykling af 3 naboer").*

Bevis. **(1):** Det er nok at betragte et produkt $\sigma = (x_1, x_2)(y_1, y_2)$ af 2 transpositioner. Er transpositionerne disjunkte, har vi

$$\sigma = (x_1, x_2)(y_1, y_2) = (x_1, x_2, y_1)(y_1, y_2, x_2).$$

Har de et eller to elementer fælles, må du selv prøve!
(2) og (3): Prøv selv. Du må gerne bruge Sætning (2.5)♡

3. Gruppevirkninger. Repræsentationer.

(3.1) DEFINITION. Lad $(G, \cdot)$ være en gruppe med det neutrale element 1, og lad X være en mængde. Ved en *virkning* af gruppen G på mængden X forstås en afbildning $: G \times X \to X$, betegnet $(g, x) \mapsto g.x$, således at der for alle $g, h \in G$ og $x \in X$ gælder:

$$(gh).x = g.(h.x)$$
$$1.x = x\,.$$

Er der givet en virkning af G på X siges G at *virke* som *transformationsgruppe* på X eller at *operere* på X.

(3.2) Er der givet en virkning af G på X kan vi for hvert element $g \in G$ betragte den ved

$$g_X : x \to g.x$$

definerede afbildning $g_X : X \to X$. Af betingelserne ovenfor følger, at afbildningen g_X er bijektiv, idet afbildningen $x \mapsto g^{-1}.x$ er den inverse. Vi har altså $g_X \in Aut(X)$. Videre følger det af betingelserne, at den ved $g \mapsto g_X$ bestemte afbildning:

$$G \to Aut(X)$$

er en homomorfi. Med den indførte notation er 1_X = billedet af den neutrale element = den identiske afbildning : $x \mapsto x$.

DEFINITION. Homomorfien $: G \to Aut(X)$ kaldes den til virkningen hørende *repræsentation* af gruppen G i mængden X. Ved denne "repræsenteres" altså gruppeelementet $g \in G$ ved automorfien $g_X : X \to X$. Hvis homomorfien $: G \to Aut(X)$ er injektiv, siges repræsentationen at være *tro.*

Har vi omvendt givet en gruppehomomorfi

$$\rho : G \to Aut(X),$$

ses det let, at der ved

$$g.x := \rho(g)(x)$$

defineres en virkning $: G \times X \to X$. Vi får således en bijektiv forbindelse mellem virkninger af G på X og repræsentationer $: G \to Aut(X)$.

EKSEMPEL. Den *trivielle* virkning af G på X er bestemt ved

$$g.x := x, \quad g \in Aut(G), x \in X.$$

Den tilhørende repræsentation er den identiske homomorfi:

$$Aut(X) \xrightarrow{=} Aut(X)$$

(3.3) DEFINITION. Lad der være givet en virkning : $G \times X \to X$ af G på X. For enhver undergruppe $H \subseteq G$ defineres da ved *restriktion* en virkning : $H \times X \to X$ af undergruppen H på X.

En delmængde $Y \subseteq X$ siges at være *stabil* (eller *invariant*) under virkningen, hvis der for alle $g \in G$ gælder:

$$y \in Y \Rightarrow g.y \in Y.$$

For en stabil delmængde $Y \subseteq X$ defineres ved *restriktion* en virkning : $G \times Y \to Y$ af G på delmængden Y.

(3.4) DEFINITION. Lad der være givet en virkning af G på X.

Det er let at se, at der ved

$$x' \underset{G}{\sim} x \quad \overset{\text{DEF}}{\Longleftrightarrow} \quad \exists g \in G : x' = g.x$$

defineres en ækvivalensrelation $\underset{G}{\sim}$ i mængden X. Ækvivalensklasserne herved kaldes *baner*. Banen, der indeholder x, er delmængden

$$G.x := \{g.x \mid g \in G\}.$$

En banes elementantal kaldes også dens *længde*. Mængden af baner, altså kvotientmængden $X/\underset{G}{\sim}$ kaldes *banerummet*, og betegnes

$$X/G := X/\underset{G}{\sim} \qquad \text{(læses: "}X \text{ modulo } G\text{")}.$$

For et element $x \in X$ er det let at se, at delmængden

$${}_xG := \{g \in G \mid g.x = x\}$$

er en undergruppe i G. Den kaldes *isotropigruppen* for x.

Et element $x \in X$ siges at være *fixpunkt for gruppeelementet* $g \in G$ eller at være *g-invariant*, hvis $g.x = x$. Ofte skrives

$$X^g := \{x \in X \mid g.x = x\}.$$

Et element $x \in X$ siges at være *G-invariant*, eller at være et *fixpunkt for virkningen* af gruppen G, hvis der for alle $g \in G$ gælder:

$$g.x = x.$$

Ækvivalent kan dette udtrykkes ved at banen $G.x$ kun består af ét element (dvs. er en såkaldt *et-punkts-bane*), eller ved at isotropigruppen ${}_xG$ er hele G. Mængden af fixpunkter for virkningen betegnes X^G, altså

$$X^G := \{x \in X \mid \forall g \in G : g.x = x\}.$$

BEMÆRKNING. Elementerne i banerummet er delmængder af X af formen $G.x$, med $x \in X$. Under visse omstændigheder er det mest naturligt at betegne banerummet $G\backslash X$ (kan læses: "X modulo G til venstre"). Det må imidlertid understreges, at ved alle de indførte betegnelser er det underforstået hvilken virkning, der er givet.

(3.5) DEFINITION. Lad der være givet en virkning af G på mængden X, og lad Y være endnu en mængde. En afbildning $\phi : X \to Y$ kaldes *G-invariant*, hvis

$$\phi(g.x) = \phi(x), \quad x \in X, g \in G.$$

Dette gælder øjensynlig netop når afbildningen $\phi : X \to Y$ respekterer ækvivalensrelationen $\underset{G}{\sim}$ i X. Af Udvidelsessætning for mængder fås derfor følgende:

UDVIDELSESSÆTNING. *En G-invariant afbildning $\phi : X \to Y$ kan entydigt udvides til en afbildning $\bar{\phi} : X/G \to Y$ fra banerummet*♠

BEMÆRKNING. Ved $(g.\phi)(x) := \phi(g^{-1}.x)$ defineres virkning $(g, \phi) \mapsto g.\phi$ af gruppen G på mængden $Afb(X, Y)$. Det er klart, at de G-invariante afbildninger $\phi : X \to Y$ netop er de elementer $\phi \in Afb(X, Y)$, der er fixelementer under denne virkning.

(3.6) TRANSLATION. For enhver gruppe $(G, \cdot)$ kan vi definere en virkning : $G \times G \to G$ af G på sig selv ved

$$g.x := gx, \quad g, x \in G.$$

Denne virkning kaldes *venstre-translation*. Der er kun en bane, og for hvert element $x \in G$ er isotropigruppen triviel. Den tilhørende repræsentation er tro : $G \to Aut(G)$. Gruppen G er derfor isomorf med en undergruppe i den fulde transformationsgruppe $Aut(G)$. Er gruppen endelig kaldes resultatet også:

CAYLEY'S SÆTNING. *En endelig gruppe G er isomorf med en undergruppe i den symmetriske gruppe S_n, hvor $n = |G|$*♠

Er $H \subseteq G$ en undergruppe, får vi ved restriktion en virkning : $H \times G \to G$. Banerne er her delmængderne

$$Hx = \{hx \mid h \in H\}, x \in G,$$

altså netop højre-sideklasserne modulo H, og betegnelsen $H\backslash G$ for banerummet, jfr. Bemærkning (3.4), harmonerer således med den tidligere indførte betegnelse for mængden af højre-sideklasser.

(3.7) KONJUGERING. For enhver gruppe $(G, \cdot)$ kan vi definere en virkning : $G \times G \to G$ af G på sig selv betegnet

$$(g, x) \longmapsto {}^g x := gxg^{-1}.$$

Denne virkning kaldes *konjugering*. Den til virkningen hørende ækvivalensrelation $\sim$, jfr. Definition (3.4), er bestemt ved

$$x' \sim x \quad \overset{\text{DEF}}{\Longleftrightarrow} \quad \exists g \in G : x' = gxg^{-1}.$$

Den kaldes også *"konjugeret med"*. Banerne kaldes *konjugeret-klasser* eller blot *klasser* i G. Bemærk, at automorfierne $x \mapsto {}^g x$ her er gruppeautomorfier af G. Klassen, der indeholder $x \in G$ er altså delmængden

$$\{gxg^{-1} \mid g \in G\}.$$

Isotropigruppen for $x \in G$ kaldes her *centralisatoren* for x og betegnes $C(x)$. Det er altså undergruppen

$$C(x) := \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}.$$

Et element $x \in G$ er fixpunkt under denne virkning, hvis $gxg^{-1} = x$ for alle $g \in G$, altså hvis

$$gx = xg, \quad \text{for alle} \quad g \in G,$$

dvs. hvis x kommuterer med alle elementer i G. Et sådant element kaldes også *centralt*, og mængden af centrale elementer kaldes gruppens *centrum* og betegnes $\mathrm{Cent}(G)$. Det er let at se, at centret $\mathrm{Cent}(G)$ er en undergruppe i G.

(3.8) Sætning. *Lad der være givet en virkning af gruppen G på mængden X, og et element $x \in X$. Den ved $g \mapsto g.x$ bestemte afbildning $: G \to X$ inducerer da en bijektiv afbildning:*

$$G/_x G \xrightarrow{\sim} G.x$$

af venstresideklasserne modulo isotropigruppen ${}_xG$ på banen $G.x$.

Bevis. Vi anvender Isomorfisætning for mængder på den ved $g \mapsto g.x$ definerede afbildning $: G \to X$. Billedmængden er øjensynlig netop $G.x$. Endvidere er:

$$g'.x = g.x \quad \Leftrightarrow \quad g^{-1}g'.x = x \quad \Leftrightarrow \quad g^{-1}g' \in {}_xG,$$

så den til afbildningen hørende ækvivalensrelation i G er venstreækvivalens modulo ${}_xG$, jfr. Definition (1.5). Heraf følger påstanden♠

Korrollar. *Længden af en bane $B \subseteq X$ er bestemt ved*

$$|B| = |G : {}_xG|, \quad x \in B,$$

altså ved index af isotropigruppen for et vilkårligt element x i banen.

Bevis. Når $x \in B$, er $|B| = |G.x| = |G/_x G| = |G : {}_xG|$♠

Når gruppen G er endelig, har altså specielt hver bane B en længde, der er divisor i gruppens orden.

(3.9) Tælleformlen. *Lad der være givet en virkning af gruppen G på mængden X. Da gælder:*

$$|X| = |X^G| + \sum_j |G : {}_{x_j}G| \,,$$

hvor $|X^G|$ er antallet af fixpunkter, og hvor der i summationen er valgt ét element x_j fra hver bane, der **ikke** *er en et-punkts-bane.*

Bevis. Da banerne udgør en klassedeling af X, kan elementantallet $|X|$ bestemmes som summen af banernes længder. Et-punkts-banerne bidrager her med $|X^G|$ 1-taller, og hver af de øvrige baner B_j bidrager med $|B_j| = |G : {}_{x_j}G|, \quad x_j \in B_j$♠

Eksempel. Tælleformlens vigtighed beror på, at tallene i $\sum_j$ er divisorer i G's orden, og > 1. Er der f.eks. givet en gruppe G, hvis orden er en primtalspotens:

$$|G| = p^r, \quad p \text{ primtal} \,,$$

og en virkning af G på en endelig mængde X, så er de enkelte led i $\sum_j$ potenser af p, og > 1, og altså specielt $\equiv 0 \pmod p$. Følgelig er

$$|X| \equiv |X^G| \pmod p$$

i dette tilfælde.

(3.10) For den ved konjugering, jfr. (3.7), bestemte virkning af gruppen G på sig selv er banerne konjugentklasserne.

Længden af en klasse $K \subseteq G$ kan derfor bestemmes ved:

$$|K| = |G : C(x)|, \quad x \in K,$$

altså som index af centralisatoren for et element $x \in K$. Indsættelse i Tælleformlen (3.9) giver følgende ligning, der sædvanligvis kaldes:

Klasseformlen. *Lad G være en gruppe G. Da gælder:*

$$|G| = |\mathrm{Cent}(G)| + \sum_j |G : C(x_j)| \,,$$

hvor $|\mathrm{Cent}(G)|$ er centrets orden, og hvor der i summationen er valgt ét element x_j fra hver klasse udenfor centret♠

Eksempel. En endelig gruppe G, hvis orden er en primtalspotens $|G| = p^r$, har et ikke-trivielt centrum, dvs. centret indeholder mere end det neutrale element 1, thi vi har: $|\mathrm{Cent}(G)| \equiv |G| \equiv 0 \pmod{p}$, jfr. Eksempel (3.9), og da $1 \in \mathrm{Cent}(G)$, må der således være mindst p elementer i $\mathrm{Cent}(G)$.

(3.11) Burnside's Formel. *Lad der være givet en virkning af en endelig gruppe G på en mængde X. Da er antallet af baner bestemt ved:*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g| \,,$$

hvor $X^g = \{x \in X \mid g.x = x\}, \quad g \in G.$

Bevis. Lad $I \subseteq G \times X$ betegne delmængden

$$I := \{(g, x) \mid g.x = x\}.$$

Projektionerne $p : (g, x) \mapsto g$ og $q : (g, x) \mapsto x$ definerer da afbildninger $p : I \to G$ og $q : I \to X$, så elementantallet i I kan bestmmes som

$$\sum_{g \in G} |p^{-1}(g)| = |I| = \sum_{x \in X} |q^{-1}(x)|.$$

For hvert $g \in G$ har vi $p^{-1}(g) = \{(g, x) \mid g.x = x\} \simeq X^g$, og altså

$$|I| = \sum_{g \in G} |X^g|. \tag{1}$$

For hvert $x \in X$ har vi $q^{-1}(x) = \{(g, x) \mid g.x = x\} \simeq {}_xG$, og altså

$$|I| = \sum_{x \in X} |{}_xG|. \tag{2}$$

Her er funktionen $x \mapsto |{}_xG|$ konstant på hver bane B, thi når $x \in B$, har vi (jfr. Korollar (3.8))

$$|{}_xG| = \frac{|G|}{|G : {}_xG|} = \frac{|G|}{|B|} \,.$$

Ligningen (2) kan derfor skrives

$$|I| = \sum_B \sum_{x \in B} |{}_xG| = \sum_B \sum_{x \in B} \frac{|G|}{|B|} = \sum_B |B| \cdot \frac{|G|}{|B|} = |X/G| \cdot |G|,$$

og sammenligning med (1) giver det ønskede ♠

I Burnside's formel er funktionen $g \mapsto |X^g|$ konstant på hver konjugeretklasse $K \subseteq G$, thi er $g_1, g_2 \in K$, $g_2 = {}^h g_1 = hg_1h^{-1}$, så definerer $x \mapsto h.x$ en bijektiv afbildning : $X^{g_1} \xrightarrow{\sim} X^{g_2}$. Er $g_0 \in K$, har vi derfor $\sum_{g\in K} |X^g| = |K| \cdot |X^{g_0}| = |G : C(g_0)| \cdot |X^{g_0}| = \frac{|G|}{|C(g_0)|}|X^{g_0}|$. Indsættelse i Burnside's formel giver:

BANEFORMLEN. *Lad der være givet en virkning af en endelig gruppe G på en mængde X. Da er antallet af baner bestemt ved:*

$$|X/G| = \sum_i \frac{|X^{g_i}|}{|C(g_i)|}\,,$$

hvor der i $\sum_i$ er valgt ét element g_i fra hver konjugeretklasse i G♠

(3.12) DEFINITION. Lad X være en endelig mængde. Den fulde permutationsgruppe $Aut(X)$ virker da på X (jfr. Eksempel (3.2)), og for en permutation $\sigma \in Aut(X)$ fås ved restriktion en virkning af den cykliske undergruppe $\langle\sigma\rangle$. Banerne for denne virkning af $\langle\sigma\rangle$ er delmængderne af X af formen

$$\{\sigma^i(x) \mid i \in \mathbf{Z}\}, \text{ for } x \in X.$$

De kaldes også *banerne for permutationen σ*. Det ses, at banerne netop svarer til fremstillingen af σ som produkt af disjunkte cykler, idet fixpunkterne for σ medregnes som 1-cykler.

Betegnes for $p \in \mathbf{N}$ med $m_p = m_p(\sigma)$ antallet af baner af længde p for permutationen σ, får vi en følge

$$m_1, m_2, m_3, \ldots$$

af tal ≥ 0, der kaldes *cykeltypen* for permutationen σ. Bemærk, at $m_p = 0$, når $p > |X|$, og at

$$\sum_p pm_p = |X|.$$

En given cykeltype anskueliggøres ofte ved et *billede*

$$\overbrace{(*)\cdots(*)}^{m_1}\ \overbrace{(*,*)\cdots(*,*,)}^{m_2}\cdots\overbrace{(*,\cdots,*)\cdots(*,\cdots,*)}^{m_p}\cdots$$

hvor der er m_1 symboler af formen $(*)$ (svarende til "1-cyklerne", dvs. fixpunkterne), m_2 symboler af formen $(*,*)$ osv. For en given endelig mængde X er antallet af cykeltyper bestemt som antallet af løsninger $m_p \geq 0$ til ligningen

$$\sum_{p=1}^{\infty} pm_p = |X|.$$

SÆTNING. *Lad X være en endelig mængde. To permutationer er da konjugerede i $Aut(X)$, hvis og kun hvis de har samme cykeltype.*

Bevis. **"kun hvis":** Cykeltypen af σ er bestemt ved fremstillingen af σ som et produkt af disjunkte cykler. For en p-cykel $(x_1, \ldots, x_p)$ og en permutation τ finder vi let

$$\tau(x_1, \ldots, x_p)\tau^{-1} = (\tau(x_1), \ldots, \tau(x_p)).$$

Konjugering afbilder altså en p-cykel på en p-cykel, og da "disjunkthed" bevares, følger påstanden.

"hvis": Vælg en fremstilling af den ene permutation som produkt af disjunkte cykler (medregn fixelementerne som 1-cykler), og opskriv fremstillingen, så at der først kommer alle 1-cykler, dernæst alle 2-cykler osv. Opskriv i en række umiddelbart herunder en tilsvarende fremstilling af den anden permutation. Da de to permutationer har samme type, står der i de to rækker en p-cykel. Den permutation : $X \to X$, der bestemmes ved at et element $x \in X$ afbildes over i det element, som i opskrivningen står umiddelbart under x i den nederste række, vil da konjugere den første permutation over i den anden således som det fremgår af udregningen under "kun hvis"♡

(3.13) For en endelig mængde X svarer konjugeretklasser K i $Aut(X)$ altså til cykeltyper $(m_1, m_2, \ldots)$ med

$$\sum pm_p = |X|,$$

og det er således et kombinatorisk problem at bestemme antallet. Det er ligeledes et kombinatorisk problem at bestemme, hvor mange permutationer, der har en given cykeltype, dvs. at bestemme antallet af elementer i en given konjugeretklasse K. Det sidste svarer i øvrigt til for et givet $\sigma \in K$ at bestemme hvor mange permutationer, der kommuterer med σ, idet vi har

$$|K| = |Aut(X) : C(\sigma)|$$

hvor $C(\sigma)$ er centralisatoren for σ, jfr. (3.10).

EKSEMPEL. For $|X| = 4$, hvor altså $Aut(X) = S_4$ har orden 24, får vi følgende tabel, hvor vi ud for hver type har skrevet antallet af elementer af denne type, og ordenen af centralisatoren for et element af denne type. Bemærk, at det er de sidste tal, der indgår i Baneformlen (3.11).

Type	$\lvert K_g \rvert$	$\lvert C(g) \rvert$
I $(*)(*)(*)(*)$	1	24
II $(*)(*)(*,*)$	6	4
III $(*)(*,*,*)$	8	3
IV $(*,*)(*,*)$	3	8
V $(*,*,*,*)$	6	4

Der er altså 5 konjugeretklasser i S_4. Det ses, at elementer af typerne I, III og V er karakteriseret ved deres orden (som er 1, 3 og 4). Elementer af både type II og IV har orden 2. Men de kendes fra hinanden ved antallet af fixpunkter (som er 2 og 0).

For den naturlige virkning af S_4 på mængden $\{1,2,3,4\}$ er baneformlen identiteten:

$$1 = \frac{4}{24} + \frac{2}{4} + \frac{1}{3} + \frac{0}{8} + \frac{0}{4}\,.$$

RINGE

1. Ringbegrebet.

(1.1) Definition. En *ring* $(\Lambda, +, \cdot)$ er en mængde Λ forsynet med to kompositioner, en *addition* $: \Lambda \times \Lambda \to \Lambda$ betegnet $(\lambda, \mu) \mapsto \lambda + \mu$ og en *multiplikation* $: \Lambda \times \Lambda \to \Lambda$ betegnet $(\lambda, \mu) \mapsto \lambda\mu$, således at følgende er opfyldt:

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

(m) Med hensyn til multiplikation er Λ et monoid.

(d) Multiplikation er distributiv mht. addition.

Den kommutative gruppe $(\Lambda, +)$ kaldes ringens additive gruppe, og betegnes ofte Λ^+. Dens neutrale element kaldes ringens *nul-element* og betegnes 0_Λ (eller blot: 0).

Det inverse mht. additon af et element $\lambda \in \Lambda$ kaldes det *modsatte* til λ og betegnes $-\lambda$. Monoidet $(\Lambda, \cdot)$ kaldes ringens multiplikative monoid, og betegnes af og til $\Lambda^\times$. Dets neutrale element kaldes ringens *et-element* og betegnes 1_Λ (eller blot: 1).

Betingelserne kan udtrykkes ved ligningerne:

$$(a) \quad \begin{cases} \lambda + \mu = \mu + \lambda \\ (\lambda + \mu) + \nu = \lambda + (\mu + \nu) \\ \lambda + 0 = \lambda \\ \lambda + (-\lambda) = 0 \end{cases}$$

$$(m) \quad \begin{cases} (\lambda\mu)\nu = \lambda(\mu\nu) \\ 1\lambda = \lambda = \lambda 1 \end{cases}$$

$$(d) \quad \begin{cases} \lambda(\mu + \nu) = \lambda\mu + \lambda\nu \\ (\lambda + \mu)\nu = \lambda\nu + \mu\nu. \end{cases}$$

Observation. For alle $\lambda \in \Lambda$ gælder

$$0\lambda = 0 = \lambda 0 \quad \text{og} \quad (-1)\lambda = -\lambda = \lambda(-1),$$

thi den første ligning følger for eksempel af at

$$0\lambda + 0\lambda = (0 + 0)\lambda = 0\lambda,$$

og den sidste af at

$$\lambda + \lambda(-1) = \lambda 1 + \lambda(-1) = \lambda[1 + (-1)] = \lambda 0 = 0.$$

BEMÆRKNING. Det forudsættes ikke, at $0_\Lambda \neq 1_\Lambda$. Er imidlertid $0_\Lambda = 1_\Lambda$, finder vi $\lambda = 1\lambda = 0\lambda = 0$ for alle $\lambda \in \Lambda$, så Λ indeholder i så fald kun ét element. Denne ring kaldes *nulringen* og betegnes (også) 0. I alle andre ringe er altså $0 \neq 1$.

(1.2) DEFINITION. Ringen Λ kaldes *kommutativ*, hvis der for alle $\lambda, \mu \in \Lambda$ gælder

$$\lambda\mu = \mu\lambda.$$

EKSEMPEL. De hele tal udgør en kommutativ ring $(\mathbf{Z}, +, \cdot)$.

(1.3) DEFINITION. En afbildning $\varphi : \Gamma \to \Lambda$ mellem ringe Γ og Λ kaldes en *(ring-)homomorfi*, hvis den respekterer strukturen i den forstand, at

$$\begin{aligned} \varphi(\gamma + \mu) &= \varphi(\gamma) + \varphi(\mu) \\ \varphi(\gamma\mu) &= \varphi(\gamma)\varphi(\mu) \qquad \text{for alle } \gamma, \mu \in \Gamma \\ \varphi(1_\Gamma) &= 1_\Lambda. \end{aligned}$$

Ved *kernen* for homomorfien $\varphi : \Gamma \to \Lambda$ forstås originalmængden $\varphi^{-1}(0_\Lambda)$. Det er let at se, at φ er injektiv, netop når kernen er $\varphi^{-1}(0_\Lambda) = \{0_\Gamma\}$.

Det er klart, at sammensætning af homomorfier $\varphi : \Gamma \to \Lambda$ og $\psi : \Delta \to \Gamma$ er en homomorfi $\varphi \circ \psi : \Delta \to \Lambda$. Endvidere er den identiske afbildning $Id_\Lambda : \lambda \mapsto \lambda$ en homomorfi $Id_\Lambda : \Lambda \to \Lambda$.

En bijektiv homomorfi $\varphi : \Gamma \to \Lambda$ kaldes også en *(ring-)isomorfi*. For en sådan er også den inverse afbildning en isomorfi $\varphi^{-1} : \Lambda \to \Gamma$.

En homomorfi $\varphi : \Lambda \to \Lambda$ af ringen Λ ind i sig selv kaldes også en *endomorfi*, og hvis den er bijektiv også en *automorfi*.

(1.4) DEFINITION. Ved en *delring* af en ring Λ forstås en delmængde $\Gamma \subseteq \Lambda$, som er stabil under addition og multiplikation, og som med sine inducerede kompositioner selv er en ring med samme et-element som Λ. Den sidste betingelse sikrer, at inklusionsafbildningen $\gamma \mapsto \gamma$ er en ringhomomorfi $: \Gamma \hookrightarrow \Lambda$.

OBSERVATION. En stabil delmængde $\Gamma \subseteq \Lambda$ er en delring, når blot $-1_\Lambda \in \Gamma$,

thi i så fald finder vi først $1 = -(-1) = (-1)(-1) \in \Gamma$, dernæst $0 = 1 + (-1) \in \Gamma$ og endelig $-\gamma = (-1)\gamma \in \Gamma$, når $\gamma \in \Gamma$.

(1.5) DEFINITION. Ved et *ideal* i en ring Λ forstås en delmængde $\mathcal{A} \subseteq \Lambda$, som opfylder:

(a) $\mathcal{A}$ er en undergruppe i den additive gruppe $(\Lambda, +)$.

(m) $\mathcal{A}$ er stabil over for multiplikation med et vilkårligt element fra Λ , dvs. opfylder

$$\alpha \in \mathcal{A} \wedge \lambda \in \Lambda \quad \Rightarrow \quad \alpha\lambda \in \mathcal{A} \wedge \lambda\alpha \in \mathcal{A}.$$

De *trivielle idealer* i Λ er delmængderne $\{0\}$ (også betegnet (0)) og hele Λ.

HOVEDIDEALSÆTNING. *Idealerne i ringen* $\mathbf{Z}$ *er netop delmængderne af formen*

$$\mathcal{A} = \mathbf{Z}n = \{qn \mid q \in \mathbf{Z}\}, \quad n \geq 0.$$

Tallet n *er entydigt bestemt ved idealet* $\mathcal{A}$*, nemlig som* $n = 0$*, hvis* $\mathcal{A} = (0)$*, og* $n =$*mindste positive tal i* $\mathcal{A}$*, hvis* $\mathcal{A} \neq (0)$.

Bevis. De anførte delmængder er som bekendt samtlige undergrupper i $(\mathbf{Z}, +)$, og da de øjensynlig er idealer, følger påstanden♠

(1.6) Som bekendt er der en entydig forbindelse mellem idealer $\mathcal{A}$ i ringen Λ og kongruensrelationer i Λ. Den til idealet $\mathcal{A}$ hørende kongruensrelation er $\underset{\mathcal{A}}{\equiv}$ ("kongruens modulo $\mathcal{A}$") defineret ved

$$\lambda' \underset{\mathcal{A}}{\equiv} \lambda \quad \overset{\text{DEF}}{\Longleftrightarrow} \quad \lambda' - \lambda \in \mathcal{A}.$$

Ækvivalensklassen, der indeholder λ, er altså delmængden

$$\lambda + \mathcal{A} := \{\lambda + \alpha \mid \alpha \in \mathcal{A}\}.$$

Den tilhørende *kvotientring* betegnes $\Lambda/\mathcal{A}$, og $\lambda \mapsto \boxed{\lambda}$ betegner den *kanoniske* homomorfi : $\Lambda \to \Lambda/\mathcal{A}$. Med hensyn til denne gælder som bekendt:

UDVIDELSESSÆTNINGEN. *En ringhomomorfi* $\varphi : \Lambda \to \Gamma$*, som forsvinder på idealet* $\mathcal{A} \subseteq \Lambda$*, kan entydigt udvides til en ringhomomorfi fra kvotienten* $\bar{\varphi} : \Lambda/\mathcal{A} \to \Gamma$*. I diagramform:*

$$\begin{array}{ccc} \Lambda & \xrightarrow{\square} & \Lambda/\mathcal{A} \\ {\scriptstyle\varphi}\big\downarrow & \swarrow & \\ \Gamma & & \end{array} \qquad \spadesuit$$

Homomorfien $\bar{\varphi}$ er den *inducerede* homomorfi.

Videre gælder som bekendt:

ISOMORFISÆTNINGEN. *Lad* $\varphi : \Lambda \to \Gamma$ *være en ringhomomorfi. Da er kernen* $\varphi^{-1}(0)$ *et ideal i* Λ*, billedmængden* $\varphi(\Lambda)$ *er en delring af* Γ*, og homomorfien* φ *inducerer en isomorfi* $\bar{\varphi} : \Lambda/\varphi^{-1}(0) \xrightarrow{\sim} \varphi(\Lambda)$ *af kvotienten på billedet. I diagramform:*

$$\begin{array}{ccc} \Lambda & \xrightarrow{\varphi} & \Gamma \\ \square\big\downarrow & & \big\uparrow \\ \Lambda/\varphi^{-1}(0) & \underset{\bar{\varphi}}{\xrightarrow{\sim}} & \varphi(\Lambda) \end{array} \qquad \spadesuit$$

EKSEMPEL. Kvotientringen $\mathbf{Z}/\mathbf{Z}n$ hørende til idealet $\mathbf{Z}n$, hvor $n \geq 1$, er restklasseringen modulo n. Den betegnes også $\mathbf{Z}/n$.

(1.7) KARAKTERISTIK OG PRIMRING. Som bekendt findes for enhver ring Λ en og kun én ringhomomorfi $: \mathbf{Z} \to \Lambda$, nemlig den *kanoniske ringhomomorfi:*

$$q \mapsto q1_\Lambda, \quad q \in \mathbf{Z}.$$

Kernen for den kanoniske ringhomomorfi $: \mathbf{Z} \to \Lambda$ er et ideal i $\mathbf{Z}$, og altså af formen $\mathbf{Z}n$, hvor $n \geq 0$ er entydigt bestemt, jfr. Hovedidealsætning (1.5).

DEFINITION. Tallet $n \geq 0$ kaldes *karakteristikken* af ringen Λ, og billedet ved den kanoniske ringhomomorfi $: \mathbf{Z} \to \Lambda$ kaldes *primringen* i Λ. Karakteristikken af Λ kan betegnes $\mathrm{char}(\Lambda)$. Primringen i Λ er delmængden

$$\{q1_\Lambda \mid q \in \mathbf{Z}\}.$$

Det er øjensynlig den mindste delring af Λ. Af beskrivelsen i Hovedidealsætning (1.5) fremgår følgende:

RESULTAT. *Ringen Λ har karakteristik 0, netop når*

$$\overbrace{1_\Lambda + \cdots + 1_\Lambda}^{m} \neq 0_\Lambda \quad \textit{for alle} \quad m \in \mathbf{N}.$$

I dette tilfælde er den kanoniske ringhomomorfi $: \mathbf{Z} \to \Lambda$ injektiv, og primringen i Λ er (isomorf med) $\mathbf{Z}$.

Ringen Λ har karakteristik $n \geq 1$, netop når n er det mindste naturlige tal således at

$$\overbrace{1_\Lambda + \cdots + 1_\Lambda}^{n} = 0_\Lambda.$$

I dette tilfælde får vi af Isomorfisætningen en isomorfi af restklasseringen $\mathbf{Z}/n$ på primringen i Λ.

OBSERVATION. Hvis Λ har karakteristik $n \geq 1$, så er $\overbrace{\lambda + \cdots + \lambda}^{n} = 0_\Lambda$ for alle $\lambda \in \Lambda$, thi så er $\overbrace{\lambda + \cdots + \lambda}^{n} = (\overbrace{1 + \cdots + 1}^{n}) \cdot \lambda = 0 \cdot \lambda = 0$.

EKSEMPEL. Ringen $\mathbf{Z}$ har karakteristik 0. Restklasseringen $\mathbf{Z}/n$, hvor $n \geq 1$, har karakteristik n [hvorfor?]. En endelig ring har karakteristik > 0 [hvorfor?].

(1.8) REGULÆRT OG INVERTIBELT ELEMENT. DEFINITION. Lad Λ være en ring.

Et element $\lambda \in \Lambda$ kaldes *regulært*, hvis der for alle $\xi \in \Lambda$ gælder

$$\lambda\xi = 0 \Rightarrow \xi = 0 \quad \text{og} \quad \xi\lambda = 0 \Rightarrow \xi = 0.$$

Mængden af regulære elementer i Λ kan betegnes Λ^{reg}.

Et element $\lambda \in \Lambda$ kaldes *invertibelt* (eller en *enhed*), hvis der findes et element $\lambda' \in \Lambda$, således at

$$\lambda\lambda' = 1 = \lambda'\lambda.$$

I bekræftende fald er elementet λ' entydigt bestemt. Det kaldes det *inverse* til λ og betegnes λ^{-1}. Mængden af invertible elementer i Λ betegnes Λ^*.

Observationer. (1) Ethvert invertibelt element $\lambda \in \Lambda$ er regulært, thi af $\lambda\xi = 0$ følger $0 = \lambda^{-1}0 = \lambda^{-1}\lambda\xi = 1\xi = \xi$, og analogt hvis $\xi\lambda = 0$.

(2) Delmængden Λ^{reg} er stabil under multiplikation og indeholder et-elementet 1. Vi kan altså opfatte Λ^{reg} som et monoid.

(3) Delmængden Λ^* er stabil under multiplikation, indholder et-elementet og med et element λ tillige det inverse λ^{-1}. Vi kan altså opfatte Λ^* som en gruppe (med multiplikation som komposition og et-elementet som neutralt element).

Eksempel. For ringen $\mathbf{Z}$ har vi

$$\mathbf{Z}^{reg} = \mathbf{Z} \setminus \{0\}, \qquad \mathbf{Z}^* = \{\pm 1\}.$$

(1.9) Integritetsområde og (Skæv-)legeme. Definition. I ringen Λ siges *nul-reglen* at gælde, hvis vi for alle elemente $\lambda, \mu \in \Lambda$ har

$$\lambda\mu = 0 \quad \Rightarrow \quad \lambda = 0 \vee \mu = 0.$$

Ringen Λ kaldes et *integritetsområde* (eller blot et *område*), hvis

$$\Lambda^{reg} = \Lambda \setminus \{0\},$$

og et *skævlegeme*, hvis

$$\Lambda^* = \Lambda \setminus \{0\}.$$

Et *legeme* er et kommutativt skævlegeme. Ved et *dellegeme* af et legeme forstås en delring, som selv er et legeme. Det er sædvane for elementer λ, μ i et legeme, $\mu \neq 0$, at sætte $\frac{\lambda}{\mu} := \lambda\mu^{-1}$. Specielt er altså $\frac{1}{\mu} = \mu^{-1}$.

Bemærkninger. Nul-reglen udsiger, at alle elementer $\neq 0$ er regulære, altså at

$$\Lambda \setminus \{0\} \subseteq \Lambda^{reg}.$$

Dette gælder formelt for nul-ringen. I nul-ringen er nul-elementet regulært, så nul-ringen er **ikke** et integritetsområde. Det følger, at en ring $\Lambda \neq 0$ er et integritetsområde, netop når nul-reglen gælder. Tilsvarende ses, at nul-ringen **ikke** er et skævlegeme, og at en ring $\Lambda \neq 0$ er et skævlegeme, netop når ethvert element $\neq 0$ i Λ er invertibelt.

EKSEMPEL. De hele tals ring $\mathbf{Z}$ er et kommutativt integritetsområde, men ikke et legeme. De rationale tal udgør legemet $\mathbf{Q}$.

SÆTNING. *For et integritetsområde (og specielt for et legeme) Λ er karakteristikken n enten 0 eller et primtal.*

Bevis. (Indirekte). Vi har $n \neq 1$ (idet kun nul-ringen har karakteristik 1), og hvis n var et sammensat tal, $n = ad$, $1 < a < n$, $1 < d < n$, ville

$$a1_\Lambda \neq 0_\Lambda, \quad d1_\Lambda \neq 0_\Lambda, \quad (a1_\Lambda)(d1_\Lambda) = n1_\Lambda = 0_\Lambda,$$

jfr. (1.7), være i modstrid med nul-reglen♠

(1.10) LEGEMERNE $\mathbf{F}_p$. SÆTNING. *Enhver endelig ring Λ, hvis elementantal p er et primtal, er et legeme, isomorft med restklasseringen $\mathbf{Z}/p$.*

Bevis. Da $|\Lambda| = p > 1$, er Λ ikke nul-ringen. For at vise, at hvert element $\Lambda \neq 0$ i Λ er invertibelt, betragtes i den additive gruppe $(\Lambda, +)$ undergruppen

$$\mathbf{Z}\lambda = \{q\lambda \mid q \in \mathbf{Z}\}$$

bestående af (additive) potenser af λ. Denne undergruppes orden er > 1 (idet den indeholder både 0 og λ). Ifølge Lagrauge's sætning er ordenen $|\mathbf{Z}\lambda|$ divisor i $|\Lambda| = p$, som er et primtal, og vi har følgelig $|\mathbf{Z}\lambda| = |\Lambda|$ og dermed $\mathbf{Z}\lambda = \Lambda$. Specielt findes et helt tal $q \in \mathbf{Z}$, således at $q\lambda = 1_\Lambda$. Af

$$(q1_\Lambda)\lambda = \lambda(q1_\Lambda) = q\lambda = 1$$

fremgår, at λ er invertibel (med den inverse $\lambda^{-1} = q1_\Lambda$). Følgelig er Λ et skævlegeme. Anvendes ovenstående på elementet $\lambda = 1_\Lambda \in \Lambda$, ses at

$$\mathbf{Z}1_\Lambda = \{q1_\lambda \mid q \in \mathbf{Z}\} = \Lambda.$$

Den kanoniske homomorfi : $\mathbf{Z} \to \Lambda$ er altså surjektiv, og inducerer derfor en isomorfi:

$$\mathbf{Z}/n \xrightarrow{\sim} \Lambda,$$

hvor n er karakteristikken af Λ. Specielt er Λ kommutativ, da $\mathbf{Z}/n$ er kommutativ. Endelig er

$$n = |\mathbf{Z}/n| = |\Lambda| = p \quad ♠$$

KOROLLAR. *Restklasseringen* $\mathbf{Z}/p$*, hvor* p *er et primtal, er et (endeligt) legeme*♠

NOTATION. For et primtal p betegnes legemet $\mathbf{Z}/p$ også $\mathbf{F}_p$.

BEMÆRKNING. Det fremgår af Sætning (1.9), at restklasseringene $\mathbf{Z}/n$, hvor $n \geq 1$ **ikke** er et primtal, ikke er integritetsområder.

(1.11) PRIMLEGEME. Lad L være et legeme, og lad

$$R = \{q1_L \mid q \in \mathbf{Z}\}$$

betegne primringen i L. Som delring af L er R et kommutativt integritetsområde, så vi kan i L betragte *brøklegemet* for R:

$$\{(a1_L)(s1_L)^{-1} \mid a, s \in \mathbf{Z}, s1_L \neq 0_L\}.$$

[Det er let at se, at denne delmængde er et dellegeme af L.]

DEFINITION. Dette brøklegeme kaldes *primlegemet* i legemet L. Blandt dellegemerne af L er primlegemet øjensynlig det midste. Hvis legemet L har karakteristik 0, er primringen isomorf med $\mathbf{Z}$, og primlegemet følgelig isomorft med $\mathbf{Q}$. Hvis legemet L har karakteristik $p > 0$, så er p et primtal, jfr. Sætning (1.9), og primringen $\mathbf{Z}/p$ er selv et legeme. Primlegemet er altså $\mathbf{F}_p$.

(1.12) KOMMUTATION. DEFINITION. I ringen Λ siges elementer $\lambda, \mu \in \Lambda$ at *kommutere*, hvis

$$\lambda\mu = \mu\lambda.$$

Elementet $\lambda \in \Lambda$ kaldes *centralt*, hvis det kommuterer med alle elementer $\mu \in \Lambda$. Delmængden bestående af centrale elementer i Λ kaldes *centrum* i Λ. Den betegnes ofte $Cent(\Lambda)$. En ringhomomorfi $\varphi : \Gamma \to \Lambda$ kaldes *central*, hvis $\varphi(\gamma)$ er centralt i Λ for alle $\gamma \in \Gamma$.

OBSERVATION. Centret i en ring Λ er en (kommutativ) delring.

(1.13) DEFINITIONER. Et element λ i ringen Λ kaldes *involutorisk*, hvis

$$\lambda^2 = 1,$$

idempotent, hvis

$$\lambda^2 = \lambda,$$

og *nilpotent*, hvis der findes et $N \in \mathbf{N}$, så at

$$\lambda^N = 0.$$

OBSERVATION. Hvis nul-reglen gælder, så er 1 og -1 de eneste involutioner, 0 og 1 er de eneste idempotenter, og 0 er det eneste nilpotente element,

thi ligningerne ovenfor kan skrives

$$(\lambda - 1) \cdot (\lambda + 1) = 0, \quad \lambda \cdot (\lambda - 1) = 0, \quad \lambda \cdots \lambda = 0.$$

(1.14) BEMÆRKNING. I enhver ring Λ kan en *modsat multiplikation* defineres ved

$$\lambda \overset{op}{\cdot} \mu := \mu\lambda.$$

Det er let at se, at $(\Lambda, +, \overset{op}{\cdot})$ er en ring. Den kaldes Λ's *modsatte ring* og betegnes Λ^{op}. Hvis Λ er kommutativ, er $\Lambda = \Lambda^{op}$.

En ringhomomorfi $\varphi : \Gamma^{op} \to \Lambda$ er en afbildning, som opfylder:

$$\begin{aligned} \varphi(\gamma + \mu) &= \varphi(\gamma) + \varphi(\mu) \\ \varphi(\gamma\mu) &= \varphi(\mu)\varphi(\gamma) \qquad \text{for alle } \gamma, \mu \in \Gamma \\ \varphi(1_\Gamma) &= 1_\Lambda. \end{aligned}$$

Den siges også at være en *anti–homomorfi* $\varphi : \Gamma \to \Lambda$.

2. Polynomiumsringen i én variabel over en kommutativ ring.

I det følgende betegner R en **kommutativ** ring.

(2.1) Beskrivelse. Til den givne ring R kan man konstruere en større kommutativ ring $R[X]$ kaldet *polynomiumsringen* over R. Den indeholder R som delring og yderligere et bestemt element betegnet X, og opfylder, at ethvert element $p \in R[X]$ kan skrives

$$p = p_0 + p_1X + \cdots + p_nX^n, \qquad \text{hvor } n \geq 0 \text{ og } p_i \in R \text{ for } i = 0, \ldots, n,$$

og at denne fremstilling er entydig bortset fra en eventuel tilføjelse/fjernelse af led af formen $0X^i$.

Elementerne p i ringen $R[X]$ kaldes *polynomier* (med koefficienter i R), og elementerne $p_i \in R$ for $i = 0, 1, 2, \ldots$ kaldes *koefficienterne* i polynomiet p.

Observation. Kompositionerne i ringen $R[X]$ er helt bestemt ved beskrivelsen, thi for givne polynomier

$$p = p_0 + p_1X + \cdots + p_nX^n, \qquad q = q_0 + q_1X + \cdots + q_mX^m$$

(hvor f.eks. $m \geq n$) finder vi blot ved brug af regnereglerne, at

$$p + q = (p_0 + q_0) + (p_1 + q_1)X + \cdots + (p_n + q_n)X^n + q_{n+1}X^{n+1} + \cdots + q_mX^m$$
$$pq = (p_0q_0) + (p_0q_1 + p_1q_0)X + (p_0q_2 + p_1q_1 + p_2q_0)X^2 + \cdots + p_nq_mX^{n+m}.$$

Bemærkning. Af entydigheden af fremstillingen

$$p = p_0 + p_1X + \cdots + p_nX^n, \quad p_i \in R,$$

følger, at polynomiet $p \in R[X]$ helt bestemmer sine koefficienter $p_i \in R$. Koefficienterne p_i er definerede for alle $i = 0, 1, 2, \cdots$, og de er $= 0$, når i er tilstrækkelig stor. Polynomier kan derfor defineres som værende sådanne følger af koefficienter. Af de fundne udtryk for sum og produkt af polynomier ses, hvordan sum og produkt af sådanne koefficientfølger så må defineres.

(2.2) Definition. Opfattet som polynomier kaldes elementerne i R også *konstanter*. De er karakteriseret ved, at koefficienterne er $p_i = 0$, når $i > 0$. *Nulpolynomiet* er konstanten 0, hvis koefficienter er $p_i = 0$ for alle i. For alle polynomier $p \neq 0$ findes en koefficient $p_i \neq 0$.

Lad $p \in R[X]$ være et polynomium $\neq 0$. Det største tal $n \geq 0$, så at $p_n \neq 0$, kaldes da *graden* af polynomiet p og betegnes $\text{grad}(p)$ og elementet $p_n \in R$, $n = \text{grad}(p)$, kaldes den *ledende koefficient* i p. Hvis den ledende koefficient er et-elementet $1 \in R$, siges p at være et *normeret* polynomium. Polynomierne af grad n er altså polynomierne af formen

$$p = p_0 + \cdots + p_n X^n, \qquad \text{hvor } p_i \in R \text{ for } i = 0, \ldots, n \text{ og } p_n \neq 0,$$

og heraf har de normerede formen

$$p = X^n + p_{n-1}X^{n-1} + \cdots + p_0, \qquad \text{hvor } p_i \in R \text{ for } i = 0, \ldots, n-1.$$

Tilføjelse. Vi har ikke ovenfor tillagt nulpolynomiet nogen grad, og nulpolynomiet har således **ingen** ledende koefficient og det er specielt **ikke** normeret. Det er ofte hensigtsmæssigt at tillægge nulpolynomiet en grad, der er $<$ alle andre grader (dvs. < 0). I det følgende tillægger vi nulpolynomiet graden $-\infty$ [med oplagte konventioner for regning med $-\infty$]. Polynomier $p \in R[X]$ af grad $\leq n$ har altså formen

$$p = aX^n + \cdots, \qquad a \in R,$$

hvor "$\cdots$" står for et polynomium af grad $< n$. Hvis $\text{grad}(p) = n$, dvs. hvis $a \neq 0$, så er a den ledende koefficient. Specielt ses, at polynomierne af grad ≤ 0 består af konstanterne, dvs. af elementerne i R.

(2.3) Observation. Af de fundne udtryk for sum og produkt fremgår umiddelbart, at vi for polynomier $p, q \in R[X]$ har:

$$\text{grad}(p+q) \leq \max\{\text{grad}(p), \text{grad}(q)\} \tag{1}$$

$$\text{grad}(pq) \leq \text{grad}(p) + \text{grad}(q), \tag{2}$$

og at der gælder "$<$" i (1), netop når p og q har samme grad ≥ 0 og modsatte ledende koefficienter. Videre ses, at der i (2) gælder "$=$", når $p, q \neq 0$ og produktet af de ledende koefficienter er $\neq 0$. Specielt fremhæves, at "$=$" gælder i (2), når et af polynomierne har en ledende koefficient, der er regulær. Lidt mere specielt fremhæves følgende:

(2.4) Sætning. *Lad R være et integritetsområde. Da er*

$$\text{grad}(pq) = \text{grad}(p) + \text{grad}(q), \quad \textit{for alle } p, q \in R[X].$$

Polynomiumsringen $R[X]$ er også et integritetsområde, og de invertible polynomier er netop de konstanter, der er invertible i R.

Bevis. Ligningen følger af det observerede, og heraf følger også nulreglen. Da $R \subseteq R[X]$, har vi $R^* \subseteq (R[X])^*$. For at vise " $\supseteq$ " betragtes $p \in R[X]^*$. Der findes altså $q \in R[X]$, så at $1 = pq$. Heraf fås $0 = \text{grad}(1) = \text{grad}(pq) = \text{grad}(p) + \text{grad}\,(q)$, hvoraf $0 = \text{grad}(p) = \text{grad}(q)$. Altså er $p, q \in R$, og af $1 = pq$ følger $p \in R^*$♠

(2.5) DIVISIONSSÆTNING. *Lad $d \in R[X]$ være et polynomium $\neq 0$, hvis ledende koefficient er invertibel. Til hvert polynomium $p \in R[X]$ findes da entydigt bestemte polynomier $q, r \in R[X]$, så at*

$$p = qd + r \quad og \quad grad(r) < \text{grad}(d).$$

Bevis. Sættes $n := \text{grad}(d) \geq 0$, har vi

$$d = uX^n + \cdots,$$

hvor $u \in R$ er invertibel.
Eksistens: Hvis polynomiet p har grad $< n$ har vi fremstillingen

$$p = 0d + p, \qquad \text{hvor } q = 0 \text{ og } r = p \text{ har grad } < n.$$

Antag derfor, at p har grad $m \geq n$ og ledende koefficient p_m, dvs. at p har formen

$$(*) \qquad p = p_m X^m + \cdots, \quad \text{hvor } p_m \neq 0.$$

Da polynomiet $u^{-1}d$ er normeret, har polynomiet $p_m u^{-1} d X^{m-n}$ også formen $(*)$, og polynomiet $p - p_m u^{-1} X^{m-n} d$ har derfor grad $< m$. Induktivt har vi derfor en fremstilling

$$p - p_m u^{-1} X^{m-n} d = \tilde{q}d + r, \quad \text{grad}(r) < \text{grad}(d),$$

og så er

$$p = (p_m u^{-1} X^{m-n} + \tilde{q})d + r$$

en fremstilling af p som ønsket.
Entydighed: Det er nok at betragte en fremstilling

$$0 = qd + r, \quad \text{hvor grad}(r) < \text{grad}(d).$$

Da den ledende koefficient i d er normeret, fås heraf, at

$$\text{grad}(r) = \text{grad}(-qd) = \text{grad}(q) + \text{grad}(d),$$

jfr. Observation (2.3). Var $q \neq 0$ og dermed grad $(q) \geq 0$, ville vi få modstriden $\text{grad}(r) \geq \text{grad}(d)$. Altså er $q = 0$ og dermed også $r = 0$ ♠

BEMÆRKNING. Divisionssætningen kan specielt anvendes på ethvert normeret polynomium. Hvis ringen R er et legeme, kan Divisionssætningen anvendes med et vilkårligt polynomium $d \neq 0$.

(2.6) DEFINITION. Lad der være givet et polynomium

$$p = p_0 + p_1 X + \cdots + p_n X^n \in R[X]$$

og et element $a \in R$. Elementet $p_0 + p_1 a + \cdots + p_n a^n \in R$ betegnes da $p(a)$, altså

$$p(a) := p_0 + p_1 a + \cdots + p_n a^n \in R,$$

og det siges at fremkomme ved at *indsætte elementet a i polynomiet p*. Hvis $p(a) = 0$, siges a at være *rod* i polynomiet p.

OBSERVATION. For et fast element $a \in R$ er afbildningen

$$p \mapsto p(a)$$

en surjektiv ringhomomorfi : $R[X] \to R$. Dens kerne består af de polynomier, der har a som rod. De udgør altså et ideal i $R[X]$.

BEMÆRKNING. For et givet polynomium $p = p_0 + p_1 X + \cdots p_n X^n \in R[X]$ vil udtrykket $p_0 + p_1 \alpha + \cdots + p_n \alpha^n$ have mening, når blot α er et element i en ring Λ, der indeholder R som delring. Også i denne generelle situation skrives

$$p(\alpha) := p_0 + p_1 \alpha + \cdots + p_n \alpha^n \in \Lambda.$$

Da $R[X] \supseteq R$, kan vi altså specielt skrive

$$p = p(X).$$

(2.7) SÆTNING. *Polynomiet $p \in R[X]$ har elementet $a \in R$ som rod, hvis og kun hvis det kan skrives*

$$p = q \cdot (X - a),$$

med et polynomium $q \in R[X]$.

Bevis. Anvendes Divisionssætningen (2.5) med 1^{ste}-gradspolynomiet $d := X - a$ fås en entydig fremstilling

$$p = q \cdot (X - a) + r, \quad \text{hvor } \operatorname{grad}(r) < 1.$$

Polynomiet $r \in R[X]$ har altså grad ≤ 0, og er derfor konstant. Indsættelse af a giver

$$p(a) = q(a) \cdot 0 + r = r \in R.$$

Vi har altså $p(a) = 0$, hvis og kun hvis $r = 0$ ♠

KOROLLAR. *Hvert polynomium $p \neq 0$ af grad n i $R[X]$ har en fremstilling*

$$p = \tilde{p} \cdot (X - a_1) \cdots (X - a_k), \quad \textit{hvor } k \leq n \textit{ og } a_i \in R \textit{ for } i = 1, \ldots, k\,,$$

hvor polynomiet $\tilde{p} \in R[X]$ ikke har rødder i R. Hvis R er et integritetsområde, er fremstillingen entydig (bortset fra permutation af 1^{ste}-gradsfaktorerne), og

$$\{a_1, \ldots, a_k\} = \{a \in R \mid p(a) = 0\}.$$

Specielt er i dette tilfælde antallet af rødder i p endeligt og $\leq \operatorname{grad}(p)$.

Bevis. Hvis p ikke har rødder i R, får vi den ønskede fremstilling med $\tilde{p} := p$ og $k := 0$. Hvis p har en rod a_1, kan vi skrive $p = p_1 \cdot (X - a_1)$, og da $X - a_1$ er normeret, er $\operatorname{grad}(p_1) = \deg(p) - 1 = n - 1$. Fortsættes nu med polynomiet p_1, får vi efter højst n skridt den ønskede fremstilling.

Antag nu, at R er et integritetsområde. Ud fra en fremstilling

$$p = \tilde{p} \cdot (X - a_1) \cdots (X - a_k), \quad \text{hvor } \tilde{p} \text{ er uden rødder,}$$

aflæser vi, at

$$\{a_1, \ldots, a_k\} = \{a \in R \mid p(a) = 0\},$$

thi " $\subseteq$ " er oplagt, og er omvendt $p(a) = 0$, så er

$$0 = \tilde{p}(a)(a - a_1) \cdots (a - a_k);$$

da $\tilde{p}(a) \neq 0$, og da nul-reglen gælder, må en af de øvrige faktorer være 0.
Vi viser nu entydigheden ved induktion efter graden n. Entydigheden er klar, hvis $n = 0$, da p så er konstant. Er $n > 0$, og har vi endnu en fremstilling

$$p = \tilde{q} \cdot (X - b_1) \cdots (X - b_l), \quad \text{hvor } \tilde{q} \text{ er uden rødder,}$$

så er b_l rod i p, altså ifølge det viste $b_l \in \{a_1, \ldots, a_k\}$. Vi kan antage, at $b_l = a_k$. Af

$$p = \tilde{p} \cdot (X - a_1) \cdots (X - a_{k-1}) \cdot (X - a_k) = \tilde{q} \cdot (X - b_1) \cdots (X - b_{l-1}) \cdot (X - a_k)$$

følger imidlertid (da nul-reglen gælder i $R[X]$), at

$$\tilde{p} \cdot (X - a_1) \cdots (X - a_{k-1}) = \tilde{q} \cdot (X - b_1) \cdots (X - b_{l-1}).$$

Dette er fremstillinger af et polynomium af grad $n-1$, og induktionsforudsætningen giver derfor : $\tilde{p} = \tilde{q}, k-1 = l-1$ og (eventuelt efter permutation) $a_1 = b_1, \ldots, a_{k-1} = b_{k-1}$ ♠

BEMÆRKNING. Lad $\nu \in \tilde{\mathbf{N}}$. Et element $a \in R$ siges da at være (mindst) *ν-dobbelt rod* eller at være en *rod af multiplicitet* $\geq \nu$ i polynomiet $p \in R[X]$, hvis p kan skrives

$$p = q \cdot (X-a)^{\nu}.$$

Hvis R er et integritetsområde, ses, at antallet af rødder i p, "talt med multiplicitet", er $\leq \deg(p)$.

(2.8) Lad $d = X^n + d_{n-1}X^{n-1} + \cdots + d_1X + d_0 \in R[X]$ være et normeret polynomium af grad $n \geq 1$. Sættes

$$(d) := \{qd \mid q \in R[X]\},$$

er (d) øjensynlig et ideal i $R[X]$, og vi kan betragte kvotienten $\Lambda := R[X]/(d)$ og den kanoniske homomorfi

$$\boxed{\ } : R[X] \to \Lambda.$$

Den sammensatte homomorfi $a \mapsto \boxed{a}$, der til et element $a \in R$ knytter ækvivalensklassen, der indeholder det konstante polynomium $a \in R[X]$, er da en injektiv homomorfi : $R \to \Lambda$, thi $\boxed{a} = 0_\Lambda$ betyder, at $a \in (d)$, og da polynomierne $\neq 0$ i (d) har grad $\geq n \geq 1$, kan dette kun være opfyldt, når konstanten a er $= 0$. Idet vi identificerer elementerne $a \in R$ med deres billeder i Λ, kan vi opfatte R som en delring: $R \subseteq \Lambda$. Herom gælder følgende:

STRUKTURSÆTNING FOR POLYNOMIUMSKVOTIENTER. *Lad*

$$d = X^n + d_{n-1}X^{n-1} + \cdots + d_1X + d_0, \quad n \geq 1,$$

være et normeret polynomium i $R[X]$. Kvotientringen $\Lambda := R[X]/(d)$ er da en kommutativ ring, som indeholder R, og sættes

$$\xi := \boxed{X} \in \Lambda,$$

kan hvert element $\lambda \in \Lambda$ entydigt skrives

$$\lambda = r_0 + r_1\xi + \cdots + r_{n-1}\xi^{n-1}, \quad \textit{med } r_0, r_1, \ldots, r_{n-1} \in R.$$

Endvidere gælder i Λ ligningen

$$(*) \qquad \xi^n = -d_0 - d_1\xi - \cdots - d_{n-1}\xi^{n-1}.$$

Bevis. Da ringen $R[X]$ er kommutativ, er også kvotientringen Λ kommutativ. Lad $r_0, r_1, \ldots, r_{n-1}$ være elementer i R. Da $\boxed{\ }: R[X] \to \Lambda$ er en homomorfi, har vi med de indførte identifikationer:

$$r_0 + r_1\xi + \cdots + r_{n-1}\xi^{n-1} = \boxed{r_0} + \boxed{r_1} \cdot \boxed{X} + \cdots + \boxed{r_{n-1}} \cdot \boxed{X}^{n-1}$$
$$= \boxed{r_0 + r_1 X + \cdots + r_{n-1}X^{n-1}}.$$

Ethvert element λ i kvotienten Λ har formen $\boxed{p}$, hvor $p \in R[X]$. Vi har altså

$$\boxed{p} = r_0 + r_1\xi + \cdots + r_{n-1}\xi^{n-1},$$

netop når $\boxed{p} = \boxed{r_0 + r_1 1X + \cdots + r_{n-1}X^{n-1}}$, dvs. netop når p kan skrives

$$p = qd + r_0 + r_1 X + \cdots + r_{n-1}X^{n-1}, \quad \text{med } q \in R[X].$$

Da Divisionssætningen (2.5) udsiger, at ethvert polynomium p har en sådan entydig fremstilling, følger det, at enhver ækvivalensklasse $\lambda \in \Lambda$ entydigt kan skrives $\lambda = r_0 + r_1\xi + \cdots + r_{n-1}\xi^{n-1}$, med elementer $r_0, r_1, \ldots, r_{n-1} \in R$. Endvidere har vi i Λ :

$$0_\Lambda = \boxed{0} = \boxed{d} = \boxed{d_0 + d_1 X \ \cdots + d_{n-1} + X^n} = d_0 + d_1\xi + \cdots + d_{n-1}\xi^{n-1} + \xi^n,$$

og det er netop den anførte ligning ♠

Bemærkninger. (1) Hvis ringen $R = L$ er et legeme, ser vi, at $1, \xi, \ldots, \xi^{n-1}$ er en basis for Λ som vektorrum over L. Dimensionen er netop graden n af det givne polynomium d.
(2) Multiplikationen i ringen Λ er bestemt af den anførte ligning $(*)$, thi vi har

$$\xi^{n+1} = \xi^n\xi = -d_0\xi - d_1\xi^2 - \cdots - d_{n-2}\xi^{n-1} - d_{n-1}\xi^n,$$

og v.hj.a. $(*)$ kan $-d_{n-1}\xi^n$ skrives som "linearkombination" af $1, \xi, \ldots, \xi^{n-1}$. Induktivt får vi alle potenser $\xi^{n+1}, \xi^{n+2}, \ldots$ skrevet som "linearkombinationer" af $1, \xi, \ldots, \xi^{n-1}$.
(3) Opfattes det givne polynomium d som et polynomium med koefficienter i den større ring $\Lambda = R[X]/(d) \supseteq R$:

$$d \in R[X] \subseteq \Lambda[X],$$

ser vi, at det givne polynomium d i Λ har roden ξ, thi ligningen $(*)$ kan skrives

$$d(\xi) = 0.$$

(2.9) Struktursætningen behandler kun kvotienter $R[X]/\mathcal{A}$, hvor idealet har formen

$$\mathcal{A} = (d) = \{qd \mid q \in R[X]\}$$

med et normeret polynomium d af grad ≥ 1, og vi vil ikke her beskæftige os med idealer af andre typer. Hvis ringen R er et legeme, er der essentielt ikke andre typer idealer. Dette er indholdet i følgende:

HOVEDIDEALSÆTNING. *Lad L være et legeme. For hvert ideal $\mathcal{A}$ i polynomiumsringen $L[X]$ findes et polynomium $d \in L[X]$, så at*

$$\mathcal{A} = \{qd \mid q \in L[X]\}.$$

Bevis. Hvis $\mathcal{A} = \{0\}$, kan vi øjensynlig bruge $d = 0$. Antag derfor, at $\mathcal{A} \neq \{0\}$. Vælg et polynomium $d \in \mathcal{A} \setminus \{0\}$, hvis grad er mindst blandt alle grader af polynomier i $\mathcal{A} \setminus \{0\}$. Det påstås, at

$$\mathcal{A} = \{qd \mid q \in L[X]\} = (d).$$

Her er " $\supseteq$ " klart, thi da $d \in \mathcal{A}$ og $\mathcal{A}$ er et ideal, er også $qd \in \mathcal{A}$ når $q \in L[X]$. Lad omvendt $p \in \mathcal{A}$. Ifølge Divisionssætningen (2.5) kan vi skrive

$$p = qd + r, \qquad \deg(r) < \deg(d).$$

Da $\mathcal{A}$ er et ideal og $p, d \in \mathcal{A}$, vil $r = p - qd \in \mathcal{A}$. Hvis $r \neq 0$, ville vi have

$$r \in \mathcal{A} \setminus \{0\} \quad \text{og} \quad \deg(r) < \deg(d),$$

og det er i modstrid med valget af d. Følgelig er $r = 0$, og altså $p = qd \in (d)$♠

(2.10) DEFINITION. For et polynomium

$$p = p_0 + p_1X + \cdots + p_nX^n \in R[X]$$

er det *afledede* polynomium $p' := p_1 + 2p_2X + \cdots + np_nX^{n-1}$, hvor $ip_i = \overbrace{p_i + \cdots + p_i}^{i}$. Det er let at eftervise de sædvanlige regneregler:

$$(p+q)' = p' + q', \quad (pq)' = p'q + pq'.$$

SÆTNING. *Lad $a \in R$ være rod i polynomiet $p \in R[X]$. Da er a en rod af multiplicitet ≥ 2, netop når a også er rod i det afledede polynomium p'.*

Bevis. Prøv selv!♡

IDEALER I KOMMUTATIVE RINGE

I det følgende betegner R en **kommutativ** ring.

1. Idealer. Hovedidealer.

(1.1) Vi minder om, at et *ideal* i R er en delmængde $\mathcal{A} \subseteq R$, som opfylder:

(a1) $$a_1, a_2 \in \mathcal{A} \quad \Longrightarrow \quad a_1 + a_2 \in \mathcal{A}$$

(a2) $$0 \in \mathcal{A}$$

(a3) $$a \in \mathcal{A} \quad \Longrightarrow \quad -a \in \mathcal{A}$$

(m) $$a \in \mathcal{A} \wedge r \in R \quad \Longrightarrow \quad ra \in \mathcal{A}.$$

Betingelserne (a1), (a2), (a3) udsiger, at $\mathcal{A}$ er en undergruppe i ringens additive gruppe $(R, +)$. De *trivielle idealer* i R er delmængden $\{0\}$ og hele mængden R.

Observation. (a3) følger af (m), thi $-a = (-1)a$.

(1.2) Idealoperationerne. Det er let at se, at en vilkårlig fællesmængde af idealer i R igen er et ideal i R. For endelig mange idealer $\mathcal{A}_1, \ldots, \mathcal{A}_n$ i R er også delmængden

$$\mathcal{A}_1 + \cdots + \mathcal{A}_n := \{a_1 + \cdots + a_n \mid a_1 \in \mathcal{A}_1 \wedge \cdots \wedge a_n \in \mathcal{A}_n\}$$

et ideal i R. Det er øjensynlig det mindste ideal i R, der indeholder alle idealerne $\mathcal{A}_1, \ldots, \mathcal{A}_n$. For et element $a \in R$ er delmængden

$$Ra := \{ra \mid r \in R\}$$

et ideal i R, og det er øjensynlig det mindste ideal i R, som indeholder elementet a. For endelig mange elementer $a_1, \ldots, a_n \in R$ finder vi

$$Ra_1 + \cdots + Ra_n = \{r_1a_1 + \cdots + r_na_n \mid r_1, \ldots, r_n \in R\},$$

og dette ideal er øjensynlig det mindste ideal, der indeholder elementerne $a_1, \ldots, a_n$.

Definition. Idealet $\mathcal{A}_1 + \cdots + \mathcal{A}_n$ kaldes *summen* af idealerne $\mathcal{A}_1, \ldots, \mathcal{A}_n$.

Idealet Ra kaldes *idealet frembragt af* a, og det betegnes ofte (a). Et ideal $\mathcal{A} \subseteq R$, der har formen $\mathcal{A} = Ra$ med $a \in R$, kaldes et *hovedideal*.

Idealet $Ra_1 + \cdots + Ra_n$ kaldes *idealet frembragt* af $a_1, \ldots, a_n$. Hvis misforståelser er udelukket, betegnes det ofte $(a_1, \ldots, a_n)$. Et ideal $\mathcal{A} \subseteq R$, der har formen $\mathcal{A} = Ra_1 + \cdots + Ra_n$ med $a_1, \ldots, a_n \in R$, siges at være *endelig frembragt*.

OBSERVATION. De trivielle idealer i R kan skrives $\{0\} = (0)$ og $R = (1)$. De er altså hovedidealer.

(1.3) En vilkårlig foreningsmængde af idealer i R vil sædvanligvis ikke være et ideal. Herom gælder imidlertid følgende:

SÆTNING. *Lad $\mathcal{A}_1 \subseteq \mathcal{A}_2 \subseteq \ldots$ være en stigende følge af idealer i R. Da er foreningsmængden $\mathcal{A} := \bigcup_{n\in\mathbf{N}} \mathcal{A}_n$ et ideal.*

Bevis. Lad $a_1, a_2 \in \mathcal{A}$. Der findes da $n_1, n_2 \in \mathbf{N}$, så at $a_1 \in \mathcal{A}_{n_1}$, $a_2 \in \mathcal{A}_{n_2}$. Er $\mathcal{A}_m$ det største af idealerne $\mathcal{A}_{n_1}$ og $\mathcal{A}_{n_2}$, har vi således $a_1, a_2 \in \mathcal{A}_m$, og så er

$$a_1 + a_2 \in \mathcal{A}_m \subseteq \bigcup_n \mathcal{A}_n = \mathcal{A}.$$

Delmængden $\mathcal{A} \subseteq R$ opfylder således betingelsen (1.1)(a1). De øvrige betingelser er trivielt opfyldt♡

(1.4) DEFINITION. En ring R kaldes en *hovedidealring*, hvis alle dens idealer er hovedidealer. Er ringen R desuden et integritetsområde, kaldes den et *hovedidealområde*.

Følgende er et velkendt

RESULTAT. *De hele tals ring $\mathbf{Z}$ og enhver polynomiumsring $L[X]$, hvor L er et legeme, er hovedidealområder.*

Beviserne (for $\mathbf{Z}$ og for $L[X]$) har fælles træk, der abstrakt kan formuleres som en

NUMERISK BETINGELSE. *Antag, at der i ringen R er givet en funktion $\nu : R \to \mathbf{Z}$, som er nedad begrænset og har følgende egenskab: For ethvert $d \neq 0$ i R og ethvert $a \in R$ findes et element $q \in R$, så at*

$$\nu(a - qd) < \nu(d).$$

Da er R en hovedidealring.

Bevis. Lad $\mathcal{A} \subseteq R$ være et ideal. Vi skal vise, at der findes et element $d \in R$, således at $\mathcal{A} = Rd$. Hvis $\mathcal{A} = \{0\}$, kan vi bruge $d = 0$. Hvis $\mathcal{A} \supset \{0\}$, kan vi betragte det mindste af tallene

$$\nu(r), \quad \text{hvor } r \in \mathcal{A} \setminus \{0\}.$$

[Det findes, da funktionen ν er nedad begrænset]. Det har formen $\nu(d)$, hvor d er element i $\mathcal{A} \setminus \{0\}$. Nu gælder

$$\mathcal{A} = Rd,$$

thi da $d \in \mathcal{A}$ har vi trivielt "$\supseteq$", og er omvendt $a \in \mathcal{A}$, kan vi finde $q \in R$, så at $r := a - qd$ opfylder

$$\nu(r) < \nu(d).$$

Da $a \in \mathcal{A}$ og $qd \in Rd \subseteq \mathcal{A}$, vil også $r = a - qd \in \mathcal{A}$. Hvis $r \neq 0$, er $\nu(r) < \nu(d)$ i modstrid med valget af d. Følgelig har vi $r = 0$, og altså $a = qd \in Rd$ ♠

Bemærkning. For $R = \mathbf{Z}$ følger det af Divisionssætningen, at funktionen $\nu : p \mapsto |p|$ har ovennævnte egenskab. For $R = L[X]$, hvor L er et legeme, følger det af Divisionssætningen for polynomier, at funktionen $\nu : p \mapsto \deg(p)$ [hvor nulpolynomiet tillægges graden -1] har ovennævnte egenskab.

(1.5) Den opstigende kædes egenskab. *Lad R være en hovedidealring. I enhver voksende følge af idealer*

$$\mathcal{A}_1 \subseteq \mathcal{A}_2 \subseteq \dots$$

gælder da "$=$" fra et vist trin [dvs. der findes et $N \in \mathbf{N}$, så at $\mathcal{A}_N = \mathcal{A}_{N+1} = \dots$].

Bevis. Foreningsmængden $\mathcal{A} := \bigcup_{n\in\mathbf{N}} \mathcal{A}_n$ er et ideal ifølge Sætning (1.3). Da R er en hovedidealring, har vi $\mathcal{A} = Ra$, med et $a \in R$. Da $a \in Ra = \mathcal{A} = \bigcup_{n\in\mathbf{N}} \mathcal{A}_n$ findes et $N \in \mathbf{N}$, således at $a \in \mathcal{A}_N$. Men så vil $Ra \subseteq \mathcal{A}_N$, og af

$$Ra \subseteq \mathcal{A}_N \subseteq \mathcal{A}_{N+1} \subseteq \cdots \subseteq \bigcup_{n\in\mathbf{N}} \mathcal{A}_n = Ra$$

følger $\mathcal{A}_N = \mathcal{A}_{N+1} = \dots$ ♠

2. Primideal og maksimalideal.

(2.1) Der er som bekendt en bijektiv forbindelse mellem idealer i ringen R og kongruensrelationer i R. Den til idealet $\mathcal{A} \subseteq R$ hørende kongruensrelation $\underset{\mathcal{A}}{\equiv}$, kaldet kongruens modulo $\mathcal{A}$, er bestemt ved

$$x' \underset{\mathcal{A}}{\equiv} x \overset{\text{DEF}}{\iff} x' - x \in \mathcal{A}.$$

Den tilhørende kvotientring $R/\mathcal{A}$ består af ækvivalensklasserne, og den kanoniske afbildning : $x \mapsto \boxed{x}$, der afbilder et element $x \in R$ over i den ækvivalensklasse, der indeholder x, er en surjektiv ringhomomorfi

$$\boxed{\ } : R \to R/\mathcal{A}.$$

(2.2) Definition. Et ideal $\mathcal{P}$ i R kaldes et *primideal*, hvis $\mathcal{P} \subset R$ og der for alle $x, y \in R$ gælder:

$$xy \in \mathcal{P} \Rightarrow x \in \mathcal{P} \vee y \in \mathcal{P}.$$

(2.3) Bemærkning. Ifølge definitionen er det trivielle ideal R **ikke** et primideal i R. Det trivielle ideal (0) kan derimod godt være et primideal, idet der øjensynlig gælder:

Idealet (0) er et primideal i R, hvis og kun hvis R er et integritetsområde.

Mere generelt gælder følgende:

Karakterisering af primidealer. *Et ideal $\mathcal{P}$ i R er et primideal, hvis og kun hvis kvotientringen $R/\mathcal{P}$ er et integritetsområde.*

Bevis. "**hvis**": Da et integritetsområde ikke er nulringen, har vi $R/\mathcal{P} \neq 0$, og altså $\mathcal{P} \subset R$. Antag, at $xy \in \mathcal{P}$ og at $x \notin \mathcal{P}$. Da er $xy \equiv 0$ og $x \not\equiv 0$, og i $R/\mathcal{P}$ har vi derfor:

$$\boxed{x} \cdot \boxed{y} = \boxed{xy} = \boxed{0} \quad \text{og} \quad \boxed{x} \neq \boxed{0}.$$

Da nul-reglen gælder i $R/\mathcal{P}$, må vi have $\boxed{y} = \boxed{0}$, altså $y \in \mathcal{P}$.
"**kun hvis**": Da $\mathcal{P} \subset R$, er $R/\mathcal{P} \neq 0$, så vi skal blot vise, at nul-reglen gælder i $R/\mathcal{P}$. Lad altså X, Y være elementer i $R/\mathcal{P}$, så at

$$XY = \boxed{0} \quad \text{og} \quad X \neq \boxed{0}.$$

Vælges repræsentanter: $X = \boxed{x}$, $Y = \boxed{y}$, har vi $\boxed{xy} = \boxed{x} \cdot \boxed{y} = XY = \boxed{0}$, altså $xy \in \mathcal{P}$, og $\boxed{x} = X \neq \boxed{0}$, altså $x \notin \mathcal{P}$. Heraf følger $y \in \mathcal{P}$, og dermed $Y = \boxed{y} = \boxed{0}$ ♠

KOROLLAR. *Lad $\varphi : R \to R'$ være en ringhomomorfi. Hvis R' er et integritetsområde, så er φ's kerne et primideal.*

Bevis. Lad $\mathcal{P} := \varphi^{-1}(0)$ være kernen for φ. Ifølge Isomorfisætningen for ringe har vi en isomorfi:

$$R/\mathcal{P} \xrightarrow{\approx} \varphi(R).$$

Her er billedringen $\varphi(R) \subseteq R'$ en delring af et integritetsområde og dermed selv et integritetsområde. Det følger, at $R/\mathcal{P}$ er et integritetsområde, og $\mathcal{P}$ er derfor et primideal♠

(2.4) Mængden af idealer i R udgør, med inklusion $\subseteq$ som ordning, en (partielt) ordnet mængde.

DEFINITION. Et ideal $\mathcal{M}$ i R kaldes et *maksimalideal*, hvis det er maksimalt blandt idealerne $\subset R$.

Idealet $\mathcal{M}$ er således et maksimalideal, hvis $\mathcal{M} \subset R$ og der for alle idealer $\mathcal{A} \subseteq R$ gælder:

$$\mathcal{M} \subseteq \mathcal{A} \subset R \Rightarrow \mathcal{M} = \mathcal{A}.$$

OBSERVATION. Betingelsen kan udtrykkes således: Af idealer $\mathcal{A}$ i R, som opfylder

$$\mathcal{M} \subseteq \mathcal{A} \subseteq R,$$

findes der præcis 2, nemlig $\mathcal{A} = \mathcal{M}$ og $\mathcal{A} = R$.

(2.5) BEMÆRKNING. Ifølge definitionen er det trivielle ideal R **ikke** et maksimalideal. Det trivielle ideal (0) kan derimod godt være et maksimalideal, idet vi ifølge Observationen ovenfor har:

Idealet (0) er et maksimalideal, hvis og kun hvis R har præcis 2 idealer. Denne egenskab karakteriserer legemerne, idet der mere generelt gælder følgende:

KARAKTERISERING AF MAKSIMALIDEALER. *Et ideal $\mathcal{M}$ i R er et maksimalideal, hvis og kun hvis kvotientringen $R/\mathcal{M}$ er et legeme.*

Bevis. "**hvis**": Da et legeme ikke er nulringen, har vi $R/\mathcal{M} \neq 0$, og altså $\mathcal{M} \subset R$. Antag nu, at $\mathcal{A}$ er et ideal, så at

$$\mathcal{M} \subset \mathcal{A} \subseteq R.$$

Vi skal da vise, at $\mathcal{A} = R$. Vælg et element $a \in \mathcal{A} \setminus \mathcal{M}$. Da er $a \not\equiv 0$ modulo $\mathcal{M}$, og i $R/\mathcal{M}$ har vi derfor $\boxed{a} \neq \boxed{0}$. Da $R/\mathcal{M}$ er et legeme, er $\boxed{a}$ derfor invertibel, så der findes et element $X \in R/\mathcal{M}$, med $X \cdot \boxed{a} = \boxed{1}$. Vælges en repræsentant: $X = \boxed{x}$, har vi altså

$$\boxed{1} = X \cdot \boxed{a} = \boxed{x} \cdot \boxed{a} = \boxed{xa}.$$

Følgelig er $1 \equiv xa$, så vi kan skrive

$$1 = xa + m, \text{ hvor } m \in \mathcal{M}.$$

Da $a \in \mathcal{A}$, og $m \in \mathcal{M} \subseteq \mathcal{A}$, slutter vi, at også $1 \in \mathcal{A}$, men så er for et vilkårligt element $r \in R$ også

$$r = r1 \in \mathcal{A}.$$

Altså er $\mathcal{A} = R$.
"**kun hvis**": Da $\mathcal{M} \subset R$, er $R/\mathcal{M} \neq 0$, så vi skal blot vise, at hvert element $A \neq \boxed{0}$ i $R/\mathcal{M}$ er invertibelt. Vælg en repræsentant: $A = \boxed{a}$. Da $\boxed{a} = A \neq \boxed{0}$, er $a \notin \mathcal{M}$. Det følger for idealet $Ra + \mathcal{M}$, at vi har

$$\mathcal{M} \subset Ra + \mathcal{M},$$

og heraf følger, at $Ra + \mathcal{M} = R$. Specielt er $1 \in Ra + \mathcal{M}$, dvs. af formen

$$1 = xa + m, \quad x \in R,\, m \in \mathcal{M}.$$

Nu finder vi

$$\boxed{1} = \boxed{xa} = \boxed{x} \cdot \boxed{a} = \boxed{x} \cdot A,$$

og A er derfor invertibel (med $\boxed{x}$ som invers)♠

(2.6) Sætning. *Ethvert maksimalideal er et primideal.*

Bevis. Da et legeme er et integritetsområde, fås dette umiddelbart af Karakteriseringerne i (2.3) og (2.5)♠

(2.7) Sætning. *For et primtal p er restklasseringen $\mathbf{F}_p := \mathbf{Z}/\mathbf{Z}p$ et legeme.*

Bevis. Ifølge Karakteriseringen (2.5) skal vi vise, at idealet $\mathbf{Z}p$ i $\mathbf{Z}$ er et maksimalideal. Det er klart, at $\mathbf{Z}p \subset \mathbf{Z}$. Lad derfor $\mathcal{A} \subseteq \mathbf{Z}$ være et ideal, således at

$$\mathbf{Z}p \subseteq \mathcal{A} \subseteq \mathbf{Z}.$$

Vi skal vise, at $\mathcal{A} = \mathbf{Z}p$ eller $\mathcal{A} = \mathbf{Z}$. Ifølge Hovedidealsætningen har idealet $\mathcal{A}$ formen

$$\mathcal{A} = \mathbf{Z}d,$$

og vi kan antage $d \geq 0$. Af $p \in \mathbf{Z}p \subseteq \mathbf{Z}d$ følger, at p har formen $p = qd$, med $q \in \mathbf{Z}$. Dermed er $d \geq 0$ en divisor i p, og så er enten $d = p$, og altså $\mathcal{A} = \mathbf{Z}d = \mathbf{Z}p$, eller $d = 1$, og altså $\mathcal{A} = \mathbf{Z}d = \mathbf{Z}1 = \mathbf{Z}$♠

(2.8) Bemærkning. Under brug af Zorn's lemma kan man vise, at der til hvert ideal $\mathcal{A} \subset R$ findes et maksimalideal $\mathcal{M} \supseteq \mathcal{A}$. Hvis R er en hovedidealring, kan det bevises således: Enten er $\mathcal{A}$ selv et maksimalideal (og så er vi færdige), eller også er $\mathcal{A}$ ikke et maksimalideal, og så findes et ideal $\mathcal{A}_1$ med $\mathcal{A} \subset \mathcal{A}_1,\ \mathcal{A}_1 \subset R$. Her er enten $\mathcal{A}_1$ et maksimalideal (og så er vi færdige), eller $\mathcal{A}_1$ er ikke et maksimalideal, og så findes et ideal $\mathcal{A}_2$ med $\mathcal{A}_1 \subset \mathcal{A}_2,\ \mathcal{A}_2 \subset R$. Her er enten $\ldots$ $\cdots$. Af Den opstigende kædes egenskab (1.5) følger, at dette kun kan fortsætte et endeligt antal skridt. Og når det stopper, er vi nået til et maksimalideal.

3. Faktorielle ringe.

Vi vil her forudsætte, at den kommutative ring R er et **integritetsområde**. Af en ligning $rx = ry$, hvor $r \neq 0$, følger altså, at $x = y$.

(3.1) DEFINITIONER. Et element $u \in R$ kaldes en *enhed*, hvis det er invertibelt, dvs. hvis $u \in R^*$.

Et element $a \in R$ kaldes *associeret med* et element $b \in R$, hvis der findes en enhed $u \in R^*$, så at $a = ub$.

Et element $d \in R$ siges at være *divisor* i elementet $a \in R$, eller at *gå op i* a, hvis der findes et element $r \in R$, så at $rd = a$. I så fald skrives

$$d \,|\, a,$$

og a kaldes et *multiplum af* d, eller siges at være *delelig* med d. Bemærk, at der gælder: $d \,|\, a \;\Leftrightarrow\; a \in Rd$.

De *trivielle divisorer* i et element a er enhederne og elementerne associerede med a.

Et element $q \in R$ kaldes *irreducibelt*, hvis $q \notin \{0\} \cup R^*$ og q kun har trivielle divisorer.

Et element $p \in R$ kaldes et *primelement*, hvis $p \notin \{0\} \cup R^*$ og der for alle $x, y \in R$ gælder:

$$p \,|\, xy \quad \Rightarrow \quad p \,|\, x \vee p \,|\, y.$$

(3.2) OBSERVATION. Et element $p \notin \{0\} \cup R^*$ er irreducibelt, hvis og kun hvis der af en ligning $p = d_1 d_2$ følger, at d_1 eller d_2 er en enhed.

SÆTNING. *Ethvert primelement $p \in R$ er irreducibelt.*

Bevis. Antag, at $p = d_1 d_2$. Vi skal vise, at d_1 eller d_2 er en enhed. Vi har specielt $p \,|\, d_1 d_2$, så p går op i en af faktorerne, f.eks. i d_2. Vi kan altså skrive $up = d_2$ med $u \in R$, og så får vi $p = d_1 d_2 = d_1 up$. Da $p \neq 0$, får vi $1 = d_1 u$, og d_1 er således en enhed (med $d_1^{-1} = u$)♠

(3.3) KARAKTERISERING VED HOVEDIDEALER. SÆTNING. *I et integritetsområde R afspejler de indførte begreber sig i relationer mellem hovedidealer, idet der gælder:*

(1) *u er en enhed* $\iff (u) = R (= (1))$.
(2) *a er associeret med b* $\iff (a) = (b)$.
(3) *d er divisor i a* $\iff (a) \subseteq (d)$.
(4) *d er triviel divisor i a* $\iff (d) = R \vee (d) = (a)$.
(5) *q irreducibelt* $\iff q \neq 0$ *og* (q) *er maksimalt blandt hovedidealer* $\subset R$.
(6) *p er et primelement* $\iff p \neq 0$ *og* (p) *er et primideal.*

Bevis. **(1):** Hvis u er en enhed, findes $v \in R$ med $vu = 1$, og så gælder for hvert $r \in R$, at $r = r1 = (rv)u \in (u)$. Er omvendt $(u) = R$, så er specielt $1 \in (u)$, og altså $1 = vu$, med $v \in R$.
(2): Hvis a er associeret med b, altså $a = ub$, hvor $u \in R^*$, så er $ra = rub \in (b)$, og altså $(a) \subseteq (b)$, og da vi også har $b = va$ (med $v = u^{-1}$), får vi tilsvarende $(b) \subseteq (a)$. Er omvendt $(a) = (b)$, så har vi $a \in (a) = (b)$, altså $a \in (b)$, og tilsvarende $b \in (a)$, og kan skrive

$$a = ub, \qquad b = va, \qquad u, v \in R.$$

Hvis $b = 0$, får vi straks $a = 0$. Hvis $b \neq 0$, følger det af $b = va = vub$, at $1 = vu$. Elementet u er derfor en enhed, og a er følgelig associeret med b.
(3): Vi har: $d \mid a \Leftrightarrow a \in (d) \Leftrightarrow (a) \subseteq (d)$.
(4): Følger umiddelbart af (1) og (2).
(5): Ifølge (3) og (4) svarer divisorerne d i q netop til de hovedidealer (d), som opfylder

$$(q) \subseteq (d) \subseteq R,$$

og d er triviel divisor i q, hvis og kun hvis der her gælder et af de to mulige "=" (altså $(q) = (d)$ eller $(d) = R$). Heraf følger påstanden umiddelbart.
(6): Idet $p \mid xy \Leftrightarrow xy \in (p)$, $p \mid x \Leftrightarrow x \in (p)$ og $p \mid y \Leftrightarrow y \in (p)$, fås påstanden direkte ud fra definitionen på et primideal♠

(3.4) Sætning. *Lad R være et hovedidealområde. Da er et element $p \in R$ irreducibelt, hvis og kun hvis det er et primelement. Hovedidealet (p) frembragt af et sådant element er et maximalideal i R.*

Bevis. **"hvis":** gælder i ethvert integritetsområde, jfr. Sætning (3.2).
"kun hvis": Lad $p \in R$ være irreducibelt. Ifølge Sætning (3.3)(5) er idealet (p) maksimalt blandt hovedidealer $\subset R$. Da alle idealer i R er hovedidealer, betyder det, at (p) er et maksimalideal i R. Heraf følger, at (p) er et primideal, jfr. Sætning (2.6). Da $p \neq 0$, slutter vi heraf (Sætning (3.3)(6)), at p er et primelement.

Den sidste påstand så vi undervejs♠

(3.5) Definition. Er der i R givet elementer $a, d_1, \ldots, d_s$ så at $a = d_1 \cdots d_s$, siger vi kort, at $a = d_1 \cdots d_s$ er en *opløsning* af a i faktorerne $d_1, \ldots, d_s$. Opløsningen kaldes *irreducibel*, hvis faktorerne er irreducible, og en *primopløsning*, hvis faktorerne er primelementer.

Bemærkning. Ethvert element $a \in R$ har trivielle opløsninger af formen $a = u(u^{-1}a)$, hvor den ene faktor u er en enhed (og den anden er associeret med a). Ifølge Observation (3.2) har et irreducibelt element kun sådanne trivielle opløsninger. I en irreducibel opløsning $a = q_1 \cdots q_s$ kan faktorerne q_i altså kun trivielt opløses yderligere.

(3.6) Sætning. *Primopløsninger er entydige i følgende forstand: Er $p_1, \ldots, p_s$ og $q_1, \ldots, q_t$ primelementer i R, og er $p_1 \cdots p_s$ associeret med $q_1 \cdots q_t$, så er $s = t$, og der gælder efter en passende permutation af q_i'erne, at p_i er associeret med q_i for $i = 1, \ldots, s$.*

Bevis. Der findes en enhed $u \in R$, så at

$$up_1 \cdots p_s = q_1 \cdots q_t.$$

Da primelementet p_s således går op i produktet $q_1 \cdots q_t$, må det gå op i et af q_i'erne. Vi kan antage, at p_s går op i q_t. Da q_t er irreducibel (Sætning (3.2)), må p_s endda være en triviel divisor i q_t, og da p_s ikke er en enhed, må p_s være associeret med q_t. Vi har altså $p_s = vq_t$, med en enhed $v \in R$, og får ved indsættelse:

$$uvp_1 \cdots p_{s-1}q_t = q_1 \cdots q_{t-1}q_t.$$

Da $q_t \neq 0$ følger heraf, at

$$(uv)p_1 \cdots p_{s-1} = q_1 \cdots q_{t-1},$$

og $p_1 \cdots p_{s-1}$ er derfor associeret med $q_1 \cdots q_{t-1}$.

Ved at fortsætte således fås det ønskede♠

(3.7) Definition. Integritetsområdet R kaldes en *faktoriel ring*, hvis ethvert element $a \notin \{0\} \cup R^*$ i R kan skrives som et produkt $a = p_1 \cdots p_s$ af primelementer $p_1, \ldots, p_s$.

I en faktoriel ring R har altså ethvert element $a \notin \{0\} \cup R^*$ en primopløsning $a = p_1 \cdots p_s$, og af sætningen ovenfor fremgår, at disse opløsninger (bortset fra "permutation og associering") er entydige.

Sætning. *For et integritetsområde R er følgende betingelser ækvivalente:*

(i) *R er en faktoriel ring.*

(ii)
- (a) *Hvert element $a \notin \{0\} \cup R^*$ har en irreducibel opløsning*
- *og*
- (b) *Hvert irreducibelt element i Rer et primelement.*

(iii)
- (a) *Hvert element $a \notin \{0\} \cup R^*$ har en irreducibel opløsning*
- *og*
- (c) *Irreducible opløsninger er entydige.*

Bemærkning. Med den i (c) nævnte entydighed menes: Hvis $p_1, \ldots, p_s, q_1, \ldots, q_t$ er irreducible elementer i R, således at $p_1 \cdots p_s = q_1 \cdots q_t$, så er $s = t$ og (bortset fra "permutation og associering") $p_i = q_i$ for $i = 1, \ldots, s$.

Bevis for sætningen. Det er klart, at (a) $\wedge$ (b) $\Rightarrow$ (i). Af Sætning (3.2) følger (i) $\Rightarrow$ (a), og af Sætning (3.6) fås (b) $\Rightarrow$ (c). Det er derfor nok at vise, at (i) $\Rightarrow$ (b), og at (a) $\wedge$ (c) $\Rightarrow$ (b).
(i) $\Rightarrow$ (b): Lad q være et irreducibelt element, og betragt en primopløsning af q. Da q er irreducibelt, har det kun trivielle opløsninger. Primopløsningen har derfor kun én faktor, og q er derfor et primelement.
(a) $\wedge$ (c) $\Rightarrow$ (b): Lad q være et irreducibelt element, og antag, at $q|xy$. Vi skal vise, at $q|x$ eller $q|y$. Det er oplagt, hvis x eller y er $= 0$ eller en enhed. I modsat fald skriver vi

$$rq = xy, \quad \text{hvor } r \in R,$$

og her er $r \neq 0$. Ifølge (a) kan vi finde irreducible opløsninger: $x = x_1 \cdots x_s$ og $y = y_1 \cdots y_t$ og $r = r_1 \cdots r_n$ [i det mindste, hvis r ikke er en enhed. Overvej selv hvorledes det følgende skal modificeres, hvis r er en enhed!]. Indsættes, fås:

$$r_1 \cdots r_n q = x_1 \cdots x_s y_1 \cdots y_t.$$

Ifølge (c) må den irreducible faktor q på venstre side også forekomme (på nær associering) på højre side. Vi kan antage, at q er associeret med x_1. Men så er q specielt divisor i x_1, og dermed også divisor i $x = x_1(x_2 \cdots x_s)\heartsuit$

(3.8) Lemma. *Lad R være et integritetsområde, hvori der findes et element $a \notin \{0\} \cup R^*$, der ikke kan skrives som et produkt af irreducible elementer. Da findes i R en uendelig følge af elementer*

$$(a =)\, a_0, a_1, a_2, \ldots,$$

således at a_i er en ikke-triviel divisor i a_{i-1} for $i = 1, 2, \ldots$

Bevis. Ifølge forudsætningen findes i R et element a, der har følgende egenskab:

$(*)$ $a \notin \{0\} \cup R^*$ og a kan ikke skrives som produkt af irreducible elementer.

Et sådant element kan specielt ikke selv være irreducibelt, så det kan skrives

$$a = a'a'',$$

hvor a' og a'' er ikke-trivielle divisorer i a. Specielt er begge divisorer $\neq$ enhed, og da $a'a'' = a \neq 0$, er begge divisorer $\neq 0$. Hvis både a' og a'' var et produkt af irreducible elementer, ville vi ved indsættelse i $a = a'a''$ se, at a var et produkt af irreducible elementer i modstrid med antagelsen. Følgelig vil mindst en af de to divisorer opfylde, at den ikke kan skrives som et produkt af irreducible, og denne divisor vil altså have egenskaben $(*)$.

Vi har vist, at hvert element med egenskaben $(*)$ har en ikke-triviel divisor med egenskaben $(*)$.

Startende med $a_0 = a$ kan vi derfor finde en følge som ønsket (endda således at hvert a_i har egenskaben $(*)$)♠

KOROLLAR 1. *Antag, at der i integritetsområdet R er givet en funktion $\nu : R \to \mathbf{Z}$, som er nedad begrænset og har følgende egenskab: For hvert $a \neq 0$ i R og hver ikke-triviel divisor a_1 i a gælder*

$$\nu(a_1) < \nu(a).$$

Da har hvert element $a \notin \{0\} \cup R^*$ en irreducibel opløsning.

Bevis. I modsat fald ville der findes en uendelig følge $a_0, a_1, a_2, \ldots$ som angivet i Lemma'et, og så ville

$$\nu(a_1) > \nu(a_2) > \cdots$$

være i modstrid med at $\nu : R \to \mathbf{Z}$ var nedad begrænset♠

KOROLLAR 2. *Lad R være et hovedidealområde. Da har hvert $a \notin \{0\} \cup R^*$ en irreducibel opløsning.*

Bevis. I modsat fald ville der findes en uendelig følge $a_0, a_1, a_2, \ldots$ som angivet i Lemma'et, og så ville

$$(a_0) \subset (a_1) \subset (a_2) \subset \ldots$$

være i modstrid med Den opstigende kædes egenskab (1.5)♠

(3.9) Vi samler nu resultaterne om hovedidealområder i følgende:

HOVEDSÆTNING. *Lad R være et hovedidealområde. Da er R en faktoriel ring. Primidealerne $\neq (0)$ i R er netop idealerne af formen (p), hvor p er irreducibel, og disse idealer er maksimalidealer.*

Bevis. R er en faktoriel ring ifølge Sætning (3.7), thi betingelsen (ii,a) følger af Korollar (3.8)(2) ovenfor, og betingelsen (ii,b) er indeholdt i Sætning (3.4). Af Sætning (3.4) følger videre, at idealer af formen (p), hvor p er irreducibelt, er maksimalidealer, og er omvendt $\mathcal{P} \neq (0)$ et primideal, så er $\mathcal{P}$ et hovedideal $\mathcal{P} = (p)$ (da R var en hovedidealring), og p er et primelement, og dermed irreducibelt♠

(3.10) ANVENDELSE PÅ $\mathbf{Z}$. De hele tals ring $\mathbf{Z}$ er en faktoriel ring. I $\mathbf{Z}$ er enhederne ± 1. Ethvert helt tal $\neq 0$ er således associent med netop et positivt tal. De positive irreducible elementer er netop primtallene. Primidealerne $\neq (0)$ i $\mathbf{Z}$ er altså idealerne af formen $(p) = \mathbf{Z}p$, hvor p er et primtal, og disse idealer er maksimalidealer (og kvotienten $\mathbf{F}_p := \mathbf{Z}/\mathbf{Z}p$ er altså et legeme). Videre er $(0) \subset \mathbf{Z}$ et primideal, der ikke er et maksimalideal.

(3.11) Anvendelse på $L[X]$. Enhver polynomiumsring $L[X]$, hvor L er et legeme, er en faktoriel ring. I $L[X]$ er enhederne konstanterne $\neq 0$. Ethvert polynomium $\neq 0$ er således associeret med netop ét normeret polynomium.

For et normeret irreducibelt polynomium

$$p = X^n + p_{n-1}X^{n-1} + \cdots + p_1X + p_0 \in L[X],$$

er kvotienten $K := L[X]/(p)$ altså et legeme. Ifølge Struktursætningen for polynomiumskvotienter indeholder det således konstruerede legeme K det givne legeme L som dellegeme, og sætter vi $\xi := \boxed{X} \in K$, kan hvert element i K entydigt skrives

$$r_0 + r_1\xi + \cdots + r_{n-1}\xi^{n-1}, \quad r_0, r_1, \ldots, r_{n-1} \in L.$$

Endvidere er $\xi^n = -p_0 - p_1\xi - \cdots - p_{n-1}\xi^{n-1}$.

Eksempel. Polynomiet $X^2 + 1 \in \mathbf{R}[X]$ er irreducibelt, thi ellers var det et produkt af to 1^{ste}-gradspolynomier i $\mathbf{R}[X]$, og så ville det have en rod i $\mathbf{R}$.

Det følger, at vi kunne indføre følgende

Definition. De komplexe tals legeme $\mathbf{C}$ er kvotienten

$$\mathbf{C} := \mathbf{R}[X]/(X^2 + 1),$$

thi dette legeme indeholder $\mathbf{R}$, og sætter vi $i := \boxed{X} \in \mathbf{C}$, kan hvert element i $\mathbf{C}$ entydigt skrives

$$r_0 + r_1 i, \qquad r_0, r_1 \in \mathbf{R}.$$

Da vi endvidere har $i^2 = -1$, harmonerer dette med den sædvanlige definition af $\mathbf{C}$.

Bemærkning. Spørgsmålet om hvilke polynomier i $L[X]$, der er irreducible, afhænger i høj grad af hvilket legeme L, der betragtes. I almindelighed er alle 1^{ste}-grads polynomier irreducible, og 2^{den}- og 3^{die}-grads polynomier er irreducible, netop når de ikke har rødder i L.

Algebraens fundamentalsætning udsiger, at i $\mathbf{C}[X]$ er de irreducible polynomier netop 1^{ste}-gradspolynomierne. Heraf følger let, at i $\mathbf{R}[X]$ er de irreducible polynomier netop 1^{ste}-gradspolynomierne og de 2^{den}-gradspolynomier, der ikke har reelle rødder.

Man kan vise, at polynomierne $X^n - 2$ for $n = 1, 2, 3, \ldots$ er irreducible polynomier i $\mathbf{Q}[X]$. I $\mathbf{Q}[X]$ findes altså irreducible polynomier af enhver grad ≥ 1.

(3.12) I en faktoriel ring R tænkes ofte valgt et *repræsentantsystem* Π for primelementerne, dvs. en mængde Π af primelementer med den egenskab, at ethvert primelement i R er associent med netop ét primelement i Π. Efter et sådant valg kan primelementerne q i R altså entydigt skrives

$$q = up, \quad \text{med } u \in R^* \text{ og } p \in \Pi.$$

Indsætter vi i en primopløsning

$$a = q_1 \cdots q_k$$

for de enkelte faktorer q_i en sådan fremstilling: $q_i = u_i p_i$, hvor $u_i \in R^*$ og $p_i \in \Pi$, får vi en opløsning af formen

$$a = u p_1^{\nu_1} \cdots p_k^{\nu_k},$$

hvor $u \in R^*$, elementerne $p_1, \ldots, p_k \in \Pi$ er indbyrdes forskellige og $\nu_1, \ldots, \nu_k \in \mathbf{N}$. Idet vi om fornødent tilføjer potenser med eksponent 0, kan opløsningen skrives

$$a = u \prod_{p \in \Pi} p^{\nu_p},$$

hvor u er en enhed og kun endelig mange af eksponenterne ν_p, hvor $p \in \Pi$, er > 0. Denne fremstilling, som vi ofte også kalder *primopløsningen* af a, er entydig i den forstand, at enheden u og eksponenterne $\nu_p \geq 0$, for $p \in \Pi$, er entydigt bestemt ved a. Det ses, at også enhederne i R har en sådan opløsning, nemlig med alle $\nu_p = 0$.

Af entydigheden følger, at hvis et element $b \in R \setminus \{0\}$ har primopløsningen

$$b = w \prod_{p \in \Pi} p^{\mu_p},$$

så er b divisor i a, netop når $\mu_p \leq \nu_p$ for alle $p \in \Pi$.

Specielt ses, at "på nær associering" er antallet af divisorer i et element $a \neq 0$ med primopløsningen

$$a = u \prod_{p \in \Pi} p^{\nu_p},$$

bestemt som tallet

$$\prod_{p \in \Pi} (\nu_p + 1),$$

idet jo $\nu_p + 1$ er antallet af eksponenter μ_p med $0 \leq \mu_p \leq \nu_p$.

4. Største fælles divisor.

(4.1) DEFINITION. Lad a, b være elementer i et integritetsområde R. Et element $c \in R$, som er divisor i a og i b, kaldes en *fælles divisor* for a og b, og c kaldes en *største fælles divisor* for a og b, hvis c er en fælles divisor for a og b, og hvis der for enhver fælles divisor d for a og b gælder, at d er divisor i c.

At a og b kun har enhederne som fælles divisorer betyder således, at $c = 1$ er en største fælles divisor for a og b. Er dette tilfældet siges a og b at være *primiske*.

Tilsvarende defineres største fælles divisor for endelig mange elementer $a_1, \ldots, a_n$ i R, og vi siger, at $a_1, \ldots, a_n$ *er primiske*, hvis de har 1 som største fælles divisor.

BEMÆRKNING. At $a_1, \ldots, a_n \in R$ er primiske, er svagere end at elementerne er parvis primiske. F.eks. er tallene $6, 10, 15 \in \mathbf{Z}$ primiske, men (slet) ikke parvis primiske.

OBSERVATION. Betingelsen for at et element $c \in R$ er største fælles divisor for a og b kan skrives på en af følgende ækvivalente måder:

(i) $$\forall d \in R : d|a \wedge d|b \Leftrightarrow d|c$$

(ii) $$\forall d \in R : a \in (d) \wedge b \in (d) \Leftrightarrow (c) \subseteq (d)$$

(iii) $$\forall d \in R : (a, b) \subseteq (d) \Leftrightarrow (c) \subseteq (d)$$

(iv) $$\bigcap\{(d) \mid (a, b) \subseteq (d)\} = (c),$$

hvor der for (ii) $\Leftrightarrow$ (iii) udnyttes, at et ideal indeholder både a og b, netop når det indeholder idealet $(a, b) = Ra + Rb$ frembragt af a og b.

(4.2) SÆTNING. *Elementer a, b i et integritetsområde R har en største fælles divisor, hvis og kun hvis fællesmængden*

$$\bigcap\{(d) \mid (a, b) \subseteq (d)\}$$

er et hovedideal. I bekræftende fald er de største fælles divisorer for a og b netop frembringerne for dette hovedideal.

Bevis. Følger umiddelbart af Observation (4.1)(iv) ovenfor♠

(4.3) SÆTNING. *Hvis R er et hovedidealområde, så har elementer $a, b \in R$ altid en største fælles divisor. De største fælles divisorer for a og b er netop frembringerne for (hoved-)idealet $(a, b) = Ra + Rb$. Elementerne a og b er primiske, hvis og kun hvis der findes elementer $x, y \in R$, så at $xa + yb = 1$.*

Bevis. I et hovedidealområde er idealet (a, b) selv et hovedideal. De første påstande følger derfor umiddelbart af Sætning (4.2). Endvidere har vi $(a, b) = (1) = R$, netop når $1 \in (a, b)$, og det er jo den sidste påstand♠

BEMÆRKNING. Tilsvarende ses i et hovedidealområde R, at de største fælles divisorer for elementer $a_1, \ldots, a_n$ netop er frembringerne for (hoved-)idealet $(a_1, \ldots, a_n)$, og at $a_1, \ldots, a_n$ er primiske, hvis og kun hvis der findes elementer $x_1, \ldots, x_n \in R$, så at $x_1a_1 + \cdots + x_na_n = 1$.

NOTATION. I et hovedidealområde skrives ofte "$(a, b) = c$" i betydningen "c er en største fælles divisor for a og b". Skrivemåden "$(a, b) = 1$" udtrykker altså, at a og b er primiske.

(4.4) Vi har tidligere set, at hvis der i et integritetsområde R er givet en funktion $\nu : R \to \mathbf{Z}$, som er nedad begrænset og har følgende egenskab: For hvert $d \neq 0$ i R og hvert $a \in R$ findes et $q \in R$, så at

$$\nu(a - qd) < \nu(d),$$

så er R et hovedidealområde (Sætning (1.4)). Specielt har altså i en sådan ring to elementer a og b altid en største fælles divisor. En sådan kan bestemmes under brug af:

EUKLIDS ALGORITME. *Lad a og b være elementer $\neq 0$ i R. Antag, at $\nu(a) \geq \nu(b)$ og sæt $d_0 := a, \quad d_1 := b$.*
Da $d_1 \neq 0$, *kan vi bestemme $q_1 \in R$, så at*

$$\nu(d_0 - q_1d_1) < \nu(d_1), \text{ og vi sætter } d_2 := d_0 - q_1d_1.$$

Hvis $d_2 \neq 0$, *bestemmes $q_2 \in R$, så at*

$$\nu(d_1 - q_2d_2) < \nu(d_2), \text{ og vi sætter } d_3 := d_1 - q_2d_2.$$

Hvis $d_3 \neq 0$, *bestemmes $q_3 \in R$, så at*

$$\nu(d_2 - q_3d_3) < \nu(d_3), \text{ og vi sætter } d_4 := d_2 - q_3d_3.$$

Osv.

Denne proces vil stoppe efter endelig mange skridt, i den forstand, at der findes et $n \geq 1$, så at

$$d_{n-1} - q_nd_n = 0.$$

For dette n er d_n en største fælles divisor for $a = d_0$ og $b = d_1$.

Bevis. Hvis processen ikke stoppede, ville vi få en uendelig følge $d_0, d_1, d_2, \ldots$, og

$$\nu(d_0) \geq \nu(d_1) > \nu(d_2) > \ldots$$

ville være i modstrid med at funktionen ν var nedad begrænset.

For elementer $x, y, q \in R$ har vi øjensynlig

$$(x, y) = (x - qy, y).$$

Det følger, at vi har

$$\begin{aligned}(a, b) &= (d_0, d_1) = (d_0 - q_1 d_1, d_1) = (d_2, d_1) \\ &= (d_1, d_2) = (d_1 - q_2 d_2, d_2) = (d_3, d_2) \\ &= (d_2, d_3) = \dots \\ &= (d_{n-1}, d_n) = (d_{n-1} - q_n d_n, d_n) = (0, d_n) \\ &= (d_n)\end{aligned}$$

Idealet (a, b) er således (hoved-)idealet (d_n)♠

(4.5) I en faktoriel ring R kan spørgsmål om delelighed afgøres ud fra primopløsninger, jfr. (3.12). Vi får derfor umiddelbart følgende:

SÆTNING. *Hvis R er en faktoriel ring, så har elementer $a, b \in R$ altid en største fælles divisor. Er der i R valgt et repræsentantsystem Π for primelementerne, og er der givet primopløsninger*

$$a = up_1^{\nu_1} \dots p_r^{\nu_r}, \quad b = vp_1^{\mu_1} \dots p_r^{\mu_r}, \quad \textit{hvor } u, v \in R^* \textit{ og } p_i \in \Pi,$$

så er de største fælles divisorer netop elementerne associerede med

$$c = p_1^{\lambda_1} \dots p_r^{\lambda_r},$$

hvor $\lambda_i = \min\{\nu_i, \mu_i\}$ for $i = 1, \dots, r$ ♠

(4.6) LEMMA. *Lad der i en faktoriel ring R være givet* **parvis** *primiske elementer $d_1, \dots, d_n$, og sæt*

$$a_i := d_1 \dots d_{i-1} d_{i+1} \dots d_n, \quad i = 1, \dots, n.$$

Da er elementerne $a_1, \dots, a_n$ primiske.

Bevis. I modsat findes et primelement p, der er divisor i alle a_i´erne. Da p går op i $a_1 = d_2 \dots d_n$, vil p gå op i en af faktorerne, f.eks. i d_j. Da p også går op i $a_j = \prod_{i \neq j} d_i$, vil p gå op i et d_i, hvor $i \neq j$. Men så er p en fælles divisor for d_j og d_i i modstrid med, at d_j og d_i var primiske♠

(4.7) Da et hovedidealområde er en faktoriel ring, kan vi i et hovedidealområde kombinere Sætning (4.3) med ovenstående resultater. Som en anvendelse viser vi:

DEN KINESISKE RESTKLASSESÆTNING. *Lad der i et hovedideal område R være givet* **parvis** *primiske elementer $d_1, \ldots, d_n$, og sæt $d := d_1 \ldots d_n$. Lad $\boxed{x}_i$ betegne ækvivalensklasse modulo idealet (d_i) for $i = 1, \ldots, n$. Den ved*

$$x \mapsto (\boxed{x}_1, \ldots, \boxed{x}_n)$$

bestemte ringhomomorfi $: R \to R/(d_1) \times \cdots \times R/(d_n)$ er da surjektiv, og dens kerne er hovedidealet (d).

Bevis. Sættes $a_i := d_1 \ldots d_{i-1} d_{i+1} \ldots d_n$, har vi

$$d = a_i d_i \quad \text{for } i = 1, \ldots, n \tag{1}$$

$$a_i \in (d_j) \quad \text{for } i, j = 1, \ldots, n \text{ og } j \neq i. \tag{2}$$

Ifølge Lemma (4.6) er $a_1, \ldots, a_n$ primiske, og da R er et hovedidealområde, findes i R elementer $r_1, \ldots, r_n$, så at

$$r_1 a_1 + \cdots + r_n a_n = 1 \tag{3}$$

Kernen: At x tilhører kernen, betyder, at $x \in (d_i), i = 1, \ldots, n$. Af (1) følger så, at $a_i x \in (d), i = 1, \ldots, n$, og så vil også

$$x = (r_1 a_1 + \cdots + r_n a_n)x = r_1 a_1 x + \cdots + r_n a_n x \in (d).$$

Omvendt er det klart, at hvert element i (d) tilhører kernen.
Surjektivitet: Hvert element y i produktringen $R/(d_1) \times \cdots \times R/(d_n)$ er af formen $y = (\boxed{y_1}_1, \ldots, \boxed{y_n}_n)$, hvor $y_1, \ldots, y_n \in R$. Sæt

$$x = r_1 a_1 y_1 + \ldots, + r_n a_n y_n \in R,$$

og slut v.hj.a. (2) og (3), at $x \equiv r_j a_j y_j \equiv y_j$ modulo (d_j), og altså, at billedet af x er $(\boxed{x}_1, \ldots, \boxed{x}_n) = y \heartsuit$

KOROLLAR. *Homomorfien inducerer en isomorfi:*

$$R/(d) \xrightarrow{\sim} R/(d_1) \times \cdots \times R/(d_n) \heartsuit$$

5. Gauss' sætning.

(5.1) Vi betragter ringen $R[X]$ af polynomier med koefficienter i ringen R. Enhederne i $R[X]$ er som bekendt de invertible konstanter, dvs. enhederne i R. At et polynomium $A \in R[X]$ er deleligt med en konstant $d \in R$, betyder, at alle A's koefficienter er delelige med d. Hovedidealet $dR[X]$ frembragt af d i $R[X]$ består altså af de polynomier, hvis koefficienter alle tilhører hovedidealet $dR \subseteq R$.

SÆTNING. *Hvis p er et primelement i R, så er p ligeledes et primelement i $R[X]$.*

Bevis. Den kanoniske homomorfi : $R \to R/pR$, der til et element $a \in R$ lader svare restklassen $\boxed{a} \in R/pR$ kan udvides til en afbildning : $R[X] \to (R/pR)[X]$ betegnet $A \mapsto \bar{A}$, idet vi for et polynomium

$$A = a_0 + a_1X + \cdots + a_nX^n \in R[X]$$

sætter

$$\bar{A} = \boxed{a_0} + \boxed{a_1}X + \cdots + \boxed{a_n}X^n \in (R/pR)[X].$$

Det er klart, at $A \mapsto \bar{A}$ er en ringhomomorfi:

$$R[X] \to R/pR[X],$$

hvis kerne er hovedidealet $pR[X]$.

Er p et primelement i R, altså pR et primideal i R, så er kvotienten R/pR et integritetsområde, og følgelig er også polynomiumsringen $R/pR[X]$ et integritetsområde. Homomorfiens kerne, altså $pR[X]$, er derfor et primideal i $R[X]$, men det betyder netop, at p er et primelement i $R[X]$♠

(5.2) DEFINITION. Et polynomium $A \in R[X]$ kaldes *primitivt*, hvis dets koefficienter er primiske i R. Dette betyder altså, at de eneste konstanter, der er divisorer i polynomiet A, er de trivielle, dvs. enhederne.

(5.3) GAUSS' LEMMA. *Lad R være en faktoriel ring. Hvis $A, B \in R[X]$ er primitive polynomier, så er også produktet AB et primitivt polynomium.*

Bevis. At elementer i en faktoriel ring er primiske, er ensbetydende med, at intet primelement er divisor i dem alle. Var AB ikke et primitivt polynomium, ville der i R findes et primelement p, som var divisor i AB. Da p også er et primelement i $R[X]$ (Sætning (5.1)), kunne vi slutte, at p var divisor i A eller i B, i modstrid med at både A og B var primitive polynomier♠

(5.4) Udover integritetsområdet R betragter vi dets brøklegeme K og polynomiumsringen $K[X]$. Vi har da

$$\begin{array}{ccc} R & \subseteq & R[X] \\ \bigcap| & & \bigcap| \\ K & \subseteq & K[X] \end{array}$$

LEMMA. *Hvis R er faktoriel, så kan ethvert polynomium $\Phi(X) \neq 0$ i $K[X]$ skrives*

$$\Phi(X) = \frac{a}{s}F(X),$$

hvor $a, s \in R$ er primiske, og hvor $F(X)$ er et primitivt polynomium i $R[X]$.

Bevis. Koefficienterne i $\Phi(X)$ er jo endelig mange brøker. For disse kan vi finde en fælles nævner t (f.eks. produktet af alle nævnerne), dvs. vi kan skrive

$$\Phi(X) = \frac{a_0}{t} + \frac{a_1}{t}X + \cdots + \frac{a_n}{t}X^n = \frac{1}{t}(a_0 + a_1X + \cdots + a_nX^n),$$

hvor $a_0, \ldots, a_n \in R$. Er d en største fælles divisor for $a_0, \ldots, a_n$, kan vi skrive

$$a_0 + a_1X + \ldots a_nX^n = dF(X),$$

hvor $F(X)$ er et primitivt polynomium. Vi får så

$$\Phi(X) = \frac{d}{t}F(X),$$

og forkortes brøken $\frac{d}{t}$ med en største fælles divisor for d og t, får vi den ønskede fremstilling♠

(5.5) KOROLLAR TIL GAUSS' LEMMA. *Lad R være en faktoriel ring, lad $A(X) \in R[X]$ være et primitivt polynomium og lad $\Phi(x) \in K[X]$ være et polynomium med koefficienter i brøklegemet K. Hvis $\Phi(X)A(X) \in R[X]$, så vil $\Phi(X) \in R[X]$.*

Bevis. Ifølge Lemma (5.4) kan vi skrive

$$\Phi(X) = \frac{a}{s}F(X),$$

hvor $a, s \in R$ er primiske, og hvor $F(X) \in R[X]$ er et primitivt polynomium, og vi viser, at elementet s må være en enhed i R.

Vi sætter $G(X) := \Phi(X)A(X) \in R[X]$. Multipliceres med s får vi i $R[X]$:

$$sG(X) = s\Phi(X)A(X) = aF(X)A(X).$$

Hvis s ikke er en enhed, findes i R et primelement p, som er divisor i s. Dette element p er ikke divisor i a (da a og s var primiske) og det er heller ikke divisor i $F(X)$ eller $A(X)$ (da disse polynomier er primitive). Da p er divisor i produktet $aF(X)A(X)$ er dette i modstrid med at p er et primelement i $R[X]$ (Sætning (5.1)) ♠

[Bemærk at (5.5) egentlig kom ud som korollar til (5.1)].

(5.6) Er $A(X), G(X)$ polynomier i $R[X]$ således at der i $K[X]$ gælder, at $A(X)$ er divisor i $G(X)$, kan vi i almindelighed ikke slutte, at $A(X)$ er divisor i $G(X)$ inden for $R[X]$. (F.eks. er $A(X) = 2X + 2 \in \mathbf{Z}[X]$ en divisor i $G(X) = X^2 - 1 \in \mathbf{Z}[X]$ inden for $\mathbf{Q}[X]$, men ikke inden for $\mathbf{Z}[X]$).

Korollar (5.5) udsiger imidlertid for polynomier $A(X), G(X)$ med koefficienter i en faktoriel ring R, at hvis $A(X)$ er divisor i $G(X)$ inden for $K[X]$, og $A(X)$ er et primitivt polynomium, så er $A(X)$ divisor i $G(X)$ inden for $R[X]$.

(5.7) Gauss' Sætning. *Lad R være en faktoriel ring med brøklegemet K. Da er også polynomiumsringen $R[X]$ faktoriel, og primelementerne i $R[X]$ er dels de konstanter, der er primelementer i R, dels de polynomier, der er primitive i $R[X]$ og irreducible i $K[X]$.*

Vi minder om, at ringen $K[X]$ er et hovedidealområde og dermed en faktoriel ring.

Bevis. 1° Polynomier $P(X)$ i $R[X]$ af den angivne form er primelementer i $R[X]$. Er nemlig $P(X)$ en konstant, følger dette af Sætning (5.1) og er $\text{grad}(P) \geq 1$, følger dette af Korollar (5.5). Er nemlig P inden for $R[X]$ divisor i et produkt AB, kan vi, da P er et primelement i $K[X]$, slutte, at P inden for $K[X]$ er divisor i en af faktorerne, og da P yderligere er primitivt, kan vi slutte, at P endda inden for $R[X]$ er divisor i denne faktor.

2° Hvert polynomium $A(X)$ i $R[X]$, som ikke er 0 eller en enhed, har en opløsning i (prim-)faktorer af den angivne form. Er nemlig A en konstant, følger dette af at R er faktoriel, og er $\text{grad}(A) \geq 1$, betragter vi først en primopløsning af $A(X)$ i $K[X]$:

$$A(X) = \Pi_1(X) \cdots \Pi_r(X).$$

Ifølge Lemma (5.4) kan vi for hvert $i = 1, \ldots, r$ skrive $\Pi_i(X) = \alpha_i P_i(X)$, hvor $\alpha_i \in K^*$ og $P_i(X) \in R[X]$ er primitivt; da $\Pi_i(X)$ er irreducibel i $K[X]$, er også $P_i(X)$ irreducibel i $K[X]$, og altså af den angivne form. Sætter vi $\alpha = \alpha_1 \cdots \alpha_r \in K^*$, har vi

$$A(X) = \alpha P_1(X) \cdots P_r(X).$$

Her er produktet $P_1 \cdots P_r$ igen et primitivt polynomium (Gauss' lemma(5.3)), og af Korollar (5.5) kan vi derfor slutte, at $\alpha \in R$. Idet vi nu primopløser α i R, får vi den søgte opløsning af $A(X)$:

$$A(X) = p_1 \cdots p_s P_1(X) \cdots P_r(X).$$

3° Det følger nu, at $R[X]$ er faktoriel. At samtlige primelementer i $R[X]$ er af den angivne form følger nu let enten af 2° eller ved at bemærke, at samtlige irreducible elementer i $R[X]$ må være af den angivne form♠

(5.8) Korollar. *Polynomiumsringen $\mathbf{Z}[X_1, \ldots, X_n]$ i n variable (specielt polynomiumsringen $\mathbf{Z}[X]$ i én variabel) er en faktoriel ring.*

Polynomiumsringen $L[X_1, \ldots, X_n]$ i n variable med koefficienter i et legeme L er en faktoriel ring.

Bevis. Begge resultater bevises ved induktion ud fra Gauss' sætning, idet vi har

$$R[X_1, \ldots, X_n] \simeq R[X_1, \ldots, X_{n-1}][X_n] \heartsuit$$

(5.9) Schönemann–Eisenstein's Irreducibilitetskriterium. *Lad R være en faktoriel ring, og lad*

$$f = a_0 + a_1 X + \cdots + a_n X^n \in R[X]$$

være et primitivt polynomium. Hvis der findes et primelement $p \in R$, så at

$$p \mid a_0,\ p \mid a_1, \ldots,\ p \mid a_{n-1} \quad \text{og} \quad p^2 \nmid a_0,$$

så er f et primelement i $R[X]$. Er K brøklegemet for R, så er f et irreducibelt polynomium i $K[X]$.

Bevis. Da polynomiumsringen $R[X]$ er faktoriel ifølge Gauss' sætning (5.7), er det nok at vise, at f er irreducibel. Indirekte antager vi derfor, at $f(X) = g(X)h(X)$ i $R[X]$, hvor g og h ikke er enheder. Da f er et primitivt polynomium, må vi have grad $g \geq 1$, grad $h \geq 1$:

$$a_0 + \cdots + a_n X^n = (b_0 + \cdots + b_k X^k)(c_0 + \cdots + c_{n-k} X^{n-k}),$$

hvor $0 < k < n$. Da f er primitivt, følger det af forudsætningerne, at $p \nmid a_n$.

Ved overgang til restklasseringen R/pR får vi i $(R/pR)[X]$:

$$\boxed{a_n} X^n = (\boxed{b_0} + \cdots + \boxed{b_k} X^k)\,(\boxed{c_0} + \cdots + \boxed{c_{n-k}} X^{n-k}) \quad \text{og} \quad \boxed{a_n} \neq 0.$$

Nu er pR et primideal, og R/pR et integritetsområde. Vi slutter derfor let, at vi må have $\boxed{b_0} = \cdots = \boxed{b_{k-1}} = 0$ og $\boxed{c_0} = \cdots = \boxed{c_{n-k-1}} = 0$. Specielt er altså $p \mid b_0$ og $p \mid c_0$, men så er $p^2 \mid b_0 c_0 = a_0$ i modstrid med forudsætningen

Den anden påstand er en konsekvens af den første, jfr. Gauss' sætning (5.7)♠

(5.10) Eksempler. (1) Polynomiet $X^n \pm p$, hvor p er et primtal, er irreducibelt i $\mathbf{Z}[X]$ (eller $\mathbf{Q}[X]$). Derimod er $X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$ reducibelt i $\mathbf{Z}[X]$.

(2) Polynomiet $F_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1 = \frac{X^p - 1}{X - 1}$, hvor p er et primtal, er irreducibelt i $\mathbf{Z}[X]$ (eller $\mathbf{Q}[X]$), idet kriteriet kan anvendes på

$$F_p(X + 1) = \frac{(X + 1)^p - 1}{X} = X^{p-1} + \sum_{1<i<p} \binom{p}{i} X^{i-1} + p,$$

hvor de optrædende binomialkoefficienter jo er delelige med p.
(3) Er $n \in \mathbf{N}$ og er L et legeme, således at $n1 \neq 0$ i L (dvs. L's karakteristik er ikke divisor i n), så er polynomiet

$$X^n + Y^n - 1$$

irreducibelt i $L[X, Y] = L[Y][X]$, thi for primelementet $Y - 1 \in L[Y]$ finder vi, at $Y - 1 \,|\, Y^n - 1$, og da $Y^n - 1 = [(Y - 1) + 1]^n - 1 = \sum_{1 \leq i \leq n} \binom{n}{i} (Y - 1)^i$ er af formen $n(Y - 1) + (Y - 1)^2 q(Y)$, har vi $(Y - 1)^2 \nmid Y^n - 1$.

6. Appendix: Kvadratiske talringe.

(6.1) Definition. Et tal $\xi \in \mathbf{C}$ kaldes et *(helt) kvadratisk* tal, hvis der findes et normeret 2^{den}-gradspolynimium

$$X^2 + bX + c \in \mathbf{Z}[X],$$

der har ξ som rod.

Indføres for polynomiet $X^2 + bX + c$ *diskriminanten*

$$D = b^2 - 4c,$$

kan polynomiet skrives

$$X^2 + bX + c = (X + \frac{b}{2})^2 - \frac{D}{4}.$$

Det følger, at et kvadratisk tal har formen

$$\xi = \frac{-b \pm \sqrt{D}}{2}, \quad b, D \in \mathbf{Z}, \quad D \equiv b^2 \,(\mathrm{mod}\ 4)$$

[hvor vi sætter $\sqrt{D}$ = sædvanlig kvadratrod (≥ 0), hvis $D \geq 0$, og $\sqrt{D} = i\sqrt{-D}$, hvis $D < 0$]. Et kvadratisk tal kan være **reelt** (nemlig når $D \geq 0$) eller **imaginært** (nemlig når $D < 0$).

Observation. Diskriminanten ovenfor er et helt tal, $\equiv 0$ eller $1 \pmod 4$, thi $D \equiv b^2 \pmod 4$, og et kvadrat b^2 er altid $\equiv 0$ eller $1 \pmod 4$. [Hvorfor?]

Bemærkning. Et kvadratisk tal ξ er enten irrationalt (dvs. $\in \mathbf{C} \setminus \mathbf{Q}$) eller et sædvanligt helt tal (dvs. $\in \mathbf{Z}$). Er nemlig ξ en rational rod i $X^2 + bX + c$ hvor $b, c \in \mathbf{Z}$, og skrives $\xi = a/s$, hvor $a \in \mathbf{Z}$ og $s \in \mathbf{N}$, kan vi antage, at intet primtal går op i både a og s. Af $(a/s)^2 + b(a/s) + c = 0$ får vi ved multiplikation med s^2, at

$$s(-ba - cs) = a^2.$$

Ethvert primtal, der går op i s, går derfor også op i a^2 og dermed op i a. Det følger, at $s = 1$, således at $\xi = a/1 \in \mathbf{Z}$.

(6.2) Lemma. *Lad $\xi \in \mathbf{C}$ være et komplekst tal. Da er ξ kvadratisk, hvis og kun hvis der findes et tal $\eta \in \mathbf{C}$, så at*

$$\xi + \eta \in \mathbf{Z} \quad og \quad \xi\eta \in \mathbf{Z}.$$

Bevis. For polynomier udtrykker ligningen:

$$(*) \qquad X^2 + bX + c = (X - \xi)(X - \eta),$$

at

$$b = -(\xi + \eta) \quad \text{og} \quad c = \xi\eta.$$

"hvis": Polynomiet X^2+bX+c defineret ved ligningen $(*)$ har ifølge forudsætningen koefficienter i $\mathbf{Z}$. Da det øjensynlig har ξ som rod, er ξ kvadratisk.
"kun hvis": Hvis ξ er kvadratisk, og altså rod i et polynomium $X^2 + bX + c$, hvor $b, c \in \mathbf{Z}$, kan dette polynomium skrives på formen $(*)$. Som η kan altså bruges "den anden rod" i dette polynomium. ♠

(6.3) Observation. Hvis et kvadratisk tal ξ er irrationalt, så er det i Lemma (6.2) nævnte tal η entydigt bestemt.

Er nemlig $\tilde{\eta} \in \mathbf{C}$ endnu et tal, der opfylder betingelserne, fås

$$\tilde{\eta} - \eta \in \mathbf{Z}, \quad \xi(\tilde{\eta} - \eta) \in \mathbf{Z}.$$

Af $\eta \neq \tilde{\eta}$ følger derfor $\xi \in \mathbf{Q}$.

Definition. For et irrationalt kvadratisk tal ξ kaldes ovennævnte entydigt bestemte tal η for ξ's *konjugerede* tal, og det betegnes ξ'. Hvis et kvadratisk tal ξ er rationalt, og dermed helt, jfr. Bemærkning (6.1), sættes $\xi' = \xi$. Tallet

$$N(\xi) := \xi\xi'$$

kaldes *normen* af det kvadratiske tal ξ, og tallet

$$D(\xi) := (\xi - \xi')^2 = (\xi + \xi')^2 - 4\xi\xi'.$$

kaldes *diskriminanten* af ξ.

(6.4) Observation. Hvis et irrationalt kvadratisk tal ξ er rod i polynomiet $X^2 + bX + c$, og altså af formen

$$\xi = \frac{-b \pm \sqrt{D}}{2} \quad \text{med } D = b^2 - 4c,$$

finder vi for det konjugerede tal:

$$\xi' = \frac{-b \mp \sqrt{D}}{2},$$

og videre:

$$\xi + \xi' = -b, \quad N(\xi) = \xi\xi' = c, \quad D(\xi) = (\xi - \xi')^2 = D.$$

Er det kvadratiske tal ξ derimod rationalt, og altså $\xi = a \in \mathbf{Z}$, finder vi

$$N(a) = a^2, \qquad D(a) = 0.$$

Normen og diskriminanten er altså i begge tilfælde hele tal.

BEMÆRKNING. Hvis et kvadratisk tal ξ er imaginært, så er dets konjugerede ξ' det sædvanlige komplekst konjugerede tal $\bar{\xi}$. Det følger, at $N(\xi) = \xi\bar{\xi} = |\xi|^2$. Specielt er altså i så fald $N(\xi) \geq 0$.

(6.5) SÆTNING. *Lad $\xi \in \mathbf{C}$ være et irrationalt kvadratisk tal, rod i polynomiet $X^2 + bX + c$, hvor $b, c \in \mathbf{Z}$. Da er delmængden*

$$\mathbf{Z}[\xi] := \{x + y\xi \mid x, y \in \mathbf{Z}\} \subseteq \mathbf{C}$$

en delring af $\mathbf{C}$, og for tal $\alpha \in \mathbf{Z}[\xi]$ er fremstillingen

$$\alpha = x + y\xi, \quad \textit{med } x, y \in \mathbf{Z},$$

entydig. Alle tal $\alpha \in \mathbf{Z}[\xi]$ er kvadratiske, og konjugering:

$$\alpha \mapsto \alpha'$$

er en involutorisk automorfi i ringen $\mathbf{Z}[\xi]$.

Bevis. Det er klart, at $\mathbf{Z}[\xi] \supseteq \mathbf{Z}$, og at $\mathbf{Z}[\xi]$ er stabil under addition. Da vi endvidere har

$$\xi^2 = -c - b\xi \in \mathbf{Z}[\xi],$$

følger det let, at $\mathbf{Z}[\xi]$ er stabil under multiplikation. Følgelig er $\mathbf{Z}[\xi] \subseteq \mathbf{C}$ en delring.

Entydigheden af en fremstilling $\alpha = x + y\xi$ med $x, y \in \mathbf{Z}$ følger let af, at tallet ξ ikke er rationalt.

For det konjugerede tal ξ' har vi

$$\xi + \xi' = -b \quad , \quad \xi\xi' = c.$$

For et tal $\alpha = x + y\xi \in \mathbf{Z}[\xi]$ finder vi derfor

$$\alpha + (x + y\xi') = 2x + y(-b) \in \mathbf{Z} \text{ og } \alpha(x + y\xi') = x^2 - bxy + cy^2 \in \mathbf{Z}.$$

Af Lemma (6.2) følger nu, at α er kvadratisk. Hvis α er irrational, følger det videre, at $\alpha' = x+y\xi'$, og hvis α er rational, må vi have $y = 0$ [hvorfor?], og altså $\alpha' = \alpha = x$. I begge tilfælde gælder altså

$$\alpha' = x + y\xi'.$$

Da $\xi' = -b - \xi \in \mathbf{Z}[\xi]$, følger det, at $\alpha' \in \mathbf{Z}[\xi]$. At konjugering er involutorisk (altså at $(\alpha')' = \alpha$) følger umiddelbart af Definition (6.3). At $\alpha \mapsto \alpha'$ er en ringhomomorfi (altså at $(\alpha\beta)' = \alpha' + \beta'$, $(\alpha\beta)' = \alpha'\beta'$ og $1' = 1$) fås let af det fundne udtryk for α'. At $\alpha \mapsto \alpha'$ er en automorfi følger af, at en involution er bijektiv♡

Definition. En delring $R \subseteq \mathbf{C}$ af formen $R = \mathbf{Z}[\xi]$ med et passende irrationalt kvadratisk tal ξ kaldes en *kvadratisk talring*. Den kaldes *reel* eller *imaginær* eftersom tallet ξ er reelt eller imaginært.

Korollar. *For en kvadratisk talring R er normen en multiplikativ homomorfi*

$$N : R \to \mathbf{Z},$$

og for $\alpha \in R$ gælder:

$$N(\alpha) = 0 \quad \Longleftrightarrow \quad \alpha = 0.$$

Bevis. Da afbildningen $\alpha \mapsto \alpha'$ er multiplikativ, er også afbildningen $\alpha \mapsto N(\alpha) = \alpha\alpha'$ multiplikativ. At $N(\alpha) \in \mathbf{Z}$ har vi set i Observation (6.4). Den sidste påstand følger af, at nulreglen gælder i $\mathbf{C}$♠

(6.6) Udregning. Lad ξ være en irrational rod i polynomiet $X^2 + bX + c$, hvor $b, c \in \mathbf{Z}$. For et element

$$x + y\xi, \quad \text{hvor } x, y \in \mathbf{Z},$$

i den kvadratiske talring $\mathbf{Z}[\xi]$ gælder da:

$$N(x + y\xi) = x^2 - bxy + cy^2 \quad (\text{ og } D(x + y\xi) = y^2(b^2 - 4c).)$$

Bevis. Regn selv♡

Morale. For en irrational rod ξ i polynomiet $X^2 + bX + c$, hvor $b, c \in \mathbf{Z}$, svarer elementerne $\alpha = x + y\xi$ i den kvadratiske talring $\mathbf{Z}[\xi]$ bijektivt til par $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ af hele tal.

Elementer $\alpha \in \mathbf{Z}[\xi]$ med en given norm $N(\alpha) = k$, hvor $k \in \mathbf{Z}$, svarer bijektivt til løsninger $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ til ligningen

$$\boxed{x^2 - bxy + cy^2 = k}$$

Det er her forudsat, at diskriminanten $D = b^2 - 4c$ ikke er et kvadrat i ringen $\mathbf{Z}$.

BEMÆRKNING. Idet vi på sædvanlig måde opfatter $\mathbf{C}$ som et 2-dimensionalt vektorrum over $\mathbf{R}$, ser vi for en **imaginær** kvadratisk talring $\mathbf{Z}[\xi]$, at "vektorerne" $1, \xi \in \mathbf{C}$ er en basis, og elementerne $\alpha \in \mathbf{Z}[\xi]$ kan opfattes som de vektorer $\alpha \in \mathbf{C}$, der har heltalskoordinater mht. denne basis. De kan anskueliggøres som gitterpunkter i planen.

Vi minder om, at vi i denne situation har $N(\alpha) = |\alpha|^2$. Elementer $\alpha \in \mathbf{Z}[\xi]$ med en given norm $N(\alpha) = k \in \mathbf{N}$ svarer således til gitterpunkter på cirklen med radius $\sqrt{k}$ og centrum i 0.

(6.7) SÆTNING. *Lad $R = \mathbf{Z}[\xi]$ være en kvadratisk talring. Et element $\varepsilon \in R$ er da en enhed i R, hvis og kun hvis $N(\varepsilon) = \pm 1$.*

Bevis. **"hvis":** Af $N(\varepsilon) = \varepsilon\varepsilon' = \pm 1$, følger $\varepsilon(\pm\varepsilon') = 1$. Da $\pm\varepsilon' \in R$, er ε altså invertibel (med $\pm\varepsilon'$ som invers).
"kun hvis": Af en ligning $\varepsilon\eta = 1$ i ringen R, får vi $N(\varepsilon)N(\eta) = N(1) = 1$ i ringen $\mathbf{Z}$. Det følger, at $N(\varepsilon)$ er en enhed i $\mathbf{Z}$, altså at $N(\varepsilon)) \pm 1$♠

MORALE. For en irrational rod ξ i polynomiet $X^2 + bX + c$, hvor $b, c \in \mathbf{Z}$, svarer enhederne ε i $R = \mathbf{Z}[\xi]$ til løsninger $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ til ligningen

$$\boxed{x^2 - bxy + cy^2 = \pm 1}$$

At $\varepsilon \in R^* \Rightarrow \pm\varepsilon^n \in R^*$, når $n \in \mathbf{Z}$, kan derfor udnyttes til ud fra én løsning (x, y) til ligningen at bestemme yderligere en række.

SIDEBEMÆRKNING 1. For en **imaginær** kvadratisk talring $R = \mathbf{Z}[\xi]$, hvor ξ er rod i polynomiet $X^2 + bX + c$ med $b, c \in \mathbf{Z}$, og hvor altså $D = b^2 - 4c < 0$, gælder, at

$$R^* = \{\pm 1\}, \text{ undtagen hvis}$$

$D = -3$, hvor $R^* = \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$ med $\zeta = \frac{1+\sqrt{-3}}{2}$, eller hvis $D = -4$, hvor $R^* = \{1, i, i^2, i^3\}$ (med $i = \sqrt{-1}$).

Bevis. Vi antager i $\xi = (-b + \sqrt{D})/2$, at $\sqrt{D}$ er valgt med positiv imaginærdel. Da $D \equiv 0$ eller $1 \pmod 4$, har vi $D \leq -3$. Det er klart, at vi altid har $\{\pm 1\} \subseteq R^*$. Antag derfor, at $\varepsilon = u + v\xi$, $u, v \in \mathbf{Z}$, er en enhed $\neq \pm 1$. Det følger, at ε må være imaginær og kvadratisk, og da $\varepsilon\bar{\varepsilon} = 1$, må ε følgelig være rod i et polynomium

$$X^2 + eX + 1, \text{ hvor } e \in \mathbf{Z} \text{ og } e^2 - 4 < 0.$$

Heraf følger $e = 0$ eller $e = \pm 1$.

Hvis $e = 0$, har vi $\varepsilon = \pm i$, og dermed

$$-4 = (\varepsilon - \bar{\varepsilon})^2 = D(\varepsilon) = v^2 D,$$

jfr. Udregning (6.6), hvoraf $D = -4$ (og $v = \pm 1$) (idet $D = -1$ er udelukket).

Er **omvendt** $D = -4$, så må b være lige, og da $\xi = \frac{-b+\sqrt{-4}}{2} = -\frac{b}{2} + i$, ses at $i = \frac{b}{2} + \xi \in \mathbf{Z}[\xi]$. Og så er $\{1, i, -1, -i\} \subseteq R^*$.

Hvis $e = \pm 1$, har vi $\varepsilon = \frac{\pm 1+\sqrt{-3}}{2} \in \{\zeta, \zeta^2\}$, og dermed

$$-3 = (\varepsilon - \bar{\varepsilon})^2 = D(\varepsilon) = v^2 D,$$

hvoraf $D = -3$ (og $v = \pm 1$) (idet $D = -1$ er udelukket).

Er **omvendt** $D = -3$, så må b være ulige, og da $\xi = \frac{-b+\sqrt{-3}}{2}$, ses, at $\zeta = \frac{b+1}{2} + \xi \in \mathbf{Z}[\xi]$. Og så er også $\{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\} \subseteq R^*$. Explicit er $\zeta^2 = \zeta - 1 = \frac{b-1}{2} + \xi$, $\zeta^3 = -1$, $\zeta^4 = -\zeta = -\frac{b+1}{2} - \xi$ og $\zeta^5 = -\zeta^2 = -\frac{b-1}{2} - \xi$.

Heraf følger påstandene ♡

MORALE 1. Ligningen

$$\boxed{x^2 - bxy + cy^2 = 1}, \quad \text{hvor } b, c \in \mathbf{Z} \text{ og } D = b^2 - 4c < 0,$$

har af løsninger $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ kun de trivielle

$$(\pm 1, 0), \text{ undtagen hvis}$$

$D = -3$, hvor løsningerne er $(\pm 1, 0)$ og $(\frac{b\pm 1}{2}, \pm 1)$, eller hvis $D = -4$, hvor løsningerne er $(\pm 1, 0)$, $(\frac{b\pm 1}{2}, 1)$ og $(\frac{-b\pm 1}{2}, -1)$.

SIDEBEMÆRKNING 2. For en **reel** kvadratisk talring $R = \mathbf{Z}[\xi]$, hvor ξ er rod i polynomiet $X^2 + bX + c$ med $b, c \in \mathbf{Z}$, og hvor altså $D = b^2 - 4c > 0$ ikke er et kvadrat, kan man bevise, at der altid findes en enhed $\varepsilon_0 \neq \pm 1$ i R, så at

$$R^* = \{\pm \varepsilon_0^n \mid n \in \mathbf{Z}\}.$$

Specielt er der altid uendelig mange enheder. En sådan enhed ε_0 kaldes en *grundenhed*. [Hvis grundenheden ε_0 har $N(\varepsilon_0) = 1$, ses, at alle enheder $\varepsilon \in R^*$ har $N(\varepsilon) = 1$. Er derimod $N(\varepsilon_0) = -1$, ses, at

$$\{\varepsilon \in R \mid N(\varepsilon) = 1\} = \{\pm(\varepsilon_0^2)^n \mid n \in \mathbf{Z}\}.]$$

MORALE 2. Ligningen

$$\boxed{x^2 - bxy + cy^2 = \pm 1}, \text{ hvor } b, c \in \mathbf{Z}, \text{ og } D = b^2 - 4c > 0 \text{ ikke er et kvadrat},$$

har af løsninger $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ altid en ikke-triviel grundløsning (u_0, v_0), således at den fuldstændige løsning er givet ved

$$\pm(u_n, v_n), \quad \text{hvor } n \in \mathbf{Z},$$

hvor u_n og v_n er bestemt ved ligningen

$$(u_0 + v_0\xi)^n = u_n + v_n\xi, \quad \text{hvor } \xi \text{ er en rod i } X^2 + bX + c.$$

[Et tilsvarende resultat gælder for ligningen $x^2 - bxy + cy^2 = 1$].

(6.8) Sætning. *Lad $R = \mathbf{Z}[\xi]$ være en kvadratisk talring, og lad $\alpha, \delta \in R$. Hvis δ er divisor i α, så gælder i ringen $\mathbf{Z}$, at $N(\delta)$ er divisor i $N(\alpha)$, og divisoren δ er en ikke–triviel divisor, hvis og kun hvis $N(\delta)$ i ringen $\mathbf{Z}$ er en ikke–triviel divisor i $N(\alpha)$.*

Bevis. Hvis $\alpha = \delta\beta$ med $\beta \in R$, får vi i $\mathbf{Z}$, at $N(\alpha) = N(\delta)N(\beta)$, hvoraf den første påstand. Den anden påstand følger nu af Sætning (6.7)♠

Korollar. *I en kvadratisk talring $R = \mathbf{Z}[\xi]$ har hvert element $\notin \{0\} \cup R^*$ i R en irreducibel opløsning.*

Bevis. Dette følger af Korollar (3.8)(1), thi af Sætning (6.8) følger straks, at den ved $\nu(\alpha) := |N(\alpha)|$ definerede funktion

$$\nu : R \to \mathbf{Z}$$

har den i Korollar (3.8)(1) nævnte egenskab♡

Bemærkning. En kvadratisk talring $R = \mathbf{Z}[\xi]$ er delring af legemet $\mathbf{C}$. For elementer $\alpha, \delta \in R$ med $\delta \neq 0$ ser vi derfor, at δ er divisor i α, netop når det komplekse tal $\frac{\alpha}{\delta}$ tilhører R. Vi har $\frac{\alpha}{\delta} = \frac{\alpha\delta'}{\delta\delta'}$. Tælleren er $\alpha\delta' \in R$, og den har derfor formen $\alpha\delta' = x + y\xi$ med $x, y \in \mathbf{Z}$. Nævneren er $\delta\delta' = N(\delta) \in \mathbf{Z} \setminus \{0\}$,, og den har derfor formen $\delta\delta' = s$ med $s \in \mathbf{Z}$. Følgelig har vi $\frac{\alpha}{\delta} = \frac{x}{s} + \frac{y}{s}\xi$, så $\frac{\alpha}{\delta}$ har formen

$$(*) \qquad \frac{\alpha}{\delta} = \lambda + \mu\xi, \quad \text{med } \lambda, \mu \in \mathbf{Q}.$$

Det er let at se, at komplekse tal af formen $\frac{\alpha}{\delta}$, hvor $\alpha, \delta \in R$ og $\delta \neq 0$, udgør et dellegeme af $\mathbf{C}$. Dette dellegeme kaldes *brøklegemet* for R. For elementer i dette brøklegeme ses ganske som i beviset for Sætning (6.5), at fremstillingen $(*)$ er entydig. Vi ser, at δ er divisor i α, netop når koefficienterne λ, μ i fremstillingen $(*)$ tilhører $\mathbf{Z}$.

Det er således en simpel sag for givne $\alpha, \delta \in R$ at afgøre, om δ er divisor i α, men det må fremhæves, at det for et givet $\alpha \in R$ sædvanligvis er kompliceret at bestemme de δ'er, der er divisorer i α.

(6.9) Specielle Resultater.

(1) *Den kvadratiske tal ring $\mathbf{Z}[\sqrt{-1}]$ er et hovedidealområde.*
(2) *Den kvadratiske talring $\mathbf{Z}[\sqrt{2}]$ er et hovedidealområde.*
(3) *Den kvadratiske talring $\mathbf{Z}[\sqrt{-5}]$ er ikke faktoriel.*

Bevis. **(1):** Vi viser for $R = \mathbf{Z}[\sqrt{-1}]$, at den ved $\alpha \mapsto N(\alpha) = |\alpha|^2$ definerede funktion $\nu : R \to \mathbf{Z}$ har den i Sætning (1.4) nævnte egenskab. Funktionen er nedad begrænset, idet $\nu(\alpha) \geq 0$, så vi mangler at vise for givne $\delta, \alpha \in R,\ \delta \neq 0$, at der findes et element $\eta \in R$ med $\nu(\alpha - \eta\delta) < \nu(\delta)$. Denne ulighed er øjensynlig ensbetydende med uligheden

$$(*) \qquad |\frac{\alpha}{\delta} - \eta| < 1.$$

Idet tallene $\eta \in R$ er gitterpunkterne $x + yi,\ x, y \in \mathbf{Z}$, ser vi, at der for ethvert komplekst tal $w \in \mathbf{C}$ findes et gitterpunkt η, hvis afstand til w er $\leq \frac{1}{2} \cdot$ (diagonalen i et kvadrat med side 1) $= \frac{1}{2}\sqrt{2}$. For hvert $w \in \mathbf{C}$ kan vi altså opfylde uligheden

$$|w - \eta| \leq \frac{1}{2}\sqrt{2}, \quad \eta \in R,$$

og dermed for $w = \frac{\alpha}{\delta}$ specielt uligheden $(*)$.
(2): Vi anvender igen Sætning (1.4) på $R = \mathbf{Z}[\sqrt{2}]$ med $\nu : R \to \mathbf{Z}$ givet ved $\nu(\alpha) := |N(\alpha)| = |\alpha\alpha'|$, og skal altså for givne $\alpha = a + b\sqrt{2}$, $\delta = c + d\sqrt{2} \in R,\ \delta \neq 0$, bestemme $\eta = x + y\sqrt{2} \in R$, så at

$$\nu(\alpha - \eta\delta) < \nu(\delta).$$

Efter division med $|\delta\delta'| = \nu(\delta)$ fås den ensbetydende ulighed

$$|(\frac{\alpha}{\delta} - \eta)(\frac{\alpha'}{\delta'} - \eta')| < 1.$$

Indsættes her $\frac{\alpha}{\delta} = \lambda + \mu\sqrt{2},\ \lambda, \mu \in \mathbf{Q}$, jfr. Bemærkning (6.8), og $\eta = x + y\sqrt{2}$, kan uligheden skrives

$$|(\lambda - x)^2 - 2(\mu - y)^2| < 1.$$

Her er λ, μ specielt reelle tal, og vi kan følgelig finde hele tal $x, y \in \mathbf{Z}$, så at $|\lambda - x| \leq \frac{1}{2}$ og $|\mu - y| \leq \frac{1}{2}$. Med dette valg af x og y er den søgte ulighed specielt opfyldt.
(3): I ringen $R = \mathbf{Z}[\sqrt{-5}]$ har vi øjensynlig opløsninger

$$(*) \qquad 6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Tallet $2 \in R$ har normen $N(2) = 2^2$. En ikke-triviel divisor $\delta = x + y\sqrt{-5}$ måtte derfor ifølge Sætning (6.8) have normen $N(\delta) = x^2 + 5y^2 = 2$, men denne ligning kan øjensynlig ikke være opfyldt med $(x, y) \in \mathbf{Z} \times \mathbf{Z}$. Følgelig er tallet 2 et irreducibelt element i R, og det er derfor nok at vise, at 2 ikke er et primelement.

Tallet 2 er hverken divisor i $1 + \sqrt{-5}$ eller i $1 - \sqrt{-5}$ thi

$$\frac{1 + \sqrt{-5}}{2} = \frac{1}{2} + \frac{1}{2}\sqrt{-5} \notin R \quad \text{og} \quad \frac{1 - \sqrt{-5}}{2} = \frac{1}{2} - \frac{1}{2}\sqrt{-5} \notin R.$$

Af $(*)$ fremgår imidlertid, at 2 er divisor i produktet $(1+\sqrt{-5})(1-\sqrt{-5})$, og 2 er derfor ikke et primelement ♠

(6.10) Eksempel. I den kvadratiske talring $R = \mathbf{Z}[\sqrt{-5}]$ har elementet 6 to forskellige irreducible opløsninger

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

thi ganske som i beviset ovenfor følger det, at elementerne $2, 3$ og $1 \pm \sqrt{-5}$ er irreducible i R.

(6.11) Man ved ikke, om der er uendelig mange reelle kvadratiske talringe, der er faktorielle. Man kan vise (men det er svært!), at der blandt de imaginære kun er 9, der er faktorielle.

Forgreningssætning. *Lad $R = \mathbf{Z}[\xi]$ være en kvadratisk talring, og* **antag**, *at R er en faktoriel ring. Ethvert sædvanligt primtal $p \in \mathbf{N}$ vil da mht. R være af en af følgende 3 typer:*
Type 1: *Primtallet p er et primelement i R.*
Type 2: *Primtallet p har i R en primopløsning $p = \pm\pi\pi'$, hvor det konjugerede primelement π' ikke er associeret med π.*
Speciel type: *Primtallet p har i R en primopløsning $p = \pm\pi\pi'$, hvor det konjugerede primelement π' er associeret med π.*

Desuden gælder, at hvert primelement π i R er associeret med et af primelementerne nævnt under de 3 typer.

Bevis. Et primtal p er ikke en enhed i R, og der findes derfor et primelement π i R, som er divisor i p. Følgelig er $N(\pi)$ inden for $\mathbf{Z}$ divisor i $N(p) = p^2$, jfr. Sætning (6.8), så vi har $N(\pi) = \pm p^2$ eller $N(\pi) = \pm p$.
Hvis $N(\pi) = \pm p^2$, er π en triviel divisor i p, og derfor associeret med p, og så er også p et primelement i R, og altså af type 1.
Hvis derimod $N(\pi) = \pm p$, så har vi $p = \pm N(\pi) = \pm\pi\pi'$, og så er p af type 2 eller af speciel type.

Er omvendt π et primelement, så er $\pi\pi' = N(\pi) \in \mathbf{Z}$. Skrives dette tal inden for $\mathbf{Z}$ som et produkt af $\pm$primtal, går π altså op i produktet, og dermed i en af faktorerne. Der findes derfor et sædvanligt primtal $p \in \mathbf{N}$, så at π er divisor i p. Heraf følger påstanden, idet vi ovenfor har angivet primopløsninger i R for alle sædvanlige primtal p ♠

(6.12) Det må fremhæves, at inddelingen af primtallene i de 3 typer, der også kaldes primtallenes *forgrening*, naturligvis afhænger af den givne **(faktorielle)** kvadratiske talring R.

Vi vil her betragte den kvadratiske talring $\mathbf{Z}[\sqrt{-1}] = \mathbf{Z}[i]$, som også kaldes *Gauss' talring*. Vi har set i Resultat (6.9), at $\mathbf{Z}[i]$ er et hovedidealområde, og dermed en faktoriel ring. Enhederne $\varepsilon = x + yi \in \mathbf{Z}[i]$ svarer ifølge Morale (6.7) til løsninger $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ til ligningen $x^2 + y^2 = 1$. Løsningerne er øjensynlig $(\pm 1, 0)$ og $(0, \pm 1)$, og enhederne er derfor

$$1, i, -1, -i.$$

Videre gælder følgende resultat:

FORGRENING I GAUSS' TALRING. *Mht. Gauss' talring* $\mathbf{Z}[i]$ *falder de sædvanlige primtal i følgende typer:*

Type 1 *er netop primtallene* $\equiv 3 \pmod 4$.

Type 2 *er netop primtallene* $\equiv 1 \pmod 4$

Speciel type *har kun primtallet* 2 *(med primopløsningen* $2 = (1+i)(1-i)$*).*

Bevis. **Speciel type:** Primtallet $2 = (1+i)(1-i)$ er specielt, da $1 - i = (-i)(1+i)$ er associeret med $1 + i$. Er omvendt p et specielt primtal, så har vi en primopløsning $p = \pi\bar{\pi}$, hvor $\pi = x + iy$ er et primelement associeret med $\bar{\pi}$, altså

$$\bar{\pi} = \pi, \quad \bar{\pi} = i\pi, \quad \bar{\pi} = -\pi \quad \text{eller } \bar{\pi} = (-i)\pi.$$

Var $\bar{\pi} = \pi$, ville $\pi = x \in \mathbf{Z}$, og dermed $p = \pi\bar{\pi} = x^2$, være i modstrid med at p var et primtal. Tilsvarende er $\bar{\pi} \neq -\pi$, thi ellers var $\pi = yi$, og $p = \pi\bar{\pi} = y^2$. Følgelig er $\bar{\pi} = \pm i\pi$, hvoraf $\pi = x \pm xi$, og så er $p = \pi\bar{\pi} = 2x^2$, og da p er et primtal, får vi endelig $p = 2$.

Type 2: Lad p være et primtal af type 2. Vi har da $p = \pi\bar{\pi}$ med et primelement $\pi = x + yi \in \mathbf{Z}[i]$, og altså

$$p = \pi\bar{\pi} = x^2 + y^2, \qquad x, y \in \mathbf{Z}.$$

Da et kvadrat i $\mathbf{Z}$ er $\equiv 0$ eller $1 \pmod 4$ [hvorfor?], har vi følgelig $p \equiv 0$ eller 1 eller $2 \pmod 4$. Da primtallet p er $\neq 2$ (ifølge det allerede viste) og dermed ulige, må vi have $p \equiv 1 \pmod 4$. For at fuldføre beviset, er det nok at vise, at et primtal $p \equiv 1 \pmod 4$ ikke kan være af type 1(!).

Lad altså p være et primtal $\equiv 1 \pmod 4$. Det er velkendt, jfr. "Hele tal", Korollar (6.10), at kongruensen

$$x^2 \equiv -1 \pmod p$$

da har løsninger. Der findes altså tal $x, d \in \mathbf{Z}$, så at

$$pd = x^2 + 1.$$

I Gauss' talring kan denne ligning skrives

$$pd = (x + i)(x - i),$$

og p er altså divisor i produktet $(x+i)(x-i)$. **Hvis** p var af type 1, ville p være et primelement i $\mathbf{Z}[i]$, og dermed divisor i en af faktorerne, men det er i modstrid med, at hverken

$$\frac{x+i}{p} = \frac{x}{p} + \frac{1}{p}i \quad \text{eller} \quad \frac{x-i}{p} = \frac{x}{p} - \frac{1}{p}i$$

tilhører $\mathbf{Z}[i]$, jfr. (6.8)♠

KOROLLAR. *For hvert primtal $p \equiv 1$ (mod 4) har ligningen*

$$x^2 + y^2 = p$$

løsninger $(x, y) \in \mathbf{Z} \times \mathbf{Z}$.

Bevis. Er $p = \pi\bar{\pi}, \pi = x + iy \in \mathbf{Z}[i]$, så er (x, y) en løsning ♠

(6.13) For bedre at kunne udnytte primopløsninger i Gauss´ talring $\mathbf{Z}[i]$ er det hensigtsmæssigt at fastlægge et repræsentantsystem for primelementerne. For hvert primelement π er de associerede tallene $\pi, i\pi, -\pi, -i\pi$. Da multiplikation med de 4 enheder $1, i, -1, -i$ svarer til drejninger med vinkler $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}$ [Bemærk, at der er to slags π'er i spil!], er hvert primelement associeret med netop ét primelement i området bestemt ved

$$-\frac{\pi}{4} < Arg(\alpha) \leq \frac{\pi}{4},$$

og som repræsentantsystem Π væler vi primelementer i dette område. Ifølge de fundne resultater er primelementerne i Π **enten** $1 + i$ (svarende til det specielle primtal 2, der har primopløsningen $2 = (-i)(1+i)^2$), **eller** de er sædvanlige primtal $q \equiv 3 \pmod 4$, **eller** de findes i par $\pi, \bar{\pi}$, hvor $\pi\bar{\pi} = p$ er et sædvanligt primtal $\equiv 1 \pmod 4$.

Hvert element $\alpha \neq 0$ i $\mathbf{Z}[i]$ har altså en entydig primopløsning af formen

$$(*) \qquad \alpha = \varepsilon(1+i)^\lambda q_1^{\nu_1} \cdots q_r^{\nu_r} \pi_1^{\mu'} \bar{\pi}_1^{\mu''} \cdots \pi_s^{\mu'_s} \bar{\pi}_s^{\mu''_s} \quad \text{med } \pi_j\bar{\pi}_j = p_j,$$

hvor ε er en enhed, dvs. $\in \{1, i, -1, -i\}$.

Lad os vise følgende

ANVENDELSE. *Lad $k \in \mathbf{N}$ være et naturligt tal med primopløsningen*

$$(\triangle) \qquad k = 2^l q_1^{n_1} \cdots q_r^{n_r} p_1^{m_1} \cdots p_s^{m_s},$$

hvor primtallene q_i er $\equiv 3 \pmod 4$ og primtallene p_j er $\equiv 1 \pmod 4$. Ligningen

$$x^2 + y^2 = k$$

har da løsninger $(x, y) \in \mathbf{Z} \times \mathbf{Z}$, *hvis og kun hvis eksponenterne* $n_1, \ldots, n_r$ *alle er lige. I bekræftende fald er antallet af løsninger netop tallet*

$$4(m_1 + 1) \cdots (m_s + 1).$$

Bevis. Idet par $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ svarer til tal $\alpha = x + iy \in \mathbf{Z}[i]$ ses, at vi skal bestemme de tal $\alpha \in \mathbf{Z}[i]$ som opfylder

$$N(\alpha) = k.$$

Idet α er bestemt ved sin primopløsning $(*)$ [Ved eventuelt at tilføje faktorer med eksponent 0 i $(*)$ og $(\triangle)$ kan vi antage, at de optrædende q_i'er og p_j'er er de samme], finder vi

$$N(\alpha) = 2^{\lambda} q_1^{2\nu_1} \cdots q_r^{2\nu_r} p_1^{\mu_1' + \mu_1''} \cdots p_s^{\mu_s' + \mu_s''}.$$

Vi har altså $N(\alpha) = k$, netop når eksponenterne i $(*)$ opfylder ligningerne

$$\lambda = l, \quad 2\nu_1 = n_1, \ldots, \; 2\nu_r = n_r, \quad \mu_1' + \mu_1'' = m_1, \ldots, \; \mu_s' + \mu_s'' = m_s.$$

Dette er naturligvis kun muligt, når n_i'erne er lige. Og er det tilfældet, kan vi løse ligningerne, og frit vælge μ_1' så at $0 \leq \mu_1' \leq m_1$, $\ldots$, μ_s' så at $0 \leq \mu_s \leq m_s$. Desuden har vi 4 mulige valg af enheden ε, altså i alt $4(m_1 + 1) \cdots (m_s + 1)$ elementer α, som opfylder $N(\alpha) = k$ ♠

(6.14) Det fremgår af beviset ovenfor, at vi explicit kan besteme løsningerne til ligningen $x^2 + y^2 = k$ ud fra primopløsningen af tallet k i ringen $\mathbf{Z}[i]$. Og denne primopløsning fås ud fra den sædvanlige primopløsning ved at skrive hvert $p_j \equiv 1 \pmod 4$ på formen $p_j = \pi_j \bar{\pi}_j$, dvs. ved at løse ligningerne $x_j^2 + y_j^2 = p_j$.

Som eksempel vil vi betragte *pytagoræiske talsæt*, dvs. talsæt $(x, y, z) \in \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}$, som er en løsning til ligningen

$$x^2 + y^2 = z^2.$$

En sådan løsning vil vi kalde ikke–triviel hvis x og y er primiske [Er $d > 1$ divisor i både x og y, så er d også divisor i z [hvorfor?], så vi kan skrive $x = dx'$, $y = dy'$, $z = dz'$. En triviel løsning har altså formen $(x, y, z) = (dx', dy', dz')$, hvor også (x', y', z') er pytagoræisk og (specielt) $|z'| < |z|$].

Endvidere vil vi kalde to løsninger *essentielt ens*, hvis man kan komme fra den ene til den anden ved at erstatte (x, y) med $(\pm x, \pm y)$ eller $(\pm y, \pm x)$.

Idet vi kalder et tal $k \in \mathbf{N}$ *pytagoræisk*, hvis ligningen

$$x^2 + y^2 = k^2$$

har en ikke-triviel løsning, gælder følgende:

Sætning om Pytagoræiske tal. *Et naturligt tal* $k > 1$ *med primopløsningen*

$$k = p_1^{m_1} \cdots p_s^{m_s}, \quad \textit{hvor } m_j \geq 1 \textit{ for } j = 1, \ldots, s\,,$$

er pytagoræisk, hvis og kun hvis primfaktorerne p_j alle er $\equiv 1 \pmod 4$. I bekræftende fald har ligningen

$$x^2 + y^2 = k^2$$

præcis 2^{s-1} essentielt forskellige, ikke–trivielle løsninger.

Bevis. Skrives som i Anvendelsen ovenfor k's primopløsning på formen

$$k = 2^l q_1^{n_1} \cdots q_r^{n_r} p_1^{m_1} \cdots p_s^{m_s},$$

skal vi vise:

$$k \text{ er pytagoræisk} \iff l = 0,\ n_1 = 0, \ldots,\ n_r = 0.$$

Udfra primopløsningen af k får vi

$$k^2 = 2^{2l} q_1^{2n_1} \cdots q_r^{2n_r} p_1^{2m_1} \cdots p_s^{2m_s}\,.$$

Ligningen $x^2 + y^2 = k^2$ har derfor altid løsninger, svarende til elementer $\alpha = x + yi$ i $\mathbf{Z}[i]$ med primopløsningen

$$\alpha = \varepsilon(1+i)^{2l} q_1^{n_1} \cdots q_r^{n_r} \pi_1^{\mu_1'} \bar{\pi}_1^{\mu_1''} \cdots \pi_s^{\mu_s'} \bar{\pi}_s^{\mu_s''}, \quad \text{hvor } \mu_j' + \mu_j'' = 2m_j.$$

For et naturligt tal $d > 1$ har vi, at d er divisor i både x og y, hvis og kun hvis d er divisor i $\alpha = x + iy$. Det sidste kan vi afgøre ud fra ovenstående primopløsning af α, og vi ser, at $\alpha = x + yi$ giver en ikke–triviel løsning (x, y), netop når:

$$l = 0,\ n_1 = 0, \ldots,\ n_r = 0 \quad \text{og for hvert } j \text{ er enten } \mu_j' = 0 \text{ eller } \mu_j'' = 0.$$

Der er således ikke–trivielle løsninger netop når k har den angivne form. Er dette tilfældet får vi præcis $4 \cdot 2^s$ ikke–trivielle løsninger, og da disse kommer i grupper på 8 essentielt ens løsninger (nemlig med α også $i\alpha, -\alpha, -i\alpha$ og de 4 konjugerede, som er 8 forskellige løsninger) er der kun $\frac{1}{8} \cdot 4 \cdot 2^s = 2^{s-1}$ essentielt forskellige løsninger♠

Bemærk, at vi også her explicit får beskrevet løsningerne til $x^2 + y^2 = k^2$ ved at løse ligningerne $x_j^2 + y_j^2 = p_j,\ j = 1, \ldots, s$.

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 Λ-*modul* $(M, +, \Lambda)$ er en mængde M forsynet med en (indre) komposition : $M \times M \to M$, kaldet *addition* og betegnet $(x, y) \mapsto x + y$, og en ydre komposition : $\Lambda \times M \to M$, kaldet *multiplikation* 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:

$$\text{(m)}\begin{cases} \text{(i)} & \lambda(x+y) & = \lambda x + \lambda y & \\ \text{(ii)} & (\lambda+\mu)x & = \lambda x + \mu x & \text{for } x, y \in M \\ \text{(iii)} & (\lambda\mu)x & = \lambda(\mu x) & \text{og } \lambda, \mu \in \Lambda. \\ \text{(iv)} & 1x & = x & \end{cases}$$

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

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

Den kommutative gruppe $(M, +)$ siges også at være *organiseret* (via multiplikationen: $\Lambda \times M \to M$) som *modul over* Λ.

Observation. I en Λ-modul M gælder:

$$0x = 0_M = \lambda 0_M \quad \text{og} \quad (-\lambda)x = -(\lambda x) = \lambda(-x) \qquad \text{for } \lambda \in \Lambda \text{ og } x \in M,$$

ganske som (det formelt tilsvarende) for ringe.

(1.2) Terminologi. Hvis ringen Λ er et legeme (f.eks. $\mathbf{R}$ eller $\mathbf{C}$) 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 **R**-modul.) I overensstemmese 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 præsist: Λ-vektorrum) vil vi dog kun benytte for Λ-moduler, når Λ er et skæv-legeme.

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

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

At der herved defineres en **Z**-modul, dvs. at betingelserne (i), (ii), (iii) og (iv) er opfyldt, er netop indholdet af potensreglerne.

En kommutativ gruppe $(M,+)$ kan altså opfattes som en **Z**-modul $(M,+,\mathbf{Z})$. Det er iøvrigt klart, at ovenstående multiplikation : $\mathbf{Z}\times M \to M$ er den eneste via hvilken $(M,+)$ kan organiseres som **Z**-modul, thi er $(n,x) \mapsto n\cdot x$ en sådan multiplikation fås af (1.1) (i) 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 *venstre-modul*. I modsætning hertil defineres en *højre-modul* $(M,+,\Lambda)$ som en mængde M med to kompositioner:

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

som opfylder kravene i (1.1), bortset fra at multiplikationsbetingelsen (iii) erstattes af:

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

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

Notation. 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:

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

(1.5) Nul-modulen. *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 addition i modulen Λ er addition i ringen Λ og multiplikation 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 (index s for sinistra = venstre).

Tilsvarende kan Λ opfattes som en højre-Λ-modul Λ_d (index 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 alle n-sæt $x = (x_1, \ldots, x_n)$, hvor $x_v \in \Lambda$, opfattes som Λ-modul med "koordinativise kompositioner", dvs. at

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n)$$
$$\lambda(x_1, \ldots, x_n) := (\lambda x_1, \ldots, \lambda x_n).$$

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 $x = (x_1, \ldots, x_n) \in \Lambda_d^n$ her er

$$(x_1, \ldots, x_n)\lambda := (x_1\lambda, \ldots, x_n\lambda) \ .$$

(1.8) MATRICER. For givne $n, p \in \mathbf{N}$ kan vi betragte mængden $\mathrm{Mat}_{n,p}(\Lambda)$ af $n \times p$-matricer:

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

Matricen er kvadratisk, hvis $n = p$ [og vi skriver $\mathrm{Mat}_n := \mathrm{Mat}_{n,n}$].

For matricer $\alpha, \beta \in \mathrm{Mat}_{n,p}(\Lambda)$ (af samme størrelse) er *matrix-summen* $\alpha + \beta$ i $\mathrm{Mat}_{n,p}(\Lambda)$ defineret ved

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

og er $\alpha \in \mathrm{Mat}_{n,p}(\Lambda)$ og $\gamma \in \mathrm{Mat}_{p,r}(\Lambda)$ er *matrix-produktet* $\alpha\gamma$ i $\mathrm{Mat}_{n,r}(\Lambda)$ defineret ved

$$(\alpha\gamma)_{ik} := \sum_{j=1}^{p} \alpha_{ij}\gamma_{jk}.$$

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

REGNEREGLER. *Matrix-multiplikation er associativ og distributiv mht. matrix-addition. Mængden* $\mathrm{Mat}_n(\Lambda)$ *af kvadratiske* $n \times n$*-matricer er en ring. Mængden* $\mathrm{Mat}_{n,p}(\Lambda)$ *af* $n \times p$*-matricer er en venstre-*$\mathrm{Mat}_n(\Lambda)$*-modul og en højre* $\mathrm{Mat}_p(\Lambda)$*-modul.*

BEMÆRKNING 1. Ringen $\mathrm{Mat}_n(\Lambda)$ indeholder alle *skalar-matricer*, dvs. matricer af formen $\begin{pmatrix} \lambda & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda \end{pmatrix}$, hvor $\lambda \in \Lambda$. Disse matricer udgør øjensynlig en med Λ isomorf delring af $\mathrm{Mat}_n(\Lambda)$, og multiplikation af en matrix med en skalar-matrix med λ i diagonalen svarer til multiplikation med λ på alle pladser i matricen. Herved organiseres $\mathrm{Mat}_{n,p}(\Lambda)$ som venstre- og højre-modul over Λ.

BEMÆRKNING 2. Et n-sæt $x \in \Lambda^n$ kan opfattes som en søjlematrix: $x \in \mathrm{Mat}_{n,1}(\Lambda)$ og som en rækkematrix: $x \in \mathrm{Mat}_{1,n}(\Lambda)$. Følgelig kan Λ^n opfattes som venstre-$\mathrm{Mat}_n(\Lambda)$-modul og som højre-$\mathrm{Mat}_n(\Lambda)$-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 *homoteti med faktor* λ og den betegnes $\lambda_M : M \to M$. Betingelsen (1.1)(i) udsiger, at λ_M er en homomorfi fra $(M,+)$ til $(M,+)$, 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:

$$\Lambda \to End(M).$$

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 tilsvarende 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.

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

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

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

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

$$f(x+y) = f(x) + f(y) \qquad \text{og}$$
$$f(\lambda x) = \lambda f(x) \qquad \text{for } x, y \in M \text{ og } \lambda \in \Lambda.$$

Ved *kernen* for homomorfien $f : M \to N$ forstås originalmængden $f^{-1}(0)$. Kernen for homomorfien f betegnes også $\mathrm{Ker} f$. Da en Λ-homomorfi 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 Λ-*isomorfi*. 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 M ind i sig selv kaldes også en Λ-*endomorfi*, og hvis den er bijektiv også en Λ-*automorfi*.

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 $: M \to M$. Yderligere 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
$Hom_\Lambda(M,N)$ mængden af Λ-homomorfier $: M \to N$, med
$End_\Lambda(M)$ mængden af Λ-endomorfier $: M \to M$ og med
$Aut_\Lambda(M)$ mængden af Λ-automorfier $: M \to M$.

Observation. $(Hom_\Lambda(M,N), +)$ er en kommutativ gruppe [nemlig en undergruppe i gruppen $Afb(M,N)$ af alle afbildninger af M ind i den kommutative gruppe N].

$(End_\Lambda(M), +, \circ)$ er en ring [nemlig en delring af ringen $End(M)$ af additive endomorfier i $(M,+)$].

$(Aut_\Lambda(M), \circ)$ er en gruppe [nemlig en undergruppe af den fulde automorfigruppe for M].

Gruppen $Aut_\Lambda(M)$ er øjensynlig gruppen af invertible elementer i ringen $End_\Lambda(M)$. ∎

(1.11) Sætning. *Λ-homomorfierne $: \Lambda_s^m \to \Lambda_s^p$ er netop afbildningerne af formen:*

$$x \mapsto x\alpha$$

med en entydigt bestemt matrix $\alpha \in \mathrm{Mat}_{m,p}(\Lambda)$*, hvor vi opfatter elementer i* Λ_s^m *og* Λ_s^p *som rækkematricer.*

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

$$\delta_i = (0, \ldots, 1, \ldots, 0) \in \Lambda_s^m \,,$$

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

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

Sættes $f(\delta_i) = (\alpha_{i1}, \ldots, \alpha_{ip}) \in \Lambda_s^p$ finder vi, da f er lineær:

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

Entydigheden af matricen følger af, at

$$\delta_i\alpha = i\text{'te række i matricen } \alpha.$$

Rækkerne i matricen få således ved at anvende den lineære afbildning på vektorerne δ_i for $i = 1, \ldots, m$ ♠.

Bemærkning. Den i sætningen beskrevne bijektive afbildning fra $\mathrm{Mat}_{m,p}(\Lambda)$ til $Hom_\Lambda(\Lambda_s^m, \Lambda_s^p)$ bevarer addition og er altså en gruppeisomorfi. Men multiplikation af matricer svarer til sammensætning af afbildninger i **den modsatte rækkefølge**. Specielt ses for $m = p$, at

$$\mathrm{Mat}_m(\Lambda) \xrightarrow{\sim} End_\Lambda(\Lambda_s^m)$$

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

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):

$$x \equiv x' \wedge y \equiv y' \implies x + y \equiv x' + y'$$

og med multiplikationen i den forstand, at

$$x \equiv x' \implies \lambda x \equiv \lambda x' \quad \text{for } \lambda \in \Lambda.$$

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:

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

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

$$\boxed{x} + \boxed{y} = \boxed{x+y} \quad \text{og}$$
$$\lambda\boxed{x} = \boxed{\lambda x}, \quad \text{for } x, y \in M.$$

Her betegner $\boxed{\ }$ som sædvanlig den kanoniske afbildning ind i kvotienten $\boxed{\ } : M \to M/N$. Denne afbildning er altså en Λ-homomorfi. Modulen M/N kaldes en *kvotientmodul* af M.

(2.3) Vi får nu på velkendt måde følgende:
Udvidelsessætning. *Enhver Λ-homomorfi $f : M \to P$, som forsvinder på undermodulen $N \subseteq M$, kan entydigt udvides til en Λ-homomorfi $\bar{f} : M/N \to P$.*

Dette betyder, at der findes netop én Λ-homomorfi $\bar{f} : M/N \to P$, så at $\bar{f} \circ \boxed{\ } = f$.

Afbildningen $\bar{f} : M/N \to P$ siges at være *induceret* 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 fås på velkendt måde følgende:

ISOMORFISÆTNING. *Den inducerede Λ-homomorfi $: M/f^{-1}(0) \to P$ er en isomorfi $\bar{f} : M/f^{-1}(0) \xrightarrow{\sim} f(M)$ af kvotienten $M/f^{-1}(0)$ på billedet $f(M)$.*

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 *trivielle 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 *venstreidealer* i ringen Λ. Det er klart, at en delmængde $I \subseteq \Lambda$ er et venstreideal, netop når der gælder:

$$\begin{gathered} 0 \in I, \\ \alpha \in I \wedge \beta \in I \implies \alpha + \beta \in I \quad \text{og} \\ \lambda \in \Lambda \wedge \alpha \in I \implies \lambda\alpha \in I. \end{gathered}$$

(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 $S = \emptyset$, så er $\Lambda S = (0) \subseteq M$.
(1) Hvis S består af ét element, $S = \{e\}$, så er $\Lambda S = \{\lambda e \mid \lambda \in \Lambda\}$.
(n) Hvis S er endelig, $S = \{e_1, \ldots, e_n\}$, så er $\Lambda S = \Lambda e_1 + \cdots + \Lambda e_n$, hvor

$$\Lambda e_1 + \cdots + \Lambda e_n := \{\lambda_1 e_1 + \cdots + \lambda_n e_n \mid \lambda_1, \ldots, \lambda_n \in \Lambda\}.$$

(∞) Hvis S er vilkårlig, så består ΛS af de elementer $x \in M$, der er linearkombinationer:

$$x = \lambda_1 s_1 + \cdots + \lambda_k s_k, \qquad \text{hvor } \lambda_1, \ldots, \lambda_k \in \Lambda,$$

af endelig mange elementer $s_1, \ldots, s_k \in S$.

(2.8) DEFINITION. Lad M være en Λ-modul. Hvis der for en delmængde $S \subseteq M$ gælder, at $\Lambda S = M$, siges M at være *frembragt* af S.

Hvis M kan frembringes af en endelig mængde, siges M at være *endeligt frembragt*. Betingelsen er altså, at der findes en endelig delmængde $\{e_1, \ldots, e_n\}$ af M, så at

$$M = \Lambda e_1 + \cdots + \Lambda e_n.$$

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

$$M = \Lambda e.$$

(2.9) Definition. Lad M være en Λ-modul og lad e være et element i M. Et element $\alpha \in \Lambda$ siges at *annullere* e, hvis $\alpha e = 0$, og mængden af sådanne elementer $\alpha \in \Lambda$ kaldes *annullatoren* for e og betegnes $\operatorname{Ann} e$, altså

$$\operatorname{Ann} e = \{\alpha \in \Lambda \mid \alpha e = 0\}.$$

Ved $\lambda \mapsto \lambda e$ defineres øjensynlig en Λ-homomorfi : $\Lambda_s \to M$. Kernen, der øjensynlig er $\operatorname{Ann} e$, 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:

$$\Lambda_s/\operatorname{Ann} e \xrightarrow{\sim} \Lambda e.$$

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 *annullerer* M, dvs. annullerer hvert element i M, kaldes *annullatoren* for M og betegnes $\operatorname{Ann} M$.

Det ses, at $\lambda \in \operatorname{Ann} M$, netop når homotetien $\lambda_M : x \mapsto \lambda x$ er nul-afbildningen. Annullatoren for M er således kerne for ringhomomorfien : $\Lambda \to End(M)$, 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*

$$\{\textit{undermoduler } N \textit{ i } M \mid N \supseteq N_0\} \overset{\longleftarrow}{\longrightarrow} \{\textit{undermoduler } Q \textit{ i } P\}.$$

Denne forbindelse bevarer inklusionen $\subseteq$, og for undermoduler $N \supseteq N_0$ af M gælder:

$$f(N) \cong N/N_0 \qquad \textit{og} \qquad P/f(N) \cong M/N.$$

Bevis. For en undermodul Q i P har vi øjensynlig $f^{-1}(Q) \supseteq N_0$, 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 $x \in f^{-1}(f(N))$, så har vi $f(x) = f(n)$, med $n \in N$, og derfor er $f(x - n) = f(x) - f(n) = 0$. Det følger, at $x - n \in \mathrm{Ker} f = N_0 \subseteq N$, og så er også

$$x = n + (x - n) \in N.$$

Af den generelle Isomorfisætning (2.4) 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:

$$M \overset{f}{\to} P \overset{\square}{\longrightarrow} P/f(N)$$

har kernen $f^{-1}(f(N)) = N$ ♠

(3.2) Specielt kan f være den kanoniske homomorfi $\square : M \to M/N_0$, hvor $N_0 \subseteq M$ er en given undermodul. Hvis $N \supseteq N_0$ er en undermodul i M, kan vi identificere billedet $f(N) \subseteq M/N_0$ 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 fællesmængden $N_1 \cap N_2$ er en undermodul. Videre er det let at se, at summen $N_1 + N_2$, 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 der gælder:

NOETHERS FØRSTE ISOMORFISÆTNING. *Lad N_1 og N_2 være undermoduler i Λ-modulen M. Da 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:

$$N_1 \overset{i}{\hookrightarrow} N_1 + N_2 \overset{k}{\to} (N_1 + N_2)/N_2.$$

Denne homomorfi er surjektiv, thi hvert element i kvotienten $(N_1 + N_2)/N_2$ er af formen $\boxed{n_1 + n_2} = \boxed{n_1} = k \circ i(n_1)$. Da kernen for denne homomorfi øjensynlig er $N_1 \cap N_2$, følger påstanden af den generelle Isomorfisætning (2.4) ♠

4. Direkte sum af moduler. Basis.

(4.1) Definition. Lad M være en Λ-modul. Ved *summen* af undermoduler $N_1, \ldots, N_n$ i M forstås delmængden

$$N_1 + \cdots + N_n := \{x_1 + \cdots + x_n \mid x_i \in N_i \text{ for } i = 1, \ldots, n\}.$$

Summen er øjensynlig selv en undermodul, endda den mindste, som indeholder alle N_i for $i = 1, \ldots, n$.

At M *er sum* af undermodulerne $N_1, \ldots, N_n$ betyder, at $M = M_1 + \cdots + M_n$, altså at der for hvert $x \in M$ findes en fremstilling:

$$x = x_1 + \cdots + x_n, \quad \text{hvor } x_i \in N_i \text{ for } i = 1, \ldots, n.$$

(4.2) Definition. Lad M være en Λ-modul. Undermoduler $N_1, \ldots, N_n$ i M kaldes da *uafhængige* eller siges at *danne direkte sum*, hvis der af

$$x_1 + \cdots + x_n = 0, \qquad \text{hvor } x_i \in N_i \text{ for } i = 1, \ldots, n\,,$$

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:

$$x = x_1 + \cdots + x_n, \qquad \text{hvor } x_i \in N_i \text{ for } i = 1, \ldots, n\,,$$

er entydig.

(4.3) Definition. Lad M være en Λ-modul. Vi siger da, at M *er direkte sum af undermodulerne* $N_1, \ldots, N_n$, 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:

$$x = x_1 + \cdots + x_n, \qquad \text{hvor } x_i \in N_i \text{ for } i = 1, \ldots, n.$$

Observation. To undermoduler N_1 og N_2 i M er uafhængige, netop når $N_1 \cap N_2 = (0)$, thi ligningen $x_1 + x_2 = 0$, hvor $x_1 \in N_1$ og $x_2 \in N_2$, svarer til ligningen $x + (-x) = 0$, hvor $x \in N_1 \cap N_2$.

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 $N_1, \ldots, N_n$. Lad der være givet homomorfier $f_i : N_i \to P$ for $i = 1, \ldots, n$ ind i en Λ-modul P. Da findes en og kun én homomorfi $f : M \to P$, så at $f|N_i = f_i$ for $i = 1, \ldots, n$.*

Bevis. **Entydighed:** Lad $f : M \to P$ være en homomorfi, der opfylder det stillede krav. Da M er sum af undermodulerne $N_1, \ldots, N_n$ har hvert $x \in M$ en fremstilling:

$$(*) \quad x = x_1 + \cdots + x_n, \qquad \text{hvor } x_i \in N_i \text{ for } i = 1, \ldots, n,$$

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 $N_1, \ldots, N_n$ 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 $f|N_i = f_i$ for $i = 1, \ldots, n \heartsuit$

(4.4) Konstruktion. Betragt nu vilkårlige Λ-moduler $M_1, \ldots, M_n$. 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 for $i = 1, \ldots, n$. Vi vil oftest skrive disse n-sæt som søjler, og vi organiserer dem som Λ-modul ved kompositionerne:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} + \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} := \begin{pmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{pmatrix} \quad \text{og} \quad \lambda \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} \lambda x_1 \\ \vdots \\ \lambda x_n \end{pmatrix} \quad \text{for } \lambda \in \Lambda.$$

Opfattet som Λ-modul betegnes produktmængden sædvanligvis $M_1 \oplus \cdots \oplus M_n$.

For hvert $i = 1, \ldots, n$ er den i-te *projektion*, dvs. afbildningen:

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto x_i \,,$$

øjensynlig en surjektiv homomorfi : $M_1 \oplus \cdots \oplus M_n \to M_i$.

For hvert $i = 1, \ldots, n$ definerer vi den i-te *injektion* som afbildningen:

$$y \mapsto \begin{pmatrix} 0 \\ \vdots \\ y \\ \vdots \\ 0 \end{pmatrix} \qquad \text{for } y \in M_i.$$

Det er let at se, at injektionen er en injektiv homomorfi : $M_i \hookrightarrow M_1 \oplus \cdots \oplus M_n$. Hvis misforståelser er udelukket, vil vi oftest indentificere modulen M_i med sit billede ved den i-te injektion 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:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ x_2 \\ \vdots \\ 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 \\ 0 \\ \vdots \\ x_n \end{pmatrix},$$

hvor altså det i-te led tilhører undermodulen M_i for $i = 1, \ldots, n$. Den konstruerede modul $M_1 \oplus \cdots \oplus M_n$ 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 den *(ydre) direkte sum* af de givne moduler $M_1, \ldots, M_n$.

(4.5) Lad $N_1, \ldots, N_n$ være undermoduler i en given Λ-modul M. Vi kan da betragte den ydre direkte sum $N_1 \oplus \cdots \oplus N_n$. Ved

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto x_1 + \cdots + x_n \in M$$

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 $N_1, \ldots, N_n$,
(2) injektiv, netop når undermodulerne $N_1, \ldots, N_n$ er uafhængige og
(3) bijektiv, netop når M er direkte sum at undermodulerne $N_1, \ldots, N_n$.

Det følger, at M er direkte sum af undermodulerne $N_1, \ldots, N_n$, 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:

$$N_1 \oplus \cdots \oplus N_n = M \qquad (\text{eller } M = N_1 \oplus \cdots \oplus N_n).$$

(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 *komplement* 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 $\boxed{k} = 0$ 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 $\boxed{k}$, hvor $k \in K$, 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 $\boxed{n+k} = \boxed{k}$ 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 underrum i et 2-dimensionalt vektorrum har således som komplement ethvert andet 1-dimensionalt underrum.

(3) Til en given undermodul behøver der ikke at findes komplementer. I $\mathbf{Z}$-modulen $\mathbf{Z}$ må et komplement til $N = \mathbf{Z}n$, hvor $n \geq 0$, have formen $K = \mathbf{Z}k$ med $k \geq 0$. Da $kn \in \mathbf{Z}n \cap \mathbf{Z}k = (0)$, må vi have $n = 0$ (og dermed $N = (0)$) eller $k = 0$ (og dermed $\mathbf{Z} = N + K = N$). Det er således kun de trivielle undermoduler $N = (0)$ og $N = \mathbf{Z}$, der har komplementer.

(4.8) DEFINITION. Lad M være en Λ-modul. En undermodul $N \subseteq M$ siges at være *direkte sumand* i M, hvis der findes et komplement til N, dvs. en undermodul $K \subseteq M$, så at

$$M = N \oplus K.$$

SÆTNING. *Lad N være en undermodul i M, lad $i : N \hookrightarrow M$ være inklusionsafbildningen (dvs. $i(x) = x$ for $x \in N$) og lad $p : M \to M/N$ være den kanoniske homomorfi (dvs. $p(x) = \boxed{x}, x \in M$). Da er følgende betingelse 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:

$$x = n + k, \qquad \text{hvor } n \in N \text{ og } k \in K,$$

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)⇒(ii)**. Videre følger det, jfr. Sætning (4.6), at hvert element $X \in M/N$ har formen $X = \boxed{k}$ 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 $\boxed{s(X)} = X$, når $X \in M/N$. Altså er $p \circ s = 1_{M/N}$, så vi har vist, at **(i)⇒(iii)**.

"(ii)⇒(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)⇒(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 $0 = \boxed{n} = p(n) = ps(X) = X$, dvs. $X = 0$, og dermed $n = 0$. Følgelig er $N \cap K = 0$. Videre har vi for $x \in M$, at

$$x = (x - s(\boxed{x})) + s(\boxed{x}),$$

og her er $p(x - s(\boxed{x})) = \boxed{x} - ps(\boxed{x}) = \boxed{x} - \boxed{x} = 0$, dvs. $x - s(\boxed{x}) \in N$ og $s(\boxed{x}) \in K$. Følgelig er $M = N + K$ ♠

(4.9) Definition. Lad M være en Λ-modul. Et sæt $(v_1, \ldots, v_n)$ af elementer i M kaldes et *frembringersystem* for M, hvis hvert element $x \in M$ har en fremstilling som en linearkombination:

$$x = \lambda_1 v_1 + \cdots + \lambda_n v_n, \quad \text{hvor } \lambda_i \in \Lambda \text{ for } i = 1, \ldots, n.$$

Sættet kaldes et *frit system* eller et *lineært uafhængigt system* i M, hvis der af

$$0 = \lambda_1 v_1 + \cdots + \lambda_n v_n, \quad \text{hvor } \lambda_i \in \Lambda \text{ for } i = 1, \ldots, n,$$

følger, at $\lambda_1 = \cdots = \lambda_n = 0$.

Sættet kaldes en *fri basis* for M, hvis det både er et frembringersystem og et frit system.

Bemærkninger. Sættet $(v_1, \ldots, v_n)$ er øjensynlig et frembringersystem for M, netop når delmængden $\{v_1, \ldots, v_n\} \subseteq M$ frembringer M.

Et enkelt element $v \in M$ udgør et frit system i M, netop når der af

$$\lambda v = 0, \qquad \text{hvor } \lambda \in \Lambda,$$

følger, at $\lambda = 0$. Et sådant element $v \in M$ kaldes også et *frit element* i M.

En ligning

$$\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$$

kaldes også en *lineær relation* mellem v_i'erne. At et sæt $(v_1, \ldots, v_n)$ 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. er et *lineært afhængigt* 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 følgende: Sættet $(v_1, \ldots, v_n)$ er et frembringersystem, netop når M er sum af undermodulerne $\Lambda v_1, \ldots, \Lambda v_n$, dvs. når

$$M = \Lambda v_1 + \cdots + \Lambda v_n.$$

Sættet er et frit system, netop når undermodulerne $\Lambda v_1, \ldots, \Lambda v_n$ er uafhængige og hvert v_i er et frit element. Sættet er en fri basis, netop når

$$M = \Lambda v_1 \oplus \cdots \oplus \Lambda v_n, \text{ og hvert } v_i \text{ er et frit element.}$$

Bemærkning. Det er sædvane at kalde et sæt $(v_1, \ldots, v_n)$ i M for en *basis* for M, hvis

$$M = \Lambda v_1 \oplus \cdots \oplus \Lambda v_n \text{ og } v_i \neq 0 \text{ for } i = 1, \ldots, n.$$

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 $(v_1, \ldots, v_n)$, kaldes også en *fri* 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 element λ i $\Lambda_s = \Lambda$ har den entydige fremstilling $\lambda = \lambda 1$. Mere generelt gælder for $n \in \mathbf{N}$, at søjlerne

$$\delta_1 := \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ \delta_2 := \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \ \delta_n := \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

er en fri basis for Λ-modulen Λ_s^n. 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 $(\delta_1, \ldots, \delta_n)$ kaldes også den *kanoniske basis* for Λ_s^n.

(4.12) Sætning. *Antag, at Λ-modulen M har en fri basis $(u_1, \ldots, u_n)$. Lad der være givet elementer $v_1, \ldots, v_n$ i en Λ-modul P. Da findes en og kun én homomorfi $f : M \to P$, så at $f(u_i) = v_i$ for $i = 1, \ldots, n$.*

Bevis. Resultatet vises enten analogt med beviset for Sætning (4.3) eller som et korollar til Sætning (4.3) ♡

(4.13) Lad $(v_1, \ldots, v_n)$ være et sæt af elementer i en Λ-modul M. Ved

$$\begin{pmatrix}\lambda_1\\ \vdots\\ \lambda_n\end{pmatrix} \mapsto \lambda_1 v_1 + \cdots + \lambda_n v_n$$

defineres øjensynlig en homomorfi : $\Lambda_s^n \to M$. Det er for øvrigt den entydigt bestemte homomorfi : $\Lambda_s^n \to M$, som opfylder $\delta_i \mapsto v_i$ for $i = 1, \ldots, n$, jfr. Sætning (4.12).

Af Definition (4.9) fås umiddelbart følgende:

Observation. Homomorfien : $\Lambda_s^n \to M$ er

(1) surjektiv, netop når $(v_1, \ldots, v_n)$ er et frembringersystem,
(2) injektiv, netop når $(v_1, \ldots, v_n)$ er et frit system, og
(3) bijektiv, netop når $(v_1, \ldots, v_n)$ er en fri basis.

Det følger, at $(v_1, \ldots, v_n)$ 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 $(u_1, \ldots, u_n)$ være et sæt i N, lad $(w_1, \ldots, w_p)$ være et sæt i P, og vælg elementer $v_j \in M$ med $f(v_j) = w_j$ for $j = 1, \ldots, p$. Da gælder:*

Er $(u_1, \ldots, u_n)$ et frembringersystem (resp. et frit system, resp. en fri basis) i N og er $(w_1, \ldots, w_p)$ et frembringersystem (resp. et frit system, resp. en fri basis) i P, så er $(u_1, \ldots, u_n, v_1, \ldots, v_p)$ et frembringersystem (resp. et frit system, resp. en fri basis) i M.

Bevis. (1) **"frembringersystem":** For $x \in M$ har vi $f(x) = \lambda_1 w_1 + \cdots + \lambda_p w_p$ 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 $x - \lambda_1 v_1 - \cdots - \lambda_p v_p = \mu_1 u_1 + \cdots + \mu_n u_n$ med $\mu_i \in \Lambda$. Heraf fås den ønskede fremstilling af x.
(2) **"frit system":** Antag, at $0 = \mu_1 u_1 + \cdots + \mu_n u_n + \lambda_1 v_1 + \cdots + \lambda_p v_p$. Anvendes homomorfien f fås ligningen $0 = \lambda_1 w_1 + \cdots + \lambda_p w_p$. Følgelig er $\lambda_1 = \cdots = \lambda_p = 0$. Den første ligning kan nu skrives $0 = \mu_1 u_1 + \cdots + \mu_n u_n$, og så er også $\mu_1 = \cdots = \mu_n = 0$.
(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 $(w_1, \ldots, w_k)$ være en fri basis for kvotienten M/N og lad $p : M \to M/N$ være den kanoniske afbildning.

Vi efterviser betingelsen (4.8)(iii). Vælg elementer $v_j \in M$, så at $p(v_j) = w_j$ for $j = 1, \ldots, k$. Der findes da (Sætning (4.12), "eksistensen") en homomorfi $s : M/N \to M$, så at

$$s(w_j) = v_j \quad \text{for } j = 1, \ldots, k.$$

For den sammensatte homomorfi $p \circ s : M/N \to M/N$ fås derfor

$$p \circ s(w_j) = p(v_j) = w_j \qquad \text{for } j = 1, \ldots, k,$$

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 *frembringersystem* for M, hvis hvert element $x \in M$ kan skrives som en linearkombination af endelig mange elementer fra familien, dvs. hvis der for hvert $x \in M$ findes en endelig delmængde $\{i_1, \ldots, i_k\} \subseteq I$ og koefficienter $\lambda_1, \ldots, \lambda_k$ så at

$$(*) \quad x = \lambda_1 v_{i_1} + \cdots + \lambda_k v_{i_k}.$$

Familien kaldes et *frit system* eller et *lineært uafhængigt system* i M, hvis enhver endelig delfamilie udgør et frit system, dvs. hvis der for enhver endelig delmængde $\{i_1, \ldots, i_k\} \subseteq I$ (med forskellige elementer $i_1, \ldots, i_k$) gælder, at der af

$$(\circ) \quad 0 = \lambda_1 v_{i_1} + \cdots + \lambda_k v_{i_k}, \qquad \text{hvor } \lambda_1, \ldots, \lambda_k \in \Lambda,$$

følger, at $\lambda_1 = \cdots = \lambda_k = 0$.

Familien kaldes en *fri basis* 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 $(\circ)$, kan man til højresiden tilføje led af formen λe_i, når blot $\lambda = 0$. Heraf følger let, at ovennævnte definition stemmer overens med Definition (4.9), når indexmængden er den endelige mængde $I = \{1, \ldots, n\}$. 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 $i \neq i_1, \ldots, i_k$, 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 højresiden 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 da på oplagt måde som en Λ-modul, idet vi for afbildninger $\varphi, \psi : I \to \Lambda$ definere summen $\varphi + \psi$ som afbildningen:

$$i \mapsto \varphi(i) + \psi(i), \qquad \text{dvs. } (\varphi + \psi)(i) = \varphi(i) + \psi(i),$$

og produktet $\lambda\varphi$ med skalaren $\lambda \in \Lambda$, som afbildningen:

$$i \mapsto \lambda\varphi(i), \qquad \text{dvs. } (\lambda\varphi)(i) = \lambda\varphi(i).$$

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

$$\varphi(i) = \begin{cases} \lambda_1 & \text{hvis } i = i_1 \\ \quad\vdots & \\ \lambda_k & \text{hvis } i = i_k \\ 0 & \text{hvis } i \neq i_1, \ldots, i_k. \end{cases}$$

Når $\varphi \in \Lambda^{\oplus I}$, så 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 basiselementerne δ_i i den fri basis).

(4.18) Definition. Lad M være en Λ-modul og lad $(v_i)_{i \in I}$ 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 øjensynlig minimalt, netop når "det holder op med at være et frembringersystem, når der fjernes et (vilkårligt) element fra systemet". Et frit system er øjensynlig 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 $\lambda v = 0$ og $\lambda \neq 0$ følger, at $0 = \lambda^{-1}\lambda v = 1v = v$. Enhver basis for M er således en fri basis.

Bevis for Sætningen. **(i)⇒(iii)**: 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 $v_{i_0}, v_{i_1}, \ldots, v_{i_k}$ 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:

$$(*) \quad v_{i_0} = \mu_1 v_{i_1} + \cdots + \mu_k vi_k \quad (\text{hvor } \mu_j := -\lambda_0^{-1}\lambda_j \in \Lambda).$$

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.
(iii)⇒(i): 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:

$$v_{i_0} = \lambda_1 v_{i_1} + \cdots + \lambda_k v_{i_k}, \qquad \text{hvor } \lambda_i \in \Lambda,$$

og $i_1, \ldots, i_k \in I \setminus \{i_0\}$. 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:

$$x = \mu_1 v_{i_1} + \cdots + \mu_k v_{i_k} \qquad (\text{hvor } \mu_j = -\lambda^{-1}\lambda_j \in \Lambda).$$

Men så er x en linearkombination af endelig mange vektorer 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) *Vektorrummet M er en fri modul, dvs. der findes en basis for M.*
(b) *Alle baser for M er ækvipotente.*

Bevis. 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 endelig 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 tre lemma'er ♡

LEMMA 1. *Lad M være en modul over en vilkårlig ring. Hvis M har et endeligt frembringersystem, så har M også et endeligt minimalt frembringersystem.*

Bevis. Fra et endeligt frembringersystem kan vi successivt fjerne eventuelt overflødige elementer, og så fås efter endelig mange skridt et minimalt frembringersystem ♠

LEMMA 2. *Lad M være en modul over en vilkårlig ring Λ. Da findes en delmængde af M, som er et maksimalt frit 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 for $j \in J$ 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 $s_1, \ldots, s_k \in S$. Da $S = \bigcup_j S_j$, findes for hvert $i = 1, \ldots, k$ 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 $S_{j_1}, \ldots, S_{j_k}$, f.eks. S_{j_1}, omfatte de øvrige S_{j_i}'er. Følgelig er $s_i \in S_{j_1}$ for $i = 1, \ldots, k$, og så er $(*)$ en lineær relation mellem endelig mange forskellige elementer i S_{j_1}. Og så er koefficenterne $\lambda_1 = \cdots = \lambda_k = 0$, da S_{j_1} var et frit system ♠

LEMMA 3. *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 har I højst samme mægtighed som 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

$$(*) \quad u_j \text{ er en linearkombination af } v_i\text{'er med } i \in I_j.$$

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 ifølge $(*)$ 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, så er I derfor en endelig foreningsmængde af endelige mængder, og dermed endelig.
2°: Hvis mængden J er uendelig, så vælger vi for hvert $j \in J$ en surjektiv afbildning af $\mathbf{N}$ på den endelige mængde I_j. Herudfra fås klart en surjektiv afbildning : $J\times\mathbf{N} \to \bigcup_{j\in J} I_j = I$, og så findes som bekendt også en injektiv afbildning : $I \to J \times \mathbf{N}$. For en uendelig mængde J er det imidlertid velkendt, at $J \times \mathbf{N}$ er ækvipotent med J. Idet vi derfor kan sammensætte med en bijektiv afbildning : $J \times \mathbf{N} \to J$, får vi en injektiv afbildning : $I \to J$ ♠

(4.21) Bemærk forskellen på konklusionerne i de to tilfælde i Lemma 3 (4.20). 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 ikke, at de har samme elementantal.

Eksempel. Som $\mathbf{Z}$-modul er $\mathbf{Z}$ fri med 1 som fri basis. Sættet med 1 som eneste element er altså et minimalt frembringersystem. Af ligningen $x = x \cdot 3 - x \cdot 2$ for $x \in \mathbf{Z}$ fremgår, at også sættet (3,2) er et frembringersystem. Og det er øjensynlig også minimalt.

5. Simple moduler.

(5.1) Definition. En Λ-modul S kaldes en *simpel modul*, 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 trivielle (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) *Modulen S er en simpel modul.*
(ii) *Modulen S er $\neq 0$, og for hvert element $e \neq 0$ i S er $\Lambda e = S$.*
(iii) *Modulen 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 for Sætningen. **(i)⇒(ii)**: 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 $\Lambda e = S$.
(ii)⇒(i): 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 $(\Lambda e =)N = S$.
(i)⇔(iii): 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 Noether's 2. isomorfisætning (3.1) er der så en bijektiv forbindelse mellem undermoduler af $S = \Lambda/I$ 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 ♠

Korollar. *En simpel modul er cyklisk* ♡

(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 $\Lambda \neq 0$, 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_s).*

Bevis. En cyklisk modul $\neq 0$ er isomorf med en kvotient Λ_s/I, hvor $I \subset \Lambda$ er et venstre-ideal. Da Λ_s er simpel, har Λ kun trivielle venstre-idealer, så må vi have $I = (0)$ ♠

(5.4) EKSEMPEL. De simple kommutative grupper, dvs. de simple $\mathbf{Z}$-moduler, er de endelige cykliske grupper af primtalsorden, thi maksimalidealerne i den kommutative ring $\mathbf{Z}$ er som bekendt idealerne $\mathbf{Z}p$, hvor p er et primtal, og kvotientgruppen $\mathbf{Z}/\mathbf{Z}p$ har orden p.

(5.5) SÆTNING. *Lad M være en Λ-modul $\neq 0$, og antag, at der i M findes et endeligt frembringersystem $(v_1, \ldots, v_n)$. 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, hvor $j \in J$, 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

$$x + y, \quad \lambda x, \text{ (for } \lambda \in \Lambda) \text{ og nul-elementet } 0$$

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 for $i = 1, \ldots, n$, så at $v_i \in N_{j_i}$. Da N_j'erne var totalt ordnede, vil en af modulerne $N_{j_1}, \ldots, N_{j_n}$, f.eks. N_{j_1} omfatte de øvrige. Men så er $v_1, \ldots, v_n \in N_{j_1}$ 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 $\Lambda \neq 0$, 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 Noether's 2. isomorfisætning (3.1) 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 $\mathbf{Z}$ har ingen simple undermoduler. Af Eksempel (5.4) fremgår nemlig specielt, at de simple $\mathbf{Z}$-moduler er endelige, og blandt undermodulerne i $\mathbf{Z}$ (nødvendigvis af formen $\mathbf{Z}n$) 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 $(M_j)_{j=0,\ldots,n}$ af undermoduler i M, således at

$$(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_{n-1} \subseteq M_n = M,$$

kaldes en *kæde* i M. Tallet n kaldes kædens *længde*. Kvotientmodulerne M_{j+1}/M_j for $j = 0, \ldots, n-1$ kaldes kædens *kvotienter* (eller *faktorer*). Antallet af kvotienter er altså kædens længde. En kæde siges at have *gentagelser*, hvis der for et j gælder $M_j = M_{j+1}$. Dette er ensbetydende med at der for den tilsvarende kvotient gælder $M_{j+1}/M_j = (0)$.

En kæde $(N_j)_{j=0,\ldots,n}$ i M siges at være en *forfining* af kæden $(M_i)_{i=0,\ldots,m}$ i M, hvis der findes $0 \leq j_0 < j_1 < \cdots < j_m \leq n$, således at

$$N_{j_i} = M_i \qquad \text{for } i = 0, \ldots, m.$$

Dette betyder, at vi kan tænke på kæden (N_j) som fremkommet ud fra kæden (M_i) ved at der mellem M_i og M_{i+1} er indskudt visse N'er:

$$(M_i =)N_{j_i} \subseteq N_{j_i+1} \subseteq N_{j_i+2} \subseteq \cdots \subseteq N_{j_{i+1}} (= M_{i+1}).$$

En kæde $(M_i)_{i=0,\ldots,m}$ kan *trivielt forfines* ved at gentage visse af M_i'erne.

En kæde (M_i), hvori alle kvotienterne er simple moduler, kaldes en *Jordan–Hölder kæde* i M. Undermodulerne i en kvotient M_{i+1}/M_i svarer til undermoduler N, som opfylder, at $M_i \subseteq N \subseteq M_{i+1}$. Det følger heraf, at en kæde (M_i) i M er en Jordan–Hölderkæde, hvis og kun hvis den er uden gentagelser og kun trivielt kan forfines.

(6.2) Eksempler. (1) 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, altså de 1-dimensionale vektorrum, jfr. Korollar (5.3). At kæden er en Jordan–Hölder kæde betyder altså at $\dim V_1 = 1$, $\dim V_2/V_1 = 1$, ... ,$\dim V_n/V_{n-1} = 1$, 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–Hölder kæder i endeligdimensionale vektorrum, og alle Jordan–Hölder kæder i et sådant vektorrum V har den samme længde, nemlig $\dim V$.

(2) En $\mathbf{Z}$-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 $\mathbf{Z}$-moduler er grupper, hvis orden er et primtal p (nødvendigvis isomorfe med $\mathbf{Z}/p$). At kæden er en Jordan–Hölder kæde betyder altså, at alle indices:

$$|M_1| = |M_1{:}M_0|, |M_2{:}M_1|, \ldots, |M_n{:}M_{n-1}| = |M{:}M_{n-1}|$$

er primtal. Ifølge Indexsætningen (Lagrange's formel) er $|M_i| = |M_i{:}M_{i-1}| \cdot |M_{i-1}|$ for $i = 1, \ldots, n$, så ved induktion fås, at $|M| = |M_n| = |M_n{:}M_{n-1}| \cdots |M_1{:}M_0|$. Hvis (M_i) er en Jordan–Hölder kæde i M, så er altså

$$|M| = |M_n{:}M_{n-1}| \cdots |M_2{:}M_1| \cdot |M_1|$$

en primopløsning af $|M|$. Specielt er altså M en endelig gruppe, og længden n af Jordan–Hölder kæden er antallet af primfaktorer i $|M|$.

(3) Kæden

$$(0) \subseteq 12\mathbf{Z} \subseteq 6\mathbf{Z} \subseteq \mathbf{Z}$$

i $\mathbf{Z}$ er ikke en Jordan–Hölder kæde. Dens kvotienter er (på isomorfi nær): $\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z}$ og $\mathbf{Z}/6\mathbf{Z}$.

(6.3) I analogi med de foregående eksempler gælder for moduler over en vilkårlig ring følgende:

JORDAN'S SÆTNING. *To vilkårlige Jordan–Hölder kæder i en Λ-modul M har samme længde.*

Denne sætning er en følge af Hölders sætning herunder.

(6.4) DEFINITION. To kæder $(M_i)_{i=0,\ldots,m}$ og $(N_j)_{j=0,\ldots,n}$ 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 σ af $\{0, \ldots, m-1\}$, således at M_{i+1}/M_i er isomorf med $N_{\sigma_i+1}/N_{\sigma_i}$ for $i = 0, \ldots, m-1$. To ækvivalente kæder i M har specielt samme længde.

HÖLDER'S SÆTNING. *To vilkårlige Jordan–Hölder kæder i en Λ-modul M er ækvivalente.*

Denne sætning følger af:

SCHREIER'S FORFININGSSÆTNING. *To vilkårlige kæder i en Λ-modul M har ækvivalente forfininger.*

Det er klart, at forfiningssætningen medfører Hölders sætning, idet en Jordan–Hölder kæde kun har trivielle forfininger.

Bevis for forfiningssætningen. Lad de to kæder i M være $(M_i)_{i=0,\ldots,m}$ og $(N_j)_{j=0,\ldots,n}$. Ved hjælp af kæden (N_j) indskyder vi nu mellem M_i og M_{i+1} en hel række undermoduler og vi får herved en forfining af kæden (M_i): Vi sætter

$$M_{ij} := (M_{i+1} \cap N_j) + M_i \quad \text{for } i = 0, \ldots, m-1 \text{ og } j = 0, \ldots, n.$$

Vi har $M_i = M_{i0} \subseteq M_{i1} \subseteq \cdots \subseteq M_{i,n-1} \subseteq M_{in} = M_{i+1}$. Af kæden (M_i) 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

$$M_{i,j+1}/M_{i,j} \qquad \text{for } i = 0, \ldots, m-1 \text{ og } j = 0, \ldots, n-1.$$

Tilsvarende sætter vi

$$N_{ji} := (M_i \cap N_{j+1}) + N_j,$$

og vi får en forfining af kæden (N_j), af længden nm og med kvotienterne:

$$N_{j,i+1}/N_{j,i} \qquad \text{for } j = 0, \ldots, n-1 \text{ og } i = 0, \ldots, m-1.$$

Vi viser, at de to opnåede forfininger er ækvivalente, ved at vise, at der for alle j, i gælder:

$$M_{i,j+1}/M_{i,j} \simeq N_{j,i+1}/N_{j,i}$$

altså:

$$\frac{M_{i+1} \cap N_{j+1}) + M_i}{(M_{i+1} \cap N_j) + M_i} \simeq \frac{(M_{i+1} \cap N_{j+1}) + N_j}{(M_i \cap N_{j+1}) + N_j}.$$

Denne påstand involverer de fire undermoduler $M_i \subseteq M_{i+1}$ og $N_j \subseteq N_{j+1}$, og den 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 Zassenhaus' lemma. 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 $(M'' \cap N'') \cap [(M'' \cap N') + M']$. Det er let at se, at

$$(M'' \cap N'') \cap [(M'' \cap N') + M'] = (M'' \cap N') + (M' \cap N''),$$

og 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, idet venstre siden ovenfor er "symmetrisk i M og N" ♠

Hermed er beviset for Forfiningssætningen (og dermed for de foregående sætninger) fuldført ♠

(6.5) En Λ-modul M, i hvilken der findes en Jordan Hölder kæde, kaldes en *Jordan–Hölder modul* eller en modul af *endelig længde*. *Længden* af en sådan modul M kan ifølge Jordans sætning defineres som længden af en vilkårlig Jordan–Hölder kæde i M. Denne længde betegnes $\log(M)$.

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 forfiningssætningen giver følgende:

KOROLLAR. *I en Jordan–Hölder modul M kan enhver kæde uden gentagelser forfines til en Jordan–Hölder kæde* ♡

Specielt har enhver kæde uden gentagelser en længde $\leq \log(M)$.

(6.7) SÆTNING. *Lad N være en undermodul i Λ-modulen M. Da er M en Jordan–Hölder modul, hvis og kun hvis både N og M/N er Jordan–Hölder moduler. Er dette tilfældet, gælder:*

$$\log M = \log N + \log M/N.$$

Bevis. I følge Noethers anden isomorfisætning (3.1) er der en entydig forbindelse mellem kæder i kvotienten 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_{i+1}/M_i i følgen $(*)$. 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 undermodulen N, og en Jordan–Hölder kæde i M/N svarende til en følge:

$$N = M_0 \subset M_1 \subset \cdots \subset M_m = M$$

med simple kvotienter. Heraf får vi 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 $(0) = N_0 \subset \cdots \subset N_{n-1} \subset N$ er Jordan–Hölder kæde i N og af resten af følgen: $N \subset M_1 \subset \cdots \subset M_m = M$ får vi som nævnt en Jordan–Hölder kæde 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 $Q_j := M_j/M_{j-1}$ for $j = 1, \ldots, n$. Da er M en Jordan–Hölder modul, hvis og kun hvis alle kvotienterne Q_j er Jordan–Hölder moduler. Er dette tilfældet, gælder:

$$\operatorname{long} M = \operatorname{long} Q_1 + \cdots + \operatorname{long} Q_n.$$

Bevis. Følger af Sætning (6.7) 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_j er Jordan–Hölder moduler. Er dette tilfældet, gælder:*

$$\operatorname{long}(N_1 \oplus \cdots \oplus N_n) = \operatorname{long} N_1 + \cdots + \operatorname{long} N_n.$$

Bevis. I den direkte sum M har vi kæden:

$$(0) \subseteq N_1 \subseteq N_1 \oplus N_2 \subseteq \cdots \subseteq N_1 \oplus \cdots \oplus N_n = M,$$

hvis kvotienter er $N_1, \ldots, N_n$. Påstanden følger nu af Korollar (6.8) ♠

(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*

$$\operatorname{long}(N_1 \cap N_2) + \operatorname{long}(N_1 + N_2) = \operatorname{long} N_1 + \operatorname{long} N_2.$$

Bevis. Dette følger ved gentagen anvendelse af sætning (6.7) i forbindelse med Noethers første isomorfi (3.3):

$$(N_1 + N_2)/N_1 \simeq N_1/N_1 \cap N_2 \text{ ♠}$$

(6.11) LEMMA. *Lad* $(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ *være en kæde, hvis kvotienter* M_j/M_{j-1} *er cykliske, og vælg for hvert* $j = 1, \ldots, n$ *et element* $e_j \in M_j$, *hvis ækvivalensklasse* $\boxed{e_j} \in M_j/M_{j-1}$ *frembringer* M_j/M_{j-1}. *Da er* $(e_1, \ldots, e_n)$ *et frembringersystem for* M.

Bevis. Induktivt kan vi antage, at $(e_1, \ldots, e_{n-1})$ er et frembringersystem for M_{n-1}. Og så følger påstanden af Sætning (4.14) ♠

BEMÆRKNING. Er omvendt $(e_1, \ldots, e_n)$ et frembringersystem i en modul M, så defineres ved $M_j := \Lambda e_1 + \cdots + \Lambda_j$ for $j = 0, 1, \ldots, n$ en kæde i M, hvis kvotienter M_j/M_{j-1} for $j = 1, \ldots, n$ er cykliske, thi i kvotienten M_j/M_{j-1} gælder:

$$\boxed{\lambda_1 e_1 + \cdots + \lambda_j e_j} = \boxed{\lambda_j e_j} = \lambda_j \boxed{e_j},$$

hvoraf følger, at $\boxed{e_j}$ frembringer M_j/M_{j-1}.

SÆTNING. *En Jordan–Hölder modul er endeligt frembragt.*

Bevis. Følger af Lemma'et, da en simpel modul er cyklisk, jfr. Sætning (5.2) ♠

(6.12) DEFINITION. Ringen Λ siges at have *endelig længde*, hvis Λ-modulen Λ_s har endelig længde, dvs. hvis Λ_s er en Jordan–Hölder modul. En ring af endelig længde siges mere præcist at have endelig venstre-længde. Tilsvarende kunne vi nemlig have defineret højre-længde ved at betragte højre-modulen Λ_d. Kæder i Λ-modulen Λ_s svarer til følger:

$$(0) = I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n = \Lambda$$

af venstre-idealer i Λ, hvorimod kæder i højre-modulen Λ_d svarer til følger af højre-idealer i Λ.

(6.13) EKSEMPEL. Hvis ringen Λ er et skævlegeme, så er Λ_s en simpel Λ-modul ifølge Sætning (5,3). Følgelig har Λ den endelige venstre-længde $\mathrm{long}\Lambda_s = 1$. Tilsvarende er også $\mathrm{long}\Lambda_d = 1$. Man kan vise, at matrixringen $\mathrm{Mat}_n(\Lambda)$, når Λ er et skævlegeme, 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 vektor $a \in A$ med en skalar $\lambda \in \Lambda$ defineres som produktet λa in ringen A. Venstre-idealerne i ringen A er da specielt underrum i vektorrummet A. Hvis vektorrummet A er endelig dimensionalt, så har ringen A altså endelig længde, endda

$$\mathrm{long}\, A_s \leq \dim_L A.$$

Specielt følger det for et legeme L, at enhver delring $A \subseteq \mathrm{Mat}_n(L)$, som indeholder skalar-matricerne $\begin{pmatrix} \lambda & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda \end{pmatrix}$, hvor $\lambda \in \Lambda$, har endelig længde og at

$$\operatorname{long} A_s \leq n^2 \qquad \text{og} \qquad \operatorname{long} A_d \leq n^2.$$

(6.15) Eksempel. Man kan vise, at der for ringen $A := \begin{pmatrix} \mathbf{C} & \mathbf{C} \\ 0 & \mathbf{R} \end{pmatrix}$ bestående at 2×2-matricer $\begin{pmatrix} z & w \\ 0 & t \end{pmatrix}$, hvor $z, w \in \mathbf{C}$ og $t \in \mathbf{R}$, gælder, at

$$\operatorname{long} A_s = 3 \qquad \text{og} \qquad \operatorname{long} A_d = 4.$$

Bemærk, at $\dim_{\mathbf{R}} A = 5$.

For den tilsvarende ring $B =: \begin{pmatrix} \mathbf{C} & \mathbf{C} \\ 0 & \mathbf{Q} \end{pmatrix}$ kan man vise, at $\operatorname{long} B_s = 3$ og at B ikke har endelig højre-længde.

(6.16) Sætning. *Hvis Λ er en ring af endelig længde, så har enhver endeligt frembragt Λ-modul M endelig længde.*

Bevis. Et frembringersystem $(e_1, \dots, e_n)$ for M definerer en surjektiv homomorfi : $\Lambda_s^n \to M$, jfr. Observation (1)(4.13). Følgelig er M isomorf med en kvotient af Λ_s^n. Da Λ_s har endelig længde, har Λ_s^n endelig længde ifølge Korollar (6.9) og så har kvotienten M endelig længde ifølge 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) *Vektorrummet V har endelig længde.*
(2) *Vektorrummet 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 øjensynlig 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 $V_i := \Lambda u_1 + \cdots + \Lambda u_i$, altså

$$V_i = V_{i-1} + \Lambda u_i \qquad \text{for } i = 1, \ldots, r.$$

Kvotienten V_i/V_{i-1} er cyklisk, frembragt af $\boxed{u_i}$, og dermed isomorf med en kvotient af den simple modul Λ. Hvis $\boxed{u_i} = 0$ i kvotienten V_i/V_{i-1}, ville $u_i \in V_{i-1}$ være en linearkombination af vektorerne $u_1, \ldots, u_{i-1}$ i modstrid med, at $(u_1, \ldots, u_r)$ er et minimalt frembringersystem. Følgelig er $\boxed{u_i} \neq 0$, og V_i/V_{i-1} er derfor en simpel modul. Men så er $(*)$ en Jordan–Hölder kæde i V, og derfor 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

$$\dim V = \operatorname{long} V.$$

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 $\mu, \lambda \in R$ og $x \in M$ har vi $\mu_M(\lambda x) = \lambda\mu_M(x)$, idet jo $\mu_M(\lambda x) = \mu(\lambda x) = (\mu\lambda)x = (\lambda\mu)x = \lambda(\mu x) = \lambda\mu_M(x)$

(1.3) For R-moduler M, N er den kommutative gruppe $Hom_R(M, N)$ 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

$$\lambda f : x \mapsto \lambda f(x) \ (= f(\lambda x).$$

Bemærk, at $\lambda f = \lambda_N \circ f = f \circ \lambda_M$.

(1.4) Specielt er for en R-modul M ringen $End_R(M)$ igen en R-modul, og den omfatter delringen bestående af homotetierne. For $f \in End_R(M)$ 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) De R-lineære afbildninger $f : R^p \to R^n$ er netop afbildningerne af formen

$$x \mapsto \alpha x, \quad \text{for } x \in R^p,$$

med en matrix $\alpha \in Mat_{n,p}(R)$. Her fortolkes $\alpha \in R^p$ som en søjle, og de p søjler i matricen α er billederne ved f af den kanoniske basis $\begin{pmatrix} 1 \\ \vdots \\ 0 \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ \vdots \\ 1 \end{pmatrix}$ for R^p.

(1.6) Den i (1.5) beskrevne bijektive afbildning:

$$Hom_R(R^p, R^n) \tilde{\to} Mat_{n,p}(R)$$

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 $\lambda \in R$ annullerer elementerne $e_1, \ldots, e_n$ i modulen M, vil λ også annullere undermodulen $Re_1 + \cdots + Re_n \subseteq M$.

2. Alternerende lineære afbildninger. Determinant.

(2.1) DEFINITION. Lad $N_1, \dots, N_n, M$ være R-moduler. Ved en *multilineær* afbildning

$$\varphi : N_1 \times \cdots \times N_n \to M$$

forstås en afbildning, som er lineær i hver variabel, dvs. opfylder

$$\begin{aligned} \varphi(\dots, x_i' + x_i'', \dots) &= \varphi(\dots, x_i', \dots) + \varphi(\dots, x_i'', \dots) \\ \varphi(\dots, \lambda x_i, \dots) &= \lambda\varphi(\dots, x_i, \dots) \end{aligned}$$

[hvor $(\dots$ og $\dots)$ står for $(x_1, \dots, x_{i-1}$ og $x_{i+1}, \dots, x_n)$] for alle $\lambda \in R$ og $x_i', x_i'', x_i \in N_i$ for $i = 1, \dots, n$ [og $x_j \in N_j$ for $j \neq i$].

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

$$\varphi : N^n \to M \qquad (N^n = \overbrace{N \times \cdots \times N}^{n})$$

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. hvor 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 af skrive de variable på pladserne $\neq i, j$ finder vi

$$\begin{aligned} 0 &= \varphi(x_i + x_j, x_i + x_j) = \varphi(x_i, x_i) + \varphi(x_i, x_j) + \varphi(x_j, x_i) + \varphi(x_j, x_j) \\ &= \varphi(x_i, x_j) + \varphi(x_j, x_i) \ , \end{aligned}$$

og det er netop påstanden ♠

BEMÆRKNING. En n-lineær afbildning $\varphi : N^n \to M$, som opfylder ligningen ovenfor, kaldes *anti-symmetrisk*. 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 hvis der i sættet $(x_1, \ldots, x_n)$ gælder, at $x_i = x_j =: x$ for et $i \neq j$, 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

$$\varphi(x_1, \ldots, x_i + \sum_{j \neq i} \lambda_j x_j \, , \ldots, x_n) = \varphi(x_1, \ldots, x_i, \ldots, x_n) \; .$$

["Værdien ændres ikke, dersom man til én af de variable adderer en linearkombination af de øvrige".]

(2.5) Motivation. Lad $\varphi : N^n \to M$ være en alternerende n-lineær afbildning og lad $x = (x_1, \ldots, x_n) \in N^n$. Lad $y = (y_1, \ldots, y_n)$ være endnu et sæt og antag, at hvert y_i er en linearkombination af $x_1, \ldots, x_n$. Af multi-lineariteten følger da, at φ's værdi på $y = (y_1, \ldots, y_n)$ kan udtrykkes ved φ's værdi på $x = (x_1, \ldots, x_n)$ og sæt, der fremgår heraf ved permutation. Lidt mere præcist:

Skriv for $j = 1, \ldots, n$ elementet y_j som linearkombination af $x_1, \ldots, x_n$ og anbring koefficienterne som j-te søjle i $n \times n$ matricen α. Vi har altså

$$y_j = \sum_{i=1}^{n} \alpha_{ij} x_i \quad \text{for } j = 1, \ldots, n,$$

dvs., med oplagt matrixmultiplikation,

$$(y_1, \ldots, y_n) = (x_1, \ldots, x_n) \begin{pmatrix} \alpha_{11} & \ldots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{n1} & \ldots & \alpha_{nn} \end{pmatrix} ,$$

eller kort:

$$y = x\alpha \quad \text{med } \alpha \in \; Mat_n(R).$$

Heraf får vi:

$$\varphi(y) = \varphi(y_1, \ldots, y_n) = \varphi(\sum_{\sigma_1=1}^{n} \alpha_{\sigma_1 1} x_{\sigma_1}, \ldots, \sum_{\sigma_n=1}^{n} \alpha_{\sigma_n n} x_{\sigma_n}),$$

hvor vi har brugt forskellige summationsindices i de n summer. Multilineariteten giver

$$\varphi(y) = \sum_{\sigma_1=1}^{n} \alpha_{\sigma_1 1} \sum_{\sigma_2=1}^{n} \alpha_{\sigma_2 2} \cdots \sum_{\sigma_n=1}^{n} \alpha_{\sigma_n n}\, \varphi(x_{\sigma_1}, \ldots, x_{\sigma_n})\,,$$

eller, som multibel sum,

$$\varphi(y) = \sum_{(\sigma_1, \ldots, \sigma_n)} \alpha_{\sigma_1 1} \cdots \alpha_{\sigma_n n}\, \varphi(x_{\sigma_1}, \ldots, x_{\sigma_n})\,,$$

hvor der summeres over alle sæt $\sigma_1, \ldots, \sigma_n$ af tal med $1 \leq \sigma_k \leq n$ for $k = 1, \ldots, n$.

Et sådant sæt $(\sigma_1, \ldots, \sigma_n)$ af tal kan opfattes som en afbildning σ af mængden $\{1, \ldots, n\}$ ind i sig selv. Da φ er alternerende, kan $\varphi(x_{\sigma_1}, \ldots, x_{\sigma_n})$ kun være $\neq 0$, når σ_k'erne er forskellige, dvs. når $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ er en injektiv (og dermed bijektiv) afbildning. Disse afbildninger er netop permutationerne $\sigma \in S_n$, så vi får

$$\varphi(y) = \sum_{\sigma \in S_n} \alpha_{\sigma_1 1} \cdots \alpha_{\sigma_n n}\, \varphi(x_{\sigma_1}, \ldots, x_{\sigma_n})\,.$$

Af Sætning (2.3) fås endelig:

$$\varphi(y) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \alpha_{\sigma_1 1} \ldots \alpha_{\sigma_n n} \varphi(x_1, \ldots, x_n)\ .$$

(2.6) Definition. Lad $\alpha \in \ Mat_n(R)$ være en kvadratisk matrix. Ved *determinanten* 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 $x = (x_1, \ldots, x_n) \in N^n$ og lad $\alpha \in \ Mat_n(R)$. Da er*

$$\varphi(x\alpha) = \det(\alpha)\varphi(x)\ .$$

Bevis. Dette var resultatet i 2.5 ♠

Bemærkning. Det 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

$$\det :\ Mat_n(R) \to R\ .$$

Forskellige værdier af n giver naturligvis forskellige afbildninger, men det fører sædvanligvis ikke til misforståelser, at lade det betegne en vilkårlig given af disse afbildninger.

tom side 6 tilføjet i 2011

3. Determinantsætninger.

(3.1) Sætning. *For den transponerede matrix α^t til en matrix $\alpha \in Mat_n(R)$ gælder:*

$$\det(\alpha^t) = \det(\alpha).$$

Bevis. Den transponerede matrix α^t er bestemt ved $\alpha^t_{ij} = \alpha_{ji}$, så ifølge definitionen er

$$\det(\alpha^t) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \alpha_{1\sigma_1} \cdots \alpha_{n\sigma_n}$$

Når σ gennemløber gruppen S_n vil også σ^{-1} gennemløbe S_n, og da $\operatorname{sign}(\sigma^{-1}) = \operatorname{sign}(\sigma)$, får vi

$$\det(\alpha^t) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \alpha_{1\sigma^{-1}(1)} \cdots \alpha_{n\sigma^{-1}(n)}\,.$$

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 produktet er

$$\alpha_{1\sigma^{-1}(1)} \cdots \alpha_{n\sigma^{-1}(n)} = \alpha_{\sigma(1)1} \cdots \alpha_{\sigma(n)n} \ (= \alpha_{\sigma_1 1} \cdots \alpha_{\sigma_n n})\,,$$

og så er øjensynlig

$$\det(\alpha^t) = \det(\alpha) \spadesuit$$

(3.2) Sætning. *Determinanten af en kvadratisk blokmatrix*

$$\alpha = \begin{pmatrix} \beta & \gamma \\ 0 & \delta \end{pmatrix},$$

hvor $\beta \in Mat_p(R)$ og $\delta \in Mat_q(R)$ er kvadratiske matricer og $\gamma \in Mat_{p,q}(R)$ og 0 betegner nul-matricen $0 \in Mat_{q,p}(R)$, er:

$$\det \begin{pmatrix} \beta & \gamma \\ 0 & \delta \end{pmatrix} = \det(\beta) \det(\delta)$$

Bevis. Vi klassedeler mængden $\{1, \ldots, n\}$, hvor $n := p + q$, i de 2 delmængder $P := \{1, \ldots, p\}$ og $Q := \{p+1, \ldots, p+q\}$.

I summen

$$\det(\alpha) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \alpha_{\sigma_1 1} \cdots \alpha_{\sigma_n n}$$

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

$$\operatorname{sign}(\sigma) \alpha_{\sigma_1 1} \cdots \alpha_{\sigma_n n}$$

indeholde faktoren $\alpha_{\sigma_j j}$, som er $= 0$ ifølge forudsætningen om at α er en blokmatrix af den angivne form.

Permutationerne $\sigma \in S_n$ med $\sigma(P) \subseteq P$ må opfylde, at $\sigma(P) = P$ og $\sigma(Q) = Q$ [hvorfor?]. 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 af $\{1, \ldots, q\}$, dvs. $\sigma'' \in S_q$. Med disse indentifikationer er $\operatorname{sign}(\sigma) = \operatorname{sign}(\sigma') \operatorname{sign}(\sigma'')$ og for det tilsvarende led i summen får vi:

$$\operatorname{sign}(\sigma)\alpha_{\sigma_1 1} \cdots \alpha_{\sigma_p p} \cdots \alpha_{\sigma_n n} = \operatorname{sign}(\sigma')\beta_{\sigma'_1 1} \cdots \beta_{\sigma'_p p} \cdot \operatorname{sign}(\sigma'')\delta_{\sigma''_1 1} \cdots \delta_{\sigma''_q q}\,.$$

Og så følger påstanden ♠

(3.3) Korollar. *Determinanten af en kvadratisk "øvre" blokmatrix*

$$\begin{pmatrix} \beta_1 & ? & & ? \\ 0 & \beta_2 & & ? \\ & & \ddots & \\ 0 & 0 & & \beta_s \end{pmatrix}$$

i $Mat_n(R)$ med kvadratiske matricer $\beta_1, \ldots, \beta_s$ langs diagonalen er:

$$\det \begin{pmatrix} \beta_1 & ? & & ? \\ 0 & \beta_2 & & ? \\ & & \ddots & \\ 0 & 0 & & \beta_s \end{pmatrix} = \det(\beta_1) \cdots \det(\beta_s).$$

Bevis. Følger umiddelbart ved induktion efter s ♠

Bemærkning. Af Sætning (3.1) fås nu et tilsvarende resultat om "nedre" blokmatricer.

Korollar. *Determinanten af en øvre trekantsmatrix i $Mat_n(R)$ med elementer $\lambda_1, \ldots, \lambda_n$ i diagonalen er:*

$$\det \begin{pmatrix} \lambda_1 & ? & & ? \\ 0 & \lambda_2 & & ? \\ & & \ddots & \\ 0 & 0 & & \lambda_n \end{pmatrix} = \lambda_1 \cdots \lambda_n.$$

Determinanten af en diagonalmatrix i $Mat_n(R)$ med elementer $\lambda_1, \ldots, \lambda_n$ i diagonalen er:

$$\det \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix} = \lambda_1 \cdots \lambda_n.$$

Determinanten af enhedsmatricen i $Mat_n(R)$ er:

$$\det \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} = 1 \,.$$

Bevis. ♡

(3.4) En matrix $\alpha \in Mat_n(R)$ kan opfattes som et n-sæt $\alpha = (\alpha_1, \ldots, \alpha_n)$ bestående af matricens n-søjler (hvor altså hver søjle α_i tilhører R^n). Determinanten kan derfor 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 fast $k = 1, \ldots, n$ vise, at afbildningen

$$x \mapsto \det(\alpha_1, \ldots, x, \ldots, \alpha_n) \quad \text{for} \quad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in R^n$$

(hvor x er placeret som den k-te søjle og de øvrige søjler $\alpha_j \in R^n$ for $j \neq k$ er konstante) er lineær afbildning : $R^n \to R$.

Vi har

$$\det(\alpha_1, \ldots, x, \ldots, \alpha_n) = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \alpha_{\sigma_1 1} \cdots x_{\sigma_k} \cdots \alpha_{\sigma_n n} \,.$$

Summerer vi her for hvert $i = 1, \ldots, n$ de led, i hvilke faktoren x_i forekommer, dvs. led svarende til permutationer σ med $\sigma_k = i$, får resultatet formen $A_i x_i$, hvor $A_i \in R$ kun afhænger af søjlerne α_j for $j \neq k$. Følgelig er

$$\det(\alpha_1, \ldots, x, \ldots, \alpha_n) = A_1 x_1 + \cdots + A_n x_n,$$

Heraf fremgår lineariteten.

For at vise, at afbildningen det er alternerende, betragtes determinanten

$$\Delta := \det(\alpha_1, \ldots, x, \ldots, x, \ldots, \alpha_n),$$

hvor $x \in R^n$ er placeret som k-te og l-te søjle ($k < l$). Vi har

$$\Delta = \sum_{\sigma \in S_n} \operatorname{sign}(\sigma) \alpha_{\sigma_1 1} \cdots x_{\sigma_k} \cdots x_{\sigma_l} \cdots \alpha_{\sigma_n n} = \sum_{\sigma} \lambda_\sigma \,,$$

hvor $\lambda_\sigma \in R$ betegner leddet svarende til $\sigma \in S_n$. Er $S' \subseteq S_n$ delmængden bestående af permutationer σ med $\sigma_k < \sigma_l$, så består komplementærmængden $S'' := S_n \setminus S'$ af permutationer $\tau \in S_n$ med $\tau_k > \tau_l$. Idet (k,l) betegner transpositionen, der ombytter k og l, ses det, at S'' består at permutationerne

$$\sigma \circ (k,l), \quad \text{hvor } \sigma \in S'.$$

Vi kan følgelig skrive

$$\begin{aligned}\Delta = \sum_{\sigma\in S_n} \lambda_\sigma &= \sum_{\sigma\in S'} \lambda_\sigma + \sum_{\tau\in S''} \lambda_\tau = \sum_{\sigma\in S'} \lambda_\sigma + \sum_{\sigma\in S'} \lambda_{\sigma\circ(k,l)} \\ &= \sum_{\sigma\in S'} \left(\lambda_\sigma + \lambda_{\sigma\circ(k,l)}\right).\end{aligned}$$

Her er

$$\begin{aligned}\lambda_{\sigma\circ(k,l)} &= \operatorname{sign}(\sigma\circ(k,l))\,\alpha_{\sigma_1 1}\cdots x_{\sigma_l}\cdots x_{\sigma_k}\cdots\alpha_{\sigma_n n} \\ &= -\operatorname{sign}(\sigma)\alpha_{\sigma_1 1}\cdots x_{\sigma_k}\cdots x_{\sigma_l}\cdots\alpha_{\sigma_n n} \\ &= -\lambda_\sigma\end{aligned}$$

og følgelig er $\Delta = 0$. Altså er afbildningen det alternerende ♠

(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 $\alpha, \beta \in Mat_n(R)$ gælder:*

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

Bevis. Opfattes β som sættet $\beta = (\beta_1, \ldots, \beta_n)$ bestående af de n søjler i β, kan vi med notationen fra 2.5 betragte sættet

$$(\gamma_1, \ldots, \gamma_n) := (\beta_1, \ldots, \beta_n)\alpha.$$

Opfattes sættet som matrix, $\gamma := (\gamma_1, \ldots, \gamma_n)$, gælder øjensynlig, at γ er matrixproduktet $\gamma = \beta\alpha$. Påstanden følger derfor af Sætning (2.6) ♠

4. Udviklinger. Cramer's 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

$$(\alpha_1, \ldots, x, \ldots, \alpha_n)$$

betegne den matrix, der fremgår af α ved at erstatte den k-te søjle med søjlen x. Som nævnt i (3.4) har vi da:

$$(*) \qquad \det(\alpha_1, \ldots, x, \ldots, \alpha_n) = A_{k1}x_1 + \cdots + A_{kn}x_n \quad [x \text{ som } k\text{-te søjle}],$$

hvor koefficenterne $A_{ki} \in R$ kun afhænger af matricen α (og endda kun af søjlerne α_j, hvor $j \neq k$).

Definition. Elementet $A_{ki} \in R$ kaldes *komplementet* til den (i,k)-te plads i matricen α.

(4.2) Idet δ_i er den i-te søjle i enhedsmatricen i $Mat_n(R)$, dvs. δ_i har et-elementet $1 \in R$ som i-te koordinat og nul-elementet $0 \in R$ som de øvrige koordinater, får vi, ved at indsætte $x = \delta_i$ i ligningen $(*)$ ovenfor, at

$$\det(\alpha_1, \ldots, \delta_i, \ldots, \alpha_n) = A_{ki} \quad [\delta_i \text{ som } k\text{-te søjle}]$$

for $i = 1, \ldots, n$. 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 op som første række, får vi en matrix β, der tilsvarende har determinant

$$\det\beta = (-1)^{i-1}(-1)^{k-1}A_{ki} = (-1)^{i+k}A_{ki}\,.$$

Matricen β har imidlertid formen

$$\beta = \begin{pmatrix} 1 & ? & \ldots & ? \\ 0 & & & \\ \vdots & & \alpha_{\hat{\imath}\hat{k}} & \\ 0 & & & \end{pmatrix},$$

hvor $\alpha_{\hat{\imath}\hat{k}}$ 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 $\det\beta = \det(\alpha_{\hat{\imath}\hat{k}})$, og dermed følgende:

SÆTNING. *Komplementet A_{ki} til den (i,k)-te plads i matricen α er*

$$A_{ki} = (-1)^{k+i} \det(\alpha_{\hat{\imath}\hat{k}}),$$

hvor $\alpha_{\hat{\imath}\hat{k}}$ betegner den $(n-1)\times(n-1)$-matrix, der fremgår af α ved at slette i-te række og k-te søjle.

BEMÆRKNING. Indsættes ovenstående udtryk i ligningen (4.1)(∗) får vi formlen

$$\det(\alpha_1,\ldots,x,\ldots,\alpha_n) = \sum_{i=1}^{n}(-1)^{k+i}\det(\alpha_{\hat{\imath}\hat{k}})x_i \quad [x \text{ som } k\text{-te søjle}],$$

der også kaldes *udvikling* af determinanten efter k-te søjle.

(4.3) NOTATION. I det følgende er det bekvemt med en klassisk notation, at indicere rækkerne i en matrix ved at anbringe index som en exponent. For en matrix α i $Mat_{pn}(R)$ betegner vi således med α^i den i-te række for $i = 1,\ldots,p$ og med α_j den j-te søjle for $j = 1,\ldots,n$. Som konsekvens heraf kan vi for elementet på den (i,j)-te plads i matricen α skrive $\alpha_{ij} = \alpha^i_j$ (såfremt dette ikke kan forveksles med potensopløftning).

Lad $\alpha \in Mat_n(R)$ være en kvadratisk matrix. Idet vi altså med $\alpha^1,\ldots,\alpha^n$ betegner de n rækker i α, får vi af Sætning (3.1), at der for alle $y \in R^n$ gælder:

$$\det\begin{pmatrix}\alpha^1\\ \vdots\\ y\\ \vdots\\ \alpha^n\end{pmatrix} = B_{k1}y_1 + \cdots + B_{kn}y_n \quad [y \text{ som } k\text{-te række}],$$

hvor B_{ki} er komplementet til den (i,k)-te plads i matricen α^t. Af Sætning (4.2) og Sætning (3.1) følger, at $B_{ki} = A_{ik}$. Vi har derfor

$$(*)^t \qquad \det\begin{pmatrix}\alpha^1\\ \vdots\\ y\\ \vdots\\ \alpha^n\end{pmatrix} = y_1A_{1k} + \cdots + y_nA_{nk} \quad [y \text{ som } k\text{-te række}]$$

og dermed en tilsvarende *rækkeudvikling* af determinanten efter k-te række.

(4.4) DEFINITION. Lad α være en matrix i $Mat_n(R)$. Den matrix i $Mat_n(R)$, der på den (k,i)-te plads har komplementet 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

$$\tilde{\alpha}_{ij} = A_{ij} = (-1)^{i+j}\det(\alpha_{\hat{\imath}\hat{\jmath}}).$$

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 søjler i α.

Ved indsættelse i (4.1)$(*)$ og (4.3)$(*)^t$ fås umiddelbart følgende:

FORMLER. *For en matrix $\alpha \in Mat_n(R)$ og $k = 1, \ldots, n$ gælder:*

$$(*) \qquad \det(\alpha_1, \ldots, x, \ldots, \alpha_n) = \tilde{\alpha}^k x,$$

hvor $x \in R^n$ er placeret som k-te søjle, og

$$(*)^t \qquad \det \begin{pmatrix} \alpha^1 \\ \vdots \\ y \\ \vdots \\ \alpha^n \end{pmatrix} = y\tilde{\alpha}_k,$$

hvor $y \in R^n$ er placeret som k-te række.

(4.5) SÆTNING. *For en matrix $\alpha \in Mat_n(R)$ gælder:*

$$\alpha\tilde{\alpha} = \tilde{\alpha}\alpha = \det(\alpha)1,$$

hvor $\det(\alpha)1$ *betegner den diagonalmatrix, der har elementet* $\det(\alpha) \in R$ *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

$$\tilde{\alpha}^i\alpha_j = \det(\alpha_1, \ldots, \alpha_j, \ldots, \alpha_n),$$

hvor søjlen α_j i matricen på højre side er placeret som i-te søjle og de øvrige søjler er søjlerne i α. Hvis $i \neq j$, så har denne matrix 2 ens søjler og den har følgelig determinant 0. Er derimod $i = j$, så er matricen $= \alpha$, og dens determinant er altså $\det(\alpha)$. Vi har følgelig

$$\tilde{\alpha}^i\alpha_j = \det(\alpha)\delta_{ij} \quad \text{hvor } \delta_{ij} = \begin{cases} 0 & \text{hvis } i \neq j \\ 1 & \text{hvis } i = j, \end{cases}$$

og det er netop indholdet af matrixligningen $\tilde{\alpha}\alpha = \det(\alpha)1$. Tilsvarende følger ligningen $\alpha\tilde{\alpha} = \det(\alpha)1$ af Formel (4.4)$(*)^t$ ♠

(4.6) KOROLLAR. *En matrix $\alpha \in Mat_n(R)$ er invertibel i ringen $Mat_n(R)$, 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. **"hvis":** 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 $\alpha^{-1} = \beta$.
"kun hvis": Er α invertibel i $Mat_n(R)$, så findes en matrix $\beta \in Mat_n(R)$ 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 komentative ring R (med $\det(\alpha)^{-1} = \det(\beta)$) ♠

Tilføjelse. En matrix $\alpha \in Mat_n(R)$ er invertibel, hvis der findes en matrix $\beta \in Mat_n(R)$, 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, så har ligningen

$$\alpha x = b,$$

hvor $a, x \in R^n$ opfattes som søjler, for hver værdi af $b \in R^n$ 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 $\alpha^{-1} = \det(\alpha)^{-1}\tilde{\alpha}$, så løsningen er $x = \det(\alpha)^{-1}\tilde{\alpha}b$. Løsningens koordinater er derfor

$$x_i = \det(\alpha)^{-1}\tilde{\alpha}^i b \quad \text{for } i = 1, \ldots, n.$$

Indsættelse i Formel 4.4(∗) giver $\tilde{\alpha}^i b = \det(\alpha_1, \ldots, b, \ldots, \alpha_n)$ og dermed

Cramer's Formel. *Lad α være en matrix i $Mat_n(R)$ med invertibel determinant. For hver søjle $b \in R^n$ er den entydigt bestemte løsning $x \in R^n$ til ligningen $\alpha x = b$ bestemt ved*

$$x_i = \frac{\det(\alpha_1, \ldots, b\ , \ldots, \alpha_n)}{\det(\alpha_1, \ldots, \alpha_i, \ldots, \alpha_n)}\ ,$$

hvor søjlen b er placeret som i-te søjle for $i = 1, \ldots, n$ ♠

(4.8) Definition. Gruppen af invertible elementer i ringen $Mat_n(R)$ kaldes den *generelle lineære gruppe* (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 herfor, der består af de matricer, der har determinant 1, er altså en normal undergruppe i $GL_n(R)$. Den kaldes den *specielle lineære gruppe* (over R) og den betegnes

$$SL_n(R) \subseteq GL_n(R).$$

MODULER OVER HOVEDIDEALOMRÅDER

I det følgende betegner R et hovedidealområde. [Et hovedidealområde hedder på engelsk 'Primcipal Ideal Domain (P.I.D)']. 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

$$\operatorname{rg} M \leq \dim M.$$

For en fri modul F gælder, at $\operatorname{rg} F = \dim F$ 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* $\operatorname{rg} N \leq \operatorname{rg} F$.

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 undermodul $N \subseteq R$ er altså et ideal i R. Da R er et hovedidealområde, er N af formen $N = Ra$, hvor $a \in R$. 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 fri moduler af rang n.

Vi kan antage, at $F = R^{n+1}$, og vi betragter den R-lineære projektion fra R^{n+1} til R^n bestemt ved

$$\begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Kernen K for denne projektion består af alle $(n+1)$-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 ved projektionen 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 $= \operatorname{rg} N_0 + \operatorname{rg} \bar{N} \leq 1 + n$ ♠

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 $(e_1, \cdots, e_d)$ 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

$$\dim N \leq n \leq d \text{ ♠}$$

2. Torsionsfri moduler.

(2.1) Definition. Et frit element x i en R-modul M kaldes også *torsionsfrit*. Som bekendt betyder det, at der for $\lambda \neq 0$ i R gælder, at $\lambda x \neq 0$. 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 $e_1, \ldots, e_n$ 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) for $i = 1, \ldots, n$, og så er $x = 0$.

Eksempel. Ethvert vektorrum V over et legeme L af karakteristik 0 (dvs. $L \supseteq \mathbf{Z}$) er torsionsfrit som $\mathbf{Z}$-modul, thi af $nv = 0$, hvor $n \in \mathbf{Z} \setminus \{0\}$, følger, at $v = \frac{1}{n}(nv) = 0$, 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 $e_1, \ldots, e_d$ for M med det mindst mulige antal elementer, dvs. $d = \dim M$, er en fri basis. Lad $M' \subseteq M$ være undermodulen frembragt af $e_1, \ldots, e_{d-1}$, 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 $e_1, \ldots, e_{d-1}$ er en fri basis for M'. Hvis $e_1, \ldots, e_d$ ikke var et frit system, ville der findes en egentlig lineær relation:

$$(*) \quad \lambda_1 e_1 + \cdots + \lambda_{d-1} + \lambda_d e_d = 0, \quad \text{hvor } \lambda_1, \ldots, \lambda_{d-1}, \lambda_d \in R.$$

Her gælder om koefficienten λ_d, at

$$\lambda_d \neq 0,$$

thi ellers ville $(*)$ være en en egentlig relation mellem $e_1, \ldots, e_{d-1}$.

Af $(*)$ følger, at $\lambda_d e_d \in M'$. Da vi trivielt har $\lambda_d e_i \in M'$ for $i = 1, \ldots, d-1$, 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 $\dim M = d$ ♠

BEMÆRKNING. 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 let, 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 *torsionselement*, hvis det ikke er torsionsfrit, dvs. hvis der findes $\mu \in R$ med $\mu \neq 0$, så at $\mu x = 0$. Mængden af torsionselementer i M kaldes *torsionsundermodulen* i M og betegnes M_{tor}. Modulen M kaldes en *torsionsmodul*, hvis $M_{\text{tor}} = M$.

OBSERVATION. Delmængden $M_{\text{tor}} \subseteq M$ af torsionselementer er en undermodul, thi $0 \in M_{\text{tor}}$, da $1 \cdot 0 = 0$, og er $x \in M_{\text{tor}}$ med $\mu x = 0$, hvor $\mu \in R \setminus \{0\}$, så er også $\mu(\lambda x) = \lambda \mu x = 0$, og dermed $\lambda x \in M_{\text{tor}}$ for $\lambda \in R$, og er også $y \in M_{\text{tor}}$ med $\gamma y = 0$, hvor $\gamma \in R \setminus \{0\}$, så er $\mu\gamma(x+y) = \gamma\mu x + \mu\gamma y = 0$, og her er $\mu\gamma \neq 0$, og altså er $x + y \in M_{\text{tor}}$.

(2.5) LEMMA. *Lad M være en R-modul. Da er kvotienten M/M_{tor} en torsionsfri R-modul.*

Bevis. Lad $X \in M/M_{\text{tor}}$, 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}:

$$0 = \lambda X = \lambda \boxed{x} = \boxed{\lambda x},$$

og følgelig er $\lambda x \in M_{\text{tor}}$ 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 $x \in M_{\text{tor}}$, og så er $X = \boxed{x} = 0$ 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 Lemma'et, er den fri ifølge Sætning (2.3). Da kvotienten er fri, følger det som bekendt, at undermodulen M_{tor} er direkte sumand i M. Et komplement K til M_{tor} afbildes ved den kanoniske homomorfi $: M \to M/M_{\text{tor}}$ isomorft på M/M_{tor}. Følgelig er K fri af rang $\operatorname{rg} K = \operatorname{rg}(M/M_{\text{tor}})$. Det er klart, at der for undermodulen $K \subseteq M$ gælder, at $\operatorname{rg} K \leq \operatorname{rg} M$.

Omvendt vil ethvert frit system i M med p elementer frembringe en fri undermodul $F \subseteq M$ af rang p. Da F er torsionsfri ifølge Observation (2.2)(2), er $F \cap M_{\text{tor}} = (0)$, så ved den kanoniske homomorfi $M \to M/M_{\text{tor}}$ afbildes F isomorft på en undermodul i M/M_{tor}. Men så er $p = \operatorname{rg} F \leq \operatorname{rg} M/M_{\text{tor}} = \operatorname{rg} K$, og følgelig er $\operatorname{rg} M \leq \operatorname{rg} K$ ♠

tom side 5 tilføjet i 2011

3. Matricer over hovedidealområder.

(3.1) Lad $\alpha \in \mathrm{Mat}_{n,p}(R)$ være en matrix med de p søjler $\alpha_1, \ldots, \alpha_p$. At omforme α med en *elementær søjleoperation* betyder, at man til en af søjlerne i α adderer et multiplum af en af de øvrige, altså at man for passende $j \neq k$ erstatter j-te søjle α_j med $\alpha_j + \lambda\alpha_k$, hvor $\lambda \in R$.

Eksempel. Sucessive 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) permutere søjlerne, når samtidig én af søjlerne multipliceres med permutationens fortegn, og
(2) multiplicere en søjle med et invertibelt element $\varepsilon \in R$ (specielt med -1), når samtidig en anden søjle multipliceres med ε^{-1},

thi (1) 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 *elementære rækkeoperationer.*

(3.2) Idet $\delta_1, \ldots, \delta_p \in R^p$ betegner de p søjler i enhedsmatricen $1 = \begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$ i $\mathrm{Mat}_p(R)$ har vi:

$$(\alpha_1, \ldots, \alpha_j + \lambda\alpha_k, \ldots, \alpha_p) = (\alpha_1, \ldots, \alpha_p)(\delta_1, \ldots, \delta_j + \lambda\delta_k, \ldots, \delta_p).$$

Den elementære søjleoperation beskrevet i (3.1) kan altså udføres ved at multiplicere matricen $\alpha \in \mathrm{Mat}_{n,p}(R)$ fra højre med matricen:

$$(\delta_1, \ldots, \delta_j + \lambda\delta_k, \ldots, \delta_p) = \begin{pmatrix} 1 & & & \\ & \ddots & \lambda & \\ & & \ddots & \\ & & & 1 \end{pmatrix},$$

der for $j, k \in \{1, \ldots, p\}$ med $j \neq k$ og $\lambda \in R$ har λ på den (i, j)-te plads og ellers 0'er uden for diagonalen. En sådan matrix siges at være en *elementær* 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 $\alpha \in \mathrm{Mat}_{n,p}(R)$ kan altså udføres ved at multiplicere α fra højre med et endeligt produkt af elementære matricer i $\mathrm{Mat}_p(R)$. Det fremgår, at mængden af sådanne endelige produkter af elementære matricer udgør en undergruppe i $GL_p(R)$. Vi kalder den den *elementære* 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 $\varepsilon \in R^*$)

$$\begin{pmatrix} 1 & \varepsilon \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1-\varepsilon^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \varepsilon - 1 & 1 \end{pmatrix} = \begin{pmatrix} \varepsilon & 0 \\ 0 & \varepsilon^{-1} \end{pmatrix}.$$

Matricerne på højresiderne tilhører altså gruppen $E_2(R)$.

Bemærkning. Tilsvarende kan naturligvis elementære rækkeoperationer på matricen $\alpha \in \mathrm{Mat}_{n,p}(R)$ 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 *specielle søjleoperation*, der består i for givne

$$\lambda_1, \lambda_2, \mu_1, \mu_2 \in R \quad \text{med } \lambda_1\mu_2 - \lambda_2\mu_1 = 1$$

at erstatte de to første søjler α_1 og α_2 i matricen α med de to søjler $\lambda_1\alpha_1 + \lambda_2\alpha_2$ og $\mu_1\alpha_1 + \mu_2\alpha_2$.

Denne specielle søjleoperation udføres øjensynlig ved at multiplicere $n \times p$-matricen α fra højre med den *specielle* $p \times p$-matrix:

$$\begin{pmatrix} \lambda_1 & \mu_1 & & & \\ \lambda_2 & \mu_2 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \qquad \text{hvor } \lambda_1\mu_2 - \lambda_2\mu_1 = 1.$$

OBSERVATION. De specielle søjleoperationer berører kun de to første søjler i matricen α. Da vi ved hjælp af elementære søjleoperationer kan permutere søjlerne, jfr. Observation (3.1)(1), kan vi herved lave operationer svarende til de specielle på vilkårlige to givne søjler i α.

BEMÆRKNING. Tilsvarende kan en *speciel rækkeoperation* 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 specielle lineære gruppe (bestående af $p \times p$-matricer med determinant 1).

De specielle 2×2-matricer er ifølge definitionen 2×2-matricerne $\left(\begin{smallmatrix} \lambda_1 & \mu_1 \\ \lambda_2 & \mu_2 \end{smallmatrix}\right)$ med determinant $\lambda_1\mu_2 - \lambda_1\mu_1 = 1$. Heraf følger, at enhver speciel matrix har determinant 1. Videre ses, at den "inverse" til en speciel operation igen er en speciel operation svarende til matricen:

$$\begin{pmatrix} \lambda_1 & \mu_1 \\ \lambda_2 & \mu_2 \end{pmatrix}^{-1} = \begin{pmatrix} \mu_1 & -\mu_1 \\ -\lambda_2 & \lambda_1 \end{pmatrix}.$$

Specielt følger det, at elementære og specielle 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:

$$\begin{aligned} \delta = \lambda_1\alpha_1 + \lambda_2\alpha_2 \qquad & \text{med } \lambda_1, \lambda_2 \in R \text{ og} \\ \alpha_1 = \mu_1\delta \quad \text{og} \quad \alpha_2 = \mu_2\delta \qquad & \text{med } \mu_1, \mu_2 \in R. \end{aligned}$$

Vi kan antage $\delta \neq 0$, og får derfor:

$$1 = \lambda_1\mu_1 + \lambda_2\mu_2, \quad \text{og} \quad \mu_2\alpha_1 = \mu_1\alpha_2,$$

og så er matricen

$$\begin{pmatrix} \lambda_1 & -\mu_2 \\ \lambda_2 & \mu_1 \end{pmatrix} \text{ speciel og } (\alpha_1, \alpha_2) \begin{pmatrix} \lambda_1 & -\mu_2 \\ \lambda_2 & \mu_1 \end{pmatrix} = (\delta, 0) \spadesuit$$

(3.6) Elementardivisorsætningen. *Lad R være et hovedidealområde. Da kan enhver matrix $\alpha \in \mathrm{Mat}_{n,p}(R)$ 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 $\delta_1 \mid \delta_2, \ldots, \delta_{r-1} \mid \delta_r$ og $\delta_r \neq 0$ (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 (3.5) 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 $\alpha_{11}, \alpha'_{11}, \alpha''_{11}, \ldots, \alpha^{(m)}_{11}, \ldots$, hvori $\alpha^{(m)}_{11}$ er ægte divisor i $\alpha^{(m-1)}_{11}$. 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 β_{i1} i første søjle er multipla af β_{11}. Subtraheres et passende multiplum af første søjle fra den j-te søjle for $j = 2, \ldots, p$, kan vi opnå, at $\beta_{1j} = 0$ for $j = 2, \ldots, p$ og tilsvarende, at $\beta_{i1} = 0$ for $i = 2, \ldots, n$.
2. skridt: Hvis der i den omformede matrix β findes et element β_{ij}, hvor $i \geq 2$ og $j \geq 2$, 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, som opfylder, at $\delta_{11} \neq 0$, $\delta_{1j} = 0$, $\delta_{i1} = 0$ og δ_{ij} er delelig med δ_{11} for $i, j \geq 2$.
3. skridt: Den omformede matrix har nu formen:

$$\delta = \begin{pmatrix} \delta_1 & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & \delta_1\alpha' & \\ 0 & & & \end{pmatrix},$$

hvor $\delta_1 = \delta_{11} \neq 0$ og hvor α' er en $(n-1) \times (p-1)$-matrix. Et oplagt induktionsargument anvendt på matricen α' 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:

$$\begin{pmatrix} \delta_1 & & \\ & \ddots & \\ & & \delta_r \\ & & \end{pmatrix}$$

Da omformningen ikke ændrer determinanten, har denne matrix determinant 1. Følgelig er $r = p$ 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 $\nu : R \to \mathbf{Z}$, som er nedad begrænset og opfylder, at der for alle $\alpha, \beta \in R$ med $\beta \neq 0$ findes $\lambda \in R$ så at

$$\nu(\alpha - \lambda\beta) < \nu(\beta),$$

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 $\nu : R \to \mathbf{Z}$ med egenskaberne ovenfor. Da kan enhver matrix $\alpha \in \mathrm{Mat}_{n,p}(R)$ ved hjælp af elementære (række- og søjle-) operationer omformes til en matrix:*

$$\begin{pmatrix} \delta_1 & & \\ & \ddots & \\ & & \delta_r \\ & & \end{pmatrix},$$

hvor $\delta_1 \,|\, \delta_2, \ldots, \delta_{r-1} \,|\, \delta_r$ og $\delta_r \neq 0$

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 α i $SL_p(R)$ 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 $\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)$ og $\left(\begin{smallmatrix} 1 & 0 \\ \lambda & 1 \end{smallmatrix}\right)$, hvor $\lambda \in R$. 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 $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ og $\left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)$, hvor $\lambda \in R$.

EKSEMPEL. For $R = \mathbf{Z}$ har funktionen $q \mapsto |q|$ som bekendt den i (3.8) nævnte egenskab. Sætningen og Korollaret gælder altså for matricer med hele koefficienter. Da vi yderligere har:

$$\begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^q, \text{ for } q \in \mathbf{Z},$$

følger det, at gruppen $SL_2(\mathbf{Z})$ 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.

(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 $(v_1, \ldots, v_n)$ for F og skalarer $\delta_1 \mid \delta_2, \ldots, \delta_{p-1} \mid \delta_p$, med $p \leq n$, så at $(\delta_1 v_1, \ldots, \delta_p v_p)$ er en fri basis for N.*

Bevis. Lad $(u_1, \ldots, u_n)$ 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 $(w_1, \ldots, w_p)$ for N. Da $(u_1, \ldots, u_n)$ er en basis for F, findes en relation:

$$(w_1, \ldots, w_p) = (u_1, \ldots, u_n)\alpha, \quad \text{med } \alpha \in \mathrm{Mat}_{n,p}(R),$$

hvor j-te søjle i α består af de koefficienter, der optræder, når w_j skrives som R-linearkombination af $u_1, \ldots, u_n$. Ifølge Elementardivisorsætningen (3.6) findes specielt invertible matricer $\sigma \in GL_n(R)$ og $\tau \in GL_p(R)$, så at $\sigma\alpha\tau$ har formen:

$$\sigma\alpha\tau = \begin{pmatrix} \delta_1 & & \\ & \ddots & \\ & & \delta_r \\ & & \end{pmatrix}, \quad \text{hvor } \delta_1 \mid \delta_2, \ldots, \delta_{r-1} \mid \delta_r.$$

Da $\sigma \in GL_n(R)$ er invertibel, følger det, at også sættet $(v_1, \ldots, v_n)$ defineret ved $(v_1, \ldots, v_n) := (u_1, \ldots, u_n)\sigma^{-1}$ er en fri basis for F. Tilsvarende er $(w_1, \ldots, w_p)\tau$ en fri basis for N, og denne nye basis for N er:

$$\begin{aligned}(w_1, \ldots, w_p)\tau &= (u_1, \ldots, u_n)\alpha\tau = (u_1, \ldots, u_n)\sigma^{-1}\sigma\alpha\tau \\ &= (v_1, \ldots, v_n)\sigma\alpha\tau \\ &= (\delta_1 v_1, \ldots, \delta_r v_r, 0, \ldots, 0).\end{aligned}$$

Her må vi have $r = p$ (altså ingen 0'er), og $(v_1, \ldots, v_n)$ er derfor den søgte fri basis for F ♠

(4.2) Basissætningen. *Enhver endeligt frembragt R-modul M har en basis $(e_1, \ldots, e_n)$, endda med* $\mathrm{Ann}(e_1) \supseteq \cdots \supseteq \mathrm{Ann}(e_n)$.

Bemærkning. Vi minder om, at elementer $e_1, \ldots, e_n \in M$ er en basis, netop hvis M er direkte sum af de cykliske moduler $Re_1, \ldots, Re_n$:

$$M = Re_1 \oplus \cdots \oplus Re_n, \quad \text{hvor } e_i \neq 0 \text{ for } i = 1, \ldots, n.$$

Disse cykliske moduler har formen $R/(\delta_i)$, hvor (hoved-)idealet (δ_i) er annullatoren for Re_i. Ækvivalent kan Basissætningen derfor formuleres: *Enhver endeligt frembragt R-modul er isomorf med en direkte sum:*

$$R/(\delta_1) \oplus \cdots \oplus R/(\delta_n),$$

endda med $\delta_1 \mid \delta_2, \ldots, \delta_{n-1} \mid \delta_n$ *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:

$$F \simeq R \oplus \cdots \oplus R$$

således at undermodulen N herved svarer til

$$N \simeq R\delta_1 \oplus \cdots \oplus R\delta_p \oplus 0 \oplus \cdots \oplus 0, \quad \text{hvor } \delta_1 \mid \delta_1, \ldots, \delta_{p-1} \mid \delta_p.$$

Tilføjes eventuelt $\delta_{p+1} = \cdots = \delta_n = 0$, har vi

$$N \simeq R\delta_1 \oplus \cdots \oplus R\delta_n,$$

og så er øjensynlig

$$M \simeq F/N \simeq R/R\delta_1 \oplus \cdots \oplus R/R\delta_n.$$

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 $e_1, \ldots, e_n$:

$$M = Re_1 \oplus \cdots \oplus Re_n$$

svarende til en isomorfi:

$$M \simeq R/(\delta_1) \oplus \cdots \oplus R/(\delta_n)$$

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 $e_1, \ldots, e_n$ således at $e_1, \ldots, e_p$ er torsionselementer og $e_{p+1}, \ldots, e_n$ er torsionsfri, svarende til at $\delta_1, \ldots, \delta_p$ er $\neq 0$ og $\delta_{p+1}, \ldots, \delta_n$ er $= 0$ (hvor $0 \leq p \leq n$). For de tilsvarende undermoduler:

$$N := Re_1 \oplus \cdots \oplus Re_p, \quad \text{og} \quad K := Re_{p+1} \oplus \cdots \oplus Re_n.$$

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 $x = n + k$, hvor $n \in N$ og $k \in K$, får vi $0 = \lambda x = \lambda n + \lambda k$, og heraf følger, at $\lambda k = 0$. 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 $e_1, \ldots, e_n$, hvor

$$R \supset \mathrm{Ann}(e_1) \supseteq \cdots \supseteq \mathrm{Ann}(e_n) \supset (0),$$

svarende til en isomorfi:

$$M \simeq R/(\delta_1) \oplus \cdots \oplus R/(\delta_n),$$

hvor $(\delta_i) = \mathrm{Ann}(e_i)$ og altså $\delta_1 \mid \delta_2, \ldots, \delta_{n-1} \mid \delta_n$ og $\delta_n \neq 0$. 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 $\delta_i \mid \delta_n$ for $i \leq n$, følger omvendt, 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

$$\mathrm{Ann}(M) = \mathrm{Ann}(e_n),$$

og har dermed vist følgende:
KOROLLAR. *Lad M være en endelig frembragt torsionsmodul. Da findes et element $e \in M$, så at*

$$\mathrm{Ann}(M) = \mathrm{Ann}(e) \spadesuit$$

DEFINITION. Ligningen $\mathrm{Ann}(M) = \mathrm{Ann}(e)$ er øjensynlig ensbetydende med at der gælder: $\mathrm{Ann}(e) \subseteq \mathrm{Ann}(x)$ for alle $x \in M$. Et sådant element siges også at have *minimal annullator*. En frembringer for (hoved-)idealet $\mathrm{Ann}(M)$ kaldes også et *minimalt element* for M.

(4.5) EKSEMPEL. En endelig kommutativ gruppe M er som $\mathbf{Z}$-modul naturligvis en endeligt frembragt torsionsmodul, og Basissætningen giver for en sådan gruppe en isomorfi:

$$M \simeq \mathbf{Z}/d_1\mathbf{Z} \oplus \cdots \oplus \mathbf{Z}/d_n\mathbf{Z}$$

af M på en direkte sum af endelige cykliske grupper (endda med $d_1 \,|\, d_2, \ldots, d_{n-1} \,|\, d_n$) For $x \in M$ er ordenen af x netop den positive frembringer for idealet $\mathrm{Ann}(x) \in \mathbf{Z}$. 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 **maksimal** (mht. "$<$" og "$|$") 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 $\mu = \pi_1 \dots \pi_r$.*

Bevis. Hvis δ er divisor i μ med $\mu'\delta = \mu$, hvor $\mu' \in R$, så er

$$R\mu \subseteq R\delta \subseteq R.$$

Af Noethers 2. isomorfisætning følger, at $R\delta$ svarer til en undermodul $M' = R\delta/R\mu$ i kvotienten $M = R/R\mu$ med $M/M' \simeq R/R\delta$. Vi har øjensynlig en surjektiv homomorfi fra R til $M' = R\delta/R\mu$ defineret ved $\lambda \mapsto \lambda\boxed{\delta} = \boxed{\lambda\delta}$, og den har kernen $R\mu'$, thi da μ og dermed δ 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:

$$(0) \subseteq M' \subseteq M \text{ med } M' \simeq R/(\mu') \text{ og } M/M' \simeq R/(\delta).$$

Ved induktion fås af $\mu = \pi_1 \dots \pi_r$ en kæde af længde r i $M = R/(\mu)$ med kvotienterne $R/(\pi_i)$ for $i = 1, \dots, r$. Er π_i'erne primelementer, så er (π_i)'erne maximalidealer og kvotienterne $R/(\pi_i)$ altså simple moduler. Og så er $r = \text{long}M$ ♠

(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} for $i = 1, \dots, k$. Da vil $\mu := \mu_1 \cdots \mu_k$ annullere M.*

Bevis. Lad $x \in M$. Da μ_k annullerer M/M_{k-1}, er $\mu_k\boxed{x} = \boxed{0}$, altså $\mu_k x \in M_{k-1}$. Induktivt fås derfor

$$\mu x = \mu_1 \cdots \mu_{k-1}(\mu_k x) = 0$$ ♠

Sætning. *Betragt for en R-modul M følgende betingelser:*

(i) *Modulen M er en endeligt frembragt torsionsmodul.*
(ii) *Der findes en kæde: $(*)$ $(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_k = M$, med kvotienter $M_i/M_{i-1} \simeq R/(\mu_i)$, hvor $\mu_i \neq 0$ for $i = 1, \dots, k$.*
(iii) *Modulen M er endeligt frembragt og der findes en skalar $\mu \neq 0$, der annullerer M.*
(iv) *Modulen M har endelig længde.*

Da gælder: (i) $\Longleftrightarrow$ (ii) $\Longleftrightarrow$ (iii) $\Longrightarrow$ (iv). *Hvis R ikke er et legeme, er betingelsen* (iv) *ækvivalent med de øvrige betingelser.*

Bevis. **(i)⇒(ii):** Da M er endeligt frembragt, findes en kæde $(*)$ med cykliske kvotienter $M_i/M_{i-1} \simeq R/(\mu_i)$ for $i = 1, \dots, k$. 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 lemma'et 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 $\mu \in R/\{0\}$ annullerer M. Lad*

$$\mu = \varepsilon \pi_1^{n_1} \cdots \pi_r^{n_r}$$

være en primopløsning af μ [hvor altså ε er en enhed og primelementerne π_i og π_j ikke er associerede, når $i \neq j$]. Sæt

$$M_i := \{x \in M \mid \pi_i^{n_i} x = 0\} \quad \textit{for } i = 1, \ldots, r.$$

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 $\mathrm{Ann}(x) = (\alpha)$. 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 $\mathrm{Ann}(x) = (\pi^n)$. 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 $\mathrm{Ann}(x) = (\pi^n) = (\pi_i^n)$ og dermed

$$\pi_i^{n_i} x = \pi_i^{n_i - n} \pi_i^n x = 0,$$

og altså $x \in M_i$, hvor i er det entydigt bestemte index således at π er associeret med π_i.

Vi mangler at vise, at M er direkte sum af M_i'erne. Skriv:

$$\mu = \mu_i \pi_i^{n_i}, \text{ hvor } \mu_i := \frac{\mu}{\pi^{n_i}} = \varepsilon \pi_1^{n_1} \cdots \pi_{i-1}^{n_{i-1}} \pi_{i+1}^{n_{i+1}} \cdots \pi_r^{n_r} \quad \text{for } i = 1, \ldots, r.$$

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 $\mu x = 0$, og fremstillingen viser derfor, at $M = M_1 + \cdots + M_r$.

Og summen er direkte. Betragt nemlig en fremstilling:

$$0 = x_1 + \cdots + x_r, \qquad \text{hvor } x_i \in M_i \text{ for } i = 1, \ldots, r$$

Når $j \neq i$, er $\pi_j^{n_j}$ divisor i μ_i og følgelig er

$$\mu_i x_j = 0, \quad \text{når } i \neq j.$$

Følgelig er

$$x_i = \sum_j \lambda_j \mu_j x_i = \lambda_i \mu_i x_i = \sum_j \lambda_i \mu_i x_j = \lambda_i \mu_i 0 = 0$$

for hvert $i = 1, \ldots, r$ ♠

PRIMÆRBASISSÆTNING. *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 en skalar $\mu \neq 0$, der annullerer M, jfr. Sætning (4.7). Af Sætning (4.9) fås nu en dekomposition $M = M_1 \oplus \cdots \oplus M_r$, hvor M_i er en π_i-primær undermodul for $i = 1, \ldots, r$. Vælg nu ifølge Basissætningen (4.2) i hver undermodul M_i en basis (nødvendigvis bestående af π_i-primære elementer). Da udgør de valgte elementer en primær-basis for M ♠

BEMÆRKNING. Basissætningen (4.2) udsiger, at enhver endeligt frembragt torsionsmodul er en direkte sum af cykliske moduler, dvs. moduler isomorfe med $R/(\delta)$,

hvor $\delta \neq 0$. Af ovenstående Primærbasissætning følger, at de cykliske moduler kan vælges primære, dvs. isomorfe med $R/(\pi^n)$, hvor π er et primelement i R. 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 endeligt frembragt torsionsmodul, findes ifølge Sætning (4.7) en Jordan–Hölder kæde

$$(0) = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_k = M.$$

Ifølge Hölder's Sætning afhænger de simple kvotienter M_i/M_{i-1} for $i = 1, \ldots, k$ på nær isomorfi og rækkefølge kun af modulen M (og ikke af den valgte kæde). Idealerne $\operatorname{Ann} M_i/M_{i-1}$ for $i = 1, \ldots, k$ afhænger derfor (bortset fra rækkefølgen) kun af M. Skrives $\operatorname{Ann} M_i/M_{i-1} = (\pi_i)$ for hvert $i = 1, \ldots, k$, følger det, at elementet:

$$\chi := \pi_1 \cdots \pi_k$$

på nær associering er entydigt bestemt ved M. Det har derfor mening, at indføre følgende:
DEFINITION. Elementet $\chi := \pi_1 \cdots \pi_k$ og dets associerede kaldes *karakteristiske elementer* 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 primopløsning 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 primopløsning af μ. Af (beviset for) Sætning (4.6) fremgår, at C har en Jordan-Hölder kæde med kvotienter $R/(\pi_i)$ for $i = 1, \ldots, n$. 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. Ganske som beviset for at $\operatorname{long} M' + \operatorname{long} M/M' = \operatorname{long} M$ ♡

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 element for kvotienten M_i/M_{i-1} for $i = 1, \ldots, k$, så er $\chi := \chi_1 \cdots \chi_k$ karakteristisk element for M.*

(2) Hvis $M = M_1 \oplus \cdots \oplus M_k$ er en direkte sum og χ_i er karakteristisk element for M_i for $i = 1, \ldots, k$, 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. $(\alpha) = \mathrm{Ann}(M)$. 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 $\chi \in \mathrm{Ann}(M) = (\alpha)$, 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 associent med et af π_i'erne. Her er $(\pi_i) = \mathrm{Ann} M_i/M_{i-1}$ annullator for en kvotient i en Jordan-Hölder følge 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 $M_i/M_{i-1} \simeq \mathbf{Z}/(p_i)$ og p_i er et primtal for $i = 1, \ldots, k$, bestemmes det karakteristiske element for M som $\chi := p_1 \ldots p_k$, jfr. Definition (4.11). På den anden side gælder ifølge Lagrange's indexsætning:

$$\begin{aligned} |M| &= |M_{k-1}| \cdot |M_k/M_{k-1}| = \cdots = |M_1| \cdot |M_2/M_1| \cdots |M_k/M_{k-1}| \\ &= p_1 \cdot p_2 \cdots p_k. \end{aligned}$$

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.*

Bevis. Vi slutter nemlig, at $p|\alpha$, så $p\lambda = \alpha$ med $\lambda \in \mathbf{Z}$, 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 $\alpha_1, \ldots, \alpha_n$ i α. Da er følgende betingelser ækvivalente:*

(i) *Kvotientmodulen F/N er en endeligt frembragt torsionsmodul.*
(ii) *Matricen $\alpha = (\alpha_1, \ldots, \alpha_n)$ har determinant $\neq 0$.*
(iii) *Søjlerne $\alpha_1, \ldots, \alpha_n$ 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 $\alpha_1, \ldots, \alpha_n$ 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)⇔(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 $e_1, \ldots, e_n$ den kanoniske basis for $F = R^n$, så er altså $\mu \boxed{e_i} = 0$ i $F/\alpha(F)$, og der findes derfor $\beta_i \in F$ med $\mu e_i = \alpha(\beta_i)$ for $i = 1, \ldots, n$. Er $\beta : F \to F$ bestemt ved matricen $\beta = (\beta_1, \ldots, \beta_n)$, så 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 $(v_1, \ldots, v_n)$ for F, og skalarer $\delta_1 \ldots, \delta_p \in R$ så at $(\delta_1 v_1, \ldots, \delta_p v_p)$ er en fri basis for N. Her er specielt $\delta_i \neq 0$ for $i = 1, \ldots, p$, 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 $\chi := \delta_1 \ldots \delta_n$ er karakteristisk element for F/N. Idet $(e_1, \ldots, e_n)$ og $(\alpha_1, \ldots, \alpha_n)$ er baser for $F = R^n$ og N, har vi "basisskiftematricer" $\sigma, \tau \in GL_n(R)$ bestemt ved:

$$(e_1, \ldots, e_n) = (v_1, \ldots, v_n)\sigma \quad \text{og} \quad (\alpha_1, \ldots, \alpha_n) = (\delta_1 v_1, \ldots, \delta_n v_n)\tau.$$

Idet v betegner matricen med søjlerne $v_1, \ldots, v_n$ og δ betegner diagonalmatricen med elementerne $\delta_1, \ldots, \delta_n$ 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 $R = \mathbf{Z}$, 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 endelig dimensionalt vektorrum over $\mathbf{C}$ og lad $\varphi : V \to V$ være en $\mathbf{C}$-lineær endomorfi. Da findes en basis for V, hvori φ beskrives ved en Jordan-matrix, dvs. en blokmatrix:*

$$\begin{pmatrix} \alpha_1 & & & \\ & \alpha_2 & & \\ & & \ddots & \\ & & & \alpha_r \end{pmatrix}$$

med kvadratiske blokke α_i langs diagonalen og 0'er udenfor og hvor de kvadratiske blokke langs diagonalen har formen:

$$\begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \lambda & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda \end{pmatrix}, \quad \textit{hvor } \lambda \in \mathbf{C}.$$

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 $(e_1, \ldots, e_n)$ en given basis for V, kan hver vektor $v \in V$ skrives som linearkombination:

$$(*) \quad v = v_1 e_1 + \cdots + v_n e_n$$

med entydigt bestemte koefficienter $v_i \in L$ for $i = 1, \ldots, n$.

Sættet bestående af de n koefficienter er vektorens *koordinatsæt* mht. den givne basis. Vi vil altid skrive sættet 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:

$$(**) \quad v = (e_1, \ldots, e_n)\underline{\underline{v}} \quad [\text{Kort: } v = e\underline{\underline{v}}].$$

Ved matricen hørende til endomorfien φ mht. den givne basis forstås den matrix $\underline{\underline{\varphi}} \in \mathrm{Mat}_n(L)$, hvori den i-te søjle $\underline{\underline{\varphi}}_i$ er koordinatsættet for billedet $\varphi(e_i)$ af den i-te basisvektor. Vi har altså:

$$\varphi(e_i) = (e_1, \ldots, e_n)\underline{\underline{\varphi}}_i, \qquad \text{for } i = 1, \ldots, n, \quad \text{dvs.}$$

$$(\varphi(e_i), \ldots, \varphi(e_n)) = (e_1, \ldots, e_n)\underline{\underline{\varphi}} \quad [\text{Kort: } \varphi(e) = e\underline{\underline{\varphi}}].$$

Heraf følger, at matricen $\underline{\underline{\varphi}}$ beskriver endomorfien $\varphi : V \to V$ i den forstand, at der for enhver vektor $v \in V$ gælder:

$$\underline{\underline{\underline{\underline{\varphi(v)}}}} = \underline{\underline{\varphi}}\,\underline{\underline{v}}\,,$$

thi da φ er lineær og derfor bevarer linearkombinationer fås:

$$\begin{aligned}\varphi(v) &= \varphi((e_1, \ldots, e_n)\underline{\underline{v}}) = (\varphi(e_1), \ldots, \varphi(e_n))\underline{\underline{v}} \\ &= [(e_1, \ldots, e_n)\underline{\underline{\varphi}}]\underline{\underline{v}} = (e_1, \ldots, e_n)[\underline{\underline{\varphi}}\,\underline{\underline{v}}].\end{aligned}$$

Bemærk, at i betegnelserne v og $\underline{\underline{\varphi}}$ er den givne basis $(e_1, \ldots, e_n)$ underforstået. Hvis der for en matrix $\alpha \in \mathrm{Mat}_n(L)$ eksisterer en basis for V mht. hvilken $\underline{\underline{\varphi}} = \alpha$, siger vi, at φ kan *beskrives* ved α eller at α *hører til* φ.

Observation. Hvis der til endomorfien $\varphi : V \to V$ mht. en given basis $(e_1, \ldots, e_n)$ hører matricen $\underline{\underline{\varphi}}$ i $\mathrm{Mat}_n(L)$, så er de øvrige matricer, der hører til φ, netop de matricer, der er regulær-ækvivalente med $\underline{\underline{\varphi}}$, dvs. har formen

$$\sigma^{-1}\underline{\underline{\varphi}}\sigma \qquad \text{med } \sigma \in GL_n(L).$$

(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 $L[X]$, ved hjælp 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: $X^{n+1}.v = X^n.(X.v) = \varphi^n(\varphi(v)) = \varphi^{n+1}(v)$) og dermed generelt:

$$(*) \quad (a_0 + a_1X + \cdots + a_nX^n).v = a_0v + a_1\varphi(v) + \cdots + a_n\varphi^n(v).$$

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 underrum $W \subseteq V$, som er φ-invariante, thi en undergruppe $W \subseteq V$ er et φ-invariant underrum, netop når der gælder:

(1) $$aw \in W \text{ og } \varphi(w) \in W \text{ for alle } a \in L \text{ og } w \in W,$$

og en $L[X]$-undermodul, netop når der gælder:

(2) $$f.w \in W \text{ for alle } f = a_0 + a_1X + \cdots + a_nX^n \in L[X] \text{ og } w \in W.$$

Da $L \subseteq L[X]$ og $\varphi(w) = X.w$, er det klart, at (2)⇒(1). Omvendt følger det let af ligningen $(*)$ ovenfor, at (1)⇒(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

$$\sigma : U \to V$$

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 $\sigma(X.u) = X.\sigma(u)$ for $u \in U$.

(5.5) Definition. Hvis en $L[X]$-modul V er endelig dimensional (som vektorrum) siges matricerne hørende til endomorfien $X_V = \varphi$ også at *høre til* modulen V eller at kunne *beskrive* modulen V.

Sætning. *Endelig dimensionale $L[X]$-moduler V og W er isomorfe, hvis og kun hvis de kan beskrives ved regulær-ækvivalente matricer (og dermed også ved samme matrix).*

Bevis. **"kun hvis":** Sæt $\varphi := X_V$ og $\psi := X_W$. Lad $\sigma : V \to W$ være en $L[X]$-isomorfi. Da er σ en L-isomorfi og $\sigma \circ \varphi = \psi \circ \sigma$. Lad $(e_1, \ldots, e_n)$ være en basis for V og lad $\alpha \in \mathrm{Mat}_n(L)$ være den tilhørende matrix for φ, dvs.

$$(*) \quad (\varphi(e_1), \ldots, \varphi(e_m)) = (e_1, \ldots, e_m)\alpha.$$

Sæt $e'_i := \sigma(e_i)$ for $i = 1, \ldots, n$, og anvend afbildningen σ på de to sider af $(*)$. Da $\sigma(\varphi(e'_i)) = \psi(\sigma(e_i)) = \psi(e'_i)$ for $i = 1, \ldots, n$, fås:

$$(\psi(e'_1), \ldots, \psi(e'_n)) = (e'_1, \ldots, e'_n)\alpha.$$

Da σ er en L-ismorfi, er $(e'_1, \ldots, e'_n)$ en basis for W, og den fundne ligning udsiger netop, at α er matricen hørende til ψ mht. denne basis.

"hvis": Hvis φ og ψ kan beskrives ved regulær-ækvivalente matricer, kan de, jfr. Observation (5.2), også beskrives ved samme matrix. Antag derfor, at matricen α i

$\mathrm{Mat}_n(L)$ beskriver φ mht. basen $(e_1,\ldots,e_n)$ for V og ψ mht. basen $(e'_1,\ldots,e'_n)$ for W. Da er

$$(\varphi(e_1),\ldots,\varphi(e_n)) = (e_1,\ldots,e_n)\alpha \quad \text{og}$$
$$(\psi(e'_1),\ldots,\psi(e'_n)) = (e'_1,\ldots,e'_n)\alpha.$$

Lad $\sigma : V \to W$ være L-isomorfien bestemt ved $\sigma(e_i) = e'_i$ for $i = 1,\ldots,n$. Da finder vi:

$$\begin{aligned}\sigma(\varphi(e_i)) &= \sigma((e_1,\ldots,e_n)\alpha_i) = (e'_1,\ldots,e'_n)\alpha_i \\ &= \psi(e'_i) = \psi(\sigma(e_i)).\end{aligned}$$

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. Lad $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in L[X]$ være et normeret polynomium. En $L[X]$-modul V er isomorf med kvotientmodulen $L[X]/(f)$, hvis og kun hvis modulen V kan beskrives ved matricen:

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{pmatrix},$$

thi ifølge Struktursætningen for polynomiumskvotienter udgør ækvivalensklasserne:

$$e_0 := \boxed{1},\ e_1 := \boxed{X},\ \ldots,\ e_{n-1} := \boxed{X^{n-1}}$$

en L-basis for kvotienten $V = L[X]/(f)$. Vi finder:

$$\begin{aligned} X.e_0 &= X.\boxed{1} = \boxed{X} = e_1, \\ X.e_1 &= X.\boxed{X} = \boxed{X^2} = e_2, \\ &\vdots \\ X.e_{n-1} &= X.\boxed{X^{n-1}} = \boxed{X^n} = \boxed{-a_0 - a_1X - \cdots - a_{n-1}X^{n-1}} \\ &= -a_0\boxed{1} - a_1\boxed{X} - \cdots - a_{n-1}\boxed{X^{n-1}} \\ &= -a_0e_0 - a_1e_1 - \cdots - a_{n-1}e_{n-1}, \end{aligned}$$

og det betyder netop, at X_V mht. basen $(e_0, \ldots, e_{n-1})$ beskrives ved den angivne matrix.

(5.7) Eksempel. Lad $\lambda \in L$ og lad $n \in \mathbf{N}$. 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

$$\begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \lambda & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda \end{pmatrix},$$

thi blandt polynomierne $(X-\lambda)^i$ for $i = 0, \ldots, n-1$ 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:

$$e_0 := \boxed{1}, e_1 := \boxed{X-\lambda}, \ldots, e_{n-1} := \boxed{(X-\lambda)^{n-1}}$$

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 mht. basen $(e_{n-1}, \ldots, e_1, e_0)$ 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:*

$$\begin{pmatrix} \alpha & ? \\ 0 & \gamma \end{pmatrix}.$$

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 mht. basen $(e_1, \ldots, e_r)$ for W og at γ beskriver ψ mht. basen $(e'_1, \ldots, e'_s)$ for V/W. Vælg vektorer $e_{r+1}, \ldots, e_{r+s}$ i V, hvis ækvivalensklasser (modulo W) er:

$$\boxed{e_{r+i}} = e'_i \qquad \text{for } i = 1, \ldots, s.$$

Da er $(e_1, \ldots, e_r, e_{r+1}, \ldots, e_{r+s})$ 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 mht. en basis $(e_1, \ldots, e_n)$ beskrives ved en blokmatrix af formen:

$$\begin{pmatrix} \alpha & ? \\ 0 & \gamma \end{pmatrix},$$

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:

$$\begin{pmatrix} \alpha_1 & ? & \ldots & ? \\ 0 & \alpha_2 & \ldots & ? \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \alpha_k \end{pmatrix},$$

hvor $\alpha_1, \ldots, \alpha_k$ er kvadratiske blokke langs diagonalen og matricen har 0'er under disse blokke, 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} for $i = 1, \ldots, k$.

(5.9) SÆTNING. *Lad $V_1, \ldots, V_k$ være $L[X]$-moduler, så at matricen α_i hører til V_i for $i = 1, \ldots, k$. Da kan den direkte sum $V = V_1 \oplus \cdots \oplus V_k$ beskrives ved blokmatricen:*

$$\begin{pmatrix} \alpha_1 & 0 & \ldots & 0 \\ 0 & \alpha_2 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \alpha_k \end{pmatrix},$$

der har kvadratiske blokke langs diagonalen og 0'er udenfor.

Bevis. Ganske som beviset i (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 i (5.3)$(*)$ fremgår, at for et polynomium:

$$f = a_0 + a_1X + \cdots + a_nX^n \in L[X]$$

er homoteti med f i $L[X]$-modulen (V,φ) afbildningen:

$$v \mapsto f.v = a_0v + a_1\varphi(v) + \cdots + a_n\varphi^n(v).$$

Homoteti med f er således endomorfien:

$$a_0 1_V + a_1\varphi + \cdots + a_n\varphi^n \in End_L(V).$$

Den siges at fremkomme ved *indsættelse* 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 $f(\varphi)$ er nulendomorfien, dvs. netop når $f(\varphi) = 0 \in End_L(V)$. Er dette tilfældet, siges endomorfien φ af *være rod* 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. **(i)⇒(ii)**, thi undermodulerne i (V,φ) er specielt underrum i vektorrummet V og følgelig er $\operatorname{long}(V,\varphi) \leq \dim V$.
(ii)⇒(i): Hvis (V,φ) har endelig længde, så 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 $L[X]/\mathcal{M}$, hvor $\mathcal{M} \subseteq L[X]$ er et maksimalideal. Specielt er $\mathcal{M} \neq (0)$, og så er $\mathcal{M}$ et hovedideal frembragt af et normeret polynomium. Af Struktursætningen for polynomiumskvotient følger derfor, at kvotienten er endelig dimensional som vektorrum over L.
(ii)⇔(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 de generelle resultater om torsionsmoduler i 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 *minimale polynomium* 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.

(5.13) Lad α være en matrix hørende til endomorfien φ. Matricen $X1-\alpha$ har da koefficienter i $L[X]$ ($X1$ betegner matricen $X\begin{pmatrix}1 & & \\ & \ddots & \\ & & 1\end{pmatrix} = \begin{pmatrix}X & & \\ & \ddots & \\ & & X\end{pmatrix}$) og dens determinant:

$$\chi_\alpha := \det(X1-\alpha)$$

er derfor et polynomium, øjensynlig normeret. Polynomiet χ_α 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, at

$$X1-\beta = \sigma^{-1}(X1)\sigma - \beta = \sigma^{-1}(X1)\sigma - \sigma^{-1}\alpha\sigma = \sigma^{-1}(X1-\alpha)\sigma \text{ og følgelig:}$$
$$\chi_\beta = \det(X1-\beta) = \det(\sigma^{-1})\det(X1-\alpha)\det(\sigma) = \chi_\alpha.$$

Matricen β har altså samme karakteristiske polynomium som matricen α. Vi kan derfor indføre følgende:

DEFINITION. Det normerede polynomium $\det(X1-\alpha) \in L[X]$ defineret ud fra en matrix α hørende til φ kaldes det *karakteristiske polynomium* for endomorfien φ og betegnes χ_φ.

SÆTNING. *For en endomorfi φ i et endeligt dimensionalt vektorrum V gælder: Det minimale polynomium f_φ er minimalt element for $L[X]$-modulen (V,φ). Det karakteristiske polynomium χ_φ er karakteristisk element for $L[X]$-modulen (V,φ). Begge polynomier er normerede.*

Bevis. Annullatoren for (V,φ) består af de polynomier f, for hvilke homoteti med f er nul, altså (jfr. Definition (5.10)) netop af de polynomier, der har φ som rod. Af Definition (5.12) fremgår derfor, at f_φ er (den normerede) frembringer for annulatoren for (V,φ). Den første påstand følger derfor af definitionen på minimalt element for en modul.

For at vise den anden påstand bemærker vi, at V som $L[X]$-modul har en kæde af undermoduler:

$$(0) = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_k = V,$$

hvor kvotienterne V_i/V_{i-1} er cykliske $L[X]$-moduler for $i = 1, \ldots, k$. Hvis matricen α_i hører til V_i/V_{i-1}, så hører til V en blokmatrix α af formen:

$$\alpha = \begin{pmatrix} \alpha_1 & ? & \ldots & ? \\ 0 & \alpha_2 & \ldots & ? \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & \alpha_k \end{pmatrix},$$

jfr. Bemærkning 2 (5.8), og en let determinant udregning giver, at $\chi_\alpha = \chi_{\alpha_1} \cdots \chi_{\alpha_k}$. På den anden side gælder ifølge Korollar 1 (4.13), 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 påstanden under forudsætning af, at V er cyklisk som $L[X]$-modul. Vi kan derfor antage, at V er en kvotient $L[X]/(f)$, hvor f er et normeret polynomium

$$f = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in L[X].$$

Af Sætning (4.12) fremgår nu, at f er karakteristisk element for $L[X]$-modulen V, altså at $f = \chi_\varphi$. På den anden side kan V beskrives ved den i Eksempel (5.6) angivne matrix. Det er derfor nok at vise, at denne matrix har karakteristisk polynomium f, altså at

$$\begin{vmatrix} X & 0 & \ldots & 0 & a_0 \\ -1 & X & \ldots & 0 & a_1 \\ 0 & -1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & X & a_{n-2} \\ 0 & 0 & \ldots & -1 & X + a_{n-1} \end{vmatrix} = X^n + a_{n-1}X^{n-1} + \cdots + a_0.$$

Og det ses let ved induktion efter n ved at udvikle determinanten efter første række.

Den sidste på stand er en umiddelbar følge af definitionerne på de to polynomier ♠

(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. Under brug af den foregående sætning er dette netop indholdet af Sætning (4.14) ♠

Observation. Det karakteristiske polynomium χ_φ har øjensynlig graden $\dim V$, idet φ beskrives ved en $n \times n$-matrix, hvor $n = \dim V$. Det minimale polynomium har derfor grad $\leq \dim V$.

Eksempel. (1) $n \times n$-matricen $\begin{pmatrix} \lambda & & \\ & \ddots & \\ & & \lambda \end{pmatrix}$, hvor $\lambda \in L$, beskriver øjensynlig homotetien $v \mapsto \lambda v$. Dens karakteristiske polynomium er $(X - \lambda)^n$ og det minimale polynomium er øjensynlig $X - \lambda$.

(2) $n \times n$-matricen $\alpha = \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \lambda & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda \end{pmatrix}$, hvor $\lambda \in L$, har også karakteristisk polynomium $(X-\lambda)^n$, så det minimale polynomium er divisor heri og dermed af formen $(X-\lambda)^k$, hvor $k \leq n$. Matricen $\alpha - \lambda 1$ er matricen:

$$\begin{pmatrix} 0 & 1 & & & \\ & 0 & 1 & & \\ & & 0 & \ddots & \\ & & & \ddots & 1 \\ & & & & 0 \end{pmatrix},$$

der har 1'er på "skrålinien" hvor $j - i = 1$ og 0'er udenfor, og ved udregning ses, at matricen $(\alpha - \lambda 1)^k$ er en tilsvarende matrix med 1'er på "skrålinien", hvor $j - i = k$ og 0'er udenfor. Matricen α er derfor først rod i polynomiet $(X-\lambda)^k$, når $k = n$, så det minimale polynomium er også $(X-\lambda)^n$.

(5.15) Et element $\lambda \in L$ kaldes som bekendt en *egenværdi* for φ, hvis der i V findes en til λ hørende *egenvektor* $v \neq 0$, dvs. en vektor $v \in V \setminus \{0\}$, således at

$$\varphi(v) = \lambda v.$$

Opfattes V som $L[X]$-modul, er betingelsen ækvivalent med følgende:

$$\operatorname{Ann} v = (X - \lambda),$$

thi at $\operatorname{Ann} v \supseteq (X-\lambda)$, er ensbetydende med at $X-\lambda$ annullerer v, dvs. ensbetydende med at $\varphi(v) - \lambda v = 0$, og da $(X-\lambda) \subseteq L[X]$ er et maximalideal, gælder der her "=", netop når $v \neq 0$.

SÆTNING. *For en skalar $\lambda \in L$ er følgende betingelser ækvivalente:*

(i) *Skalaren λ er egenværdi for endomorfien φ.*
(ii) *Skalaren λ er rod i det minimale polynomium f_φ.*
(iii) *Skalaren 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 **(ii)⇔(iii)**.
(i)⇒(ii): Antag, at $v \neq 0$ er egenvektor hørende til λ, altså at $\operatorname{Ann} v = (X-\lambda)$. Da f_φ annuller enhver vektor, er $f_\varphi \in (X-\lambda)$, så $X-\lambda$ er divisor i f_φ.
(ii)⇒(i): 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 der 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:*

$$\chi_\varphi = (X-\lambda_1)\cdots(X-\lambda_n), \quad \text{hvor } \lambda_i \in L \text{ for } i = 1,\ldots,n,$$

af førstegradspolynomier.
(iv) *Det minimale polynomium f_φ er et produkt:*

$$f_\varphi = (X-\lambda_1)\cdots(X-\lambda_s), \quad \text{hvor } \lambda_i \in L \text{ for } i = 1,\ldots,s,$$

af førstegradspolynomier.

Bevis. **(i)⇒(ii)**, thi en Jordan-matrix er specielt en øvre trekantsmatrix.
(ii)⇒(iii), thi det karakteristiske polynomium for en øvre trekantsmatrix er øjensynlig $(X-\lambda_1)\cdots(X-\lambda_n)$, hvor $\lambda_1,\ldots,\lambda_n$ er elementerne i diagonalen.
(iii)⇒(iv) ifølge Hamilton-Cayley's Sætning (5.14).
(iv)⇒(i): Af Primær-basissætningen (4.10) følger, at V som $L[X]$-modul er en direkte sum:

$$V = V_1 \oplus \cdots \oplus V_k,$$

hvor hver af undermodulerne V_j for $j = 1,\ldots,k$ er cyklisk og isomorf med en kvotientmodul 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 undermodulen V_j, er p^n divisor i f_φ.

Af forudsætningen om f_φ følger derfor, at p har formen $p = X-\lambda$ med $\lambda \in \{\lambda_1,\ldots,\lambda_s\}$. Undermodulen V_j er altså isomorf med en kvotientmodul af formen $L[X]/((X-\lambda)^n)$. Af Eksempel (5.7) følger derfor, at undermodulen V_j kan beskrives ved en matrix af formen

$$\begin{pmatrix} \lambda & 1 & & \\ & \lambda & \ddots & \\ & & \ddots & 1 \\ & & & \lambda \end{pmatrix}.$$

Den direkte sum $V = V_1 \oplus \cdots \oplus V_k$ kan derfor 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 $f_\varphi = (X-\lambda_1)\cdots(X-\lambda_s)$, hvor $\lambda_i \in L$ for $i = 1,\ldots,s$, af forskellige førstegradspolynomier.*

Bevis. **"hvis"**: 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.
"kun hvis": Hvis α er en diagonalmatrix og $\lambda_1, \ldots, \lambda_s \in L$ betegner de forskellige elemeneter i diagonalen, så er matrix-produktet $(\alpha - \lambda_1 1) \cdots (\alpha - \lambda_s 1)$ lig med nulmatricen [idet diagonalmatricer 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 $f \in \mathbf{C}[X]$ kan skrives som produkt:

$$f = (X - \lambda_1) \cdots (X - \lambda_s), \quad \text{hvor } \lambda_j \in \mathbf{C} \text{ for } j = 1, \ldots, s.$$

For $L = \mathbf{C}$ indeholder Hovedsætning (5.16) derfor Sætning (5.1) om Jordan's normalform.

For normerede polynomier f med reelle koefficienter, $f \in \mathbf{R}[X]$, medfører algebraens fundamentalsætning, at f kan skrives som et produkt:

$$(*) \quad f = p_1 \cdots p_t,$$

hvor de reelle polynomier p_k for $k = 1, \ldots, t$ enten er førstegradspolynomier $p_k = X - \lambda$, hvor $\lambda \in \mathbf{R}$, eller andengradspolynomier $p_k = (X - a)^2 + b^2$, hvor $a \in \mathbf{R}$ og $b \in \mathbf{R} \setminus \{0\}$, uden reelle rødder. I $\mathbf{C}[X]$ har vi nemlig fremstillingen:

$$(**) \quad f = (X - \lambda_1) \cdots (X - \lambda_s), \quad \text{hvor } \lambda_j \in \mathbf{C} \text{ for } j = 1, \ldots, s,$$

og herudfra fås ved komplex konjugering (idet jo $\overline{f} = f$), at

$$f = (X - \overline{\lambda}_1) \cdots (X - \overline{\lambda}_s).$$

Da fremstillingen $(**)$ er entydig bortset fra permutation af faktorerne, ses, at for hver ikke-reel faktor $X - \lambda$, hvor $\lambda = a + ib$ med $a \in \mathbf{R}$ og $b \in \mathbf{R} \setminus \{0\}$, i $(**)$ forekommer også faktoren $X - \overline{\lambda}$ i $(**)$, endda det samme antal gange. De ikke-reelle faktorer i $(**)$ kan derfor to og to multipliceres sammen til

$$(X - \lambda)(X - \overline{\lambda}) = (X - a - ib)(X - a + ib) = (X - a)^2 + b^2,$$

og så fås fremstillingen $(*)$.

Det følger, at de normerede, irreducible polynomier (dvs. primelementer) i $\mathbf{R}[X]$ er polynomierne $X - \lambda$, hvor $\lambda \in \mathbf{R}$, og $(X - a)^2 + b^2$, hvor $a \in \mathbf{R}$ og $b \in \mathbf{R} \setminus \{0\}$.

(5.18) SÆTNING. *Lad V være et endelig dimensionalt vektorrum over $\mathbf{R}$ og lad $\varphi : V \to V$ være en $\mathbf{R}$-lineær endomorfi. Da kan φ beskrives ved en blokmatrix:*

$$\begin{pmatrix} \alpha_1 & & & \\ & \alpha_2 & & \\ & & \ddots & \\ & & & \alpha_r \end{pmatrix}$$

med kvadratiske blokke α_i langs diagonalen og 0'er udenfor og hvor de kvadratiske blokke langs diagonalen har formen:

$$(1) \quad \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \lambda & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda \end{pmatrix}, \quad \textit{hvor } \lambda \in \mathbf{C}, \textit{ eller} \quad (2) \quad \begin{pmatrix} \mu & \epsilon & & & \\ & \mu & \epsilon & & \\ & & \mu & \ddots & \\ & & & \ddots & \epsilon \\ & & & & \mu \end{pmatrix},$$

hvor μ og ϵ er 2×2-matricer af formen:

$$\mu = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad \textit{og} \qquad \epsilon = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

med $a \in \mathbf{R}$ og $b \in \mathbf{R} \setminus \{0\}$.

Bevis. Ifølge Primær-basissætningen (4.10) er V som $\mathbf{R}[X]$-modul en direkte sum af moduler af formen $[X]/(p^n)$, hvor p er et primelement i $\mathbf{R}[X]$. Det er derfor nok at vise for et sådant primelement p, som vi kan antage er normeret, at $\mathbf{R}[X]$-modulen $V = \mathbf{R}[X]/(p^n)$ kan beskrives ved en matrix af en af de anførte to typer. Hvis $p = X - \lambda$, hvor $\lambda \in \mathbf{R}$, har vi vist i Eksempel (5.7), at X_V kan beskrives ved en matrix af den første type. Antag derfor, at $p = (X-a)^2 + b^2$, hvor $a \in \mathbf{R}$ og $b \in \mathbf{R} \setminus \{0\}$. Blandt de $2n$ polynomier: $\frac{1}{b^i}p^i$ og $\frac{1}{b^i}\frac{X-a}{b}p^i$ for $i = 0, \ldots, n-1$ 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 ækvivalensklasserne:

$$e_{2i} := \boxed{\frac{1}{b^i}p^i} \quad \text{og} \quad e_{2i+1}; = \boxed{\frac{1}{b^i}\frac{X-a}{b}p^i} \text{ for } i = 0, \ldots, n-1$$

derfor udgør en $\mathbf{R}$-basis for kvotienten $V = \mathbf{R}[X]/(p^n)$. Vi finder:

$$\frac{X-a}{b}.e_{2i} = e_{2i+1} \qquad \text{for } i = 0, \ldots, n-1, \quad \text{og dermed}$$

$$\begin{aligned}(X-a).e_{2i+1} &= \frac{(X-a)^2}{b}.e_{2i} \\ &= \frac{p}{b}.e_{2i} - be_{2i} = \begin{cases} e_{2i+2} - be_{2i}, & \text{for } i = 0, \ldots, n-2, \\ -be_{2n-2}, & \text{når } i = n-1, \end{cases}\end{aligned}$$

og det betyder netop, at X_V mht. basen $(e_{2n-1}, \ldots, e_1, e_0)$ beskrives ved en matrix af den anden type ♠

4. Oversigt over de grundlæggende egenskaber ved de hele tal.

(4.1) BESKRIVELSE. Systemet af *hele tal* er en (additivt skrevet) kommutativ gruppe $(\mathbf{Z}, +)$ (også betegnet $\mathbf{Z}^+$), der indeholder de naturlige tal $\mathbf{N}$ som en stabil delmængde. Det neutrale element i gruppen $(\mathbf{Z}, +)$ kaldes *nul* og betegnes 0. Ethvert helt tal $p \in \mathbf{Z}$ kan skrives som en differens

$$p = a - s \quad (= a + (-s))$$

mellem naturlige tal $a, s \in \mathbf{N}$.

(4.2) POTENSER. For et element a i en gruppe $(G, \cdot)$ med neutralt element e defineres *potenser* med *hel eksponent* $p \in \mathbf{Z}$,

$$a^p \in G,$$

som en udvidelse af potens med naturlig eksponent, og således at $a^0 = e$ og $a^{-n} = (a^n)^{-1}$.

[For en (kommutativ) additivt skrevet gruppe $(G, +)$ bruges betegnelsen

$$pa \in G$$

for den p'te potens af a for $p \in \mathbf{Z}$.]

(4.3) FUNDAMENTALE STRUKTURER. Udover den givne *addition* i $\mathbf{Z}$ er *multiplikation* i $\mathbf{Z}$ kompositionen $(p, q) \mapsto p \cdot q$ defineret ved

$$p \cdot q := pq = p\text{'te potens af } q \text{ i gruppen } (\mathbf{Z}, +),$$

og relationen *"mindre end"* i $\mathbf{Z}$, betegnet $<$, er defineret ved

$$p < q \overset{DEF}{\iff} q - p \in \mathbf{N}.$$

(4.4) REGNEREGLER. *Strukturerne ovenfor udvider de tilsvarende strukturer på delmængden* $\mathbf{N}$, *og* $(\mathbf{Z}, +, \cdot, <)$ *er en kommutativ ordnet ring, med* $1 \in \mathbf{N}$ *som etelement, hvis positive elementer er de naturlige tal:* $\mathbf{N} = \mathbf{Z}_+$.

(4.5) POTENSREGLER. *For elementer* a *og* b *i en gruppe* G *og hele tal* p *og* q *gælder*

1. potensregel:	$a^{p+q} = a^p a^q$	$[(p+q)a = pa + qa]$
2. potensregel:	$a^{pq} = (a^p)^q$	$[(pq)a = p(qa)]$
3. potensregel:	$(ab)^p = a^p b^p$, *når* $ab = ba$	$[p(a+b) = pa + pb]$.

(4.6) Potenssætning. *Lad der være givet en gruppe $(G, \cdot)$ og et element $a \in G$. Da findes netop en homomorfi $: (\mathbf{Z}, +) \to (G, \cdot)$, som afbilder $1 \mapsto a$, nemlig afbildningen $p \mapsto a^p$.*

(4.7) Ordningssætning. *Enhver ikke-tom, nedad begrænset delmængde $P \subseteq \mathbf{Z}$ har et mindste element. Enhver ikke-tom, opad begrænset delmængde $Q \subseteq \mathbf{Z}$ har et største element.*

5. Yderligere egenskaber ved de hele tal.

(5.1) Sætning om den kanoniske ringhomomorfi. *For enhver ring Λ findes netop én ringhomomorfi $: \mathbf{Z} \to \Lambda$, nemlig afbildningen*

$$p \mapsto p1_\Lambda \ (= p\text{'te potens af } 1_\Lambda \text{ i gruppen } (\Lambda, +)).$$

Bevis. En ringhomomorfi skal afbilde $1 \mapsto 1_\Lambda$, og da den skal bevare addition, er den eneste mulighed afbildningen

$$p \mapsto p1_\Lambda,$$

der er en homomorfi $: (\mathbf{Z}, +) \to (\Lambda, +)$, jfr. Potenssætningen. Det er derfor nok at vise, at denne afbildning også bevarer multiplikation, altså at

$$(pq)1_\Lambda = (p1_\Lambda)(q1_\Lambda).$$

Betragt hertil for et fast $q \in \mathbf{Z}$ de to sider som afbildningerne $: \mathbf{Z} \to \Lambda$ givet ved

$$p \mapsto (pq)1_\Lambda \qquad \text{og} \qquad p \mapsto (p1_\Lambda)(q1_\Lambda).$$

Da de begge er homomorfier $: (\mathbf{Z}, +) \to (\Lambda, +)$ [hvorfor?], er det ifølge Potenssætningen nok at indse, at de stemmer overens for $p = 1$. Og det er klart ♠

(5.2) Eksempel. Endomorfiring. Lad $(M, +)$ være en (additivt skrevet) kommutativ gruppe. *Endomorfiringen* for M, betegnet $\mathrm{End}\,(M)$, er da mængden af homomorfier $\varphi : (M, +) \to (M, +)$, organiseret ved sædvanlig addition [Summen $\varphi + \psi$ er altså afbildningen $x \mapsto \varphi(x) + \psi(x)$] og sammensætning som multiplikation [Produktet $\varphi \circ \psi$ er altså afbildningen $x \mapsto \varphi(\psi(x))$]. Herved er $\mathrm{End}\,(M)$ en ring [nul-elementet er den konstante afbildning $x \mapsto 0$, og et-elementet er den identiske afbildning $x \mapsto x$].

Det er let at se, at den kanoniske ringhomomorfi $: \mathbf{Z} \to \mathrm{End}\,(M)$ er givet ved

$$p \mapsto [x \mapsto px],$$

jfr. de tre Potensregler.

(5.3) Sætning. *I ringen $(\mathbf{Z}, +, \cdot)$ gælder nul-reglen, og for hvert naturligt tal n er* $\overbrace{1 + \cdots + 1}^{n} \neq 0$.

Bevis. Dette gælder generelt for ordnede ringe ($\neq 0$), og indses således:
Nulreglen udsiger, at når $p \neq 0$ og $q \neq 0$ er hele tal, så er også $pq \neq 0$. Vi kan antage, at $0 < p$ og $0 < q$ [hvorfor?], altså at $p, q \in \mathbf{Z}_+ = \mathbf{N}$, men så er også $pq \in \mathbf{Z}_+$, altså specielt $pq \neq 0$.

Tilsvarende følger af $1 \in \mathbf{Z}_+ = \mathbf{N}$, at også $n1 = \overbrace{1 + \cdots + 1}^{n} \in \mathbf{Z}_+$, og specielt, at $n1 \neq 0$ ♠

(5.4) DIVISIONSSÆTNINGEN. *Lad $d \in \mathbf{N}$ være et givet naturligt tal. Til hvert tal $a \in \mathbf{Z}$ findes da entydigt bestemte tal $q, r \in \mathbf{Z}$ således at*

$$a = qd + r \qquad og \qquad 0 \leq r < d.$$

Bevis. **Eksistens:** Lad $P \subseteq \mathbf{Z}$ være delmængden

$$P := \{p \in \mathbf{Z} \mid pd \leq a\}.$$

Da er P ikke-tom [hvorfor?] og opad begrænset [hvorfor?], og P har derfor ifølge Ordningssætningen et største element $=: q$. Nu er $a = qd + r$, med $r := a - qd$, og da $q \in P$, er $0 \leq r$. Da $q + 1 \notin P$, er $a < (q + 1)d = qd + d$, og altså $r = a - qd < d$.
Entydighed: Det er nok at betragte en fremstilling

$$0 = qd + r \qquad \text{med} \quad 0 \leq r < d.$$

Indsættes $r = (-q)d$ i de sidste uligheder, får vi

$$0d = 0 \leq (-q)d < d = 1d.$$

Da $d > 0$, følger heraf, at

$$0 \leq -q < 1.$$

Følgelig må vi have $q = 0$ (og dermed også $r = 0$) ♠

DEFINITION. Det i sætningen nævnte tal r kaldes den *principale rest* af a ved division med $d \in \mathbf{N}$.

BEMÆRKNING. Forudsættes om d blot, at det er et helt tal $\neq 0$, fås let en fremstilling

$$a = qd + r, \qquad \text{hvor} \qquad 0 \leq r < |d|.$$

(5.5) HOVEDIDEALSÆTNINGEN. *For ethvert tal $d \in \mathbf{Z}$ er delmængden*

$$\mathbf{Z}d := \{qd \mid q \in \mathbf{Z}\}$$

en undergruppe i $(\mathbf{Z}, +)$. Omvendt gælder, at enhver undergruppe H i $(\mathbf{Z}, +)$ har formen

$$H = \mathbf{Z}d, \qquad hvor \qquad d \geq 0,$$

og d er entydigt bestemt ved H, nemlig som

$$d = 0, \quad \text{når } H = \{0\}$$
$$d = \text{mindste positive tal i } H, \quad \text{når } H \neq \{0\}.$$

Bevis. Den første påstand ses enten direkte, eller ved at bemærke, at $\mathbf{Z}d$ er billedet ved den ved $q \mapsto qd$ bestemte homomorfi : $(\mathbf{Z}, +) \to (\mathbf{Z}, +)$.
Hvis den givne undergruppe er $H = \{0\}$, har vi $H = \mathbf{Z}0$. Er $H \neq \{0\}$, findes et element $x \neq 0$ i H. Nu vil også $-x \in H$, og af de to tal x og $-x$ i H er det ene positivt. Da der således findes positive elementer i H, kan vi lade d betegne det mindste positive element i H. Det påstås, at

$$\mathbf{Z}\, d = H.$$

Her er "$\subseteq$" klart, thi da $d \in H$, og H er en undergruppe, vil også $qd \in H$ for alle $q \in \mathbf{Z}$.
For at vise "$\supseteq$" betragtes et vilkårligt tal $a \in H$. Ifølge Divisionssætningen (5.4) kan vi skrive

$$a = qd + r, \qquad \text{hvor } 0 \leq r < d.$$

Nu er $r = a + (-q)d$, og da $a \in H$ og $(-q)d \in H$ og H er en undergruppe, vil også $r \in H$. Da $0 \leq r$, og $r < d =$ mindste positive tal i H, må vi have $r = 0$, og altså $a = qd \in \mathbf{Z}d$.

Endelig er det klart, at tallet $d \geq 0$ udfra delmængden $H = \mathbf{Z}\, d$ kan bestemmes på den i sætningen angivne måde ♠

(5.6) Definition. For hele tal $a, d \in \mathbf{Z}$ siger vi, at d er *divisor* i a eller at a er et *multiplum* af d, hvis der findes et tal $q \in \mathbf{Z}$, så at $a = qd$. Relationen skrives også

$$d \,|\, a \qquad [\text{læses:"}d \text{ går op i } a\text{".}]$$

Ethvert tal $a \in \mathbf{Z}$ har de *trivielle divisorer* $1, -1, a, -a$.

To tal a og b kaldes *primiske*, hvis de kun har 1 og -1 som fælles divisorer.

Observation. Der gælder:

$$d \,|\, a \iff a \in \mathbf{Z}d \iff \mathbf{Z}a \subseteq \mathbf{Z}d \subseteq \mathbf{Z}\,.$$

De trivielle divisorer d i a svarer til, at vi her har

$$\mathbf{Z}a \subseteq \mathbf{Z}d = \mathbf{Z} \qquad \text{eller} \qquad \mathbf{Z}a = \mathbf{Z}d \subseteq \mathbf{Z}\,.$$

Bemærkning. Da tallene a og $-a$ har de samme divisorer, og da d er divisor i a, hvis og kun hvis $-d$ er divisor i a, er vi ofte kun interesserede i positive divisorer d i

positive tal a. I denne situation følger af $a = qd$, at $q \geq 1$, og dernæst, at $1 \leq d \leq a$. Er n et tal $\neq 0$, er der derfor kun endelig mange divisorer i n, og for hvert tal a er der kun endelig mange fælles divisorer for a og n. Den største af de fælles divisorer for a og n kaldes den *største fælles divisor* for a og n, og betegnes (med en klassisk betegnelse og hvis misforståelser er udelukket) med (a, n). Skrivemåden $(a, n) = d$ udtrykker altså, at tallet d er største fælles divisor for a og n. Specielt udtrykker $(a, n) = 1$, at a og n er primiske.

(5.7) Sætning. *For hele tal $a, n \in \mathbf{Z}$, hvor $n \neq 0$, er følgende betingelser ækvivalente:*

(i) *Tallet a er primisk med n.*
(ii) *Der findes tal $x, y \in \mathbf{Z}$, så at $1 = xa + yn$.*
(iii) *For alle tal $z \in \mathbf{Z}$ gælder: $n \mid az \implies n \mid z$.*

Bevis. **(i)⇒(ii)**: I gruppen $(\mathbf{Z}, +)$ er delmængden

$$H := \{xa + yn \mid x, y \in \mathbf{Z}\}$$

klart en undergruppe, og den har derfor ifølge Hovedidealsætningen (5.5) formen $H = \mathbf{Z}d$ med et tal $d \geq 0$. Vi har $a \in H = \mathbf{Z}d$ og $n \in H = \mathbf{Z}d$, altså $d \mid a$ og $d \mid n$, så d er en fælles divisor for a og n. Da $d \geq 0$, følger det af forudsætningen, at $d = 1$. Af $H = \mathbf{Z}1$ følger nu, at $1 \in H$, og det er jo netop påstanden.
(ii)⇒(iii): Vi har $1 = xa + yn$ med $x, y \in \mathbf{Z}$. Hvis $n \mid az$, kan vi skrive $az = qn$ med et $q \in \mathbf{Z}$, og så er

$$z = (xa + yn)z = xaz + ynz = xqn + yzn = (xq + yz)n$$

et multiplum af n.
(iii)⇒(i): Er tallet $d \in \mathbf{Z}$ divisor i både a og n, kan vi skrive

$$a = ud, \quad n = zd \qquad \text{med } u, z \in \mathbf{Z}.$$

Heraf fås $un = uzd = az$, så $n \mid az$, og dermed ifølge forudsætningen $n \mid z$. Vi kan derfor skrive

$$z = vn, \qquad \text{med } v \in \mathbf{Z}\,.$$

Nu er $n = zd = nvd$, og altså $n(1 - vd) = 0$. Da Nul-reglen gælder i $\mathbf{Z}$ og $n \neq 0$, fås $vd = 1$, og så er $d = \pm 1$ ♠

(5.8) Definition af primtal. Et *primtal* er et helt tal $p > 1$, som kun har trivielle divisorer.

Observation. Er p et primtal, og er $a \in \mathbf{Z}$, så gælder:

$$a \text{ er primisk med } p \iff p \nmid a\,.$$

SÆTNING. *Et primtal p, der går op i et produkt az, vil gå op i en af faktorerne.*

Bevis. Påstanden kan skrives

$$p \,|\, az \;\wedge\; p \not| \, a \;\Longrightarrow\; p \,|\, z,$$

og den følger derfor af Sætning (5.7)(iii) ♠

(5.9) SÆTNING. *Hvis tallene $a, b \in \mathbf{Z}$ begge er primiske med tallet $n \neq 0$, så er også produktet ab primisk med n.*

Bevis. Anvend f.eks. betingelsen (iii) i Sætning (5.7) to gange ♡

(5.10) OBSERVATION. To primtal p og q er primiske, hvis og kun hvis de er forskellige.

KOROLLAR. *Hvis tallene*

$$a = p_1 \cdots p_r \quad \textit{og} \quad n = q_1 \cdots q_s$$

er produkter af primtal $p_1, \ldots, p_r, q_1, \ldots, q_s$, så er a og n primiske, hvis og kun hvis mængderne

$$\{p_1, \ldots, p_r\} \quad \textit{og} \quad \{q_1, \ldots, q_s\}$$

er disjunkte.

Bevis. **"kun hvis"**: Et (prim-)tal, som ligger i begge de to mængder, er øjensynlig en ikke-triviel divisor i både a og n.
"hvis": Et fast q_i er forskelligt fra – og dermed primisk med – ethvert p_j, og derfor primisk med produktet $a = p_1 \cdots p_r$ ifølge Sætning (5.9). Da a således er primisk med ethvert q_i, er a også primisk med produktet $n = q_1 \cdots q_s$ (igen ifølge Sætning (5.9)) ♠

(5.11) KOROLLAR. *Hvis $n = n_1 \cdots n_r$ er et produkt af parvis primiske naturlige tal $n_1, \ldots, n_r$, så gælder for alle hele tal x, at*

$$n \,|\, x \;\Longleftrightarrow\; n_1 \,|\, x \;\wedge \cdots \wedge\; n_r \,|\, x\,.$$

Bevis. "⇒" er trivielt.
"⇐": Sættes $a := n_1 \cdots n_{r-1}$, kan vi induktivt antage, at $a \,|\, x$, og vi kan altså skrive $x = az$ med $z \in \mathbf{Z}$. Vi har altså

$$an_r = n \qquad \text{og} \qquad az = x.$$

Da n_r er primisk med produktet $a = n_1 \cdots n_{r-1}$ ifølge Sætning (5.9) og $n_r \,|\, x = az$, følger det, at $n_r \,|\, z$. Og så er $an_r \,|\, az$, altså $n \,|\, x$ ♠

(5.12) Hovedsætning om primopløsning. *Ethvert tal $n > 1$ kan skrives som et produkt*

$$n = p_1 \cdots p_r$$

af primtal $p_1, \ldots, p_r$, og denne fremstilling er entydig, bortset fra permutation af faktorerne.

Bevis. **Eksistens**: Lad $n > 1$ være givet. Den mindste blandt divisorerne > 1 i tallet n er da et primtal [Hvorfor?]. Kaldes dette primtal for p_1, kan vi skrive

$$n = p_1 n_1, \qquad \text{hvor altså} \quad 1 \leq n_1 < n.$$

Hvis $n_1 = 1$, er $n = p_1$ den ønskede fremstilling, og hvis $n_1 > 1$ kan vi tilsvarende skrive $n_1 = p_2 n_2$, hvor p_2 er et primtal, og vi har så

$$n = p_1 p_2 n_2, \qquad \text{med} \quad 1 \leq n_2 < n_1 < n.$$

Det ses, at vi efter højst n skridt får den ønskede fremstilling

$$n = p_1 p_2 \cdots p_r n_r \qquad \text{med} \quad 1 = n_r \,.$$

Entydighed: Vi skal vise for primtal $p_1, \ldots, p_r, q_1, \ldots, q_s$, at hvis

$$p_1 \cdots p_r = q_1 \cdots q_s,$$

så er $r = s$ og der gælder, eventuelt efter permutation af faktorerne, at $q_i = p_i$ for $i = 1, \ldots, r$. Vi kan antage, at $r \leq s$, og vi viser påstanden ved induktion efter r. I tilfældet $r = 1$ følger det af

$$p_1 = q_1 \cdots q_s \,,$$

at q_1 er divisor i p_1, og da p_1 er et primtal og $q_1 > 1$, må vi have $q_1 = p_1$, og $s = 1$. Antag nu, at $r > 1$ og at påstanden gælder for $r - 1$. . Af Korollar (5.10) fås, at mængderne $\{p_1, \ldots, p_r\}$ og $\{q_1 \ldots, q_r\}$ ikke er disjunkte. Efter eventuel permutation kan vi antage, at et fælles element i de to mængder er primtallet $p_r = q_s$. Af

$$(p_1 \cdots p_{r-1})p_r = (q_1 \cdots q_{s-1})q_s$$

får vi

$$p_1 \cdots p_{r-1} = q_1 \cdots q_{s-1}$$

ifølge Nul-reglen, og induktionsantagelsen giver nu det ønskede ♠

6. Appendix: Restklasser modulo n.

(6.1) Definition. Lad n være et naturligt tal. For hele tal $a, b \in \mathbf{Z}$ siger vi, at a er *kongruent med* b *modulo* n, og vi skriver

$$a \equiv b \pmod{n},$$

hvis n går op i $b - a$. Vi har altså

$$a \equiv b \pmod{n} \overset{DEF}{\iff} b - a \in \mathbf{Z}n.$$

Det er let at se, at denne relation i $\mathbf{Z}$ er en ækvivalensrelation. Ækvivalensklasserne kaldes *restklasser modulo* n. Restklassen, der indeholder et givet $a \in \mathbf{Z}$, er delmængden

$$\boxed{a} = \{a + qn \mid q \in \mathbf{Z}\} =: a + \mathbf{Z}n.$$

Hvis tallet a tilhører en restklasse X, siges a også at være en repræsentant for X. Dette betyder, at $X = \boxed{a}$.

Mængden af restklasser modulo n betegnes $\mathbf{Z}/\mathbf{Z}n$. Elementerne $X \in \mathbf{Z}/\mathbf{Z}n$ har altså formen

$$X = \boxed{a},$$

hvor $a \in \mathbf{Z}$ er en repræsentant for X. Vi har

$$\boxed{a} = \boxed{b} \iff a \equiv b \pmod{n}.$$

Af Divisionssætningen (5.4) følger, at hver restklasse X entydigt kan skrives

$$X = \boxed{r}, \qquad \text{hvor } 0 \leq r < n.$$

Mængden $\mathbf{Z}/\mathbf{Z}n$ består således af de n elementer

$$\boxed{0}, \boxed{1}, \boxed{2}, \ldots, \boxed{n-1}.$$

Specielt er

$$|\mathbf{Z}/\mathbf{Z}n| = n.$$

(6.2) Regning med restklasser. Det er let at se, at den ovenfor definerede ækvivalensrelation harmonerer med kompositionerne + og · i $\mathbf{Z}$ i den forstand, at

(*) $$x' \equiv x \wedge y' \equiv y \implies x' + y' \equiv x + y \wedge x'y' \equiv xy.$$

Vi kan derfor indføre kompositioner + og · i mængden $\mathbf{Z}/\mathbf{Z}n$ af restklasser på følgende måde: For givne restklasser X og Y vælges repræsentanter : $X = \boxed{x}$, $Y = \boxed{y}$. Summen $X + Y$ er da restklassen

$$X + Y := \boxed{x + y}$$

og produktet XY er restklassen

$$XY := \boxed{xy}.$$

Af (*) følger, at disse restklasser er veldefinerede, dvs. ikke afhænger af de foretagne valg af repræsentanter.

Det er let at se, at mængden $\mathbf{Z}/\mathbf{Z}n$ af restklasser med disse to kompositioner er en kommutativ ring $(\mathbf{Z}/\mathbf{Z}n, +, \cdot)$. Den kaldes *restklasseringen modulo n* og betegnes også $\mathbf{Z}/n$ [eller evt. $\mathbf{Z}_n$]. Nul-elementet er restklassen $\boxed{0}$ og et-elementet er restklassen $\boxed{1}$.

Af definitionen fremgår umiddelbart, at afbildningen $x \mapsto \boxed{x}$, der afbilder det hele tal x over i sin restklasse modulo n, er en surjektiv ringhomomorfi : $\mathbf{Z} \to \mathbf{Z}/n$.

(6.3) Eksempel. For $n = 6$ fås restklasseringen $\mathbf{Z}/6$ der indeholder de 6 elementer $\boxed{0}, \boxed{1}, \boxed{2}, \boxed{3}, \boxed{4}, \boxed{5}$. Idet vi udelader $\boxed{\ }$ i betegnelserne bliver kompositionstavlerne

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

(6.4) Sætning. *For hele tal $a, n \in \mathbf{Z}$, $n \geq 1$, er følgende betingelser ækvivalente:*

(i) *a er primisk med n.*
(ii) *Der findes tal $x, y \in \mathbf{Z}$, så at $1 = xa + yn$.*
(iii) *For alle tal $z \in \mathbf{Z}$ gælder : $n \mid az \implies n \mid z$.*
(iv) *Restklassen $\boxed{a}$ er invertibel i ringen $\mathbf{Z}/n$.*
(v) *Restklassen $\boxed{a}$ er regulær i $\mathbf{Z}/n$.*

Bevis. At betingelserne (i), (ii) og (iii) er ækvivalente er netop indholdet af Sætning (5.7). Det er derfor nok at vise, at at (ii)⇔(iv) og (iii)⇔(v).
(ii)⇒(iv): Af $1 = xa + yn$ følger $1 \equiv xa \pmod{n}$, og så er $\boxed{1} = \boxed{xa} = \boxed{x}\boxed{a}$. Følgelig er $\boxed{a}$ invertibel (med $\boxed{x}$ som invers).
(iv)⇒(ii): Hvis $\boxed{a}$ er invertibel, findes en restklasse X, så at $X\boxed{a} = \boxed{1}$. Er $x \in \mathbf{Z}$ en repræsentant for X, har vi altså $\boxed{1} = X\boxed{a} = \boxed{x}\boxed{a} = \boxed{xa}$. Følgelig er $1 \equiv xa \pmod{n}$, så vi kan skrive $1 = xa + yn$ med $y \in \mathbf{Z}$.
(iii)⇒(v): Lad Z være en restklasse således at $\boxed{a}\,Z = \boxed{0}$. Vi skal vise, at $Z = \boxed{0}$. Lad $z \in \mathbf{Z}$ være en repræsentant for Z. Da er $\boxed{0} = \boxed{a}\,Z = \boxed{a}\boxed{z} = \boxed{az}$, og følgelig er $n \mid az$. Heraf sluttes $n \mid z$, altså $Z = \boxed{z} = \boxed{0}$.
(v)⇒(iii): Hvis $n \mid az$, har vi $\boxed{0} = \boxed{az} = \boxed{a}\boxed{z}$. Da $\boxed{a}$ er regulær, følger heraf $\boxed{z} = \boxed{0}$, altså $n \mid z$ ♠

De invertible elementer i $\mathbf{Z}/n$ er altså restklasser af formen $\boxed{a}$, hvor a er primisk med n. De kaldes også *primiske restklasser*. Med multiplikation som komposition udgør de en kommutativ gruppe, nemlig gruppen $(\mathbf{Z}/n)^*$ af invertible elementer i ringen $\mathbf{Z}/n$.

(6.5) Sætning. *Lad p være et primtal. Da er restklasseringen $\mathbf{Z}/p$ et legeme.*

Bevis. Vi skal vise, at alle elementer $\neq \boxed{0}$ i $\mathbf{Z}/p$ er invertible. Disse elementer er de $p-1$ restklasser

$$\boxed{1}, \ldots, \boxed{p-1},$$

og de er øjensynlig alle primiske med p, når p er et primtal. Påstanden følger nu af Sætning (6.4) ♠

Notation. Legemet $\mathbf{Z}/p$, hvor p er et primtal, betegnes også $\mathbf{F}_p$.

(6.6) Er der givet r naturlige tal $n_1, \ldots, n_r$ kan vi betragte restklasseringene $\mathbf{Z}/n_1, \ldots, \mathbf{Z}/n_r$ og produktringen $\mathbf{Z}/n_1 \times \cdots \times \mathbf{Z}/n_r$.

Den kinesiske restklassesætning. Lad $n = n_1 \cdots n_r$ være et produkt af parvis primiske naturlige tal $n_1, \ldots, n_r$. Den kanoniske ringhomomorfi ind i produktringen, $\mathbf{Z} \to \mathbf{Z}/n_1 \times \cdots \times \mathbf{Z}/n_r$, inducerer da en ringisomorfi:

$$\mathbf{Z}/n \xrightarrow{\approx} \mathbf{Z}/n_1 \times \cdots \times \mathbf{Z}/n_r.$$

Bevis. Lad $\Lambda = \mathbf{Z}/n_1 \times \cdots \times \mathbf{Z}/n_r$ være produktringen. Idet vi med $\boxed{a}_i$ betegner a's restklasse modulo n_i, er nul-elementet og et-elementet i Λ givet ved

$$0_\Lambda = (\boxed{0}_1, \ldots, \boxed{0}_r), \qquad 1_\Lambda = (\boxed{1}_1, \cdots, \boxed{1}_r),$$

og den kanoniske ringhomomorfi : $\mathbf{Z} \to \Lambda$ er bestemt ved

$$x \mapsto x1_\Lambda = (\boxed{x}_1, \cdots, \boxed{x}_r).$$

Ifølge Korollar (5.11) har vi

$$\begin{aligned} x1_\Lambda = 0_\Lambda &\iff \boxed{x}_1 = \boxed{0}_1 \wedge \cdots \wedge \boxed{x}_r = \boxed{0}_r \\ &\iff n_1 \,|\, x \wedge \cdots \wedge n_r \,|\, x \\ &\iff n \,|\, x \iff x \in \mathbf{Z}n. \end{aligned}$$

Kernen for den kanoniske ringhomomorfi er således idealet $\mathbf{Z}n$. Ifølge Isomorfisætning for ringe induceres der derfor en injektiv ringhomomorfi:

$$\mathbf{Z}/n \hookrightarrow \Lambda = \mathbf{Z}/n_1 \times \cdots \times \mathbf{Z}/n_r.$$

Da de to ringe har samme elementantal (nemlig $n = n_1 \cdots n_r$), må denne injektive afbildning være bijektiv ♠

BEMÆRKNING. Surjektiviteten udsiger: Til givne hele tal $a_1, \ldots, a_r \in \mathbf{Z}$ findes et helt tal $x \in \mathbf{Z}$, så at

$$x \equiv a_1 \pmod{n_1} \wedge \cdots \wedge x \equiv a_r \pmod{n_r},$$

og injektiviteten udsiger, at et sådant tal x er entydigt bestemt "modulo n".

(6.7) DEFINITION. For et naturligt tal n betegnes med $\varphi(n)$ antallet af naturlige tal $a \leq n$, der er primiske med n. De naturlige tal $\leq n$ svarer netop til de n elementer

$$\boxed{1}, \boxed{2}, \ldots, \boxed{n-1}, \boxed{n} = \boxed{0}.$$

Det følger, jfr. (6.4), at $\varphi(n)$ er antallet af primiske restklasser modulo n, altså at

$$\varphi(n) = |(\mathbf{Z}/n)^*|$$

er ordenen af gruppen $(\mathbf{Z}/n)^*$ af invertible elementer i ringen $\mathbf{Z}/n$.

Funktionen $n \mapsto \varphi(n)$ kaldes *Euler's φ-funktion.*

OBSERVATION. Man finder let : $\varphi(1) = 1$, og at der for et hvert **primtal** p gælder: $\varphi(p) = p - 1,\ \varphi(p^\nu) = p^\nu - p^{\nu-1} = p^\nu(1 - \frac{1}{p})$.

SÆTNING. *Euler's φ-funktion er multiplikativ i den forstand, at hvis $n = n_1 \cdots n_r$ er et produkt af parvis primiske naturlige tal $n_1, \ldots, n_r$, så er*

$$\varphi(n) = \varphi(n_1) \cdots \varphi(n_r).$$

Bevis. Af ringisomorfien:

$$\mathbf{Z}/n \xrightarrow{\sim} \mathbf{Z}/n_1 \times \cdots \times \mathbf{Z}/n_r,$$

jfr. Den kinesiske restklassesætning (6.5), får vi en gruppeisomorfi:

$$(\mathbf{Z}/n)^* \xrightarrow{\sim} (\mathbf{Z}/n_1)^* \times \cdots \times (\mathbf{Z}/n_r)^*$$

mellem grupperne af invertible elementer i de to ringe. Sammenligning af elementantallene giver nu det ønskede ♠

(6.8) Sætning. *Lad n være et naturligt tal. Hvis tallet $a \in \mathbf{Z}$ er primisk med n, så er*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Bevis. Restklassen $\boxed{a}$ er et element i den multiplikative gruppe $(\mathbf{Z}/n)^*$. Da denne gruppe har orden $\varphi(n)$ har vi

$$\boxed{1} = \boxed{a}^{\varphi(n)} = \boxed{a^{\varphi(n)}},$$

og det er netop påstanden ♠

Som specialtilfælde fås:

Fermat's "lille" sætning. Lad p være et primtal. Hvis tallet $a \in \mathbf{Z}$ ikke er et multiplum af p, så er

$$a^{p-1} \equiv 1 \pmod{p}$$♠

(6.9) Wilson's sætning. Lad p være et ulige primtal. Da er

$$(p-1)! \equiv -1 \pmod{p}.$$

Bevis. Legemet $\mathbf{F}_p = \mathbf{Z}/p$ har p elementer, og den multiplikative gruppe $\mathbf{F}_p^* = \mathbf{F}_p \setminus \{0\}$ har derfor orden $p-1$. For hvert element $\alpha \neq 0$ i $\mathbf{F}_p$ har vi derfor $\alpha^{p-1} = \boxed{1}$. Det kan udtrykkes således: Polynomiet $X^{p-1} - \boxed{1} \in \mathbf{F}_p[X]$ har i $\mathbf{F}_p$ som rødder alle α, hvor $\alpha \in \mathbf{F}_p^*$, dvs. de $p-1$ elementer $\boxed{1}, \boxed{2}, \cdots, \boxed{p-1}$. Da polynomiet er normeret og har grad $p-1$, har vi følgelig

$$X^{p-1} - \boxed{1} = (X - \boxed{1})(X - \boxed{2}) \cdots (X - \boxed{p-1}).$$

Sammenligning af koefficienterne giver en række ligninger. Specielt får vi for konstantleddene:

$$\boxed{-1} = -\boxed{1} = (-\boxed{1})(-\boxed{2}) \cdots (-\boxed{p-1}) = \boxed{(-1)^{p-1}(p-1)!}.$$

For ulige p er det netop påstanden (og for $p = 2$ er det uinteressant) ♠

(6.10) Sætning. *Lad p være et ulige primtal. Da vil halvdelen af de $p-1$ tal $1, 2, \ldots, p-1$ opfylde kongruensen*

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

og den resterende halvdel vil opfylde kongruensen

$$x^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Bevis. Som vi har set i beviset for Wilson's sætning (6.9), vil rødderne i polynomiet $X^{p-1} - \boxed{1} \in \mathbf{F}_p[X]$ netop være elementerne $\boxed{1}, \boxed{2}, \cdots, \boxed{p-1}$. Da p er ulige, har vi

$$X^{p-1} - \boxed{1} = \left(X^{\frac{p-1}{2}} - \boxed{1}\right)\left(X^{\frac{p-1}{2}} + \boxed{1}\right).$$

Hvert af de $p-1$ elementer er derfor rod i $X^{\frac{p-1}{2}} - \boxed{1}$ eller i $X^{\frac{p-1}{2}} + \boxed{1}$. De to polynomier har begge graden $\frac{p-1}{2}$ og kan altså hver højst have $\frac{p-1}{2}$ rødder. Vi slutter derfor, at netop $\frac{p-1}{2}$ af elementerne er rødder i $X^{\frac{p-1}{2}} - \boxed{1}$, og at de øvrige $\frac{p-1}{2}$ elementer er rødder i $X^{\frac{p-1}{2}} + \boxed{1}$. Og det er netop påstanden ♠

(6.11) Korollar. Lad p være et primtal, således at $p \equiv 1 \pmod{4}$. Da findes et tal $y \in \mathbf{Z}$, så at

$$y^2 \equiv -1 \pmod{p}.$$

Bevis. Da $p \equiv 1 \pmod{4}$, kan vi skrive $p - 1 = 4h$ med $h \in \mathbf{N}$. Vælg nu et tal x, så at $x^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Sættes $y = x^h$ har vi følgelig

$$y^2 = x^{2h} = x^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

som ønsket ♠

Bemærk. Kongruensen $y^2 \equiv -1 \pmod{p}$ har højst 2 løsninger modulo p (hvorfor?). Man kan vise, at den ingen løsninger har, hvis $p \equiv 3 \pmod{4}$.

BRØKRING
DE RATIONALE TAL

1. Brøker i en ring. Analyse.

(1.1) ANALYSE. Lad der være givet en kommutativ ring R og i R en *multiplikativ* delmængde S, dvs. en delmængde $S \subseteq R$, som en stabil over for multiplikation og indeholder et-elementet 1. Vi ønsker, at indlægge R i en (større) ring A, hvori elementerne fra S er invertible, f.eks. for at kunne løse ligninger af formen

$$xs = a, \quad \text{hvor } s \in S, \text{ og } a \in R,$$

der jo i den større ring A har løsningen $x = as^{-1}$.

Lad os antage, at problemet er løst i den forstand, at der er givet en indlejring $R \hookrightarrow A$, d.v.s. en injektiv ringhomomorfi

$$\varphi : R \to A,$$

således at elementerne $\varphi(s)$, hvor $s \in S$, er invertible i A. Vi udleder en række konsekvenser:

0: Selv om ringen A ikke forudsættes kommutativ, gælder for elementer $a \in R$ og $s \in S$, at

$$\varphi(a)\varphi(s) = \varphi(s)\varphi(a)$$

(idet begge er sider er $= \varphi(as) = \varphi(sa)$), da R var forudsat kommutativ), og at

$$\varphi(s)^{-1}\varphi(a) = \varphi(a)\varphi(s)^{-1}$$

(multiplicér med $\varphi(s)^{-1}$ først fra venstre, dernæst fra højre).

1: Betragtes i A delmængden

$$R\underset{\varphi}{\bullet}S^{-1} := \{\varphi(a)\varphi(s)^{-1} \mid a \in R \wedge s \in S\} \ ,$$

gælder, at $R\underset{\varphi}{\bullet}S^{-1}$ *er en delring af* A, thi

$$\begin{aligned}
\varphi(a)\varphi(s)^{-1} + \varphi(b)\varphi(t)^{-1} &= \varphi(a)\varphi(t)\varphi(t)^{-1}\varphi(s)^{-1} + \varphi(b)\varphi(s)\varphi(s)^{-1}\varphi(t)^{-1} \\
&= \varphi(at)\varphi(st)^{-1} + \varphi(bs)\varphi(st)^{-1} \\
&= [\varphi(at) + \varphi(bs)]\varphi(st)^{-1} \\
&= \varphi(at + bs)\varphi(st)^{-1} \in R\underset{\varphi}{\bullet}S^{-1}, \\
\varphi(a)\varphi(s)^{-1} \cdot \varphi(b)\varphi(t)^{-1} &= \varphi(a)\varphi(b)\varphi(s)^{-1}\varphi(t)^{-1} \\
&= \varphi(ab)\varphi(st)^{-1} \in R\underset{\varphi}{\bullet}S^{-1}
\end{aligned}$$

og

$$-1_A = -\varphi(1) = \varphi(-1)\varphi(1)^{-1} \in R\underset{\varphi}{\bullet}S^{-1}.$$

(2): Videre gælder, at *delringen* $R\underset{\varphi}{\bullet}S^{-1}$ *indeholder billedringen* $\varphi(R)$, thi for alle $a \in R$ er

$$\varphi(a) = \varphi(a)\varphi(1)^{-1}.$$

Vi kan derfor betragte indlejringen : $R \hookrightarrow A$ som en indlejring:

$$R \hookrightarrow R\underset{\varphi}{\bullet}S^{-1} \ ,$$

og elementerne $\varphi(s)$, hvor $s \in S$, *er også invertible i delringen* $R\underset{\varphi}{\bullet}S^{-1}$, idet

$$\varphi(s)^{-1} = \varphi(1)\varphi(s)^{-1}.$$

(3): Endelig gælder, at *den herved fundne indlejring* : $R \hookrightarrow R\underset{\varphi}{\bullet}S^{-1}$ *kun afhænger af* R *og* S (og ikke af den givne indlejring $\varphi : R \hookrightarrow A$). Indføres nemlig i produktmængden $R \times S$ kompositionerne $+$ og $\cdot$ givet ved

$$(a, s) + (b, t) := (at + bs, st)$$
$$(a, s) \cdot (b, t) := (ab, st),$$

og betragtes afbildningen $\Phi : R \times S \to A$ defineret ved

$$\Phi(a, s) := \varphi(a)\varphi(s)^{-1},$$

følger det af **(1)**, at Φ er en homomorfi

$$\Phi : (R \times S, +, \cdot) \to (A, +, \cdot).$$

Billedet ved Φ er øjensynlig netop delringen $R\underset{\varphi}{\bullet}S^{-1}$, så ifølge isomorfisætningen induceres en isomorfi:

$$(R \times S, +, \cdot)/\underset{\Phi}{\sim} \xrightarrow{\sim} (R\underset{\varphi}{\bullet}S^{-1}, +, \cdot),$$

hvor $\underset{\Phi}{\sim}$ er den til Φ hørende kongruensrelation.

Og denne relation afhænger ikke af φ, thi vi har

$$\begin{aligned}
(a, s) \underset{\Phi}{\sim} (a', s') &\overset{DEF}{\iff} \Phi(a, s) = \Phi(a', s') \\
&\iff \varphi(a)\varphi(s)^{-1} = \varphi(a')\varphi(s')^{-1} \\
&\iff \varphi(a)\varphi(s') = \varphi(a')\varphi(s) \\
&\iff \varphi(as') = \varphi(a's) \\
&\iff as' = a's,
\end{aligned}$$

da φ var forudsat at være en injektiv afbildning.

(1.2) Bemærkning. Hvis den givne ring R overhovedet kan indlejres i en større ring A, hvori elementerne fra S er invertible, viser den foregående analyse, hvordan vi kan **konstruere** en sådan indlejring: Vi skal betragte produktmængden $R \times S$ med kompositionerne $+$ og $\cdot$ defineret i (1.1)(3), og heri kongruensrelationen $\sim$ fundet i (1.1)(3). Kvotienten $(R \times S, +, \cdot)/\sim$ er da den søgte ring. Problemet er imidlertid, at den i (1.1)(3) bestemte relation

$$(a, s) \sim (a', s') \overset{DEF}{\iff} as' = a's$$

i $R \times S$ i almindelighed **ikke** er en ækvivalensrelation. Det er jo også på forhånd klart, at vi ikke for enhver multiplikativ delmængde $S \subseteq R$ kan indlægge R i en større ring A, hvori elementerne fra S er invertible, idet en nødvendig betingelse herfor er, at elementerne fra S er regulære.

(1.3) Brøknotation. Hvis den givne ring R er delring af en ring A, hvori elementerne i S er invertible, skrives ofte

$$\frac{a}{s} := as^{-1} = s^{-1}a, \qquad \text{når } a \in R \text{ og } s \in S.$$

Sådanne elementer i A kaldes *brøker*.

2. Brøkringen.

(2.1) Brøker. Lad R være en kommutativ ring, lad $S \subseteq R$ være en multiplikativ delmængde, og betragt produktmængden $R \times S$ bestående af par (a, s), hvor $a \in R$ og $s \in S$. Et par af formen (au, su), hvor $u \in S$, siges at fremgå af parret (a, s) ved at *forlænge med* u.

I $R \times S$ defineres kompositioner $+$ og $\cdot$ ved

$$(a, s) + (b, t) := (at + bs, st)$$
$$(a, s) \cdot (b, t) := (ab, st)$$

og en relation $\equiv$ (kaldet "kongruens") ved

$$(a, s) \equiv (a', s') \overset{DEF}{\iff} \exists u, u' \in S : (au, su) = (a'u', s'u').$$

To par er således kongruente, netop hvis de kan forlænges til samme par. Det er let at se, at

$$(a, s) \equiv (a', s') \iff \exists t \in S : tas' = ta's.$$

Videre gælder følgende:

Lemma. *Kompositionen $+$ i $R \times S$ er kommutativ, associativ og har (0,1) som neutralt element. Kompositionen $\cdot$ i $R \times S$ er kommutativ, associativ, og har (1,1) som neutralt element. Relationen $\equiv$ er en kongruensrelation i $(R \times S, +, \cdot)$.*

Bevis. Der er meget at eftervise, men det er let ♡

Definition. En *brøk* (med tæller fra R og nævner fra S) er en ækvivalensklasse i $R \times S$. Ækvivalensklassen, der indeholder et givet par $(a, s) \in R \times S$ betegnes a/s, og kaldes brøken med *tæller* a og *nævner* s. Enhver brøk X kan skrives på formen $X = a/s$, med en passende *repræsentant* $(a, s) \in R \times S$.

Bemærk, at $au/su = a/s$ for $u \in S$, da $(au, su) = (a, s)$.

(2.2) Brøkregning. Ifølge Lemma (2.1) kan vi i mængden af brøker, dvs. i kvotienten $R \times S/\equiv$, definere kompositioner ved regning med repræsentanter: Har brøken X repræsentanten (a, s) og brøken Y repræsentanten (b, t), defineres *summen* $X + Y$ som brøken, der indeholder summen

$$(a, s) + (b, t) = (at + bs, st)$$

af repræsentanterne, og *produktet* $X \cdot Y$ som brøken, der indeholder produktet

$$(a, s) \cdot (b, t) = (ab, st)$$

af repræsentanterne. Vi har altså

$$a/s + b/t = (at + bs)/st$$
$$a/s \cdot b/t = ab/st\,.$$

Sætning. *Med kompositionerne defineret ovenfor er mængden af brøker, altså kvotienten* $(R \times S, +, \cdot)/\equiv$*, en kommutativ ring med nul-elementet* $0/1$ *og ét-elementet* $1/1$.

Bevis. De i Lemma (2.1) anførte egenskaber ved kompositionerne $+$ og $\cdot$ i $R \times S$ nedarves umiddelbart til kvotienten $R \times S/\equiv$. Det er derfor nok at vise, at hver brøk X har en modsat mht. $+$, og at $\cdot$ er distributiv mht. $+$. Vælges en repræsentant (a, s) for X, har vi $X = a/s$, og vi ser, at

$$X + (-a)/s = a/s + (-a)/s = 0/s^2 = (0 \cdot s^2)/(1 \cdot s^2) = 0/1\,.$$

Da $0/1$ er nul-element i kvotienten, følger det, at brøken $(-a)/s$ er modsat til brøken $X = a/s$.

For at vise den distributive lov, betragtes brøker $X = a/s$, $y = b/t$ og $Z = c/u$. Vi finder

$$\begin{aligned} XZ + YZ &= a/s \cdot c/u + b/t \cdot c/u = ac/su + bc/tu \\ &= (actu + bcsu)/sutu \\ &= (act + bcs)u/sutu = (at + bs)c/stu \\ &= (at + bs)/st \cdot c/u = [a/s + b/t] \cdot c/u \\ &= (X + Y) \cdot Z \spadesuit \end{aligned}$$

Definition. Den ovenfor konstruerede ring $(R \times S, +, \cdot)/\equiv$ kaldes den til $S \subseteq R$ hørende *brøkring*, og den betegnes $R[S^{-1}]$. Den siges, at fremgå af R ved at *invertere* elementerne i S.

(2.3) Den kanoniske homomorfi. Det er klart, at den ved

$$a \mapsto a/1$$

bestemte afbildning er en ringhomomorfi:

$$R \to R[S^{-1}].$$

Den kaldes *den kanoniske homomorfi* af ringen R ind i brøkringen $R[S^{-1}]$.

SÆTNING. *Den kanoniske homomorfi* $: R \to R[S^{-1}]$ *er injektiv, hvis og kun hvis elementerne i* S *er regulære. I bekræftende fald er kongruensrelationen* $\equiv$ *bestemt ved*

$$(a, s) \equiv (a', s') \iff as' = a's.$$

Bevis. **"hvis":** Er $a/1 = b/1$, så er parrene $(a, 1)$ og $(b, 1)$ kongruente, og der findes derfor et $u \in S$, så at $ua1 = ub1$. Da u er regulær, følger heraf $a = b$.
"kun hvis": Er $sa = 0$, så er $a/1 = sa/s = 0/s = 0/1$, og følgelig er $a = 0$.
"⇐": Dette gælder øjensynlig uden forudsætning om S.
"⇒": Er $(a, s) \equiv (a', s')$, så findes $u \in S$, så at $uas' = ua's$. Da u er regulær, følger heraf, at $as' = a's$ ♠.

(2.4) OBSERVATION. Ved den kanoniske homomorfi $: R \to R[S^{-1}]$ afbildes elementer i S over i invertible elementer i ringen $R[S{-}1]$,

thi når $s \in S$, så er $1/s$ en brøk, og den er klart invers til $s/1$.

Det følger således, at R kan indlejres i en ring A, hvori elementerne i S er invertible, netop når elementerne i S er regulære i R.

(2.5) DEN TOTALE BRØKRING. Af særlig interesse er tilfældet, hvor vi i en given kommutativ ring R inverterer alle regulære elementer, dvs. som S bruger mængden R^{reg} af regulære elementer i R. Den herved fremkomne brøkring $R[(R^{\text{reg}})^{-1}]$ kaldes også den *totale brøkring* for R.

Af Sætning (2.3) følger, at enhver ring R kan opfattes som en delring af sin totale brøkring.

(2.6) BRØKLEGEME. For et kommutativt integritetsområde R har vi $R^{\text{reg}} = R\backslash\{0\}$. Den toltale brøkring

$$R[(R\backslash\{0\})^{-1}]$$

fås altså ved at invertere alle elementer $\neq 0$ i R.

SÆTNING. *Lad* R *være et kommutativt integritetsområde. Da er den totale brøkring* $R[(R\backslash\{0\})^{-1}]$ *et legeme.*

Bevis. Lad X være en brøk forskellig fra nul-elementet $0/1$, og skriv X på formen $X = a/s$, hvor $a, s \in R$ og $s \neq 0$. Da er specielt $a \neq, 0$, altså $a \in R \setminus \{0\}$, så vi kan betragte brøken s/a. Vi har

$$X \cdot s/a = a/s \cdot s/a = as/as = 1/1,$$

hvoraf følger, at X er invertibel (med $X^{-1} = s/a$) ♠

DEFINITION. Dette legeme kaldes integritetsområdets *brøklegeme.*

Det følger, at et kommutativt integritetsområde R kan opfattes som en delring af sit brøklegeme. Opfattet således kan enhver brøk X skrives

$$X = a/s = \frac{a}{s} = as^{-1}, \quad \text{med } a \in R \text{ og } s \in R \setminus \{0\}.$$

(2.7) Division med nul. I almindelighed forudsættes ikke, at ringens nul-element ikke tilhører S. Hvis $0 \in S$, så er konstruktionen af brøkringen imidlertid ikke særlig interessant, idet vi har følgende:

Observation. Brøkringen $R[S^{-1}]$ er nul-ringen, hvis og kun hvis $0 \in S$,

thi nul-ringen er som bekendt karakteriseret ved at dens nul-element også er et-element, og vi har

$$0/1 = 1/1 \iff \exists s \in S : s \cdot 0 \cdot 1 = s \cdot 1 \cdot 1 \iff 0 \in S.$$

(2.8) I almindelighed gælder for den kanoniske homomorfi $: R \to R[S^{-1}]$ følgende:

Udvidelsessætning. *Enhver ringhomomorfi $\varphi : R \to A$, der afbilder elementer i S over i invertible elementer i A, kan entydigt udvides til en ringhomomorfi $\bar{\varphi} : R[S^{-1}] \to A$ fra brøkringen. I diagramform:*

$$\begin{array}{ccc} R & \longrightarrow & R[S^{-1}] \\ {\scriptstyle\varphi}\downarrow & \swarrow & \\ A & & \end{array}$$

Bevis. **"Entydighed":** Enhver brøk X kan skrives

$$X = a/s, \quad \text{hvor } a \in R \text{ og } s \in S,$$

og så er $X \cdot s/1 = a/s \cdot s/1 = as/s = a/1$. Hvis homormorfien $\bar{\varphi} : R[S^{-1}] \to A$ er en udvidelse af $\varphi : R \to A$, så får vi $\varphi(a) = \bar{\varphi}(a/1) = \bar{\varphi}(X \cdot s/1) = \bar{\varphi}(X)\bar{\varphi}(s/1) = \bar{\varphi}(X)\varphi(s)$, hvoraf

$$\bar{\varphi}(X) = \varphi(a)\varphi(s)^{-1}.$$

Heraf følger entydigheden af φ.
"Eksistens": Overvej, at afbildningen $: R \times S \to A$ defineret ved

$$(a, s) \mapsto \varphi(a)\varphi(s)^{-1}$$

er en homomorfi $: (R \times S, +, \cdot) \to (A, +, \cdot)$, og at den respekterer ækvivalensrelationen $\equiv$. Overvej, at den inducerede homomorfi $(R \times S, +, \cdot)/\equiv \to A$ fra kvotienten opfylder de stillede krav ♡

3. De rationale tal.

(3.1) Definition. Brøklegemet $\mathbf{Z}[(\mathbf{Z}\setminus\{0\})^{-1}]$ dannet ud fra det kommutative integritetsområde $\mathbf{Z}$ kaldes de *rationale tals legeme* og betegnes $\mathbf{Q}$. Elementerne i $\mathbf{Q}$ kaldes *rationale tal*. Da elementerne i $\mathbf{Z}\setminus\{0\}$ er regulære, er den kanoniske homomorfi $: (\mathbf{Z}, +, \cdot) \to (\mathbf{Q}, +, \cdot)$ injektiv. Vi vil (næsten) altid identificere elementerne i $\mathbf{Z}$ med deres billeder i $\mathbf{Q}$ ved denne afbildning, og altså opfatte $\mathbf{Z}$ som en delring af $\mathbf{Q}$. Den kanoniske homomorfi er da inklusionsafbildningen

$$\mathbf{Z} \hookrightarrow \mathbf{Q}.$$

Et rationalt tal er altså en brøk. Med den indførte identifikation kan hvert rationalt tal λ i $\mathbf{Q}$ skrives

$$\lambda = a/s = \frac{a}{s} = as^{-1}, \quad \text{hvor} a \in \mathbf{Z} \text{ og } s \in \mathbf{Z}\setminus\{0\},$$

dvs. som en kvotient mellem hele tal $a, s \in \mathbf{Z}$ hvor $s \neq 0$.

(3.2) Ordning. I mængden $\mathbf{Q}$ defineres en relation kaldet *mindre end* og betegnet $<$ ved

$$\lambda < \mu \overset{DEF}{\iff} \mu - \lambda \in \{m/n \mid m, n \in \mathbf{N}\}.$$

Sætning. *Med den ovenfor definerede relation er* $(\mathbf{Q}, +, \cdot, <)$ *et ordnet legeme, hvis positive elementer er elementerne i*

$$\mathbf{Q}_+ = \{m/n \mid m, n \in \mathbf{N}\}.$$

Bevis. Lad $P \subseteq \mathbf{Q}$ betegne delmængden

$$\{m/n \mid m, n \in \mathbf{N}\}.$$

Det er klart, at delmængden P er stabil under $+$ og $\cdot$. Endvidere ses det let, at $0 \notin P$. Ifølge generelle resultater om ordnede ringe er det derfor nok at vise, at der for hvert rationalt tal $\lambda \neq 0$ gælder: $\lambda \in P$ eller $-\lambda \in P$. Hertil skrives $\lambda = a/s$, hvor $a, s \in \mathbf{Z}$ og $s \neq 0$. Da $a/s = [(-1)a]/[(-1)s] = (-a)/(-s)$, kan vi endda antage, at λ har formen

$$\lambda = p/n, \quad \text{hvor } p \in \mathbf{Z} \text{ og } n \in \mathbf{N}.$$

Da $\lambda \neq 0$, er specielt $p \neq 0$. Følgelig er enten $p \in \mathbf{N}$, dvs. $\lambda \in P$, eller $-p \in \mathbf{N}$, dvs. $-\lambda \in P$ ♠

Bemærkning. Det er klart, at denne relation på delmængden $\mathbf{Z}$ stemmer overens med den allerede indførte relation "mindre end" i $\mathbf{Z}$.

(3.3) Fælles nævner. Da $a/s = (-a)/(-s)$, følger det, at hvert rationalt tal λ kan skrives

$$\lambda = p/n, \quad \text{hvor } p \in \mathbf{Z} \text{ og } n \in \mathbf{N},$$

altså med positiv nævner. Endvidere kan endelig mange rationale tal $\lambda_1, \ldots, \lambda_k$ altid skrives på formen

$$\lambda_1 = p_1/n\,, \ldots, \lambda_k/n, \quad \text{hvor } p_1, \ldots, p_k \in \mathbf{Z} \text{ og } n \in \mathbf{N},$$

altså med en fælles, positiv nævner, thi er $\lambda_i = q_i/n_i$, hvor $q_i \in \mathbf{Z}$ og $n \in \mathbf{N}$ for $i = 1, \ldots, k$, så kan vi som fælles nævner f.eks. bruge produktet $n := n_1 \cdots n_k$.

For rationale tal p/n og q/n med samme positive nævner $n \in \mathbf{Z}$ har vi øjensynlig

$$\frac{p}{n} + \frac{q}{n} = \frac{p+q}{n}, \qquad \frac{p}{n} - \frac{q}{n} = \frac{p-q}{n}, \qquad \frac{p}{n} < \frac{q}{n} \iff p < q.$$

(3.4) Udvidelsessætning. Den generelle Udvidelsessætning (2.2) for brøkringe omhandler her ringhomomorfier $\varphi : \mathbf{Z} \to A$, som afbilder tal $\neq 0$ i $\mathbf{Z}$ over i invertible elementer i ringen A. Vi bemærker først, at det hertil er nok, at ringhomomorfien $\varphi : \mathbf{Z} \to A$ afbilder positive tal, dvs. elementer i $\mathbf{N}$, over i invertible elementer i ringen A, thi når $\varphi(n)$ er invertibel i A, så er også $\varphi(-n) = -\varphi(n)$ invertibel (med den inverse $[\varphi(-n)]^{-1} = -[\varphi(n)]^{-1}$). Videre minder vi om, at der for enhver ring A findes netop én ringhomomorfi : $\mathbf{Z} \to A$, nemlig afbildningen

$$p \mapsto p1_A.$$

Udvidelsessætningen er altså her følgende:

Sætning. *Lad A være en ring, hvori elementerne*

$$n1_A = \overbrace{1_A + \cdots + 1_A}^{n}, \quad \textit{med } n \in \mathbf{N},$$

er invertible. Da findes netop én ringhomomorfi : $\mathbf{Q} \to A$ ♠

Observation. En ringhomomorfi $\varphi : \mathbf{Q} \to A$, hvor A ikke er nulringen, er injektiv,

thi hvis φ ikke er injektiv, så findes et rationalt tal $\lambda \neq 0$, så at $\varphi(\lambda) = \varphi(0) = 0_A$, og så er $1_A = \varphi(1) = \varphi(\lambda\lambda^{-1}) = \varphi(\lambda)\varphi(\lambda^{-1}) = 0_A\varphi(\lambda^{-1}) = 0_A$, og A er følgelig nulringen.

Korollar. *Lad L være et legeme, hvori elementerne*

$$n1_L = \overbrace{1_L + \cdots + 1_L}^{n}, \quad \textit{med } n \in \mathbf{N},$$

er invertible. Da findes netop én ringhomomorfi $: \mathbf{Q} \to L$*, og den er injektiv* ♠

BEMÆRKNING. Et legeme med ovennævnte egenskab siges også at have *karakteristik* 0, og billedet af $\mathbf{Q}$ ved ovennævnte injektive homomorfi, der jo så er et dellegeme af L isomorft med $\mathbf{Q}$, kaldes *primlegeme*t i L.

(3.5) POTENSER. En (additivt skrevet) kommutativ gruppe $(M, +)$ kaldes *entydigt delelig*, hvis der for hvert $a \in M$ og hvert $n \in \mathbf{N}$ gælder, at ligningen

$$nx = a$$

har en og kun én løsning $x \in M$.

For hvert $n \in \mathbf{N}$ er afbildningen

$$\pi_n : x \mapsto nx$$

en endomorfi $\pi_n : (M, +) \to (M, +)$. Vi kan derfor opfatte π_n som element i endomorfiringen $End(M)$ for den kommutative gruppe $(M, +)$, jfr. "Hele tal", Eksempel (5.2). Videre er π_n netop billedet af $n \in \mathbf{N}$ ved den kanoniske ringhomomorfi

$$\pi : \mathbf{Z} \to End(M).$$

Det er klart, at gruppen $(L, +)$ er entydigt delelig, netop når afbildningerne π_n er bijektive for alle $n \in \mathbf{N}$. Da de bijektive endomorfier netop er de invertible elementer i ringen $End(M)$, ser vi, at $(M, +)$ er entydigt delelig, netop når endomorfiringen $A := End(M)$ opfylder forudsætningen i Sætning (3.4). Hvis $(M, +)$ er entydigt delelig, følger det derfor af Sætning (3.4), at der findes netop én ringhomomorfi $: \mathbf{Q} \to End(M)$.

DEFINITION. Lad $(M, +)$ være en entydigt delelig kommutativ gruppe. Den entydigt bestemte ringhomomorfi $: \mathbf{Q} \to End(M)$ betegnes da $\lambda \mapsto \pi_\lambda$, og for hvert $\lambda \in \mathbf{Q}$ betegnes endomorfien π_λ også $x \mapsto \lambda x$. Billedet $\lambda x := \pi_\lambda(x)$ af et element $x \in M$ ved denne endomorfi kaldes den *λ'te potens* af x.

(3.6) POTENSREGLERNE. *Lad $(M, +)$ være en entydigt delelig, kommutativ gruppe. For elementer $x, y \in M$ og rationale tal $\lambda, \mu \in \mathbf{Q}$ gælder da:*

1. regel	$(\lambda + \mu)x = \lambda x + \mu x$
2. regel	$(\lambda\mu)x = \lambda(\mu x)$
3. regel	$\lambda(x + y) = \lambda x + \lambda y.$

Bevis. Den 3. regel udsiger, at afbildningen $\pi_\lambda : x \mapsto \lambda x$ er en endomorfi, altså at $\pi_\lambda \in End(M)$, og den 1. og 2. regel udsiger, at afbildningen $\lambda \mapsto \pi_\lambda$ er additiv og multiplikativ $: \mathbf{Q} \to End(M)$ ♠

(3.7) En multiplikativt skrevet gruppe $(M, \cdot)$ er entydigt delelig, hvis der for alle $a \in M$ og $n \in \mathbf{N}$ gælder, at ligningen

$$x^n = a$$

har en og kun én løsning $x \in M$. For en sådan gruppe betegner vi naturligvis med x^λ den λ'te potens af x, og potensreglerne er her:

$$x^{\lambda+\mu} = x^\lambda x^\mu, \quad x^{\lambda\mu} = (x^\lambda)^\mu, \quad (xy)^\lambda = x^\lambda y^\lambda.$$

(3.8) Observation. For et element b i en entydigt delelig, kommutativ gruppe $(M, +)$ og et rationalt tal $\lambda = p/n$, hvor $p \in \mathbf{Z}$ og $n \in \mathbf{N}$, er potensen $x := (p/n)b$ bestemt som den entydige løsning til ligningen $nx = pb$,
thi $n((p/n)b) = (n(p/n))b = pb$.

Potenssætning. *Lad a være et element i en entydigt delelig, kommutativ gruppe $(M, +)$. Da findes netop én gruppehomomorfi $: (\mathbf{Q}, +) \to (M, +)$ så at $1 \mapsto a$, nemlig afbildningen $\lambda \mapsto \lambda a$.*

Bevis. Den 1. Potensregel (i forbindelse med at $1a = a$) udsiger, at afbildningen $\lambda \mapsto \lambda a$ opfylder de stillede krav. Er omvendt $\varphi : \mathbf{Q} \to M$ en afbildning, der opfylder de stillede krav, følger det af Potenssætningen for hele tal, at vi har

$$\varphi(p) = pa \quad \text{for alle } p \in \mathbf{Z}.$$

For en brøk $\lambda = p/n$, hvor $p \in \mathbf{Z}$ og $n \in \mathbf{N}$ får vi derfor, at

$$n\varphi(p/n) = \varphi(n(p/n)) = \varphi(p) = pa.$$

Og så er $\varphi(p/n) = (p/n)a$ ♠

FØLGER, FULDSTÆNDIGHED ORDNING, KONTINUITET DE REELLE TAL

1. Fundamentalfølger. Fuldstændighed.

(1.1) Definitioner. I det følgende betragter vi en kommutativ, ordnet gruppe G. Vi vil sædvanligvis skrive kompositionen additivt, og udførligt for G skrive $(G, +, <)$. Ved en *følge* i G forstås som bekendt en afbildning $\alpha : \mathbf{N} \to G$. Følgen betegnes ofte $n \mapsto \alpha_n$ eller $(\alpha_1, \alpha_2, \dots)$ eller blot (α_n). Specielle følger en de *konstante* følger $(a, a, \dots)$, hvor a er et element i G. Ved en *delfølge* af følgen $\alpha : \mathbf{N} \to G$ forstås som bekendt en følge af formen $\alpha \circ j$, hvor $j : \mathbf{N} \to \mathbf{N}$ er en strengt voksende afbildning (dvs. en homomorfi: $(\mathbf{N}, <) \to (\mathbf{N}, <)$). Delfølgen $\alpha \circ j$ kan betegnes $(\alpha_{j_1}, \alpha_{j_2}, \dots)$ eller (α_{j_n}).

Følgen $\alpha = (\alpha_n)$ kaldes *voksende*, hvis α er en homomorfi $\alpha : (\mathbf{N}, \leq) \to (G, \leq)$, altså hvis

$$\alpha_1 \leq \alpha_2 \leq \cdots .$$

Tilsvarende defineres *aftagende*. Som fælles betegnelse bruges *monoton*.

Følgen $\alpha = (\alpha_n)$ kaldes *begrænset*, hvis der findes elementer $C_1, C_2 \in G$, således at

$$C_1 \leq \alpha_n \leq C_2 \qquad \text{for alle } n \in \mathbf{N}.$$

Følgen $\alpha = (\alpha_n)$ siges at have *grænseværdien* a (hvor a er et element i G) eller at *konvergere* mod a, hvis der til hvert $\varepsilon > 0$ i G findes et naturligt tal N, således at der for alle naturlige tal $n \geq N$ gælder $|\alpha_n - a| < \varepsilon$, altså hvis

$$\forall \varepsilon \in G_+ \exists N \in \mathbf{N} \forall n \in \mathbf{N} : n \geq N \Rightarrow |\alpha_n - a| < \varepsilon.$$

En følge, der har en grænseværdi, kaldes *konvergent*. En følge, der konvergerer mod 0, kaldes en *nulfølge*.

Bemærkning. Et udsagn af formen:

$$\exists N \in \mathbf{N} \forall n \in \mathbf{N} : n \geq N \Rightarrow p(n),$$

hvor $p(n)$ er et udsagn om det naturlige tal n (et prædikat) skrives ofte: "fra et vist trin gælder $p(n)$" eller "for næsten alle n gælder $p(n)$" eller "på nær for endelig mange n gælder $p(n)$". Negationen af et sådant udsagn, altså udsagnet:

$$\forall N \in \mathbf{N} \exists n \in \mathbf{N} : n \geq N \wedge \ \text{non}\, p(n)$$

kan skrives "for uendelig mange n gælder $\operatorname{non} p(n)$". Det betyder, at der findes naturlige tal $j_1 < j_2 < \cdots$, således at $\operatorname{non} p(j_n)$ gælder for alle n.

En følge $\alpha = (\alpha_n)$ kaldes en *fundamentalfølge* (eller en *Cauchy-følge*), hvis

$$\forall \varepsilon \in G_+ \exists N \in \mathbf{N} \forall n, m \in \mathbf{N} : n, m \geq N \Rightarrow |\alpha_n - \alpha_m| < \varepsilon.$$

(1.2) Den ordnede gruppe $(G, +, <)$ kaldes *diskret ordnet*, hvis der findes et første element i G_+ (et mindste positivt element). I meget af det følgende vil dette tilfælde kræve en helt triviel særbehandling, som vi oftest udelader. For en følge $\alpha = (\alpha_n)$ i en diskret ordnet gruppe $(G, +, <)$ gælder:

$$\begin{aligned}(\alpha \text{ er en fundamentalfølge }) &\iff (\alpha \text{ er konvergent}) \\ &\iff (\alpha \text{ er konstant fra et vist trin}).\end{aligned}$$

Dette fås ved at anvende definitionerne med $\varepsilon :=$ mindste positive element i G.

En ordnet gruppe $(G, +, <)$, som ikke er diskret ordnet, siges at være *tæt ordnet*. I en sådan gruppe kan vi til hvilkesomhelst to elementer $a', a'' \in G$ med $a' < a''$ finde et $a \in G$, således at $a' < a < a''$, thi da $a'' - a' \in G_+$ ikke er det mindste positive element, findes et element $\delta \in G_+$ således at $\delta < a'' - a'$. Af $0 < \delta < a'' - a'$ følger nu, at $a' < a' + \delta < a''$. Videre gælder, at vi i en tæt ordnet gruppe $(G, +, <)$ til et givet $\varepsilon > 0$ og et givet $k \in \mathbf{N}$ kan bestemme et $\varepsilon' > 0$, således at

$$0 < k\varepsilon' < \varepsilon,$$

thi vi kan successivt bestemme $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k \in G_+$, således at $0 < \varepsilon_1 < \varepsilon$, $0 < \varepsilon_2 < \varepsilon_1$, $\ldots$, $0 < \varepsilon_k < \varepsilon_{k-1}$. Er ε' det mindste blandt ε_k, $\varepsilon_{k-1} - \varepsilon_k$, $\ldots$, $\varepsilon_1 - \varepsilon_2$, så finder vi:

$$0 < k\varepsilon' = \varepsilon' + \cdots + \varepsilon' \leq (\varepsilon_1 - \varepsilon_2) + \cdots + (\varepsilon_{k-1} - \varepsilon_k) + \varepsilon_k = \varepsilon_1 < \varepsilon.$$

Eksempel. Gruppen $(\mathbf{Z}, +, <)$ er diskret ordnet. Gruppen $(\mathbf{Q}, +, <)$ er tæt ordnet.

(1.3) Bemærkning. Betragt en ordnet gruppe $(G, +, <)$, der har følgende egenskab:

(†) Enhver nulfølge i G er konstant (nødvendigvis $= 0$) fra et vist trin.

For følger $\alpha = (\alpha_n)$ i en sådan gruppe finder vi også:

$$\begin{aligned}(\alpha \text{ er en fundamentalfølge }) &\iff (\alpha \text{ er konvergent}) \\ &\iff (\alpha \text{ er konstant fra et vist trin}).\end{aligned}$$

Det er ikke oplagt, at der findes tæt ordnede grupper, der har egenskaben (†).

(1.4) Af definitionerne følger en række elementære:
SÆTNINGER.
En konvergent følge har netop én grænseværdi.
En konvergent følge er en fundamentalfølge.
En fundamentalfølge er begrænset.

Bevis. Idéerne er velkendte. Lad os f.eks. vise, at en konvergent følge $\alpha = (\alpha_n)$ er en fundamentalfølge: Lad $\varepsilon > 0$ være givet. Vi kan antage, at ordningen er tæt, og kan derfor bestemme $\varepsilon' > 0$, så at $2\varepsilon' \leq \varepsilon$. Da følgen har en grænseværdi $a \in G$, kan vi til dette ε' bestemme $N \in \mathbf{N}$, således at $|\alpha_n - a| < \varepsilon'$ for alle $n \leq N$. For alle $n, m \geq N$ finder vi nu:

$$\begin{aligned} |\alpha_n - \alpha_m| &= |(\alpha_n - a) + (a - \alpha_m)| \leq |\alpha_n - a| + |\alpha_m - a| \\ &< \varepsilon' + \varepsilon' \leq \varepsilon \quad \heartsuit \end{aligned}$$

(1.5) NOTATION. Med $\mathcal{F}(G)$ betegner vi mængden af følger i den ordnede gruppe $(G, +, <)$. I mængden $\mathcal{F}(G)$ defineres en komposition $+$ ved "argumentvis addition": Summen $\alpha + \beta = (\alpha_n + \beta_n)$ er følgen $n \mapsto \alpha_n + \beta_n$. Det er klart, at $(\mathcal{F}(G), +)$ er en kommutativ gruppe. I $\mathcal{F}(G)$ betegner vi med $\mathcal{BF}(G)$, $\mathcal{FF}(G)$, $\mathcal{KF}(G)$ og $\mathcal{NF}(G)$ delmængderne bestående af **b**egrænsede **f**ølger, **f**undamental**f**ølger, **k**onvergente **f**ølger og **n**ul**f**ølger.

SÆTNING. *Delmængderne $\mathcal{BF}(G)$, $\mathcal{FF}(G)$, $\mathcal{KF}(G)$ og $\mathcal{NF}(G)$ er undergrupper i $(\mathcal{F}(G), +)$ og der gælder:*

$$\mathcal{F}(G) \supseteq \mathcal{BF}(G) \supseteq \mathcal{FF}(G) \supseteq \mathcal{KF}(G) \supseteq \begin{cases} \mathcal{NF}(G) \\ \{\textit{konstante følger}\}. \end{cases}$$

Bevis. Lad os nøjes med at vise, at summen $\alpha+\beta = (\alpha_n+\beta_n)$ af to fundamentalfølger $\alpha = (\alpha_n)$ og $\beta = (\beta_n)$ igen er en fundamentalfølge: Lad $\varepsilon > 0$ være givet. Vi kan antage, at ordningen er tæt, og kan derfor bestemme $\varepsilon' > 0$, således at $2\varepsilon' \leq \varepsilon$. Til dette ε' kan vi bestemme $N_1, N_2 \in \mathbf{N}$, så at

$$\begin{aligned} |\alpha_n - \alpha_m| &< \varepsilon' \qquad \text{for alle } n, m \geq N_1 \text{ og} \\ |\beta_n - \beta_m| &< \varepsilon' \qquad \text{for alle } n, m \geq N_2. \end{aligned}$$

Vi sætter $N := \max\{N_1, N_2\}$. For alle $n, m \geq N$ er da begge ovenstående uligheder opfyldt, og vi får:

$$\begin{aligned} |(\alpha_n + \beta_n) - (\alpha_m + \beta_m)| &\leq |\alpha_n - \alpha_m| + |\beta_n - \beta_m| \\ &< \varepsilon' + \varepsilon' \leq \varepsilon. \end{aligned}$$

Følgelig er summen $\alpha + \beta$ er fundamentalfølge ♡

I beviset for at $\mathcal{KF}(G)$ er en undergruppe i $(\mathcal{F}(G), +)$ viser man mere præcist, at hvis følgerne $\alpha = (\alpha_n)$ og $\beta = (\beta_n)$ har grænseværdierne a og b, så har sumfølgen $\alpha+\beta = (\alpha_n+\beta_n)$ (resp. den modsatte følge $-\alpha = (-\alpha_n)$) grænseværdien $a+b$ (rexp. $-a$). Idet vi for en konvergent følge $\alpha = (\alpha_n)$ med $\lim \alpha$ (eller $\lim_{n\to\infty} \alpha_n$) betegner følgens entydigt bestemte grænseværdi, får vi: *Afbildningen* lim *er en homomorfi* : $(\mathcal{KF}(G), +) \to (G, +)$. Kernen for lim er øjensynlig undergruppen $\mathcal{NF}(G)$ af nulfølger.

(1.6) I analogi med et velkendt begreb inden for læren om metriske rum indfører vi følgende:

DEFINITION. En kommutativ ordnet gruppe $(G, +, <)$ kaldes *fuldstændig*, hvis enhver fundamentalfølge i G er konvergent. Dette betyder altså, at $\mathcal{FF}(G) = \mathcal{KF}(G)$.

En diskret ordnet gruppe $(G, +, <)$, som f.eks. $(\mathbf{Z}, +, <)$, er fuldstændig. Mere generelt: En ordnet gruppe $(G, +, <)$, der opfylder betingelsen (†) i (1.3), er fuldstændig.

Derimod er $(\mathbf{Q}, +, <)$ ikke fuldstændig. F.eks. er følgen $n \mapsto \sum_{v=1}^{n} 2^{-v^2}$ en ikkekonvergent fundamentalfølge i $\mathbf{Q}$.

En ifølge ovenstående definition fuldstændig kommutativ ordnet gruppe kan mere præcist kaldes *følgefuldstændig*.

2. Følgekompletion.

(2.1) Vi betragter stadig en kommutativ ordnet gruppe $(G, +, <)$, og vi vil vise, at vi på "fornuftig" måde kan indlejre $(G, +, <)$ i en fuldstændig kommutativ ordnet gruppe $(\widehat{G}, +, <)$, kaldet kompletionen af G.

DEFINITION. To følger $\alpha = (\alpha_n)$ og $\beta = (\beta_n)$ i G kaldes *ækvivalente*, og vi skriver $\alpha \equiv \beta$, hvis differensfølgen $\alpha - \beta = (\alpha_n - \beta_n)$ er en nulfølge.

SÆTNING. *Relationen $\equiv$ er en kongruensrelation i gruppen $(\mathcal{F}(G), +)$ af alle følger i G.*

Dette betyder, at relationen $\equiv$ er en ækvivalensrelation i $\mathcal{F}(G)$, og at den harmonerer med kompositionen $+$ i $\mathcal{F}(G)$.

Bevis. For to følger $\alpha = (\alpha_n)$ og $\beta = (\beta_n)$ har vi ifølge definitionen:

$$\alpha \equiv \beta \iff \alpha - \beta \in \mathcal{NF}(G).$$

Heraf følger påstanden, da $\mathcal{NF}(G)$ er en undergruppe i $(\mathcal{F}(G), +)$ ♠

(2.2) Relationen $\equiv$ definerer specielt en kongruensrelation i hver af undergrupperne $\mathcal{BF}(G)$, $\mathcal{FF}(G)$ og $\mathcal{KF}(G)$. Da disse undergrupper indeholder $\mathcal{NF}(G)$, får vi endvidere følgende:

SÆTNING. *En følge $\alpha = (\alpha_n)$ i G, der er ækvivalent med en begrænset følge (resp. fundamentalfølge, resp. konvergent følge, resp. nulfølge), er selv en begrænset følge (resp. fundamentalfølge, resp. konvergent følge, resp. nulfølge)*

Bevis. Vi kan nemlig skrive $\alpha = \alpha' + \nu$, hvor α' er en begrænset følge (resp. ...) og ν er en nulfølge. Her er ν specielt en begrænset følge (resp. ...), og $\alpha = \alpha' + \nu$ er således sum af to begrænsede følger (resp. ...) og dermed selv en begrænset følge (resp. ...) ♠

(2.3) Det er klart, at en følge $\alpha = (\alpha_n)$ i G er konvergent, hvis og kun hvis den er ækvivalent med en konstant følge. Mere præcist: Følgen $\alpha = (\alpha_n)$ har grænseværdien a, hvis og kun hvis den er ækvivalent med den konstante følge $(a, a, \ldots)$.

Vi vil ofte udnytte "kun hvis"-delen af følgende:

SÆTNING. *En følge $\alpha = (\alpha_n)$ i G er en fundamentalfølge, hvis og kun hvis den er ækvivalent med enhver af sine delfølger.*

Bevis. **"kun hvis"** følger umiddelbart af definitionerne, idet vi bemærker, at der for en delfølge (α_{j_n}) af (α_n) gælder $j_n \geq n$. Hvis $|\alpha_n - \alpha_m| < \varepsilon$ for alle $n, m \geq N$, så er altså specielt $|\alpha_n - \alpha_{j_n}| < \varepsilon$ for alle $n \geq N$.

"hvis": Antag omvendt, at følgen $\alpha = (\alpha_n)$ ikke er en fundamentalfølge. Idet vi "negerer definitionen", ser vi, at der findes et $\delta > 0$, således at

$$\forall K \in \mathbf{N} \exists j, k \in \mathbf{N} : j, k \geq K \wedge |\alpha_j - \alpha_k| \geq \delta.$$

For $K = 1$ kan vi altså finde $j_1, k_1 \geq 1$, så at $|\alpha_{j_1} - \alpha_{k_1}| \geq \delta$. Vælger vi nu et $K = K_2 > j_1, k_1$, kan vi finde $j_2, k_2 \geq K_2$, således, at $|\alpha_{j_2} - \alpha_{k_2}| \geq \delta$. Dernæst vælger vi et $K_3 > j_2, k_2$ og finder $j_3, k_3 \geq K_3$ så at $|\alpha_{j_3} - \alpha_{k_3}| \geq \delta$. Idet vi fortsætter således, finder vi $j_1 < j_2 < j_3 < \dots$ og $k_1 < k_2 < k_3 < \cdots$, som opfylder:

$$|\alpha_{j_n} - \alpha_{k_n}| \geq \delta \qquad \text{for alle } n \in \mathbf{N}.$$

Delfølgerne (α_{j_n}) og (α_{k_n}) er derfor ikke ækvivalente og kan derfor ikke begge være ækvivalente med α ♠

KOROLLAR. *En fundamentalfølge, der har en konvergent delfølge, er selv konvergent (med samme grænseværdi).*

Devis. Fundamentalfølgen er i så fald ækvivalent med en delfølge, der er ækvivalent med en konstant følge $(a, a, \dots)$ ♠

(2.4) NOTATION. Vi betragter nu specielt gruppen $(\mathcal{FF}(G), +)$ af fundamentalfølger i G, og kongruensrelationen $\equiv$ heri. Kvotienten $(\mathcal{FF}(G), +)/\equiv$, som jo er kvotientgruppen $\mathcal{FF}(G)/\mathcal{NF}(G)$, betegner vi $(\widehat{G}, +)$. Elementerne i $\widehat{G}$ er ækvivalensklasser mht. $\equiv$. Ækvivalensklassen, der indeholder fundamentalfølgen α, betegnes $\boxed{\alpha}$. Kompositionen $+$ i $\widehat{G}$ er bestemt ved, at

$$\boxed{\alpha} + \boxed{\beta} = \boxed{\alpha + \beta}.$$

Som kvotient af en kommutativ gruppe er $(\widehat{G}, +)$ igen en kommutativ gruppe, og afbildningen $\alpha \mapsto \boxed{\alpha}$ er en homomorfi : $(\mathcal{FF}(G), +) \to (\widehat{G}, +)$.

(2.5) NOTATION. For et element $a \in G$ betegner vi med $\hat{a} \in \widehat{G}$ den ækvivalensklasse, der indeholder den konstante følge $(a, a, a, \dots)$. Det er klart, at der ved $a \mapsto \hat{a}$ defineres en injektiv homomorfi:

$$(G, +) \hookrightarrow (\widehat{G}, +)$$

Vi vil oftest indentificere elementerne i G med deres billeder i $\widehat{G}$ ved denne homomorfi, og altså opfatte G som en undergruppe: $G \subseteq \widehat{G}$.

BEMÆRKNING. Opfattet som delmængde af $\mathcal{FF}(G)$ består ækvivalensklassen $\hat{a}$ øjensynlig af de følger, der konvergerer mod a.

(2.6) Vi vil nu udvide ordningen i G til en ordning i $\widehat{G}$:

DEFINITION. Idet vi med $P \subseteq \widehat{G}$ betegnes delmængden bestående af de elementer $A \neq 0$ i $\widehat{G}$, der har en repræsentant $\alpha = (\alpha_n)$, for hvilken der gælder:

$$\alpha_n \geq 0 \quad \text{for alle } n \in \mathbf{N},$$

defineres en relation $<$ i $\widehat{G}$ ved:

$$X < Y \overset{DEF}{\iff} Y - X \in P.$$

SÆTNING. *Med den ovenfor definerede relation $<$ er $(\widehat{G}, +, <)$ en ordnet gruppe, hvis positive elementer er elementerne i P. Afbildningen $a \mapsto \hat{a}$ er en homomorfi:*

$$(G, +, <) \hookrightarrow (\widehat{G}, +, <).$$

Bevis. Ifølge et generelt resultat om ordnede grupper skal vi om $P \subseteq \widehat{G}$ vise, at $0 \notin P$, at P er stabil, og at der for hvert $X \neq 0$ i $\widehat{G}$ gælder: $X \in P$ eller $-X \in P$. Det første er klart ifølge definitionen. For at vise, at P er stabil, vælges for elementer $A, B \in P$ repræsentanter: $A = \boxed{\alpha}$ og $B = \boxed{\beta}$, så at $\alpha_n \geq 0$ og $\beta_n \geq 0$ for alle n. Da er $\alpha + \beta$ en repræsentant for $A + B$ med $\alpha_n + \beta_n \geq 0$ for alle n, og $A + B \in P$, thi ellers var $A + B = 0$, og altså $\alpha + \beta = (\alpha_n + \beta_n)$ en nulfølge, og så kunne vi af:

$$0 \leq \alpha_n \leq \alpha_n + \beta_n$$

slutte, at også $\alpha = (\alpha_n)$ var en nulfølge, i modstrid med at $\boxed{\alpha} = A \neq 0$.

Betragt videre et element $X \neq 0$ i $\widehat{G}$, og vælg en repræsentant: $X = \boxed{\xi}$. Da gælder: **Enten** er $\xi_n \leq 0$ for uendelig mange n. I så fald har $\xi = (\xi_n)$ en delfølge, hvis elementer alle er ≥ 0, og da denne delfølge ifølge Korollar (2.3) også er repræsentant for X, ser vi, at $X \in P$. **Eller** også er $\xi_n < 0$ fra et vist trin. Da følgen $-\xi = (-\xi_n)$ er en repræsentant for $-X$, hvis elementer er ≥ 0 (endda > 0) fra et vist trin, ser vi tilsvarende, at vi i så fald har $-X \in P$.

Sætningens sidste påstand følger let af definitionen på ordningen i $\widehat{G}$ ♠

(2.7) Det følger af definitionen, at den herved definerede ordning i $\widehat{G}$ på gruppen G opfattet som delmængde $G \subseteq \widehat{G}$ stemmer overens med den givne ordning i G.

DEFINITION. Den ovenfor konstruerede kommutative ordnede gruppe $(\widehat{G}, +, <)$, indeholdende $(G, +, <)$, kaldes *kompletionen* (mere præcist: *følgekompletionen*) af $(G, +, <)$.

Hvis $(G, +, <)$ er fuldstændig, så er $G = \widehat{G}$. Som vi om lidt skal se, er $(\widehat{G}, +, <)$ altid fuldstændig.

(2.8) Observation. Hvis $\alpha = (\alpha_n)$ og $\beta = (\beta_n)$ er fundamentalfølger i G, således at

$$\alpha_n \leq \beta_n \quad \text{for uendelig mange } n,$$

så er

$$\boxed{\alpha} \leq \boxed{\beta} \quad \text{i gruppen } \widehat{G},$$

thi $\boxed{\beta} - \boxed{\alpha} = \boxed{\beta - \alpha}$ har da en repræsentant, nemlig en delfølge af differensfølgen $\beta - \alpha = (\beta_n - \alpha_n)$, hvis elementer alle er ≥ 0, så vi slutter, at $\boxed{\beta} - \boxed{\alpha} = 0$ eller at $\boxed{\beta} - \boxed{\alpha} \in P$.

(2.9) Sætning. *Til hvert element $E \in \widehat{G}_+$ findes et element $\varepsilon \in G_+$, så at $0 < \hat{\varepsilon} \leq E$.*

Bevis. Da $E \in \widehat{G}_+ = P$, har E en repræsentant $\alpha = (\alpha_n)$, så at $\alpha_n \geq 0$ for alle n. Da $E \neq 0$, er α ikke en nulfølge, så der findes i G et $\varepsilon > 0$, så at

$$\varepsilon \leq \alpha_n \quad \text{for uendelig mange } n.$$

Anvendes Observation (2.8) på følgen $\alpha = (\alpha_n)$ og den konstante følge $(\varepsilon, \varepsilon, \varepsilon, \dots)$, får vi i $\widehat{G}$, at $0 < \hat{\varepsilon} \leq \boxed{\alpha} = E$ ♠

Bemærkning. Heraf ses, at hvis en følge $\alpha = (\alpha_n)$ i G har en af egenskaberne 'fundamentalfølge', 'konvergent mod a', 'nulfølge', så vil den opfattet som følge i G have samme egenskab. Derimod kan en følge $\alpha = (\alpha_n)$ i G godt være konvergent i $\widehat{G}$ uden at den er konvergent i G, idet grænseværdien ikke nødvendigvis tilhører G.

(2.10) Sætning. *Lad $\alpha = (\alpha_n)$ være en fundamentalfølge i G. Da er følgen $(\hat{\alpha}_n)$ i $\widehat{G}$ konvergent med grænseværdien $\boxed{\alpha}$.*

Bevis. Ifølge Sætning (2.9) er det nok at vise, at der for ethvert $\varepsilon \in G_+$ findes $N \in \mathbf{N}$, så at

$$\left|\hat{\alpha}_n - \boxed{\alpha}\right| < \hat{\varepsilon} \quad \text{for alle } n \geq N.$$

Da $\alpha = (\alpha_n)$ er en fundamentalfølge, kan vi til det givne $\varepsilon \in G_+$ finde $N \in \mathbf{N}$, således at vi for $n, m \geq N$ har:

$$-\varepsilon < \alpha_n - \alpha_m < \varepsilon.$$

For et fast $n \geq N$ gælder disse uligheder specielt for uendelig mange m, og anvendes Observation (2.8) på følgen $(\alpha_n - \alpha_1, \alpha_n - \alpha_2, \alpha_n - \alpha_3, \dots)$ og de konstante følger $(-\varepsilon, -\varepsilon, -\varepsilon, \dots)$ og $(\varepsilon, \varepsilon, \varepsilon, \dots)$, så får vi i $\widehat{G}$:

$$-\hat{\varepsilon} \leq \hat{\alpha}_n - \boxed{\alpha} \leq \hat{\varepsilon}.$$

Altså har vi:

$$\left|\hat{\alpha}_n - \boxed{\alpha}\right| \leq \hat{\varepsilon} \text{ for alle } n \leq N.$$

Dette er den søgte ulighed, blot med '$\leq$' i stedet for '$<$'. Hvis G er tæt ordnet, er dette tilstrækkeligt. Og hvis G er diskret ordnet, er Sætningen triviel ♠

BEMÆRKNING. Herefter vil vi altid indentificere elementer $a \in G$ med deres billeder $\hat{a} \in \widehat{G}$, og altså opfatte G som en delmængde $G \subseteq \widehat{G}$.

(2.11) Vi kan nu vise følgende:
SÆTNING. *For kompletionen* $(\widehat{G}, +, <) \subseteq (G, +, <)$ *gælder:*

(1) *Enhver fundamentalfølge i* G *er konvergent i* $\widehat{G}$.
(2) *Ethvert element i* $\widehat{G}$ *er grænseværdi for en følge i* G.
(3) *Den ordnede gruppe* $(\widehat{G}, +, <)$ *er fuldstændig.*

Bevis. Påstandene (1) og (2) er begge indeholdt i den foregående sætning. Lad os vise, at (3) er en konsekvens af (1) og (2): Hvis $(\widehat{G}, +, <)$ har egenskaben (†) i (1.3), altså hvis enhver nulfølge i $\widehat{G}$ er $= 0$ fra et vist trin, så er påstanden triviel. Vi kan derfor antage, at der i $\widehat{G}$ findes en nulfølge, som indeholder uendelig mange elementer $\neq 0$. Ved først at udvælge en delfølge heraf, og ved dernæst at betragte absolutværdien af dennes elementer, ser vi, at der findes en nulfølge (Δ_n) i $\widehat{G}$ bestående af elementer $\Delta_n \in \widehat{G}_+$.

Lad nu (A_n) være en fundamentalfølge i $\widehat{G}$. For hvert $n \in \mathbf{N}$ er A_n ifølge (2) grænseværdi for en følge i G, så vi kan specielt bestemme et element α_n i G, således at $|A_n - \alpha_n| < \Delta_n$. Herved får vi en følge (α_n) med elementer i G, således at vi i $\widehat{G}$ har :

$$|A_n - \alpha_n| < \Delta_n \quad \text{for alle } n.$$

Heraf slutter vi, at følgerne (A_n) og (α_n) er ækvivalente følger i $\widehat{G}$. Da (A_n) var en fundamentalfølge i $\widehat{G}$, er også (α_n) en fundamentalfølge i $\widehat{G}$. Heraf følger imidlertid, at (α_n) er en fundamentalfølge i G, og da (1) gælder, må (α_n) være en konvergent følge i $\widehat{G}$. Da (A_n) og (α_n) var ækvivalente følger i $\widehat{G}$, er også (A_n) en konvergent følge i $\widehat{G}$ ♠

(2.12) Kompletionen af $(\mathbf{Z}, +, <)$ er $(\mathbf{Z}, +, <)$, da $(\mathbf{Z}, +, <)$ er diskret ordnet og dermed fuldstændig.

Kompletionen af $(\mathbf{Q}, +, <)$ er de reelle tals ordnede gruppe $(\mathbf{R}, +, <)$, som vi senere skal se nærmere på.

INDEX

MAT 2AL

1987–88

l

m

r

s

t