Matematik 211, 1982

Anders Thorup

Talsystemets opbygning

Håndskrevne noter

DE NATURLIGE TAL

1. Aksiomerne
2. Potenser. Tredie potensregel
3. Addition. Første potensregel
4. Multiplikation. Anden potensregel
5. Ordning
6. Endelige og uendelige mængder. Kardinaltal
7. Oversigt over de grundlæggende egenskaber

DE HELE TAL. BRØKGRUPPE

1. Brøker i en gruppe. Analyse
2. Konstruktion af brøkgruppe
3. De hele tal
4. Oversigt over de grundlæggende egenskaber
5. Yderligere resultater
6. Appendix: Resklasser modulo n

BRØKER. DE RATIONALE TAL

1. Brøker i en ring. Analyse
2. Konstruktion af brøkring
3. De rationale tal

FØLGER. ORDNING, FULDSTÆNDIGHED, KONTINUITET. DE REELLE TAL

1. Fundamentalfølge. Fuldstændighed
2. Følgekompletion
3. Kontinuitet
4. Multiplikation
5. Supremum og infimum
6. Supremum og infimum i en ordnet gruppe
7. De reelle tal

Talsystemets opbygning 1981-82

TALSYSTEMETS OPBYGNING

DE NATURLIGE TAL.

1. Aksiomerne.
2. Potenser. Tredie potensregel.
3. Addition. Første potensregel.
4. Multiplikation. Anden potensregel.
5. Ordning.
6. Endelige og uendelige mængder. Kardinaltal.
7. Oversigt over de grundlæggende egenskaber ved de naturlige tal.

DE HELE TAL. BRØKGRUPPE.

1. Brøker i en gruppe. Analyse.
2. Konstruktion af brøkgruppe.
3. De hele tal.
4. Oversigt over de grundlæggende egenskaber ved de hele tal.
5. Yderligere resultater om de hele tal.
6. Appendix: Restklasser modulo n.

BRØKER. DE RATIONALE TAL.

1. Brøker i en ring. Analyse.
2. Konstruktion af brøkring.
3. De rationale tal.

FØLGER. DE REELLE TAL.

1. Fundamentalfølge. Fuldstændighed.
2. Følgekompletion.
3. Kontinuitet.
4. Multiplikation.
5. Supremum og infimum.
6. Supremum og infimum i en ordnet gruppe.
7. De reelle tal.

NATURLIGE TAL

1. Aksiomerne. 1.1: Definition af naturligt tripel. 1.2: Entydighed af naturligt tripel. 1.3: Det fundamentale eksistensaksiom. 1.4: Definition ved induktion. 1.5: Homomorfi af tripler. 1.6: Sætning om $\varepsilon(\mathbb{N})$. 1.7: Induktionsaksiomet. 1.8: Uendelighedsaksiomet. 1.9-13: Peanos aksiomer.

2. Potenser i en semigruppe. Tredie potensregel. 2.1: Notation for semigrupper. 2.2: Definition af n-te potens. 2.3-5: Tredie potensregel.

3. Addition i $\mathbb{N}$. Første potensregel. 3.1: Definition af addition. 3.2: Additionsreglerne. 3.3: Første potensregel. 3.4: Homomorfier af $(\mathbb{N},+)$ ind i en semigruppe.

4. Multiplikation i $\mathbb{N}$. Anden potensregel. 4.1: Definition af multiplikation. 4.2: Multiplikationsreglerne. 4.3: Anden potensregel.

5. Ordning i $\mathbb{N}$. Velordning. 5.1: Definition af "mindre end". 5.2-3: Ordningsreglerne. 5.4-7: $(\mathbb{N},\leqslant)$ som velordnet mængde. 5.8: Definition af velordning. 5.9: Sætning om transfinit induktion. 5.10: Sætning om fuldstændig induktion. 5.11-12: Karakterisering af $(\mathbb{N},\leqslant)$ som ordnet mængde. 5.13: Sætning om definition ved rekursion.

6. Endelige og uendelige mængder. Kardinaltal. 6.1: Sætning om injektive afbildninger : $\mathbb{N}_a \to \mathbb{N}_a$. 6.2: Endelige og uendelige mængder. Kardinaltal. 6.3-7: Sætninger om endelige mængder. 6.8: Sætning om uendelighed af $\mathbb{N}$. 6.9: Eksistens af injektive afbildninger : $\mathbb{N} \hookrightarrow \mathbb{Q}$. 6.10: Udvalgsaksiomet.

7. Oversigt over de grundlæggende egenskaber ved de naturlige tal. 7.1: Beskrivelse. 7.2: Fundamentale aksiomer. 7.3: Potenser. 7.4: Fundamentale strukturer. 7.5: Regnereglerne. 7.6: Potensreglerne. 7.7: Potenssætningen. 7.8: Velordning. 7.9: Kardinaltal. 7.10: Betegnelser. Positionssystemet.

DE NATURLIGE TAL.

1. Aksiomerne.

1.1. Vi vil i det følgende betragte systemer (Q, q_1, φ) bestående af en mængde Q, et udvalgt element $q_1 \in Q$ og en afbildning $\varphi: Q \to Q$. Et sådant system omtales kort som et tripel (Q, q_1, φ)

DEFINITION. Et tripel (N, n_1, η) kaldes naturligt, hvis det har følgende egenskab: Til hvert tripel (Q, q_1, φ) findes en og kun én afbildning $f: N \to Q$, således at $f(n_1) = q_1$ og $f(\eta(n)) = \varphi(f(n))$ for alle $n \in N$.

At $f(\eta(n)) = \varphi(f(n))$ for alle $n \in N$. betyder, at $f \circ \eta = \varphi \circ f$.

1.2. Af definitionen følger, at alle naturlige tripler er isomorfe i følgende forstand:

SÆTNING. *Lad (N, n_1, η) og $(\bar{N}, \bar{n}_1, \bar{\eta})$ være naturlige tripler. Der findes da en og kun én bijektiv afbildning $f: N \to \bar{N}$, således at $f(n_1) = \bar{n}_1$ og $f \circ \eta = \bar{\eta} \circ f$.*

Bevis. Da (N, n_1, η) er et naturligt tripel, findes en og kun én afbildning $f: N \to \bar{N}$, således at $f(n_1) = \bar{n}_1$ og $f \circ \eta = \bar{\eta} \circ f$. Vi skal nu blot vise, at f er bijektiv. Da også $(\bar{N}, \bar{n}_1, \bar{\eta})$ er et naturligt tripel, findes en (og endda kun én) afbildning $\bar{f}: \bar{N} \to N$ således at $\bar{f}(\bar{n}_1) = n_1$ og $\bar{f} \circ \bar{\eta} = \eta \circ \bar{f}$; vi viser, at $\bar{f}$ er den til f hørende inverse afbildning. Betragt den sammensatte afbildning $\bar{f} \circ f: N \to N$. Vi finder

$$(\bar{f} \circ f)(n_1) = \bar{f}(\bar{n}_1) = n_1,$$

og

$$(\bar{f}\circ f)\circ\eta = \bar{f}\circ f\circ\eta = \bar{f}\circ\bar{\eta}\circ f = \eta\circ\bar{f}\circ f = \eta\circ(\bar{f}\circ f).$$

Vi ser, at også den identiske afbildning $Id_N : N \to N$ opfylder $Id_N(n_1) = n_1$ og $Id_N\circ\eta = \eta\circ Id_N$. Da (N, n_1, η) er et naturligt tripel, er der kun én afbildning $: N \to N$, som opfylder disse betingelser, og vi slutter, at $\bar{f}\circ f = Id_N$. Tilsvarende får vi, at $f\circ\bar{f} = Id_{\bar{N}}$, og disse ligninger viser, at f er bijektiv (med den inverse $f^{-1} = \bar{f}$). ▨

1.3. Det er ikke på forhånd givet, at der findes naturlige tripler. Vi må derfor postulere eksistensen af naturlige tripler, altså antage, at der gælder følgende

FUNDAMENTALE EKSISTENSAKSIOM. Der findes naturlige tripler.

Blandt de naturlige tripler trækker vi os en gang for alle udvalgt et bestemt, som vi kalder triplet af naturlige tal og betegner $\mathbb{N}$. Den til det udvalgte tripel hørende mængde betegner sædvanligvis med det samme symbol $\mathbb{N}$; dens elementer kaldes naturlige tal. Det udvalgte element i $\mathbb{N}$ betegnes 1, og den til triplet hørende afbildning $: \mathbb{N} \to \mathbb{N}$ kaldes efterfølgerafbildningen og betegnes $\varepsilon : \mathbb{N} \to \mathbb{N}$ eller $x \longmapsto x^+$. Det udvalgte tripel er altså triplet $(\mathbb{N}, 1, \varepsilon)$.

1.4. At $(N, 1, \varepsilon)$ er et naturligt tripel udsiger, at der gælder følgende, som også kaldes

SÆTNING OM DEFINITION VED INDUKTION. Til hvert tripel (Q, q_1, φ) findes netop én afbildning $f : \mathbb{N} \to Q$, således at $f(1) = q_1$ og $f(x^+) = \varphi(f(x))$ for alle $x \in \mathbb{N}$.

1.5. Lad (Q, q_1, φ) og (Q', q_1', φ') være tripler. I stedet

for at sige, at en afbildning $f: Q \to Q'$ opfylder $f(q_1) = q_1'$ og $f \circ \varphi = \varphi' \circ f$, siger vi, at f er en homomorfi (af tripler) : $(Q, q_1, \varphi) \to (Q', q_1', \varphi')$. Det er klart, at den identiske afbildning $Id_Q : Q \to Q$ er en homomorfi $Id_Q : (Q, q_1, \varphi) \to (Q, q_1, \varphi)$, og at vi ved sammensætning af to homomorfier $f: (Q, q_1, \varphi) \to (Q', q_1', \varphi')$ og $f': (Q', q_1', \varphi') \to (Q'', q_1'', \varphi'')$ får en homomorfi $f' \circ f: (Q, q_1, \varphi) \to (Q'', q_1'', \varphi'')$.

At et tripel (N, n_1, η) er naturligt, betyder altså, at der til hvert tripel (Q, q_1, φ) findes netop én homomorfi $f: (N, n_1, \eta) \to (Q, q_1, \varphi)$. Specielt er identiteten $Id_N : (N, n_1, \eta) \to (N, n_1, \eta)$ den eneste homomorfi af et naturligt tripel ind i sig selv.

Beviset for at to naturlige tripler (N, n_1, η) og $(\bar{N}, \bar{n}_1, \bar{\eta})$ er isomorfe forløber nu således: Der findes homomorfier $f: (N, n_1, \eta) \to (\bar{N}, \bar{n}_1, \bar{\eta})$ og $\bar{f}: (\bar{N}, \bar{n}_1, \bar{\eta}) \to (N, n_1, \eta)$. Ved sammensætning får vi homomorfier $\bar{f} \circ f : (N, n_1, \eta) \to (N, n_1, \eta)$ og $f \circ \bar{f} : (\bar{N}, \bar{n}_1, \bar{\eta}) \to (\bar{N}, \bar{n}_1, \bar{\eta})$, og dit følger, at $\bar{f} \circ f = Id_N$ og $f \circ \bar{f} = Id_{\bar{N}}$. Disse ligninger betyder, at f og $\bar{f}$ er bijektive (og "hinandens inverse").

Den til hvert tripel (Q, q_1, φ) hørende homomorfi : $(\mathbb{N}, 1, \varepsilon) \to (Q, q_1, \varphi)$ (sætning 1.4.) kaldes den naturlige homomorfi.

1.6. I dit følgende udleder vi en række egenskaber for tripelet $(\mathbb{N}, 1, \varepsilon)$. Af isomorfisætningen (1.2.) følger at disse egenskaber – bortset fra valg af betegnelser – gælder for ethvert naturligt tripel.

SÆTNING. For tripelet $(\mathbb{N}, 1, \varepsilon)$ af naturlige tal gælder, at $\varepsilon(\mathbb{N}) = \mathbb{N} \setminus \{1\}$.

Sætningen udsiger, at 1 ikke er efterfølger og at hvert naturligt tal $\neq 1$ er en efterfølger (d.v.s. af formen x^+).

Bevis. Lad Q være en mængde bestående af to forskellige elementer q_1 og q_2, altså $Q = \{q_1, q_2\}$, og lad $\varphi: Q \to Q$ være defineret ved $\varphi(q_1) = \varphi(q_2) = q_2$. Vi kan da betragte tripletten (Q, q_1, φ). Det ses, at en afbildning $f: \mathbb{N} \to Q$ er en homomorfi: $(\mathbb{N}, 1, \varepsilon) \to (Q, q_1, \varphi)$, hvis og kun hvis der gælder

$$(*) \quad f(1) = q_1 \text{ og } f(x) = q_2 \text{ for alle } x \in \varepsilon(\mathbb{N}).$$

Da $(\mathbb{N}, 1, \varepsilon)$ er et naturligt tripel, eksisterer der en afbildning $f: \mathbb{N} \to Q$, som opfylder betingelsen $(*)$. Da $q_1 \neq q_2$, må der gælde $1 \notin \varepsilon(\mathbb{N})$. Da $f: \mathbb{N} \to Q$ er den eneste afbildning, som opfylder $(*)$, kan vi videre slutte, at $\mathbb{N} = \{1\} \cup \varepsilon(\mathbb{N})$, thi hvis der fandtes et element $a \in \mathbb{N}$, således at $a \notin \{1\} \cup \varepsilon(\mathbb{N})$, kunne vi ved

$$f_i(y) = \begin{cases} f(y), & y \neq a \\ q_i & y = a, \end{cases}$$

$i = 1, 2$, definere to forskellige afbildninger $f_1, f_2: \mathbb{N} \to Q$, som begge opfylder betingelsen $(*)$ (og hvoraf den ene er $= f$) ▨

1.7. For tripletten $(\mathbb{N}, 1, \varepsilon)$ af naturlige tal gælder følgende sætning, der ofte kaldes

INDUKTIONSAKSIOMET. Hvis en delmængde S af $\mathbb{N}$ opfylder

$$1 \in S \quad \text{og} \quad \varepsilon(S) \subseteq S,$$

så er $S = \mathbb{N}$.

Bevis. Da $\varepsilon(S) \subseteq S$, bestemmer ε ved restriktion en afbildning $\varepsilon_S: S \to S$, og vi kan betragte tripletten $(S, 1, \varepsilon_S)$. Det er klart, at inklusionsafbildningen $i: S \hookrightarrow \mathbb{N}$ er en homomorfi $i: (S, 1, \varepsilon_S) \to (\mathbb{N}, 1, \varepsilon)$.

Lad $f: (\mathbb{N}, 1, \varepsilon) \to (S, 1, \varepsilon_S)$ være den naturlige homomorfi. Ved sammensætning får vi en homomorfi $i \circ f: (\mathbb{N}, 1, \varepsilon) \to (\mathbb{N}, 1, \varepsilon)$, og vi slutter, at $i \circ f = Id_{\mathbb{N}}$, og dermed specielt, at i er surjektiv. At inklusionsafbildningen $i: S \hookrightarrow \mathbb{N}$ er surjektiv betyder imidlertid, at $S = \mathbb{N}$. ▨

1.8. En del af sætning 1.6. lader vi indgå i følgende sætning, som vi kalder

VENDELIGHEDSAKSIOMET. <u>For tripler $(\mathbb{N}, 1, \varepsilon)$ af naturligetal gælder, at ε er injektiv og $1 \notin \varepsilon(\mathbb{N})$.</u>

Afbildningen $\varepsilon: \mathbb{N} \to \mathbb{N}$ er således injektiv, men ikke surjektiv.

Bevis. Vi mangler at vise injektiviteten: Vi supplerer $\mathbb{N}$ til en mængde $\tilde{\mathbb{N}}$ ved at tilføje et element $0 \notin \mathbb{N}$:

$$\tilde{\mathbb{N}} = \mathbb{N} \cup \{0\},$$

og udvider $\varepsilon: \mathbb{N} \to \mathbb{N}$ til en afbildning $\tilde{\varepsilon}: \tilde{\mathbb{N}} \to \tilde{\mathbb{N}}$ ved

$$\tilde{\varepsilon}(x) = \begin{cases} 1 & x = 0 \\ \varepsilon(x) & \text{for } x \in \mathbb{N}. \end{cases}$$

Vi har da et tripel $(\tilde{\mathbb{N}}, 0, \tilde{\varepsilon})$ og kan betragte den naturlige homomorfi $f: (\mathbb{N}, 1, \varepsilon) \to (\tilde{\mathbb{N}}, 0, \tilde{\varepsilon})$. For den sammensatte afbildning $f \circ \varepsilon: \mathbb{N} \to \tilde{\mathbb{N}}$ finder vi $(f \circ \varepsilon)(1) = (\tilde{\varepsilon} \circ f)(1) = \tilde{\varepsilon}(0) = 1$, og $(f \circ \varepsilon) \circ \varepsilon = (\tilde{\varepsilon} \circ f) \circ \varepsilon = \tilde{\varepsilon} \circ (f \circ \varepsilon)$, så at $f \circ \varepsilon$ er en homomorfi af tripler:

$$f \circ \varepsilon: (\mathbb{N}, 1, \varepsilon) \to (\tilde{\mathbb{N}}, 1, \tilde{\varepsilon}).$$

På den anden side ser vi let, at også inklusionsafbildningen $j: \mathbb{N} \hookrightarrow \tilde{\mathbb{N}}$ er en homomorfi af tripler

$$j: (\mathbb{N}, 1, \varepsilon) \to (\tilde{\mathbb{N}}, 1, \tilde{\varepsilon}).$$

Af entydigheden følger nu, at $f \circ \varepsilon = j$, og da $f \circ \varepsilon$ således er injektiv, må ε være injektiv ▨

1.9. Induktionsaksiomet og uendelighedsaksiomet kaldes under et for Peanos aksiomer. Disse aksiomer har mening for ethvert tripel (Q, q_1, φ). Vi kan betragte tripler (Q, q_1, φ), som opfylder induktionsaksiomet (hvorom det altså gælder, at hvis en delmængde $S \subseteq Q$ opfylder $q_1 \in S$ og $\varphi(S) \subseteq S$, så er $S = Q$), eller tripler (Q, q_1, φ), som opfylder uendelighedsaksiomet (hvorom det altså gælder, at φ er en injektiv afbildning og $q_1 \notin \varphi(Q)$). Herom gælder

1.10. SÆTNING. *Lad (Q, q_1, φ) være et tripel, som opfylder induktionsaksiomet. Den naturlige homomorfi $f: (\mathbb{N}, 1, \varepsilon) \to (Q, q_1, \varphi)$ er da en surjektiv afbildning $f: \mathbb{N} \to Q$.*

Bevis. Påstanden fås ved at anvende induktionsaksiomet på delmængden $S = f(\mathbb{N}) \subseteq Q$ □

1.11. SÆTNING. *Lad (Q, q_1, φ) være et tripel, som opfylder uendelighedsaksiomet. Den naturlige homomorfi $f: (\mathbb{N}, 1, \varepsilon) \to (Q, q_1, \varphi)$ er da en injektiv afbildning $f: \mathbb{N} \to Q$.*

Bevis. Vi viser – under brug af induktionsaksiomet for $\mathbb{N}$ – at delmængden

$$S = \{x \in \mathbb{N} \mid \forall y \in \mathbb{N} : f(y) = f(x) \Rightarrow y = x\}$$

er hele $\mathbb{N}$.

Vi har $1 \in S$: Hvert $y \neq 1$ kan skrives $y = \varepsilon(z)$ (sætning 1.6), så for et sådant y finder vi

$$f(y) = f(\varepsilon(z)) = \varphi(f(z)) \in \varphi(Q).$$

Heraf følger $f(y) \neq f(1)$, da $f(1) = q_1 \notin \varphi(Q)$.

Vi har $\varepsilon(S) \subseteq S$: Lad nemlig $x \in S$. For at vise, at også $\varepsilon(x) \in S$, betragter vi et $y \in \mathbb{N}$ således at $f(y) = f(\varepsilon(x))$, og vi skal vise, at $y = \varepsilon(x)$. Af $f(y) = f(\varepsilon(x)) = \varphi(f(x)) \in \varphi(Q)$ følger – idet $f(1) = q_1 \notin \varphi(Q)$ – at $y \neq 1$. Vi kan derfor skrive

$y = \varepsilon(z)$, og har nu $\varphi(f(z)) = f(\varepsilon(z)) = f(y) = f(\varepsilon(x)) = \varphi(f(x))$. Da φ er injektiv, slutter vi, at $f(z) = f(x)$, og da $x \in S$, følger heraf videre, at $z = x$, men så er $y = \varepsilon(z) = \varepsilon(x)$. ▨

1.12. Som korollar af disse to sætninger får vi, at Peanos aksiomer karakteriserer de naturlige tal, altså

SÆTNING. Lad (N, n_1, η) være et tripel, som opfylder Peanos aksiomer. Den naturlige homomorfi $f: (\mathbb{N}, 1, \varepsilon) \to (N, n_1, \eta)$ er da en isomorfi.

1.13. BEMÆRKNING. Specielt ser vi, at et tripel (N, n_1, η), der opfylder Peanos aksiomer, er et naturligt tripel. Det er værd at bemærke, at det her givne bevis har forudsat eksistensen af et naturligt tripel (nemlig $(\mathbb{N}, 1, \varepsilon)$); vi har altså udnyttet det fundamentale eksistensaksiom 1.3. Peanos aksiomer ligger til grund for Peanos og Dedekinds beskrivelser af de naturlige tal. Det vises her – uden brug af eksistensaksiomet 1.3. – at et tripel (N, n_1, η), som opfylder Peanos aksiomer, er et naturligt tripel. Det fundamentale eksistensaksiom 1.3. kan derfor erstattes med et aksiom, der sikrer, at der findes tripler, som opfylder Peanos aksiomer.

2. Potenser i en semigruppe. Tredie potensregel.

2.1. En ikke-tom mængde M med en associativ komposition kaldes en <u>semigruppe</u>. Hvor intet andet er nævnt skrives kompositionen <u>multiplikativt</u>: $(x,y) \mapsto x \cdot y$ (eller blot $(x,y) \mapsto xy$), og semigruppen betegnes udførligt $(M,\cdot)$. Hvis kompositionen i semigruppen er kommutativ, skrives den dog ofte <u>additivt</u>: $(x,y) \mapsto x+y$, og semigruppen betegnes udførligt $(M,+)$. Hvor misforståelser er udelukket, betegnes semigruppen simpelthen M.

2.2. Lad a være et element i en semigruppe $(M,\cdot)$. Afbildningen $x \mapsto x \cdot a$ kaldes <u>højremultiplikation</u> med a, og betegnes $r_a : M \to M$. Af sætningen om definition ved induktion 1.4. følger, at der findes netop én afbildning $\pi : \mathbb{N} \to M$ således at $\pi(1) = a$ og $\pi(n^+) = \pi(n) \cdot a$ for alle $n \in \mathbb{N}$, nemlig den naturlige homomorfi : $(\mathbb{N}, 1, \varepsilon) \to (M, a, r_a)$.

DEFINITION. Elementet $\pi(n) \in M$ kaldes den <u>n-te potens af a</u>, og betegnes a^n eller $\overbrace{a \cdots a}^{n}$.

Hvis kompositionen er skrevet additivt, bruges betegnelserne na eller $\overbrace{a+\cdots+a}^{n}$ for den n-te potens af a. Vi har $a^1 = a$ $(1a = a)$ og $a^{n^+} = a^n \cdot a$ $(n^+a = na + a)$.

2.3. Ved induktion vises den såkaldte

TREDIE POTENSREGEL. <u>Hvis elementerne a og b i semigruppen M kommuterer</u> (d.v.s. hvis $ab = ba$), <u>så gælder for alle $n \in \mathbb{N}$, at $ab^n = b^n a$ og</u>

$$\boxed{(ab)^n = a^n b^n}$$

Er semigruppen kommutativ, gælder reglen for alle

elementer $a,b \in M$. Skrives kompositionen additivt, får reglen udseendet

$$\boxed{n(a+b) = na + nb}$$

Bevis. Sæt $S = \{n \in \mathbb{N} \mid ab^n = b^n a \wedge (ab)^n = a^n b^n\}$. At $1 \in S$ er klart, og hvis $n \in S$ finder vi

$$ab^{n^+} = ab^n b = b^n ab = b^n ba = b^{n^+} a$$

og

$$(ab)^{n^+} = (ab)^n ab = a^n b^n ab = a^n a\, b^n b = a^{n^+} b^{n^+}.$$

Følgelig er $n^+ \in S$ ▨

2.4. Det ses specielt, at vi har $aa^n = a^n \cdot a$, og dermed $a \cdot a^n = a^{n^+}$ for alle $n \in \mathbb{N}$. Vi får således de samme potenser, hvis vi i definitionen erstatter højremultiplikationen r_a med venstremultiplikationen $l_a : x \longmapsto a \cdot x$.

2.5. For en given mængde Q udgør afbildningerne $\varphi : Q \to Q$ en semigruppe med sammensætning som komposition. Den n-te potens af en afbildning $\varphi : Q \to Q$ betegnes φ^n eller – mere udførligt – $\varphi^{\circ n}$. Hvis (Q, q_1, φ) er et tripel, vises det let ved induktion, at den naturlige homomorfi $f : (\mathbb{N}, 1, \varepsilon) \to (Q, q_1, \varphi)$ opfylder $f(n^+) = \varphi^n(q_1)$ for alle $n \in \mathbb{N}$.

3. Addition i $\mathbb{N}$. Første potensregel.

3.1. I mængden $\mathbb{N}$ af naturlige tal ønsker vi at definere en addition, således at $\varepsilon(x) = x^+ = x + 1$

(efterfølgerafbildningen ε er afbildningen "læg 1 til"), og således at $x+n$ fås udfra x ved "n gange at lægge 1 til". Vi ledes derfor til følgende

DEFINITION. I mængden $\mathbb{N}$ defineres en komposition kaldet addition og betegnet $(x,n) \mapsto x+n$ ved

$$x + n = \varepsilon^n(x),$$

hvor $\varepsilon^n = \overbrace{\varepsilon \circ \cdots \circ \varepsilon}^{n}$ er den n-te potens af afbildningen $\varepsilon : \mathbb{N} \to \mathbb{N}$.

3.2. SÆTNING. For additionen i $\mathbb{N}$ gælder følgende regler:

(0) $x + 1 = x^+$

(1) $x + n = n + x$

(2) $x + (n+m) = (x+n) + m$

(3) $x + n = y + n \Rightarrow x = y.$

Egenskaberne (1), (2) og (3) udsiger, at $(\mathbb{N},+)$ er en kommutativ semigruppe, hvori forkortningsreglen gælder.

Bevis. For alle $n \in \mathbb{N}$ gælder $\varepsilon^{n^+} = \varepsilon^n \circ \varepsilon = \varepsilon \circ \varepsilon^n$, og dermed $\varepsilon^{n^+}(x) = \varepsilon^n(\varepsilon(x)) = \varepsilon(\varepsilon^n(x))$ for alle $x \in \mathbb{N}$. For alle $x, n \in \mathbb{N}$ har vi derfor

$$x + n^+ = x^+ + n = (x+n)^+.$$

Påstandene vises nu som følger:

(0) er en konsekvens af definitionen, da $\varepsilon^1 = \varepsilon$.

(1): For alle $n \in \mathbb{N}$ er $1 + n = n + 1$. Dette udsagn vises ved induktion; det er sandt for $n = 1$, og hvis det er sandt for et $n \in \mathbb{N}$, finder vi

$$1 + n^+ = (1+n)^+ = (n+1)^+ = n^+ + 1,$$

og slutter, at det også er sandt for n^+.

Vi kan nu vise (1) ved induktion efter x, dvs vi sætter $S = \{x \in \mathbb{N} \mid \forall n \in \mathbb{N} : x + n = n + x\}$, og viser, at $S = \mathbb{N}$: Vi har $1 \in S$ i følge det allerede viste, og hvis $x \in S$ finder vi for alle n:

$$x^+ + n = (x+n)^+ = (n+x)^+ = n + x^+,$$

og ser, at $x^+ \in S$.
(2) vises ved induktion efter m, altså ved at vise, at mængden

$$S = \{m \in \mathbb{N} \mid \forall x, n \in \mathbb{N} : (x+n)+m = x+(n+m)\}$$

er hele $\mathbb{N}$. Vi har $1 \in S$, thi for $x, n \in \mathbb{N}$ er

$$(x+n)+1 = (x+n)^+ = x+n^+ = x+(n+1),$$

og hvis $m \in S$ er

$$(x+n)+m^+ = [(x+n)+m]^+ = [x+(n+m)]^+$$
$$= x+(n+m)^+ = x+(n+m^+),$$

hvoraf vi ser, at $m^+ \in S$.
(3) udsiger, at $\varepsilon^n(x) = \varepsilon^n(y) \Rightarrow x = y$, altså at afbildningen ε^n er injektiv. Mere generelt vises det lit ved induktion, at potenserne af en injektiv afbildning (her ε) alle er injektive. □

3.3. Potenser i en semigruppe harmonerer med additionen i $\mathbb{N}$, idet der gælder:
FØRSTE POTENSREGEL. Hvis a er et element i semigruppen M, så gælder for alle $n, m \in \mathbb{N}$, at

$$\boxed{a^{n+m} = a^n a^m.}$$

Er kompositionen additivt skrevet, får reglen udseendet

$$\boxed{(n+m)a = na + ma}$$ □

3.4. Første potensregel udsiger, at afbildningen $n \mapsto a^n$ er en homomorfi : $(\mathbb{N},+) \to (M,\cdot)$; endvidere har vi jo $a^1 = a$. Det er ofte bekvemt at udnytte, at $n \mapsto a^n$ er den eneste afbildning : $\mathbb{N} \to M$ med disse egenskaber, altså at der gælder følgende POTENSSÆTNING. Lad a være et element i semigruppen $(M,\cdot)$. Der findes netop én homomorfi : $(\mathbb{N},+) \to (M,\cdot)$ således at $1 \mapsto a$, nemlig afbildningen $n \mapsto a^n$.

Bevis. Er $\pi : \mathbb{N} \to M$ en sådan afbildning, har vi specielt $\pi(1) = a$ og $\pi(n^+) = \pi(n+1) = \pi(n)\pi(1) = \pi(n)a$. Heraf følger, at $\pi(n) = a^n$. ▨

4. Multiplikation i $\mathbb{N}$. Anden potensregel.

4.1. DEFINITION. I mængden $\mathbb{N}$ defineres en komposition kaldet <u>multiplikation</u> og betegnet $(p,n) \mapsto p \cdot n$ ved

$$p \cdot n = \overbrace{n + \ldots + n}^{p}$$

Produktet $p \cdot n$ er altså den p-te potens af elementet n i semigruppen $(\mathbb{N},+)$, og det kan uden fare for misforståelser betegnes pn.

4.2. SÆTNING. <u>For multiplikationen i $\mathbb{N}$ gælder følgende regler:</u>

(1) $\underline{pn = np}$

(2) $\underline{(pq)n = p(qn)}$

(3) $\underline{p1 = 1p = p}$

(4) $\underline{pn = qn \Rightarrow p = q}$.

(5) $\underline{(p+q)n = pn + qn}$, $\underline{p(n+m) = pn + pm}$.

Reglerne (1)-(4) udsiger, at $(\mathbb{N},\cdot)$ er en <u>kommutativ semigruppe</u> med <u>neutralt element 1</u>, hvori <u>forkortningsreglen gælder</u>, og (5) udsiger at multiplikationen er <u>distributiv</u> m.h.t. additionen.

Bevis. Sætningen kan (som sætning 3.2.) vises ved induktion. Påstanden (4) er dog noget omstændelig. Elegantere (?) er det imidlertid at gå frem som følger:
De to distributive love (5) er simpelthen første og tredie potensregel i den kommutative semigruppe $(\mathbb{N},+)$.

For at vise (3), bemærker vi, at afbildningerne $p \mapsto p1$, $p \mapsto 1p$ og $p \mapsto p$ alle er homomorfier: $(\mathbb{N},+) \to (\mathbb{N},+)$ (de to første iflg (5), den sidste trivielt). Da de stemmer overens for $p=1$, må de være identiske (sætning 3.4.).

For at vise (1) betragter vi for et fast $n \in \mathbb{N}$ afbildningerne $p \mapsto pn$ og $p \mapsto np$. De er begge homomorfier: $(\mathbb{N},+) \to (\mathbb{N},+)$ (iflg. (5)), de stemmer overens for $p=1$ (iflg (3)), og de er derfor identiske (sætning 3.4.).

Udsagnet (2) vises analogt ved for faste $q, n \in \mathbb{N}$ at betragte afbildningerne $p \mapsto p(qn)$ og $p \mapsto (pq)n$

Endelig udsiger (4), at afbildningen $p \mapsto pn$ er en injektiv afbildning: $\mathbb{N} \to \mathbb{N}$. I følge definitionen er denne afbildning den naturlige homomorfi: $(\mathbb{N}, 1, \varepsilon) \to (\mathbb{N}, n, r_n)$, hvor r_n er højre"multiplikationen": $x \mapsto x+n$. For at vise, at afbildningen er injektiv, er det derfor (sætning 1.11) nok at vise, at triplet $(\mathbb{N}, n, r_n)$ opfylder uendelighedsaksiomet, altså at $r_n : \mathbb{N} \to \mathbb{N}$ er injektiv, og at $n \notin r_n(\mathbb{N})$. At r_n er injektiv følger af at forkortningsreglen gælder i $(\mathbb{N},+)$ (sætning 3.2.(3)), og at $n \notin r_n(\mathbb{N})$ følger ligeledes heraf, thi af $n = x+n$ ville følge $1+n = 1+(x+n) = (x+1)+n$, og altså $1 = x+1 = x^+$, hvilket er en modstrid. ▨

4.3. Også multiplikationen i $\mathbb{N}$ harmonerer med potensen i en semigruppe, idet vi har

ANDEN POTENSREGEL. <u>Hvis a er et element i semigruppen M, så gælder for alle $p, n \in \mathbb{N}$, at</u>

$$\boxed{a^{pn} = (a^p)^n}$$

Er kompositionen additivt skrevet, kan reglen skrives - idet $pn = np$ - $\boxed{(pn)a = p(na)}$ □

5. Ordning i $\mathbb{N}$. Velordning.

5.1. Vi ønsker at definere en ordning $<$ i $\mathbb{N}$, således at $x<y$ betyder, at "vi kommer fra x til y ved at tælle videre", altså ved at "lægge 1 til" et passende antal gange. Vi ledes derfor til følgende

DEFINITION. I mængden $\mathbb{N}$ defineres en relation kaldet <u>mindre end</u> og betegnet $<$ ved

$$x < y \iff \exists\, n \in \mathbb{N} : x+n = y.$$

5.2. SÆTNING. <u>Relationen "mindre end" i $\mathbb{N}$ er en total, irrefleksiv ordensrelation.</u>

Bevis. Relationen er irrefleksiv, thi var $x+n=x$, ville vi få $x+n+1 = x+1$, og videre - da forkortningsreglen gælder i $(\mathbb{N},+)$ - $n^+ = n+1 = 1$, og dette kan ikke være tilfældet.

Relationen er transitiv, thi af $x+n=y$, $y+m=z$ følger $x+(n+m)=z$.

Vi viser endelig, at relationen er total. For naturlige tal $x,y \in \mathbb{N}$ siger vi, at "x er sammenlignelig med y", og vi skriver x smlg y, hvis der gælder $x<y$ eller $x=y$ eller $y<x$. Vi skal altså vise, at hvilkesomhelst to naturlige tal er sammenlignelige. Vi bemærker først, at der gælder

$$x < y \Rightarrow x^+ < y^+,$$

og slutter heraf, at

$$x \text{ smlg } y \Rightarrow x^+ \text{ smlg } y^+$$

Videre bemærker vi, at 1 er sammenlignelig med ethvert $y \in \mathbb{N}$, thi hvis $y \neq 1$ kan vi skrive $y = n^+ = n+1 = 1+n$, og har altså $1<y$.

Vi viser nu ved induktion, at mængden

$$S = \{x \in \mathbb{N} \mid \forall y \in \mathbb{N} : x \text{ smlg } y\}$$

er hele $\mathbb{N}$.

Som allerede bemærket har vi $1 \in S$. Antag nu, at $x \in S$, og betragt et $y \in \mathbb{N}$. Hvis $y = 1$, er y sammenlignelig med ethvert naturligt tal, altså specielt med x^+. Hvis $y \neq 1$, kan vi skrive $y = z^+$; da $x \in S$, har vi x smlg z, og heraf følger som bemærket, at x^+ smlg z^+, altså at x^+ smlg y. Følgelig er $x^+ \in S$. ▨

5.3. SÆTNING. For relationen "mindre end" i $\mathbb{N}$ gælder

(1) $p < q \Rightarrow p + n < q + n$

(2) $p < q \Rightarrow pn < qn$.

Bevis. En simpel konsekvens af definitionen og sætningerne 3.2.(1), 3.2.(2) og 4.2.(5). □

Vi kan nu give et nyt bevis for at forkortningsreglen gælder i $(\mathbb{N}, \cdot)$, thi er $p \neq q$, har vi enten $p < q$ og dermed $pn < qn$ eller $q < p$ og dermed $qn < pn$; i begge tilfælde er altså $pn \neq qn$.

5.4. SÆTNING. Den ordnede mængde $(\mathbb{N}, \leqslant)$ har intet sidste element.

Bevis. For hvert $x \in \mathbb{N}$ gælder $x < x + 1$ ▨

5.5. SÆTNING. For hvert $x \in \mathbb{N}$ gælder $1 \leqslant x$, d.v.s. den ordnede mængde $(\mathbb{N}, \leqslant)$ har 1 som første element.

Bevis. Hvert $x \neq 1$ kan skrives $x = y^+ = 1 + y$, hvoraf følger $1 < x$. ▨

5.6. SÆTNING. For alle $x, y \in \mathbb{N}$ gælder: $x < y \Rightarrow x^+ \leqslant y$.

Bevis. Hvis $x < y$, kan vi skrive $x + n = y$. Da $1 \leqslant n$ (5.5.) er $x + 1 \leqslant x + n$ (5.3.(1)), altså $x^+ = x + 1 \leqslant x + n = y$. ▨

5.7. SÆTNING. Enhver ikke-tom delmængde P af $\mathbb{N}$ har et første element. (m.h.t. $\leq$).

Bevis. Lad S være mængden af minoranter for P, altså $S = \{x \in \mathbb{N} \mid \forall p \in P : x \leq p\}$. Det er klart, at $1 \in S$. Hvis der for hvert $a \in S$ galdt $a^+ \in S$, kunne vi ved induktion slutte, at $S = \mathbb{N}$, hvilket øjensynlig ikke kan være tilfældet. Der findes følgelig et element $a \in S$ således at $a^+ \notin S$. For ethvert $p \in P$ gælder $a \leq p$. Hvis $a \notin P$, ville der endda for ethvert $p \in P$ gælde $a < p$, og dermed $a^+ \leq p$, i modstrid med at $a^+ \notin S$. Altså er $a \in P$, og det er nu klart, at a er første element i P. ▨

5.8. DEFINITION. En ordnet mængde $(M, \prec)$ kaldes velordnet, hvis enhver ikke-tom delmængde P af M har et første element. Sætning 5.7. udsiger altså at $(\mathbb{N}, \leq)$ er velordnet.

En velordnet ikke-tom mængde $(M, \prec)$ har specielt et første element. Endvidere har hvert element $x \in M$, som ikke er sidste element i M, et (og naturligvis kun ét) umiddelbart følgende, d.v.s. et element $x' \in M$, som opfylder

$$x \prec x' \text{ og } x \prec y \Rightarrow x' \preceq y,$$

nemlig det første element i den ikke-tomme mængde $\{y \in M \mid x \prec y\}$. Det første element i $(\mathbb{N}, \leq)$ er 1; for hvert $x \in \mathbb{N}$ har vi $x < x^+$, og sætning 5.6. viser, at det umiddelbart følgende til x er x^+.

5.9. Hvis a er et element i en ordnet mængde $(M, \prec)$, betegner vi med $M_{\prec a}$ delmængden

$$M_{\prec a} = \{x \in M \mid x \prec a\}.$$

For velordnede mængder gælder nu

SÆTNING OM TRANSFINIT INDUKTION. *Lad $(M, \preceq)$ være en velordnet mængde. Hvis en delmængde S af M opfylder*

$$\forall a \in M : M_{\prec a} \subseteq S \Rightarrow a \in S,$$

så er $S = M$.

Bevis. Hvis delmængden $M \setminus S$ af M ikke var tom, ville den indeholde et første element a, og for alle $x \prec a$ ville vi få $x \in S$. Følgelig måtte $M_{\prec a} \subseteq S$, men dette er i modstrid med forudsætningen, da $a \notin S$. ▨

5.10. Da $(\mathbb{N}, \leqslant)$ er velordnet, har vi følgende – fra induktionsaksiomet 1.7. forskellige – gyldige

SÆTNING. *Hvis en delmængde S af $\mathbb{N}$ opfylder*

$$\forall a \in \mathbb{N} : \mathbb{N}_{<a} \subseteq S \Rightarrow a \in S,$$

så er $S = \mathbb{N}$, der også kaldes

SÆTNINGEN OM FULDSTÆNDIG INDUKTION.

5.11. For den ordnede mængde $(\mathbb{N}, \leqslant)$ gælder yderligere følgende

SÆTNING. *Enhver ikke-tom, opad begrænset delmængde Q af $\mathbb{N}$ har et sidste element.*

Bevis. Lad P være mængden af majoranter for Q, altså

$$P = \{x \in \mathbb{N} \mid \forall q \in Q : q \leqslant x\}.$$

I følge forudsætningen er $P \neq \emptyset$. Da $(\mathbb{N}, \leqslant)$ er velordnet findes et første element $p \in P$. Det er nu ikke svært at vise, at p er sidste element i Q. □

5.12. Egenskaberne i sætningerne 5.4, 5.7 og 5.11 karakteriserer den ordnede mængde $(\mathbb{N}, \leqslant)$ idet der gælder:

SÆTNING. Lad $(N, \prec)$ være en ikke-tom, ordnet mængde, som tilfredsstiller følgende betingelser:

(1) N har ikke et største element.

(2) N er velordnet ved $\prec$.

(3) Enhver ikke-tom, opad begrænset delmængde af N har et største element.

Der findes da netop én isomorfi: $(\mathbb{N}, \leqslant) \to (N, \prec)$.

Bevis: Betingelserne (1) og (2) sikrer, at vi kan definere en afbildning $\varphi: N \to N$ ved at afbilde hvert element $x \in N$ på det umiddelbart følgende. Idet n_1 betegner det første element i N får vi et tripel (N, n_1, φ), og det er klart, at en isomorfi: $(\mathbb{N}, \leqslant) \to (N, \prec)$ må være en isomorfi af tripler: $(\mathbb{N}, 1, \varepsilon) \to (N, n_1, \varphi)$. Heraf følger entydigheden.

For at vise eksistensen, betragter vi den naturlige homomorfi: $f: (\mathbb{N}, 1, \varepsilon) \to (N, n_1, \varphi)$. Det er let at se, at f er bijektiv (surjektiviteten sikres af betingelsen (3)), og det vises ved induktion (eller transfinit induktion), at f er ordenstro $\square$

5.13. En delmængde af $\mathbb{N}$ af formen $\mathbb{N}_{<a}$ kaldes et afsnit. For $a = 1$ finder vi $\mathbb{N}_{<a} = \emptyset$; alle andre afsnit er $\neq \emptyset$. Da hvert naturligt tal $\neq 1$ er af formen a^+, kan de ikke-tomme afsnit skrives

$$\mathbb{N}_{<a^+} = \{x \in \mathbb{N} \mid x < a^+\} = \{x \in \mathbb{N} \mid x \leqslant a\}.$$

Afsnittet $\mathbb{N}_{<a^+}$ betegnes også $\mathbb{N}_a$, $[1, a]$ eller $\{1, \dots, a\}$.

Lad nu Q være en vilkårlig mængde. En afbildning $f: \mathbb{N} \to Q$ kaldes også en følge i Q; billedelementet $f(n)$ betegnes f_n, og vi skriver også

$$f = (f_1, f_2, \dots).$$

Mængden af følger i Q betegnes $Q^{\mathbb{N}}$.
En afbildning $f: \mathbb{N}_p \to Q$, hvor $\mathbb{N}_p$ er afsnittet $\{1, \cdots, p\}$, kaldes et <u>p-sæt i Q</u>, og vi skriver

$$f = (f_1, \cdots, f_p).$$

Mængden af p-sæt i Q, altså mængden af afbildninger: $\mathbb{N}_p \to Q$, betegnes Q^p.

Sætningen om definition ved induktion 1.4. er et middel til at definere følger i en mængde Q, idet den udsiger, at hvis vi har givet et element $q_1 \in Q$ og en afbildning $\varphi: Q \to Q$, så findes netop en følge $f = (f_1, f_2, \cdots)$ i Q, således at

$$(*) \quad f_1 = q_1 \text{ og } f_{n+1} = \varphi(f_n) \text{ for alle } n \in \mathbb{N}.$$

Vi siger, at følgen $f = (f_1, f_2, \cdots)$ er defineret <u>rekursivt</u> ved $(*)$. Ofte vil vi definere følgen ved mere generelle former for rekursion. Den gælder:

SÆTNING OM DEFINITION VED REKURSION. <u>Lad der være givet et element $q_1 \in Q$ og en "forskrift" Φ, der til hvert $n \in \mathbb{N}$ og hvert n-sæt $(x_1, \cdots, x_n)$ i Q knytter et element $\Phi(x_1, \cdots, x_n) \in Q$. Der findes da en og kun én følge $f = (f_1, f_2, \cdots)$ i Q, således at</u>

$$\underline{f_1 = q_1 \text{ og } f_{n+1} = \Phi(f_1, \cdots, f_n) \text{ for alle } n \in \mathbb{N}.}$$

Vi kan tænke på forskriften Φ som en familie af afbildninger $\Phi_n: Q^n \to Q$.
Vi vil ikke bevise denne sætning. Den kan formuleres for enhver velordnet mængde $(N, \prec)$ (i stedet for $(\mathbb{N}, \leqslant)$), og den kan bevises ved transfinit induktion.

6. Endelige og uendelige mængder. Kardinaltal.

6.1. SÆTNING. *Lad a være et naturligt tal, og betragt afsnittet $\mathbb{N}_a = \{1, \cdots, a\}$. Enhver injektiv afbildning $s : \mathbb{N}_a \to \mathbb{N}_a$ er bijektiv.*

Bevis. Påstanden vises ved induktion. For $a = 1$ er den triviel, thi vi har $\mathbb{N}_1 = \{1\}$, og den eneste afbildning $\{1\} \to \{1\}$ er den identiske afbildning. Antag nu at sætningen er vist for det naturlige tal a, og betragt en injektiv afbildning $s : \mathbb{N}_{a^+} \to \mathbb{N}_{a^+}$. Hvis $s(a^+) = a^+$, bestemmer s ved restriktion en injektiv afbildning $s' : \mathbb{N}_a \to \mathbb{N}_a$; det følger, at s' er surjektiv, og dermed at s er surjektiv. Hvis $s(a^+) \neq a^+$, defineres ved

$$t(x) = \begin{cases} x, & x \neq s(a^+), a^+ \\ a^+ & x = s(a^+) \\ s(a^+) & x = a^+ \end{cases} \qquad x \in \mathbb{N}_{a^+}$$

en afbildning $t : \mathbb{N}_{a^+} \to \mathbb{N}_{a^+}$, som øjensynlig er bijektiv. Den sammensatte afbildning $t \circ s$ er injektiv, og opfylder $(t \circ s)(a^+) = a^+$; den er derfor bijektiv ifølge det allerede viste, men så er også $s = t^{-1} \circ (t \circ s)$ bijektiv. ▨

6.2. DEFINITION. En mængde M kaldes *endelig*, hvis den er ækvipotent med et afsnit i $\mathbb{N}$. En mængde, der ikke er endelig, kaldes *uendelig*. Den tomme mængde $\emptyset$ er endelig, nemlig ækvipotent med afsnittet $\mathbb{N}_{<1}$. En ikke-tom endelig mængde M er ækvipotent med et afsnit af formen $\mathbb{N}_a = \{1, \cdots, a\}$. Dette tal a er entydigt bestemt, thi var M også ækvipotent med et afsnit $\mathbb{N}_b$, og antog vi f.eks. at $a < b$, da kunne vi ved sammensætning få en afbildning $\mathbb{N}_b \twoheadrightarrow M \xrightarrow{\sim} \mathbb{N}_a \hookrightarrow \mathbb{N}_b$, der var injektiv,

men ikke surjektiv, i modstrid med sætning 6.1.
Det entydigt bestemte naturlige tal a kaldes kardinaltallet for den ikke-tomme mængde M, og betegnes Card(M) eller $|M|$.

I denne forbindelse tilføjes ofte til de naturlige tal et element betegnet 0. Til den herved fremkomne udvidede mængde $\tilde{\mathbb{N}} = \mathbb{N} \cup \{0\}$, kan vi på velkendt måde udvide additionen, multiplikationen og ordningen fra de naturlige tal. Den tomme mængde $\emptyset$ tilskrives kardinaltallet 0. Elementerne i $\tilde{\mathbb{N}}$ kaldes de endelige kardinaltal. Bemærk, at der for afsnittene $\tilde{\mathbb{N}}_{<x}$ i den udvidede mængde gælder

$$|\tilde{\mathbb{N}}_{<a}| = a \,, \quad a \in \tilde{\mathbb{N}}.$$

Vi anfører en række velkendte sætninger om endelige mængder. De kan alle vises ved "induktion efter kardinaltallet".

SÆTNING.
6.3. Lad $f: Q \to M$ være en injektiv afbildning. Hvis M er endelig, er også Q endelig og $|Q| \leqslant |M|$. □

SÆTNING.
6.4. Lad $g: M \to P$ være en surjektiv afbildning. Hvis M er endelig, er også P endelig og $|P| \leqslant |M|$. □

SÆTNING.
6.5. Lad $M_1 \times M_2$ være det kartesiske produkt af mængderne M_1 og M_2. Hvis M_1 og M_2 er endelige, er også $M_1 \times M_2$ endelig, og $|M_1 \times M_2| = |M_1| \cdot |M_2|$. □

SÆTNING.
6.6. Lad M_1 og M_2 være delmængder af en mængde Q. Hvis M_1 og M_2 er endelige, er også $M_1 \cup M_2$ og $M_1 \cap M_2$ endelige, og $|M_1 \cup M_2| + |M_1 \cap M_2| = |M_1| + |M_2|$. □

SÆTNING.
6.7. Lad $(M, \prec)$ være en totalt ordnet mængde. Hvis M er endelig, er $(M, \prec)$ velordnet. □

6.8. Endvidere gælder:

SÆTNING. Mængden $\mathbb{N}$ af naturlige tal er uendelig.

Bevis. Af definitionerne og sætning 6.1. følger, at hvis en mængde M er endelig, så er enhver injektiv afbildning $: M \to M$ surjektiv. Af uendelighedsaksiomet fremgår, at $\varepsilon : \mathbb{N} \to \mathbb{N}$ er en injektiv, ikke-surjektiv afbildning. Følgelig kan $\mathbb{N}$ ikke være endelig. ▨

6.9. Til sidst viser vi

SÆTNING. Lad Q være en uendelig mængde. Der findes en injektiv afbildning $f: \mathbb{N} \hookrightarrow Q$.

Bevis. Vi vælger et element $f_1 \in Q$. Nu er $\{f_1\}$ ikke hele Q, så vi kan vælge $f_2 \in Q$ med $f_2 \neq f_1$. Nu er $\{f_1, f_2\}$ ikke hele Q, så vi kan vælge $f_3 \in Q$, således at $f_3 \notin \{f_1, f_2\}$. Vi kan fortsætte således, thi i det n-te skridt har vi indbyrdes forskellige elementer $f_1, \dots, f_n$. Her kan $\{f_1, \dots, f_n\}$ ikke være hele Q, da Q ellers ville være ækvipotent med afsnittet $\mathbb{N}_n$. Vi kan derfor vælge $f_{n+1} \in Q$, således at $f_{n+1} \notin \{f_1, \dots, f_n\}$. Altså kan vi finde en følge $f = (f_1, f_2, \dots)$ i Q, som klart er en injektiv afbildning $f: \mathbb{N} \to Q$. ▨

KOROLLAR. En mængde Q er uendelig, hvis og kun hvis der findes en injektiv, ikke surjektiv afbildning $\varphi : Q \to Q$.
En mængde M er endelig, hvis og kun hvis enhver injektiv afbildning $s: M \to M$ er bijektiv.

Bevis. Følger af sætningerne 6.1 og 6.9. ⊛

6.10. Bemærkning. Vi vil af og til senere møde – og uden videre godtage beviser analoge med det for sætning 6.9. givne. Lad os her et øjeblik se nærmere på

beviset. Vi har argumenteret for eksistensen af den ønskede afbildning $f: \mathbb{N} \to Q$ på en måde, der meget minder om definition ved rekursion (sætning 5.13.). Blot har vi i det n-te skridt ingen forskrift, der til hvert n-sæt $(x_1, \cdots, x_n) \in Q^n$ knytter et element i Q; elementet f_{n+1} fik vi jo ud fra $f_1, \cdots, f_n$ ved at vælge (blandt mange mulige). For at bestemme afbildningen $f: \mathbb{N} \to Q$ har vi måttet foretage uendelig mange valg, endda på en sådan måde, at hvert valg afhænger af de foregående valg.

For i en sådan situation at kunne godtgøre eksistensen af visse afbildninger, er det nødvendigt i mængdelæren at antage det såkaldte

UDVALGSAKSIOM. Lad Q være en mængde og lad $\mathbb{P}^*(Q)$ betegne mængden af ikke-tomme delmængder af Q. Der findes da afbildninger $u: \mathbb{P}^*(Q) \to Q$, således at $u(A) \in A$ for alle $A \in \mathbb{P}^*(Q)$.

En sådan afbildning $u: \mathbb{P}^*(Q) \to Q$ kaldes en udvalgsfunktion på Q. Den knytter altså til hvert element $A \in \mathbb{P}^*(Q)$, d.v.s. til hver ikke-tom delmængde $A \subseteq Q$, et udvalgt element $u(A) \in A$.

I det foregående har vi ikke nævnt hvilke antagelser (aksiomer), vi har forudsat fra mængdelæren. Det kan derfor synes unødigt her at fremhæve udvalgsaksiomet, der vel virker ret selvfølgeligt. På den anden side er det værd at bemærke, at man ikke kan "angive" en udvalgsfunktion f.eks. på mængden $\mathbb{R}$ af reelle tal. (prøv!).

Vender vi tilbage til sætning 6.9 er det let ud fra en udvalgsfunktion u på Q at definere den ønskede afbildning $f: \mathbb{N} \to Q$ rekursivt ved

$$f_1 = u(Q), \quad f_{n+1} = u\left(Q \setminus \{f_1, \ldots, f_n\}\right). \quad \square$$

7. Oversigt over de grundlæggende egenskaber ved de naturlige tal.

7.1. BESKRIVELSE. Systemet af naturlige tal er en mængde $\mathbb{N}$ i hvilken der er givet et udvalgt element $1 \in \mathbb{N}$ (kaldet én) og en afbildning $\varepsilon : \mathbb{N} \to \mathbb{N}$ kaldet efterfølger-afbildningen.

7.2. FUNDAMENTALE AKSIOMER.

AKSIOM OM INDUKTIV DEFINITION. Er der givet en mængde Q, et udvalgt element $q_1 \in Q$ og en afbildning $\varphi : Q \to Q$, så findes der netop én afbildning $f : \mathbb{N} \to Q$, som opfylder:

$$f(1) = q_1 \quad \text{og} \quad f(\varepsilon(n)) = \varphi(f(n)) \text{ for alle } n \in \mathbb{N}.$$

UENDELIGHEDSAKSIOMET. Efterfølgerafbildningen $\varepsilon : \mathbb{N} \to \mathbb{N}$ er injektiv, og $1 \notin \varepsilon(\mathbb{N})$.

INDUKTIONSAKSIOMET. Er $S \subseteq \mathbb{N}$ en delmængde, som opfylder:

$$1 \in S \quad \wedge \quad \varepsilon(S) \subseteq S,$$

så er $S = \mathbb{N}$.

7.3. POTENSER. For et element a i en semigruppe $(M, \cdot)$ definerer potenser med naturlig eksponent $n \in \mathbb{N}$

$$a^1 = a, \qquad a^n = \overbrace{a \cdots a}^{n}.$$

[Er kompositionen additivt skrevet, bruges betegnelsen

$$1a = a \qquad na = \overbrace{a + \ldots + a}^{n}. \;]$$

7.4. FUNDAMENTALE STRUKTURER. Addition i $\mathbb{N}$ er kompositionen $(x,n) \mapsto x+n$ defineret ved

$$x+n := \varepsilon^n(x) = \overbrace{\varepsilon \circ \cdots \circ \varepsilon}^{n}(x).$$

Multiplikation i $\mathbb{N}$ er kompositionen $(n,p) \mapsto n \cdot p$ defineret ved

$$n \cdot p := np = \overbrace{p + \cdots + p}^{n}.$$

Relationen "mindre end" i $\mathbb{N}$ er relationen $<$ defineret ved

$$x < y \overset{\text{DEF}}{\iff} \exists n \in \mathbb{N} : x+n = y.$$

7.5. REGNEREGLERNE. For naturlige tal p, q og r gælder:

$$\begin{cases} p+q = q+p \\ p+(q+r) = (p+q)+r \end{cases}$$ (+ er kommutativ), (+ er associativ)

$$\begin{cases} pq = qp \\ p(qr) = (pq)r \\ p1 = 1p = p \end{cases}$$ (· er kommutativ), (· er associativ), (1 er neutralt element for ·)

$$\begin{cases} p(q+r) = pq + pr \\ (p+q)r = pr + qr \end{cases}$$ (· er distributiv m.h.t. +)

$$\begin{cases} p \not< p \\ p<q \wedge q<r \Rightarrow p<r \\ p<q \vee q<p \vee p=q \end{cases}$$ (< er irrefleksiv), (< er transitiv), (< er total)

$$\begin{cases} p<q \Rightarrow p+r < q+r \\ p<q \Rightarrow pr < qr \end{cases}$$ (< harmonerer med +), (< harmonerer med ·)

$$\begin{cases} p+r = q+r \Rightarrow p=q \\ pr = qr \Rightarrow p=q \end{cases}$$ (forkortningsregel for +), (forkortningsregel for ·)

7.6. POTENSREGLERNE. For elementer a og b i en semigruppe M og naturlige tal n og m gælder

1. potensregel: $a^{n+m} = a^n a^m$ $\quad [(n+m)a = na + ma]$
2. potensregel: $a^{nm} = (a^n)^m$ $\quad [(nm)a = n(ma)]$
3. potensregel: $(ab)^n = a^n b^n$, når $ab = ba$. $\quad [n(a+b) = na + nb]$

7.7. POTENSSÆTNINGEN. Lad der være givet en semigruppe $(M,\cdot)$ og et element $a \in M$. Da findes netop én homomorfi: $(\mathbb{N},+) \to (M,\cdot)$, som afbilder $1 \mapsto a$, nemlig afbildningen $n \mapsto a^n$.

7.8. VELORDNING. Den ordnede mængde $(\mathbb{N},<)$ er <u>velordnet</u>, d.v.s. enhver ikke-tom delmængde $P \subseteq \mathbb{N}$ har et mindste element. Endvidere er $1 \in \mathbb{N}$ det mindste element i $\mathbb{N}$, og for hvert element $n \in \mathbb{N}$ er $\varepsilon(n) = n+1$ det umiddelbart følgende.
SÆTNING OM FULDSTÆNDIG INDUKTION. Er $S \subseteq \mathbb{N}$ en delmængde, som opfylder:

$$\forall n \in \mathbb{N} : \mathbb{N}_{<n} \subseteq S \Rightarrow n \in S ,$$

så er $S = \mathbb{N}$.

7.9. KARDINALTAL. Enhver endelig ikke-tom mængde Q er ækvipotent med et <u>afsnit</u> $\mathbb{N}_{\leq n} = \{1,\cdots,n\}$ af de naturlige tal. Tallet $n \in \mathbb{N}$ er entydigt bestemt ved Q. Det kaldes <u>kardinaltallet</u> for Q og betegnes

$$n = \#Q = |Q| .$$

7.10. BETEGNELSER. Ofte udvides de naturlige tal $\mathbb{N}$ med et element betegnet 0 til en mængde $\tilde{\mathbb{N}} = \mathbb{N} \cup \{0\}$, og strukturerne (d.v.s. $+$, $\cdot$ og $<$) udvides på velkendt måde til $\tilde{\mathbb{N}}$. Den tomme mængde tillægges kardinaltallet $|\emptyset| = 0$.

For de første naturlige tal indføres betegnelserne

$$\varepsilon(1) = 2,\ \varepsilon(2) = 3,\ \varepsilon(3) = 4,\ \varepsilon(4) = 5,\ \varepsilon(5) = 6,\ \varepsilon(6) = 7,\ \varepsilon(8) = 9 .$$

Ethvert naturligt tal n kan da entydigt skrives

$$n = a_k \varepsilon(9)^k + \cdots + a_1 \varepsilon(9) + a_0, \quad k \in \tilde{\mathbb{N}},\ 0 \leq a_i \leq 9,\ 1 \leq a_k .$$

Er misforståelser udelukket, skrives også

$$n = a_k \cdots a_1 a_0 \qquad (\underline{\text{Positionssystemet}}) .$$

Specielt er

$$\varepsilon(9) = 10 .$$

DE HELE TAL. BRØKGRUPPE.

1. Bróker i en gruppe. Analyse 1.1: Analyse. 1.2: Bemærkning.

2. Brókgruppen. 2.1: Bróker. 2.2: Brókregning. 2.3: Den kanoniske homomorfi. Sætning. 2.4: Udvidelsessætning. 2.5: Notation.

3. De hele tal. 3.1: Definition. 3.2: Sætning om $\mathbb{Z} \setminus \mathbb{N}$. 3.3: Potens med hel eksponent. 3.4: Potenssætning. 3.5: Multiplikation. 3.6: Potensreglerne. 3.7: Ordning. 3.8: Ordningssætning.

4. Oversigt over de grundlæggende egenskaber ved de hele tal. 4.1: Beskrivelse. 4.2: Potenser. 4.3: Fundamentale strukturer. 4.4: Regnereglerne. 4.5: Potensreglerne. 4.6: Potenssætning. 4.7: Ordningssætning.

5. Yderligere egenskaber ved de hele tal. 5.1: Den kanoniske ringhomomorfi. 5.2: Eksempel. Endomorfiring. 5.3: Nulreglen m.m. 5.4: Divisionssætningen. 5.5: Hovedidealsætningen. 5.6: Divisor. Primisk. 5.7: Sætning. 5.8: Primtal. 5.9-10: Forbindelse med primisk. 5.11: Produkt af parvis primiske tal. 5.12: Hovedsætning om primtalsopløsning.

6. Appendix: Restklasser modulo n. 6.1: Kongruens modulo n. Restklasser. 6.2-3: Regning med restklasser. 6.4: Primiske restklasser. 6.5: Legemet $\mathbb{F}_p := \mathbb{Z}/p$, p primtal. 6.6: Den kinesiske restklassesætning. 6.7: Eulers φ-funktion. 6.8: Fermat's "lille" sætning. 6.9: Wilson's sætning. 6.10: Kongruensen $X^{\frac{p-1}{2}} \equiv 1$ og $Y^2 \equiv -1$ modulo et primtal p.

DE HELE TAL

BRØKGRUPPE

1. Bróker i en gruppe. Analyse

1.1. ANALYSE. Lad der være givet en kommutativ (ikke-tom) semigruppe $(H,\cdot)$. Vi ónsker, at indlægge H i en (større) gruppe, f.eks. for at kunne betragte ligninger

$$x\,s = a\,, \qquad \text{hvor } s,a \in H,$$

der jo i den større gruppe har lósningen $x = a\,s^{-1}$.

Lad os antage, at problemet er lóst i den forstand, at der er givet en indlejring $H \hookrightarrow G$, d.v.s. en injektiv homomorfi

$$\varphi : (H,\cdot) \hookrightarrow (G,\cdot),$$

hvor $(G,\cdot)$ er en gruppe med det neutrale element e. Vi udleder en række konsekvenser:

(0) Selv om gruppen G ikke forudsættes kommutativ, gælder for elementer $s,a \in H$, at

$$\varphi(a)\,\varphi(s) = \varphi(s)\,\varphi(a)$$

(idet begge er $= \varphi(as) = \varphi(sa)$, H var kommutativ), og at

$$\varphi(s)^{-1}\varphi(a) = \varphi(a)\,\varphi(s)^{-1}$$

(multiplicér med $\varphi(s)^{-1}$ først fra venstre, dernæst fra højre).

(1) Delmængden

$$H :_{\varphi} H^{-1} := \{\, \varphi(a)\varphi(s)^{-1} \mid (a,s) \in H\times H \,\}$$

er stabil i $(G,\cdot)$, idet

$$\left[\varphi(a)\,\varphi(s)^{-1}\right]\left[\varphi(b)\,\varphi(t)^{-1}\right] = \varphi(ab)\,\varphi(st)^{-1};$$

(2) den indeholder det neutrale element, idet

$$e = \varphi(s)\,\varphi(s)^{-1} \quad \text{med et } s \in H,$$

(3) og <u>den indeholder med ethvert element også dets inverse</u>, idet

$$\left[\varphi(a)\,\varphi(s)^{-1}\right]^{-1} = \varphi(s)\,\varphi(a)^{-1}!$$

(4) Delmængden $H \dot{\varphi} H^{-1} \subseteq G$ er således en <u>undergruppe</u> i G, og den indeholder billedmængden $\varphi(H)$, idet

$$\varphi(a) = \varphi(as)\,\varphi(s)^{-1} \quad \text{med et } s \in H.$$

Vi kan derfor betragte indlejringen som en indlejring:

$$H \hookrightarrow H \dot{\varphi} H^{-1}$$

(5) Videre gælder, at den <u>herved bestemte indlejring</u>: $H \hookrightarrow H \dot{\varphi} H^{-1}$ <u>kun afhænger af H</u> (og ikke af den givne indlejring $\varphi : H \hookrightarrow G$). Indføres nemlig i mængden $H \times H$ af par (a,s) kompositionen $\cdot$ defineret ved

$$(a,s)\cdot(b,t) = (ab, st)$$

og betragtes afbildningen $\Phi : H \times H \to G$ defineret ved

$$\Phi(a,s) = \varphi(a)\,\varphi(s)^{-1},$$

følger det af (1), at Φ er en homomorfi

$$\Phi : (H\times H, \cdot) \longrightarrow (G, \cdot)$$

Billedet ved Φ er øjensynlig netop gruppen $H \dot{\varphi} H^{-1}$, så ifølge isomorfisætningen induceres en isomorfi:

$$(H\times H, \cdot)/\widetilde{\Phi} \xrightarrow{\approx} (H \dot{\varphi} H^{-1}, \cdot),$$

hvor $\widetilde{\Phi}$ er den til Φ hørende kongruensrelation i $H \times H$, bestemt ved

$$(a,s) \mathrel{\widetilde{\Phi}} (a',s') \Leftrightarrow \Phi(a,s) = \Phi(a',s').$$

Og denne relation afhænger ikke af φ, thi

$$\begin{aligned}(a,s) \mathrel{\widetilde{\Phi}} (a',s') &\Leftrightarrow \varphi(a)\,\varphi(s)^{-1} = \varphi(a')\,\varphi(s')^{-1}\\ &\Leftrightarrow \varphi(a)\,\varphi(s') = \varphi(a')\,\varphi(s)\\ &\Leftrightarrow \varphi(as') = \varphi(a's)\\ &\Leftrightarrow as' = a's,\end{aligned}$$

da φ var injektiv.

1.2. BEMÆRKNING. Hvis den givne semigruppe $(H,\cdot)$ overhovedet kan indlejres i en gruppe, viser den foregående analyse, hvordan vi kan konstruere en sådan indlejring: Vi skal betragte produktmængden $H \times H$ med komposition $\cdot$ defineret i 1.1.(5), og heri kongruensrelationen $\sim$ fundet i 1.1.(5). Kvotienten $(H\times H,\cdot)/\sim$ er da den søgte gruppe. Problemet er imidlertid, at den i 1.1.(5) bestemte relation

$$(a,s) \sim (a',s') \Leftrightarrow as' = a's$$

i almindelighed ikke er en ækvivalensrelation. Det er jo også på forhånd klart, at ikke enhver semigruppe H kan indlejres i en gruppe, idet en nødvendig betingelse herfor er, at forkortningsreglen gælder i H.
Vi vil imidlertid vise, at den ovenfor skitserede konstruktion med en lille modifikation fører til en gruppe.

2. Brøkgruppen.

2.1. BRØKER. Lad $(H,\cdot)$ være en ikke-tom semigruppe, og betragt produktmængden $H\times H$, altså mængden af par (a,s), $a\in H, s\in H$. Et par af formen (au,su), $u\in H$ siges at fremgå af (a,s) ved at forlænge med u.

I $H\times H$ defineres en komposition $\cdot$ ved

$$(a,s)\cdot(b,t) := (ab,st)$$

og en relation $\equiv$ (kaldet "kongruens") ved

$$(a,s) \equiv (a',s') \overset{DEF}{\Leftrightarrow} \exists u,u'\in H : (au,su) = (a'u',s'u').$$

To par er således kongruente, hvis de kan forlænges til samme par. Det er let at se, at relationen opfylder

$$(a,s) \equiv (a',s') \Leftrightarrow \exists\, t\in H : tas' = ta's.$$

Videre gælder:

LEMMA. Kompositionen $\cdot$ i $H\times H$ er kommutativ og associativ (og $(H\times H,\cdot)$ er altså en kommutativ semigruppe), og relationen $\equiv$ er en kongruensrelation i $(H\times H,\cdot)$.
BEVIS. Prøv selv □

DEFINITION. En <u>brøk</u> (med teller og nævner fra H) er en ækvivalensklasse i $H\times H$. Ækvivalensklassen, der indeholder et givet par $(a,s)\in H\times H$ kaldes <u>brøken med teller a og nævner s</u> og betegnes a/s. Enhver brøk X kan skrives på formen $X=a/s$ med en passende <u>repræsentant</u> $(a,s)\in H\times H$.
Bemærk, at $au/su = a/s$, da $(au,su)\equiv(a,s)$.

2.2. BRØKREGNING. I følge Lemma 2.1 kan vi i mængden af brøker, d.v.s. i kvotienten $H\times H/\equiv$, definere et <u>produkt</u> ved regning med repræsentanter: Har brøken X repræsentanten (a,s) og brøken Y repræsentanten (b,t), defineres produktet $X\cdot Y$ som ækvivalensklassen, der indeholder produktet $(a,s)\cdot(b,t)=(ab,st)$ af repræsentanterne. Vi har altså

$$a/s \cdot b/t = ab/st .$$

SÆTNING. Kvotienten $(H\times H,\cdot)/\equiv$ er en kommutativ gruppe. Dens neutrale element er brøken $E=u/u$ (der ikke afhænger af $u\in H$), og for en brøk af formen $X=a/s$ er den inverse bestemt ved $X^{-1}=s/a$.
BEVIS. Da kompositionen $\cdot$ i $H\times H$ er kommutativ og associativ, nedarves dette til kvotienten. En vilkårlig brøk X kan skrives $X=a/s$, og da parrene (a,s) og (au,su) er ækvivalente, har vi

$$X\cdot E = a/s\cdot u/u = au/su = a/s = X.$$

Brøken $E=u/u$ er derfor neutralt element (og specielt uafhængig af u). Vælges for brøken X en repræsentant (a,s) finder vi

$$X \cdot s/a = a/s \cdot s/a = as/sa = as/as = E$$

Brøken $X = a/s$ er derfor invertibel, med $X^{-1} = s/a$ ▨

DEFINITION. Gruppen $(H\times H, \cdot)/\equiv$ kaldes den til semigruppen H hørende brøkgruppe, og den betegnes

$$H[H^{-1}] := (H\times H, \cdot)/\equiv .$$

2.3. DEN KANONISKE HOMOMORFI. For et givet $a \in H$ er alle par (au, u), $u \in H$, åbenbart ækvivalente. Brøken au/u, der altså ikke afhænger af $u \in H$, betegnes

$$\boxed{a} := au/u .$$

OBSERVATION. Den ved $a \mapsto \boxed{a}$ bestemte afbildning

$$\square : H \longrightarrow H[H^{-1}]$$

er en homomorfi,
thi $\boxed{a}\cdot\boxed{b} = au/u \cdot bv/v = ab(uv)/uv = \boxed{ab}$.
Den kaldes den kanoniske homomorfi af H ind i brøkgruppen $H[H^{-1}]$.
Enhver brøk X kan skrives på formen

$$X = \boxed{a}\cdot\boxed{s}^{-1}, \quad a \in H, \ s \in H,$$

thi vælges for X en repræsentant (a, s) finder vi

$$\boxed{a}\cdot\boxed{s}^{-1} = au/u \cdot (sv/v)^{-1} = au/u \cdot v/sv$$
$$= a(uv)/s(uv) = a/s = X.$$

SÆTNING. Den kanoniske homomorfi $\square : H \to H[H^{-1}]$ er injektiv, hvis og kun hvis forkortningsreglen gælder i H. I bekræftende fald er kongruensrelationen $\equiv$ bestemt ved

$$(a, s) \equiv (a', s') \Leftrightarrow as' = a's.$$

BEVIS. "hvis": Er $\boxed{a} = \boxed{b}$, altså $au/u = bv/v$, så er parrene (au, u) og (bv, v) ækvivalente. Der findes altså $s, t \in H$, så at $(aus, us) = (bvt, vt)$. Med $w := us = vt$ har vi derfor $aw = bw$, men så er $a = b$.
"kun hvis": Er $aw = bw$, så er $\boxed{a} = aw/w = bw/w = \boxed{b}$, og dermed $a = b$.

"$\Leftarrow$": Er $as' = a's$, så er $(as', ss') = (a's, s's)$, og følgelig $(a,s) \equiv (a',s')$.
"$\Rightarrow$": Er $(a,s) \equiv (a',s')$, så findes (jfr. 2.1.) et $t \in H$, således at $tas' = ta's$. Gælder forkortningsreglen, får vi heraf $as' = a's$ ▨

Af sætningen følger, at den kommutative semigruppe H kan indlejres i en gruppe, netop når forkortningreglen gælder i H. Også uden denne forudsætning gælder imidlertid følgende:

2.4. UDVIDELSESSÆTNING FOR BRØKGRUPPER. Lad H være en kommutativ semigruppe og betragt den kanoniske homomorfi $\square : H \to H[H^{-1}]$ ind i brøkgruppen. Enhver homomorfi $\varphi : (H,\cdot) \to (G,\cdot)$ fra semigruppen H til en gruppe G kan da entydigt udvides til en homomorfi $\tilde{\varphi} : H[H^{-1}] \to G$ fra brøkgruppen.
BEVIS. "Entydighed: Enhver brøk X kan skrives

$$X = a/s = \boxed{a} \cdot \boxed{s}^{-1}, \quad a, s \in H,$$

og så er $X \cdot \boxed{s} = \boxed{a}$. Hvis homomorfien $\tilde{\varphi}$ er en udvidelse af φ, får vi $\varphi(a) = \tilde{\varphi}(\boxed{a}) = \tilde{\varphi}(X \cdot \boxed{s})$ $= \tilde{\varphi}(X)\,\tilde{\varphi}(\boxed{s}) = \tilde{\varphi}(X)\,\varphi(s)$, hvoraf

$$\tilde{\varphi}(X) = \varphi(a)\,\varphi(s)^{-1}$$

Heraf følger entydigheden.
Eksistens: Overvej, at den ved $(a,s) \mapsto \varphi(a)\varphi(s)^{-1}$ definerede afbildning $: H \times H \to G$ er en homomorfi, der respekterer $\equiv$. Overvej, at den inducerede homomorfi $: (H \times H, \cdot)/\equiv \to G$ fra kvotienten opfylder de stillede krav □

2.5. NOTATION. Den foregående konstruktion er gennemført i tilfældet, hvor kompositionen er multiplikativt skrevet, men kan naturligvis gennemføres for enhver kommutativ semigruppe uanset hvilket tegn, der benyttes for kompositionen. I den mere generelle situation bruges betegnelser som "brøk", "brøkgruppe" og lignende.

For en additivt skrevet, kommutativ semigruppe $(H,+)$ er kompositionen i $H\times H$ bestemt ved

$$(a,s)+(b,t) = (a+b, s+t),$$

og kongruensrelationen bestemt ved

$$(a,s) \equiv (a',s') \Leftrightarrow \exists\, u,u'\in H: (a+u, s+u) = (a'+u', s'+u').$$

Ækvivalensklassen, d.v.s. "brøken", der indeholder et par (a,s) betegnes $\textcircled{a,s}$. Den tilhørende "brøkgruppe" skrives også additivt, og den betegnes $H[-H]$. Ifølge 2.3. kan enhver "brøk" X skrives

$$X = \boxed{a} - \boxed{s}\ , \quad a,s\in H.$$

3. De hele tal.

3.1. DEFINITION. "Brøkgruppen" $\mathbb{N}[-\mathbb{N}]$ dannet ud fra den kommutative semigruppe $(\mathbb{N},+)$ kaldes de hele tals additive gruppe og betegnes $(\mathbb{Z},+)$ (eller $\mathbb{Z}^+$ eller blot $\mathbb{Z}$). Elementerne i $\mathbb{Z}$ kaldes hele tal. Da forkortningsreglen gælder i $(\mathbb{N},+)$, er den kanoniske homomorfi $(\mathbb{N},+)\to(\mathbb{Z},+)$ injektiv. Vi vil (næsten) altid identificere elementer i $\mathbb{N}$ med deres billeder i $\mathbb{Z}$ ved denne afbildning, og altså opfatte $\mathbb{N}$ som en stabil delmængde af $(\mathbb{Z},+)$. Den kanoniske homomorfi er da inklusionsafbildningen: $\mathbb{N}\hookrightarrow\mathbb{Z}$.

Et helt tal er altså en "brøk". Med den indførte identifikation kan altså hvert helt tal $x\in\mathbb{Z}$ skrives

$$x = a - s\ , \quad a,s\in\mathbb{N}$$

som en differens mellem to elementer i (delmængden) $\mathbb{N}$.

Det neutrale element i den kommutative gruppe $(\mathbb{Z},+)$ kaldes <u>nul</u> og betegnes 0.

3.2. Vi kan nemt få et overblik over hvilke elementer $\mathbb{Z}$ indeholder udover elementerne i $\mathbb{N}$.

SÆTNING. For hvert helt tal $x \in \mathbb{Z}$ indtræffer netop en af følgende tre muligheder:

$$x \in \mathbb{N} \; ; \quad x = 0 \; ; \quad -x \in \mathbb{N}.$$

BEVIS. Betragtes en vilkårlig fremstilling af x som en differens $x = a - s$, $a, s \in \mathbb{N}$, gælder:

$$(+) \quad x \in \mathbb{N} \iff s < a$$

$$(0) \quad x = 0 \iff s = a$$

$$(-) \quad -x \in \mathbb{N} \iff a < s.$$

At $a - s = x \in \mathbb{N}$ kan jo udtrykkes ved at der findes et $n \in \mathbb{N}$ (nemlig $n = x$), så at $a = s + n$, og det betyder jo netop, at $s < a$. At (0) gælder, er trivielt, og (-) følger af (+), idet vi for $-x$ har fremstillingen $-x = s - a$. Sætningen følger nu af at relationen $<$ er en total, irrefleksiv ordensrelation i $\mathbb{N}$. ▨

3.3. Udvidelsessætningen 2.4 omhandler for semigruppen $(\mathbb{N},+)$ homomorfier: $(\mathbb{N},+) \to (G,\cdot)$, hvor G er en gruppe, altså afbildninger af formen $n \mapsto a^n$, hvor a er et element i gruppen G. Er a et element i en gruppe $(G,\cdot)$, kan homomorfien $n \mapsto a^n$ altså entydigt udvides til en homomorfi fra brökgruppen, d.v.s. til en homomorfi:

$$(\mathbb{Z},+) \longrightarrow (G,\cdot).$$

DEFINITION. Den udvidede homomorfi: $(\mathbb{Z},+) \to (G,\cdot)$ betegnes (også) $p \mapsto a^p$, $p \in \mathbb{Z}$, og billedet a^p af et helt tal p kaldes den <u>p'te potens af a</u>. Hvis gruppen er en additivt skrevet (kommutativ) gruppe $(G,+)$, bruges betegnelsen

$$pa \; , \quad p \in \mathbb{Z}, \; a \in G$$

for den p'te potens af a.

BEMÆRKNING. Da afbildningen $p \mapsto a^p$ er en homomorfi: $(\mathbb{Z},+) \to (G,\cdot)$, har vi

a^0 = neutrale element i G

a^{-p} = inverse til a^p.

I forbindelse med sætning 3.2 fås herved en bestemmelse af a^p, $p \in \mathbb{Z}$. Det ses også, at den sædvanlige betegnelse for det inverse til $a \in G$ harmonerer med den indførte potens a^{-1}.

Af den såkaldte potenssætning for $\mathbb{N}$ (Naturlige tal, sætning 3.4) får vi:

3.4. POTENSSÆTNING. Lad a være et element i gruppen $(G,\cdot)$. Der findes netop én homomorfi: $(\mathbb{Z},+) \to (G,\cdot)$, så at $1 \mapsto a$, nemlig afbildningen $p \mapsto a^p$.

BEVIS □

3.5. MULTIPLIKATION. DEFINITION. I mængden $\mathbb{Z}$ defineres en komposition kaldet <u>multiplikation</u> og betegnet $(p,q) \mapsto p \cdot q$ ved

$$p \cdot q := pq = p\text{'te potens af } q \text{ i gruppen } (\mathbb{Z},+).$$

Det er klart, at denne komposition på delmængden $\mathbb{N}$ stemmer overens med den allerede indførte multiplikation i $\mathbb{N}$.

SÆTNING. Med denne multiplikation er $(\mathbb{Z},+,\cdot)$ en kommutativ ring, hvis et-element er det naturlige tal 1.

BEVIS. Vi skal vise, at ligningerne (1), (2), (3) og (5) (Naturlige tal, sætning 4.2) gælder for hele tal. Det der givne bevis kan ordret kopieres, under brug af sætning 3.4. □

3.6. POTENSREGLERNE. For elementer a og b i en multiplikativt [resp. additivt] skrevet gruppe G, og hele tal p og q gælder:

1. regel: $a^{p+q} = a^p \cdot a^q$ $\quad [(p+q)a = pa + qa]$.

2. regel: $a^{pq} = (a^p)^q$ $\quad [(pq)a = p(qa)]$.

3. regel: $(ab)^p = a^p b^p$ når $ab = ba$ $\quad [p(a+b) = pa + pb]$.

BEVIS. 1. regel udsiger, at afbildningen $p \mapsto a^p$ er en homomorfi: $(\mathbb{Z},+) \to (G,\cdot)$, jfr. definition 3.3.
2. regel indses ved for et fast $p \in \mathbb{Z}$ at betragte afbildningen $q \mapsto a^{pq}$. Den er en homomorfi: $(\mathbb{Z},+) \to (G,\cdot)$, og da den sender $1 \mapsto a^p$, må vi have $a^{pq} = (a^p)^q$ for alle $q \in \mathbb{Z}$.
3. regel fås f.eks. udfra den tilsvarende regel for eksponent i $\mathbb{N}$ v.hj.a. bemærkning 3.4. □

3.7. ORDNING. DEFINITION. I mængden $\mathbb{Z}$ defineres en relation kaldet "mindre end" og betegnet $<$ ved

$$p < q \overset{\text{DEF}}{\iff} q - p \in \mathbb{N}.$$

Det er klart, at denne relation på delmængden $\mathbb{N}$ stemmer overens med den allerede indførte relation "mindre end" i $\mathbb{N}$.

SÆTNING. Med denne relation er $(\mathbb{Z},+,\cdot,<)$ en ordnet ring, hvis positive elementer er de naturlige tal.
BEVIS. Delmængden $\mathbb{N}$ er stabil under $+$ og $\cdot$. Påstanden følger derfor af sætning 3.2 under brug af et generelt resultat om ordnede ringe □

3.8. Yderligere gælder følgende
ORDNINGSSÆTNING. Enhver ikke-tom nedad begrænset delmængde $P \subseteq \mathbb{Z}$ har et mindste element. Enhver ikke-tom opad begrænset delmængde $Q \subseteq \mathbb{Z}$ har et største element.

BEVIS. Lad tallet $r \in \mathbb{Z}$ være en minorant for P. Hvis $p \in P$, er $r \leq p$, og følgelig $p - r + 1 \in \mathbb{N}$. Ved

$$p \longmapsto p - r + 1$$

definerer derfor en ordenstro afbildning af P på en ikke-tom delmængde P' af $\mathbb{N}$. Da $\mathbb{N}$ er velordnet har P' et mindste element p_0', og så er $p_0 := p_0' + r - 1$ det mindste element i P.

Sætningens anden påstand følger af den første, idet q_0 er det største element i Q, hvis og kun hvis $-q_0$ er det mindste element i mængden

$$-Q := \{ -q \mid q \in Q \}$$ ▨

4. Oversigt over de grundlæggende egenskaber ved de hele tal.

4.1. BESKRIVELSE. Systemet af hele tal er en (additivt skrevet) kommutativ gruppe $(\mathbb{Z},+)$ (også betegnet $\mathbb{Z}^+$), der indeholder de naturlige tal $\mathbb{N}$ som en stabil delmængde. Det neutrale element i gruppen $(\mathbb{Z},+)$ kaldes nul og betegnes 0. Ethvert helt tal $p \in \mathbb{Z}$ kan skrives som en differens

$$p = a - s \quad (= a + (-s))$$

mellem naturlige tal $a, s \in \mathbb{N}$.

4.2. POTENSER. For et element a i en gruppe $(G,\cdot)$ med neutralt element e defineres potenser med hel eksponent $p \in \mathbb{Z}$

$$a^p \in G$$

som en udvidelse af potens med naturlig eksponent, og således at $a^0 = e$ og $a^{-n} = (a^n)^{-1}$.

Er gruppen additivt skrevet, bruges betegnelsen

$$pa \in G$$

for den p'te potens af a, $p \in \mathbb{Z}$.

4.3. FUNDAMENTALE STRUKTURER. Udover den givne addition i $\mathbb{Z}$ er multiplikation i $\mathbb{Z}$ kompositionen $(p,q) \mapsto p \cdot q$ defineret ved

$$p \cdot q := pq = p\text{'te potens af } q \text{ i gruppen } (\mathbb{Z},+),$$

og relationen "mindre end" i $\mathbb{Z}$, betegnet $<$, er defineret ved

$$p < q \overset{\text{DEF}}{\iff} q - p \in \mathbb{N}.$$

4.4. REGNEREGLERNE. Disse strukturer udvider de tilsvarende strukturer på delmængden $\mathbb{N}$, og $(\mathbb{Z},+,\cdot,<)$ er en kommutativ ordnet ring, med $1 \in \mathbb{N}$ som ét-element, hvis positive elementer er de naturlige tal: $\mathbb{N} = \mathbb{Z}_+$.

4.5. POTENSREGLERNE. For elementer a og b i en gruppe G og hele tal p og q gælder

1. potensregel: $a^{p+q} = a^p a^q$. $[(p+q)a = pa + qa]$

2. potensregel: $a^{pq} = (a^p)^q$ $[(pq)a = p(qa)]$

3. potensregel: $(ab)^p = a^p b^p$, når $ab = ba$. $[p(a+b) = pa + pb]$.

4.6. POTENSSÆTNINGEN. Lad der være givet en gruppe $(G,\cdot)$ og et element $a \in G$. Da findes netop en homomorfi: $(\mathbb{Z},+) \to (G,\cdot)$, som afbilder $1 \mapsto a$, nemlig afbildningen $p \mapsto a^p$.

4.7. ORDNINGSSÆTNING. Enhver ikke-tom, nedad begrænset delmængde $P \subseteq \mathbb{Z}$ har et mindste element. Enhver ikke-tom, opad begrænset delmængde $Q \subseteq \mathbb{Z}$ har et største element.

5. Yderligere egenskaber ved de hele tal.

5.1. SÆTNING OM DEN KANONISKE RINGHOMOMORFI. For enhver ring Λ findes netop én ringhomomorfi: $\mathbb{Z} \to \Lambda$, nemlig afbildningen

$$p \mapsto p1_\Lambda \quad (= p\text{'te potens af } 1_\Lambda \text{ i gruppen } (\Lambda,+)).$$

BEVIS. En ringhomomorfi skal afbilde $1 \mapsto 1_\Lambda$, og da den skal bevare addition, er den eneste mulighed afbildningen

$$p \mapsto p1_\Lambda,$$

der er en homomorfi: $(\mathbb{Z},+) \to (\Lambda,+)$, jfr. Potenssætningen. Det er derfor nok at vise, at denne afbildning også bevarer multiplikation, altså at

$$(pq)1_\Lambda = (p1_\Lambda)(q1_\Lambda).$$

Betragt hertil for et fast $q \in \mathbb{Z}$ de to sider som afbildningerne: $\mathbb{Z} \to \Lambda$ givet ved

$$p \mapsto (pq)1_\Lambda \qquad \text{og} \qquad p \mapsto (p1_\Lambda)(q1_\Lambda).$$

Da de begge er homomorfier: $(\mathbb{Z},+) \to (\Lambda,+)$ (hvorfor?), er det ifølge Potenssætningen nok at indse, at de stemmer overens for $p = 1$. Og det er klart ▨

5.2. EKSEMPEL. ENDOMORFIRING. Lad $(M,+)$ være en (additivt skrevet) kommutativ gruppe. Endomorfiringen for M, betegnet $\mathrm{End}(M)$, er da mængden af homomorfier $\varphi: (M,+) \to (M,+)$, organiseret ved sædvanlig addition [Summen $\varphi+\psi$ er altså afbildningen: $x \mapsto \varphi(x)+\psi(x)$] og sammensætning som multiplikation [Produktet $\varphi\circ\psi$ er altså afbildningen: $x \mapsto \varphi(\psi(x))$]. Hermed er $\mathrm{End}(M)$ en ring [nul-elementet er den konstante afbildning: $x \mapsto 0$, og ét-elementet er den identiske afbildning: $x \mapsto x$].

Det er let at se, at den kanoniske ringhomomorfi: $\mathbb{Z} \to \mathrm{End}(M)$ er givet ved

$$p \longmapsto [x \longmapsto px],$$

jfr. de fire Potensregler.

5.3. SÆTNING. I ringen $(\mathbb{Z},+,\cdot)$ gælder nul-reglen, og for hvert naturligt tal n er $\overbrace{1+\cdots+1}^{n} \neq 0$.

BEVIS. Dette gælder generelt for ordnede ringe ($\neq 0$), og indses således:

Nulreglen udsiger, at når $p \neq 0$ og $q \neq 0$ er hele tal, så er også $pq \neq 0$. Vi kan antage, at $0<p$ og $0<q$ (hvorfor?), altså at $p, q \in \mathbb{Z}_+ = \mathbb{N}$, men så er også $pq \in \mathbb{Z}_+$, altså specielt $pq \neq 0$.

Tilsvarende følger af $1 \in \mathbb{Z}_+ = \mathbb{N}$, at også $n1 = \overbrace{1+\cdots+1}^{n} \in \mathbb{Z}_+$, og specielt, at $n1 \neq 0$ ▨

5.4. DIVISIONSSÆTNINGEN. Lad $d \in \mathbb{N}$ være et givet naturligt tal. Til hvert tal $a \in \mathbb{Z}$ findes da entydigt bestemte tal $q, r \in \mathbb{Z}$ således at

$$a = qd + r \quad \text{og} \quad 0 \leq r < d.$$

BEVIS. Eksistens: Lad $P \subseteq \mathbb{Z}$ være delmængden

$$P := \{p \in \mathbb{Z} \mid pd \leq a\}.$$

Da er P ikke-tom (hvorfor?) og opad begrænset (hvorfor?), og P har derfor ifølge Ordningssætningen et største element $=: q$.

Nu er $a = qd + r$, med $r := a - qd$, og da $q \in P$, er $0 \leq r$.

Da $q+1 \notin P$, er $a < (q+1)d = qd + d$, og altså $r = a - qd < d$.

Entydighed: Det er nok, at betragte en fremstilling

$$0 = qd + r \quad , \quad 0 \leq r < d.$$

Af

$$0d = 0 \leq (-q)d < d = 1d$$

følger imidlertid

$$0 \leq -q < 1,$$

hvoraf $q = 0$ (og dermed også $r = 0$) ▨

DEFINITION. Det i sætningen nævnte tal r kaldes den <u>principale rest</u> af a ved division med $d \in \mathbb{N}$.

BEMÆRKNING. Forudsættes om d blot, at det er et helt tal

$\neq 0$, fås lit en fremstilling

$$a = qd + r, \quad \text{hvor} \quad 0 \leq r < |d|.$$

5.5. HOVEDIDEALSÆTNINGEN. For ethvert tal $d \in \mathbb{Z}$ er delmængden

$$\mathbb{Z}d := \{ qd \mid q \in \mathbb{Z} \}$$

en undergruppe i $(\mathbb{Z},+)$. Omvendt gælder, at enhver undergruppe H i $(\mathbb{Z},+)$ har formen

$$H = \mathbb{Z}d, \quad \text{hvor } d \geq 0,$$

og d er entydigt bestemt ved H, nemlig som

$d = 0$, når $H = \{0\}$

$d =$ mindste positive tal i H, når $H \neq \{0\}$.

BEVIS. Den første påstand ses enten direkte, eller ved at bemærke, at $\mathbb{Z}d$ er billedet ved den ved $q \mapsto qd$ bestemte homomorfi: $(\mathbb{Z},+) \to (\mathbb{Z},+)$.

Hvis den givne undergruppe er $H = \{0\}$, har vi $H = \mathbb{Z}0$.

Er $H \neq \{0\}$, findes et element $x \neq 0$ i H. Nu vil også $-x \in H$, og af de to tal x og $-x$ i H er det ene positivt. Da der således findes positive elementer i H, kan vi lade d betegne det mindste positive element i H. Det påstås, at

$$\mathbb{Z}d = H.$$

Her er "$\subseteq$" klart, thi da $d \in H$, og H er en undergruppe, vil også $\mathbb{Z}d = \{ qd \mid q \in \mathbb{Z} \} \subseteq H$.

Lad omvendt $a \in H$. I følge Divisionssætningen kan vi skrive

$$a = qd + r, \quad \text{hvor } 0 \leq r < d.$$

Nu er $r = a + (-q)d$, og da $a \in H$ og $(-q)d \in H$, vil også $r \in H$. Da $0 \leq r$, og $r < d =$ mindste positive tal i H, må vi have $r = 0$, og altså $a = qd \in \mathbb{Z}d$.

Endelig er det klart, at tallet $d \geq 0$ udfra delmængden $H = \mathbb{Z}d$ kan bestemmes på den i sætningen angivne måde ▨

5.6. DEFINITION. For hele tal $a, d \in \mathbb{Z}$ siger vi, at d er <u>divisor i</u> a (eller at a er et <u>multiplum af</u> d), hvis der findes et tal $q \in \mathbb{Z}$, så at

$$a = qd.$$

Relationen skrives også

$$d \mid a \qquad (\text{læses: } d \underline{\text{går op i}}\ a)$$

Ethvert tal $a \in \mathbb{Z}$ har de <u>trivielle divisorer</u> $1, -1, a$ og $-a$.

To tal $a, n \in \mathbb{Z}$ kaldes <u>primiske</u>, hvis de kun har 1 og -1 som fælles divisorer.

OBSERVATION. Der gælder

$$d \mid a \iff a \in \mathbb{Z}d \iff \mathbb{Z}a \subseteq \mathbb{Z}d.$$

De trivielle divisorer d i a svarer således til

$$\mathbb{Z}a \subseteq \mathbb{Z}d = \mathbb{Z} \quad \text{eller} \quad \mathbb{Z}a = \mathbb{Z}d \subseteq \mathbb{Z}.$$

BEMÆRKNING. Da tallene a og $-a$ har de samme divisorer, og da d er divisor i a, hvis og kun hvis $-d$ er divisor i a, er vi ofte kun interesserede i positive divisorer d i positive tal a. I denne situation følger af $a = qd$, at $q \geqslant 1$, og dernæst, at $1 \leqslant d \leqslant a$. Der er specielt kun endelig mange divisorer i et positivt tal a.

5.7. SÆTNING. For hele tal $a, n \in \mathbb{Z}$, hvor $n \neq 0$, er følgende betingelser ækvivalente:

(i) a er primisk med n.

(ii) Der findes tal $x, y \in \mathbb{Z}$, så at $1 = xa + yn$.

(iii) For alle tal $z \in \mathbb{Z}$ gælder $n \mid az \Rightarrow n \mid z$.

BEVIS. <u>(i) $\Rightarrow$ (ii)</u>: I $\mathbb{Z}$ er delmængden

$$H := \{ xa + yn \mid x, y \in \mathbb{Z} \}$$

klart en undergruppe, og derfor ifølge Hovedidealsætningen 5.5 af formen $H = \mathbb{Z}d$, med $d \geqslant 0$. Vi har $a \in H = \mathbb{Z}d$ og $n \in H = \mathbb{Z}d$, altså $d \mid a$ og $d \mid n$, hvoraf $d = 1$. Af $H = \mathbb{Z}1 = \mathbb{Z}$ følger $1 \in H$, og dét er netop påstanden.

(ii) ⇒ (iii): Vi har $1 = xa + yn$, $x, y \in \mathbb{Z}$. Hvis $n \mid az$, kan vi skrive $az = qn$, $q \in \mathbb{Z}$, og så er

$$z = (xa+yn)z = xaz + ynz = xqn + yzn = (xq+yz)n$$

et multiplum af n.

(iii) ⇒ (i): Er $d \in \mathbb{Z}$ divisor i både a og n, kan vi skrive

$$a = ud, \quad n = zd, \text{ med } u, z \in \mathbb{Z}.$$

Heraf fås

$$un = uzd = az,$$

så $n \mid az$, og dermed $n \mid z$. Vi kan derfor skrive

$$z = vn, \text{ med } v \in \mathbb{Z}.$$

Af

$$n = zd = nvd \quad \text{fås} \quad n(1 - vd) = 0.$$

Da Nul-reglen gælder i $\mathbb{Z}$, og da $n \neq 0$, fås $vd = 1$, men så er $d = \pm 1$. ▨

5.8. DEFINITION AF PRIMTAL. Et <u>primtal</u> er et helt tal $p > 1$, som kun har trivielle divisorer.

OBSERVATION. Er p et primtal, og er $a \in \mathbb{Z}$ gælder

$$a \text{ er primisk med } p \iff p \nmid a.$$

SÆTNING. Et primtal p, der går op i et produkt, vil gå op i en af faktorerne.

BEVIS. Påstanden kan skrives:

$$p \mid az \wedge p \nmid a \Rightarrow p \mid z,$$

og den følger derfor af Sætning 5.7. (iii) ▨

5.9. SÆTNING. Hvis tallene $a, b \in \mathbb{Z}$ begge er primiske med tallet $n \neq 0$, så er også produktet ab primisk med n.

BEVIS. Anvend f.eks. betingelsen (iii) i Sætning 5.7 to gange □

5.10. OBSERVATION. To primtal p og q er primiske, hvis og kun hvis de er forskellige.

KOROLLAR. Hvis tallene

$$a = p_1 \cdots p_r \quad \text{og} \quad n = q_1 \cdots q_s$$

er skrevet som produkter af primtal $p_1, \cdots, p_r, q_1, \cdots, q_s$, så er a og n primiske, hvis og kun hvis mængderne

$$\{p_1, \cdots, p_r\} \quad \text{og} \quad \{q_1, \cdots, q_s\}$$

er disjunkte.

BEVIS. "kun hvis": Et (prim-)tal, som ligger i begge de to mængder, er øjensynlig en ikke-triviel divisor i både a og n.

"hvis": Et fast q_i er forskelligt fra – og dermed primisk med – ethvert p_j, og derfor (Sætning 5.9) primisk med produktet $a = p_1 \cdots p_r$. Da a således er primisk med ethvert q_i, er a også primisk med produktet $n = q_1 \cdots q_s$ (igen Sætning 5.9) ▨

5.11. KOROLLAR. Hvis $n = n_1 \cdots n_r$ er et produkt af parvis primiske naturlige tal $n_1, \cdots, n_r$, så gælder for hele tal x:

$$n \mid x \iff n_1 \mid x \wedge \cdots \wedge n_r \mid x.$$

BEVIS. "$\Rightarrow$" er trivielt.

"$\Leftarrow$": Sættes $a = n_1 \cdots n_{r-1}$, kan vi induktivt antage, at $a \mid x$, og kan altså skrive $x = az$, $z \in \mathbb{Z}$. Da n_r er primisk med produktet $a = n_1 \cdots n_{r-1}$ (Sætning 5.9.), og da $n_r \mid x = az$, følger dit, at $n_r \mid z$. Og så er $an_r \mid az$, altså $n \mid x$. ▨

5.12. HOVEDSÆTNING OM PRIMTALSOPLØSNING. Ethvert tal $n > 1$ kan skrives som et produkt

$$n = p_1 \cdots p_r$$

af primtal $p_1, \cdots, p_r$, og denne fremstilling er entydig, bortset fra permutation af faktorerne.

BEVIS. Eksistens: Lad $n > 1$ være givet. Den mindste blandt divisorerne > 1 i tallet n er da et primtal. Kaldes dette primtal p_1, kan vi skrive

$$n = p_1 n_1, \quad \text{hvor altså} \quad 1 \leqslant n_1 < n.$$

Hvis $n_1 = 1$, er $n = p_1$ den ønskede fremstilling, og hvis $n_1 > 1$, kan vi tilsvarende skrive $n_1 = p_2 n_2$, hvor p_2 er et primtal, og altså

$$n = p_1 p_2 n_2 , \qquad 1 \leq n_2 < n_1 < n.$$

Det ses, at vi efter højst n skridt får den ønskede fremstilling

$$n = p_1 p_2 \cdots p_r n_r , \qquad 1 = n_r .$$

<u>Entydighed:</u> Det skal vises for primtal $p_1, \cdots, p_r, q_1, \cdots, q_s$, $r \leq s$, at hvis

$$p_1 \cdots p_r = q_1 \cdots q_s ,$$

så er $r = s$, og - eventuelt efter permutation af faktorerne - $q_i = p_i$, $i = 1, \cdots, r$. Dette vises ved induktion efter r. Hvis $r = 1$, ser vi af

$$p_1 = q_1 \cdots q_s ,$$

at $q_1 > 1$ er divisor i p_1, og da p_1 er et primtal, må vi have $q_1 = p_1$, og videre $s = 1$. Hvis $r > 1$, ser vi af Korollar 5.10, at mængderne $\{p_1, \cdots, p_r\}$ og $\{q_1, \cdots, q_s\}$ <u>ikke</u> er disjunkte. Efter en eventuel permutation kan vi antage, at et fælles element er primtallet $p_r = q_s$. Af

$$(p_1 \cdots p_{r-1}) p_r = (q_1 \cdots q_{s-1}) q_s$$

får vi

$$p_1 \cdots p_{r-1} = q_1 \cdots q_{s-1}$$

ifølge multiplikationsreglen, og induktionsantagelsen giver nu det ønskede. ▨

6. Appendix: Restklasser modulo n.

6.1. DEFINITION. Lad n være et naturligt tal. For hele tal $a, b \in \mathbb{Z}$ siger vi, at a er kongruent med b modulo n, og vi skriver

$$a \equiv b \pmod{n},$$

hvis n går op i $a-b$. Vi har altså

$$a \equiv b \pmod{n} \overset{\text{DEF}}{\iff} b - a \in \mathbb{Z}n.$$

Det er let at se, at denne relation i $\mathbb{Z}$ er en ækvivalensrelation. Ækvivalensklasserne kaldes restklasser modulo n. Restklassen, der indeholder et givet $a \in \mathbb{Z}$, er delmængden

$$\textcircled{a} = \{a + qn \mid q \in \mathbb{Z}\} =: a + \mathbb{Z}n.$$

Hvis tallet a tilhører en restklasse X, siges a også at være en repræsentant for X. Dette betyder, at $X = \textcircled{a}$.

Mængden af restklasser modulo n betegnes $\mathbb{Z}/\mathbb{Z}n$. Elementerne $X \in \mathbb{Z}/\mathbb{Z}n$ har altså formen

$$X = \textcircled{a},$$

hvor $a \in \mathbb{Z}$ er en repræsentant for X. Vi har

$$\textcircled{a} = \textcircled{b} \iff a \equiv b \pmod{n}.$$

Af Divisionssætningen 5.4 følger, at hver restklasse X entydigt kan skrives

$$X = \textcircled{r}, \quad 0 \leqslant r < n.$$

Mængden $\mathbb{Z}/\mathbb{Z}n$ består således af de n elementer

$$\textcircled{0}, \textcircled{1}, \textcircled{2}, \ldots, \textcircled{n-1}.$$

Specielt er

$$|\mathbb{Z}/\mathbb{Z}n| = n.$$

6.2. REGNING MED RESTKLASSER. Det er let at se, at den ovenfor definerede ækvivalensrelation harmonerer med kompositionerne + og · i $\mathbb{Z}$ i den forstand, at

$$(*)\quad x' \equiv x \ \wedge\ y' \equiv y \ \Rightarrow\ x'+y' \equiv x+y \ \wedge\ x'\cdot y' \equiv xy.$$

Vi kan derfor indføre kompositioner + og · i mængden $\mathbb{Z}/\mathbb{Z}n$ af restklasser på følgende måde: For givne restklasser X og Y vælges repræsentanter: $X = \textcircled{x}$, $Y = \textcircled{y}$. Summen $X+Y$ er da restklassen

$$X + Y := \textcircled{x+y}$$

og produktet XY er restklassen

$$XY := \textcircled{xy}.$$

Af (*) følger, at disse restklasser er veldefinerede, dvs ikke afhænger af de foretagne valg af repræsentanter.

Det er let at se, at mængden $\mathbb{Z}/\mathbb{Z}n$ af restklasser med disse to kompositioner er en kommutativ ring $(\mathbb{Z}/\mathbb{Z}n\ ,\ +\ ,\ \cdot\ )$. Den kaldes <u>restklasseringen modulo n</u> og betegnes også $\mathbb{Z}/n$ [eller evt. $\mathbb{Z}_n$]. Nul-elementet er restklassen $\textcircled{0}$ og et-elementet er restklassen $\textcircled{1}$.

Af definitionen fremgår umiddelbart, at $x \mapsto \textcircled{x}$ er en surjektiv ringhomomorfi: $\mathbb{Z} \to \mathbb{Z}/n$.

6.3. EKSEMPEL. For $n=6$ fås restklasseringen $\mathbb{Z}/6$ med de 6 elementer $\textcircled{0}, \textcircled{1}, \textcircled{2}, \textcircled{3}, \textcircled{4}, \textcircled{5}$. Idet vi udelader $\bigcirc$ i betegnelserne bliver kompositionstavlerne:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

.

6.4. SÆTNING. For hele tal $a, n \in \mathbb{Z}$, $n \geq 1$, er følgende betingelser ækvivalente:

(i) a er primisk med n.

(ii) Der findes tal $x, y \in \mathbb{Z}$, så at $1 = xa + yn$.

(iii) For alle tal $z \in \mathbb{Z}$ gælder: $n \mid az \Rightarrow n \mid z$.

(iv) Restklassen $\textcircled{a}$ er invertibel i ringen $\mathbb{Z}/n$.

(v) Restklassen $\textcircled{a}$ er regulær i $\mathbb{Z}/n$.

BEVIS. At betingelserne (i), (ii) og (iii) er ækvivalente er netop indholdt af Sætning 5.7. Det er derfor nok at vise, at (ii) $\Leftrightarrow$ (iv) og (iii) $\Leftrightarrow$ (v).

(ii) $\Rightarrow$ (iv): Af $1 = xa + yn$ følger $1 \equiv xa \pmod{n}$, og så er $\textcircled{1} = \textcircled{xa} = \textcircled{x}\textcircled{a}$. Følgelig er $\textcircled{a}$ invertibel (med $\textcircled{x}$ som invers).

(iv) $\Rightarrow$ (ii): Hvis $\textcircled{a}$ er invertibel, findes en restklasse X, så at $X\textcircled{a} = \textcircled{1}$. Er $x \in \mathbb{Z}$ en repræsentant for X, har vi altså $\textcircled{1} = X\textcircled{a} = \textcircled{x}\textcircled{a} = \textcircled{xa}$. Følgelig er $1 \equiv xa \pmod{n}$, så vi kan skrive $1 = xa + yn$, $y \in \mathbb{Z}$.

(iii) $\Rightarrow$ (v): Lad Z være en restklasse således at $\textcircled{a} \cdot Z = \textcircled{0}$. Vi skal vise, at $Z = \textcircled{0}$. Lad $z \in \mathbb{Z}$ være en repræsentant for Z. Da er $\textcircled{0} = \textcircled{a} \cdot Z = \textcircled{a}\textcircled{z} = \textcircled{az}$, og følgelig er $n \mid az$. Heraf sluttes $n \mid z$, altså $Z = \textcircled{z} = \textcircled{0}$.

(v) $\Rightarrow$ (iii): Hvis $n \mid az$, har vi $\textcircled{0} = \textcircled{az} = \textcircled{a}\textcircled{z}$. Da $\textcircled{a}$ er regulær, følger heraf $\textcircled{z} = \textcircled{0}$, altså $n \mid z$. ▨

De invertible elementer i $\mathbb{Z}/n$ er altså restklasser af formen $\textcircled{a}$, hvor a er primisk med n. De kaldes også <u>primiske</u> restklasser. Med multiplikation som komposition udgør de en kommutativ gruppe, nemlig gruppen $(\mathbb{Z}/n)^*$ af invertible elementer i ringen $\mathbb{Z}/n$.

6.5. SÆTNING. Lad p være et primtal. Da er rest-

klasseringen $\mathbb{Z}/p$ et legeme.

BEVIS. Vi skal vise, at alle elementer $\neq \overline{0}$ i $\mathbb{Z}/p$ er invertible. Disse elementer er de $p-1$ restklasser

$$\overline{1}, \dots, \overline{p-1},$$

og de er øjensynlig alle primiske med p, når p er et primtal. Påstanden følger nu af Sætning 6.4 ▨

NOTATION. Legemet $\mathbb{Z}/p$, hvor p er et primtal, betegnes også $\mathbb{F}_p$.

6.6. Er der givet r naturlige tal $n_1, \dots, n_r$ kan vi betragte restklasseringene $\mathbb{Z}/n_1, \dots, \mathbb{Z}/n_r$ og produktringen $\mathbb{Z}/n_1 \times \dots \times \mathbb{Z}/n_r$.

DEN KINESISKE RESTKLASSESÆTNING. Lad $n = n_1 \cdots n_r$ være et produkt af parvis primiske naturlige tal $n_1, \dots, n_r$. Den kanoniske ringhomomorfi : $\mathbb{Z} \to \mathbb{Z}/n_1 \times \dots \times \mathbb{Z}/n_r$ inducerer da en ringisomorfi :

$$\mathbb{Z}/n \xrightarrow{\approx} \mathbb{Z}/n_1 \times \dots \times \mathbb{Z}/n_r.$$

BEVIS. Lad $\Lambda = \mathbb{Z}/n_1 \times \dots \times \mathbb{Z}/n_r$ være produktringen. Idet vi med $\overline{a}_i$ betegner a's restklasse modulo n_i, er nulelementet og et-elementet i Λ givet ved

$$0_\Lambda = (\overline{0}_1, \dots, \overline{0}_r), \quad 1_\Lambda = (\overline{1}_1, \dots, \overline{1}_r),$$

og den kanoniske ringhomomorfi : $\mathbb{Z} \to \Lambda$ er bestemt ved

$$x \longmapsto x1_\Lambda = (\overline{x}_1, \dots, \overline{x}_r).$$

I følge Korollar 5.11 har vi

$$\begin{aligned} x1_\Lambda = 0_\Lambda &\iff \overline{x}_1 = \overline{0}_1 \wedge \dots \wedge \overline{x}_r = \overline{0}_r \\ &\iff n_1 \mid x \wedge \dots \wedge n_r \mid x \\ &\iff n \mid x \iff x \in \mathbb{Z}n. \end{aligned}$$

Kernen for den kanoniske ringhomomorfi er således

idealet $\mathbb{Z}n$. I følge Isomorfisætning for ringe inducerer der en injektiv ringhomomorfi:

$$\mathbb{Z}/n \longrightarrow \Lambda = \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r.$$

Da de to ringe har samme elementantal (nemlig $n = n_1 \cdots n_r$), må denne injektive afbildning være bijektiv. ▨

BEMÆRKNING. Surjektiviteten udsiger: Til givne hele tal $a_1, \ldots, a_r \in \mathbb{Z}$ findes et helt tal $x \in \mathbb{Z}$, så at

$$x \equiv a_1 \pmod{n_1} \wedge \cdots \wedge x \equiv a_r \pmod{n_r},$$

og injektiviteten udsiger, at et sådant tal x er entydigt bestemt "modulo n".

6.7. DEFINITION. For et naturligt tal n betegnes med $\varphi(n)$ antallet af naturlige tal $a \leqslant n$, der er primiske med n. De naturlige tal $\leqslant n$ svarer netop til de n elementer

$$①, ②, \cdots, (n-1), (n) = ⓪$$

Det følger, jfr. 6.4, at $\varphi(n)$ er antallet af primiske restklasser modulo n, altså at

$$\varphi(n) = |(\mathbb{Z}/n)^*|$$

er ordenen af gruppen $(\mathbb{Z}/n)^*$ af invertible elementer i ringen $\mathbb{Z}/n$.

Funktionen $n \mapsto \varphi(n)$ kaldes <u>Eulers φ-funktion</u>.

OBSERVATION. Man finder let: $\varphi(1) = 1$, og for et <u>primtal</u> p: $\varphi(p) = p - 1$, $\varphi(p^\nu) = p^\nu - p^{\nu-1} = p^\nu(1 - \frac{1}{p})$.

SÆTNING. Eulers φ-funktion er multiplikativ i den forstand, at hvis $n = n_1 \cdots n_r$ er et produkt af parvis primiske naturlige tal $n_1, \ldots, n_r$, så er

$$\varphi(n) = \varphi(n_1) \cdots \varphi(n_r).$$

BEVIS. Af ring-isomorfien

$$\mathbb{Z}/n \xrightarrow{\approx} \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_r$$

(jfr. Den kinesiske restklassesætning 6.5) får vi en gruppe-isomorfi

$$(\mathbb{Z}/n)^* \xrightarrow{\approx} (\mathbb{Z}/n_1)^* \times \cdots \times (\mathbb{Z}/n_r)^*.$$

Sammenligning af elementantallene giver nu det ønskede ▨

6.8. SÆTNING. Lad n være et naturligt tal. Hvis tallet $a \in \mathbb{Z}$ er primisk med n, så er

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

BEVIS. Restklassen $\overline{a}$ er et element i den multiplikative gruppe $(\mathbb{Z}/n)^*$. Da denne gruppe har orden $\varphi(n)$ har vi

$$\overline{1} = \overline{a}^{\varphi(n)} = \overline{a^{\varphi(n)}},$$

og det er netop påstanden ▨

Som specialtilfælde fås:

FERMAT'S "LILLE" SÆTNING. Lad p være et primtal. Hvis tallet $a \in \mathbb{Z}$ ikke er et multiplum af p, så er

$$a^{p-1} \equiv 1 \pmod{p}$$ ▨

6.9. WILSON'S SÆTNING. Lad p være et ulige primtal. Da er

$$(p-1)! \equiv -1 \pmod{p}.$$

BEVIS. Legemet $\mathbb{F}_p = \mathbb{Z}/p$ har p elementer, og den multiplikative gruppe $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ har derfor orden $p-1$. For hvert element $\alpha \neq 0$ i $\mathbb{F}_p$ har vi derfor $\alpha^{p-1} = \overline{1}$ (Nøjagtig som vi så i beviset for Fermats lille sætning). Det kan udtrykkes således: Polynomiet $X^{p-1} - \overline{1} \in \mathbb{F}_p[X]$ har i $\mathbb{F}_p$ rødderne α, $\alpha \in \mathbb{F}_p^*$, dvs de $p-1$ elementer $\overline{1}, \overline{2}, \cdots, \overline{p-1}$. Da polynomiet er normeret, og har grad $p-1$, har vi følgelig

$$X^{p-1} - \overline{1} = (X - \overline{1})(X - \overline{2}) \cdots (X - \overline{p-1}).$$

Sammenligning af koefficienterne giver en række ligninger. Specielt får vi for konstantleddene:

$$\overline{-1} = -\overline{1} = (-\overline{1})(-\overline{2}) \cdots (-\overline{p-1}) = (-1)^{p-1}\overline{(p-1)!}$$

For ulige p er det netop påstanden (og for $p=2$ er det uinteressant) ▨

6.10. SÆTNING. Lad p være et ulige primtal. Da vil halvdelen af de $p-1$ tal: $1, 2, \dots, p-1$ opfylde kongruensen

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

og den resterende halvdel vil opfylde kongruensen

$$x^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

BEVIS. Som vi har set (i beviset for Wilson's sætning 6.9), vil rødderne i polynomiet $X^{p-1} - \textcircled{1} \in \mathbb{F}_p[X]$ netop være elementerne $\textcircled{1}, \textcircled{2}, \dots, \textcircled{p-1}$. Da p er ulige, har vi

$$X^{p-1} - \textcircled{1} = \left(X^{\frac{p-1}{2}} - \textcircled{1}\right)\left(X^{\frac{p-1}{2}} + \textcircled{1}\right).$$

Hvert af de $p-1$ elementer er derfor rod i $X^{\frac{p-1}{2}} - \textcircled{1}$ eller i $X^{\frac{p-1}{2}} + \textcircled{1}$. De to polynomier har grad $\frac{p-1}{2}$ og kan derfor højst have $\frac{p-1}{2}$ rødder. Vi slutter derfor, at netop $\frac{p-1}{2}$ af elementerne er rod i $X^{\frac{p-1}{2}} - \textcircled{1}$, og at de øvrige $\frac{p-1}{2}$ elementer er rod i $X^{\frac{p-1}{2}} + \textcircled{1}$. Og dét er netop påstanden ▨

KOROLLAR. Lad p være et primtal, således at $p \equiv 1 \pmod{4}$. Da findes et tal $y \in \mathbb{Z}$, så at

$$y^2 \equiv -1 \pmod{p}.$$

BEVIS. Da $p \equiv 1 \pmod{4}$, kan vi skrive $p - 1 = 4h$, $h \in \mathbb{N}$. Vælg nu et tal x, så at $x^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. Sættes $y = x^h$ har vi følgelig

$$y^2 = x^{2h} = x^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

som ønsket ▨

BEMÆRK. Kongruensen $y^2 \equiv -1 \pmod{p}$ har højst 2 løsninger modulo p (hvorfor?). Man kan vise, at den ingen løsninger har, hvis $p \equiv 3 \pmod{4}$.

BRØKRING. DE RATIONALE TAL.

1. Bróker i en ring. Analyse. 1.1: Analyse. 1.2: Bemærkning. 1.3: Brøknotation.

2. Brøkringen. 2.1: Bróker. 2.2: Brøkregning. 2.3: Den kanoniske homomorfi. Sætning. 2.4: Observation. 2.5: Den totale brøkring. 2.6: Brøklegeme. 2.7: Division med nul. 2.8: Udvidelsessætning.

3. De rationale tal. 3.1: Definition. 3.2: Ordning. 3.3: Fælles nævner. 3.4: Udvidelsessætning. Indlejring af $\mathbb{Q}$ i legemer. 3.5: Potens med rational eksponent. 3.6-7: Potensreglerne. 3.8: Potenssætningen.

BRØKRING

DE RATIONALE TAL

1. Bróker i en ring. Analyse.

1.1. ANALYSE. Lad der være givet en kommutativ ring R og i R en multiplikativ delmængde S, d.v.s. en delmængde $S \subseteq R$, som er stabil over for multiplikation og indeholder et-elementet 1. Vi ónsker at indlægge R i en (større) ring A, hvori elementerne fra S er invertible, f.eks. for at betragte ligninger af formen

$$x s = a, \qquad s \in S,\ a \in R,$$

der jo i den større ring A har lósningen $x = a s^{-1}$.

Lad os antage, at problemet er lóst i den forstand at der er givet en indlejring $R \hookrightarrow A$, d.v.s. en injektiv ringhomomorfi

$$\varphi : R \to A,$$

således at elementerne $\varphi(s)$, $s \in S$, er invertible i A. Vi udleder en række konsekvenser:

(0) Selv om ringen A ikke forudsættes kommutativ, gælder for elementer $a \in R$, $s \in S$, at

$$\varphi(a)\varphi(s) = \varphi(s)\varphi(a)$$

(idet begge er $= \varphi(as) = \varphi(sa)$, R var jo kommutativ), og at

$$\varphi(s)^{-1}\varphi(a) = \varphi(a)\varphi(s)^{-1}$$

(multiplicér med $\varphi(s)^{-1}$ først fra venstre, dernest fra højre).

(1) Betragtes i A delmængden

$$R_\varphi S^{-1} := \{ \varphi(a)\varphi(s)^{-1} \mid a \in R \wedge s \in S \},$$

gælder, at $R_\varphi S^{-1}$ er en delring, thi

$$\varphi(a)\varphi(s)^{-1} + \varphi(b)\varphi(t)^{-1} = \varphi(a)\varphi(t)\varphi(t)^{-1}\varphi(s)^{-1} + \varphi(b)\varphi(s)\varphi(s)^{-1}\varphi(t)^{-1}$$
$$= \varphi(at)\,\varphi(st)^{-1} + \varphi(bs)\,\varphi(st)^{-1}$$
$$= [\varphi(at)+\varphi(bs)]\,\varphi(st)^{-1}$$
$$= \varphi(at+bs)\,\varphi(st)^{-1};$$

$$\varphi(a)\varphi(s)^{-1}\cdot\varphi(b)\varphi(t)^{-1} = \varphi(a)\varphi(b)\varphi(s)^{-1}\varphi(t)^{-1}$$
$$= \varphi(ab)\,\varphi(st)^{-1}$$

og

$$-1_A = -\varphi(1) = \varphi(-1)\,\varphi(1)^{-1}$$

(2) Delringen $\underline{R_\varphi S^{-1}}$ indeholder billedringen $\varphi(R)$, thi

$$\varphi(a) = \varphi(a)\,\varphi(1)^{-1}.$$

Vi kan derfor betragte indlejringen som en indlejring

$$R \hookrightarrow R_\varphi S^{-1},$$

og elementerne $\varphi(s)$, $s \in S$, er også invertible i $R_\varphi S^{-1}$, idet

$$\varphi(s)^{-1} = \varphi(1)\,\varphi(s)^{-1}.$$

(3) Endelig gælder, at den herved fundne indlejring: $R \hookrightarrow R_\varphi S^{-1}$ kun afhænger af R og S (og ikke af den givne indlejring $\varphi: R \hookrightarrow A$). Indføres nemlig i produktmængden $R\times S$ kompositionerne $+$ og $\cdot$ givet ved

$$(a,s) + (b,t) := (at+bs,\ st)$$
$$(a,s)\cdot(b,t) := (ab,\ st),$$

og betragtes afbildningen $\phi: R\times S \to A$ defineret ved

$$\phi(a,s) = \varphi(a)\,\varphi(s)^{-1},$$

følger det af (1), at ϕ er en homomorfi

$$\phi: (R\times S, +, \cdot) \longrightarrow (A, +, \cdot).$$

Billedet ved ϕ er øjensynlig netop delringen $R_\varphi S^{-1}$, så ifølge isomorfisætningen inducerer en isomorfi:

$$(R\times S, +, \cdot)/\tilde{\phi} \xrightarrow{\ \approx\ } (R_\varphi S^{-1}, +, \cdot)$$

hvor $\tilde{\phi}$ er den til ϕ hørende kongruensrelation.

Og denne relation afhænger ikke af φ, thi vi har

$$(a,s) \mathrel{\tilde{\Phi}} (a',s') \overset{\text{DEF}}{\Leftrightarrow} \Phi(a,s) = \Phi(a',s')$$
$$\Leftrightarrow \varphi(a)\varphi(s)^{-1} = \varphi(a')\varphi(s')^{-1}$$
$$\Leftrightarrow \varphi(a)\varphi(s') = \varphi(a')\varphi(s)$$
$$\Leftrightarrow \varphi(as') = \varphi(a's)$$
$$\Leftrightarrow as' = a's,$$

da φ var injektiv.

1.2. BEMÆRKNING. Hvis den givne ring R overhovedet kan indlejres i en større ring A, hvori elementerne fra S er invertible, viser den foregående analyse, hvordan vi kan <u>konstruere</u> en sådan indlejring: Vi skal betragte produktmængden $R \times S$ med kompositionerne $+$ og $\cdot$ defineret i 1.1 (3), og heri kongruensrelationen $\sim$ fundet i 1.1 (3). Kvotienten $(R \times S, +, \cdot)/\sim$ er da den søgte ring. Problemet er imidlertid, at den i 1.1 (3) angivne relation

$$(a,s) \sim (a',s') \Leftrightarrow as' = a's$$

i $R \times S$ i almindelighed ikke er en ækvivalensrelation. Det er jo også på forhånd klart, at vi ikke for enhver multiplikativ delmængde $S \subseteq R$ kan indlægge R i en større ring A, hvori elementerne fra S er invertible, idet en nødvendig betingelse herfor er, at elementerne fra S er regulære.

1.3. BRØKNOTATION. Hvis den givne ring R er delring af en ring A, hvori elementerne i S er invertible, skrives ofte

$$\frac{a}{s} := as^{-1} = s^{-1}a, \quad a \in R, \ s \in S.$$

Sådanne elementer kaldes <u>bróker</u>.

2. Brókringen

2.1. BRØKER. Lad R være en kommutativ ring, lad $S \subseteq R$ være en multiplikativ delmængde, og betragt produktmængden $R \times S$ af par (a,s), $a \in R$, $s \in S$.

Et par af formen (au, su) siges at fremgå af (a,s) ved at <u>forlænge med u</u>.

I $R \times S$ defineres kompositioner $+$ og $\cdot$ ved

$$(a,s) + (b,t) := (at + bs, st)$$

$$(a,s) \cdot (b,t) := (ab, st)$$

og en relation $\equiv$ (kaldet "kongruens") ved

$$(a,s) \equiv (a',s') \overset{\text{DEF}}{\iff} \exists u,u' \in S : (au, su) = (a'u', s'u').$$

To par er således kongruente, hvis de kan forlænges til samme par. Det er let at se, at

$$(a,s) \equiv (a',s') \iff \exists t \in S : tas' = ta's.$$

Videre gælder følgende

LEMMA. Kompositionen $+$ i $R \times S$ er kommutativ, associativ, og har $(0,1)$ som neutralt element. Kompositionen $\cdot$ i $R \times S$ er kommutativ, associativ, og har $(1,1)$ som neutralt element. Relationen $\equiv$ er en kongruensrelation i $(R \times S, +, \cdot)$.

BEVIS. Der er meget at eftervise, men det er let $\square$

DEFINITION. En <u>brók</u> (med tæller fra R og nævner fra S) er en ækvivalensklasse i $R \times S$. Ækvivalensklassen, der indeholder et givet par $(a,s) \in R \times S$ <u>betegnes</u> a/s, og kaldes bróken med <u>tæller a og nævner s</u>. Enhver brók X kan skrives på formen $X = a/s$, med en passende <u>repræsentant</u> $(a,s) \in R \times S$.

Bemærk, at $au/su = a/s$, da $(au, su) \equiv (a,s)$.

2.2. BRØKREGNING. Ifølge Lemma 2.1 kan vi i mængden af bróker, d.v.s. i kvotientten $R \times S / \equiv$, definere kompositioner ved regning med repræsentanter: Har bróken X repræsentanten (a,s) og bróken Y repræsentanten (b,t), defineres <u>summen</u> $X+Y$ som bróken, der indeholder

summen

$$(a,s)+(b,t) = (at+bs, st)$$

af repræsentanterne, og <u>produktet</u> $X\cdot Y$ som brøken, der indeholder produktet

$$(a,s)\cdot(b,t) = (ab, st)$$

af repræsentanterne. Vi har altså

$$a/s + b/t = (at+bs)/st$$

$$a/s \cdot b/t = ab/st.$$

SÆTNING. Med disse kompositioner er mængden af brøker, altså kvotienten $(R\times S,+,\cdot)/\equiv$, en kommutativ ring med nul-elementet $0/1$ og ét-elementet $1/1$.

BEVIS. De i Lemma 2.1 anførte egenskaber ved kompositionerne $+$ og $\cdot$ i $R\times S$ nedarves umiddelbart til kvotienten $R\times S/\equiv$. Det er derfor nok at vise, at hver brøk X har en modsat m.h.t. $+$, og at $\cdot$ er distributiv m.h.t. $+$. Vælges en repræsentant (a,s) for X finder vi

$$X + {}^{-a}/_{s} = a/s + {}^{-a}/_{s} = 0/s^2 = 0\cdot s^2/1\cdot s^2 = 0/1$$

hvoraf følger, at brøken ${}^{-a}/_{s}$ er modsat til $X = a/s$.

For at vise den distributive lov betragtes brøker $X = a/s$, $Y = b/t$ og $Z = c/u$. Vi finder

$$\begin{aligned} XZ + YZ &= a/s\cdot c/u + b/t\cdot c/u = ac/su + bc/tu \\ &= (actu + bcsu)/sutu \\ &= (act + bcs)u\ /\ sutu = (at+bs)c/stu \\ &= at+bs/st\ \cdot\ c/u = [a/s + b/t\,]\cdot c/u \\ &= (X+Y)\cdot Z \qquad \blacksquare \end{aligned}$$

DEFINITION. Den ovenfor konstruerede ring $(R\times S,+,\cdot)/\equiv$ kaldes den til $S\subseteq R$ hørende <u>brøkring</u>, og den betegnes $R[S^{-1}]$. Den siges at fremgå af R ved at <u>"invertere"</u> elementerne i S.

2.3. DEN KANONISKE HOMOMORFI. Det er klart, at den ved

$$a \longmapsto a/1$$

bestemte afbildning er en ringhomomorfi:

$$R \longrightarrow R[S^{-1}].$$

Den kaldes <u>den kanoniske homomorfi</u> af ringen R ind i brókringen $R[S^{-1}]$.

SÆTNING. Den kanoniske homomorfi $: R \to R[S^{-1}]$ er injektiv, hvis og kun hvis elementerne i S er regulære. I bekræftende fald er kongruensrelationen $\equiv$ bestemt ved

$$(a,s) \equiv (a',s') \iff as' = a's.$$

BEVIS. <u>"hvis"</u>: Er $a/1 = b/1$, så er parrene $(a,1)$ og $(b,1)$ kongruente, og der findes derfor et $u \in S$, så at $ua1 = ub1$. Da u er regulær, følger heraf $a = b$.

<u>"kun hvis"</u>: Er $sa = 0$, så er $a/1 = sa/s = 0/s = 0/1$, og følgelig er $a = 0$.

<u>"$\Leftarrow$"</u>: Gælder uden forudsætning om S.

<u>"$\Rightarrow$"</u>: Er $(a,s) \equiv (a',s')$, så findes $u \in S$, så at $uas' = ua's$. Da u er regulær, følger heraf $as' = a's$. ▨

2.4. OBSERVATION. Ved den kanoniske homomorfi $: R \to R[S^{-1}]$ afbildes elementer i S over i invertible elementer i $R[S^{-1}]$, thi når $s \in S$, så er $1/s$ en brók, og den er klart invers til $s/1$.

Det følger således, at R kan indlyses i en ring A, hvori elementerne i S er invertible, netop når elementerne i S er regulære.

2.5. DEN TOTALE BRØKRING. Af særlig interesse er tilfældet hvor vi i en given kommutativ ring R inverterer alle regulære elementer, d.v.s. som S bruger mængden R^{reg} af regulære elementer i R. Den herved fremkomne brókring $R[(R^{reg})^{-1}]$ kaldes også den <u>totale brókring</u> for R.

Af Sætning 2.3 følger, at enhver ring R kan opfattes som en delring af sin totale brøkring.

2.6. BRØKLEGEME. For et kommutativt integritetsområde R har vi $R^{reg} = R \setminus \{0\}$. Den totale brøkring

$$R\left[\,(R\setminus\{0\})^{-1}\,\right]$$

fås altså ved at invertere alle elementer $\neq 0$ i R.

SÆTNING. Lad R være et kommutativt integritetsområde. Da er den totale brøkring $R[(R\setminus\{0\})^{-1}]$ et legeme.

BEVIS. Lad X være en brøk forskellig fra nul-elementet $0/1$, og skriv $X = a/s$. Da er specielt $a \neq 0$, altså $a \in R\setminus\{0\}$, så vi kan betragte brøken s/a. Vi har

$$X \cdot s/a = a/s \cdot s/a = as/as = 1/1,$$

hvoraf følger, at X er invertibel (med $X^{-1} = s/a$) ▨

DEFINITION. Dette legeme kaldes integritetsområdets <u>brøklegeme</u>.

Det følger, at et kommutativt integritetsområde R kan opfattes som en delring af sit brøklegeme. Opfattet således kan enhver brøk X skrives

$$X = a/s = \frac{a}{s} = a s^{-1}, \quad a \in R,\ s \in R\setminus\{0\}.$$

2.7. DIVISION MED NUL. I almindelighed forudsættes ikke, at ringens nul-element ikke tilhører S. Hvis $0 \in S$, er konstruktionen af brøkringen imidlertid ikke særlig interessant, idet vi har følgende:

OBSERVATION. Brøkringen $R[S^{-1}]$ er nulringen, hvis og kun hvis $0 \in S$,

thi nul-ringen er som bekendt karakteriseret ved at dens nul-element også er ét-element, og vi har

$$0/1 = 1/1 \iff \exists s \in S : s\cdot 0\cdot 1 = s\cdot 1\cdot 1 \iff 0 \in S.$$

2.8. I almindelighed gælder for den kanoniske homomorfi: $R \to R[S^{-1}]$ følgende:

UDVIDELSESSÆTNING. Enhver ringhomomorfi $\varphi: R \to A$, der afbilder elementer i S over i invertible elementer i A, kan entydigt udvides til en ringhomomorfi $\bar{\varphi} : R[S^{-1}] \to A$ fra brókringen.

$$\begin{array}{ccc} R & \longrightarrow & R[S^{-1}] \\ {\scriptstyle\varphi}\downarrow & \swarrow & \\ A & & \end{array} \qquad \bar{\varphi}$$

BEVIS. "Entydighed": Enhver brók X kan skrives

$$X = a/s \,, \quad a \in R, \; s \in S,$$

og så er $X \cdot s/1 = a/s \cdot s/1 = as/s = a/1$.
Hvis homomorfien $\bar{\varphi} : R[S^{-1}] \to A$ er en udvidelse af $\varphi : R \to A$, får vi $\varphi(a) = \bar{\varphi}(a/1) = \bar{\varphi}(X \cdot s/1) = \bar{\varphi}(X)\,\bar{\varphi}(s/1) = \bar{\varphi}(X)\,\varphi(s)$, hvoraf

$$\bar{\varphi}(X) = \varphi(a)\,\varphi(s)^{-1}.$$

Heraf følger entydigheden af $\bar{\varphi}$.
"Eksistens": Overvej, at afbildningen $R \times S \to A$ defineret ved

$$(a, s) \longmapsto \varphi(a)\,\varphi(s)^{-1}$$

er en homomorfi: $(R \times S, +, \cdot) \longrightarrow (A, +, \cdot)$, og at den respekterer kongruensrelationen $\equiv$. Overvej, at den inducerede homomorfi: $(R \times S, +, \cdot)/\equiv \;\to A$ fra kvotienten opfylder de stillede krav. □

3. De rationale tal.

3.1. DEFINITION. Brøklegemet $\mathbb{Z}[(\mathbb{Z}\setminus\{0\})^{-1}]$ dannet ud fra det kommutative integritetsområde $\mathbb{Z}$ kaldes <u>de rationale tals legeme</u> og betegnes $\mathbb{Q}$. Elementerne i $\mathbb{Q}$ kaldes <u>rationale tal</u>. Da elementerne i $\mathbb{Z}\setminus\{0\}$ er regulære, er den kanoniske homomorfi: $(\mathbb{Z},+,\cdot) \to (\mathbb{Q},+,\cdot)$ injektiv. Vi vil (næsten) altid identificere elementerne i $\mathbb{Z}$ med deres billeder i $\mathbb{Q}$ ved denne afbildning, og altså opfatte $\mathbb{Z}$ som en delring af $\mathbb{Q}$. Den kanoniske homomorfi er da inklusionsafbildningen:

$$\mathbb{Z} \hookrightarrow \mathbb{Q}.$$

Et rationalt tal er altså en brøk. Med den indførte identifikation kan hvert rationalt tal $\in \mathbb{Q}$ skrives

$$x = a/s = \frac{a}{s} = a\cdot s^{-1}, \quad a \in \mathbb{Z},\ s \in \mathbb{Z}\setminus\{0\}$$

som en kvotient mellem hele tal $a, s \in \mathbb{Z}$, $s \neq 0$.

3.2. ORDNING. I mængden $\mathbb{Q}$ defineres en relation kaldet <u>"mindre end"</u> og betegnet $<$ ved

$$x < y \overset{\text{DEF}}{\iff} y - x \in \{ m/n \mid m, n \in \mathbb{N} \}.$$

SÆTNING. Med denne relation er $(\mathbb{Q},+,\cdot,<)$ et ordnet legeme, hvis positive elementer er elementerne i

$$\mathbb{Q}_+ = \{ m/n \mid m, n \in \mathbb{N} \}.$$

BEVIS. Lad $P \subseteq \mathbb{Q}$ betegne delmængden

$$P = \{ m/n \mid m, n \in \mathbb{N} \}.$$

Det er klart, at delmængden P er stabil under $+$ og $\cdot$. Endvidere ses det lit, at $0 \notin P$. I følge de generelle resultater om ordnede ringe, er det derfor nok at

vise, at der for hvert rationalt tal $\lambda \neq 0$ gælder $\lambda \in P$ eller $-\lambda \in P$. Hertil skrives $\lambda = a/s$, $a, s \in \mathbb{Z}$, $s \neq 0$. Da $a/s = (-1)a/(-1)s = -a/-s$, kan vi endda antage, at

$$\lambda = p/n \quad , \quad p \in \mathbb{Z}, \; n \in \mathbb{N}.$$

Da $\lambda \neq 0$, er specielt $p \neq 0$, men så er enten $p \in \mathbb{N}$, dvs. $\lambda \in P$, eller $-p \in \mathbb{N}$, dvs. $-\lambda = -p/n \in P$ ▨

BEMÆRKNING. Det er klart, at denne relation på delmængden $\mathbb{Z}$ stemmer overens med den allerede indførte relation "mindre end" i $\mathbb{Z}$.

3.3. FÆLLES NÆVNER. Da $a/s = -a/-s$ følger det, at hvert rationalt tal λ kan skrives

$$\lambda = p/n \quad , \quad p \in \mathbb{Z}, \; n \in \mathbb{N},$$

altså med positiv nævner. Endvidere kan endelig mange rationale tal $\lambda_1, \cdots, \lambda_k \in \mathbb{Q}$ altid skrives på formen $\lambda_1 = p_1/n, \cdots, \lambda_k = p_k/n$, $p_1, \cdots, p_k \in \mathbb{Z}$, $n \in \mathbb{N}$, altså med en fælles, positiv nævner, thi er $\lambda_i = q_i/n_i$, $q_i \in \mathbb{Z}$, $n_i \in \mathbb{N}$, kan vi som fælles nævner bruge $n = n_1 \cdots n_k$.

For rationale tal p/n, q/n, $p, q \in \mathbb{Z}$, $n \in \mathbb{N}$, med samme positive nævner, har vi øjensynlig

$$\frac{p}{n} + \frac{q}{n} = \frac{p+q}{n}, \quad \frac{p}{n} - \frac{q}{n} = \frac{p-q}{n}, \quad \frac{p}{n} < \frac{q}{n} \Leftrightarrow p < q.$$

3.4. UDVIDELSESSÆTNINGEN. Den generelle udvidelsessætning 2.2 for brøkringe omhandler her ringhomomorfier $\varphi : \mathbb{Z} \to A$, som afbilder elementer i $\mathbb{Z} \setminus \{0\}$ over i invertible elementer i A. Vi bemærker først, at det hertil er nok, at ringhomomorfien $\varphi : \mathbb{Z} \to A$ afbilder elementer i $\mathbb{N}$ over i invertible elementer i A, thi når $\varphi(n)$, $n \in \mathbb{N}$, er invertibel i

A, så er også $\varphi(-n) = -\varphi(n)$ invertibel i A (med den inverse $\varphi(-n)^{-1} = -\varphi(n)^{-1}$). Videre minder vi om, at der for enhver ring A findes netop én ringhomomorfi: $\mathbb{Z} \to A$, nemlig afbildningen

$$p \longmapsto p\,1_A .$$

Udvidelsessætningen udsiger derfor:

Lad A være en ring, hvori elementerne

$$n\,1_A = \overbrace{1_A + \cdots + 1_A}^{n} \quad , \quad n \in \mathbb{N},$$

er invertible. Da findes netop én ringhomomorfi: $\mathbb{Q} \to A$.

OBSERVATION. En ringhomomorfi $\varphi: \mathbb{Q} \to A$, hvor A ikke er nul-ringen, er injektiv,

thi hvis ringhomomorfien $\varphi: \mathbb{Q} \to A$ ikke er injektiv, findes et rationalt tal $\lambda \neq 0$, så at $\varphi(\lambda) = \varphi(0) = 0_A$, og så er $1_A = \varphi(1) = \varphi(\lambda^{-1}\cdot\lambda) = \varphi(\lambda^{-1})\varphi(\lambda) = \varphi(\lambda^{-1})\cdot 0_A = 0_A$, og A er følgelig nul-ringen.

KOROLLAR. Lad L være et legeme, hvori elementerne

$$n\,1_L = \overbrace{1_L + \cdots + 1_L}^{n} \quad , \quad n \in \mathbb{N},$$

er $\neq 0$. Da findes netop én ringhomomorfi : $\mathbb{Q} \to L$, og den er injektiv □

3.5. POTENSER. En (additivt skrevet) kommutativ gruppe $(M,+)$ kaldes entydigt delelig, hvis der for hvert $a \in M$ og hvert $n \in \mathbb{N}$ gælder, at ligningen

$$nx = a$$

har en og kun én løsning $x \in M$.

For hvert $n \in \mathbb{N}$ er afbildningen

$$\pi_n : x \longmapsto nx$$

en endomorfi : $(M,+) \to (M,+)$, og kan altså opfattes som element i endomorfiringen $\mathrm{End}(M)$, jfr. "Hele Tal", Eksempel 5.2. Videre er $\pi_n \in \mathrm{End}(M)$ netop billedet af $n \in \mathbb{N}$ ved den kanoniske ringhomomorfi

$$\pi : \mathbb{Z} \to \mathrm{End}(M).$$

Betingelsen udsiger, at afbildningerne π_n, $n \in \mathbb{N}$, er bijektive, dvs. invertible elementer i ringen $End(M)$. Er betingelsen opfyldt følger derfor af Udvidelsessætning 3.4, at der findes netop én ringhomomorfi: $\mathbb{Q} \to End(M)$.

DEFINITION. Lad $(M,+)$ være en entydigt delelig, kommutativ gruppe. Ringhomomorfien $\mathbb{Q} \to End(M)$ betegnes $\lambda \mapsto \pi_\lambda$, og for hvert $\lambda \in \mathbb{Q}$ betegnes endomorfien π_λ også $\pi_\lambda : x \mapsto \lambda x$. Billedet $\lambda x = \pi_\lambda(x)$ af et element $x \in M$ kaldes den λ'te potens af x.

3.6. POTENSREGLERNE. Lad $(M,+)$ være en entydigt delelig, kommutativ gruppe. For elementer $x, y \in M$ og rationale tal λ, μ gælder:

1. regel: $(\lambda+\mu)x = \lambda x + \mu x$
2. regel: $(\lambda\mu)x = \lambda(\mu x)$
3. regel $\lambda(x+y) = \lambda x + \lambda y$.

BEVIS. 3. regel udsiger, at afbildningen $\pi_\lambda : x \mapsto \lambda x$ er en endomorfi, altså at $\pi_\lambda \in End(M)$, og 1. og 2. regel udsiger, at afbildningen $\lambda \mapsto \pi_\lambda$ er additiv og multiplikativ: $\mathbb{Q} \to End(M)$ ▨

3.7. BEMÆRKNING. En multiplikativt skrevet, kommutativ gruppe $(M,\cdot)$ er entydigt delelig, hvis der for hvert $a \in M$ og hvert $n \in \mathbb{N}$ gælder, at ligningen

$$x^n = a$$

har en og kun en løsning $x \in M$.

For en sådan betegner vi naturligvis med x^λ den λ'te potens af $x \in M$, og potensreglerne er

$$x^{\lambda+\mu} = x^\lambda x^\mu, \quad x^{\lambda\mu} = (x^\lambda)^\mu, \quad (xy)^\lambda = x^\lambda y^\lambda.$$

3.8. OBSERVATION. For et element x i en entydigt delelig, kommutativ gruppe $(M,+)$ og et rationalt tal p/n, $p \in \mathbb{Z}$, $n \in \mathbb{N}$, er potensen $y = (p/n)\,x$ bestemt som den entydige løsning til ligningen

$$n\,y = p\,x,$$

thi $n\,(p/n\;x) = (n\,p/n)\,x = p\,x$.

POTENSSÆTNING. Lad x være et element i en entydigt delelig, kommutativ gruppe $(M,+)$. Der findes netop én homomorfi : $(\mathbb{Q},+) \longrightarrow (M,+)$, så at $1 \mapsto x$, nemlig afbildningen $\lambda \mapsto \lambda x$.

BEVIS. 1.ste potensregel (i forbindelse med $1x = x$) udsiger, at afbildningen $\lambda \mapsto \lambda x$ opfylder det stillede krav. Er omvendt $\varphi : \mathbb{Q} \to M$ en afbildning, der opfylder det stillede krav, følger det af Potenssætningen for hel eksponent, "Hele Tal" 3.4 (eller 4.6), at vi har

$$\varphi(p) = p\,x\;,\quad p \in \mathbb{Z}.$$

For en brøk p/n, $p \in \mathbb{Z}$, $n \in \mathbb{N}$ har vi derfor

$$n\,\varphi(p/n) = \varphi(n\,p/n) = \varphi(p) = p\,x,$$

hvoraf $\varphi(p/n) = (p/n)\,x$ ▨

FØLGER. ORDNING, FULDSTÆNDIGHED, KONTINUITET. DE REELLE TAL.

1. Fundamentalfølger. Fuldstændighed. 1.1: Definitioner. 1.2: Diskret og tæt ordning. 1.3: Egenskaben (K). 1.4: Sætninger. 1.5: Undergrupperne $BF(G)$, $FF(G)$, $KF(G)$, $NF(G)$ i gruppen $F(G)$. 1.6: Følge fuldstændig gruppe.

2. Følgekompletion. 2.1-2: Ækvivalens af følger. 2.3: Sætning om fundamentalfølger. 2.4-5: Notation. 2.6: Ordning i $\hat{G}$. 2.7: Kompletionen $(\hat{G},+,<)$. 2.8. Observation. 2.9: Sætning. 2.10: Fundamentalfølger i G er konvergente i $\hat{G}$. 2.11: $\hat{G}$ er fuldstændig.

3. Kontinuitet. 3.1: Kontinuert afbildning. 3.2: Sætning. 3.3: Kontinuerte homomorfier. 3.4: Udvidelsessætning for uniformt kontinuerte afbildninger. 3.5: Udvidelsessætning for kontinuerte homomorfier. 3.6: Udvidelsessætning for kontinuerte, ordenstro homomorfier.

4. Multiplikation. 4.1: Kontinuert multiplikation. 4.2: Ordnet legeme. 4.3-5: Kompletion af ordnet ring. 4.6: Kompletion af ordnet legeme. 4.7: Definition af reelle tal.

4*. Kompletion af ordnet legeme. 4*.1: Udvidelse af multiplikationen. 4*.2: Følgekompletion af ordnet legeme. Spec. $(\mathbb{R},+,\cdot,<)$.

5. Supremum og infimum. 5.1: Definitioner. 5.2: Snit. 5.3: Snitfuldstændighed.

6. Supremum og infimum i en ordnet gruppe. 6.1: Arkimedisk ordning. 6.2: Ækvivalente betingelser for fuldstændighed. 6.3: Diskret ordnede grupper. 6.4: Gruppen $(\mathbb{R}_+,\cdot,<)$. 6.5-8: Sætninger om arkimedisk ordnede grupper. 6.9: p-te rødder af positive reelle tal.

7. De reelle tal. 7.1: De reelle tal. 7.2: Hovedsætning. 7.3: Potenssætning. 7.4: Indlejringer i $(\mathbb{R},+,<)$. 7.5: Logaritme. 7.6: Sætning.

FØLGER.

ORDNING, FULDSTÆNDIGHED, KONTINUITET

DE REELLE TAL.

1. Fundamentalfølge. Fuldstændighed.

DEFINITIONER.

1.1 I det følgende betragter vi en kommutativ, ordnet gruppe G. Vi vil sædvanligvis skrive kompositionen additivt, og undertiden for G skrive $(G,+,<)$.

Ved en <u>følge i G</u> forstås som bekendt en afbildning $\alpha : \mathbb{N} \to G$. Følgen betegnes ofte $n \mapsto \alpha_n$ eller $(\alpha_1, \alpha_2, \dots)$ eller blot (α_n). Speciel følge er de <u>konstante</u> følger $(a, a, \dots)$, hvor a er et element i G. Ved en <u>delfølge</u> af følgen $\alpha : \mathbb{N} \to G$ forstås som bekendt en følge af formen $\alpha \circ j$, hvor $j : \mathbb{N} \to \mathbb{N}$ er en strengt voksende afbildning (d.v.s. en homomorfi $(\mathbb{N},<) \to (\mathbb{N},<)$). Delfølgen $\alpha \circ j$ kan betegnes $(\alpha_{j_1}, \alpha_{j_2}, \dots)$ eller (α_{j_n}).

Følgen $\alpha = (\alpha_n)$ kaldes <u>voksende</u>, hvis α er en homomorfi $\alpha : (\mathbb{N}, \leqslant) \to (G, \leqslant)$, altså hvis

$$\alpha_1 \leqslant \alpha_2 \leqslant \dots .$$

Tilsvarende definieres <u>aftagende</u>. Som fælles betegnelse bruges <u>monoton</u>.

Følgen $\alpha = (\alpha_n)$ kaldes <u>begrænset</u>, hvis der findes elementer $c_1, c_2 \in G$, således at

$$c_1 \leqslant \alpha_n \leqslant c_2 \quad \text{for alle } n \in \mathbb{N}.$$

Følgen $\alpha = (\alpha_n)$ siges at have <u>grænseværdien a</u> (hvor a er et element i G) eller at <u>konvergere mod a</u>,

hvis der til hvert $\varepsilon > 0$ i G findes et naturligt tal N, således at der for alle naturlige tal $n \geqslant N$ gælder $|\alpha_n - a| < \varepsilon$, altså hvis

$$\forall \varepsilon \in G_+ \; \exists N \in \mathbb{N} \; \forall n \in \mathbb{N} : n \geqslant N \Rightarrow |\alpha_n - a| < \varepsilon.$$

En følge, der har en grænseværdi kaldes konvergent. En følge, der konvergerer mod 0 kaldes en nulfølge.

BEMÆRKNING: Et udsagn af formen

$$\exists N \in \mathbb{N} \; \forall n \in \mathbb{N} : n \geqslant N \Rightarrow p(n),$$

hvor $p(n)$ er et udsagn om det naturlige tal n (et prædikat) skrives ofte: "fra et vist trin gælder $p(n)$", "på nær for endelig mange n gælder $p(n)$" eller "for næsten alle n gælder $p(n)$". Negationen af et sådant udsagn, altså udsagnet

$$\forall N \in \mathbb{N} \; \exists n \in \mathbb{N} : n \geqslant N \wedge \text{non } p(n)$$

kan skrives "for uendelig mange n gælder non $p(n)$" Det betyder, at der findes naturlige tal $j_1 < j_2 < \cdots$ således at non $p(j_n)$ gælder for alle n.

En følge $\alpha = (\alpha_n)$ kaldes en fundamentalfølge (eller en Cauchy-følge), hvis

$$\forall \varepsilon \in G_+ \; \exists N \in \mathbb{N} \; \forall n, m \in \mathbb{N} : n, m \geqslant N \Rightarrow |\alpha_n - \alpha_m| < \varepsilon.$$

1.2. Den ordnede gruppe $(G, +, <)$ kaldes diskret ordnet, hvis der findes et første element i G_+ (et mindste positivt element). I meget af det følgende vil dette tilfælde kræve en helt triviel særbehandling, som vi oftest udelader. For en følge $\alpha = (\alpha_n)$ i en diskret ordnet gruppe $(G, +, <)$ gælder:

$$(\alpha \text{ er en fundamentalfølge}) \Leftrightarrow (\alpha \text{ er konvergent}) \Leftrightarrow (\alpha \text{ er konstant fra et vist trin}).$$

Dette fås ved at anvende definitionerne med $\varepsilon =$ mindste positive element i G.

En ordnet gruppe $(G,+,<)$, som ikke er diskret ordnet, siges at være tæt ordnet. I en sådan gruppe kan vi til hvilkesomhelst to elementer $a', a'' \in G$, med $a' < a''$ finde et $a \in G$, således at $a' < a < a''$, thi da $a'' - a' \in G_+$ ikke er det mindste positive element, findes et element $\delta \in G_+$ således at $\delta < a'' - a'$. Af $0 < \delta < a'' - a'$ følger nu $a' < a' + \delta < a''$.

Videre gælder, at vi i en tæt ordnet gruppe $(G,+,<)$ til et givet $\varepsilon > 0$ og et givet $k \in \mathbb{N}$ kan bestemme et $\varepsilon' > 0$ således at

$$0 < k\varepsilon' < \varepsilon,$$

thi vi kan successivt bestemme $\varepsilon_1, \varepsilon_2, \cdots, \varepsilon_k \in G_+$ således at $0 < \varepsilon_1 < \varepsilon$, $0 < \varepsilon_2 < \varepsilon_1, \cdots, 0 < \varepsilon_k < \varepsilon_{k-1}$; er ε' det mindste blandt $\varepsilon_k, \varepsilon_{k-1} - \varepsilon_k, \cdots, \varepsilon_1 - \varepsilon_2$ finder vi $0 < k\varepsilon' = \varepsilon' + \cdots + \varepsilon' \leqslant (\varepsilon_1 - \varepsilon_2) + \cdots + (\varepsilon_{k-1} - \varepsilon_k) + \varepsilon_k = \varepsilon_1 < \varepsilon$.

EKSEMPEL. $(\mathbb{Z},+,<)$ er diskret ordnet; $(\mathbb{Q},+,<)$ er tæt ordnet.

1.3. BEMÆRKNING. Betragt en ordnet gruppe $(G,+,<)$, der har følgende egenskab:

(K) Enhver nulfølge i G er konstant (nødvendigvis $=0$) fra et vist trin.

For følger $\alpha = (\alpha_n)$ i en sådan gruppe finder vi også

(α er en fundamentalfølge) $\Leftrightarrow$ (α er konvergent)
$\Leftrightarrow$ (α er konstant fra et vist trin)

Det er ikke oplagt, at der findes tæt ordnede grupper, der har egenskaben (K).

1.4. Af definitionerne følger en række elementære SÆTNINGER.

En konvergent følge har netop én grænseværdi.

<u>En konvergent følge er en fundamentalfølge.</u>
<u>En fundamentalfølge er begrænset.</u>

BEVISERNES idéer er velkendte. Lad os f. eks. vise, at en konvergent følge $\alpha = (\alpha_n)$ er en fundamentalfølge: Lad $\varepsilon > 0$ være givet. Vi kan antage, at ordningen er tæt, og kan derfor bestemme $\varepsilon' > 0$ så at $2\varepsilon' \leqslant \varepsilon$. Da følgen har en grænseværdi $a \in G$, kan vi til dette ε' bestemme $N \in \mathbb{N}$, således at $|\alpha_n - a| < \varepsilon'$ for alle $n \geqslant N$. For alle $n, m \geqslant N$ finder vi nu

$$|\alpha_n - \alpha_m| = |(\alpha_n - a) + (a - \alpha_m)| \leqslant |\alpha_n - a| + |\alpha_m - a|$$
$$< \varepsilon' + \varepsilon' \leqslant \varepsilon \quad \square$$

1.5. Med $\mathcal{F}(G)$ betegner vi mængden af følger i den ordnede gruppe $(G, +, <)$. I mængden $\mathcal{F}(G)$ defineres en komposition $+$ ved "argumentvis addition": $\alpha + \beta = (\alpha_n + \beta_n)$ er følgen $n \mapsto \alpha_n + \beta_n$. Det er klart, at $(\mathcal{F}(G), +)$ er en kommutativ gruppe. I $\mathcal{F}(G)$ betegner vi med $\mathcal{BF}(G)$, $\mathcal{FF}(G)$, $\mathcal{KF}(G)$, $\mathcal{NF}(G)$ delmængderne bestående af <u>begrænsede</u> følger, <u>fundamentalfølger</u>, <u>konvergente</u> følger, <u>nulfølger</u>.

SÆTNING. <u>$\mathcal{BF}(G)$, $\mathcal{FF}(G)$, $\mathcal{KF}(G)$, $\mathcal{NF}(G)$ er undergrupper i $(\mathcal{F}(G), +)$, og vi har</u>

$$\mathcal{F}(G) \supseteq \mathcal{BF}(G) \supseteq \mathcal{FF}(G) \supseteq \mathcal{KF}(G) \supseteq \mathcal{NF}(G)$$
$$\supseteq \{\text{konst. følgen}\}.$$

BEVIS. Lad os nøjes med at vise, at summen $\alpha + \beta = (\alpha_n + \beta_n)$ af to fundamentalfølger $\alpha = (\alpha_n)$ og $\beta = (\beta_n)$ igen er en fundamentalfølge: Lad $\varepsilon > 0$ være givet. Vi kan antage, at ordningen er tæt, og kan derfor bestemme $\varepsilon' > 0$ således at $2\varepsilon' \leqslant \varepsilon$. Til dette ε' kan vi bestemme $N_1, N_2 \in \mathbb{N}$, så at

$$|\alpha_n - \alpha_m| < \varepsilon' \text{ for alle } n, m \geqslant N_1$$

og

$$|\beta_n - \beta_m| < \varepsilon' \text{ for alle } n, m \geqslant N_2.$$

Vi sætter $N = \max\{N_1, N_2\}$. For alle $n, m \geq N$ er da begge ovenstående uligheder opfyldt, og vi får

$$|(\alpha_n+\beta_n) - (\alpha_m+\beta_m)| \leq |\alpha_n - \alpha_m| + |\beta_n - \beta_m| < \varepsilon' + \varepsilon' \leq \varepsilon \quad \square$$

I beviset for at $KF(G)$ er en undergruppe i $(F(G),+)$ viser man mere præcist, at hvis følgerne $\alpha = (\alpha_n)$ og $\beta = (\beta_n)$ har grænseværdierne a og b, så har summen $\alpha + \beta = (\alpha_n + \beta_n)$ (resp. den modsatte $-\alpha = (-\alpha_n)$) grænseværdien $a+b$ (resp. $-a$). Idet vi for en konvergent følge $\alpha = (\alpha_n)$ med $\lim \alpha$ (eller $\lim_{n\to\infty} \alpha_n$) betegner følgens entydigt bestemte grænseværdi, får vi:

Afbildningen lim er en homomorfi: $(KF(G),+) \to (G,+)$.

Kernen for lim er ögensynlig undergruppen $NF(G)$ af nulfølger.

1.6. I analogi med et velkendt begreb inden for læren om metriske rum indfører vi følgende:

DEFINITION. En kommutativ ordnet gruppe $(G,+,<)$ kaldes fuldstændig, hvis enhver fundamentalfølge i G er konvergent. Dette betyder altså at $FF(G) = KF(G)$.

En diskret ordnet gruppe $(G,+,<)$ (f.eks. $(\mathbb{Z},+,<)$) er fuldstændig. Mere generelt:
En ordnet gruppe $(G,+,<)$, der opfylder betingelsen (K) i 1.3. er fuldstændig.
Derimod er $(\mathbb{Q},+,<)$ ikke fuldstændig. F.eks. er følgen $n \longmapsto \sum_{\nu=1}^{n} 2^{-\nu^2}$ en ikke-konvergent fundamentalfølge i $\mathbb{Q}$. $(\square)$.
En ifølge ovenstående definition fuldstændig kommutativ ordnet gruppe kan – mere korrekt – kaldes følgefuldstændig

2. Følgekompletion.

2.1. Vi betragter stadig en kommutativ ordnet gruppe $(G,+,<)$, og vi vil vise, at vi på "fornuftig" måde kan indlejre $(G,+,<)$ i en fuldstændig kommutativ ordnet gruppe $(\hat{G},+,<)$, kaldet kompletionen af G.

DEFINITION. To følger $\alpha=(\alpha_n)$, $\beta=(\beta_n)$ i G kaldes ækvivalente, og vi skriver $\alpha\equiv\beta$, hvis differensfølgen $\alpha-\beta=(\alpha_n-\beta_n)$ er en nulfølge.

SÆTNING. Relationen $\equiv$ er en kongruensrelation i gruppen $(\mathcal{F}(G),+)$ af følger i G.

Dette betyder, at relationen $\equiv$ er en ækvivalensrelation i $\mathcal{F}(G)$, og at den harmonerer med kompositionen $+$ i $\mathcal{F}(G)$.

BEVIS. For to følger $\alpha=(\alpha_n)$ og $\beta=(\beta_n)$ har vi ifølge definitionen

$$\alpha\equiv\beta \Leftrightarrow \alpha-\beta\in\mathcal{N}\mathcal{F}(G).$$

Heraf følger påstanden, da $\mathcal{N}\mathcal{F}(G)$ er en undergruppe i $(\mathcal{F}(G),+)$ ▨

2.2. Relationen $\equiv$ definerer specielt en kongruensrelation i hver af undergrupperne $\mathcal{B}\mathcal{F}(G)$, $\mathcal{F}\mathcal{F}(G)$ og $\mathcal{K}\mathcal{F}(G)$. Da disse undergrupper indeholder $\mathcal{N}\mathcal{F}(G)$, får vi endvidere følgende:

SÆTNING. En følge $\alpha=(\alpha_n)$ i G, der er ækvivalent med en begrænset følge (resp. fundamentalfølge, resp. konvergent følge, resp. nulfølge), er selv en begrænset følge (resp. fundamentalfølge, resp. konvergent følge, resp. nulfølge).

BEVIS. Vi kan nemlig skrive $\alpha=\alpha'+\nu$, hvor α' er en begrænset følge (resp. ...) og ν er en nulfølge.

Her er ν specielt en begrænset følge (resp. ...), og $\alpha = \alpha' + \nu$ er således sum af to begrænsede følger (resp. ...) og dermed selv en begrænset følge (resp. ...). ▨

2.3. Det er klart, at en følge $\alpha = (\alpha_n)$ i G er konvergent, hvis og kun hvis den er ækvivalent med en konstant følge. Mere præcist: Følgen $\alpha = (\alpha_n)$ har grænseværdien a, hvis og kun hvis den er ækvivalent med den konstante følge $(a, a, \dots)$.

Vi vil ofte udnytte "kun hvis"-delen af følgende:

SÆTNING. <u>En følge $\alpha = (\alpha_n)$ i G er en fundamentalfølge, hvis og kun hvis den er ækvivalent med enhver af sine delfølger</u>.

BEVIS. "<u>kun hvis</u>" følger umiddelbart af definitionerne, idet vi bemærker, at der for en delfølge (α_{f_n}) af (α_n) gælder $f_n \geqslant n$. Hvis $|\alpha_n - \alpha_m| < \varepsilon$ for alle $n, m \geqslant N$, er altså specielt $|\alpha_n - \alpha_{f_n}| < \varepsilon$ for alle $n \geqslant N$.

"<u>hvis</u>": Antag omvendt, at følgen $\alpha = (\alpha_n)$ ikke er en fundamentalfølge. Idet vi "negerer definitionen", ser vi, at der findes et $\delta > 0$, således at

$$\forall K \in \mathbb{N}\ \exists f, k \in \mathbb{N} : f, k \geqslant K \wedge |\alpha_f - \alpha_k| \geqslant \delta.$$

For $K = 1$ kan vi altså finde $f_1, k_1 \geqslant 1$ så at $|\alpha_{f_1} - \alpha_{k_1}| \geqslant \delta$. Vælger vi nu et $K = K_2 > f_1, k_1$, kan vi finde $f_2, k_2 \geqslant K_2$, således at $|\alpha_{f_2} - \alpha_{k_2}| \geqslant \delta$. Dernæst vælger vi et $K_3 > f_2, k_2$ og finder $f_3, k_3 \geqslant K_3$ så at $|\alpha_{f_3} - \alpha_{k_3}| \geqslant \delta$. Idet vi fortsætter således finder vi $f_1 < f_2 < f_3 < \cdots$ og $k_1 < k_2 < k_3 < \cdots$ som opfylder

$$|\alpha_{f_n} - \alpha_{k_n}| \geqslant \delta \text{ for alle } n.$$

Delfølgerne (α_{f_n}) og (α_{k_n}) er derfor ikke ækvivalente, og kan derfor ikke begge være ækvivalente med α. ▨

KOROLLAR. En fundamentalfølge, der har en konvergent delfølge er selv konvergent (med samme grænseværdi).
thi fundamentalfølgen er ækvivalent med en delfølge, der er ækvivalent med en konstant følge $(a,a,\dots)$ ▨

NOTATION.

2.4. Vi betragter nu specielt gruppen $(FF(G),+)$ af fundamentalfølger i G, og kongruensrelationen $\equiv$ heri. Kvotienten $(FF(G),+)/\equiv$ $(= FF(G)/NF(G))$ betegner vi $(\hat{G},+)$. Elementerne i $\hat{G}$ er ækvivalensklasser m.h.t. $\equiv$. Ækvivalensklassen, der indeholder fundamentalfølgen α, betegnes $\textcircled{\alpha}$. Komposition en $+$ i $\hat{G}$ er bestemt ved

$$\textcircled{\alpha} + \textcircled{\beta} = \textcircled{\alpha+\beta}.$$

$(\hat{G},+)$ er altså en kommutativ gruppe, og afbildningen $\alpha \mapsto \textcircled{\alpha}$ er en homomorfi: $(FF(G),+) \to (\hat{G},+)$.

2.5. NOTATION. For et element $a \in G$ betegner vi med $\hat{a} \in \hat{G}$ den ækvivalensklasse, der indeholder den konstante følge $(a,a,a,\dots)$. Det er klart, at der ved $a \mapsto \hat{a}$ defineres en injektiv homomorfi:

$$(G,+) \longrightarrow (\hat{G},+).$$

Vi vil oftist identificere elementerne i G med deres billeder i $\hat{G}$, og altså opfatte G som en undergruppe: $G \subseteq \hat{G}$.

BEMÆRKNING. Som delmængde af $FF(G)$ består ækvivalensklassen $\hat{a}$ øjensynlig af de følger, der konvergerer mod a.

2.6. Vi vil nu udvide ordningen i G til en ordning i $\hat{G}$:

DEFINITION. Med $P \subseteq \hat{G}$ betegnes delmængden bestående af de elementer $A \neq 0$ i $\hat{G}$, der har en repræsentant $\alpha = (\alpha_n)$, for hvilken der gælder

$$\alpha_n \geqslant 0 \quad \text{for alle } n.$$

Ved for elementer X, Y i $\hat{G}$ at skrive

$$X < Y \overset{\text{DEF}}{\Leftrightarrow} Y - X \in P$$

defineres da en relation $<$ i $\hat{G}$.

SÆTNING. Med den ovenfor definerede relation $<$ er $(\hat{G}, +, <)$ en ordnet gruppe, hvis positive elementer er elementerne i P. Afbildningen $a \longmapsto \hat{a}$ er en homomorfi : $(G, <) \hookrightarrow (\hat{G}, <)$.

BEVIS. Ifølge et generelt resultat om ordnede grupper skal vi om $P \subseteq \hat{G}$ vise, at $0 \notin P$, at P er stabil, og at der for hvert $X \neq 0$ i $\hat{G}$ gælder $X \in P$ eller $-X \in P$. Det første er klart ifølge definitionen. For at vise, at P er stabil, vælges for elementer $A, B \in P$ repræsentanter: $A = \textcircled{\alpha}$, $B = \textcircled{\beta}$, så at $\alpha_n \geqslant 0$, $\beta_n \geqslant 0$ for alle n. Da er $\alpha + \beta$ en repræsentant for $A + B$ med $\alpha_n + \beta_n \geqslant 0$ for alle n, og $A + B \in P$, thi ellers var $A + B = 0$, og altså $\alpha + \beta = (\alpha_n + \beta_n)$ en nulfølge, og så kunne vi af

$$0 \leqslant \alpha_n \leqslant \alpha_n + \beta_n$$

slutte, at også $\alpha = (\alpha_n)$ var en nulfølge, i modstrid med at $\textcircled{\alpha} = A \neq 0$.

Betragt videre et element $X \neq 0$ i $\hat{G}$, og vælg en repræsentant : $X = \textcircled{\xi}$. Da gælder: Enten er $\xi_n \geqslant 0$ for uendelig mange n. I så fald har $\xi = (\xi_n)$ en delfølge, hvis elementer alle er $\geqslant 0$, og da denne delfølge også er repræsentant for X, ser vi, at $X \in P$. Eller også er $\xi_n < 0$ fra et vist trin. Da følgen

$-\xi = (-\xi_n)$ er en repræsentant for $-X$, hvis elementer er $\geqslant 0$ (endda >0) fra et vist trin, ser vi tilsvarende, at vi i så fald har $-X \in P$.

Sætningens sidste påstand er triviel. ▨

2.7. Det følger, at den herved definerede ordning i $\hat{G}$ på G opfattet som delmængde $G \subseteq \hat{G}$ stemmer overens med den givne ordning i G.

DEFINITION. Den ovenfor konstruerede kommutative ordnede gruppe $(\hat{G},+,<)$, indeholdende $(G,+,<)$, kaldes <u>kompletionen</u> (mere præcist: <u>følgekompletionen</u>) af $(G,+,<)$.

Hvis $(G,+,<)$ er fuldstændig, er $G = \hat{G}$. Som vi om lidt skal se, er $(\hat{G},+,<)$ altid fuldstændig.

2.8. OBSERVATION. <u>Hvis $\alpha=(\alpha_n)$ og $\beta=(\beta_n)$ er fundamentalfølger i G, således at</u>

<u>$\alpha_n \leq \beta_n$ for uendelig mange n,</u>

<u>så er</u>

<u>$\textcircled{\alpha} \leqslant \textcircled{\beta}$ i $\hat{G}$</u>

thi $\textcircled{\beta} - \textcircled{\alpha} = \textcircled{\beta-\alpha}$ har da en repræsentant (nemlig en delfølge af $\beta-\alpha = (\beta_n-\alpha_n)$), hvis elementer alle er $\geqslant 0$, så vi slutter at $\textcircled{\beta}-\textcircled{\alpha} = 0$ eller at $\textcircled{\beta}-\textcircled{\alpha} \in P$.

2.9. SÆTNING. <u>Til hvert element $E \in \hat{G}_+$ findes et element $\varepsilon \in G_+$, så at $0 < \hat{\varepsilon} \leqslant E$.</u>

BEVIS. Da $E \in \hat{G}_+ = P$, har E en repræsentant $\alpha = (\alpha_n)$, så at $\alpha_n \geqslant 0$ for alle n. Da $E \neq 0$, er α ikke en nulfølge, så der findes i G et $\varepsilon > 0$, så at

$$\varepsilon \leqslant \alpha_n \quad \text{for uendelig mange } n.$$

Anvendes Observation 2.8 på følgen $\alpha = (\alpha_n)$ og den konstante følge $(\varepsilon, \varepsilon, \varepsilon, \cdots)$, får vi i $\hat{G}$: $0 < \hat{\varepsilon} \leqslant \textcircled{\alpha} = E$ ▨

BEMÆRKNING. Heraf ses, at hvis en følge $\alpha = (\alpha_n)$ i G har en af egenskaberne "fundamentalfølge", "konvergent mod a", "nulfølge", så vil den opfattet som følge i $\hat{G}$ have den samme egenskab. Omvendt gælder trivielt, at hvis følgen $\alpha = (\alpha_n)$ i G opfattet som følge i $\hat{G}$ har en af egenskaberne "fundamentalfølge", "nulfølge", så vil den som følge i G have samme egenskab. Derimod kan en følge $\alpha = (\alpha_n)$ i G godt være konvergent i $\hat{G}$ uden at den er konvergent i G, idet grænseværdien ikke nødvendigvis tilhører G.

2.10. SÆTNING. Lad $\alpha = (\alpha_n)$ være en fundamentalfølge i G. Da er følgen $(\hat{\alpha}_n)$ i $\hat{G}$ konvergent med grænseværdien $\textcircled{\alpha}$.

BEVIS. Ifølge Sætning 2.9 er det nok at vise, at der for ethvert $\varepsilon \in G_+$ findes $N \in \mathbb{N}$, så at

$$|\hat{\alpha}_n - \textcircled{\alpha}| < \hat{\varepsilon} \quad \text{for alle } n \geqslant N.$$

Da $\alpha = (\alpha_n)$ er en fundamentalfølge, kan vi til det givne $\varepsilon \in G_+$ finde $N \in \mathbb{N}$, således at vi for $n, m \geqslant N$ har

$$-\varepsilon < \alpha_n - \alpha_m < \varepsilon$$

For et fast $n \geqslant N$ gælder disse uligheder specielt for uendelig mange m, og anvendes Observation 2.8 på følgen $(\alpha_n - \alpha_1, \alpha_n - \alpha_2, \alpha_n - \alpha_3, \cdots)$ og de konstante følger $(-\varepsilon, -\varepsilon, -\varepsilon, \cdots)$ og $(\varepsilon, \varepsilon, \varepsilon, \cdots)$, får vi i $\hat{G}$:

$$-\hat{\varepsilon} \leqslant \hat{\alpha}_n - \textcircled{\alpha} \leqslant \hat{\varepsilon}.$$

Altså har vi:

$$|\hat{\alpha}_n - \textcircled{\alpha}| \leq \hat{\varepsilon} \quad \text{for alle } n \geq N.$$

Dette er den søgte ulighed, blot med "$\leq$" i stedet for "$<$". Hvis G er tæt ordnet, er dette tilstrækkeligt. Og hvis G er diskret ordnet, er sætningen triviel ▨

BEMÆRKNING. Herefter vil vi altid identificere elementer $a \in G$ med deres billeder $\hat{a} \in \hat{G}$, og altså opfatte G som en delmængde $G \subseteq \hat{G}$.

2.11. Vi kan nu vise

SÆTNING. <u>For kompletionen $(\hat{G},+,<) \supseteq (G,+,<)$ gælder</u>

(1) <u>Enhver fundamentalfølge i G er konvergent i $\hat{G}$.</u>

(2) <u>Ethvert element i $\hat{G}$ er grænseværdi for en følge i G.</u>

(3) <u>$(\hat{G},+,<)$ er fuldstændig.</u>

BEVIS. Påstandene (1) og (2) er begge indeholdt i den foregående sætning. Lad os vise, at (3) er en konsekvens af (1) og (2): Hvis $(\hat{G},+,<)$ har egenskaben (K) i 1.3., altså hvis enhver nulfølge i $\hat{G}$ er $=0$ fra et vist trin, er påstanden triviel. Vi kan derfor <u>antage</u>, at der i $\hat{G}$ findes en nulfølge, som indeholder uendelig mange elementer $\neq 0$. Ved først at udvælge en delfølge heraf, og ved dernæst at betragte absolutværdien af dennes elementer, ser vi, at der findes en nulfølge (Δ_n) i $\hat{G}$ bestående af elementer $\Delta_n \in \hat{G}_+$.

Lad nu (A_n) være en fundamentalfølge i $\hat{G}$. For hvert $n \in \mathbb{N}$ kan vi – da A_n er grænseværdi for en følge i G (2) – bestemme et element α_n i G, således at $|A_n - \alpha_n| < \Delta_n$. Herved får vi en følge (α_n) med elementer i G, således at vi i $\hat{G}$ har

$$|A_n - \alpha_n| < \Delta_n \text{ for alle } n.$$

Heraf slutter vi, at følgerne (A_n) og (α_n) er

ækvivalente følger i $\hat{G}$. Da (A_n) var en fundamentalfølge, er også (α_n) en fundamentalfølge i $\hat{G}$. Heraf følger imidlertid, at (α_n) er en fundamentalfølge i G, og da (1) gælder, må (α_n) være en konvergent følge i $\hat{G}$. Da (A_n) og (α_n) var ækvivalente følger i $\hat{G}$, er også (A_n) en konvergent følge i $\hat{G}$. ▨

2.12. Kompletionen af $(\mathbb{Z},+,<)$ er $(\mathbb{Z},+,<)$, da $(\mathbb{Z},+,<)$ er diskret ordnet og dermed fuldstændig.
Kompletionen af $(\mathbb{Q},+,<)$ er de reelle tals ordnede gruppe $(\mathbb{R},+,<)$, som vi senere skal se nærmere på.

3. Kontinuitet.

3.1 Vi betragter nu foruden $(G,+,<)$ endnu en kommutativ ordnet gruppe $(H,+,<)$.

DEFINITION. En afbildning $f: G \to H$ kaldes kontinuert i a, hvor a er et element i G, hvis

$$\forall \varepsilon \in H_+ \; \exists \delta \in G_+ \; \forall x \in G : |x-a| < \delta \Rightarrow |f(x)-f(a)| < \varepsilon.$$

Afbildningen $f: G \to H$ kaldes kontinuert, hvis den er kontinuert i hvert element $a \in G$.

SÆTNING. Lad $f: G \to H$ være en kontinuert afbildning. Hvis en følge $\alpha = (\alpha_n)$ i G har grænseværdien a, så har billedfølgen $f\alpha = (f(\alpha_n))$ i H grænseværdien $f(a)$. □

3.2. En kontinuert afbildning afbilder altså konvergente følger i G på konvergente følger i H. Derimod vil fundamentalfølger i G i almindelighed ikke afbildes på fundamentalfølger i H.

DEFINITION. En afbildning $f: G \to H$ kaldes uniformt (eller ligeligt) kontinuert, hvis

$$\forall \varepsilon \in H_+ \; \exists \delta \in G_+ \; \forall x,y \in G : |x-y| < \delta \Rightarrow |f(x)-f(y)| < \varepsilon.$$

SÆTNING. En uniformt kontinuert afbildning $f: G \to H$ er kontinuert. Den afbilder fundamental-følge i G på fundamentalfølge i H og den afbilder to ækvivalente følger i G på to ækvivalente følger i H. □

Absolutværdien i G, opfattet som en afbildning $|\,|: G \to G$, er uniformt kontinuert. Dette følger af uligheden $\big||x|-|y|\big| \leqslant |x-y|$.

3.3. For homomorfier $: (G,+) \to (H,+)$ får vi et let anvendeligt kriterium for uniform kontinuitet, idet der gælder

SÆTNING. *En homomorfi $f: (G,+) \to (H,+)$, som er kontinuert i 0, er uniformt kontinuert.*

Bevis. Lad $\varepsilon \in H_+$ være givet. Da f er en homomorfi, er $f(0) = 0$, og kontinuiteten i 0 sikrer derfor, at vi kan finde $\delta \in G_+$, så at $|f(x)| < \varepsilon$ når $|x| < \delta$. For alle $x, y \in G$ med $|x-y| < \delta$ finder vi derfor

$$|f(x) - f(y)| = |f(x-y)| < \varepsilon. \quad \blacksquare$$

Inklusionsafbildningen $: (G,+,<) \hookrightarrow (\hat{G},+,<)$ er kontinuert, endda uniformt. Dette følger let af sætning 2.9 i forbindelse med at afbildningen er ordenstro. En vilkårlig ordenstro homomorfi $f: (G,+,<) \to (H,+,<)$ vil derimod i almindelighed ikke være kontinuert.

3.4 UDVIDELSESSÆTNING. *Enhver uniformt kontinuert afbildning $f: G \to H$, hvor $(H,+,<)$ er fuldstændig, kan entydigt udvides til en uniformt kontinuert afbildning $\hat{f}: \hat{G} \to H$.*

Bevis. Entydighed. Hvis en udvidelse $\hat{f}: \hat{G} \to H$ blot er kontinuert, så gælder for hvert element $A \in \hat{G}$ og enhver følge $\alpha = (\alpha_n)$ i G, som konvergerer mod A, at billedfølgen $\hat{f}(\alpha) = (\hat{f}(\alpha_n)) = (f(\alpha_n))$ konvergerer mod $\hat{f}(A)$. Vi har altså

$$(*) \quad \lim_{n\to\infty} \alpha_n = A \Rightarrow \lim_{n\to\infty} f(\alpha_n) = \hat{f}(A).$$

Heraf følger specielt entydigheden af $\hat{f}$.

Eksistens. Til hvert element $A \in \hat{G}$ findes følgen $\alpha = (\alpha_n)$ i G, som konvergerer mod A. Er (α_n) en sådan følge, så er $\alpha = (\alpha_n)$ en fundamentalfølge i G. Da f er uniformt kontinuert, er $f(\alpha) = (f(\alpha_n))$ en fundamentalfølge i H, og da H er fuldstændig, har følgen $(f(\alpha_n))$ en grænseværdi. Denne grænseværdi afhænger ikke af hvilken følge $\alpha = (\alpha_n)$ vi betragter.

Er nemlig $\alpha' = (\alpha_n')$ endnu en følge i G, som konvergerer mod $A \in \hat{G}$, så er følgerne α og α' ækvivalente i G. Da f er uniformt kontinuert, er også billedfølgerne $f(\alpha) = (f(\alpha_n))$ og $f(\alpha') = (f(\alpha_n'))$ ækvivalente i H. Følgelig har $f(\alpha') = (f(\alpha_n'))$ samme grænseværdi som $f(\alpha) = (f(\alpha_n))$.

Betegnes denne grænseværdi $\hat{f}(A)$, har vi altså defineret en afbildning $\hat{f}: \hat{G} \to H$, således at der for følger $\alpha = (\alpha_n)$ i G gælder

$$\lim_{n\to\infty} \alpha_n = A \implies \lim_{n\to\infty} f(\alpha_n) = \hat{f}(A).$$

Det er klart, at $\hat{f}$ er en udvidelse af f, så vi mangler blot at vise, at $\hat{f}: \hat{G} \to H$ er uniformt kontinuert. Hvis $(H,+,<)$ er diskret ordnet, vises dette let. Vi antager derfor, at $(H,+,<)$ er tæt ordnet, og betragter et givet $\varepsilon \in H_+$. Hertil kan vi vælge $\varepsilon' \in H_+$ med $\varepsilon' < \varepsilon$, og til dette ε' kan vi vælge $\delta \in G_+$, så at vi for $a, b \in G$ har

$$|a-b| < \delta \implies |f(a) - f(b)| < \varepsilon'.$$

Til elementer $A, B \in \hat{G}$ kan vi finde følger (α_n) og (β_n) i G med $\lim_{n\to\infty} \alpha_n = A$ og $\lim_{n\to\infty} \beta_n = B$, og altså $\lim_{n\to\infty} f(\alpha_n) = \hat{f}(A)$ og $\lim_{n\to\infty} f(\beta_n) = \hat{f}(B)$. Heraf slutter vi, at $\lim_{n\to\infty} (\alpha_n - \beta_n) = A - B$ og $\lim_{n\to\infty} (f(\alpha_n) - f(\beta_n)) = \hat{f}(A) - \hat{f}(B)$. Hvis $|A-B| < \delta$, har vi derfor $|\alpha_n - \beta_n| < \delta$ fra et vist trin, og dermed $|f(\alpha_n) - f(\beta_n)| < \varepsilon'$ fra et vist trin. For grænseværdien har vi derfor

$$|\hat{f}(A) - \hat{f}(B)| \leqslant \varepsilon' < \varepsilon \quad \blacksquare$$

3.5. For homomorfier $f: (G,+) \to (H,+)$ får vi en tilsvarende UDVIDELSESSÆTNING. <u>Enhver kontinuert homomorfi $f: (G,+) \to (H,+)$, hvor $(H,+,<)$ er fuldstændig, har en entydig udvidelse til en kontinuert homomorfi $\hat{f}: (\hat{G},+) \to (H,+)$.</u>

Bevis. Da en homomorfi er kontinuert, hvis og kun hvis den er uniformt kontinuert, er det nok at vise, at den entydigt bestemte udvidelse af f til en kontinuert afbildning $\hat{f}: \hat{G} \to H$ er en homomorfi : $(\hat{G},+) \to (H,+)$. Hvis $A, B \in \hat{G}$, findes følger $\alpha = (\alpha_n)$, $\beta = (\beta_n)$ i G, der konverger mod A, B. Her er $\hat{f}(A), \hat{f}(B)$ grænseværdierne for følgerne $f\alpha = (f(\alpha_n))$, $f\beta = (f(\beta_n))$ i H. Da følgen $\alpha+\beta = (\alpha_n+\beta_n)$ konvergerer mod $A+B$, vil følgen $f(\alpha+\beta) = (f(\alpha_n+\beta_n))$ konvergere mod $\hat{f}(A+B)$. Her er $f(\alpha+\beta) = (f(\alpha_n+\beta_n)) = (f(\alpha_n)+f(\beta_n))$ summen af følgerne $f\alpha$ og $f\beta$. Grænseværdien er derfor $\hat{f}(A)+\hat{f}(B)$. ▨

3.6. UDVIDELSESSÆTNING. <u>Enhver kontinuert homomorfi $f: (G,+,<) \to (H,+,<)$, hvor $(H,+,<)$ er fuldstændig, har en entydig udvidelse til en kontinuert homomorfi $\hat{f}: (\hat{G},+,<) \to (H,+,<)$.</u>

Bevis. f kan entydigt udvides til en kontinuert homomorfi $\hat{f}: (\hat{G},+) \to (H,+)$, og vi skal blot vise, at udvidelsen $\hat{f}$ er ordnstro : $(\hat{G},<) \to (H,<)$. Det er nok at vise, at der for hvert element $E \in \hat{G}_+$ gælder $\hat{f}(E) \in H_+$. Elementet $E \in \hat{G}_+$ har en repræsentant $\alpha = (\alpha_n)$, der opfylder $\alpha_n \geqslant 0$ for alle n. Følgelig er også $f(\alpha_n) \geqslant 0$ for alle n, og da $\lim_{n\to\infty} \alpha_n = E$, må vi have $\hat{f}(E) = \lim_{n\to\infty} f(\alpha_n) \geqslant 0$.

For at vise, at der gælder det skarpe "$<$", bruger vi Sætning 2.9. Der findes et $\varepsilon \in G_+$, så at $0 < \varepsilon \leqslant E$. Vi har $E-\varepsilon \geqslant 0$ og dermed i følge det allerede viste $\hat{f}(E-\varepsilon) \geqslant 0$, men så er $0 < f(\varepsilon) \leqslant f(\varepsilon)+\hat{f}(E-\varepsilon) = f(\varepsilon)+\hat{f}(E)-f(\varepsilon) = \hat{f}(E)$. ▨

4. Multiplikation

4.1. Lad $(\Lambda,+,\cdot,<)$ være en ordnet ring. Da er $(\Lambda,+,<)$ en kommutativ ordnet gruppe, og vi kan betragte kompletionen $(\hat{\Lambda},+,<)$. I almindelighed kan multiplikationen i Λ ikke på fornuftig måde udvides til en multiplikation i $\hat{\Lambda}$. Dette hænger sammen med at afbildningerne $x \mapsto xa$, $x \mapsto ax$ (høje- og venstremultiplikation med elementet $a \in \Lambda$) ikke nødvendigvis er kontinuerte afbildninger $: \Lambda \to \Lambda$.

DEFINITION. En ordnet ring $(\Lambda,+,\cdot,<)$ siges at have kontinuert multiplikation, hvis der for hvert $a \in \Lambda$ gælder, at afbildningerne $x \mapsto xa$ og $x \mapsto ax$ er kontinuerte afbildninger $: \Lambda \to \Lambda$. I følge Sætning 3.3. er det nok at kræve, at disse afbildninger er kontinuerte i 0. Hvis det er tilfældet, vil de endda være uniformt kontinuerte, de vil afbilde fundamentalfølger på fundamentalfølger og konvergente følger på konvergente følger, og de vil bevare ækvivalens.

4.2. SÆTNING. Et ordnet legeme $(L,+,\cdot,<)$ har kontinuert multiplikation.

BEVIS. Det er nok at vise, at der for hvert $a \neq 0$ i L gælder, at afbildningen $x \mapsto ax$ er kontinuert i $0 \in L$. Lad $\varepsilon \in L_+$ være givet. Det er let at se, at også $|a|^{-1}\varepsilon \in L_+$. Sættes $\delta = |a|^{-1}\varepsilon$, finder vi for alle x med $|x| < \delta$, at

$$|ax| = |a||x| < |a||a|^{-1}\varepsilon = \varepsilon. \quad \square$$

4.3. For to følger $\alpha = (a_n)$, $\beta = (\beta_n)$ i en ordnet ring $(\Lambda,+,\cdot,<)$ defineres produktfølgen $\alpha\beta$ ved

$$\alpha \cdot \beta = (\alpha_n \beta_n).$$

Det er let at se, at mængden $\mathcal{F}(\Lambda)$ af følger i Λ med denne komposition og den tidligere indførte addition er en ring $(\mathcal{F}(\Lambda), +, \cdot)$.

SÆTNING. *Lad $(\Lambda, +, \cdot, <)$ være en ordnet ring med kontinuert multiplikation. Idet vi med $\mathcal{BF}(\Lambda)$, $\mathcal{FF}(\Lambda)$, $\mathcal{KF}(\Lambda)$, $\mathcal{NF}(\Lambda)$ betegner mængderne bestående af begrænsede følger, fundamentalfølger, konvergente følger, nulfølger i Λ gælder:*

(1) $\beta \in \mathcal{BF}(\Lambda) \wedge \nu \in \mathcal{NF}(\Lambda) \Rightarrow \nu\beta \in \mathcal{NF}(\Lambda) \wedge \beta\nu \in \mathcal{NF}(\Lambda)$

(2) $\beta \in \mathcal{BF}(\Lambda) \wedge \alpha \equiv \alpha' \Rightarrow \beta\alpha \equiv \beta\alpha' \wedge \alpha\beta \equiv \alpha'\beta$

(3) $\alpha \in \mathcal{FF}(\Lambda) \wedge \beta \in \mathcal{FF}(\Lambda) \Rightarrow \alpha\beta \in \mathcal{FF}(\Lambda)$

(4) $\alpha \in \mathcal{KF}(\Lambda) \wedge \beta \in \mathcal{KF}(\Lambda) \Rightarrow \alpha\beta \in \mathcal{KF}(\Lambda)$ (og $\lim \alpha\beta = (\lim \alpha)(\lim \beta)$)

BEVIS. (1): Da $\beta = (\beta_n)$ er begrænset, findes et element $c \in \Lambda_+$, således at $|\beta_n| \leqslant c$ for alle n. Nu finder vi

$$0 \leqslant |\beta_n \nu_n| = |\beta_n||\nu_n| \leqslant c|\nu_n| \text{ for alle } n.$$

Da $\nu = (\nu_n)$ er en nulfølge, er også følgen $(|\nu_n|)$ en nulfølge, og da multiplikation med c er kontinuert, er også følgen $(c|\nu_n|)$ en nulfølge. Uligheden medfører nu, at $\beta\nu = (\beta_n\nu_n)$ er en nulfølge. Tilsvarende med $\nu\beta$.

(2): følger let af (1), idet vi har $\alpha \equiv \alpha' \Leftrightarrow \alpha' - \alpha \in \mathcal{NF}(\Lambda)$.

(3): Da en følge er en fundamentalfølge, hvis og kun hvis den er ækvivalent med enhver af sine delfølger (Sætning 2.3.), er det nok at vise, at $\alpha\beta = (\alpha_n\beta_n)$ er ækvivalent med en vilkårlig delfølge $(\alpha\beta)\circ j = (\alpha_{j_n}\beta_{j_n})$. Nu er $\alpha \equiv \alpha \circ j$, $\beta \equiv \beta \circ j$, så ved gentagen anvendelse af (2) får vi $(\alpha\beta)\circ j = (\alpha \circ j)(\beta \circ j) \equiv \alpha(\beta \circ j) \equiv \alpha\beta$.

(4): følger ligeledes af (2) ved at benytte, at en følge er konvergent netop når den er ækvivalent med en konstant følge. □

4.4. SÆTNING. *Lad $(\Lambda,+,\cdot,<)$ være en ordnet ring med kontinuert multiplikation. Multiplikationen i Λ har da en entydig udvidelse til en komposition $\cdot$ i $\hat{\Lambda}$, således at $(\hat{\Lambda},+,\cdot,<)$ bliver en ordnet ring med kontinuert multiplikation.*

BEVIS. Entydighed. Hvis $X,Y\in\hat{\Lambda}$, kan vi finde følger $\alpha=(\alpha_n)$, $\beta=(\beta_n)$ i Λ, med grænseværdierne X,Y i $\hat{\Lambda}$. For en komposition $\hat{\cdot}$ i $\hat{\Lambda}$ med de anførte egenskaber, må vi have (Sætning 4.3. (4)):

$$X\hat{\cdot}Y=\lim_{n\to\infty}\alpha_n\hat{\cdot}\beta_n=\lim_{n\to\infty}\alpha_n\cdot\beta_n.$$

Heraf er produktet $X\hat{\cdot}Y$ udtrykt ved multiplikationen i Λ.

Eksistens. Gruppen $(\hat{\Lambda},+)$ er kvotienten $(FF(\Lambda),+)/NF(\Lambda)$. Af Sætning 4.3. (3) og (1) følger specielt, at $FF(\Lambda)$ er en delring af $(F(\Lambda),+,\cdot)$, og at $NF(\Lambda)$ er et ideal i denne delring. Vi kan derfor betragte $\hat{\Lambda}$ som en kvotientring $\hat{\Lambda}:=(FF(\Lambda),+,\cdot)/NF(\Lambda)$.

Det er trivielt (men noget omstændeligt) at vise, at den herved definerede multiplikation i $\hat{\Lambda}$ opfylder de stillede krav. □

4.5. *Hvis $(\Lambda,+,\cdot,<)$ er en ordnet ring med kontinuert multiplikation, kaldes den ovenfor konstruerede ordnede udvidelse $(\hat{\Lambda},+,\cdot,<)$ for kompletionen af $(\Lambda,+,\cdot,<)$.*

4.6 Specielt har hvert ordnet legeme $(L,+,\cdot,<)$ en kompletion $(\hat{L},+,\cdot,<)$.

SÆTNING. *Kompletionen $(\hat{L},+,\cdot,<)$ af et ordnet legeme $(L,+,\cdot,<)$ er igen et ordnet legeme.*

BEVIS. Det er nok at vise, at hvert element $A\in\hat{L}_+$ er invertibelt. Elementet A har da en repræsentant $\alpha=(\alpha_n)$, som opfylder,

at $0 \leqslant \alpha_n$ for alle n. Da $\alpha = (\alpha_n)$ ikke er en nulfølge, findes et $\delta \in L_+$ så at uligheden $\delta \leqslant \alpha_n$ gælder for uendelig mange n. I stedet for at erstatte α med en (ækvivalent) delfølge, kan vi antage, at

$$0 < \delta \leqslant \alpha_n \quad \text{for alle } n.$$

Lad os først vise, at der for denne repræsentant $\alpha = (\alpha_n)$ for A gælder, at følgen $\alpha^{-1} = (\alpha_n^{-1})$ er en fundamentalfølge i L. Lad $\varepsilon \in L_+$ være givet. Vi kan da finde $N \in \mathbb{N}$, således at

$$|\alpha_n - \alpha_m| < \varepsilon\delta^2 \quad \text{for alle } n, m \geqslant N,$$

men så er

$$|\alpha_n^{-1} - \alpha_m^{-1}| = |\alpha_n - \alpha_m|\,|\alpha_n^{-1}|\,|\alpha_m^{-1}| \leqslant |\alpha_n - \alpha_m|\,\delta^{-2} < \varepsilon.$$

for alle $n, m \geqslant N$.
Nu er det klart, at $(\alpha^{-1}) \in \hat{L}$ er invers til $(\alpha) = A$. ▨

DEFINITION.

4.7. Kompletionen af de rationale tals ordnede legeme $(\mathbb{Q}, +, \cdot, <)$ kaldes de reelle tals ordnede legeme og betegnes $(\mathbb{R}, +, \cdot, <)$. Den ordnede gruppe $(\mathbb{R}, +, <)$ er de reelle tals ordnede gruppe, jfr. 2.12.

4* Kompletion af ordnet legeme.

4*.1. Lad $(L,+,\cdot,<)$ være et ordnet legeme. Da kan vi specielt betragte den kommutative, ordnede gruppe $(L,+,<)$ og dennes kompletion $(\hat{L},+,<)$.

SÆTNING. Multiplikationen i L kan entydigt udvides til en komposition $\hat{\cdot}$ i $\hat{L}$ således at $(\hat{L},+,\hat{\cdot},<)$ er et ordnet legeme.

BEVISSKITSE. Overvej først, at multiplikationen i et ordnet legeme er kontinuert i den forstand, at for konvergente følger (α_n) og (β_n) er også produktfølgen $(\alpha_n\beta_n)$ konvergent og dens grænseværdi er produktet af grænseværdierne. Heraf fås entydigheden: For givne elementer A,B i $\hat{L}$ kan vi vælge følger (α_n) og (β_n) i delmængden L med A og B som grænseværdier. For en komposition $\hat{\cdot}$ i $\hat{L}$, som opfylder de stillede krav må vi derfor have

$$(*)\quad A\hat{\cdot}B = \lim\alpha_n \hat{\cdot} \lim\beta_n = \lim \alpha_n\hat{\cdot}\beta_n = \lim \alpha_n\cdot\beta_n,$$

og da højresiden kun afhænger af den givne multiplikation $\cdot$ i L følger entydigheden.

Eksistens: Vis først, at ligningen $(*)$ definerer en komposition i $\hat{L}$, d.v.s. at højresiden kun afhænger af A og B og ikke af de foretagne valg. Vis dernæst, at den således definerede komposition $\hat{\cdot}$ opfylder de stillede krav. □

4*.2. DEFINITION. Det således konstruerede ordnede legeme $(\hat{L},+,\cdot,<)$ (hvor multiplikationen som sædvanlig blot betegnes $\cdot$) kaldes (følge-)kompletionen af det ordnede legeme $(L,+,\cdot,<)$. Kompletionen af de rationale tals ordnede legeme $(\mathbb{Q},+,\cdot,<)$ kaldes de reelle tals ordnede legeme og betegnes $(\mathbb{R},+,\cdot,<)$, jfr. 2.12.

5. Supremum og infimum.

5.1. DEFINITION. Lad $(M,<)$ være en irrefleksivt, totalt ordnet mængde. Ved et snit i M forstås et par (P,Q) af ikke-tomme delmængder af M, som opfylder

$$P = \{\text{minoranter for } Q\} \qquad Q = \{\text{majoranter for } P\}.$$

Idet vi for et vilkårligt element $a \in M$ sætter

$$M_{\leqslant a} = \{x \in M \mid x \leqslant a\} \quad \text{og} \quad M_{\geqslant a} = \{x \in M \mid a \leqslant x\}$$

er $(M_{\leqslant a}, M_{\geqslant a})$ øjensynlig et snit i M. Et snit af denne form siges at være elementbestemt (ved a)

5.2. SÆTNING. For et vilkårligt snit (P,Q) i M gælder, at $P \cup Q = M$, og at $P \cap Q$ højst indeholder ét element. Snittet er elementbestemt, hvis og kun hvis $P \cap Q \neq \emptyset$. Hertil er det nok, at P har et supremum (eller at Q har et infimum).

BEVIS. Lad $x \in M$. Enten er x minorant for Q, og så er $x \in \{\text{minoranter for } Q\} = P$, eller x er ikke minorant for Q, og så findes $q \in Q$ med $q < x$. Her er q majorant for P, og så er også $x \in \{\text{majoranter for } P\} = Q$. Altså er $M = P \cup Q$.

Et element $a \in P \cap Q$ vil dels tilhøre P, dels tilhøre $Q = \{\text{majoranter for } P\}$ og det vil derfor være sidste element og dermed supremum for P. Antag omvendt, at P har et supremum a. Da er a det mindste element i $\{\text{majoranter for } P\} = Q$, og så er $Q = M_{\geqslant a}$ og $P = \{\text{minoranter for } M_{\geqslant a}\} = M_{\leqslant a}$ ∎

5.3. SÆTNING. For en ordnet mængde $(M,<)$ er følgende betingelser ækvivalente:

(i') Enhver ikke-tom, opad begrænset delmængde har et supremum.

(i'') Enhver ikke-tom, nedad begrænset delmængde har et infimum.

(i) Ethvert snit i M er elementbestemt.

BEVIS. Det er nok at vise, at $(i') \Leftrightarrow (i)$, idet beviset for $(i'') \Leftrightarrow (i)$ forløber analogt (eller ved at udnytte, at $(i') \Leftrightarrow (i)$ gælder for mængden $(M, >)$ med den modsatte ordning $>$).
$(i') \Rightarrow (i)$: Lad (P, Q) være et snit i M. Her er $P \neq \emptyset$, og P er opad begrænset (da $Q \neq \emptyset$). Følgelig har P et supremum p, og af sætning 5.1 følger, at (P, Q) er elementbestemt (ved p).
$(i) \Rightarrow (i')$: Lad S være en ikke-tom, opad begrænset delmængde af M, og sæt $Q = \{$majoranter for $S\}$, $P = \{$minoranter for $Q\}$. Her er $Q \neq \emptyset$, da S var opadbegrænset, og $P \neq \emptyset$, da vi klart har $P \supseteq S$, og $S \neq \emptyset$. I følge definitionen er

$$P = \{\text{minoranter for } Q\};$$

der gælder også

$$Q = \{\text{majoranter for } P\},$$

thi "$\subseteq$" er oplagt, og hvis x er en majorant for P, så er x specielt en majorant for delmængden $S \subseteq P$, og dermed element i Q. Vi slutter, at (P, Q) er et snit i M. I følge forudsætningen er et sådant snit elementbestemt ved et element p. Dette element p er første element i Q, altså supremum for S. ▨

DEFINITION. En ordnet mængde $(M, <)$, som opfylder en af disse ækvivalente betingelser, vil vi kalde <u>snitfuldstændig</u>.

EKSEMPLER. $(\mathbb{N}, <)$ er snitfuldstændig. Der gælder endda at enhver ikke-tom, opad begrænset delmængde af $\mathbb{N}$ har et sidste element ("Naturlige tal" Sætning 5.11.) Analogt med $(\mathbb{Z}, <)$. Derimod er er $(\mathbb{Q}, <)$ ikke snitfuldstændig.

6. Supremum og infimum i en ordnet gruppe.

6.1. Vi betragter en kommutativ, ordnet gruppe $(G,+,<)$. Den kaldes snit fuldstændig, hvis $(G,<)$ er snitfuldstændig (5.2).

DEFINITION. $(G,+,<)$ siges at være arkimedisk (eller eudoxisk) ordnet, hvis der til hvert element $a \in G$ og hvert element $\varepsilon \in G_+$ findes et naturligt tal n, således at $a < n\varepsilon$.

Det er klart, at betingelsen er ækvivalent med at $\{0\}$ er den eneste begrænsede undergruppe i G.

EKSEMPLER. Det ses let, at $(\mathbb{Z},+,<)$ og $(\mathbb{Q},+,<)$ er arkimedisk ordnede.

SÆTNING. *Et ordnet legeme $(L,+,\cdot,<)$ er arkimedisk ordnet, hvis og kun hvis følgen $n \mapsto n^{-1}$ er en nulfølge i L.*

BEVIS. Ethvert ordnet legeme indeholder de rationale tals legeme som delegeme ("Bröker" 3.4), så det har mening i L at betragte elementer af formen $n^{-1} = \frac{1}{n}$.

"hvis" Lad $a, \varepsilon \in L$ være givne elementer, med $\varepsilon > 0$. Hvis $a \leqslant 0$, har vi $a < n\varepsilon$ for alle n. Vi kan derfor antage, at $a > 0$. Da $(\frac{1}{n})$ er en nulfølge, gælder $\frac{1}{n} < \varepsilon a^{-1}$ for næsten alle n, specielt for mindst et n. For dette n gælder derfor $a < n\varepsilon$.

"kun hvis". Lad $\varepsilon \in L_+$ være givet. Der findes et $N \in \mathbb{N}$, så at $1 < N\varepsilon$. For alle $n \geqslant N$ finder vi derfor $1 < N\varepsilon \leqslant n\varepsilon$, men så er

$$\left|\frac{1}{n}\right| = \frac{1}{n} < \varepsilon \quad \text{for alle } n \geqslant N. \qquad \square$$

6.2. SÆTNING. *For en kommutativ, ordnet gruppe $(G,+,<)$ er følgende betingelser ækvivalente:*

(i) *G er snitfuldstændig.*

(ii) *Enhver voksende, opad begrænset følge i G er konvergent.*

(iii) Enhver begrænset følge i G har en konvergent delfølge.

(iv) G er følgefuldstændig og arkimedisk ordnet.

BEVISet forløber efter følgende diagram: (i) $\Leftrightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv)

(i) $\Rightarrow$ (ii): Er $\alpha = (\alpha_n)$ en voksende, begrænset følge, og sættes $a = \sup\{\alpha_n \mid n \in \mathbb{N}\}$ vil α have grænseværdien a. Lad nemlig $\varepsilon \in G_+$ være givet. Da $a - \varepsilon < a$, er $a - \varepsilon$ ikke majorant for mængden $\{\alpha_n \mid n \in \mathbb{N}\}$, så der findes et $N \in \mathbb{N}$, således at $a - \varepsilon < \alpha_N$. For alle $n \geq N$ finder vi nu, da følgen er voksende, at

$$a - \varepsilon < \alpha_N \leq \alpha_n \leq a < a + \varepsilon.$$

Vi har altså $|\alpha_n - a| < \varepsilon$ for alle $n \geq N$ (▨).

(ii) $\Rightarrow$ (i): Vi føren beviset indirekte, antager altså at der findes et snit (P, Q) i G, som ikke er elementbestemt. Da P ikke har et sidste element, findes til hvert $p \in P$ et $\varepsilon > 0$, således at også $p + \varepsilon \in P$. Lad os nu først vise, at dette ε kan bestemmes således at vi yderligere har $p + 2\varepsilon \in Q$: Vi bestemmer først ε', således at $p + \varepsilon' \in P$, og betragter følgen $\alpha = (\alpha_n)$, hvor $\alpha_n = p + 2^{n-1}\varepsilon'$. Denne følge er ikke konvergent, da differensen $(\alpha_{n+1} - \alpha_n) = (2^{n-1}\varepsilon')$ åbenbart ikke er en nulfølge. Da den er voksende, slutter vi af (ii), at den ikke kan være begrænset. Specielt kan α_n ikke tilhøre P for alle n, så der må findes naturlige tal n, således at $\alpha_n \in Q$. Vi har $\alpha_1 \in P$, og vælger vi det mindste naturlige tal n, således at $\alpha_{n+1} \in Q$, finder vi $\alpha_n \in P$, $\alpha_{n+1} \in Q$, d.v.s.

$$p + 2^{n-1}\varepsilon' \in P, \quad p + 2^n\varepsilon' \in Q.$$

Med $\varepsilon = 2^{n-1}\varepsilon'$ har vi altså opnået det ønskede.

Vi starter nu med et vilkårligt element α_0 i P, og danner følger $\alpha = (\alpha_n)$, $\beta = (\beta_n)$ i G på følgende måde: Først vælges $\varepsilon_1 > 0$ i G, således at

$$\alpha_1 = \alpha_0 + \varepsilon_1 \in P, \quad \beta_1 = \alpha_0 + 2\varepsilon_1 \in Q.$$

Tilsvarende vælger vi, når $\alpha_n \in P$ er bestemt, et $\varepsilon_{n+1} > 0$, således at

$$\alpha_{n+1} = \alpha_n + \varepsilon_{n+1} \in P, \ \beta_{n+1} = \alpha_n + 2\varepsilon_{n+1} \in Q.$$

Følgen (α_n) er voksende og begrænset (f.eks. af et element i Q). I følge (ii) konvergerer den derfor mod en grænseværdi $a \in G$. Da (α_n) er konvergent, er differensen $(\varepsilon_n) = (\alpha_n - \alpha_{n-1})$ en nulfølge, og da $(\beta_n) = (\alpha_n + \varepsilon_n)$, slutter vi, at følgen (β_n) konvergerer mod den samme grænseværdi a. Hvis $a \in P$, findes et $\varepsilon > 0$, således at $a + \varepsilon \in P$, men dette strider mod, at der fra et vist trin gælder $\beta_n < a + \varepsilon$ og $\beta_n \in Q$. Og hvis $a \in Q$, findes et $\varepsilon > 0$, således at $a - \varepsilon \in Q$, men dette strider mod, at der fra et vist trin gælder $a - \varepsilon < \alpha_n$ og $\alpha_n \in P$.
Vi slutter derfor, at der må gælde $a \notin P \cup Q$, men dette er i modstrid med at der for et snit (P,Q) i G gælder $P \cup Q = G$. (☒).

(ii) ⇒ (iii): Af (ii) følger let, at også enhver begrænset, aftagende følge $\alpha = (\alpha_n)$ er konvergent, thi for en sådan følge er $-\alpha = (-\alpha_n)$ begrænset og voksende, og (α_n) vil derfor konvergere mod $-\lim_{n\to\infty}(-\alpha_n)$. For at vise (ii) ⇒ (iii). er det derfor nok at vise, at <u>enhver følge $\alpha = (\alpha_n)$ i en ordnet gruppe $(G,+,<)$ har en monoton delfølge</u>.

> Vi forsøger at udtage en voksende delfølge, og viser, at hvis forsøget mislykkes, så findes der en aftagende delfølge: Vi tager om muligt et j_1, således at der gælder $\alpha_{j_1} \leqslant \alpha_n$ for uendelig mange n. I det vi om nødvendigt erstatter α med en delfølge, kan vi antage, at der gælder $\alpha_{j_1} \leqslant \alpha_n$ for alle $n \geqslant j_1$. Vi tager nu om muligt et $j_2 > j_1$, således at der gælder $\alpha_{j_2} \leqslant \alpha_n$ for uendelig mange n. I det vi om nødvendigt erstatter α med en delfølge, kan vi antage, at der gælder $\alpha_{j_2} \leqslant \alpha_n$ for alle $n \geqslant j_2$. Hvis denne proces ikke stopper, fremkommer en

voksende delfølge (α_{j_n}) af α. Hvis processen derimod stopper efter det k-te skridt, har vi (efter eventuelt k gange at have erstattet α med delfølgen) et element α_{j_k} af følgen, således at $\alpha_{j_k} \leqslant \alpha_n$ for alle $n \geqslant j_k$. At processen ikke kan fortsættes her, betyder, at for hvert $j > j_k$ er uligheden $\alpha_j \leqslant \alpha_n$ kun opfyldt for endelig mange n. Specielt vil der så for hvert $j > j_k$ findes et $j' > j$, således at $\alpha_j > \alpha_{j'}$, men så kan vi klart udtage en (strengt) aftagende delfølge. (▨)

(iii) ⇒ (iv): Af (iii) følger let, at G er følgefuldstændig, En fundamentalfølge $\alpha = (\alpha_n)$ er nemlig begrænset, og hvis den har en konvergent delfølge, er den selv konvergent. Endvidere må G være arkimedisk ordnet. Ellers fandtes nemlig et element $\delta > 0$ i G og et element $a \in G$, således at $n\delta \leqslant a$ for alle n. Følgen $(n\delta)$ ville altså være begrænset. For alle $n \neq p$ har vi imidlertid $|n\delta - p\delta| \geqslant \delta$, og enhver delfølge af $(n\delta)$ vil have den samme egenskab. Heraf slutter vi let, at ingen delfølge af $(n\delta)$ kan være konvergent, men da $(n\delta)$ var begrænset, er dette i modstrid med (iii) (▨).

(iv) ⇒ (ii): Lad $\alpha = (\alpha_n)$ være en voksende, begrænset følge. Det er nok at vise, at $\alpha \cdot$ er en fundamentalfølge, og hertil bruger vi, at ordningen er arkimedisk. Da følgen er begrænset, kan vi finde $c_1, c_2 \in G$, således at $c_1 \leqslant \alpha_n \leqslant c_2$ for alle n. Hvis følgen ikke var en fundamentalfølge, kunne vi finde $\delta > 0$, således at der til hvert $N \in \mathbb{N}$ findes naturlige tal $j, k \geqslant N$, således at $|\alpha_j - \alpha_k| \geqslant \delta$. Vi kan så finde en delfølge (α_{j_n}) af (α_n) således at $\alpha_{j_{n+1}} - \alpha_{j_n} = |\alpha_{j_{n+1}} - \alpha_{j_n}| \geqslant \delta$. for alle n. Men så er

$$n\delta \leqslant \alpha_{j_{n+1}} - \alpha_{j_1} \leqslant c_2 - c_1 \quad \text{for alle } n,$$

i modstrid med at ordningen var arkimedisk. (▨)

▨

6.3. Som nævnt er de hele tals gruppe $(\mathbb{Z},+,<)$ fuldstændig (nemlig diskret) og arkimedisk ordnet. Gruppen $(\mathbb{Z},+,<)$ har derfor alle de i Sætning 6.2. nævnte egenskaber, hvad der naturligvis også let direkte eftervises.

Enhver diskret ordnet gruppe $(G,+,<)$ er fuldstændig. En sådan gruppe har altså de i sætning 6.2 nævnte egenskaber, hvis og kun hvis den er arkimedisk ordnet. Der gælder nu yderligere:

SÆTNING. <u>Enhver kommutativ, diskret og arkimedisk ordnet gruppe $(G,+,<)$ er kanonisk isomorf med $(\mathbb{Z},+,<)$.</u>

BEVIS. Lad ε_0 være det første element i G_+ (det mindste positive). Vi viser, at afbildningen $p \mapsto p\varepsilon_0$ af $\mathbb{Z} \to G$ er en isomorfi $(\mathbb{Z},+,<) \xrightarrow{\sim} (G,+,<)$. Det ses let, at afbildningen er en homomorfi: $(\mathbb{Z},+,<) \to (G,+,<)$. Specielt er den altså injektiv, så vi skal blot vise, at den er surjektiv. Det er nok at vise, at hvert element $a \in G_+$ tilhører billedet. Under brug af at ordningen er arkimedisk, ser vi let, at der findes et naturligt tal n, således at

$$n\varepsilon_0 \leq a < (n+1)\varepsilon_0.$$

Her må endda gælde $n\varepsilon_0 = a$, thi ellers var $0 < a - n\varepsilon_0 < (n+1)\varepsilon_0 - n\varepsilon_0 = \varepsilon_0$ i modstrid med at ε_0 var det mindste positive. □

6.4. De reelle tals ordnede gruppe $(\mathbb{R},+,<)$ er ifølge konstruktionen følgefuldstændig, og ses let at være arkimedisk ordnet. Gruppen $(\mathbb{R},+,<)$ har derfor alle de i sætning 6.2. nævnte egenskaber.

Som et mindre trivielt eksempel kan vi betragte gruppen $(\mathbb{R}_+,\cdot,<)$ af positive reelle tal med multiplikation som komposition. Ordningen er den sædvanlige ordning af reelle tal. Det ses let, at

$(\mathbb{R}_+, \cdot, <)$ er en (multiplikativt skrevet) kommutativ ordnet gruppe. Bemærk, at nok er ordningen den sædvanlige, men de "positive" elementer i denne gruppe er $\{a \in \mathbb{R}_+ \mid 1 < a\}$, og "absolutværdien" af et element a er det største af tallene a og a^{-1}. Det er klart at $(\mathbb{R}_+, \cdot, <)$ er tæt ordnet. For at vise at den har de i sætning 6.2. nævnte egenskaber, er det nok at vise, at enhver ikke-tom, opad begrænset delmængde af $\mathbb{R}_+$ har et supremum i $(\mathbb{R}_+, <)$. Denne egenskab vedrører kun ordningen, og den følger trivielt af at $(\mathbb{R}, <)$ har den tilsvarende egenskab. Vi har altså:

<u>$(\mathbb{R}_+, \cdot, <)$ er en fuldstændig, arkimedisk og tæt ordnet kommutativ gruppe.</u>

6.5. Vi skal senere se, at enhver arkimedisk og tæt ordnet, fuldstændig gruppe er isomorf med $(\mathbb{R}, +, <)$. Lad os her vise en række almindelige sætninger om arkimedisk ordnede grupper. Af definitionen følger lit, at vi i en sådan gruppe $(G, +, <)$ til hvert element $a \in G$, og hvert element $\varepsilon \in G_+$ kan bestemme et helt tal $p \in \mathbb{Z}$, således $p\varepsilon \leqslant a < (p+1)\varepsilon$.

SÆTNING. <u>Lad $v = (v_n)$ være en følge i en arkimedisk ordnet gruppe $(G, +, <)$. Hvis følgen (nv_n) er begrænset, så er følgen $v = (v_n)$ en nulfølge.</u>

BEVIS. Der findes et element $c \in G_+$, således at $|nv_n| \leqslant c$ for alle n. Lad $\varepsilon \in G_+$ være givet. Der findes et naturligt tal N, så at $c < N\varepsilon$. Når $n \geqslant N$ finder vi følgelig

$$n|v_n| = |nv_n| \leqslant c < N\varepsilon \leqslant n\varepsilon,$$

men så $|v_n| < \varepsilon$ for alle $n \geqslant N$. ▨

6.6 SÆTNING. *Enhver homomorfi $f: (G,+,<) \to (H,+,<)$ mellem arkimedisk ordnede grupper er kontinuert. Hvis $(G,+,<)$ desuden er tæt ordnet og fuldstændig, er f en isomorfi.*

BEVIS. Hvis G er diskret ordnet, er enhver afbildning fra G kontinuert. Vi kan derfor i resten af beviset antage, at G er tæt ordnet. Vi vælger et element $a_0 \in G_+$ og sætter $b_0 = f(a_0) \in H_+$. Da G er tæt ordnet, kan vi for hvert naturligt tal n bestemme et element $\delta_n \in G_+$, således at $n\delta_n \leq a_0$. Vi finder nu $0 < n f(\delta_n) \leq b_0$, og af sætning 6.5. følger der for, at følgen $(f(\delta_n))$ er en nulfølge i H. Heraf følger kontinuiteten let, thi er $\varepsilon \in H_+$ givet, kan vi bestemme et $\delta = \delta_n$ i følgen, så at $f(\delta) \leq \varepsilon$, og hvis $|x-a| < \delta$ finder vi $|f(x) - f(a)| < f(\delta) \leq \varepsilon$.

Vi antager nu yderligere, at G er fuldstændig, og skal vise, at f er en isomorfi. Da en ordenstro homomorfi er injektiv, skal vi blot vise, at f er surjektiv. Lad b være et element i H. Til hvert $n \in \mathbb{N}$ kan vi finde et $p \in \mathbb{Z}$, så at

$$p f(\delta_n) \leq b < (p+1) f(\delta_n),$$

og dermed $0 \leq b - f(p\delta_n) < f(\delta_n)$. Sætter vi $\alpha_n = p\delta_n$, får vi en følge $\alpha = (\alpha_n)$ i G, for hvilken der gælder

$$0 \leq b - f(\alpha_n) < f(\delta_n).$$

Da $(f(\delta_n))$ er en nulfølge, har følgen $(f(\alpha_n))$ i H altså grænseværdien b. Specielt er $(f(\alpha_n))$ en fundamentalfølge i H, og dette medfører – da f var en homomorfi $(G,+,<) \to (H,+,<)$ – at $\alpha = (\alpha_n)$ er en fundamentalfølge i G. Da G er fuldstændig, er $\alpha = (\alpha_n)$ altså konvergent, og da f er kontinuert, slutter vi endelig

$$b = \lim_{n\to\infty} f(\alpha_n) = f\left(\lim_{n\to\infty} \alpha_n\right),$$

og ser, at $b \in f(G)$. ▨

6.7 KOROLLAR. *Enhver homomorfi $f: (G,+,<) \to (H,+,<)$ mellem arkimedisk og tæt ordnede, fuldstændige grupper er en isomorfi.*
BEVIS. Følger umiddelbart af den foregående sætning. ▨

6.8. SÆTNING. *Enhver arkimedisk og tæt ordnet, fuldstændig gruppe $(G,+,<)$ er entydigt delelig.*
BEVIS. Vi skal vise, at afbildningen $x \mapsto px$ er en isomorfi : $(G,+) \to (G,+)$ for ethvert helt tal $p \in \mathbb{Z} \setminus \{0\}$. Hvis $p > 0$, er denne afbildning en homomorfi : $(G,+,<) \to (G,+,<)$, og hvis $p < 0$, er afbildningen en homomorfi : $(G,+,>) \to (G,+,<)$. I alle tilfælde følger påstanden af Sætning 6.7. ▨

6.9. Som nævnt (6.4) er gruppen $(\mathbb{R}_+,\cdot,<)$ arkimedisk og tæt ordnet og fuldstændig. Denne gruppe er altså entydigt delelig. Hvis $p \neq 0$, har *hvert positivt reelt tal altså en og kun én positiv p-te rod.*

Vi vil nu samle resultaterne om reelle tal.

7. De reelle tal.

7.1. Vi har tidligere defineret de reelle tals ordnede gruppe $(\mathbb{R},+,<)$ som følgekompletionen af den ordnede gruppe $(\mathbb{Q},+,<)$. De reelle tal omfatter altså de rationale tal. Endvidere har vi set, hvorledes multiplikationen i $\mathbb{Q}$ kan udvides til en kontinuert multiplikation i $\mathbb{R}$, således at $(\mathbb{R},+,\cdot,<)$ bliver et ordnet legeme, de reelle tals ordnede legeme:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}.$$

7.2. Det er klart, at $(\mathbb{R},+,<)$ er tæt ordnet. (Dette gælder for ethvert ordnet legeme). Endvidere har vi:

HOVEDSÆTNING. De reelle tals ordnede gruppe $(\mathbb{R},+,<)$ har følgende egenskaber:

(i') Enhver ikke-tom, opad begrænset delmængde har et supremum.

(i'') Enhver ikke-tom, nedad begrænset delmængde har et infimum

(i) Ethvert snit er elementbestemt.

(ii) Enhver voksende begrænset følge er konvergent.

(iii) Enhver begrænset følge har en konvergent delfølge.

(iv) Enhver fundamentalfølge er konvergent og ordningen er arkimedisk.

Enhver af disse egenskaber karakteriserer $(\mathbb{R},+,<)$ blandt de tæt ordnede kommutative grupper $(G,+,<)$. Hermed menes, at enhver tætordnet gruppe $(G,+,<)$, der har blot én af disse egenskaber, er isomorf med $(\mathbb{R},+,<)$.

BEVIS. Vi har vist (Sætning 5.3 og 6.2), at disse egenskaber er ækvivalente i enhver ordnet gruppe $(G,+,<)$. Da $(\mathbb{R},+,<)$ har den sidste egenskab (iv), vil $(\mathbb{R},+,<)$

have dem alle. Den sidste påstand er en konsekvens af følgende:

7.3. POTENSSÆTNING. Lad a være et element i en arkimedisk, tæt ordnet, fuldstændig gruppe $(G,+,<)$. Der findes da netop én kontinuert homomorfi $\varphi_a : (\mathbb{R},+) \to (G,+)$, således at $1 \mapsto a$. Hvis $a>0$, er φ_a en isomorfi : $(\mathbb{R},+,<) \xrightarrow{\sim} (G,+,<)$. Hvis $a=0$, er φ_a nulhomomorfien. Hvis $a<0$, er φ_a en isomorfi : $(\mathbb{R},+,>) \xrightarrow{\sim} (G,+,<)$.

BEVIS. (Vi antager $a>0$). Der findes netop én homomorfi $\varphi_a : (\mathbb{Q},+) \to (G,+)$, så at $1 \mapsto a$, da $(G,+)$ er entydigt delelig (Sætning 6.8, jfr. "Bøker" Potenssætning 3.8). Da $a>0$, ses det let, at φ_a er en homomorfi : $(\mathbb{Q},+,<) \to (G,+,<)$. Af sætning 6.6 følger, at φ_a er kontinuert, og vi kan derfor (Udvidelsessætning 3.6) entydigt udvide φ_a til en kontinuert homomorfi $\hat{\varphi}_a : (\mathbb{R},+,<) \to (G,+,<)$. Af sætning 6.6 følger, at φ_a er en isomorfi ☒

7.4. SÆTNING. Lad $(G,+,<)$ være en arkimedisk ordnet gruppe. Til hvert element $a \in G_+$ og hvert reelt tal $\rho \in \mathbb{R}_+$ findes netop én homomorfi : $(G,+,<) \to (\mathbb{R},+,<)$, så at $a \mapsto \rho$.

BEVIS. (Vi antager $\rho = 1$). Påstanden følger enten af Sætning 7.3 ved at betragte kompletionen:
$(G,+,<) \hookrightarrow (\hat{G},+,<) \xrightarrow[\approx]{\varphi_a^{-1}} (\mathbb{R},+,<)$, hvis ordningen er tæt, eller direkte: Entydighed. Antag, at $f : (G,+,<) \to (\mathbb{R},+,<)$ er en homomorfi med $f(a)=1$. Lad $x \in G$. Hvis $p \in \mathbb{Z}$, $n \in \mathbb{N}$, finder vi

$$pa \leq nx \Leftrightarrow pf(a) \leq nf(x) \Leftrightarrow p \leq nf(x) \Leftrightarrow \frac{p}{n} \leq f(x).$$

Heraf følger let, at

$$(*) \qquad f(x) = \sup\left\{ \frac{p}{n} \;\middle|\; p \in \mathbb{Z}, n \in \mathbb{N}, pa \leq nx \right\},$$

og dermed entydigheden.

Eksistens. Først vises, at der findes en afbildning $f: G \to \mathbb{R}$, som tilfredsstiller (*). Hertil kræves for hvert $x \in G$, at mængden $\{\frac{p}{n} \mid p \in \mathbb{Z} \wedge n \in \mathbb{N} \wedge pa \leqslant nx\} \subseteq \mathbb{R}$ er ikke-tom og opad begrænset. Dernæst vises, at denne afbildning opfylder de stillede krav. □

7.5 Som tidligere nævnt er $(\mathbb{R}_+, \cdot, <)$ en fuldstændig, tæt og arkimedisk ordnet kommutativ gruppe. Et "positivt" element i denne gruppe er et reelt tal > 1. Til hvert reelt tal $a > 1$ findes altså en og kun én homomorfi: $(\mathbb{R}_+, \cdot, <) \longrightarrow (\mathbb{R}, +, <)$, så at $a \mapsto 1$. Denne homomorfi betegnes $\log_a$. Af Sætning 6.7 følger, at $\log_a$ er en isomorfi

$$\log_a : (\mathbb{R}_+, \cdot, <) \xrightarrow{\sim} (\mathbb{R}, +, <)$$

Den inverse afbildning betegnes $\exp_a : (\mathbb{R}, +, <) \to (\mathbb{R}_+, \cdot, <)$ eller $x \longmapsto a^x$. Det ses, at denne afbildning også kan defineres ved som afbildningen φ_a i 7.3 at betragte a^x først for $x \in \mathbb{N}$, dernæst for $x \in \mathbb{Z}$, dernæst for $x \in \mathbb{Q}$ og endelig for $x \in \mathbb{R}$.
Afbildningen $\log_a$ kaldes logaritmen med grundtal a.

Af Korollar 6.7 og Sætning 7.4 følger, at enhver homomorfi $(\mathbb{R}_+, \cdot, <) \to (\mathbb{R}, +, <)$ er en logaritme.
Hvis $0 < a < 1$, sætter vi $\log_a(y) = -\log_{\frac{1}{a}}(y)$, og $\exp_a(x) = a^x = (\frac{1}{a})^{-x}$. Det ses, at $\log_a$ i dette tilfælde er en isomorfi

$$\log_a : (\mathbb{R}_+, \cdot, <) \xrightarrow{\sim} (\mathbb{R}, +, >).$$

7.6. På det udviklede grundlag kan den videre analyse af tallene bygges på velkendt måde. Lad os blot her minde om, at denne analyse tillader at vise:
SÆTNING. Ethvert polynomium af ulige grad med reelle koefficienter har en reel rod.

1. For naturlige tal $a \geq b$ defineres afbildningen $\varepsilon_{ab} : \mathbb{N}_a \to \mathbb{N}_a$ ved

$$\varepsilon_{ab}(x) = \begin{cases} x^+ & \text{hvis } x < a \\ b & \text{hvis } x = a \end{cases}, \quad x \in \mathbb{N}_a.$$

Vis, at ethvert tripel (Q, q_1, φ), der opfylder induktionsaksiomet, er isomorft med netop et af tripplerne $(\mathbb{N}, 1, \varepsilon)$, $(\mathbb{N}_a, 1, \varepsilon_{ab})$.

2. Vis, at der for enhver homomorfi $f : (\mathbb{N}, <) \to (\mathbb{N}, <)$ gælder $n \leq f(n)$ for alle n.

3. Lad $(M, \prec)$ være en (refleksivt eller irrefleksivt) ordnet mængde, og lad $f : \mathbb{N} \to M$ være en afbildning, som opfylder $f(n) \prec f(n+1)$ for alle $n \in \mathbb{N}$. Vis, at f er en homomorfi $: (\mathbb{N}, <) \to (M, \prec)$.

4. Lad $* : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ være en komposition i $\mathbb{N}$, som er distributiv m.h.t. addition og opfylder $1 * 1 = 1$. Vis, at $*$ er den sædvanlige multiplikation i $\mathbb{N}$.

5. Vis, at mængden $M = \{ n - \frac{1}{m} \mid n, m \in \mathbb{N} \}$ er velordnet ved den ordning der arves fra den sædvanlige ordning af rationale tal $[(M, <) \hookrightarrow (\mathbb{Q}, <)]$.

6. Som en konsekvens af udvalgsaksiomet kan det vises, at enhver mængde kan velordnes. Specielt findes der velordnede mængder, som hverken er endelige eller numerable. Slut heraf: Der findes en velordnet mængde $(M, \prec)$, som hverken er endelig eller numerabel, men for hvilken ethvert afsnit $M_{\prec a}$ er er endeligt eller numerabelt.

6a. Vis, at der findes en totalt ordnet mængde $(M, <)$, uden sidste element, med følgende egenskab: Enhver numerabel delmængde af M er opad begrænset [Vink: M kan endda vælges velordnet. Brug, at en numerabel forening af numerable mængder igen er numerabel].

7. Vis, at en mængde Q er endelig, hvis og kun hvis enhver injektiv afbildning $s: Q \to Q$ er bijektiv.

8. Lad $(M, *)$ være en mængde med en komposition. Vis, at der for hvert $p \in \mathbb{N}$ og hvert p-sæt $\alpha = (\alpha_1, \dots, \alpha_p) \in M^p$ findes en og kun én afbildning $\sigma: \mathbb{N}_p \to M$, således at $\sigma(1) = \alpha_1$ og $\sigma(j+1) = \sigma(j) * \alpha_{j+1}$ for alle $j < p$. Elementet $\sigma(p) \in M$ betegnes $*\alpha$ eller $\overset{*}{\underset{j=1}{\overset{p}{}}} \alpha_j$.

Hvis kompositionsforskriften er associativ, bruges også betegnelsen $\alpha_1 * \dots * \alpha_p$ for $*\alpha$. Vis, at der i dette tilfælde gælder

$$(\alpha_1 * \dots * \alpha_{q+r}) = (\alpha_1 * \dots * \alpha_q) * (\alpha_{q+1} * \dots * \alpha_{q+r}).$$

Vis hvorledes man – hvis kompositionen $*$ desuden er kommutativ – for hver endelig mængde $I \neq \emptyset$ og hver afbildning $\alpha: I \to M$ kan tillægge

$$\overset{*}{\underset{i \in I}{}} \alpha_i$$

en fornuftig mening.

9. Vis, at sætningen om definition ved rekursion ("Naturlige tal" 5.13) følger af sætningen om definition ved induktion ved at betragte triplet $(\underline{Q}, q_1, \Phi)$, hvor $\underline{Q} = Q^{\mathbb{N}}$, $q_1 = (q_1, q_1, \dots)$ og $\Phi: \underline{Q} \to \underline{Q}$ er givet ved

$$x = (x_1, x_2, \dots) \longmapsto \Phi(\underline{x}) = (x_1, \phi(x_1), \phi(x_1 x_2), \dots).$$

10. Lad M være en mængde, og lad $(G,+)$ være en kommutativ gruppe. Mængden af afbildninger $\varphi: M \to G$ betegnes G^M. For to elementer $\varphi, \psi \in G^M$ defineres $\varphi+\psi$ ved argumentvis addition: $\varphi+\psi$ er afbildningen: $x \longmapsto \varphi(x)+\psi(x)$. Vis, at $(G^M,+)$ er en kommutativ gruppe.

Delmængden af G^M bestående af de afbildninger $\varphi: M \to G$, for hvilke $\varphi(x) \neq 0$ kun gælder for endelig mange $x \in M$, betegnes $G^{(M)}$. Vis, at $G^{(M)}$ er en undergruppe i $(G^M,+)$.

11. Lad M være en mængde. For hvert $a \in M$ betegner vi med δ_a den ved

$$\delta_a(x) = \begin{cases} 0 & x \neq a \\ 1 & x = a \end{cases}$$

definerede afbildning $\delta_a: M \to \mathbb{Z}$. Det er klart, at $\delta_a \in \mathbb{Z}^{(M)}$. Vis, at hvert fra 0 forskelligt element $\varphi \in \mathbb{Z}^{(M)}$ entydigt kan skrives som en endelig sum

$$\varphi = n_1 \delta_{a_1} + \cdots + n_k \delta_{a_k}$$

hvor $a_1, \ldots, a_k$ er indbyrdes forskellige elementer i M, og $n_1, \ldots, n_k$ er hele tal $\neq 0$. Idet vi formelt i en sådan sum kan tilføje vilkårlig mange led med koefficient 0, kan hvert element $\varphi \in \mathbb{Z}^{(M)}$ altså entydigt skrives

$$\varphi = \sum_{a \in M} n_a \delta_a, \quad n_a \neq 0 \text{ kun for endelig mange } a \in M.$$

Gruppen $\mathbb{Z}^{(M)}$ kaldes den <u>fri (kommutative) gruppe frembragt af M</u>. Ofte identificeres mængden M med delmængden $\{\delta_a \mid a \in M\}$ af $\mathbb{Z}^{(M)}$. Med denne identifikation kan elementet $\varphi \in \mathbb{Z}^{(M)}$ skrives

$$\varphi = \sum_{a \in M} n_a a$$

12. Vis, at den fri gruppe $\mathbb{Z}^{(M)}$ frembragt af en mængde M har følgende egenskab: Til hver afbildning $f: M \to G$ af mængden M ind i en kommutativ gruppe $(G,\cdot)$ findes netop én homomorfi $\tilde{f}: (\mathbb{Z}^{(M)},+) \to (G,\cdot)$, således at $\tilde{f}\circ\delta = f$.

13. Lad $(H,\cdot)$ være en kommutativ semigruppe og betragt afbildningen $\delta: H \to \mathbb{Z}^{(H)}$. Denne afbildning er naturligvis ikke en homomorfi(!). Med $N \leq \mathbb{Z}^{(H)}$ betegnes den mindste undergruppe af $\mathbb{Z}^{(H)}$, som indeholder alle elementer af formen $\delta_{a\cdot b} - \delta_a - \delta_b$, $a,b \in H$. Vis, at den sammensatte afbildning

$$H \xrightarrow{\delta} \mathbb{Z}^{(H)} \xrightarrow{0} \mathbb{Z}^{(H)}/N$$

er en homomorfi af semigruppen H ind i kvotientgruppen $\mathbb{Z}^{(H)}/N$. Vis, at $\mathbb{Z}^{(H)}/N$ er isomorf med brøkgruppen $H[H^{-1}]$.

14. Lad S være en ikke-tom stabil delmængde af den additive semigruppe $(\mathbb{N},+)$. Vis, at "semi brøkgruppen" $(\mathbb{N}[-S],+)$ er isomorf med $(\mathbb{Z},+)$.

15. Vis, at der findes netop to relationer $\prec$ i $\mathbb{Z}$, således at $(\mathbb{Z},+,\prec)$ er en ordnet gruppe, nemlig den sædvanlige ordning $<$ og dens modsatte $>$.

16. Vis, at en ordnet mængde $(M,\prec)$ uden første eller sidste element, der har de i "Bróken", sætning 6.5 nævnte egenskaber, er isomorf med $(\mathbb{Z},<)$.

17. Lad c være et element i en gruppe $(G,\cdot)$. Vis, at delmængden

$$\{c^p \mid p \in \mathbb{Z}\} \subseteq G$$

er en kommutativ undergruppe i G. Den kaldes den af c frembragte cykliske undergruppe, og dens orden (= elementantal) kaldes ordenen af elementet c. Vis, at c har orden n (hvor $n \in \mathbb{N}$), hvis og kun hvis $c^n = e$ og $c^j \neq e$ når $1 \leq j < n$. Vis, at c's orden er divisor i G's orden.

18. En gruppe $(C,\cdot)$ kaldes cyklisk, hvis der findes et element $c \in C$, således at $C = \{c^p \mid p \in \mathbb{Z}\}$. Vis, at en gruppe, hvis orden er et primtal, er cyklisk, og at den kun indeholder to undergrupper, mulig de to trivielle. Vis, at enhver undergruppe i og enhver kvotientgruppe af en cyklisk gruppe igen er cyklisk.

19. Vis, at kvotientringen $\mathbb{Z}/n$, hvor $n \geqslant 1$ er et integritetsområde, hvis og kun hvis n er et primtal (jfr. "Bróken", sætning 6.7). Præcisér hvilken egenskab ved primtal, der benyttes til at vise "hvis".

20. Vis, at et endeligt integritetsområde $(A,+,\cdot)$ er et skævlegeme [Vink: For hvert $a \in A$ kan vi betragte højremultiplikationen $r_a : x \longmapsto xa$. A er et integritetsområde, hvis og kun hvis r_a er injektiv for alle $a \neq 0$ og et skævlegeme, hvis og kun hvis r_a er bijektiv for alle $a \neq 0$. Vis, at dette gælder for enhver ring $A \neq 0$. Betragt dernæst tilfældet, hvor A (som mængde) er endelig.]

21. Af opgave 19 og 20 følger, at kvotientringen $\mathbb{Z}/p$, hvor p er et primtal, er et legeme med p elementer. Dette legeme betegnes $\mathbb{F}_p$.

Lad $(A,+,\cdot)$ være et endeligt skævlegeme. Dets karakteristik kan ikke være 0 og må følgelig være et primtal p. Følgelig vil A (som primring) indeholde legemet $\mathbb{F}_p$. Vis, at antallet af elementer i A er en potens af p [Vink: udnyt, at A kan opfattes som vektorrum over legemet $\mathbb{F}_p$, og vælg en en basis].
Man kan vise, at ethvert endeligt skævlegeme er kommutativt (altså et legeme), og at der for enhver primtalspotens p^r findes et (og på isomorfi nær kun ét) legeme med p^r elementer.

22. Lad p være et primtal. Vis uden brug af resultaterne i opgave 19, 20 og 21, at enhver ring $(A,+,\cdot)$ med p elementer er et legeme isomorft med $\mathbb{Z}/p$. [Vink: Betragt højremultiplikationerne $\tau_a : x \mapsto xa$, og anvend opgave 18].

23. Lad $\rightarrow$ være en relation i en mængde M. Angiv betingelser tilstrækkelige til at sikre, at den ved

$$a_1 \rightleftharpoons a_2 \iff \exists a \in M : a_1 \rightarrow a \wedge a_2 \rightarrow a$$

definerede relation $\rightleftharpoons$ i M er en ækvivalensrelation
(Sammenlign med relationen "kan forlænges til" i $H \times S$)

24. Lad $(G_1,+,<)$ og $(G_2,+,<)$ være kommutative ordnede grupper. Produktmængden $G = G_1 \times G_2$ organiseres til en gruppe ved komponentvis addition:

$$(g_1', g_2') + (g_1'', g_2'') = (g_1' + g_1'', g_2' + g_2'').$$

Vis, at der findes en relation $<$ i G, således at $(G,+,<)$ er en ordnet gruppe, hvis positive elementer er elementerne i $\{(g_1,g_2) \mid g_1 > 0 \vee (g_1 = 0 \wedge g_2 > 0)\}$.

24 fortsat. Vis, at afbildningerne $g_1 \mapsto (g_1, 0)$ og $g_2 \mapsto (0, g_2)$ er homomorfier $(G_1, +, <) \to (G, +, <)$ og $(G_2, +, <) \to (G, +, <)$. Vis, at hvis elementerne i G_1 og G_2 identificeres med deres billeder ved disse afbildninger, så gælder i G at $(G_2)_+ < (G_1)_+$

25. Lad $(M, <)$ være en ordnet mængde og lad $(G, +, <)$ være en ordnet gruppe. Vi betragter gruppen $G^{(M)}$, jfr. opgave 10. Til hvert element $\varphi \neq 0$ i $G^{(M)}$ findes endelig mange elementer $x_1, \ldots, x_n \in M$ således at $\varphi(x_i) \neq 0$ for $i = 1, \ldots, n$, $\varphi(x) = 0$ for alle $x \notin \{x_1, \ldots, x_n\}$. Idet x_{max} (resp. x_{min}) betegner det største (resp. mindste) blandt elementerne $x_1, \ldots, x_n$ i M, sætter vi $\varphi_{max} = \varphi(x_{max})$ (resp $\varphi_{min} = \varphi(x_{min})$. Vis, at der findes en relation $<_{max}$ (resp $<_{min}$) i $G^{(M)}$, således at $(G^{(M)}, +, <_{max})$ (resp. $(G^{(M)}, +, <_{min})$) bliver en ordnet gruppe, hvis positive elementer er elementerne i

$$\{\varphi \in G^{(M)} \setminus \{0\} \mid \varphi_{max} > 0\}$$

(resp.

$$\{\varphi \in G^{(M)} \setminus \{0\} \mid \varphi_{min} > 0\}).$$

26. Gruppen $\mathbb{Z} \times \mathbb{Z}$ kan indlejres i $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$. Herved svarer elementer i $\mathbb{Z} \times \mathbb{Z}$ til "gitter"-punkter i $\mathbb{R}^2$ med heltalskoordinater, og addition i $\mathbb{Z} \times \mathbb{Z}$ svarer til sædvanlig vektoraddition. Lad t være en linie gennem $(0,0)$ i $\mathbb{R}^2$ med irrational hældningskoefficient ξ, og lad delmængden $S_\xi \subseteq \mathbb{Z} \times \mathbb{Z}$ bestå af de elementer, der opfattet som punkter i $\mathbb{R}^2$, ligger over linien t. Vis, at der findes en relation $<_\xi$ i $\mathbb{Z} \times \mathbb{Z}$, således at $(\mathbb{Z} \times \mathbb{Z}, +, <_\xi)$ er en ordnet gruppe, hvis positive elementer er elementerne i S_ξ

27. Lad $(A,+,\cdot,<)$ være en ordnet ring, og betragt polynomiumsringen $(A[X],+,\cdot)$. Vis, at den additive gruppe $(A[X],+)$ kan identificeres med gruppen $(A^{(\tilde{\mathbb{N}})},+)$ (jfr opg. 10), hvor $\tilde{\mathbb{N}} = \{0,1,2,\cdots\}$

Idet $\tilde{\mathbb{N}}$ forsynes med den sædvanlige ordning, får vi (jfr. opg. 25) ordningen $<_{max}$ og $<_{min}$ i $A[X]$. Vis, at $(A[X],+,\cdot,<_{max})$ og $(A[X],+,\cdot,<_{min})$ er ordnede ringe, og at inklusionsafbildningen $A \hookrightarrow A[X]$ definerer homomorfier $(A,+,\cdot,<) \hookrightarrow (A[X],+,\cdot,<_{max})$ og $(A,+,\cdot,<) \hookrightarrow (A[X],+,\cdot <_{min})$. Vis, at der gælder

$$0 <_{max} A_+ <_{max} X \quad (\text{"}X \text{ er uendelig stor og positiv"}) \text{ og}$$

$$0 <_{min} X <_{min} A_+ \quad (\text{"}X \text{ er uendelig lille og positiv"})$$

Undersøg hvilke af de nævnte inklusioner, der er kontinuerte, og hvorvidt multiplikationen i $A[X]$ er kontinuert m.h.t. $<_{min}$ og m.h.t. $<_{max}$.

28. Lad $(A,+,\cdot,<)$ være en kommutativ ordnet ring, og lad $(L,+,\cdot)$ være bøkleguemt for $(A,+,\cdot)$. Vis, at ordningen i A kan udvides til en ordning $<$ i L, således at $(L,+,\cdot,<)$ er et ordnet legeme.

29. Vis, at en entydigt delelig kommutativ gruppe er "det samme som" et vektorrum over $\mathbb{Q}$.

30. Betragt gupperne $\mathbb{Z}\times\mathbb{Q}$ og $\mathbb{Q}\times\mathbb{Z}$ med ordningerne definerut i opg. 24. Hvilken af gupperne er diskret ordnet. Angiv for hver af de to grupper nulfølgerne, fundamentalfølgerne, kompletionen.

31. Vis, at den ordnede gruppe $(\mathbb{Z}\times\mathbb{Z}, +, <_\xi)$ definieret i opg. 26 er tæt ordnet.

32. Lad $(M,<)$ være en ordnet mængde uden sidste element med den egenskab, at enhver numerabel delmængde af M er opadbegrænset, jfr. opg. 6a. Vis, at den ordnede gruppe $(\mathbb{Z}^{(M)}, +, <_{min})$ (opg. 25) er tæt ordnet, og at enhver nulfølge heri er konstant fra et vist trin.

33. Lad $(A,+,\cdot,<)$ være en ordnet ring, og betragt de to ordninger $<_{min}$ og $<_{max}$ i polynomiumsringen $A[X]$. Angiv for hver af de to ordninger nulfølgerne og fundamentalfølgerne.
Vis, at kompletionen af $(A[X],+,\cdot,<_{min})$ kan identificeres med ringen $A[[X]]$ af formelle potensrækker.
Kompletionen af $(A[X],+,<_{max})$ kan identificeres med en undergruppe af $(\hat{A}[X],+)$. Hvilken?

34. Vis, at gruppen $(\mathbb{Z}\times\mathbb{Z}, +, <_\xi)$, defineret i opgave 26, er arkimedisk ordnet. Vis, at den entydigt bestemte homomorfi $(\mathbb{Z}\times\mathbb{Z},+,<_\xi) \to (\mathbb{R},+,<)$, som sender $(0,1)\mapsto 1$ er givet ved

$$(x,y) \longmapsto y - x\xi.$$

35. Vis, at en arkimedisk ordnet ring $(A,+,;<)$ er kommutativ. Vis, at der findes netop en ringhomomorfi $(A,+,\cdot,<) \to (\mathbb{R},+,\cdot,<)$. Bestem alle arkimediske ordnede fuldstændige ringe.

36. Vis, at en arkimedisk og tæt ordnet, fuldstændig gruppe "er det samme som" et 1-dimensionalt vektorrum over $\mathbb{R}$ med en orientering.