

# Konstruktion af de reelle tal

Rasmus Villemoes

11. februar 2006

## Indledning

De fleste tager eksistensen af de reelle tal  $\mathbb{R}$  for givet. I Matematisk Analyse-bogen *Funktioner af en og flere variable* af Ebbe Thue Poulsen er eksistensen faktisk et postulat, og det er givetvis fornuftigt nok ikke at begynde filosofiske diskussioner angående „eksistensen og entydigheden“ af  $\mathbb{R}$  i et førsteårskursus. For den almindelige rus, og for den sags skyld også for praktiserende matematikere, er det tilstrækkeligt at vide at man *kan* konstruere et tallegeme der har de egenskaber som man – ofte ubevidst – anvender hele tiden.

Imidlertid hører det, som så meget andet, til den almene dannelse i det mindste at have set en konstruktion. Der er flere mulige tilgangsvinkler, men som vi vil se på de følgende sider, kræver en af de simpleste blot kendskab til de rationale tal samt begreberne Cauchy-følge og ækvivalensrelation. For at det ikke skal virke som om problemet blot bliver skubbet en tand, nemlig til „Hvorfor findes de rationale tal?“, starter vi med en diskussion af hvor vi har de rationale tal  $\mathbb{Q}$  fra. Denne vil lede os til at overveje hvorfor vi i det hele taget har noget vi kalder *tal*.

## Indhold

<b>1</b>	<b>Sådan begyndte det hele</b>	<b>2</b>
1.1	Aksiomatisk mængdelære . . . . .	2
1.2	De naturlige tal . . . . .	5
1.3	De hele tal . . . . .	9
1.4	De rationale tal . . . . .	10
<b>2</b>	<b>Konstruktion af de reelle tal</b>	<b>11</b>
2.1	Fuldstændighed . . . . .	13
2.2	Supremumsegenskaben . . . . .	15

## 1 Sådan begyndte det hele

Vi indleder med to citater, som gerne skulle medvirke til at sætte det følgende i perspektiv.

*Gud har skabt de hele tal, alt andet er menneskeværk.*

— Leopold Kronecker (1823–1891)

*Gud har INTET skabt. Alt andet er menneskeværk.*

— Flemming Topsøe (1938–)

Fra et matematikhistorisk synspunkt er begge disse citater interessante. I slutningen af 1800-tallet begyndte man at spekulere over fundamentet for matematikken. Der var mange problemer som man ikke anede hvordan man skulle håndtere, og efterhånden gik det op for matematikerne at et væsentligt problem var, at ingen havde en helt præcis definition af hvad et reelt tal er. Dedekind løste dette problem ved hjælp af en konstruktion, kendt som Dedekind-snit, der minder en smule om den konstruktion der præsenteres i afsnit 2 nedenfor.

Imidlertid stillede dette ikke matematikerne tilfredse, for Dedekinds arbejde krævede at man vidste hvad de rationale tal var. Det er dog ikke svært at konstruere de rationale tal ud fra de hele tal (dette er fx gjort i Algebra 1-bogen i Appendix A.2). Mange mente, at de hele tal og deres aritmetik var så velforstået og naturlig, at man ikke behøvede definere nærmere hvad man mente med  $\mathbb{Z}$ , og det er formentlig i dette lys man skal se Kroneckers udsagn.

Andre mente derimod, at når man ikke engang havde en rimelig definition af hvad en mængde er, kan man heller ikke bare tage eksistensen af en mængde med så nydelige egenskaber som  $\mathbb{Z}$  for givet. Problemer såsom det berømte Russels paradoks og andre af samme skuffe førte til forkastelsen af den såkaldte „naive mængdelære“. Der skulle andre boller på suppen.

### 1.1 Aksiomatisk mængdelære

Vejen frem var at gøre som Euklid allerede havde gjort 2000 år tidligere, nemlig at aksiomatisere teorien. Stort set al matematik i dag bygger på, eller kan bygges på, Zermelo-Fraenkels aksiomer for mængdelæren, kendt som ZF. Hvis man inkluderer udvalgsaksiomet omtales systemet ofte som ZFC.

Det vil føre for vidt at give en grundig omtale af aksiomerne i ZFC, da dette blandt andet ville kræve en lang udredning om førsteordens-logik

og masser af andre spidsfindigheder, som undertegnede på ingen måde vil påstå at kende nok til. Men for at tilfredsstille læserens nysgerrighed er aksiomerne her. I ZF er *alt* mængder, inklusiv elementerne i mængderne. Derfor skal udsagn som  $\forall A \exists B$  læses som „For enhver mængde  $A$  gælder at der findes en mængde  $B$  således at...“.

**Aksiom 1** (Udvidelse). *To mængder er ens hvis og kun hvis de har de samme elementer.*

$$\forall A \forall B : A = B \iff (\forall C : C \in A \iff C \in B)$$

**Aksiom 2** (Tom mængde). *Der findes en mængde uden elementer.*

$$\exists \emptyset \forall A : \neg(A \in \emptyset)$$

Bemærk at Aksiom 1 medfører, at den tomme mængde er entydigt bestemt. Thi hvis  $\forall C : \neg(C \in \emptyset)$  og  $\forall C : \neg(C \in \emptyset')$  følger det klart at  $\emptyset = \emptyset'$ . Derfor er det meningsfyldt at snakke om *den* tomme mængde.

**Aksiom 3** (Parring). *For vilkårlige to mængder  $A$  og  $B$  findes der en mængde der indeholder netop  $A$  og  $B$  som elementer.*

$$\forall A \forall B \exists C \forall D : D \in C \iff (D = A \vee D = B)$$

**Aksiom 4** (Forening). *For enhver mængde  $A$  findes der en mængde  $B$ , således at elementerne i  $B$  netop er elementerne i  $A$ .*

$$\forall A \exists B \forall C : C \in B \iff (\exists D : C \in D \wedge D \in A)$$

**Aksiom 5** (Uendelig). *Der findes en mængde  $N$ , således at den tomme mængde er element i  $N$ , og så det for ethvert element  $A$  i  $N$  gælder at  $A \cup \{A\}$  er element i  $N$ .*

$$\exists N : \emptyset \in N \wedge (\forall A : A \in N \implies A \cup \{A\} \in N)$$

Her er aksiomet om parring, Aksiom 3, underforstået anvendt til at konstruere singletonmængden  $\{A\}$  (overvej!). Dernæst er det samme aksiom anvendt til at konstruere mængden  $\{A, \{A\}\}$ , og endelig er aksiomet om forening, Aksiom 4, anvendt til at danne mængden  $A \cup \{A\}$ . Som det vil fremgå af afsnit 1.2 nedenfor er det ikke tilfældigt at jeg har anvendt bogstavet  $N$  om denne mængde.

**Aksiom 6** (Potensmængde). *For enhver mængde  $A$  findes der en mængde  $B$ , hvis elementer netop er delmængderne af  $A$ .*

$$\forall A \exists B \forall C : C \in B \iff (\forall D : D \in C \implies D \in A)$$

Dette  $B$  er entydigt bestemt, så det er rimeligt at betegne det  $\mathcal{P}(A)$  eller  $2^A$  og kalde det potensmængden af  $A$ . Thi hvis  $B$  og  $B'$  opfylder betingelsen har vi at

$$\forall C : C \in B \iff (\forall D : D \in C \implies D \in A) \iff C \in B'$$

og ifølge Aksiom 1 medfører dette at  $B = B'$ .

**Aksiom 7** (Regularitet). *Enhver ikke-tom mængde  $A$  indeholder et element  $B$  således at  $A$  og  $B$  er disjunkte.*

$$\forall A : A \neq \emptyset \implies \exists B : B \in A \wedge \neg(\exists C : C \in A \wedge C \in B)$$

Dette aksiom har blandt andet som konsekvens, at ingen mængde kan være element i sig selv. Thi hvis  $A$  er en sådan mængde, kan vi konstruere mængden  $B = \{A\}$  jf. Aksiom 3. Ifølge regularitetsaksiomet skal  $B$  indholde et element således at  $B$  er disjunkt fra dette element. Da det eneste element i  $B$  er  $A$ , er vi tvunget til at vælge dette. Men  $A$  er netop ikke disjunkt fra  $B$ , da begge mængder jo indeholder  $A$ ! Derfor kan  $A$  ikke findes.

**Aksiom 8** (Delmængde). *Givet en mængde  $A$  og en proposition  $P$ , findes der en delmængde  $B$  af  $A$  bestående af netop de elementer  $C$  for hvilke  $P(C)$  er sand.*

$$\forall A \exists B \forall C : C \in B \iff (C \in A \wedge P(C))$$

Det næstsidste aksiom kræver en lille omformulering af hvad vi normalt forstår ved en *afbildning*. Nedenfor er en afbildning et udsagn  $P(\cdot, \cdot)$ , så der for ethvert  $X$  man måtte finde på at stikke ind på første plads findes netop et  $Y$  således at  $P(X, Y)$  er sand. I symboler lyder dette

$$\forall X : (\exists Y : P(X, Y)) \wedge (\forall Y_1 \forall Y_2 : P(X, Y_1) \wedge P(X, Y_2) \implies Y_1 = Y_2).$$

**Aksiom 9** (Udskiftning). *Lad  $P$  være en afbildning. For enhver mængde  $A$  findes der en mængde  $B$  bestående af „billederne“ af  $A$  under  $P$ .*

$$\forall A \exists B \forall C : C \in B \iff (\exists D : D \in A \wedge P(D, C))$$

**Aksiom 10** (Udvalgsaksiomet). *For enhver mængde bestående af indbyrdes disjunkte, ikke-tomme mængder, findes der en mængde der har netop et element tilfælles med hver af de ikke-tomme mængder.*

Det er noget rod at skrive dette sidste udsagn med kvantorer, men vi kan prøve at bryde det op i mindre dele. At  $A$  består af ikke-tomme, indbyrdes disjunkte mængder kan vi skrive

$$(\forall B : B \in A \implies (\exists C : C \in B)) \wedge \\ (\forall B_1 \forall B_2 : B_1 \in A \wedge B_2 \in A \implies ((\exists C : C \in B_1 \wedge C \in B_2) \implies B_1 = B_2))$$

Første linje betyder klart at elementerne i  $A$  er ikke-tomme mængder. Den anden linje skal læses som følger: Hvis  $B_1$  og  $B_2$  er elementer i  $A$ , så gælder det at [hvis der findes et element  $C$  som er element i  $B_1$  og  $B_2$ , så er  $B_1 = B_2$ ], og udtrykker netop at mængderne er disjunkte. Lad os kalde hele denne smøre for  $(*)$ . Indtil videre har vi altså at  $\forall A : (*) \implies \exists D$ , hvor  $D$  er den mængde der påstås at findes. Det vi mangler nu er at udtrykke egenskaberne ved  $D$  ved hjælp af kvantorer. Et bud ville være

$$\forall B : B \in A \implies ((\exists C : C \in B \wedge C \in D) \wedge \\ (\forall C_1, C_2 : C_1, C_2 \in B \wedge C_1, C_2 \in D \implies C_1 = C_2))$$

hvor  $\forall C_1, C_2$  naturligvis er en forkortelse for  $\forall C_1 \forall C_2$ , og hvor  $C_1, C_2 \in B$  tilsvarende er en forkortelse for  $C_1 \in B \wedge C_2 \in B$ ; ligeså for  $C_1, C_2 \in D$ . Hvis vi kalder denne smøre for  $(**)$  er udvalgsaksiomet nu det simple udsagn

$$\forall A : (*) \implies (\exists D : (**)).$$

De ovenstående aksiomer sætter en i stand til at udføre alle de operationer vi er vant til på mængder, såsom forening, snit, relativt komplement og ikke mindst Cartesisk produkt. Herved er det også muligt at give mening til hvad vi forstår ved en funktion  $f$  fra en mængde  $X$  til en mængde  $Y$ . En måde at definere det på er at  $f$  er en tripel  $f = (X, F, Y)$  hvor  $F$  er en vis delmængde af  $X \times Y$ , med den egenskab at  $\forall x \in X \exists ! y \in Y : (x, y) \in F$ .

## 1.2 De naturlige tal

Udstyret med ZF (og gerne C) er vi i stand til at konstruere mængden af naturlige tal. Oven i hatten er vi i stand til at udstyre denne mængde med operationerne  $+$  og  $\cdot$ , og når først dette er på plads er der ikke så langt til notens egentlige mål, de reelle tal.

En berømt model for de naturlige tal er Peanos aksiomer. De lyder i al sin enkelhed

- (1) Der findes et naturligt tal 0.

- (2) Ethvert naturligt tal  $a$  har en efterfølger,  $S(a)$ .
- (3) Der er intet naturligt tal hvis efterfølger er 0.
- (4) Forskellige naturlige tal har forskellige efterfølgere;  $a \neq b \implies S(a) \neq S(b)$ .
- (5) Hvis 0 har en given egenskab, og efterfølgeren til ethvert naturligt tal som har den givne egenskab også har den givne egenskab, så haves egenskaben af samtlige naturlige tal.

Ovenstående er naturligvis kun aksiomer, og vi har endnu ikke vist at der findes noget der fortjener navnet „de naturlige tal“. Vi definerer en *Dedekind-Peano-struktur* som en tripel  $(X, x, f)$  som opfylder

- (1)  $X$  er en mængde,  $x \in X$  og  $f$  er en afbildning  $X \rightarrow X$ .
- (2)  $x$  tilhører ikke billedet af  $f$ .
- (3)  $f$  er injektiv.
- (4) Hvis  $A$  er en delmængde af  $X$  som opfylder  $x \in A$  og  $a \in A \implies f(a) \in A$ , så er  $A = X$ .

Vi vil bevise eksistensen af en sådan struktur, og vise at den opfylder Peanos aksiomer. Lad  $F$  betegne funktionen, som til en mængde  $a$  knytter mængden  $a \cup \{a\}$ . En mængde  $A$  kaldes *induktiv* hvis  $a \in A \implies F(a) \in A$ . Definer  $0 = \{\} = \emptyset$ . Aksiom 5 fortæller altså præcis at der findes en induktiv mængde som indeholder 0; lad  $\mathbb{N}$  betegne den mindste sådanne. At man faktisk kan give mening til fællesmængden af alle induktive mængder som indeholder 0 er måske ikke helt oplagt, men ikke desto mindre sandt. Endelig lader vi  $S$  betegne restriktionen af  $F$  til  $\mathbb{N}$ ; idet  $\mathbb{N}$  er induktiv er  $S$  en afbildning  $\mathbb{N} \rightarrow \mathbb{N}$ .

Ligesom vi indførte speciel notation for  $\emptyset$  bruger man som bekendt symbolerne  $1, 2, 3, \dots$  for

$$\begin{aligned} 1 &= S(0) = 0 \cup \{0\} = \{0\} \\ 2 &= S(1) = 1 \cup \{1\} = \{0, 1\} = \{\emptyset, \{\emptyset\}\} \\ 3 &= S(2) = 2 \cup \{2\} = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \end{aligned}$$

Påstanden er nu, at  $(\mathbb{N}, 0, S)$  er en Dedekind-Peano-struktur, kaldet *systemet af naturlige tal*. Punkt (1) er oplagt, og ligeså oplagt er det at  $0 = \emptyset \neq S(a) = a \cup \{a\}$  for ethvert  $a \in \mathbb{N}$ , så også (2) er opfyldt.

Punkt (3) kræver en lille overvejelse. Hvis  $S(a) = a \cup \{a\} = b \cup \{b\} = S(b)$  skal vi vise at  $a = b$ . Lad  $c \in a$ . Vi skal så vise at  $c \in b$ . Da  $c \in a \cup \{a\} = b \cup \{b\}$  er der to muligheder; enten  $c \in b$  eller  $c = b$ . I det første tilfælde er vi færdige. Hvis ikke har vi altså  $c = b \in a$ . Men hvis  $b \in a$  kan vi ikke have at  $a \in b$ , fordi det ville stride med regularitetsaksiomet (man kan vise at dette medfører at der for enhver mængde  $x_0$  ikke kan findes en uendelig kæde  $\dots \in x_2 \in x_1 \in x_0$ ), altså  $a \notin b$ . Men da  $a \in a \cup \{a\} = b \cup \{b\}$  må vi så have at  $a \in \{b\}$ , hvilket præcis vil sige at  $a = b$ . Dette viser at  $a \subseteq b$ , og pr. symmetri har vi også at  $b \subseteq a$ .

Antag nu endelig, at  $A \subseteq \mathbb{N}$  opfylder  $0 \in A$  og  $a \in A \implies S(a) \in A$ . Disse antagelser betyder præcis at  $A$  er en induktiv mængde som indeholder 0, så pr. definition er  $\mathbb{N} \subseteq A$ ; således er  $A = \mathbb{N}$  og  $(\mathbb{N}, 0, S)$  er en Dedekind-Peano-struktur.

Bemærk at vi ikke blot har fået konstrueret os en stor mængde, men at den faktisk kommer forsynet med en masse struktur; nok til at vi kan definere regneoperationerne  $+$  og  $\cdot$ .

Vi lader  $a+0 = a$  for alle  $a \in \mathbb{N}$ , og definerer rekursivt  $a+S(b) = S(a+b)$  for  $a, b \in \mathbb{N}$ . Nedenfor viser jeg, at  $(\mathbb{N}, +)$  bliver en såkaldt kommutativ monoide (en „gruppe“ hvor man dropper kravet om eksistensen af inverse).

Tilsvarende defineres multiplikation ved hjælp af addition; vi lader  $a \cdot 0 = 0$  og  $a \cdot S(b) = a \cdot b + a$  for  $a, b \in \mathbb{N}$ . Hvis man har god tid kan man sætte sig ned og bevise at  $\cdot$  er kommutativ, og at den distributive lov  $(a+b) \cdot c = (a \cdot c) + (b \cdot c)$  gælder.

Endelig giver  $S$  anledning til en total ordning på  $\mathbb{N}$ . Vi siger at  $a \leq b$  hvis der findes et naturligt tal  $c$  således at  $c + a = b$ . Heraf følger klart at  $0 \leq b$  for alle naturlige tal  $b$ , og at  $b \leq 0 \implies b = 0$ .

Her følger et par yderst nyttige lemmaer, som tilsammen blandt andet viser påstanden om at  $(\mathbb{N}, +)$  er en kommutativ monoide. Bemærk specielt at jeg undervejs viser at  $0 + a = a$ ; et faktum som ikke er oplagt fra definitionen af  $+$ .

**Lemma 1.1** (Associativitet). *For alle naturlige tal  $a, b$  og  $c$  gælder, at  $(a+b)+c = a+(b+c)$ .*

*Bevis.* Lad  $a$  og  $b$  være givne tal, og lad  $C$  betegne delmængden af de naturlige tal bestående af de tal  $c$  for hvilke  $(a+b)+c = a+(b+c)$ . Vi har så at  $(a+b)+0 = a+b$  og  $a+(b+0) = a+b$  pr. definition af  $+$ , så vi ser at  $0 \in C$ . Antag nu at  $c \in C$ . Så har vi at  $(a+b)+S(c) = S((a+b)+c) = S(a+(b+c)) = a+S(b+c) = a+(b+S(c))$ , hvilket beviser at  $S(c) \in C$ . Men disse to ting medfører tilsammen at  $C = \mathbb{N}$ .  $\square$

Man kan også relativt let overbevise sig om at  $+$  er kommutativ. Vi deler det op i to lemmaer.

**Lemma 1.2.** *For alle naturlige tal  $a, b$  gælder at  $a + S(b) = S(a) + b$ .*

*Bevis.* Som man nok forventer lader vi  $a$  være et givet naturligt tal, og lader  $B$  betegne mængden af de  $b$  for hvilke  $a + S(b) = S(a) + b$ . Vi har at  $a + S(0) = S(a + 0) = S(a) = S(a) + 0$ , så  $0 \in B$ . Antag  $b \in B$ . Så har vi altså at  $a + S(b) = S(a) + b$ . Vi beregner så

$$a + S(S(b)) = S(a + S(b)) = S(S(a) + b) = S(a) + S(b) \quad (1)$$

hvilket viser at  $S(b) \in B$ . Således er  $B = \mathbb{N}$  og vi er færdige.  $\square$

**Lemma 1.3** (Kommutativitet). *For alle naturlige tal  $a, b$  gælder at  $a + b = b + a$ .*

*Bevis.* Beviset er lige ud af landevejen, når først man kender melodien. Vi viser først at  $0$  kommuterer med alting, altså at  $a + 0 = 0 + a$  for alle naturlige tal  $a$ . For  $a = 0$  er det klart. Antag nu at  $0$  kommuterer med  $a$ . Så har vi at  $S(a) + 0 = a + S(0) = S(a + 0) = S(0 + a) = 0 + S(a)$ , hvilket viser at  $0$  kommuterer med  $S(a)$ . Altså kommuterer  $0$  med alle naturlige tal.

Lad  $a$  være et givet naturligt tal, og lad  $B$  betegne mængden af de  $b$  for hvilke  $a + b = b + a$ . Vi har så lige vist at  $0 \in B$ . Antag nu at  $b \in B$ . Så har vi at  $a + S(b) = S(a + b) = S(b + a) = b + S(a) = S(b) + a$ , hvor det sidste lighedstegn følger af Lemma 1.2. Dette viser at  $S(b) \in B$ , og dermed at  $B = \mathbb{N}$ .  $\square$

**Lemma 1.4** (Forkortning). *For alle naturlige tal  $a, b$  og  $x$  gælder der, at hvis  $a + x = b + x$ , så er  $a = b$ .*

*Bevis.* Lad  $a$  og  $b$  være givne naturlige tal. Vi lader  $A$  betegne mængden af de naturlige tal  $x$  for hvilke

$$a + x = b + x \implies a = b. \quad (2)$$

Det er klart at  $0 \in A$ , for hvis  $a + 0 = b + 0$  følger fra definitionen af  $+$  at  $a = b$ . Antag nu  $x \in A$ , og at  $a + S(x) = b + S(x)$ . Pr. definition af  $+$  er dette det samme som  $S(a + x) = S(b + x)$ , og da  $S$  er injektiv følger heraf at  $a + x = b + x$ . Men da  $x \in A$  følger så at  $a = b$ , hvilket viser at  $S(x) \in A$ . Altså er  $A = \mathbb{N}$ .  $\square$

Det overlades nu til læseren at vise den associative lov for multiplikation,  $a(bc) = (ab)c$ , den distributive lov  $a(b + c) = ab + ac$  samt at multiplikation er kommutativ,  $ab = ba$ .

### 1.3 De hele tal

Næste trin er at konstruere ringen af hele tal. Betragt mængden  $\mathbb{N} \times \mathbb{N}$  bestående af alle ordnede par af naturlige tal. Ideen er at repræsentere et helt tal som  $(a, b)$ , hvor  $a$  er den „positive“ del og  $b$  er den „negative“ del. Fx vil vi skrive tallet  $-2$  som  $(0, 2)$ . Et talpar såsom  $(7, 3)$  skal tolkes som  $7 - 3 = 4$ , og skal således betragtes som det samme tal som  $(4, 0)$ . Vi er med andre ord ude efter en *ækvivalensrelation* på mængden  $\mathbb{N} \times \mathbb{N}$ . Vi vil betragte to talpar  $(a, b)$  og  $(a', b')$  som ækvivalente hvis  $a - b = a' - b'$ . Problemet med denne definition er at den ikke giver mening; minus er ikke en veldefineret operation på  $\mathbb{N}$ , og så meget desto mindre kan vi spørge om de to differenser er ens. Løsningen er at „flytte over“, og vi definerer altså nu

$$(a, b) \sim (a', b') \iff a + b' = a' + b.$$

At dette er en ækvivalensrelation er på ingen måde svært at se; det følger direkte af at  $=$  på  $\mathbb{N}$  er en ækvivalensrelation.

Definer nu mængden  $\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim$ . Vi ønsker at udvide  $+$  og  $\cdot$  til at være binære operationer på denne mængde. Som man måske kan gætte foregår addition ved koordinatvis addition af repræsentanter:

$$[(a, b)] + [(c, d)] = [(a + c, b + d)]$$

Hvis bare vi kan vise at dette er veldefineret, følger associativitet og kommutativitet direkte af de tilsvarende egenskaber for  $+$  på  $\mathbb{N}$ . Så antag nu at  $(a, b) \sim (a', b')$  og  $(c, d) \sim (c', d')$ . Disse antagelser betyder at  $a + b' = a' + b$  og  $c + d' = c' + d$ , og lægger vi disse identiteter sammen får vi  $a + c + b' + d' = a' + c' + b + d$  (her benytter jeg at  $+$  er kommutativ til at flytte lidt rundt på leddene, og at  $+$  er associativ til at undlade at sætte parenteser), hvilket lige præcis betyder at  $(a + c, b + d) \sim (a' + c', b' + d')$ . Altså er  $+$  veldefineret.

Nu kan man så bevise at  $(\mathbb{Z}, +)$  er en gruppe. Associativitet følger som sagt let fra det faktum at  $(\mathbb{N}, +)$  er en monoide. Neutralelementet er  $[(0, 0)]$ , hvilket også er let at indse. Det inverse element til  $[(a, b)]$  er  $[(b, a)]$ , idet  $[(a, b)] + [(b, a)] = [(a + b, b + a)] = [(0, 0)]$ .

Man kan næsten gætte sig til hvordan multiplikation skal defineres. Da  $(a - b)(c - d) = ac + bd - (ad + bc)$  ledes man naturligt til at definere

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

Man skal naturligvis igen vise at dette er veldefineret. Antagelserne er altså at

$$a + b' = a' + b \qquad c + d' = c' + d$$

Den første af disse ligninger ganges igennem med henholdsvis  $c$  og  $d$ , og den anden med henholdsvis  $b'$  og  $a'$ , hvilket giver (jeg har vendt ligning 2 og 3 om)

$$\begin{array}{ll} ac + b'c = a'c + bc & b'c' + b'd = b'c + b'd' \\ a'd + bd = ad + b'd & a'c + a'd' = a'c' + a'd' \end{array}$$

Lægges alle fire ligninger sammen får man

$$\begin{aligned} ac + b'c + b'c' + b'd + a'd + bd + a'c + a'd' \\ = a'c + bc + b'c + b'd' + ad + b'd + a'c' + a'd'. \end{aligned}$$

Ser man efter kan man bruge Lemma 1.4 til at forkorte fire led bort på hver side, og tilbage står

$$ac + bd + a'd' + b'c' = a'c' + b'd' + ad + bc$$

hvilket præcis betyder at  $(ac + bd, ad + bc) \sim (a'c' + b'd', a'd' + b'c')$ , så multiplikation i  $\mathbb{Z}$  er veldefineret. Man kan nu slavisk tjekke de sædvanlige aksiomer for en ring; fx er 1-elementet  $[(1, 0)]$ .

## 1.4 De rationale tal

Det er et generelt faktum, som man også ser i Algebra 1, at hvis man har en ring  $R$  som er et integritetsområde (kommutativ ring uden nuldivisorer), kan man konstruere brøkleget  $Q(R)$  af ringen. Det er et legeme med den universelle egenskab, at der findes en entydig injektiv ringhomomorfi  $\varphi: R \rightarrow Q(R)$ , og så enhver injektiv ringhomomorfi fra  $R$  til et legeme  $K$  faktoriserer entydigt igennem  $\varphi$ .

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & Q(R) \\ & \searrow & \vdots \\ & & K \end{array}$$

I en vis forstand er  $Q(R)$  altså det mindste legeme der indeholder  $R$  som delring. Et standardargument viser at hvis  $Q'(R)$  er et andet legeme med ovenstående universelle egenskab, så er  $Q(R)$  og  $Q'(R)$  på kanonisk vis isomorfe som ringe.

Konstruktionen af  $Q(R)$  ud fra  $R$  er ret ligetil. Man skal blot lægge en passende ækvivalensrelation på mængden  $R \times (R - \{0\})$  og derefter indse at

addition og multiplikation kan defineres fornuftigt. Afbildningen  $\varphi$  definerer næsten sig selv, og den universelle egenskab følger også ganske trivielt.

Det overlades til læseren selv at udføre de nødvendige trin, eller at slå det op i Algebra 1-bogen hvordan det gøres. Vi lader altså  $\mathbb{Q} = Q(\mathbb{Z})$ .

## 2 Konstruktion af de reelle tal

De rationale tal  $\mathbb{Q}$  er et totalt ordnet legeme, altså et legeme forsynet med en total ordning kompatibel med regneoperationerne i legemet. Alligevel er  $\mathbb{Q}$  i mange sammenhænge ikke god nok. Fx er der ikke ret mange rationale tal som har kvadratrødder. Mere generelt har  $\mathbb{Q}$  den skavank, at talfølger som „burde“ konvergere ikke er konvergente; fx monotone begrænsede følger.

Udvidelserne  $\mathbb{N} \rightsquigarrow \mathbb{Z}$  og  $\mathbb{Z} \rightsquigarrow \mathbb{Q}$  er sket ved at betragte mængden af par  $(a, b)$  og forsyne denne med en ækvivalensrelation, hvorefter operationerne  $+$  og  $\cdot$  er defineret på den nye og større mængde. Imidlertid ved vi jo godt at vi prøver at konstruere en overtællelig mængde, så det kan ikke nytte at prøve at starte med mængden  $\mathbb{Q} \times \mathbb{Q}$  og lave en ækvivalensrelation på denne, så lad os i stedet hive fat i de følger som bør konvergere.

En Cauchy-følge er som bekendt en talfølge  $\{a_n\}_{n=0}^{\infty}$  som opfylder betingelsen

$$\forall \varepsilon > 0 \exists N \in \mathbb{N} \forall m, n \in \mathbb{N} : m, n \geq N \implies |a_m - a_n| < \varepsilon \quad (3)$$

Bemærk at denne definition af Cauchy-følge giver mening, selvom vi ikke endnu har defineret mængden af reelle tal. Det  $\varepsilon$  der optræder skal man blot tænke på som et rationalt tal. På tilsvarende vis kan man sagtens snakke om konvergens af rationale talfølger uden at kende til de reelle tal;  $\{a_n\}_{n=0}^{\infty}$  siges at være konvergent hvis

$$\exists a \in \mathbb{Q} \forall \varepsilon > 0 \exists N \in \mathbb{N} \forall n \in \mathbb{N} : n \geq N \implies |a - a_n| < \varepsilon. \quad (4)$$

Hvis et sådant  $a$  findes er det let at vise at det er entydigt, og kaldes derfor *grænseværdien* af følgen.

Det er let at overbevise sig om at en konvergent følge er en Cauchy-følge (det følger af trekantsuligheden), men inden for de rationale tal er det omvendte som bekendt ikke tilfældet. Fx er

$$a_n = \sum_{k=0}^n 1/k!$$

en Cauchy-følge af rationale tal som ikke er konvergent (inden for  $\mathbb{Q}$ ).

Vi kan imidlertid benytte os af Cauchy-følger til at konstruere en model for de reelle tal. Betragt mængden  $M = \mathbb{Q}_c^{\mathbb{N}}$  af Cauchy-følger af rationale tal. Her betegner  $\mathbb{Q}^{\mathbb{N}}$  mængden af afbildninger  $\mathbb{N} \rightarrow \mathbb{Q}$  (en følge er formelt en sådan afbildning), og subscriptet  $c$  antyder at vi betragter den delmængde som opfylder betingelsen (3). Ideen er at lade en Cauchy-følge repræsentere „det reelle tal som den konvergerer imod“. Nu findes der jo i almindelighed mange Cauchy-følger som konvergerer mod et givet reelt tal, så vi har brug for en ækvivalensrelation  $\sim$  på  $M$  der fortæller hvornår to Cauchy-følger repræsenterer det samme reelle tal. Definitionen er så ligetil som den næsten kan være. Hvis  $a = \{a_n\}$  og  $b = \{b_n\}$  er to Cauchy-følger skriver vi  $a \sim b$  hvis følgen  $a - b = \{a_n - b_n\}$  er *konvergent* mod 0, altså hvis

$$\forall \varepsilon > 0 \exists N \in \mathbb{N} \forall n \in \mathbb{N} : n \geq N \implies |a_n - b_n| < \varepsilon.$$

Det er umiddelbart klart at  $\sim$  er reflektiv, da  $a - a = \{0\}$  oplagt er konvergent mod 0. Symmetri af  $\sim$  er lige så oplagt da  $|a_n - b_n| = |b_n - a_n|$ . Transitiviteten følger af, at hvis  $a, b, c$  er tre Cauchy-følger hvor  $a - b$  og  $b - c$  konvergerer mod 0, da vil summen  $(a - b) + (b - c) = a - c$  også være en konvergent følge med grænseværdi 0.

Det giver derfor nu mening at definere  $\mathbb{R} = M/\sim$ . Tilbage er at definere regneoperationer på  $\mathbb{R}$ , vise at  $\mathbb{R}$  er et legeme, udstyre  $\mathbb{R}$  med en ordning samt ikke mindst vise at  $\mathbb{R}$  er fuldstændig i den forstand at Cauchyfølger er konvergente.

Det er ganske ligetil at definere regneoperationerne. Lad  $a = \{a_n\}$  og  $b = \{b_n\}$  være to Cauchy-følger af rationale tal, og lad  $[a], [b]$  betegne deres ækvivalensklasser i  $\mathbb{R}$ . Da defineres  $[a] + [b] = [\{a_n + b_n\}]$ . Her er der to ting at vise; for det første at den koordinatvise sum af to Cauchy-følger igen er en Cauchy-følge, samt at definitionen ikke afhænger af valgene af repræsentanter for  $[a], [b]$ .

Vi har at  $|a_n + b_n - (a_m + b_m)| = |a_n - a_m + b_n - b_m| \leq |a_n - a_m| + |b_n - b_m|$ , og da begge disse led kan vurderes mindre end et givet  $\varepsilon$  for  $n, m$  store nok, er summen af to Cauchy-følger altså en Cauchy-følge.

Antag nu at  $[a] = [a']$  og  $[b] = [b']$ , altså at  $a_n - a'_n$  og  $b_n - b'_n$  konvergerer mod 0. Så har vi at også følgen  $a_n + b_n - (a'_n + b'_n)$  konvergerer mod 0, men det vil lige præcis sige at  $[a] + [b] = [a + b] = [a' + b'] = [a'] + [b']$ . Altså er  $+$  veldefineret, og det er ganske åbenlyst at  $(\mathbb{R}, +)$  er en gruppe.

Multiplikation defineres også som man forventer det, nemlig ved  $[a][b] = [\{a_n \cdot b_n\}]$ . Igen skal man tjekke at produktet af to Cauchy-følger er en Cauchy-følge, dette overlades til læseren. At produktet er veldefineret følger

af at

$$\begin{aligned} |a_n b_n - a'_n b'_n| &= |a_n(b_n - b'_n) + (a_n - a'_n)b'_n| \\ &\leq |a_n(b_n - b'_n)| + |(a_n - a'_n)b'_n|. \end{aligned}$$

Følgen  $b_n - b'_n$  konvergerer pr. antagelse mod 0. Da  $a$  er en Cauchy-følge er den begrænset, så også produktet  $a_n(b_n - b'_n)$  konvergerer mod 0, og tilsvarende for det andet led. Hvis man regner efter ser man at  $\mathbb{R}$  bliver en ring.

Den skarpsindige læser har måske bemærket, at det vi egentlig har vist er at  $M$  er en ring (med hensyn til de koordinatvise operationer), og at mængden af Cauchy-følger som er konvergente med grænseværdi 0 udgør et ideal i denne ring.

For at indse at  $\mathbb{R}$  er et legeme skal man gøre sig en observation angående Cauchy-følger af rationale tal som ikke repræsenterer 0 i  $\mathbb{R}$ : En sådan Cauchy-følge er forskellig fra 0 fra et vist trin. Når man har overbevist sig om dette er det ikke svært at konstruere det inverse element til  $[a] \neq 0$ .

Den totale ordning  $\geq$  på  $\mathbb{Q}$  udvides til  $\mathbb{R}$  som følger: Vi siger at  $x \geq 0$  hvis  $x$  har en repræsentant  $\{a_n\}$  hvor de rationale tal  $a_n$  fra et vist trin er  $\geq 0$ , og vi skriver  $x \geq y$  hvis  $x - y \geq 0$ . Man kan overbevise sig om at denne ordning er kompatibel med regneoperationerne (såsom at  $x \geq y \implies x + z \geq y + z$  for alle reelle tal  $x, y, z$ ), og at  $\geq$  er en total ordning.

## 2.1 Fuldstændighed

Det påstås nu at  $\mathbb{R}$  er fuldstændig, i den forstand at enhver følge  $\{x_n\}_{n=0}^{\infty}$  af reelle tal som opfylder betingelsen

$$\forall \varepsilon > 0 \exists N \in \mathbb{N} \forall m, n \in \mathbb{N} : m, n \geq N \implies |x_n - x_m| < \varepsilon$$

er konvergent, altså opfylder at der findes et reelt tal  $x$  således at

$$\forall \varepsilon > 0 \exists N \in \mathbb{N} \forall n \in \mathbb{N} : n \geq N \implies |x - x_n| < \varepsilon.$$

For at vise dette skal vi først have et par lemmaer der giver os frihed til at vælge andre repræsentanter for et givet reelt tal.

**Lemma 2.1.** *Lad  $\{a_n\}$  være en Cauchy-følge af rationale tal, og lad  $\{a_{k_n}\}_{n=1}^{\infty}$  være en delfølge (dvs.  $k_1 < k_2 < k_3 < \dots$  er en voksende følge af naturlige tal). Så repræsenterer  $\{a_n\}$  og  $\{a_{k_n}\}$  samme reelle tal.*

*Bevis.* Vi skal vise at  $a_n - a_{k_n}$  konvergerer mod 0. Lad  $\varepsilon > 0$  være givet, og vælg  $N$  så stort at  $|a_n - a_m| < \varepsilon$  for  $n, m \geq N$ . Idet  $k_n \geq n$  har vi dermed at  $|a_n - a_{k_n}| < \varepsilon$ .  $\square$

Vi kan altså uden videre vælge at udskifte en repræsentant for et reelt tal med en delfølge af repræsentanten. Vi får brug for et helt specielt valg af delfølge, som formuleret i følgende lemma.

**Lemma 2.2.** *Lad  $\{a_n\}$  være en Cauchy-følge af rationale tal. Så findes en delfølge  $\{b_n\} = \{a_{k_n}\}$  med den egenskab at  $|b_n - b_{n+1}| < 2^{-n}$  for alle naturlige tal  $n$ .*

*Bevis.* Vi udnytter Cauchy-egenskaben ved  $a_n$  gentagne gange. For ethvert naturligt tal  $r$  vælger vi  $N_r$  så  $|a_n - a_m| < 2^{-r}$  for alle  $m, n \geq N_r$ . Sæt nu  $k_1 = N_1$ , og definer rekursivt  $k_n = \max(N_n, k_{n-1} + 1)$  for  $n \geq 2$ . Så er  $k_1 < k_2 < \dots$ , og vi har at

$$|b_n - b_{n+1}| = |a_{k_n} - a_{k_{n+1}}| < 2^{-n}$$

da  $k_{n+1} > k_n \geq N_n$ .  $\square$

Bemærk at vi for  $m > n$  får at

$$\begin{aligned} |b_n - b_m| &\leq |b_n - b_{n+1}| + |b_{n+1} - b_{n+2}| + \dots + |b_{m-1} - b_m| \\ &\leq 2^{-n} + 2^{-n-1} + \dots + 2^{-m+1} \\ &< 2^{-n+1}. \end{aligned}$$

Vi er nu i stand til at vise at  $\mathbb{R}$  er fuldstændig. Lad  $\{x_n\}$  være en Cauchy-følge af reelle tal. Vi kan jævnfør de to foregående lemmaer vælge repræsentanter  $\{a_{n,k}\}_{k=1}^{\infty}$  for  $x_n$  som opfylder at  $|a_{n,k} - a_{n,k+1}| < 2^{-k}$  for alle  $k$ . Definer følgen  $b = \{b_n\}_{n=1}^{\infty}$  ved  $b_n = a_{n,n}$ . Det påstås dels at  $b_n$  er en Cauchy-følge af rationale tal (som derved repræsenterer et reelt tal), dels at  $x_n$  konvergerer mod  $[b]$ .

Lad  $\varepsilon > 0$  være givet. Der findes så et  $N \in \mathbb{N}$  så det for alle  $m, n \geq N$  gælder at  $|x_n - x_m| < \varepsilon/2$ . Det betyder, at fra et vist trin  $K$  i Cauchy-følgen  $\{|a_{nk} - a_{mk}|\}_{k=1}^{\infty}$  gælder at

$$|a_{n,k} - a_{m,k}| < \varepsilon/2 \tag{5}$$

for  $k \geq K$ .

Vælg nu et  $N \in \mathbb{N}$  så stort, at  $|x_n - x_m| < \varepsilon/2$  for  $n, m \geq N$  og så  $2^{-N+1} < \varepsilon/4$ . Lad  $m, n \geq N$ . Så har vi for alle naturlige tal  $k$  vurderingen

$$\begin{aligned} |b_n - b_m| &= |a_{n,n} - a_{m,m}| \\ &\leq |a_{n,n} - a_{n,k}| + |a_{n,k} - a_{m,k}| + |a_{m,k} - a_{m,m}| \end{aligned}$$

Ved at vælge  $k$  tilstrækkelig stor (større end  $m$  og  $n$ , og så stor at (5) holder) ser vi at vi kan vurdere  $|b_n - b_m|$  mindre end

$$2^{-n+1} + \varepsilon/2 + 2^{-m+1} < \varepsilon/4 + \varepsilon/2 + \varepsilon/4 = \varepsilon.$$

Altså er  $\{b_n\}_{n=1}^{\infty}$  en Cauchy-følge.

Vi skal vise at  $x_n$  konvergerer mod  $b$ . Lad  $\varepsilon > 0$  være givet. Vi skal så vise at der findes et  $N$  så stort, at for alle  $n \geq N$  gælder at  $|x_n - b| < \varepsilon$ . Dette vil sige, at det for alle  $n$  skal gælde, at for store nok  $k$  er  $|a_{n,k} - b_k| < \varepsilon$ . Hvis vi nu vælger  $N$  så stor at  $2^{-N+1} < \varepsilon/2$  og så  $|b_n - b_m| < \varepsilon/2$  for alle  $n, m \geq N$  har vi for  $n \geq N$  og  $k \geq n$  at

$$|a_{n,k} - b_k| \leq |a_{n,k} - a_{n,n}| + |a_{n,n} - a_{k,k}| < 2^{-n+1} + \varepsilon/2 < \varepsilon$$

Dette viser at  $x_n$  konvergerer mod det reelle tal som følgen  $b_n$  repræsenterer, og således er  $\mathbb{R}$  fuldstændig.  $\square$

## 2.2 Supremumseggen skaben

I Matematisk Analyse-bogen er fuldstændigheden af de reelle tal formuleret ved hjælp af supremumseggen skaben, som siger at enhver ikke-tom opad begrænset delmængde af de reelle tal har en mindste øvre grænse. I bogen benyttes denne egenskab til at vise at Cauchy-følger af reelle tal er konvergente. Lad os for fuldstændighedens skyld (pun intended) vise at konvergen sen af Cauchy-følger fører til supremumseggen skaben, så de to formuleringer af fuldstændighed faktisk er ækvivalente (den opmærksomme læser vil vide, at konvergen sen af Cauchy-følger er „den rigtige“ formulering, da det er denne som generaliserer til vilkårlige metriske rum).

Lad derfor  $A \subseteq \mathbb{R}$  være en ikke-tom, opad begrænset delmængde af de reelle tal. Der findes derfor et tal  $M_0$  med den egenskab, at  $a \leq M_0$  for alle  $a \in A$ . Da  $A$  ikke er tom findes der et  $a_0$  i  $A$ . Betragt tallet  $\frac{a_0 + M_0}{2}$ . Der er to muligheder; det er enten en øvre grænse for  $A$  eller også er det ikke. Hvis det er en øvre grænse sætter vi  $M_1 = \frac{a_0 + M_0}{2}$  og  $a_1 = a_0$ . Hvis det ikke er en øvre grænse må der findes et  $a_1 \in A$  så  $a_1 > \frac{a_0 + M_0}{2}$ . I dette tilfælde sætter vi  $M_1 = M_0$ . I begge tilfælde bliver  $M_1$  altså en øvre grænse for  $A$ . Som man måske kan gætte definerer vi nu rekursivt  $a_i$  og  $M_i$  ved

$$M_{i+1} = \begin{cases} (a_i + M_i)/2 & \text{hvis } (a_i + M_i)/2 \text{ er en øvre grænse for } A \\ M_i & \text{ellers.} \end{cases}$$

$$a_{i+1} = \begin{cases} a_i & \text{hvis } (a_i + M_i)/2 \text{ er en øvre grænse for } A \\ \text{et vilkårligt tal } (a_i + M_i)/2 < a \in A & \text{ellers} \end{cases}$$

Følgen  $M_i$  er altså en følge af øvre grænser for  $A$ . Vi vil nu vise at det er en Cauchy-følge, og at dens grænseværdi  $M$  faktisk er den mindste øvre grænse for  $A$ .

Vi har at  $M_i \geq a_i$  for alle  $i$ , da  $M_i$  er en øvre grænse for  $A$  og  $a_i \in A$ . Første påstand er

$$0 \leq M_i - a_i \leq 2^{-i}(M_0 - a_0) \quad (6)$$

for alle  $i$ . For  $i = 0$  er dette klart, så antag at uligheden er rigtig for  $i$ . Vi har så at

$$M_{i+1} - a_{i+1} = \frac{M_i + a_i}{2} - a_i = \frac{M_i - a_i}{2} \leq 2^{-i-1}(M_0 - a_0)$$

hvis  $\frac{M_i + a_i}{2}$  er en øvre grænse for  $A$ , og

$$M_{i+1} - a_{i+1} = M_i - a < M_i - \frac{M_i + a_i}{2} = \frac{M_i - a_i}{2} \leq 2^{-i-1}(M_0 - a_0)$$

hvis  $\frac{M_i + a_i}{2}$  ikke er en øvre grænse for  $A$ , idet tallet  $a$  er større end  $\frac{M_i + a_i}{2}$ .

Som konsekvens heraf fås let at  $0 \leq M_i - M_{i+1} \leq 2^{-i-1}(M_0 - a_0)$ , idet  $M_{i+1} - M_i$  enten er 0 eller  $\frac{M_i - a_i}{2}$ . Men så har vi for alle naturlige tal  $n \geq m$  at

$$\begin{aligned} M_n - M_m &= M_n - M_{n+1} + M_{n+1} - \cdots - M_{m-1} + M_{m-1} - M_m \\ &\leq (2^{-n-1} + 2^{-n-2} + \cdots + 2^{-m})(M_0 - a_0) \\ &\leq 2^{-n}(M_0 - a_0). \end{aligned}$$

Heraf ser man, at hvis man blot vælger  $N$  så stor at  $2^{-N}(M_0 - a_0) < \varepsilon$  har vi at  $|M_n - M_m| < \varepsilon$  for alle  $m, n \geq N$ , og derfor er  $M_n$  en Cauchy-følge. Kald dens grænseværdi  $M$ .

Det påstås nu at  $M$  er en øvre grænse for  $A$ . Lad derfor  $a \in A$  være et vilkårligt element. Da vi har at  $M_n \geq a$  for ethvert  $n \in \mathbb{N}$  gælder det også at  $M \geq a$  (hvis ikke kunne man vælge  $\varepsilon = (a - M)/2$  og derefter finde et  $N$  så  $|M_N - M| < \varepsilon$ , hvilket ville stride mod at  $M_N \geq a$ ).

Vi mangler at vise at  $M$  er den mindste øvre grænse for  $A$ . Hertil er det nok at bemærke, at følgen  $a_i$  også er konvergent med grænseværdi  $M$ . Vi har nemlig at  $|M - a_i| \leq |M - M_i| + M_i - a_i$ , og da  $M_i$  konvergerer mod  $M$  følger af (6) at vi kan gøre dette så småt vi ønsker. Enhver øvre grænse for  $A$  vil være større end hvert  $a_i$ , og dermed større end  $\lim_{i \rightarrow \infty} a_i = M$ .

Det giver derfor mening at sætte  $\sup A = M$ , idet en mindste øvre grænse (hvis den findes) naturligvis er entydigt bestemt. Man kan så tilsvarende for en nedad begrænset mængde  $B$  definere  $\inf B = -\sup(-B)$ .