MATEMATIK 2AL

Noter af Jørn Børling Olsson
1990-1992

Indhold:

Kapitel 0. Lidt om mængder og afbildninger.

(Kan med fordel læses efter Kapitel 1 og 2.)

De matematiske discipliner er baserede på et vist mængdeteoretisk grundlag. I princippet burde dette grundlag være helt afklaret før man starter på en fremstilling af matematik. Paradoksalt nok kan man imidlertid have svært ved at værdsætte eller bare forstå en stringent fremstilling af det mængdeteoretiske grundlag uden at have en vis matematisk modenhed. Begynderen i matematik opnår hurtigt en intuitiv opfattelse af, hvad det drejer sig om. Man "ved", hvad en mængde M er, og hvad udsagnet "$x \in M$" (x er element i mængden M) betyder. Man illustrerer de mængdeteoretiske operationer $\cup$ (foreningsmængde), $\cap$ (fællesmængde), $\setminus$ (differensdannelse), $\times$ (kartesisk produkt) m.fl. ved hjælp af diagrammer og eksempler og indfører skrivemåden

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

hvor $p(x)$ er et udsagn, der specificerer en mængde M's elementer. Den intuitive opfattelse kan være tilstrækkelig et stykke ad vejen, men der kommer et punkt (også i dette kursus), hvor man er nødt til at tænke lidt mere over grundlaget. Det drejer sig her især om anvendelsen af "Zorns lemma" [ZL], der egentlig ikke er noget lemma (= hjælpesætning), men ækvivalent til et aksiom i mængdelæren, udvalgsaksiomet [UA].

Et sæt af aksiomer for mængdelæren blev opstillet af Zermelo & Fraenkel, og det er beskrevet i forskellige lærebøger. Vi vil her ikke beskæftige os med det, men derimod lede op til formuleringen af [UA] ved at beskæftige os lidt med afbildinger.

(0.1) DEFINITION: Lad A, B være mængder og $f : A \to B$ en afbildning. f kaldes

- *injektiv*, hvis der gælder:
  For alle $x, x' \in A$ gælder $f(x) = f(x') \Rightarrow x = x'$.
- *surjektiv*, hvis der gælder:
  For alle $y \in B$ findes et $x \in A$ så $f(x) = y$.
- *bijektiv*, hvis f er injektiv og surjektiv.

□

Den *identiske afbildning* på en mængde A betegnes 1_A. Der gælder altså $1_A(x) = x$ for alle $x \in A$. Hvis $f : A \to B$, $g : B \to C$ er afbildningen betegner $g \circ f$ sammensætningen af f og g. Så $g \circ f : A \to C$ er fastlagt ved $(g \circ f)(x) = g(f(x))$.

(0.2). DEFINITION: Lad A, B være mængder og $f : A \to B$, $g : B \to A$ afbildninger. g kaldes

- *venstreinvers til* f, hvis $g \circ f = 1_A$.
- *højreinvers til* f, hvis $f \circ g = 1_B$.
- *invers til* f, hvis $g \circ f = 1_A$ og $f \circ g = 1_B$, (og så skrives $g = f^{-1}$).

□

(0.3) ØVELSE: Lad $f : A \to B$ være en afbildning. Vis:

(1) Hvis der findes en venstreinvers afbildning til f, så er f injektiv.
(2) Hvis der findes en højreinvers afbildning til f, så er f surjektiv.
(3) Hvis der findes en invers afbildning til f, så er f bijektiv.

□

Det er ikke svært at se, at de "omvendte" udsagn til (0.3) (1) og (0.3) (3) gælder:

(0.4) SÆTNING. *Lad $f : A \to B$ være en afbildning, $A \neq \emptyset$.*

(1) *Hvis f er injektiv, findes der en venstreinvers afbildning g til f.*
(3) *Hvis f er bijektiv, findes der en invers afbildning g til f.*

Før beviset af (0.4) anfører vi følgende notation og bemærkninger:

For $y \in B$ er $f^{-1}(y) = \{x \in A \mid f(x) = y\}$. Denne delmængde af A er *urbilledet* af y under f. Bemærk følgende: f er injektiv hvis og kun hvis der gælder: For alle $y \in B$ består $f^{-1}(y)$ højst af 1 element. (Overvej!)

Vi sætter

$$f(A) = \{y \in B \mid \text{Der findes et } x \in A \text{ så } f(x) = y\}.$$

Dette er f's *billedmængde*. Bemærk følgende: f er surjektiv hvis og kun hvis $f(A) = B$. (Overvej!)

BEVIS FOR (0.4): (1) Da $A \neq \emptyset$ (den tomme mængde) kan vi vælge et element $z \in A$. Lad $y \in B$. Hvis $y \notin f(A)$, sætter vi $g(y) = z$. Hvis $y \in f(A)$, findes et element $x \in A$ med $f(x) = y$. Da f er injektiv, er x det eneste element i A med $f(x) = y$. Vi sætter $g(y) = x$ i dette tilfælde. Hermed er $g : B \to A$ defineret. Hvis $x \in A$, er $y = f(x) \in f(A)$ og dermed $g(y) = x$ ifølge definitionen af g. Så er $(g \circ f)(x) = g(f(x)) = g(y) = x = 1_A(x)$. Vi har vist $g \circ f = 1_A$, så g er venstreinvers til f.

(3) Hvis f er bijektiv (altså injektiv og surjektiv) er det ikke svært at se, at afbildningen g, beskrevet i (1) er invers til f: Vi ved allerede at $g \circ f = 1_A$. Hvis $y \in B$, er $y \in f(A)$ $(f(A) = B$ da f er surjektiv). Lad $x \in A$ opfylde $f(x) = y$. Ifølge definitionen af g er $g(y) = x$. Dermed er $(f \circ g)(y) = f(g(y)) = f(x) = y$, så $f \circ g = 1_B$. □

Det viser sig, måske lidt overraskende, at beviset for det udsagn, vi vil kalde (0.4)(2) ("Hvis f er surjektiv, findes der en højreinvers afbildning g til f"), må baseres på udvalgsaksiomet, som vi nu præsenterer.

Når A er en mængde, betegner $\mathcal{P}(A)$ A's potensmængde (altså mængden af delmængder af A, se også (1.2)(1)). Her er udvalgsaksiomet:

[UA]. Lad A, B være mængder. Lad der være givet en afbildning $p : B \to \mathcal{P}(A)$ således at der for alle $y \in B$ gælder at $p(y) \neq \emptyset$, (altså at delmængden $p(y)$ af A ikke er tom). Så findes der en afbildning $g : B \to A$ således at $g(y) \in p(y)$ for alle $y \in B$.

Efter lidt overvejelse vil man måske finde udsagnet [UA] rimeligt (altså at man i en "samling" af ikke tomme mængder kan "udvælge" et element i hver af disse). Men når man ser de udsagn, der kan udledes fra [UA], f.eks. [ZL] lidt senere, vil det være klart, at [UA] ikke er helt så harmløst, som det ser ud. Vi vil, som man også almindeligvis gør, antage at [UA] gælder og bevise

(0.4) SÆTNING. *Lad $f : A \to B$ være en afbildning. (2) Hvis f er surjektiv findes der en højreinvers afbildning g til f.*

BEVIS: Vi definerer en afbildning $p : B \to \mathcal{P}(A)$ ved $p(y) = f^{-1}(y)$ for alle $y \in B$. Hvis $y \in B$ findes der, da f er surjektiv, et $x \in A$ med $f(x) = y$. Dermed er $x \in f^{-1}(y) = p(y)$, så $p(y) \neq \emptyset$. Ifølge [UA] anvendt på A, B og p findes der $g : B \to A$, så $g(y) \in p(y) = f^{-1}(y)$ for alle $y \in B$. Da $g(y) \in f^{-1}(y)$ er $f(g(y)) = y$. Dermed er $f \circ g = 1_B$, så g er højreinvers til f. □

Lad os nævne en variant af [UA], som er nemmere at formulere (og huske?)

[UA]* Lad A være en mængde. Der findes en (udvalgs-)funktion

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

således at der gælder:

$$\text{For alle} \quad X \in \mathcal{P}(A), X \neq \emptyset, \quad \text{er} \quad u(X) \in X.$$

(0.5) ØVELSE: Vis, at udsagnene [UA] og [UA]* er ensbetydende. □

(0.6) ØVELSE: Betragt funktionerne $f_1, f_2, f_3 : \mathbb{N} \to \mathbb{N}$ defineret nedenfor. Overvej om de er injektive, surjektive, bijektive og angiv i givet fald en venstreinvers, højreinvers, invers afbildning (Sætning (0.4))

$$\text{For alle } n \in \mathbb{N} \text{ lad } \begin{cases} f_1(n) & = 2n \\ f_2(n) & = \begin{cases} \frac{1}{2}(n+2) & \text{hvis } n \text{ er lige} \\ \frac{1}{2}(n+1) & \text{hvis } n \text{ er ulige} \end{cases} \end{cases}$$

Endvidere er $f_3 = f_1 \circ f_2$.

("lige" betyder delelig med 2, "ulige" ikke delelig med 2, se Kapitel 2.) □

(0.7) DEFINITION: Lad A, B være mængder. Vi skriver

- $A \preceq B$ hvis der findes en injektiv afbildning $f : A \to B$
- $A \approx B$ hvis der findes en bijektiv afbildning $f : A \to B$
- $A \prec B$ Hvis der gælder $A \preceq B$ men *ikke* $A \approx B$.

□

(0.8) ØVELSE: Hvis $n \in \mathbb{N}$, betegner $\underline{n}$ mængden $\underline{n} = \{1, 2, \ldots, n\}$. Lad $n, m \in \mathbb{N}$. Undersøg hvornår der gælder $\underline{m} \preceq \underline{n}$, $\underline{m} \prec \underline{n}$, $\underline{m} \approx \underline{n}$. □

(0.9) ØVELSE: Vis, under anvendelse af (0.3), (0.4), at der for to mængder A, B gælder

$$A \preceq B$$
$$\Updownarrow$$
Der findes en surjektiv afbildning $g : B \to A$

□

(0.10) SÆTNING. *(Egenskaber ved $\preceq, \approx, \prec$.)*

(1) $A \approx B \Rightarrow A \preceq B$
(2) $A \preceq A$, $A \approx A$. *Der gælder ikke* $A \prec A$
(3) $A \preceq B$ *og* $B \preceq C \Rightarrow A \preceq C$
$A \approx B$ *og* $B \approx C \Rightarrow A \approx C$
$A \prec B$ *og* $B \prec C \Rightarrow A \prec C$
(4) $A \preceq B$ *og* $B \preceq A \Rightarrow A \approx B$
(5) $A \approx B \Rightarrow B \approx A$.

de 2 første udsagn.

BEVISET UDELADES: (Det anbefales som en let *øvelse* at bevise (1), (2), (3) og (5). F.eks. hænger det første udsagn i (3) sammen med følgende: Hvis $f : A \to B$ og $g : B \to C$ er injektive, så er $g \circ f : A \to C$ injektiv. Derimod er beviset for (4) ("Bernsteins ækvivalenssætning") noget vanskeligere.) □

(0.11) BEMÆRKNING: Hvis vi betragter en given fastlagt mængde $\mathcal{P}$ af mængder, er $\preceq, \approx$ og $\prec$ relationer på $\mathcal{P}$ (se Kapitel 1). (0.10)(2) behandler betingelsen [BRR], (0.10)(3) betingelsen [BRT] og (0.10)(5) [BRS]. Så $\approx$ er en ækvivalensrelation på $\mathcal{P}$. Endvidere inducerer, som man uden store vanskeligheder kan se, $\preceq$ en ordningsrelation på mængden $P(\approx)$ af $\approx$-ækvivalensklassen i $\mathcal{P}$. (Man bør overveje, hvad der menes hermed).

Vi kan ikke lade $\mathcal{P}$ være "mængden af *alle* mængder". Hvis man opererer med dette begreb, føres man til et paradoks ifølge B. Russell. □

(0.12) ØVELSE: (1) Gør rede for, at hvis B er en delmængde af A, gælder $B \preceq A$.
(2) Hvis $f : A \to B$ er injektiv overvejes, at $A \approx f(A)$. □

(0.13) DEFINITION: Lad A være en mængde. A kaldes

- *tællelig* hvis $A \preceq \mathbb{N}$
- *numerabel* hvis $A \approx \mathbb{N}$
- *endelig* hvis $A = \emptyset$ eller der findes et $n \in \mathbb{N}$ så $A \approx \underline{n}$ ($\underline{n}$ er defineret i (0.8))

Hvis $A \approx \underline{n}$ skriver vi $|A| = n$. □

(0.14) SÆTNING. *Lad A være en mængde. Der gælder*

$$A \text{ er tællelig } \Leftrightarrow \begin{cases} A & \text{er numerabel} \\ \text{eller} & \\ A & \text{er endelig} \end{cases}$$

BEVISET UDELADES: ($\Leftarrow$ kan let bevises ved hjælp af (0.10). $\Rightarrow$ er lidt vanskeligere, men kan bevises ved hjælp af betingelsen [MIN] fra Kapitel 2.) □

Lad os bemærke at elementerne i en tællelig mængde A kan "tælles": Lad ifølge (0.14) f være en bijektiv afbildning enten fra $\mathbb{N} \to A$ eller fra $\underline{n} \to A$, $n \in \mathbb{N}$. Så udgør $f(1), f(2), \ldots$ en tælling af alle elementer i A. Vi tæller altså $f(1)$ som det første element i A, $f(2)$ som det andet, osv.

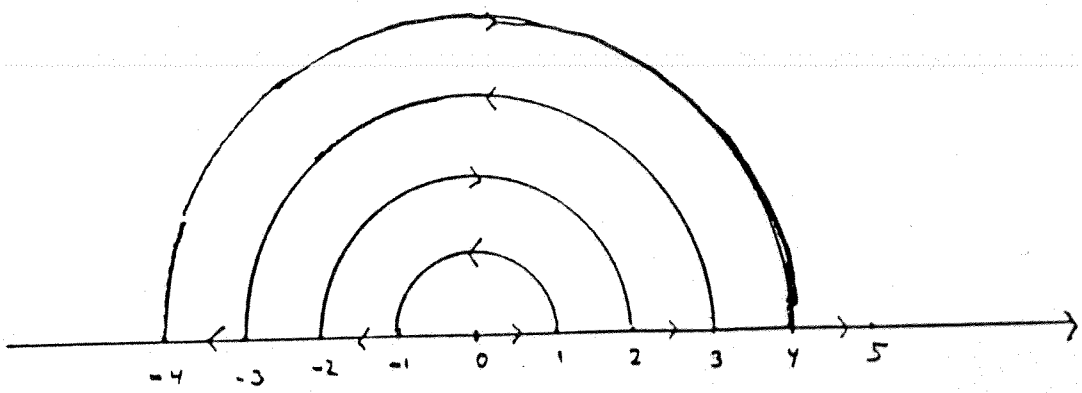
(0.15) SÆTNING. *$\mathbb{N} \approx \mathbb{N} \times \mathbb{N}$, så $\mathbb{N} \times \mathbb{N}$ er numerabel.*

BEVIS: Vi tænker os elementerne i $\mathbb{N} \times \mathbb{N}$, altså talpar af naturlige tal, placeret som følger talpar af naturlige tal, placeret som følger

$$\begin{array}{ccccccc}
\vdots & & & & & & \\
\uparrow & & & & & & \\
(4,1) & & (4,2) & & & & \\
& \nwarrow & & & & & \\
(3,1) & & (3,2) & & (3,3) & & (3,4) \quad \cdots \\
\uparrow & \searrow & & \nwarrow & & & \\
(2,1) & & (2,2) & & (2,3) & & (2,4) \quad \cdots \\
& \nwarrow & & \searrow & & \nwarrow & \\
(1,1) & \to & (1,2) & & (1,3) & \to & (1,4) \quad \cdots
\end{array}$$

Så angiver pilene en systematisk måde at gennemløbe alle talparrene på. En bijektiv afbildning $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ er altså givet ved $f(1) = (1,1), f(2) = (1,2), f(3) = (2,1), f(4) = (3,1), f(5) = (2,2)$, etc. □

(0.16) SÆTNING. *(1) $\mathbb{N} \approx \mathbb{Z}$, (2) $\mathbb{N} \approx \mathbb{Q}$ så $\mathbb{Z}$ og $\mathbb{Q}$ er numerable.*



BEVIS: (1) Lad os betragte tallene i $\mathbf{Z}$ på en tallinie

Så angiver pilene en systematisk måde at gennemløbe alle tallene i $\mathbf{Z}$ på.

(2) Afbildningen $(a,b) \to \frac{a}{b}$ er en surjektiv afbildning fra $\mathbf{Z} \times \mathbf{N} \to \mathbf{Q}$. Det skyldes at ethvert rationalt tal kan skrives som en heltallig brøk med positiv nævner. Dermed er $\mathbf{Q} \preceq \mathbf{Z} \times \mathbf{N}$ ifølge (0.9). Da $\mathbf{N} \approx \mathbf{Z}$ fås $\mathbf{Z} \times \mathbf{N} \approx \mathbf{N} \times \mathbf{N}$ (overvej!). Da $\mathbf{N} \times \mathbf{N} \approx \mathbf{N}$ fås i alt $\mathbf{Q} \preceq \mathbf{N}$. Da $\mathbf{N} \preceq \mathbf{Q}$ må $\mathbf{N} \approx \mathbf{Q}$. □

(Et andet bevis for (0.16)(2) kan fås ved en udnyttelse af bevisideen for (0.15)).

(0.17) BEMÆRKNINGER: (1) En delmængde af en tællelig mængde er tællelig.

(2) Hvis A og B begge er tællelige (hhv. numerable, hhv. endelige), så er $A \times B$ tællelig, hhv. numerabel, hhv. endelig. (Beviset for (2) hænger nøje sammen med (0.15) samt den kendsgerning, at $\underline{n} \times \underline{m} \approx \underline{nm}$. □

(0.18) SÆTNING. *$\mathbf{R}$ er ikke tællelig (eller numerabel).*

BEVISET kan gennemføres ved at vise, at $[0,1[= \{x \in \mathbf{R} \mid 0 \leq x < 1\}$ ikke er tællelig. Dertil anvendes f.eks. decimalbrøkudviklingen af reelle tal mellem 0 og 1. Vi vender tilbage til spørgsmålet i slutningen af Kapitel 5. □

I den sidste del af dette kapitel behandles Zorns lemma [ZL]. Vi forudsætter kendskab til relationer på mængder som beskrevet i Kapitel 1.

Vi betragter også følgende betingelse for en relation R på mængden A

[BRL] For alle $a, b \in A$ gælder aRb eller bRa.

Dette er den *lineære* betingelse, som udsiger at to elementer i A kan "sammenlignes" ved R. Et typisk eksempel er ordningen $\leq$ på $\mathbf{N}$ (eller på $\mathbf{Z}, \mathbf{R}$) som opfylder [BRL]. Hvis R er en relation på A er det klart at R "inducerer" en relation R på enhver delmængde B af A: Hvis $a, b \in B$ skrives aRb (i B), hvis aRb gælder i A. Det er så klart, at hvis R opfylder [BRR], [BRS], [BRT], [BRA] eller [BRL] i A, opfylder R de samme betingelser i B.

(0.19) DEFINITION: En *partielt ordnet mængde (po-mængde)* er et par $(M, \leq)$, hvor M er en mængde og $\leq$ en ordningsrelation på M, (så $\leq$ opfylder [BRR], [BRT], [BRA]). Hvis $\leq$ også opfylder [BRL] kaldes $(M, \leq)$ en *lineær ordnet mængde (lo-mængde)*. □

(0.20) DEFINITION: Lad $(M, \leq)$ være en po-mængde, $m \in M$. m kaldes

maksimalt hvis :	For alle $x \in M : m \leq x \Rightarrow m = x$
minimalt hvis :	For alle $x \in M : x \leq m \Rightarrow x = m$
førsteelement hvis :	For alle $x \in M : m \leq x$
sidsteelement hvis :	For alle $x \in M : x \leq m$.

Et sidsteelement er også maksimalt og et førsteelement er også minimalt, men det omvendte gælder ikke (overvej!) For lo-mængder falder begreberne maksimalt og sidsteelement og begreberne minimalt og førsteelement sammen. □

(0.21) DEFINITION: Lad $(M, \leq)$ være en po-mængde, $X \subseteq M$.

(1) X kaldes en *kæde*, hvis $(X, \leq)$ er en lo-mængde.
(2) Elementet $m \in M$ kaldes en *majorant* for X, hvis der gælder $n \leq m$ for alle $n \in X$.
(3) Hvis $\mathrm{Maj}(X)$ er mængden af majoranter for X, kaldes et førsteelement i $(\mathrm{Maj}(X), \leq)$ et *supremum* for X. (Læseren bør overveje definitionen af *minorant* og *infinimum*.)

□

(0.22) EKSEMPLER: (1) Betragt po-mængden $(\mathcal{P}(A), \subseteq)$ (Kapitel 1), A en mængde. Hvis $a, b \in A$, $a \neq b$ gælder hverken $\{a\} \subseteq \{b\}$ eller $\{b\} \subseteq \{a\}$, så $(\mathcal{P}(A), \subseteq)$ er ingen lo-mængde. Derimod er i dette tilfælde $X = \{\emptyset, \{a\}, \{a, b\}\}$ en kæde i $(\mathcal{P}(A), \subseteq)$. Enhver delmængde af A, som indeholder a og b, er en majorant for X, hvorimod $\{a, b\}$ er supremum for X. Mængden A er det eneste maksimale og $\emptyset$ det eneste minimale element i $(\mathcal{P}(A), \subseteq)$.

(2) Lad $\mathcal{P}_3(\mathbb{N})$ være mængden af delmængder af $\mathbb{N}$ med højst 3 elementer. Enhver delmængde af $\mathbb{N}$ med 3 elementer er maksimalt element i po-mængden $(\mathcal{P}_3(\mathbb{N}), \subseteq)$. Den eneste majorant (og supremum) for $\mathcal{P}_3(\mathbb{N})$ i $\mathcal{P}(\mathbb{N})$ er $\mathbb{N}$. □

Da vi ovenfor netop har givet de nødvendige definitioner, vil vi her nævne *SUPREMUMSEGENSKABEN* for en po-mængde $(M, \leq)$, som vil spille en rolle i vores senere konstruktion af de reelle tal $\mathbb{R}$.

[SUP] Lad $X \neq \emptyset$, $X \subseteq M$. Antag, at X er opad begrænset (dvs. $\mathrm{Maj}(X) \neq \emptyset$). Så findes der et supremum for X i M (dvs. $(\mathrm{Maj}(X), \leq)$ har et førsteelement).

(Man kan på dette sted overveje, hvorfor $(\mathbb{Z}, \leq)$ opfylder [SUP], men $(\mathbb{Q}, \leq)$ ikke.)
Her er så Zorns lemma:

[ZL] Lad $(M, \leq)$ være en po-mængde, $M \neq \emptyset$. Antag, at der for enhver kæde X i $(M, \leq)$ findes en majorant for X i M. Så har M et maksimalt element.

Som nævnt tidligere gælder følgende

(0.23) SÆTNING. *Betingelserne [UA] og [ZL] er logisk ækvivalente.*

BEVISET UDELADES: . □

I beviset for (5.3) gives et typisk eksempel på anvendelsen af [ZL].

(0.24) BEMÆRKNING: Lad $(M, \leq)$ være en po-mængde. Hvis der for enhver ikke tom delmængde X af M gælder, at $(X, \leq)$ indeholder et førsteelement, kaldes $(M, \leq)$ en *velordnet* mængde. (Sammenlign med betingelsen [MIN] i Kapitel 2). Det viser sig, at betingelsen

[VO] *Enhver* mængde kan velordnes

(altså: Hvis M er en mængde, findes en relation $\leq$ på M, så $(M, \leq)$ er velordnet) også er logisk ækvivalent med [UA] og [ZL]. Dette illustrerer yderligere [UA]'s styrke. Betingelsen [VO] ligger bag beviser med "transfinit induktion", en væsentlig og meget benyttet udvidelse af de velkendte beviser ved induktion. (Se også Kapitel 2). □

Kapitel 1. Lidt om relationer og kompositioner.

Den "abstrakte" algebra er studiet af "algebraiske strukturer", dvs. mængder med en eller flere kompositioner (kompositionsforskrifter).

Man tænker sig, at disse kompositioner opfylder visse regler (aksiomer) og forenklet kan man sige, at opgaven er at undersøge, hvilke konsekvenser disse regler har.

Den interesserede læser kan hente yderligere oplysninger om algebraens historie, formål og anvendelser i et tillæg (på engelsk) til disse noter, som er taget fra bogen

R.B.J.T. ALLENBY: RINGS, FIELDS AND GROUPS
(Edward Arnold Publ., London, England, 1983)
(ISBN 0–7131–3476–3)

Denne bog, der er meget bredt og udførligt skrevet, kan ses som det vigtigste supplement til disse noter, men den er ikke nødvendig for forståelsen.

Lad A og B være vilkårlige mængder. Vi lader

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

være det kartesiske produkt af A og B.

(1.1) DEFINITION OG NOTATION: En *(binær) relation* på mængden A er en delmængde $R \subseteq A \times A$. Lad $a, b \in A$. Hvis $(a, b) \in R$ skriver vi aRb og siger, at *a står i relation til b* (m.h.t. R). Hvis $(a, b) \notin R$ skriver vi $a \not R b$ og siger at *a står ikke i relation til b* (m.h.t. R) □

(1.2) EKSEMPLER: (1) Når M er en vilkårlig mængde lader vi i disse noter $\mathcal{P}(M)$ betegne M's *potensmængde*, dvs. mængden af alle delmængder af M. Hvis $A = \mathcal{P}(M)$ for en mængde M, så er $\subseteq$ ("delmængde af") en relation på A. Som delmængde af $A \times A$ er relationen $\subseteq$ det følgende

$$\subseteq = \{(X, Y) \mid X, Y \in A \text{ og ethvert element i } X \text{ er også element i } Y\}.$$

Denne skrivemåde virker måske ved første øjekast temmelig absurd, og vi vil ikke i praksis beskrive en relation på denne måde. Det bliver snarere gjort som i de følgende eksempler.

(2) Vi definerer relationer R_1, R_2 og R_3 på mængden $\mathbb{Z}$ af hele tal som følger: Lad $a, b \in \mathbb{Z}$

$$aR_1b \Leftrightarrow ab \neq 0$$
$$aR_2b \Leftrightarrow a \leq b - 2 \quad \text{(se også næste kapitel)}$$
$$aR_3b \Leftrightarrow a - b \quad \text{er delelig med } 3$$

(Relationen R_3 kommer i næste kapitel til at hedde $\equiv_3$, "kongruent modulo 3"). □

Her er nogle specielle betingelser, som er særlig vigtige for en relation R på A. (Betingelser = aksiomer bliver i disse noter altid identificeret ved et symbol skrevet i en kantet parantes, som for eksempel [BRR]. Dette symbol bliver fastholdt som etiket i resten af noterne.) [Dette gælder *kun* for kurset 2AL, ikke universelt].

[BRR] For alle $a \in A$ gælder aRa (R er *refleksiv*)
[BRS] For alle $a, b \in A$ gælder $aRb \Rightarrow bRa$ (R er *symmetrisk*)
[BRT] For alle $a, b, c \in A$ gælder $(aRb) \wedge (bRc) \Rightarrow aRc$ (R er *transitiv*)
[BRA] For alle $a, b \in A$ gælder $(aRb) \wedge (bRa) \Rightarrow a = b$ (R er *antisymmetrisk*).

(1.3) DEFINITION: En relation R der opfylder [BRR], [BRS] og [BRT] kaldes en *ækvivalensrelation.* Hvis den opfylder [BRR], [BRT] og [BRA] kaldes den en *ordningsrelation.* □

(1.4) ØVELSE: Overvej, om [BRS] og [BRA] kan være opfyldt *samtidigt* for en relation R. □

(1.5) EKSEMPLER: Vi henviser til eksemplerne i (1.2).

(1) Relationen $\subseteqq$ i (1.2) (1) er en ordningsrelation. I almindelighed er [BRS] ikke opfyldt for $\subseteqq$ (se eventuelt (1.4)). Som regel er det nemmest at eftervise ikke-opfyldelsen af et aksiom ved at give et eksempel. Læseren opfordres til at gøre dette i de følgende eksempler i det omfang, det ikke bliver gjort dér.

(2) Relationen R_1 i (1.2) (2) opfylder [BRS] og [BRT]. (Hvis $ab \neq 0$ så er $ba \neq 0$. Hvis $ab \neq 0$ og $bc \neq 0$ er $a, b, c \neq 0$. Men så er $ac \neq 0$. (Se aksiomet [NU] i Kap. 2). R_1 opfylder ikke [BRR] og [BRA]. (F.eks. er $0 \not R_1 0$, da $00 = 0$).

(3) Relationen R_2 i (1.2) (2) opfylder ikke [BRR] og [BRS]. Den opfylder [BRT]. Lad os se på [BRA]. Der findes *ikke* hele tal a og b med aR_2b og bR_2a (dvs. $a \leq b-2$ og $b \leq a-2$). Hermed er [BRA] trivielt (tomt) opfyldt.

(4) Relationen R_3 i (1.2) (2) er en ækvivalensrelation. [BRA] er ikke opfyldt (se (1.4)). □

Ækvivalensrelationerne på en given mængde A hænger nøje sammen med *partitionerne* af A:

(1. 6) DEFINITION: En *partition* (= *klassedeling*) af mængden A er en delmængde $P \subseteq \mathcal{P}(A)$ (A's potensmængde) som opfylder

(1) For alle $X \in P$ er $X \neq \varnothing$
(2) For alle $X, Y \in P$ gælder enten $X = Y$ eller $X \cap Y = \varnothing$
(3) Foreningsmængden af alle mængderne i P er A, altså $\cup_{X \in P} X = A$.

□

(F.eks. er $\{\{1\}, \{2,3\}\}$ en partition af $\{1,2,3\}$).

(1.7) SÆTNING. *Lad P være en partition af A, så er relationen $R(P)$ på A, defineret ved*

$$aR(P)b \Leftrightarrow \text{Der findes en mængde } X \in P, \text{ så } a, b \in X$$

er ækvivalensrelation.

BEVIS: Det er oplagt at relationen $R(P)$ opfylder [BRR] og [BRS]. (Begrund dette under anvendelse af (1.6) (3).) Vi viser, at $R(P)$ opfylder [BRT]. Antag at $aR(P)b$ og at $bR(P)c$. Ifølge definitionen af $R(P)$ eksisterer $X, Y \in P$, således at $a, b \in X$ og $b, c \in Y$. Så er $b \in X \cap Y$, dvs. $X \cap Y \neq \emptyset$. Nu viser (1.6) (2) at $X = Y$ og dermed er $a, c \in X(= Y)$. Det betyder, at $aR(P)c$, som ønsket. □

(1.8) SÆTNING. *Lad R være en ækvivalensrelation på mængden A. Hvis $a \in A$ kaldes delmængden*

$$\widehat{a} = \{b \in A \mid aRb\}$$

af A for a's ækvivalensklasse. Der gælder så, at

$$P(R) = \{\widehat{a} \mid a \in A\}$$

er en partition af A. ($P(R)$ betegnes ofte som A/R i litteraturen.)

BEVIS: Vi antager at R opfylder [BRR], [BRS] og [BRT]. Hvis $a \in A$ gælder aRa ifølge [BRR], så $a \in \widehat{a}$. Dermed er $\widehat{a} \neq \emptyset$ og $\cup_{a \in A} \widehat{a} = A$, så (1.6) (1) og (1.6) (3) er opfyldt for $P(R)$. Vi viser nu at (1.6) (2) også er opfyldt. Antag $a, b \in A$ og at $\widehat{a} \cap \widehat{b} \neq \emptyset$. Det vises, at så er $\widehat{a} = \widehat{b}$:

Lad $c \in \widehat{a} \cap \widehat{b}$. Det betyder, at aRc og bRc. [BRS] viser, at cRb, og så viser [BRT], at aRb. Vi har altså aRb og dermed også bRa.

Lad $d \in \widehat{b}$, dvs. bRd. Da aRb fås fra [BRT] at aRd, altså $d \in \widehat{a}$. Dermed er vist at $\widehat{b} \subseteq \widehat{a}$.

Analogt ses $\widehat{a} \subseteq \widehat{b}$, så $\widehat{a} = \widehat{b}$. □

BEMÆRKNING Så er
(1.9) ~~ØVELSE:~~ Lad P være en partition af mængden A. ~~Gør rede for, at~~ $P(R(P)) = P$. (Altså, anvend (1.7) på P til at få ækvivalensrelationen $R(P)$. Anvend (1.8) på $R(P)$ til at få partitionen $P(R(P))$. ~~Vis at~~ Denne partition er den samme, som den vi startede med). □

BEMÆRKNING Så er
(1.10) ~~ØVELSE~~: Lad R være en ækvivalensrelation på A. ~~Gør rede for at~~ $R(P(R)) = R$. □

(1.11) EKSEMPEL: Lad os betragte ækvivalensrelationen R_3 fra (1.2) (2). Der er tre forskellige ækvivalensklasser for R_3 på $\mathbb{Z}$, nemlig $\widehat{0}, \widehat{1}$ og $\widehat{2}$. Vi har

$$\widehat{0} = \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\}$$
$$\widehat{1} = \{\cdots, -8, -5, -2, 1, 4, 7, 10, \cdots\}$$
$$\widehat{2} = \{\cdots, -7, -4, -1, 2, 5, 8, 11, \cdots\}$$

For eksempel er $10 \in \widehat{1}$, da $1 - 10 = -9$ er delelig med 3. Ifølge beviset for (1.8) er derfor $\widehat{10} = \widehat{1}$. □

(1.12) DEFINITION: En *komposition* (= *kompositionsforskrift*) på mængden A er en afbildning

$$S : A \times A \to A.$$

Vi benytter følgende skrivemåde: Hvis $a, b \in A$ er altså $S(a,b) \in A$. Vi betegner dette element med aSb. Altså $aSb = S(a,b)$. □

(1.13) EKSEMPLER: (1) $\cap$ og $\cup$ (fællesmængde- og foreningsmængde-dannelse) er kompositioner på $A = \mathcal{P}(M)$, hvor M er en mængde.

(2) $+, -, \cdot$ (plus-dannelse, minus-dannelse, produkt-dannelse) er kompositioner på $\mathbf{Z}$.

(3) $a \circ b = ab + 1$ er en komposition på $\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}$.

(4) $a * b = a$ er en komposition på en vilkårlig mængde A.

(5) $a \S b = e^a + e^b$ er en komposition på $\mathbf{R}$. □

($\mathbf{N}, \mathbf{Q}, \mathbf{R}$ betegner mængden af naturlige, rationelle, reelle tal, henholdsvis).

(1.14) ØVELSE: Begrund at : (divisions-dannelse) er en komposition på $\mathbf{Q} \setminus \{0\}$, men ikke på $\mathbf{Q}$. □

De følgende betingelser er af særlig interesse for en komposition S på A:

[KK] For alle $a, b \in A$ gælder $aSb = bSa$
(S er *kommutativ*)

[KA] For alle $a, b, c \in A$ gælder $(aSb)Sc = aS(bSc)$
(S er *associativ*)

[KE] Der eksisterer et $e \in A$ således at der for alle $a \in A$ gælder $eSa = aSe = a$.

(Der eksisterer et *neutralt element* (= *enhedselement* = 1-*element* for S). □

(1.15) EKSEMPLER: (1) $\cap$ og $\cup$ er kommutative og associative kompositioner på $A = \mathcal{P}(M)$. Der eksisterer også neutrale elementer for dem: M er neutralt element for $\cap$ idet $M \cap X = X \cap M = X$ for alle $X \in P(M)$. Analogt ses, at $\emptyset$ er neutralt element for $\cup$.

(2) Kompositionen $-$ på $\mathbf{Z}$ opfylder hverken [KK], [KA] eller [KE]: $1 - (1 - 1) = 1$ men $(1 - 1) - 1 = -1$, $1 - 2 \neq 2 - 1$. Hvis man antager at $a \in \mathbf{Z}$ er neutralt for $-$ må der gælde $a - 1 = 1 - a = 1$. Dette er ikke opfyldt for noget element $a \in \mathbf{Z}$. □

(1.16) ØVELSE: Undersøg hvilke af betingelserne [KK], [KA] og [KE] er opfyldt for de resterende kompositioner i Eksempel (1.13). □

(1.17) ØVELSE: Lad S være en kommutativ komposition på A. Vi definerer en relation $D(S)$ ("deler med hensyn til S") som følger

$$bD(S)a \Leftrightarrow \text{Der eksisterer } c \in A \text{ således at } a = bSc.$$

(1) Vis, at hvis S opfylder [KE] så er $D(S)$ refleksiv ([BRR])
(2) Vis, at hvis S opfylder [KA] så er $D(S)$ transitiv ([BRT])
(3) Undersøg hvad relationen $D(S)$ betyder for kompositionerne i Eksempel (1.13) (1) og (1.13) (2).

□

(1.18) SÆTNING. *Lad S være en associativ komposition. Hvis $a_1, a_2, \ldots, a_n$ er elementer i A så vil produktet $a_1 a_2 \ldots a_n$ have den samme værdi uanset hvordan man sætter paranteser.*

BEVISET UDELADES. (Se f.eks. S 80 i Allenbys bog).
(F.eks. er altså, når S er associativ

$$(((a_1 S a_2) S a_3) S a_4) S a_5 = a_1 S((a_2 S a_3) S (a_4 S a_5)) \quad) \square$$

(1.19) DEFINITION: Lad S være en komposition på A. En ikke-tom delmængde B af A kaldes *lukket* (*stabil*) (m.h.t. S) hvis der gælder:
For alle $a, b \in B$ er $aSb \in B$. □

(A er altid en lukket delmængde med hensyn til enhver komposition på A).

(1.20) EKSEMPLER: (1) $\mathbf{N}$ er en lukket delmængde af $\mathbf{Z}$ m.h.t. $+$ og $\cdot$, men ikke m.h.t. $-$.
(2) Lad $A = \mathcal{P}(M)$. Lad $X \in \mathcal{P}(M)$. Så er delmængden

$$\{Y \in \mathcal{P}(M) \mid X \subseteq Y\} \quad \text{af} \quad \mathcal{P}(M)$$

lukket m.h.t. $\cap$ og $\cup$. □

(1.21) ØVELSE: Undersøg om følgende kompositioner på $\mathcal{P}(M)$, M mængde, opfylder [KK], [KA], [KE]:

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

□

(1.22) ØVELSE: Giv eksempler på lukkede delmængder af $\mathbf{Z}$ (forskellig fra $\mathbf{Z}$ og $\{0\}$) m.h.t. kompositionerne $+, -, \cdot$ og $\circ$ fra (1.13) (2) of (1.13) (3). □

Kapitel 2. De hele tals ring.

Som nævnt i Kapitel 1 ((1.13)(2)) er $+$ og $\cdot$ kompositioner på mængden $\mathbb{Z}$ af hele tal. $(\mathbb{Z}, +, \cdot)$ er et eksempel på den algebraiske struktur, der kaldes en *ring*. Vi vil her betragte egenskaber ved $\mathbb{Z}$, som kan være af interesse som aksiomer for algebraiske strukturer. Vi undersøger, hvilke andre egenskaber ved $\mathbb{Z}$, der kan udledes ved kun at bruge de nævnte (aksiom-)egenskaber. Dette tjener som indøvelse af de abstrakte/formelle beviser, der er typiske for algebraen. Flere af de nedenstående sætninger, som vi viser for $\mathbb{Z}$, gælder mere generelt i ringteorien og derfor er elementerne ikke specificeret. Disse sætninger er markerede med en stjerne. Læseren skal være velkommen til at tilføje "$\in \mathbb{Z}$" og så bevise sætningerne igen i Kapitel 3, 4 og 5 for ringe.

Hvis a, b, c ($\in \mathbb{Z}$) er vilkårlige gælder disse regler:

[RAK] $a + b = b + a$ ($+$ opfylder [KK])

[RAA] $(a + b) + c = a + (b + c)$ ($+$ opfylder [KA])

[RAN] Der eksisterer et element 0, således at $a + 0 = 0 + a = a$ ($+$ opfylder [KE])

[RAI] Der findes et element, kaldet $(-a)$ som opfylder $a + (-a) = (-a) + a = 0$

[RMK] $ab = ba$ ($\cdot$ opfylder [KK])

[RMA] $(ab)c = a(bc)$ ($\cdot$ opfylder [KA])

[RMN] Der findes et element $1 \neq 0$, således at $a1 = 1a = a$ ($\cdot$ opfylder [KE])

[RD] $a(b + c) = ab + ac$, $(a + b)c = ac + bc$ (de *distributive* love).

Egenskaberne [RAK] – [RD] beskriver $\mathbb{Z}$ som en *kommutativ ring med* 1*-element.*

De ovenstående navne på aksiomer er "forkortelser". Således betyder f.eks. [RAK] "Ring Addition Kommutativ" og [RMN] "Ring Multiplikation Neutralt element".

(Som ring kaldes $\mathbb{Z}$ "kommutativ", fordi [RMK] gælder og "med 1-element", fordi [RMN] gælder. De øvrige betingelser karakteriserer en ring.)

Hvis $a, b \in \mathbb{Z}$, sætter vi $a - b = a + (-b)$, hvor $(-b)$ er bestemt ifølge [RAI]. Denne "differens" af hele tal stemmer selvfølgelig overens med den velkendte. Men i en vilkårlig ring eller i andre algebraiske strukturer ville man benytte ligningen $a - b = a + (-b)$ som*definition* af differens. (Se f.eks. Definition 27.4 (1) i HBF. HBF henviser til Hans-Bjørn Foxbys forelæsningsnoter om lineær algebra).

(2.1)* SÆTNING. *For alle a, b, c gælder*

(1) $a + b = c \Leftrightarrow a = c - b$
(2) $0a = a0 = 0$
(3) $-(ab) = (-a)b = a(-b)$
(4) $-(a + b) = -a - b, \quad -(a - b) = -a + b.$

BEVIS: ~~Det er helt analogt til~~ Man kan lade sig inspirere af beviset 27.4 (3) i HBF. Vi nøjes med at udlede (1).

Antag, at $a+b=c$. Så er

$$\begin{aligned} a &= a+0 && \text{(ifølge [RAN])} \\ &= a+(b+(-b)) && \text{(ifølge [RAI])} \\ &= (a+b)+(-b) && \text{(ifølge [RAA])} \\ &= c+(-b) && \text{(ifølge antagelsen)} \\ &= c-b && \text{(ifølge definition af differens).} \end{aligned}$$

Omvendt, hvis $a=c-b$, så er

$$\begin{aligned} a+b &= (c-b)+b = (c+(-b))+b \\ &= c+((-b)+b) = c+0 = c. \end{aligned}$$

Også her benyttede vi kun [RAA], [RAN] og [RAI]. □

(2.2)* ØVELSE: Bevis resten af (2.1) under anvendelse kun af [RAK]–[RAI], [RMA] og [RD]. □

Motivationen for det udførlige bevis af (2.1) (1) er at vise, at dette udsagn gælder for *enhver* mængde med en komposition, der opfylder [RAA], [RAN] og [RAI]. Disse egenskaber karakteriserer en GRUPPE som algebraisk struktur, således at et udsagn analog til (2.1) (1) gælder i *enhver* gruppe (se et senere kapitel om Grupper). Tilsvarende vil resten af (2.1) være opfyldt i enhver ring.

Hvis man sammenligner (2.1) med 27.4 (2) i HBF, vil man opdage, at et udsagn analogt til regnereglen

$$(e) \qquad d\underline{x} = \underline{0} \Leftrightarrow d = 0 \vee \underline{x} = 0$$

ikke forekommer. Det er klart, at det tilsvarende udsagn for $\mathbb{Z}$ er

$$[\text{NU}] \qquad ab = 0 \Leftrightarrow a = 0 \vee b = 0.$$

Dette kaldes *nuldelerbetingelsen*. Kan man så udlede [NU], som jo er opfyldt i $\mathbb{Z}$, fra betingelserne [RAK] – [RD]? Retningen $\Leftarrow$ er netop (2.1) (2). Men senere i dette kapitel vil vi gennem et eksempel illustrere, at [RAK] – [RD] kan være opfyldt (for en ring) uden at [NU] er opfyldt! Så svaret på spørgsmålet er nej. (Se (2.35)).

Her er nogle flere betingelser, som $\mathbb{Z}$ opfylder og som ikke er konsekvenser af [RAK] – [RD]. Det er *ordningsbetingelsen*, *induktionsbetingelsen* og *mindsteelementbetingelsen*.

[ORD] Der findes en delmængde N, således at der gælder

(1) Ethvert a er i netop én af delmængderne $N, \{0\}, -N$, hvor $-N = \{-n \mid n \in N\}$

(2) Hvis $a, b \in N$ er $a+b \in N$ og $ab \in N$.

(For $\mathbb{Z}$ er N selvfølgelig delmængden $\mathbb{N}$ af naturlige tal). (Er [ORD] opfyldt i $\mathbb{Q}, \mathbb{R}$?)

[IND] Hvis U er en delmængde af N, således at $1 \in U$ og således at $a \in U \Rightarrow a+1 \in U$, så er $U = N$.

[MIN] Lad $T \subseteq N$, $T \neq \emptyset$. Der findes et element $t \in T$, således at $t \leq s$ for alle $s \in T$.

Det viser sig, at [IND] og [MIN] er logisk ækvivalente. [ORD] er det aksiom, der bevirker ordningen på $\mathbb{Z}$ og andre ringe og som ligger bag begrebet absolut-værdi.

Antag, at [ORD] gælder. Så skriver vi for givne a, b

$$b < a, \text{hvis } a - b \in N$$
$$b \leq a, \text{hvis } a - b \in N \cup \{0\}.$$

Man skriver ofte $a \geq b$ i stedet for $b \leq a$.

Betingelse (1) i [ORD] viser, at når a, b er givne, så gælder netop én af relationerne $b < a$, $b = a$, $a < b$ (eftersom $a-b \in N, a-b = 0, a-b \in -N$. (Vi benytter (2.1) (4): $a - b = -(b-a)$, således at $a - b \in -N \Leftrightarrow b - a \in N$). Ved hjælp af [RAK] – [RD] og [ORD] alene kan vi bevise:

(2.3)* SÆTNING. *For alle a, b, c gælder*

(1) $c < b \wedge b < a \Rightarrow c < a$ (*< opfylder* [BRT])
(1)′ $c \leq b \wedge b \leq a \Rightarrow c \leq a$ (*≤ opfylder* [BRT])
(2) $b < a \wedge 0 < c \Rightarrow bc < ac$
(2)′ $b \leq a \wedge 0 \leq c \Rightarrow bc \leq ac$
(3) $a \leq b \wedge b \leq a \Rightarrow a = b$ (*≤ opfylder* [BRA])
(4) $0 \leq a \Leftrightarrow -a \leq 0$.

BEVIS: (1) Antag at $c < b \wedge b < a$. Så er $b - c \in N$ og $a - b \in N$. Da N er lukket under $+$ ifølge [ORD] (2) fås $(a-b)+(b-c) \in N$. Men $(a-b)+(b-c) = (a+(-b))+(b+(-c)) \overset{[RAA]}{=} (a+((-b)+b))+(-c) \overset{[RAI]}{=} (a+0)+(-c) \overset{[RAN]}{=} a+(-c) = a-c$. Dermed er $a - c \in N$, dvs. $c < a$. (1)′ bevises analogt. (2): Antag $b < a \wedge 0 < c$. Så er $a - b \in N$ og $c = c - 0 \in N$. Da N er lukket under $\cdot$ fås $(a-b)c \in N$. Da $ac - bc = (a-b)c$ ifølge [RD] og definitionen af differens, er $ac - bc \in N$, dvs. $bc < ac$. (2)′ bevises analogt. (3): Hvis $a \leq b$ og $b \leq a$ gælder $b - a \in N \cup \{0\}$ og $a - b \in N \cup \{0\}$. Men $b - a \in N \cup \{0\}$ medfører $a - b \in (-N) \cup \{0\}$ idet $b - a = -(a-b)$ ifølge (2.1) (4). Så er

$$a - b \in (N \cup \{0\}) \cap ((-N) \cup \{0\}) = \{0\}$$

ifølge [ORD] (1), dvs. $a - b = 0$. Så er $a = b$ ifølge (2.1) (1). (4): Ifølge [RAI] er $-(-a) = a$. (Hvorfor?) Derfor er $a - 0 = a = -(-a) = 0 - (-a)$. Heraf følger (4) umiddelbart. □

(2.4)* ØVELSE: Gør rede for, hvorfor betingelsen [NU] kan udledes fra betingelsen [ORD] samt [RAK] – [RD]. □

Absolutværdien (*modulus*) af a er

$$|a| = \begin{cases} a & \text{hvis } 0 \leq a \\ -a & \text{hvis } a < 0. \end{cases}$$

(så $|-3| = 3$, $|3| = 3$, f.eks.). Der gælder

(2.5)* SÆTNING. *For alle a, b gælder*

(1) $0 \leq |a|$; $\quad |a| = 0 \Leftrightarrow a = 0$
(2) $|a| = |-a|$
(3) $|ab| = |a||b|$
(4) $|a+b| \leq |a| + |b|$.

BEVIS: (1) følger af (2.3) (4) og (2) følger fra definitionen af $|\cdot|$. (3) kan bevises ved hjælp af (2.1) (3). (4): Hvis $a \geq 0, b \geq 0$ er $a+b \geq 0$ og $|a+b| = a+b = |a| + |b|$. Hvis $a \leq 0, b \leq 0$ er $a+b \leq 0$ og $|a+b| = -(a+b) = -a-b = |a| + |b|$. Hvis $a \geq 0, b < 0$ er $|a| + |b| = a - b$ og $|a+b| = (a+b)$ eller $|a+b| = -(a+b) = -a-b$. Men $a+b \leq a-b$, da $b \leq -b$ ifølge (2.3) (4) og $-a-b \leq a-b$, da $-a \leq a$ ifølge (2.3) (4). Tilfældet $a < 0$, $b \geq 0$ behandles analogt. □

Betingelsen [IND] gør *induktionsbeviser* mulige: Lad os forestille os, at vi vil bevise et udsagn $U(n)$, som afhænger af n, for alle $n \in \mathbb{N}$. Vi betragter mængden

$$U = \{n \in \mathbb{N} \mid U(n) \text{ er sand}\}.$$

Induktionsstarten viser at $1 \in U$ og induktionsskridtet, at hvis $a \in U$ så er $a+1 \in U$. [IND] udsiger så at $U = \mathbb{N}$, altså at $U(n)$ er sand for alle n.

(2.6) SÆTNING. *Betingelserne* [IND] *og* [MIN] *er ensbetydende (logisk ækvivalente).*

BEVISET UDELADES.

□

Vi indfører nu nogle begreber i forbindelse med "division". Vi formulerer disse begreber således, som det traditionelt gøres i vilkårlige ringe med 1-element, og undersøger, hvad de betyder i $\mathbb{Z}$.

(2.7)* DEFINITION: (Sammenlign med (1.17)). Lad a, b være vilkårlige elementer

$$b \mid a \Leftrightarrow \text{ Der findes et } c, \text{ så } a = bc.$$

□

(2.8)* DEFINITION: Lad a, b, c være vilkårlige elementer.

(1) a kaldes *invertibel*, hvis der findes et b, så $ab = ba = 1$.
(2) a kaldes *irreducibel*, hvis $a \neq 0$, a ikke er invertibel og der gælder

$$a = bc \Rightarrow b \text{ eller } c \text{ er invertibel}$$

(3) a kaldes *prim* (primelement), hvis $a \neq 0$, a ikke er invertibel og der gælder

$$a \mid bc \Rightarrow a \mid b \vee a \mid c$$

(4) a og b kaldes *associerede*, hvis der findes et invertibelt element c, således at $a = bc$.

□

(2.9) EKSEMPEL: I $\mathbb{Z}$ gælder $2|4, -2|4, 2|0, 0|0, -1|a$ for alle a. Derimod gælder $-10 \not| -5, 0 \not| 2$. □

(2.10)* ØVELSE: (1) Gør rede for, at produktet af to invertible elementer igen er et invertibelt element. Gælder a invertibel $\Leftrightarrow a \mid 1? \Leftrightarrow a \mid b$ for alle $b \in R$?

(2) Gør rede for, at relationen "være associeret" er en ækvivalensrelation.
(I denne øvelse må (2.13) *ikke* anvendes.)

(3) Lad a og b være associerede. Vis a irr $\Leftrightarrow b$ irr, a prim $\Leftrightarrow b$ prim. □

(2.11)* ØVELSE: Gør rede for (under anvendelse af [NU] og *uden* at anvende (2.13)), at

$$a \text{ og } b \text{ er associerede} \Leftrightarrow a \mid b \wedge b \mid a.$$

□

Den følgende definition er sikkert velkendt:

(2.12) DEFINITION: Et element $p \in \mathbb{N}$, $p \neq 1$ kaldes *primtal*, hvis der gælder:

$$a \mid p \wedge a \in \mathbb{N} \Rightarrow a = 1 \vee a = p.$$

(Så primtallene er $2, 3, 5, 7, 11, 13, 17, \ldots$). □

(2.13) BEMÆRKNINGER: (1) I $\mathbb{Z}$ er de eneste invertible elementer $+1$ og -1. (Overvej dette!) I vilkårlige ringe ser det anderledes ud: I et *legeme* (f.eks. $\mathbb{Q}$) (se den lineære algebra eller Kapitel 3) er ethvert element $\neq 0$ invertibelt, således at der ikke findes irreducible elementer og primelementer. Se også (2.37).

(2) I $\mathbb{Z}$ er mængden af irreducible elementer lig mængden af primelementer (og lig $\{\pm p \mid p \text{ primtal}\}$). I vilkårlige ringe er begreberne forskellige. (Se Kapitel 4).

(3) Under anvendelse af (1) er det klart, at $a, b \in \mathbb{Z}$ netop da er associerede, når $|a| = |b|$. □

(2.14) ØVELSE: Hvilke elementer i $\mathbb{Q}$ er associerede til 1 (hhv. 0)? □

(2.15)* SÆTNING. *Når* [RAK] – [RD] *og* [NU] *er opfyldte, så er ethvert primelement irreducibelt.*

BEVIS: Antag, at a er et primelement og at $a = bc$. Da gælder specielt, at $a \mid bc$, $(a = (bc)1)$. Da a er et primelement, fås $a \mid b \vee a \mid c$. Lad os antage, at $a \mid b$. (Tilfældet $a \mid c$ behandles analogt). Så er $b = ad$. Vi får $a = bc = (ad)c = a(dc)$.

Altså er $a(1-dc) = a - adc = a - a = 0$. Da a er et primelement, er $a \neq 0$. [NU] medfører så, at $1 - dc = 0$, dvs. $1 = cd$. Så er c invertibel. □

(2.16) BEMÆRKNING: Vi vil senere give et eksempel på, at [RAK] – [RD] og [NU] kan være opfyldte, uden at ethvert irreducibelt element er et primelement. (Se (4.5)). □

(2.17) SÆTNING. *Ethvert element $a \in \mathbb{N}, a > 1$, er et produkt af endelig mange irreducible elementer.*

BEVISET: er baseret på [MIN]-betingelsen. Vi antager, at der findes et naturligt tal > 1, som ikke er et produkt af endelig mange irreducible elementer, og vil føre denne antagelse til modstrid. Vi antager altså, at delmængden

$$T = \{a \in \mathbb{N} \mid a > 1 \text{ og } a \text{ er ikke produkt af endelig mange irreducible elementer}\}$$

af $\mathbb{N}$ er ikke-tom. Lad $t \in T$ således at $t \leq s$ for alle $s \in T$. (Her er [MIN] anvendt). Så er t ikke irreducibel (da t så ville være et produkt af ét irreducibelt element (sig selv)). Derfor kan vi skrive $t = t_1 t_2$, hvor hverken t_1 eller t_2 er invertibelt. Ifølge (2.13) (1) må $1 < t_1 < t$ og $1 < t_2 < t$. Dermed er t_1 og t_2 ikke i T, så hvert af disse elementer er et produkt af endelig mange irreducible elementer. Det er $t = t_1 t_2$ altså også, en modstrid. □

Det følgende resultat er velkendt

(2.18) SÆTNING. *(Divisionsalgoritmen). Lad $a, b \in \mathbb{Z}$ med $b \neq 0$. Der eksisterer entydigt bestemte tal $m, r \in \mathbb{Z}$, således at $a = mb + r$ og $0 \leq r < |b|$.*

Et *bevis* for denne sætning kan gives ved at anvende [MIN] på $T = \{a - mb > 0 \mid m \in \mathbb{Z}\}$ i det tilfælde hvor $b \nmid a$. Hvis $b \mid a$ er udsagnet trivielt. Entydigheden er baseret på en anvendelse af [NU]. Vi udelader et detaljeret bevis. (Se Allenby S 28). En generalisering af resultatet bliver beskrevet i Kapitel 4.

□

(2.19) ØVELSE: Hvis $n \in \mathbb{Z}$ sætter vi $\mathbb{Z}n = \{an \mid a \in \mathbb{Z}\}$, mængden af tal som er delelige med n. Lad $I \neq \emptyset, I \neq \{0\}$ være en delmængde af $\mathbb{Z}$, som opfylder

$$a, b \in I \Rightarrow a - b \in I.$$

Vis, at der eksisterer et $n \in \mathbb{N}$, således at $I = \mathbb{Z}n$.

(Løsningsforslag: Vis først, at $T = \{a \in I \mid a > 0\}$ er ikke-tom. Anvend [MIN] på delmængden $T \subseteq \mathbb{N}$ og kald det mindste element i T for n (!)) □

(Denne øvelse generaliseres senere i Kapitel 4).

(2.20)* DEFINITION: Lad a, b være vilkårlige. Et element c kaldes *største fælles divisor* (sfd) for a og b hvis der gælder

(1) $c \mid a$ og $c \mid b$
(2) Hvis $d \mid a$ og $d \mid b$, så gælder $d \mid c$.

□

(2.21) BEMÆRKNING OG NOTATION: Hvis c og c' er sfd for a og b, gælder ifølge (2.20) (2) at $c \mid c'$ og $c' \mid c$. Så hvis [NU] er opfyldt, er c og c' associerede ifølge (2.11). I $\mathbb{Z}$ betyder dette, at $c = \pm c'$ ifølge (2.13). Så hvis $a, b \in \mathbb{Z}$ ikke begge er 0, findes netop en sfd c, således at $0 < c$. Dette element c betegner vi med (a, b). □

Det er let at se, at hvis $d \mid a$ og $d \mid b$ gælder $d \mid ka + \ell b$ for alle k, ℓ. (Begrund dette). Specielt gælder, at hvis $a, b \in \mathbb{Z}$ ikke begge er 0, så er $(a, b) \mid ka + \ell b$ for alle $k, \ell \in \mathbb{Z}$.

(2.22) ØVELSE: Lad $m, n \in \mathbb{Z}$ og lad $\mathbb{Z}m, \mathbb{Z}n$ være som i (2.19). Vis, at $\mathbb{Z}m \subseteq \mathbb{Z}n \Leftrightarrow n \mid m$. □

(2.23) ØVELSE: Lad $a, b \in \mathbb{Z}$, a, b ikke begge 0. Sæt

$$I = \{ka + \ell b \mid k, \ell \in \mathbb{Z}\}.$$

(1) Gør rede for at I opfylder betingelsen i (2.19), således at der eksisterer et $m \in \mathbb{N}$, med $I = \mathbb{Z}m$.
(2) Gør rede for, at $\mathbb{Z}a \subseteq I$ og at $\mathbb{Z}b \subseteq I$.
(3) Gør rede for, at hvis $n \in \mathbb{Z}$ og $n \mid a$ og $n \mid b$, gælder $n \mid m$.
(4) Bevis ved hjælp af (2.22), at $m = (a, b)$.

□

Vi formulerer resultatet fra (2.23) som

(2.24) SÆTNING. *(Bézout) Lad $a, b \in \mathbb{Z}$, a, b ikke begge 0. Der eksisterer $k, \ell \in \mathbb{Z}$, således at*

$$(a, b) = ka + \ell b.$$

(Se også opgave (2D)). □

(2.25) EKSEMPEL: Vi beskriver ved et eksempel *Euklids Algoritme*, der kan anvendes til et bestemme (a, b), når $a, b \in \mathbb{Z}$ er givne. Vi kan vælge notationen så $|a| > |b|$ og starter så med at anvende (2.18) (divisionsalgoritmen) på a og b. (Hvis $b = 0$, er $(a, b) = a$ og Euklids algoritme overflødig.) Lad $a = 2385$, $b = 291$. Vi skriver

$$2385 = 8 \cdot 291 + 57 \quad (\text{så } m = 8, r = 57 \text{ i } (2.18))$$

$$291 = 5 \cdot 57 + 6 \quad (\text{så } m = 5, r = 6 \text{ i } (2.18))$$

$$57 = 9 \cdot 6 + 3 \leftarrow$$

Her står $(a, b) = (2385, 291) = 3$ som den sidste "rest" forskellig fra 0

$$6 = 2 \cdot 3 + 0$$

Man kan se, at Euklids algoritme giver det ønskede resultat, ved at bemærke, at hvis $a = mb + r$, så er $(a, b) = (b, r)$. (Overvej dette!) Ved at regne "baglæns" i Euklids algoritme kan man også beregne $k, \ell \in \mathbb{Z}$, så $(a, b) = ka + \ell b$:

$$\begin{aligned} 3 &= 57 - 9 \cdot 6 = 57 - 9(291 - 5 \cdot 57) \\ &= -9 \cdot 291 + 46 \cdot 57 \qquad (46 = (-9)(-5) + 1) \\ &= -9 \cdot 291 + 46(2385 - 8 \cdot 291) \\ &= \underbrace{46 \cdot 2385}_{(109710)} - \underbrace{377 \cdot 291}_{(109707)} \qquad (377 = 46 \cdot 8 + 9) \end{aligned}$$

Så en mulighed for k og ℓ er $k = 46, \ell = -377$. □

I (2.15) viste vi, at der under visse omstændigheder (f.eks. i $\mathbb{Z}$) gælder, at ethvert primelement irreducibelt. Se også (2.16). Vi kan vise

(2.26) SÆTNING. *I $\mathbb{Z}$ er ethvert irreducibelt element et primelement.*

BEVIS: Lad $a \in \mathbb{Z}$ være irreducibelt. Antag, at $a \mid bc$ og at $a \top b$. Vi må vise, at $a \mid c$. Hvis $d \mid a$ gælder $d \in \{1, -1, a, -a\}$, da a er irreducibel. (Hvis $a = ed$ er enten d invertibel, dvs. $d = \pm 1$, eller e invertibel, dvs. $e = \pm 1$, og derfor $d = \pm a$). Da $(a, b) \mid a$ og $\pm a \top b$ fås $(a, b) = 1$. Ifølge (2.24) eksisterer $k, \ell \in \mathbb{Z}$, så $ka + \ell b = 1$. Ved at gange med c fås $kac + \ell bc = c$. Nu er $a \mid kac$ (trivielt) og $a \mid \ell bc$ (da $a \mid bc$ ifølge antagelsen), så $a \mid c$. □

(2.27) ØVELSE: Vis ved hjælp af (2.24) at hvis $(a, c) = (b, c) = 1$, så er $(ab, c) = 1$. □

(2.28) ØVELSE: Beregn ved hjælp af Euklids algoritme (a, b) og tal $k, \ell \in \mathbb{Z}$ med $ka + \ell b = (a, b)$ i følgende tilfælde

(1) $a = 102, b = 63$ (2) $a = 2001, b = 1066$.

□

(2.29) ØVELSE: Vis, at der for ethvert $n \in \mathbb{Z}$ gælder $(5n + 2, 12n + 5) = 1$. (Løsningshjælp (?): Hvis $c = (a, b)$ er $c \mid 12a - 5b$). □

Ved benyttelse af (2.15), (2.17) og (2.26) kan man vise

(2.30) SÆTNING. *(Aritmetikkens fundamentalsætning) Ethvert $a \in \mathbb{Z}$, $a \neq 0$ kan entydigt skrives som et produkt af et invertibelt element (dvs. ± 1) med endelig mange primtal.*

□

Vi udelader beviset. Denne sætning generaliseres i Kapitel 4. (Der er 2 beviser i Allenby, s. 33–34.)

Vi betragter nu de såkaldte *restklasseringe* $\mathbb{Z}_n$, hvor $n \in \mathbb{Z}$. Dette er et eksempel på *faktorringe* som behandles i Kapitel 3. Lad $n \in \mathbb{Z}$ være vilkårlig. Vi definerer en relation $\equiv_n$ ("kongruent modulo n") på $\mathbb{Z}$ som følger:

$$a \equiv_n b \Leftrightarrow n \mid a - b.$$

I litteraturen finder man oftest notationen $a \equiv b \pmod{n}$ eller $a \equiv b(n)$ i stedet for $a \equiv_n b$. F.eks. er $-2 \equiv_7 19$ idet $7 \mid -2-19(=-21)$. Derimod er $3 \not\equiv_7 4$ da $3-4=-1$ ikke er delelig med 7. Vi nævner at $a \equiv_1 b$ for alle a, b og at $a \equiv_0 b \Leftrightarrow a = b$.

(2.31) SÆTNING. *(1) For alle n er $\equiv_n$ en ækvivalensrelation. (2) Der gælder at $\equiv_n$ og $\equiv_{-n}$ er den samme relation. (3) Når $n \neq 0$ er der $|n|$ ækvivalensklasser for $\equiv_n$.*

BEVIS: (1) $n \mid 0 = a - a$, så [BRR] er opfyldt. $a \equiv_n b \wedge b \equiv_n c \Rightarrow n \mid a-b \wedge n \mid b-c \Rightarrow n \mid (a-b)+(b-c) \Rightarrow n \mid a-c \Rightarrow a \equiv_n c$. ([BRT]).
$a \equiv_n b \Rightarrow n \mid a-b \Rightarrow n \mid b-a = -(a-b) \Rightarrow b \equiv_n a$. ([BRS]).
(2) er triviel, da $n \mid c \Leftrightarrow -n \mid c$.
(3) Ifølge (2) kan vi antage $n \in \mathbb{N}$. Hvis $0 \leq i < j < n$ er $i \not\equiv_n j$, da $0 < j - i \leq j < n$. Derfor er ækvivalensklasserne $\widehat{0}, \widehat{1}, \ldots, \widehat{n-1}$ forskellige. Men hvis $a \in \mathbb{Z}$, kan vi ifølge (2.18) skrive $a = mn + r$, hvor $0 \leq r < n$. Så er $a \equiv_n r$, dvs. $a \in \widehat{r}$. Derfor er et vilkårligt $a \in \mathbb{Z}$ i en af de n ækvivalensklasser $\widehat{0}, \widehat{1}, \ldots, \widehat{n-1}$. □

(2.32) BEMÆRKNING: Hvis $0 \leq r < n$ består ækvivalensklassen $\widehat{r}$ for $\equiv_n$ netop af de hele tal, hvis *rest* er r efter division med n (som i (2.18)) altså af tallene $mn+r$, $m \in \mathbb{Z}$. Ækvivalensklasserne for $\equiv_n$ kaldes derfor også *restklasser (modulo n)*. Restklasserne modulo 3 er angivet i (1.11). □

Vi vil gerne give mængden af restklasser modulo n en ringstruktur. Dertil har vi brug for:

(2.33) SÆTNING. *Lad $n, a, b, c, d \in \mathbb{Z}$. Antag at $a \equiv_n c$, $b \equiv_n d$. Så gælder*

(1) $a + b \equiv_n c + d$
(2) $ab \equiv_n cd$

BEVIS: Antagelsen viser, at $a - c = kn$, $b - d = \ell n$, $k, \ell \in \mathbb{Z}$. Altså gælder $a = c + kn$, $b = d + \ell n$. Vi adderer og multiplicerer disse ligninger.

(1) $a + b = c + d + kn + \ell n = (c + d) + (k + \ell)n$, altså $a + b \equiv_n c + d$
(2) $ab = cd + c\ell n + knd + k\ell n^2 = cd + (c\ell + kd + k\ell n)n$, altså $ab \equiv_n cd$.

□

(2.34) DEFINITION AF RESTKLASSERINGE: Lad $n \in \mathbb{N}$ og lad $\mathbb{Z}_n$ være mængden af de n restklasser $\widehat{0}, \widehat{1}, \ldots, \widehat{n-1}$ modulo n. ((2.31)). For $a \in \mathbb{Z}$ er $\widehat{a} = \widehat{r}$, hvor $0 \leq r < n-1$, netop når a har rest r efter division med n. Vi definerer addition og multiplikation af $\widehat{a}, \widehat{b} \in \mathbb{Z}_n$ ved

$$\widehat{a} + \widehat{b} = \widehat{a+b} \ , \ \widehat{a}\widehat{b} = \widehat{ab}.$$

Hvis nu $\widehat{a} = \widehat{c}$, $\widehat{b} = \widehat{d}$, er vi nødt til at overveje om $\widehat{a}+\widehat{b} = \widehat{c}+\widehat{d}$, $\widehat{a}\widehat{b} = \widehat{c}\widehat{d}$ i ovenstående definition, idet den ellers er ubrugelig (*ikke veldefineret*). Heldigvis gælder dette ifølge (2.33)! (Når $\widehat{a} = \widehat{c}$ og $\widehat{b} = \widehat{d}$ gælder $\widehat{a+b} = \widehat{c+d}$ og $\widehat{ab} = \widehat{cd}$.) Da $(\mathbb{Z}, +, \cdot)$ opfylder betingelserne [RAK]–[RD], er det let at se, at $(\mathbb{Z}_n, +, \cdot)$ også *opfylder* [RAK]–[RD].

For $\mathbb{Z}_n$ spiller $\widehat{0}$ og $\widehat{1}$ rollen som elementerne 0 og 1 i [RAN] og [RMN]. F.eks. er beviset for, at [RAK] gælder i $(\mathbb{Z}_n, +, \cdot)$, som følger

$$\begin{aligned} \widehat{a} + \widehat{b} &= \widehat{a+b} \quad \text{(definition af + i } \mathbb{Z}_n) \\ &= \widehat{b+a} \quad \text{(da [RAK] gælder i } \mathbb{Z}) \\ &= \widehat{b} + \widehat{a} \quad \text{(definition af + i } \mathbb{Z}_n) \end{aligned}$$

De andre betingelser bevises på analog måde. □

(2.35) EKSEMPEL: Lad $n = 6$, $\mathbb{Z}_6 = \{\widehat{0}, \widehat{1}, \widehat{2}, \widehat{3}, \widehat{4}, \widehat{5}\}$. Så er $\widehat{3} + \widehat{4} = \widehat{3+4} = \widehat{7} = \widehat{1}$ da $7 \equiv_6 1$. Vi har også $\widehat{3} \cdot \widehat{4} = \widehat{3 \cdot 4} = \widehat{12} = \widehat{0}$, da $12 \equiv_6 0$. Denne sidste relation $\widehat{3} \cdot \widehat{4} = \widehat{0}$ viser at $\mathbb{Z}_6$ *ikke* opfylder [NU]-betingelsen! Så $\mathbb{Z}_6$ leverer eksemplet på at man *ikke* kan udlede [NU] fra [RAK] – [RD]. Vi opstiller nu "kompositionstavler" for + og · i $\mathbb{Z}_6$:

+	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$	$\widehat{4}$	$\widehat{5}$
$\widehat{0}$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$	$\widehat{4}$	$\widehat{5}$
$\widehat{1}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$	$\widehat{4}$	$\widehat{5}$	$\widehat{0}$
$\widehat{2}$	$\widehat{2}$	$\widehat{3}$	$\widehat{4}$	$\widehat{5}$	$\widehat{0}$	$\widehat{1}$
$\widehat{3}$	$\widehat{3}$	$\widehat{4}$	$\widehat{5}$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$
$\widehat{4}$	$\widehat{4}$	$\widehat{5}$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$
$\widehat{5}$	$\widehat{5}$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$	$\widehat{4}$

·	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$	$\widehat{4}$	$\widehat{5}$
$\widehat{0}$	$\widehat{0}$	$\widehat{0}$	$\widehat{0}$	$\widehat{0}$	$\widehat{0}$	$\widehat{0}$
$\widehat{1}$	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$	$\widehat{4}$	$\widehat{5}$
$\widehat{2}$	$\widehat{0}$	$\widehat{2}$	$\widehat{4}$	$\widehat{0}$	$\widehat{2}$	$\widehat{4}$
$\widehat{3}$	$\widehat{0}$	$\widehat{3}$	$\widehat{0}$	$\widehat{3}$	$\widehat{0}$	$\widehat{3}$
$\widehat{4}$	$\widehat{0}$	$\widehat{4}$	$\widehat{2}$	$\widehat{0}$	$\widehat{4}$	$\widehat{2}$
$\widehat{5}$	$\widehat{0}$	$\widehat{5}$	$\widehat{4}$	$\widehat{3}$	$\widehat{2}$	$\widehat{1}$

I disse tavler står der $\widehat{a} + \widehat{b}$ (hhv. $\widehat{a} \cdot \widehat{b}$) på den plads som er i rækken med $\widehat{a}$ og søjlen med $\widehat{b}$. På grund af at [RAK] og [RMK] er opfyldte i $\mathbb{Z}_n$, er tavlerne symmetriske i diagonalen. De *invertible* elementer i $\mathbb{Z}_6$ er dem, hvis række i $\cdot$-diagrammet indeholder $\widehat{1}$, altså $\widehat{1}$ og $\widehat{5}$. (Begrund dette). □

(2.36) ØVELSE: Opstil kompositionsdiagrammer analoge til de ovenstående i $\mathbb{Z}_7$. Gør rede for at *alle* elementer $\neq \widehat{0}$ i $\mathbb{Z}_7$ er invertible, ved hjælp af $\cdot$-diagrammet. □

Det generelle spørgsmål, *hvilke* elementer der er invertible i $\mathbb{Z}_n$, besvares her:

(2.37) SÆTNING. *Lad $\widehat{a} \in \mathbb{Z}_n$, $n \in \mathbb{N}$. Så er $\widehat{a}$ invertibel i $\mathbb{Z}_n$ netop da, når $(a, n) = 1$.*

BEVIS: $\widehat{a}$ er invertibel i $\mathbb{Z}_n$, netop når der eksisterer et $\widehat{k} \in \mathbb{Z}_n$ med $\widehat{a}\widehat{k} = \widehat{ak} = \widehat{1}$. Men $\widehat{ak} = \widehat{1}$ netop når der eksisterer et ℓ så $1 - ak = \ell n$ dvs. $ka + \ell n = 1$. Sætningen følger under anvendelse af (2.24). (Overvej dette). □

(2.38) ØVELSE: Angiv det "inverse" element til $\widehat{a}$ for alle $\widehat{a} \in \mathbb{Z}_7$, $\widehat{a} \neq \widehat{0}$ med hensyn til multiplikation (altså et $\widehat{b}$, så $\widehat{a}\widehat{b} = \widehat{1}$). □

(2.39) ØVELSE: Lad p være et ulige primtal. Angiv alle $\widehat{a} \in \mathbb{Z}_p$ som opfylder $\widehat{a}^2 = \widehat{1}$. (Her er $\widehat{a}^2 = \widehat{a}\,\widehat{a} = \widehat{a^2}$). □

(2.40) ØVELSE: (1) Gør rede for, at der i $\mathbb{Z}_p$ gælder $\widehat{1}\,\widehat{2}\ldots\widehat{p-1} = \widehat{p-1}$, når p er et ulige primtal.

(2) Bevis *Wilson's sætning*

$$1 \cdot 2 \cdot 3 \ldots (p-1) \equiv_p -1$$

når p er et ulige primtal. □

Kapitel 3. Ringteori. Indledning.

I det forrige kapitel betragtede vi $\mathbf{Z}$ og $\mathbf{Z}_n$ som eksempler på ringe. Vi vil nu gå i gang med den abstrakte ringteori og undersøge hvorledes nogle af de begreber og sætninger, der blev beskrevet i Kapitel 2, kan udvides. Det gælder især teorien for faktorringe i dette kapitel, og faktoriseringsteorien i Kapitel 4.

En RING er et tripel $(R, +, \cdot)$, hvor R er en mængde og $+$ og $\cdot$ er kompositioner på R. Givet $a, b \in R$ har vi altså en *sum* $a + b \in R$ og et *produkt* $a \cdot b = ab \in R$. Vi antager, at kompositionerne $+$, $\cdot$ opfylder betingelserne [RAK], [RAA], [RAN], [RAI], [RMA] og [RD] fra Kapitel 2.

Ringen R kaldes *kommutativ* hvis yderligere [RMK] gælder (så $\cdot$ er kommutativ) og kaldes *unitær* (eller *med 1-element*) hvis [RMN] gælder.

(3.1) EKSEMPLER PÅ RINGE: Foruden $\mathbf{Z}$ og $\mathbf{Z}_n$ som er kommutative ringe med 1-element, nævner vi:

(1) $2\mathbf{Z} = \{2a \mid a \in \mathbf{Z}\}$. Med $+$, $\cdot$ fra $\mathbf{Z}$ er $2\mathbf{Z}$ en ring uden 1-element. (Begrund dette.)

(2) Lad $n \in \mathbf{N}$ og lad $\mathbf{R}_n^n$ betegne mængden af $n \times n$-matricer med reelle koefficienter. Med den sædvanlige sum og det sædvanlige produkt af matricer er $\mathbf{R}_n^n$ en ring. (Læseren opfordres til at finde de udsagn i noterne om lineær algebra, som beviser [RAK] – [RAI], [RMA] og [RD], samt give et eksempel på, at [RMK] ikke er opfyldt for $n \geq 2$). Derimod er $E_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$ 1-element.

(3) Her er et meget eksotisk eksempel: Lad $\mathcal{P}(M)$ være potensmængden af mængden M (se (1.2) (1)). Vi definerer en komposition $+$ (den såkaldte *symmetriske differens*) ved:

For alle $A, B \in \mathcal{P}(M)$ er $A + B = (A \cup B) \setminus (A \cap B)$.

Så er $(\mathcal{P}(M), +, \cap)$ en ring!

Altså skal $\cap$ (fællesmængde-dannelse) spille rollen som "multiplikation" i $\mathcal{P}(M)$. Nulelementet er $\varnothing$ (den tomme mængde) og M er et 1-element. Den interesserede læser kan prøve at eftervise, at $(\mathcal{P}(M), +, \cap)$ opfylder alle aksiomerne [RAK] – [RD]. Det viser sig imidlertid, at dette eksempel er et specielt tilfælde af det næste, selv om det måske ikke ser sådan ud ved første øjekast.

(4) Lad R være en ring og M en mængde $\neq \varnothing$. Lad R^M være mængden af funktioner $f : M \to R$. Ved hjælp af kompositionerne $+$ og $\cdot$ i R defineres kompositioner (også kaldet $+$ og $\cdot$) i R^M:

Lad $f, g \in R^M$. Sæt

$$(f + g)(m) = f(m) + g(m)$$
$$(fg)(m) = f(m)g(m)$$

for alle $m \in M$.

Så er $f+g$ og fg funktioner fra M til R idet $f(m)$ og $g(m)$ jo er elementer i R. Det er let at se, at hvert af aksiomerne [RAK] – [RD] i R medfører det tilsvarende aksiom i R^M. Nulelementet i R^M er funktionen, hvis værdi på ethvert $m \in M$ er 0 og tilsvarende beskrives 1-elementet (hvis R opfylder [RMN]!) Når $f \in R^M$, er funktionen $-f$ defineret ved $(-f)(m) = -f(m)$.

(5) Vi forklarer nu, hvorfor eksempel (3) ovenfor er "indeholdt" i eksempel (4). Vi lader R være ringen $\mathbf{Z}_2 = \{\widehat{0}, \widehat{1}\}$. Der findes en bijektiv afbildning mellem $\mathcal{P}(M)$ og mængden $\mathbf{Z}_2^M$: Hvis $A \in \mathcal{P}(M)$ lad $f_A \in \mathbf{Z}_2^M$ være defineret ved

$$f_A(m) = \begin{cases} \widehat{1} & \text{hvis } m \in A \\ \widehat{0} & \text{hvis } m \notin A \end{cases}$$

Så f_A er "indikatorfunktionen" for A. Det er velkendt at afbildningen $A \to f_A$ derfor er en bijektion. Kompositionstavlerne i $\mathbf{Z}_2$ er

$+$	$\widehat{0}$	$\widehat{1}$
$\widehat{0}$	$\widehat{0}$	$\widehat{1}$
$\widehat{1}$	$\widehat{1}$	$\widehat{0}$

$\cdot$	$\widehat{0}$	$\widehat{1}$
$\widehat{0}$	$\widehat{0}$	$\widehat{0}$
$\widehat{1}$	$\widehat{0}$	$\widehat{1}$

Derfor er det let at se, at der gælder:

$$\text{For alle } A, B \in \mathcal{P}(M): \quad f_A + f_B = f_{A+B}$$
$$f_A \cdot f_B = f_{A \cap B}.$$

Kompositionerne $+$, $\cdot$ på venstre side af ligningerne er i $\mathbf{Z}_2^M$ og kompositionerne $+$, $\cap$ på højre side er i $\mathcal{P}(M)$. Hvis vi derfor "identificerer" A med f_A for alle A ser vi, at ringene $(\mathcal{P}(M), +, \cap)$ og $(\mathbf{Z}_2^M, +, \cdot)$ falder sammen (inklusiv kompositionerne). Hvis dette forekommer lidt uklart, kan det siges, at vi netop har givet vores første eksempel på en *ringisomorfi*. (Se senere). □

Som nævnt i begyndelsen af Kapitel 2 vil man i en vilkårlig ring R definere "differensen" $a - b$ af $a, b \in R$ som $a + (-b)$, hvor $(-b)$ er bestemt fra b ved [RAI]. Udsagnene i (2.1) gælder i vilkårlige ringe, da beviset kun er baseret på de udsagn, der er ring-
aksiomerne. ([RMK] og [RMN] benyttes ikke.) Vi vil i det følgende benytte disse regler uden for det meste yderligere at henvise til dem.

(3.2) ØVELSE: Betragt $\mathbf{Z}$ med den sædvanlige addition. Vi definerer en ny komposition $*$ på $\mathbf{Z}$ ved $a * b = 2ab$. Undersøg hvilke af aksiomerne [RAK] – [RD] er opfyldte i $(\mathbf{Z}, +, *)$. (Man erstatter altså $\cdot$ i [RMK] – [RD] med $*$). Er $(\mathbf{Z}, +, *)$ en ring? Hvad sker med [RMN], hvis vi erstatter den underliggende mængde $\mathbf{Z}$ med mængden $\mathbf{Q}$ af rationelle tal? Kan $\frac{1}{2}$ være 1-element? □

(3.3) DEFINITION: Lad $(R, +, \cdot)$ være en ring, $S \neq \emptyset$ en delmængde af R. Hvis der gælder

(1) For alle $s, t \in S$ er $s + t \in S$ og $st \in S$.
(2) For alle $s \in S$ er $(-s) \in S$,

kaldes S en *delring* af R. Hvis der yderligere gælder

(3) For alle $a \in R$, $s \in S$ er $as \in S$ og $sa \in S$

kaldes S et *ideal* i R.

Man kan opdele (3) i de to delbetingelser

$(3)_V$ For alle $a \in R$, $s \in S$ er $as \in S$,
$(3)_H$ For alle $a \in R$, $s \in S$ er $sa \in S$.

Hvis S opfylder (1), (2) og $(3)_V$ (hhv. $(3)_H$), kaldes S et *venstreideal* (hhv. *højreideal*) i R. □

(3.4) BEMÆRKNINGER OG EKSEMPLER: 3.3 (1) udsiger, at S er lukket mht. R's kompositioner. Det er ikke svært at se (men heller ikke trivielt!) at en delmængde S af R netop da er en delring, når S er en ring med R's kompositioner. Imidlertid vil man i praksis altid anvende (3.3) (1)–(2) for at eftervise, at S er en delring af R. (Et bevis for den ovenstående påstand kan findes i Allenby s 96–97.)

(2) Hvis R hat et 1-element (kaldet 1_R) og S er en delring af R forlanges det *ikke*, at $1_R \in S$. Alligevel kan S have et (andet) 1-element 1_S, som eksemplet i (3) nedenfor viser. Men *hvis* $1_R \in S$, så er 1_R også 1-element i S. (Overvej).

(3) Betragt delmængden $S = \{\widehat{0}, \widehat{2}, \widehat{4}, \widehat{6}, \widehat{8}\}$ af $\mathbf{Z}_{10}$. Det er let at se, at S er en delring af $\mathbf{Z}_{10}$, endda et ideal. Men S har $\widehat{6}$ som 1-element! (F.eks. er $\widehat{6} \cdot \widehat{4} = \widehat{24} = \widehat{4}$ da $24 \equiv_{10} 4$ og $\widehat{6} \cdot \widehat{8} = \widehat{48} = \widehat{8}$, da $48 \equiv_{10} 8$). Men 1-elementet $\widehat{1} \in \mathbf{Z}_{10}$ er ikke i S.

(4) Hvis S er et *ideal* i R og R's 1-element 1_R er indeholdt i S, så er $R = S$. Ifølge (3) er jo $a = a \cdot 1_R \in S$ for alle $a \in R$.

(5) En ring R har altid de *trivielle* delringe $\{0\}$ af R. Disse er også idealer i R.

(6) I kommutative ringe er betingelserne (3.3) $(3)_V$ og (3.3) $(3)_H$ identiske, (idet $as = sa$) men dette er ikke tilfældet i ikke-kommutative ringe, som det følgende viser:

(7) Lad $R = \mathbf{R}_2^2$ (se (3.1) (2)). Så R er mængden af reelle 2×2-matricer. Betragt delmængden

$$I = \left\{ \begin{bmatrix} b & 0 \\ c & 0 \end{bmatrix} \middle| b, c \in \mathbf{R} \right\}.$$

Hvis $A = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \in R$ og $B = \begin{bmatrix} b & 0 \\ c & 0 \end{bmatrix} \in I$ så er

$$AB = \begin{bmatrix} a_1 b + a_2 c & 0 \\ a_3 b + a_4 c & 0 \end{bmatrix} \in I$$

men

$$BA = \begin{bmatrix} ba_1 & ba_2 \\ ca_1 & ca_2 \end{bmatrix} \notin I \quad (\text{hvis } bca_2 \neq 0).$$

Den første ligning viser, at (3.3) $(3)_V$ er opfyldt og den anden, at (3.3) $(3)_H$ ikke er opfyldt. Det er derfor oplagt, at I er et venstreideal men *ikke* et højreideal i $\mathbf{R}_2^2$. □

(3.5) ØVELSE: Vis, under anvendelse af (2.19), at delringene i $\mathbf{Z}$ netop er $\mathbf{Z}m$, $m \geq 0$. Gør rede for, at begreberne "delring" og "ideal" er sammenfaldende i $\mathbf{Z}$. □

(3.6) ØVELSE: Betragt potensmængderingen $(\mathcal{P}(M), +, \cap)$, M mængde (se (3.1) (3)). Vis, at hvis $A \in \mathcal{P}(M)$, så er $\{\emptyset, A\}$ en delring af $\mathcal{P}(M)$. Er $\{\emptyset, A\}$ et ideal? □

(3.7) ØVELSE: I (3.4) har vi set at $I = \left\{ \begin{bmatrix} b & 0 \\ c & 0 \end{bmatrix} \middle| b, c \in \mathbf{R} \right\}$ er et venstreideal i $\mathbf{R}_2^2$. For $r \in \mathbf{R}$ sætter vi

$$I_r = \left\{ \begin{bmatrix} b & br \\ c & cr \end{bmatrix} \middle| b, c \in \mathbf{R} \right\}$$

$$J = \left\{ \begin{bmatrix} 0 & b \\ 0 & c \end{bmatrix} \middle| b, c \in \mathbf{R} \right\}.$$

(1) Vis, at I_r, $r \in \mathbf{R}$ og J er venstreidealer i $\mathbf{R}_2^2$.

(2) Gør rede for, at $\{0\}, \mathbf{R}_2^2, J$ og I_r, $r \in \mathbf{R}$ er *samtlige* venstreidealer i $\mathbf{R}_2^2$. (Løsningshjælp: Lad K være et venstreideal i $\mathbf{R}_2^2$, $M \in K$. Vis, at hvis man omformer M til en echelon matrix F ved tilladte omformninger, så er $F \in K$. Betragt de forskellige echelonmatricer i $\mathbf{R}_2^2$.)

(3) Bestem alle idealer i $\mathbf{R}_2^2$. □

(3.8) SÆTNING. *Lad R være en ring. Lad M være en mængde, og antag, at der for ethvert $m \in M$ er givet en delring (hhv. et ideal, venstreideal, højreideal) S_m i R. Så er fællesmængden $\cap_{m \in M} S_m$ igen en delring (hhv. et ideal, venstreideal, højreideal) i R.*

BEVIS: En let *øvelse*. □

(3.9) ØVELSE: Lad $X \neq \emptyset$ være en delmængde af ringen R. Sæt

$$_RX = \{a \in R \mid \text{Der findes } m \in \mathbf{N} \text{ og } a_1, \ldots, a_m \in R \text{ og } x_1, \ldots, x_m \in X, \text{ således at } a = a_1x_1 + \cdots + a_mx_m\}.$$

(1) Vis, at $_RX$ er et venstreideal i R.

(2) Vis, at hvis $X \subseteq I$ hvor I er et venstreideal i R, så er $_RX \subseteq I$. ($_RX$ er en analog til den lineære algebras "span X".) (Se også kapitlet om moduler senere). □

(3.10) ØVELSE: Beregn $_RX$ (fra Øvelse (3.9)) i det tilfælde hvor $R = \mathbf{Z}2$ (de hele tal, som er delelige med 2) og $X = \{6\}$. Er $X \subseteq {}_RX$? □

(3.11) DEFINITION: Lad R og S være ringe. Vi betegner kompositionerne i R og S med $+_R$, $\cdot_R$ (for R) og $+_S$, $\cdot_S$ (for S). En funktion $\varphi : R \to S$ kaldes en (*ring-homomorfi* hvis der for alle $r, s \in R$ gælder:

(1) $$\varphi(r +_R s) = \varphi(r) +_S \varphi(s)$$

(2) $$\varphi(r \cdot_R s) = \varphi(r) \cdot_S \varphi(s).$$

Vi har udelukkende medtaget R og S som indices i kompositionerne for at specificere den ring som kompositionerne foretages i. I lighed med definitionen af "lineær afbildning" (se den lineære algebra) skriver vi fra nu af betingelserne (1) og (2) som: For alle $r, s \in R$ gælder

$$(1)\ \varphi(r+s) = \varphi(r) + \varphi(s), \quad (2)\ \varphi(rs) = \varphi(r)\varphi(s).$$

□

(3.12) EKSEMPLER: (1) $\varphi, \psi : R \to R$ givet ved $\varphi(a) = a$ og $\psi(a) = 0$ er homomorfier for alle ringe R.

(2) $\varphi : \mathbf{Z} \to \mathbf{Z}_n$ givet ved $\varphi(a) = \widehat{a}$ er en homomorfi.

(3) $\varphi : \mathbf{Z} \to \mathbf{Z}$ givet ved $\varphi(a) = 2a$ er *ikke* en homomorfi, da (3.11) (2) ikke er opfyldt.

(4) $\psi : \mathbf{Z} \to \mathbf{Z}$ givet ved $\psi(a) = |a|$ er *ikke* en homomorfi, da (3.11) (1) ikke er opfyldt.

(5) Lad $\varphi : R \to S$ være en homomorfi, M en mængde. Så er afbildningen $\varphi^M : R^M \to S^M$ givet ved $\varphi^M(a) = \varphi \circ a$ en homomorfi. (Hvis $a : M \to R$ er en afbildning, så er $\varphi \circ a : M \to S$ afbildningen givet ved $(\varphi \circ a)(m) = \varphi(a(m))$). □

(3.13) SÆTNING. *Lad $\varphi : R \to S$ være en (ring-) homomorfi. Der gælder:*

For alle $a, b \in R$: $\varphi(a-b) = \varphi(a) - \varphi(b)$. Specielt gælder (når $a = b$) $\varphi(0) = 0$ og (når $a = 0$) $\varphi(-b) = -\varphi(b)$.

BEVIS: Vi har $\varphi(a-b)+\varphi(b) = \varphi((a-b)+b) = \varphi((a+(-b))+b) = \varphi(a+((-b)+b)) = \varphi(a+0) = \varphi(a)$ altså $\varphi(a-b)+\varphi(b) = \varphi(a)$. Ifølge (2.1) (1) (anvendt i S) fås $\varphi(a-b) = \varphi(a) - \varphi(b)$. □

(3.14) DEFINITION: Lad $\varphi : R \to S$ være en homomorfi. Vi definerer *kernen af φ* og *billedet af φ* ved

$$\ker\varphi = \{a \in R \mid \varphi(a) = 0\}$$
$$\varphi(R) = \{b \in S \mid \text{Der findes et } a \in R \text{ så } \varphi(a) = b\}.$$

(Sammenlign med tilsvarende begreber i lineær algebra.) □

(3.15) SÆTNING. *Lad $\varphi : R \to S$ være en homomorfi. Der gælder*

(1) *$\ker\varphi$ er et ideal i R*

(2) *$\varphi(R)$ er en delring (men i almindelighed ikke et ideal) i S.*

BEVIS: (1) Lad $a, b \in \ker\varphi$, så $\varphi(a) = \varphi(b) = 0$. Så er $\varphi(a+b) = \varphi(a) + \varphi(b) = 0 + 0 = 0$ og $\varphi(ab) = \varphi(a)\varphi(b) = 0 \cdot 0 = 0$. (At $0 \cdot 0 = 0$ fås f.eks. fra (2.1) (2) anvendt på S!) Lad $r \in R$. Så er $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$ (igen (2.1) (2)) og

analogt $\varphi(ar) = 0$. Fra (3.13) ses at $\varphi(-a) = -\varphi(a) = -0 = 0$. Hermed er (3.3) (1)–(3) opfyldte og $\ker\varphi$ ideal.

(2) Beviset for, at $\varphi(R)$ er en delring af S overlades til læseren. At $\varphi(R)$ ikke er et ideal vises ved et eksempel: Lad $R = \mathbf{Z}$, $S = \mathbf{Q}$ og $\varphi : R \to S$ givet ved $\varphi(a) = a$. φ er en homomorfi af $\varphi(R) = \mathbf{Z}$ (som delring af $\mathbf{Q}$). Men $\mathbf{Z}$ er ikke et ideal i $\mathbf{Q}$ ifølge (3.4) (4). □

(3.16) DEFINITION: Hvis I er en delring af R defineres relationen $\equiv_I$ (*"kongruent modulo I"*) ved

$$a \equiv_I b \Leftrightarrow a - b \in I.$$

□

Relationen $\equiv_n$ fra (2.31) er et specielt tilfælde af det ovenstående, idet $\mathbf{Z}n$ er en delring af $\mathbf{Z}$ (se (3.5)) og så er $\equiv_n$ det samme som $\equiv_{\mathbf{Z}n}$. Derfor er de næste resultater udvidelser fra (2.31) (1) og (2.33).

(3.17) SÆTNING. *Hvis I er en delring af R, så er $\equiv_I$ en ækvivalensrelation.*

BEVIS: $a - a = 0 \in I$, så [BRR] er opfyldt. Hvis $a - b \in I$ så er $b - a = -(a - b) \in I$, så [BRS] er opfyldt. Hvis $a - b \in I$ og $b - c \in I$ så er $a - c = (a - b) + (b - c) \in I$, så [BRT] er opfyldt. □

(3.18) SÆTNING. *Lad I være et ideal i ringen R, $a, b, c, d \in R$. Antag, at $a \equiv_I c$, $b \equiv_I d$. Så gælder*

(1) $a + b \equiv_I c + d$,
(2) $ab \equiv_I cd$.

BEVIS: Lad $a - c = k \in I$ og $b - d = \ell \in I$. Så er $(a + b) - (c + d) = k + \ell \in I$. Desuden gælder, da I er et ideal, at $kb \in I$, da $k \in I$ og $c\ell \in I$, da $\ell \in I$. Dermed er $kb + c\ell \in I$. Men $kb + c\ell = (a - c)b + c(b - d) = ab - cb + cb - cd = ab - cd$. □

(Lad os nævne, at vi i det ovenstående bevis ikke har benyttet noget udsagn om at R skal være kommutativ. Ved beregning af produkter i generelle ringe er faktorernes orden *ikke* ligegyldig.)

(3.19) DEFINITION AF FAKTORRINGE: Lad I være et ideal i ringen R. Lad R/I betegne mængden af ækvivalensklasser for ækvivalensrelationen $\equiv_I$. Så $R/I = \{\widehat{a} \mid a \in R\}$, $\widehat{a} = \{b \in R \mid a - b \in I\}$. ($\widehat{a}$ kaldes en *restklasse modulo I*). Vi definerer addition og multiplikation af $\widehat{a}, \widehat{b} \in R/I$ ved

$$\widehat{a} + \widehat{b} = \widehat{a + b}, \quad \widehat{a}\,\widehat{b} = \widehat{ab}.$$

Som i (2.34) må vi overveje om der gælder $\widehat{a} + \widehat{b} = \widehat{c} + \widehat{d}$, $\widehat{a}\,\widehat{b} = \widehat{c}\,\widehat{d}$ hvis $a \equiv_I c$ og $b \equiv_I d$. Men dette følger af (3.18). Det er så let at se, at R/I opfylder mindst de

samme aksiomer (blandt [RAK]-[RD]) som R, så R/I er en ring, kaldet *faktorringen modulo* I. □

(3.20) DEFINITION: Lad $\varphi : R \to S$ være en homomorfi, φ kaldes en *monomorfi*, hvis φ er injektiv, en *epimorfi*, hvis φ er surjektiv, og en *isomorfi*, hvis φ er en bijektion. Vi skriver $R \simeq S$, hvis der findes en isomorfi mellem R og S. □

(3.21) ØVELSE: Lad R, S og T være ringe. Lad $\varphi : R \to S$ og $\psi : S \to T$ være homomorfier. Lad $\psi \circ \varphi$ være den sammensatte afbildning $R \to T$. Vis:

(1) $\psi \circ \varphi$ er en homomorfi.
(2) Hvis φ er en isomorfi, da er φ^{-1} en isomorfi.
(3) φ er en monomorfi $\Leftrightarrow \ker \varphi = \{0\}$.

(Man kan lade sig inspirere af beviser i den lineære algebra.) □

(3.22) SÆTNING. *Lad I være et ideal i R. Afbildningen $\pi : R \to R/I$ givet ved $\pi(a) = \widehat{a}$ er en (ring-)epimorfi og $\ker \pi = I$.*

BEVIS: Det er helt oplagt, at π er en surjektiv homomorfi (f.eks. er $\pi(a+b) = \widehat{a+b} = \widehat{a} + \widehat{b} = \pi(a) + \pi(b)$). Hvis $a \in I$ så er $a \equiv_I 0$ og dermed $\widehat{a} = \widehat{0}$. Da $\widehat{0}$ er nulelementet i R/I (hvorfor ?) er $a \in \ker \pi$. Omvendt, lad $a \in \ker \pi$. Så er $\widehat{a} = \pi(a) = \widehat{0}$, altså $\widehat{a} = \widehat{0}$, dvs. $a \equiv_I 0$ eller $a \in I$. □

(3.23) BEMÆRKNING: Hvis vi kombinerer (3.15) (1) og (3.22) ser vi at der gælder:
Hvis I er en delmængde af R, så er I netop da et ideal i R når der findes en ring S og en ringhomomorfi $\varphi : R \to S$ med $\ker \varphi = I$. □

(3.24) SÆTNING. *(Isomorfisætningen for ringe):*
Lad $\varphi : R \to S$ være en homomorfi. Afbildningen $\bar{\varphi} : R/\ker \varphi \to \varphi(R)$ defineret ved $\bar{\varphi}(\widehat{a}) = \varphi(a)$ er en isomorfi. Der gælder altså

$$R/\ker \varphi \simeq \varphi(R).$$

BEVIS: For at vise, at $\bar{\varphi}$ overhovedet er veldefineret må vises, at hvis $\widehat{a} = \widehat{b}$ så er $\varphi(a) = \varphi(b)$: $\widehat{a} = \widehat{b} \Rightarrow a - b \in \ker \varphi \Rightarrow \varphi(a) - \varphi(b) = \varphi(a-b) = 0 \Rightarrow \varphi(a) = \varphi(b)$. Det er klart, at $\bar{\varphi}$ er surjektiv ($\widehat{a}$ er et urbillede for $\varphi(a)$ under $\bar{\varphi}$). Endvidere gælder $\widehat{a} \in \ker \bar{\varphi} \Leftrightarrow \varphi(a) = 0 \Leftrightarrow a \in \ker \varphi \Leftrightarrow a - 0 \in \ker \varphi \Leftrightarrow a \equiv_{\ker \varphi} 0 \Leftrightarrow \widehat{a} = \widehat{0}$, så $\ker \bar{\varphi} = \{\widehat{0}\}$. Ifølge (3.21) (3) er det så nok at vise, at $\bar{\varphi}$ er en homomorfi. Men

$$\begin{aligned}
\bar{\varphi}(\widehat{a} + \widehat{b}) &= \bar{\varphi}(\widehat{a+b}) && \text{(addition i } R/\ker\varphi) \\
&= \varphi(a+b) && \text{(definition af } \bar{\varphi}) \\
&= \varphi(a) + \varphi(b) && (\varphi \text{ en homomorfi}) \\
&= \bar{\varphi}(\widehat{a}) + \bar{\varphi}(\widehat{b}) && \text{(definition af } \bar{\varphi}).
\end{aligned}$$

Analogt vises $\bar{\varphi}(\widehat{a}\,\widehat{b}) = \bar{\varphi}(\widehat{a})\bar{\varphi}(\widehat{b})$. □

(3.25) BEMÆRKNING: Der findes tilsvarende isomorfisætninger som (3.24) for andre algebraiske strukturer, f.eks. for vektorrum og grupper. For vektorrum kan isomorfisætningen beskrives som følger: Lad U være et underrum af vektorrummet V. Så er relationen $\equiv_U$ defineret ved $\underline{v} \equiv_U \underline{w} \Leftrightarrow \underline{v} - \underline{w} \in U$ en ækvivalensrelation på V. På mængden V/U af ækvivalensklasser for $\equiv_U$ defineres en vektorrumsstruktur ved

$$\widehat{\underline{v}} + \widehat{\underline{w}} = \widehat{\underline{v} + \underline{w}}$$

$$\underline{v}, \underline{w} \in V, c \in \mathbf{R}$$

$$c\widehat{\underline{v}} = \widehat{c\underline{v}}$$

Hvis $\varphi : V \to W$ er en lineær afbildning gælder at $V/\ker\varphi \simeq \varphi(V)$ (isomorfi af vektorrum). Dette er isomorfisætningen for vektorrum. Det er let at se, at $\dim(V/\ker\varphi) = \dim V - \dim\ker\varphi$ så denne isomorfisætning er logisk ækvivalent med *Dimensionssætningen for lineær afbildning*. Hvis det ønskes, kan denne bemærkning uddybes i en øvelsestime. Se også kapitlet om moduler. □

Vi betragter nu endnu en betingelse som er ring R med 1-element kan opfylde

[*RMI*] For alle $a \neq 0$ eksisterer et element a^{-1}, således at $aa^{-1} = a^{-1}a = 1$.

(3.26) DEFINITION: Lad $R \neq \{0\}$ være en *kommutativ* ring med 1-*element*. Hvis R opfylder [NU] kaldes R en *integritetsring* (= *integritetsområde*, *domain*). Hvis $R \neq \{0\}$ opfylder [RMI] kaldes R et *legeme*. (Man kan evt. sammenligne med definitionen af legeme i den lineære algebra.) □

(3.27) ØVELSE: Gør rede for at i en kommutativ ring med 1 medfører [RMI] betingelsen [NU]. (Man kan lade sig inspirere af beviset for HBF 27.4 (2) (e)!). Dette viser, at et *legeme er en integritetsring*. Ringen $\mathbf{Z}$ er en integritetsring men ikke et legeme. □

(3.28) DEFINITION: Lad $I(\neq R)$ være et ideal i ~~den kommutative ring~~ R~~, med 1-element~~. Vi betragter betingelserne:

[IM] Hvis J er et ideal i R med $I \subseteq J \subseteq R$ gælder enten $I = J$ eller $J = R$.

[IP] Hvis $a, b \in R$ opfylder $ab \in I$, gælder enten $a \in I$ eller $b \in I$.

Når I opfylder [IM] kaldes I et *maksimalt ideal*. Når I opfylder [IP], kaldes I et *primideal*. □

Teorien for faktorringe giver en interessant og vigtig forbindelse mellem definitionerne (3.26) og (3.28):

(3.29) SÆTNING. *Lad I være et ideal i den kommutative ring R med 1-element. Der gælder*

(1) *I er et primideal $\Leftrightarrow$ R/I er en integritetsring.*
(2) *I er et maksimalt ideal $\Leftrightarrow$ R/I er et legeme.*
(3) *Hvis I er maksimalt, så er I et primideal.*

BEVIS: (1) $\Rightarrow$ Lad I være et primideal. Antag, at $\widehat{a}, \widehat{b} \in R/I$ og $\widehat{a}\,\widehat{b} = \widehat{0}$. Så er $\widehat{ab} = \widehat{0}$, så $ab \in I$. Ifølge [IP] gælder enten $a \in I$ (altså $\widehat{a} = \widehat{0}$) eller $b \in I$ (altså $\widehat{b} = \widehat{0}$). Dermed opfylder R/I [NU]. $\Leftarrow$ Antag, at R/I opfylder [NU]. Lad $a, b \in R$ så $ab \in I$. Så er $\widehat{a}\,\widehat{b} = \widehat{ab} = \widehat{0}$. Ifølge [NU] gælder så $\widehat{a} = \widehat{0}$ (altså $a \in I$) eller $\widehat{b} = \widehat{0}$ (altså $b \in I$). Dermed opfylder I betingelsen [IP].

(2) $\Rightarrow$ Lad I være et maksimalt ideal i R. Lad $\widehat{a} \in R/I$, $\widehat{a} \neq \widehat{0}$. Dermed er $a \notin I$. Betragt delmængden $J = I + Ra = \{i + ra \mid i \in I, r \in R\}$. Det er let at se, at J er et ideal i R (overvej dette, eller vent til Øvelse (3.32).) Det er klart, at $I \subseteq J$ ($r = 0$). På den anden side er $I \neq J$, da $a = 0 + 1a \in J$ og $a \notin I$. [IM] medfører at $J = R$. Da $1 \in R$ eksisterer $i \in I$, $r \in R$ så $i + ra = 1$. Så er $\widehat{r}\,\widehat{a} = \widehat{ra} = \widehat{1 - i} = \widehat{1} - \widehat{i} = \widehat{1}$, da $\widehat{i} = \widehat{0}$ ($i \in I$). Vi har også $\widehat{a}\,\widehat{r} = 1$, så $\widehat{r}$ er "inverst" element til $\widehat{a}$. $\Leftarrow$ Lad R/I være et legeme og J et ideal med $I \subseteq J \subseteq R$. Det er let at se, at $\widehat{J} = \{\widehat{j} \mid j \in J\}$ er et ideal i R/I. Dermed en enten $\widehat{J} = \{\widehat{0}\}$ eller $\widehat{J} = R/I$. (Se Øvelse (3.31)). Da $I \subseteq J$, er det let at se, at hvis $\widehat{J} = \{\widehat{0}\}$ er $I = J$. Ellers er $J = R$.

(3) I maksimalt ideal $\Rightarrow$ R/I legeme (ifølge (2))
$\Rightarrow$ R/I integritetsring (ifølge (3.27)).
$\Rightarrow$ I primideal (ifølge (1)).

□

(3.30) ØVELSE: Bestem alle maksimale idealer og alle primidealer i $\mathbb{Z}$. (Man kan anvende (3.5) og (2.22).) □

(3.31) ØVELSE: Lad I være et ideal i legemet R. Vis under anvendelse af [RMI], at hvis $I \neq 0$ er $1 \in I$. Slut heraf, at $\{0\}$ og R er de eneste idealer i R. □

(3.32) ØVELSE: Lad I, J være idealer i R.

(1) Gør rede for, at

$$I + J = \{i + j \mid i \in I, j \in J\}$$

og

$$I \cdot J = \{a \mid \text{Der findes et } m \in \mathbb{N} \text{ og elementer } i_1, \ldots, i_m \in I, j, \ldots, j_m \in J \text{ så } a = i_1 j_1 + \cdots + i_m j_m\}$$

er idealer i R.

(2) Bestem $I + J$ og $I \cdot J$ i det tilfælde, hvor $R = \mathbb{Z}$, $I = 6\mathbb{Z}$, $J = 4\mathbb{Z}$.

□

(3.33) ØVELSE: Lad N være en delmængde af mængden M. Definer en afbildning $\varphi_N : \mathcal{P}(M) \to \mathcal{P}(N)$ ved

$$\varphi_N(A) = A \cap N.$$

Vis, at φ_N er en ringepimorfi. Hvad er $\ker \varphi_N$? □

(3.34) ØVELSE: Undersøg om afbildningen $\varphi : \mathbf{Z}_{12} \to \mathbf{Z}_{12}$ givet ved

$$\varphi(\widehat{a}) = \widehat{4a}$$

er en ringhomomorfi og bestem i givet fald ker φ. □

(3.35) ØVELSE: Lad R være en kommutativ ring med 1. For $e \in R$ defineres en afbildning $m_e : R \to R$ ved $m_e(a) = ea$. Vis, at m_e er en homomorfi netop da, når $e^2 = e$. (Er denne øvelse relevant til (3.34)?) □

(3.36) ØVELSE: Lad $\varphi : R \to S$ være en ringisomorfi. Vis I er et ideal i $R \Leftrightarrow \varphi(I)$ er et ideal i S. □

(3.37) SÆTNING (KORRESPONDANCE MELLEM IDEALER). *Lad I være et ideal i R og $\pi : R \to R/I$ defineret ved $\pi(r) = \widehat{r}$ (den "kanoniske epimorfi"). Så inducerer π en bijektion mellem*

(1) *Mængden af idealer i R, som indeholder I og*
(2) *Mængden af idealer i faktorringen R/I.*

Denne bijektion bevarer maksimale idealer.

BEVIS: Øvelse. (Den naturlige bijektion f er givet ved, at hvis J er et ideal i R, som indeholder I, så er $f(J) := \pi(J)$.) □

Kapitel 4. Faktoriseringsteori i kommutative ringe.

Vi starter med et par nye eksempler på ringe, som vil være nyttige illustrationer i det følgende.

(4.1) EKSEMPLER: (1) Lad R være en kommutativ ring med 1-element. Vi betragter *polynomiumsringen i* R, $R[t]$. Et polynomium $p(t)$ med koefficienter i R er et udtryk

$$p(t) = a_m t^m + a_{m-1} t^{m-1} + \cdots + a_1 t + a_0,$$

hvor $a_0, a_1, \ldots, a_m \in R$ (og $m \in \mathbb{N} \cup \{0\}$). Hvis $a_m \neq 0$ siges $p(t)$ at have *grad* m og vi skriver $\deg(p) = m$ og a_m kaldes *højestegradkoefficienten.* Vi kalder a_0 *konstantleddet.* (Vi vil *ikke*, som det somme tider gøres, betragte $p(t)$ som en funktion fra $R \to R$, men foretrækker en mere "formel" beskrivelse, hvor t er en "variabel"). Hvis $p(t)$ er som ovenfor skriver vi

$$p(t) = \sum_{i=0}^{m} a_i t^i \qquad \text{(således at } t^0 = 1\text{)}$$

Summationsrækkefølgen er underordnet. Hvis

$$p(t) = \sum_{i=0}^{m} a_i t^i, \quad q(t) = \sum_{i=0}^{n} b_i t^i$$

er polynomier, anses de for ens, hvis $a_i = b_i$ for alle relevante i, og vi sætter generelt

$$(p+q)(t) = \sum_{i=0}^{\max(m,n)} (a_i + b_i) t^i$$

og

$$(pq)(t) = \sum_{i=0}^{m+n} c_i t^i,$$

hvor $c_i = \sum_{j=0}^{i} a_j b_{i-j}$. (Altså $c_0 = a_0 b_0, c_1 = a_0 b_1 + a_1 b_0, \ldots$). I begge tilfælde antages $a_i = 0$ for $i \geq m+1$, $b_i = 0$ for $i \geq n+1$. Når $R[t]$ er mængden af polynomier med koefficienter i R, så er $(R[t], +, \cdot)$ en kommutativ ring med 1-element. (1-elementet er polynomiet med konstantleddet lig 1 og alle andre koefficienter 0). Vi kan betragte R som delring af $R[t]$, dvs. som mængden af polynomier med alle koefficienter lig 0 pånær konstantleddet (de "konstante" polynomier).

(2) Et tal $n \in \mathbb{Z}$, $n \neq 0, 1$ kaldes *kvadratfri*, hvis der gælder for alle $d \in \mathbb{Z}$: $n | d^2 \Rightarrow n | d$. Det betyder, at primfaktorerne, som indgår i faktoriseringen af n ((2.30)) alle er forskellige. (F.eks. er altså $30 = 2 \cdot 3 \cdot 5$ kvadratfri, men $12 = 2 \cdot 2 \cdot 3$ ikke). Lad $n \in \mathbb{Z}$ være kvadratfri. Så er

$$\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$$

en delring af legemet $\mathbb{C}$ af komplekse tal ($\mathbb{C} = \{x + iy \mid x, y \in \mathbb{R}\}$, $i^2 = -1$. Se de relevante dele af Mat 1). (Hvis $r = a + b\sqrt{n}$, $s = c + d\sqrt{n}$ er i $\mathbb{Z}[\sqrt{n}]$ så er også $r + s = (a + c) + (b + d)\sqrt{n}$, og $rs = (ac + bdn) + (ad + bc)\sqrt{n} \in \mathbb{Z}[\sqrt{n}]$).

Hvis $n > 0$ er $\mathbb{Z}[\sqrt{n}]$ endda en delring af $\mathbb{R}$. Når $n < 0$ er $-n > 0$ og $\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{-n}i \mid a, b \in \mathbb{Z}\}$ ($\subseteq \mathbb{C}$).

Af speciel interesse er $\mathbb{Z}[\sqrt{-1}] = \{a + bi \mid a, b \in \mathbb{Z}\}$, ringen af "gaussiske hele tal". Ringene $\mathbb{Z}[\sqrt{n}]$ har en vigtig *normafbildning* N, hvis definition og fundamentale egenskaber beskrives i den næste øvelse.

(3) Man kan også betragte delringene

$$\mathbb{Q}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Q}\}$$

af $\mathbb{C}$, hvor igen n er kvadratfri. □

(4.2) ØVELSE: Lad $n \in \mathbb{Z}$ være kvadratfri. Betragt afbildningen $N : \mathbb{Z}[\sqrt{n}] \to \mathbb{N} \cup \{0\}$ defineret ved $N(r) = |a^2 - b^2 n|$, hvor $r = a + b\sqrt{n}$, $a, b \in \mathbb{Z}$. Vis, at der gælder

$$\text{For alle } r, s \in \mathbb{Z}[\sqrt{n}] : \begin{cases} N(rs) = N(r)N(s) \\ N(r) = 0 \Leftrightarrow r = 0. \end{cases}$$

($|\cdot|$ er absolutværdien som defineret i §2. Det er klart, at (2.5) (1) og (2.5) (3) spiller en rolle i beviset.) □

(4.3) SÆTNING. *Lad R være en kommutativ ring med 1-element. For alle $p, q \in R[t]$ gælder*

(1) $\deg(p + q) \leq \max(\deg(p), \deg(q))$.
(2) $\deg(pq) \leq \deg p + \deg q$.
(3) *Hvis R er en integritetsring, gælder lighedstegn i (2).*
(4) *R er en integritetsring $\Leftrightarrow$ $R[t]$ er en integritetsring.*

(Før beviset af (4.3) må vi overveje, hvad $\deg p$ er, når p er nulpolynomiet (alle koefficienter $= 0$). Hvis man sætter $\deg p = -\infty$ *for nulpolynomiet* og benytter regnereglen: $(-\infty) + m = -\infty$, samt antager $-\infty \leq m$ for alle m, er det let at se, at (4.3) (1)–(3) er rigtige, hvis p eller q er nulpolynomiet).

BEVIS FOR (4.3): (1) og (2) følger let fra definitionerne.

(3) Antag at R er en integritetsring. Antag at $p \neq 0, q \neq 0$. Lad a_m og b_n være højestegradskoefficienterne i p og q, hvor $m = \deg p, n = \deg q$. Så er $a_m b_n \neq 0$ ifølge [NU], således at $a_m b_n$ er højestegradkoefficient i pq. Dermed er

$$\deg pq = m + n = \deg p + \deg q.$$

(4) Ifølge definitionen er $p \neq 0 \Leftrightarrow \deg p \geq 0$. Derfor viser (3), at $p \neq 0 \wedge q \neq 0 \Rightarrow pq \neq 0$ eller (hvad der er det samme) $pq = 0 \Rightarrow p = 0 \vee q = 0$. Så når R opfylder

[NU], så gør $R[t]$ det også. På den anden side er det klart, at hvis $R[t]$ opfylder [NU], så vil enhver delring af $R[t]$ (specielt R) opfylde [NU]. □

I resten af dette kapitel vil vi antage, at R er en *integritetsring*.

Vi overtager delelighedsbegreberne fra Kapitel 2. Når $a, b \in R$, beskrives relationen $b|a$ som i (2.7) og definitionen af et *invertibelt*, hhv. *irreducibelt*, hhv. *prim-element* overtages ordret fra (2.8)(1)–(3), ligesom definitionen af *associerede elementer* overtages fra (2.8)(4).

Ifølge (2.15) gælder i R

(4.4) SÆTNING. *Ethvert primelement i R er irreducibelt.*

□

(4.5) EKSEMPEL: Vi betragter $R = \mathbf{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbf{Z}\}$. Formålet med dette eksempel er at vise: (1) Elementet $4 \in R$ har to essentielt forskellige* faktoriseringer som produkt af irreducible elementer i R. (2) Elementet $2 \in R$ er irreducibelt men *ikke* et primelement i R. Vi starter med nogle observationer: (3) Hvis $a+b\sqrt{-3} = c+d\sqrt{-3}$, $a, b, c, d \in \mathbf{Z}$ så er $a = c$ og $b = d$. (Dette gælder da $\sqrt{-3} \notin \mathbf{Q}$.) (4) De eneste invertible elementer i R er ± 1. (Vi betragter normafbildningen $N : R \to \mathbf{N} \cup \{0\}$ defineret som $N(a+b\sqrt{-3}) = a^2+3b^2$. Det er så klart at kun ± 1 har norm 1. Antag nu at $r = a + b\sqrt{-3}$, $s = c + d\sqrt{-3}$ og at $rs = 1$. Så er $N(r)N(s) = N(rs) = N(1) = 1$ ifølge (4.2). Derfor må $N(r) = N(s) = 1$, så vi har $r = s = \pm 1$.) (5) Elementerne $1 + \sqrt{-3}$, $1 - \sqrt{-3}$ og 2 er irreducible i R. (Antag at $1 + \sqrt{-3} = rs$, hvor $r = a + b\sqrt{-3}$, $s = c + d\sqrt{-3}$. Så er $4 = N(1+\sqrt{-3}) = N(r)N(s)$. Hvis hverken r eller s er invertibelt, er $N(r) \neq 1$ og $N(s) \neq 1$, så vi får $N(r) = N(s) = 2$. Men det er let at se, at der ikke findes hele tal a, b med $a^2 + 3b^2 = 2$. Derfor findes ingen elementer i R af norm 2. Så enten r eller s er invertibelt. Da $1 - \sqrt{-3}$ og 2 har norm 4 fås analogt, at $1 - \sqrt{-3}$ og 2 er irreducible.) Det er klart, at

$$4 = 2 \cdot 2 = (1 - \sqrt{-3})(1 + \sqrt{-3})$$

og at $2 \top 1 + \sqrt{-3}$, $2 \top 1 - \sqrt{-3}$. (Overvej!) Dermed er 2 ikke et primelement. De ovenstående faktoriseringer af 4 som produkt af irreducible elementer er forskellige.

□

(4.6) ØVELSE: (1) Vis, at de eneste invertible elementer i $\mathbf{Z}[\sqrt{-1}] = \mathbf{Z}[i]$ er ± 1 og $\pm i$.

(2) Vis, at $2 - \sqrt{3}$ er invertibelt i $\mathbf{Z}[\sqrt{3}]$.

(3) Er $1 - \sqrt{3}$ invertibelt i $\mathbf{Z}[\sqrt{3}]$?

□

(4.7) ØVELSE: Vis på en analog måde til (4.5), at

$$21 = 7 \cdot 3 = (1 - 2\sqrt{-5})(1 + 2\sqrt{-5}) \quad (\text{i } \mathbf{Z}[\sqrt{-5}])$$

* "essentiell forskellig" præciseres i (1.22).

giver 2 essentielt forskellige faktoriseringer af 21 som produkt af irreducible elementer, og at 3 ikke er et primelement i $\mathbf{Z}[\sqrt{-5}]$. □

Vi vil nu anvende tre aspekter af faktoriseringsteorien i $\mathbf{Z}$ til at definere tre klasser af ringe: *Euklidiske ringe* (udgangspunkt er eksistensen af en norm/absolutværdi; for $\mathbf{Z}$ er det "modulus", se (2.5) og (2.18)), *Hovedidealringe* (ethvert ideal har formen $Rm, m \in R$; for $\mathbf{Z}$ er dette (2.19) og (3.5)), *Gaussiske ringe* (eksistens af entydig primelementfaktorisering; for $\mathbf{Z}$ er det (2.30)). Vores mål vil være at vise

$$R \text{ Euklidisk} \overset{(4.15)}{\Rightarrow} R \text{ Hovedidealring} \overset{(4.25)}{\Rightarrow} R \text{ Gaussisk.}$$

(4.8) DEFINITION: R kaldes *Euklidisk* hvis der findes en (norm-)afbildning

$$\delta : R \setminus \{0\} \longrightarrow \mathbf{N} \cup \{0\}$$

som opfylder

(1) For alle $a, b \in R \setminus \{0\}$ er $\delta(a) \leq \delta(ab)$.
(2) For alle $a, b \in R$, $b \neq 0$ eksisterer $m, r \in R$ således at $a = mb + r$ og $\delta(r) < \delta(b)$, hvis $r \neq 0$.

□

(4.9) EKSEMPLER PÅ EUKLIDISKE RINGE: (1) $\mathbf{Z}$ med $\delta(a) = |a|$.
(2) $\mathbf{Q}[t]$ med $\delta(p) = \deg p$ (se Øvelse (4.11)).
(3) $\mathbf{Z}[i]$ med $\delta(a) = N(a)$ (som i (4.2)). Dette gør vi nu rede for: At (4.8)(1) er opfyldt følger af (4.2). Sæt $R = \mathbf{Z}[i]$. R er en delring af legemet $\mathbf{C}$ af komplekse tal. Normen N på R kan selvfølgelig udvides til vilkårlige komplekse tal $x + iy$, $(x, y \in \mathbf{R})$ ved $N(x + iy) = x^2 + y^2$. (Dette er kvadratet af den sædvanlige "norm" i $\mathbf{C}$). Når $x + iy \in \mathbf{C} \setminus \{0\}$ er $(x + iy)^{-1} = (x - iy)/N(x + iy) = (x - iy)/(x^2 + y^2)$ netop det inverse element til $x + iy$ i $\mathbf{C}$. Lad $a, b \in R$, $b \neq 0$. Vi betragter (det komplekse tal) $ab^{-1} = x + iy$. Så $x, y \in \mathbf{R}$. (Faktisk er $x, y \in \mathbf{Q}$ ifølge den ovennævnte formel for inverse elementer). Vælg hele tal $k, \ell \in \mathbf{Z}$ således at $|x - k| \leq \frac{1}{2}$, $|y - \ell| \leq \frac{1}{2}$. (Hvorfor findes sådanne tal k, ℓ?) Sæt $m = k + i\ell$, $r = a - bm$. Da $k, \ell \in \mathbf{Z}$ er $m \in R$. Da $a, b \in R$ fås også $r \in R$. De ovenstående ligninger viser, at

$$(x - k) + i(y - \ell) = ab^{-1} - m = rb^{-1}.$$

Dermed er (da $N(b^{-1}) = N(b)^{-1}$), når $r \neq 0$

$$\begin{aligned} &N(r)N(b)^{-1} = N(r)N(b^{-1}) = N(rb^{-1}) \\ &= N((x - k) + i(y - \ell)) = (x - k)^2 + (y - \ell)^2 \leq (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 < 1 \end{aligned}$$

altså

$$N(r)N(b)^{-1} < 1 \quad \text{eller} \quad N(r) < N(b).$$

Dermed har m, r de ønskede egenskaber. (Dette argument er måske det mest avancerede vi har set indtil nu i disse noter. Man kan overveje, om vi "snyder" ved at forlade R og gå ud i $\mathbb{C}$ for at bevise en påstand om R! Men da $\mathbb{C}$ jo findes og vi kun har anvendt kendte egenskaber ved $\mathbb{C}$, er vores argument holdbart. Det repræsenterer på sin vis en nyttig standardargumentation i algebraen.) □

(4.10) ØVELSE: Vis at $\mathbb{Z}[\sqrt{-2}]$ er en Euklidisk ring, og at $\mathbb{Q}[i]$ er et legeme. □

(4.11) ØVELSE: Vis at $\mathbb{Q}[t]$ er en Euklidisk ring. □

(4.12) EKSEMPEL: Som nævnt skal elementer i Gaussiske ringe have en entydig "primelementfaktorisering". Derfor viser (4.5) og (4.7) at $\mathbb{Z}[\sqrt{-3}]$ og $\mathbb{Z}[\sqrt{-5}]$ ikke er Gaussiske ringe og altså (se senere) heller ikke Euklidiske ringe. □

(4.13) DEFINITION: Hvis $m \in R$, sættes $Rm = \{rm | r \in R\}$. Da R er kommutativ er det let at se, at Rm er et ideal i R. Et ideal i R på formen Rm kaldes et *hovedideal*. Hvis ethvert ideal i R er et hovedideal, kaldes R en *hovedidealring*. ($\mathbb{Z}$ er et eksempel herpå, (3.5)). (Hoved-ideal-ring på engelsk P.I.D., principal ideal domain) □

(4.14) BEMÆRKNING: Lad Rm og Rn være hovedidealer i R. Der gælder $Rm \subseteq Rn \Leftrightarrow n|m$. (Overvej!) Så $Rm = Rn \Leftrightarrow m$ og n er associerede. (Se (2.11)). Da $R = R1$ gælder specielt: $Rm = R \Leftrightarrow m$ invertibel. (Selvfølgelig er netop de invertible elementer associeret til 1). □

(4.15) SÆTNING. *Enhver Euklidisk ring er en hovedidealring.*

BEVIS: Lad $I \neq \{0\}$ være et ideal i den Euklidiske ring R med norm δ. Delmængden $T = \{\delta(a) \mid a \in I, a \neq 0\}$ af $\mathbb{N} \cup \{0\}$ er ikke-tom, så ifølge [MIN] eksisterer et $t \in T$ så $t \leq s$ for alle $s \in T$. Lad $b \in I$ således at $\delta(b) = t$. Vi påstår at $I = Rb$. I hvert fald gælder $Rb \subseteq I$, (da $b \in I$ og I er et ideal). Antag nu at $a \in I$. Under anvendelse af (4.8)(2) skrives $a = mb + r$, hvor $\delta(r) < \delta(b)$, hvis $r \neq 0$. (Hvorfor er $b \neq 0$?) Da $mb \in I$ og $a \in I$ er $r = a - mb \in I$. Ifølge valget af b gælder $\delta(b) \leq \delta(r)$, hvis $r \neq 0$. Derfor må $r = 0$, altså $a = mb \in Rb$. Vi har så også vist at $I \subseteq Rb$, altså $I = Rb$ er et hovedideal. Da I var vilkårligt ($\neq \{0\}$) valgt (selvfølgelig er $\{0\} = R0$ et hovedideal) er R en hovedidealring. □

(Det kan være interessant at sammenligne det ovenstående bevis med (2.19).)

I hovedidealringe (og altså også i Euklidiske ringe) er der en pæn teori for "største fælles divisor" (s.f.d). Når $a, b \in R$ benytter vi (2.20) til at definere en s.f.d. c for a og b. Hvis $c, c' \in R$ og c er en s.f.d. for a, b så er c' netop da en s.f.d. for a, b når c og c' er associerede. (Se (2.21)). Det følgende er åbenbart en udvidelse af (2.23) og (2.24):

(4.16) SÆTNING. *Lad R være en hovedidealring. Lad $a, b \in R$. Betragt idealet $I = Ra + Rb = \{ka + \ell b \mid k, \ell \in R\}$ i R.*

(1) *Der gælder $I = Rc$ for et $c \in R$ netop da når c er en s.f.d. for a og b.*

(2) *Der findes en s.f.d. c for a og b, og c kan skrives som $c = ka + \ell b$ for passende $k, \ell \in R$.*

BEVIS: Da I er et ideal og R er en hovedidealring kan I skrives som $I = Rc$ for et $c \in R$. Derfor er (2) en følge af (1). Vi beviser (1). Antag først at $I = Rc$. Da $Ra \subseteq I$ fås $c|a$ ifølge (4.14) og analogt ses $c|b$. Hvis $d|a$ og $d|b$ gælder $Ra \subseteq Rd$ og $Rb \subseteq Rd$ og dermed $Rc = I = Ra + Rb \subseteq Rd$, da Rd er et ideal. Ifølge (4.14) er så $d|c$. Omvendt, lad c være en s.f.d. af a og b. Lad $c' \in R$ være valgt, så $Ra + Rb = Rc'$. Så er c' en s.f.d. af a, b ifølge det ovenstående. Dermed er c og c' associerede ifølge (2.11) og altså $Rc' = Rc$, dvs. $Rc = Ra + Rb = I$. □

(4.17) EKSEMPEL: Vi har set af $\mathbf{Z}[i]$ er en Euklidisk ring og derfor en hovedidealring. Så der findes altså største fælles divisorer af elementer i $\mathbf{Z}[i]$. Vi illustrerer hvorledes disse beregnes:

Opgave: Beregn en s.f.d. af $7 + 4i$ af $1 + 7i \in \mathbf{Z}[i]$.

1. Metode ("Slavemetoden", der altid giver resultat og som er analog til (2.25)).

$$\frac{7+4i}{1+7i} = \frac{(7+4i)(1-7i)}{(1+7i)(1-7i)} = \frac{35-45i}{50} = \frac{7-9i}{10}$$
$$= (1-i) + \frac{-3+i}{10}$$

(1 (hhv. -1)) er det hele tal der er nærmest $\frac{7}{10}$ (hhv. $\frac{-9}{10}$); derfor skal vores "m" være $1-i$). Vi ganger ligningen med $(1+7i)$ og får

$$7 + 4i = (1-i)(1+7i) + \frac{(-3+i)(1+7i)}{10}$$
$$= (1-i)(1+7i) + (-1-2i) \; (= m(1+7i) + r, r = -1-2i).$$

Derfor er den søgte s.f.d. også en s.f.d. af $1+7i$ og $1+2i$. Men

$$\frac{1+7i}{1+2i} = \frac{(1+7i)(1-2i)}{5} = \frac{15+5i}{5} = 3+i,$$

så $1+2i \mid 1+7i$. Derfor er $1+2i$ en s.f.d. af $7+4i$ og $1+7i$. De andre s.f.d. fås ved at multiplicere med alle invertible elementer i $\mathbf{Z}[i]$, dvs. ± 1 og $\pm i$.

2. Metode ("Ad hoc metoden", som er lidt mere vagt formuleret, men som kan være meget effektiv). Vi lader $((a,b))$ være mængden af s.f.d. for a, b. Tilsvarende lader vi $((a))$ være mængden af elementer som er associerede til a (så $((a)) = \{au \mid u \text{ invertibel}\}$). For $a, b \in \mathbf{Z}[i]$ gælder åbenbart $((a,b)) = ((a+kb, b))$ for alle $k \in \mathbf{Z}[i]$ og $((a,b)) = ((a,bu)) = ((au,b))$ når u er invertibel. Derfor er

$$\begin{aligned}((7+4i,1+7i)) &= ((7i-4,1+7i)), \quad (\text{da } i \text{ invertibel})\\ &= ((-5,1+7i)), \quad (\text{da } -5=(7i-4)-(1+7i))\\ &= ((5i,1+7i)), \quad (\text{da } -i \text{ er invertibel})\\ &= ((5i,1+2i)), \quad (\text{da } 1+2i=1+7i-5i)\\ &= ((1+2i)) \quad (\text{fordi } 5=(1+2i)(1-2i), \text{ så } 1+2i|5|5i).\end{aligned}$$

□

(4.18) ØVELSE: Beregn $((10+11i,8+i))$ i $\mathbb{Z}[i]$. □

(4.19) ØVELSE: Lad $a,b \in \mathbb{Z}[i]$. Vis at der gælder:

(1) $N(a)$ primtal i $\mathbb{Z} \Rightarrow a$ irreducibelt i $\mathbb{Z}[i]$.
(2) $(N(a),N(b))=1 \Rightarrow ((a,b))=(1)$.

Overvej om de omvendte udsagn til (1) og (2) gælder. □

(4.20) BEMÆRKNING: Det kan vises, at en vis delring af $\mathbb{Q}[\sqrt{-19}]$ er en hovedidealring men ingen Euklidisk ring. □

Som en forberedelse til den næste sætning har vi brug for det følgende resultat:

(4.21) ØVELSE: Antag at $I_1, I_2, \ldots, I_n, \ldots$ er idealer i R således at $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$. Vis at $I = \bigcup_{n\geq 1} I_n$ også er et ideal i R. Hvorfor er inklusionsbetingelsen vigtig? □

Vi kommer nu til definitionen af *Gaussiske ringe*, som også kaldes *faktorielle ringe* (UFD på engelsk).

(4.22) DEFINITION: R kaldes *Gaussisk* hvis der gælder
(1) Ethvert ikke-invertibelt element $a \neq 0$ i R er et produkt af endelig mange irreducible elementer $r_1, r_2, \ldots, r_m$; altså
$a = r_1 r_2 \ldots r_m$.
(2) Hvis $a = s_1 s_2 \ldots s_n$ hvor $s_1, \ldots, s_n$ er irreducible elementer i R, så er $n=m$, og der eksisterer en bijektiv afbildning σ på mængden $\{1,2,\ldots,m\}$ således at $((r_i)) = ((s_{\sigma(i)}))$. (Dette betyder at r_i og $s_{\sigma(i)}$ er associerede.) (Så (1) er en *eksistens*betingelse og (2) et udsagn om at faktoriseringen er essentielt *entydig*, altså entydig pånær multiplikation med invertible elementer). □

Hvis man benytter (4.16) i stedet for (2.24) kan man kopiere beviset for (2.26) til at vise:

(4.23) SÆTNING. *Hvis R er en hovedidealring, så er ethvert irreducibelt element i R også et primelement. (Se også (4.36) om Gaussiske ringe!)*

(4.24) ØVELSE: Bevis (4.23). □

(4.25) SÆTNING. *Hvis R er en hovedidealring, så er R Gaussisk.*

BEVIS: Vi antager at R er en hovedidealring. Vi viser (4.22)(1) for R: Antag at $a \neq 0$ ikke er invertibelt, og at a ikke opfylder (4.22)(1). Så er a ikke selv irreducibelt. (Ellers vælg $m = 1$, og $r_1 = a$). Derfor er $a = a_1 b_1$, hvor a_1 og b_1 begge er ikke-invertible. Enten er a_1 eller b_1 *ikke* et produkt af irreducible elementer. Hvis det er a_1, er a_1 ikke irreducibel og vi kan skrive $a_1 = a_2 b_2$, hvor a_2 og b_2 ikke er invertible og a_2 *ikke* er et produkt af irreducible elementer. Hvis vi fortsætter på denne måde får vi en følge af elementer $a_1, a_2, a_3, \ldots$ hvor $a_{i+1} \mid a_i$ og hvor a_{i+1} og a_i ikke er associerede. Der gælder så ifølge (4.14)

$$Ra_1 \subseteq Ra_2 \subseteq \cdots \subseteq Ra_m \subseteq \ldots$$

således at $I = \bigcup_{i \geq 1} Ra_i$ er et ideal i R ifølge (4.21). Da R er en hovedidealring må $I = Rb$ for et $b \in R$. Da $b \in I$ eksisterer et $i \geq 1$ således at $b \in Ra_i$. Så er $I = Rb \subseteq Ra_i \subseteq I$, altså $I = Ra_i$. Dermed er $Ra_i = Ra_{i+1}$ $(= I)$, hvorfor a_i og a_{i+1} er associerede ifølge (4.14). Dette er en modstrid.

Vi beviser nu (4.22)(2) for R. Antag at $a = r_1 r_2 \ldots r_m = s_1 s_2 \ldots s_n$, hvor r_i'erne og s_i'erne er irreducible. Ifølge (4.23) er de også primelementer. Da $r_1 \mid a = s_1 s_2 \ldots s_n$ gælder enten $r_1 \mid s_1$ eller $r_1 \mid s_2 \ldots s_n$. I det sidste tilfælde gælder enten $r \mid s_2$ eller $r_1 \mid s_3 \ldots s_n$. En gentagelse af denne overvejelse viser, at der eksisterer et j, således at $r_1 \mid s_j$. Vi skriver $s_j = r_1 u_1$. Da s_j er irreducibel og r_1 ikke er invertibel, må u_1 være invertibel. Dermed er $((r_1)) = ((s_j))$ og vi sætter $\sigma(1) = j$. Vi har nu

$$r_1 r_2 \ldots r_m = r_1 u_1 s_1 \ldots s_{j-1} s_{j+1} \ldots s_n$$

så $[NU]$ viser at

$$r_2 \ldots r_m = u_1 s_1 \ldots s_{j-1} s_{j+1} \ldots s_n.$$

En gentagelse af det ovenstående argument viser, at da $r_2 \mid u_1 s_1 \ldots s_{j-1} s_{j+1} \ldots s_n$, eksisterer et $k \neq j$ så $((r_2)) = ((s_k))$. Vi sætter $\sigma(2) = k$ og anvender [NU]. Ved at fortsætte på denne måde afsluttes beviset. □

(4.26) ØVELSE: Lad p og q være irreducible elementer i R. Vis: $p|q \Leftrightarrow p$ og q er associerede. □

(4.27) ØVELSE: Lad $p \in R \setminus \{0\}$. Vis: p er et primelement i $R \Leftrightarrow Rp$ er et primideal i R. □

(4.28) SÆTNING. *Lad R være* hovedidealring, *$p \in R \setminus \{0\}$. Der gælder:*

$\Updownarrow$ *p er et irreducibelt element i R.*
Rp er et maksimalt ideal i R.

BEVIS: $\Downarrow$: Lad p være irreducibelt. Sæt $I = Rp$. Da p ikke er invertibelt, er $I \neq R$ ((4.14)). Lad J være et ideal i R, så $I \subseteq J \subseteq R$. Der findes et $q \in R$, så $J = Rq$. Ifølge (4.14) er $q|p$. Lad altså $p = qr$, $r \in R$. Da p er irreducibelt, er enten q

invertibel, og derfor $R = Rq$ ((4.14)), eller r invertibel. Så er p og q associerede og derfor $I = J$ ((4.14)).

$\Uparrow$: Rp maksimalt ideal $\overset{(3.29)(3)}{\Rightarrow}$ Rp primideal $\overset{(4.27)}{\Rightarrow}$ p primelement $\overset{(4.4)}{\Rightarrow}$ p irreducibelt. □

(4.29) ØVELSE: Vis at et primideal $\neq \{0\}$ også er et maksimalt ideal i en hovedidealring. □

Vi giver et par anvendelser af det ovenstående i den "elementære" talteori. De illustrerer det interessante princip, at man kan benytte "større" ringe end $\mathbf{Z}$ til at bevise resultater om $\mathbf{Z}$.

Et *kvadrattal* i $\mathbf{N}$ er et tal på formen a^2, hvor $a \neq 0$, $a \in \mathbf{Z}$. Man kan så spørge: Hvilke naturlige tal er en sum af $1, 2, 3, 4, \ldots$ kvadrattal? F.eks. er $13 = 2^2 + 3^2$ en sum af 2 kvadrattal, hvorimod $7 = 1^2 + 1^2 + 1^2 + 2^2$ er en sum af 4 kvadrattal, men ikke af $1, 2$ eller 3 kvadrattal. Der en en sætning som siger, at *ethvert naturligt tal er en sum af højst* 4 *kvadrattal.* Ved at gå ud i $\mathbf{Z}[i]$ vil vi her undersøge hvilke primtal der er en sum af 2 kvadrattal. Selvfølgelig er $2 = 1^2 + 1^2$ et sådant primtal.

(4.30) SÆTNING. (Euler). *Lad $p \in \mathbf{Z}$ være et primtal, $p \neq 2$. Der gælder:*

$$p \text{ er en sum af 2 kvadrater} \Leftrightarrow p \equiv_4 1.$$

Endvidere gælder, at hvis $p = a^2 + b^2 = c^2 + d^2$, hvor $a, b, c, d \in \mathbf{N}$, så er $a = c$ og $b = d$ eller $a = d$ og $b = c$.

BEVIS: Hvis $a = 2k + 1$ er ulige, så er $a^2 = 4k^2 + 4k + 1$, og derfor $a^2 \equiv_4 1$. Hvis $a = 2k$ er lige er $a^2 = 4k^2 \equiv_4 0$. Derfor er en sum af 2 kvadrattal kongruent til $0, 1$ eller 2 modulo 4. (Altså $a^2 + b^2 \equiv_4 0$ eller $a^2 + b^2 \equiv_4 1$ eller $a^2 + b^2 \equiv_4 2$). Så hvis p er ulige og $p = a^2 + b^2$ må $p \equiv_4 1$. Omvendt, lad p være et primtal, $p \equiv_4 1$. I (4.31) viser vi at der findes et $x \in \mathbf{N}$ så $p | 1 + x^2$. Så gælder at $p | (1 + ix)(1 - ix)$ (i $\mathbf{Z}[i]$!) Imidlertid er det klart, at $p \top (1 + ix)$ og $p \top (1 - ix)$ i $\mathbf{Z}[i]$. (Hvis $(1 + ix) = p(r + is)$ må $pr = 1$, for eksempel). Derfor er p ikke et primelement i $\mathbf{Z}[i]$ og derfor heller ikke irreducibelt (ifølge (4.9)(3), (4.15) og (4.23).) Ifølge definitionen på et irreducibelt element kan man skrive $p = (a + ib)(c + id)$ for passende $a, b, c, d \in \mathbf{Z}$ og hvor $a + ib$, $c + id$ ikke er invertible. Vi har

$$p^2 = N(p) = N(a + ib)N(c + id) = (a^2 + b^2)(c^2 + d^2).$$

Da $a^2 + b^2 \neq 1$ og $c^2 + d^2 \neq 1$ fordi $a + ib$ og $c + id$ ikke er invertible, fås $a^2 + b^2 = c^2 + d^2 = p$, altså $p = a^2 + b^2$. Antag nu at $a, b, c, d \in \mathbf{N}$ så $p = a^2 + b^2 = c^2 + d^2$. Så er $N(a + ib) = N(c + id) = N(a - ib) = N(c - id) = p$, og derfor er $a \pm ib$ og $c \pm id$ primelementer i $\mathbf{Z}[i]$ (ifølge (4.19)(1)). Vi har så $p = (a+ib)(a-ib) = (c+id)(c-id)$, to faktoriseringer af p som produkt af irreducible elementer i $\mathbf{Z}[i]$. Da $\mathbf{Z}[i]$ er Gaussisk fås fra (4.22)(2) at $a + ib = u(c + id)$ hvor u er invertibel i $\mathbf{Z}[i]$, altså $u = \pm 1$ eller $u = \pm i$. Heraf følger den sidste påstand i (4.30) let. □

(4.31) BEMÆRKNING: Hvis p er et primtal, $p = 4k+1$ gælder $p \mid 1+((2k)!)^2$. Dette ses ved at anvende Wilson's sætning (2.40)(2), der siger, at $p \mid 1+(4k)!$ Vi overvejer at $(4k)! \equiv_p ((2k)!)^2$: Da $p = 4k+1$ gælder for $i = 1, 2, \ldots, 2k$ at $2k+i \equiv_p -(2k-(i-1))$. Ved at multiplicere disse $2k$ kongruenser fås (anvend (2.33))

$$(2k+1)(2k+2)\cdots 4k \equiv_p (-1)^{2k} 2k(2k-1)\cdots 2\cdot 1 = (2k)!$$

Derfor er $(2k)!(2k)! \equiv_p (2k)!(2k+1)(2k+2)\cdots 4k = (4k)!$ □

(4.32) BEMÆRKNING: Beviset for (4.30) er ikke "konstruktivt". Vi viser at et primtal $p \equiv_4 1$ kan skrives som $p = a^2 + b^2$, men *ikke* hvordan man kan beregne a og b, når p er givet. Dette er en typisk situation i algebraen. □

Den anden talteoretiske sætning *er* "konstruktiv".

(4.33) SÆTNING. (Fermat). *Antag at $x, y \in \mathbf{N}$ således at $x^2 + 2 = y^3$. Så er $x = 5$ og $y = 3$.*

BEVIS: Antag at $x, y \in \mathbf{N}$, så $x^2 + 2 = y^3$. Vi arbejder i den Euklidiske ring $R = \mathbf{Z}[\sqrt{-2}]$ ((4.10)), som altså også er Gaussisk. I R gælder

$$x^2 + 2 = (x + \sqrt{-2})(x - \sqrt{-2}).$$

Vi viser først at $((x+\sqrt{-2}, x-\sqrt{-2})) = ((1))$. Ellers findes et primelement (= irreduciblt element) $r \in R$, så $r \mid x+\sqrt{-2}$ og $r \mid x-\sqrt{-2}$. Så er

$$r \mid 2\sqrt{-2} = (x+\sqrt{-2}) - (x-\sqrt{-2})$$

altså $r \mid (\sqrt{-2})^3$. Da r er et primelement, fås $r \mid \sqrt{-2}$. Men $\sqrt{-2}$ er irreducibelt i R (som man let ser ved et normargument), så $((r)) = ((\sqrt{-2}))$, altså $r = \pm\sqrt{-2}$. Så må $r|x$, da $r|x+\sqrt{-2}$ altså $r^2 = -2|x^2$. Så $2|x^2$ og derfor må x være lige. Men så er $x^2 \in 4\mathbf{Z}$. Men da $2|x^2 + 2 = y^3$ fås at y er lige, så $y^3 \in 8\mathbf{Z}$. Specielt er $y^3 \equiv_4 0$. På den anden side er

$$y^3 = x^2 + 2 \equiv_4 2 \quad \text{da } x^2 \equiv_4 0.$$

Dette er en modstrid, så vi har vist

$$((x+\sqrt{2}, x-\sqrt{2})) = ((1)).$$

Da $x+\sqrt{-2}$ og $x-\sqrt{-2}$ altså ikke har nogen fælles irreducible faktorer, og da

$$(x+\sqrt{-2})(x-\sqrt{-2}) = y^3$$

fås ved anvendelse af (4.22)(2) at der eksisterer elementer s og $t \in R$ så $s^3 = x-\sqrt{-2}$, $t^3 = x+\sqrt{-2}$. Skriv $s = a + b\sqrt{-2}$, hvor $a, b \in \mathbf{Z}$. Så er

$$x - \sqrt{-2} = s^3 = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}.$$

Heraf følger at $x = a^3 - 6ab^2 = a(a^2 - 6b^2)$ og at $-1 = 3a^2b - 2b^3 = b(3a^2 - 2b^2)$. (Hvorfor det?)

Da jo $a, b \in \mathbf{Z}$ fås fra den sidste ligning at $b = \pm 1$, altså $\mp 1 = 3a^2 - 2$. Heraf fås $b = -1$ og $a = \pm 1$. Så er $x = a(a^2 - 6b^2) = a(1 - 6) = a \cdot 5 = \pm 5$. Da $x \in \mathbf{N}$ må $x = 5$. Så er $x^2 + 2 = 27$, så $y = 3$. □

Til sidst vil vi beskæftige os med sammenhængen mellem faktoriseringsteorierne i R og i polynomiumsringen $R[t]$.

(4.34) DEFINITION: Lad $p(t) \in R[t]$ være et polynomium, $p(t) = \sum_{i=0}^{m} a_i t^i$, $a_i \in R$. Hvis $r \in R$ sættes $p(r) = \sum_{i=0}^{m} a_i r^i$, hvor $r^i = \overbrace{rr \ldots r}^{i \text{ gange}}$, altså

$$p(r) = a_0 + a_1 r + a_2 r^2 + \cdots + a_m r^m \in R.$$

Når $r \in R$ er givet er det let at se, at afbildningen $\varphi_r : R[t] \to R$ givet ved $\varphi_r(p(t)) = p(r)$ er en homomorfi. φ_r kaldes en *indsættelseshomomorfi* og $p(r)$ er *værdien* af $p(t)$ ved *indsættelse af* r. Vi kaldes r en *rod* i $p(t)$, når $p(r) = 0$. Så er

$$\ker \varphi_r = \{p(t) \in R[t] \mid r \text{ er rod i } p(t)\}.$$

□

(4.35) SÆTNING. *Følgende udsagn er ensbetydende*

(1) *R er et legeme.*
(2) *$R[t]$ er en Euklidisk ring.*
(3) *$R[t]$ er en hovedidealring.*

BEVIS: (1) ⇒ (2) kan bevises analogt til (4.11).

(2) ⇒ (3) følger af (4.15).

(3) ⇒ (1): Antag at $R[t]$ er en hovedidealring. Betragt indsættelseshomomorfien $\varphi_0 : R[t] \to R$. φ_0 afbilder det konstante polynomium $p(t) = a_0$ på a_0, så φ_0 er en epimorfi. Dermed er $R[t]/\ker\varphi_0 \simeq R$ ifølge (3.24) (isomorfisætningen for ringe). Ifølge (3.29)(1) er $\ker\varphi_0$ et primideal $\neq \{0\}$ og derfor også et maksimalt ideal, da $R[t]$ er en hovedidealring ((4.29)). Men så er $R \simeq R[t]/\ker\varphi_0$ et legeme ifølge (3.29)(2). □

(4.36) ØVELSE: Vis, at ethvert irreducibelt element i en *Gaussisk* ring R også er et primelement. (Løsningsforslag: Lad $p \in R$ være irreducibel, $a, b \in R$, $p|ab$. Der findes altså et $c \in R$ så $pc = ab$. Betragt faktoriseringerne af a, b og c som produkt af irreducible elementer.) □

(4.37) ØVELSE: Antag at de ikke-invertible elementer a, b i den Gaussiske ring R har faktoriseringerne $a = p_1 p_2 \ldots p_r$, $b = q_1 q_2 \ldots q_s$ som produkt af irreducible elementer. Antag (efter eventuelt at have ændret faktorernes rækkefølge) at p_1 og q_1, p_2 og

$q_2, \ldots, p_m$ og q_m er associerede medens intet $p_i, m < i \leq r$ er associeret til noget q_j, $m < j \leq s$. Vis at $p_1 p_2 \ldots p_m$ er en største fælles divisor (s.f.d.) af a og b i R. Illustrer derefter dette gennem et eksempel i den Gaussiske ring $\mathbb{Z}$. □

(4.38) ØVELSE: Antag at ethvert element i R har mindst én faktorisering som produkt af irreducible elementer. Vis at R er Gaussisk, hvis og kun hvis ethvert irreducibelt element i R er et primelement. (Løsningshjælp: Man kan anvende (4.36) samt sidste del af beviset for (4.25)!) □

(4.39) ØVELSE: Betragt R som en delring af $R[t]$.

(1) Vis at de invertible elementer i $R[t]$ netop er de invertible elementer i R.
(2) Lad $a \in R$. Vis at a er irreducibel i $R \Leftrightarrow a$ er irreducibel i $R[t]$.

((4.3)(3) spiller en rolle i beviserne.) □

(4.40) ØVELSE: Antag at $R[t]$ er Gaussisk. Vis at R er Gaussisk. □

(4.41) SÆTNING. *Følgende udsagn er ækvivalente*

(1) *R Gaussisk.*
(2) *$R[t]$ Gaussisk.*

BEVIS: Ifølge (4.40) skal vi vise (1) $\Rightarrow$ (2). Vi antager at R er Gaussisk. Hvis $f \in R[t]$, $f = a_0 + a_1 t + \cdots + a_n t^n$, definerer vi *indholdet* $I(f)$ af f ved

$$I(f) = ((a_0, a_1, a_2, \ldots, a_n)).$$

Her betegner $((a_0, a_1, \ldots, a_n))$ mængden af s.f.d. for $a_0, a_1, \ldots, a_n$ (som tidligere). Største fælles divisorer eksisterer i R ifølge (4.37). Hvis $a \in I(f)$ kan vi skrive $f = a\tilde{f}$, hvor $\tilde{f} \in R[t]$ og $I(\tilde{f}) = ((1))$. (Overvej dette nøje!). Et polynomium $\tilde{f}$ kaldes *primitivt* hvis $I(\tilde{f}) = ((1))$. Hvis $f = b\tilde{\tilde{f}}$ hvor $\tilde{\tilde{f}}$ er primitivt, så er $b \in I(f)$. (Overvej dette). Hvis $\tilde{f}$ og $\tilde{g}$ er primitive polynomier, så er $\tilde{f}\,\tilde{g}$ også primitivt. Dette ses som følger: Lad $\tilde{f} = b_0 + b_1 t + \cdots + b_m t^m$, $\tilde{g} = c_0 + c_1 t + \cdots + c_n t^n$, hvor $((b_0, \ldots, b_m)) = ((c_0, \ldots, c_n)) = ((1))$. Antag at $p \in R$ er irreducibelt og at p går op i alle $\tilde{f}\,\tilde{g}$'s koefficienter. Antag at $p|b_0, p|b_1, \ldots, p|b_{r-1}, p \top b_r, p|c_0, p|c_1, \ldots, p|c_{s-1}, p \top c_s$, for passende r, s, $0 \leq r \leq m$, $0 \leq s \leq n$. (Findes sådanne r, s?). Koefficienten til t^{r+s} i $\tilde{f}\,\tilde{g}$ er da ikke delelig med p. (Overvej dette). Derfor har vi en modstrid, så $\tilde{f}\,\tilde{g}$ er primitivt. Hvis $f, g \in R[t]$ gælder nu $I(f)I(g) = I(fg)$: Skriv $f = a\tilde{f}$, $g = b\tilde{g}$ hvor $a \in I(f)$, $b \in I(g)$ og $\tilde{f}$ og $\tilde{g}$ er primitive. Så er $fg = ab\tilde{f}\,\tilde{g}$ og $\tilde{f}\,\tilde{g}$ primitivt. Derfor er $ab \in I(fg)$. Heraf fås $I(f)I(g) = I(fg)$, da $I(f), I(g)$ og $I(fg)$ består af klasser af associerede elementer. (Man anvender (2.10).)

Vi antager nu, at $R[t]$ ikke er Gaussisk. Under anvendelse af (4.3) er det let at se, at et primitivt polynomium af positiv grad er et produkt af irreducible polynomier af positiv grad. Derfor har ethvert polynomium i $R[t]$ en faktorisering som produkt af irreducible elementer. Da $R[t]$ ikke er Gaussisk findes et polynomium $f \in R[t]$ af mindst mulig grad, hvor denne faktorisering ikke er essentielt entydig.

$$(*) \qquad f = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$$

skal være to forskellige faktoriseringer af f, $p_1, \ldots, p_r$, $q_1, \ldots, q_s$ irreducible. Hvis $p_i | q_j$ for et i og j, $1 \leq i \leq r$, $1 \leq j \leq s$ er p_i og q_j associerede ifølge (4.26) og derfor $p_i = uq_j$ for et invertibelt $u \in R$ ((4.39)(1)). Så kan q_j forkortes på begge sider af $(*)$. (Anvend (4.3)(4)). Derfra kan vi uden indskrænkning antage, at $p_i \top q_j$ for alle i, j. Vi antager

$$d = \deg p_1 \geq \deg p_2 \geq \cdots \geq \deg p_r$$
$$e = \deg q_1 \geq \deg q_2 \geq \cdots \geq \deg q_s,$$

og at $e \geq d$. (Ingen indskrænkning.) Da f ikke kan have grad 0 (fordi R er Gaussisk), må $d \geq 1$ ifølge (4.3). Lad a og b være højestegradskoefficienterne i p_1 og q_1, henholdsvis. Sæt $g = p_1 t^{e-d} q_2 \ldots q_s$, $q_1^* = aq_1 - bp_1 t^{e-d}$ og

$$F = af - bg = q_1^* q_2 \ldots q_s.$$

Da $p_1 | f$ og $p_1 | g$ må $p_1 | F$. Graden af q_1^* er højst $e - 1$, da aq_1 og $bp_1 t^{e-d}$ har den samme højestegradskoefficient ab. Derfor er $\deg F < \deg f$. Vi påstår, at $p_1 | aq_1$. Hvis $F = 0$ må $q_1^* = 0$, da $R[t]$ er en integritetsring, og så er påstanden oplagt. Ellers har F en essentielt entydig faktorisering som produkt af irreducible elementer, da $\deg F < \deg f$. Derfor er $p_1 | F$ associeret til en irreducibel faktor i F. Da $p_1 \top q_j$ fås $p_1 | q_1^*$ og igen $p_1 | aq_1$. Skriv $aq_1 = p_1 p_1^*$ for et passende polynomium p_1^*. Da p_1 og q_1 er irreducible af positiv grad er $I(p_1) = I(q_1) = ((1))$. Derfor er

$$((a)) = I(aq_1) = I(p_1 p_1^*) = I(p_1) I(p_1^*) = I(p_1^*)$$

ifølge vore overvejelser om indholdet. Vi får $a \in I(p_1^*)$ så $a | p_1^*$. Ved at forkorte a i ligningen $aq_1 = p_1 p_1^*$ så $p_1 | q_1$, hvilket er en modstrid til antagelsen $p_i \top q_j$ for alle i, j. □

(4.42) BEMÆRKNING: Ifølge (4.35) og (4.41) er $\mathbb{Z}[t]$ *en Gaussisk ring, men ikke en hovedidealring.* □

(4.43) BEMÆRKNING: Beviset for (4.41) kan forenkles betydeligt ved at benytte ringen R's *brøklegeme*, se næste kapitel. Et bevis af denne art findes i Allenby's bog. □

Kapitel 5. Om legemer.

I dette kapitel behandles nogle få aspekter af den meget righoldige teori for legemer, specielt konstruktionen af legemer med visse givne egenskaber.

Oversigt over delafsnittene

1° Legemer fra ringe, brøklegemer.

Vi starter med et par sætninger om, hvordan man ud fra kommutative ringe med 1-element kan danne legemer. Betragt følgende "duale" spørgsmål for en *kommutativ ring R med 1-element*:

(5.1) SPØRGSMÅL: For hvilke R findes der et legeme L og en (ring) *epimorfi* (se (3.20)) $\varphi : R \to L$? □

(5.2) SPØRGSMÅL: For hvilke R findes der et legeme L og en (ring) *monomorfi* (se (3.20)) $\varphi : R \to L$? □

Til (5.1) kan siges følgende: Hvis $\varphi : R \to L$ er en epimorfi, så er ifølge (3.24) $R/\operatorname{Ker}\varphi \simeq L$. Da L er et legeme må altså $R/\operatorname{Ker}\varphi$ være et legeme, og derfor må $\operatorname{Ker}\varphi$ ifølge (3.29)(2) være et maksimalt ideal i R. Hvis omvendt I er et maksimalt ideal i R, så er R/I et legeme og $r \longrightarrow \widehat{r}$ (fra $R \to R/I$) en epimorfi. Så (5.1) er ækvivalent til spørgsmålet "Hvilke kommutative ringe med 1-element har et maksimalt ideal?" Svaret er "alle". Dette ses ved at anvende følgende sætning på idealet $\{0\}$ i R:

(5.3) SÆTNING. *Lad $X \neq R$ være et ideal i den kommutative ring R med 1-element. Der findes et maksimalt ideal i R, som indeholder X.*

BEVISET byder på en anvendelse af Zorns Lemma [ZL], se Kapitel 0. Sæt

$$\mathcal{J} = \{I \mid I \text{ ideal i } R, I \neq R \text{ og } X \subseteq I\}.$$

Ved den sædvanlige mængdeteoretiske inklusion $\subseteq$ er $(\mathcal{J}, \subseteq)$ en *po*-mængde. Da $X \in \mathcal{J}$ er $\mathcal{J} \neq \varnothing$. Det er let at se, at et maksimalt element i $(\mathcal{J}, \subseteq)$ også er et maksimalt ideal i R. (Overvej!) Vi viser ved hjælp af [ZL], at $(\mathcal{J}, \subseteq)$ *har* et

maksimalt element. Dermed vil sætningen altså være bevist. Lad $\mathcal{K}$ være en kæde i $(\mathcal{J}, \subseteq)$. Det betyder, at der gælder

$(*)$ For alle $I, J \in \mathcal{K}$ er $I \subseteq J$ eller $J \subseteq I$.

Vi sætter $A = \cup_{I \in \mathcal{K}} I$ og viser $A \in \mathcal{J}$. Det vil medføre, at $A \in \mathrm{Maj}(\mathcal{K})$, så $\mathrm{Maj}(\mathcal{K}) \neq \emptyset$, og så viser [ZL], at $(\mathcal{J}, \subseteq)$ har et maksimalt element, som ønsket. Lad $x, y \in A$, $r \in R$. Der findes $I, J \in \mathcal{K}$, så $x \in I$, $y \in J$. Lad os ifølge $(*)$ antage at $I \subseteq J$. Så er $x \in J$, $y \in J$ og derfor $x + y \in J$ da J er et ideal. Da $J \subseteq A$ fås $x + y \in A$. Endvidere er $rx \in I \subseteq A$, da $x \in I$ og I er et ideal. Så A er et ideal. Det er klart at $X \subseteq A$. Hvis $A \notin \mathcal{J}$, er $A = R$. Så er $1 \in A$, så der eksisterer et $I \in \mathcal{K}$ så $1 \in I$. Det betyder, at $I = R$ ((3.4)(5)), en modstrid. Dermed er $A \in \mathcal{J}$, som ønsket. □

Så (5.1) har svaret: For alle ringe. Det er ikke tilfældet med (5.2). Vi viser:

(5.4) SÆTNING.

R opfylder [NU] (dvs. R integritetsring)

$\Updownarrow$

Der findes et legeme L og en monomorfi

$\varphi : R \to L$.

Det er let at se, at $\Uparrow$ gælder i (5.4): Antag at $\varphi : R \to L$ er en monomorfi. Så er billedet af R, $\varphi(R)$, en delring af L, og da L opfylder [NU] gælder dette også for $f(R)$. Da $R \simeq \varphi(R)$ ifølge isomorfisætningen for ringe, er det klart, at når $\varphi(R)$ opfylder [NU], så gør R det også. (Overvej dette). For at bevise $\Downarrow$ konstruerer vi R's *brøklegeme* (kvotientlegeme). Til forståelse af denne konstruktion ser vi først på det mest kendte eksempel.

(5.5) EKSEMPEL: ($\mathbf{Q}$ som brøklegeme af $\mathbf{Z}$).

Elementerne i $\mathbf{Q}$ opfattes normalt som *brøker* $\frac{a}{b}$, $a, b \in \mathbf{Z}, b \neq 0$. Men dette er ikke helt korrekt, idet vi jo må identificere $\frac{a}{b} = \frac{c}{d}$ når $ad = bc$. Man ser så elementerne i $\mathbf{Q}$ som *ækvivalensklasser* af brøker med hensyn til ækvivalensrelationen $\frac{a}{b} \sim \frac{c}{d} \Leftrightarrow ad = bc$. Addition og multiplikation af brøker er velkendt

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \qquad \frac{a}{b}\frac{c}{d} = \frac{ac}{bd}$$

og afhænger ikke af den valgte repræsentant i ækvivalensklassen. □

(5.6) HJÆLPESÆTNING. *Lad R være en integritetsring. Sæt $A(R) = \{(a, b) \mid a, b \in R, b \neq 0\}$. Relationen $\sim$ på $A(R)$ defineret ved $(a, b) \sim (c, d) \Leftrightarrow ad = bc$ er en ækvivalensrelation.*

BEVIS: $(a, b) \sim (a, b)$ da $ab = ba$ (R er kommutativ). Hvis $(a, b) \sim (c, d)$ gælder $ad = bc$ og derfor $cb = da$, dvs. $(c, d) \sim (a, b)$. Antag endelig, at $(a, b) \sim (c, d)$ og

at $(c,d) \sim (e,f)$. Så er $ad = bc$ og $cf = de$. Vi multiplicerer disse ligninger og får $adcf = bcde$ dvs. $(af - be)cd = 0$. Så viser [NU] at $c = 0$ eller $c \neq 0$ og $af - be = 0$. Hvis $c = 0$ er $ad = cb = 0$ og $de = cf = 0$, så $a = e = 0$ ([NU]). Igen fås $af - be = 0$, altså $(a,b) \sim (e,f)$. □

(5.7) DEFINITION OG SÆTNING. *Lad $Q(R)$ være mængden af ækvivalensklasser i $A(R)$, hvor R er en integritetsring. Hvis $(a,b) \in A(R)$ betegner vi $\widehat{(a,b)}$ med $[a,b]$. (Så $Q(R) = \{[a,b] \mid a,b \in R, b \neq 0\}$, hvor $[a,b] = [c,d] \Leftrightarrow ad = bc$). På $Q(R)$ defineres kompositioner $+, \cdot$ ved*

$$[a,b] + [c,d] = [ad + bc, bd]$$
$$[a,b] \cdot [c,d] = [ac, bd].$$

Disse kompositioner er veldefinerede og $(Q(R), +, \cdot)$ er et legeme, kaldet R's brøklegeme. Afbildningen $r \to [r,1]$ fra $R \to Q(R)$ er en (ring)monomorfi.

BEVIS: Først vises veldefineretheden: Lad $[a,b] = [a',b']$, $[c,d] = [c',d']$, altså $ab' = a'b$, $cd' = c'd$. Der gælder

$$(ad + bc)b'd' = ab'dd' + bb'cd'$$
$$= a'bdd' + bb'c'd = (a'd' + b'c')bd.$$

Derfor er $[ad + bc, bd] = [a'd' + b'c', b'd']$. En lignende udregning viser at $[ac, bd] = [a'c', b'd']$. Så viser vi, at $Q(R)$ er et legeme. Det er oplagt, at [RAK], [RMK], [RMA] er opfyldte. [RAN] og [RMN] er opfyldte med $[0,1]$ som 0-element og $[1,1]$ som 1-element. Det negative af $[a,b]$ og $[-a,b]$ og det inverse til $[a,b] \neq 0$ er $[b,a]$. (Bemærk at $[a,b] \neq 0 \Leftrightarrow a \neq 0$. Overvej dette!) Vi har $[a,b][b,a] = [ab,ab] = 1$, da $(ab,ab) \sim (1,1)$. Vi mangler at vise [RAA] og [RD]:

$$\text{[RAA]} : ([a,b] + [c,d]) + [e,f] = [ad + bc, bd] + [e,f]$$
$$= [adf + bcf + bde, bdf] = [a,b] + [cf + de, df]$$
$$= [a,b] + ([c,d] + [e,f]).$$

Beviset for [RD] er en *øvelse*. Det er klart, at afbildningen $\varphi : r \to [r,1]$ er en homomorfi. Hvis $[r,1] = 0$ er $(r,1) \sim (0,1)$ altså $r1 = 0 \cdot 1 = 0$, $r = 0$. Dermed er $\operatorname{Ker}\varphi = 0$, så φ er en monomorfi, ifølge (3.21)(3). □

Vi har hermed også afsluttet beviset af (5.4) og besvaret spørgsmål (5.2). Da det i algebraen er sædvanligt at identificere isomorfe algebraiske strukturer, (hvis der ikke er grunde, der taler for ikke at gøre det) vil vi identificere R med delringen $\varphi(R)$ af $Q(R)$, når R er en integritetsring. Så kan (5.4) formuleres på følgende måde:

(5.4)* SÆTNING. *R er en integritetsring hvis og kun hvis R er en delring af et legeme.* □

Det samme princip med at identificere isomorfe strukturer anvendes i (5.12)–(5.12)* og senere. Det forenkler formuleringen af resultaterne betydeligt, som jo også en sammenligning af (5.4) og (5.4)* viser. Derved kommer det væsentlige i resultatet tydeligere frem.

(5.8) ØVELSE: Gør rede for at $Q(\mathbf{Z}) \simeq \mathbf{Q}$. □

(5.9) ØVELSE: Gør rede for at

$$R \text{ er et legeme } \Leftrightarrow \ Q(R) \simeq R$$

□

(5.10) ØVELSE: Gør rede for at $Q(\mathbf{Z}[i]) \simeq \mathbf{Q}[i]$. □

2° Udvidelseslegemer. Spaltningslegemer.

(5.11) DEFINITION: Antag, at L er et legeme og at $\emptyset \neq K \neq \{0\}$ er en delmængde af L. Hvis der gælder

(1) For alle $s, t \in K$ er $s + t \in K$ og $st \in K$.
(2) For alle $s \in K$ er $-s \in K$.
(3) For alle $s \in K$, $s \neq 0$ er $s^{-1} \in K$,

kaldes K et *dellegeme* af L. Så er K et legeme (med L's kompositioner). Hvis K er et dellegeme af L kaldes L et *udvidelseslegeme* af K. □

For eksempel er $\mathbf{Q}$ et dellegeme af $\mathbf{R}$ og $\mathbf{C}$ et udvidelseslegeme af $\mathbf{R}$.

Vi ved, at polynomiet $t^2+1 \in \mathbf{R}[t]$ ikke har nogen rod i $\mathbf{R}$. (For definitionen af *rod*, se (4.34)). Derimod har det roden i i udvidelseslegemet $\mathbf{C}$ af $\mathbf{R}$, idet $i^2+1 = -1+1 = 0$. Man kan så spørge om et vilkårligt polynomium (af grad ≥ 1) i $K[t]$, K legeme, har en rod i et passende udvidelseslegeme L af K. (Selvfølgelig har et polynomium af grad 0, altså et konstant polynomium $\neq 0$, ikke nogen rod i K eller i en udvidelse af K.) Vi viser i det følgende, at dette spørgsmål kan besvares positivt, men først må vi igen gå ind på identificering af isomorfe algebraiske strukturer. Hvis R og R^* er ringe og $\varphi : R \to R^*$ en (ring)homomorfi, er afbildningen

$$\varphi_t : R[t] \to R^*[t]$$

defineret ved

$$\varphi_t\left(\sum_{i=0}^{m} a_i t^i\right) = \sum_{i=0}^{m} \varphi(a_i) t^i$$

også en (ring)homomorfi, og det er klart at φ er en monomorfi (hhv. epimorfi, hhv. isomorfi) netop da når φ_t er en monomorfi (hhv. epimorfi, hhv. isomorfi). Hvad vi helt præcis viser i det følgende er:

(5.12) SÆTNING. *Lad $p(t) \in K[t]$, K legeme, $\deg \geq 1$. Der eksisterer et legeme L og en ringmonomorfi $\varphi : K \to L$ således at $\varphi_t(p(t))$ har en rod i L.*

□

I denne sætning kan φ opfattes som en isomorfi mellem K og $K^* = \varphi(K)$. Så giver φ_t en isomorfi mellem $K[t]$ og $K^*[t]$. Når vi identificerer K med K^* og $K[t]$ med $K^*[t]$ kan (5.12) formuleres på følgende måde:

(5.12)* SÆTNING. *Lad $p(t) \in K[t]$, K legeme, $\deg p \geq 1$. Der eksisterer et udvidelseslegeme L af K, således at $p(t)$ har en rod i L.*

□

Den bemærkelsesværdige sætning (5.12) ((5.12)*) blev først bevist af Kronecker, og den har også et bemærkelsesværdigt abstrakt bevis, hvis sidste del måske vil få den uerfarne læser til at føle sig ført bag lyset. (Den skeptiske læser opfordres til at prøve at konkretisere en eventuel kritik af beviset. Denne kan så danne diskussionsgrundlag i en øvelsestime.)

BEVIS FOR (5.12): Da K er et legeme, er $K[t]$ en Euklidisk ring og altså også en hovedidealring og en Gaussisk ring. (Se (4.35) og (4.25)). Da $\deg p \geq 1$, er p ikke et invertibelt element i $K[t]$. (Begrund dette). Derfor er p et produkt af irreducible polynomier (dvs. irreducible elementer i ringen $K[t]$), $p = p_1 p_2 \cdots p_n$, p_i irreducibel. Betragt idealet $I = K[t]p_1(t)$ i $K[t]$. Da $K[t]$ er en hovedidealring, er I et maksimalt ideal i $K[t]$ ifølge (4.28). Derfor er $L = K[t]/I$ et *legeme* ifølge (3.29)(2). Når $q(t) \in K[t]$ er et vilkårligt polynomium sætter vi som sædvanlig $\widehat{q(t)} = q(t) + I$ (altså $q(t)$'s ækvivalensklasse mht. ækvivalensrelationen $\equiv_I$, se (3.16)). Vi definerer $\varphi : K \to L$ som følger: Når $a \in K$, er a et konstant polynomium $a \in K[t]$. Vi sætter $\varphi(a) = \widehat{a}(= a + I) \in L$. Det er let at se, at φ er en homomorfi. Når $a \neq 0$ er $a \notin I$ og dermed $\widehat{a} \neq 0$. (Hvis $a = q(t)p_1(t)$ er $0 = \deg a = \deg q(t) + \deg p_1(t) \geq \deg p_1(t) \geq 1$, en modstrid), så $\widehat{a} = 0 \Leftrightarrow a \in I \Leftrightarrow a = 0$. Altså er $\operatorname{Ker} \varphi = 0$, dvs. φ er en monomorfi ((3.21)(3)). Nu er $t = 0 + 1 \cdot t + 0 \cdot t^2 + \cdots \in K[t]$. Vi sætter $\ell = \widehat{t} \in L$ og påstår at *ℓ er en rod i $\varphi_t(p_1)$*! Antag at $p_1(t) = a_0 + a_1 t + \cdots + a_m t^m$. Ifølge definitionen af I er $p_1(t) \in I$, altså $\widehat{p_1(t)} = \widehat{0}$. Så er

$$\left.\begin{aligned} \widehat{0} = \widehat{p_1(t)} &= (a_0 + a_1 t + \widehat{\cdots} + a_m t^m) \\ &= \widehat{a}_0 + \widehat{a}_1 \widehat{t} + \cdots + \widehat{a}_m \widehat{t}^m \\ &= \widehat{a}_0 + \widehat{a}_1 \ell + \cdots + \widehat{a}_m \ell^m \\ &= (\varphi_t(p_1))(\ell), \end{aligned}\right\} \text{se næste side!}$$

som ønsket.

(Da $\varphi(a) = \widehat{a}$ for alle $a \in K$ er $(\varphi_t(p))(t) = \widehat{a}_0 + \widehat{a}_1 t + \cdots + \widehat{a}_m t^m$. Ved indsætning af legemselementet $\ell \in L$ i $\varphi_t(p_1)(t)$ fås

$$\varphi_t(p_1)(\ell) = \widehat{a}_0 + \widehat{a}_1 \ell + \cdots + \widehat{a}_m \ell^m.$$

Men vi har jo at $\ell^i = \widehat{t^i}$ for alle i, da $\ell = \widehat{t}$.)

Da $\varphi_t(p) = \varphi_t(p_1)\varphi_t(p_2)\ldots\varphi_t(p_n)$ og ℓ er en rod i $\varphi_t(p_1)$, er ℓ også en rod i $\varphi_t(p)$, som ønsket. □

Før vi kikker på udvidelser af (5.12)*, giver vi et direkte bevis for følgende

(5.13) SÆTNING. *Lad R være en kommutativ ring med 1-element. Lad $p(t) \in R[t], r \in R$. Der gælder*

$$r \text{ er en rod i } p(t) \Leftrightarrow t - r \mid p(t) \quad (\text{i } R[t]).$$

BEVIS: For $i \geq 1$ sætter vi

$$p_i(t, r) = t^{i-1} + rt^{i-2} + \cdots + r^{i-2}t + r^{i-1} \in R[t].$$

Det er let at se, at der så gælder

$$t^i - r^i = p_i(t, r)(t - r).$$

Hvis $p(t) = \sum_{i=0}^m a_i t^i$, er $p(r) = \sum_{i=0}^m a_i r^i$, og derfor er

$$p(t) - p(r) = \sum_{i=1}^m a_i(t^i - r^i) = \left(\sum_{i=1}^m a_i p_i(t, r)\right)(t - r).$$

Da $p_i(t, r) \in R[t]$ er også $n(t) = \sum_{i=1}^m a_i p_i(t, r) \in R[t]$ og vi har

$$p(t) = p(r) + n(t)(t - r)$$

så

$$t - r \mid p(t) \Leftrightarrow t - r \mid p(r) \Leftrightarrow p(r) = 0.$$

□

Vi har nu følgende udvidelse af (5.12)*:

(5.14) SÆTNING. *Lad $p(t) \in K[t]$, K legeme, $\deg p = m$. Der findes et udvidelseslegeme L af K og elementer $\ell_1, \ell_2, \ldots, \ell_m \in L$, således at*

$$p(t) = a_m(t - \ell_1)(t - \ell_2)\ldots(t - \ell_m)$$

(i $L[t]$) hvor a_m er højestegradkoefficienten i p.

BEVIS: Vi benytter induktion efter $\deg p = m \geq 1$. (For $m = 0$ er sætningen triviel). For $m = 1$ kan vi vælge $K = L$. (Hvis $p(t) = a_1 t + a_0$ er $p(t) = a_1(t + a_0 a_1^{-1})$.) Antag, at (5.14) er vist for alle legemer og alle polynomier af grad $\leq m - 1$. Lad $p(t) \in K[t]$ have grad m. Ifølge (5.12)* eksisterer en udvidelse L_1 af K, således at $p(t)$ har en rod ℓ_1 i L_1. Så er i $L[t]$ $p(t) = (t - \ell_1)p_1(t)$, hvor $p_1(t) \in L_1[t]$ har grad $m - 1$. (Anvend (5.13)). Ifølge induktionsantagelsen anvendt på L_1 og $p_1(t)$ eksisterer en udvidelse L af L_1 og elementer $\ell_2, \ldots, \ell_m \in L$, således at

$$p_1(t) = a_m(t - \ell_2)(t - \ell_3)\ldots(t - \ell_m),$$

hvor a_m er højestegradkoefficienten i $p(t)$ (hvorfor det?), og vi har

$$p(t) = a_m(t - \ell_1)\ldots(t - \ell_m),$$

hvor $\ell_1, \ldots, \ell_m \in L$. Men da L er en udvidelse af K, er sætningen bevist. □

(5.15) BEMÆRKNING: Lad K være et legeme. Det kan vises, at der findes et udvidelseslegeme L af K således at der for *ethvert* $p(t) \in K[t]$, $\deg p = m$ eksisterer elementer $\ell_1, \ldots, \ell_m \in L$ således at $p(t) = a_m(t-\ell_1)(t-\ell_2)\ldots(t-\ell_m)$. Dette udsagn er selvfølgelig meget stærkere end (5.14). (Den "algebraiske afslutning" af K). □

(5.16) DEFINITION: Et legeme L, som opfylder betingelserne i (5.14), kaldes et *spaltningslegeme* for p, hvis der ikke findes noget legeme L_1, $K \subseteq L_1 \subsetneq L$, som opfylder betingelserne i (5.14). □

(5.17) EKSEMPEL: $\mathbf{Z}_2$ er et legeme med kun 2 elementer $\widehat{0}$ og $\widehat{1}$, som vi her kalder 0 og 1. Betragt polynomiet $p(t) = t^2 + t + 1 \in \mathbf{Z}_2[t]$. Da $p(0) = p(1) = 1 \neq 0$, har p ikke nogen rod i $\mathbf{Z}_2$. Betragt et udvidelseslegeme L af $\mathbf{Z}_2$ hvor $p(t)$ har en rod ℓ. For ethvert element $k \in L$ er $k + k = 0$, $k = -k$, da $k + k = 1k + 1k = (1 + 1)k = 0k = 0$. Specielt er $-\ell = \ell$. Vi har også $p(\ell) = \ell^2 + \ell + 1 = 0$, så $\ell^2 = -(\ell + 1) = \ell + 1$. Lad os bemærke, at $\ell + 1$ også er rod i p, idet $p(\ell + 1) = (\ell + 1)^2 + (\ell + 1) + 1 = \ell^2 + \ell + \ell + 1 + \ell + 1 + 1 = \ell^2 + \ell + 1 = 0$ (da $\ell + \ell = 1 + 1 = 0$). Så $p(t) = (t - \ell)(t - (\ell + 1))$. Vi påstår at $L_1 = \{0, 1, \ell, \ell + 1\}$ er et dellegeme af L, således at L_1 er spaltningslegeme for $p(t)$ over $\mathbf{Z}_2$ og altså et eksempel på et legeme med 4 elementer! (I øvrigt det

eneste). Her er kompositionstavlerne for L_1:

$+$	0	1	ℓ	$\ell+1$
0	0	1	ℓ	$\ell+1$
1	1	0	$\ell+1$	ℓ
ℓ	ℓ	$\ell+1$	0	1
$\ell+1$	$\ell+1$	ℓ	1	0

$\cdot$	0	1	ℓ	$\ell+1$
0	0	0	0	0
1	0	1	ℓ	$\ell+1$
ℓ	0	ℓ	$\ell+1$	1
$\ell+1$	0	$\ell+1$	1	ℓ

(F.eks. er $\ell+(\ell+1) = (\ell+\ell)+1 = 0+1 = 1$ og $(\ell+1)(\ell+1) = \ell^2+\ell+\ell+1 = \ell^2+1 = \ell$, da $\ell^2+\ell+1 = 0$.) Kompositionstavlerne viser, at L_1 er lukket under $+$, $\cdot$. Desuden er ℓ og $\ell+1$ hinandens inverse elementer, så L_1 *er* et legeme. □

(5.18) ØVELSE: Gør rede for, at legemet L_1 i (5.17) er et spaltningslegeme for $q(t) = t^3+1 \in \mathbf{Z}_2[t]$. □

(5.19) ØVELSE: Gøre rede for, at $q_1(t) = t^3+t^2+t+1 \in \mathbf{Z}_2[t]$ har $\mathbf{Z}_2$ som spaltningslegeme. □

3° Primlegemer. Karakteristik.

(5.20) DEFINITION: Et legeme L kaldes *primlegeme*, hvis det kun har L selv som dellegeme. □

(5.21) SÆTNING. *(1) Et primlegeme er isomorf til netop ét af legemerne $\mathbf{Q}$ eller $\mathbf{Z}_p$, p primtal.*

(2) Ethvert legeme indeholder netop et dellegeme, som er et primlegeme.

BEVIS: Lad K være et vilkårligt legeme. Det er let at se, at hvis $L_i, i \in I$, er en samling af dellegemer af K, så er $\bigcap_i L_i$ også et dellegeme af K. Derfor er $P = \bigcap_{\{L \mid L \text{ dellegeme af } K\}} L$ et dellegeme af K.

Da et dellegeme af P også er et dellegeme af K, er P et primlegeme. Hvis nu Q er et andet dellegeme af K, som er et primlegeme, så er $P \subseteq Q$, da P er fællesmængden af *alle* dellegemer. Men så må P være et dellegeme af Q og derfor lig Q, da Q er et primlegeme. Hermed er (2) bevist.

(1) Lad P være et primlegeme. Betragt for $n \in \mathbf{N}$ elementet $n' \in P$ defineret som $n' = \underbrace{1+1+\cdots+1}_{n \text{ gange}}$. Det er klart, at $(m+n)' = m'+n', (mn)' = m'n'$ for alle $m, n \in \mathbf{N}$. Antag først, at der eksisterer et $q \in \mathbf{N}$, således at $q' = 0$. Lad p være det mindste $p \in \mathbf{N}$ med $p' = 0$. (Anvend [MIN]). Hvis p ikke er et primtal, $p = rs$, $r, s \neq 1$, så er $p' = r's' = 0$, men $r', s' \neq 0$, hvilket strider mod [NU]. Så p er et

primtal. Det er så klart, at afbildningen $\widehat{i} \to i'$ er en monomorfi mellem $\mathbf{Z}_p$ og P. Da P er et primlegeme, er det en isomorfi. (Overvej dette). Hvis $q' \neq 0$ for alle $q \in \mathbf{N}$, danner $\{0' = 0, \pm 1', \pm 2', \dots\}$ en delring af P, som er isomorf til $\mathbf{Z}$. Men så er $Q(\mathbf{Z}) \simeq \mathbf{Q}$ isomorf til et dellegeme af P, altså isomorf til P. □

(5.22) DEFINITION: Lad K være et legeme. *Karakteristikken af* K, char K, er defineret ved

$$\text{char } K = \begin{cases} p & \text{hvis } \mathbf{Z}_p \text{ er } K\text{'s primlegeme} \\ 0 & \text{hvis } \mathbf{Q} \text{ er } K\text{'s primlegeme} \end{cases}$$

Så char K er 0 eller et primtal. □

4° Ordnede ringe og legemer.

(5.23) DEFINITION: En *ordnet ring* (hhv. *ordnet legeme*) er en kommutativ ring med 1-element ($\neq \{0\}$) (hhv. et legeme), der opfylder betingelsen [ORD] fra Kapitel 2. □

I en ordnet ring findes der altså en delmængde N, som vi i det følgende vil kalde mængden af *positive elementer* i R og betegne R^+, som opfylder

(1) Ethvert element i R er i netop én af mængderne $R^+, \{0\}, R^- = -R^+$.
(2) R^+ er lukket under $+$ og $\cdot$ (se (1.19)).

I så tilfælde har vi altså relationer $<$ og $\leq$ på R defineret ved

$$a < b \Leftrightarrow b - a \in R^+$$
$$a \leq b \Leftrightarrow b - a \in R^+ \quad \text{eller } a = b$$

og en *absolutværdi* (*norm*, *valuering*)

$$|a| = \begin{cases} a & \text{hvis } a \in R^+ \\ -a & \text{ellers,} \end{cases}$$

så $0 \leq |a|$ for alle $a \in R$. Idet beviserne for (2.3) og (2.5) kun er baserede på [RAK] – [RD] og [ORD], er alle udsagn i disse sætninger opfyldte for $\leq, <$ og $|\cdot|$ defineret ovenfor. Specielt er $(R, \leq)$ en *po*-mængde. Betingelse (1) ovenfor viser at [BRL] er opfyldt for $\leq$, så $(R, \leq)$ er en *lo*-mængde ((0.19)).

Endvidere fås fra (2.4):

(5.24) SÆTNING. *En ordnet ring er en integritetsring.*

□

(5.25) ØVELSE: Lad R være en ordnet ring.

(1) Vis, at $0 < a^2$ for alle $a \in R, a \neq 0$. Specielt er $0 < 1$, hvor 1 er R's etelement.

(2) For $n \in \mathbb{N}$ lader vi $n' = \underbrace{1+1+\cdots+1}_{n \text{ gange}} \in R$. Vis, at $0 < n'$.

(3) Vis, at et ordnet legeme har karakteristik 0.

□

(5.26) DEFINITION: Lad R og S være ordnede ringe.

(1) Hvis S er en delring af R siger vi at ordningen i R *udvider* ordningen i S, hvis der gælder

$$R^+ \cap S = S^+$$

(så for alle $s \in S$ gælder: $0 < s$ (i S) $\Leftrightarrow 0 < s$ (i R).) Vi har altså $(S, \leq) \subseteq (R, \leq)$.

(2) En (ring)homomorfi $\varphi : R \to S$ kaldes *ordningsbevarende*, hvis der gælder

$$\varphi(R^+) \subseteq S^+,$$

(altså $0 < r \Rightarrow 0 < \varphi(r)$). □

(5.27) BEMÆRKNING: Hvis $n \in \mathbb{N}$ lader vi n' være som i (5.25)(2), og sætter $(-n)' = -n'$, $0' = 0$, således at der for hvert $z \in \mathbb{Z}$ er defineret et $z' \in R$. (Sml. beviset for (5.21)(1)). Så er afbildningen $z \longrightarrow z'$ en ordningsbevarende monomorfi fra den ordnede ring $\mathbb{Z}$ til R, når R er en ordnet ring. I overensstemmelse med det tidligere nævnte princip om at identificere isomorfe algebraiske strukturer, vil vi identificere $\mathbb{Z}$ med dens indlejring i R. Vi opfatter altså $\mathbb{Z}$ som en delring af R, og ordningen i R udvider så ordningen i $\mathbb{Z}$ ifølge (5.25)(2). På tilsvarende måde vil et ordnet *legeme* K have $\mathbb{Q}$ som dellegeme, således at ordningen i K udvider ordningen i $\mathbb{Q}$. I en ordnet ring R (hhv. ordnet legeme K) har derfor udtryk som $zx, z \in \mathbb{Z}, x \in R$ (hhv. $qx, q \in \mathbb{Q}, x \in K$) en veldefineret mening som elementer i R (hhv. K). □

(5.28) ØVELSE: Betragt polynomringen $\mathbb{Q}[t]$. Vi sætter

$$\mathbb{Q}[t]^+ = \{f \in \mathbb{Q}[t] \mid f \neq 0 \text{ og højestegradkoefficienten i } f \text{ er positiv (i } \mathbb{Q})\}$$

(1) Vis, at med dette valg af $\mathbb{Q}[t]^+$ er $\mathbb{Q}[t]$ en ordnet ring.

(2) Vis, at der for alle $n \in \mathbb{Z}$ gælder $n < t$ (ved ordningen i $\mathbb{Q}[t]$). □

Den ovenstående øvelse viser, at følgende betingelse for en ring er *stærkere* end [ORD].

[AORD] R opfylder [ORD] og der gælder yderligere:
For alle $x \in R$ findes et $n \in \mathbb{N}$ så $x < n$.

(5.29) DEFINITION: En *arkimedisk ordnet ring* (hhv. arkimedisk ordnet legeme) er en kommutativ ring med 1-element (hhv. et legeme), der opfylder betingelsen [AORD]. □

Det er klart at $\mathbb{Z}, \mathbb{Q}$ opfylder [AORD]. Med ordningen fra (5.28) opfylder $\mathbb{Q}[t]$ [ORD], men *ikke* [AORD].

(5.30) ØVELSE: Lad R være en ordnet ring, $a, b, c, d \in R$, $b, d \neq 0$. Antag, at $ad = bc$ og at $0 < ab$. Vis, at $0 < cd$. (Man kan anvende udsagn fra (2.3)). □

(5.31) ØVELSE: Lad $Q(R)$ være brøklegemet af den ordnede ring R. Vis, at $Q(R)$ kan ordnes på netop én måde ved en udvidelse af ordningen i R. (Løsningshjælp: Antag, at en ordning på $Q(R)$ udvider R's ordning. Hvis $a, b \in R$, $b \neq 0$ må (da $b^2 \in R^+$ og $[a,b]b^2 = [a,b][b^2,1] = [ab,1] = ab$)

$$(*) \qquad [a,b] \in Q(R)^+ \Leftrightarrow ab \in R^+.$$

Hvis man så benytter $(*)$ som *eneste mulige* definition af $Q(R)^+$, viser (5.30), at det er veldefineret. Altså $Q(R)^+ = \{[a,b] \in Q(R) \mid 0 < ab\}$. Det må så vises, at med dette valg af positive elementer er [ORD] opfyldt i $Q(R)$.) □

5° Fuldstændiggørelse af et ordnet legeme. De reelle tal.

Det er muligt at opbygge væsentlige dele af den matematiske analyse (som præsenteret i Mat 1 m.m.) på en aksiomatisk beskrivelse af de reelle tals legeme $\mathbb{R}$.

Man antager, at $\mathbb{R}$ er en mængde med kompositioner $+, \cdot$ og en ordningsrelation $\leq$, som gør $\mathbb{R}$ til et "totalt ordnet legeme med supremumsegenskaben". Dette betyder

(1) $\mathbb{R}$ er et ordnet legeme (som defineret i (5.23)).
(2) Den lineært ordnede mængde (ℓo-mængden) $(\mathbb{R}, \leq)$ opfylder [SUP] (se Kapitel 0).

(I (2) er $\leq$ selvfølgelig den ordningsrelation, der kommer fra [ORD]-betingelsen på $\mathbb{R}$).

Vi viser i det følgende at et ordnet legeme kan "fuldstændiggøres": Givet et ordnet legeme K konstruerer vi et ordnet legeme $F(K)$ og en ordningsbevarende monomorfi fra K til $F(K)$. Legemet $F(K)$ har den egenskab, at enhver Cauchy følge (fundamentalfølge) af elementer fra $F(K)$ har en grænseværdi i $F(K)$. ($F(K)$ er "fuldstændigt"). (F.eks. er $\mathbb{Q}$ et ikke-fuldstændigt ordnet legeme). Yderligere vises, at hvis K er arkimedisk ordnet, så er $F(K)$ det også, og i dette tilfælde opfylder $F(K)$ supremumsbetingelsen [SUP]. Hvis vi (som tidligere) identificerer K med dets indlejring i $F(K)$ vil $F(K)$ være et udvidelseslegeme af K, hvis ordning udvider K's ordning. Hvis vi specielt anvender denne konstruktion på det arkimedisk ordnede legeme $\mathbb{Q}$ fås som fuldstændiggørelse et legeme, der opfylder de aksiomer, $\mathbb{R}$ skal opfylde. Dette sikrer altså *eksistensen* af $\mathbb{R}$. Det kan vises, at de ovennævnte aksiomatiske egenskaber karakteriserer $\mathbb{R}$ pånær en ordningsbevarende isomorfi.

I resten af dette kapitel vil K være et ordnet legeme. Som i 4° betegner K^+ mængden af positive elementer. Før læseren går videre, bør han/hun læse (5.27)

igen. Vi betragter altså $\mathbb{Q} \subseteq K$. I den følgende definition bruger vi ordningen $<$ ($\leq$) på K og absolutværdien $|\cdot|$ på K, (4°). Definitionen ligner noget velkendt fra $\mathbb{R}$, men vi arbejder altså i et "abstrakt" ordnet legeme K.

(5.32) DEFINITION: Lad $(a_0) = (a_1, a_2, \ldots, a_n, \ldots)$ være en (uendelig) følge af elementer i K.

(1) Følgen (a_i) kaldes en *Cauchy-følge* (*fundamentalfølge*) hvis der gælder

For alle $\varepsilon \in K^+$ findes et $n = n(\varepsilon) \in \mathbb{N}$, således at $|a_p - a_q| < \varepsilon$ for alle $p, q \geq n$.

(2) Følgen (a_i) kaldes en *nulfølge*, hvis der gælder

For alle $\varepsilon \in K^+$ findes et $n = n(\varepsilon) \in \mathbb{N}$, således at $|a_p| < \varepsilon$ for alle $p \geq n$.

(3) Mængden af Cauchy følger af elementer fra K betegnes $CF(K)$. Tilsvarende betegnes mængden af nulfølger med $CF_0(K)$. □

(5.33) SÆTNING. *(1) $CF_0(K) \subseteq CF(K)$, (altså en nulfølge er en Cauchy-følge.)*

(2) Lad $(a_i) \in CF(K)$. Der eksisterer $m \in K^+$ således at $|a_i| \leq m$ for alle $i \in \mathbb{N}$. (En Cauchy-følge er begrænset.)

BEVIS: (1) Lad (a_i) være en nulfølge. Lad $\varepsilon \in K^+$. Vælg ifølge (5.32)(2) et $n = n(\frac{\varepsilon}{2})$ således at $|a_p| < \frac{\varepsilon}{2}$ for alle $p \geq n$. Så gælder for alle $p, q \geq n$ (under anvendelse af (2.5)(4))

$$|a_p - a_q| \leq |a_p| + |a_q| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon.$$

(2) Lad (a_i) være en Cauchy-følge. Lad $\varepsilon \in K^+$. Vælg $n = n(\varepsilon)$ så $|a_p - a_q| < \varepsilon$ for alle $p, q \geq n$. Specielt gælder så for alle $p \geq n$: $|a_n - a_p| < \varepsilon$. For $p \geq n$ fås så

$$|a_p| = |(a_p - a_n) + a_n| \leq |a_p - a_n| + |a_n| < |a_n| + \varepsilon.$$

Så vil ethvert $m \in K^+$, som opfylder de endelig mange betingelser

$$|a_1| \leq m, |a_2| \leq m, \ldots, |a_{n-1}| \leq m, |a_n| + \varepsilon \leq m,$$

opfylde $|a_i| \leq m$ for alle i. (Overvej, hvorfor et sådant $m \in K^+$ findes? Kan f.eks. $m = |a_1| + |a_2| + \cdots + |a_{n-1}| + |a_n| + \varepsilon$ bruges?) □

(5.34) DEFINITION: Lad (a_i) og (b_i) være følger af elementer fra K. Vi definerer følgernes *sum* og *produkt* ved

$$(a_i) + (b_i) = (a_i + b_i), \quad (a_i)(b_i) = (a_i b_i)$$

(så f.eks. er $(a_i) + (b_i) = (a_1 + b_1, a_2 + b_2, \ldots, a_p + b_p, \ldots)$). □

(5.35) HJÆLPESÆTNING. *Lad $(a_i), (b_i) \in CF(K)$. Der gælder*

(1) $(a_i) + (b_i) \in CF(K)$

(2) $(a_i)\ (b_i) \in CF(K)$

(3) *Hvis $(b_i) \in CF_0(K)$ er $(a_i)(b_i) \in CF_0(K)$*

(4) *Hvis $(a_i), (b_i) \in CF_0(K)$ er $(a_i) + (b_i) \in CF_0(K)$.*

BEVIS: (1) Lad $\varepsilon \in K^+$ være givet. Vælg $n_1, n_2 \in \mathbb{N}$ således at $|a_p - a_q| < \frac{\varepsilon}{2}$ for alle $p, q \geq n_1$ og $|b_p - b_q| < \frac{\varepsilon}{2}$ for alle $p, q \geq n_2$. Hvis $n \geq n_1$, og $n \geq n_2$ gælder for $p, q \geq n$ (igen benyttes (2.5)(4))

$$\begin{aligned} |(a_p + b_p) - (a_q + b_q)| &= |(a_p - a_q) + (b_p - b_q)| \\ &\leq |a_p - a_q| + |b_p - b_q| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon. \end{aligned}$$

(2) Vælg ifølge (5.33)(2) $m_1, m_2 \in K^+$ så $|a_i| \leq m_1$ for alle $i \geq 1$ og $|b_i| \leq m_2$ for alle $i \geq 1$. Lad $\varepsilon \in K^+$ være givet. Vælg $n_1, n_2 \in \mathbb{N}$ således at

$$(*) \qquad \begin{cases} |a_p - a_q| < \frac{1}{2}\varepsilon m_2^{-1} & \text{for alle } p, q \geq n_1 \\ |b_p - b_q| < \frac{1}{2}\varepsilon m_1^{-1} & \text{for alle } p, q \geq n_2. \end{cases}$$

Hvis $n \geq n_1, n \geq n_2$ gælder for $p, q \geq n$

$$\begin{aligned} |a_p b_p - a_q p_q| &= |a_p(b_p - b_q) + (a_p - a_q)b_q| \\ &\leq |a_p(b_p - b_q)| + |(a_p - a_q)b_q| && ((2.5)(4)) \\ &= |a_p||b_p - b_q| + |a_p - a_q||b_q| && ((2.5)(3)) \\ &\leqq m_1|b_p - b_q| + |a_p - a_q|m_2 && ((2.3)(2)') \\ &< m_1\left(\frac{1}{2}\varepsilon m_1^{-1}\right) + \left(\frac{1}{2}\varepsilon m_2^{-1}\right)m_2 && ((*) \text{ ovenfor}) \\ &= \frac{1}{2}\varepsilon + \frac{1}{2}\varepsilon = \varepsilon. \end{aligned}$$

□

(5.36) ØVELSE: Bevis (5.35)(3)–(4). □

(5.37) HJÆLPESÆTNING. *Lad $(a_i) \in CF(K) \setminus CF_0(K)$. Der findes et $\delta \in K^+$ og et $n \in \mathbb{N}$, således at*

$$|a_p| \geq \delta \quad \textit{for alle } p \geq n.$$

(Specielt er så $a_p \neq 0$ for alle $p \geq n$).

BEVISET føres indirekte: Hvis hjælpesætningens udsagn er forkert, gælder:

$$(1) \qquad \begin{cases} \text{For alle } \delta \in K^+ \text{ og for alle } n \in \mathbb{N} \text{ eksisterer} \\ \text{et } p \geq n \text{ så } |a_p| < \delta. \end{cases}$$

Lad $\varepsilon \in K^+$ være givet. Da (a_i) er en Cauchy-følge, eksisterer et $n' \in \mathbb{N}$, så $|a_p - a_q| < \frac{1}{2}\varepsilon$ for alle $p, q \geq n'$. Idet vi anvender udsagnet (1) for $\delta = \frac{1}{2}\varepsilon$ og $n = n'$ ses, at der findes et $p' > n'$, så $|a_{p'}| < \frac{1}{2}\varepsilon$. For $q \geq n'$ gælder da

$$\begin{aligned} |a_q| &= |a_q - a_{p'} + a_{p'}| \\ &\leq |a_q - a_{p'}| + |a_{p'}| < \frac{1}{2}\varepsilon + \frac{1}{2}\varepsilon = \varepsilon. \end{aligned}$$

Men så er (a_i) en nulfølge, hvilket strider mod antagelsen. □

(5.38) ØVELSE: (1) Lad (b_i) være en følge af elementer fra K, der opfylder: Der findes et $n \in \mathbf{N}$, således at $b_p = 0$ for alle $p \geq n$. Vis at $(b_i) \in CF_0(K)$.

(2) Lad $(a_i) \in CF(K) \setminus CF_0(K)$. Vis (under anvendelse af (5.37)), at der findes en følge $(b_i) \in CF_0(K)$ således at $a_i + b_i \neq 0$ for alle $i \in \mathbf{N}$. □

(5.39) HJÆLPESÆTNING. *Lad $(c_i) \in CF(K) \setminus CF_0(K)$. Antag, at $c_i \neq 0$ for alle $i \in \mathbf{N}$. Hvis $d_i = c_i^{-1}$ for alle i, er $(d_i) \in CF(K)$.*

BEVIS: Ifølge (5.37) eksisterer $\delta \in K^+$ og $n \in \mathbf{N}$ så $|c_p| \geq \delta$ for alle $p \geq n$. Vælger vi η som det "mindste" (hvad er det?) af $|c_1|, \ldots, |c_n|, \delta$ er $\eta \in K^+$ og $\eta \leq |c_i|$ for alle $i \in \mathbf{N}$. Lad $\varepsilon \in K^+$ være givet. Vælg $n = n(\varepsilon\eta^2)$, således at $|c_p - c_q| < \varepsilon\eta^2$ for alle $p, q \geq n$. Antag, at der findes $p, q \geq n$, så $|d_p - d_q| \geqq \varepsilon$. Så er

$$|c_p - c_q| = |c_p c_q (d_q - d_p)| = |c_p||c_q||d_p - d_q| \geq \eta^2 \varepsilon,$$

en modstrid. Altså må $|d_p - d_q| < \varepsilon$ for alle $p, q \geq n$. □

(5.40) ØVELSE: Lad (d_i) være som i (5.39). Vis at (d_i) ikke er en nulfølge. (Man kan anvende, at $|c_i| \geq \eta$ for alle $i \in \mathbf{N}$). □

(5.41) ØVELSE: Betragt polynomringen $\mathbf{Q}[t]$ fra Øvelse (5.28) med ordningen givet dér. Udvid (ifølge (5.31)) ordningen på $\mathbf{Q}[t]$ til en ordning på $L = Q(\mathbf{Q}[t])$, brøklegemet af $\mathbf{Q}[t]$. Gør rede for, at følgen

$$\left(1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}, \ldots\right)$$

er en Cauchy-følge i $\mathbf{Q}$ men ikke i L. Er følgen

$$(1, t^{-1}, t^{-2}, \ldots, t^{-n}, \ldots)$$

en Cauchy-følge i L? □

(5.42) SÆTNING. *(1) $(CF(K), +, \cdot)$ er en kommutativ ring med 1-element.*

(2) $CF_0(K)$ er et maksimalt ideal i $CF(K)$.

BEVIS: (5.35)(1)–(2) viser at $+, \cdot$ er kompositioner på $CF(K)$. Det er klart, at et hvilket som helst af ringaksiomerne [RAK] – [RD] gælder i $CF(K)$, fordi det gælder i K.

(F.eks.: Vi vil vise [RMK] i $CF(K)$. Der gælder

$$(a_i)(b_i) = (a_i b_i) \quad \text{og} \quad (b_i)(a_i) = (b_i a_i).$$

Da [RMK] gælder i K, er $a_ib_i = b_ia_i$ for alle $i \in \mathbb{N}$, og derfor $(a_i)(b_i) = (b_i)(a_i)$. 1-elementet i $CF(K)$ er den konstante følge (1).)

(5.35)(3)–(4) viser, at $CF_0(K)$ er et ideal i $CF(K)$. $CF_0(K) \neq CF(K)$, da den konstante følge (1) ikke er en nulfølge. Lad I være et ideal i $CF(K)$, så $CF_0(K) \subseteq I$, $CF_0(K) \neq I$. Lad $(a_i) \in I \setminus CF_0(K)$. Ifølge (5.38)(2) findes en følge $(b_i) \in CF_0(K)$, således, at hvis $(c_i) = (a_i) + (b_i)$, så er $c_i \neq 0$ for alle $i \in \mathbb{N}$. Da $(a_i) \in I$ og $(b_i) \in CF_0(K) \subseteq I$, er $(c_i) \in I$. Hvis $d_i = c_i^{-1}$ for alle i, er $(d_i) \in CF(K)$ ifølge (5.39). Da I er et ideal i $CF(K)$ og $(c_i) \in I$, er $(d_i)(c_i) = (1) \in I$. Dermed er $I = CF(K)$ ifølge (3.4)(4). □

(5.43) DEFINITION: I notationen fra (5.42) sættes

$$F(K) = CF(K)/CF_0(K).$$

Ifølge (3.29)(2) er $F(K)$ et legeme, som vi kalder *fuldstændiggørelsen* af K. □

(5.44) HJÆLPESÆTNING. *Afbildningen $d : K \to L = F(K)$ defineret ved $d(a) = \widehat{(a)}$ er en monomorfi. (Her er (a) følgen, hvor alle elementer er lig a, og $\widehat{(a)}$ er (a)'s restklasse i $L = F(K)$, se (3.19)).*

BEVIS: Lad os bemærke at (a) er en nulfølge netop når $a = 0$. Med denne bemærkning bevises sætningen let. □

Vi identificerer K med dets indlejring i L ved d og betragter K som dellegeme af $L = F(K)$.

(5.45) HJÆLPESÆTNING. *Lad $(a_i) \in CF(K) \setminus CF_0(K)$. Der findes et $\delta \in K^+$ og et $n \in \mathbb{N}$ således at*

enten (i) $a_p > \delta$ *for alle* $p \geq n$
eller (ii) $a_p < -\delta$ *for alle* $p \geq n$.

BEVIS: Vælg ifølge (5.37) $\delta \in K^+$ og $n_1 \in \mathbb{N}$ således at $|a_p| \geq \delta$ for alle $p \geq n_1$. Da (a_i) er en Cauchy-følge, eksisterer et n_2, således at $|a_p - a_q| < \delta$ for alle $p, q \geq n_2$. Lad n være det største af tallene n_1, n_2. For ethvert $p \geq n$ gælder $|a_p| \geq \delta$, altså, ifølge definitionen af $|\cdot|$,

$$\text{enten} \quad a_p \geq \delta \quad \text{eller} \quad -a_p \geq \delta.$$

Vi antager at $a_p \geq \delta$ for et $p \geq n$ og viser så at $a_q \geq \delta$ for alle $q \geq n$. (Tilfældet $-a_p \geq \delta$, altså $-\delta \geq a_p$, behandles analogt). Hvis der findes et $q \geq n$ så $-a_q \geq \delta$, er $a_p - a_q = a_p + (-a_q) \geq \delta + \delta = 2\delta$, en modstrid, da $|a_p - a_q| < \delta$ for $p, q \geq n$. □

(5.46) DEFINITION: En følge $(a_i) \in CF(K) \setminus CF_0(K)$ kaldes *positiv*, hvis (i) forekommer i (5.45). Ellers kaldes den *negativ*. □

(5.47) ØVELSE: (1) Lad $(a_i) \in CF(K) \setminus CF_0(K)$, $(b_i) \in CF_0(K)$. Vis

$$(a_i) \quad \text{positiv} \quad \Leftrightarrow \quad (a_i) + (b_i) \quad \text{positiv}.$$

(2) Lad $(a_i), (b_i) \in CF(K) \setminus CF_0(K)$ være positive. Vis, at $(a_i) + (b_i)$ og $(a_i)(b_i)$ er positive. □

(5.48) ØVELSE: Lad $a \in K \setminus \{0\}$. Vis

$$(a) \quad \text{positiv} \Leftrightarrow \quad a \in K^+.$$

□

(5.49) DEFINITION: Vi sætter

$$F(K)^+ = \{\widehat{(a_i)} \in F(K) \mid (a_i) \text{ er positiv}\}.$$

Dette er veldefineret ifølge (5.47)(1). □

(5.50) SÆTNING. *Med $F(K)^+$ som mængden af positive elementer er $F(K)$ et ordnet legeme, hvis ordning udvider ordningen i K.*

BEVIS: En øvelse. (Man kan finde alle relevante kendsgerninger i (5.45),(5.47) og (5.48)). □

Vores næste opgave er at vise, at enhver Cauchy-følge i $F(K)$ er konvergent i $F(K)$, og at K er "overalt tæt" i $F(K)$. Denne opgave må først forberedes lidt.

(5.51) BEMÆRKNINGER: Lad $f = \widehat{(a_i)} \in F(K)$, hvor altså $(a_i) \in CF(K)$.

(1) Hvis der findes et $n \in \mathbb{N}$, således at $0 \leq a_p$ (ulighed i K) for alle $p \geq n$, gælder $0 \leq f$ (i $F(K)$). (Der gælder nemlig, at enten er (a_i) en nulfølge og dermed $f = 0$, eller også er $(a_i) \in CF(K) \setminus CF_0(K)$, og så må tilfældet (i) optræde i (5.45). Det betyder at (a_i) er positiv, altså $0 < f$.

(2) Analogt ses, at hvis der findes et $n \in \mathbb{N}$, således at $a_p \leq 0$ for alle $p \geq n$, gælder $f \leq 0$.

(3) Lad yderligere $a \in K$. Hvis der findes et $n \in \mathbb{N}$, således at $a \leq a_p$ for alle $p \geq n$ (hhv. $a_p \leq a$ for alle $p \geq n$), gælder

$$a \leq f \ \text{(i } F(K)) \quad (\text{hhv. } f \leq a \ \text{(i } F(K))).$$

Dette ses ved at anvende (1) og (2) på $f - a = \{\widehat{a_i - a}\}$. □

(5.52) HJÆLPESÆTNING. *Hvis $f \in F(K)^+$, eksisterer et $a \in K^+$, så $a < f$.*

BEVIS: Lad $f = \widehat{(a_i)}$. Da (a_i) er positiv, eksisterer et $\delta \in K^+$ og et $n \in \mathbb{N}$, så $a_p \geq \delta$ for alle $p \geq n$. Ifølge (5.51)(3) er $\delta \leq f$. Sæt $a = \frac{1}{2}\delta$. Så er $a < \delta \leq f$, altså $a < f$. Da $\delta \in K^+$, er $a \in K^+$. □

Da der er "flere" positive elementer i $F(K)$ end i K, kræver følgende udsagn et bevis:

(5.53) HJÆLPESÆTNING. *En nulfølge i K er også en nulfølge i $F(K)$.*

BEVIS: Lad $(a_i) \in CF_0(K)$. Lad $f \in F(K)^+$. Vi skal vise, at der eksisterer et $n = n(f)$, så $|a_p| < f$ (i $F(K)$) for alle $p \geq n$. Vælg ifølge (5.52) $\varepsilon \in K^+$, så $\varepsilon < f$. Da (a_i) er en nulfølge i K, findes et $n' = n(\varepsilon)$, således at $|a_p| < \varepsilon$ for alle $p \geq n'$. Men så gælder også $|a_p| < f$, da $\varepsilon < f$. Som $n(f)$ kan vi altså vælge n'. □

(5.54) ØVELSE: Lad (a_i) være en Cauchy følge i $F(K)$. Antag, at $a_i \in K$ for alle $i \in \mathbf{N}$. Vis $(a_i) \in CF(K)$. □

(5.55) DEFINITION: Lad L være et vilkårligt ordnet legeme (f.eks. K eller $F(K)$ ovenfor). En følge (ℓ_i) af elementer fra L siges at *konvergere* mod $\ell \in L$, hvis $(\ell_i - \ell) \in CF_0(L)$.

(Det betyder altså, at der for alle $\varepsilon \in L^+$ findes et $n = n(\varepsilon)$, således at $|\ell_p - \ell| < \varepsilon$ for alle $p \geq n$.) Vi skriver så $\lim(\ell_i) = \ell$. Følgen (ℓ_i) kaldes *konvergent* hvis der eksisterer et $\ell \in L$ så $\lim(\ell_i) = \ell$. □

(5.56) ØVELSE: Lad (ℓ_i) og (ℓ_i') være følger i det ordnede legeme L. Lad $\ell, \ell' \in L$ så $\lim(\ell_i) = \ell$, $\lim(\ell_i) = \ell'$. Vis

$$\lim(\ell_i + \ell_i') = \ell + \ell' \quad \lim(\ell_i - \ell_i') = \ell - \ell'$$
$$\lim(\ell_i \ell_i') = \ell\ell'. \qquad \text{(Anvend f.eks. (5.35))}$$

□

(5.57) HJÆLPESÆTNING. *Lad $f = \widehat{(a_i)} \in F(K)$. Der gælder $\lim(a_i) = f$.*

BEVIS: Der skal bevises et udsagn om konvergens i $F(K)$, idet a_i'erne opfattes som elementer i $F(K)$. Lad $\varepsilon \in F(K)^+$. Vi søger et n, således at $|f - a_p| < \varepsilon$ (i $F(K)$) for alle $p \geq n$. Vælg ifølge (5.52) $\delta \in K^+$, så $\delta < \varepsilon$. Vælg $n = n(\delta)$, således at $|a_q - a_p| < \delta$ for alle $p, q \geq n$. Vi påstår, at $|f - a_p| < \varepsilon$ for $p \geq n$. Det er nok at vise, at $|f - a_p| \leq \delta$ for $p \geq n$. Nu er $f - a_p = \widehat{(a_i - a_p)}$, så $f - a_p$ er repræsenteret af den Cauchy-følge, hvis i'te element er $a_i - a_p$. For $q \geq n$ er $-\delta < a_q - a_p < \delta$, og derfor er $-\delta \leq f - a_p \leq \delta$ ifølge (5.51)(3), altså $|f - a_p| \leq \delta$, som ønsket. □

(5.58) BEMÆRKNING: Hvis $f \in F(K)$, $\varepsilon \in F(K)^+$, eksisterer et $a \in K$, således at $|f - a| < \varepsilon$. Dette er en direkte følge af beviset for (5.57) (Overvej!) □

(5.59) SÆTNING. *Lad $f, g \in F(K)$, $f < g$. Der eksisterer et $a \in K$, så $f < a < g$. (Dette udtrykker, at K er overalt tæt i $F(K)$.)*

BEVIS: Sæt $\varepsilon = \frac{1}{2}(g - f)$, $h = \frac{1}{2}(f + g)$. Så er $\varepsilon \in F(K)^+$. Vælg ifølge (5.58) $a \in K$, så $|h - a| < \varepsilon$. Det betyder, at $-\varepsilon < h - a < \varepsilon$, hvilket kan omformes til $h - \varepsilon < a < h + \varepsilon$. Men $h + \varepsilon = g$ og $h - \varepsilon = f$. □

(5.60) ØVELSE: Lad $(f_i) \in CF(L)$, L ordnet legeme. Sæt $\varepsilon_i = |f_i - f_{i+1}|$ for alle $i \in \mathbf{N}$. Vis, at (ε_i) er en nulfølge. □

(5.61) SÆTNING. *Enhver Cauchy følge i $F(K)$ er konvergent i $F(K)$.*

BEVIS: Lad (f_i) være en Cauchy følge i $F(K)$. Hvis følgen er konstant fra et vist trin, altså hvis der eksisterer $n \in \mathbf{N}$, $f \in F(K)$, så $f_p = f$ for $p \geq n$, så er $\lim(f_i) = f$, og vi er færdige. Vi antager nu, at (f_i) *ikke* er konstant fra noget trin. Vi kan så definere en uendelig delfølge (g_i) af (f_i) som følger:

Lad $g_1 = f_1$. Sæt $T_1 = \{t \in \mathbf{N} \mid t \geq 2 \text{ og } f_t \neq g_1\}$. Da (f_i) ikke er konstant fra noget trin er $T_1 \neq \emptyset$. Lad ifølge [MIN] $t_1 \in T_1$, så $t_1 \leq t$ for alle $t \in T_1$. Lad $g_2 = f_{t_1}$. Sæt $T_2 = \{t \in \mathbf{N} \mid t \geq t_1 \text{ og } f_t \neq g_2\}$. Igen er $T_2 \neq \emptyset$. Lad $g_3 = f_{t_2}$, hvor $t_2 \in T_2$ og $t_2 \leq t$ for alle $t \in T_2$. Idet vi fortsætter på denne måde, fås delfølgen (g_i), der ifølge dens definition har egenskaben, at $g_i \neq g_{i+1}$ for alle i. Nu er (f_i) konvergent netop når (g_i) er konvergent (overvej!) og i dette tilfælde har de samme den samme grænseværdi. Denne overvejelse tjener kun til at indse, at vi uden indskrænkning kan antage, at $f_i \neq f_{i+1}$ for alle $i \in \mathbf{N}$. I dette tilfælde sættes $\varepsilon_i = |f_i - f_{i+1}|$ således at $\varepsilon_i \in F(K)^+$ for alle $i \in \mathbf{N}$. Endvidere er (ε_i) en nulfølge. ((5.60)). Lad $i \in \mathbf{N}$. Ifølge (5.58) eksisterer et $a_i \in K$ således at $|f_i - a_i| < \varepsilon_i$. Vi sætter $f = \widehat{(a_i)}$ og påstår, at $\lim(f_i) = f$. Først må vises at $(a_i) \in CF(K)$. Da (ε_i) er en nulfølge og $|f_i - a_i| < \varepsilon_i$, er $(f_i - a_i)$ en nulfølge (i $F(K)$). Da (f_i) er en Cauchy-følge, må $(a_i) = (f_i) - (f_i - a_i)$ være Cauchy- følge i $F(K)$. Ifølge (5.54) er så $(a_i) \in CF(K)$. Nu vises at $\lim f_i = f$. Ifølge (5.57) er $\lim(a_i) = f$. Da $(f_i - a_i)$ er en nulfølge, er $\lim(f_i - a_i) = 0$. Da $(f_i) = (f_i - a_i) + (a_i)$, viser (5.56), at $\lim(f_i) = f$, som ønsket. □

(5.62) ØVELSE: (1) Lad $f \in F(K)$. Vis, at der findes et $a \in K$ så $f \leq a$.
(2) Vis, at hvis K er arkimedisk ordnet, så er $F(K)$ arkimedisk ordnet. □

(5.63) LEMMA. *Lad K være arkimedisk ordnet. For alle $\varepsilon \in K^+$ eksisterer $n \in \mathbf{N}$, så $\frac{1}{2^n} < \varepsilon$.*

BEVIS: Vælg $n \in \mathbf{N}$ så $\varepsilon^{-1} \leq n$. Det er klart, at $n < 2^n$, så $\varepsilon^{-1} < 2^n$. Så er $\frac{1}{2^n} < \varepsilon$, som ønsket. (Hvis man ikke ved, hvorfor $n < 2^n$, kan man let bevise det, f.eks. ved induktion.) □

(5.64) SÆTNING. *Hvis K (og dermed $F(K)$) er arkimedisk ordnet, opfylder $F(K)$ supremumsbetingelsen [SUP].*

BEVIS: Lad $X \subseteq F(K)$, $X \neq \emptyset$. Antag, at $\mathrm{Maj}(X)$, mængden af majoranter for X, er $\neq \emptyset$. Vi skal vise at der findes $f \in \mathrm{Maj}(X)$ således at $f \leq g$ for alle $g \in \mathrm{Maj}(X)$.

Lad $s \in \mathrm{Maj}(X)$, $y \in X$. Vælg $n, n' \in \mathbf{N}$ så $s < n$, $-y < n'$. Så er $-n' < y(\leq s) < n$. Dette viser, at

$$(1) \qquad -n' \notin \mathrm{Maj}(X), \quad n \in \mathrm{Maj}(X).$$

For $p \in \mathbf{N}$ sættes

$$I_p = \left\{ \frac{k}{2^p} \mid k \in \mathbf{Z}, -n' \leq \frac{k}{2^p} \leq n \right\}$$

og

$$M_p = I_p \cap \mathrm{Maj}(X).$$

Så M_p er endelig og ikke-tom, da $n \in M_p$. Lad a_p være det *mindste* element i M_p. Da $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_p \subseteq \ldots$, fås $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_p \subseteq \ldots$ og derfor $a_1 \geq a_2 \geq \cdots \geq a_p \geq \ldots$, dvs.

(2) $$\text{For } p \geq q \text{ er } a_q \leq a_p.$$

Yderligere gælder

(3) $$a_p - \frac{1}{2^p} < a_q \quad \text{for alle } p, q.$$

Dette ses som følger: Da $a_p \neq -n'$ ifølge (1) (a_p er en majorant, $-n'$ ikke), fås $a_p - \frac{1}{2^p} \in I_p$. Da a_p er minimal i M_p, er $a_p - \frac{1}{2^p} \notin \mathrm{Maj}(X)$, så der findes et $x \in X$ med $a_p - \frac{1}{2^p} < x$. Da $a_q \in \mathrm{Maj}(X)$, er $x \leq a_q$, hvormed (3) er bevist. Ved at kombinere (2) og (3) fås

$$a_p - \frac{1}{2^p} < a_q \leq a_p \quad \text{for alle } q \geq p, \text{ så}$$

(4) $$|a_p - a_q| \leq \frac{1}{2^p} \quad \text{for alle } q \geq p.$$

Vi påstår, at $(a_i) \in CF(K)$: Lad $\varepsilon \in K^+$. Vælg ifølge (5.63) $n \in \mathbf{N}$ så $\frac{1}{2^n} < \varepsilon$. For $q \geq p \geq n$ er så ifølge (4) $|a_p - a_q| \leq \frac{1}{2^p} \leq \frac{1}{2^n} < \varepsilon$.

Vi sætter $f = \widehat{(a_i)}$ og viser, at f er det ønskede supremum. Ifølge (2) og (5.51)(3) er

(5) $$f \leq a_p \quad \text{for alle } p.$$

Hvis $x \in X$ er $x \leq a_p$ for alle p, da $a_p \in \mathrm{Maj}(X)$. Derfor viser (5.51)(3), at $x \leq f$. Så $f \in \mathrm{Maj}(X)$. Lad $g \in \mathrm{Maj}(X)$. Vi skal vise $f \leq g$. Hvis ikke, er $g < f$, så $f - g \in F(K)^+$. Vælg ifølge (5.63) $n \in \mathbf{N}$, så

(6) $$\frac{1}{2^n} < f - g.$$

Da $a_n - \frac{1}{2^n} \notin \mathrm{Maj}(X)$ (se ovenfor), eksisterer $x \in X$, så $a_n - \frac{1}{2^n} < x$. Da $g \in \mathrm{Maj}(X)$, er $x \leq g$, så

(7) $$a_n - \frac{1}{2^n} < g.$$

Ved at addere (6) og (7) fås $a_n < f$, hvilket strider mod (5). □

6° De reelle tal kan ikke tælles.

Som det blev lovet i Kapitel 0, vil vi her forklare, hvorfor $\mathbb{R}$ ikke er tællelig. ((0.18)). Vi giver faktisk et bevis baseret på den ovenstående beskrivelse af $\mathbb{R}$ som fuldstændiggørelsen $F(\mathbb{Q})$ af det arkimedisk ordnede legeme $\mathbb{Q}$. *Beviset for (0.18)* opdeles i to skridt:

1* Vi beskriver en ikke-tællelig mængde $\mathcal{E}$.
2* Vi definerer en injektiv adbildning $d : \mathcal{E} \to \mathbb{R}$.

Så er delmængden $d(\mathcal{E})$ af $\mathbb{R}$ ikke tællelig, og derfor er $\mathbb{R}$ heller ikke tællelig ((0.17)(2)).

1* Sæt

$$\mathcal{E} = \left\{ (e_i) \,\middle|\, \begin{array}{l} e_i \in \mathbb{Z},\ 0 \le e_i \le 9 \text{ og for alle} \\ p \in \mathbb{N} \text{ eksisterer et } q \ge p \text{ så, } a_q \ne 9 \end{array} \right\}$$

(Så $\mathcal{E}$ består af følger af hele tal mellem 0 og 9 som *ikke* er konstant lig 9 fra noget trin). Antag, at $\mathcal{E}$ er tællelig. Ifølge (0.9) findes en surjektiv afbildning $\varphi : \mathbb{N} \to \mathcal{E}$. Antag, at

$$\varphi(n) = (e_{n1}, e_{n2}, \dots, e_{nk}, \dots)$$

Vi definerer

$$f_i = \begin{cases} e_{ii} - 1 & \text{hvis } e_{ii} \ne 0 \\ 1 & \text{hvis } e_{ii} = 0. \end{cases}$$

Da $f_i \ne 9$ for alle i er $(f_i) \in \mathcal{E}$. Da φ er surjektiv findes et $\ell \in \mathbb{N}$, så $\varphi(\ell) = (f_i)$, altså

$$(f_1, f_2, \dots, f_n, \dots) = (e_{\ell 1}, e_{\ell 2}, \dots, e_{\ell n}, \dots).$$

Så må $f_\ell = e_{\ell\ell}$, hvilket strider mod definitionen af f_e. Vi har ført antagelsen, at $\mathcal{E}$ er tællelig til en modstrid. Dermed er $\mathcal{E}$ *ikke tællelig.*

2* Vi har brug for den følgende identitet, som let kan bevises (f.eks. ved induktion)

$$\text{For } p \in \mathbb{N} \text{ er } 9 \cdot \sum_{k=1}^{p} 10^{-k} = 1 - 10^{-p} \tag{8}$$

(altså $0.9 = 1 - 10^{-1}, 0.99 = 1 - 10^{-2}$, etc.)

Lad $E = (e_1, e_2, \dots, e_n, \dots) \in \mathcal{E}$. Vi sætter

$$a_i^{(E)} = \sum_{k=1}^{i} e_k 10^{-k} \quad \text{for } i \in \mathbb{N}. \tag{9}$$

Hvis $p, q \in \mathbf{N}$, $p \leq q$ er

$$a_q^{(E)} - a_p^{(E)} = \sum_{k=p+1}^{q} e_k 10^{-k} \leq \sum_{k=p+1}^{q} 9 \cdot 10^{-k} = 10^{-p} - 10^{-q}$$

ifølge (8), altså

$$(10) \qquad \begin{cases} a_q^{(E)} - a_p^{(E)} \leq 10^{-p} - 10^{-q} \text{ for } p \leq q \\ \text{med lighed netop når } e_{p+1} = \cdots = e_q = 9. \end{cases}$$

Specielt er

$$(11) \qquad a_q(E) - a_p(E) < 10^{-p} \text{ for } p \leq q.$$

Det er let at se fra (9), at

$$(12) \qquad \begin{cases} a_p^{(E)} \leq a_q^{(E)} \text{ for } p \leq q \\ \text{med lighed netop når } e_{p+1} = \cdots = e_q = 0. \end{cases}$$

Fra (11) og (12) fås let, at $(a_i^{(E)})$ er en Cauchy-følge (overvej dette!) Vi definerer så

$$d(E) = \widehat{\left(a_i^{(E)}\right)} \in F(\mathbf{Q}) = \mathbf{R}$$

således at d er en afbildning $d : E \to \mathbf{R}$. Man kan forestille sig tallet $d(E)$ som $d(E) = 0.e_1e_2e_3\ldots$, et reelt tal mellem 0 og 1. Hvis f.eks. $E = (1, 0, 2, 4, \ldots)$ "er" $d(E) = 0.1024\ldots$. Men i denne skrivemåde er f.eks.

$$0.1999\cdots = 0.2000\ldots$$

og det er grunden til at vi i $\mathcal{E}$ udelader følger, der er konstant 9 fra et vist trin. Som vi skal se, sikrer denne udeladelse, at d er injektiv.

Lad igen $E = (e_i) \in \mathcal{E}$ og lad $f = d(E)$. Vi bemærker, at

$$(13) \qquad a_p^{(E)} \leq f \leq a_p^{(E)} + 10^{-p} \quad \text{for } p \in \mathbf{N}.$$

(Antagelsen $f < a_p^{(E)}$ giver modstrid til den kendsgerning, at $\lim a_i^{(E)} = f$, idet så $0 < a_p^{(E)} - f \leq a_q^{(E)} - f$ for alle $q \geq p$. At $f \leq a_p^{(E)} + 10^{-p}$ følger fra (11) og (5.51)(3).)

Lad $E = (e_i)$, $\widetilde{E} = (\tilde{e}_i) \in \mathcal{E}$. Antag, at $d(E) = d(\widetilde{E}) = f$ og at $E \neq \widetilde{E}$. Vi søger en modstrid. Da $E \neq \widetilde{E}$, kan vi antage

$$(14) \qquad \begin{cases} e_1 = \tilde{e}_1, \ldots, e_{r-1} = \tilde{e}_{r-1}, e_r > \tilde{e}_r \\ \text{for et } r \in \mathbf{N}. \end{cases}$$

Vi har så

$$\begin{aligned} 10^{-r} &\leq (e_r - \tilde{e}_r)10^{-r} && \text{(ifølge (14))} \\ &= a_r^{(E)} - a_r^{(\tilde{E})} && \text{(definition)} \\ &\leq f - a_r^{(\tilde{E})} \leq 10^{-r} && \text{(ifølge (13))} \end{aligned}$$

således at der må gælde lighed overalt. Specielt er

$$f - a_r^{(\tilde{E})} = 10^{-r}. \tag{15}$$

Vi har nu for $s \geq r$

$$\begin{aligned} 10^{-r} - 10^{-s} &\leq 10^{-r} - (f - a_s^{(\tilde{E})}) && \text{(ifølge (13))} \\ &= (f - a_r^{(\tilde{E})}) - (f - a_s^{(\tilde{E})}) \\ &= a_s^{(\tilde{E})} - a_r^{(\tilde{E})} \leq 10^{-r} - 10^{-s} && \text{(ifølge (10))} \end{aligned}$$

Vi får ifølge (10) at $\tilde{e}_s = 9$ for alle $s > r$, hvilket strider mod at $\widetilde{E} \in \mathcal{E}$. Hermed er vist, at d er injektiv, så beviset for (0.18) er afsluttet.

(5.65) ØVELSE: Vis, at

$$d(\mathcal{E}) = [0,1[= \{f \in \mathbf{R} \mid 0 \leq f < 1\}$$

□

(5.66) ØVELSE: Hvordan ser $E \in \mathcal{E}$ ud når

$$(1) \quad d(E) = \frac{1}{3} \qquad (2) \quad d(E) = \frac{1}{6} \qquad (3) \quad d(E) = \frac{\sqrt{2}}{2}?$$

□

Det ovenstående svarer til *decimalbrøkudviklingen* af reelle tal mellem 0 og 1.

TILLÆG TIL KAP 5

Om talsystemets opbygning

At en grundig og omhyggelig Opbygning af Talbegrebet udfra de naturlige d. v. s. de positive hele Tal gennem de rationale Tal til de reelle Tal og derefter de komplekse Tal maa være et af Hovedemnerne ved Undervisningen til Lærerprøven, ligger i Sagens Natur. Ganske bortset fra Spørgsmaalet om, hvorvidt dette Stof egner sig til Undervisningen i selve Skolerne, turde det være en Selvfølge, at enhver Gymnasielærer under sin Studietid indgaaende maa have beskæftiget sig med de her foreliggende interessante og fængslende Problemer, hvis Udredning jo er et af selve Fundamenterne for Matematikken som et eksakt Fag.

Harald Bohr.

Det er ikke vanskeligt at overføre ovenstående udtalelse af H. Bohr (i forordet til Svend Bundgaards bog: „Tallene og den abstrakte algebras grundbegreber", som desværre har været udsolgt i mange år) til nutidig sprogbrug.

Jeg vil her kort give en sammenfattende beskrivelse af "Talbegrebets Opbygning"

1. Man starter med $\mathbb{N}$. De naturlige tal kan beskrives abstrakt som en mængde, der opfylder de såkaldte „Peano-aksiomer". Den interesserede læser kan hente nærmere detaljer her. (Lånt fra N. Jacobson's fortræffelige bog „Basic Algebra I")

0.4 THE NATURAL NUMBERS

The system of natural numbers, or counting numbers, 0, 1, 2, 3, ... is fundamental in algebra in two respects. In the first place, it serves as a starting point for constructing more elaborate systems: the number systems of integers, of rational numbers and ultimately of real numbers, the ring of residue classes modulo an integer, and so on. In the second place, in studying some algebraic structures, certain maps of the set of natural numbers into the given structure play an important role. For example, in a structure S in which an associative binary composition and a unit are defined, any element $a \in S$ defines a map $n \to a^n$ where $a^0 = 1$, $a^1 = a$, and $a^k = a^{k-1}a$. Such maps are useful in studying the structure S.

A convenient and traditional starting point for studying the system $\mathbb{N}$ of natural numbers is an axiomatization of this system due to Peano. From this point of view we begin with a non-vacuous set $\mathbb{N}$, a particular element of $\mathbb{N}$, designated as 0, and a map $a \to a^+$ of $\mathbb{N}$ into itself, called the *successor* map. Peano's axioms are:

1. $0 \neq a^+$ for any a (that is, 0 is not in the image of $\mathbb{N}$ under $a \to a^+$).
2. $a \to a^+$ is injective.
3. (Axiom of induction.) Any subset of $\mathbb{N}$ which contains 0 and contains the successor of every element in the given subset coincides with $\mathbb{N}$.

Axiom 3 is the basis of proofs by the *first principle of induction*. This can be stated as follows. Suppose that for each natural number n we have associated a statement $E(n)$ (e.g., $0 + 1 + 2 + \cdots + n = n(n+1)/2$). Suppose $E(0)$ is true and $E(r)$ is true *whenever* $E(r)$ is true. (The second part is called the inductive step.) Then $E(n)$ is true for all $n \in \mathbb{N}$. This follows directly from axiom 3. Let S be the subset of $\mathbb{N}$ of s for which $E(s)$ is true. Then $0 \in S$ and if $r \in S$, then so does r^+. Hence, by axiom 3, $S = \mathbb{N}$, so $E(n)$ holds for all natural numbers.

Proofs by induction are very common in mathematics and are undoubtedly familiar to the reader. One also encounters quite frequently—without being conscious of it—definitions by induction. An example is the definition mentioned above of a^n by $a^0 = 1$, $a^{n+1} = a^n a$. Definition by induction is not as trivial as it may appear at first glance. This can be made precise by the following

RECURSION THEOREM. *Let S be a set, φ a map of S into itself, a an element of S. Then there exists one and only one map f from $\mathbb{N}$ to S such that*

$$1.\ f(0) = a, \qquad 2.\ f(n^*) = \varphi(f(n)),\ n \in \mathbb{N}.^6$$

Proof. Consider the product set $\mathbb{N} \times S$. Let Γ be the set of subsets U of $\mathbb{N} \times S$ having the following two properties: (i) $(0, a) \in U$, (ii) if $(n, b) \in U$ then $(n^*, \varphi(b)) \in U$. Since $\mathbb{N} \times S$ has these properties it is clear that $\Gamma \neq \varnothing$. Let I be the intersection of all the subsets U contained in Γ. We proceed to show that f is the desired function from $\mathbb{N}$ to S. In the first place, it follows by induction that if $n \in \mathbb{N}$, there exists a $b \in S$ such that $(n, b) \in I$. To prove that I is a map of $\mathbb{N}$ to S it remains to show that if (n, b) and $(n, b') \in I$ then $b = b'$. This is equivalent to showing that the subset T of $n \in \mathbb{N}$ such that (n, b) and $(n, b') \in I$ imply $b = b'$ is all of $\mathbb{N}$. We prove this by induction. First, $0 \in T$. Otherwise, we have $(0, a)$ and $(0, a') \in I$ but $a \neq a'$. Then let I' be the subset of I obtained by deleting the element $(0, a')$ from I. Then it is immediate that I' satisfies the defining conditions (i) and (ii) for the sets $U \in \Gamma$. Hence $I' \supseteq I$. But $I' \subsetneq I$ since I' was obtained by dropping $(0, a')$ from I. This contradiction proves that $0 \in T$. Now suppose we have a natural number r such that $r \in T$ but $r^* \notin T$. Let $(r, b) \in I$. Then $(r^*, \varphi(b)) \in I$ and since $r^* \notin T$, we have a $c \neq \varphi(b)$ such that $(r^*, c) \in I$. Now consider the subset I'' of I obtained by deleting (r^*, c). Since $r^* \neq 0$ and I contains $(0, a)$, I'' contains $(0, a)$. The same argument shows that if $n \in \mathbb{N}$ and $n \neq r$ and $(n, d) \in I''$ then $(n^*, \varphi(d)) \in I''$. Now suppose $(r, b') \in I''$ then $b' = b$ and $(r^*, \varphi(b)) \in I''$ since $(r^*, \varphi(b))$ was not deleted in forming I'' from I. Thus we see that $I'' \in \Gamma$ and this again leads to the contradiction: $I'' \supseteq I$, $I'' \subsetneq I$ We have therefore proved that if $r \in T$ then $r^* \in T$. Hence $T = \mathbb{N}$ by induction, and so we have proved the existence of a function f satisfying the given conditions. To prove uniqueness, let g be any map satisfying the conditions. Then $g \in \Gamma$ so $g \supseteq I$. But $g \supseteq I$ for two maps I and g implies $I = g$, by the definition of a map. Hence I is unique.

Addition and multiplication of natural numbers can be defined by the recursion theorem. Addition of m to n can be defined by taking $a = m$ and φ to be the successor map $n \to n^*$. This amounts to the two formulas:

(a) $\qquad 0 + m = m$

(b) $\qquad n^* + m = (n + m)^*$.

For multiplication by m we use $a = 0$ and φ is the map $n \to n + m$. Thus we have

(a) $\qquad 0m = 0$

(b) $\qquad n^* m = nm + m$.

It can be proved that we have the associative, commutative, and cancellation laws of addition and multiplication:[7]

A1	$(x + y) + z = x + (y + z)$	(Associative law)
A2	$x + y = y + x$	(Commutative law)
A3	$x + z = y + z \Rightarrow x = y$	(Cancellation law)
M1	$(xy)z = x(yz)$	
M2	$xy = yx$	
M3	$xz = yz,\ z \neq 0 \Rightarrow x = y$	

We also have the fundamental rule connecting addition and multiplication:

D $\qquad z(x + y) = zx + zy$ (Distributive law)

A fundamental concept for the system $\mathbb{N}$ is the relation of order defined by stating that the natural number a is greater than or equals the natural number b (notation: $a \geq b$ or $b \leq a$) if the equation $a = b + x$ has a solution $x \in \mathbb{N}$. The following are the basic properties of this relation:

O1 $\quad x \geq y$ and $y \geq x \Leftrightarrow x = y$.

O2 $\quad x \geq y$ and $y \geq z \Rightarrow x \geq z$.

O3 $\quad$ For any $(x, y) \in \mathbb{N} \times \mathbb{N}$ either $x \geq y$ or $y \geq x$.

We also have the following *well-ordering property* of the set of natural numbers.

O4 $\quad$ In any non-vacuous subset S of $\mathbb{N}$ there is a least number, that is, an $l \in S$ such that $l \leq s$ for every $s \in S$.

Proof. Let M be the set of natural numbers m such that $m \leq s$ for every $s \in S$. Then $0 \in M$, and if $s \in S$ then $s^* \notin M$. Hence $M \neq \mathbb{N}$ and so, by the axiom of induction, there exists a natural number $l \in M$ such that $l^* \notin M$. Then l is the required number, since $l \leq s$ for every $s \in S$. Moreover, $l \in S$ since otherwise $l < s$ for every $s \in S$ and then $l^* \leq s$ for every $s \in S$. This contradicts $l^* \notin M$.

The well-ordering property is the basis of the following *second principle of induction*. Suppose that for every $n \in \mathbb{N}$ we have a statement $E(n)$. Suppose it can be shown that $E(r)$ is true for a particular r if $E(s)$ is true for all $s < r$. (Note that this implies that it can be shown that $E(0)$ is true.) Then $E(n)$ is true for all n. To prove this we must show that the subset F of $\mathbb{N}$ of r such that $E(r)$ is false is vacuous. Now, if F is not vacuous, then, by O4, F contains a least element t. Then $E(t)$ is false but $E(s)$ is true for every $s < t$. This contradicts the hypothesis and proves $F = \varnothing$.

The main relations governing order and addition and order and multiplication are given in the following statements:

OA $\quad a \geq b \Rightarrow a + c \geq b + c$.

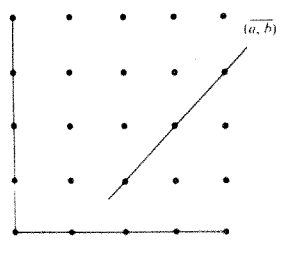
OM $\quad a \geq b \Rightarrow ac \geq bc$.

2. Fra $\mathbb{N}$ opbygges $\mathbb{Z}$. De hele tal betragtes, formelt som „ækvivalensklasser af talpar (a, b), $a, b \in \mathbb{N}$". Den interesserede læser kan heute nærmere detaljer her:

0.5 THE NUMBER SYSTEM $\mathbb{Z}$ OF INTEGERS

Instead of following the usual procedure of constructing this system by adjoining to $\mathbb{N}$ the negatives of the elements of $\mathbb{N}$ we shall obtain the system of integers in a way that seems more natural and intuitive. Moreover, the method we shall give is analogous to the standard one for constructing the number system $\mathbb{Q}$ of rational numbers from the system $\mathbb{Z}$.

Our starting point is the product set $\mathbb{N} \times \mathbb{N}$. In this set we introduce the relation $(a, b) \sim (c, d)$ if $a + d = b + c$. It is easy to verify that this is an equivalence relation. What we have in mind in making this definition is that the equivalence class $\overline{(a, b)}$ determined by (a, b) is to play the role of the difference of a and b. If we represent the pair (a, b) in the usual way as the point with abscissa a and ordinate b, then $\overline{(a, b)}$ is the set of points with natural number coordinates on the line of slope 1 through $\overline{(a, b)}$. We call the equivalence classes $\overline{(a, b)}$ *integers*



and we denote their totality as $\mathbb{Z}$. As a preliminary to defining addition we note that if $(a, b) \sim (a', b')$ and $(c, d) \sim (c', l')$ then

$$(a + c, b + d) \sim (a' + c', b' + d');$$

for the hypotheses are that $a + b' = a' + b$ and $c + d' = c' + d$. Hence $a + c + b' + d' = a' + c' + b + d$, which means that $(a + c, b + d) \sim (a' + c', b' + d')$. It follows that the integer $\overline{(a + c, b + d)}$ is uniquely determined by $\overline{(a, b)}$ and $\overline{(c, d)}$. We define this integer to be the *sum* of the integers $\overline{(a, b)}$ and $\overline{(c, d)}$:

$$\overline{(a, b)} + \overline{(c, d)} = \overline{(a + c, b + d)}.$$

It is easy to verify that the rules A1, A2, and A3 hold. Also we note that $(a, a) \sim (b, b)$ and if we set $0 = \overline{(a, a)}$ (not to be confused with the 0 of $\mathbb{N}$), then

A4 $\qquad 0 + x = x$ for every $x \in \mathbb{Z}$.

Finally, every integer has a negative: If $x = \overline{(a, b)}$, then we denote $\overline{(b, a)}$ (which is independent of the representative (a, b) in $\overline{(a, b)}$) as $-x$. Then we have

A5 $\qquad x + (-x) = 0$.

We note next that if $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, then $a + b' = a' + b$, $c + d' = c' + d$. Hence

$$c(a + b') + d(a' + b) + a'(c + d') + b'(c' + d') = c(a' + b) + d(a + b') + a'(c' + d) + b'(c + d')$$

so that

TC 3

$$ac + b'c + a'd + bd + a'c + a'd' + b'c' + b'd$$
$$= a'c + bc + ad + b'a + a'c' + a'd + b'c + b'd'.$$

The cancellation law gives

$$ac + bd + a'd' + b'c' = bc + ad + a'c' + b'd',$$

which shows that $(ac + bd, ad + bc) \sim (a'c' + b'd', a'd' + b'c')$. Hence, if we define

$$(\overline{a, b})(\overline{c, d}) = (\overline{ac + bd, ad + bc})$$

we obtain a single-valued product. It can be verified that this is associative and commutative and distributive with respect to addition. The cancellation law holds if the factor z to be cancelled is not 0.

We regard $(\overline{a, b}) \geq (\overline{c, d})$ if $a + d \geq b + c$. The relation is well defined (that is, it is independent of the choice of the representatives in the equivalence classes). One can verify easily that O1, O2, O3, and OA hold.

The property OM has to be modified to state:

OM′ If $x \geq y$ and $z \geq 0$ then $xz \geq yz$.

We now consider the set '$\mathbb{N}$' of non-negative integers. By definition, this is the subset of $\mathbb{Z}$ of elements $x \geq 0$, hence, of elements x of the form $(\overline{b + u, b})$. It is immediate that $(b + u, b) \sim (c + u, c)$. Now let u be a natural number (that is, an element of '$\mathbb{N}$') and define $u' = (\overline{b + u, b})$. Our remarks show that $u \to u'$ defines a map of '$\mathbb{N}$' into $\mathbb{Z}$ whose image is '$\mathbb{N}$'. Moreover, if $(b + u, b) \sim (c + v, c)$, then $b + u + c = b + c + v$ so $u = v$. Thus $u \to u'$ is injective. It is left to the reader to verify the following properties:

$$(u + v)' = u' + v'$$

$$(uv)' = u'v'$$

$$u \geq v \Leftrightarrow u' \geq v'.$$

These and the fact that $u \to u'$ is bijective of '$\mathbb{N}$' into '$\mathbb{N}$' imply that these two systems are indistinguishable as far as the basic operations and relation of order are concerned. In view of this situation we can now discard the original system of natural numbers and replace it by the set of non-negative integers, a subset of $\mathbb{Z}$. Also we can appropriate the notations originally used for '$\mathbb{N}$' for this subset of $\mathbb{Z}$. Hence from now on we denote the latter as '$\mathbb{N}$' and its elements as $0, 1, 2, \ldots$. It is easily seen that the remaining numbers in $\mathbb{Z}$ can be listed as $-1, -2, \ldots$.

3. Fra $\mathbb{Z}$ opbygges $\mathbb{Q}$ som $\mathbb{Z}$'s brøklegeme, $\mathbb{Q} = Q(\mathbb{Z})$, se (5.7) og (5.8)

4. Fra $\mathbb{Q}$ opbygges $\mathbb{R}$ som $\mathbb{Q}$'s fuldstændiggørelse $\mathbb{R} = F(\mathbb{Q})$, se afsnit 5° i Kap 5.

5. Fra $\mathbb{R}$ opbygges $\mathbb{C}$. Dette kan gøres på flere måder F.eks er $\mathbb{C}$ spaltningslegemet for polynomiet t^2+1 over $\mathbb{R}$, se (5.16) $\left\{\begin{pmatrix} x & -y \\ y & x \end{pmatrix} \middle| x, y \in \mathbb{R}\right\}$

6. Fra $\mathbb{C}$ opbygges $\mathbb{H}$. Men det er en helt anden historie! (En divisionsring (skållegeme) er en ring med 1-element, som opfylder [RM$\overline{1}$], men ikke nødvendigvis [RM$\overline{3}$]). Hvad siger Jacobson?

2.4 QUATERNIONS

In 1843, W. R. Hamilton constructed the first example of a division ring in which the commutative law of multiplication does not hold. This was an extension of the field of complex numbers, whose elements were quadruples of real numbers $(\alpha, \beta, \gamma, \delta)$ for which the usual addition and a multiplication were defined so that $1 = (1, 0, 0, 0)$ is the unit and $i = (0, 1, 0, 0)$, $j = (0, 0, 1, 0)$, and $k = (0, 0, 0, 1)$ satisfy $i^2 = j^2 = k^2 = -1 = ijk$.[3] Hamilton called his quadruples quaternions. Previously he had defined complex numbers as pairs of real numbers (α, β) with the product $(\alpha, \beta)(\gamma, \delta) = (\alpha\gamma - \beta\delta, \alpha\delta + \beta\gamma)$. Hamilton's discovery of quaternions led to a good deal of experimentation with other such "hypercomplex" number systems and eventually to a structure theory whose goal was to classify such systems. A good deal of important algebra thus evolved from the discovery of quaternions.

We shall not follow Hamilton's way of introducing quaternions. Instead we shall define this system as a certain subring of the ring $M_2(\mathbb{C})$ of 2×2 matrices with complex number entries. This will have the advantage of reducing the calculations to a single simple verification.

We consider the subset $\mathbb{H}$ of the ring $M_2(\mathbb{C})$ of complex 2×2 matrices that have the form

[3] It seems to have taken Hamilton ten years to arrive at this multiplication table. In fact, he had spent a good deal of effort trying to construct a field of triples of real numbers (which is not possible) before he realized that it was necessary to go to quadruples and to drop the commutativity of multiplication. Perhaps this bit of history may serve as an encouragement to the student who sometimes finds himself on the wrong track in attacking a problem. (See Carl A. Boyer, *A History of Mathematics*, New York, Wiley, 1968, p. 625.

TC 4

(14) $$x = \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = \begin{pmatrix} \alpha_0 + \alpha_1\sqrt{-1} & \alpha_2 + \alpha_3\sqrt{-1} \\ -\alpha_2 + \alpha_3\sqrt{-1} & \alpha_0 - \alpha_1\sqrt{-1} \end{pmatrix}, \quad \alpha_i \text{ real.}$$

We claim that $\mathfrak{H}$ is a subring of $\mathfrak{C}_2$. Since $\overline{a_1 - a_2} = \bar{a}_1 - \bar{a}_2$ for complex numbers it is clear that $\mathfrak{H}$ is closed under subtraction; hence $\mathfrak{H}$ is a subgroup of the additive group of $M_2(\mathbb{C})$. We obtain the unit matrix by taking $a = 1, b = 0$ in (14). Hence $1 \in \mathfrak{H}$. Since

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix}\begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix} = \begin{pmatrix} ac - b\bar{d} & ad + b\bar{c} \\ -\bar{b}c - \bar{a}\bar{d} & -\bar{b}d + \bar{a}\bar{c} \end{pmatrix}$$

and $\overline{a_1 a_2} = \bar{a}_1\bar{a}_2$, the right-hand side has the form

$$\begin{pmatrix} u & v \\ -\bar{v} & \bar{u} \end{pmatrix}$$

where $u = ac - b\bar{d}$, $v = ad + b\bar{c}$. Hence $\mathfrak{H}$ is closed under multiplication and so $\mathfrak{H}$ is a subring of $M_2(\mathbb{C})$.

We shall now show that $\mathfrak{H}$ is a division ring. We note first that

$$\Delta \equiv \det \begin{pmatrix} \alpha_0 + \alpha_1\sqrt{-1} & \alpha_2 + \alpha_3\sqrt{-1} \\ -\alpha_2 + \alpha_3\sqrt{-1} & \alpha_0 - \alpha_1\sqrt{-1} \end{pmatrix} = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2.$$

Since the α_i are real numbers this is real, and is 0 only if every $\alpha_i = 0$, that is, if the matrix is 0. Hence every non-zero element of $\mathfrak{H}$ has an inverse in $\mathfrak{C}_2$. Moreover, we have, by the definition of the adjoint given in section 2.3, that

$$\operatorname{adj}\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = \begin{pmatrix} \bar{a} & -b \\ \bar{b} & a \end{pmatrix}.$$

Since $\bar{\bar{a}} = a$ this is obtained from the x in (14) by replacing a by $\bar{a}$ and b by $-b$, and so it is contained in $\mathfrak{H}$. Thus if the matrix x is $\neq 0$ then its inverse is

$$\begin{pmatrix} \bar{a}\Delta^{-1} & -b\Delta^{-1} \\ \bar{b}\Delta^{-1} & a\Delta^{-1} \end{pmatrix}$$

and this is contained in $\mathfrak{H}$. Hence $\mathfrak{H}$ is a division ring.

The ring $\mathfrak{H}$ contains in its center the field $\mathbb{R}$ of real numbers identified with the set of diagonal matrices $\operatorname{diag}(\alpha, \alpha)$, $\alpha \in \mathbb{R}$. $\mathfrak{H}$ also contains the matrices

$$i = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \quad j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}.$$

We verify that

(15) $$x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$$

and if $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k$, $\beta_i \in \mathbb{R}$, then

$$\begin{pmatrix} \alpha_0 + \alpha_1\sqrt{-1} & \alpha_2 + \alpha_3\sqrt{-1} \\ -\alpha_2 + \alpha_3\sqrt{-1} & \alpha_0 - \alpha_1\sqrt{-1} \end{pmatrix} = \begin{pmatrix} \beta_0 + \beta_1\sqrt{-1} & \beta_2 + \beta_3\sqrt{-1} \\ -\beta_2 + \beta_3\sqrt{-1} & \beta_0 - \beta_1\sqrt{-1} \end{pmatrix}$$

so $\alpha_i = \beta_i$, $0 \le i \le 3$. Thus any x in $\mathfrak{H}$ can be written in one and only one way in the form (15). The product of two elements in $\mathfrak{H}$

$$(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)(\beta_0 + \beta_1 i + \beta_2 j + \beta_3 k)$$

is determined by the product and sum in $\mathbb{R}$, the distributive laws and the multiplication table

(16) $$i^2 = j^2 = k^2 = -1$$
$$ij = -ji = k, \; jk = -kj = i, \; ki = -ik = j.$$

Incidentally, because these show that $\mathfrak{H}$ is not commutative we have constructed a division ring that is not a field. The ring $\mathfrak{H}$ is called the *division ring of real quaternions.*

7. Fra $\mathfrak{H}$ opbygges ? ? er „octonionerne" = „Cayley-algebraen", som ikke er nogen ring, idet [RMA] ikke er oppfyldt!

8. Fra ? opbygges ??

„The rest is silence" (W. Shakespeare).

Kapitel 6. Gruppeteori. Indledning.

En gruppe er en mængde med en komposition der opfylder tre bestemte aksiomer. Den er dermed en enklere algebraisk struktur end ringe og legemer, hvor der er to kompositioner og flere aksiomer. Alligevel har gruppeteorien vist sig at være særdeles frugtbar både i forskningen og i anvendelserne. I begyndelsen betragtede man kun grupper bestående af permutationer (= bijektive afbildninger af en mængde på sig selv) på mængden af rødder i et polynomium. Dette viste sig at være af interesse under forsøget på at finde generelle løsningsmetoder til ligninger af grad ≥ 3.

Den bedst forståelige begrundelse for at en sådan generel løsningsmetode ikke findes for ligninger af grad ≥ 5 blev givet ved at koble teorien for ligninger sammen med teorien for grupper. (Det drejer sig om den såkaldte "Galois teori", som vi *desværre* af tidsgrunde ikke vil kunne beskæftige os med her).

Lad G være en mængde med en komposition $\cdot$, $G \times G \to G$, $(a,b) \to a \cdot b = ab$. Vi betragter følgende aksiomer: Lad $a,b,c \in G$ være vilkårlige

[GA] $a(bc) = (ab)c$ ($\cdot$ opfylder [KE]).
[GN] Der findes et $1 \in G$ så $1a = a1 = a$ ($\cdot$ opfylder [KE]) (1 kaldes det *neutrale element*).
[GI] Der findes et element, kaldet a^{-1}, så $aa^{-1} = a^{-1}a = 1$.
[GK] $ab = ba$ ($\cdot$ opfylder [KK]).

Hvis $(G,\cdot)$ opfylder [GA], [GN] og [GI] kaldes G en *gruppe*. Hvis også [GK] er opfyldt kaldes gruppen *abelsk* (eller *kommutativ.*)

På samme måde som i [RAN] og i [RMI] er det "inverse" element til a *entydigt* bestemt: Hvis $ab = ba = 1$, $ac = ca = 1$ så er $b = c$ idet $\underline{b} = b1 = b(ac) = (ba)c = 1c = \underline{c}$. Så der findes i [GI] netop ét inverst element a^{-1}. Dette viser også, at når $a,b \in G$ gælder $(a^{-1})^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$.

I øvrigt viser [RAK]–[RAI] at når R er en ring, så er $(R,+)$ en abelsk gruppe. På samme måde er $(R \setminus \{0\},\cdot)$ en abelsk gruppe, når R er et legeme, ifølge [RMK], [RMA], [RMN] og [RMI].

(6.1) EKSEMPLER PÅ GRUPPER:

(1) Lad M være en mængde. Vi lader $S(M)$ være mængden af permutationer af M, altså mængden af bijektive afbildninger $f : M \to M$. Sammensætning af funktioner giver en komposition $\circ$ på $S(M)$:

For $f,g \in S(M)$ er $f \circ g \in S(M)$ defineret ved

$$(f \circ g)(m) = f(g(m)) \quad \text{for alle } m \in M.$$

Så er $(S(M),\circ)$ en gruppe. Det neutrale element 1 er den identiske afbildning $1(m) = m$ og det inverse element til f er den sædvanlige inverse afbildning f^{-1} til f, (Kapitel 0). Når M har mindst 3 elementer er $S(M)$ ikke abelsk: Lad $a,b,c \in M$ være forskellige. Sæt $f(a) = b$, $f(b) = a$, $f(m) = m$ for $m \neq a,b$ og $g(b) = c$, $g(c) = b$,

$g(m) = m$ for $m \neq b, c$. Så er $(f \circ g)(a) = f(g(a)) = f(a) = b$, men $(g \circ f)(a) = g(f(a)) = g(b) = c$, så $f \circ g \neq g \circ f$. Det er imidlertid klart at $f, g \in S(M)$. Når $M = \{1, 2, \ldots, n\}$, $n \in \mathbb{N}$, skriver vi S_n i stedet for $S(M)$. S_n kaldes *den symmetriske gruppe (af grad n)*, og når M er vilkårlig kaldes $S(M)$ den *symmetriske gruppe på M*.

(2) Hvis L er et legeme og $n \in \mathbb{N}$, er L_n^n mængden af $n \times n$ matricer $A = (a_{ij})$, hvor $a_{ij} \in L$. Vi sætter

$$GL(n, L) = \{A \in L_n^n \mid \text{Det } A \neq 0\}.$$

Så $GL(n, L)$ er mængden af invertible matricer i L_n^n. Hvis $A, B \in GL(n, L)$ er også $AB \in GL(n, L)$ idet $\text{Det}(AB) = (\text{Det } A)(\text{Det } B) \neq 0$, når $\text{Det } A \neq 0$, $\text{Det } B \neq 0$. (Anvend [NU] i L). Derfor danner $GL(n, L)$ med den sædvanlige matrixmultiplikation en gruppe kaldet den *generelle lineære gruppe (af grad n over L)*.

(3) Lad $p \in \mathbb{N}$ være en primtal. Sæt

$$\mathbb{Z}(p^\infty) = \{a \in \mathbb{C} \setminus \{0\} \mid \text{Der findes et } n \in \mathbb{N}, \text{ så } a^{p^n} = 1\}$$

Det er let at se (næste øvelse), at produktet (i $\mathbb{C}$) af 2 elementer i $\mathbb{Z}(p^\infty)$ igen er i $\mathbb{Z}(p^\infty)$ og at når $a \in \mathbb{Z}(p^\infty)$ så er $a^{-1} \in \mathbb{Z}(p^\infty)$. Derfor er $\mathbb{Z}(p^\infty)$ en gruppe (en undergruppe af $(\mathbb{C} \setminus \{0\}, \cdot)$, se senere). $\mathbb{Z}(p^\infty)$ er abelsk. □

(6.2) ØVELSE: Vis, at når $a, b \in \mathbb{Z}(p^\infty)$ så er $ab^{-1} \in \mathbb{Z}(p^\infty)$. (Se (6.6)). □

(6.3) ØVELSE: Hvilke af grupperne $GL(n, L)$, $n \in \mathbb{N}$, L legeme, er abelske? □

(6.4) ØVELSE: Lad L være et legeme. Sæt

$$H(L) = \{(a, b) \mid a, b \in L, a \neq 0\}.$$

Vi definerer en komposition på $H(L)$ ved

$$(a, b)(c, d) = (ac, ad + b).$$

Vis, at $H(L)$ er en gruppe med denne komposition. (Selvfølgelig skal ac, $ad + b$ opfattes som elementer i L). □

(6.5) DEFINITION: Lad G være en gruppe, $H \neq \emptyset$ en delmængde af G. Hvis der gælder

(1) For alle $a, b \in H$ er $ab \in H$ (H er lukket).
(2) For alle $a \in H$ er $a^{-1} \in H$

kaldes H en *undergruppe* af G. Hvis der yderligere gælder

(3) For alle $a \in H$, $g \in G$ er $gag^{-1} \in H$

kaldes undergruppen H *normal* (eller *invariant*) i G. Normale undergrupper spiller i grupper den samme rolle som idealer i ringe (mht. faktorstruktur). Vi skriver $H \triangleleft G$, hvis H er en normal undergruppe i G. □

(6.6) SÆTNING. *Lad $H \neq \emptyset$ være en delmængde af gruppen G. Der gælder*

$$H \text{ er en undergruppe af } G \Leftrightarrow \text{ For alle } a, b \in H \text{ er } ab^{-1} \in H.$$

BEVIS: Antag, at H er en undergruppe og at $a, b \in H$. Ifølge (6.5)(2) er $b^{-1} \in H$ og derfor $ab^{-1} \in H$ ifølge (6.5)(1). Omvendt, antag, at der gælder $ab^{-1} \in H$ for alle $a, b \in H$. Vælg $a \in H$. Så er $1 = aa^{-1} \in H$, altså $1 \in H$. Derfor er også $a^{-1} = 1a^{-1} \in H$. Hermed er (6.5)(2) opfyldt. Når $a, b \in H$ er $b^{-1} \in H$ ifølge (6.5)(2) og derfor er $a(b^{-1})^{-1} \in H$. Men $(b^{-1})^{-1} = b$ så $ab \in H$. Hermed er også (6.5)(1) bevist. □

(6.7) ØVELSE: Lad $K \neq \{0\}$, $K \neq \emptyset$, være en delmængde af legemet L. Gør rede for, at K er et dellegeme af L netop da når der gælder

(1) For alle $a, b \in K$ er $a - b \in K$.
(2) For alle $a, b \in K$, $b \neq 0$ er $ab^{-1} \in K$.

□

(6.8) ØVELSE: Undersøg om følgende delmængder af $H(L)$ (fra (6.4)) er undergrupper (hhv. normale undergrupper)

$$B = \{(1, b) \mid b \in L\}$$
$$A = \{(a, 0) \mid a \in L, a \neq 0\}.$$

□

(6.9) DEFINITIONER: Lad A og B være (ikke tomme) delmængder af gruppen G. Sæt

$$AB = \{ab \mid a \in A, b \in B\}$$

som igen er en delmængde af G. AB kaldes *produktet* af A og B. Hvis $A = \{a\}$ kun har et element skrives aB i stedet for $\{a\}B$ og analogt skrives Ab i stedet for $A\{b\}$. Hvis H er en undergruppe i G kaldes delmængderne aH, $a \in G$, for H's *venstresideklasser* og delmængderne Ha, $a \in G$ for H's *højresideklasser* (i G). □

(6.10) DEFINITION: Lad $a \in G$, G gruppe. Vi definerer afbildninger V_a, $H_a : G \to G$ ved

$$V_a(x) = ax, \quad H_a(x) = xa.$$

□

(6.11) SÆTNING. *V_a og H_a er bijektive afbildninger $G \to G$, når $a \in G$, G gruppe. Specielt inducerer V_a (hhv. H_a) bijektive afbildninger mellem A og aA (hhv. mellem A og Aa), når A er en vilkårlig delmængde af G. Så $|A| = |aA| = |Aa|$.*

BEVIS: Vi nøjes med at betragte V_a:

V_a er injektiv: $V_a(x) = V_a(y) \Rightarrow ax = ay \Rightarrow a^{-1}(ax) = a^{-1}(ay) \Rightarrow x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}(ay) = (a^{-1}a)y = 1y = y$, altså $x = y$.
V_a er surjektiv: Lad $y \in G$. Så er $V_a(a^{-1}y) = a(a^{-1}y) = (aa^{-1})y = y$, så $a^{-1}y$ er et urbillede for y under V_a.

Det er klart, at V_a afbilder et element i A ind i aA. Dette viser, at V_a afbilder A bijektivt på aA. □

(6.12) ØVELSE: $\circ$ betegner den sædvanlige sammensætning af afbildninger. Lad G være en gruppe, $a, b \in G$. Undersøg om der gælder

(1) $V_a \circ V_b = V_{ab}$, (2) $H_a \circ H_b = H_{ab}$
(3) $V_a \circ H_b = H_b \circ V_a$.

□

(6.13) SÆTNING. *Lad H være en undergruppe af gruppen G. Betragt relationerne v_H og h_H på G defineret ved*

$$a v_H b \Leftrightarrow a^{-1}b \in H$$
$$a h_H b \Leftrightarrow ab^{-1} \in H.$$

Så er v_H (hhv. h_H) en ækvivalensrelation på G og ækvivalensklasserne for v_H (hhv. h_H) er H's venstresideklasser (hhv. højresideklasser) i G.

BEVIS: Vi betragter v_H:

[BRR] $a\ v_H a$ da $a^{-1}a = 1 \in H$.
[BRS] $a\ v_H b \Rightarrow a^{-1}b \in H \Rightarrow b^{-1}a = (a^{-1}b)^{-1} \in H$. Det betyder $b\ v_H a$.
[BRT] $(a\ v_H b)$ og $(b\ v_H c) \Rightarrow a^{-1}b \in H$ og $b^{-1}c \in H \Rightarrow (a^{-1}b)(b^{-1}c) = (a^{-1}(bb^{-1}))c = (a^{-1}1)c = a^{-1}c \in H \Rightarrow a\ v_H c$.

(I beviset for [BRS] benyttes (6.5)(2) og i beviset for [BRT] (6.5)(1)). Lad os betragte a's v_H-ækvivalensklasse, $a \in G$. $\widehat{a} = \{b \mid a\ v_H b\} = \{b \mid a^{-1}b \in H\} = \{b \mid a(a^{-1}b) \in aH\} = \{b \mid (aa^{-1})b \in aH\} = aH$. □

(6.14) ØVELSE: Lad H være en undergruppe af G. Gør rede for, at H netop da er *normal* i G ($H \triangleleft G$), når $aH = Ha$ for alle $a \in G$ (altså netop da når ækvivalensrelationerne v_H og h_H i (6.13) er ens.) □

(6.15) DEFINITION: Hvis G er en gruppe kaldes antallet af elementer i G for G's *orden* og betegnes med $|G|$. Hvis H er en undergruppe i G lader vi $|G : H|$ betegne

antallet af forskellige venstresideklasser af H i G. $|G:H|$ kaldes *index af H i G*. $|G:H|$ er også antallet af højresideklasser af H i G, (se (6.16)). Hvis $|G| < \infty$ kaldes G *endelig*. □

(6.16) ØVELSE: Lad H være en undergruppe i G, $a \in G$. Vis

(1) For alle $x \in G$ gælder $x \in aH \Leftrightarrow x^{-1} \in Ha^{-1}$
(2) Afbildningen $aH \to Ha^{-1}$ er en (veldefineret) bijektion mellem mængden af venstresideklasser og mængden af højresideklasser til H i G.

□

(6.17) SÆTNING. (Lagrange) *Lad H være en undergruppe af den endelige gruppe G. Der gælder*

$$|G| = |G:H||H|.$$

Specielt gælder $|H| \mid |G|$.

BEVIS: Betragt v_H-ækvivalensklasserne i G, altså venstresideklasserne af H i G. Der er $|G:H|$ sådanne ækvivalensklasser. Ifølge (6.11) har enhver ækvivalensklasse aH netop $|H|$ elementer. Da ethvert element i G er i netop én ækvivalensklasse, er $|G|$ = (antal ækvivalensklasser) (antal elementer i en ækvivalensklasse) $= |G:H||H|$. □

(6.18) DEFINITION: Lad $a \in G$, G gruppe. For $n \in \mathbb{N}$ definerer vi ved induktion $a^n = aa^{n-1}$, $a^0 = 1$. For $n \in -\mathbb{N}$ sættes $a^n = (a^{-n})^{-1}$. Hermed er a^n defineret for alle $n \in \mathbb{Z}$. Det er ikke svært at se, at der gælder

$$a^{n+m} = a^n a^m \quad \text{og} \quad a^{mn} = (a^m)^n, \quad \text{for alle } m, n \in \mathbb{Z}$$

og $\{a^n \mid n \in \mathbb{Z}\}$ danner en undergruppe, kaldet $\langle a \rangle$, af G (den af a *frembragte* undergruppe). Elementerne a^n, $n \in \mathbb{Z}$, kaldes *potenserne* af a. Ordenen $|\langle a \rangle|$ af undergruppen $\langle a \rangle$ kaldes *ordenen af a* og betegnes $|a|$. □

Ordenen af a kan også beskrives på følgende måde:

(6.19) SÆTNING. *Lad $a \in G$, G gruppe. Netop én af følgende 2 muligheder optræder:*

(1) *Elementerne a^n, $n \in \mathbb{Z}$, er alle forskellige og $|a| = \infty$. Vi har $a^m \neq 1$ for alle $m \neq 0$.*
(2) *Der findes et $m \neq 0$, så $a^m = 1$. Så er $|a| = t$, hvor t er det mindste naturlige tal med $a^t = 1$.*

BEVIS: (1) Det er klart at $|a| = \infty$, når a's potenser er forskellige. (2) Antag, at $a^n = a^{n'}$, hvor $n, n' \in \mathbb{Z}$, $n > n'$. Så er $a^{n-n'} = a^n a^{-n'} = a^n (a^{n'})^{-1} = 1$, og $n - n' \in \mathbb{N}$. Ifølge [MIN] findes et $t \in \mathbb{N}$ således at $a^t = 1$, men $a^r \neq 1$ for $1 \leq r < t$. Hvis $n \in \mathbb{Z}$ kan vi skrive $n = mt + r$, hvor $m \in \mathbb{Z}$ og $0 \leq r \leq t-1$. Så er $a^n = a^{mt+r} =$

$a^{mt}a^r = (a^t)^m a^r = 1^m a^r = a^r$, altså $a^n = a^r$. Derfor er $\langle a\rangle = \{1, a, a^2, \ldots, a^{t-1}\}$. Da $1, a, a^2, \ldots, a^{t-1}$ alle er forskellige (hvorfor?) er $|a| = |\langle a\rangle| = t$. □

(6.20) SÆTNING. *Hvis G er en endelig gruppe, $a \in G$ gælder $|a| \mid |G|$.*

BEVIS: Da der kun er endelig mange elementer i G kan (6.19)(1) *ikke* optræde for a. Derfor er (6.20) et specielt tilfælde af (6.17). □

(6.21) BEMÆRKNING: Fra beviset af (6.19) ses også:
Lad $a \in G$ have endelig orden. For $m \in \mathbb{Z}$ gælder

$$a^m = 1 \Leftrightarrow |a| \mid m.$$

□

(6.22) SÆTNING. *Lad G være endelig, $a \in G$. Der gælder*

$$a^{|G|} = 1.$$

BEVIS: Ifølge (6.20) er $|a| \mid |G|$. Derfor fås det ønskede fra (6.21). □

(6.23) ØVELSE: Lad $H \neq \emptyset$ være en delmængde af den *endelige* gruppe G. Vis

$$H \text{ er en undergruppe af } G \Leftrightarrow \text{For alle } a, b \in H \text{ er } ab \in H.$$

Hvad kan man slutte af eksemplet $\mathbb{N} = H \subseteq G = \mathbb{Z}$? □

(6.24) SÆTNING. *Lad $a \in G$, G gruppe, $|a| = t < \infty$.*
(1) *Hvis $t = rs$, $r, s \in \mathbb{N}$ gælder $|a^r| = s$.*
(2) *Hvis $m \in \mathbb{Z}$ er vilkårlig, gælder $\langle a^m\rangle = \langle a^{(m,t)}\rangle$.*
(3) *Hvis $m \in \mathbb{Z}$ er vilkårlig, gælder $|a^m| = t/(m,t)$.*

BEVIS: (Som i §2 er (m,t) s.f.d.) (1) Lad $|a^r| = s'$. Da $(a^r)^s = a^{rs} = a^t = 1$ er $s' | s$ ifølge (6.21). På den anden side er $a^{rs'} = (a^r)^{s'} = 1$ da $|a^r| = s'$. Ifølge (6.21) fås $t = rs | rs'$, altså $s | s'$. Dermed er $s = s'$. (2) Da $(m,t) | m$ er a^m en potens af $a^{(m,t)}$. Derfor er enhver potens af a^m en potens af $a^{(m,t)}$, altså $\langle a^m\rangle \subseteq \langle a^{(m,t)}\rangle$. Ifølge Bézouts sætning (2.24) findes $k, \ell \in \mathbb{Z}$, så $(m,t) = km + \ell t$. Så er $(a^m)^k = a^{(m,t)}$ idet $(a^m)^k = a^{mk} = a^{mk} \cdot 1^\ell = a^{mk}(a^t)^\ell = a^{km+\ell t} = a^{(m,t)}$. Derfor er $a^{(m,t)}$ en potens af a^m, altså $\langle a^{(m,t)}\rangle \subseteq \langle a^m\rangle$. (3) Ifølge (2) er $|a^m| = |a^{(m,t)}|$, og ifølge (1) er $|a^{(m,t)}| = t/(m,t)$. □

(6.25) BEMÆRKNING: (Frobenius) Lad $a \in G$ have orden $|a| = mn$ hvor $(m,n) = 1$, $m, n \in \mathbb{N}$. Skriv (Bézout) $1 = km + \ell n$, $k, \ell \in \mathbb{Z}$. Sæt $x = a^{\ell n}$, $y = a^{km}$. Så er (se (6.24))

$$(*) \qquad a = xy, \qquad xy = yx, \qquad |x| = m, \quad |y| = n.$$

Antag omvendt, at $x, y \in G$ opfylder $(*)$. Så er

$$\begin{aligned} x = x^{\ell n + km} &= x^{\ell n} 1 && (\text{da } |x| = m) \\ &= x^{\ell n} y^{\ell n} && (\text{da } |y| = n) \\ &= (xy)^{\ell n} && (\text{da } xy = yx) \\ &= a^{\ell n}, \end{aligned}$$

altså $x = a^{\ell n}$. Analogt ses $y = a^{km}$. Så faktoriseringen $(*)$ af a er *entydig*. □

Beviserne for (6.24)–(6.25) er vores første eksempler på den nøje sammenhæng mellem visse sætninger i den elementære talteori og i den elementære gruppeteori. Kernen i det ovenstående er jo anvendelsen af Bézouts sætning! På den anden side kan Bézouts sætning udledes fra (6.24)(2). Vi giver med det samme et gruppeteoretisk bevis for en talteoretisk sætning:

(6.26) SÆTNING (Fermat). *Lad p være et primtal i $\mathbb{N}$, $a \in \mathbb{Z}$ og $(a, p) = 1$ (altså a er ikke delelig med p). Så gælder*

$$a^{p-1} \equiv_p 1.$$

BEVIS: Vi har tidligere set at $\mathbb{Z}_p$ er et legeme (med den sædvanlige addition og multiplikation af restklasser). Derfor er $(\mathbb{Z}_p \setminus \{\widehat{0}\}, \cdot)$ en gruppe. Da $(a, p) = 1$ er $\widehat{a} \neq \widehat{0}$, altså $\widehat{a} \in \mathbb{Z}_p \setminus \{\widehat{0}\}$. Da $|\mathbb{Z}_p \setminus \{\widehat{0}\}| = p - 1$ fås ifølge (6.22), at $\widehat{a}^{p-1} = \widehat{1}$. Dette betyder, at $a^{p-1} \equiv_p 1$, som ønsket. (Eksempel: $3^4 = 81 \equiv_5 1$.) □

(6.27) DEFINITION: En gruppe G kaldes *cyklisk*, hvis der findes et $a \in G$, så $\langle a \rangle = G$. □

(6.28) SÆTNING. (1) *Enhver undergruppe af en cyklisk gruppe er cyklisk.*

(2) *Hvis G er cyklisk, $|G| = m < \infty$ og $n|m$, har G netop én undergruppe af orden n.*

BEVIS: (1) Lad H være en undergruppe af $G = \langle a \rangle$. Hvis $H = \{1\}$ er $H = \langle 1 \rangle$ cyklisk. Antag $H \neq \{1\}$ og lad $b \in H, b \neq 1$. Da $b \in G$ er $b = a^n$ for et $n \in \mathbb{Z}$, $n \neq 0$. Så er $b^{-1} = a^{-n} \in H$, og derfor er $T = \{s \in \mathbb{N} \mid a^s \in H\} \neq \emptyset$. Lad ifølge [MIN], $t \in T$, $t \leq s$ for alle $s \in T$. Så er $\langle a^t \rangle \subseteq H$. Lad $b = a^n \in H$ være vilkårlig. Skriv $n = mt + r$, $0 \leq r < t$. Så er $a^r = a^n \cdot (a^{mt})^{-1} \in H$, da $a^n \in H$ og $a^t \in H$. Hvis $r \neq 0$, er $r \in T$, en modstrid til definitionen af t. Derfor er $r = 0$ og $b = a^n = a^{mt}$, altså $b \in \langle a^t \rangle$. Dermed er $H \subseteq \langle a^t \rangle$, altså $H = \langle a^t \rangle$.

(2) Det er klart fra (6.24)(1) at G har en undergruppe af orden n, nemlig $U = \langle a^t \rangle$ hvor $nt = m$. Hvis på den anden side $H = \langle a^s \rangle$ er en undergruppe af G af orden n gælder ifølge (6.24)(3)

$$n = |a^s| = m/(m, s) = n \cdot t/(m, s)$$

så $t = (m, s)$. Specielt er $t|s$, så $a^s \in U$. Vi får $H \subseteq U$, altså $H = U$. □

(6.29) ØVELSE: Vis, at en endelig gruppe af primtalsorden er *cyklisk*. □

(6.30) ØVELSE: Lad G være en gruppe, hvor $a^2 = 1$ for alle $a \in G$. Vis, at G er abelsk. (Benyt $(ab)^{-1} = b^{-1}a^{-1}$). □

(6.31) ØVELSE: Lad $H \subseteq K$ være undergrupper af den endelige gruppe G. Vis (ved at anvende (6.17) 3 gange!) at

$$|G : H| = |G : K||K : H|.$$

□

(6.32) DEFINITION: Lad G og H være grupper. En afbildning $\varphi : G \to H$ kaldes en *homomorfi* (gruppehomomorfi), hvis der gælder:

$$\text{For alle } a, b \in G : \varphi(ab) = \varphi(a)\varphi(b).$$

Hvis φ er injektiv (hhv. surjektiv, hhv. bijektiv) kaldes φ en *monomorfi* (hhv. *epimorfi*, hhv. *isomorfi*). Hvis der findes en isomorfi mellem G og H skrives $G \simeq H$. En isomorfi $\varphi : G \to G$ kaldes en *automorfi* af G. □

(6.33) EKSEMPLER: (1) $\varphi, \psi : G \to G$ defineret ved $\varphi(a) = a, \psi(a) = 1$ er homomorfier.

(2) $\varphi : \mathbb{Z} \to \mathbb{Z}$ givet ved $\varphi(a) = 2a$ er en homomorfi fra $(\mathbb{Z}, +)$ til $(\mathbb{Z}, +)$. (Sml. (3.12)(3)!)

(3) $\kappa : \mathbb{R} \to \mathbb{C}$ givet ved $\kappa(t) = e^{it} = \cos t + i \sin t$ er en homomorfi fra $(\mathbb{R}, +)$ til $(\mathbb{C} \setminus \{0\}, \cdot)$.

(4) Lad $n \in \mathbb{N}$ og lad $G = \langle a \rangle$ en cyklisk gruppe af orden n. Så er afbildningen $\widehat{i} \mapsto a^i$ en isomorfi mellem $(\mathbb{Z}_n, +)$ og $(G, \cdot)$, (se (6.41)).

(5) Lad $g \in G$, G gruppe. Definer

$$\iota_g : G \to G \quad \text{ved} \quad \iota_g(a) = gag^{-1} \quad \text{for alle } a \in G.$$

Så er ι_g en automorfi af G (kaldet en *indre* automorfi). Vi har

$$\begin{aligned} \iota_g(a)\iota_g(b) &= (gag^{-1})(gbg^{-1}) = ((ga)(g^{-1}g))bg^{-1} \\ &= (ga)(bg^{-1}) = g(ab)g^{-1} = \iota_g(ab), \end{aligned}$$

så ι_g er en homomorfi. Det er let at se, at $\iota_{g^{-1}}$ er en invers afbildning til ι_g, så $\iota_g : G \to G$ er en bijektion. Generelt gælder for $g, h \in G$, at $\iota_{gh} = \iota_g \circ \iota_h$, idet der for alle $a \in G$ gælder

$$\begin{aligned} (\iota_g \circ \iota_h)(a) &= \iota_g(\iota_h(a)) = \iota_g(hah^{-1}) = g(hah^{-1})g^{-1} \\ &= (gh)a(h^{-1}g^{-1}) = (gh)a(gh)^{-1} = \iota_{gh}(a). \end{aligned}$$

□

(6.34) ØVELSE: (1) Vis, at hvis $\varphi : G \to G$ er en automorfi gælder $|\varphi(a)| = |a|$ for alle $a \in G$.

(2) Vis, at der for alle $a, b \in G$ gælder

$$|a| = |bab^{-1}|.$$

(3) Vis, at der for alle $a, b \in G$ gælder

$$|ab| = |ba|.$$

(Man kan bevise (3) ved hjælp af (2)!) □

(6.35) SÆTNING. *Lad $\varphi : G \to H$ være en (gruppe-)homomorfi. Der gælder:*

$$\textit{For alle } a, b \in G : \varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1}.$$

Specielt gælder (når $a = b$) $\varphi(1) = 1$ og (når $a = 1$) $\varphi(b^{-1}) = \varphi(b)^{-1}$.

BEVIS: Man kan kopiere beviset for (3.13) til at vise $\varphi(ab^{-1})\varphi(b) = \varphi(a)$. Multiplicer denne ligning fra højre med $\varphi(b)^{-1}$. □

(6.36) DEFINITION: Lad $\varphi : G \to H$ være en homomorfi. Vi definerer *kernen af φ* og *billedet af φ* ved

$$\ker\varphi = \{a \in G \mid \varphi(a) = 1\}$$
$$\varphi(G) = \{b \in H \mid \text{Der findes et } a \in G \text{ så } \varphi(a) = b\}.$$

□

(6.37) SÆTNING. *Lad $\varphi : G \to H$ være en homomorfi. Der gælder*

(1) $\ker\varphi$ *er en normal undergruppe i G, altså* $\ker\varphi \triangleleft G$.

(2) $\varphi(G)$ *er en undergruppe i H (men i almindelighed ikke normal).*

(3) Hvis U er en undergruppe i G, så er $\varphi(U)$ undergruppe i H.

BEVIS: (1) Vi nøjes med at vise (6.5)(3) for $H = \ker f$: Hvis $a \in \ker\varphi$, $g \in G$ er $\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g^{-1}) = \varphi(g)\varphi(a)\varphi(g)^{-1} = \varphi(g)1\varphi(g)^{-1} = 1$ (under anvendelse af (6.35)), altså $gag^{-1} \in \ker\varphi$.

(2) Vi viser, at $\varphi(G)$ i almindelighed ikke er normal i H. Der findes en gruppe G med en undergruppe K, således at K ikke er normal i G (f.eks. undergruppen A fra (6.8)). Så er inklusionshomomorfien $\varphi : K \to G$ defineret ved $\varphi(k) = k$ et eksempel af den ønskede type. (3) Led ! □

(6.38) SÆTNING. *Lad N være en* normal *undergruppe i G, $a, b, c, d \in G$. Hvis $av_N c$ og $bv_N d$ er $(ab)v_N(cd)$.*

BEVIS: Lad $a^{-1}c = k \in N$ og $b^{-1}d = \ell \in N$. Da $k \in N$, $b \in G$ er $b^{-1}kb \in N$, da N er normal. Derfor er $(b^{-1}kb)\ell \in N$, da også $\ell \in N$. Men

$$\begin{aligned} b^{-1}kb\ell &= (b^{-1}(a^{-1}c))(b(b^{-1}d)) = (b^{-1}(a^{-1}c))((bb^{-1})d) \\ &= (b^{-1}a^{-1})(cd) = (ab)^{-1}cd. \end{aligned}$$

Dermed er $(ab)v_N(cd)$. □

(6.39) DEFINITION AF FAKTORGRUPPER: Lad $N \triangleleft G$ (en normal undergruppe i G). Lad G/N være mængden af venstresideklasser af N i G. (Ifølge (6.14) er G/N også mængden af højresideklasser af N i G). Så $G/N = \{\widehat{a} \mid a \in G\}$, hvor $\widehat{a} = \{b \in G \mid av_N b\} = aN$. Vi definerer en komposition (multiplikation) på G/N ved

$$\widehat{a}\,\widehat{b} = \widehat{ab}.$$

Ifølge (6.38) er denne multiplikation veldefineret og derfor er det let at se, at $(G/N, \cdot)$ er en gruppe, kaldet *faktorgruppen (af G modulo N)*. □

(6.40) SÆTNING. *Lad $N \triangleleft G$.*
Afbildningen $\widehat{p} : G \to G/N$ defineret ved

$$\widehat{p}(a) = \widehat{a} = aN$$

er en epimorfi og $\ker \widehat{p} = N$.

BEVIS: Helt analog til beviset for (3.22). □

(6.41) SÆTNING. (1. Isomorfisætning for grupper):
Lad $\varphi : G \to H$ være en homomorfi. Afbildningen $\bar{\varphi} : G/\ker\varphi \to \varphi(G)$ defineret ved $\bar{\varphi}(\widehat{a}) = \varphi(a)$ er en isomorfi. Der gælder altså

$$G/\ker\varphi \simeq \varphi(G)\,.$$

BEVIS: Helt analogt til beviset for (3.24). □

(6.42) ØVELSE: Opskriv detaljerede beviser for (6.40) og (6.41). □

Det er almindeligt at bevise 3 isomorfisætninger for grupper (og for de andre algebraiske strukturer). Den 2. og 3. isomorfisætning er imidlertid i det væsentlige specielle tilfælde af den 1. isomorfisætning. Vi går i det følgende kort ind på dette

og overlader til læseren at overveje hvorledes de tilsvarende sætninger formuleres for ringe (og vektorrum, jfr. (3.25)!)

(6.43) SÆTNING. *Lad N og K være undergrupper af G. Der gælder (i notationen fra (6.9)*

$$NK \text{ er en undergruppe af } G \Leftrightarrow NK = KN.$$

Hvis specielt $N \lhd G$, er NK en undergruppe af G.

BEVIS: $\Rightarrow$ Da $K \subseteq NK$, $N \subseteq NK$ (hvorfor?) og NK er en undergruppe fås $KN \subseteq NK$. Lad $a \in NK$. Vi viser $a \in KN$. Da NK er en undergruppe, er $a^{-1} \in NK$. Skriv $a^{-1} = nk$, $n \in N$, $k \in K$. Så er $a = k^{-1}n^{-1} \in KN$, da $k^{-1} \in K$, $n^{-1} \in N$.

$\Leftarrow$ Lad $a = nk$, $b = n_1k_1 \in NK$, $n, n_1 \in N$, $k, k_1 \in K$. Vi viser, at $ab^{-1} \in NK$ og så følger det ønskede fra (6.6). Vi har $ab^{-1} = n\left((kk_1^{-1})n_1^{-1}\right)$. Da $(kk_1^{-1})n_1^{-1} \in KN \subseteq NK$ eksisterer $n_2 \in N$, $k_2 \in K$, så $(kk_1^{-1})n_1^{-1} = n_2k_2$. Så er $ab^{-1} = (nn_2)k_2 \in NK$, som ønsket.

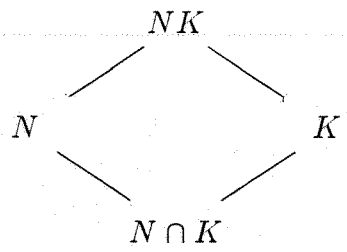
Sætningens sidste udsagn følger fra (6.14). □

(6.44) SÆTNING. (2. isomorfisætning for grupper): *Lad N og K være undergrupper i G, $N \lhd G$. Der gælder*

(1) *N er en normal undergruppe af NK.*

(2) *Afbildningen $\widehat{\widehat{p}} : K \to NK/N$ defineret ved*

$$\widehat{\widehat{p}}(k) = \widehat{k} \ (= kN)$$



er en epimorfi med kerne $K \cap N$.

(3) *$K/K \cap N \cong NK/N$.*

(Lad os igen bemærke, at både N og K er undergrupper af gruppen NK. Det vil sige, at da $k \in K$, er $k \in NK$, og derfor er $\widehat{k} \in NK/N$).

BEVIS: (1) Da N er normal i G og N er indeholdt i NK, er det klart fra definitionen at N er normal i NK.

(2) Afbildningen $\widehat{\widehat{p}}$ i (2) er indskrænkningen af homomorfien $\widehat{p}$ fra (6.40) til K. Så $\widehat{\widehat{p}}$ er en homomorfi. Lad $\widehat{a} = aN \in NK/N$. Skriv $a \in NK$ som $a = nk$, $n \in N$, $k \in K$. Så er $\widehat{a} = \widehat{n}\,\widehat{k} = \widehat{1}\,\widehat{k} = \widehat{k}$, og derfor $\widehat{a} = \widehat{\widehat{p}}(k)$. Dermed er $\widehat{\widehat{p}}$ surjektiv. Lad $k \in K$. Så er $k \in \ker\widehat{\widehat{p}} \Leftrightarrow \widehat{k} = \widehat{1} \Leftrightarrow k \in K \cap N$. Derfor er $\ker\widehat{\widehat{p}} = K \cap N$. Nu følger (3) fra den 1. isomorfisætning. □

(6.45) SÆTNING. *Lad N og K være som i (6.44). Antag at G er endelig. Der gælder*

$$|NK| = |N||K|/|N \cap K|.$$

BEVIS: Det er klart at isomorfe grupper har samme orden, da der jo findes en bijektion mellem mængderne af deres elementer. Ifølge (6.44) er så

$$|K/K \cap N| = |NK/N|.$$

Nu er

$$|K/K \cap N| = |K : K \cap N| = |K|/|K \cap N|$$
$$\text{og } |NK/N| = |NK : N| = |NK|/|N|.$$

(Antallet af elementer i en faktorgruppe er per definition antallet af sideklasser, altså netop et index. Hermed gælder de første lighedstegn ovenfor. De andre lighedstegn følger af (6.17)). Vi har altså

$$\frac{|K|}{|K \cap N|} = \frac{|NK|}{|N|},$$

hvoraf det ønskede følger. □

(6.46) BEMÆRKNING: Lad $H \subseteq K$ være undergrupper i G. Antag at både H og K er *normale* i G. For at kunne adskille elementerne i de to faktorgrupper G/H og G/K skriver vi for $a \in G$

$$\widehat{a} = aH \in G/H \quad \text{og} \quad \widehat{\widehat{a}} = aK \in G/K.$$

Da $H \subseteq K$ er det klart, at når vi betragter $\widehat{a}$ og $\widehat{\widehat{a}}$ som *mængder* (af elementer i G), så er $\widehat{a} \subseteq \widehat{\widehat{a}}$. Specielt har vi også, at hvis $\widehat{a} = \widehat{b}$ (altså $a^{-1}b \in H$), så er $\widehat{\widehat{a}} = \widehat{\widehat{b}}$ $(a^{-1}b \in K)$. Dette viser at afbildningen

$$\varphi : G/H \to G/K,$$

defineret ved $\varphi(\widehat{a}) = \widehat{\widehat{a}}$, er en (veldefineret) (gruppe-)epimorfi. Vi har

$$\widehat{a} \in \ker\varphi \Leftrightarrow \widehat{\widehat{a}} = \widehat{\widehat{1}} \Leftrightarrow a \in K.$$

Derfor er

$$\ker\varphi = \{\widehat{a} \mid a \in K\}.$$

Når vi betragter H som en normal undergruppe af K (hvad den jo er!), ser vi, at

$$\ker\varphi = K/H.$$

Derfor viser en anvendelse af den 1. isomorfisætning det næste resultat. □

(6.48) SÆTNING. (3. isomorfisætning for grupper): *Lad $H \subseteq K$ være normale undergrupper i G. Så er $K/H = \{aH \mid a \in K\}$ en normal undergruppe i G/H og der gælder*

$$G/H \Big/ K/H \simeq G/K. \qquad \square$$

(6.49) ØVELSE: Lad $n \in \mathbb{N}$, L et legeme. Lad $GL(n, L)$ være som i (6.1)(2). Sæt

$$SL(n, L) = \{A \in L_n^n \mid \operatorname{Det} A = 1\}.$$

Vis, at $SL(n, L)$ er en normal undergruppe i $GL(n, L)$, og at $GL(n, L)/SL(n, L) \simeq (L \setminus \{0\}, \cdot)$, altså L's multiplikative gruppe. □

(6.50) ØVELSE: Lad $N \triangleleft G$. For $a \in G$ lad $\widehat{a} = aN \in G/N$. Lad G være endelig.

(1) Vis, at $|\widehat{a}| \mid |a|$ for alle $a \in G$.

(2) Gælder følgende: Hvis $\widehat{a} = \widehat{b}$ så er $|a| = |b|$?

□

Kapitel 7. Gruppeteori. Fortsat.

I dette kapitel behandles i kortfattet form nogle centrale emner fra gruppeteorien. Desværre kan det kun blive til smagsprøver.

Oversigt:

1° Om de symmetriske grupper S_n.

Disse grupper blev beskrevet i (6.1)(1). Gruppen S_n's elementer ($n \in \mathbb{N}$) er permutationerne af mængden $\{1, 2, \ldots, n\}$. Et element $\pi \in S_n$ er altså en bijektiv afbildning af $\{1, 2, \ldots, n\}$ på sig selv. Den *udførlige skrivemåde* for $\pi \in S_n$ er

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n) \end{pmatrix}$$

Vi repræsenterer altså π ved en matrix med $1, 2, \ldots, n$ i første række og $\pi(1), \pi(2), \ldots, \pi(n)$ i anden række. Hvis $\pi, \rho \in S_n$, har deres *produkt* $\pi \circ \rho$ (som vi fra nu af vil betegne $\pi\rho$) skrivemåden

$$\pi \circ \rho = \pi\rho = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(\rho(1)) & \pi(\rho(2)) & \ldots & \pi(\rho(n)) \end{pmatrix}$$

(7.1) EKSEMPEL: Lad $\pi, \rho \in S_4$ være repræsenteret som

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

Vi har

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow \rho & \downarrow \rho & \downarrow \rho & \downarrow \rho \\ 2 & 3 & 4 & 1 \\ \downarrow \pi & \downarrow \pi & \downarrow \pi & \downarrow \pi \\ 2 & 1 & 3 & 4 \end{array}$$

så

$$\pi\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

Tilsvarende er (regn efter!)

$$\rho\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

□

(7.2) DEFINITIONER: Når $\pi \in S_n$, kaldes $i \in \{1, 2, \ldots, n\}$ et *fixpunkt* for π, hvis $\pi(i) = i$. Mængden af fixpunkter for π betegnes $F(\pi) \subseteq \{1, 2, \ldots, n\}$. To permutationer π, ρ kaldes *disjunkte*, når $F(\pi) \cup F(\rho) = \{1, 2, \ldots, n\}$. Hvis vi sætter $\widetilde{F}(\pi) = \{1, 2, \ldots, n\} \setminus F(\pi)$, altså mængden af *ikke–fixpunkter* er π og ρ netop da disjunkte når $\widetilde{F}(\pi) \cap \widetilde{F}(\rho) = \varnothing$.

(Idet ovenstående eksempel er $F(\pi) = \{2\}, F(\rho) = \varnothing$, så π og ρ er ikke disjunkte).

□

(7.3) HJÆLPESÆTNING. *Når $\pi, \rho \in S_n$ er disjunkte, gælder $\pi\rho = \rho\pi$.*

BEVIS: Lad $x \in \{1, 2, \ldots, n\}$. Vi viser $\pi\rho(x) = \rho\pi(x)$ i 3 tilfælde:

$1^*: x \in F(\pi) \cap F(\rho)$, $2^*: x \notin F(\pi)$ dvs. $x \in \widetilde{F}(\pi)$.

$3^*: x \notin F(\rho)$ dvs. $x \in \widetilde{F}(\rho)$.

1^* : Her er $\pi\rho(x) = \pi(x) = x = \rho(x) = \rho\pi(x)$.

2^* : $x \in \widetilde{F}(\pi)$. Så er $\pi(x) \in \widetilde{F}(\pi)$ (idet $\pi(x) \in F(\pi) \Rightarrow \pi(\pi(x)) = \pi(x) \Rightarrow \pi(x) = x$ (da π er injektiv) $\Rightarrow x \in F(\pi)$, modstrid). Da $x, \pi(x) \in \widetilde{F}(\pi)$ fås $x, \pi(x) \notin \widetilde{F}(\rho)$ altså $x, \pi(x) \in F(\rho)$. Dermed er $\rho\pi(x) = \pi(x) = \pi\rho(x)$.

3^* : Analog til 2^* med π og ρ byttet om. □

(7.4) DEFINITION: Lad $r \in \mathbb{N}$. Et element $\pi \in S_n$ kaldes en *r–cykel* (*cykel af længde r*), hvis der findes r forskellige elementer $x_1, x_2, \ldots, x_r \in \{1, 2, \ldots, n\}$ således at

$$\pi(x_1) = x_2, \pi(x_2) = x_3, \ldots, \pi(x_{r-1}) = x_r, \pi(x_r) = x_1$$
$$\pi(x) = x \quad \text{for} \quad x \neq x_1, x_2, \ldots, x_r.$$

Det er så klart, at $\widetilde{F}(\pi) = \{x_1, \ldots, x_r\}$, når $r \geq 2$, $\widetilde{F}(\pi) = \varnothing$, når $r = 1$. Vi benytter en *forenklet skrivemåde* for π som

$$\pi = (x_1, x_2, \ldots, x_r).$$

Fra det ovenstående er det klart at

$$(x_1, x_2, \ldots, x_r) = (x_2, x_3, \ldots, x_r, x_1) = (x_3, x_4, \ldots, x_r, x_1, x_2) = \ldots$$

Vi ved også at ét af tallene $x_1, \ldots, x_r$ er det mindste af $x_1, \ldots, x_r$. Hvis dette tal er x_i vælger vi $(x_i, x_{i+1}, \ldots, x_r, x_1, \ldots, x_{i-1})$ som den *normerede* skrivemåde og indicerer dette ved at understrege det første (mindste) tal i cyklen. □

(7.5) EKSEMPEL:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix} \quad \text{er en 3-cykel,}$$

nemlig

$$\pi = (4, 2, 5) \qquad \text{(forenklet).}$$

Den normerede skrivemåde for π er

$$\pi = (\underline{2}, 5, 4), \quad \text{da} \quad 2 < 4 \quad \text{og} \quad 2 < 5.$$

(Vi har *ikke* $\pi = (\underline{2}, 4, 5)$!!) □

(7.6) SÆTNING OG ALGORITME. *Ethvert element $\pi \in S_n$ er et produkt af disjunkte cykler. Når cyklerne er normerede, er denne fremstilling af π som et produkt af cykler entydig pånær rækkefølgen af cyklerne (jfr. (7.3)).*

BEVIS: Vi bestemmer et tal $r \in \mathbb{N}$ og elementer $x_2, \ldots, x_r \in \{1, 2, \ldots, n\}$ ved

$$\pi(1) = x_2, \quad \pi(x_2) = x_3, \ldots, \pi(x_{r-1}) = x_r, \quad \pi(x_r) = 1.$$

Her forlanges, at $x_1 = 1, x_2, \ldots, x_r$ alle er forskellige. (Muligheden at $r = 1$ er *ikke* udelukket). Vælg y_1 som det mindste tal i $\{1, 2, \ldots, n\} \setminus \{x_1, x_2, \ldots, x_r\}$ (hvis $r \neq n$), og bestem forskellige elementer $y_2, \ldots, y_s \in \{1, \ldots, n\}$ ved $\pi(y_1) = y_2, \pi(y_2) = y_3, \ldots, \pi(y_s) = y_1$. Det er klart, at $\{x_1, \ldots, x_r\} \cap \{y_1, y_2, \ldots, y_s\} = \varnothing$ (overvej dette!) Hvis $r + s < n$, vælges z_1 minimalt i $\{1, 2, \ldots, n\} \setminus (\{x_1, \ldots, x_r\} \cup \{y_1, \ldots, y_s\})$ og vi bestemmer elementer $z_2, \ldots, z_t$ ved $\pi(z_1) = z_2, \pi(z_2) = z_3, \ldots, \pi(z_t) = z_1$. Vi fortsætter på denne måde indtil alle elementer i $\{1, 2, \ldots, n\}$ er opbrugte og har så

$$\pi = (\underline{1}, x_2, \ldots, x_r)(\underline{y_1}, y_2, \ldots, y_s)(\underline{z_1}, \ldots, z_t) \ldots$$

som ønsket.

Antag nu at

$$\pi = (\underline{x'_1}, x'_2, \ldots, x'_{r'})(\underline{y'_1}, y'_2, \ldots, y'_{s'}) \ldots$$

er en fremstilling af π som et produkt af disjunkte cykler i normeret skrivemåde. Da 1 er det mindste af $\{1, 2, \ldots, n\}$ må 1 være et af de understregede tal i fremstillingen. Ved eventuelt at ændre cyklernes rækkefølge ved (7.3) kan vi antage $x'_1 = 1$. Så er $x'_2 = \pi(x'_1) = \pi(1) = x_2$, og vi ser let at $(\underline{x_1}, x_2, \ldots, x_r) = (\underline{x'_1}, x'_2, \ldots, x'_{r'})$. Da y_1 er det mindste tal $\neq x_1, x_2, \ldots, x_r$ kan vi antage $y_1 = y'_1$ og får så $(\underline{y_1}, \ldots, y_s) = (\underline{y'_1}, y'_2, \ldots, y'_{s'})$. Ved at fortsætte på denne måde afsluttes beviset. □

(7.7) EKSEMPLER: (1) Vi skriver

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 7 & 3 & 6 & 10 & 1 & 12 & 9 & 5 & 8 & 2 & 11 \end{pmatrix}$$

som produkt af disjunkte cykler (normeret)

$$1 \xrightarrow{\pi} 4 \xrightarrow{\pi} 6 \xrightarrow{\pi} 1 \quad \text{giver cyklen} \quad (\underline{1},4,6).$$

Det mindste tal $\neq 1,4,6$ er 2

$$2 \xrightarrow{\pi} 7 \xrightarrow{\pi} 12 \xrightarrow{\pi} 11 \xrightarrow{\pi} 2 \quad \text{giver cyklen} \quad (\underline{2},7,12,11).$$

Det mindste tal $\neq 1,2,4,6,7,11,12$ er 3

$$3 \xrightarrow{\pi} 3 \quad \text{giver cyklen} \quad (\underline{3}).$$

Dernæst er 5 der mindste tal

$$5 \xrightarrow{\pi} 10 \xrightarrow{\pi} 8 \xrightarrow{\pi} 9 \xrightarrow{\pi} 5 \quad \text{giver} \quad (\underline{5},10,8,9).$$

Hermed er den ønskede fremstilling

$$\pi = (\underline{1},4,6)(\underline{2},7,12,11)(\underline{3})(\underline{5},10,8,9).$$

Det er normalt at udelade 1-cykler i sådanne fremstillinger, og vi vil skrive

$$\pi = (\underline{1},4,6)(\underline{2},7,12,11)(\underline{5},10,8,9)$$

(2) Permutationen π kan også skrives som et produkt af cykler på følgende måde, men disse cykler er *ikke* disjunkte:

$$\pi = (\underline{1},4,6)(\underline{2},7,12,11)(\underline{1},5)(\underline{1},10,8,9)(\underline{1},5).$$

(3) Lad $\rho_1 = (\underline{1},5,4,2)(\underline{3},6)$, $\rho_2 = (\underline{2},3)$. Så er

$$\begin{aligned} &\rho_1\rho_2 = (\underline{1},5,4,2,6,3) \\ &(1 \xrightarrow{\rho_2} 1 \xrightarrow{\rho_1} 5, 5 \xrightarrow{\rho_2} 5 \xrightarrow{\rho_1} 4, 4 \xrightarrow{\rho_2} 4 \xrightarrow{\rho_1} 2, \\ &\quad 2 \xrightarrow{\rho_2} 3 \xrightarrow{\rho_1} 6, 6 \xrightarrow{\rho_2} 6 \xrightarrow{\rho_1} 3, 3 \xrightarrow{\rho_2} 2 \xrightarrow{\rho_1} 1) \end{aligned}$$

$$\text{Endvidere er} \left\{ \begin{array}{c} \rho_2\rho_1 = (\underline{1},5,4,3,6,2) \\ \rho_2\rho_1\rho_2 = (\underline{1},5,4,3)(\underline{2},6) \end{array} \right\}. \qquad \text{(Overvej dette)}$$

□

(7.8) ØVELSE: Lad

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{pmatrix} \quad \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ \underline{1} & 3 & 2 & 4 & 6 & 5 \end{pmatrix} \in S_6$$

Skriv $\pi, \rho, \rho\pi$ og $\pi\rho$ som produkt af disjunkte cykler. □

(7.9) SÆTNING. (Regneregler for cykler) *Lad* $(x_1, x_2, \ldots, x_r)$, $(y_1, y_2, \ldots, y_s)$ *være disjunkte cykler i* S_n. *Lad* $\rho \in S_n$. *Der gælder*

(1) $$\rho(x_1, x_2, \ldots, x_r)\rho^{-1} = (\rho(x_1), \rho(x_2), \ldots, \rho(x_r))$$

(2) $$\left.\begin{aligned}(x_1, x_2, \ldots, x_r) &= (x_1, x_r)(x_1, x_2, \ldots, x_{r-1}) \\ &= (x_1, x_2)(x_2, x_3, \ldots, x_{r-1}, x_r)\end{aligned}\right\} r \geq 2$$

(3) $$\left.\begin{aligned}(x_1, x_2, \ldots, x_r) &= (x_1, x_r)(x_1, x_{r-1}) \ldots (x_1, x_2) \\ &= (x_1, x_2)(x_2, x_3) \ldots (x_{r-1}, x_r)\end{aligned}\right\} r \geq 2$$

(4) $$(x_1, x_i)(x_1, x_2, \ldots, x_r) = (x_1, \ldots, x_{i-1})(x_i, \ldots, x_r), \ 2 < i < r$$

(5) $$\begin{aligned}&(x_1, y_1)(x_1, x_2, \ldots, x_r)(y_1, y_2, \ldots, y_s) \\ &\quad = (x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_s)\end{aligned}$$

BEVIS: Vi nøjes med at vise (5) og overlader de andre (som en ØVELSE) til læseren. Sæt $\alpha = (x_1, y_1), \beta = (x_1, x_2, \ldots, x_r), \gamma = (y_1, y_2, \ldots, y_s)$. For $1 \leq i \leq r-1$ er

$$x_i \xrightarrow{\gamma} x_i \xrightarrow{\beta} x_{i+1} \xrightarrow{\alpha} x_{i+1}.$$

For $i = r$ er

$$x_r \xrightarrow{\gamma} x_r \xrightarrow{\beta} x_1 \xrightarrow{\alpha} y_1.$$

For $1 \leq j \leq s-1$ er

$$y_j \xrightarrow{\gamma} y_{j+1} \xrightarrow{\beta} y_{j+1} \xrightarrow{\alpha} y_{j+1}.$$

For $j = s$ er

$$y_s \xrightarrow{\gamma} y_1 \xrightarrow{\beta} y_1 \xrightarrow{\alpha} x_1.$$

Derfor er $\alpha\beta\gamma = (x_1, x_2, \ldots, x_r, y_1, y_2, \ldots, y_s)$. □

(7.10) DEFINITION (OG SÆTNING): En 2-cykel (x_1, x_2) kaldes også en *transposition*. Hvis vi kombinerer (7.6) (som siger, at enhver permutation er et produkt af cykler) og (7.9)(3) (som siger, at enhver cykel af længde ≥ 2 er et produkt af transpositioner) ses at *enhver permutation er et produkt af transpositioner.* □

(7.11) EKSEMPEL: Vi har $(1,4,6) = (1,4)(4,6)$, $(2,7,12,11) = (2,11)(2,12)(2,7)$, $(5,10,8,9) = (10,8,9,5) = (10,8)(8,9)(9,5)$ således at én (af *mange*) fremstilling af permutationen π fra (7.7)(1) som produkt af transpositioner er

$$\pi = (1,4)(4,6)(2,11)(2,12)(2,7)(8,10)(8,9)(5,9).$$

Vi har også (f.eks.)

$$\begin{aligned}\pi =&(1,4)(4,6)(3,8)(2,7)(7,12)(11,12)(3,8)(2,4)(1,5)\\ &(1,9)(1,8)(4,5)(1,10)(4,5)(1,5)(2,4).\end{aligned}$$

I det første tilfælde er π skrevet som et produkt af 8 transpositioner, og i det andet som et produkt af 16 transpositioner. Vi viser i det følgende, at hvis en permutation ρ kan skrives som et produkt af k transpositioner og som et produkt af ℓ transpositioner, så er $k \equiv_2 \ell$. □

(7.12) ØVELSE: Skriv permutationerne π, ρ, $\rho\pi$ og $\pi\rho$ fra (7.8) som et produkt af transpositioner. □

(7.13) DEFINITION: Lad $\pi \in S_n$ være skrevet som et produkt af disjunkte cykler af længde $r_1, r_2, \ldots, r_t$ (hvor $r_i \in \mathbb{N}$ og $r_1 + r_2 + \cdots + r_t = n$). Så er *transpositionstallet* $T(\pi)$ for π defineret ved

$$T(\pi) = n - t = r_1 + r_2 + \cdots + r_t - t = \sum_{i=1}^{t}(r_i - 1).$$

Bemærk, at π's fixpunkter (1-cyklerne) ikke bidrager til transpositionstallet for π. På grund af entydighedsudsagnet i (7.6) er transpositionstallet veldefineret. Det samme gælder derfor for π's *fortegn*, der betegnes $\operatorname{sign}(\pi)$ og er defineret ved

$$\operatorname{sign}(\pi) = (-1)^{T(\pi)}.$$

Hvis $T(\pi)$ er lige ($T(\pi) \equiv_2 0$) er $\operatorname{sign}\pi = 1$ og π kaldes *lige*. Hvis $T(\pi)$ er ulige ($T(\pi) \equiv_2 1$) er $\operatorname{sign}(\pi) = -1$ og π kaldes *ulige*. □

(7.14) EKSEMPEL: Lad π være som i (7.7)(1). Der gælder $T(\pi) = 8$, $\operatorname{sign}(\pi) = 1$, π er lige. □

(7.15) HJÆLPESÆTNING. *Lad $\rho \in S_n$ være vilkårlig og lad $\tau \in S_n$ være en transposition. Der gælder enten $T(\tau\rho) = T(\rho) + 1$ eller $T(\tau\rho) = T(\rho) - 1$. Under alle omstændigheder gælder*

$$\operatorname{sign}(\tau\rho) = -\operatorname{sign}(\rho).$$

BEVIS: Antag, at ρ er skrevet som produkt af disjunkte cykler, hvor vi medregner 1-cyklerne (ρ's fixpunkter). Lad $\tau = (z_1, z_2)$. Der er to muligheder: 1* Der findes en cykel $(x_1, x_2, \ldots, x_r)$ mellem ρ's disjunkte cykler således at z_1 og z_2 begge forekommer mellem $x_1, x_2, \ldots, x_r$. 2* Der findes to forskellige cykler $(x_1, x_2, \ldots, x_r)$, $(y_1, y_2, \ldots, y_s)$ mellem ρ's disjunkte cykler således at z_1 forekommer mellem $x_1, x_2, \ldots, x_r$ og z_2 forekommer mellem $y_1, y_2, \ldots, y_s$.

1* Da $(x_1, x_2, \ldots, x_r) = (x_2, x_3, \ldots, x_r, x_1) = (x_3, x_4, \ldots, x_r, x_1, x_2) = \ldots$ ser vi, at vi, (efter eventuelt at have ændret notationen), kan antage, at $z_1 = x_1$. Så er $z_2 = x_i$ for et $i \geq 2$. Hvis $i = 2$ er $\tau(x_1, \ldots, x_r) = (x_2, x_3, \ldots, x_r)$, og hvis $i = r$ er $\tau(x_1, x_2, \ldots, x_r) = (x_1, x_2, \ldots, x_{r-1})$ ifølge (7.9)(2). For $2 < i < r$ er $\tau(x_1, \ldots, x_r) = (x_1, \ldots, x_{i-1})(x_i, \ldots, x_r)$ ifølge (7.9)(4). Derfor er under alle omstændigheder $T(\tau(x_1, \ldots, x_r)) = r - 2$. De resterende cykler fra ρ indgår uændret i $\tau\rho$, da τ ikke involverer deres elementer. Alt i alt fås $T(\tau\rho) = T(\rho) - 1$.

2* Efter eventuelt at have ændret notation kan vi antage $z_1 = x_1$, $z_2 = y_1$. Ifølge (7.9)(5) er

$$\tau(x_1, \ldots, x_r)(y_1, \ldots, y_s) = (x_1, \ldots, x_r, y_1, \ldots, y_s)$$

således, at $T(\tau(x_1, \ldots, x_r)(y_1, \ldots, y_s)) = r + s - 1 = (r - 1) + (s - 1) + 1$. Da τ ikke involverer elementer fra de resterende cykler i ρ, fås alt i alt $T(\tau\rho) = T(\rho) + 1$. Herefter følger udsagnet $\operatorname{sign}(\tau\rho) = -\operatorname{sign}\rho$ fra definitionen af fortegn. □

(7.16) SÆTNING. *Lad $\pi, \rho \in S_n$. Der gælder*

(1) *Hvis π er et produkt af k transpositioner, er* $\operatorname{sign}(\pi) = (-1)^k$.

(2) $\operatorname{sign}(\pi\rho) = \operatorname{sign}(\pi)\operatorname{sign}(\rho)$.

BEVIS: (1) Antag, at $\pi = \tau_1\tau_2 \ldots \tau_k$ hvor $\tau_1, \ldots, \tau_k$ er transpositioner. Da $\tau_i = \tau_i^{-1}$ er $\pi^{-1} = \tau_k\tau_{k-1} \ldots \tau_1$. Derfor er $1 = (-1)^0 = (-1)^{T(1)} = \operatorname{sign}(1) = \operatorname{sign}(\tau_k\tau_{k-1} \ldots \tau_1\pi) = -\operatorname{sign}(\tau_{k-1} \ldots \tau_1\pi) = \cdots = (-1)^k \operatorname{sign}(\pi)$, ((7.15)), altså $\operatorname{sign}(\pi) = (-1)^k$.

(2) Hvis π er et produkt af k og ρ et produkt af ℓ transpositioner, er (trivielt) $\pi\rho$ et produkt af $k + \ell$ transpositioner. Derfor følger (2) fra (1). □

(7.17) BEMÆRKNING: Det er klart, at $(\{1, -1\}, \cdot)$ er en (cyklisk) gruppe af orden 2. (7.16) viser, at sign er en homomorfi fra S_n ind i denne gruppe. Når $n \geq 2$ indeholder S_n transpositioner, f.eks. $(1, 2)$. Disse har alle fortegn -1, således at sign er en epimorfi. Ifølge (6.37) er derfor for $n \geq 2$

$$\ker(\operatorname{sign}) = \{\pi \in S_n \mid \operatorname{sign}\pi = 1\}$$

en normal undergruppe af index 2 i S_n. Denne undergruppe betegnes A_n og kaldes den *alternerende* gruppe af grad n. For $n = 1$ sættes $A_n = S_n = \{(1)\}$. For $n \geq 2$ er $|S_n : A_n| = 2$. □

(7.18) ØVELSE: Vis, at ordenen af en permutation $\sigma \in S_n$ er mindste fælles multiplum af længderne af de disjunkte cykler, som indgår i fremstillingen af σ. □

(7.19) ØVELSE: Når $\pi \in S_n$ defineres π's permutationsmatrix $P(\pi) = (a_{ij})$ som følger

$$a_{ij} = \begin{cases} 1 & \text{hvis} \quad i = \pi(j) \\ 0 & \text{hvis} \quad i \neq \pi(j) \end{cases}$$

(1) Vis, at for $\pi, \rho \in S_n$ gælder $P(\pi)P(\rho) = P(\pi\rho)$.
(2) Vis, at for alle $\pi \in S_n$ gælder

$$\det P(\pi) = \operatorname{sign} \pi.$$

(Til beviset af (2) kan man benytte (1), (7.16) samt resultatet 19.3(1), se også 19.1(6)(c), fra HBF.)

(3) Er det rigtigt at

$$P(\pi)^t = P(\pi^{-1}) \quad \text{for alle} \quad \pi \in S_n \ ?$$

□

(7.20) REKREATIV ØVELSE: Her en en beskrivelse af *Ombytningsspillet* (som en ekspert vil kalde Transpositionsspillet). Til spillet benyttes nogle mønter af forskellig værdi som lægges i en række på bordet i vilkårlig rækkefølge. F.eks. lader vi mønterne

1	2	3	4	5	6
25 øre	50 øre	1 kr	5 kr	10 kr	20 kr

ligge på bordet i følgende rækkefølge $(*)$

$(*)$

5	3	4	6	1	2
10 kr	1 kr	5 kr	20 kr	25 øre	50 øre

To spillere, A og B, skiftes til at trække. Et *træk* er følgende: Ombyt to mønter x og y, hvor

(1) x ligger til venstre for y.
(2) x's værdi er *større* end y's værdi.

Den første spiller, der ikke er i stand til at trække, har *tabt* spillet. Hvem vinder spillet, hvis vi har rækkefølgen $(*)$ som udgangspunkt, og A begynder? □

2° Operationer af grupper på mængder.

Vi beskriver her en fundamental og meget anvendelig begrebsdannelse i gruppeteorien. Når M er en mængde betegner $S(M)$ den symmetriske gruppe på M (se (6.1)(1)).

Vi er i den situation, at vi har givet en gruppe G og en vilkårlig mængde M. Mængden af alle bijektive afbildninger fra M ind i M betegnes $S(M)$, den symmetriske gruppe på M. Det er velkendt, at $S(M)$ med kompositionen "sammensætning af funktioner" er en gruppe. Altså har vi to grupper: G og $S(M)$.

(7.21) DEFINITION: Lad G være en gruppe og M en vilkårlig mængde. En homomorfi mellem grupperne G og $S(M)$

$$\rho : G \to S(M)$$

kaldes en *operation af G på M*.

Dvs. til ethvert $g \in G$ knytter vi en bijektion af M ind i sig selv. Sagt på en anden måde: $\rho(g) \in S(M)$ eller $\rho(g) : M \to M$ bijektiv. At $\rho : G \to S(M)$ er en homomorfi betyder at

$$\text{For alle } g, h \in G : \rho(gh) = \rho(g) \circ \rho(h) .$$

Yderligere gælder ifølge (6.35), at ρ afbilder det neutrale element i G over i det neutrale element i $S(M)$, der jo er identitetsafbildningen 1_M på M. Altså

$$\rho(1) = 1_M .$$

Omvendt har vi følgende

BEMÆRKNING: Lad G være en gruppe, M en mængde. Med M^M betegnes mængden af afbildninger fra M ind i M. Givet en afbildning $\rho : G \to M^M$ der opfylder

(1) $\rho(gh) = \rho(g) \circ \rho(h)$
(2) $\rho(1) = 1_M$

kan vi slutte, at ρ er en operation af gruppen G på mængden M. (Overvej dette).

Hvis $\rho : G \to S(M)$ er en operation af G på M inducerer ρ en såkaldt "ydre komposition" på M. Vi får en afbildning

$$G \times M \to M \qquad (g, m) \mapsto gm$$

ved at sætte $gm := \rho(g)(m)$. Vi bemærker, at $\rho(g)$ er en (bijektiv) afbildning fra $M \to M$ således at $\rho(g)(m) \in M$. I denne skrivemåde betyder udsagnet, at ρ er en homomorfi (altså $\rho(gh) = \rho(g) \circ \rho(h)$), at der gælder

$$(*) \qquad \begin{cases} (gh)m = g(hm) & \text{for alle } g, h \in G,\ m \in M \\ 1m = m \end{cases}$$

På den anden side, hvis der er *givet* en afbildning $G \times M \to M$, $(g,m) \to gm$ som opfylder $(*)$, kan vi få en operation af G på M ved at sætte $\rho(g)(m) := gm$. (Overvej dette, jfr. ovenstående bemærkning).

(7.22) EKSEMPLER: (1) Hvis H er en undergruppe af S_n, opererer H på $M = \{1,2,\ldots,n\}$ ved inklusionshomomorfien $H \overset{\rho}{\hookrightarrow} S_n = S(M)$. For $\pi \in H$ og $m \in M$ er altså $\rho(\pi)(m) = \pi(m)$.

(2) En vilkårlig gruppe kan operere på sig selv (altså på mængden af sine elementer) på flere måder, f.eks. gennem de indre automorfier: Vi definerer $\rho : G \to S(G)$ ved $\rho(g) = \iota_g$, hvor ι_g er som i (6.33)(5). I (6.33)(5) er bevist, at ι_g er en automorfi af G, altså specielt en bijektion $G \to G$. Endvidere er det vist, at $\iota_g \circ \iota_h = \iota_{gh}$ og $(\iota_g)^{-1} = \iota_{g^{-1}}$. Så dette giver en operation af G på G.

(3) Det er klart man ved de indre automorfier også kan definere operationer af (undergrupper af) G på visse delmængder af $\mathcal{P}(G)$. Som M kan man vælge f.eks. $\mathcal{P}(G)$, eller mængden af undergrupper af G.

(4) Lad H være en undergruppe i G. Lad Ω_H være mængden af *venstresideklasser* af H i G. Det vil sige

$$\Omega_H = \{xH \mid x \in G\}.$$

G opererer på Ω_H som følger: For $g \in G$, $xH \in \Omega_H$ lad $\rho_H(g)(xH) = gxH$. [Vi overvejer at $\rho_H(g)$ er veldefineret: Hvis $xH = yH$ for $x,y \in G$ må vises at $gxH = gyH$. Men

$$xH = yH \overset{(6.13)}{\Leftrightarrow} y^{-1}x \in H \Leftrightarrow y^{-1}(g^{-1}g)x \in H$$

$$\Leftrightarrow (gy)^{-1}gx \in H \overset{(6.13)}{\Leftrightarrow} gxH = gyH. \qquad]$$

Hvis specielt $H = \{1\}$ kan Ω_H identificeres med G, da H's sideklasser alle består af netop ét element i G. Så $\rho_{\{1\}}$ giver en anden operation (end den i (2)) af G på sig selv. □

(7.23) ØVELSE: Lad G være en gruppe og lad $H = G \times G = \{(x,y) \mid x,y \in G\}$. H er en gruppe ved "koordinatvis" multiplikation: $(x,y)(x',y') := (xx',yy')$. For $(x,y) \in H$, $g \in G$ sættes $\rho(x,y)(g) = xgy^{-1}$. Vis at dette giver en operation af H på G. □

(7.24) ØVELSE: (1) Lad V være et $\mathbb{R}$-vektorrum. Gør rede for, at gruppen $\mathbb{R} \setminus \{0\}$ opererer på V ved $\rho(\alpha)\underline{v} = \alpha\underline{v}$, $\alpha \in \mathbb{R} \setminus \{0\}, \underline{v} \in V$. □

(2) Lad L være et legeme, $n \in \mathbb{N}$. Vis, at $GL(n,L)$ opererer på mængden L_1^n af $n \times 1$-matricer over L ved matrixmultiplikation. □

(7.25) DEFINITION OG SÆTNING. *Lad $\rho : G \to S(M)$ være en operation af G på M. Vi definerer en relation $\sim_\rho$ på M ved*

$$m \sim_\rho m' \Leftrightarrow \textit{Der findes } g \in G \textit{ så } \rho(g)(m) = m'.$$

Så er $\sim_\rho$ en ækvivalensrelation på M. Ækvivalensklasserne for $\sim_\rho$ kaldes baner *eller* transitivitetsområder *(for ρ). ρ kaldes* transitiv, *hvis der kun er én bane for ρ, altså hvis der gælder:*

$$\text{For alle } m, m' \in M \quad \text{eksisterer } g \in G \text{ så } \rho(g)(m) = m'.$$

BEVISET for at $\sim_\rho$ er en ækvivalensrelation er en ØVELSE. □

(7.26) EKSEMPLER: (1) S_n er transitiv på $M = \{1, \ldots, n\}$. (2) Banerne ved operationer af G på sig selv fra (7.22)(2) kaldes for G's *konjugationsklasser* af elementer, (se afsnit 3°). Denne operation er kun transitiv når $G = \{1\}$! (3) Operationen Ω_H fra (7.22)(4) er transitiv. (Overvej dette). □

(7.27) DEFINITION OG SÆTNING. *Lad $\rho : G \to S(M)$ være en operation af G på M. For $m \in M$ er m's* stabilisator $\mathrm{Stab}_\rho(m) := \{g \in G \mid \rho(g)(m) = m\}$. *Det er klart, at m's stabilisator er en undergruppe af G. (Hvis $g, h \in \mathrm{Stab}_\rho(m)$ er $\rho(gh^{-1})(m) = \rho(g)(\rho(h^{-1})(m)) = \rho(g)(\rho(h)^{-1}(m)) = \rho(g)(m) = m$, så $gh^{-1} \in \mathrm{Stab}_\rho(m)$.)*

□

Det næste resultat er meget anvendeligt. I resten af 2° antager vi at *G og M er endelige.*

(7.28) SÆTNING. *Lad $\rho : G \to S(M)$ være en transitiv operation af G på M. Der gælder for $m \in M$*

$$|M| = |G : \mathrm{Stab}_\rho(m)|.$$

BEVIS: Lad $H = \mathrm{Stab}_\rho(m)$, således at $|\Omega_H| = |G : \mathrm{Stab}_\rho(m)|$. Vi definerer en bijektion f mellem Ω_H og M som følger: Lad $xH \in \Omega_H$. Vi sætter $f(xH) = \rho(x)(m)$. Vi viser, at f er veldefineret: Hvis $xH = yH$ må vises $\rho(x)(m) = \rho(y)(m)$.

$$xH = yH \Rightarrow y^{-1}x \in H \Rightarrow m = \rho(y^{-1}x)(m) = \rho(y)^{-1}(\rho(x)m) \Rightarrow \rho(y)(m) = \rho(x)(m),$$

som ønsket. Da ρ er transitiv, er f surjektiv. f er også injektiv, idet

$$f(xH) = f(yH) \Rightarrow \rho(x)(m) = \rho(y)(m) \Rightarrow \rho(y^{-1}x)(m) = m \Rightarrow y^{-1}x \in H \Rightarrow xH = yH.$$

□

(7.29) ØVELSE: Lad H være en undergruppe af G, $x \in G$. Vis, at xHx^{-1} er en undergruppe af G, og at $H \simeq xHx^{-1}$. □

(7.30) ØVELSE: Lad H være en undergruppe af G. Lad ρ_H være operationen på Ω_H defineret i (7.22)(4). Lad $x \in G$.

(1) Vis

$$\mathrm{Stab}_{\rho_H}(xH) = xHx^{-1}.$$

(2) Hvad udsiger (7.28) i dette tilfælde?

(3) Beskriv $\ker \rho_H$.

□

(7.31) DEFINITION: Lad $\rho : G \to S(M)$ være en operation af G på M. En delmængde $T = \{m_1, m_2, \ldots, m_k\}$ af M kaldes et *repræsentantsystem for* ρ's *baner*, hvis der gælder

(i) For alle $m \in M$ findes $i \in \{1, \ldots, k\}$ så $m \sim_\rho m_i$.
(ii) Hvis $i, j \in \{1, 2, \ldots, k\}$, $i \neq j$ gælder $m_i \not\sim_\rho m_j$.

□

(7.32) BEMÆRKNING: Lad notationen være som i (7.31) og antag, at T *er* et repræsentantsystem for ρ's baner. For $1 \leq i \leq k$ sættes

$$M_i = \{m \in M \mid m \sim_\rho m_i\}.$$

Der gælder så $|M| = |M_1| + |M_2| + \cdots + |M_k|$. Det skyldes, at M_i'erne netop er de forskellige $\sim_\rho$-ækvivalensklasser. □

(7.33) SÆTNING. *Lad $\rho : G \to S(M)$ være en operation af G på M. Lad $T = \{m_1, \ldots, m_k\}$ være et repræsentantsystem for ρ-banerne. Der gælder*

$$|M| = \sum_{i=1}^{k} |G : \mathrm{Stab}_\rho(m_i)|.$$

BEVIS: Lad $1 \leq i \leq k$. Sæt $M_i = \{m \in M \mid m \sim_\rho m_i\}$. Vi lader G operere på M_i ved $\rho_i : G \to S(M_i)$, hvor ρ_i er defineret ved

$$\rho_i(x)(m) = \rho(x)(m) \quad \text{for } x \in G, m \in M_i.$$

[Når $m \in M_i$ vil også $\rho(x)(m) \in M_i$, da $m \sim_\rho \rho(x)(m)$ og M_i er en ρ-bane.] Det er klart, at ρ_i er transitiv, idet M_i er den eneste ρ_i-bane. Ifølge (7.28) gælder derfor

$$|M_i| = |G : \mathrm{Stab}_{\rho_i}(m_i)|.$$

Men fra definitionen af ρ_i er det klart, at $\mathrm{Stab}_{\rho_i}(m_i) = \mathrm{Stab}_\rho(m_i)$ (overvej!). Så

$$|M_i| = |G : \mathrm{Stab}_\rho(m_i)|.$$

Nu følger (7.33) fra (7.32). □

(7.34) ØVELSE: Lad π være permutationen i eksempel (7.7)(1),
$\pi = (1,4,6)(2,7,12,11)(5,10,8,9) \in S_{12}$. Lad $G = \langle \pi \rangle$ operere på $M = \{1, 2, \ldots, 12\}$ som beskrevet i (7.22)(1). (Altså $\rho(\pi^k)(i) = \pi^k(i)$ for $k \in \mathbb{Z}$, $i \in M$.)

(1) Bestem banerne for ρ på M.
(2) Bestem $\mathrm{Stab}_\rho(i)$ for $i = 1, 2, 3, 5$.

□

3° Anvendelser. Klasseligningen.

3.1. Indledende betragtninger.

Vi lægger ud med et vigtigt eksempel, der vil spille en gennemgående rolle i dette afsnit.

(7.35) DEFINITION: Lad G være en (endelig) gruppe, U en undergruppe af G. Vi definerer en ækvivalensrelation på G som følger:

$$a \sim_U b \iff \exists u \in U : b = uau^{-1}.$$

Det er let at se, at $\sim_U$ faktisk *er* en ækvivalensrelation på G (regn selv efter). Hvis $a \sim_U b$ siger vi, at a og b er *U-konjugerede*. Er $U = G$ vil vi ofte blot sige, at a og b er konjugerede. Ækvivalensklassen indeholdende a, lad os betegne den $\hat{a}$, er

$$\hat{a} = \{\, b \in G \mid \exists u \in U : b = uau^{-1} \,\} = \{\, uau^{-1} \mid u \in U \,\}.$$

Denne observation giver anledning til følgende definition:

(7.36) DEFINITION: Når G er en endelig gruppe, U en undergruppe af G, $g \in G$, defineres *U-konjugationsklassen* af g, $\mathcal{C}(g, U)$, til at være

$$\mathcal{C}(g, U) = \{\, xgx^{-1} \mid x \in U \,\}.$$

Vi bemærker, at $\hat{a}$ i (7.35) netop er U-konjugationsklassen af a. Da U-konjugationsklasser er ækvivalensklasser for en ækvivalensrelation gælder, at to U-konjugationsklasser enten er identiske eller disjunkte.

(7.37) EKSEMPEL: Betragt undergruppen $U = \langle (1,2) \rangle = \{(1), (1,2)\}$ af S_4. Hvis $x = (2,3,4)$ er

$$\mathcal{C}(x, U) = \{(2,3,4), (1,3,4)\},$$

idet $(1,2)(2,3,4)(1,2)^{-1} = (1,3,4)$.
Vi minder om en regneregel for cykler ((7.9)(1)) som vi benyttede i ovenstående eksempel og som vil blive benyttet utallige gange i det følgende: Hvis $\rho \in S_n$ og $(x_1, \ldots, x_r)$ er en r-cykel i S_n gælder

$$\rho(x_1, \ldots, x_r)\rho^{-1} = \big(\rho(x_1), \ldots, \rho(x_r)\big).$$

Med andre ord: Tager vi en r-cykel og konjugerer med $\rho \in S_n$, dvs. udregner $\rho(x_1, \ldots, x_r)\rho^{-1}$, så får vi igen en r-cykel. Derfor kan vi også opfatte ækvivalensrelationen $\sim_U$ som en ækvivalensrelation på mængden af r-cykler i S_n, når U er en undergruppe af S_n. Hvis altså M er mængden af r-cykler i S_n, giver $\sim_U$ anledning til en klassedeling af M.

(7.38) EKSEMPEL: Lad U være som i det foregående eksempel, og lad K være mængden af alle transpositioner i S_4. Vi har indset, at $\sim_U$ giver anledning til en klassedeling af K, og de forskellige *U-konjugationsklasser af transpositioner* er

$$\{(1,2)\}, \{(1,3),(2,3)\}, \{(1,4),(2,4)\}, \{(3,4)\}.$$

F.eks. danner $\{(3,4)\}$ en U-konjugationsklasse, da $(1,2)(3,4)(1,2)^{-1} = (3,4)$.

(7.39) ØVELSE: Lad $U = \langle (1,2) \rangle$ være en undergruppe af S_4. Beregn de forskellige U-konjugationsklasser af 3-cykler i S_4.

3.2. Om cykeltyper.

Vi skal her undersøge hvornår to permutationer er konjugerede i S_n, dvs. for givne π og ρ i S_n vil vi undersøge netop hvornår der findes τ i S_n med egenskaben at $\tau\pi\tau^{-1} = \rho$. Dette problem har en ganske simpel løsning, som vi vil se.

Lad $\pi \in S_n$ være givet. Som bekendt kan π fremstilles på entydig måde som et produkt af disjunkte cykler. Betegnes for $p \in \mathbb{N}$ med $m_p = m_p(\pi)$ antallet af cykler af længde p i denne fremstilling, får vi en følge

$$m_1, m_2, m_3, \ldots$$

af tal ≥ 0, der kaldes *cykeltypen* for permutationen π. Bemærk, at $m_p = 0$, når $p > n$, og at

$$\sum_p p m_p = n.$$

En given cykeltype anskueliggøres ofte ved et *billede*

$$\overbrace{(*)\cdots(*)}^{m_1}\overbrace{(*,*)\cdots(*,*)}^{m_2}\cdots\overbrace{(*,\ldots,*)\cdots(*,\ldots,*)}^{m_p}\cdots,$$

hvor der er m_1 symboler af formen $(*)$ svarende til "1-cyklerne", dvs. fixpunkterne, m_2 symboler af formen $(*,*)$ osv. For et givet $n \in \mathbb{N}$ er antallet af cykeltyper i S_n bestemt som antallet af løsninger $m_p \geq 0$ til ligningen

$$\sum_{p=1}^{\infty} p m_p = n.$$

Vi kan nu svare på det spørgsmål, som vi stillede os selv i starten.

(7.40) SÆTNING. *Lad $n \in \mathbb{N}$ være givet. To permutationer er da konjugerede i S_n, hvis og kun hvis de har samme cykeltype.*

BEVIS: $\Rightarrow$: Cykeltypen af π er bestemt ved fremstillingen af π som et produkt af disjunkte cykler. For en p-cykel og en permutation τ ved vi at

$$\tau(x_1, \ldots, x_p)\tau^{-1} = \big(\tau(x_1), \ldots, \tau(x_p)\big).$$

Konjugering afbilder altså en p-cykel på en p-cykel, og da "disjunkthed" bevares, følger påstanden.

$\Leftarrow$: 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. Den permutation i S_n, der bestemmes ved, at et element $i \in \{1, 2, \ldots, n\}$ afbildes over i det element, som i opskrivningen står umiddelbart under i i den nederste række, vil da konjugere den første permutation over i den anden ifølge (7.9)(1). □

3.3 Generalisering af begreberne.

For en god ordens skyld medtager vi følgende generelle definition som udvider, hvad vi allerede har set.

(7.41) DEFINITION: Lad G være en (endelig) gruppe, $\mathcal{K} \subseteq \mathcal{P}(G)$ en mængde af delmængder af G, og U en undergruppe af G. Vi definerer en ny delmængde $\mathcal{C}(\mathcal{K}, U) \subseteq \mathcal{P}(G)$, kaldet *$U$-konjugationsmængden* af $\mathcal{K}$, ved

$$\mathcal{C}(\mathcal{K}, U) = \{\, xKx^{-1} \mid K \in \mathcal{K},\ x \in U \,\}.$$

Specielt skriver vi $\mathcal{C}(K, U)$ for $\mathcal{C}(\{K\}, U)$, og $\mathcal{C}(g, U)$ for $\mathcal{C}(\{g\}, U)$. Disse mængder kaldes også *U-konjugationsklassen* af K og g, henholdsvis. Der gælder altså

$$\mathcal{C}(K, U) = \{\, xKx^{-1} \mid x \in U \,\}$$

og

$$\mathcal{C}(g, U) = \{\, xgx^{-1} \mid x \in U \,\}.$$

En U-konjugationsklasse kaldes *triviel*, hvis den kun indeholder ét element.
Vi definerer en operation (regn efter!) $\rho^{\mathcal{K},U}$ af U på $\mathcal{C}(\mathcal{K}, U)$ ved

$$\rho^{\mathcal{K},U}(u)(L) = uLu^{-1}$$

for $u \in U$, $L \in \mathcal{C}(\mathcal{K}, U)$. Da U er en undergruppe af G, er det klart, at $uLu^{-1} \in \mathcal{C}(\mathcal{K}, U)$: Da $L \in \mathcal{C}(\mathcal{K}, U)$, har L formen xKx^{-1} for et passende $x \in U$. Så er $uLu^{-1} = (ux)K(ux)^{-1}$, og $ux \in U$. Analogt indføres operationer $\rho^{K,U}$ af U på $\mathcal{C}(K, U)$ og $\rho^{g,U}$ af U på $\mathcal{C}(g, U)$. Det følger umiddelbart fra definitionerne, at $\rho^{K,U}$ er *transitiv* på $\mathcal{C}(K, U)$ og $\rho^{g,U}$ er *transitiv* på $\mathcal{C}(g, U)$.

(7.42) EKSEMPEL: Igen betragtes undergruppen $U = \langle (1,2) \rangle$ af S_4. Hvis $\mathcal{K} = \{\{(1,3),(1,2)\}, \{2,3,4\}\}$ er

$$\mathcal{C}(\mathcal{K}, U) = \mathcal{K} \cup \{\{(2,3),(1,2)\}, \{(1,3,4)\}\}.$$

(7.43) DEFINITION: Lad K være en delmængde af gruppen G, $g \in G$ og U en undergruppe af G. Vi definerer

$$\begin{aligned} N_U(K) &= \{\, x \in U \mid xKx^{-1} = K \,\} \\ C_U(g) &= \{\, x \in U \mid xgx^{-1} = g \,\} \quad . \\ &= \{\, x \in U \mid xg = gx \,\} \end{aligned}$$

Vi kalder $N_U(K)$ for K's *normalisator* (i U) og $C_U(g)$ for g's *centralisator* (i U).
Man kan indse at $N_U(K) = \mathrm{Stab}_{\rho^{K,U}}(K)$ og $C_U(g) = \mathrm{Stab}_{\rho^{g,U}}(g)$. Overvej! □

(7.44) SÆTNING. *Lad K være en delmængde af gruppen G, $g \in G$ og U en undergruppe af G. Der gælder: $N_U(K)$ og $C_U(g)$ er undergrupper af G og*

$$\begin{aligned} |U : N_U(K)| &= |\mathcal{C}(K, U)| \\ |U : C_U(g)| &= |\mathcal{C}(g, U)|. \end{aligned}$$

U-konjugationsklassen af K, hhv. g, er triviel hvis $U = N_U(K)$, hhv. $U = C_U(g)$.

BEVIS: Følger umiddelbart fra (7.28). □

(7.45) SÆTNING. *Lad K være en undergruppe af G. Der gælder*

$$K \lhd G \iff N_G(K) = G.$$

BEVIS: Øvelse! □

Fra (7.45) ses også: *Hvis K er en undergruppe af G, er $N_G(K)$ den største undergruppe af G, som indeholder K som normal undergruppe.* Overvej!

(7.46) EKSEMPLER: (1) Der gælder $N_{S_n}(A_n) = S_n$ ifølge (7.17) og (7.42).
(2) Lad $g = (1,2,3) \in S_5$. Vi beregner $C_{S_5}(g)$. Antag, at $\rho \in S_5$. Ifølge (7.9)(1) er

$$\rho g \rho^{-1} = (\rho(1), \rho(2), \rho(3)),$$

så $\rho \in C_{S_5}(g) \Leftrightarrow (1,2,3) = (\rho(1), \rho(2), \rho(3)$. Det betyder, at der er 3 muligheder for $\rho(1), \rho(2), \rho(3)$:

$$\begin{aligned} &\rho(1) = 1, \quad \rho(2) = 2, \quad \rho(3) = 3 \quad \text{eller} \\ &\rho(1) = 2, \quad \rho(2) = 3, \quad \rho(3) = 1 \quad \text{eller} \\ &\rho(1) = 3, \quad \rho(2) = 1, \quad \rho(3) = 2 \quad \text{(jfr. (7.4)!)} \end{aligned}$$

(Hvorfor er f.eks. $\rho(1) = 1, \rho(2) = 3, \rho(3) = 2$ ikke mulig??) Derimod har værdierne $\rho(4), \rho(5)$ ingen indflydelse på $\rho g \rho^{-1}$, så der er 2 muligheder for $\rho(4), \rho(5)$:

$$\rho(4) = 4, \rho(5) = 5 \quad \text{eller} \quad \rho(4) = 5, \rho(5) = 4.$$

Derfor er der i alt $6 = 3 \cdot 2$ muligheder for g, så

$$C_{S_5}(g) = \{(1), (1,2,3), (1,3,2), (4,5), (1,2,3)(4,5), (1,3,2)(4,5)\}.$$

Endvidere er

$$C_{A_5}(g) = \{(1), (1,2,3), (1,3,2)\} = \langle g \rangle,$$

idet de andre permutationer i $C_{S_5}(g)$ er ulige.

(3) Lad $K = \langle (1,2,3) \rangle \subseteq S_5$, en undergruppe af orden 3. Vi beregner $N_{S_5}(K)$.

$$\text{Hvis } \rho \in N_{S_5}(K) \text{ må } \rho(1,2,3)\rho^{-1} = (\rho(1), \rho(2), \rho(3)) \in K.$$

Selvfølgelig er muligheden $\rho(1,2,3)\rho^{-1} = (1)$ udelukket, (hvorfor?) Så vi ser nu, at

$$\rho \in N_{S_5}(K) \Leftrightarrow \begin{array}{l} \text{(i)} \quad (\rho(1), \rho(2), \rho(3)) = (1,2,3) \\ \text{eller} \\ \text{(ii)} \quad (\rho(1), \rho(2), \rho(3)) = (1,3,2). \end{array}$$

I (2) ovenfor, bestemte vi alle ρ som opfylder (i). Tilsvarende ses, at netop følgende permutationer opfylder (ii)

$$\{(2,3), (1,3), (1,2), (2,3)(4,5), (1,3)(4,5), (1,2)(4,5)\}$$

således at

$$\begin{aligned} N_{S_5}(K) = \{&(1), (1,2,3), (1,3,2), (4,5), (1,2,3)(4,5), \\ &(1,3,2)(4,5), (1,2), (1,3), (2,3), \\ &(1,2)(4,5), (1,3)(4,5), (2,3)(4,5)\} \end{aligned}$$

en gruppe af orden 12. □

(7.47) ØVELSE: Lad $h = (1,2,3,4) \in S_6$ og $H = \langle h \rangle$. Beregn $C_{S_6}(h)$ og $N_{S_6}(H)$. Det viser sig, at $|C_{S_6}(h)| = 8$ og $|N_{S_6}(H)| = 16$. □

(7.48) ØVELSE: Lad L være et legeme og $G = H(L)$ være som i (6.4).

(1) Lad $(a,b) \in G$. Vis, at $(c,d) \in C_G((a,b)) \iff (a-1)d = (c-1)b$.
(2) Lad A være som i (6.8). Beregn $C_G(g)$ for alle $g \in A$.
(3) Undersøg om $N_G(A) = A$. □

(7.49) DEFINITION: Lad G være en gruppe, U en undergruppe af G. Vi sætter

$$\begin{aligned} C_G(U) &= \{\, g \in G \mid \text{For alle } x \in U \text{ er } g^{-1}xg = x \,\} \\ &= \{\, g \in G \mid \text{For alle } x \in U \text{ er } gx = xg \,\}. \end{aligned}$$

Det er let at se, at $C_G(U)$ er en undergruppe af G. Den består netop af de elementer i G, hvis U-konjugationsklasse er triviel (overvej!). $C_G(U)$ kaldes U's *centralisator* i G. Vi har

$$C_G(U) = \bigcap_{x \in U} C_G(x).$$

Specielt betegnes $C_G(G) = Z(G)$. $Z(G)$ kaldes gruppen G's *centrum* og består netop af de elementer som kommuterer (dvs. er ombyttelige) med alle G's elementer. Løst sagt angiver $Z(G)$ "hvor tæt G er på at være abelsk" – G er jo abelsk netop hvis $Z(G) = G$. □

(7.50) ØVELSE: Lad U være en undergruppe af G. Vis at

$$C_G(U) \triangleleft N_G(U).$$

□

3.4. Klasseligningen.

Lad G være en endelig gruppe. På G har vi indført ækvivalensrelationen $\sim$ ved:

$$a \sim b \iff \exists g \in G : a = gbg^{-1}$$

Vi stiller os selv følgende spørgsmål:

Hvor mange elementer indeholder elementet i a's ækvivalensklasse $\hat{a}$?

Hertil minder vi om, at

$$C_G(a) = \{\, g \in G \mid ga = ag \,\}, \quad a\text{'s centralisator i } G.$$

Husk, at $C_G(a)$ er en undergruppe af G. Bemærk at

$$\begin{aligned} |G : C_G(a)| = 1 &\iff C_G(a) = G \\ &\iff \forall g \in G : ag = ga \\ &\iff a \in Z(G). \end{aligned}$$

Ved optællingsargument fås så "klasseligningen". Helt præcist har vi vist:

(7.51) SÆTNING. *(Klasseligningen for en endelig gruppe). Lad G være en endelig gruppe. Lad $T = \{g_1, g_2, \ldots, g_\ell\}$ være et repræsentantsystem for de ikke-trivielle G-konjugationsklasser. Der gælder*

$$|G| = |Z(G)| + \sum_{i=1}^{\ell} |G : C_G(g_i)|.$$

□

(7.52) EKSEMPLER: Lad $G = S_4 = U$. Der gælder $Z(G) = \{(1)\}$. Som T kan vi vælge

$$T = \{(1,2), (1,2,3), (1,2)(3,4), (1,2,3,4)\}$$

(jfr. (7.9) (1)) Ved hjælp af metoden beskrevet i (7.43) kan vi beregne

$$|C_{S_4}((1,2))| = 4, |C_{S_4}((1,2,3))| = 3, |C_{S_4}((1,2)(3,4))| = 8$$
$$|C_{S_4}((1,2,3,4))| = 4$$

således at klasseligningen for S_4 er

$$\begin{aligned} 24 &= 1 + \frac{24}{4} + \frac{24}{3} + \frac{24}{8} + \frac{24}{4} \\ &= 1 + 6 + 8 + 3 + 6 \end{aligned}$$

□

(7.53) ØVELSE: Bevis påstandene om centralisatorernes orden i (7.51). □

(7.54) ØVELSE: Beregn klasseligningerne for S_3 og for A_4. □

Vi slutter dette afsnit med en standard-anvendelse af (7.50).

(7.55) SÆTNING. *Lad p være et primtal, $a \in \mathbb{N}$. Lad G være en gruppe med $|G| = p^a$. Så er $Z(G) \neq \{1\}$. ("En endelig p-gruppe har et ikke trivielt centrum").*

BEVIS: Betragt klasseligningen for G

$$(*) \qquad |G| = p^a = |Z(G)| + \sum_{i=1}^{\ell} |\, G : C_G(g_i)|$$

For $1 \leq i \leq \ell$ er $|G : C_G(g_i)| = |\mathcal{C}(G, g_i)| > 1$, da g_i's G-konjugationsklasse ifølge antagelsen er ikke-triviel. Vi har så

$$|G : C_G(g_i)| \mid p^a \quad \text{og} \quad |G : C_G(g_i)| \neq 1.$$

Derfor er $p \mid |G : C_G(g_i)|$, altså $|G : C_G(g_i)| \equiv_p 0$. Da også $|G| \equiv_p 0$, fås fra $(*)$, at

$$|Z(G)| \equiv_p 0.$$

Specielt er $|Z(G)| \neq 1$, da $1 \not\equiv_p 0$ □

(7.56) ØVELSE: Antag at den endelige gruppe G har netop 2 konjugationsklasser, således at alle elementer i G (forskellig fra 1) er konjugerede i G. Vis at G er cyklisk af orden 2. □

(7.57) ØVELSE: Lad p være et primtal og G en gruppe af orden p^3. Vis at G mindst har 4 konjugationsklasser. □

4° Direkte produkter.

(7.58) DEFINITION: Lad $G_1, G_2 \ldots, G_n$ være grupper. Vi giver det kartesiske produkt $G = G_1 \times \cdots \times G_n$ en gruppestruktur ved "koordinatvis" multiplikation: Hvis

$$(x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \in G \qquad (\text{så } x_i, y_i \in G_i)$$

sættes

$$(x_1, \ldots, x_n)(y_1, \ldots, y_n) = (x_1 y_1, \ldots, x_n y_n) \in G.$$

Gruppen G kaldes det *ydre direkte produkt* af $G_1, G_2, \ldots, G_n$ og vi skriver $G = G_1 \times \cdots \times G_n$. □

(7.59) DEFINITION: Lad G være en gruppe og $H_1, H_2, \ldots, H_n$ undergrupper af G således at der gælder:

(1) For alle $g \in G$ eksisterer $x_1 \in H_1$, $x_2 \in H_2, \ldots, x_n \in H_n$ så $g = x_1 x_2 \ldots x_n$.
(2) Hvis $x_1, y_1 \in H_1, \ldots, x_n, y_n \in H_n$ og $x_1 x_2 \ldots x_n = y_1 y_2 \ldots y_n$, gælder $x_1 = y_1, x_2 = y_2, \ldots, x_n = y_n$.
(3) Hvis $x_i \in H_i$, $x_j \in H_j$ og $i \neq j$ er $x_i x_j = x_j x_i$.

Så kaldes G et *indre direkte produkt* af (under-)grupperne $H_1, \ldots, H_n$, og vi skriver $G = H_1 \boxtimes H_2 \boxtimes \cdots \boxtimes H_n$. □

(7.60) ØVELSE: Vis, at hvis $G = H_1 \boxtimes H_2 \boxtimes \cdots \boxtimes H_n$, så er $H_i \triangleleft G$ for $i = 1, \ldots, n$. □

(7.61) ØVELSE: Lad $G = S_4 : H_1 = A_4$ og $H_2 = \langle (1,2) \rangle = \{(1), (1,2)\}$. Undersøg, hvilke af betingelserne (1)–(3) i (7.56) er opfyldte. □

Vi forklarer i de næste sætninger, hvorfor ydre og indre produkter er "det samme", pånær isomorfi.

(7.62) SÆTNING. *Lad $G = G_1 \times \cdots \times G_n$ (ydre direkte produkt). For $1 \leq i \leq n$ sættes*

$$H_i = \{(1, \ldots, 1, \underset{\uparrow i\text{'te plads}}{x_i}, 1, \ldots, 1) \mid x_i \in G_i\}.$$

Så er $G = H_1 \boxtimes H_2 \boxtimes \cdots \boxtimes H_n$ og $G_i \simeq H_i$, $1 \leq i \leq n$.

BEVIS: For $x_i \in G_i$ lader vi $\tilde{x}_i = (1, \ldots, 1, x_i, 1, \ldots, 1) \in H_i$. Det er klart, at afbildningen $x_i \to \tilde{x}_i$ er en isomorfi $G_i \to H_i$. Hvis $x_1 \in G_1, x_2 \in G_2, \ldots, x_n \in G_n$ er $\tilde{x}_1 \tilde{x}_2 \ldots \tilde{x}_n = (x_1, x_2, \ldots, x_n)$, ifølge definitionen af multiplikation i $G = G_1 \times \cdots \times G_n$. Derfor ses let (overvej!), at (1), (2) og (3) i (7.56) er opfyldte for $H_1, \ldots, H_n$. □

(7.63) SÆTNING. *Antag, at $G = H_1 \boxtimes H_2 \boxtimes \cdots \boxtimes H_n$ for undergrupper $H_1, \ldots, H_n$ af G. Så er $G \simeq H_1 \times \cdots \times H_n$.*

BEVIS: Vi betragter en afbildning $\varphi : H_1 \times \cdots \times H_n \to G$ givet ved $\varphi(h_1, h_2, \ldots, h_n) = h_1 h_2 \ldots h_n$. Ifølge (7.56)(2) er φ injektiv, og ifølge (7.56)(1) er φ surjektiv. Dermed

er φ bijektiv. Vi viser, at φ også er en homomorfi: Hvis for $1 \leq i \leq n$, $h_i, h_i' \in H_i$ gælder

$$(*) \qquad (h_1 h_2 \dots h_n)(h_1' h_2' \dots h_n') = (h_1 h_1')(h_2 h_2') \dots (h_n h_n').$$

Dette ses ved gentagen anvendelse af (7.56)(3). (Overvej!) Men så er

$$\begin{aligned}
&\varphi((h_1, h_2, \dots, h_n)(h_1', h_2', \dots, h_n')) \\
&\quad = \varphi(h_1 h_1', h_2 h_2', \dots, h_n h_n') && \text{(def. af } \cdot \text{ i } H_1 \times \cdots \times H_n) \\
&\quad = (h_1 h_1')(h_2 h_2') \dots (h_n h_n') && \text{(def. af } \varphi) \\
&\quad = (h_1 h_2 \dots h_n)(h_1' h_2' \dots h_n') && ((*) \text{ ovenfor}) \\
&\quad = \varphi(h_1, \dots, h_n)\varphi(h_1', h_2', \dots, h_n') && \text{(def. af } \varphi).
\end{aligned}$$

□

(7.64) ØVELSE: Antag, at G er (indre eller ydre) direkte produkt af de endelige grupper $G_1, G_2, \dots, G_n$. Vis, at $|G| = |G_1||G_2| \dots |G_n|$. □

Hvis man vil vise, at en gruppe er indre direkte produkt af visse undergrupper, er følgende sætning meget nyttig:

(7.65) SÆTNING. *Lad $H_1, H_2, \dots, H_n$ være* normale *undergrupper af G, således at $G = H_1 H_2 \dots H_n$. Der gælder*

$$\begin{aligned}
&G = H_1 \boxtimes H_2 \boxtimes \cdots \boxtimes H_n \\
&\Updownarrow \\
&\text{For alle } i \in \{1, 2, \dots, n-1\} \text{ gælder } H_{i+1} \cap (H_1 \dots H_i) = \{1\}.
\end{aligned}$$

BEVIS: $\Downarrow$ Antag, at $x \in H_{i+1} \cap (H_1 H_2 \dots H_i)$. Vi skriver $x = x_1 x_2 \dots x_i$, hvor $x_1 \in H_1, x_2 \in H_2, \dots, x_i \in H_i$. Hvis vi sætter $x_{i+1} = x^{-1}, x_{i+2} = \cdots = x_n = 1$, $y_1 = y_2 = \cdots = y_n = 1$, fås $x_1 x_2 \dots x_n = y_1 y_2 \dots y_n = 1$ (hvorfor det?). Så viser (7.56)(2) specielt at $x^{-1} = x_{i+1} = 1$, altså $x = 1$. Derfor er $H_{i+1} \cap (H_1 \dots H_i) = 1$.

$\Uparrow$: Da $G = H_1 H_2 \dots H_n$, er (7.56)(1) opfyldt. Vi viser først (7.56)(3): Lad $x_i \in H_i, x_j \in H_j$, $i \neq j$. Antag, at $i < j$. Så er $H_i \subseteq H_1 H_2 \dots H_{j-1}$, og derfor er $H_i \cap H_j \subseteq (H_1 H_2 \dots H_{j-1}) \cap H_j = \{1\}$, altså $H_i \cap H_j = \{1\}$. Betragt $z = x_i x_j x_i^{-1} x_j^{-1}$. Vi viser $z = 1$, hvoraf følger $x_i x_j = z\, x_j x_i = x_j x_i$. Da $z = x_i(x_j x_i^{-1} x_j^{-1})$ og $x_j x_i^{-1} x_j \in H_i$ fordi $H_i \lhd G$, fås $z \in H_i$. Analogt ses, at da $z = (x_i x_j x_i^{-1}) x_j^{-1}$ er $z \in H_j$. Dermed er $z \in H_i \cap H_j = \{1\}$, altså $z = 1$. Til sidst vises (7.56)(2): Antag, at $x_1 x_2 \dots x_n = y_1 y_2 \dots y_n$. Så er

$$x_n y_n^{-1} = (x_1 x_2 \dots x_{n-1})(y_1 y_2 \dots y_{n-1})^{-1} = (x_1 y_1^{-1})(x_2 y_2^{-1}) \dots (x_{n-1} y_{n-1}^{-1}),$$

idet $x_i y_j = y_j x_i$ for $i \neq j$. (Overvej dette nøje).
Derfor er $x_n y_n^{-1} \in H_n \cap (H_1 H_2 \dots H_{n-1}) = \{1\}$, altså $x_n = y_n$. Dernæst vises analogt, at $x_{n-1} y_{n-1}^{-1} \in H_{n-1} \cap (H_1 \dots H_{n-2}) = \{1\}$, altså $x_{n-1} = y_{n-1}$, osv. □

(7.66) BEMÆRKNING: Beviset for (7.62) (nærmere betegnet beviset for (7.56)(3) i ⇑) viser følgende: Antag, at $H \lhd G, K \lhd G$, $H \cap K = \{1\}$. Hvis $h \in H, k \in K$ gælder $hk = kh$. □

(7.67) DEFINITIONER: Lad X være en delmængde af gruppen G. Så betegner $\langle X \rangle$ den mindste undergruppe af G, som indeholder X. Det er klart, at $\langle X \rangle$ er fællesmængden af alle undergrupper i G, som indeholder X. $\langle X \rangle$ kaldes *den af X frembragte undergruppe* i G. Hvis $X = \{x_1, \dots, x_n\}$ er endelig, skrives også $\langle x_1, x_2, \dots, x_n \rangle$ for $\langle X \rangle$. Specielt er $\langle x \rangle, x \in G$, de cykliske undergrupper af G, (se (6.27)). □

(7.68) ØVELSE: Lad $H = \langle X \rangle$, hvor $X \subseteq G$. Sæt $\mathcal{X} = X \cup X^{-1} = \{y \in G \mid y \in X \text{ eller } y^{-1} \in X\}$. Vis

$$H = \{g \in G \mid \text{Der eksisterer elementer } y_1, y_2, \dots, y_r \in \mathcal{X}, \text{ således at } g = y_1 y_2 \dots y_r\}.$$

□

(7.69) ØVELSE: Som i 1° er S_n den symmetriske gruppe og (i, j) betegner en transposition, (se (7.10)).

(1) Lad $2 \leq i, j \leq n$, $i \neq j$. Vis, at

$$(i, j) = (1, i)(1, j)(1, i).$$

(2) Vis, at $S_n = \langle (1,2), (1,3), \dots, (1,n) \rangle$.

(Benyt (7.10) og (1) til at vise (2).) □

(7.70) ØVELSE: Antag, at $H = \langle x_1, x_2, \dots, x_n \rangle$, og at $a \in \langle x_2, x_3, \dots, x_n \rangle$. Vis, at $H = \langle a x_1, x_2, \dots, x_n \rangle$. □

(7.71) ØVELSE: Lad $G = \langle x \rangle$ være en cyklisk gruppe af orden $|G| = |x| = mn$, hvor m og n er relativ prime (sfd. $(m, n) = 1$), $m, n \in \mathbb{N}$. Vis, at $G = \langle x^n \rangle \boxtimes \langle x^m \rangle$. (Her kan (6.25) og (7.62) måske være nyttige). (Denne øvelse viser at $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$ (som grupper), når $(m, n) = 1$). □

5° Kompositionsrækker.

Sidste del af dette kapitel handler om kompositionsrækker for grupper. Som forberedelse beviser vi et resultatet, kendt som "Zassenhaus' sommerfuglelemma", der kan ses som en generalisering af den 2. isomorfisætning.

(7.72) ØVELSE: Lad U være en undergruppe af G.
Lad X, Y være undergrupper i $N_G(U)$. (Se (7.40)).

(1) Vis (under anvendelse af (6.43)), at UX og UY er undergrupper i G.
(2) Vis, at hvis $X \lhd Y$ så er $UX \lhd UY$.
(3) Vis, at hvis $X \lhd Y$ er $UY = (UX)Y$ og

$$UY \Big/ UX \simeq Y \Big/ UX \cap Y.$$

□

(7.73) SÆTNING. *Lad H, H_1, K, K_1 være undergrupper i G, således at $H_1 \lhd H$, $K_1 \lhd K$. Der gælder:*

(1) *Delmængderne*

$$A = H_1(H \cap K), \quad B = H_1(H \cap K_1)$$
$$C = K_1(H \cap K), \quad D = K_1(H_1 \cap K)$$

er undergrupper i G.
(2) *Der gælder $B \lhd A$ og $D \lhd C$.*
(3) *Der gælder*

$$A \Big/ B \simeq C \Big/ D.$$

BEVIS: (1) At $H_1 \lhd H$ (hhv. $K_1 \lhd K$) betyder ifølge definitionen, at $H \subseteq N_G(H_1)$ (hhv. $K \subseteq N_G(K_1)$). Derfor har vi

$$H \cap K_1 \subseteq H \cap K \subseteq H \subseteq N_G(H_1)$$
$$H_1 \cap K \subseteq H \cap K \subseteq K \subseteq N_G(K_1).$$

Nu viser 4 anvendelser af (7.69)(1), at (1) gælder.
(2)–(3). Hvis vi i (7.69)(2)–(3) sætter

$$U = H_1, \quad X = H_1 \cap K_1, \quad Y = H \cap K,$$

fås $UX = B \lhd A = UY$ (hvorfor er $H \cap K_1 \lhd H \cap K$?), og at

$$A/B \cong H \cap K \Big/ (H \cap K) \bigcap H_1(H \cap K_1).$$

Analogt fås, hvis vi i (7.69)(2)–(3) sætter

$$U = K_1, \quad X = H_1 \cap K, \quad Y = H \cap K$$

at $UX = D \lhd C = UY$ og at

$$C/D \simeq H \cap K \Big/ (H \cap K) \bigcap K_1(H_1 \cap K).$$

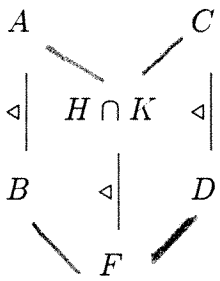
For at afslutte beviset er det tilstrækkeligt at vise, at $(H \cap K) \cap H_1(H \cap K_1) = (H \cap K) \bigcap K_1(H_1 \cap K)$. Vi viser $\subseteq$ og overlader $\supseteq$ (som i øvrigt er åbenlys af symmetrigrunde) til læseren. Lad $a \in (H \cap K) \bigcap H_1(H \cap K_1)$. Skriv $a = h_1 x$, $x \in (H \cap K_1)$, $h_1 \in H_1$. Da $a \in K$ og $x \in K_1 \subseteq K$ er $h_1 = ax^{-1} \in K$ og dermed $h_1 \in H_1 \cap K$. Så er $a = h_1 x \in (H_1 \cap K)K_1 = K_1(H_1 \cap K)$ (da $K_1(H_1 \cap K)$ er en undergruppe). Heraf fås det ønskede. □

(7.74) BEMÆRKNINGER: (1) Beviset for (7.70) er baseret på to anvendelser af den 2. isomorfisætning. Men den 2. isomorfisætning er også "indeholdt" i (7.70): Hvis N, K er undergrupper i G, $N \lhd G$ sættes i (7.70) $H = NK$, $H_1 = N$, $K = K$, $K_1 = 1$. Så er $A = NK$, $B = N$, $C = K$, $D = N \cap K$, og altså $NK/N = A/B \simeq C/D = K/N \cap K$, hvilket er den 2. isomorfisætning!

(2) Sætter vi beviset for (7.70)

$$(H \cap K) \bigcap H_1(H \cap K_1) = F = (H \cap K) \bigcap K_1(H_1 \cap K)$$

fås følgende "diagram af undergrupper", hvor stregerne angiver inklusion:



At $A/B \simeq C/D$ bevises ved at vise $A/B \simeq H \cap K/F$ og $H \cap K/F \simeq C/D$. Diagrammet forklarer måske, hvorfor (7.70) kaldes "sommerfuglelemmaet". □

Det følgende resultat har analoge formuleringer for andre algebraiske strukturer:

(7.75) SÆTNING. *Lad $\varphi : G \to H$ være en gruppe epimorfi. Hvis U er en undergruppe af H sættes*

$$U^* = \varphi^{-1}(U) = \{x \in G \mid \varphi(x) \in U\}.$$

Afbildningen $U \to U^*$ er en bijektion mellem mængden af undergrupper af H og mængden af de undergrupper i G, som indeholder $\ker\varphi$. *Vi har* $U \lhd H \Leftrightarrow U^* \lhd G$.

BEVIS: *Øvelse.* □

(7.76) DEFINITIONER: (1) En kæde $\mathfrak{G}$ af undergrupper

$$\mathfrak{G} : \{1\} = G_r \subseteq G_{r-1} \subseteq \cdots \subseteq G_0 = G,$$

i en gruppe G kaldes en *subnormal række*, hvis $G_i \lhd G_{i-1}$ for $1 \leq i \leq r$. Så kaldes grupperne $F_i = F_i(\mathfrak{G}) = G_{i-1}/G_i$, $1 \leq i \leq r$ for rækkens *faktorer* og $r = \ell(\mathfrak{G})$ for rækkens *længde*. Vi kalder $\ell_*(\mathfrak{G}) = |\{i \mid F_i(\mathfrak{G}) \neq \{\widehat{1}\}\}|$ rækkens *ægte længde*.

(2) Lad os betragte to subnormalrækker for G:

$$\mathfrak{G} : \{1\} = G_r \subseteq G_{r-1} \subseteq \cdots \subseteq G_0 = G$$
$$\mathfrak{H} : \{1\} = H_s \subseteq H_{s-1} \subseteq \cdots \subseteq H_0 = G.$$

$\mathfrak{H}$ kaldes en *forfining* af $\mathfrak{G}$ hvis der for alle i, $0 \leq i \leq r$ findes et j så $H_j = G_i$. En forfining $\mathfrak{H}$ af $\mathfrak{G}$ kaldes *ægte* hvis $\ell_*(\mathfrak{H}) > \ell_*(\mathfrak{G})$. Rækkerne $\mathfrak{G}$ og $\mathfrak{H}$ kaldes ækvivalente hvis $r = \ell(\mathfrak{G}) = \ell(\mathfrak{H}) = s$, og hvis der findes en bijektiv afbildning σ på mængden $\{1, 2, \ldots, r\}$ således at $F_i(\mathfrak{G}) \simeq F_{\sigma(i)}(\mathfrak{H})$ for $1 \leq i \leq r$.

(3) Rækken $\mathfrak{G}$ kaldes en *kompositionsrække* for G hvis $\ell(\mathfrak{G}) = \ell_*(\mathfrak{G})$, og hvis $\mathfrak{G}$ ikke har nogen ægte forfining. Så kaldes $\{F_i(\mathfrak{G}) \mid 1 \leq i \leq r\}$ *kompositionsfaktorer* for G. □

(7.77) EKSEMPLER: (1) $\{1\} \lhd G$ er en subnormalrække i enhver gruppe G. Denne subnormalrække er netop da en kompositionsrække når G er *simpel*, dvs. G har ingen ægte normal undergruppe (= en normal undergruppe $\neq \{1\}, G$).

(2) Lad os i en subnormalrække

$$\mathfrak{G} : \{1\} = G_r \subseteq G_{r-1} \subseteq \cdots \subseteq G_0 = G$$

betragte en faktor $F_i = F_i(\mathfrak{G}) = G_{i-1}/G_i$. Afbildningen $x \to \widehat{x} = xG_i$ er en epimorfi fra $G_{i-1} \to F_i$. Hvis U er en normal undergruppe af F_i er U^* (se (7.72)) en normal undergruppe af G_{i-1} som indeholder G_i. Derfor er

$$\mathfrak{H} : \{1\} = G_r \subseteq \cdots \subseteq G_i \subseteq U^* \subseteq G_{i-1} \subseteq \cdots \subseteq G_0 = G$$

en forfining af $\mathfrak{G}$. Ifølge (7.72) ses, at $\mathfrak{H}$ netop da er en ægte forfining af $\mathfrak{G}$, når U er en ægte normal undergruppe af F_i. Så en subnormalrække er netop da en kompositionsrække, når alle faktorer er simple og $\neq \{1\}$.

(3) Lad $G = \mathbb{Z}_9$, $G_1 = \{\widehat{0}, \widehat{3}, \widehat{6}\} \subseteq Z_9$. Så er $\{\widehat{0}\} \subseteq G_1 \subseteq Z_9$ en kompositionsrække for $(\mathbb{Z}_9, +)$. Faktorerne er to cykliske grupper af orden 3.

(4) Ifølge (2) er det let at se at enhver *endelig* gruppe har en kompositionsrække.

(5) Derimod har $(\mathbb{Z},+)$ ingen kompositionsrække, idet $(\mathbb{Z},+)$ ikke har nogen simpel undergruppe $\neq \{0\}$. (Den sidste faktor i en kompositionsrække *er* en simpel undergruppe, hvorfor?) Undergrupperne af $(\mathbb{Z},+)$ $(\neq \{0\})$ er $n\mathbb{Z}$, $n \in \mathbb{N}$. Men $\{0\} \neq 2n\mathbb{Z} \triangleleft n\mathbb{Z}$ er en ægte normal undergruppe i $n\mathbb{Z}$.

(6) (Anvender 1° i Kapitel 7). I den symmetriske gruppe S_4 betragtes $V = \{(1),(12)(34),(13)(24),(14)(23)\}$. Det er let at se, at V er en undergruppe i S_4 og ved anvendelse af (7.9)(1) ses let, at $V \triangleleft S_4$. (V kaldes "Kleins firegruppe"). Så er følgende en kompositionsrække for S_4

$$\{(1)\} \subset \{(1),(12)(34)\} \subset V \subset A_4 \subset S_4.$$

Faktorerne er (isomorfe til) $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2$. □

Vi vil nu vise, at to kompositionsrækker for en gruppe er ækvivalente, således at kompositionsfaktorerne er entydige på nær isomorfi (hvis de findes). Dette er et specielt tilfælde af et stærkere resultat:

(7.78) SÆTNING. (Schreier) *To subnormalrækker for G har forfininger, der er ækvivalente.*

BEVIS: Lad

$$\mathfrak{G} : \{1\} = G_r \subseteq G_{r-1} \subseteq \cdots \subseteq G_0 = G$$
$$\mathfrak{H} : \{1\} = H_s \subseteq H_{s-1} \subseteq \cdots \subseteq H_0 = G$$

være subnormalrækker for G. Vi har altså

$$G_i \triangleleft G_{i-1} \quad \text{for} \quad 1 \leq i \leq r$$
$$H_{j+1} \triangleleft H_j \quad \text{for} \quad 0 \leq j \leq s-1.$$

For fast valgt i, j, $1 \leq i \leq r$, $0 \leq j \leq s-1$ anvender vi som sommerfuglelemmaet på

$$H = G_{i-1}, \quad H_1 = G_i$$
$$K = H_j, \quad K_1 = H_{j+1}.$$

I notationen fra (6.52) fås

$$(\circ)\begin{cases} A &= G_i(G_{i-1} \cap H_j), \quad B = G_i(G_{i-1} \cap H_{j+1}) \\ C &= H_{j+1}(G_{i-1} \cap H_j), \quad D = H_{j+1}(G_i \cap H_j) \end{cases}$$

Hvis vi derfor sætter

$$G_{i,j} = G_i(G_{i-1} \cap H_j) \quad \text{for} \quad 1 \leq i \leq r, 0 \leq j \leq s$$

og

$$H_{i,j} = H_j(G_i \cap H_{j-1}) \quad \text{for} \quad 0 \leq i \leq r, 1 \leq j \leq s$$

får vi fra (o), at

$$G_{i,j}\Big/G_{i,j+1} \simeq H_{i-1,j+1}\Big/H_{i,j+1} \quad \text{for} \quad \begin{matrix} 1 \le i \le r \\ 0 \le j \le s-1 \end{matrix}$$

i alt $r \cdot s$ isomorfier. Disse isomorfier viser at følgende normalrækker i G er ækvivalente

$$\mathfrak{G}_1 \begin{cases} (G_r =)G_{r,s} = 1 \lhd G_{r,s-1} \lhd \cdots \lhd G_{r,1} \\ \lhd (G_{r-1} =)G_{r-1,s} \lhd G_{r-1,s-1} \lhd \cdots \lhd G_{r-1,1} \\ \lhd (G_{r-2} =)G_{r-2,s} \lhd G_{r-2,s-1} \lhd \cdots \lhd \\ \vdots \\ \lhd (G_1 =)G_{1,s} \lhd G_{1,s-1} \lhd \cdots \lhd G_{1,1} \lhd G_{1,0} = G \end{cases}$$

og

$$\mathfrak{H}_1 \begin{cases} (H_s =)H_{r,s} \lhd H_{r-1,s} \lhd \cdots \lhd H_{1,s} \\ \lhd (H_{s-1} =)H_{r,s-1} \lhd H_{r-1,s-1} \lhd \cdots \lhd H_{1,s-1} \\ \vdots \\ \lhd (H_1 =)H_{r,1} \lhd H_{r-1,1} \lhd \cdots \lhd H_{1,1} \lhd H_{0,1} = G \end{cases}$$

idet vi bemærker, at

$$\begin{aligned} G_{i0} = G_{i-1} = G_{i-1s} \quad &\text{for} \quad 2 \le i \le r \\ H_{0j} = H_{j-1} = H_{rj-1} \quad &\text{for} \quad 2 \le j \le s. \end{aligned}$$

Men det er klart, at $\mathfrak{G}_1$ forfiner $\mathfrak{G}$ og $\mathfrak{H}_1$ forfiner $\mathfrak{H}$. □

(7.79) SÆTNING. *To kompositionsrækker for G er ækvivalente.*

BEVIS: Følger fra (7.75). Overvej dette! □

(7.80) ØVELSE: Angiv samtlige kompositionsrækker for en cyklisk gruppe af orden 6. □

(7.81) ØVELSE: Lad G være en cyklisk gruppe af orden $p_1^{a_1} \dots p_r^{a_r}$, hvor p_i'erne er primtal. Vis, at enhver kompositionsrække for G har længde $a_1 + a_2 + \cdots + a_r$. □

(I opgaverne (7.77)–(7.78) kan (6.28) være nyttig. Hvilke cykliske grupper er simple?)

(7.82) ØVELSE: En undergruppe U i G kaldes *subnormal* hvis den indgår i en subnormalrække for G. Dette betyder, at der findes en subnormalrække for G på formen

$$\mathfrak{G}_U : \{1\} = G_r \subseteq G_{r-1} = U \subseteq G_{r-2} \subseteq \cdots \subseteq G_0 = G.$$

Vis, at hvis U og V er subnormale undergrupper, så er også $U \cap V$ subnormal. (Anvend beviset for (7.75) på $\mathfrak{G}_U$ og på en tilsvarende subnormalrække $\mathfrak{G}_V$ med V som næstsidste led.) □

Kapitel 8. Moduler.

Abelske grupper og vektorrum er specielle eksempler på *moduler*. Et hovedtema i dette kapitel vil være overvejelser vedrørende udvidelse af vigtige sætninger om vektorrum, kendte fra den lineære algebra.

Man kan opfatte modulteorien som en (meget vigtig) gren af ringteorien og flere resultater i dette kapitel vil illustrere den nøje sammenhæng mellem (strukturen af) en ring og dens moduler. En modul er en abelsk gruppe, hvorpå en ring R opererer som en ring af endomorfier. Dette er i analogi med Kapitel 7, 2°, hvor en gruppe opererede som permutationsgruppe på en mængde.

Vi starter med at se på *endomorfiringe*. I dette kapitel vil kompositionen i en abelsk gruppe M blive skrevet additivt ($(a,b) \mapsto a+b$). Tilsvarende betegnes den "m'te potens" af $x \in M$ som mx (i stedet for x^m).

(8.1) DEFINITION: Lad $(M,+)$ være en abelsk gruppe. En *endomorfi* af M er en (gruppe)homomorfi $\varphi : M \to M$. Vi definerer kompositioner $+,\cdot$ på mængden $\mathrm{End}(M)$, således at $(\mathrm{End}(M),+,\cdot)$ er en ring (med 1-element), *endomorfiringen* af M. Hvis $\varphi,\psi \in \mathrm{End}(M)$, sættes $(\varphi+\psi)(x) = \varphi(x)+\psi(x)$ og $(\varphi\cdot\psi)(x) = \varphi(\psi(x))$ (for $x \in M$). □

Lad os se på et par eksempler:

(8.2) EKSEMPLER: (1) Lad $M = \mathbb{Z}$. Betragt $\varphi \in \mathrm{End}(\mathbb{Z})$. Hvis $\varphi(1) = n \in \mathbb{Z}$ må $\varphi(x) = xn$ for alle $x \in \mathbb{Z}$. (Overvej!) Det betyder, at værdien $\varphi(1)$ alene bestemmer φ fuldstændigt. På den anden side, hvis $n \in \mathbb{Z}$ defineres $\mu(n) \in \mathrm{End}(\mathbb{Z})$ ved $\mu(n)(x) = xn$. Da $\mu(n+m) = \mu(n)+\mu(m)$, $\mu(nm) = \mu(n)\cdot\mu(m)$ for alle $n,m \in \mathbb{Z}$ (f.eks. $\mu(nm)(x) = xnm = (xm)n = \mu(n)(\mu(m)(x))$ er $\mu : \mathbb{Z} \to \mathrm{End}(\mathbb{Z})$ en homomorfi. Det er klart, at μ er injektiv ($\mu(n) = 0 \in \mathrm{End}(\mathbb{Z}) \Rightarrow 0 = \mu(n)(1) = n$), og ifølge det ovenstående er μ surjektiv; altså som *ring* er $\mathbb{Z}$ isomorf til endomorfiringen for den abelske gruppe $(\mathbb{Z},+)$.

(2) Hvis $M = \mathbb{Z}_m$, $m \in \mathbb{N}$, ses analogt til (1), at restklasseringen $\mathbb{Z}_m$ er isomorf til endomorfiringen af $(\mathbb{Z}_m,+)$.

(3) Lad $M = \mathbb{Z}\times\mathbb{Z} = \mathbb{Z}^2$. Vi viser, at $\mathrm{End}(M) \simeq \mathbb{Z}_2^2$, ringen af 2×2 matricer over $\mathbb{Z}$ (se Kapitel 3). Betragt $\varphi \in \mathrm{End}(\mathbb{Z}^2)$. Antag, at $\varphi((1,0)) = (a_{11},a_{21})$, $\varphi((0,1)) = (a_{12},a_{22})$. Så er for $(x_1,x_2) \in \mathbb{Z}^2$

$$(*)\qquad \begin{aligned}\varphi(x_1,x_2) &= \varphi(x_1(1,0)+x_2(0,1)) = \varphi(x_1(1,0))+\varphi(x_2(0,1))\\ &= x_1\varphi(1,0)+x_2\varphi(0,1) = (a_{11}x_1+a_{12}x_2, a_{21}x_1+a_{22}x_2)\end{aligned}$$

Denne formel minder måske læseren om en matrixmultiplikation, og det er det selvfølgelig også. Faktisk er en lignende beregning gennemført i den lineære algebra. Hvis vi skriver et element $(x_1,x_2) \in \mathbb{Z}^2$ på søjleform som $\begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$ og sætter $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$

kan $(*)$ skrives som

$$\varphi \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = A \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.$$

I analogi med (1) kan vi definere en isomorfi $\mu : \mathbb{Z}_2^2 \to \mathrm{End}(\mathbb{Z}^2)$ ved at lade

$$\mu(A) \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = A \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}.$$

□

(8.3) ØVELSE: Resultatet i (8.2)(3) kan formuleres som $\mathrm{End}(\mathbb{Z}^2) \simeq (\mathrm{End}(\mathbb{Z}))_2^2$, da jo ifølge (8.2)(1) $\mathrm{End}(\mathbb{Z}) \simeq \mathbb{Z}$. I denne øvelse generaliseres dette resultat. Lad M være en abelsk gruppe. Betragt gruppehomomorfier

$$\iota_1, \iota_2 : M \to M^2, \quad \pi_1, \pi_2 : M^2 \to M$$

defineret ved

$$\iota_1(x) = (x, 0), \iota_2(x) = (0, x), \pi_1(x_1, x_2) = x_1, \pi_2(x_1, x_2) = x_2.$$

Så kan man ved hjælp af et $\varphi \in \mathrm{End}(M^2)$ definere $\varphi_{ij} \in \mathrm{End}(M)$, $i, j \in \{1, 2\}$ ved $\varphi_{ij} = \pi_i \circ \varphi \circ \iota_j$

$$\begin{array}{ccc} M & \xrightarrow[\varphi_{ij}]{} & M \\ \downarrow{\scriptstyle \iota_j} & & \uparrow{\scriptstyle \pi_i} \\ M \times M & \xrightarrow[\varphi]{} & M \times M \end{array}$$

Fra hvert $\varphi \in \mathrm{End}(M^2)$ fås altså 4 φ_{ij}'er i $\mathrm{End}(M)$. Vis:

(1) Hvis $\varphi(x_1, x_2) = (y_1, y_2)$ så er

$$y_1 = \varphi_{11}(x_1) + \varphi_{12}(x_2), y_2 = \varphi_{21}(x_1) + \varphi_{22}(x_2)$$

(2) Afbildningen $\mu : \mathrm{End}(M^2) \to (\mathrm{End}(M))_2^2$ givet ved

$$\mu(\varphi) = \begin{bmatrix} \varphi_{11} & \varphi_{12} \\ \varphi_{21} & \varphi_{22} \end{bmatrix}$$

er en ringhomomorfi.

(3) Er μ en isomorfi?

□

Det ovenstående skulle demonstrere, at der er muligheder for at udvide begreber og metoder fra den lineære algebra, så de bliver anvendelige i andre situationer.

Lad os nu se på ringhomomorfier mellem generelle ringe og endomorfiringe af abelske gruppper.

Betragt en ring R, en abelsk gruppe M og en ringhomomorfi

$$\mu : R \to \mathrm{End}(M).$$

Ved hjælp af μ kan vi definere en afbildning

$$R \times M \to M \qquad \begin{array}{c}(r,x) \to \underbrace{r \cdot x} \\ \uparrow\uparrow \qquad\quad \uparrow \\ RM \qquad\quad M\end{array}$$

på følgende måde

$$r \cdot x = \mu(r)(x).$$

At $\mu(r)$ er en endomorfi på M betyder

$$\underline{r \cdot (x+y)} = \mu(r)(x+y) = \mu(r)(x) + \mu(r)(y) = \underline{r \cdot x + r \cdot y}$$

(for alle $r \in R$, $x, y \in M$). At $\mu(r+s) = \mu(r) + \mu(s)$ betyder

$$\underline{(r+s) \cdot x} = \mu(r+s)(x) = \mu(r)(x) + \mu(s)(x) = \underline{r \cdot x + s \cdot x}$$

(for alle $r, s \in R$, $x \in M$). Tilsvarende fås,

$$\underline{r \cdot (s \cdot x)} = \mu(r)(\mu(s)x)) = (\mu(r)\mu(s))(x) = \mu(rs)(x) = \underline{(rs) \cdot x}$$

(for alle $r, s \in R$, $x \in M$), da $\mu(r)\mu(s) = \mu(rs)$.

Idet vi igen udelader "multiplikationstegnet" har vi altså

$$\left.\begin{array}{ll}\text{[MD1]} & r(x+y) = rx + ry \\ \text{[MD2]} & (r+s)x = rx + sx \\ \text{[MA]} & r(sx) = (rs)x\end{array}\right\} \text{for alle } r, x \in R, x, y \in M$$

Dette leder op til definitionen af en *R-modul*:

(8.4) DEFINITION: Lad R være en ring. En *R-modul* er en abelsk gruppe M og en afbildning

$$R \times M \to M \qquad (r,m) \mapsto rm$$

(en såkaldt ydre komposition på M) der opfylder betingelserne [MD1], [MD2], [MA] ovenfor. Hvis yderligere R har et 1-element og der gælder

$$[\text{MU}] \qquad 1x = x \quad \text{for alle } x \in M$$

kaldes modulen M *unitær*. □

Det ovenstående viser, at enhver ringhomomorfi $R \to \text{End}(M)$ giver en R-modul struktur på M, og omvendt giver en R-modul struktur på M en ringhomomorfi $\mu : R \to \text{End}(M)$ ved at *definere* $\mu(r)(x) = rx$.

(8.5) EKSEMPLER: (1) Enhver abelsk gruppe M er en unitær $\mathbb{Z}$-modul. Hvis $x \in M$, $r \in \mathbb{Z}$, er rx defineret som den r'te potens af x (som i begyndelsen af dette kapitel). Betingelsen [MD1] er så oplagt, da gruppen er abelsk, og betingelserne [MD2], [MA] er netop potensreglerne, der er anført i (6.18), omskrevet i den additive notation, f.eks. $(a^{n+m} = a^n \cdot a^m \leftrightarrow (n+m)a = na + ma)$.

(2) En ring R er en modul over sig selv, hvis vi lader modulstrukturen $R \times R \to R$ stemme overens med den sædvanlige multiplikation i R. Så følger [MD1] og [MD2] fra de distributive love [RD] for R og [MA] fra den associative lov [RMA] for multiplikation. ([MU] er [RMN]).

(3) Hvis L er et legeme er en unitær L-modul det samme som et L-vektorrum. (Læseren opfordres til at overveje dette nøje!)

(4) En abelsk gruppe M er en $\text{End}(M)$-modul og selvfølgelig også en R-modul for enhver delring R af $\text{End}(M)$.

(5) Hvis M er en R-modul og S er en delring af R, er M (ved indskrænkning af den ydre komposition) også en S-modul.

(6) Hvis M er en R-modul og $\varphi : S \to R$ en ringhomomorfi kan man gøre R til en S-modul ved at definere $sm = \varphi(s)m$. ($\varphi(s) \in R$, så da M er en R-modul, er $\varphi(s)m \in M$!) Lad os f.eks. verificere [MD2]. For $s, t \in S$, $x, y \in M$ er

$$\begin{aligned}
(s+t)x &= \varphi(s+t)x && \text{(definition)} \\
&= (\varphi(s) + \varphi(t))x && (\varphi \text{ homomorfi}) \\
&= \varphi(s)x + \varphi(t)x && (\text{[MD2] i } R\text{-modulen } M) \\
&= sx + tx && \text{(Definition)}
\end{aligned}$$

(Selvfølgelig er (5) et specielt tilfælde af (6), ikke?) □

(Vi har valgt ovenfor at betragte hvad man kan kalde *venstre*-moduler for R. Man kunne selvfølgelig også betragte *højre*-moduler for R. En R højre-modul er en abelsk gruppe M og en afbildning $M \times R \to M$ således at

$$\left.\begin{array}{ll}
[\text{MD1}]^* & (x+y)r = xr + yr \\
[\text{MD2}]^* & x(r+s) = xr + xs \\
[\text{MA}]^* & (xr)s = x(rs) \\
([\text{MU}]^* & x1 = x)
\end{array}\right\} \text{for alle } r, s \in R, x, y \in M.$$

Det er klart, at studiet af venstre- eller højre-moduler er ækvivalente. Vi har valgt venstre-moduler, fordi de passer bedre med vor notation for afbildninger).

(8.6) ØVELSE: Vis, at hvis R er en kommutativ ring og M er en (venstre-)R-modul, kan man gøre M til en højre R-modul ved at sætte

$$xr = rx \quad \text{for} \quad r \in R, x \in M.$$

Hvorfor skal R være kommutativ? □

(8.7) DEFINITION: Lad M være en R-modul. En undergruppe N af M kaldes *undermodul*, hvis

$$rx \in N \quad \text{for alle} \quad r \in R, x \in N.$$

□

(8.8) EKSEMPLER: Vi henviser i det følgende til de enkelte punkter i Eksemplerne (8.5).

(1) $\mathbb{Z}$-undermodulerne af en abelsk gruppe er netop dens undergrupper.

(2) R-undermodulerne af R (betragtet som R-modul) er netop venstreidealerne i R. (Overvej!)

(3) Her svarer undermoduler til underrum af vektorrummet.

(4) I denne situation kan man ikke generelt sige noget om undermodulerne.

(5)-(6) Her er R-undermoduler også S-undermoduler, men det omvendte gælder ikke (Eksempel?) □

Før vi går videre bør vi nævne nogle regneregler for R-moduler, hvis bevis overlades til læseren. (Når M er en R-modul, og $r \in R$, er altså "multiplikation med r" en homomorfi $M \to M$, så f.eks. er (6.35) relevant.)

(8.9) SÆTNING. *Lad M være en R-modul, $r \in R, x \in M$. Der gælder*

$$r0 = 0, \quad 0x = 0, \quad r(-x) = -rx = (-r)x \qquad \square$$

(Fra (8.9) fås også regler som $r(x - y) = rx - ry$, etc.)

(8.10) ØVELSE: Lad M være en R-modul. Sæt

$$M_0 = \{x \in M \mid \text{For alle } r \in R \text{ gælder } rx = 0\}$$

Vis, at M_0 er en undermodul af M. □

(8.11) ØVELSE: Lad M være en R-modul, R en *integritetsring*. Sæt

$$M_{\text{tor}} = \{x \in M \mid \text{Der findes } r \in R \setminus \{0\} \text{ så } rx = 0\}$$

(1) Vis, at M_{tor} er en undermodul af M.
(2) Beskriv M_{tor} i tilfældet hvor $R = \mathbb{Z}$ (så M er "bare" en abelsk gruppe.) □

(8.12) ØVELSE: Lad M være en R-modul, $x \in M$. Sæt

$$\text{Ann}(x) = \{r \in R \mid rx = 0\} \qquad \text{(Annihilatoren af } x\text{)}$$

Vis, at $\text{Ann}(x)$ er et venstreideal i R. □

(8.13) SÆTNING. *Lad N_1, N_2 være undermoduler af R-modulen M. Så er undergrupperne $N_1 \cap N_2$ og $N_1 + N_2$ af M også undermoduler.*

BEVIS: *Øvelse.* □

I det følgende vil vi gøre følgende antagelse. Vi betragter kun ringe med 1-element og alle moduler antages at være unitære ([MU]). Dette er gjort for at udelukke tilfælde, der er uinteressante.

(8.14) DEFINITIONER: Lad X være en delmængde af R-modulen M. Vi definerer $\text{span}(X)$, *den af X frembragte undermodul af M*, som den mindste undermodul af M, der indeholder X. I analogi med den lineære algebra (se også (3.9)) kan $\text{span}(X)$ beskrives på følgende måde:

$$\text{span}(X) = \left\{ x \in M \,\middle|\, \begin{array}{c} \text{Der findes } m \in \mathbb{N}, r_1, r_2, \ldots, r_m \in R \\ \text{og } x_1, \ldots, x_m \in X \text{ så } x = \sum_{i=1}^{m} r_i x_i \end{array} \right\}$$

En *linearkombination* af $x_1, \ldots, x_m \in M$ er et element $x \in M$ på formen $r_1 x_1 + \cdots + r_m x_m$, $(r_i \in R)$. (Så $\text{span}(X)$ er mængden af linearkombinationer af elementer i X). Modulen M kaldes *endelig frembragt*, hvis $M = \text{span}(X)$, hvor X er endelig. Vi skriver også $M = \text{span}(x_1, \ldots, x_m)$, hvis $X = \{x_1, \ldots, x_m\}$. M er *cyklisk*, hvis $M = \text{span}(x)$ for et $x \in M$. Delmængden $X \subseteq M$ kaldes *lineær uafhængig*, hvis 0 kun kan fremstilles *trivielt* som linearkombinationer af elementer i X ($r_1 x_1 + \cdots + r_m x_m = 0, r_i \in R, x_i \in X \Rightarrow r_1 = \cdots = r_m = 0$). Som i den lineære algebra er det klart, at X er lineær uafhængig, hvis og kun hvis ethvert element i $\text{span}(X)$ har netop én fremstilling som linearkombination af elementerne i X. Endelig kaldes X en *basis*

for M, hvis X er lineær uafhængig og $M = \text{span}(X)$. M kaldes *fri*, hvis M har en basis. □

(8.15) EKSEMPLER: (1) I $\mathbb{Z}^2$ danner $X = \{(1,0),(0,1)\}$ en basis for $\mathbb{Z}^2$ (som $\mathbb{Z}$-modul). Mængden $Y = \{(2,0),(0,1)\}$ er lineær uafhængig, men ingen basis, da $\text{span}(Y) = \{(x,y) \in \mathbb{Z}^2 \mid x \equiv_2 0\}$, (så $(1,0) \notin \text{span}(Y)$).

(2) Lad os betragte $\mathbb{Z}^2$ som $\text{End}(\mathbb{Z}^2)$-modul. Hvis $\mu : \mathbb{Z}_2^2 \to \text{End}(\mathbb{Z}^2)$ er som i (8.2)(3), og $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \in \mathbb{Z}_2^2$ er $\mu(A)(1,0) = (a_{11}, a_{21})$. Dette viser, at $\mathbb{Z}^2$ er en cyklisk $\text{End}(\mathbb{Z}^2)$-modul frembragt af $(1,0)$. Men $X = \{(1,0)\}$ er ingen basis. Hvis f.eks. $\varphi = \mu\left(\begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}\right)$ er $\varphi x = 0$, men $\varphi \neq 0$. Faktisk vil *intet* element i $\mathbb{Z}^2$ kunne indgå i en basis, idet det har en annihilator (se (8.12)) som er $\neq \{0\}$: Hvis $(x_1, x_2) \in \mathbb{Z}^2$ er ifølge (8.2)(3) f.eks. $\mu\left(\begin{bmatrix} x_2 & -x_1 \\ x_2 & -x_1 \end{bmatrix}\right) \in \text{Ann}((x_1, x_2))$. Som $\text{End}(\mathbb{Z}^2)$-modul er $\mathbb{Z}^2$ cyklisk, men har ingen basis. Der findes selvfølgelig enklere eksempler på dette fænomen. □

Disse eksempler understreger forskellen mellem moduler og vektorrum. En række fundamentale sætninger for vektorrum gælder *ikke* for moduler.

(8.16) ØVELSE: Giv 2–3 eksempler på sådanne sætninger. □

(8.17) DEFINITION: Lad M, N være R-moduler. En afbildning $\varphi : M \to N$ kaldes (*modul-*)*homomorfi* hvis der gælder

$$\left.\begin{aligned} \varphi(x+y) &= \varphi(x) + \varphi(y) \\ \varphi(rx) &= r\varphi(x) \end{aligned}\right\} \text{for } x, y \in M, r \in R$$

I analogi med tidligere defineres *monomorfi*, *epimorfi*, *isomorfi*, *endomorfi* for R-moduler. Hvis $\varphi : M \to N$ er en (modul-)homomorfi sættes

$$\ker\varphi = \{x \in M \mid \varphi(x) = 0\} \qquad \text{(kernen af } \varphi\text{)}$$
$$\varphi(M) = \{y \in N \mid \text{Der findes } x \in M \text{ så } \varphi(x) = y\}$$

□

(8.18) SÆTNING. *Hvis $\varphi : M \to N$ er en R-modul homomorfi, er $\ker\varphi$ en undermodul af M og $\varphi(M)$ er en undermodul af N.*

BEVIS: Vi viser kun den sidste påstand. Lad $y_1, y_2 \in \varphi(M), r \in R$. Vælg $x_1, x_2 \in M$ med $\varphi(x_1) = y, \varphi(x_2) = y_2$. Vi viser $y_1 + y_2 \in \varphi(M)$, $ry_1 \in \varphi(M)$: $y_1 + y_2 = \varphi(x_1) + \varphi(x_2) = \varphi(x_1 + x_2)$, $ry_1 = r\varphi(x_1) = \varphi(rx_1)$. □

(8.19) EKSEMPLER: (1) Lad $x \in M$, M R-modul. Hvis vi betragter R som R-modul, er afbildningen $r \mapsto rx$ en (modul-)homomorfi. Kernen er $\mathrm{Ann}(x)$, så (8.12) kan ses som specielt tilfælde af (8.18), jvf. (8.8)(2).

(2) Gruppehomomorfier mellem abelske grupper er også $\mathbb{Z}$-modul-homomorfier, og omvendt. Lineære afbildninger mellem L-vektorrum, L legeme, er netop L-modul-homomorfier. □

(8.20) SÆTNING. *Lad N være en undermodul af R-moduler M. Betragt faktorgruppen M/N. For $\widehat{x}, \widehat{y} \in M/N$, $r \in R$ defineres*

$$\widehat{x} + \widehat{y} = \widehat{x+y}, \quad r\widehat{x} = \widehat{rx}$$

Disse kompositioner er veldefinerede og gør M/N til en R-modul, faktormodulen af M moduler N.

BEVIS: At kompositionen $+$ er veldefineret skyldes (6.39). Vi skal vise, at hvis $x \equiv_N y$ så er $rx \equiv_N ry$. Men $x \equiv_N y \Rightarrow x - y \in N \Rightarrow r(x-y) \in N$ (da N undermodul) $\Rightarrow rx - ry \in N \Rightarrow rx \equiv_N ry$. Modulaksiomerne [MD1], [MD2], [MA] for M/N følger fra det tilsvarende aksiom for M. F.eks. er

$$r(s\widehat{x}) = r(\widehat{sx}) = \widehat{r(sx)} = \widehat{(rs)x} = (rs)\widehat{x}.$$

□

I fuldstændig analogi til §6 kan vi vise 3 isomorfisætninger for R-moduler. Disse sætninger har altså de tilsvarende sætninger for vektorrum som specielt tilfælde! (Se (3.25)). Læseren opfordres til på egen hånd at opskrive detaljerede beviser.

(8.21) SÆTNING. *(1. isomorfisætning) Lad $\varphi : M \to N$ være en (modul-)homomorfi. Der gælder*

$$M/\ker\varphi \simeq \varphi(M). \qquad \square$$

(8.22) SÆTNING. *(2. isomorfisætning) Lad N og K være undermoduler af R-modulen M. Der gælder*

$$(N+K)/N \simeq K/K \cap N. \qquad \square$$

(8.23) SÆTNING. *(3. isomorfisætning) Lad N, K være undermoduler af R-modulen M, hvor $K \subseteq N$. Der gælder*

$$M/N \simeq (M/K)\Big/(N/K). \qquad \square$$

For $n \in \mathbb{N}$ og R en ring, betragtes $R^n = \underbrace{R \times \cdots \times R}_{n}$ som en R-modul ved koordinatvis addition og ved den ydre komposition $r(r_1, r_2, \ldots, r_n) = (rr_1, \ldots, rr_n)$, $r \in R$, $(r_1, \ldots, r_n) \in R^n$.

(8.24) SÆTNING. *Lad R-modulen M være endelig frembragt: $M = \operatorname{span}(x_1, x_2, \ldots, x_n)$. Så er afbildningen $\varphi : R^n \to M$ defineret ved $\varphi(r_1, \ldots, r_n) = r_1x_1 + r_2x_2 + \cdots + r_nx_n$ en (R-modul-)epimorfi. Hvis $X = \{x_1, \ldots, x_n\}$ er lineær uafhængig, er φ en isomorfi, så $R^n \simeq M$.*

BEVIS: Det er let at se, at φ er en homomorfi. F.eks.:

$$\begin{aligned}
&\varphi((r_1, \ldots, r_n) + (s_1, \ldots, s_n)) = \varphi(r_1 + s_1, \ldots, r_n + s_n) \\
&\quad = (r_1 + s_1)x_1 + \cdots + (r_n + s_n)x_n && \text{(definition af } \varphi) \\
&\quad = r_1x_1 + s_1x_1 + \cdots + r_nx_n + s_nx_n && \text{([MD2])} \\
&\quad = (r_1x_1 + \cdots + r_nx_n) + (s_1x_1 + \cdots + s_nx_n) && \text{(+ er kommutativ)} \\
&\quad = \varphi(r_1, \ldots, r_n) + \varphi(s_1, \ldots, s_n) && \text{(definition af } \varphi)
\end{aligned}$$

φ er *surjektiv*: Lad $x \in M$. Da $M = \operatorname{span}(X)$ findes $r_1, \ldots, r_n \in R$ så $x = r_1x_1 + \cdots + r_nx_n$. Men så er $x = \varphi(r_1, \ldots, r_n)$.

Lad X være lineær uafhængig. Så er $\ker\varphi = 0$ og derfor φ også injektiv: Hvis $(r_1, \ldots, r_n) \in \ker\varphi$ er $0 = \varphi(r_1, \ldots, r_n) = r_1x_1 + \cdots + r_nx_n$. Men så må $r_1 = \cdots = r_n = 0$, altså $(r_1, \ldots, r_n) = 0$. □

Man kan nu spørge om følgende: *Antag at en fri R-modul M har 2 baser X, Y, som begge er endelige. Gælder der $|X| = |Y|$?* Ifølge (8.24) er dette spørgsmål ækvivalent til det følgende: *Lad $n, m \in \mathbf{N}$. Hvis $R^n \simeq R^m$ (som R-moduler), er så $n = m$?* Vi vil vise, at svaret er *ja*, hvis R er kommutativ.

Som forberedelse hertil må vi først kikke på en "udvidelse" af determinantbegrebet, der er kendt fra den lineære algebra. Den tyske matematiker K. Weierstrass opdagede, at man kan karakterisere determinanten af en $n \times n$-matrix entydigt ved visse formelle egenskaber. (I HBF findes en variation af dette i (18.3.(1)). Disse egenskaber inkluderer altid

(1) En linearitetsbetingelse mht. søjler eller rækker (se f.eks. HBF 18.3.1 (b) og (c) samt 18.4.4).

(2) En normeringsbetingelse: "Determinanten" af enhedsmatricen

$$E_n = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$$ er 1 (f.eks. HBF 18.3.1 (a)).

Desuden er der en yderligere betingelse (3), der afhænger af, hvor vidtgående (1) er. (I HBF er det "søjleudviklingsreglen" 18.3. (1)(d). Men hvis man forstærker (1), kan (3) erstattes med en betingelse, der forlanger at "determinanten" ændrer fortegn når man ombytter 2 søjler/rækker. Under alle omstændigheder er det altid sådan, at de formelle egenskaber (1)–(3) kan formuleres for en funktion

$$d_n : R_n^n \to R$$

når R er en vilkårlig kommutativ ring med 1-element. (R_n^n er altså ringen af $n \times n$-matricer med koefficienter fra ringen R.) Ved *udelukkende* at benytte egenskaberne (1)–(3) for d_n viser man (som f.eks. i HBF), at der findes *netop én* funktion d_n der opfylder (1)–(3). Denne funktion kaldes så *determinanten*, og da beviset er helt formelt findes en sådan determinant også for kommutative ringe. Det er ikke vanskeligt at vise, at følgende funktion det : $R_n^n \to R$ opfylder (1)–(3), hvilket betyder, at den *er* "determinantfunktionen".

Lad $A = (a_{ij}) \in R_n^n$, $a_{ij} \in R$, $1 \leq i, j \leq n$. Sæt

$$\det A = \sum_{\pi \in S_n} \operatorname{sign}(\pi) a_{1\pi(1)} a_{2\pi(2)} \cdots a_{n\pi(n)} \tag{8.25}$$

(sammenlign HBF 19.9 (5)). De forskellige fundamentale egenskaber af determinanten kan udledes fra dette udtryk eller direkte fra (1)–(3). Det gælder f.eks. følgende: Hvis $A \in R_n^n$ og $1 \leq i, j \leq n$ lader vi $/_i\ A\ _j\backslash$ være den $(n-1) \times (n-1)$ matrix, der opstår fra A ved at slette den i'te række og den j'te søjle i A. Sæt

$$\widetilde{a}_{ij} = (-1)^{i+j} \det(/_i\ A\ _j\backslash)$$

og $\widetilde{A} = (\widetilde{a}_{ij})$. Så er

$$\widetilde{A}^t A = A\widetilde{A}^t = (\det A) E_n. \tag{8.26}$$

Heraf fås straks følgende:

> *Hvis ringelementet* $\det A \in R$ *er invertibelt i ringen* R, *så er matricen* $\det(A)^{-1} \cdot \widetilde{A}^t$ *et inverst element til elementet* $A \in R_n^n$.

Altså

$$\det A \text{ invertibel i } R \Rightarrow A \text{ invertibel i } R_n^n \tag{8.27(1))}$$

Men det omvendte gælder også:

$$A \text{ invertibel i } R_n^n \Rightarrow \det A \text{ invertibel i } R. \tag{8.27(2))}$$

Dette kan udledes fra følgende resultat:

$$\text{Lad } A, B \in R_n^n. \text{ Så er } \det(AB) = (\det A)(\det B). \tag{8.28}$$

Lad os antage, at (8.28) gælder: Så er specielt følgende opfyldt: Hvis $AB = BA = E_n$, er $\det A \det B = \det B \det A = \det E_n = 1$. Derfor er $\det B$ inverst element til $\det A$ i R, så $\det A$ er invertibel; dvs. (8.27)(2) er bevist.

Spørgsmålet er så, hvorledes (8.28) kan bevises, når R kun er en ring og ikke et legeme. Beviset fra HBF kan ikke umiddelbart overføres. I nogle benyttede resultater

er det anvendt, at elementer $\neq 0$ i et legeme er invertible. I stedet kan man give et bevis baseret på de formelle egenskaber (1)–(3), der blev nævnt tidligere. Ideen er den følgende:

Lad $A \in R_n^n$ være givet. Betragt funktionen $d_A : R_n^n \to R$ defineret ved

$$d_A(B) = \det(AB).$$

Det viser sig at funktionen d_A opfylder linearitetsbetingelsen (1) mht. søjler. Dette følger faktisk fra den tilsvarende betingelse for d_n. Ligeledes opfylder d_A betingelsen (3). Derimod bliver betingelsen (2) erstattet med

$(2)_A$ $$d_A(E_n) = \det A.$$

Man kan så gentage argumentet for at der findes *netop én funktion* der opfylder (1)–(3) til at vise, at der findes *netop én* funktion der opfylder (1), $(2)_A$ og (3). Da funktionen $\widetilde{d}_A : R_n^n \to R$ defineret ved

$$\widetilde{d}_A(B) = \det A \cdot \det B$$

også opfylder (1), $(2)_A$ og (3), må $d_A = \widetilde{d}_A$, dvs.

$$\det AB = d_A(B) = \widetilde{d}_A(B) = \det A \det B.$$

Denne form for formelle eller "universelle" beviser er meget anvendelige i visse grene af algebraen.

(8.29) EKSEMPEL: Lad $R = \mathbb{Z}_{10}$ være restklasseringen modulo 10. Betragt

$$A = \begin{pmatrix} \widehat{9} & \widehat{7} \\ \widehat{5} & \widehat{2} \end{pmatrix} \in R_2^2.$$

Vi har ifølge (8.25): $\det A = \widehat{9} \cdot \widehat{2} - \widehat{5} \cdot \widehat{7} = \widehat{18} - \widehat{35} = \widehat{8} - \widehat{5} = \widehat{3}$. Nu er $\widehat{3}$ invertibel i $\mathbb{Z}_{10}$, ifølge (2.37). Vi har $\widehat{3}^{-1} = \widehat{7}$, da $\widehat{3} \cdot \widehat{7} = \widehat{21} = \widehat{1}$. Idet $\widetilde{a}_{ij}$ er defineret som ovenfor, ses at

$$\widetilde{a}_{11} = \widehat{2}, \quad \widetilde{a}_{12} = -\widehat{5} = \widehat{5}, \quad \widetilde{a}_{21} = -\widehat{7} = \widehat{3}, \quad \widetilde{a}_{22} = \widehat{9},$$

således at

$$\widetilde{A} = \begin{pmatrix} \widehat{2} & \widehat{5} \\ \widehat{3} & \widehat{9} \end{pmatrix}.$$

Ifølge (8.26) er $\widehat{3}^{-1}\widetilde{A}^t = \widehat{7} \cdot \widetilde{A}^t$ den inverse matrix til A, altså

$$A^{-1} = \widehat{7}\begin{pmatrix} \widehat{2} & \widehat{3} \\ \widehat{5} & \widehat{9} \end{pmatrix} = \begin{pmatrix} \widehat{14} & \widehat{21} \\ \widehat{35} & \widehat{63} \end{pmatrix} = \begin{pmatrix} \widehat{4} & \widehat{1} \\ \widehat{5} & \widehat{3} \end{pmatrix}.$$

□

(8.30) ØVELSE: Lad R være restklasseringen $\mathbf{Z}_9$. Undersøg om følgende matricer $A \in R_2^2$, $B \in R_3^3$ er invertible og angiv i givet fald deres inverse matrix:

$$A = \begin{pmatrix} \widehat{3} & \widehat{1} \\ \widehat{2} & \widehat{5} \end{pmatrix} \quad B = \begin{pmatrix} \widehat{1} & \widehat{2} & \widehat{1} \\ \widehat{1} & \widehat{1} & \widehat{1} \\ \widehat{1} & \widehat{2} & \widehat{4} \end{pmatrix}$$

□

(8.31) SÆTNING (OG DEFINITION). *Antag, at den fri R-modul M har 2 baser X, Y, som er endelige. Antag, at R er kommutativ. Så er $|X| = |Y|$. Dette fælles tal $|X|(= |Y|)$ kaldes modulens rang, $\operatorname{rg} M = |X|$. Vi giver nulmodulen rang 0 (og basis $\varnothing$).*

BEVIS: Lad $X = \{x_1, x_2, \ldots, x_n\}$, $Y = \{y_1, y_2, \ldots, y_m\}$. Da $y_j \in \operatorname{span}(X)$ findes $a_{ji} \in R$, $j \in \{1, \ldots, m\}$, $i \in \{1, \ldots, n\}$ så

(1) $y_j = \sum_{i=1}^{n} a_{ji} x_i$.

Da $x_i \in \operatorname{span}(Y)$ findes $b_{ij} \in R$, $i \in \{1, \ldots, n\}$, $j \in \{1, \ldots, m\}$ så

(2) $x_i = \sum_{j=1}^{m} b_{ij} y_j$

Lad os antage $m \leq n$ og indsætte (1) i (2). Vi får

$$x_i = \sum_{j=1}^{m} \sum_{k=1}^{n} b_{ij}\, a_{jk}\, x_k = \sum_{k=1}^{n} \left(\sum_{j=1}^{m} b_{ij}\, a_{jk} \right) x_k.$$

Hvis $c_{ik} = \sum_{j=1}^{m} b_{ij}\, a_{jk}$ gælder altså

$$x_i = \sum_{k=1}^{n} c_{ik}\, x_k.$$

Da X er lineær uafhængig fås heraf

(3) $c_{ii} = 1, \quad c_{ik} = 0$ for $i \neq k$. $\quad (i, k \in \{1, 2, \ldots, n\})$

Betragt matricerne $A, B \in R_n^n$ defineret ved

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & & & \\ a_{m1} & a_{m2} & \ldots & a_{mn} \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & & \\ 0 & 0 & \ldots & 0 \end{bmatrix}, \quad B = \begin{bmatrix} b_{11} & b_{12} & \ldots & b_{1m} & 0 & \ldots & 0 \\ b_{21} & b_{22} & \ldots & b_{2m} & 0 & \ldots & 0 \\ \vdots & & & & & & \\ b_{n1} & b_{n2} & \ldots & b_{nm} & 0 & \ldots & 0 \end{bmatrix}$$

I A er de sidste $n - m$ rækker og i B de sidste $n - m$ søjler 0. Så viser ligningerne (3), at

(4) $BA = E_n$.

Ifølge (8.28) er derfor $\det B \cdot \det A = 1$ og (da R er kommutativ) $\det A \cdot \det B = 1$, således at $\det A$ er invertibel i R. Det betyder, ifølge (8.27), at A er invertibel i R_n^n. Hvis $C = A^{-1}$ gælder altså $AC = CA = E_n$. Men så er

$$B = BE_n = B(AC) = (BA)C = E_nC = C$$

altså $B = C$. Det betyder, at $AB = E_n$. Hvis nu $m < n$, er den sidste række i AB konstant 0, hvilket strider mod $AB = E_n$. Derfor må $m = n$. Vi har vist $m \leq n \Rightarrow m = n$. Analogt fås selvfølgelig $n \leq m \Rightarrow n = m$. □

Lad os se på nogle forfininger af (8.31).

(8.32) SÆTNING. *R kommutativ. Lad M være en fri R-modul af endelig rang n. Hvis Y er en endelig frembringermængde for M gælder $n \leq |Y|$.*

BEVIS: Lad $X = \{x_1, \ldots, x_n\}$ basis, $Y = \{y_1, \ldots, y_m\}$ og a_{ji}, b_{ij}, c_{ik} være som i beviset for (8.31). Da X er lineær uafhængig gælder ligningen (3) for c_{ik}'erne stadig. Vi får stadig, at hvis $m = |Y| \leq |X| = n$, må $m = n$. Derfor er det *umuligt* at $|Y| < |X|$. Så $|X| \leq |Y|$. □

(8.33) SÆTNING. *R kommutativ. Lad X være en endelig basis for R-modulen M og Y en frembringermængde for M med $|X| = |Y|$. Så er Y en basis for M.*

BEVIS: Som beviset for (8.31) kan vi definere koefficienterne a_{ji}, b_{ij}, c_{ik}. Idet også A og B er defineret som i beviset (med $m = n$!) fås $BA = E_n$. Men så er også (se beviset) $AB = E_n$. Hvis $d_1, \ldots, d_n \in R$ og $d_1y_1 + d_2y_2 + \cdots + d_ny_n = 0$ fås fra (1) i (8.31)

$$\sum_{i=1}^{n} \left(\sum_{j=1}^{n} d_j\, a_{ji} \right) x_i = 0.$$

Da X er lineær uafhængig er $\sum_{j=1}^{n} d_j\, a_{ji} = 0$ for alle i. Hvis

$$D = (d_1, d_2, \ldots, d_n), \quad \text{er altså } DA = (0, 0, \ldots, 0)$$

(multiplikation af matricer). Da $AB = E_n$ fås

$$D = DAB = (0, 0, \ldots, 0)B = (0, 0, \ldots, 0), \quad \text{altså } d_1 = \cdots = d_n = 0$$

Dermed er Y lineær uafhængig. □

(8.34) BEMÆRKNING: Hvis R-modulen M har en endelig basis X og hvis Y er en lineær uafhængig mængde i M med $|X| = |Y|$, så er Y *ikke* nødvendigvis en basis. Se f.eks. (8.15)(1). □

I beviserne for (8.31)–(8.33) var det essentielt at $\text{span}(X) = \text{span}(Y)$ for at man kunne finde elementerne a_{ji}, b_{ij} og dermed matricerne A og B. Derfor er metoden uegnet til at behandle undermoduler af (frie) endeligt frembragte moduler. Man kan stille følgende spørgsmål:

(8.35) Er en undermodul af en fri modul fri?

(8.36) Er en undermodul af en endelig frembragt modul endelig frembragt?

Der er selvfølgelig også talrige varianter af disse spørgsmål.

Det viser sig at begge spørgsmål har et negativt svar i almindelighed, også for kommutative ringe. Men der findes klasser af ringe hvor spørgsmålene har positive svar for alle moduler. (F.eks. er svarene jo positive, når R er et legeme. Overvej!)

(8.37) DEFINITION: Lad M være en R-modul. Antag, at der for enhver følge af undermoduler $M_1, M_2, \ldots, M_n, \ldots$ af M, som opfylder

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \ldots$$

findes et $m \in \mathbb{N}$, således at $M_n = M_m$ for alle $n \geq m$. Så kaldes M en *noethersk* modul.* En ring kaldes *noethersk*, hvis den er noethersk som modul over sig selv (jvf. (8.5)(2)), og hvis den er kommutativ. (I dette tilfælde er undermodulerne netop ringens idealer). Betingelsen for at en modul er noethersk udtrykkes ofte på følgende måde: "Enhver voksende kæde af undermoduler bliver stationær". (Jfr. Kap. 0!) □

Vi starter med at vise

(8.38) SÆTNING. *Lad N være en undermodul af R-modulen M. Følgende udsagn er ensbetydende*

(1) *M er noethersk.*
(2) *Modulerne N og M/N er noetherske.*

I beviset for denne sætning får vi brug for

(8.39) SÆTNING. *Lad $\varphi : M \to K$ være en epimorfi af R-moduler. Hvis U er en undermodul i K sættes $U^* = \varphi^{-1}(U) = \{x \in M \mid \varphi(x) \in U\}$. Så er afbildningen $U \mapsto U^*$ en bijektion mellem mængden af undermoduler af K og mængden af undermoduler af M, som indeholder $\ker\varphi$. Der gælder $U \subseteq U_1 \Leftrightarrow U^* \subseteq U_1^*$.*

BEVIS: Det tilsvarende resultat for ringe og grupper (se f.eks. (7.7.5)) er dukket op tidligere og beviset her er igen en *øvelse*. □

*Emmy Noether, tysk matematiker (1882–1935)

BEVIS FOR (8.38): (1) $\Rightarrow$ (2) Lad M være noethersk. Da undermoduler af N også er undermoduler af M er det klart, at N er noethersk. Betragt epimorfien $\varphi : x \to \widehat{x}$ fra $M \to K = M/N$. Antag, at $U_1 \subseteq U_2 \subseteq \cdots \subseteq U_n \subseteq \cdots$ er en voksende kæde af undermoduler i K. Så er $U_1^* \subseteq U_2^* \subseteq \cdots \subseteq U_n^* \subseteq \cdots$ en voksende kæde af undermoduler i M ((8.39)). Da M er noethersk eksisterer et $m \in \mathbb{N}$ således at $U_n^* = U_m^*$ for $n \geq m$. Det medfører, at $U_n = U_m$ for $n \geq m$ (da $U \to U^*$ er en bijektion).

(2) $\Rightarrow$ (1) Lad N og $K = M/N$ være noetherske. Lad $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_k \subseteq \cdots$ være en voksende kæde af undermoduler af M. Så er

$$M_1 \cap N \subseteq M_2 \cap N \subseteq \cdots \subseteq M_k \cap N \subseteq \cdots$$

en voksende kæde af undermoduler i N og

$$(M_1 + N)/N \subseteq (M_2 + N)/N \subseteq \cdots \subseteq (M_k + N)/N \subseteq \cdots$$

en voksende kæde af undermoduler i K. Der findes ifølge antagelsen $m_1, m_2 \in \mathbb{N}$ således at

$$M_n \cap N = M_{m_1} \cap N \quad \text{for } n \geq m_1$$
$$(M_n + N)/N = (M_{m_2} + N)/N \quad \text{for } n \geq m_2$$

Lad $m \geq m_1$, $m \geq m_2$. Vi påstår, at $M_n = M_m$ for $n \geq m$. Hvis $n \geq m$ viser det ovenstående, at $M_m \subseteq M_n$, $M_m + N = M_n + N$, $M_m \cap N = M_n \cap N$. Lad $x \in M_n$. Vi skal vise, at $x \in M_m$. Da $x \in M_n \subseteq M_n + N = M_m + N$ kan vi skrive $x = x_1 + z$, hvor $x_1 \in M_m$, $z \in N$. Men $x \in M_n$ og $x_1 \in M_m \subseteq M_n$, så $z = x - x_1 \in M_n$, altså $z \in M_n \cap N$. Nu er $M_n \cap N = M_m \cap N$, så $z \in M_m$. Da $x_1 \in M_m$ og $z \in M_m$ er også $x = x_1 + z \in M_m$, som ønsket. □

(8.40) ØVELSE: Lad $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$ være en voksende kæde af undermoduler af R-moduler M. Vis, at $N = \cup_{i \in \mathbb{N}} M_i$ også er en undermodul af M. (Løsningshjælp: Man kan lade sig inspirere af (en del af) beviset for (5.3)!) □

(Selvfølgelig gælder (8.40) for en vilkårlig kæde i *po*-mængden, der består af undermodulerne af M, ordnet ved inklusion.)

(8.41) EKSEMPLER: (1) $\mathbb{Z}$ er en noethersk ring. Faktisk er *enhver hovedidealring* R *noethersk*: Hvis $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_k \subseteq \cdots$ er en voksende kæde af idealer i R, så er $I = \cup_{i \in \mathbb{N}} I_i$ et ideal i R. Der findes altså $x \in I$ således at $I = Rx$. Da $x \in I$ eksisterer et m, så $x \in I_m$. Men så er $Rx = I \subseteq I_m$, da I_m er et ideal. For $n \geq m$ er $I \subseteq I_m \subseteq I_n \subseteq I = \cup I_i$, så $I_m = I_n$ $(= I)$.

(2) Ringen $R = \mathbb{Z}^{\mathbb{Z}}$ af funktioner $f : \mathbb{Z} \to \mathbb{Z}$ (jvf. (3.1)(4)) er ikke noethersk. For $k \in \mathbb{N}$, lad

$$I_k = \{f \in R \mid f(n) = 0 \quad \text{for } n \geq k\}.$$

Det er let at se, at I_n er et ideal i R og at $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$. For $k \in \mathbf{N}$ lad $g_k \in R$ være defineret ved

$$g_k(k) = 1, \quad g_k(n) = 0 \quad \text{for } n \neq k.$$

Så er det klart, at $g_k \notin I_k$, da $g_k(k) \neq 0$, men $g_k \in I_{k+1}$, da $g_k(k+1) = g_k(k+2) = \cdots = 0$. Derfor er $I_k \neq I_{k+1}$ for alle k. Det betyder, at kæden af I_k'er ikke bliver stationær. □

Forbindelsen mellem noetherske moduler og spørgsmålet (8.36) gives her:

(8.42) SÆTNING. *Lad M være en R-modul. Følgende udsagn er ensbetydende:*

(1) *M er noethersk.*
(2) *Enhver undermodul af M er en endelig frembragt.*

BEVIS: (1) $\Rightarrow$ (2) Lad M være noethersk. For at vise (2) er det ifølge (8.38) tilstrækkeligt at bevise, at M er endelig frembragt. Vi definerer induktivt undermoduler $M_1, M_2, \ldots$ som følger: $M_1 = \{0\}$. Antag, at vi har defineret M_i, $i \in \mathbf{N}$. Så defineres M_{i+1} som følger

(i) Hvis $M_i = M$ sættes $M_{i+1} = M$.
(ii) Hvis $M_i \neq M$ vælges $x \in M \setminus M_i$ og vi sætter $M_{i+1} = M_i + Rx$. Så er $M_i \neq M_{i+1}$, da $x \in M_{i+1}$, $x \notin M_i$.

Så er $M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n \subseteq \cdots$ en voksende kæde af undermoduler af M. Ved induktion ses let, at ethvert M_i er endelig frembragt, da M_{i+1} fremgår fra M_i ved højst at tilføje én frembringer. Da M er noethersk bliver kæden stationær: Der findes et $m \in \mathbf{N}$ så $M_m = M_{m+1}$. Men så må, ifølge definitionen, tilfældet (i) forekomme, og derfor er $M_m = M$, altså M endelig frembragt.

(2) $\Rightarrow$ (1): Vi antager, at enhver undermodul af M er endelig frembragt. Lad

$$M_1 \subseteq M_2 \subseteq \cdots \subseteq M_k \subseteq \cdots$$

være en voksende kæde af undermoduler af M. Ifølge (8.40) er $\bigcup_i M_i = N$ en undermodul af M, og derfor endelig frembragt. Antag, at $N = \operatorname{span}(x_1, \ldots, x_t)$. Da $N = \bigcup_i M_i$ findes for ethvert j, $1 \leq j \leq t$ et $n_j \in \mathbf{N}$, så $x_j \in M_{n_j}$. Lad $m \geq n_1, n_2, \ldots, n_t$. Så er $x_j \in M_{n_j} \subseteq M_m$ for $1 \leq j \leq t$, og derfor $N = \operatorname{span}(x_1, \ldots, x_t) \subseteq M_m$. For $n \geq m$ er så

$$N \subseteq M_n \subseteq M_n \subseteq N = \bigcup_i M_i,$$

altså $M_m = M_n$ $(= N)$. □

(Den opmærksomme læser vil have bemærket, at argumentet i (8.41)(1) er et specielt tilfælde af den sidste del af beviset for (8.42).)

Den ovenstående sætning viser, at kun for noetherske moduler er enhver undermodul endelig frembragt. Da der imidlertid findes moduler, der ikke er noetherske (f.eks. ringen R i (8.40)(2) som modul over sig selv) er (8.36) *forkert* i almindelighed. Ringen R er, som enhver ring (med 1-element), endda en fri modul over sig selv med basis $X = \{1\}$, $|X| = 1$. Denne enkle bemærkning giver os også et let *modeksempel til* (8.35): Lad R være en kommutativ ring (med 1-element), som ikke opfylder nuldelerbetingelsen [NU], (altså f.eks. $\mathbf{Z}_4$). Antag, at $a, b \in R$, $a, b \neq 0$ men $ab = 0$. Så er idealet Ra en undermodul af den fri modul R. Men intet element $x \in Ra$ kan være med i en basis for Ra, da $bx = 0$ med $b \neq 0$ og $\{x\}$ altså ikke er lineær uafhængig.

Vi kunne selvfølgelig afslutte diskussionen af (8.35) og (8.36) her, men de er jo opfyldte for vektorrum, (altså R-moduler, hvor R er et legeme.) Dette antyder, at *ringen R spiller en rolle.* Vi spørger derfor:

(8.35)* For hvilke ringe R er enhver R-modul fri?

(8.35)** For hvilke ringe R er enhver undermodul af en fri R-modul fri?

(8.36)* For hvilke ringe R er enhver endelig frembragt R-modul noethersk?

Vi kan faktisk besvare (8.36)* med det samme!

(8.43) SÆTNING. *Lad R være en kommutativ ring. Følgende udsagn er ækvivalente*

(1) *R er noethersk.*

(2) *Enhver endelig frembragt R-modul er noethersk.*

BEVIS: (2) $\Rightarrow$ (1) er oplagt, idet R jo er endelig frembragt (af $X = \{1\}$) som modul over sig selv.

(1) $\Rightarrow$ (2) Lad R være noethersk og $M = \operatorname{span}(x_1, \ldots, x_n)$ en endelig frembragt R-modul. Ifølge (8.24) findes en epimorfi $\varphi : R^n \to M$. Ifølge (8.21) er $M \simeq R^n / \ker \varphi$. Ifølge (8.38) er det tilstrækkeligt at vise at R^n er en noethersk R-modul. Dette gøres ved induktion efter n. For $n = 1$ er $R^n \simeq R$ noethersk ifølge antagelsen. Antag, at R^{n-1} er noethersk, $n \geq 2$. Undermodulen

$$N = \{(x_1, \ldots, x_n) \in R^n \mid x_1 = 0\}$$

er isomorf til R^{n-1}, idet afbildningen

$$(x_2, x_3, \ldots, x_n) \to (0, x_2, \ldots, x_n)$$

fra R^{n-1} til N er en isomorfi. Ifølge induktionsantagelsen er N ($\simeq R^{n-1}$) noethersk. Men R^n/N er også noethersk idet $R^n/N \simeq R$: Afbildningen

$$x \mapsto (x, \widehat{0, 0}, \ldots, 0)$$

er en isomorfi mellem R og R^n/N. At eftervise dette overlades til læseren som en *øvelse.* Da R^n/N og N er noetherske, er R^n noethersk ifølge (8.38). □

Spørgsmålene (8.35)* og (8.35)** vil vi kun besvare for kommutative ringe.

(8.44) SÆTNING. *Lad R være en kommutativ ring. Følgende betingelser er ensbetydende:*

(1) *R er et legeme.*
(2) *Enhver R-modul har en basis.*

BEVIS: (1) $\Rightarrow$ (2) er kendt fra den lineære algebra, idet mindste for endeligt frembragte R-moduler (vektorrum). For at vise, at *ethvert* vektorrum V har en basis kan man anvende Zorns Lemma [ZL] på *po*-mængden $(\mathcal{M}, \subseteq)$, hvor

$$\mathcal{M} = \{A \subseteq V \mid A \quad \text{er lineær uafhængig}\}$$

og $\subseteq$ er inklusionsordningen. Det er ikke svært at se, at hvis $\mathcal{X}$ er en kæde i $\mathcal{M}$, så er $(\cup_{A\in\mathcal{X}} A) \in \mathcal{M}$ og derfor en majorant for $\mathcal{X}$. Men et maksimalt element i $\mathcal{M}$ er åbenbart en basis for V. (Overvej!)

(2) $\Rightarrow$ (1) Antag, at enhver R-modul har en basis. Lad os først bemærke, at R opfylder [NU]: Hvis $a \neq 0$ er en nuldeler, har R-modulen Ra (en undermodul af R) ingen basis (se det ovenstående modeksempel til (8.35)). Da R er en integritetsring, kan vi danne R's brøklegeme $Q(R)$ (se §5). Vi overtager notationen fra (5.7)

$$Q(R) = \{[a,b] \mid a,b \in R, b \neq 0\}$$

hvor $[a,b] = [c,d] \Leftrightarrow ad = bc$. Idet R identificeres med delringen $\{[r,1] \mid r \in R\}$ af $Q(R)$, er $Q(R)$ altså en R-modul (jvf. (8.5)(5)):

$$r[a,b] = [r,1][a,b] = [ra,b]$$

(for $r \in R$, $[a,b] \in Q(R)$). Lad X være en basis for R-modulen $Q(R)$. Vi påstår først at $|X| = 1$: Hvis $[a,b]$ og $[a',b'] \in X$ er a, a', b, b' alle $\neq 0$ og

$$\begin{aligned} a'b[a,b] - ab'[a',b'] &= [a'ab,b] - [aa'b',b'] \\ &= [a'a,1] - [aa',1] = [0,1] = 0 \end{aligned}$$

Hvis $[a,b] \neq [a',b']$ er det ovenstående en ikke-triviel linearkombination af de to elementer, en modstrid. Så hvis $X = \{[a,b]\}$ er, $Q(R) = R[a,b]$. Vi skal vise, at $R = Q(R)$: Da $[1,b^2] \in Q(R)$ eksisterer et $r \in R$, så

$$r[a,b] = [ra,b] = [1,b^2]$$

Det betyder, at $rab^2 = b$ og derfor er $rab = 1$ og $ra^2b = a$. Så er $[a,b] = [ra^2,1] \in R$, altså $[a,b] \in R$. Dette viser $Q(R) \subseteq R$, dvs. $Q(R) = R$. □

Efter dette måske lidt skuffende svar på (8.35)* vil det være en trøst, at man i (8.35)** får en større klasse af kommutative ringe.

Herom mere i næste kapitel.

Vi slutter med nogle øvelser, der giver en sammenhæng mellem "rang" og "dimension".

Lad R være kommutativ og M en R-modul.

(8.45) ØVELSE: Lad I være et ideal i R. Sæt

$$IM = \{\sum_i p_i m_i \mid p_i \in I,\ m_i \in M\}$$

(altså mængden af endelige "I-linearkombinationer" af elementer i M. Vis, at IM er en undermodul af M. □

(8.46) ØVELSE: Antag, at $I = Rp$ er et hovedideal i R. Vis, at

$$IM = pM = \{pm \mid m \in M\}. \quad \square$$

(8.47) ØVELSE: Lad $I \neq R$ være et ideal i R. Sæt $\overline{R} = R/I$, $\overline{M} = M/IM$. Vis, at der ved

$$\widehat{a}\widehat{m} = \widehat{am}\ ,\ \widehat{a} \in \overline{R},\ \widehat{m} \in \overline{M}$$

defineres en $\overline{R}$-modul struktur på $\overline{M}$.

(Husk: Veldefinerethed!) □

(8.48) ØVELSE: Lad $I \neq R$ være et ideal i R, $\overline{R}$ og $\overline{M}$ som ovenfor. Antag, at M er en fri R-modul med basis $\{x_1, \ldots, x_s\}$. Vis, at $\overline{M}$ er en fri $\overline{R}$-modul med basis $\{\widehat{x}_1, \ldots, \widehat{x}_s\}$. □

(8.49) ØVELSE: Lad I være et maksimalt ideal i R, således at $\overline{R} = R/I$ er et legeme og $\overline{M} = M/IM$ et $\overline{R}$-vektorrum. Antag, at M har en basis $\{x_1, \ldots, x_s\}$. Vis, at $s = \dim_{\overline{R}} \overline{M}$. Benyt denne øvelse til at give et alternativt bevis for Sætning (8.31). □

Kapitel 9. Moduler over hovedidealringe.

I dette kapitel behandler vi et interessant og meget anvendeligt hjørne af modulteorien.

Vi beskriver den eksplicitte struktur af endelig frembragte R-moduler, hvor R er en hovedidealring. Desuden vil vi betragte anvendelser i gruppeteorien og i den lineære algebra. Vi starter med i fortsættelse af sidste kapitel at se på spørgsmålet (8.35)**. I dette kapitel betragtes kun *kommutative ringe med 1-element*, og som i Kapitel 8 antages alle moduler at være unitære.

(9.1) SÆTNING. *Følgende udsagn er ækvivalente:*

(1) *R er en hovedidealring.*
(2) *Ethvert ideal i R er frit som R-modul.*

BEVIS: (1) $\Rightarrow$ (2) Hvis $I \neq \{0\}$ er et ideal i hovedidealringen R, er $I = Ra$ for et $a \in I$, så $\{a\}$ frembringer I. Da R opfylder [NU] er a ingen nuldeler og derfor $\{a\}$ lineær uafhængig.

(2) $\Rightarrow$ (1) Som i beviset for (8.44) (2) $\Rightarrow$ (1) ses at R er en integritetsring. Lad $I \neq \{0\}$ være et ideal i R og X en basis for I. Vi får igen $|X| = 1$. Hvis $a \in X$ er altså $I = Ra$, så I er et hovedideal. □

En umiddelbar følge af dette er:

(9.2) SÆTNING. *Hvis enhver undermodul af en fri R-modul er fri, så er R en hovedidealring.*

□

Vi viser kun det omvendte udsagn til (9.2) i et specielt tilfælde.

(9.3) SÆTNING. *Lad R være en hovedidealring. Lad M være en fri R-modul af rang $n(< \infty)$. Hvis N er en undermodul af M, så er N fri og $\operatorname{rg}(N) \leq n$.*

BEVIS: Induktion efter $n = \operatorname{rg}(M)$.

Hvis $n = 1$ er $M \simeq R$ (som R-modul) og resultatet følger fra (9.1). Lad $n > 1$ og antag, at resultatet er bevist for frie moduler af rang $\leq n-1$. Lad $X = \{x_1, x_2, \ldots, x_n\}$ være en basis for M. Sæt $K = \operatorname{span}(x_1, x_2, \ldots, x_{n-1})$. Da $\{x_1, x_2, \ldots, x_{n-1}\}$ er lineær uafhængig, er K fri of rang $n-1$. Derfor er ifølge induktionsantagelsen $N_1 = N \cap K$ fri af rang $\operatorname{rg} N_1 \leq n-1$. Vi sætter $\operatorname{rg} N_1 = m-1$ for et $m \geq 1$ og lader $Y_1 = \{y_1, y_2, \ldots, y_{m-1}\}$ være en basis for N_1. (Så $m-1 \leq n-1$ og $m \leq n$).

Modulen M/K er også fri med $\{\widehat{x}_n\}$ som basis: For det første er $M/K = \operatorname{span}(\widehat{x}_1, \widehat{x}_2, \ldots, \widehat{x}_n) = \operatorname{span}(\widehat{x}_n)$ (idet for $1 \leq i \leq n-1$, $x_i \in K$ og dermed $\widehat{x}_i = \widehat{0}$). For det andet er $\{\widehat{x}_n\}$ lineær uafhængig. Hvis $a \in R$ og $a\,\widehat{x}_n = \widehat{0}$, så er $\widehat{a\,x_n} = \widehat{0}$, $a\,x_n \in K = \operatorname{span}(x_1, \ldots, x_{n-1})$. Der findes altså $a_1, a_2, \ldots, a_{n-1} \in R$ så

$$a\,x_n = a_1 x_1 + a_2 x_2 + \cdots + a_{n-1} x_{n-1}\,.$$

Da X er lineær uafhængig fås heraf $a = 0$ $(= a_i)$.

Da M/K er fri af rang 1, er undermodulen $\widehat{N} = N + K/K$ af M/K fri af rang 0 eller 1.

1* Antag, at $\operatorname{rg}\widehat{N} = 0$, altså $\widehat{N} = \{\widehat{0}\}$. Det betyder $N + K/K = \{\widehat{0}\}$, eller $N + K = K$. Derfor er $N \subseteq K$, så $N = N_1$ er fri af rang $m - 1 \leq n$.

2* Antag, at $\operatorname{rg}\widehat{N} = 1$. Lad $\{\widehat{y}_m\}$ være en basis for $\widehat{N}$, hvor $y_m \in N + K$. Hvis vi skriver $y_m = y'_m + z$, hvor $y'_m \in N$, $z \in K$, så er $\widehat{y}_m = \widehat{y'_m + z} = \widehat{y}'_m + \widehat{z} = \widehat{y}'_m$ da $\widehat{z} = \widehat{0}$. Vi kan derfor antage at $y_m \in N$. Vi påstår:

$$Y = \{y_1, y_2, \ldots, y_{m-1}, y_m\} \quad \text{er en basis for } N\,.$$

(Dette vil afslutte beviset, idet N så er fri og $\operatorname{rg} N = m \leq n$). Først vises, at $N = \operatorname{span}(y_1, y_2, \ldots, y_m)$: Lad $x \in N$. Skriv $\widehat{x} \in \widehat{N}$ som $\widehat{x} = a_m\,\widehat{y}_m$, hvor $a_m \in R$. Så er $x - a_m y_m \in N_1$. Da $N_1 = \operatorname{span}(y_1, \ldots, y_{m-1})$ eksisterer $a_1, a_2, \ldots, a_{m-1} \in R$, så

$$x - a_m y_m = a_1 y_1 + \cdots + a_{m-1} y_{m-1}$$

eller $x = a_1 y_1 + \cdots + a_m y_m$. Sluttelig vises, at Y er lineær uafhængig. Antag, at

$$a_1 y_1 + a_2 y_2 + \cdots + a_m y_m = 0$$

for $a_1, \ldots, a_m \in R$. Så er $(i\ \widehat{N})$, $\widehat{0} = \widehat{a_m y_m} = a_m \widehat{y}_m$ (da $\widehat{y}_i = 0$ for $1 \leq i \leq m-1$). Da $\{\widehat{y}_m\}$ er lineær uafhængig fås $a_m = 0$. Derfor er $a_1 y_1 + \cdots + a_{m-1} y_{m-1} = 0$. Da Y_1 er lineær uafhængig fås også $a_1 = \cdots = a_{m-1} = 0$. □

For at have opfyldt, at en undermodul af en (endeligt frembragt) fri R-modul er fri, må man altså forlange, at R er en hovedidealring. På den anden side kan der eksistere moduler over en hovedidealring, der ikke er fri, f.eks. $\mathbb{Z}$-modulen $\mathbb{Z}_2$.

Vi viser i dette kapitel, at en endeligt frembragt R-modul, R hovedidealring, er en direkte sum af en fri undermodul og en torsions undermodul. Hver af disse undermoduler er en direkte sum af cykliske undermoduler og vi undersøger, i hvilken grad denne fremstilling er entydig.

Hovedsætningen for endeligt frembragte R-moduler står i sammenhæng med en slags udvidet "echelonsætning" for matricer i R_n^m, dvs. for $m \times n$-matricer

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix} \quad , \quad a_{ij} \in R\,.$$

Specielt er R_m^m en ring, og vi har set i (8.27), at $A \in R_m^m$ er invertibel i R_m^m hvis og kun hvis $\det A \in R$ er invertibel i R.

(9.4) DEFINITION: Vi definerer en ækvivalensrelation $\approx$ på R_n^m , $m, n \in \mathbb{N}$ ved

$$A \approx B \Leftrightarrow \begin{cases} \text{Der eksisterer invertible matricer} \\ X \in R_m^m \, , Y \in R_n^n \, , \text{så } XAY = B \, . \end{cases}$$

□

Det er klart, at $\approx$ *er* en ækvivalensrelation. Vi viser, at når R er en hovedidealring, så er $A \in R_n^m$ $\approx$-ækvivalent til en matrix på formen

$$\begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$$

hvor D er en diagonalmatrix af en særlig art og nullerne repræsenterer nulmatricer. Først ser vi på et specielt tilfælde:

(9.5) EKSEMPEL: I HBF, Kapitel 9, defineres en relation $\sim$ på $\mathbb{R}_n^m$ ved:

$$A \sim B \Leftrightarrow A \text{ kan omformes til } B \text{ (ved tilladte rækkeoperationer)}$$

(HBF 9.6(2)). Relationen $\sim$ kan også beskrives som

$$A \sim B \Leftrightarrow \begin{cases} \text{Der eksisterer en invertibel matrix} \\ X \in \mathbb{R}_m^m \, , \text{ så } XA = B \, . \end{cases}$$

At de to beskrivelser af $\sim$ er ækvivalente (*se* HBF 12.4(1)) hænger sammen med det følgende:

(i) En matrix er invertibel hvis og kun hvis den er et produkt af operationsmatricer (HBF 12.3(2)).

(ii) Der er en korrespondance mellem tilladte rækkeoperationer og multiplikation fra venstre med operationsmatricer (HBF 9.1(5), 9.2(3) og 9.3(3), se også nedenfor).

Det ses nu let, f.eks. ved matrix-transponering, at der gælder

A kan omformes til B ved tilladte *søjle* operationer

$\Leftrightarrow$

Der eksisterer en invertibel matrix $Y \in \mathbb{R}_n^n$, så $AY = B$.

Vi får derfor følgende i $\mathbb{R}_n^m$

$A \approx B$

$\Leftrightarrow$

A kan omformes til B ved (en blanding af) tilladte række- og søjleoperationer .

Heraf kan vi slutte følgende:

$$\text{Hvis } A \in \mathbb{R}_n^m \text{ er } A \approx \begin{bmatrix} E & 0 \\ 0 & 0 \end{bmatrix} = F'$$

hvor E er en $r \times r$-enhedsmatrix og $r = \operatorname{rg} A$, rangen af A.

Dette ses som følger: A kan omformes til en echelonmatrix F med $r = \operatorname{rg} A$ initialettaller ved tilladte rækkeoperationer (HBF 6.2(1), 15.4(3) og 15.4(5)). På den anden side er det oplagt, at en echelonmatrix med r initialettaller kan omformes til den ovenstående matrix F' ved en række tilladte søjleoperationer (overvej dette!) □

I det ovenstående eksempel indgik en del resultater om $\mathbb{R}_n^m$, der ikke umiddelbart kan overføres til R_n^m, hvor R er en (hovedideal-)ring. I beviserne indgår mange steder at $\mathbb{R}$ er et legeme, altså at elementerne i $\mathbb{R} \setminus \{0\}$ alle er invertible. Dette er f.eks. helt essentielt i beviset for echelonsætningen. Men udsagnet (ii) i eksemplet gælder generelt.

(9.6) DEFINITION: (1) Hvis $1 \leq i, j \leq m$, $i \neq j$ og $c \in R$, da er $\text{Æ}_{ij}(c) \in R_m^m$ den matrix, hvori alle diagonalelementerne er 1, og alle andre elementer er 0 undtagen elementet på plads (i, j); dette element er c.

(2) Hvis $1 \leq i \leq n$ og $c \in R \setminus \{0\}$, da er $\text{Ø}_i(c) \in R_m^m$ diagonalmatricen med 1 i diagonalen undtagen på plads (i, i), hvor der står c.

(3) Hvis $1 \leq i, j \leq n$ og $i \neq j$, da er Å_{ij} permutationsmatricen $P((i, j))$, hvor $(i, j) \in S_m$ er en transposition (se (7.19)). □

(9.7) ØVELSE: Betragt matricerne $\text{Æ}_{ij}(c)$, $\text{Ø}_i(c)$, Å_{ij} fra (9.6). Vis, at der gælder

$$\det \text{Æ}_{ij}(c) = 1\,, \quad \det \text{Ø}_i(c) = c\,, \quad \det \text{Å}_{ij} = -1$$

således at $\text{Æ}_{ij}(c)$ og Å_{ij} altid er invertible matricer, medens $\text{Ø}_{ij}(c)$ er invertibel hvis og kun hvis $c \in R$ er invertibel. □

(9.8) SÆTNING. *Lad $X \in R_n^m$, $c \in R$.*

(1) *Matricen $\text{Æ}_{ij}(c)X$ opnås fra X ved at addere c gange den j'te række til den i'te række i X.*
(2) *Matricen $\text{Ø}_i(c)X$ opnås fra X ved at multiplicere den i'te række med c.*
(3) *Matricen $\text{Å}_{ij}X$ opnås fra X ved at ombytte den i'te og den j'te række.*

(9.9) SÆTNING. *Lad $X \in R_m^n$, $c \in R$.*

(1) *Matricen $X\text{Æ}_{ij}(c)$ opnås fra X ved at addere c gange den j'te søjle til den i'te søjle i X.*
(2) *Matricen $X\text{Ø}_i(c)$ opnås fra X ved at multiplicere den i'te søjle med c.*
(3) *Matricen $X\text{Å}_{ij}$ opnås fra X ved at ombytte den i'te og den j'te søjle.*

BEVISER: (9.8) bevises som i HBF, og (9.9) fås fra (9.8) ved transponering. □

Som i HBF betegner $\Delta(d_1,\dots,d_k)$ en $k\times k$-diagonalmatrix med $d_1,\dots,d_k$ i diagonalen.

I resten af dette kapitel antages, at R er en *hovedidealring*.

(9.10) SÆTNING. *Lad $A\in R_n^m$.*

(1) *Der gælder*

$$A\approx\begin{bmatrix}D & 0\\ 0 & 0\end{bmatrix}$$

hvor $D=\Delta(d_1,d_2,\dots,d_k)$ er en diagonalmatrix og $d_1|d_2|\cdots|d_k$, $d_k\neq 0$.

(2) *Hvis yderligere*

$$A\approx\begin{bmatrix}D' & 0\\ 0 & 0\end{bmatrix}$$

hvor $D'=\Delta(d_1',d_2',\dots,d_\ell')$ og $d_1'|d_2'|\cdots|d_\ell'$, $d_\ell'\neq 0$, gælder $k=\ell$ og at d_i og d_i' er associerede for $1\le i\le k$ (altså $Rd_i=Rd_i'$).

BEVIS: Lad os bemærke at (1) kan ses som et eksistensudsagn og (2) som et entydighedsudsagn. Vi vil med det samme bevise (1) under anvendelse af resultater fra Kapitel 4 og udskyder beviset for (2) lidt.

Bevis for (1): Lad $A=[a_{ij}]$. Beviset er ved induktion efter $m+n\ge 2$. Vi betragter to tilfælde.

1* Der eksisterer i,j således at $a_{ij}\mid a_{k\ell}$ for alle k,ℓ.

2* For alle i,j eksisterer k,ℓ så $a_{ij}\nmid a_{k\ell}$.

1* Vi antager, at $a_{ij}\mid a_{k\ell}$ for alle k,ℓ. Ved at gange A med Å_{1j} fra venstre og Å_{1i} fra højre fås en matrix, som er ækvivalent til A, og som har a_{ij} på plads $(1,1)$. Vi kan derfor antage, at $a_{11}\mid a_{k\ell}$ for alle k,ℓ. Skriv $a_{k\ell}=a_{11}\cdot b_{k\ell}$ hvor $b_{k\ell}\in R$. Ved at gange A fra venstre med $\text{Æ}_{21}(-b_{21})\text{Æ}_{31}(-b_{31})\dots\text{Æ}_{m1}(-b_{m1})$ og fra højre med $\text{Æ}_{21}(-b_{12})\text{Æ}_{31}(-b_{13})\cdots\text{Æ}_{n1}(-b_{1n})$ fås en matrix, som er ækvivalent til A på formen

$$\overline{A}=\begin{bmatrix}a_{11} & 0 & 0 & \dots & 0\\ 0 & & & & \\ \vdots & & & C & \\ 0 & & & & \end{bmatrix}$$

hvor $C\in R_{n-1}^{m-1}$ har den egenskab, at $a_{11}\mid a_{k\ell}$ for alle k,ℓ. Ifølge induktionsantagelsen eksisterer invertible matricer $X'\in R_{m-1}^{m-1}$, $Y'\in R_{n-1}^{n-1}$ således at

$$X'\,C\,Y'=\begin{bmatrix}\tilde{D} & 0\\ 0 & 0\end{bmatrix}\quad\text{hvor }\tilde{D}=\Delta(\tilde{d}_1,\dots,\tilde{d}_{k-1})$$

opfylder $\tilde{d}_1|\tilde{d}_2|\cdots|\tilde{d}_{k-1}$. Da elementerne i $\tilde{D}$ er R-linearkombinationer af elementerne i C, ses at $a_{11}|\tilde{d}_1|\cdots|\tilde{d}_{k-1}$. Sættes

$$X = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & X' & \\ 0 & & & \end{bmatrix}, Y = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & Y' & \\ 0 & & & \end{bmatrix}$$

er

$$X\overline{A}Y = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix} \quad \text{hvor } D = \Delta(a_{11}, \tilde{d}_1, \dots, \tilde{d}_{k-1}).$$

Da $A \approx \overline{A}$, fås resultatet i dette tilfælde.

2* For alle i, j eksisterer k, ℓ så $a_{ij} \nmid a_{k\ell}$. Specielt kan intet a_{ij} være invertibelt, da et invertibelt element er divisor i ethvert andet element i R. Vi skriver alle $a_{ij} \neq 0$ som produkt af irreducible elementer ((4.25)). Vælg et $a_{ij} \neq 0$ med et mindste antal irreducible faktorer. Som før kan vi antage, at a_{11} har det mindste antal irreducible faktorer.

Hvis $a_{11} \nmid a_{1j}$ for et $j \in \{2, \dots, n\}$ ses ved søjleombytning, at vi kan antage $a_{11} \nmid a_{12}$. Hvis $a_{11} \nmid a_{i1}$ for et $i \in \{2, \dots, n\}$ ses ved rækkeombytning, at vi kan antage $a_{11} \nmid a_{21}$.

Hvis $a_{11} \mid a_{1j}$ for $j = 2, \dots, n$ og $a_{11} \mid a_{i1}$ for $i = 2, \dots, m$ fås som i forrige tilfælde, at A er ækvivalent til en matrix på formen

$$\overline{A} = \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & C & \\ 0 & & & \end{bmatrix}$$

hvor der i dette tilfælde eksisterer k, ℓ, så $a_{11} \nmid c_{k\ell}$. Ved at foretage en Æ-operation adderes den k'te række i C til den første række $[a_{11}, 0, \dots, 0]$ i $\overline{A}$. Derefter foretages en søjleombytning, så vi får en matrix med $[a_{11}, c_{k\ell}, *, \dots, *]$ som første søjle, hvor $*$ betyder elementer i R. Dette argument viser, at vi kan antage:

$$\text{Enten er } a_{11} \nmid a_{12} \text{ eller } a_{11} \nmid a_{21}.$$

Vi betragter tilfældet hvor $a_{11} \nmid a_{21}$. Tilfældet $a_{11} \nmid a_{12}$ behandles analogt. Vi har før set, at a_{11} har det mindst mulige antal irreducible faktorer blandt elementerne i A, lad os sige d faktorer. Lad $Ra_{11} + Ra_{21} = Rb$, således at b er en sfd. af a_{11} og a_{21}. (Se Kapitel 4). Skriv $b = r_1a_{11} + r_2a_{21}$, hvor $r_1, r_2 \in R$. Nu må r_1 og r_2 være relativt prime, så $Rr_1 + Rr_2 = R$. (Overvej dette!) Vælg $s_1, s_2 \in R$ så $1 = r_1s_1 - r_2s_2$. (Hvorfor kan det gøres?) Sæt

$$X = \begin{bmatrix} r_1 & r_2 & 0 \\ s_2 & s_1 & \\ 0 & & E \end{bmatrix} \in R_m^n$$

hvor E er en $(m-2)\times(m-2)$ enhedsmatrix. Så er $XA \approx A$, da X er invertibel, og XA har $r_1a_{11}+r_2a_{21}=b$ på plads $(1,1)$. Nu er $b|a_{11}$ og b er ikke associeret til a_{11} (hvorfor?), så b har færre irreducible faktorer end a_{11}, altså højst $d-1$. Efter gentagelse af dette argument højst d gange opnås en matrix, som er ækvivalent til A og som har et invertibelt element på plads $(1,1)$. På denne matrix anvendes argumentet fra tilfælde 1*. □

Vi mangler at bevise entydighedsudsagnet fra (9.10) og gør dette ved at angive en algoritme, hvordan elementerne d_i i praksis kan beregnes, når A er givet.

(9.11) DEFINITION: Lad $A \in R_n^m$. Hvis $k \le m, k \le n$ er en $k\times k$-*delmatrix* af A en matrix der opnås fra A ved at slette $m-k$ rækker og $n-k$ søjler i A. Vi lader $\mathcal{D}_k(A)$ være mængden af $k\times k$-delmatricer i A. Endvidere defineres

$$D_k(A) = \sum_{B\in\mathcal{D}_k(A)} R(\det B)\,.$$

Dermed er $D_k(A)$ idealet i R, der er frembragt af elementerne $\det B$, $B\in\mathcal{D}_k(A)$. Med $\delta_k(A)$ betegnes et frembringende element for $D_k(A)$ og $\delta_k(A)$ er altså en sfd. af $\det B$, $B\in\mathcal{D}_k(A)$. ($\delta_k(A)$ er entydig pånær multiplikation med invertible elementer fra R). □

(9.12) EKSEMPEL:

$$\text{Lad } A = \begin{bmatrix}1&2&3\\4&5&6\end{bmatrix} \in \mathbb{Z}_3^2$$

$\delta_1(A)$ er en sfd. af $1,2,3,4,5,6$, altså f.eks. $\delta_1(A)=1$

$$\mathcal{D}_2(A) = \left\{\begin{bmatrix}1&2\\4&5\end{bmatrix}, \begin{bmatrix}1&3\\4&6\end{bmatrix}, \begin{bmatrix}2&3\\5&6\end{bmatrix}\right\}$$

så $\delta_2(A)$ er en sfd. af $-3,-6,-3$, altså f.eks. $\delta_2(A)=3$. □

(9.13) HJÆLPESÆTNING. *Lad $A\in R_n^m$, $k\le m, m\le n$, $k\ge 2$. Der gælder $D_k(A)\subseteqq D_{k-1}(A)$, og derfor $\delta_{k-1}(A)\mid\delta_k(A)$.*

BEVIS: Ifølge søjleudviklingsreglen for determinanter (jfr. bemærkningerne om determinanter i Kapitel 8) er determinanten af $B\in\mathcal{D}_k(A)$ en R-kombination af determinanter af matricer $C\in\mathcal{D}_{k-1}(A)$. Derfor er $\det B\in D_{k-1}(A)$ for alle $B\in\mathcal{D}_k(A)$. Heraf fås $D_k(A)\subseteqq D_{k-1}(A)$. □

(9.14) HJÆLPESÆTNING. *Lad $A\in R_n^m$, $k\le m, k\le n$. Lad $X\in R_m^m$, $Y\in R_n^n$. Der gælder $D_k(XAY)\subseteqq D_k(A)$ og derfor $\delta_k(A)\mid\delta_k(XAY)$.*

BEVIS: Det er tilstrækkeligt at vise $D_k(XA)\subseteq D_k(A)$ og $D_k(AY)\subseteq D_k(A)$, for så er

$$D_k(X(AY))\subseteq D_k(AY)\subseteq D_k(A)\,.$$

Vi nøjes med at vise $D_k(XA) \subseteq D_k(A)$ og lader den anden inklusion være en *øvelse*. Rækkerne i XA er R-linear kombinationer af rækkerne i A (jfr. HBF). Nu er determinantafbildningen R-lineær som funktion af matricens rækker (se f.eks. HBF 19.1(1). I vort tilfælde kan denne kendsgerning let udledes fra (8.25)). Derfor vil determinanten af $B \in \mathcal{D}_k(XA)$ være en R-linear kombination af determinanter af visse $C \in \mathcal{D}_k(A)$, altså $\det B \in D_k(A)$. Hermed er $D_k(XA) \subseteq D_k(A)$. □

(9.15) SÆTNING. *Hvis $A, B \in R_n^m$ og $A \approx B$, så er for $k \leq m, k \leq n$, $\delta_k(A)$ og $\delta_k(B)$ associerede i R.*

BEVIS: Umiddelbar følge af (9.14). □

(9.16) BEMÆRKNING. *Lad $D = \Delta(d_1, \ldots, d_k)$, hvor $d_1|d_2|\cdots|d_k$ og*

$$A = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix} \in R_n^m .$$

Så er $Rd_1 = R\delta_1(A)$, $Rd_1d_2 = R\delta_2(A), \ldots, Rd_1 \ldots d_k = R\delta_k(A)$ og $\delta_\ell(A) = 0$ for $\ell > k$.

BEVIS: Når $\ell > k$ indeholder $B \in \mathcal{D}_\ell(A)$ en nulsøjle, så $\det B = 0$. Når $\ell \leq k$ er de eneste matricer i $\mathcal{D}_\ell(A)$, som ikke indeholder en nulsøjle på formen $B = \Delta(d_{i_1}, \ldots, d_{i_\ell})$, $i_1 < i_2 < \cdots < i_\ell$. Ifølge divisionsbetingelsen for d_i'erne må $d_1 \cdots d_\ell \mid \det B$. Heraf følger, at $\delta_\ell(B) = d_1 \ldots d_\ell$, hvormed beviset afsluttes. □

Vi er nu i stand til at bevise entydighedsudsagnet i (9.10).

BEVIS FOR (9.10)(2): Antag, at

$$\overline{A} = \begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix} \approx \overline{A}' = \begin{bmatrix} D' & 0 \\ 0 & 0 \end{bmatrix}$$

hvor $D = \Delta(d_1, \ldots, d_k)$, $d_1|d_2|\cdots|d_k$, $d_k \neq 0$ og $D' = \Delta(d_1', \ldots, d_\ell')$, $d_1'|d_2'|\cdots d_\ell'$, $d_\ell' \neq 0$. Antag, at $k \leq \ell$. Hvis $k \neq \ell$ er $\delta_\ell(\overline{A}) = 0$ og $\delta_\ell(\overline{A}') \neq 0$ ifølge (9.16). Dette strider mod, at $\delta_\ell(\overline{A})$ og $\delta_\ell(\overline{A}')$ er associerede ifølge (9.15). Altså må $k = \ell$. Nu viser (9.15) og (9.16) at for $i = 1, \ldots, k$ er $d_1d_2 \ldots d_i$ og $d_1'd_2' \ldots d_i'$ associerede. Heraf ses det at d_i og d_i' er associerede for $1 \leq i \leq k$ (overvej dette!) □

(9.17) DEFINITION: Lad $A \in R_n^m$. Matricen $\begin{bmatrix} D & 0 \\ 0 & 0 \end{bmatrix}$ fra (9.10)(1) kaldes en *normalform for A*. Hvis $D = \Delta(d_1, d_2, \ldots, d_k)$, $d_k \neq 0$, kaldes $d_1, d_2, \ldots, d_k$ de *invariante faktorer* for A. Ifølge (9.10)(2) er de invariante faktorer entydige pånær multiplikation med invertible elementer. Tallet k kaldes *rangen* af A. □

(9.18) ØVELSE: Hvis R er et legeme, stemmer definitionen af rangen af $A \in \mathbb{R}_n^m$ givet i (9.17) overens med definitionen fra den lineære algebra (HBF). □

(9.19) BEMÆRKNING: Givet $A \in R_n^m$ kan man f.eks. beregne de invariante faktorer for A (og dermed A's normalform) på følgende måde: Beregn $\delta_1(A), \delta_2(A), \ldots, \delta_k(A)$ indtil $k = m$, $k = n$ eller $\delta_k(A) \neq 0$, $\delta_{k+1}(A) = 0$. Vi ved, at $\delta_1(A) | \delta_2(A) | \ldots | \delta_k(A)$. Så er $d_1 = \delta_1(A)$, $d_2 = \delta_2(A)/\delta_1(A), \ldots, d_k = \delta_k(A)/\delta_{k-1}(A)$ de invariante faktorer for A. En anden mulighed er at lave række- og søjleomformningen af type Æ og Å, jfr. (9.8) og (9.9) samt (hvis man mener at sagen forenkles) af type $\varnothing_i(c)$, hvor c da *skal være invertibel* i R, jfr. (9.7).

Man kan selvfølgelig også "blande" de nævnte metoder og f.eks. bruge række- og søjleomformninger til at skaffe mange nuller, hvilket gør beregningen af $\delta_i(A)$ lettere. □

(9.20) EKSEMPLER: Vi har tidligere set forskellige eksempler på hovedidealringe, f.eks. $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{-2}]$ samt $L[t]$ når L er et legeme. Disse ringe er endda Euklidiske (se Kapitel 4). Vi kan således lade R være en af disse ringe.
(1) Hvis A er som i (9.12) er

$$A \approx \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{bmatrix}$$

så 1 og 3 er de invariante faktorer. En anden mulighed er

$$\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix} \underset{R}{\approx} \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 0 \end{bmatrix} \underset{R}{\approx} \begin{bmatrix} 3 & 3 & 3 \\ 2 & 1 & 0 \end{bmatrix} \underset{S}{\approx} \begin{bmatrix} 0 & 0 & 3 \\ 2 & 1 & 0 \end{bmatrix}$$
$$\underset{S}{\approx} \begin{bmatrix} 0 & 0 & 3 \\ 0 & 1 & 0 \end{bmatrix} \approx \begin{bmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \end{bmatrix}$$

(Her betyder $\approx_R$ rækkeoperationer, $\approx_S$ søjleoperationer af type Æ.)
(2)

$$B = \begin{bmatrix} 2+2i & 2 \\ 1+3i & 3+i \end{bmatrix} \in R_2^2, \quad R = \mathbb{Z}[i].$$

B har $(1+i)$ og 2 som invariante faktorer: Da $2+2i = 2(1+i)$, $2 = (1-i)(1+i)$, $1+3i = (2+i)(1+i)$ og $3+i = (2-i)(1+i)$ er $1+i$ en sfd. af B's elementer, altså $d_1 = \delta_1(B) = (1+i)$. Endvidere er

$$\delta_2(B) = \det B = (2+2i)(3+i) - 2(1+3i) = 4+8i-2-6i = 2(1+i), \text{ så } d_2 = 2.$$

I dette eksempel er det måske nemmere at starte med at trække i gange den anden søjle i B fra den første. Vi får

$$B \approx \begin{bmatrix} 2 & 2 \\ 2 & 3+i \end{bmatrix} \underset{S}{\approx} \begin{bmatrix} 2 & 0 \\ 2 & 1+i \end{bmatrix} \underset{R}{\approx} \begin{bmatrix} 2 & 0 \\ 0 & 1+i \end{bmatrix} \approx \begin{bmatrix} 1+i & 0 \\ 0 & 2 \end{bmatrix}$$

(3)

$$C = \begin{bmatrix} t+3 & t & t+2 \\ 0 & t+1 & 0 \\ 1 & t^3 & 1 \end{bmatrix} \in R_3^3, \quad R = \mathbb{Q}[t].$$

Da f.eks. $t+3$ og t er relativt prime er $\delta_1(C)=1$. Da

$$\det\begin{bmatrix} t+3 & t+2 \\ 1 & 1 \end{bmatrix} = 1 \quad \text{er} \quad \delta_2(C)=1.$$

Endvidere er $\det C = t+1$, så de invariante faktorer fra C er $1,1,t+1$. Det bør selvfølgelig bemærkes, at det i dette tilfælde var overflødigt at beregne $\delta_1(C), \delta_2(C)$ idet jo $\delta_3(C)=t+1$ er et irreducibelt element i R. □

(9.21) OPGAVE: Antag, at $A \in R_n^n$. Antag, at $\det A = p\cdot q$ hvor p og q er forskellige (ikke-associerede) irreducible elementer i R. Bestem A's invariante faktorer og A's normalform. Hvilke muligheder er der, hvis $p=q$? □

(9.22) OPGAVE: Beregn en normalform og de invariante faktorer for $\mathbb{Z}$-matricen

$$\begin{bmatrix} 6 & 2 & 3 & 0 \\ 2 & 3 & -4 & 1 \\ -3 & 3 & 1 & 2 \\ -1 & 2 & -3 & 5 \end{bmatrix}.$$

□

(9.23) OPGAVE: Beregn en normalform og de invariante faktorer for $\mathbb{Z}[i]$-matricen

$$\begin{bmatrix} 7+16i & 9+7i \\ 1+3i & 2+i \end{bmatrix}$$

□

(9.24) OPGAVE: Beregn en normalform og de invariante faktorer for $\mathbb{Q}[t]$-matricen

$$\begin{bmatrix} t^2+3t-2 & t^2+t-2 & t-1 \\ t+3 & t+2 & 1 \end{bmatrix}$$

□

Vi går nu igang med strukturteorien for endeligt frembragte R-moduler. Først beskriver vi den (indre) *direkte sum* af moduler som svarer til det (indre) direkte produkt $\boxtimes$ af grupper (Kapitel 7, 4°).

(9.25) DEFINITION: (Jfr. (7.5)) Lad $M_1, M_2, \ldots, M_n$ være undermoduler af R-modulen M, således at der gælder

(1) For alle $x \in M$ eksisterer $x_1 \in M_1, \ldots, x_n \in M_n$ så $x = x_1 + \cdots + x_n$.
(2) Hvis $x_i, y_i \in M_i$, $1 \leq i \leq n$ og $x_1 + \cdots + x_n = y_1 + \cdots + y_n$, gælder $x_i = y_i$ for $1 \leq i \leq n$.

Så kaldes M en (indre) *direkte sum* af undermodulerne $M_1, \ldots, M_n$ og vi skriver

$$M = M_1 \oplus \cdots \oplus M_n .$$

□

I analogi med (7.6) har vi

(9.26) SÆTNING. *Lad $M_1, M_2, \ldots, M_n$ være undermoduler af R-modulen M. Der gælder*

$$\begin{array}{l} M = M \oplus \cdots \oplus M_n \\ \Updownarrow \\ \begin{cases} (1) & M = M_1 + \cdots + M_n \\ (2) & \text{For } 2 \leq i \leq n \text{ gælder } M_i \cap (M_1 + \cdots + M_{i-1}) = \{0\} \end{cases} \end{array}$$

(9.27) ØVELSE: Bevis (9.26). □

(9.28) DEFINITION: R-modulen M kaldes *dekomposabel* hvis der findes undermoduler M_1, M_2 af M med $M_1 \neq \{0\}$ og $M_2 \neq \{0\}$, således at $M = M_1 \oplus M_2$. Hvis M *ikke* er dekomposabel, kaldes M *indekomposabel*. □

Lad os bemærke, at (9.25)–(9.28) selvfølgelig har mening og gælder for moduler over vilkårlige ringe.

Først ser vi, hvad (9.10) betyder for undermoduler af fri moduler.

(9.29) SÆTNING. *Lad M være en fri R-modul af rang $n < \infty$, N en undermodul af M. Der eksisterer en basis $\{z_1, \ldots, z_n\}$ for M og $d_1, \ldots, d_m \in R \setminus \{0\}$, således at $d_1 | d_2 | \ldots | d_m$ og $\{d_1 z_1, \ldots, d_m z_m\}$ er en basis for N. (Så N har rang m).*

BEVIS: Lad $\{x_1, \ldots, x_n\}$ være en basis for M og $\{y_1, \ldots, y_m\}$ en basis for N (Jfr. (9.3)). Skriv for $1 \leq i \leq m$

$$(1) \qquad y_i = \sum_{j=1}^{n} a_{ij} x_j$$

således at $A = [a_{ij}] \in R_n^m$. Ifølge (9.10) eksisterer invertible matricer $X \in R_m^m$, $Y \in R_n^n$ således at

$$XAY^{-1} = \left[\begin{array}{c|c} D & 0 \end{array}\right], D = \Delta(d_1, \ldots, d_m),\ d_1 | \ldots | d_m . \tag{2}$$

Da X er invertibel, er $\{z_1', \ldots, z_m'\}$ en basis for N hvor $X = [r_{ij}]$ og

$$z_i' = \sum_{j=1}^{m} r_{ij} y_j . \tag{3}$$

Tilsvarende er $\{z_1, \ldots, z_n\}$ en basis for M, hvor $Y = [s_{ij}]$ og

$$z_i = \sum_{j=1}^{n} s_{ij} x_j . \tag{4}$$

Ved hjælp af (3), (1) og (4) skrives z_i''erne som linearkombinationer af $z_1, \ldots, z_n$. (Bemærk, at Y^{-1} er transformationsmatricen, når man skriver x_j'erne som linearkombinationer af z_i'erne.) Vi får $z_i' = \sum b_{ij} z_j$, hvor $B = [b_{ij}] = XAY^{-1}$. Derfor er $z_i' = d_i z_i$, $1 \leq i \leq m$ som ønsket. Det er nu klart at $d_i \neq 0$ for $1 \leq i \leq m$. □

(9.30) DEFINITION: Lad M være en R-modul. For $x \in M$ sættes

$$\mathrm{Ann}(x) = \{r \in R \mid rx = 0\}$$

(*annihilatoren* af x.) Endvidere er $\mathrm{Ann}(M) = \cap_{x \in M} \mathrm{Ann}(x)$. Ifølge (8.12) er $\mathrm{Ann}(x)$ et ideal i R. (Husk, at R er kommutativ). Hvis $\mathrm{Ann}(x) \neq \{0\}$ kaldes x et *torsionselement* og vi sætter

$$M_{\mathrm{tor}} = \{x \in M \mid x \text{ torsionselement}\} .$$

Så er M_{tor} en undermodul af M (ifølge (8.11)), kaldet *torsionsundermodulen* af M. Hvis $M_{\mathrm{tor}} = \{0\}$ kaldes M *torsionsfri*. Det er let at se, at faktormodulen M/M_{tor} er torsionsfri (Overvej dette!) □

(9.31) ØVELSE: En fri modul er torsionsfri. □

(9.32) SÆTNING. *Lad M være en endeligt frembragt R-modul. Der eksisterer en fri undermodul F af M af endelig rang, således at*

$$M = M_{\mathrm{tor}} \oplus F .$$

BEVIS: Lad $M = \mathrm{span}(x_1, \ldots, x_n)$. Betragt som i (8.24) R-modul epimorfien $\varphi : R^n \to M$ defineret ved

$$\varphi(r_1, \ldots, r_n) = \sum_{i=1}^{n} r_i x_i .$$

Selvfølgelig er R^n en fri R-modul og $N = \ker\varphi$ en undermodul af R^n. Ifølge (9.29) eksisterer en basis $z_1, \ldots, z_n$ for R^n og $d_1, d_2, \ldots, d_m \in R$ med $d_1|d_2|\ldots|d_m$ således at $\{d_1z_1, \ldots, d_mz_m\}$ er en basis for N. Nu er $F_1 = \text{span}(z_{m+1}, \ldots, z_n)$ en undermodul af R^n og dermed $F = \varphi(F_1)$ en undermodul af M. Betragt homomorfien $\varphi_1 : F_1 \to F$ givet ved $x \mapsto \varphi(x)$ for $x \in F_1$ (indskrænkningen af φ til F_1). Det er klart, at φ_1 er surjektiv. Hvis $x \in \ker\varphi_1$ er $\varphi(x) = 0$, så

$$x \in \ker\varphi \cap F_1 = \text{span}(d_1z_1, \ldots, d_mz_m) \cap \text{span}(z_{m+1}, \ldots, z_n)\,.$$

Da $z_1, z_2, \ldots, z_n$ er lineært uafhængige, fås let heraf at $x = 0$ (Overvej dette nøje). Hermed er φ_1 også injektiv, således at φ_1 er en isomorfi. Da F_1 er en fri modul, er F også fri.

Lad $a \in M$. Vælg $x \in R^n$ med $\varphi(x) = a$. Skriv x som linearkombination af basiselementerne $z_1, \ldots, z_n$ for M,

$$x = r_1z_1 + \cdots + r_nz_n\,, \quad r_i \in R\,.$$

Lad $x_1 = r_1z_1 + \cdots + r_mz_m$, $x_2 = r_{m+1}z_{m+1} + \cdots + r_nz_n$ og $a_i = \varphi(x_i)$, $i = 1, 2$. Så er $a_2 \in F$. Endvidere er $a_1 \in M_{\text{tor}}$, idet $d_m \in \text{Ann}(a_i)$: Da $d_i|d_m$, $1 \le i \le m$, kan vi skrive $d_m = d_ie_i$, $e_i \in R$. Så er

$$d_mx_1 = \sum_{i=1}^{m}(r_ie_i)(d_iz_i) \in \text{span}(d_1z_1, \ldots, d_mz_m) = N\,,$$

altså $0 = \varphi(d_mx_1) = d_m\varphi(x_1) = d_ma_1$. Da $a = a_1 + a_2$, $a_1 \in M_{\text{tor}}$, $a_2 \in F$ har vi vist, at

$$M = M_{\text{tor}} + F\,.$$

Ifølge (9.31) er $M_{\text{tor}} \cap F = \{0\}$, så $M = M_{\text{tor}} \oplus F$ ifølge (9.26). □

(9.33) ØVELSE: Vis, at R er indekomposabel som R-modul. □

(9.34) ØVELSE: Lad M være en endelig frembragt R-modul. Antag, at F og F_1 er frie undermoduler af M, således at

$$M = M_{\text{tor}} \oplus F = M_{\text{tor}} \oplus F_1\,.$$

Vis, at F og F_1 har samme rang. □

(9.35) ØVELSE: Antag, at den fri R-modul F har basis $\{x_1, \ldots, x_n\}$. Vis

$$M = Rx_1 \oplus \cdots \oplus Rx_n\,.$$

og at $Rx_i \simeq R$ som R-modul. □

De ovenstående øvelser viser, at en fri R-modul af rang n er en direkte sum af n indekomposable moduler, som hver er isomorfe til R. For at afslutte vores undersøgelse af strukturen af endeligt frembragte R-moduler M_1, kan vi derfor koncentrere os om at forstå torsionsdelen og kan antage $M = M_{\text{tor}}$. I dette tilfælde er modulen F fra (9.32) lig 0. Hvis $M = M_{\text{tor}}$ kaldes M en *torsionsmodul*.

(9.36) SÆTNING. *Lad M være en endeligt frembragt R-torsionsmodul. Der eksisterer elementer $y_1, y_2, \ldots, y_m \in M$, $d_1, \ldots, d_m \in R$ således at*

(1) $M = Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_m$
(2) $d_1 | d_2 | \ldots | d_m$, *d_i ikke invertibel*, $d_i \neq 0$, $1 \leq i \leq m$
(3) $\mathrm{Ann}(y_i) = Rd_i$, $1 \leq i \leq m$.

BEVIS: Vælg en frembringermængde $\{x_1, \ldots, x_m\}$ for M med færrest mulig elementer ([MIN]), $M = \mathrm{span}(x_1, \ldots, x_m)$. Lad $\varphi : R^m \to M$ være epimorfien fra (8.24) og $N = \ker \varphi$. Som i beviset for (9.32) eksisterer en basis $z_1, \ldots, z_m$ for R^m og elementer $d_1, d_2, \ldots, d_{m'} \in R$ med $d_1 | d_2 | \ldots | d_{m'}$, således at $\{d_1 z_1, \ldots, d_{m'} z_{m'}\}$ er en basis for N. Beviset for (9.32) viser, at M må indeholde en fri undermodul af rang $m - m'$. Da M er en torsionsmodul fås $m = m'$. Sæt $y_i = \varphi(z_i)$, $1 \leq i \leq m$. Da φ er en epimorfi er

$$M = \mathrm{span}(y_1, \ldots, y_m) = Ry_1 + Ry_2 + \cdots + Ry_m .$$

Lad $r \in R$. Der gælder for $1 \leq i \leq m$

$$\begin{aligned} r \in \mathrm{Ann}(y_i) &\Leftrightarrow ry_i = 0 \\ &\Leftrightarrow r\varphi(z_i) = \varphi(rz_i) = 0 \\ &\Leftrightarrow rz_i \in N \\ &\Leftrightarrow d_i \mid r . \end{aligned}$$

(Overvej den sidste "$\Leftrightarrow$". Man bruger, at $d_i z_i$ er et basiselement for N). Vi har hermed vist, at $\mathrm{Ann}(y_i) = Rd_i$, altså (3). Hvis $d_i = 0$ er $y_i \in M$ ikke et torsionselement, en modstrid. Hvis d_i er invertibel, er $Rd_i = R$, hvorfor $y_i = 0$. Det ville betyde, at $\{y_1, \ldots, y_{i-1}, y_{i+1}, \ldots, y_m\}$ er en frembringermængde for M med $m - 1$ elementer, også en modstrid. For at vise at summen i (1) er direkte viser vi:

Hvis $r_1, \ldots, r_m \in R$ og $r_1 y_1 + \cdots + r_m y_m = 0$, så er $r_i y_i = 0$, $1 \leq i \leq m$.

Antag $\sum_{i=1}^m r_i y_i = 0$, $r_i \in R$. Så er $\varphi(\sum_{i=1}^m r_i z_i) = 0$, altså $\sum_i^m r_i z_i \in N$. Da $\{d_1 z_1, \ldots, d_m z_m\}$ er en basis for N, eksisterer $s_1, \ldots, s_m \in R$ så $\sum_i s_i (d_i z_i) = \sum_i r_i z_i$. Da $\{z_1, \ldots, z_m\}$ er en basis for R^m, fås $r_i = s_i d_i$, $1 \leq i \leq m$. Det betyder, at

$$r_i y_i = s_i d_i y_i = s_i \varphi(d_i z_i) = s_i 0 = 0 ,$$

da $d_i z_i \in N = \ker \varphi$. □

Vi sammenfatter de hidtidige resultater:

(9.37) SÆTNING. *(Struktursætningen) Lad M være en endeligt frembragt R-modul. Der eksisterer*
$y_1, y_2, \ldots, y_n \in M$, $d_1, \ldots, d_n \in R$ således at

(1) $M = Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_n$
(2) $d_1 | d_2 | \ldots | d_n$, *d_i ikke invertibel*, $1 \leq i \leq n$
(3) $\mathrm{Ann}(y_i) = Rd_i$, $1 \leq i \leq n$.

BEVIS: Den eneste forskel mellem (1)–(3) i (9.36) og i (9.37) er udeladelsen af betingelsen $d_i \neq 0$ i (9.37)(2). Ifølge (9.32) er $M = M_{\text{tor}} \oplus F$. Skriv $M_{\text{tor}} = Ry_1 \oplus \cdots \oplus Ry_m$ som i (9.36) og $F = Ry_{m+1} \oplus \cdots \oplus Ry_n$ (jfr. (9.35); rangen af F er $n - m$). Hvis $\text{Ann}(y_i) = Rd_i$, $1 \leq i \leq n$ gælder $d_1 | \ldots | d_m$ ifølge (9.36) og $d_{m+1} = \cdots = d_n = 0$. □

En endeligt frembragt R-modul er altså direkte sum af cykliske moduler (moduler frembragt af et element). Man kan spørge om en cyklisk R-modul er indekomposabel. Hvis $M = Ry$ er cyklisk og y ikke er et torsionselement ($\text{Ann}(y) = \{0\}$) er M indekomposabel ifølge (9.33), idet jo $Ry \simeq R$ som R-modul. Men hvis y er et torsionselement, ser det anderledes ud.

(9.38) SÆTNING. *Lad $M = Ry$ være en cyklisk torsionsmodul med $\text{Ann}(y) = Rd$, $d \neq 0$. Antag, at $d = ab$, hvor $a, b \in R$ er relativt prime (altså $Ra + Rb = R$; eller sfd. af a og b er 1). Så gælder*

$$M = Ry = Ray \oplus Rby\,.$$

og $\text{Ann}(ay) = Rb\,, \text{Ann}(by) = Ra$.

BEVIS: Skriv $1 = ra + sb$. Så er $y = r(ay) + s(by) \in Ray + Rby$, således at $Ry \subseteq Ray + Rby$. Da trivielt $Ray \subseteq Ry$, $Rby \subseteq Ry$ fås $Ry = Ray + Rby$. Vi mangler at vise, at $Ray \cap Rby = \{0\}$. Lad altså $z \in Ray \cap Rby$. Skriv $z = tay = uby$, hvor $t, u \in R$. Så er $(ta - ub)y = 0$, altså $(ta - ub) \in \text{Ann}(y) = Rd$. Vi får at $d = ab \mid ta - ub$, og derfor er $b \mid ta$ (overvej!) Vi får $b \mid t$ (overvej!), altså $t = t'b$. Så er $z = tay = t'dy = 0$, da $dy = 0$. Udsagnene om $\text{Ann}(ay)$ og $\text{Ann}(by)$ er oplagte. □

(9.39) BEMÆRKNING: Her gøres rede for, at resultatet i (7.68) er indeholdt i (9.38). Som nævnt i (8.5)(1) er en $\mathbb{Z}$-modul det samme som en abelsk gruppe. Ringen $\mathbb{Z}$ er jo en hovedidealring og en cyklisk $\mathbb{Z}$-modul er det samme som en cyklisk gruppe. Lad os betragte den cykliske gruppe $G = \langle y \rangle$, så $G = \{y^m \mid m \in \mathbb{Z}\}$. Derfor er (jfr. (8.5)(1)) $\text{Ann}(y) = \{m \mid y^m = 1\}$. Ifølge (6.19) er $\text{Ann}(y) = 0 \Leftrightarrow |y| = \infty$. Og hvis $|y| = d < \infty$ er $\text{Ann}(y) = Rd$. (Se (6.21)!) Ved at sammenligne definitionerne ses det umiddelbart ☒ for (multiplikativt skrevne) abelske grupper svarer til $\oplus$ for (additivt skrevne) $\mathbb{Z}$-moduler. Hvis $|y| = d$ svarer $(\langle y \rangle, \cdot)$ til $(\mathbb{Z}_d, +)$. Så (7.68) er den multiplikative skrevne version af et specielt tilfælde af (9.38) med $R = \mathbb{Z}$. □

(9.40) DEFINITION: Lad M være en R-modul og $p \in R$ et primelement (= irreducibelt element, jfr. Kapitel 4). M kaldes *p-primær*, hvis der findes et $n \in \mathbb{N}$, således at $\text{Ann}(M) = Rp^n$. Modulen M kaldes primær, hvis der findes et primelement $p \in R$, således at M er p-primær. Bemærk at primære moduler er torsionsmoduler. □

(9.41) SÆTNING. *En endeligt frembragt R-torsionsmodul er en direkte sum af endelig mange primære moduler.*

BEVIS: Ifølge (9.36) er det tilstrækkeligt at vise sætningen for cykliske torsionsmoduler. Hvis $M = Ry$, $\text{Ann}(y) = Rd$, findes endelig mange forskellige (dvs. parvis

ikke-associerede) primelementer $p_1, p_2, \ldots, p_r$ og naturlige tal $n_1, \ldots, n_r$ således at d er associeret til ${p_1}^{n_1}{p_2}^{n_2}\ldots{p_r}^{n_r}$ (jfr. (4.25)). Ved gentagen anvendelse af (9.38) ses at $Ry = Ry_1 \oplus \cdots \oplus Ry_r$, hvor Ry_i er p_i-primær: Vælg i (9.38) $a = {p_2}^{n_2}\ldots{p_r}^{n_r}$, $b = {p_1}^{n_1}$. Så er $Ry = Ray \oplus Rby$, hvor Ray er p_1-primær og $\mathrm{Ann}(by) = R{p_2}^{n_2}\ldots{p_r}^{n_r}$. Hvis $r \geq 3$ kan vi anvende (9.38) på Rby og dekomponere den yderligere. □

(9.42) ØVELSE: Lad M være en endeligt frembragt R-torsionsmodul. Lad $p \in R$ være et primelement. Sæt

$$M_p = \{y \in M \mid \text{Der findes } e \in \mathbb{N} \text{ så } p^e y = 0\}.$$

Vis

(1) M_p er en undermodul af M
(2) Der findes endelig mange primelementer $p_1, p_2, \ldots, p_r \in R$ således at

$$M = M_{p_1} \oplus M_{p_2} \oplus \cdots \oplus M_{p_r}.$$

□

(9.43) ØVELSE: Lad y være et element i en R-modul. Lad $\mathrm{Ann}(y) = Rd$. Vis

$$R/Rd \simeq Ry$$

som R-moduler. □

(9.44) ØVELSE: Lad y være et torsionselement i en R-modul. Vis

$$Ry \text{ er indekomposabel } \Leftrightarrow Ry \text{ er primær}.$$

□

(9.45) SÆTNING. *Lad M være en p-primær endelig frembragt R-modul.*
(1) Der findes $y_1, y_2, \ldots, y_n \in M$ og $e_1 \leq e_2 \leq \cdots \leq e_n \in \mathbb{N}$ således at

$$M = Ry_1 \oplus \cdots \oplus Ry_n.$$

og

$$\mathrm{Ann}(y_i) = Rp^{e_i}, \quad 1 \leq i \leq n.$$

(2) Hvis yderligere $y'_1, y'_2, \ldots, y'_m \in M$ og $e'_1 \leq e'_2 \leq \cdots \leq e'_m \in \mathbb{N}$ således at

$$M = Ry'_1 \oplus \cdots \oplus Ry'_m$$

og

$$\mathrm{Ann}(y'_i) = Rp^{e'_i}, \quad 1 \leq i \leq m$$

gælder $n = m$ *og* $e_i = e_i'$ *for* $1 \leq i \leq n$.

BEVIS: (1) følger umiddelbart fra (9.36) og definitionen af p-primær.

(2) bevises med den metode, der blev anvendt i øvelserne (8.45)–(8.49): For $e \in \mathbb{N}$ sættes $M^{(e)} = p^e M$. Ifølge (8.45)–(8.46) (eller det ses direkte) er $M^{(e)}$ en undermodul af M. Det er klart, at

$$\cdots \subseteq M^{(e)} \subseteq \cdots \subseteq M^{(1)} \subseteq M^{(0)} = M$$

og ifølge (8.47) er $\overline{M}^{(e)} = M^{(e)}/M^{(e+1)}$ en $\overline{R} = R/Rp$-modul. Ifølge (4.28) og (3.29) er $\overline{R}$ et legeme. Vi påstår, at

$$\dim_{\overline{R}} \overline{M}^{(e)} = |\{i \mid e_i > e\}|$$

og

$$\dim_{\overline{R}} \overline{M}^{(e)} = |\{i \mid e_i' > e\}|$$

Heraf følger påstandene $n = m$, $e_i = e_i'$ let. Da definitionen af $\overline{M}^{(e)}$ ikke afhænger af de frembringende elementer for M er det tilstrækkeligt at vise $\dim \overline{M}^{(e)} = |\{i \mid e_i > e\}|$ for alle $e \geq 0$.

Da $M = Ry_1 \oplus \cdots \oplus Ry_n$ er det let at se, at $M^{(e)} = p^e M = Rp^e y_1 \oplus \cdots \oplus Rp^e y_n$.

Lad os sætte $\overline{M}_i^{(e)} = Rp^e y_i + M^{(e+1)}/M^{(e+1)} \subseteq \overline{M}^{(e)}$. Der gælder, at

$$\overline{M}^{(e)} = \overline{M}_1^{(e)} \oplus \cdots \oplus \overline{M}_n^{(e)}\,.$$

Dette ses ved anvendelse af (9.26): Betingelsen (9.26)(1) følger af at $M^{(e)} = Rp^e y_1 + \cdots + Rp^e y_n$. Endvidere er $Rp^e y_i \cap (Rp^e y_1 + \cdots + Rp^e y_{i-1} + M^{(e+1)}) \subseteq M^{(e+1)}$ (overvej dette), hvoraf betingelsen (9.26) kan udledes. Nu er $\overline{M}_i^{(e)}$ en cyklisk $\overline{R}$-modul, frembragt af $p^e y_i + M^{(e+1)}$. Derfor $\dim \overline{M}_i^{(e)} = 0$, hvis $\overline{M}_i^{(e)} = 0$ og $\dim \overline{M}_i^{(e)} = 1$, hvis $\overline{M}_i^{(e)} \neq 0$. Men

$$\begin{aligned} \overline{M}_i^{(e)} &= Rp^e y_i + M^{(e+1)}/M^{(e+1)} \\ &\simeq Rp^e y_i / Rp^e y_i \cap M^{(e+1)} \\ &= Rp^e y_i / Rp^{e+1} y_i \end{aligned}$$

så

$$\overline{M}_i^{(e)} \neq 0 \Leftrightarrow Rp^e y_i \neq 0 \Leftrightarrow e_i > e\,.$$

Da $\dim \overline{M}^{(e)} = \sum_i \dim \overline{M}_i^{(e)}$ fås resultatet. □

Vi sammenfatter de ovenstående resultater i

(9.46) SÆTNING. *(Invarianssætningen) En endelig frembragt R-modul M er en direkte sum af en fri modul F og endelig mange primære moduler $M_{p_1}, \ldots, M_{p_r}$ hvor $p_i \neq p_j$ for $i \neq j$. Hvert M_{p_i} er en direkte sum af endelig mange cykliske moduler. Rangen af F og antallet af cykliske summander i hvert M_{p_i} samt deres annihilatorer er entydigt bestemt ved M.*

□

Vi betragter til sidst nogle anvendelser af teorien, der er blevet beskrevet i dette kapitel.

Lad os først formulere invarianssætningen for $\mathbb{Z}$-moduler = abelske grupper.

(9.47) SÆTNING. *(Hovedsætningen for endeligt frembragte abelske grupper) En endeligt frembragt abelsk gruppe G er et (indre) direkte produkt*

$$G = F \boxtimes T$$

hvor T er en endelig abelsk gruppe og F endeligt frembragt en fri abelsk gruppe (dvs. et indre direkte produkt af endeligt mange cykliske grupper af uendelig orden). En endelig abelsk gruppe T er et direkte produkt af endelig mange cykliske grupper af primtalspotensorden. Antallet af cykliske faktorer i F og antallet af cykliske faktorer i T af en given primtalpotensorden er entydigt bestemt ved G.

BEVIS: Følger fra (9.46) og bemærkningerne i (9.39). □

(9.48) ØVELSE: Lad p være et primtal. Vis, at der (pånær isomorfi) findes netop 2 abelske grupper af orden p^2, 3 af orden p^3 og 5 af orden p^4. □

(9.49) ØVELSE: Beregn antallet af isomorfiklasser af abelske grupper af orden 12,24, 30,36 og 60. □

Vi vil også se på nogle interessante anvendelser i den lineære algebra. Først en smule forberedelse.

(9.50) DEFINITIONER: Lad $R[t]$ være polynomiumsringen i R. Et polynomium $p(t) \in R[t]$ kaldes *monisk*, hvis højestegradskoefficienten er 1. Det betyder, at $p(t) = t^n + b_{n-1}t^{n-1} + \cdots + b_0$, $b_i \in R$, $\deg(p) = n$. Hvis $p(t) = t^n + b_{n-1}t^{n-1} + \cdots + b_0$ er et monisk polynomium, betegner $A_p \in R_n^n$ matricen

$$A_p = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \ldots & 1 \\ -b_0 & -b_1 & -b_2 & \ldots & -b_{n-1} \end{bmatrix}$$

og A_p kaldes p's *ledsagematrix*. F.eks. har $t^3 + 2t^2 - t + 5$ ledsagematricen

$$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -5 & 1 & -2 \end{bmatrix}$$

□

(9.51) ØVELSE: Vis, at $p(t) \in R[t]$ er associeret til et monisk polynomium i $R[t]$ hvis og kun hvis p's højestegradskoefficient er invertibel i R. Hvad betyder dette, når R er et legeme? □

(9.52) ØVELSE: Lad $p(t) \in R[t]$ være monisk. Vis, at

$$\det(tE - A_p) = p(t)\,,$$

hvor E er en enhedsmatrix. (Løsningsforslag: Induktion efter $deg(p)$. Man kan udvikle $\det(tE - A_p)$ efter første søjle!) Denne øvelse viser, at A_p har $(-1)^n p(t)$ som karakterisktisk polynomium (jfr. HBF, Kapitel 21), og at $\det(-A_p) = p(0) = b_0$ (konstantleddet). □

(9.53) BEMÆRKNING: Lad $n \in \mathbb{N}$. Vi forklarer hvordan man kan *indsætte* en matrix $A \in R_n^n$ i et polynomium $p(t) \in R[t]$. Afbildningen $\Delta^n : R \to R_n^n$ givet ved $\Delta^n(a) = \Delta(a, a, \ldots, a)$ (der afbilder a i en diagonalmatrix med a i diagonalen) er en ringmonomorfi, der ifølge Kapitel 5, 2° inducerer en ringmonomorfi $\Delta_t^n : R[t] \to R_n^n[t]$. Man kan derfor indsætte $A \in R_n^n$ i $\Delta_t^n\, p(t)$, jfr. (4.34), så

$$p(A) = \varphi_A\,(\Delta_t^n\, p(t))\ .$$

Dette er en eksakt, men lidt besværlig beskrivelse af noget meget enkelt, der bedst illustreres ved et eksempel: Lad

$$A = \begin{bmatrix} 3 & -1 \\ -2 & 1 \end{bmatrix} \in \mathbb{Z}_2^2\,, p(t) = 5 + 2t - t^2 \in \mathbb{Z}[t]\,.$$

Vi har $A^2 = AA = \begin{bmatrix} 11 & -4 \\ -8 & 3 \end{bmatrix}$, således at

$$\begin{aligned} p(A) = 5E + 2A - A^2 &= \begin{bmatrix} 5 & 0 \\ 0 & 5 \end{bmatrix} + \begin{bmatrix} 6 & -2 \\ -4 & 2 \end{bmatrix} - \begin{bmatrix} 11 & -4 \\ -8 & 3 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 2 \\ 4 & 4 \end{bmatrix} \in \mathbb{Z}_2^2\,. \end{aligned}$$

Det er klart, at afbildningen $R[t] \to R_n^n : p \mapsto p(A)$ er en ringhomomorfi, som vi også (lidt upræcist) vil kalde φ_A. $(\varphi_A(p) = p(A))$. □

(9.54) ØVELSE: Lad $A = \begin{bmatrix} 2 & 3 \\ -1 & 1 \end{bmatrix} \in \mathbb{Z}_2^2$, $p(t) = t^2 - 3t + 5$. Beregn $p(A)$. □

(9.55) DEFINITIONER: Lad $n \in \mathbb{N}$. Afbildningen

$$\mu : R_n^n \to \mathrm{End}(R_1^n)$$

givet ved $\mu(A)v = Av$ (matrixmultiplikation) er en ringhomomorfi (jfr. (8.2)(3)), så matrixmultiplikation gør R_1^n til en R_n^n-modul. Når $A \in R_n^n$ er $\varphi_A : R[t] \to R_n^n$ en ringhomomorfi. Det er $\mu \circ \varphi_A : R[t] \to \mathrm{End}(R_1^n)$ altså også. Derfor giver $\mu \circ \varphi_A$ en $R[t]$-modulstruktur på R_1^n. Vi betegner R_1^n med denne $R[t]$-modulstruktur som M_A. Så hvis $v \in M_A$ og $p(t) = b_n t^n + \cdots + b_0 \in R[t]$, er

$$p(t)v = b_n A^n v + \cdots + b_0 v = p(A)v\,.$$

□

(9.55) EKSEMPEL: Lad $A = \begin{bmatrix} 3 & -1 \\ -2 & 1 \end{bmatrix} \in \mathbb{Z}_2^2$. Lad $p(t) = 5 + 2t - t^2$. Så er $p(A) = \begin{bmatrix} 0 & 2 \\ 4 & 4 \end{bmatrix}$. Hvis $\begin{bmatrix} -1 \\ 1 \end{bmatrix} \in M_A$ er

$$p(t)\begin{bmatrix} -1 \\ 1 \end{bmatrix} = p(A)\begin{bmatrix} -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 4 & 4 \end{bmatrix}\begin{bmatrix} -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 0 \end{bmatrix}$$

□

(9.56) ØVELSE: Lad M_A være som i (9.54). Vis, at M_A er endeligt frembragt. □

For at kunne anvende den ovenstående strukturteori på den endeligt frembragte $R[t]$-modul M_A $(A \in R_n^n)$ skal $R[t]$ være en hovedidealring. Dette er netop da tilfældet, når R er et *legeme* ((4.35)). Alligevel vil det være muligt at anvende de følgende resultater (med forsigtighed) på matricer med koefficienter fra en *integritetsring* R, idet denne jo kan indlejres i et legeme, brøklegemet $Q(R)$ (jfr. (5.7)); så $R_n^n \subseteq Q(R)_n^n$.

Fra nu af er L et *legeme* og vi betragter matricer $A \in L_n^n$ og lineære afbildninger mellem L-vektorrum.

(9.57) SÆTNING. *Lad $A \in L_n^n$. $L[t]$-modulen M_A er en endeligt frembragt torsionsmodul.*

BEVIS: Ifølge (9.56) er M_A endeligt frembragt. Lad $v \in M_A$. Så er elementerne $v, Av, A^2v, \ldots, A^nv$ i M_A lineært afhængige over L, da $\dim_L M_A = n$. Hvis derfor $b_0 v + b_1(Av) + \cdots + b_n^n(A^n v) = 0$, hvor $b_0, b_1, \ldots, b_n$ ikke alle er 0, er

$$0 \neq p(t) = \sum_{i=0}^{n} b_i t^i \in \mathrm{Ann}(v)$$

således at v er et torsionselement. □

(9.58) SÆTNING. *Lad $A \in L_n^n$. Der findes elementer $y_1, y_2, \ldots, y_m \in M_A$ og polynomier $d_1, d_2, \ldots, d_m \in L[t]$ som opfylder:*

(1) $M_A = L[t]y_1 \oplus L[t]y_2 \oplus \cdots \oplus L[t]y_m$
(2) $d_1|d_2|\ldots|d_m$ (3) $\mathrm{Ann}(y_i) = L[t]d_i$
(4) *Hvis* $\deg(d_i) = n_i$ *er* $n_i \geq 1$ *og* $n_1 + n_2 + \cdots + n_m = n$
(5) *Følgende mængde er en L-basis for M_A:*

$$\{y_1, Ay_1, \ldots, A^{n_1-1}y_1, y_2, \ldots, A^{n_2-1}y_2, \ldots, y_m, \ldots, A^{n_m}y_m\}$$

(6) *Hvert d_i er monisk.*

BEVIS: (1)–(3) følger direkte fra (9.36). Ifølge (9.36)(2) er $d_i \neq 0$ og d_i ikke invertibel i $L[t]$. Derfor er d_i ikke et konstant polynomium, så $n_i = \deg d_i \geqq 1$. Ifølge (9.51) kan d_i vælges monisk. For at vise resten af (4) og (5) er det tilstrækkeligt at vise, at

$$\{y_i, Ay_i, \ldots, A^{n_i-1}y_i\} \quad \text{er en } L\text{-basis for } L[t]y_i$$

(Lad os bemærke, at $L[t]y_i$ selvfølgelig er et underrum af L-vektorrummet $M_A = L_1^n$.) En linearkombination

$$b_0 y_i + b_1 A y_i + \cdots + b_{n_i-1}(A^{n_i-1}y_i)$$

af $y_i, \ldots, A^{N_i-1}y_i$ er lig

$$p(t)y_i$$

hvor $p(t) = \sum_{i=0}^{n_i-1} b_i t^i$.

Linearkombinationen er lig 0 hvis og kun hvis $p(t) \in \mathrm{Ann}(y_i)$, altså hvis og kun hvis $d_i|p$ ifølge (3). Da $\deg(d_i) = n_i$ ses at $\{y_i, Ay_i, \ldots, A^{n_i-1}y_i\}$ er lineært uafhængig. Det er nu klart, at de danner en basis. Dermed er $\dim_L L[t]y_i = \deg(d_i) = n_i$. □

(9.59) BEMÆRKNING OG DEFINITION: Lad $A \in L_n^n$. Afbildningen $\mu(A) : M_A \to M_A$ givet ved $\mu(A)v = Av$ (jfr. (9.55)) er en lineær afbildning af L-vektorrummet $L_1^n = M_A$ på sig selv. $\mu(A)$ har A som matrix m.h.t. den naturlige basis

$$\left\{ \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix}, \ldots, \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \right\} \quad \text{af } M_A$$

(jfr. f.eks. HBF 30.1 (4)). Men i (9.58)(5) blev angivet en anden basis for M_A. Med hensyn til denne basis har $\mu(A)$ matricen

$$RF(A) = \begin{bmatrix} A_{d_1} & 0 & \ldots & 0 \\ 0 & A_{d_2} & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \ldots & & A_{d_m} \end{bmatrix}$$

hvor A_{d_i} er ledsagematricen til polynomiet d_i fra (9.58)(2) (jfr. (9.58)(6)). Vi har jo $\mu(A)(A^i y_1) = A^{i+1} y_1$, som er en basisvektor, når $i \leq n_1 - 1$. Endvidere er

$$\mu(A)(A^{n_1-1} y_1) = A^{n_1} y_1 .$$

Hvis $d_1(t) = b_0 + b_1 t + \cdots + b_{m_1-1} t^{m_1-1} + t^{m_1}$ er $d_1(t) y_1 = 0$ så $A^{n_1} y_1 = -b_0 y_1 - b_1 A y_1 \cdots - b_{n-1} A^{n_1-1} y_1^{n_1-1}$. Herved fastlægges de første n_1 søjler i $RF(A)$ og de resterende søjler fastlægges tilsvarende. Matricen $RF(A)$ kaldes den *rationelle kanoniske form* for A.

(9.60) BEMÆRKNING: Lad $A \in L_n^n$. Der findes en invertibel matrix $C \in L_n^n$, således at

$$C^{-1} \, A \, C = RF(A) .$$

C er simpelthen basisskiftematricen fra den naturlige basis for L_1^n til basen beskrevet i (9.58)(5). (Jfr. HBF 30.6 (3)). □

(9.61) SÆTNING. *Lad $A \in L_n^n$. Lad notationen være som i (9.58). Lad $p_A(t)$ være det karakteristiske polynomium for A. Der gælder*

$$p_A(t) = (-1)^n d_1(t) \ldots d_m(t) .$$

BEVIS: Ifølge (9.60) har A og $RF(A)$ samme karakteristiske polynomium. Ifølge (9.52) har $RF(A)$ som karakteristisk polynomium $(-1)^n d_1 d_2 \ldots d_m$. □

Vi kan nu bevise en ret bemærkelsesværdig sætning!

(9.62) SÆTNING. *(Hamilton-Cayley) Lad $A \in L_n^n$ og lad d_m være som i (9.58). Der gælder $d_m(A) = 0$. Hvis $p_A(t)$ er det karakteristiske polynomium for A gælder $p_A(A) = 0$.*

BEVIS: Ifølge (9.61) gælder $d_m(t) | p_A(t)$, så det er tilstrækkeligt at vise $d_m(A) = 0$. Det er klart, at $d_m(A) = 0$ hvis $d_m(A) v = 0$ for alle $v \in L_1^n$. Skriv ifølge (9.58)(1) $v \in L_1^n = M_A$ som

$$v = p_1(t) y_1 + \cdots + p_m(t) y_m$$

hvor $p_1, \ldots, p_m \in L[t]$. Så er

$$d_m(A) v = d_m(t) v = p_1(t) d_m(t) y_1 + \cdots + p_m(t) d_m(t) y_m = 0 ,$$

da ifølge (9.58)(2)–(3) $d_m(t) \in \mathrm{Ann}(y_i)$, $1 \leq i \leq m$. □

(9.63) BEMÆRKNING: Hvis man vil beregne $RF(A)$ for $A \in L_n^n$, kan man starte med at se på normalformen for matricen $A - tE \in L[t]_n^n$. De ikke-konstante polynomier der indgår i diagonalen for normalformen for $A - tE$, er, når de vælges moniske, netop $d_1, \ldots, d_m$. Og når man kender $d_1, \ldots, d_m$ kan man let beregne deres ledsagematricer

og dermed $RF(A)$. (Vi har jo, ifølge (9.69), at $A - tE \approx RF(A) - tE$. Og hvis p er et monisk polynomium, er $A_p - tE \approx \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ & & 1 \\ 0 & & p \end{bmatrix}$). □

(9.64) ØVELSE: Vis, at hvis p er et monisk polynomium i $L[t]$ er

$$A_p - tE \approx \begin{bmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ & & & 1 \\ 0 & & & p \end{bmatrix}$$

□

(9.65) EKSEMPEL:

$$A = \begin{bmatrix} -1 & -2 & 6 \\ -1 & 0 & 3 \\ -1 & -1 & 4 \end{bmatrix} \in \mathbb{R}_3^3$$

har karakteristisk polynomium $p_A(t) = -(t-1)^3$. Ved f.eks. at benytte metoden fra (9.19) på $A - tE$ ses at

$$A \approx \begin{bmatrix} 1 & & \\ & t-1 & \\ & & (t-1)^2 \end{bmatrix}$$

Ifølge (9.63) er

$$RF(A) = \begin{bmatrix} A_{t-1} & & \\ & & \\ & & A_{(t-1)^2} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 2 \end{bmatrix}$$

Bemærk, at der ifølge (9.62) må gælde $(A - E)^2 = 0$ hvor

$$A - E = \begin{bmatrix} -2 & -2 & 6 \\ -1 & -1 & 3 \\ -1 & -1 & 3 \end{bmatrix}.$$

□

(9.66) ØVELSE: Beregn den rationelle kanoniske form for

$$A = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 2 & 0 \\ 2 & 0 & 3 \end{bmatrix} \in \mathbb{R}_3^3$$

□

(9.67) ØVELSE: Lad $a, b \in \mathbf{R}$, $(a, b) \neq (0, 0)$. Beregn den rationelle kanoniske form for

$$A = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in \mathbf{R}_2^2$$

□

(9.68) BEMÆRKNING: Eksistensen af den rationelle kanoniske form $RF(A)$ af en matrix var baseret på struktursætningen (9.36) for torsionsmoduler. Man kan i stedet vælge at benytte (9.41) og (9.45) på $R[t]$-modulen M_A. Dette er især af interesse når det karakteristiske polynomium $p_A(t)$ har formen

$$p_A(t) = (-1)^n (t - r_1)^{n_1} \dots (t - r_m)^{n_m} ,$$

hvor $n_i \geq 1$, $r_i \in L$, altså når L er et spaltningslegeme for $p_A(t)$. Vi antager $r_i \neq r_j$ når $i \neq j$. Så er M_A en direkte sum af m primære moduler, idet $t - r_1, \dots, t - r_m$ jo er primelementer (irreducible elementer) i $L[t]$. Hver af de primære moduler er en direkte sum af cykliske moduler. En cyklisk $(t - r_i)$-primær modul ($r_i \in L$) har formen $L[t]v$, hvor $\mathrm{Ann}(v) = L[t](t - r_i)^e$ for et $e \in \mathbf{N}$. Endvidere har $L[t]v$ en L-basis bestående af

$$\{v, (t - r_i)v, \dots, (t - r_i)^{e-1} v\} .$$

Hvis vi sætter alle disse baser sammen til en basis for M_A og beregner A med hensyn til den nye basis fås den *Jordanske normalform* $JN(A)$ for A. Der vil gælde

$$JN(A) = \begin{bmatrix} J_1 & & & 0 \\ & J_2 & & \\ & & \ddots & \\ 0 & & & J_d \end{bmatrix}$$

hvor hver matrix J_k er en "Jordan-blok" for A. J_k har formen

$$\begin{bmatrix} r_i & 1 & & 0 \\ & r_i & 1 & \\ & & \ddots & 1 \\ & 0 & & r_i \end{bmatrix}$$

I analogi med (9.60) vil der findes en invertibel matrix C_1 således at

$$C_1^{-1} A C_1 = JN(A) .$$

Hvis A er som i (9.65) er

$$JN(A) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} ,$$

sammensat af 2 Jordan-blokke.

□

Matematik 2AL

TILLÆGSOPGAVER

(0A) Lad $m, n \in \mathbb{N}$. Vis, at $\underline{m} \times \underline{n} \approx \underline{mn}$.

(0B) For hvilke $n \in \mathbb{N}$ er $\mathbb{N} \times \underline{n}$ numerabel?

(0C) Betragt en relation $\ll$ på $\mathbb{R}$ defineret ved $a \ll b \Leftrightarrow |a| \leq |b|$. Er $(\mathbb{R}, \ll)$ en *po*-mængde? Opfylder $\ll$ $[BRL]$? (se nedenfor!)

(0D) Angiv alle kæder i *po*-mængden $(\mathcal{P}(\underline{3}), \subseteq)$.

(0E) Vis, at delmængden

$$\{x \in \mathbb{Q} \mid x \geq 0, x^2 \leq 2\}$$

af $\mathbb{Q}$ ikke har et supremum i $\mathbb{Q}$.

Ud over $[BRR]$, $[BRS]$, $[BRT]$ og $[BRA]$ betragter vi også følgende betingelse for en relation R på A.

[BRL] For alle $a, b \in A$ gælder enten aRb eller bRa.

(1A) Lad $\mathbb{R}_2^2$ være mængden af reelle 2×2-matricer. Undersøg hvilke af ovennævnte betingelser er opfyldte for følgende relationer på $\mathbb{R}_2^2$:
Lad $A, B \in \mathbb{R}_2^2$

$$A \; R_1 \; B \Leftrightarrow AB = BA$$
$$A \; R_2 \; B \Leftrightarrow \det(A) \leqq \det(B)$$
$$A \; R_3 \; B \Leftrightarrow \det(AB) \neq 0.$$

(1B) Hvad kan man sige om en relation, der både opfylder $[BRS]$ og $[BRL]$?

(1C) Undersøg, hvilke af betingelserne $[KK]$, $[KA]$ og $[KE]$ er opfyldte for følgende kompositioner på $\mathbb{R}_2^2$: Lad $A, B \in \mathbb{R}_2^2$

$$A * B = AB + BA$$
$$A \circ B = AB - BA$$
$$A \S B = ABA + BAB.$$

(1D) Lad $\circ$ være som i **(1C)**, $A, B, C \in \mathbb{R}_2^2$. Vis

$$(A \circ B) \circ C + (B \circ C) \circ A + (C \circ A) \circ B = 0.$$

(2A) For hvilke $n \in \mathbb{N}$ gælder
(i) $(5n + 2\,,\; 5n + 4) = 1$?
(ii) $(5n + 4\,,\; 6n + 5) = 1$?
(iii) $(3n + 2\,,\; 6n - 1) = 1$?

(2B) Vis at der findes uendelig mange primtal.

(2C) Lad $a \in \mathbb{N}$ og lad $a_0, a_1, \ldots, a_r$ være cifrene i a (i 10-talssystemet), altså

$$a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_r \, 10^r \,.$$

(Hvis $a = 1234$ er $a_0 = 4$, $a_1 = 3$, $a_2 = 2$, $a_3 = 1$, for eksempel).
Vis
(i) $a \equiv_9 \; a_0 + a_1 + \ldots + a_r$
(ii) $a \equiv_{11} \; a_0 - a_1 + a_2 + \ldots + (-1)^r a_r$

(2D) Lad $a, b \in \mathbb{Z}$, a, b ikke begge 0. Vælg ifølge Bézouts sætning $k, l \in \mathbb{Z}$ så

$$(a, b) = ka + lb \,.$$

Sæt $a' = a/(a, b)$, $b' = b/(a, b)$. Lad $k_1, l_1 \in \mathbb{Z}$. Vis: Der gælder $k_1 \, a + l_1 \, b = (a, b)$ hvis og kun hvis der eksisterer et $n \in \mathbb{Z}$ således at

$$k_1 = k + n \, b' \,, \; l_1 = l - n \, a' \,.$$

(2E) Beregn alle invertible elementer i restklasseringen $R = \mathbb{Z}_{28}$ og angiv for ethvert sådant element dets inverse. Angiv alle elementer i $\mathbb{Z}_{28}$, der er associerede til $\widehat{2}$. Undersøg om der findes et element $\widehat{a} \in R$ som opfylder $\widehat{a}^2 = \widehat{8}$.

(2F) Gør rede for, at $\mathbb{Z}_n$, $n \in \mathbb{N}$, *ikke* opfylder [ORD].

Lad M være en mængde. Vi betragter *potensmængderingen* $(\mathcal{P}(M), +, \cap)$ (se eksempel (3.1)(3)). Hvis N er en delmængde af M gælder åbenbart $\mathcal{P}(N) \subseteq \mathcal{P}(M)$. Ud over delmængderne $\mathcal{P}(N)$ af $\mathcal{P}(M)$ betragter vi også følgende:

$$\mathcal{P}_e(M) = \{A \in \mathcal{P}(M) \mid A \text{ er endelig}\}$$
$$\mathcal{P}_{el}(M) = \{A \in \mathcal{P}(M) \mid A \text{ er endelig og } |A| \text{ er lige}\}$$
$$\mathcal{P}_t(M) = \{A \in \mathcal{P}(M) \mid A \text{ er tællelig}\}$$
$$\mathcal{P}_n(M) = \{A \in \mathcal{P}(M) \mid A = \emptyset \text{ eller } A \text{ er numerabel}\}$$

(3A) Lad $A, B \in \mathcal{P}(M)$. Vis

$$(A + B) + (A \cap B) = A \cup B.$$

(3B) Lad R være en delring af $\mathcal{P}(M)$. Vis, at R er lukket under $\cup$ (foreningsmængdedannelse).

(3C) Lad $N \subseteq M$. Vis, at $\mathcal{P}(N)$ er et ideal i $\mathcal{P}(M)$.

(3D) Lad M være *endelig*, R et ideal i $\mathcal{P}(M)$. Vis, at der findes en delmængde $N \subseteq M$, så $R = \mathcal{P}(N)$.

(3E) Lad M være *endelig*. Findes der delringe af $\mathcal{P}(M)$, som ikke er idealer?

(3F) Lad M være *uendelig* (ikke endelig). Undersøg om $\mathcal{P}_e(M), \mathcal{P}_{el}(M), \mathcal{P}_t(M)$, $\mathcal{P}_n(M)$ er idealer i $\mathcal{P}(M)$.

(3G) Gælder et udsagn analogt til **(3D)**, når M er uendelig?

(3H) Lad I og J være idealer i en vilkårlig ring R. Sæt

$$(I : J) = \{r \in R \mid \text{For alle } x \in I \text{ er } rx \in J\}.$$

Vis, at $(I : J)$ igen er et ideal i R og beregn $(I : J)$ i det tilfælde, hvor $R = \mathbb{Z}$, $I = 6\mathbb{Z}$, $J = 4\mathbb{Z}$.

Lad M være en delmængde af $\mathbb{N}$. Vi kalder M for *multiplikativ* hvis der gælder

$$\begin{cases} \text{for alle } m_1, m_2 \in M \text{ gælder } m_1 m_2 \in M \\ 1 \in M \end{cases}$$

Hvis M er en multiplikativ mængde sættes

$$\mathbb{Q}(M) = \left\{ \frac{a}{m} \mid a \in \mathbb{Z}, m \in M \right\}$$

$\mathbb{Q}(M)$ er altså delmængden af $\mathbb{Q}$, som består af de rationelle tal, der har en fremstilling på formen $\frac{a}{m}$, $m \in M$. Hvis altså f.eks. $M = \{1, 2, 4, 8, \ldots, 2^n, \ldots\}$ vil $\frac{1}{2} \in \mathbb{Q}(M)$ men f.eks. $\frac{1}{6}$ og $\frac{2}{6} = \frac{1}{3} \notin \mathbb{Q}(M)$.

(3K) Lad $p \in \mathbb{N}$. Vis, at følgende delmængder af $\mathbb{N}$ er multiplikative

$$\mathbb{N},\ M_p = \{1, p, p^2, \ldots, p^n, \ldots\}$$
$$M_p^* = \{n \in \mathbb{N} \mid (p, n) = 1\}.$$

(3L) Lad M være en multiplikativ mængde. Vis, at $\mathbb{Q}(M)$ er en delring af $\mathbb{Q}$, som indeholder $\mathbb{Z}$.

(3M) Lad $M' \subseteq M$, hvor M' og M er multiplikative mængder. Vis, at $\mathbb{Q}(M')$ er en delring af $\mathbb{Q}(M)$. Er $\mathbb{Q}(M')$ et ideal i $\mathbb{Q}(M)$?

Lad nu p være et primtal. Vi sætter

$$\mathbb{Q}(p^*) = \mathbb{Q}(M_p^*) = \left\{ \frac{a}{m} \mid p \nmid m, a \in \mathbb{Z} \right\}$$

Endvidere sættes

$$I(p^*) = \left\{ \frac{a}{m} \mid a, m \in \mathbb{Z}, p \nmid m, p \mid a \right\}$$

(3N) Vis at $I(p^*)$ er et ideal i $\mathbb{Q}(p^*)$.

(3O) Vis at der ved

$$\psi(n) = n + I(p^*), \quad n \in \mathbb{Z}$$

defineres en ringhomomorfi fra $\mathbb{Z} \to \mathbb{Q}(p^*)/I(p^*)$ med kerne $p\mathbb{Z}$.

(3P) Lad $m \in M(p^*)$. Skriv ifølge (2.24) $1 = am + bp$, $a, b \in \mathbb{Z}$. Vis at (med ψ som i **(3O)**) $\psi(a) = \frac{1}{m} + I(p^*)$.

(3Q) Vis at $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Q}(p^*)/I(p^*)$.

(3R) Vis at $I(p^*)$ er et maksimalt ideal i $\mathbb{Q}(p^*)$.

(4A) (Den kinesiske restklassesætning)
Lad $n = n_1 \ldots n_r$ være et produkt af parvis indbyrdes primiske naturlige tal. Vis at

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z} \quad \text{(ringisomorfi)}$$

(*Vink:* Definer passende ringhomomorfi

$$\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

og brug 1. isomorfisætning for ringe).

Opløses n i primfaktorer, $n = {p_1}^{a_1} \ldots {p_r}^{a_r}$ (p'erne parvis indbyrdes forskellige primtal) fås specielt at

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}/{p_1}^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/{p_r}^{a_r}\mathbb{Z} \quad \text{(ikke ?)}$$

(4B) Lad $n = n_1 \ldots n_r$ være som i opgave **(4A)**. Til givne hele tal $a_1, \ldots, a_r \in \mathbb{Z}$ findes et helt tal $x \in \mathbb{Z}$ så

$$\begin{aligned} x &\equiv_{n_1} a_1 \\ x &\equiv_{n_2} a_2 \\ &\vdots \\ x &\equiv_{n_r} a_r \end{aligned}$$

Et sådant x er entydigt bestemt modulo n.

(*Vink:* Benyt **(4A)** til at vise ovenstående).

(4C) Lad $R = k[X]$ være polynomiumsringen i en variabel over legemet k, og lad $I = (X)$ være idealet frembragt af X. Vis at

$$R/I \simeq k$$

(benyt 1. isomorfisætning for ringe).

Hvad siger dette om idealet $I = (X)$?

(4D) Beregn en største fælles divisor af $5 + 4\sqrt{-2}$ og $8 + 7\sqrt{-2}$ i ringen $\mathbf{Z}[\sqrt{-2}]$.

(4E) Skriv følgende elementer i ringen $\mathbf{Z}[i]$ som produkt af irreducible elementer

$$5\ ,\ 7\ ,\ 5+2i\ ,\ 3+i\ ,\ 9+2i\ ,\ 9+4i\ ,\ 21\ .$$

(4F) Beregn en største fælles divisor af elementerne

$$t^2 - \widehat{4} \quad \text{og} \quad t^4 + t^3 + t^2 + t + \widehat{1}$$

i hovedidealringen $\mathbf{Z}_p[t]$, hvor

(i) $p = 3$
(ii) $p = 5$
(iii) $p = 13$

(*Vink:* Man kan med fordel anvende (5.13). Skriv $t^2 - \widehat{4} = (t - \widehat{2})(t + \widehat{2})$ og undersøg om $\widehat{2}$ og $-\widehat{2}$ er rødder i det andet polynomium).

(4G) Lad R være en ring med 1-element og S en ring med mindst 2 elementer. Vis, at hvis der findes en ringepimorfi $\varphi : R \to S$, så har S et 1-element.

(5A) Vis, at $\mathbf{Q}[\sqrt{-3}]$ er et legeme. Vis dernæst, at $\mathbf{Q}[\sqrt{-3}]$ er (isomorf til) brøklegemet for ringen $\mathbf{Z}[\sqrt{-3}]$.

I opgaverne **(5B)**–**(5H)** er $R \neq \{0\}$ en kommutativ ring med 1-element. Vi sætter

$\mathcal{I}_R = \{a \in R \mid a \text{ er } \textit{ikke} \text{ invertibel}\}$
$\operatorname{Max}(R) = \{M \mid M \text{ er et maksimalt ideal i } R\}$
$\operatorname{Rad} R = \cap_{M \in \operatorname{Max}(R)} M$ (Rad er forkortelse for "radikal")

Bemærk, at $\operatorname{Max}(R) \neq \varnothing$ ifølge (5.3), så $\operatorname{Rad} R \neq R$.

(5B) Lad T være en delmængde af R, I et ideal i R således at $T \cap I = \varnothing$. Vis ved hjælp af Zorns lemma, at *po*-mængden

$$\mathcal{J} = \{J \mid J \text{ ideal i } R,\ I \subseteq J,\ J \cap T = \varnothing\}$$

(ordnet ved sædvanlig inklusion) har et maksimalt element. (Man kan kopiere beviset for (5.3)).

(5C) Vis, at $\operatorname{Rad} \mathbf{Z} = \{0\}$ ((3.5) og (4.28)).

(5D) Vis, at for alle $a \in \mathcal{I}_R$ eksisterer et $M \in \operatorname{Max}(R)$ så $a \in M$.
(Anvend f.eks. (5.3) på $I = Ra$. Hvorfor er $I \neq R$?)

(5E) Vis, at hvis I er et ideal i R, $I \neq R$ er $I \subseteq \mathcal{I}_R$.

(5F) ("Lokale ringe")

Vis, at følgende udsagn er ensbetydende:

(1) $R/\operatorname{Rad} R$ er et legeme.
(2) $|\operatorname{Max}(R)| = 1$ (R har netop ét maksimalt ideal).
(3) $\mathcal{I}_R$ er et ideal i R.

(Løsningshjælp (1) $\Leftrightarrow$ (2): Anvend (3.29)(2).
(2) $\Rightarrow$ (3): Lad M være det (eneste) maksimale ideal i R. Vis ved hjælp af **(5D)** og **(5E)** at $M = \mathcal{I}_R$.
(3) $\Rightarrow$ (2): Vis først, at $\mathcal{I}_R$ er et *maksimalt* ideal i R. Vis dernæst ved hjælp af (5E), at $\operatorname{Max}(R) = \{\mathcal{I}_R\}$.)

(5G) Vis, at $\operatorname{Rad}(R/\operatorname{Rad} R) = 0$.

(5H) Vis: $\operatorname{Rad} R = \{a \in R \mid \text{For alle } r \in R \text{ gælder } 1 - ra \text{ er invertibel}\}$.

(5I) Beregn $\operatorname{Rad}(\mathbf{Z}_9)$ og $\operatorname{Rad}(\mathbf{Z}_{15})$.

(5J) Lad K være et endeligt legeme, $\operatorname{char} K = 2$. Vis, at hvis $\varphi : K \to K$ er defineret ved $\varphi(x) = x^2$, er φ en automorfi af K. Vis, at for $x \in K$ gælder $\varphi(x) = x$ netop da, når x er i K's primlegeme. Overvej om et tilsvarende resultat gælder i endelige legemer af karakteristik $p > 2$ (med $\varphi(x) = x^p$).

(5K) Lad $(\mathbf{Z}, +, \odot)$ være de hele tal med sædvanlig addition og med "multiplikation" $a \odot b = 0$ for alle $a, b \in \mathbf{Z}$. Vis at $(\mathbf{Z}, +, \odot)$ er en kommutativ ring. Vis at $2\mathbf{Z}$ er et maksimalt ideal, men ikke et primideal i denne ring. Strider dette mod (3.29)?

(5L) Lad R være en kommutativ ring med 1-element. *Potensrækkeringen* $R[[t]]$ er defineret som $(R[[t]], +, \cdot)$, hvor

$$R[[t]] = \{\sum_{n=0}^{\infty} a_n t^n \mid a_i \in R\}$$

(altså mængden af (formelle) potensrækker med koefficienter fra R) med kompositionerne

$$(\sum_n a_n t^n) + (\sum_n b_n t^n) = \sum_n (a_n + b_n) t^n$$
$$(\sum_n a_n t^n)\,(\sum_n b_n t^n) = \sum_n c_n t^n$$

hvor $c_n = \sum_{i=0}^{n} a_i b_{n-i}$.

(1) Vis, at $R[[t]]$ er en kommutativ ring med 1-element, som indeholder $R[t]$ som delring.
(2) Lad $p(t) = \sum_{n=0}^{\infty} a_n t^n \in R[[t]]$. Vis at $p(t)$ er et invertibelt element i $R[[t]]$, hvis og kun hvis a_0 er et invertibelt element i R.

(3) Beregn de inverse elementer til

$$1-t\,,\ 1+t \quad \text{og} \quad 1-t^2 \text{ i } R[[t]]\,.$$

(4) Lad $R=\mathbf{R}$. Beregn det inverse element til $p(t)=\sum_{n=0}^{\infty}\frac{1}{n!}t^n$ i $R[t]$.
(Konvergensproblemer spille *ingen* rolle i denne opgave).

(5M) Lad L være et legeme, $L[[t]]$ potensrækkeringen (jfr. (5L)).

(1) Lad I være et ideal i $L[[t]]$ og lad $p(t)=\sum_n a_n t^n \in I$. Antag at $a_0=a_1=\cdots=a_{m-1}=0$ men $a_m\neq 0$. Vis, at $t^m\in I$. (Man kan anvende (5L) (2) på snedig måde!)
(2) Vis, at ethvert ideal $\neq\{0\}$ i $L[[t]]$ har formen $L[[t]]t^n$, $n\geq 0$.
(3) Vis, at $L[[t]]$ er en lokal ring (jfr. (5F)).

(5N) Lad L være et legeme og $f(t)\in L[t]$ et polynomium af grad 2 eller 3. Vis f er reducibelt $\Leftrightarrow$ f har en rod i L.

(5O) Undersøg om polynomierne

$$\left.\begin{aligned} f(t) &= t^3+\hat{2}t^2+\hat{1}\\ g(t) &= t^3+\hat{2}t+\hat{1}\end{aligned}\right\} \in \mathbf{Z}_5[t]$$

er irreducible.

(5P) (1) Beregn alle rødder til polynomiet

$$f(t)=t^3-t\in \mathbf{Z}_{10}[t]\,.$$

(2) Beregn for enhver rod $\hat{a}$ i $f(t)$ et polynomium $f_{\hat{a}}(t)\in \mathbf{Z}_{10}[t]$ således at

$$f(t)=(t-\hat{a})f_{\hat{a}}(t)\,.$$

(5Q) (Eisensteins kriterium) Lad R være en Gaussisk ring, $f(t)=a_0+a_1t+\cdots+a_nt^n\in R[t]$ et primitivt polynomium. Lad $p\in R$ være et primelement. Antag at

$$p|a_0, p|a_1,\ldots,p|a_{n-1}\,,\ p\nmid a_n\,,\ p^2\nmid a_0\,.$$

Vis at $f(t)$ er et irreducibelt polynomium i $R[t]$.

(5R) Anvend (5Q) til at vise, at

$$t^3-6t^2+4it+(1+3i)\in R[t]$$

er irreducibelt, hvor $R=\mathbf{Z}[i]$.

(5S) Undersøg om ringene $\mathbf{Z}[\sqrt{2}]$, $\mathbf{Z}[i]$ kan ordnes.

Om valueringer.

Lad R være en kommutativ ring med 1-element. En afbildning $\nu: R\to \mathbf{R}$ som opfylder: For alle $a,b\in R$

(i) $\nu(a)\geq 0$
(ii) $\nu(a)=0\Leftrightarrow a=0$
(iii) $\nu(ab)=\nu(a)\nu(b)$
(iv) $\nu(a+b)\leq \nu(a)+\nu(b)4$

kaldes en *valuering på* R. Lad i (5T)-(5V) være en ring med en valuering ν. (Selvfølgelig er $|\cdot|$ en valuering på $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, ikke?)

(5T) Vis, at R er en integritetsring.

(5U) Vis, at der for alle $a,b\in R$ gælder

$$\nu(1)=1\,,\ \nu(-a)=\nu(a)$$
$$\nu(a-b)\geq|\nu(a)-\nu(b)|\,.$$

(5V) Vis, at ν på netop én måde kan udvides til en valuering på $Q(R)$, R's brøklegeme.

(5W) Vis, at der ved

$$\left.\begin{aligned}\nu(a)&=1 \quad a\neq 0\\ \nu(0)&=0\end{aligned}\right\} \quad \text{defineres en valuering på}$$

en integritetsring R.

(5X) Vis, at valueringen i (5W) er den eneste mulige på $\mathbf{Z}_p$, p primtal.

(5Y) Lad R være en integritetsring. Undersøg om der ved

$$\nu(f)=e^{\deg f}$$

defineres en valuering på $R[t]$. (Vi antager, at $\deg 0=-\infty$ og at $e^{-\infty}=0$).

(5Z) Lad L være et legeme. En valuering ν på L kaldes *ikke-arkimedisk* hvis der gælder

$$\text{For alle } a,b\in L:\nu(a+b)\leq\max(\nu(a),\nu(b))\,.$$

For $n\in\mathbf{N}$ lader vi som sædvanlig $n'=1+1+\cdots+1$ (n summander). Vis

$$\nu \text{ ikke arkimedisk } \Leftrightarrow \nu(n')\leq 1 \text{ for alle } n\in\mathbf{N}\,.$$

(Hjælp til at bevise $\Leftarrow$: Lad $a, b \in L$ og sæt $m = \max(\nu(a), \nu(b))$. Benyt binomialformlen til at vise, at der for alle $n \in \mathbb{N}$ gælder

$$(\nu(a+b))^n \leq (n+1)m^n$$

og benyt at $\lim_{n\to\infty} \sqrt[n]{n+1} = 1$.)

(5Æ) Lad K være et legeme af karakteristik 3.

(1) Vis at der for alle $a, b \in K$ gælder

$$(a+b)^3 = a^3 + b^3$$
$$(a+b)^9 = a^9 + b^9 .$$

(2) Lad nu K være et spaltningslegeme for polynomiet

$$f(t) = t^9 - t \in \mathbb{Z}_3[t]$$

med koefficienter fra legemet $\mathbb{Z}_3$.

Vis at $K_1 = \{b \in K \mid b \text{ er rod i } f(t)\}$ er et dellegeme af K og slut at $K = K_1$.

Hvor mange elementer har legemet K?

(6A) Lad a være et element af orden 100 i en gruppe G.

(1) Beregn ordenen af elementerne a^5, a^6 og a^7 i G.

(2) Lad $b \in G$ være et element således at $b^3 = a$. Vis, at $|b| = 100$ eller $|b| = 300$.

(6B) Lad G være en gruppe og $\alpha : G \to G$ en homomorfi. Sæt

$$F(\alpha) = \{g \in G \mid \alpha(g) = g\} .$$

(1) Vis, at $F(\alpha)$ er en undergruppe i G.

Antag nu yderligere, at G er abelsk og lad $\varphi : G \to G$ være defineret ved

$$\varphi(g) = g^{-1}\alpha(g) .$$

Vis

(1) φ er en homomorfi.

(2) $\ker\varphi = F(\alpha)$.

(6C) Lad $\varphi : G \to G$ være en automorfi af gruppen G og ι_g, $g \in G$, en indre automorfi. Vis, at

$$\varphi \circ \iota_g \circ \varphi^{-1} = \iota_{\varphi(g)} .$$

(6D) Lad G være en endelig gruppe, H normal undergruppe i G. Antag $(|H|, |G : H|) = 1$. Vis at H er den eneste undergruppe i G af orden $|H|$.

(*Vink:* Benyt 2. isomorfisætning).

(6E) Antag at H er en undergruppe i G, som opfylder $|G : H| = 2$. Vis $H \lhd G$.

(6F) Lad G være en endelig gruppe, p primtal. Sæt $X = \{x \in G \mid |x| = p\}$. Vis, at $(p-1) \mid |X|$. (Løsningshjælp: Betragt ækvivalensrelationen $\sim$ på X defineret ved $x \sim y \Leftrightarrow \langle x\rangle = \langle y\rangle$)

(6G) Vis, at hvis gruppen G har netop ét element a af orden 2 gælder $a \in Z(G)$. (Se (7.46)).

(2) Vis, at hvis G har netop 2 elementer b, c af orden 3 gælder at $\{1, b, c\}$ er en normal undergruppe i G.

(7A) Lad p være et primtal. Beregn antallet af forskellige p-cykler og antallet af forskellige $(p-1)$-cykler i den symmetriske gruppe S_p. Beregn endvidere antallet af undergrupper af orden p i S_p.

(7B) Lad $\pi = (1,2,3) \in S_5$.

(i) Angiv alle elementer i $C_{S_5}(\pi)$, altså alle elementer $\rho \in S_5$ som opfylder $\rho\pi\rho^{-1} = \pi$.

(ii) Er $C_{S_5}(\pi) \subseteq A_5$?

(iii) Lad $U = \langle(1,2,3)\rangle = \langle\pi\rangle$. Angiv et element i $N_{S_5}(U)$ som *ikke* er i $C_{S_5}(U) = C_{S_5}(\pi)$.

Lad G være en gruppe. $\mathrm{Aut}(G)$ betegner automorfigruppen for G, altså mængden af automorfier af G med "sammensætning af afbildninger" som komposition. Som undergruppe har vi $\mathrm{Inn}(G) = \{\iota_g \mid g \in G\}$, de indre automorfier. For $\alpha \in \mathrm{Aut}(G)$ sættes $F(\alpha) = \{g \mid \alpha(g) = g\}$.

(7C) Vis: $\mathrm{Inn}(G)$ er normal i $\mathrm{Aut}(G)$.

(7D) Antag, at G er endelig og at $\alpha \in \mathrm{Aut}(G)$ opfylder $F(\alpha) = \{1\}$.

(i) Vis, at for alle $h \in G$ eksisterer et $g \in G$ med $h = g^{-1}\alpha(g)$. (Vis først, at afbildningen $g \mapsto g^{-1}\alpha(g)$ er injektiv).

(ii) Antag yderligere, at $\alpha^2 = \mathrm{id}_G$, altså $\alpha^2(g) = g$ for alle $g \in G$. Vis, at $\alpha(g) = g^{-1}$ for all $g \in G$, og at G er en abelsk gruppe, som ikke indeholder noget element af orden 2.

(7E) Lad G være en endelig abelsk gruppe. Vis

(1) $\varphi^{(2)} : G \to G$ defineret ved $\varphi^{(2)}(x) = x^2$ er en homomorfi.

(2) $\varphi^{(2)}$ er en monomorfi $\Leftrightarrow$ $\varphi^{(2)}$ er en epimorfi.

(3) Hvis ethvert element i G har ulige orden, er $\varphi^{(2)}$ en epimorfi.

(4) Hvis der findes et element af lige orden i G, er $\varphi^{(2)}$ ikke en monomorfi.

(5) $\varphi^{(2)}$ er en epimorfi $\Leftrightarrow$ Ethvert element i G har ulige orden.

(7F) Lad G være en endelig abelsk gruppe. Vis

(1) Ved $\rho^{(2)}(g)(x) = g^2x$ defineres en operation af G på G.
(2) Hvis $|G|$ er ulige, er $\rho^{(2)}$ transitiv.
(3) Ker $\rho^{(2)} = \{g \in G \mid |g| = 2\}$.

(7G) For $n \in \mathbf{N}$, $n \geq 2$, lad $X_n = \{(i,j) \mid 1 \leq i,j \leq n, i \neq j\} \subseteq \mathbf{N} \times \mathbf{N}$ (X_n består altså af talpar, ikke af transpositioner i S_n). Vis

(1) Ved $\rho_*^n(\pi)(i,j) = (\pi(i), \pi(j))$ defineres en operation af S_n på X_n.
(2) ρ_*^n er transitiv.
(3) Ker $\rho_*^n = \{(1)\}$.
(4) Lad specielt $n = 4$. Beregn $\mathrm{stab}_{\rho_*^4}((1,2))$, hvor $(1,2) \in X_4$.

(7H) Lad $\rho : G \to S(H)$ være en transitiv operation af den endelige gruppe G på den endelige mængde M. For $g \in G$ sættes

$$\theta(g) = |\{m \in M \mid \rho(g)(m) = m\}| .$$

Vis

$$\sum_{g \in G} \theta(g) = |G| .$$

(*Vink:* Tæl elementerne i mængden

$$S = \{(g,m) \in G \times M \mid \rho(g)(m) = m\}$$

på to måder!)

(7I) Lad G være en gruppe, $Z(G)$ centrum af G. Vis følgende:

$$G/Z(G) \text{ cyklisk } \Rightarrow G \text{ abelsk} ,$$

(7J) Vis at en gruppe G af orden p^2, p primtal, er abelsk.
(*Vink:* Benyt at $Z(G) \neq \{1\}$ (hvorfor gælder det ?) og opgave (7I) til at vise $Z(G) = G$).

(7K) Lad $U = \langle (1,2)(3,4) \rangle$. Beregn alle U-konjugationsklasser i S_4.

(7L) Lad $\pi = (1,2,3)(4,5) \in S_5$. Angiv alle elementer i $C_{S_5}(\pi)$. Lad $U = \langle \pi \rangle$. Angiv alle elementer i $N_{S_5}(U)$.

(7M) Betragt undergruppen

$$N = \langle (1,2,3) \rangle \times \langle (4,5,6) \rangle \times \langle (7,8,9) \rangle$$

af orden 27 i den symmetriske gruppe S_9. Lad $\pi = (1,4,7)(2,5,8)(3,6,9) \in S_9$.

(1) Vis, ar $\pi \in N_{S_9}(B)$, $B's$ normalisator i S_9.
(2) Vis, at $\langle \pi \rangle \cap B = \{(1)\}$.
(3) Vis, at $P = B\langle \pi \rangle$ er en undergruppe af orden 81 i S_9.

(7N) Lad $K = \mathbf{Z}_p$, $p > 2$ primtal. Lad $G = GL(2,K)$. Beregn $C_G(x)$ hvor $x = \begin{pmatrix} \widehat{1} & 0 \\ 0 & -\widehat{1} \end{pmatrix}$.

I nedenstående opgaver betegner R en ring med 1-element, og en R-modul er underforstået en unitær R-modul.

(8A) Lad M være en R-modul og lad I være et venstre ideal i R der opfylder $IM = 0$. Vis, at da er M også en R/I-modul ved

$$\widehat{r}\, m := rm , \quad \widehat{r} \in R/I , \quad m \in M .$$

(Husk veldefinerethed!)

(8B) Lad I være et venstre ideal i R, M en R-modul og N en undermodul af M. Vis at

$$I(M/N) = IM + N/N .$$

(8C) Lad M være en R-modul, N en undermodul af M. Vis

(1) M endelig frembragt $\Rightarrow M/N$ endelig frembragt.
(2) N og M/N endelig frembragte $\Rightarrow M$ endelig frembragt.

(9A) Lad $M = M_1 \oplus M_2$ være en direkte sum. Ethvert $m \in M$ kan skrives entydigt som $m = m_1 + m_2$, hvor $m_1 \in M$, $m_2 \in M_2$. Vi definerer så

$$\pi_1 : M \to M_1 , \quad \pi_2 : M \to M_2$$

ved

$$\pi_1(m) = m_1 , \quad \pi_2(m) = m_2 .$$

(1) Vis at π_1, π_2 er epimorfier og bestem deres kerner.

Lad yderligere

$$\iota_1 : M_1 \to M , \quad \iota_2 : M_2 \to M$$

være inklusionshomomorfierne.

(2) Vis

$$\pi_1 \circ \iota_1 = 1_{M_1} , \quad \pi_2 \circ \iota_2 = 1_{M_2}$$
$$\pi_2 \circ \iota_1 = 0 , \quad \pi_1 \circ \iota_2 = 0$$

$$\iota_1 \circ \pi_1 + \iota_2 \circ \pi_2 = 1_M .$$

(9B) Lad a, b være elementer i hovedidealringen R, som opfylder $ab \neq 0$. Beregn en normalform og de invariante faktorer for matricerne

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix} \quad \text{og} \quad \begin{bmatrix} a & b & b \\ b & a & b \\ a & a & b \end{bmatrix} .$$