KTH Matematik

KTHs Matematiska Cirkel

# Reella tal

Joakim Arnlind

Tomas Ekholm

Andreas Enblom

Institutionen för matematik, 2005

Finansierat av Marianne och Marcus Wallenbergs Stiftelse

# Innehåll

## Några ord på vägen

Detta kompendium är skapat för att användas som litteratur till KTHs Matematiska Cirkel under läsåret 2005–2006 och består av sju avsnitt. Kompendiet är inte tänkt att läsas enbart på egen hand, utan ska ses som ett skriftligt komplement till undervisningen på de sju träffarna.

Som den mesta matematik på högre nivå är kompendiet kompakt skrivet. Detta innebär att man i allmänhet inte kan läsa det som en vanlig bok. Istället bör man pröva nya satser och definitioner genom att på egen hand exemplifiera. Därmed uppnår man oftast en mycket bättre förståelse av vad dessa satser och deras bevis går ut på.

Övningsuppgifterna är fördelade i två kategorier. De med udda nummer har facit, och syftet med dessa är att eleverna ska kunna räkna dem och på egen hand kontrollera att de förstått materialet. De med jämna nummer saknar facit och kan användas som examination. Det rekommenderas dock att man försöker lösa även dessa uppgifter även om man inte examineras på dem. Om man kör fast kan man alltid fråga en kompis, en lärare på sin skola eller någon av oss.

Vi bör också nämna att få av uppgifterna är helt enkla. Kika därför inte i facit efter några få minuter (om du inte löst uppgiften), utan prata först med kompisar eller försök litet till. Alla uppgifter ska gå att lösa med hjälp av informationen i detta kompendium.

KTHs Matematiska Cirkel finasieras av Marianne och Marcus Wallenbergs Stiftelse. Vi tackar Dan Laksov och Roy Skjelnes, båda från Institutionen för Matematik vid KTH, för deras givande kommentarer om denna skrift.

## Några ord om Cirkeln

KTHs Matematiska Cirkel, i dagligt tal benämnd Cirkeln, startade 1999. Dess ambition är att sprida kunskap om matematiken och dess användningsområden utöver vad eleverna får genom gymnasiekurser, och att etablera ett närmare samarbete mellan gymnasieskolan och högskolan. Cirkeln skall särskilt stimulera elevernas matematikintresse och inspirera dem till fortsatta naturvetenskapliga studier. Lärarna på cirkeln kan vid behov ge eleverna förslag på ämnen till projektarbeten vid gymnasiet.

Till varje kurs skrivs ett kompendium som distribueras gratis till eleverna. Detta material, liksom övriga uppgifter om KTHs Matematiska Cirkel, finns tillgängligt på

`http://www.math.kth.se/cirkel`

Sedan 2001 godkänns Cirkeln av Stockholms Stad som en 50-poängskurs eller som matematisk breddning. Det är upp till varje skola att godkänna Cirkeln som en kurs och det är lärarna från varje skola som sätter betyg på kursen. Lärarna är självklart också välkomna till Cirkeln och många har kommit överens med sin egen skola om att få Cirkeln godkänd som fortbildning eller som undervisning. Vi vill gärna understryka att föreläsningarna är öppna för alla gymnasieelever och lärare.

Vi har avsiktligt valt materialet för att ge eleverna en inblick i matematisk teori och tankesätt och presenterar därför både några huvudsatser inom varje område och bevisen för dessa resultat. Vi har också som målsättning att bevisa alla satser som används om de inte kan förutsättas bekanta av elever från gymnasiet. Detta, och att flera ämnen är på universitetsnivå, gör att lärarna och eleverna kan uppleva programmet som tungt, och alltför långt över gymnasienivån. Meningen är emellertid inte att lärarna och eleverna skall behärska ämnet fullt ut och att lära in det på samma sätt som gymnasiekurserna. Det viktigaste är att eleverna kommer i kontakt med teoretisk matematik och får en inblick i *matematikens väsen*. Vår förhoppning är att lärarna med denna utgångspunkt skall ha lättare att upplysa intresserade elever om KTHs Matematiska Cirkel och övertyga skolledarna om vikten av att låta både elever och lärare delta i programmet.

## Några ord om betygssättning

Ett speciellt problem tidigare år har varit betygssättningen. Detta borde emellertid bara vara ett problem om lärarna använder sig av samma standard som de gör när de sätter betyg på ordinarie gymnasiekurser. Om utgångspunkten istället är att eleverna skall få insikt i matematiken genom att gå på föreläsningarna och att eleven gör sitt bästa för att förstå materialet och lösa uppgifterna, blir betygsättningen lättare. Självklart betyder det mycket vad eleverna har lärt av materialet i kursen, men lärarna kan bara förvänta sig att ett fåtal elever behärskar ämnet fullt ut. I det perspektivet blir det lätt att använda de officiella kriterierna:

*Godkänd:* Eleven har viss insikt i de moment som ingår i kursen och kan på ett godtagbart sätt redovisa valda delar av kursen såväl muntligt som skriftligt. Detta kan ske genom att eleven håller föredrag inför klassen, redovisar eller lämnar en rapport till sin matematiklärare.

*Väl godkänd:* Eleven har god insikt i flera moment från kursen. Eleven kan redovisa dessa moment både skriftligt och muntligt och dessutom uppvisa lösningar på problem som givits på kursen. Detta kan ske genom att eleven håller föredrag inför klassen, redovisar eller lämnar en rapport till sin matematiklärare.

*Mycket väl godkänd:* Eleven har mycket god insikt i flera moment av kursen och lämnar skriftliga redovisningar av flera delar av kursen eller lämnar lösningar på problem som givits på kursen. Detta kan ske genom att eleven håller föredrag inför klassen, redovisar eller lämnar en rapport till sin matematiklärare.

Det är också möjligt att skolorna samarbetar, så elever från en skola redovisar eller lämnar rapport för en lärare i en annan skola.

Författarna, augusti 2005

# 1 Mängdlära

## 1.1 Mängder

Mängdbegreppet är ett av de mest grundläggande begreppen inom matematiken. En mängd kan ses som en samling av matematiska objekt, kallade *element*.

Ett sätt att beskriva en mängd på är att räkna upp elementen som tillhör mängden. Exempelvis är

$$A = \{1, a, 4\} \tag{1.1}$$

en mängd som innehåller elementen $1, a$ och 4. Ett annat sätt att beskriva en mängd är att skriva $\{x \in D : \text{villkor på } x\}$. Med detta menar man mängden av alla element i $D$ som uppfyller de givna villkoren. Som exempel tar vi

$$B = \{n \in \{1, 2, 3, \ldots\} : n \text{ är udda}\} \tag{1.2}$$

och

$$C = \{y \in \{1, 2, 3, 4\} : x > 2\}. \tag{1.3}$$

Mängden $B$ innehåller alla udda positiva heltal, medan $C$ innehåller alla element från mängden $\{1, 2, 3, 4\}$ som är större än 2. Alltså har vi

$$B = \{1, 3, 5, 7, 9, 11, \ldots\} \quad \text{och} \quad C = \{3, 4\}. \tag{1.4}$$

Vi bryr oss inte om i vilken ordning eller hur många gånger elementen räknas upp och därmed gäller till exempel

$$\{1, 2, 3, 4\} = \{3, 1, 4, 2\} = \{1, 3, 3, 1, 2, 4, 4, 1, 3, 2\}. \tag{1.5}$$

Om $A$ är en mängd och $x$ är ett element i mängden $A$ så skriver vi $x \in A$ och säger att $x$ *tillhör* $A$. Exempelvis gäller $17 \in \{n : n \text{ är ett udda heltal}\}$ och $b \in \{a, b, 10, 3\}$. Att ett element $x$ inte tillhör mängden $A$ skrivs $x \notin A$. Den *tomma mängden* innehåller ingenting och betecknas $\emptyset$.

**Exempel 1.1.1.** Låt $A = \{4, 5, 8, 4711, 12, 18\}$ och $B = \{x \in A : x > 10\}$. Då är $B = \{12, 18, 4711\}$ medan $\{x \in A : x < 3\} = \emptyset$. ▲

**Definition 1.1.2.** Låt $A$ och $B$ vara mängder. Om alla element i mängden $A$ också är element i mängden $B$ så sägs $A$ vara en *delmängd* till $B$. Detta betecknas $A \subseteq B$.

**Exempel 1.1.3.** Mängden $\{1, a\}$ är en delmängd till $\{1, 3, a\}$, eftersom alla element i $\{1, a\}$ finns i mängden $\{1, 3, a\}$. Vi skriver $\{1, a\} \subseteq \{1, 3, a\}$. ▲

**Definition 1.1.4.** Antag att $A$ och $B$ är mängder. *Unionen* av $A$ och $B$ består av de element som ligger i någon av mängderna och betecknas $A \cup B$. *Snittet* av $A$ och $B$ består av de element som ligger i båda mängderna och betecknas $A \cap B$.

**Exempel 1.1.5.** Låt $A = \{1, 3, 5, 6\}$ och $B = \{5, 8, 3, 4711\}$. Då har vi $A \cup B = \{1, 3, 5, 6, 8, 4711\}$ och $A \cap B = \{3, 5\}$. ▲

## 1.2 Relationer

En relation på en mängd $A$ är ett sätt att beskriva när två element $x, y \in A$ är relaterade på något sätt. Om relationen betecknas $R$ så betyder $xRy$ att $x$ är relaterad till $y$ via relationen $R$. Innan vi ger en abstrakt definition av vad en relation är kan det vara på sin plats med några exempel.

**Exempel 1.2.1.** Här följer tre exempel på relationer i mängden $\{1, 2, 3, \ldots\}$.

1. Att vara mindre än något annat är en typisk relation. Exempelvis gäller $3 < 4$ och $2 < 4711$. Här använder vi alltså symbolen $<$ istället för $R$.
2. Låt $xRy$ betyda att $xy = 30$. Här gäller till exempel $5R6$, men *inte* $4R7$.
3. Vi låter $xSy$ betyda att $y = x + 2$, Som exempel har vi $2S4$ och $9S11$ men inte att $2S5$.

Som synes är det inget som säger att relationer måste betcknas just med $R$. I detta exempel betecknas de tre relationerna med $<$, $R$ och $S$. ▲

**Definition 1.2.2.** Låt $A$ vara en mängd. En *relation* på $A$ är en mängd $R$ som innehåller ordnade par $(x, y)$ där $x, y \in A$. Om $(x, y) \in R$ så skriver vi $xRy$.

**Exempel 1.2.3.** Låt oss använda denna definition på relationerna i Exempel 1.2.1. Då gäller följande:

1. $< \,=\{(x, y) : x, y = 1, 2, 3, \ldots \text{ och } x \text{ är mindre än } y\}$
2. $R = \{(1, 30), (2, 15), (3, 10), (5, 6), (6, 5), (10, 3), (15, 2), (30, 1)\}$
3. $S = \{(0, 2), (1, 3), (2, 4), \ldots\}$.

Dessa tre relationer betraktas alltså som *mängder* och innehåller ordnade par $(x, y)$ där $x, y \in \{1, 2, 3, \ldots\}$. ▲

## 1.3 Ekvivalensrelationer

**Definition 1.3.1.** Låt $A$ vara en mängd. En relation $R$ på $A$ sägs vara en *ekvivalensrelation* om den uppfyller:

1. (Reflexivitet) För varje $x \in A$ gäller $xRx$.
2. (Symmetri) Om $x, y \in A$ och $xRy$ så gäller även $yRx$.
3. (Transitivitet) Så snart både $xRy$ och $yRz$ gäller så har vi även att $xRz$.

**Definition 1.3.2.** Om $R$ är en ekvivalensrelation på en mängd $A$ och $x \in A$ så kallar vi mängden $\{y \in A : xRy\}$ för *ekvivalensklassen* till $x$. Den betecknas med $[x]_R$ eller, om det är klart vilken relation $R$ som åsyftas, med $[x]$.

**Exempel 1.3.3.** Låt $A = \{12, 12342, 11, 1000, 211, 65535, 181, 222, 130\}$ och låt $R$ vara relationen att ha samma slutsiffra. Exempelvis har vi $11R181$ och $130R130$. Låt oss börja med att visa att $R$ är en ekvivalensrelation.

1. Att $R$ är reflexiv, det vill säga uppfyller $xRx$ för alla $x \in A$ är klart eftersom $x$ har samma slutsiffra som sig själv, för varje $x \in A$.

2. Tag $x, y \in A$ och antag att $xRy$, det vill säga att $x$ och $y$ har samma slutsiffra. Då gäller naturligtvis $yRx$, alltså att $y$ och $x$ har samma slutsiffra. Detta betyder är $R$ symmetrisk.

3. För att visa transitivitet, tag $x, y, z \in A$ och antag att $xRy$ och $yRz$, det vill säga att $x$ har samma slutsiffra som $y$ och att $y$ har samma slutsiffra som $z$. Givetvis har då $x$ samma slutsiffra som $z$. Alltså gäller $xRz$.

Ekvivalensklasserna som hör till $R$ är

$$\{130, 1000\}, \{11, 181, 211\}, \{12, 222, 12342\} \text{ och } \{65535\}. \tag{1.6}$$

I själva verket gäller

$$\begin{gathered} [1000] = [130] = \{130, 1000\} \\ [11] = [211] = [181] = \{11, 181, 211\} \\ [12] = [12342] = [222] = \{12, 222, 12342\} \\ [65535] = \{65535\}. \end{gathered} \tag{1.7}$$

Här gäller alltså $A = [1000] \cup [181] \cup [12342] \cup [65535]$. Vi ser att så fort $x$ och $y$ är relaterade så är ekvivalensklassen till $x$ samma som ekvivalensklassen till $y$. Med andra ord, om $xRy$ så gäller $[x] = [y]$. Vidare har de fyra mängderna $[1000]$, $[181]$, $[12342]$ och $[65535]$ inga gemensamma element, det vill säga om $x$ inte är relaterad till $y$ så gäller $[x] \cap [y] = \emptyset$. ▲

En stunds eftertanke visar att detta exempel speglar det allmänna fallet. Ekvivalensklasserna delar in mängden $A$ i ett antal disjunkta (åtskilda) delar. Dessutom är alla element som ligger i samma ekvivalensklass relaterade till varandra. Med andra ord består $A$ av ett antal disjunkta delar, ekvivalensklasser, inom vilka alla element är relaterade till varandra. Läsaren hänvisas till Övning 1.2 – 1.4 för att reda ut detaljerna i detta. För att ytterligare förtydliga, låt $A = \{x_1, x_2, \ldots, x_n\}$. Då gäller

$$A = [x_1] \cup [x_2] \cup \cdots \cup [x_n] \tag{1.8}$$

och

$$[x] \cap [y] = \begin{cases} [x] & \text{om } xRy \\ \emptyset & \text{annars.} \end{cases} \tag{1.9}$$

**Exempel 1.3.4.** I själva verket kan ovanstående exempel generaliseras med precis samma resonemang. Låt $A$ vara en godtycklig delmängd av $\{1, 2, 3, \ldots\}$. Då är relationen att ha samma slutsiffra en ekvivalensrelation och vi får upp till tio ekivalensklasser, en för varje slutsiffra. ▲

**Exempel 1.3.5.** Relationen $<$ från Exempel 1.2.1 är *inte* en ekvivalensrelation. Exempelvis är relationen $<$ inte symmetrisk. Vi har ju att $2 < 4$ men inte att $4 < 2$. ▲

**Exempel 1.3.6 (Udda och jämna tal).** Definiera en relation $R$ på mängden $\{1, 2, 3, \ldots\}$ genom att låta $xRy$ betyda att $x + y$ är ett jämnt tal. Det är lätt att inse att detta är en ekvivalensrelation och att ekvivalensklasserna är

$$\{2, 4, 6, 8, \ldots\} \quad \text{och} \quad \{1, 3, 5, 7, \ldots\}, \tag{1.10}$$

vilket betyder att ekvivalensklasserna består av de jämna respektive de udda talen. ▲

**Exempel 1.3.7 (Ekvivalensklasser modulo $n$).** De föregående exemplen på ekvivalensrelationer är alla specialfall av moduloräkning. Vi inför notationen

$$a \equiv b \pmod{n}, \tag{1.11}$$

som betyder att $a = b + kn$ för något heltal $k$. Vi säger att *$a$ är kongruent med $b$ modulo $n$*. Man kan se det som att två tal $a$ och $b$ är kongruenta modulo $n$ om man kan lägga $n$ till det ena talet ett antal gånger och få det andra talet. Exempelvis gäller

$$2 \equiv 17 \pmod{5}, \tag{1.12}$$

eftersom $17 = 2 + 5 + 5 + 5 = 2 + 3 \cdot 5$. I själva verket gäller

$$\begin{aligned} 1 \equiv 6 \equiv 11 \equiv 16 \equiv \cdots &\pmod{5} \\ 2 \equiv 7 \equiv 12 \equiv 17 \equiv \cdots &\pmod{5} \\ 3 \equiv 8 \equiv 13 \equiv 18 \equiv \cdots &\pmod{5} \\ 4 \equiv 9 \equiv 14 \equiv 19 \equiv \cdots &\pmod{5} \\ 5 \equiv 10 \equiv 15 \equiv 20 \equiv \cdots &\pmod{5} \end{aligned} \tag{1.13}$$

och från detta kan man ana att det rör sig om en ekvivalensrelation. Låt $n$ vara ett fixerat positivt heltal. Nu har vi en relation $R$ på mängden $\{1, 2, 3, \ldots\}$ där $aRb$ betyder att $a \equiv b \pmod{n}$. Detta är en ekvivalensrelation och ekivalensklasserna består av alla tal som är kongruenta med varandra modulo $n$. Det finns $n$ stycken ekvivalensklasser, och i fallet $n = 5$ är ekvivalensklasserna just

$$\begin{gathered} \{1, 6, 11, \ldots\}, \{2, 7, 12, \ldots\}, \{3, 8, 13, \ldots\}, \\ \{4, 9, 14, \ldots\} \text{ och } \{5, 10, 15, \ldots\}. \end{gathered} \tag{1.14}$$

Ett annat sätt att se på det är att $a \equiv b \pmod{n}$ om vi får samma rest när vi dividerar $a$ respektive $b$ med $n$. Exempelvis går talet 4 två gånger i talet 11 med resten 3, och dessutom går talet 4 tre gånger i 15 med resten 3. Därmed har vi $11 \equiv 15 \pmod{4}$. Ekvivalensklasserna till modulorelationen innehåller de tal som får samma rest vid division med $n$.

Nu kan man fråga sig hur detta kan vara en generalisering av exemplen ovan. Jo, i Exempel 1.3.3 räknar vi modulo 10 i mängden $A$. Att $a$ och $b$ har samma slutsiffra betyder helt enkelt att $a$ är kongruent med $b$ modulo 10. Vidare, i Exempel 1.3.6 är det modulo 2 som gäller. Alla udda tal är kongruenta med varandra modulo 2, och detsamma gäller för de jämna talen. ▲

**Övning 1.1.** Låt $A = \{1, 2, 3, 4, \ldots\}$, $B = \{1, 3, 5, 7, \ldots\}$, $C = \{2, 4, 6, 8, \ldots\}$ och $D = \{1, 4, 19, 36, 101\}$. Bestäm mängderna

1. $B \cup C$,
2. $B \cap C$,
3. $D \cap C$,
4. $\{x \in D \,:\, x \in B\}$,
5. $\{x \in A \,:\, x = y + 1$ för något $y \in D\}$,
6. $\{x + 1 \,:\, x \in D\}$.

**Övning 1.2.** Låt $A$ vara en icke-tom mängd och $R$ en ekvivalensrelation på $A$. Låt $x, y, z \in A$ och antag att både $y$ och $z$ tillhör ekvivalensklassen $[x]$. Visa att $yRz$.

**Övning 1.3.** Låt $A$ och $R$ vara som i föregående övning. Tag $x, y \in A$ med $xRy$. Visa att

$$[x] = [y]. \tag{1.15}$$

**Övning 1.4.** Återigen är $A$ och $R$ som ovan. Antag att $x, y \in A$ inte är relaterade. Visa att

$$[x] \cap [y] = \emptyset. \tag{1.16}$$

# 2 Heltal och rationella tal

Vår föreställning om tal säger oss att de ligger ordnade längs en oändligt lång linje, *tallinjen*, och att man kan addera, subtrahera, multiplicera och dividera dem. Frågan som vi ställer oss och poängen med denna kurs är hur man gör om denna föreställning till välformulerad matematik.

Låt oss börja med några observationer. Subtraktion är i själva verket inte någon egen räkneoperation utan bara ett specialfall av addition. Vi har ju faktiskt att $x - y = x + (-y)$, så att subtrahera $y$ från $x$ är helt enkelt att addera $x$ och $-y$.

Vidare bör man reflektera över vad division är. Vad betyder uttrycket $x/y = z$? Jo, vi *definierar* detta till att betyda att $x = y \cdot z$. Alltså ser vi inte division som en räkneoperation utan som ett multiplikativt samband mellan de tre talen $x, y, z$. Att division inte skulle vara en egen räkneoperation stämmer faktiskt med det sätt på vilket man dividerar i huvudet. För att räkna ut $30/5$ så testar man vilket tal $k$ som uppfyller att $30 = 5 \cdot k$ och kommer fram till att $k = 6$. Division är alltså bara ett specialfall av multiplikation.

Så mycket för de fyra räknesätten. Det visar sig att vi egentligen bara har *två räknesätt* – addition och multiplikation. Det är på detta sätt man hanterar dessa frågor inom den abstrakta matematiken.

För att nu kunna definiera vad vi menar med tal och tallinje måste vi börja med enklast möjliga förutsättningar.

> Vi utgår från att vi känner till talen $1, 2, 3, \ldots$ med addition och multiplikation. Men det är också allt vi känner till. Hur man subtraherar och dividerar tal vet vi inte till någonting om, och inte heller hur resten av talen på tallinjen är definierade. I synnerhet känner vi inte ännu till talet 0.

## 2.1 Heltal

Det första steget blir att konstruera talet 0 och de negativa talen $-1, -2, -3, \ldots$. Tillsammans med de enda tal vi i nuläget känner till, nämligen talen $1, 2, 3, \ldots$, bildar de *heltalen*. Mängden av alla heltal betecknas $\mathbb{Z}$. Beteckningen kommmer från tyskans *zahl* som betyder tal. Intuitivt sett gäller alltså

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}, \tag{2.1}$$

men kom ihåg att än så länge är symbolerna $0, -1, -2, \ldots$ okända för oss. När talet 0 är definierat låter vi de *naturliga talen* vara

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}. \tag{2.2}$$

Vidare måste vi också definiera vad vi menar med addition och multiplikation. Kom ihåg att detta är de enda räkneoperationer vi behöver. Slutligen definierar vi relationen $<$.

Eftersom dessa konstruktioner tar en hel del tid, och vårt primära mål är de rationella, och senare de reella, talen, så låter vi konstruktionen av heltalen vara överkurs. Förståelse för denna konstruktion underlättar dock förståelsen för konstruktionen av rationella tal avsevärt.

## 2.2 Överkurs: Konstruktion av $\mathbb{Z}$

Vi utgår alltså från att vi bara känner till talen i mängden $\{1, 2, 3, \ldots\}$. Låt oss i detta avsnitt införa beteckningen $\mathbb{P}$ för denna mängd. Betrakta nu mängden

$$H = \{(n, m) \,:\, n, m \in \mathbb{P}\}. \tag{2.3}$$

Inför en relation $R$ på denna mängd genom att låta $(a, b)R(c, d)$ betyda att $a + d = b + c$. Detta är inget problem eftersom vi vet hur vi adderar tal i $\mathbb{P}$. Alltså gäller

$$R = \{((a, b), (c, d)) \,:\, a, b, c, d \in \mathbb{P} \text{ och } a + d = b + c\}\,. \tag{2.4}$$

**Anmärkning 2.2.1.** Minns att en relation består av ordnade par ur en mängd. I det här fallet är själva elementen i $H$ ordnade par. Alltså består relationen $R$ av ordnade par av ordnade par. Eftersom $2 + 6 = 3 + 5$ så är *elementen* $(2, 6)$ och $(3, 5)$ relaterade, vilket betyder att $((2, 6), (3, 5)) \in R$.

Att visa att $R$ är en ekvivalensrelation är rättframt, och något som läsaren uppmanas göra.

En ekvivalensklass hörande till ekvivalensrelationen $R$ kallas för ett *heltal*. Låt $\mathbb{Z}$ vara mängden alla ekvivalensklasser till $R$. I själva verket kommer vi att betrakta klassen $\{(0, 3), (1, 4), (2, 5), (3, 6), \ldots\}$ som talet $-3$ och ekvivalensklassen $\{(4, 0), (5, 1), (6, 2), \ldots\}$ som talet $+4$. Mer generellt kan man tänka på $[(a, b)]$ som talet $a - b$, även fast vi ännu inte vet vad $-$ är. Vi definierar alltså symbolerna

$$0 = [(1, 1)], \quad +n = [(n + 1, 1)] \quad \text{och} \quad -n = [(1, n + 1)] \tag{2.5}$$

för $n \in \mathbb{P}$. I nuläget skiljer vi alltså på *heltalet* $+n$ och talet $n \in \mathbb{P}$. Dessutom har vi infört talet 0 och negativa tal $-1, -2, -3, \ldots$.

Vidare definieras addition och multiplikation av heltalen $[(a, b)]$ och $[(c, d)]$, där $a, b, c, d \in \mathbb{N}$, via

$$[(a, b)]+[(c, d)] = [(a+c, b+d)] \quad \text{och} \quad [(a, b)]\cdot[(c, d)] = [(ac+bd, ad+bc)] \tag{2.6}$$

När man ser denna typ av definition måste man fråga sig om addition och multiplikation verkligen är väldefinierade av detta. Vi har ju att $(1, 3)R(2, 4)$ så ekvivalensklasserna $[(1, 3)]$ och $[(2, 4)]$ är desamma. Men då måste ju resultatet av additionerna $[(1,3)] + [(7,3)]$ och $[(2,4)] + [(7,3)]$ vara desamma. Frågan vi ställer oss är alltså om dessa definitioner av addition och multiplikation är oberoende av representant för ekvivalensklasserna.

Antag alltså att $(a_1, b_1)R(a_2, b_2)$ och $(c_1, d_1)R(c_2, d_2)$, där $a_1, a_2, b_1, \ldots, d_2 \in \mathbb{P}$. Då måste vi visa att

$$[(a_1, b_1)] + [(c_1, d_1)] = [(a_2, b_2)] + [(c_2, d_2)] \tag{2.7}$$

och att

$$[(a_1, b_1)] \cdot [(c_1, d_1)] = [(a_2, b_2)] \cdot [(c_2, d_2)]. \tag{2.8}$$

Detta lämnas till läsaren. Senare kommer motsvarande sak att göras för de rationella talen i Sats 3.1.2.

Nu kan vi identifiera ett tal $n \in \mathbb{P}$ med heltalet $+n \in \mathbb{Z}$ och därmed få att $\mathbb{P} \subseteq \mathbb{Z}$. För att vara helt tillfreds med detta bör man också kontrollera att $+n \neq +m$, det vill säga att klasserna $[(n+1, 1)]$ och $[(m+1, 1)]$ inte är desamma, för $n, m \in \mathbb{P}$ med $n \neq m$.

En anmärkning bör också göras kring subtraktion. Det har ju sagts att $a - b$ definieras som $a + (-b)$. Detta verkar vid första anblicken tillräckligt eftersom vi nu känner till vad symbolen $-b$ betyder för $b \in \mathbb{P}$. Men vi vill ju kunna subtrahera *alla* heltal och det som återstår är att ge mening till symbolen $-b$ där $b = 0, -1, -2, -3, \ldots$. Vi definierar således $-0 = 0$ och $-(-b) = b$ för $b \in \mathbb{P}$.

Vi har ju en intuitiv uppfattning om vilka räkneregler som gäller för heltal. Utan att gå in på vilka dessa är eller att bevisa dem bör det påpekas att det går att bevisa dessa räkneregler för heltalen med addition och multiplikation så som de konstruerats ovan. Låt oss ta ett exempel på detta.

**Exempel 2.2.2.** Tag $a, b \in \mathbb{Z}$. Då finns positiva tal $a_1, a_2, b_1, b_2 \in \mathbb{P}$ så att

$$a = [(a_1, a_2)] \quad \text{och} \quad b = [(b_1, b_2)]. \tag{2.9}$$

Nu gäller

$$\begin{aligned} a \cdot b &= [(a_1, a_2)] \cdot [(b_1, b_2)] \\ &= [(a_1 b_1 + a_2 b_2, a_1 b_2, a_2 b_1)] \\ &= [(b_1 a_1 + b_2 a_2, b_1 a_2 + b_2 a_1)] \\ &= [(b_1, b_2)] \cdot [(a_1, a_2)] \\ &= b \cdot a, \end{aligned} \tag{2.10}$$

eftersom vi vet att $n + m = m + n$ och att $n \cdot m = m \cdot n$ för positiva tal $n, m \in \mathbb{P}$. Därmed har det visats att

$$a \cdot b = b \cdot a. \tag{2.11}$$

för alla heltal $a, b$. ▲

Slutligen till relationen $<$. Tag två heltal $a$ och $b$. Vi låter $a < b$ betyda att $b - a \in \mathbb{P}$. Det är nu en intressant uppgift att visa att

$$\mathbb{P} = \{a \in \mathbb{Z} : 0 < a\}. \tag{2.12}$$

## 2.3 Konstruktion av $\mathbb{Q}$

Nu vet vi alltså vad heltalen $\ldots, -2, -1, 0, 1, 2, \ldots$ är och hur vi adderar, subtraherar och multiplicerar dem. Det som återstår är division. Men i allmänhet får man inte ett heltal när man dividerar två heltal. Därmed behöver vi utöka vårt begrepp om tal till något större där vi också kan dividera. Vi vill alltså finna tal som uppfyller det *multiplikativa* sambandet $x/y = z$. Det är här de rationella talen gör sin entré.

Inuitivt sett är ett rationellt tal ett tal på formen $a/b$ där $a, b \in \mathbb{Z}$ och $b \neq 0$. Mängden av alla rationella tal kommer att betecknas med $\mathbb{Q}$. Beteckningen $\mathbb{Q}$ kommer från engelskans *quotient* (bråk).

Kom nu ihåg att vi inte ännu vet vad vi menar med talet $a/b$. Hela poängen med detta avsnitt är att ge innebörd till detta för oss okända begrepp. En stor del av svårigheten är att vi vill att $(-2)/3$, $(-4)/6$ och $8/(-12)$ ska vara samma tal. Till detta kan man använda ekvivalensrelationer.

Låt $B$ vara mängden av alla ordnade par $(a, b)$ där $a$ och $b$ är heltal och $b$ inte är 0. Alltså:

$$B = \{(a, b) \,:\, a, b \in \mathbb{Z}, b \neq 0\}. \tag{2.13}$$

Definiera nu en relation $R$ på $B$ på följande sätt:

$$(a, b)R(c, d) \quad \text{betyder att} \quad ad = bc. \tag{2.14}$$

**Lemma 2.3.1.** *Relationen $R$ är en ekvivalensrelation.*

*Bevis.* Eftersom $ab = ba$ för heltal $a, b$ så gäller $(a, b)R(a, b)$ för alla $(a, b) \in B$. Alltså är $R$ reflexiv.

Tag godtyckliga element $(a, b), (c, d) \in B$ och antag att $(a, b)R(c, d)$, vilket betyder att $ad = bc$. Då följer $cb = da$, som i sin tur betyder att $(c, d)R(a, b)$, så $R$ är symmetrisk.

Slutligen, tag $(a, b), (c, d), (e, f) \in B$ och antag att $(a, b)R(c, d)$ och $(c, d)R(e, f)$. Då har vi att $ad = bc$ och $cf = de$ och det följer att

$$af \cdot d = ad \cdot f = bc \cdot f = b \cdot cf = b \cdot de = be \cdot d, \tag{2.15}$$

och eftersom $d \neq 0$ så följer $af = be$ vilket betyder att $(a, b)R(e, f)$. Alltså är $R$ transitiv. $\square$

**Definition 2.3.2.** Vi kallar en ekvivalensklass till ekvivalensrelationen $R$ för ett *rationellt tal* och låter $\mathbb{Q}$ vara mängden av alla rationella tal. Vi inför också beteckningen $a/b$ (eller $\frac{a}{b}$) för det rationella tal som är ekvivalensklassen till elementet $(a, b) \in B$.

Vi gör alltså *definitionen* $a/b = [(a, b)]$ för $a, b \in \mathbb{Z}$ med $b \neq 0$. Antag att $ad = bc$ och $b, d \neq 0$. Då vet vi från definitionen av ekvivalensrelationen $R$ att $(a, b)R(c, d)$ och därmed har elementen $(a, b)$ och $(c, d)$ samma ekvivalensklass, så $a/b = [(a, b)] = [(c, d)] = c/d$. Detta betyder att definitionen verkligen har täckt in att exempelvis $(-2)/3 = 4/(-6)$.

## 2.4 Heltalen är rationella tal

Givetvis vill vi se heltalen som ett specialfall av de rationella talen eftersom vår intuition om division säger oss t.ex. att $15/5 = 3$. Från vår definition följer faktiskt att $15/5 = 3/1$, eftersom $(15,5)R(3,1)$ visar att $(15,5)$ och $(3,1)$ tillhör samma ekvivalensklass. Men att det rationella talet $3/1$, som ju är en ekvivalensklass, skulle vara samma sak som heltalet 3 är inte på något sätt klart.

Det som behövs är ett tillägg till definitionerna. När vi arbetar med ett heltal $a$, åtminstone i samband med rationella tal, så bestämmer vi helt enkelt att det är underförstått att vi egentligen arbetar med det rationella talet, ekvivalensklassen, $a/1$. Även om det kan anses slarvigt så tillåter vi oss därför att skriva $a = a/1$ för alla $a \in \mathbb{Z}$. I synnerhet gäller $0 = 0/b$ för alla $b \in \mathbb{Z}$ med $b \neq 0$. Beviset för detta lämnas som en övning.

Det är en sak till som vi bör reflektera över. Om vi har två olika heltal $a$ och $b$, så vill vi ju inte att det ska betraktas som samma rationella tal. Vi måste alltså kontrollera att

$$\frac{a}{1} \neq \frac{b}{1} \quad \text{för } a, b \in \mathbb{Z} \text{ med } a \neq b. \tag{2.16}$$

Detta kan kännas självklart, men det måste ändå kontrolleras. Om $a \neq b$ så gäller $a \cdot 1 \neq 1 \cdot b$, vilket betyder att elementen $(a,1)$ och $(b,1)$ inte är relaterade. Därmed har $(a,1)$ och $(b,1)$ olika ekvivalensklasser, så

$$\frac{a}{1} = [(a,1)] \neq [(b,1)] = \frac{b}{1}. \tag{2.17}$$

**Övning 2.1.** Visa att $0 = 0/b$ för alla $b \in \mathbb{Z}$ med $b \neq 0$. *Ledning:* Vi identifierar heltalet 0 med det rationella talet $0/1$.

**Övning 2.2.** Låt $M = \{(a,b) : a, b \in \mathbb{Z}\}$ och definiera relationen $S$ på $M$ genom att låta $(a,b)S(c,d)$ betyda att $ad = bc$. Visa att $S$ *inte* är en ekvivalensrelation. Detta är anledningen till varför vi inte tillåter $b = 0$ för det rationella talet $a/b$.

# 3 Egenskaper för de rationella talen

## 3.1 Räkneoperationer i $\mathbb{Q}$

För att över huvud taget kunna använda de rationella talen måste vi ju kunna räkna med dem. Därför måste vi nu definiera räkneoperationerna för $\mathbb{Q}$. Här finns två viktiga saker som måste täckas in av definitionerna. Det första är att alla räkneregler som vi är vana vid gäller och det andra är att de definitioner vi gör överensstämmer med räkneoperationerna i $\mathbb{Z}$. Den första frågan lämnas till nästa avsnitt.

Konstruktionen av $\mathbb{Q}$ från förra kapitlet behöver ligga färskt i minnet. Där hade vi alltså mängden $B = \{(a, b) : a, b \in \mathbb{Z}, b \neq 0\}$ och en ekvivalensrelation $R$ på mängden $B$ där $(a, b)R(c, d)$ betyder att $ad = bc$. De rationella talen är ekvivalensklasserna till denna ekvivalensrelation, och vi använder beteckningen $a/b$ för ekvivalensklassen $[(a, b)]$.

**Definition 3.1.1.** Låt $a, b, c, d \in \mathbb{Z}$ med $b, c \neq 0$. Definiera

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)] \quad \text{och} \quad [(a, b)] \cdot [(c, d)] = [(ac, bd)]. \tag{3.1}$$

Om vi använder beteckningen $a/b$ och $c/d$ för klasserna $[(a, b)]$ respektive $[(c, d)]$ skrivs detta alltså som

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{och} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}. \tag{3.2}$$

Detta är alltså en definition av räkneoperationerna $+$ och $\cdot$ i mängden $\mathbb{Q}$. Innan denna definition var uttrycken $a/b+c/d$ och $a/b\cdot c/d$ bara några okända symboler. Däremot visste vi ju redan innan definitionen vad $ad + bc$, $ac$ och $bd$ i högerledet av (3.1) betydde. Detta är ju helt enkelt multiplikation och addition av heltal. Alltså är $e = ad + bc$ och $f = bd$ båda heltal som definierar ett rationellt tal $e/f = (ad + bc)/bd$.

En mycket viktig detalj som är lätt att missa är att denna definition bestämmer addition och multiplikation av två ekvivalensklasser, men resultatet av operationen bestäms av vilken representant för ekvivalensklassen vi har valt. Exempelvis vet vi ju att $2/3 = 4/6$, vilket betyder att det rationella talet $2/3$ representeras av antingen heltalsparet $(2, 3)$ eller av paret $(4, 6)$, men är det klart att $2/3 + 5/4 = 4/6 + 5/4$?

**Sats 3.1.2.** *Operationerna $+$ och $\cdot$ är väldefinierade. Detta betyder att om $a_1/b_1 = a_2/b_2$ och $c_1/d_1 = c_2/d_2$ så gäller*

$$\frac{a_1}{b_1} + \frac{c_1}{d_1} = \frac{a_2}{b_2} + \frac{c_2}{d_2} \quad \textit{och} \quad \frac{a_1}{b_1} \cdot \frac{c_1}{d_1} = \frac{a_2}{b_2} \cdot \frac{c_2}{d_2}. \tag{3.3}$$

*Bevis.* Antag att $a_1/b_1 = a_2/b_2$ och $c_1/d_1 = c_2/d_2$, vilket betyder att $a_1b_2 = b_1a_2$ och att $c_1d_2 = d_1c_2$. Nu ska vi visa att (3.3) gäller, det vill säga att

$$\frac{a_1d_1 + b_1c_1}{b_1d_1} = \frac{a_2d_2 + b_2c_2}{b_2d_2} \quad \text{och} \quad \frac{a_1c_1}{b_1d_1} = \frac{a_2c_2}{b_2d_2}. \tag{3.4}$$

Detta följer från att

$$
\begin{aligned}
(a_1d_1 + b_1c_1) \cdot b_2d_2 &= a_1d_1b_2d_2 + b_1c_1b_2d_2 \\
&= a_1b_2 \cdot d_1d_2 + b_1b_2 \cdot c_1d_2 \\
&= b_1a_2 \cdot d_1d_2 + b_1b_2 \cdot d_1c_2 \\
&= b_1d_1 \cdot (a_2d_2 + b_2c_2)
\end{aligned}
\tag{3.5}
$$

och att

$$
\begin{aligned}
a_1c_1 \cdot b_2d_2 &= a_1b_2 \cdot c_1d_2 \\
&= b_1a_2 \cdot d_1c_2 \\
&= b_1d_1 \cdot a_2c_2
\end{aligned}
\tag{3.6}
$$

eftersom detta betyder att relationerna $(a_1d_1 + b_1c_1, b_1d_1)R(a_2d_2 + b_2c_2, b_2d_2)$ och $(a_1c_1, b_1d_1)R(a_2c_2, b_2d_2)$ gäller. $\square$

Nu till frågan om de nydefinierade operationerna addition och multiplikation stämmer överens med addition och multiplikation av heltal. Frågan uppstår eftersom vi kan se heltal $a$ och $b$ som rationella tal $a/1$ och $b/1$ och eftersom vi har två uppfattningar av t.ex. addition; dels av *heltalen* $a$ och $b$ och dels av de *rationella* talen $a = a/1$ och $b = b/1$. Att det inte blir något problem är självklart eftersom definitionerna ger oss att

$$
\frac{a}{1}+\frac{b}{1} = \frac{a\cdot 1 + b \cdot 1}{1 \cdot 1} = \frac{a+b}{1} = a+b \quad \text{och} \quad \frac{a}{1}\cdot\frac{b}{1} = \frac{a\cdot b}{1\cdot 1} = \frac{a \cdot b}{1} = a\cdot b \tag{3.7}
$$

för alla $a, b \in \mathbb{Z}$. Notera att de sista identiteterna i dessa ekvationer,

$$
\frac{a+b}{1} = a+b \quad \text{och} \quad \frac{a\cdot b}{1} = a \cdot b \tag{3.8}
$$

är definitioner och inte något som räknas fram. Det är en definition att heltalet $c$ och det rationella talet $c/1$ ska betraktas som samma objekt.

Till sist inför vi en ordning på de rationella talen. För ett rationellt tal $a/b$ låter vi det hittills okända uttrycket $0 < a/b$ betyda att $0 < a \cdot b$. För två rationella tal $q$ och $r$ skriver vi $q < r$ om $0 < q - r$. Notera hur den första definitionen används i den andra. Självklart måste man ställa sig frågan om $<$ är väldefinierat av detta, det vill säga om definitionerna ovan är oberoende av hur de rationella talen representeras. Detta är Övning 3.1.

## 3.2 Mängden $\mathbb{Q}$ är en kropp

Det har nu blivit dags att fundera på om räkneoperationerna på $\mathbb{Q}$ fungerar så som vi förväntar oss. Vår föreställning om detta sammanfattas i begreppet *kropp*.

**Definition 3.2.1.** En mängd $K$ med två operationer $+$ och $\cdot$ är en *kropp* om den uppfyller följande:

(A) Axiom för addition

- (A1) Slutenhet: $x + y \in K$ för alla $x, y \in K$.
- (A2) Addition är kommutativt: $x + y = y + x$ för alla $x, y \in K$.
- (A3) Addition är associativt: $(x+y)+z = x+(y+z)$ för alla $x, y, z \in K$.
- (A4) Det finns ett element $0 \in K$ som uppfyller $0+x = x$ för alla $x \in K$.
- (A5) Till varje $x \in K$ finns ett element $-x$ med $x + (-x) = 0$.

(M) Axiom för multiplikation

- (M1) Slutenhet: $x \cdot y \in K$ för alla $x, y \in K$.
- (M2) Multiplikation är kommutativt: $x \cdot y = y \cdot x$ för alla $x, y \in K$.
- (M3) Multiplikation är associativt: $(x\cdot y)\cdot z = x\cdot(y\cdot z)$ för alla $x, y, z \in K$.
- (M4) $K$ innehåller ett element $1 \neq 0$ som uppfyller $1 \cdot x = x$ för varje $x \in K$.
- (M5) Till varje $x \in K$ med $x \neq 0$ finns ett element $x^{-1}$ som uppfyller $x \cdot x^{-1} = 1$.

(D) Den distributiva lagen: För alla $x, y, z \in K$ gäller $x\cdot(y+z) = (x\cdot y)+(x\cdot z)$.

**Sats 3.2.2.** *Mängden $\mathbb{Q}$ med operationerna $+$ och $\cdot$ är en kropp.*

Att bevisa denna sats lämnas som en övning för läsaren. Men några viktiga saker bör poängteras.

Som vi diskuterade tidigare är inte division en egen räkneoperation utan bara ett specialfall av multiplikation. I själva verket visar axiom (M5) att vi kan dividera rationella tal. Om $p, q \in \mathbb{Q}$ och $q \neq 0$ så ser man att $r = p \cdot q^{-1}$ uppfyller att $p = q \cdot r$ och därmed kan man skriva $p/q = r$. Alltså gör vi *definitionen* att $p/q = p \cdot q^{-1}$. Återigen uppstår en viss tvetydighet: $a/b$ har ju redan en innebörd för $a, b \in \mathbb{Z}$ med $b \neq 0$! Men detta är inget problem så fort man inser att

$$\left(\frac{a}{b}\right)^{-1} = \frac{b}{a} \tag{3.9}$$

för alla $a, b \in \mathbb{Z}$ med $a, b \neq 0$. Då följer ju $(a/1)/(b/1) = (a/1) \cdot (b/1)^{-1} = (a/1) \cdot (1/b) = (a \cdot 1)/(1 \cdot b) = a/b$.

När det gäller subtraktion räcker det att kommentera att det minustecken som nämns i axiom (A5) definieras av $-(a/b) = (-a)/b = a/(-b)$ för alla $a/b \in \mathbb{Q}$.

## 3.3 Uppräknelighet

Båda mängderna $\mathbb{Z}$ och $\mathbb{Q}$ innehåller oändligt många element. Frågan är om det finns något mer precist sätt att klassificera storleken på oändliga mängder. Inför den kommande diskussionen i detta ärende påminner vi oss om de naturliga talen, mängden $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$.

**Definition 3.3.1.** En mängd $A$ sägs vara *uppräknelig* om man till varje tal $n \in \mathbb{N}$ kan ordna ett element $x_n \in A$ så att $A = \{x_0, x_1, x_2, \ldots\}$. Om $A$ inte är uppräknelig sägs $A$ vara *överuppräknelig.*

Man ser det alltså som att elementen i en uppräknelig mängd kan räknas upp som $x_0, x_1, x_2, \ldots$ och att man i denna uppräkning får med *alla* element i mängden.

**Exempel 3.3.2.** Givetvis är $\mathbb{N}$ uppräknelig. Låt $x_n = n$ och få $\{x_0, x_1, \ldots\} = \{0, 1, \ldots\} = \mathbb{N}$. För att visa att även $\mathbb{Z}$ är uppräknelig, tag $n \in \mathbb{N}$ och låt

$$x_n = \begin{cases} 0 & \text{om } n = 0 \\ (n+1)/2 & \text{om } n \text{ är udda} \\ -n/2 & \text{om } n \text{ är jämn.} \end{cases} \tag{3.10}$$

Därmed gäller $x_0 = 0, x_1 = 1, x_2 = -1, x_3 = 2, x_4 = -2, x_5 = 3, x_6 = -3$ o.s.v. så $\mathbb{Z} = \{x_0, x_1, x_2, \ldots\}$. ▲

**Sats 3.3.3.** *Mängden $\mathbb{Q}$ är uppräknelig.*

*Bevis.* Precis som i avsnitt 2.3 låter vi $B = \{(a, b) : a, b \in \mathbb{Z}, b \neq 0\}$. Elementen i $B$ kan skrivas upp enligt följande:

$$\begin{tikzcd}
\ddots & \vdots & \vdots & \vdots & \vdots & \iddots \\
\cdots & (-1,-2) & (0,-2) & (1,-2) & (2,-2) & \cdots \\
\cdots & (-1,-1) \arrow[r] & (0,-1) \arrow[r] & (1,-1) \arrow[r] & (2,-1) \arrow[d] & \cdots \\
\cdots & (-1,1) \arrow[u] & (0,1) \arrow[r] & (1,1) \arrow[d] & (2,1) & \cdots \\
\cdots & (-1,2) \arrow[u] & (0,2) \arrow[l] & (1,2) \arrow[l] & (2,2) & \cdots \\
\cdots & (-1,3) & (0,3) & (1,3) & (2,3) & \cdots \\
\iddots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{tikzcd}$$

och om vi följer pilarna så får vi en uppräkning av elementen enligt

$$y_0 = (0, 1), \quad y_1 = (1, 1), \quad y_2 = (1, 2), \quad y_3 = (0, 2), \ldots \tag{3.11}$$

som uppfyller att $B = \{y_0, y_1, y_2, \ldots\}$. Minns att $\mathbb{Q}$ består av alla ekvivalensklasser i $B$, exempelvis har vi att $[(1,2)] = 1/2 = 2/4$. Om vi låter $x_n = [y_n] \in \mathbb{Q}$ för varje $n \in \mathbb{N}$ (alltså är $x_n$ den ekvivalensklass som $y_n$ tillhör) så får vi att $\mathbb{Q} = \{x_0, x_1, x_2, \ldots\}$. $\square$

**Anmärkning 3.3.4.** I detta bevis har vi alltså att

$$x_0 = 0, \quad x_1 = 1, \quad x_2 = \frac{1}{2}, \quad x_3 = 0, \quad x_4 = -\frac{1}{2}, \quad x_5 = -1, \ldots \tag{3.12}$$

vilket betyder att elementen i $\mathbb{Q}$ räknas upp flera gånger var. Men det är ändå så att $\mathbb{Q} = \{x_0, x_1, x_2, \ldots\}$ eftersom det inte gör något om elementen i en mängd räknas upp mer än en gång. Mängderna $\{1, 2, 3\}$ och $\{1, 1, 2, 3, 2, 2, 1, 3\}$ är desamma.

Till sist ett resultat som kan vara användbart i framtiden. Beviset, som lämnas som en övning, liknar det ovanstående, men sättet på vilket elementen skrivs upp är lite annorlunda.

**Sats 3.3.5.** *Antag att alla mängderna $A_1, A_2, A_3, \ldots$ är uppräkneliga. Då är unionen $A_1 \cup A_2 \cup A_3 \cup \cdots$, det vill säga mängden av alla element som tillhör någon av mängderna $A_1, A_2, \ldots$, uppräknelig.*

**Övning 3.1.** Antag att $a/b = c/d$. Visa att $0 < a/b$ om och endast om $0 < c/d$.

**Övning 3.2.** Bevisa Sats 3.2.2.

**Övning 3.3.** Använd Sats 3.3.5 för att bevisa att mängden

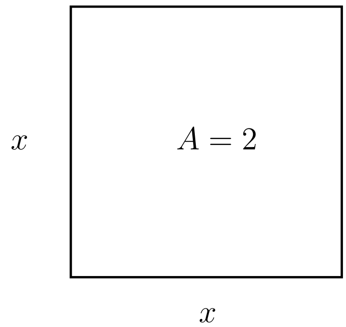
$$\mathscr{A} = \{B \subseteq \mathbb{Z} : B \text{ är ändlig}\} \tag{3.13}$$

är uppräknelig. Att en mängd är ändlig betyder att den innehåller $n$ element där $n \in \mathbb{N}$.

**Övning 3.4.** Bevisa Sats 3.3.5.

# 4 Konstruktion av de reella talen

I de föregående avsnitten har vi definierat de rationella talen $\mathbb{Q}$ utifrån heltalen och diskuterat deras egenskaper. Att behovet av rationella tal finns ter sig ganska naturligt eftersom vi vill kunna hantera divisionen $a/b$ även om det inte blir ett heltal. Det vore ganska otympligt om vi t.ex. bara kunde mäta avstånd uttryckt i hela tal. När vi nu skall närma oss de reella talen, som i någon mening är mer än de rationella talen, är det inte lika självklart att det finns ett liknande behov. Räcker det inte med de rationella talen? Vi kan beskriva godtyckligt små och stora tal med hjälp av dessa. Till exempel så vet vi att mellan två rationella tal så finns det alltid ett tredje rationellt tal. Ett argument för att vi behöver någonting mer är följande exempel.




Antag att du vill konstruera en kvadrat som har arean 2 areaenheter. Hur långa skall du göra sidorna? Ekvationen som skall lösas är

$$x^2 = 2. \tag{4.1}$$

För den praktiskt lagde är det inga problem att lösa detta problem. Man knappar in 2 på miniräknaren och trycker på $\sqrt{\phantom{x}}$-knappen. Då dyker det upp något i stil med

$$1.414213562 \tag{4.2}$$

vilket är ett svar som nog räcker för de flesta praktiska konstruktioner. I detta kompendium nöjer vi oss dock inte med ett sådant svar, utan frågar oss: Vad är det egentligen för objekt vars produkt med sig själv är lika med 2, och som vi vanligtvis brukar beteckna $\sqrt{2}$? Är det ett tal? De enda tal vi än så länge känner till är de rationella talen. Alltså, finns det ett rationellt tal $a/b$ sådant att

$$\left(\frac{a}{b}\right)^2 = 2 \quad ? \tag{4.3}$$

Svaret är nej, d.v.s. $\sqrt{2}$ är *inte* rationellt. För att bevisa detta använder vi oss av ett motsägelsebevis. Antag att $\sqrt{2}$ är rationellt. Från (4.3) följer det att

$$2b^2 = a^2. \tag{4.4}$$

Vi kan alltid anta att vi har valt $a$ så litet som möjligt. Eftersom $2b^2$ är ett jämnt tal är även $a^2$ ett jämnt tal vilket i sin tur medför att $a$ måste vara ett jämnt tal. Vi kan därför anta att $a = 2c$ för något heltal $c$. Insatt i (4.4) ger

$$b^2 = 2c^2. \tag{4.5}$$

Nu är $2c^2$ ett jämnt tal och därav är $b$ ett jämnt tal, d.v.s. $b = 2d$ där $d$ är ett heltal. Identiteten

$$\frac{a}{b} = \frac{2c}{2d} = \frac{c}{d} \tag{4.6}$$

strider mot att $a$ var valt så litet som möjligt, detta ty $\frac{c}{d}$ beskriver samma bråk som $\frac{a}{b}$ och $c < a$. Alltså måste antagandet om att $\sqrt{2}$ är rationellt vara falskt.

Om inte $\sqrt{2}$ är ett rationellt tal, vad är det då? Vi skulle gärna vilja kalla $\sqrt{2}$ ett tal, vilket betyder att vi måste vidga vårt talbegrepp bortom de rationella talen. Hur ska det gå till? Vi har redan mött begreppet "kropp" i föregående avsnitt, som formaliserade räkneoperationerna addition och multiplikation. Vi kommer nu att införa fler egenskaper som vi kräver att de reella talen ska ha, för att sedan försöka hitta en mängd av objekt som uppfyller dessa.

## 4.1 Ordnade kroppar

**Definition 4.1.1.** Låt $A$ vara en mängd. En *ordning* på $A$ är en relation $R$ med följande två egenskaper:

1. Om $x, y \in A$ då gäller en och endast en av relationerna

$$xRy, \quad x = y \quad \text{eller} \quad yRx. \tag{4.7}$$

2. Om $x, y, z \in A$, $xRy$ och $yRz$, då följer att $xRz$.

En *ordnad mängd* är en mängd $A$ på vilken en ordning är definierad. För en ordningsrelation använder man ofta symbolen $<$ istället för $R$; vi skriver alltså $x < y$ eller $y > x$ istället för $xRy$. Vi definierar också att $x \leqslant y$ om $x < y$ eller $x = y$.

**Anmärkning 4.1.2.** Notera att en ordning är en relation men *inte* en ekvivalensrelation.

**Definition 4.1.3.** En kropp $K$ är en *ordnad kropp* om det finns en ordningsrelation, betecknad med $<$, på $K$ sådan att för $x, y, z \in K$

(O1) $x + y < x + z$ om $y < z$

(O2) $xy > 0$ om $x > 0$ och $y > 0$

Definitionerna 4.1.1 och 4.1.3 formaliserar de räknelagar vi normalt använder oss av när vi räknar med olikheter. När vi skapar de reella talen vill vi förstås att de skall vara en ordnad kropp.

**Exempel 4.1.4.** På sidan 18 införde vi en ordning på $\mathbb{Q}$. Med den ordningsrelationen är $\mathbb{Q}$ en ordnad kropp. Se Övning 4.2. ▲

## 4.2 Supremumegenskapen

I Exempel 4.1.4 noterade vi att $\mathbb{Q}$ är en ordnad kropp. Alltså räcker inte detta begrepp för att beskriva de reella talens unika egenskaper. Däremot räcker det med att tillskriva dem endast en egenskap till – *supremumegenskapen*.

**Definition 4.2.1.** Låt $A$ vara en ordnad mängd och $B \subseteq A$. Om det finns ett element $y \in A$ sådant att

$$x \leqslant y \qquad \text{för alla } x \in B \tag{4.8}$$

så sägs $y$ vara en *övre begränsning* till $B$. Vidare sägs $B$ vara *uppåt begränsad* om det finns en övre begränsning till $B$.

**Definition 4.2.2.** Låt $A$ vara en ordnad mängd, $B$ en icketom delmängd till $A$ och $y$ en övre begränsning till $B$. Vi säger att $y$ är en *minsta övre begränsning* till $B$ eller *supremum* av $B$, om för varje övre begränsning $z$ till $B$ så gäller det att $y \leqslant z$. Vi skriver

$$y = \sup_A B. \tag{4.9}$$

**Anmärkning 4.2.3.** Om $y = \sup_A B$ och $z = \sup_A B$ så måste $y = z$, eftersom om $z \neq y$ så måste $z < y$ eller $y < z$ och då kan inte båda vara en *minsta* övre begränsning.

**Exempel 4.2.4.** Låt $B$ vara delmängden $\{p \in \mathbb{Q} : 0 < p < 1\}$ av $\mathbb{Q}$. Talet $3 \in \mathbb{Q}$ är en övre begränsning av $B$ medan $1 \in \mathbb{Q}$ är den minsta övre begränsningen. $B$ är alltså uppåt begränsad. Observera att mängden $B$ inte innehåller något största element, eftersom $1 \notin B$. ▲

**Definition 4.2.5.** En ordnad mängd $A$ sägs ha *supremumegenskapen* om för varje icketom, uppåt begränsad delmängd $B$ av $A$ finns det ett $y \in A$ sådant att $y = \sup_A B$.

I nästa exempel kommer vi att visa att det finns delmängder av $\mathbb{Q}$ som är uppåt begränsade men som inte har någon minsta övre begränsning. Detta betyder att $\mathbb{Q}$ inte har supremumegenskapen.

**Exempel 4.2.6.** Låt $B$ vara delmängden $\{p \in \mathbb{Q} : p^2 \leqslant 2\}$ av $\mathbb{Q}$. Antag att det finns en minsta övre begränsning $q \in \mathbb{Q}$ till $B$. Då gäller det förstås att

$q^2 \geqslant 2$. Eftersom vi har visat att $\sqrt{2} \notin \mathbb{Q}$ så betyder det att $q^2 > 2$. Vi vill nu visa att vi kan skapa ett tal $r < q$ som också är en övre begränsning. Vi sätter

$$r = q - \frac{q^2 - 2}{q + 2} = \frac{2q + 2}{q + 2}. \tag{4.10}$$

Eftersom $q^2 - 2 > 0$ följer av första likheten att $r < q$. Beräknar vi $r^2 - 2$ så får vi

$$r^2 - 2 = \frac{2(q^2 - 2)}{(q + 2)^2} > 0 \tag{4.11}$$

eftersom $q^2 > 2$. Detta betyder att $r^2 > 2$ och därmed att $r^2 > p^2$ för alla $p \in B$. Det följer att $r > p$ för alla $p \in B$. Vi har alltså konstruerat en övre begränsning $r$ som är mindre än $q$, som vi antog vara den minsta övre begränsningen. Detta motsäger antagandet och visar att $B$ ej har någon minsta övre begränsning. ▲

> Vårt mål i de följande avsnitten är att konstruera de reella talen som en ordnad kropp med supremumegenskapen. Vi kommer att använda oss av en konstruktion som härstammar från den tyske matematikern Richard Dedekind (1831–1916).

## 4.3 Snitt

Vi kommer att konstruera mängden $\mathbb{R}$, d.v.s. de reella talen, som en mängd av så kallade *snitt*. Alltså, de objekt vi kallar för reella tal kommer att vara snitt.

**Definition 4.3.1.** Ett *snitt* $\alpha$ är en delmängd av $\mathbb{Q}$ sådan att

(R1) $\alpha \neq \emptyset$ och $\alpha \neq \mathbb{Q}$.

(R2) Om $p \in \alpha$, $q \in \mathbb{Q}$ och $q < p$, då är $q \in \alpha$.

(R3) Om $p \in \alpha$, då existerar ett $r \in \alpha$ sådant att $p < r$.

**Anmärkning 4.3.2.** Egenskapen (R2) betyder att om ett rationellt tal $q$ är med i snittet, så är alla rationella tal mindre än $q$ med i snittet. Egenskapen (R3) betyder att ett snitt ej innehåller något element som är större än alla andra element i snittet.

**Exempel 4.3.3.** Låt $p \in \mathbb{Q}$ och låt $\alpha_p = \{q \in \mathbb{Q} : q < p\}$. Då är $\alpha_p$ ett snitt. För att visa detta måste vi kontrollera att mängden uppfyller de tre kraven (R1)-(R3) ovan.

(R1) Mängden $\alpha_p$ är inte tom eftersom till exempel talet $p-1 \in \alpha_p$; den kan heller inte vara hela $\mathbb{Q}$ eftersom till exempel $p+1 \notin \alpha_p$.

(R2) Detta är uppfyllt eftersom $\alpha_p$ innehåller alla tal mindre än $p$ per definition.

(R3) Tag ett godtyckligt $q \in \alpha_p$ och sätt $r = q + (p-q)/2$. Eftersom $r$ ligger halvvägs mellan $q$ och $p$ så är $r < p$, vilket betyder att $r \in \alpha_p$. Dessutom gäller $q < r$. ▲

**Definition 4.3.4.** Ett *reellt tal* är ett snitt. Mängden av alla reella tal betecknas med $\mathbb{R}$.

Vi vill naturligtvis att de rationella talen också skall vara reella tal, och eftersom $\mathbb{R}$ är en mängd av snitt så måste vi till varje rationellt tal kunna associera ett snitt. Detta gör vi enligt Exempel 4.3.3

> Vi kommer att se de rationella talen som en delmängd av de reella talen genom att till varje $p \in \mathbb{Q}$ tillskriva snittet $\alpha_p = \{q \in \mathbb{Q} \,:\, q < p\}$.

Till exempel har vi de viktiga snitten

$$1 = \{q \in \mathbb{Q} \,:\, q < 1\} \tag{4.12}$$

$$0 = \{q \in \mathbb{Q} \,:\, q < 0\} \tag{4.13}$$

som kommer att visa sig vara den multiplikativa och additiva enheten för de reella talen.

Tänk gärna på snitt som representerar rationella tal när vi i kommande avsnitt talar om snitt. Det gör det lättare att intuitivt förstå de operationer vi kommer att införa på $\mathbb{R}$. Notera att vi kommer att beteckna snitt med grekiska bokstäver såsom $\alpha, \beta, \gamma, \ldots$.

**Övning 4.1.** Visa att relationen $<$ på $\mathbb{Q}$, som definierad på sidan 18, är en ordning.

**Övning 4.2.** Visa att med ordningen $<$ är $\mathbb{Q}$ en ordnad kropp.

**Övning 4.3.** Låt $e_n = 1/n$ för $n = 1, 2, \ldots$ och sätt

$$E = \{e_1, e_2, e_3, \ldots\}. \tag{4.14}$$

Vi definierar, analogt med övre begränsning, att $y$ är en *undre begränsning* till en mängd $A$ om $y \leqslant x$ för alla $x \in A$. Vidare säger vi att $y$ är en *största* undre begränsning, eller *infimum*, av en mängd $A$ om för alla undre begränsningar $z$ till $A$ så gäller det att $z \leqslant y$. Visa att $\inf_{\mathbb{Q}} E = 0$.

**Övning 4.4.** Låt $e_n = 1 - 1/n$ för $n = 1, 2, \ldots$ och sätt

$$E = \{e_1, e_2, e_3, \ldots\}. \tag{4.15}$$

Visa att $\sup_{\mathbb{Q}} E = 1$.

# 5 Egenskaper för de reella talen

## 5.1 Ordning, addition och multiplikation

Vi vill att de reella talen skall vara en ordnad kropp med supremumegenskapen. Detta reflekterar, som tidigare sagt, de egenskaper och räkneregler som vi är vana vid. Alltså behöver vi definiera en ordning, en addition och en multiplikation på $\mathbb{R}$.

**Definition 5.1.1 (Ordning).** Vi skriver att $\alpha < \beta$ om $\alpha \subseteq \beta$ och $\alpha \neq \beta$.

**Sats 5.1.2.** *Relationen $<$ definierad ovan är en ordning.*

*Bevis.* Vi behöver verifiera de två egenskaperna i Definition 4.1.1. Den första egenskapen säger att för $\alpha, \beta \in \mathbb{R}$ så gäller en och endast en av egenskaperna $\alpha < \beta, \alpha = \beta$ eller $\beta < \alpha$. Om $\alpha = \beta$ så följer det direkt från definitionen att varken $\alpha < \beta$ eller $\beta < \alpha$ gäller. Antag nu att $\alpha < \beta$. Per definition så är $\alpha \neq \beta$, och då kan inte $\alpha \subseteq \beta$ och $\beta \subseteq \alpha$ gälla samtidigt, eftersom då är $\alpha = \beta$. På samma sätt argumenterar vi då $\beta < \alpha$.

Den andra egenskapen säger att om $\alpha, \beta, \gamma \in \mathbb{R}$ och $\alpha < \beta$ och $\beta < \gamma$ så är $\alpha < \gamma$. Vi måste alltså visa att under dessa antaganden så är $\alpha \subseteq \gamma$ och $\alpha \neq \gamma$. Tag ett godtyckligt element $q \in \alpha$. Eftersom $\alpha \subseteq \beta$ så är $q \in \beta$ och eftersom $\beta \subseteq \gamma$ så är $q \in \gamma$. Alltså är $\alpha \subseteq \gamma$. Från $\beta < \gamma$ följer det att det finns ett element $q \in \gamma$ sådant att $q \notin \beta$ och på samma sätt följer det att $q \notin \alpha$ eftersom $\alpha \subseteq \beta$. Alltså är $\alpha \neq \gamma$. ☐

Intuitivt är det ganska enkelt att förstå hur vi vill definiera addition och multiplikation, åtminstone för rationella tal. Låt $p, q \in \mathbb{Q}$ sådana att $p, q > 0$. Vi tänker oss att

$$\alpha_p + \alpha_q = \{r \in \mathbb{Q} \,:\, r < p + q\} \tag{5.1}$$

$$\alpha_p \cdot \alpha_q = \{r \in \mathbb{Q} \,:\, r < pq\}. \tag{5.2}$$

Då vi måste göra dessa definitioner för allmäna snitt blir det dock aningen mer invecklat.

**Definition 5.1.3 (Addition).** Låt $\alpha$ och $\beta$ vara två snitt. Vi definierar summan $\alpha + \beta$ som

$$\alpha + \beta = \{p + q \,:\, p \in \alpha, q \in \beta\}. \tag{5.3}$$

Givet ett snitt $\alpha$ definierar vi $-\alpha$ som

$$-\alpha = \{q \in \mathbb{Q} \,:\, -q - r \notin \alpha \text{ för något } r \in \mathbb{Q} \text{ där } r > 0\}. \tag{5.4}$$

**Anmärkning 5.1.4.** Notera att det inte är klart att $\alpha + \beta$ och $-\alpha$ verkligen är snitt. Detta måste vi bevisa när vi visar att $\mathbb{R}$ är en kropp.

**Anmärkning 5.1.5.** För ett snitt definierat som $\alpha_p = \{q \in \mathbb{Q} : q < p\}$ är det lätt att visa att $-\alpha_p = \{q \in \mathbb{Q} : q < -p\}$, vilket är precis vad vi väntar oss.

**Lemma 5.1.6.** $\mathbb{R}$ *uppfyller axiomen (A1)–(A5), samt egenskapen (O1) i Definition 4.1.3.*

*Bevis.*

(A1) Att visa att $\alpha + \beta$ är ett snitt är lämnat till läsaren i Övning 5.1.

(A2) Vi måste visa att $\alpha + \beta = \beta + \alpha$. Detta är klart eftersom

$$\alpha + \beta = \{p + q : p \in \alpha, q \in \beta\} = \{q + p : p \in \alpha, q \in \beta\} = \beta + \alpha \tag{5.5}$$

(A3) Associativiteten, d.v.s. att $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$, följer på samma sätt

$$\begin{aligned}(\alpha + \beta) + \gamma &= \{p + q : p \in \alpha + \beta, q \in \gamma\} \\ &= \{(r + s) + q : r \in \alpha, s \in \beta, q \in \gamma\} \\ &= \{r + (s + q) : r \in \alpha, s \in \beta, q \in \gamma\} \\ &= \{r + p : r \in \alpha, p \in \beta + \gamma\} \\ &= \alpha + (\beta + \gamma).\end{aligned} \tag{5.6}$$

(A4) Det existerar ett element $0 \in \mathbb{R}$ sådant att $\alpha + 0 = \alpha$ för alla $\alpha \in \mathbb{R}$. Vi vill förstås visa att det snitt vi associerar med det rationella talet 0 är det som gör jobbet.

För att visa att $\alpha + 0 = \alpha$ använder vi oss av en teknik som är vanlig inom matematiken. Genom att visa att varje element i $\alpha + 0$ är ett element i $\alpha$ och att varje element i $\alpha$ är ett element i $\alpha + 0$, så har vi visat de två inklusionerna $\alpha + 0 \subseteq \alpha$ och $\alpha \subseteq \alpha + 0$ vilket visar att $\alpha + 0 = \alpha$.

Tag ett godtyckligt element $q \in \alpha + 0$. Då kan vi skriva $q$ som $q = p + r$, där $p \in \alpha$ och $r \in 0$. Eftersom $r < 0$ så betyder det att $q < p$ vilket ger oss att $q \in \alpha$, enligt definitionen av snitt. Alltså är $\alpha + 0 \in \alpha$.

Tag nu ett godtyckligt element $q \in \alpha$. Då finns det, enligt (R3), ett element $r \in \alpha$ sådant att $r > q$. Då vi kan skriva $q = r + (q - r)$ så vet vi att $q \in \alpha + 0$ eftersom $r \in \alpha$ och $q - r \in 0$ ty $q - r < 0$. Alltså är $\alpha \subseteq \alpha + 0$, vilket tillsammans med ovanstående resultat visar att $\alpha + 0 = \alpha$.

(A5) Här måste vi visa att till varje snitt $\alpha \in \mathbb{R}$ så finns det ett snitt $\beta \in \mathbb{R}$ sådant att $\alpha + \beta = 0$. Snittet $\beta$ brukar skrivas som $-\alpha$, och vi vill visa att vår definition ovan av $-\alpha$ uppfyller detta. Vi kommer att använda samma teknik som i beviset ovan. Än så länge vet vi dock inte ens om $-\alpha$ är ett snitt. Att visa detta är lämnat som en övning.

Låt oss börja med att visa att $\alpha + (-\alpha) \subseteq 0$. Tag ett element $p \in \alpha$ och ett element $q \in -\alpha$. Då finns ett $r > 0$ sådant att $-q - r \notin \alpha$. I synnerhet ligger $-q$ inte i $\alpha$, eftersom $-q > -q - r$. Alltså har vi att $p < -q$ eftersom $\alpha$ innehåller alla rationella tal mindre än $q$. Olikheten $p < -q$ betyder att $p + q < 0$ vilket ger att $p + q \in \alpha$ för alla $p \in \alpha$ och $q \in -\alpha$. Detta betyder att $\alpha + (-\alpha) \subseteq 0$.

För att visa att $0 \in \alpha + (-\alpha)$ måste vi vara lite mer kluriga. Tag ett godtyckligt element $v \in 0$ och definiera $w = -v/2$. Då är helt klart $w > 0$. Eftersom $w$ är ett positivt rationellt tal och $\alpha$ är en uppåt begränsad mängd, så finns det ett heltal $n$ sådant att $nw \in \alpha$ men $(n+1)w \notin \alpha$. Nu definierar vi $p = -(n+2)w$ och vi ser att $p \in -\alpha$ eftersom

$$-p - w = (n+1)w \notin \alpha. \tag{5.7}$$

Vi ser vidare att

$$nw + p = -\frac{nv}{2} + p = -\frac{nv}{2} + \frac{(n+2)v}{2} = v. \tag{5.8}$$

Eftersom $v$ var ett gotyckligt element i $0$, $nw \in \alpha$ och $p \in -\alpha$, så betyder det att $0 \subseteq \alpha + (-\alpha)$. Alltså är $\alpha + (-\alpha) = 0$.

(O1) Antag att $\alpha, \beta, \gamma \in \mathbb{R}$ och $\beta < \gamma$. Vi vill visa att $\alpha + \beta < \alpha + \gamma$, d.v.s. $\alpha + \beta \subseteq \alpha + \gamma$ och $\alpha + \beta \neq \alpha + \gamma$. Att $\alpha + \beta \subseteq \alpha + \gamma$ är klart eftersom $\beta \subset \gamma$. Antag att $\alpha + \beta = \alpha + \gamma$ stämmer. Då kan vi addera $-\alpha$ till båda sidorna och få att $\beta = \gamma$, vilket motsäger att $\beta < \gamma$. Alltså är $\alpha + \beta \neq \alpha + \gamma$. □

**Anmärkning 5.1.7.** Ett viktigt specialfall av (O1) får vi om vi antar att $0 < \gamma$, väljer $\beta = 0$ och sätter $\alpha = -\gamma$. Då får vi

$$-\gamma + 0 < -\gamma + \gamma \tag{5.9}$$

vilket ger att $-\gamma < 0$. På samma sätt kan vi visa att om $\gamma < 0$ så är $-\gamma > 0$.

Att definiera multiplikation är mer komplicerat än att definiera addition, eftersom produkten av två negativa tal är positiv. Den intuitiva bilden skall dock vara klar; gör en tillbakablick till ekvation (5.2).

**Definition 5.1.8 (Multiplikation).** Låt $\alpha$ och $\beta$ vara två snitt sådana att $\alpha > 0$ och $\beta > 0$. Vi definierar produkten $\alpha \cdot \beta$ som

$$\alpha \cdot \beta = \{q \in \mathbb{Q} : q \leqslant rs \text{ för några } r \in \alpha, s \in \beta \text{ där } r > 0, s > 0\}. \tag{5.10}$$

Vi lämnar till läsaren, i Övning 5.2, att visa att $\alpha \cdot \beta$ är ett snitt. Låt nu $\alpha$ och $\beta$ vara två godtyckliga snitt. Då definierar vi, med hjälp av (5.10), $\alpha \cdot \beta$ som

$$\alpha \cdot \beta = \begin{cases} (-\alpha) \cdot (-\beta) & \text{om } \alpha < 0, \beta < 0 \\ -\big((-\alpha) \cdot \beta\big) & \text{om } \alpha < 0, \beta > 0 \\ -\big(\alpha \cdot (-\beta)\big) & \text{om } \alpha > 0, \beta < 0 \\ 0 & \text{om } \alpha = 0 \text{ eller } \beta = 0. \end{cases} \tag{5.11}$$

Låt oss för varje snitt $\alpha > 0$ definiera $\alpha^{-1}$

$$\alpha^{-1} = \{0 < q \in \mathbb{Q} \,:\, q^{-1} - r \notin \alpha \text{ för något } r > 0\} \cup \{q \in \mathbb{Q} \,:\, q \leqslant 0\}. \quad (5.12)$$

Då $\alpha < 0$ sätter vi $\alpha^{-1} = -(-\alpha)^{-1}$.

**Anmärkning 5.1.9.** Lägg märke till att vi i högerledet av ekvation (5.11) bara multiplicerar snitt $\gamma$ sådana att $\gamma > 0$ eftersom vi i Anmärkning 5.1.7 noterade att $-\gamma < 0$ om och endast om $\gamma > 0$.

**Lemma 5.1.10.** *De reella talen uppfyller axiom (O2) i Definition 4.1.3, d.v.s. för två element $\alpha, \beta \in \mathbb{R}$ gäller det att $\alpha \cdot \beta > 0$ om $\alpha > 0$ och $\beta > 0$.*

*Bevis.* Då $\alpha > 0$ och $\beta > 0$ så existerar det rationella tal $p \in \alpha$ och $q \in \beta$ sådana att $p > 0$ och $q > 0$. Enligt definitionen av multiplikation av snitt är $pq \in \alpha \cdot \beta$. Då $pq > 0$ så måste $\alpha \cdot \beta > 0$ eftersom ett snitt $\gamma$, sådant att $\gamma \leqslant 0$, ej kan innehålla några positiva rationella tal. □

**Lemma 5.1.11.** $\mathbb{R}$ *uppfyller axiomen (M1)–(M5) och (D).*

*Bevis.* Att $\mathbb{R}$ är sluten under multiplikation har du förhoppningsvis redan visat i Övning 5.2. (M2)–(M4) visas på samma sätt som i motsvarande fall för addition och lämnas också som en övning. Den knepiga biten är att visa att $\alpha \cdot \alpha^{-1} = 1$.

(M5) Det räcker med att visa att för varje $\alpha > 0$ så är $\alpha \cdot \alpha^{-1} = 1$. Detta gör vi som i fallet med addition, d.v.s. genom att visa de två inklusionerna $\alpha \cdot \alpha^{-1} \subseteq 1$ och $1 \subseteq \alpha \cdot \alpha^{-1}$. Att bevisa att $\alpha^{-1}$ verkligen är ett snitt lämnas som en övning.

Tag ett element $p \in \alpha$ och ett element $q \in \alpha^{-1}$ där $q \neq 0$. Då gäller det att $q^{-1} \notin \alpha$ vilket betyder att $p < q^{-1}$ som är ekvivalent med att $pq < 1$. Det är vidare klart att även $0 \in 1$. Alltså är $pq \in 1$ för alla $p \in \alpha$ och $q \in \alpha^{-1}$, d.v.s. $\alpha \cdot \alpha^{-1} \subseteq 1$.

Tag ett element $z \in 1$. Om $z < 0$ så är det klart att $z \in \alpha \cdot \alpha^{-1}$ eftersom $\alpha > 0$. Antag nu att $0 < z < 1$, vilket ger oss att $1/z > 1$. Låt oss först anta att $1/z \in \alpha$. Eftersom $1/z > 1$ och $\alpha$ är uppåt begränsad så måste (se Anmärkning 5.1.12) det finnas ett positivt heltal $k$ sådant att

$$x = \left(\frac{1}{z}\right)^k \in \alpha \qquad \text{och} \qquad y = \left(\frac{1}{z}\right)^{k+1} \notin \alpha. \quad (5.13)$$

Det gäller att $1/y \in \alpha^{-1}$ om inte $y$ råkar vara den minsta övre begränsningen till $\alpha$ i vilket fall vi inte kan hitta något $r > 0$ sådant att $y - r \notin \alpha$. Om $1/y \in \alpha^{-1}$ så följer det att

$$z = \frac{z^{k+1}}{z^k} = \frac{\frac{1}{z^k}}{\frac{1}{z^{k+1}}} = x\frac{1}{y}. \quad (5.14)$$

Då $x \in \alpha$ och $1/y \in \alpha^{-1}$ betyder detta att $z \in \alpha \cdot \alpha^{-1}$. Det är dock inget problem om $y$ råkar vara den minsta övre begränsningen till $\alpha$ eftersom vi då kan välja ett $x' \in \alpha$ sådant att $x' > x$ och ett $y' = yx'/x \notin \alpha$ vilket ger oss

$$x' \frac{1}{y'} = \frac{x'x}{yx'} = \frac{x}{y} = z. \tag{5.15}$$

Detta resonemang var under antagandet att $1/z \in \alpha$. Låt oss nu anta att $1/z \notin \alpha$. Antag vidare att $z \notin \alpha$. Eftersom $0 < z < 1$ och $\alpha > 0$ så måste det finnas ett heltal $k$ sådant att

$$x = z^{k+1} \in \alpha \qquad \text{och} \qquad y = z^k \notin \alpha. \tag{5.16}$$

Notera att detta fungerar även då $z \in \alpha$, men kräver lite mer eftertanke. Nu kan vi, precis som ovan, komma runt problemet med att $y$ möjligtvis är den minsta övre begränsningen till $\alpha$. Låt oss anta att detta är avklarat och att $1/y \in \alpha^{-1}$. Vi får

$$z = \frac{z^{k+1}}{z^k} = \frac{x}{y} = x \cdot \frac{1}{y}. \tag{5.17}$$

Då $x \in \alpha$ och $1/y \in \alpha^{-1}$ betyder detta att $z \in \alpha \cdot \alpha^{-1}$. Vi har alltså visat att $1 \subseteq \alpha \cdot \alpha^{-1}$, vilket tillsammans med det tidigare resultatet slutligen visar att $\alpha \cdot \alpha^{-1} = 1$.

(D) För att verifiera den distributiva lagen måste vi visa att för tre snitt $\alpha, \beta, \gamma$ så gäller det att $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$. Vi gör detta genom att bevisa de två inklusionerna

$$\alpha(\beta + \gamma) \subseteq \alpha\beta + \alpha\gamma \qquad \text{och} \qquad \alpha\beta + \alpha\gamma \subseteq \alpha(\beta + \gamma). \tag{5.18}$$

Låt oss först visa dessa två då $\alpha, \beta, \gamma > 0$. Tag ett element $r \in \alpha(\beta + \gamma)$. Om $r \leqslant 0$ så vet vi att $r \in \alpha\beta + \alpha\gamma$, eftersom $\alpha\beta + \alpha\gamma > 0$. Antag istället att $r > 0$. Vi vet att $r$ är på formen

$$r = x(y + z) \tag{5.19}$$

där $x \in \alpha, y \in \beta, z \in \gamma$ och $x, y, z > 0$; allt enligt definitionen av multiplikation. Men eftersom $r = x(y + z) = xy + xz$ så vet vi att $r \in \alpha\beta + \alpha\gamma$. Alltså är $\alpha(\beta + \gamma) \subseteq \alpha\beta + \alpha\gamma$.

Tag nu ett element $r \in \alpha\beta + \alpha\gamma$ sådant att $r > 0$. Vi vet att $r$ är på formen

$$r = x_1 y + x_2 z \tag{5.20}$$

där $x_1, x_2 \in \alpha, y \in \beta, z \in \gamma$ och $x_1, x_2, y, z > 0$. Antag nu att $x_1 \leqslant x_2$. Då vet vi att

$$\frac{x_1}{x_2} y \leqslant y \quad \text{vilket medför att} \quad \frac{x_1}{x_2} y \in \beta. \tag{5.21}$$

Vi kan skriva $r$ som

$$r = x_1 y + x_2 z = x_2 \left( \frac{x_1}{x_2} y + z \right). \tag{5.22}$$

Eftersom $x_2 \in \alpha, x_1 y / x_2 \in \beta$ och $z \in \gamma$ så är $r \in \alpha(\beta + \gamma)$. Notera att om $x_1 > x_2$ så kan vi byta plats på $x_1$ och $x_2$ ovan för att få samma resultat. Detta, tillsammans med det föregående resultatet, visar att $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ då $\alpha, \beta, \gamma > 0$.

Nu måste vi visa att detta gäller även då inte alla tre snitt är positiva. Låt oss fortfarande anta att $\alpha > 0$. Då har vi tre fall

(i) $\beta < 0$ och $\gamma < 0$. Detta visar vi med hjälp av omskrivningen

$$\alpha(\beta + \gamma) = -\alpha\big[-(\beta + \gamma)\big] = -\Big[\alpha(-\beta - \gamma)\Big]. \tag{5.23}$$

Nu är alla tre snitt, d.v.s. $\alpha, -\beta, -\gamma$, positiva och vi kan använda resultatet för positiva snitt för att erhålla

$$\alpha(\beta + \gamma) = -\Big[\alpha(-\beta - \gamma)\Big] = -\Big[-\alpha\beta - \alpha\gamma\Big] = \alpha\beta + \alpha\gamma. \tag{5.24}$$

(ii) $\beta < 0$ och $\gamma > 0$. Om $\beta + \gamma = 0$ så är det klart att likheten gäller. Antag först att $\beta + \gamma > 0$. Då kan vi skriva

$$\alpha\gamma = \alpha\Big[(\beta + \gamma) + (-\beta)\Big]. \tag{5.25}$$

Här noterar vi att de tre snitten $\alpha, \beta + \gamma, -\beta$ är positiva och vi kan använda vårt tidigare resultat för att få

$$\alpha\gamma = \alpha\Big[(\beta + \gamma) + (-\beta)\Big] = \alpha(\beta + \gamma) - \alpha\beta \tag{5.26}$$

vilket medför att

$$\alpha\gamma + \alpha\beta = \alpha(\beta + \gamma). \tag{5.27}$$

Antag nu att $\beta + \gamma < 0$. Då kan vi tänka längs samma banor och göra omskrivningen

$$-\alpha\beta = \alpha\Big[-(\beta + \gamma) + \gamma\Big]. \tag{5.28}$$

Här noterar vi igen att de tre snitten $\alpha, -(\beta + \gamma), \gamma$ är positiva. Det ger oss

$$-\alpha\beta = \alpha\Big[-(\beta + \gamma) + \gamma\Big] = -\alpha(\beta + \gamma) + \alpha\gamma \tag{5.29}$$

vilket medför att

$$\alpha(\beta + \gamma) = \alpha\gamma + \alpha\beta. \tag{5.30}$$

I fallen då $\alpha < 0$ kan vi göra precis samma bevis med skillnaden att vi byter ut $\alpha$ mot $-\alpha$, som då är ett positivt snitt. $\square$

**Anmärkning 5.1.12.** Antag att $q > 1$ är rationellt. För varje positivt heltal $n$ gäller att

$$\begin{aligned} q^n &= \Big(1 + (q-1)\Big)^n \\ &= 1 + n(q-1) + \frac{n(n-1)}{2}(q-1)^2 + \cdots + (q-1)^n \\ &\geqslant 1 + n(q-1). \end{aligned} \tag{5.31}$$

Därför kan vi för varje rationellt tal $p > q$ hitta ett heltal $k$ sådant att $q^k > p$. Dessutom kan man visa att för ett rationellt tal $z$ med $0 < z < 1$ så finns det, för varje rationellt tal $p$ med $0 < p < z$, ett positivt heltal $k$ sådant att $z^k < p$. Dessa egenskaper används i beviset för (M5) ovan.

Efter dessa bevis vet vi att $\mathbb{R}$ är en ordnad kropp. Den sista egenskapen som vi vill visa är supremumegenskapen.

**Lemma 5.1.13.** *De reella talen har supremumegenskapen, d.v.s. för varje $A \subseteq \mathbb{R}$ sådan att $A \neq \emptyset$ och $A$ är uppåt begränsad, existerar det en minsta övre begränsning $\gamma \in \mathbb{R}$ till $A$.*

*Bevis.* Notera att $A$ är en mängd av snitt som i sin tur är mängder av rationella tal. Ett element i $A$ är således ett snitt. Låt oss definiera en ny mängd av rationella tal

$$\gamma = \bigcup_{\alpha \in A} \alpha. \tag{5.32}$$

Med denna beteckning menar vi att $\gamma$ är unionen av alla mängder i $A$. Alltså består $\gamma$ av alla rationella tal i alla snitt som är element i $A$. Vad vi vill visa är att $\gamma$ är den minsta övre begränsningen till $A$, d.v.s. $\gamma = \sup_{\mathbb{R}} A$. Först och främst måste vi försäkra oss om att $\gamma$ är ett snitt. Detta är lämnat till läsaren i Övning 5.3.

Eftersom $\gamma$ är unionen av alla $\alpha \in A$ så är det klart att $\alpha \leqslant \gamma$ för alla $\alpha \in A$. Detta visar att $\gamma$ är en övre begränsning till $A$. Antag att vi har ett $\delta < \gamma$. Låt oss visa att det inte kan vara en övre begränsning. Eftersom $\delta < \gamma$ så måste det finnas ett rationellt tal $p$ sådant att $p \in \gamma$ och $p \notin \delta$. Från definitionen av $\gamma$ måste det finnas ett snitt $\alpha \in A$ sådant att $p \in \alpha$. Men detta betyder att $\delta < \alpha$ eftersom $p \in \alpha$ och $p \notin \delta$, vilket säger att $\delta$ ej kan vara en övre begränsning till $A$. Detta visar att $\gamma$ är den minsta övre begränsningen till $A$. $\square$

Vi har således visat följande sats:

**Sats 5.1.14.** *De reella talen $\mathbb{R}$ är en ordnad kropp som har supremumegenskapen.*

Vi har slutligen lyckats konstruera en mängd med de egenskaper som anses vara specifika för de reella talen. Skulle man kunna tänka sig att det går att konstruera någon annan mängd med samma egenskaper? Finns det således "fler" uppsättningar av reella tal? Svaret är nej. Man kan visa att det väsentligen bara finns en ordnad kropp med supremumegenskapen.

Det är nu förmodligen inte alldeles uppenbart att vi genom denna konstruktion har fått med alla de tal vi "saknar", till exempel $\sqrt{2}$.

**Exempel 5.1.15.** Är $\sqrt{2}$ ett reellt tal? Vi ställer oss alltså frågan: Kan vi hitta ett reellt tal $y$ sådant att $y \cdot y = 2$? Låt oss sätta

$$A = \{x \in \mathbb{R} \,:\, x^2 < 2\}. \tag{5.33}$$

Eftersom mängden helt klart är uppåt begränsad och icke-tom, så existerar supremeum av mängden enligt Lemma 5.1.13. Låt oss sätta

$$y = \sup_{\mathbb{R}} A. \tag{5.34}$$

Vi skall nu visa att $y^2 = 2$ genom att visa att de båda olikheterna $y^2 < 2$ och $y^2 > 2$ är omöjliga. Antag först att $y^2 < 2$ och låt oss välja ett $h \in \mathbb{R}$ sådant att $0 < h < 1$ och

$$h < \frac{2 - y^2}{2y + 1}. \tag{5.35}$$

Då gäller det att

$$\begin{aligned} (y + h)^2 &= y^2 + h(2y + h) < y^2 + h(2y + 1) \\ &< y^2 + \frac{2 - y^2}{2y + 1}(2y + 1) = y^2 + 2 - y^2 = 2. \end{aligned} \tag{5.36}$$

Alltså är $y + h \in A$ och eftersom $y + h > y$ så motsäger detta att $y$ är en övre begränsning till $A$. Alltså är $y^2 < 2$ omöjligt.

Antag nu att $y^2 > 2$ och låt oss sätta

$$k = \frac{y^2 - 2}{2y}. \tag{5.37}$$

Då $y^2 > 2$ så är $k > 0$. Låt oss beräkna $(y - k)^2$:

$$\begin{aligned} (y - k)^2 &= y^2 + k^2 - 2yk > y^2 - 2yk = y^2 - 2y\frac{y^2 - 2}{2y} \\ &= y^2 - (y^2 - 2) = 2. \end{aligned} \tag{5.38}$$

Det följer att $y - k$ är en övre begränsning till $A$, och eftersom $y - k < y$ så motsäger detta att $y$ är den minsta övre begränsningen till $A$. Alltså är det inte möjligt att $y^2 > 2$.

Eftersom varken $y^2 < 2$ eller $y^2 > 2$, och eftersom ordningsrelationen $<$ uppfyller ett av påståendena $x < z$, $x > z$ och $x = z$ för alla $x, z \in \mathbb{R}$, så måste $y^2 = 2$. ▲

## 5.2 Decimaltalsutvecklingar

Att använda sig av decimaltal kan i många fall vara praktiskt. Det ger oss ett enkelt sätt att jämföra storleken på olika tal. Vad har decimaltal för relation till de reella talen, d.v.s. de snitt som vi har konstruerat? Det ska vi reda ut.

Decimaltalen använder sig av ett positionssystem byggt på heltalet 10. Vad vi egentligen menar med beteckningen $a_0.a_1a_2a_3\ldots$ är en summa av rationella tal

$$a_0.a_1a_2a_3\cdots = a_0 + \frac{a_1}{10} + \frac{a_2}{100} + \frac{a_3}{1000} + \cdots = \frac{a_0}{10^0} + \frac{a_1}{10^1} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + \cdots \tag{5.39}$$

Om endast ett ändligt antal av decimalerna $a_k$ är nollskilda så blir resultatet förstås ett rationellt tal.

**Exempel 5.2.1.**

$$0.125 = \frac{0}{1} + \frac{1}{10} + \frac{2}{100} + \frac{5}{1000} = \frac{100+20+3}{1000} = \frac{125}{1000} = \frac{5}{40} = \frac{1}{8}. \tag{5.40}$$

▲

Lite svårare kan det vara att inse att $0.333\cdots$ faktiskt är det rationella talet $1/3$. Här kan vi dock använda oss av ett litet trick. Sätt $x = 0.333\cdots$. Då är $10x = 3.333\cdots$ vilket ger oss att

$$10x - x = 3.333\cdots - 0.333\cdots = 3 \tag{5.41}$$

vilket medför

$$x = \frac{1}{3}. \tag{5.42}$$

I själva verket kan man visa att alla periodiska decimalutvecklingar, d.v.s. där samma grupp siffror kommer igen efter varandra, är rationella tal.

Vårt mål är att visa att vi kan representera alla reella tal med decimaltal. För att åstadkomma detta måste vi definiera decimaltal på ett lite mer abstrakt vis.

**Definition 5.2.2.** Låt $a_0, a_1, a_2, \ldots$ vara heltal sådana att $a_0 \geqslant 0$ och $0 \leqslant a_k \leqslant 9$ för $k = 1, 2, \ldots$. Vi definierar *decimaltalet* $a_0.a_1a_2\cdots$ som

$$a_0.a_1a_2\cdots = \sup_{\mathbb{R}} \left\{ a_0 + \frac{a_1}{10} + \cdots + \frac{a_k}{10^k} \text{ för } k = 0, 1, 2, \ldots \right\} \tag{5.43}$$

Notera att mängden i högerledet ovan är en mängd av rationella tal eftersom varje element är en ändlig summa av rationella tal. Då mängden inte är tom och uppåt begränsad, till exempel av $a_0+1$, så existerar supremum av mängden enligt Lemma 5.1.13. Alltså är $a_0.a_1a_2\cdots$ ett reellt tal.

**Exempel 5.2.3.**

$$0.125 = \sup_{\mathbb{R}} \left\{ 0, \frac{1}{10}, \frac{12}{100}, \frac{125}{1000} \right\} = \frac{125}{1000} \tag{5.44}$$

▲

**Exempel 5.2.4.**

$$0.333\cdots = \sup_{\mathbb{R}} \left\{ 0, \frac{3}{10}, \frac{33}{100}, \frac{333}{1000}, \frac{3333}{10000}, \ldots \right\} \tag{5.45}$$

▲

Omvänt så är det enkelt att till ett givet snitt $\alpha$ konstruera tal $a_0, a_1, a_2, \ldots$ sådana att $a_0.a_1a_2\cdots = \alpha$. Nämligen, låt $\alpha > 0$ och låt $a_0$ vara det största positiva heltalet sådant att $a_0 \leqslant \alpha$. Låt sedan $a_1$ vara det största positiva heltalet sådant att $\alpha_0 + \alpha_1/10 \leqslant \alpha$. Låt $a_k$, för $k = 0, 1, 2, \ldots$, vara det största positiva heltalet sådant att

$$a_0 + \frac{a_1}{10} + \cdots + \frac{a_{k-1}}{10^{k-1}} + \frac{a_k}{10^k} \leqslant \alpha. \tag{5.46}$$

**Lemma 5.2.5.** *Låt $a_0, a_1, a_2, \ldots$ vara konstruerade från snittet $\alpha$, som ovan. Då är $a_0.a_1a_2\cdots = \alpha$.*

*Bevis.* Låt oss definiera

$$e_k = a_0 + \frac{a_1}{10} + \cdots + \frac{a_k}{10^k} \tag{5.47}$$

för $k = 0, 1, 2, \ldots$, och

$$E = \{e_0, e_1, e_2, \ldots\}. \tag{5.48}$$

Vi vill visa att $\alpha$ är den minsta övre begränsningen till mängden $E$. Att $\alpha$ är en övre begränsning är klart från definitionen av talen $a_k$. Från konstruktionen av $a_k$ följer det att

$$\alpha - e_k \leqslant \frac{1}{10^k}. \tag{5.49}$$

Tag nu ett godtyckligt $\beta \in \mathbb{R}$ sådant att $\beta < \alpha$. Vi vill visa att $\beta$ inte är en övre begränsning till $E$. Om vi definierar $\gamma = \alpha - \beta$ så är $\gamma > 0$ eftersom $\beta < \alpha$. Tag nu ett heltal $N$ sådant att $10^{-N} < \gamma$. Från (5.49) får vi att

$$e_N \geqslant \alpha - \frac{1}{10^N} > \alpha - \gamma = \beta. \tag{5.50}$$

Alltså kan inte $\beta$ vara en övre begränsning till $E$. Detta visar att $\alpha$ är den minsta övre begränsningen, d.v.s. supremum, till $E$. □

Vad vi har visat är att vi till varje snitt kan konstruera ett decimaltal och för alla val av $a_k$ så är $a_0.a_1a_2\cdots$ ett snitt. Det är klart att konstruktionen ovan ger oss exakt ett decimaltal för ett givet snitt $\alpha$. Frågan är om två decimaltal $a_0.a_1a_2\cdots$ och $b_0.b_1b_2\cdots$ som är olika, d.v.s. där det finns ett $k$ sådant att $a_k \neq b_k$, kan representera samma snitt? Detta besvaras av följande exempel.

**Exempel 5.2.6.** Vi ska visa att $0.999\cdots = 1$. Låt $a_0 = 0$ och $a_k = 9$ för alla $k \geqslant 1$. Vi måste visa att $a_0.a_1a_2\cdots = 1$, d.v.s.

$$\sup_{\mathbb{R}} \left\{0, \frac{9}{10}, \frac{99}{100}, \dots\right\} = 1. \tag{5.51}$$

Vi noterar att om vi definierar $e_k$ som i beviset ovan så är

$$1 - e_k = \frac{1}{10^k} \tag{5.52}$$

Vi kan nu för varje reellt tal $a$ sådant att $0 < a < 1$ hitta ett heltal $N$ sådant att $e_N > a$. Alltså måste 1 vara supremum av mängden ovan. Detta visar att $0.999\cdots = 1$. ▲

Att det finns flera olika decimaltal som representerar samma snitt är inte så farligt då vi kan visa att fallet med återkommande nior är det enda exemplet. Vi säger att ett decimaltal $a_0.a_1a_2\cdots$ innehåller *återkommande nior* om det finns något $k \geqslant 0$ sådant att $a_l = 9$ för alla $l > k$. Med andra ord så finns det ett $k \geqslant 0$ sådant att

$$a_0.a_1a_2\cdots = a_0.a_1a_2\cdots a_k999\cdots. \tag{5.53}$$

Från Exempel 5.2.6 drar vi slutsatsen om att $a_k \leqslant 8$ så är

$$a_0.a_1a_2\cdots a_k999\cdots = a_0.a_1a_2\cdots(a_k+1)000\cdots. \tag{5.54}$$

**Exempel 5.2.7.**

$$0.124999\cdots = 0.125 \tag{5.55}$$
$$1.2999\cdots = 1.3 \tag{5.56}$$

▲

**Lemma 5.2.8.** *Låt $a_0.a_1a_2\cdots$ och $b_0.b_1b_2\cdots$ vara två decimaltal som ej innehåller återkommande nior. Antag att det existerar ett $k \geqslant 0$ sådant att $a_k \neq b_k$. Då är $a_0.a_1a_2\cdots \neq b_0.b_1b_2\cdots$.*

*Bevis.* Vi inför som tidigare beteckningarna

$$e_k = a_0 + \frac{a_1}{10} + \cdots + \frac{a_k}{10^k} \tag{5.57}$$
$$f_k = b_0 + \frac{b_1}{10} + \cdots + \frac{b_k}{10^k}. \tag{5.58}$$

Låt vidare $k_0$ vara det minsta heltalet sådant att $a_{k_0} \neq b_{k_0}$. Vi kan också anta att $b_{k_0} > a_{k_0}$. Eftersom vi har antagit att $a_0.a_1a_2\cdots$ ej har några återkommande nior så finns det ett heltal $m > k_0$ sådant att $a_m \neq 9$. Alltså är $e_l \leqslant f_{k_0} - 1/10^m$ för alla $l \geqslant k_0$ vilket betyder att

$$a_0.a_1a_2\cdots \leqslant f_{k_0} - \frac{1}{10^m}. \tag{5.59}$$

Men då måste $a_0.a_1a_2\cdots \neq b_0.b_1b_2\cdots$ eftersom $b_0.b_1b_2\cdots \geqslant f_{k_0}$. □

Detta visar att det enda fall då två decimaltal med olika siffror representerar samma reella tal uppkommer genom återkommande nior.

**Övning 5.1.** Låt $\alpha$ och $\beta$ vara två snitt. Visa att $\alpha + \beta$ är ett snitt.

**Övning 5.2.** Låt $\alpha > 0$ och $\beta > 0$ vara två snitt. Visa att $\alpha \cdot \beta$ är ett snitt.

**Övning 5.3.** Låt $A$ vara en delmängd av $\mathbb{R}$ sådan att $A \neq \emptyset$ och $A$ är uppåt begränsad. Definiera $\gamma$ som

$$\gamma = \bigcup_{\alpha \in A} \alpha \tag{5.60}$$

Visa att $\gamma$ är ett snitt.

**Övning 5.4.** Sätt

$$\alpha = \{q \in \mathbb{Q} : q > 0 \text{ och } q^2 < 2\} \cup \{q \in \mathbb{Q} : q \leqslant 0\}. \tag{5.61}$$

Visa att $\alpha$ är ett snitt. *Ledning:* För att visa egenskap (R3) tag $r = p + (2 - p^2)/(p+1)$.

# 6 Algebraiska och transcendenta tal

## 6.1 Kardinaliteten av $\mathbb{R}$

**Sats 6.1.1.** *Mängden $\mathbb{R}$ av alla reella tal är överuppräknelig.*

*Bevis.* Från föregående avsnitt vet vi att vi kan från alla reella tal $x$ konstruera ett decimaltal sådant att

$$x = a_0.a_1a_2a_3\dots. \tag{6.1}$$

Vi vet också från konstruktionen att $a_0.a_1a_2\cdots$ inte kommer att innehålla några återkommande nior.

Vi ska nu konstruera ett motsägelsebevis; d.v.s. vi antar att mängden $\mathbb{R}$ är uppräknelig och visar att det leder till en motsägelse. Detta visar då att $\mathbb{R}$ är överuppräknelig.

Antag att mängden $\mathbb{R}$ är uppräknelig. Då kan vi räkna upp alla tal i $\mathbb{R}$ på följande sätt

$$\mathbb{R} = \{x^{(0)}, x^{(1)}, x^{(2)}, x^{(3)}, \dots\} \tag{6.2}$$

där

$$\begin{aligned}
x^{(0)} &= a_{00}.a_{01}a_{02}a_{03}\dots \\
x^{(1)} &= a_{10}.a_{11}a_{12}a_{13}\dots \\
x^{(2)} &= a_{20}.a_{21}a_{22}a_{23}\dots \\
x^{(3)} &= a_{30}.a_{31}a_{32}a_{33}\dots \\
&\vdots
\end{aligned} \tag{6.3}$$

Nu vill vi definiera ett nytt reellt tal $y$ och visa att det inte finns med i listan ovan. Vi sätter

$$y = c_0.c_1c_2c_3\dots \tag{6.4}$$

där vi definierar $c_k$ som

$$c_k = \begin{cases} 1 & \text{om } a_{kk} = 0 \\ 0 & \text{om } a_{kk} \in \{1,2,3,4,5,6,7,8,9\}. \end{cases} \tag{6.5}$$

Genom att definiera $c_k$ på detta sätt så har vi sett till att $c_k \neq a_{kk}$ för alla $k$. Detta betyder att det inte finns något tal i listan (6.3) som är lika med $y$, eftersom $y$ med säkerhet skiljer sig från $x^{(k)}$ i den $k$:te decimalen, och vi vet att decimaltal med olika siffror och utan återkommande nior representerar olika reella tal. Att $y$ inte innehåller några återkommande nior är klart.

Vi har från antagandet att alla tal i $\mathbb{R}$ kan räknas upp konstruerat ett reellt tal som ej finns med i uppräkningen. Detta motsäger att $\mathbb{R}$ är uppräknelig och således måste $\mathbb{R}$ vara överuppräknelig. □

## 6.2 Algebraiska tal

**Definition 6.2.1.** Ett *polynom* $p(x)$ i variabeln $x$ är en summa på formen

$$p(x) = \sum_{k=0}^{n} a_k x^k = a_n x^n + a_n x^{n-1} + \cdots + a_1 x + a_0 \tag{6.6}$$

för något heltal $n \geqslant 0$ och $a_k \in \mathbb{R}$. Vi kallar talen $a_k$ för *koefficienter* i polynomet. Om alla koefficienter i ett polynom är heltal så säger vi att polynomet är ett *heltalspolynom*. Vidare är polynomet *nollskilt* om $a_k \neq 0$ för minst ett värde på $k$. Vi definierar *graden* av ett nollskilt polynom som det största heltal $m$ sådant att $a_m \neq 0$.

**Definition 6.2.2.** Ett reellt tal $y$ är *algebraiskt* om det existerar ett nollskilt heltalspolynom $p(x)$ sådant att

$$p(y) = a_n y^n + a_n y^{n-1} + \cdots + a_1 y + a_0 = 0. \tag{6.7}$$

Vi betecknar mängden av algebraiska tal med $\mathbb{A}$.

**Exempel 6.2.3.** Alla rationella tal är algebraiska. Tag ett rationellt tal $y = a/b$; då uppfyller $y$ en ekvation av typen (6.7) där $n = 1$, $a_1 = b$ och $a_0 = -a$. Alltså

$$a_1 y + a_0 = b\frac{a}{b} - a = a - a = 0. \tag{6.8}$$

▲

**Exempel 6.2.4.** Talet $\sqrt{2}$ är algebraiskt. Tag $n = 2$, $a_2 = 1, a_1 = 0$ och $a_0 = -2$. Detta ger

$$a_2 y^2 + a_1 y + a_0 = \left(\sqrt{2}\right)^2 - 2 = 2 - 2 = 0. \tag{6.9}$$

▲

**Anmärkning 6.2.5.** För ett algebraiskt tal $y$ kan det finnas mer än ett polynom sådant att $p(y) = 0$. Tag till exempel $p(x) = x^2 - 2$ och $q(x) = x^4 - 4$. Då kan du lätt kontrollera att $p\left(\sqrt{2}\right) = q\left(\sqrt{2}\right) = 0$. Ordalydelsen ”det existerar” i definition (6.2.2) betyder att det finns minst ett sådant polynom.

**Sats 6.2.6.** *De algebraiska talen är uppräkneliga.*

*Bevis.* Vi antar att vi känner till en grundläggande sats från algebran: Ett polynom har endast ett ändligt antal rötter. Kan vi nu visa att mängden av alla heltalspolynom är uppräknelig, så vet vi att mängden av algebraiska tal är uppräknelig ty varje algebraiskt tal måste vara en rot till ett heltalspolynom och en uppräknelig union av ändliga mängder är igen uppräknelig (se Sats 3.3.5). Det är dock ganska lätt att inse att mängden av alla heltalspolynom är uppräknelig. Definiera *rangen* $N$ av ett heltalspolynom som

$$N = n + |a_0| + |a_1| + \cdots + |a_n|. \tag{6.10}$$

Vi inser nu att för ett givet $N$ så finns det bara ett ändligt antal sätt, säg $k_N$, att välja $a_0, \ldots, a_n \in \mathbb{Z}$ på, så att polynomets rang är $N$. Vi kan skriva polynomen som motsvarar dessa val som

$$E_{N,1}, E_{N,2}, \ldots, E_{N,k_N}. \tag{6.11}$$

På detta sätt kan vi numrera alla heltalspolynom med heltalen i ordningen

$$E_{1,1}, \ldots, E_{1,k_1}, E_{2,1}, \ldots, E_{2,k_2}, \ldots \tag{6.12}$$

Alltså är mängden av alla heltalspolynom uppräknelig, och satsen följer enligt resonemanget ovan. □

## 6.3 Transcendenta tal

**Definition 6.3.1.** Ett reellt tal $x$ kallas *transcendent* om det inte är algebraiskt. Vi betecknar mängden av de transcendenta talen med $\mathbb{T}$.

Den första frågan vi ställer oss är naturligtvis: Finns det några transcendenta tal? Svaret är en enkel följd av satserna ovan.

**Sats 6.3.2.** *Det existerar ett överuppräkneligt antal transcendenta tal.*

*Bevis.* Eftersom $\mathbb{R}$ är överuppräknelig och $\mathbb{A}$ är uppräknelig så måste det existera ett överuppräkneligt antal transcendenta tal, eftersom om $\mathbb{T}$ vore uppräknelig så skulle $\mathbb{R} = \mathbb{A} \cup \mathbb{T}$ vara uppräknelig enligt Sats 3.3.5. □

**Anmärkning 6.3.3.** Notera att detta betyder att de allra flesta reella tal är transcendenta.

När vi har fastställt att det finns många transcendenta tal, kan vi hitta några exempel? Två exempel som du säkert känner igen är talen $\pi$ och $e$ och vi ska i nästa avsnitt visa att $e$ verkligen är transcendent. I själva verket är det ganska svårt att hitta exempel på transcendenta tal, vilket känns tämligen olustigt då de flesta reella tal är transcendenta.

## 6.4 Definition av $e^x$

Faktulteten $n!$ av ett heltal $n \geqslant 0$ är definierad som

$$\begin{aligned} n! &= n(n-1)(n-2)\cdots 3 \cdot 2 \cdot 1 \\ 0! &= 1. \end{aligned} \tag{6.13}$$

**Exempel 6.4.1.** Vi beräknar $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$. ▲

Fakulteten är användbar i många sammanhang; det visar sig till exempel att vi kan räkna ut potenser av summan av två tal som

$$(x+h)^r = \sum_{k=0}^{r} \frac{r!}{k!(r-k)!} x^{r-k} h^k. \tag{6.14}$$

**Exempel 6.4.2.** Vi utvecklar $(x+h)^3$ enligt formeln ovan

$$\begin{aligned}(x+h)^3 &= \frac{3!}{0!3!}x^3h^0 + \frac{3!}{1!2!}x^2h^1 + \frac{3!}{2!1!}x^1h^2 + \frac{3!}{3!0!}x^0h^3 \\ &= x^3 + 3x^2h + 3xh^2 + h^3.\end{aligned} \tag{6.15}$$

▲

Då vi i nästa avsnitt vill visa att $e$ är transcendent så måste vi börja med att definiera exponentialfunktionen. Som definition på $e^x$ tar vi följande

$$e^x = \sum_{n=0}^{\infty} \frac{x^k}{n!} = \frac{1}{0!} + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots . \tag{6.16}$$

Genom att ta med ett ändligt antal av dessa termer, låt oss säga 100, kan vi få ett närmevärde för $e = e^1$

$$e \approx \sum_{n=0}^{100} \frac{1}{n!} = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots + \frac{1}{100!} \approx 2.718281828. \tag{6.17}$$

För att visa att $e$ är transcendent är vi hjälpta av att införa en mängd nya beteckningar. På detta sätt kan vi lättare strukturera beviset och dela upp det i ett par mindre delar.

Låt $\phi(h)$ vara ett polynom

$$\phi(h) = \sum_{r=0}^{n} c_r h^r = c_0 + c_1 h + c_2 h^2 + \cdots + c_n h^n. \tag{6.18}$$

Vi definierar en avbildning $T_x$ som ”förskjuter” polynomets variabel med det reella talet $x$

$$\big(T_x\phi\big)(h) = \phi(x+h) = \sum_{r=0}^{n} c_r (x+h)^r. \tag{6.19}$$

Vi ser alltså på detta som ett polynom i $h$ (där $x$ ingår i koefficienterna) och kan skriva det som

$$\big(T_x\phi\big)(h) = \sum_{r=0}^{n} d_r(x) h^r \tag{6.20}$$

där vi förstås kan beräkna $d_r(x)$ från $c_r$.

**Exempel 6.4.3.** Låt $\phi(h) = h^2 - 3$, vilket ger $c_2 = 1, c_1 = 0, c_0 = -3$. Vi får då $\big(T_x\phi\big)(h) = (x+h)^2 - 3 = h^2 + 2xh + x^2 - 3$, vilket ger $d_2(x) = 1$, $d_1(x) = 2x, d_0(x) = x^2 - 3$. ▲

Vidare definierar vi avbildningen $H$, som tar ett polynom och skapar det reella talet

$$H\big(\phi\big) = \sum_{r=0}^{n} c_r r!, \tag{6.21}$$

d.v.s. vi ersätter $h^r$ i polynomet med fakulteten på exponenten $r$.

**Exempel 6.4.4.** Låt $\phi(h)$ vara som i Exempel 6.4.3. Detta ger oss att $H(\phi) = c_2 2! + c_1 1! + c_0 0! = 1 \cdot 2 + 0 \cdot 1 - 3 \cdot 1 = -1.$ ▲

Vi kan också avbilda $\big(T_x\phi\big)(h)$ med $H$

$$H\big(T_x\phi\big) = \sum_{r=0}^{n} d_r(x) r! \tag{6.22}$$

Notera att detta är ett polynom i variabeln $x$.

**Exempel 6.4.5.** Låt $\phi(h)$ vara som i Exempel 6.4.3. Då får vi $H\big(T_x\phi\big) = d_2(x)2! + d_1(x)1! + d_0(x)0! = 2! + 2x \cdot 1! + (x^2 - 3) \cdot 0! = x^2 + 2x - 1$ ▲

Vi inför slutligen ytterligare två beteckningar, $u_r(x)$ och $\varepsilon_r(x)$, genom

$$u_r(x) = \sum_{k=1}^{\infty} \frac{r!x^k}{(r+k)!} \tag{6.23}$$

$$\varepsilon_r(x) = e^{-|x|} u_r(x) \tag{6.24}$$

för $r = 0, 1, 2, \ldots$.

**Övning 6.1.** En avbildning $L$ sägs vara *linjär* om $L(a\phi + b\psi) = aL(\phi) + bL(\psi)$, där $a, b \in \mathbb{R}$. Denna egenskap leder direkt till att vi har likheten

$$L\left[\sum_{r=0}^{n} c_r \phi_r\right] = \sum_{r=0}^{n} c_r L(\phi_r). \tag{6.25}$$

Visa att avbildningen $H$ är linjär.

**Övning 6.2.** Visa att avbildningen $T_x$ är linjär.

**Övning 6.3.** Visa att

$$(x+h)^4 = \sum_{k=0}^{4} \frac{4!}{k!(4-k)!} x^{4-k} h^k. \tag{6.26}$$

**Övning 6.4.** För ett polynom av grad $n$ definierar vi rangen $N$ som

$$N = n + |a_0| + |a_1| + \cdots + |a_n|. \tag{6.27}$$

Hur många polynom av grad 2 och rang 4 finns det?

# 7 Talet $e$ är transcendent

## 7.1 Några förberedande lemman

Vi har tidigare definierat ett antal begrepp och symboler som kommer att hjälpa oss i vårt bevis. Vi ska nu visa ett par lemman som rör dessa objekt.

**Lemma 7.1.1.** *För alla heltal $r \geqslant 0$ är $|\varepsilon_r(x)| < 1$.*

*Bevis.* Låt oss jämföra definitionerna av $e^x$ och $u_r(x)$

$$e^x = 1 + x + \frac{x^2}{2!} + \cdots \tag{7.1}$$

$$u_r(x) = \frac{x}{r+1} + \frac{x^2}{(r+1)(r+2)} + \cdots \tag{7.2}$$

Låt oss anta att $x > 0$, vilket betyder att varje term är positiv i båda summorna ovan. Eftersom nämnaren tillhörande $x^k$ i $u_r(x)$ alltid är större än motsvarande nämnare i $e^x$, så kommer $u_r(x) < e^x$. Dock kan vi inte dra denna slutsats för negativa $x$ eftersom vi då möjligtvis subtraherar mindre tal i $u_r(x)$ än i $e^x$. Vi kan därför i allmänhet bara säga att $u_r(|x|) < e^{|x|}$. Men eftersom $|u_r(x)| \leqslant u_r(|x|)$ så betyder det att $|u_r(x)| < e^{|x|}$. Detta ger oss

$$|\varepsilon_r(x)| = |e^{-|x|}u_r(x)| = e^{-|x|}|u_r(x)| < e^{-|x|}e^{|x|} = 1. \tag{7.3}$$

□

**Lemma 7.1.2.** *Låt $\phi(x) = c_0 + c_1x + \cdots + c_nx^n$ och låt $\psi(x)$ vara*

$$\psi(x) = \sum_{r=0}^{n} c_r \varepsilon_r(x) x^r \tag{7.4}$$

*med $\varepsilon_r(x)$ som i (6.24). Då följer det att*

$$e^x H(\phi) = H\big(T_x\phi\big) + \psi(x)e^{|x|}. \tag{7.5}$$

*Bevis.* Definiera polynomen $p_r(h) = h^r$ för $r = 1, 2, \ldots$, vilket ger direkt att $H(p_r) = r!$. Vi räknar ut följande uttryck

$$\begin{aligned} H\big(T_x p_r\big) &= \sum_{k=0}^{r} \frac{r!}{k!(r-k)!} x^{r-k} k! = \sum_{k=0}^{r} \frac{r!}{(r-k)!} x^{r-k} \\ &= r!\left[1 + x + \frac{x^2}{2!} + \cdots + \frac{x^r}{r!}\right] = r!\left[e^x - \sum_{k=r+1}^{\infty} \frac{x^k}{k!}\right] \\ &= r!e^x - r!\sum_{k=1}^{\infty} \frac{x^{r+k}}{(r+k)!} = r!e^x - x^r \sum_{k=1}^{\infty} \frac{r!x^k}{(r+k)!} \\ &= r!e^x - u_r(x)x^r = H(p_r)e^x - u_r(x)x^r \end{aligned} \tag{7.6}$$

vilket visar att

$$e^x H(p_r) = H\big(T_x p_r\big) + u_r(x) x^r. \tag{7.7}$$

Nu vill vi räkna ut $H(\phi)$ och noterar att eftersom $\phi(x)$ kan skrivas som

$$\phi(x) = \sum_{r=0}^{n} c_r p_r(x) \tag{7.8}$$

så blir

$$H(\phi) = H\left[\sum_{r=0}^{n} c_r p_r\right] = \sum_{r=0}^{n} c_r H(p_r) \tag{7.9}$$

(se övning 6.1). Men vi har tidigare räknat ut $e^x H(p_r)$, vilket ger oss

$$\begin{aligned} e^x H(\phi) &= \sum_{r=0}^{n} c_r e^x H(p_r) = \sum_{r=0}^{n} c_r \Big[H\big(T_x p_r\big) + u_r(x) x^r\Big] \\ &= \sum_{r=0}^{n} c_r H\big(T_x p_r\big) + \sum_{r=0}^{n} c_r u_r(x) x^r \end{aligned} \tag{7.10}$$

Från ekvation (6.24) vet vi att $u_r(x) = e^{|x|}\varepsilon_r(x)$ vilket ger oss

$$\begin{aligned} e^x H(\phi) &= H\left[T_x\left(\sum_{r=0}^{n} c_r p_r\right)\right] + \sum_{r=0}^{n} c_r e^{|x|}\varepsilon_r(x) x^r \\ &= H\big(T_x\phi\big) + e^{|x|}\psi(x) \end{aligned} \tag{7.11}$$

vilket skulle visas. □

**Lemma 7.1.3.** *Låt $b(x)$ vara ett heltalspolynom och $m \geqslant 1$. Definiera*

$$f(x) = \frac{x^{m-1}}{(m-1)!} b(x) \qquad\qquad g(x) = \frac{x^m}{(m-1)!} b(x) \tag{7.12}$$

*Då är $H(f)$ och $H(g)$ heltal och*

$$H(f) \equiv b(0) \pmod{m} \qquad\qquad H(g) \equiv 0 \pmod{m} \tag{7.13}$$

**Anmärkning 7.1.4.** Se Exempel 1.3.7 om du inte kommer ihåg hur moduloräkning definierades. Här har vi dessutom utökat definitionsområdet från de positiva heltalen till $\mathbb{Z}$. Notera vidare att $a \equiv 0 \pmod{m}$ betyder att $a$ är delbart med $m$.

*Bevis.* Vi antar alltså att $b(x)$ är ett heltalspolynom, d.v.s. vi kan skriva det som

$$b(x) = \sum_{r=0}^{n} a_r x^r \tag{7.14}$$

där $a_0, a_1, \ldots, a_n \in \mathbb{Z}$. Detta ger oss $f(x)$ som

$$f(x) = \frac{x^{m-1}}{(m-1)!} b(x) = \sum_{r=0}^{n} \frac{a_r}{(m-1)!} x^{r+m-1} \tag{7.15}$$

och vi kan beräkna $H(f)$

$$H(f) = \sum_{r=0}^{n} a_r \frac{(r+m-1)!}{(m-1)!} = a_0 + \sum_{r=1}^{n} a_r \Big[(r+m-1)(r+m-2)\cdots m\Big] \tag{7.16}$$

Vi noterar att alla termer i summan då $r \geqslant 1$ kommer att vara delbara med $m$, vilket i termer av modulorelationen betyder att de är kongruenta med 0 modulo $m$. Den enda term som kan vara kongruent med med någonting annat är den som motsvarar $r = 0$ i summan. Alltså

$$H(f) \equiv a_0 = b(0) \pmod{m} \tag{7.17}$$

På samma sätt får vi för $g(x)$ att

$$H(g) = \sum_{r=0}^{n} a_r \frac{(r+m)!}{(m-1)!} \tag{7.18}$$

Här inser vi att detta uttryck är delbart med $m$ för alla $r \geqslant 0$, vilket betyder att hela summan är delbar med $m$. Alltså är $H(g) \equiv 0 \pmod{m}$. $\square$

## 7.2 Bevis för att $e$ är transcendent

Nu närmar vi oss ett bevis för att $e$ är transcendent. De lemman som vi visat ovan uppkommer då man försöker sig på ett bevis och inser att dessa är nyckelingredienserna. Genom att lösgöra dem från huvudbeviset så uppnår vi en klarare och förhoppningsvis mer pedagogisk framställning. Beviset vi kommer att presentera kommer från ”The Theory of Numbers” av Hardy och Wright.

Innan vi ger oss in i detaljerna, låt oss först diskutera strukturen av det kommande beviset. Eftersom definitionen av ett transcendent tal (och den enda karakteriseringen vi känner till i detta kompendium) är att det *inte* är algebraiskt, så måste vi konstruera ett bevis där vi antar att $e$ är algebraiskt och visar att det leder till något som är orimligt, d.v.s. ett motsägelsebevis. Idén är alltså att vi antar att det finns ett heltalspolynom $q(x)$ sådant att

$$q(e) = \sum_{r=0}^{n} c_r e^r = 0. \tag{7.19}$$

Vi ska sedan visa att $q(e)$ är proportionellt mot en summa av två termer, $S_1$ och $S_2$, och istället för ekvationen ovan kan vi då studera $S_1 + S_2 = 0$. Slutligen visar vi, genom att ingående studera dessa två termer, att detta aldrig kan vara uppfyllt, och vi har fått vår motsägelse.

**Sats 7.2.1.** *Talet e är transcendent.*

*Bevis.* Låt oss anta att $e$ är algebraiskt, d.v.s. att det existerar ett nollskilt heltalspolynom $q(x)$ sådant att

$$q(e) = \sum_{r=0}^{n} c_r e^r = 0. \tag{7.20}$$

Vi kan alltid anta att $c_0 \neq 0$ (annars kan vi dividera hela polynomet med $e^k$, där $k$ är det minsta tal för vilket $c_k \neq 0$, vilket ger oss ett nytt polynom där $d_0 = c_k \neq 0$). Låt $p$ beteckna ett primtal som är större än både $n$ och $|c_0|$. Låt oss nu definiera

$$\phi(x) = \frac{x^{p-1}}{(p-1)!}\Big[(x-1)(x-2)\cdots(x-n)\Big]^p. \tag{7.21}$$

Vi passar på att beräkna $H(\phi)$ modulo $p$, eftersom vi kommer att behöva det lite senare. Använder vi nu Lemma 7.1.3 med $m = p$ och

$$b(x) = \Big[(x-1)(x-2)\cdots(x-n)\Big]^p \tag{7.22}$$

så följer det att

$$H(\phi) \equiv b(0) = \big((-1)(-2)\cdots(-n)\big)^p = (-1)^{np}\big(n!\big)^p \pmod{p}. \tag{7.23}$$

Vi har att

$$H(\phi)q(e) = \sum_{r=0}^{n} c_r e^r H(\phi) = 0 \tag{7.24}$$

eftersom $q(e) = 0$ enligt antagandet om att $e$ är algebraiskt. Den uppmärksamme läsaren känner nog igen faktorn $e^r H(\phi)$ och inser kanske att vi är ute efter att tillämpa Lemma 7.1.2 som säger att $e^r H(\phi) = H\big(T_x\phi\big) + \psi(r)e^{|r|}$ vilket ger oss

$$\begin{aligned} H(\phi)q(e) &= \sum_{r=0}^{n} c_r \Big(H\big(T_r\phi\big) + \psi(r)e^{|r|}\Big) && (7.25)\\ &= \sum_{r=0}^{n} c_r H\big(T_r\phi\big) + \sum_{r=0}^{n} c_r\psi(r)e^{|r|} && (7.26) \end{aligned}$$

Låt oss nu definiera $S_1$ och $S_2$ som

$$\begin{aligned} S_1 &= \sum_{r=0}^{n} c_r H\big(T_r\phi\big) && (7.27)\\ S_2 &= \sum_{r=0}^{n} c_r\psi(r)e^{|r|}. && (7.28) \end{aligned}$$

Alltså måste

$$S_1 + S_2 = 0. \tag{7.29}$$

Det vi nu skall visa är att $|S_1| \geqslant 1$ och $|S_2| \leqslant 1/2$ vilket betyder att summan av $S_1$ och $S_2$ aldrig kan vara 0. Lyckas vi med detta så har vi alltså fått en motsägelse till antagandet att $e$ är algebraiskt. Således måste $e$ vara transcendent.

Vi börjar med att visa att $|S_1| \geqslant 1$. Per definition är

$$S_1 = \sum_{r=0}^{n} c_r H\big(T_r\phi\big). \tag{7.30}$$

Första steget är att visa att $H\big(T_r\phi\big) \equiv 0 \pmod p$ då $1 \leqslant r \leqslant n$.

$$\begin{aligned}\big(T_r\phi\big)(x) &= \frac{(x+r)^{p-1}}{(p-1)!}\Big[(x+r-1)(x+r-2)\cdots x(x-1)\cdots(x+r-n)\Big]^p \\ &= \frac{x^p(x+r)^{p-1}}{(p-1)!}\Big[(x+r-1)\cdots(x+1)(x-1)\cdots(x+r-n)\Big]^p\end{aligned}$$

Betraktar vi detta som ett polynom i $x$ så kommer vi alltid kunna bryta ut en faktor $x^p$ då $1 \leqslant r \leqslant n$. Alltså

$$\big(T_r\phi\big)(x) = \frac{x^p}{(p-1)!}v(x) \tag{7.31}$$

där $v(x)$ är ett heltalspolynom (som vi förstås kan beräkna från det långa uttrycket ovan). Från Lemma 7.1.3 vet vi följdakteligen att

$$H\big(T_r\phi\big) \equiv 0 \pmod p \qquad \text{då } 1 \leqslant r \leqslant n. \tag{7.32}$$

Den enda term i summan (7.30) som möjligtvis inte är kongruent med 0 modulo $p$ är den som motsvarar $r = 0$. Detta ger oss att

$$S_1 = \sum_{r=0}^{n} c_r H\big(T_r\phi\big) \equiv c_0 H\big(T_0\phi\big) = c_0 H(\phi) \pmod p. \tag{7.33}$$

Från (7.23) får vi då att

$$S_1 \equiv c_0(-1)^{pn}\big(n!\big)^p \pmod p. \tag{7.34}$$

Vi påminner om oss att vi valde $p$ sådant att $p$ är större än både $|c_0|$ och $n$ och därför kan varken $c_0$ eller $n!$ vara delbara med $p$ och eftersom $p$ är ett primtal betyder det att $S_1 \not\equiv 0 \pmod p$. Då $S_1$ är ett heltal (eftersom $c_0$ är en koefficient i ett heltalspolynom) har vi således visat att $|S_1| \geqslant 1$.

Låt oss visa att $|S_2| \leqslant 1/2$. Minns att

$$S_2 = \sum_{r=0}^{n} c_r \psi(r) e^{|r|}. \tag{7.35}$$

Från Lemma 7.1.2 påminner vi oss om att

$$\psi(r) = \sum_{s=0}^{m} d_s \varepsilon_s(r) r^s \tag{7.36}$$

där $d_s$ är koefficienterna i polynomet $\phi(r)$

$$\phi(r) = \frac{r^{p-1}}{(p-1)!}\Big[(r-1)(r-2)\cdots(r-n)\Big]^p = \sum_{s=0}^{m} d_s r^s. \tag{7.37}$$

Eftersom $|\varepsilon_s(r)| < 1$ (enligt Lemma 7.1.1) får vi att (kom ihåg att $r > 0$)

$$\left|\sum_{s=0}^{m} d_s \varepsilon_s(r) r^s\right| \leqslant \sum_{s=0}^{m} |d_s||\varepsilon_s(r)| r^s < \sum_{s=0}^{m} |d_s| r^s. \tag{7.38}$$

Nu vill vi på något sätt kunna uppskatta denna summa. Vi studerar därför följande polynom, som är snarlikt $\phi(r)$

$$\chi(r) = \frac{r^{p-1}}{(p-1)!}\Big[(r+1)(r+2)\cdots(r+n)\Big]^p = \sum_{s=0}^{m} f_s r^s. \tag{7.39}$$

Om man tänker efter så inser man att om vi multiplicerar ut polynomen $\phi(r)$ och $\chi(r)$ så kommer vi få precis samma koefficienter framför $r^k$ så när som på tecknet. Alltså (märk att alla koefficienter i $\chi(r)$ kommer att vara positiva)

$$0 \leqslant f_k = \pm d_k \qquad k = 1, \ldots, m \tag{7.40}$$

vilket ger att $|d_k| = f_k$. Detta visar att

$$|\psi(r)| < \sum_{s=0}^{m} |d_s| r^s = \sum_{s=0}^{m} f_s r^s = \frac{r^{p-1}}{(p-1)!}\Big[(r+1)(r+2)\cdots(r+n)\Big]^p \tag{7.41}$$

Vi har inte diskuterat gränsvärden i detta kompendium, men det är ganska enkelt att åtminstone intuitivt försäkra sig om att vi tar ett (litet) tal $c$ så kan vi, oberoende av $r$ och $n$, hitta ett $p$ sådant att $|\psi(r)| < c$ . Detta beror på att $p!$ växer mycket fortare än $r^p$ då $p$ blir tillräckligt stort (se Övning 7.1). Av samma anledning kan vi, för ett givet $c > 0$, hitta ett (förmodligen mycket större) $p$ sådant att

$$|S_2| \leqslant \sum_{r=0}^{n} |c_r||\psi(r)| e^{|r|} < c \tag{7.42}$$

Speciellt kan vi välja $c = 1/2$, vilket ger oss att $|S_2| < 1/2$. Om vi nu påminnner oss om att $|S_1| \geqslant 1$ så kan aldrig ekvationen

$$H(\phi)q(e) = S_1 + S_2 = 0 \tag{7.43}$$

vara uppfylld. Detta motsäger antagandet om att $e$ är algebraiskt. Alltså är $e$ transcendent. $\square$

**Övning 7.1.** Studera polynomet

$$f(x) = \frac{x^p}{p!}.$$

Låt först $x = 10$. Hur stort $p$ måste du välja för att $f(10) < 10^{-6}$? Vad är svaret då $x = 100$ och $x = 1000$?

Denna övning är till för att utveckla en känsla för hur snabbt $p!$ växer med $p$ i förhållande till $x^p$. Man kan intuitivt tycka att om $x$ är stort så är $x^p$ mycket större än $p!$. Det visar sig dock att det för alla $x$ finns ett $p$ sådant att $p!$ är mycket större än $x^p$. I denna övning ser vi tre exempel på detta, där vi gör $p!$ cirka en miljon gånger större än $x^p$.

# 8 Lösningar till udda övningsuppgifter

**Övning 1.1.**

1. $B \cup C = A$.
2. $B \cap C = \emptyset$.
3. $D \cap C = \{4, 36\}$.
4. $\{x \in D : x \in B\} = D \cap B = \{1, 19, 101\}$.
5. $\{x \in A : x = y + 1$ för något $y \in D\} = \{2, 5, 20, 37, 102\}$.
6. $\{x + 1 : x \in D\} = \{2, 5, 20, 37, 102\}$.

**Övning 1.3.** Tag $z \in [x]$. Eftersom $xRy$ så har vi även $y \in [x]$ och därmed visar föregående uppgift att $yRz$, vilket betyder att $z \in [y]$. Eftersom $z$ var godtycklig så visar detta att $[x] \subseteq [y]$.

Omvänt, tag $z \in [y]$. Då gäller $yRz$. Vi vet också att $xRy$ och därmed visar transitiviteten hos $R$ att $xRz$ vilket betyder att $z \in [x]$. Nu följer $[y] \subseteq [x]$.

Vi har alltså visat att $[x] \subseteq [y]$ och att $[y] \subseteq [x]$. Det betyder att $[x] = [y]$.

**Övning 2.1.** Tag $b \in \mathbb{Z}$ med $b \neq 0$. Då gäller $0 \cdot b = 1 \cdot 0$ vilket betyder att $(0, 1)R(0, b)$, det vill säga $0 = 0/1 = [(0, 1)] = [(0, b)] = 0/b$.

**Övning 3.1.** Vi vet att $ad = bc$. Antag att $0 < a/b$. Detta betyder att $ab > 0$ och eftersom $d^2 > 0$ så följer $ad \cdot bd = ab \cdot d^2 > 0$. Men om vi antar att $cd \leqslant 0$ så följer $ad \cdot bd = bc \cdot bd = b^2 \cdot cd \leqslant 0$ eftersom $b^2 > 0$. Denna motsägelse visar att det inte kan vara så att $cd \leqslant 0$. Alltså gäller $cd > 0$, det vill säga $0 < c/d$.

Omvänt, antag att $0 < c/d$. Upprepa samma argument som ovan, men där $a$ och $c$ respektive $b$ och $d$ bytt plats, och få att $0 < a/b$.

**Övning 3.3.** Låt $\mathscr{A}_n = \{B \subseteq \mathbb{Z} : B$ innehåller $n$ element$\}$ för $n = 0, 1, 2, \ldots$ och notera att

$$\mathscr{A} = \mathscr{A}_0 \cup \mathscr{A}_1 \cup \mathscr{A}_2 \cup \cdots . \tag{8.1}$$

Om vi nu kan visa att $\mathscr{A}_n$ är uppräknelig för varje $n$ så visar Sats 3.3.5 att $\mathscr{A}$ är uppräknelig.

Detta visar vi med *induktion*. Eftersom $\mathscr{A}_0 = \{\emptyset\}$ så är $\mathscr{A}_0$ uppräknelig. Antag nu att $\mathscr{A}_n$ är uppräknelig för något $n \in \mathbb{N}$. Då kan vi skriva $\mathscr{A}_n = \{A_0, A_1, A_2, \ldots\}$. Låt

$$\mathscr{B}_k = \{A_j \cup \{k\} : j = 0, 1, 2, \ldots\} \tag{8.2}$$

för $k = 0, 1, 2, \ldots$ och

$$\mathscr{B} = \mathscr{B}_0 \cup \mathscr{B}_1 \cup \mathscr{B}_2 \cup \cdots . \tag{8.3}$$

Alltså består $\mathscr{B}_k$ av alla mängder i $\mathscr{A}_n$, men med elementet $k$ tillagt. Således innehåller mängderna i $\mathscr{B}_k$ $n$ eller $n+1$ element, beroende på om elementet $k$ fanns med från början eller inte. Sats 3.3.5 visar att $\mathscr{B}$ är uppräknelig och eftersom vi har att $\mathscr{A}_{n+1} \subseteq \mathscr{B}$ så är även $\mathscr{A}_{n+1}$ uppräknelig.

Vi har alltså visat:

1. Mängden $\mathscr{A}_0$ är uppräknelig.
2. För varje $n \in \mathbb{N}$, om vi antar att $\mathscr{A}_n$ är uppräknelig så följer det att $\mathscr{A}_{n+1}$ är uppräknelig.

Eftersom $\mathscr{A}_0$ är uppräknelig så visar punkt 2 att även $\mathscr{A}_1$ är uppräknelig. Använd nu punkt 2 igen och få att $\mathscr{A}_2$ är uppräknelig. Fortsätter man på detta sätt visar det sig att $\mathscr{A}_n$ är uppräknelig för alla $n$.

**Övning 4.1.** Relationen $<$ för rationella tal definierades genom

$$\frac{a}{b} > 0 \qquad \text{om} \qquad ab > 0, \tag{8.4}$$

och för $p, q \in \mathbb{Q}$ så är

$$p > q \qquad \text{om} \qquad p - q > 0. \tag{8.5}$$

Tag nu två rationella tal på formen $p = a/b$ och $q = c/d$. Att $p > q$ betyder då att

$$p - q = \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd} > 0. \tag{8.6}$$

Enligt (18) gäller detta om

$$bd(ad - bc) > 0. \tag{8.7}$$

För att visa att $<$ är en ordning så måste vi kontrollera att $<$ uppfyller kraven i Definition 4.1.1. För alla $x, y, z \in \mathbb{Q}$ skall följande gälla:

1. Endast en av följande gäller: $x < y$, $y < x$ eller $x = y$.
2. Om $x < y$ och $y < z$ så är $x < z$.

Sätt

$$x = \frac{a}{b}, \quad y = \frac{c}{d} \qquad \text{och} \qquad z = \frac{e}{f}. \tag{8.8}$$

Vi skriver ut vad de tre olika fallen i första punkten betyder

$$x < y: \qquad bd(bc - ad) > 0 \tag{8.9}$$
$$y < x: \qquad bd(ad - bc) > 0 \tag{8.10}$$
$$x = y: \qquad bd(bc - ad) = 0. \tag{8.11}$$

Eftersom $b, d \neq 0$ inser vi att endast en av relationerna kan vara uppfylld för vart och ett av de tre valen $bc - ad > 0, ad - bc > 0$ och $bc - ad = 0$.

För att visa den andra egenskapen för ordningar så antar vi att $x < y$ och $y < z$, vilket betyder att $y - x > 0$ och $z - y > 0$. Vad vi vill visa är att detta leder till att $x < z$, d.v.s. $z - x > 0$. Sätt

$$p = y - x \qquad \text{och} \qquad q = z - y. \tag{8.12}$$

Vi noterar att $p + q = z - x$. Detta gör att vi kan formulera problemet som att givet $p, q > 0$ så ska vi visa att $p + q > 0$. Tag nu $p = s/t$ och $q = u/v$ och antag att $p, q > 0$, d.v.s. $st > 0$ och $uv > 0$. Vi beräknar

$$p + q = \frac{sv + tu}{tv}. \tag{8.13}$$

Nu vill vi visa att $p + q > 0$, d.v.s. att

$$tv(sv + tu) = stv^2 + uvt^2 > 0. \tag{8.14}$$

Men detta stämmer eftersom $st > 0, uv > 0, v^2 > 0$ och $t^2 > 0$. Alltså har vi visat att $p + q > 0$, vilket, enligt resonemanget ovan, visar att $x < z$ om $x < y$ och $y < z$. Alltså är $<$ en ordning.

**Övning 4.3.** Eftersom $1/n > 0$ för alla $n \geqslant 1$ så är helt klart 0 en undre begränsning till $E$. Låt oss visa att det inte finns någon undre begränsning som är större än 0, alltså måste 0 vara den största undre begränsningen till $E$. Tag $z > 0$ och låt $n_0$ vara ett heltal sådant att $n_0 > 1/z$. Då är $1/n_0 < z$ och vi får att

$$e_{n_0} = \frac{1}{n_0} < z. \tag{8.15}$$

Eftersom $e_{n_0} \in E$ så är $z$ ej en undre begränsning till $E$.

**Övning 5.1.** Vi påminner oss om definitionen

$$\alpha + \beta = \{p + q \,:\, p \in \alpha, q \in \beta\}. \tag{8.16}$$

Vi visar att (R1)–(R3) i Definition 4.3.1 är uppfyllda.

(R1) Eftersom både $\alpha$ och $\beta$ är snitt så är de uppåt begränsade, d.v.s. det finns ett $q \in \mathbb{Q}$ sådant att $p < q$ för alla $p \in \alpha$ eller $p \in \beta$. Men då vet vi att $2q \notin \alpha + \beta$ vilket betyder att $\alpha + \beta \neq \mathbb{Q}$. Mängden $\alpha + \beta$ är inte heller den tomma mängden eftersom varken $\alpha$ eller $\beta$ är den tomma mängden.

(R2) Tag ett $a \in \alpha + \beta$ och ett $b \in \mathbb{Q}$ sådant att $b < a$. Vi vill nu konstruera $p \in \alpha$ och $q \in \beta$ sådana att $b = p + q$. Vi vet att det finns två rationella tal $s \in \alpha$ och $t \in \beta$ sådana att $a = s + t$. Definiera de två talen

$$p = s - \frac{a - b}{2} \qquad \text{och} \qquad q = t - \frac{a - b}{2}. \tag{8.17}$$

Eftersom $p < s$ och $q < t$ så är $p \in \alpha$ och $q \in \beta$ ty $\alpha$ och $\beta$ är snitt. Då

$$p + q = s + t - (a - b) = a - a + b = b \tag{8.18}$$

så har vi visat att $b \in \alpha + \beta$.

(R3) Tag ett $a \in \alpha + \beta$. Vi vill visa att det existerar ett $r \in \alpha + \beta$ sådant att $r > a$. Vi vet att vi kan skriva $a = s + t$ där $s \in \alpha$ och $t \in \beta$. Eftersom $\alpha$ är ett snitt så finns det ett $u \in \alpha$ sådant att $u > s$. Sätter vi $r = u + t$ så har vi visat att $r \in \alpha + \beta$ och $r > a$.

**Övning 5.3.** Vi verifierar egenskaperna (R1)–(R3) i Definition 4.3.1.

(R1) Mängden $\gamma \neq \emptyset$ eftersom $A$ enligt antagande innehåller minst ett snitt. Eftersom $A$ är uppåt begränsad så finns det ett snitt $\beta$ sådant att $\alpha < \beta$ för alla $\alpha \in A$. Låt $q$ vara övre begränsning till $\beta$. Då är $q \notin \gamma$, vilket betyder att $\gamma \neq \mathbb{Q}$.

(R2) Tag $q \in \gamma$. Då finns det ett $\alpha \in A$ sådant att $q \in \alpha$. Om $p < q$ så är $p \in \alpha$ vilket också betyder att $p \in \gamma$.

(R3) Tag $q \in \gamma$. Då finns det ett $\alpha \in A$ sådant att $q \in \alpha$. Då vet vi att det existerar ett $r \in \alpha$ sådant att $r > q$ vilket också betyder att $r \in \gamma$.

**Övning 6.1.** Låt $\phi$ och $\psi$ vara två polynom

$$\phi(h) = \sum_{r=0}^{n} c_r h^r \qquad \text{och} \qquad \psi(h) = \sum_{r=0}^{l} d_r h^r. \tag{8.19}$$

Låt $m$ vara det största talet av $n$ och $l$, låt oss säga $n$. Vi utvidgar summan i $\psi(h)$ till $m$ genom att sätta $d_r = 0$ då $r > l$. Vi skriver då

$$\phi(h) = \sum_{r=0}^{m} c_r h^r \qquad \text{och} \qquad \psi(h) = \sum_{r=0}^{m} d_r h^r. \tag{8.20}$$

Summan av de två polynomen kan vi skriva som

$$a\phi(h) + b\psi(h) = \sum_{r=0}^{m} (ac_r + bd_r) h^r. \tag{8.21}$$

Nu kan vi tillämpa avbildningen $H$

$$\begin{aligned} H\Big[a\phi + b\psi\Big] &= \sum_{r=0}^{m} (ac_r + bd_r) r! = a \sum_{r=0}^{m} c_r r! + b \sum_{r=0}^{m} d_r r! \\ &= a \sum_{r=0}^{n} c_r r! + \sum_{r=0}^{l} d_r r! \\ &= aH(\phi) + bH(\psi). \end{aligned} \tag{8.22}$$

Alltså är $H$ en linjär avbildning.

**Övning 6.3.** Vi beräknar $(x+h)^4$

$$\begin{aligned} (x+h)^4 &= (x+h)(x+h)(x+h)(x+h) \\ &= x^4 + 4x^3 h + 6x^2 h^2 + 4x h^3 + h^4. \end{aligned} \tag{8.23}$$

Vi beräknar summan i högerledet

$$\begin{aligned}\sum_{k=0}^{4} \frac{4!}{k!(4-k)!} x^{4-k} h^k &= \frac{4!}{0!4!} x^4 h^0 + \frac{4!}{1!3!} x^3 h^1 + \frac{4!}{2!2!} x^2 h^2 \\ &+ \frac{4!}{3!1!} x^1 h^3 + \frac{4!}{4!0!} x^0 h^4 \\ &= x^4 + 4x^3 h + 6x^2 h^2 + 4xh^3 + h^4.\end{aligned} \tag{8.24}$$

Detta visar att

$$(x+h)^4 = \sum_{k=0}^{4} \frac{4!}{k!(4-k)!} x^{4-k} h^k. \tag{8.25}$$

**Övning 7.1.** Låt oss först ta $x = 10$. Då vill vi hitta ett $p$ sådant att $10^p/p! < 10^{-6}$. Genom att till exempel använda miniräknaren kan man testa sig fram till att

$$\frac{10^{37}}{37!} \approx 0.73 \cdot 10^{-6}. \tag{8.26}$$

På samma sätt finner vi att

$$\frac{100^{282}}{282!} \approx 0.75 \cdot 10^{-6}. \tag{8.27}$$

Att försöka hitta $p$ då $x = 1000$ går kanske över gränsen för vad en miniräknare klarar av, men använder man sig av ett matematikprogram till datorn så finner man att

$$\frac{1000^{2728}}{2728!} \approx 0.45 \cdot 10^{-6}. \tag{8.28}$$

Vi sammanställer resultaten:

$$\begin{aligned} x &= 10: & p &= 37 \\ x &= 100: & p &= 282 \\ x &= 1000: & p &= 2728. \end{aligned} \tag{8.29}$$