Stockholms Matematiska Cirkel

Vad är ett tal?

Rune Suhr
Gustav Zickert

Institutionen för matematik KTH och
Matematiska institutionen Stockholms universitet
2016–2017

Innehåll

Några ord på vägen

Detta kompendium är skrivet för att användas som kurslitteratur till Stockholms Matematiska Cirkel under läsåret 2016–2017 och består av sju kapitel. Kompendiet är en omarbetad version av Joakim Arnlind, Tomas Ekholm och Andreas Enbloms kompendium "Reella tal", som användes som kurslitteratur till KTH's Matematiska Cirkel under läsåret 2005–2006.

Kompendiet är inte tänkt att läsas enbart på egen hand, utan ska ses som ett skriftligt komplement till undervisningen på de sju föreläsningarna. En bra idé kan vara att försöka läsa varje kapitel själv innan föreläsningen, så att man redan innan vet vad målet med föreläsningen är och vad som kan visa sig vara svårt.

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.

Till varje kapitel finns ett antal övningsuppgifter. Dessa är ordnade efter ungefärlig svårighetsgrad: övningar kan ha en ($\star$), två ($\star\star$) eller tre ($\star\star\star$) stjärnor. Dessutom har de udda övningarna facit längst bak i kompendiet. Syftet med dessa är att eleverna ska kunna lösa dem och på egen hand kontrollera att de förstått materialet. Övningar med jämna nummer saknar facit och kan användas som examination. Det rekommenderas dock att man försöker lösa 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 författarna. Under årets gång kommer det att finnas räknestugor där eleverna kan lösa uppgifter tillsammans, och få hjälp av oss.

Vi vill dock betona att få av uppgifterna är helt enkla. Detta betyder att läsaren inte bör titta i facit efter några få minuter, utan att först prata med kompisar om uppgiften, kanske lägga den åt sidan ett tag och tänka på annat, och sedan försöka lite till. Dessutom innebär det att få av eleverna kommer att kunna klara samtliga uppgifter, så ett krav på att eleven ska ha löst alla uppgifter bör inte ingå i examinationen. Dock rekommenderar vi starkt att alla elever åtminstone tittar på och försöker sig på alla övningar.

De flesta övningar kommer att ha många olika möjliga lösningar och det som står i facit bör endast ses som ett förslag.

Vi tackar Mats Boij och Gustav Sædén Ståhl, Institutionen för Matematik vid KTH och Sara Woldegiorgis vid Matematiska institutionen på Stockholms universitet för givande kommentarer om denna skrift.

Några ord om Cirkeln

Stockholms Matematiska Cirkel, i dagligt tal benämnd Cirkeln, är en kurs som kommer från ett nytt samarbete mellan Kungliga Tekniska högskolan och Stockholms universitet. Cirkeln har tidigare funnits under KTH:s ensamma regi med namnet KTH:s Matematiska Cirkel men bytte namn i fjol. Upplägget kommer dock fortsätta som tidigare år.

Matematiska 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 och matematiska studier. Lärarna på Cirkeln kan vid behov ge eleverna förslag på ämnen till projektarbeten vid gymnasiet eller förslag till annan förkovran inom matematik.

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

`www.math-stockholm.se/cirkel`

Cirkeln godkänns ofta som en gymnasiekurs eller som matematisk breddning på gymnasieskolorna. 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, lärare eller andra matematikintresserade.

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 Stockholms 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:

Betyg E: 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.

Betyg C: 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.

Betyg A: 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.

Betyget B ges till elever som uppfyllt kraven för betygssteget C och en övervägande del av kraven för betygssteget A. På samma sätt fås betyget D om kraven för E är uppfyllda och en övervägande del av kraven för C.

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

Författarna, augusti 2016

Introduktion

Vårt mål i detta kompendium är att undersöka frågan:

Vad är ett tal?

Kanske tycker läsaren att detta är en fråga med ett uppenbart svar, men faktum är att synen på vad ett tal är har förändrats kraftigt under mänsklighetens historia.

De första talen som användes är de positiva heltalen, det vill säga de tal som vi räknar antal med. Att talet noll också är ett tal var dock inte självklart, det uppstod först genom användning inom positionssystem, det vill säga talsystem där positionen av en siffra avgör värdet som den representerar. Den indiska matematikern Brahmagupta (cirka 598-668) var förmodligen bland de första att studera de aritmetiska egenskaperna hos talet noll.

Att subtrahera positiva tal från varandra gjordes tidigt, men att negativa tal är tal i sig själva, eller lösningar till ekvationer, betraktades fortfarande som absurt på 300-talet i Grekland. Däremot var positiva rationella tal – positiva bråktal – populära bland matematiker i antikens Grekland, vilka ansåg att alla tal är rationella. När anhängare till Pythagoras insåg att det finns tal, så som $\sqrt{2}$, som inte är rationella, betraktades detta som ett katastrofalt resultat.

Det skulle dröja ända till år 1872 innan den tyska matematikern Richard Dedekind (1831-1916) med flera gav en ordentlig konstruktion av de reella talen. De reella talen utgörs av alla tal på tallinjen och innehåller förutom de rationella talen även irrationella tal. Komplexa tal användes i smyg redan från 1500-talet och de så kallade kvaternionerna konstruerades 1843, men båda dessa talmängder förutsätter existensen av de reella talen.

Idag anser förmodligen de flesta sig ha en hyfsat klar bild av vad tal är och hur man använder dessa i beräkningar. Inom matematiken strävar man dock alltid efter att ha så tydliga definitioner som möjligt av de objekt man arbetar med. Vi kommer därför att i detta kompendium ge rigorösa – det vill säga mycket noggranna – *konstruktioner* av olika typer av tal[1]. Med en konstruktion av ett matematiskt objekt, som exempelvis en uppsättning tal, avses en beskrivning av objektet i fråga med hjälp av den mängdlära som vi kommer ge en introduktion till i kapitel ett.

När vi sedan konstruerat dessa talmängder kommer vi att undersöka deras egenskaper, så som vilka räknelagar de lyder under och hur väl lämpade de är för att lösa olika slags ekvationer.

Kompendiets syfte är inte att ge ett uttömmande svar på den filosofiska frågan om vilka matematiska objekt som bör betraktas som tal. Det ger istället en introduktion till en möjlig väg att gå i konstruktionen och studiet av diverse talmängder. Andra möjliga generaliseringar av talbegreppet så som p-adiska tal, transfinita tal och hyperreella tal behandlas inte.

[1]Det bör påpekas att vi i detta kompendium inte följer den historiska utvecklingen helt och hållet. Till exempel börjar vi inte med de positiva heltalen, utan vi utgår istället från de naturliga talen, vilka även inkluderar talet noll.

Resten av denna introduktion utgörs av en kort sammanfattning av innehållet i kompendiet.

Det första kapitlet behandlar matematisk bevisföring och teorin om mängder. Kapitlet innehåller även ett bevis av att $\sqrt{2}$ inte är ett rationellt tal.

Kapitel två inleds med en konstruktion av heltalen $\ldots -3, -2, -1, 0, 1, 2, 3 \ldots$ från de naturliga talen $0, 1, 2, 3 \ldots$.[2] Det visar sig vara betydligt mer invecklat att konstruera de negativa talen än att sätta ett minustecken framför ett positivt tal. Därefter kommer vi att konstruera de rationella talen. I kapitel tre fortsätter vi att studera de rationella talen och deras egenskaper.

I kapitel fyra kommer vi till en av kursens höjdpunkter, nämligen den detaljerade konstruktionen av de reella talen. Därefter kan vi i kapitel fem visa att de reella talen även kan representeras som decimaltal. Kapitel sex ägnas åt att studera de så kallade algebraiska och transcendenta talen, samt att visa att de reella talen är ”fler” än de naturliga talen.

I kapitel sju avslutar vi kursen med att blicka mot högredimensionella tal, nämligen tal i dimension två (komplexa tal), fyra (kvaternioner) och åtta (oktonioner). Vi kommer att visa att talen vid varje fördubbling av dimensionen förlorar en väsentlig egenskap som de reella talen åtnjuter.

[2] Vi kommer i detta kompendium att ta existensen av de naturliga talen för given, men det är även möjligt att konstruera de naturliga talen från mängdläran. En sådan konstruktion presenteras i Appendix B.

1 Grundläggande begrepp och bevisföring

I det här kapitlet kommer vi att ge en introduktion till matematisk bevisföring. Innan dess kommer vi dock att introducera lite terminologi. I matematiken använder man ofta *mängder* som ett bekvämt språk för att beskriva saker och ting, och detta kommer vi också att göra i detta kompendium. Vi börjar därför med att beskriva denna teori.

1.1 Mängder

Låt oss titta på ett av de mest grundläggande begreppen i matematiken, nämligen mängder. En *mängd* är en samling objekt, som till exempel tal, och dessa objekt kallar vi för *element* i mängden. Det enklaste sättet att beskriva en mängd är att räkna upp dess element. Ett sådant exempel är

$$A = \{1, 3, a, 7\}.$$

Detta betyder att A är en mängd som innehåller elementen $1, 3, a$ och 7. Vi bryr oss inte om i vilken ordning eller hur många gånger elementen räknas upp och därmed gäller till exempel

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

En mängd kan också ha oändligt många element, och då går det inte att skriva ned alla element. Ett exempel på en oändlig mängd är de så kallade *naturliga talen*

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

De tre punkterna betyder här att *alla* icke-negativa heltal ingår i mängden.

Exempel 1.1.1. Mängden som består av alla udda heltal mellan 0 och 10 kan skrivas som

$$\{1, 3, 5, 7, 9\}. \qquad \blacktriangle$$

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 $b \in \{a, b, 10, 3\}$. Att ett objekt x inte tillhör mängden A skrivs $x \notin A$. Den *tomma mängden* innehåller inga element och betecknas $\emptyset$.

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 $\{1, a\} \subseteq \{1, 3, a\}$. $\blacktriangle$

Ett användbart sätt att beskriva en mängd är som en delmängd av en annan mängd. Det finns ett speciellt skrivsätt för detta, nämligen

$$\{x \in D \mid \text{villkor på } x\}.$$

Med detta menar man delmängden bestående av de element i mängden D som uppfyller de givna villkoren. Strecket | utläses ”så att”. Som exempel kan vi definiera

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

och

$$C = \{y \in \{1, 2, 3, 4\} \mid y > 2\}.$$

Mängden B är delmängden av de positiva heltalen som består av alla udda positiva heltal, medan C är delmängden av $\{1, 2, 3, 4\}$ bestående av element större än 2. Alltså har vi

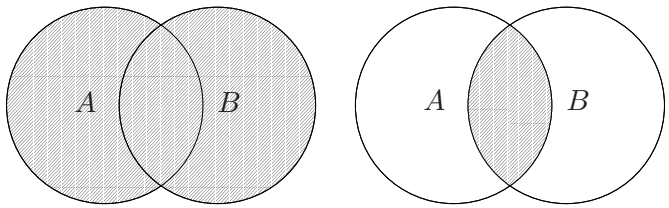
$$B = \{1, 3, 5, 7, 9, 11, \ldots\} \quad \text{och} \quad C = \{3, 4\}.$$

Exempel 1.1.4. Låt $A = \{4, 5, 8, 4711, 12, 18\}$ och $B = \{x \in A \mid x > 10\}$. Då är $B = \{12, 18, 4711\}$ medan $\{x \in A \mid x < 3\} = \emptyset$. Vidare har vi att $4 \in A$ men $4 \notin B$. ▲

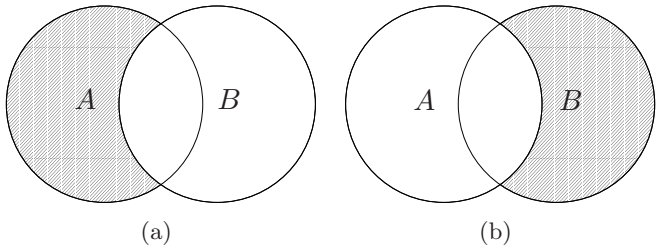
Definition 1.1.5. Antag att A och B är mängder. *Unionen* av A och B består av de element som ligger i någon av mängderna och betecknas $A \cup B$. *Snittet* av A och B består av de element som ligger i båda mängderna och betecknas $A \cap B$. *Differensen* av A och B består av alla element som ligger i A men inte ligger i B, och betecknas $A \setminus B$. Mängderna A och B kallas för *disjunkta* om $A \cap B = \emptyset$.

Exempel 1.1.6. Låt $A = \{1, 3, 5, 6\}$, $B = \{5, 8, 3, 4711\}$ och $C = \{2, 4, 7, 8\}$. Då har vi $A \cup B = \{1, 3, 5, 6, 8, 4711\}$, $A \cap B = \{3, 5\}$, $B \cap C = \{8\}$ och mängderna A och C är disjunkta. Dessutom gäller att $A \setminus B = \{1, 6\}$ och $B \setminus A = \{8, 4711\}$. Till skillnad från unionen och snittet är differensen av två mängder inte symmetrisk i A och B. ▲

Ett användbart sätt att åskådliggöra union, snitt och differens är med hjälp av så kallade *Venndiagram*, som visas i Figur 1.1 och Figur 1.2.



Figur 1.1: Venndiagram som åskådliggör mängderna (a) $A \cup B$ och (b) $A \cap B$.



Figur 1.2: Venndiagram som åskådliggör (a) $A \setminus B$ och (b) $B \setminus A$.

1.2 Matematisk bevisföring

Denna kurs kommer i huvudsak att handla om *bevis* av matematiska påståenden; varje föreläsning kommer att innehålla flera bevis, och majoriteten av övningsuppgifterna går ut på att bevisa någonting. Detta innebär antagligen en omställning från tidigare kurser i matematik. Så vad är då ett bevis egentligen? Här är en möjlig definition.

Definition 1.2.1. Ett *bevis* av ett *påstående* är en *logisk slutledning* som leder från en överenskommen uppsättning av *antaganden* fram till påståendet.

Det förekommer flera viktiga ord i föregående definition. Låt oss diskutera dem ett i taget.

Definition 1.2.2. Ett *påstående* är en logisk utsaga som antingen är sann eller falsk.

Exempel 1.2.3. Här är några exempel på påståenden:

(i) $2A + 5B > -C^2$.

(ii) $X \subseteq (Y \cap Z)$.

(iii) Alla jämna tal är delbara med 2.

(iv) Alla jämna tal är delbara med 3.

Av dessa vet vi inte om de första två är falska eller sanna, eftersom vi inte vet vad A, B, C respektive X, Y, Z betyder. Det tredje påståendet är sant eftersom varje jämnt tal kan skrivas som $2n$ för något heltal n. Påstående (iv) är dock falskt: ett motexempel ges av det jämna talet 2 som ej är delbart med 3. ▲

Exempel 1.2.4. Här är också några exempel på saker som *inte* är påståenden.

(i) $x^2 + 6x + 5$

(ii) Mängden av alla jämna tal. ▲

Påståenden kan kombineras på många olika sätt, som påminner om de sätt vi kan skapa nya mängder av gamla genom operationerna $\cap$, $\cup$ och $\setminus$. Till exempel kan vi sätta två påståenden bredvid varandra och skriva ordet "och" emellan, och vi får ett nytt påstående. Ett annat ord man kan sätta mellan två påståenden är "eller". En annan sak man kan göra är att skriva "Det är inte sant att..." före ett påstående, och detta ger också ett nytt påstående.

Men viktigast av alla sätt att skapa nya påståenden ur gamla är kanske följande.

Definition 1.2.5. Låt P och Q vara två påståenden, till exempel några av de som stod i vår lista. Med $P \implies Q$ menar vi följande påstående: "om påståendet P är sant, är även påståendet Q sant." I ord säger vi att P *implicerar* Q eller att P *medför* Q. Om $P \implies Q$ och $Q \implies P$ så skriver vi att $P \iff Q$. I ord säger vi att P gäller *om och endast om* Q gäller, alternativt att P och Q är *ekvivalenta*.

För varje par av påståenden P och Q får vi alltså ett nytt påstående, $P \implies Q$. Sanningshalten av $P \implies Q$ kan utläsas ur Tabell 1.

P	Q	$P \implies Q$
sant	sant	sant
sant	falskt	falskt
falskt	sant	sant
falskt	falskt	sant

Tabell 1: Hur $P \implies Q$ beror på P och Q.

Ur Tabell 1 ses speciellt att $P \implies Q$ alltid är sant om P är falskt. Detta kan verka ointuitivt till en början. Ett motiverande exempel för denna princip kan vara följande mening som man kan få höra på en biograf: "Om du har en mobiltelefon med dig, är den avstängd?" Om man inte har sin mobiltelefon med sig skall man alltid svara "Ja", oavsett om man har stängt av den eller inte.

Exempel 1.2.6. Det gäller att

$$5a + b = 0 \implies 5a = -b.$$

Här gäller även den omvända implikationen, så vi hade kunnat skriva $\iff$ i stället för $\implies$. Vi har också att

$$5a = -b \implies 5ac = -bc,$$

men här är omvändningen inte nödvändigtvis sann. För att gå från det högra påståendet till det vänstra måste vi nämligen dela med c, vilket vi inte vet är tillåtet om vi inte vet att $c \neq 0$. Vi har dock att

$$5ac = -bc \text{ och } c \neq 0 \implies 5a = -b. \qquad \blacktriangle$$

Exempel 1.2.7. Påståendet

$$7 > 2 \implies (\text{Alla jämna tal är delbara med } 3)$$

är falskt, eftersom det första påstående är sant medan det andra är falskt. Dock är påståendet

$$(\text{Alla jämna tal är delbara med } 3) \implies 7 > 2$$

lustigt nog sant enligt vår definition av $\implies$. $\blacktriangle$

Exempel 1.2.8. För varje påstående P gäller att påståendet $P \implies P$ är sant, oavsett om P är sant eller inte. $\blacktriangle$

Definition 1.2.9. En *logisk slutledning* är en sekvens av påståenden

$$P_1, P_2, \ldots, P_n$$

med egenskapen att påståendet $P_i \implies P_{i+1}$ är sant för alla i.

Definition 1.2.10. Ett *antagande* är ett påstående som vi förutsätter är sant. Ibland kallas dessa synonymt för *axiom* eller *postulat*.

Vi vet nu alltså vad ett bevis av ett påstående Q är: det är en kedja av mindre, enklare påståenden som låter oss dra slutsatsen att Q är sant, endast utgående ifrån en mindre uppsättning antaganden som vi i förväg har bestämt oss för att starta med.

Exempel 1.2.11. *Antag* att $\frac{3x}{2} = 6$ och att vi vill visa att $x = 4$. Låt påstående P_1 vara "$\frac{3x}{2} = 6$", P_2 vara "$3x = 12$" och P_3 vara "$x = 4$". Då gäller att påståendet $P_1 \implies P_2$ är sant eftersom vi kan gå från den första likheten till den andra genom att multiplicera båda leden med 2. På samma sätt har vi att påståendet $P_2 \implies P_3$ är sant eftersom vi kan gå från P_2 till P_3 genom att dividera med 3. Därmed har vi skapat en logisk slutledning som visar att *om vi antar att* P_1 är sant så är även P_3 sant. ▲

När vi skriver ett bevis brukar vi dock inte bara skriva en lång följd av påståenden med $\implies$ mellan – i stället brukar man försöka uttrycka beviset i vanliga ord och meningar. Symbolen $\implies$ byts till exempel ut mot konstruktioner som "vilket innebär att..." eller "eftersom... så..." eller "från vilket vi drar slutsatsen att...", och så vidare.

Speciellt värt att nämna är begreppet *motsägelsebevis*. Detta är en speciell bevisteknik där man i stället för att visa att ett påstående P är sant, så bevisar man att det *inte kan vara falskt*. Med detta menar vi att man börjar med antagandet att P inte gäller, och försöker att härleda ett påstående som man vet inte stämmer, till exempel att $0 = 1$. Enligt Tabell 1 så kan bara ett falskt påstående implicera ett falskt påstående, så vårt antagande att P inte gällde måste ha varit falskt.

1.3 Ett bevis

Vi avslutar kapitlet med att bevisa att $\sqrt{2}$ inte kan skrivas som en kvot av två heltal.

Sats 1.3.1. *Det finns inga heltal a och b så att*

$$\left(\frac{a}{b}\right)^2 = 2. \tag{1.1}$$

Bevis. Beviset är ett motsägelsesbevis. Vi antar motsatsen till det vi vill visa, det vill säga vi antar att det faktiskt finns heltal a, b så att ekvation (1.1) gäller, och härleder en motsägelse. Därifrån drar vi slutsatsen att a, b med den egenskapen ej kan finnas.

Vi kan anta att a är det minsta möjliga positiva tal så att ekvation (1.1) är uppfylld. Ekvation (1.1) är ekvivalent med ekvationen $a^2 = 2b^2$, och eftersom högerledet i den senare ekvationen är ett jämnt tal, så måste a^2 vara ett jämnt tal, vilket medför att a är ett jämnt tal, så $a = 2c$ för något positivt tal c. Vi erhåller då ekvationen $2^2c^2 = 2b^2$ vilket ger $2c^2 = b^2$. Eftersom vänsterledet

nu är jämnt, måste då även högerledet vara jämnt, och vi får att $b = 2d$ för något d. Vi får då att $2c^2 = 2^2d^2$ vilket ger

$$\left(\frac{c}{d}\right)^2 = 2.$$

Men $2c = a$, så $c < a$ och detta är en motsägelse, för vi antog ju att a var det minsta positiva tal så att ekvation (1.1) är uppfylld. □

Övningar

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

(i) $B \cup C$,

(ii) $B \cap C$,

(iii) $D \cap C$,

(iv) $\{x \in D \mid x \in B\}$,

(v) $\{x \in A \mid x = y + 1 \text{ för något } y \in D\}$,

(vi) $\{x + 1 \mid x \in D\}$.

Övning 1.2 ($\star$)**.** Betrakta mängderna $A = \{1, a\} \cup \{\pi\}$ och $B = \{a, \star\}$.

(i) Räkna upp alla element i A.

(ii) Räkna upp alla delmängder av A.

(iii) Vad är $A \cup B$ och $A \cap B$?

Övning 1.3 ($\star\star$)**.** Låt $\mathbb{N} = \{0, 1, 2, \ldots\}$ och låt $B_n = \{0, 1, 2, \ldots, n\}$ för $n = 0, 1, 2, \ldots$. Visa att $\mathbb{N} = B_0 \cup B_1 \cup B_2 \cup \ldots$.
(*Ledning:* Tag först $x \in \mathbb{N}$ och visa att $x \in B_0 \cup B_1 \cup B_2 \cup \ldots$. Tag sedan $x \in B_0 \cup B_1 \cup B_2 \cup \ldots$ och visa att $x \in \mathbb{N}$. Använd detta för att visa att mängderna är lika.)

Övning 1.4 ($\star\star$)**.** Behövs kravet att $x, y \geq 0$ för att $x \geq y$ ska vara ekvivalent med $x^2 \geq y^2$? Motivera med exempel.

Övning 1.5 ($\star$)**.** Avgör vilka av följande utsagor som är påståenden enligt vår definition av ett påstående. Vilka av dessa är sanna, vilka är falska, och vilka behöver vi mer information för att avgöra?

(i) Mängden av de naturliga talen.

(ii) a är ett positivt heltal.

(iii) Talet a är jämnt.

(iv) Varje mängd innehåller minst ett element.

(v) $a = 2$.

(vi) $a = 5$.

(vii) $x = a$ är lösningen till ekvationen $3x + 5 = 11$.

Övning 1.6 ($\star$)**.** Använd påståenden från föregående övning och bilda olika sammansatta påståenden på formen $P \implies Q$. Hitta minst två sådana påståenden som är sanna respektive falska.

Övning 1.7 ($\star\star\star$)**.** Låt A och B vara mängder. Vart och ett av följande påståenden är ekvivalent till exakt ett annat. Vilka hör ihop?

(i) $x \in A$,

(ii) $A \subseteq B$ och $B \subseteq A$,

(iii) $A \subseteq A \cap B$,

(iv) För alla x gäller: $x \in A \implies x \notin A$,

(v) $A \cup B = A$,

(vi) $A = B$,

(vii) $A = \emptyset$,

(viii) $A \subseteq B$,

(ix) $\{x\} \subseteq A$,

(x) För alla x gäller: $x \in B \implies x \in A$.

Övning 1.8 ($\star\star$)**.** Varför fungerar *inte* beviset av Sats 1.3.1 för att visa att det inte finns heltal a och b sådana att

$$\left(\frac{a}{b}\right)^2 = 4. \tag{1.2}$$

Övning 1.9 ($\star\star$)**.** Bevisa att det inte finns några heltal a och b sådana att

$$\left(\frac{a}{b}\right)^2 = 3. \tag{1.3}$$

2 Från de naturliga talen till de rationella talen

Matematik bygger på bevis: varje sats måste bevisas för att accepteras som sann. För att bevisa en sats måste alla ingående begrepp vara tydligt definierade. Det är dock oundvikligt att det alltid finns vissa begrepp som måste accepteras utan en strikt definition. Till dessa begrepp hör vanligen de grundläggande begreppen från mängdläran. I de flesta kurser i matematik – även på universitetsnivå – är även existensen av olika slags tal och dess grundläggande aritmetiska egenskaper något som tas för givet.

I detta kompendium undersöker vi dock talbegreppet från grunden och vi utgår därför endast från mängdläran och de naturliga talen $\mathbb{N} = \{0, 1, 2, \dots\}$. En detaljerad konstruktion av $\mathbb{N}$ ur mängdläran samt en genomgång av deras egenskaper finns i Appendix B. Med hjälp av de naturliga talen och teorin om mängder kommer vi att konstruera de andra "mer avancerade" talen.

Den första talmängden vi kommer konstruera är heltalen. För denna konstruktion, samt senare konstruktioner i kompendiet, behöver vi en kort introduktion till teorin om matematiska relationer.

2.1 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 2.1.1. Här följer tre exempel på "relationer"[3] på mängden av positiva heltal $\{1, 2, 3, \dots\}$.

(i) 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.

(ii) Låt xRy betyda att $xy = 30$. Här gäller till exempel $5R6$, eftersom $5 \cdot 6 = 30$, men *inte* $4R7$ då $4 \cdot 7 = 28 \neq 30$.

(iii) 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 betecknas just med R. I detta exempel betecknas de tre relationerna med $<$, R och S. ▲

Definition 2.1.2. Låt A vara en mängd. En *relation* på A är en delmängd $R \subseteq A^2 = \{(x, y) \mid x, y \in A\}$, det vill säga en mängd som innehåller ordnade par (x, y) av element $x, y \in A$. Om $(x, y) \in R$ så skriver vi xRy.

Exempel 2.1.3. Låt oss använda denna definition på relationerna i Exempel 2.1.1. Då gäller följande:

[3]Här använder vi citationstecken eftersom vi hittills inte har givit en strikt definition av vad en relation är.

(i) $< = \{(x, y) \mid x, y \in \{1, 2, 3, \ldots\}$ och x är mindre än $y\}$

(ii) $R = \{(1, 30), (2, 15), (3, 10), (5, 6), (6, 5), (10, 3), (15, 2), (30, 1)\}$

(iii) $S = \{(0, 2), (1, 3), (2, 4), \ldots\}$.

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

2.2 Ekvivalensrelationer

Definition 2.2.1. Låt A vara en mängd. En relation R på A sägs vara en *ekvivalensrelation* om den uppfyller:

(i) (Reflexivitet) För varje $x \in A$ gäller xRx.

(ii) (Symmetri) Om $x, y \in A$ och xRy så gäller även yRx.

(iii) (Transitivitet) Om xRy och yRz så gäller även att xRz.

Exempel 2.2.2. 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.

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

(ii) 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.

(iii) 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.

R uppfyller därmed Definition 2.2.3 och är därmed en ekvivalensrelation.

Definition 2.2.3. Om R är en ekvivalensrelation på en mängd A och $x \in A$ så kallar vi mängden $\{y \in A \mid xRy\}$ för *ekvivalensklassen* till x. Den betecknas med $[x]_R$ eller, om det är klart vilken relation R som åsyftas, med $[x]$.

Ekvivalensklasserna som hör till R i Exempel 2.2.2 är

$$\{130, 1000\}, \{11, 181, 211\}, \{12, 222, 12342\} \text{ och } \{65535\}. \tag{2.1}$$

I själva verket gäller

$$\begin{gathered} [1000] = [130] = \{130, 1000\} \\ [11] = [211] = [181] = \{11, 181, 211\} \\ [12] = [12342] = [222] = \{12, 222, 12342\} \\ [65535] = \{65535\}. \end{gathered} \tag{2.2}$$

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 disjunkta (åtskilda) delar.

Sats 2.2.4. *Låt $A = \{x_1, x_2, \ldots, x_n\}$. Då gäller*

$$A = [x_1] \cup [x_2] \cup \cdots \cup [x_n] \tag{2.3}$$

och

$$[x] \cap [y] = \begin{cases} [x] & \text{om } xRy \\ \emptyset & \text{annars.} \end{cases} \tag{2.4}$$

Bevis. Se Övning 2.1 – 2.3. □

Exempel 2.2.5. Relationen $<$ från Exempel 2.1.1 är *inte* en ekvivalensrelation. Exempelvis är relationen $<$ inte symmetrisk. Vi har ju att $2 < 4$ men inte att $4 < 2$. ▲

Exempel 2.2.6 (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. Vi uppmuntrar läsaren att visa att detta är en ekvivalensrelation och att ekvivalensklasserna är

$$\{2, 4, 6, 8, \ldots\} \quad \text{och} \quad \{1, 3, 5, 7, \ldots\}, \tag{2.5}$$

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

2.3 Heltalen

Ett skäl till att införa heltalen är att det ska bli möjligt att lösa alla ekvationer på formen $x+a = b$, för $a, b \in \mathbb{N}$. En sådan ekvation har nämligen ingen lösning $x \in \mathbb{N}$ om $b < a$.

Intuitivt sett vet vi givetvis redan vad heltalen är, nämligen mängden av de naturliga talen utvidgad med de negativa talen, det vill säga mängden $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$. Här nöjer vi oss dock inte med en sådan beskrivning, istället kommer vi att ge en detaljerad konstruktion av heltalen utifrån de naturliga talen.

Innan vi går vidare till denna konstruktion så vill vi först göra några observationer kring de fyra räkneoperationerna. Subtraktion är inte någon egen räkneoperation, ty om vi för varje tal y även har ett motsvarande $-y$, så gäller att $x - y = x + (-y)$. Med andra ord: att subtrahera y från x är det samma som att addera $-y$ till x.

På liknande sätt är division enbart ett specialfall av multiplikation: uttrycket $\frac{x}{y} = z$ innebär förstås att $x = y \cdot z$, så om man redan har definierat multiplikation av två tal, så kan $\frac{x}{y}$ definieras som det tal z så att $x = yz$, och speciellt är division med y enbart multiplikation med $\frac{1}{y}$.

På så vis behöver vi bara bekymra oss om att definiera två av de vanliga räkneoperationerna på våra talmängder, de två andra får vi med på köpet.

En fundamental algebraisk observation är att det naturliga talet 0 har egenskapen att $0 + a = a + 0 = a$ för alla naturliga tal a. Man säger att 0 är det *additiva enhetselementet* (se även Appendix B). Vidare definierar vi:

Definition 2.3.1. För ett givet tal a är den *additiva inversen* till a det tal b som uppfyller att $a + b = 0$, alltså att a adderat med b ger det additiva enhetselementet; vi skriver då $b = -a$.

Bland de naturliga talen är det bara 0 som har en additiv invers, och man kan säga att man får heltalen från de naturliga talen genom att lägga till additiva inverser till alla nollskilda element. Men dessa nya element måste konstrueras! De enda matematiska objekt vi har att jobba med just nu är de naturliga talen, samt dess delmängder. Vi måste således hitta ett sätt att konstruera additiva inverser – negativa tal – med hjälp av de naturliga talen och mängdoperationer.

Vi börjar med att bilda mängden $\mathbb{N}^2$ av ordnade par av naturliga tal, det vill säga

$$\mathbb{N}^2 = \{(a, b) \mid a, b \in \mathbb{N}\}.$$

Vi inför nu en relation R på $\mathbb{N}^2$ genom att kräva att $(a, b)R(c, d)$ om och endast om $a + d = b + c$.

Anmärkning 2.3.2. Vi kommer visa att man intuitivt kan tänka på ekvivalensklassen $[(a, b)]$ som talet $a - b$. I ljuset av detta är det lättare att första varför vi har definierat relationen R som ovan, ty med denna notation motsvaras likheten $[(a, b)] = [(c, d)]$ av $a - b = c - d$, vilket ju intuitivt är detsamma som att $a + d = b + c$.

Anmärkning 2.3.3. En relation R på en mängd A består enligt Definition 2.1.2 av ordnade par av element i mängden A. Vår mängd $\mathbb{N}^2$ ovan har dock element som är ordnade par; således består relationen R på $\mathbb{N}^2$ av ordnade par av ordnade par. Exempelvis har vi att $2 + 6 = 3 + 5$ och därför är elementen $(2, 3), (5, 6) \in \mathbb{N}^2$ relaterade, det vill säga $(2, 3)R(5, 6)$, vilket även kan skrivas $((2, 3), (5, 6)) \in R$.

Sats 2.3.4. *Relationen R på $\mathbb{N}^2$ ovan är en ekvivalensrelation.*

Bevis. Vi visar reflexivitet och symmetri och lämnar att visa transitivitet som Övning 2.4. Reflexivitet: tag $(a, b) \in \mathbb{N}^2$. Då gäller att $a + b = b + a$ vilket innebär att $(a, b)R(a, b)$. Symmetri: tag $(a, b), (c, d) \in \mathbb{N}^2$ och antag att $(a, b)R(c, d)$. Det betyder att $a+d = b+c$, vilket kan skrivas om till $c+b = d+a$, så $(c, d)R(a, b)$. □

Definition 2.3.5. En ekvivalensklass $[(a, b)]$ hörande till ekvivalensrelationen R kallas ett *heltal*. *Heltalen* $\mathbb{Z}$ är mängden av alla ekvivalensklasser i R.

Vårt mål är visa att vi med ovanstående definition faktiskt lyckats skapa negativa tal, det vill säga additiva inverser. En additiv invers b till ett element a definieras av att summan av a och b är lika med det additiva enhetselementet – det vill säga 0 – och än så länge har vi inte infört en addition på $\mathbb{Z}$, det vill säga vi har inte definierat vad vi menar med att addera två ekvivalensklasser. Innan vi kan tala om additiva enhetselement behöver vi därför följande definition.

Definition 2.3.6. Givet två ekvivalensklasser $[(a, b)], [(c, d)]$ definierar vi summan, respektive produkten, av dem som

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

Anmärkning 2.3.7. Om vi skriver $a - b$ istället för $[(a, b)]$, så får definitionerna av räkneoperationerna ovan följande utseende.

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

Anmärkning 2.3.8. Vi noterar att addition och multiplikation nu är definierade för ekvivalensklasser, men att operationerna är givna i termer av ett val av representanter från dessa ekvivalensklasser: vi adderar a och c samt b och d som alla tillhör $\mathbb{N}$ – med en addition som endast är definierad för $\mathbb{N}$ – i högerledet. För att definitionen ska vara matematiskt meningsfull och operationerna väldefinierade får resultatet inte bero på valet av representanter för ekvivalensklasserna, ty elementen i vänsterleden är ju samma sak oberoende av vilka representanter vi väljer, så högerledet måste också vara oberoende av detta val.

Sats 2.3.9. *Operationerna* $+$ *och* $\cdot$ *är väldefinierade: om* $(a_1, b_1)R(a_2, b_2)$ *och* $(c_1, d_1)R(c_2, d_2)$ *så gäller att*

$$[(a_1, b_1)] + [(c_1, d_1)] = [(a_2, b_2)] + [(c_2, d_2)]$$
$$[(a_1, b_1)] \cdot [(c_1, d_1)] = [(a_2, b_2)] \cdot [(c_2, d_2)].$$

Bevis. Vi visar att additionen är väldefinierad. Vi har att

$$[(a_1, b_1)] + [(c_1, d_1)] = [(a_1 + c_1, b_1 + d_1)]$$

och

$$[(a_2, b_2)] + [(c_2, d_2)] = [(a_2 + c_2, b_2 + d_2)].$$

För att visa att de två högerleden är samma ekvivalensklass räcker det att visa

$$(a_1 + c_1, b_1 + d_1)R(a_2 + c_2, b_2 + d_2),$$

det vill säga att

$$a_1 + c_1 + b_2 + d_2 = b_1 + d_1 + a_2 + c_2. \tag{2.6}$$

Men enligt antagande är $(a_1, b_1)R(a_2, b_2)$ och $(c_1, d_1)R(c_2, d_2)$ vilket per definition av R betyder att $a_1 + b_2 = b_1 + a_2$ och $c_1 + d_2 = d_1 + c_2$, och adderas dessa två ekvationer får vi (2.6). Att visa att multiplikationen är väldefinierad lämnas som Övning 2.5. □

Vi vill nu *identifiera* de naturliga talen med en delmängd av $\mathbb{Z}$. Detta betyder att vi vill para ihop varje naturligt tal med ett unikt heltal. Vi identifierar varje naturligt tal a med heltalet $[(a, 0)]$. Dessutom inför vi notationen $-a = [(0, a)]$ och $a - b = [(a, b)]$.

Identifikation ovan är sådan att räkneoperationerna i $\mathbb{N}$ är *kompatibla* med räkneoperationerna i $\mathbb{Z}$. Med detta avses att om $a, b \in \mathbb{N}$, så identifieras $a + b$ och $a \cdot b$ med heltalen $[(a, 0)]+[(b, 0)]$, respektive $[(a, 0)]\cdot[(b, 0)]$. Att så verkligen är fallet är lätt att verifiera :

$$\begin{aligned}[(a, 0)] + [(b, 0)] &= [(a + b, 0 + 0)] = [(a + b, 0)] \\ [(a, 0)] \cdot [(b, 0)] &= [(ab + 0 \cdot 0, a \cdot 0 + 0 \cdot b)] = [(ab, 0)]\end{aligned}$$

När vi nu gjort denna identifikation kan vi tänka på de naturliga talen som en delmängd av heltalen, det vill säga från och med nu påstår vi att $\mathbb{N} \subseteq \mathbb{Z}$.

Vi noterar nu att heltalet $[(0, 0)]$ fungerar som additivt enhetselement, ty för ett godtyckligt element $[(c, d)]$ har vi att

$$[(0, 0)] + [(c, d)] = [(c + 0, d + 0)] = [(c, d)].$$

Nu kan vi försöka hitta additiva inverser. Givet ett element $[(a, b)]$, vilket element $[(c, d)]$ har då egenskapen att $[(a, b)] + [(c, d)] = [(0, 0)]$? Enligt definitionen av addition har vi $[(a, b)] + [(c, d)] = [(a + c, b + d)]$, så elementet måste uppfylla att $a + c = b + d$, vilket exempelvis uppfylls av $c = b$, $d = a$. Således har vi att den additiva inversen av heltalet $[(a, b)]$ ges av

$$-[(a, b)] = [(b, a)].$$

Vi kan nu definiera subtraktion:

Definition 2.3.10. Låt n, m vara heltal. Då definierar vi

$$n - m = n + (-m).$$

Anmärkning 2.3.11. Om a, b är naturliga tal, så kan vi nu tolka uttrycket $a - b$ på två olika sätt, dels som heltalet $[(a, b)]$ och dels som heltalet $a + (-b)$. Detta är dock inget problem eftersom dessa tolkningar ger samma tal:

$$a + (-b) = [(a, 0)] + (-[(b, 0)]) = [(a, 0)] + [(0, b)] = [(a, b)].$$

När vi nu definierat additiva inverser och subtraktion är det lätt att lösa alla ekvationer på formen $x + a = b$, där $a, b \in \mathbb{N}$. Lösningen ges, inte helt oväntat, av $x = b - a$:

$$(b - a) + a = [(b, a)] + [(a, 0)] = [(a + b, a)] = [(b, 0)] = b.$$

Intuitivt så är heltalen ordnade efter storlek, -1 ligger till vänster om 0, som i sin tur ligger till vänster om 1 och så vidare. Innan vi preciserar vad vi menar med detta så vill vi passa på att definiera begreppet ordning.

Definition 2.3.12. Låt A vara en mängd. En *ordning* på A är en relation R med följande två egenskaper:

(i) Om $x, y \in A$ då gäller en och endast en av relationerna

$$xRy, \quad x = y \quad \text{eller} \quad yRx. \tag{2.7}$$

(ii) 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 2.3.13. Notera att en ordning är en relation men *inte* en ekvivalensrelation.

Definition 2.3.14. Låt $n, m \in \mathbb{N}$. Vi säger att m är större än n – och skriver $n < m$ – om det finns ett tal $k \neq 0$ så att $k + n = m$.

Exempel 2.3.15. Vi har att $0 < n$ för varje $n \neq 0$ ty $n + 0 = n$, det vill säga $k = n$ här. ▲

Definition 2.3.16. Vi kan nu enkelt införa en ordning på $\mathbb{Z}$, som är kompatibel med den redan införda ordningen på $\mathbb{N}$, genom att sätta

$$\begin{aligned}
&[(n, 0)] < [(m, 0)] \text{ om } n < m,\\
&[(0, n)] < [(0, m)] \text{ om } m < n,\\
&[(0, n)] < [(m, 0)] \text{ om } m \neq 0 \text{ eller } n \neq 0
\end{aligned}$$

Konstruktionen av heltalen är nu avslutad. Vi lämnar den otympliga notationen $[(n, 0)]$ och $[(0, n)]$; i fortsättningen skriver vi istället n respektive $-n$.

2.4 Konstruktion av de rationella talen

De rationella talen är tal på formen $\frac{a}{b}$, där $a, b \in \mathbb{Z}$, och $b \neq 0$, och det är konstruktionen av dessa som detta avsnitt handlar om. Tekniken för denna konstruktion påminner om den som vi använde för att konstruera $\mathbb{Z}$ från $\mathbb{N}$, men denna gång bildar vi mängden av ordnade par av *heltal* och inför en lämplig ekvivalensrelation på denna mängd.

Liksom vi införde heltalen bland annat för att kunna lösa fler ekvationer, så är ett skäl att införa de rationella talen att kunna lösa alla ekvationer på formen $ax = b$, där $a, b \in \mathbb{Z}$, $a \neq 0$. En sådan ekvation har en lösning $x \in \mathbb{Z}$ om och endast om $b = ca$, för något $c \in \mathbb{Z}$, vilket ju inte alltid är fallet (exempelvis saknar ekvationen $2x = 1$ en heltalslösning).

Innan vi går vidare till konstruktion av de rationella talen ska vi introducera lite terminologi. En viktig algebraisk observation är att heltalet 1 har egenskapen att $1 \cdot n = n$ för alla $n \in \mathbb{Z}$. Man säger att 1 är det *multiplikativa enhetselementet*.

Definition 2.4.1. För ett givet tal a är den *multiplikativa inversen* till a det tal b som uppfyller att $ab = 1$, alltså att a multiplicerat med b ger det multiplikativa enhetselementet; vi skriver då $b = a^{-1}$.

Anmärkning 2.4.2. Observera att det bland heltalen endast är 1 och -1 som har en multiplikativ invers. Liksom vi utvidgade de naturliga talen med additiva inverser och fick heltalen, så uppstår de rationella talen som utvidgningen av $\mathbb{Z} \setminus \{0\}$ med multiplikativa inverser. Anledningen till att vi inte har med talet 0 är att vi inte kan dividera med 0.

Målsättningen för avsnittet är, som vi nämnt ovan, att ge en innebörd till uttryck på formen $\frac{a}{b}$. En svårighet är att vi vill att $\frac{a}{b} = \frac{ca}{cb}$, för alla $0 \neq c \in \mathbb{Z}$, till exempel vill vi att $\frac{-1}{-2} = \frac{1}{2} = \frac{4}{8} = \ldots$ För att komma runt denna svårighet bildar vi, analogt med mängden $\mathbb{N}^2$ i förra avsnittet, mängden

$$\mathbb{Z}^2_\star = \{(a, b) \mid a, b \in \mathbb{Z}, b \neq 0\}, \tag{2.8}$$

och vi definierar relationen R så att $(a, b)R(c, d)$ om och endast om $ad = bc$.

Anmärkning 2.4.3. Notera att om vi istället för (a, b) skriver $\frac{a}{b}$ så är detta ekvivalent med att $\left(\frac{a}{b}\right) R \left(\frac{c}{d}\right)$ om och endast om $ad = bc$, vilket bör vara bekant för läsaren.

Hjälpsats 2.4.4. *Relationen R är en ekvivalensrelation på $\mathbb{Z}^2_\star$.*

Bevis. Vi måste bevisa att R är reflexiv, symmetrisk samt transitiv.

För att visa att R är reflexiv måste vi visa att $(a, b)R(a, b)$ för alla $a, b \in \mathbb{Z}$, men detta följer av att $ab = ba$, för alla a, b.

R är symmetrisk om $(a, b)R(c, d)$ medför att $(c, d)R(a, b)$. Men $(a, b)R(c, d)$ om $ad = bc$, vilket medför $cb = da$, vilket är ekvivalent med $(c, d)R(a, b)$.

R är transitiv om $(a, b)R(c, d)$ och $(c, d)R(e, f)$ medför $(a, b)R(e, f)$. Men om $(a, b)R(c, d)$ och $(c, d)R(e, f)$ då har vi enligt definitionen av R att $ad = bc$ samt $cf = de$. Det följer att

$$af \cdot d = ad \cdot f = bc \cdot f = b \cdot cf = b \cdot de = be \cdot d.$$

Eftersom $d \neq 0$, så följer det att $af = be$, det vill säga att $(a, b)R(e, f)$, vilket skulle visas. □

Definition 2.4.5. En ekvivalensklass till R kallas ett *rationellt tal* och vi låter $\mathbb{Q}$ vara mängden av alla rationella tal. Vi inför beteckningen $\frac{a}{b}$ för det rationella tal som är ekvivalensklassen till elementet $(a, b) \in \mathbb{Z}^2_\star$, det vill säga $\frac{a}{b} = [(a, b)]$.

Bokstaven $\mathbb{Q}$ kommer från engelskans "quotient", som betyder kvot, och ett rationellt tal är ju just en kvot mellan två heltal.

2.5 Räkneoperationer på de rationella talen

För att kunna använda oss av rationella tal måste vi definiera räkneoperationer på dem.

Definition 2.5.1. Låt $a, b, c, d \in \mathbb{Z}$, med $b, d \neq 0$. Addition samt multiplikation av rationella tal definieras som

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

Om vi istället gör omskrivningen $[(a, b)] = \frac{a}{b}$ så får definitionen ovan det kanske för läsaren mer bekanta utseendet

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

Notera dock att vi som tidigare (se Anmärkning 2.3.8) har problemet att operationerna är definierade på ekvivalensklasser, men i termer av representanter för ekvivalensklasserna. Att visa att det är en matematiskt meningsfull definition – det vill säga att den är oberoende av vilken representant vi väljer – är Övning 2.12.

För att lösa alla ekvationer på formen $ax = b$, $a, b \in \mathbb{Z}$, $a \neq 0$ måste vi visa att $\mathbb{Z}$ kan identifieras med en delmängd av $\mathbb{Q}$. Vi observerar först att $[(0, 1)] \in \mathbb{Q}$ fungerar som ett additivt enhetselement, ty

$$[(0, 1)] + [(c, d)] = [(0d + 1c, 1d)] = [(c, d)],$$

så vi identifierar $\mathbb{Z} \ni 0 = [(0, 1)] = [(0, b)] \in \mathbb{Q}$. Det multiplikativa enhetselementet är $[(1, 1)]$, vilket vi lämnar åt läsaren att verifiera, se Övning 2.8. Omskrivningen $[(a, b)] = \frac{a}{b}$ leder oss att generellt vilja göra identifikationen $\mathbb{Z} \ni n = [(n, 1)]$. Detta visar sig vara ett bra val också. Vi har nämligen att

$$[(m, 1)] \cdot [(n, 1)] = [(mn, 1)] = mn,$$
$$[(m, 1)] + [(n, 1)] = [(m + n, 1)] = m + n,$$

så att räkneoperationera i $\mathbb{Q}$ är kompatibla med dem i $\mathbb{Z}$ under denna identifikation. Från och med kommer vi därför betrakta heltalen som en delmängd av de rationella talen, det vill säga från och med nu påstår vi att $\mathbb{Z} \subseteq \mathbb{Q}$.

Anmärkning 2.5.2. Identifikationen $n = [(n, 1)]$ är en definition vi har valt att göra, dock har ovanstående stycke förhoppningsvis övertygat läsaren om att det är en naturlig definition.

Sats 2.5.3. *Varje nollskilt element* $[(a,b)] \in \mathbb{Q}$ *har en multiplikativ invers som ges av*

$$[(a,b)]^{-1} = [(b,a)].$$

Bevis. Att $[(a,b)] \neq 0$ är ekvivalent med att $a \neq 0$, och därför har vi att $[(b,a)] \in \mathbb{Q}$. Enligt definitionen av multiplikation har vi nu att

$$[(a,b)] \cdot [(b,a)] = [(ab,ba)] = [(1,1)] = 1,$$

vilket skulle visas. □

Vi kan nu definiera division:

Definition 2.5.4. Låt $p, q \in \mathbb{Q}$. Då definierar vi

$$\frac{p}{q} = p \cdot q^{-1}.$$

Anmärkning 2.5.5. Om n, m är heltal, så kan vi nu tolka uttrycket $\frac{n}{m}$ på två olika sätt, dels som det rationella talet $[(n,m)]$ och dels som det rationella talet $n \cdot m^{-1}$. Detta är dock inget problem eftersom dessa tolkningar ger samma tal:

$$n \cdot m^{-1} = [(n,1)] \cdot [(m,1)]^{-1} = [(n,1)] \cdot [(1,m)] = [(n,m)].$$

I de kommande kapitlen kommer vi att hålla oss till notationen $\frac{n}{m}$.

Vi kan nu visa att ekvationen $ax = b$ går att lösa i $\mathbb{Q}$ om $a \neq 0$. Enligt vår identifikation $n = [(n,1)]$ får vi istället ekvationen $[(a,1)]x = [(b,1)]$. Multiplicerar vi med den multiplikativa inversen $[(1,a)]$ på båda sidor erhålls lösningen $x = [(1,a)][(b,1)] = [(b,a)] = \frac{b}{a}$.

Övningar

Övning 2.1 ($\star\star$)**.** 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 2.2 ($\star\star\star$)**.** Låt A och R vara som i föregående övning. Tag $x, y \in A$ med xRy. Visa att

$$[x] = [y]. \tag{2.9}$$

Ledning: Visa att $[x] \subset [y]$ samt $[y] \subset [x]$.

Övning 2.3 ($\star\star\star$)**.** Återigen är A och R som ovan. Antag att $x, y \in A$ inte är relaterade. Visa att

$$[x] \cap [y] = \emptyset. \tag{2.10}$$

Ledning: antag att $[x] \cap [y] \neq \emptyset$ och härled en motsägelse.

Övning 2.4 ($\star$)**.** Avsluta beviset av Sats 2.3.4.

Övning 2.5 ($\star\star\star$)**.** Avsluta beviset av Sats 2.3.9.

Övning 2.6 ($\star$)**.** Låt $0 < m, n \in \mathbb{N}$. Visa att $(-m)(-n) > 0$.

Övning 2.7 ($\star$)**.** Låt $n < 0 < m$ vara två heltal. Visa att $mn < 0$.

Övning 2.8 ($\star$)**.** Visa att $[(1,1)] \in \mathbb{Q}$ är det multiplikativa enhetselementet i $\mathbb{Q}$.

Övning 2.9 ($\star\star$)**.** Visa att räknereglerna från sats B.1.10 även är giltiga för additionen och multiplikationen för $\mathbb{Z}$ givna i Definition 2.3.6.

Övning 2.10 ($\star$)**.** Visa att $0 = \frac{0}{b}$ för alla $b \in \mathbb{Z}$ med $b \neq 0$. *Ledning: Vi har identifierat heltalet* 0 *med det rationella talet* $\frac{0}{1}$.

Övning 2.11 ($\star\star$)**.** Låt $M = \{(a,b) \mid a, b \in \mathbb{Z}\}$ 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 $\frac{a}{b}$.

Övning 2.12 ($\star\star$)**.** Visa att operationerna $+$ och $\cdot$ i Definition 2.5.1 är väldefinierade. *Ledning*: använd samma teknik som i beviset av Sats 2.3.9.

Övning 2.13 ($\star$)**.** Visa att för $n \in \mathbb{N}$ och $q \in \mathbb{Q}$ gäller det att

$$n \cdot q = \underbrace{q + q + \cdots + q}_{n \text{ gånger}}.$$

3 De rationella talen och ordnade kroppar

Vi fortsätter i detta kapitel med att studera de rationella talen. Bland annat så kommer vi att visa det högst icke-intuitiva resultatet att $\mathbb{Q}$ har lika många element som $\mathbb{N}$. För att göra det behöver vi först definiera begreppet *bijektion*, som kommer från läran om funktioner.

3.1 Funktioner

Innan vi gör en allmän definition av vad en funktion är kan det vara på sin plats att titta på något välbekant, nämligen en formel som $f(x) = x^2 + 1$. Detta är ett exempel på en funktion. Formeln säger att om vi tar ett tal $x \in \mathbb{Z}$ så får vi ett nytt tal $f(x) \in \mathbb{Z}$ genom att göra beräkningen $x^2 + 1$; till exempel får vi $f(2) = 2^2 + 1 = 5$. Vi säger att f är en funktion från heltalen till heltalen, eftersom både det vi stoppar in, x, och det vi får ut, $f(x)$, är heltal. Vi brukar beteckna detta med $f\colon \mathbb{Z} \to \mathbb{Z}$.

Definition 3.1.1. Låt A och B vara mängder. En *funktion* $f\colon A \to B$ är ett sätt att till varje element $a \in A$ tilldela ett välbestämt element $b \in B$. Vi skriver $f(a) = b$. Vi säger att a *avbildas* på b och att b är *bilden* av a.

Anmärkning 3.1.2. Ofta säger man att f är en funktion från A till B istället för att använda beteckningen $f\colon A \to B$. Ett vanligt alternativ till ordet funktion är *avbildning*.

Exempel 3.1.3. Betrakta mängderna $A = \{1, 2, 3\}$ och $B = \{1, 2, \ldots, 100\}$. Ett exempel på en funktion $f\colon A \to B$ ges av $f(n) = 2n$ för $n \in A$. Vi har alltså att $f(1) = 2$, $f(2) = 4$ och $f(3) = 6$. Per definition måste vi ha $f(a) \in B$ för alla $a \in A$, och detta gäller ju här eftersom

$$f(1) = 1 \in B, \quad f(2) = 4 \in B \quad \text{och} \quad f(3) = 6 \in B.$$

I detta exempel definieras funktionen f av formeln $f(n) = 2n$, men det är inte alls nödvändigt att det finns en formel som beskriver hur funktionen verkar. Om vi som här har en funktion från den *ändliga* mängden $A = \{1, 2, 3\}$ kan man till exempel definiera funktionen med hjälp av en tabell:

n	$f(n)$
1	2
2	4
3	6

▲

Exempel 3.1.4. Låt $h\colon \mathbb{Z} \to \mathbb{Z}$ vara den funktion som definieras av formeln $h(x) = 2x^2 - x^3$. Vi har exempelvis att

$$h(1) = 2\cdot 1^2 - 1^3 = 1, \quad \text{och} \quad h(-2) = 2\cdot(-2)^2 - (-2)^3 = 2\cdot 4 - (-8) = 16. \ ▲$$

Definition 3.1.5. Låt A och B vara mängder och $f\colon A \to B$. Funktionen f är *injektiv* om den uppfyller att $a_1 \neq a_2$ medför att $f(a_1) \neq f(a_2)$. f är *surjektiv* om det för varje $b \in B$ finns ett $a \in A$ så att $f(a) = b$. Om f är både injektiv och surjektiv säger man att f är *bijektiv* eller att f är en *bijektion*.

En bijektion $f\colon A \to B$ mellan A och B parar således ihop elementen i A och B med varandra i ett "ett-till-ett" förhållande. Det är därför rimligt att förmoda att existensen av en bijektion $f\colon A \to B$ medför existensen av en bijektion $g\colon B \to A$.

Sats 3.1.6. *Antag att det finns en bijektion $f\colon A \to B$. Då finns det även en bijektion $g\colon B \to A$.*

Bevis. Vi noterar först att det för varje $b \in B$ finns ett unikt $a \in A$ så att $f(a) = b$. Ty det finns åtminstone ett sådant a eftersom f är en surjektion, och eftersom f även är en injektion så kan högst ett element avbildas på b. Vi bildar funktionen g genom att för varje $b \in B$ definiera $g(b) = a$, där $a \in A$ är det unika elementet så att $f(a) = b$. Då är $g(b)$ välbestämd, så g är en funktion $g\colon B \to A$. Det kvarstår att visa att g är en bijektion. Till varje element $a \in A$ finns ett element $b \in B$ så att $g(b) = a$, nämligen elementet $b = f(a)$, så g är en surjektion. För att visa att g även är injektiv använder vi ett motsägelsebevis. Vi antar därför att det finns $b_1, b_2 \in B$ så att $b_1 \neq b_2$, men $g(b_1) = g(b_2)$. Per definition av g har vi då att $b_1 = f(g(b_1)) = f(g(b_2)) = b_2$, vilket är en motsägelse eftersom vi antog att $b_1 \neq b_2$. Således är g en bijektion $B \to A$. □

Anmärkning 3.1.7. Funktionen g som förekommer i beviset av Sats 3.1.6 kallas *inversen* till f och skrivs f^{-1}.

3.2 Kardinaliteten av de rationella talen

Mängderna $\mathbb{N}, \mathbb{Z}$ och $\mathbb{Q}$ innehåller alla oändligt många element, och de identifikationer vi införde i förra kapitlet medför inklusionerna $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q}$. Det känns då intuitivt att säga att $\mathbb{Q}$ har fler element än $\mathbb{Z}$ som i sin tur har flera element än $\mathbb{N}$. Vi har dock inte definierat vad vi menar med begrepp som 'fler' eller 'lika många' när vi pratar om oändligheter, så innan vi kan uttala oss med matematisk säkerhet om saken, så bör vi förtydliga vad vi egentligen menar. Vi börjar med ett illustrerande exempel:

Exempel 3.2.1. Mängden $A = \{3, 9, 10^{40000}, 5\}$ har 4 element. Hur kom författarna – och förhoppningsvis läsaren – fram till det? Vi räknade, vilket betyder att vi tilldelade varje element i A ett unikt tal mellan 1 och 4. Matematiskt kan det formuleras som att vi bildade en funktion
$f\colon B_4 = \{1, 2, 3, 4\} \to A$, så att det för varje element $a \in A$ finns exakt ett $b \in B_4$ så att $f(b) = a$, vilket är ekvivalent med att f är en bijektion från B_4 till A. Vilken ordning vi räknade elementen påverkar inte antalet element i A, och därför är funktionens exakta form inte viktig. ▲

Exempel 3.2.1 leder oss till följande definition:

Definition 3.2.2. En mängd A har n element om det finns en bijektion

$$f\colon B_n = \{1, 2, \ldots, n-1, n\} \to A.$$

Två mängder A_1, A_2 sägs ha samma *kardinalitet* alternativt *lika många element* om det finns en bijektion $f\colon A_1 \to A_2$. Mängden A sägs vara en *oändlig* mängd om $A \neq \emptyset$ och det inte finns en bijektion $f\colon B_n \to A$ för något n.

Anmärkning 3.2.3. Att A_1 har lika många element som A_2 medför enligt Sats 3.1.6 att A_2 har lika många element som A_1, så vår definition av 'lika många' verkar vettig. Dessutom har vi att om A_1 har n element, och A_1 har lika många element som A_2, så har även A_2 n element. Ty då finns det en bijektion $f_1\colon B_n \to A_1$ och en bijektion $f_2\colon A_1 \to A_2$, och den sammansatta funktionen[4] $f_2 \circ f_1\colon B_n \to A_2$ är då en bijektion, vilket vi uppmanar läsaren att övertyga sig om.

Definition 3.2.2 ger en precis innebörd till påståendet att två oändliga mängder har lika många element, nämligen att det finns en bijektion mellan dem. Följande definition är praktisk.

Definition 3.2.4. En mängd A sägs vara *uppräknelig* om det finns en bijektion $f\colon \mathbb{N} \to A$. Om A är oändlig och det inte finns en bijektion $f\colon \mathbb{N} \to A$, så sägs A vara *överuppräknelig*.

Anmärkning 3.2.5. Att en mängd A är uppräknelig är ekvivalent med att man till varje $n \in \mathbb{N}$ kan ordna ett unikt element $x_n \in A$ så att

$$A = \{x_0, x_1, x_2, \dots\}.$$

En bijektion från $\mathbb{N}$ till A svarar således mot en lista, eller en *uppräkning*, av elementen i A.

Exempel 3.2.6. Mängden $\mathbb{N}$ är uppräknelig. För att visa detta behöver vi bilda en bijektion $f\colon \mathbb{N} \to \mathbb{N}$. Vi kan till exempel ta $f(n) = n$, som uppenbarligen är en bijektion. ▲

Exempel 3.2.7. Mängden $\mathbb{Z}$ är uppräknelig. Vi sätter $f(n) = x_n$ där

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

Då har vi att $x_0 = 0, x_1 = 1, x_2 = -1, x_3 = 2, x_4 = -2, x_5 = 3, x_6 = -3$, och så vidare så att $\mathbb{Z} = \{x_0, x_1, x_2, \dots\}$. ▲

Observera att elementens ordning är ändrad i ovanstående uppräkning av $\mathbb{Z}$. Detta är oundvikligt då vi inte kan börja listan i "$-\infty$".

Vi ska snart se att även $\mathbb{Q}$ är en uppräknelig mängd. Först vill vi dock illustrera vikten av att välja en uppräkning på ett elegant sätt.

Sats 3.2.8. *Mängden $A = \{1/n : n = 2, 3, 4, \dots\}$ är uppräknelig.*

[4]Givet två funktioner $f\colon A \to B$ och $g\colon B \to C$ bildas den sammansatta funktionen $h = g \circ f\colon A \to C$ genom att sätta funktionen $h(a) = g(f(a))$. Det innebär att vi får $h(a)$ genom att först utvärdera f i a och därefter g i elementet $f(a) \in B$.

Bevis. Vi påstår att $f : \mathbb{N} \to A$, med $f(n) = x_n = 1/(n+2)$ är en bijektion. För att bevisa detta behöver vi bevisa att f är injektiv och surjektiv. Att f är surjektiv följer från definitionen av mängden A. Det kvarstår att visa injektiviteten. Anta därför att $n, m \in \mathbb{N}$ och $f(n) = f(m)$. Då har vi att $1/(n+2) = 1/(m+2)$, vilket medför att $n = m$. Därmed är f injektiv. Eftersom f är både injektiv och surjektiv, så är f bijektiv. Därmed är A uppräknelig enligt Definition 3.2.4. □

Vi noterar att alla element i mängden $A = \{1/n : n = 2, 3, 4, \dots\}$ ligger mellan 0 och 1. Sats 3.2.8 visar därför att om vi försöker bilda en uppräkning av de rationella talen genom att räkna "rakt fram" i ett intervall, så kommer listan inte ens innehålla två på varandra följande heltal, och därmed inte alla rationella tal heller. Beviset av följande sats visar hur man istället bör göra:

Sats 3.2.9. *Mängden $\mathbb{Q}$ är uppräknelig.*

Bevis. Precis som i ekvation (2.8) låter vi $\mathbb{Z}^2_\star = \{(a, b) : a, b \in \mathbb{Z}, b \neq 0\}$. Elementen i $\mathbb{Z}^2_\star$ kan uppräknas upp enligt följande växande spiral:

$$
\begin{array}{ccccccc}
\ddots & \vdots & \vdots & \vdots & \vdots & \iddots \\
\cdots & (-1,-2) & (0,-2) & (1,-2) & (2,-2) & \cdots \\
\cdots & (-1,-1) & \longrightarrow (0,-1) & \longrightarrow (1,-1) & \longrightarrow (2,-1) & \cdots \\
 & \uparrow & & & \downarrow & \\
\cdots & (-1,1) & (0,1) & \longrightarrow (1,1) & (2,1) & \cdots \\
 & \uparrow & & \downarrow & & \\
\cdots & (-1,2) & \longleftarrow (0,2) & \longleftarrow (1,2) & (2,2) & \cdots \\
\cdots & (-1,3) & (0,3) & (1,3) & (2,3) & \cdots \\
\iddots & \vdots & \vdots & \vdots & \vdots & \ddots
\end{array}
$$

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

$$y_0 = (0,1), \quad y_1 = (1,1), \quad y_2 = (1,2), \quad y_3 = (0,2), \dots \tag{3.1}$$

som uppfyller att $\mathbb{Z}^2_\star = \{y_0, y_1, y_2, \dots\}$. $\mathbb{Q}$ består av ekvivalensklasser i $\mathbb{Z}^2_\star$, exempelvis har vi att $[(1,2)] = \frac{1}{2} = \frac{2}{4}$. Om vi låter $f(n) = x_n = [y_n] \in \mathbb{Q}$ för varje $n \in \mathbb{N}$ (alltså är x_n den ekvivalensklass som y_n tillhör), så får vi att $\mathbb{Q} = \{x_0, x_1, x_2, \dots\}$. Denna avbildning är inte en bijektion, ty om $[y_n] = [y_m]$ då har vi att $x_n = x_m$, och således finns det inte ett unikt element $n \in \mathbb{N}$

för varje element i $\mathbb{Q}$. Detta kan emellertid åtgärdas genom att radera alla upprepningar som förekommer i listan, och vid varje raderingar helt enkelt förskjuta alla senare termer i listan ett steg upp. Exempelvis är $x_0 = [(0,1)]$, men även $x_3 = [(0,2)] = [(0,1)]$, så vi raderar $[(0,2)]$ ur listan och sätter istället $x_3 = [(-1,2)]$. Därefter går vi bakåt i listan och kollar om detta element är en upprepning av ett tidigare element eller inte. Är det inte det låter vi det stå, är det en upprepning raderar vi det ur listan och fortsätter. Detta (oändliga) förfarande skapar en bijektion, och vi drar slutsatsen att det *finns* en bijektion mellan $\mathbb{N}$ och $\mathbb{Q}$, även om vi inte har någon formel för denna funktion. □

3.3 Irrationella tal

Är alla tal på tallinjen rationella? Frågan är förstås inte välställd då vi inte har definierat något matematiskt objekt som vi kallar "tallinjen", men den rymmer ändå en poäng. Om vi fixerar en längdenhet och placerar ut de rationella talen längs en rak linje så att talet $q \in \mathbb{Q}$ motsvarar avståndet q längdenheter från 0, så kan vi ställa frågan om alla avstånd längs linjen är representerade av rationella tal. Svaret är nej, vilket insågs redan i antikens Grekland.

Antag att vi av något skäl måste konstruera en kvadrat med arean $A = 2$, och vi därför vill hitta sidlängden s som ger en sådan kvadrat. Eftersom $A = s^2$ får vi att $s^2 = 2$, och därmed $s = \sqrt{2}$. Vid en praktisk konstruktion kan man förstås använda sig av en miniräknare för att lösa detta och får då något i stil med: $s = 1{,}414213562$. Men detta är inte en exakt lösning: vi såg redan i Sats 1.3.1 att $\sqrt{2}$ inte är ett rationellt tal.

Det finns således avstånd som inte motsvarar rationella tal. Vi kommer att konstruera tal som motsvarar dessa avstånd i kapitel 4. Tal på tallinjen som inte är rationella kallas irrationella, och de tillhör den talmängd som vi kallar de reella talen.

3.4 Kroppar

De rationella talen har många bra egenskaper, men faktumet att det finns irrationella avstånd är obekvämt och medför att vi måste utvidga vårt talbegrepp. När detta görs är det viktigt att de rationella talens grundläggande algebraiska egenskaper bevaras, så vi sammanfattar dessa i följande definition:

Definition 3.4.1. 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 $x \cdot (y+z) = (x \cdot y) + (x \cdot z)$.

Anmärkning 3.4.2. En kropp K har i grunden alltså endast två räknesätt: addition och multiplikation. Vi kan dock införa subtraktion och division genom

$$x - y = x + (-y) \tag{3.2}$$

$$\frac{x}{y} = x \cdot (y^{-1}), y \neq 0 \tag{3.3}$$

Som vi nämnt ovan utgör de rationella talen en kropp. Vi formulerar detta som en sats.

Sats 3.4.3. *Mängden $\mathbb{Q}$ med operationerna $+$ och $\cdot$ är en kropp.*

Bevis. Tag godtyckliga tal $p, q, r \in \mathbb{Q}$. Då finns heltal a, b, c, d, e och f med $b, d, f \neq 0$ så att $p = \frac{a}{b}, q = \frac{c}{d}, r = \frac{e}{f}$. Det vi måste visa är att dessa tal och operationerna $+$ och $\cdot$ uppfyller villkoren i Definition 3.4.1.

Vi bevisar här egenskaperna (A2) och (M3) och lämnar åt läsaren att bevisa de övriga egenskaperna i Övning 3.8.

(A2) Vi har att

$$p + q = \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{cb + da}{db} = \frac{c}{d} + \frac{a}{b} = q + p. \tag{3.4}$$

Alltså är addition av rationella tal kommutativt. (I den tredje likheten har vi använt att addition och multiplikation av av heltal är kommutativt.)

(M3) Associativiteten för multiplikationen av rationella tal följer från

$$(p \cdot q) \cdot r = \frac{ac}{bd} \cdot \frac{e}{f} = \frac{ace}{bdf} = \frac{a}{b} \cdot \frac{ce}{df} = p \cdot (q \cdot r). \tag{3.5}$$

(Här har vi använt att multiplikation av heltal är associativ.)

□

Anmärkning 3.4.4. Vi noterar att $\mathbb{N}$ *inte* är en kropp. Exempelvis gäller det att $-x \in \mathbb{N}$ endast om $x = 0$. Heltalen är inte heller en kropp: $x^{-1} \in \mathbb{Z}$ endast om $x = 1$.

Exemplet nedan visar att det finns kroppar som inte alls verkar likna $\mathbb{Q}$.

Exempel 3.4.5. Låt $\mathbb{Z}_2 = \{0, 1\}$. Definiera två operationer $\oplus$ "addition" och $\otimes$ "multiplikation" på denna mängd enligt följande tabeller

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0
1	0	1

I Övning 3.14 ombeds läsaren att visa att $\mathbb{Z}_2$ med operationerna definierade ovan är en kropp. ▲

3.5 Ordnade kroppar

Utöver räkneoperationerna kan $\mathbb{Q}$ även utrustas med en ordningsrelation som har ett naturligt samspel med räkneoperationerna. Denna egenskap sammanfattas i begreppet *ordnad kropp*. Vi repeterar definitionen av en ordning:

Definition 3.5.1. Låt A vara en mängd. En *ordning* på A är en relation R med följande två egenskaper:

(i) Om $x, y \in A$ då gäller en och endast en av relationerna

$$xRy, \quad x = y \quad \text{eller} \quad yRx. \tag{3.6}$$

(ii) 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* $x = y$.

Definition 3.5.2. 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) $0 < xy$ om $0 < x$ och $0 < y$

Definitionerna 3.5.1 och 3.5.2 formaliserar de räknelagar vi normalt använder oss av när vi räknar med olikheter. Alla andra regler för räkning med olikheter följer från de egenskaper som definierar en ordnad kropp. I hjälpsatserna som följer nedan går vi igenom några av dessa regler.

Hjälpsats 3.5.3. *Låt K vara en ordnad kropp och låt $x \in K$. Det gäller att $0 < x$ medför att $-x < 0$ och att $x < 0$ medför att $0 < -x$*

Bevis. Antag först att $0 < x$. (O1) i Definition 3.5.2 medför då att

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

Från egenskaperna (A4) och (A5) i Definition 3.4.1 följer det nu att $-x < 0$. Ett liknande resonemang ger att $x < 0$ medför att $0 < -x$. □

Följande hjälpsats säger att "minus gånger minus är plus":

Hjälpsats 3.5.4. *Låt K vara en ordnad kropp och $0 > x, y \in K$. Då gäller att $xy > 0$.*

Bevis. Hjälpsats 3.5.3 medför att $0 < (-x), (-y)$. Enligt (O2) i Definition 3.5.1 har vi därför att $0 < (-x)(-y)$. Därmed räcker det att visa att $xy = (-x)(-y)$. Vi visar först att $-x = (-1) \cdot x$, där -1 är den additiva inversen till det multiplikativa enhetselementet 1: Övning 3.6 ger att $(1 - 1)x = 0x = 0$, och enligt distributiva lagen har vi även att $(1 - 1)x = 1x + (-1)x$. Därmed gäller det att $1x + (-1)x = 0$. Men $1x = x$, per definition av 1, så $x + (-1)x = 0$, vilket medför att $(-1)x = -x$. Då multiplikationen i en kropp är kommutativ får vi att $(-x)(-y) = (-1)x(-1)y = (-1)(-1)xy = (-(-1))xy = 1(xy) = xy$, vilket skulle visas. □

Hjälpsats 3.5.5. *Låt K vara en ordnad kropp och låt $x, y, z \in K$ vara sådana att $x < y$ och $z > 0$. Då gäller det att $zx < zy$.*

Bevis. Beviset är lämnat åt läsaren i Övning 3.11 □

Hjälpsats 3.5.6. *Låt K vara en ordnad kropp och låt $y, z \in K$ vara sådana att $1 < y$ och $z > 0$. Då gäller det att $z < zy$.*

Bevis. Beviset är lämnat åt läsaren i Övning 3.12. □

Vi inför nu en ordning på de rationella talen.

Definition 3.5.7. För ett rationellt tal $\frac{a}{b}$ låter vi $0 < \frac{a}{b}$ betyda att $0 < a \cdot b$. För två rationella tal q och r skriver vi $q < r$ om $0 < r - q$.

Notera hur ordningen på heltal används i den första definitionen som i sin tur används i andra definitionen. Självklart måste man ställa sig frågan om relationen $<$ är väldefinierad av detta, det vill säga om definitionerna ovan är oberoende av hur de rationella talen representeras. Att visa detta är Övning 3.7.

Vi har nämnt ovan att $\mathbb{Q}$ är ordnad kropp. Vi avslutar kapitlet med att formulera detta som en sats.

Sats 3.5.8. *Mängden $\mathbb{Q}$ med operationerna $+$ och $\cdot$, samt med ordningsrelation $<$ är en ordnad kropp.*

Bevis. Beviset är lämnat åt läsaren i Övning 3.10. □

Satsen ovan medför att alla vanliga räkneregler för addition, multiplikation och olikheter gäller för $\mathbb{Q}$. Exempelvis kan vi använda alla räkneregler från Definition 3.4.1, Definition 3.5.1, Definition 3.5.2 och Hjälpsatserna 3.5.3 - 3.5.6 när vi räknar med rationella tal.

Övningar

Övning 3.1 ($\star\star$)**.** Ge ett exempel på en funktion från mängden $\{1, 2, 3, 4\}$ till mängden $\{A, B, C\}$. Hur många olika funktioner $f\colon \{1, 2, 3, 4\} \to \{A, B, C\}$ finns det?

Övning 3.2 ($\star\star$)**.**

(i) Beskriver $f(a) = \pi$, $f(b) = \star$ och $f(0) = 2$ en avbildning från mängden $\{0, a, b, 1\}$ till mängden $\{\pi, \star, 2\}$?

(ii) Beskriver $f(a) = \pi$, $f(b) = \star$ och $f(a) = \star$ en avbildning från $\{a, b\}$ till $\{\pi, \star, 2\}$?

Om svaret är nej, kan du rätta till det så att det blir funktioner?

Övning 3.3 ($\star\star\star$)**.** Antag att alla mängderna $A_1, A_2, A_3, \ldots$ är uppräkneliga. Visa att då är unionen $A_1 \cup A_2 \cup A_3 \cup \ldots$, det vill säga mängden av alla element som tillhör någon av mängderna $A_1, A_2, \ldots$, uppräknelig.

Övning 3.4 ($\star\star\star$)**.** Använd resultatet från Övning 3.3 för att bevisa att mängden

$$\mathscr{A} = \{B \subseteq \mathbb{Z} \mid B \text{ är ändlig}\} \tag{3.7}$$

är uppräknelig. Ett element i $\mathscr{A}$ är således en delmängd av $\mathbb{Z}$. (Att en mängd är ändlig betyder att den innehåller n element för något $n \in \mathbb{N}$).
OBS: För att lösa denna uppgift krävs ett induktionsbevis.

Övning 3.5 ($\star\star$)**.** Låt K vara en kropp. Visa att enhetselementen i K är unika. Med detta avses att det endast kan finnas ett element i K som uppfyller egenskap (A4), och att det endast kan finnas ett element i K som uppfyller egenskap (M4).

Övning 3.6 ($\star\star$)**.** Låt K vara en kropp och $0 \in K$ vara det additiva enhetselementet. Visa att $0 \cdot x = 0$ för alla $x \in K$.

Övning 3.7 ($\star\star$)**.** Antag att $\frac{a}{b} = \frac{c}{d}$. Visa att $0 < \frac{a}{b}$ om och endast om $0 < \frac{c}{d}$ (se Definition 3.5.7).

Övning 3.8 ($\star\star$)**.** Slutför beviset av Sats 3.4.3.

Övning 3.9 ($\star\star\star$)**.** Visa att relationen $<$ på $\mathbb{Q}$ i Definition 3.5.7 är en ordning.

Övning 3.10 ($\star\star\star$)**.** Visa att med ordningen $<$ är $\mathbb{Q}$ en ordnad kropp.

Övning 3.11 ($\star\star$)**.** Låt K vara en ordnad kropp och låt $x, y, z \in K$ vara sådana att $x < y$ och $z > 0$. Då gäller det att $zx < zy$.

Övning 3.12 ($\star$)**.** Låt K vara en ordnad kropp och låt $y, z \in K$ vara sådana att $1 < y$ och $z > 0$. Då gäller det att $z < zy$.

Ledning: använd Hjälpsats 3.5.5.

Övning 3.13 ($\star\star$)**.** Låt q, r vara två element i en ordnad kropp sådana att $q < r$. Visa att

$$q < \frac{q+r}{2} < r. \tag{3.8}$$

Övning 3.14 ($\star\star$)**.** Låt $\mathbb{Z}_2 = \{0, 1\}$. Definiera två operationer $\oplus$ "addition" och $\otimes$ "multiplikation" på denna mängd enligt följande tabeller

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0
1	0	1

Visa att $\mathbb{Z}_2$ med dessa operationer är en kropp.

4 Konstruktion av de reella talen

Ett förhoppningsvis välbekant sätt att tänka på tallinjen – det vill säga de reella talen – är som en mängd av decimaltal. Kanske inställer sig därför följande fråga hos läsaren: Kan vi inte helt enkelt kan definiera de reella talen som mängden av alla decimaltal? Problemet med detta är dock att vi hittills inte definierat vad ett decimaltal är för något. För att illustrera denna problematik, låt oss betrakta decimalutvecklingen av det reella talet $\sqrt{2}$:

$$\sqrt{2} = 1{,}41421356237\ldots$$

Ett sätt att tänka på decimalutvecklingen ovan är som ett "gränsvärde" av följande oändliga lista av rationella tal

$$\begin{aligned} e_0 &= 1 \\ e_1 &= 1{,}4 \\ e_2 &= 1{,}41 \\ e_3 &= 1{,}414 \\ &\vdots \end{aligned}$$

Men "gränsvärdet" $\sqrt{2}$ av dessa tal är inte rationellt, så vi är tvungna att ge en konkret konstruktion av en större mängd av tal – de reella talen. När det är gjort kommer vi i Kapitel 5 se att vi kan tänka på reella tal just som oändliga decimalutvecklingar.

En sak som vi önskar oss av de reella talen är de ska innehålla de rationella talen och ha räkneoperationer och en ordningsrelation som alla är kompatibla med de som redan är införda på $\mathbb{Q}$. Detta kan vi uttrycka som att vi vill att $\mathbb{Q}$ ska vara en ordnad delkropp[5] till de reella talen.

Vidare bör de reella talen inte ha några "hål". Detta innebär att de bör innehålla alla tal som motsvarar de punkter på tallinjen som vi saknar bland de rationella talen (som t.ex. $\sqrt{2}$). Den egenskap hos de reella tal som säkerställer frånvaron av hål kallas för *supremumegenskapen* (detta begrepp kommer att definieras i nästa avsnitt).

Sammantaget betyder detta att vi vill att de reella talen ska vara en ordnad kropp med supremumegenskapen, sådan att de rationella talen är en ordnad delkropp[6].

Vi formulerar detta som en sats.

Sats 4.0.9. *Det existerar en ordnad kropp $\mathbb{R}$ med supremumegenskapen, som innehåller $\mathbb{Q}$ som en ordnad delkropp.*

Att bevisa satsen ovan är vårt huvudsakliga mål i detta kapitel.

Sats 3.5.8 visar att $\mathbb{Q}$ är en ordnad kropp, men som sådan är den inte unik. Däremot är det intressant nog så att det väsentligen endast finns en ordnad kropp med supremumegenskapen.

[5] Se Appendix C för en definition av begreppet ordnad delkropp.

[6] Faktum är att varje ordnad kropp har de rationella talen som en ordnad delkropp, så det sista kravet är egentligen överflödigt.

Sats 4.0.10. *Alla ordnade kroppar med supremumegenskapen är isomorfa.*

Appendix C ger en definition av begreppet isomorfi. En skiss av beviset av Sats 4.0.10 finns i Appendix D.

Anmärkning 4.0.11. Sats 4.0.10 visar att alla ordnade kroppar med supremumegenskapen väsentligen är identiska. Satsen visar däremot *inte* att någon sådan kropp finns. Att konstruera en sådan kropp, det vill säga $\mathbb{R}$, är, som vi nämnt ovan, det huvudsakliga målet i detta kapitel.

4.1 Supremumegenskapen

Den väsentliga egenskapen som utmärker de reella talen – frånvaron av ”hål” – är supremumegenskapen.

Definition 4.1.1. Låt A vara en ordnad mängd och $B \subseteq A$. Om det finns ett element $y \in A$ sådant att

$$x \leqslant y \qquad \text{för alla } x \in B \tag{4.1}$$

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

Definition 4.1.2. Låt A vara en ordnad mängd, B en icke-tom 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 det för varje övre begränsning z till B gäller att $y \leqslant z$. Vi skriver

$$y = \sup_A B. \tag{4.2}$$

Anmärkning 4.1.3. 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 4.1.4. Låt B vara delmängden $\{p \in \mathbb{Q} \mid 0 < p < 1\}$ 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 4.1.5. En ordnad mängd A sägs ha *supremumegenskapen* om det för varje icke-tom, uppåt begränsad delmängd B av A finns ett $y \in A$ sådant att $y = \sup_A B$.

Vi har sett att $\sqrt{2}$ inte är ett rationellt tal och således motsvarar ett ”hål” i de rationella talen. Ett sätt att representera ett hål i $\mathbb{Q}$ *inom* $\mathbb{Q}$ är att skriva hålet som mängden α av alla rationella tal som ligger till vänster om hålet på tallinjen. I fallet $\sqrt{2}$ får vi då mängden: [7]

$$\alpha = \{p \in \mathbb{Q} \mid p < 0\} \cup \{p \in \mathbb{Q} \mid p^2 \leqslant 2\}.$$

[7] Vi har hittills inte definierat vad $\sqrt{2}$ är för något objekt, vilket är skälet till att vi inte skriver $\alpha = \{p \in \mathbb{Q} \mid p < \sqrt{2}\}$.

Det är klart α är icke-tom. Övning 4.3 visar att α även är uppåt begränsad i $\mathbb{Q}$, men följande exempel visar att α inte har ett supremum i $\mathbb{Q}$. Vi drar därför slutsatsen att $\mathbb{Q}$ *inte* har supremumegenskapen.

Exempel 4.1.6. Låt α vara som ovan. Antag att det finns en minsta övre begränsning $q \in \mathbb{Q}$ till α. Vi ska härleda en motsägelse till detta antagande genom att visa att inget av de tre fallen $q^2 < 2$, $q^2 = 2$ eller $2 < q^2$ kan gälla.

Till att börja med noterar vi att det måste gälla att $0 < q$: vi har ju till exempel att $1 \in \alpha$ och därmed gäller det att $0 < 1 \leqslant q$, eftersom q enligt antagande är en övre begränsning till α.

Eftersom vi redan visat att $\sqrt{2} \notin \mathbb{Q}$, så vet vi att det inte kan gälla att $q^2 = 2$.

Antag nu att $2 < q^2$ och låt

$$r = q - \frac{q^2 - 2}{q + 2} = \frac{2q + 2}{q + 2}. \tag{4.3}$$

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

$$r^2 - 2 = \frac{2(q^2 - 2)}{(q + 2)^2} > 0. \tag{4.4}$$

Detta betyder att $r^2 > 2$ och därmed gäller det, per definition av α, att varje $p \in \alpha$ uppfyller minst en av olikheterna $p < 0$ eller $p^2 \leqslant 2 < r^2$. Eftersom $q > 0$ ger den sista likheten i (4.3) att $r > 0$, vilket medför att $r > p$ för alla $p \in \alpha$ så att $p < 0$. Dessutom, för alla $p \in \alpha$ så att $p \geqslant 0$ måste det enligt ovan gälla att $p^2 < r^2$ och eftersom $r > 0$ innebär detta enligt Övning 4.2 att $p < r$. Således gäller det att $p < r$ för alla $p \in \alpha$. Vi har alltså konstruerat en övre begränsning r till α som är mindre än q, som vi antog vara den minsta övre begränsningen. Detta visar att det inte kan gälla att $2 < q^2$.

Antag nu istället att $q^2 < 2$ och låt r vara som ovan. Denna gång får vi att $q < r$ och $r^2 - 2 < 0$, vilket betyder att $r \in \alpha$. Men detta innebär att q inte är en övre begränsning till α. Därmed kan det inte gälla att $q^2 < 2$.

Vi har nu visat att $q = \sup_{\mathbb{Q}} \alpha$ medför att inget av de tre fallen $q^2 < 2$, $q^2 = 2$ eller $2 < q^2$ kan gälla. Eftersom något av dessa fall måste gälla, så måste antagandet att q var supremum till mängden α vara falskt. ▲

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).

4.2 Dedikindsnitt

Idén bakom Dedikindsnitt[8] är att identifiera varje reellt tal α med mängden av alla rationella tal som ligger till vänster om α på tallinjen. Eftersom vi hittills inte definierat vad ett reellt tal är för något, måste vi hitta ett sätt att beskriva snitt enbart med hjälp av av delmängder av $\mathbb{Q}$. Följande definition visar sig åstadkomma just detta.

Definition 4.2.1. Ett *snitt* α 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 4.2.2. 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 4.2.3. Låt $p \in \mathbb{Q}$ och låt $\alpha_p = \{q \in \mathbb{Q} \mid q < p\}$. Då är α_p ett snitt. För att visa detta måste vi kontrollera att mängden uppfyller de tre kraven (R1)-(R3) ovan.

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

(R2) Låt $p' \in \alpha_p$, $q \in \mathbb{Q}$ och $q < p'$. Då gäller det att $q < p' < p$, så $q \in \alpha_p$.

(R3) Tag $p' \in \alpha_p$ och sätt $r = \frac{p+p'}{2}$. Övning 3.13 ger att $p' < r < p$ och alltså gäller det att $r \in \alpha_p$ och $p' < r$.

▲

Definition 4.2.4. Ett *reellt tal* är ett snitt. Mängden av alla reella tal betecknas med $\mathbb{R}$.

Som vi nämnt ovan vill vi 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 4.2.3.

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

[8] För enkelhetens skull kommer vi i fortsättningen använda ordet "snitt" istället för "Dedikindsnitt".

Till exempel har vi de viktiga snitten

$$\alpha_1 = \{q \in \mathbb{Q} \mid q < 1\} \tag{4.5}$$
$$\alpha_0 = \{q \in \mathbb{Q} \mid q < 0\} \tag{4.6}$$

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

Läsaren uppmanas att tänka 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 $\mathbb{R}$.

4.3 Ordning och aritmetik på snitt

I enlighet med lydelsen av Sats 4.0.9 vill vi 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 mängden av alla snitt.

Definition 4.3.1 (Ordning)**.** Vi skriver att $\alpha < \beta$ om $\alpha \subseteq \beta$ och $\alpha \neq \beta$.

Hjälpsats 4.3.2. *Relationen $<$ definierad ovan är en ordning på $\mathbb{R}$.*

Bevis. Vi behöver verifiera de två egenskaperna i Definition 2.3.12. Den första egenskapen säger att för $\alpha, \beta \in \mathbb{R}$, så gäller en och endast en av egenskaperna $\alpha < \beta, \alpha = \beta$ eller $\beta < \alpha$. Vi delar upp beviset av detta i två delar: först bevisar vi att *åtminstone* en av $\alpha < \beta, \alpha = \beta$ eller $\beta < \alpha$ gäller och sedan bevisar vi att *maximalt* en av dessa egenskaper gäller samtidigt.

Vår strategi för att visa att åtminstone en av $\alpha < \beta, \alpha = \beta$ eller $\beta < \alpha$ gäller är att anta att $\alpha \not< \beta$, och visa att det medför att $\beta < \alpha$ eller $\alpha = \beta$. Så vi antar nu därför att $\alpha \not< \beta$. Då gäller det antingen att $\alpha \not\subseteq \beta$ eller att $\alpha = \beta$. Om det senare fallet gäller är vi klara, så vi antar att $\alpha \not\subseteq \beta$. Detta innebär att det finns ett $p \in \alpha$ så att $p \notin \beta$. Låt nu q vara ett godtyckligt element i β. Då måste $q < p$, ty om $p < q$ så måste $p \in \beta$, enligt egenskap (R2) i definitionen av snitt. Men eftersom $p \in \alpha$ måste det, återigen enligt egenskap (R2), gälla att $q \in \alpha$. Det följer att $\beta \subseteq \alpha$, och eftersom $\alpha \not\subseteq \beta$ kan det inte kan gälla att $\alpha = \beta$. Detta ger per definition att $\beta < \alpha$.

Vi ska nu visa att maximalt en av egenskaperna $\alpha < \beta, \alpha = \beta$ eller $\beta < \alpha$ kan vara uppfylld samtidigt. 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 $\alpha = \beta$. Därmed gäller det varken att $\alpha = \beta$ eller $\beta < \alpha$. 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 snitt som motsvarar rationella tal. Låt $p, q \in \mathbb{Q}$ sådana att $p, q > 0$. För att addition av snitt ska vara kompatibel med addition av rationella tal, så måste vi sätta

$$\alpha_p + \alpha_q = \{r \in \mathbb{Q} \mid r < p + q\} \tag{4.7}$$
$$\alpha_p \cdot \alpha_q = \{r \in \mathbb{Q} \mid r < pq\}. \tag{4.8}$$

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

Definition 4.3.3 (Addition)**.** Låt α och β vara två snitt. Vi definierar summan $\alpha + \beta$ som

$$\alpha + \beta = \{p + q \mid p \in \alpha, q \in \beta\}. \tag{4.9}$$

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

$$-\alpha = \{q \in \mathbb{Q} \mid -q - r \notin \alpha \text{ för något } r \in \mathbb{Q} \text{ där } r > 0\}. \tag{4.10}$$

Anmärkning 4.3.4. 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.

Hjälpsats 4.3.5. $\mathbb{R}$ *uppfyller axiomen (A1)–(A5), samt egenskapen (O1) i Definition 3.5.2.*

Bevis. Vi bevisar här att $\mathbb{R}$ uppfyller (A2) och (A3). Beviset för att $\mathbb{R}$ uppfyller (A1) är lämnat till läsaren i Övning 4.10 och de övriga bevisen finns i Appendix F.

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

$$\alpha + \beta = \{p + q \mid p \in \alpha, q \in \beta\} = \{q + p \mid p \in \alpha, q \in \beta\} = \beta + \alpha, \tag{4.11}$$

där vi använder kommutativiteten för addition av rationella tal p och q.

(A3) Associativiteten, det vill säga att $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$, följer på samma sätt

$$\begin{aligned}(\alpha + \beta) + \gamma &= \{p + q \mid p \in \alpha + \beta, q \in \gamma\} \\ &= \{(r + s) + q \mid r \in \alpha, s \in \beta, q \in \gamma\} \\ &= \{r + (s + q) \mid r \in \alpha, s \in \beta, q \in \gamma\} \\ &= \{r + p \mid r \in \alpha, p \in \beta + \gamma\} \\ &= \alpha + (\beta + \gamma).\end{aligned} \tag{4.12}$$

där vi använder att associativiteten för addition av rationella tal p, q och r.

□

Att definiera multiplikation av snitt är mer komplicerat än att definiera addition. Den intuitiva bilden skall dock vara klar; vi uppmanar läsaren att göra en tillbakablick till ekvation (4.8).

Definition 4.3.6 (Multiplikation)**.** Låt α och β vara två snitt sådana att $\alpha > 0$ och $\beta > 0$. Vi definierar produkten $\alpha \cdot \beta$ som

$$\alpha \cdot \beta = \{q \in \mathbb{Q} \mid q \leqslant rs \text{ för några } r \in \alpha, s \in \beta \text{ där } r > 0, s > 0\}. \tag{4.13}$$

Vi lämnar till läsaren, i Övning 4.9, att visa att $\alpha \cdot \beta$ är ett snitt. Låt nu α och β vara två godtyckliga snitt. Då definierar vi, med hjälp av (4.13), $\alpha \cdot \beta$ som

$$\alpha \cdot \beta = \begin{cases} (-\alpha) \cdot (-\beta) & \text{om } \alpha < 0, \beta < 0 \\ -\big((-\alpha) \cdot \beta\big) & \text{om } \alpha < 0, \beta > 0 \\ -\big(\alpha \cdot (-\beta)\big) & \text{om } \alpha > 0, \beta < 0 \\ 0 & \text{om } \alpha = 0 \text{ eller } \beta = 0. \end{cases} \tag{4.14}$$

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

$$\alpha^{-1} = \{0 < q \in \mathbb{Q} \mid q^{-1} - r \notin \alpha \text{ för något } r > 0\} \cup \{q \in \mathbb{Q} \mid q \leqslant 0\}. \tag{4.15}$$

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

Anmärkning 4.3.7. Lägg märke till att vi i högerledet av ekvation (4.14) bara multiplicerar snitt γ sådana att $\gamma > 0$ eftersom Hjälpsats 3.5.3 visar att $0 < -\gamma$ om $\gamma < 0$. Notera att beviset av Hjälpsats 3.5.3 endast använder sig av egenskaperna (O1), (A4) och (A5).

Hjälpsats 4.3.8. *De reella talen uppfyller axiom (O2) i Definition 3.5.2, det vill säga 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 γ, sådant att $\gamma \leqslant 0$, ej kan innehålla några positiva rationella tal. □

Hjälpsats 4.3.9. $\mathbb{R}$ *uppfyller axiomen (M1)–(M5) och (D).*

Bevis. Att $\mathbb{R}$ är sluten under multiplikation följer från Övning 4.9. (M2)–(M4) visas på samma sätt som i motsvarande fall för addition och lämnas också som en övning. (M5) och (D) bevisas i Appendix F. □

Hjälpsatserna i detta avsnitt visar tillsammans att $\mathbb{R}$ är en ordnad kropp. Detta innebär att alla vanliga räkneregler för addition, multiplikation och olikheter gäller för $\mathbb{R}$. Exempelvis kan vi använda alla räkneregler från Definition 3.4.1, Definition 3.5.1, Definition 3.5.2 och Hjälpsatserna 3.5.3 - 3.5.6 när vi räknar med reella tal.

Vi ska nu bevisa att $\mathbb{R}$ har supremumegenskapen.

Hjälpsats 4.3.10. *De reella talen har supremumegenskapen, det vill säga 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

$$\gamma = \bigcup_{\alpha \in A} \alpha. \tag{4.16}$$

Med denna beteckning menar vi att γ är unionen av alla mängder i A. Alltså består γ av alla rationella tal i alla snitt som är element i A. Vad vi vill visa är att γ är den minsta övre begränsningen till A, det vill säga $\gamma = \sup_{\mathbb{R}} A$. Först och främst måste vi försäkra oss om att γ är ett snitt. Detta är lämnat till läsaren i Övning 4.11.

Eftersom γ är unionen av alla $\alpha \in A$ så är det klart att $\alpha \leqslant \gamma$ för alla $\alpha \in A$. Detta visar att γ 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 γ 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 δ ej kan vara en övre begränsning till A. Detta visar att γ är den minsta övre begränsningen till A. □

Vi är nu nästan klara med beviset av Sats 4.0.9. Det kvarstår endast att visa att de rationella talen är en ordnad delkropp av de reella talen. Med andra ord ska vi visa att vår identifiering av $p \in \mathbb{Q}$ med snitt på formen $\alpha_p = \{q \in \mathbb{Q} \mid q < p\}$ ger en addition och multiplikation som är kompatibel med den vanliga additionen av rationella tal som gavs i Definition 2.5.1, samt att ordningsrelationen på $\mathbb{Q}$ (se Definition 3.5.7) bevaras.

Hjälpsats 4.3.11. *Vi har tidigare identifierat $\mathbb{Q}$ med en delmängd av $\mathbb{R}$ genom att till varje $p \in \mathbb{Q}$ tillordna snittet $\alpha_p = \{q \in \mathbb{Q} \mid q < p\}$. Följande gäller för alla $p, r \in \mathbb{Q}$:*

(i) $p \neq r$ *medför att* $\alpha_p \neq \alpha_r$

(ii) $\alpha_p + \alpha_r = \alpha_{p+r}$

(iii) $\alpha_r \cdot \alpha_p = \alpha_{p \cdot r}$

(iv) $p < r$ *medför att* $\alpha_p < \alpha_r$

Bevis. Vi bevisar ekvation (ii) här och ger de övriga bevisen i Appendix F.

Tag $q \in \alpha_p + \alpha_r$. Då finns det rationella tal p' och r' sådana att $p' < p$, $r' < r$ och $q = p' + r' < p + r$, vilket medför att $q \in \alpha_{p+r}$. Tag nu $q \in \alpha_{p+r}$. Då gäller det att $q < p + r$. Låt nu $s = \frac{q-p-r}{2}$. Vi noterar nu att $s < 0$, vilket medför att $(p + s) < p$ och $(r + s) < r$. Slutligen noterar vi att $q = (p + s) + (r + s)$ och således har vi att $q \in \alpha_p + \alpha_r$. Vi har bevisat inklusionerna $\alpha_p + \alpha_r \subseteq \alpha_{p+r}$ och $\alpha_{p+r} \subseteq \alpha_p + \alpha_r$. Därmed följer ekvation (ii). □

Övningar

Övning 4.1 ($\star$)**.** Visa att $\alpha_0 < \alpha_1$.

Övning 4.2 ($\star\star$)**.** Låt x och y vara element i en ordnad kropp sådana att $0 < x < y$. Visa att $x^2 < y^2$.
Ledning: Använd resultatet från Övning 3.11.

Övning 4.3 ($\star\star$)**.** Visa att mängden $\alpha = \{p \in \mathbb{Q} \mid p < 0\} \cup \{p \in \mathbb{Q} \mid p^2 \leqslant 2\}$ är uppåt begränsad i $\mathbb{Q}$.
Ledning: Resultatet från Övning 4.2 kan vara användbart.

Övning 4.4 ($\star$)**.** Visa att $\sup_{\mathbb{R}}[0,1] = 1$, där

$$[0,1] = \{x \in \mathbb{R} \mid 0 \leq x \leq 1\}.$$

Övning 4.5 ($\star\star$)**.** Visa att $\sup_{\mathbb{R}}(0,1) = 1$, där

$$(0,1) = \{x \in \mathbb{R} \mid 0 < x < 1\}.$$

Övning 4.6 ($\star\star$)**.** Visa att det för varje rationellt tal q finns ett naturligt tal n sådant att $q < n$.

Övning 4.7 ($\star\star$)**.** Låt $e_n = 1 - 1/n$ för $n = 1, 2, \ldots$ och sätt

$$E = \{e_1, e_2, e_3, \ldots\}. \tag{4.17}$$

Visa att $\sup_{\mathbb{Q}} E = 1$.
Ledning: Använd Övning 4.6.

Övning 4.8 ($\star\star$)**.** Låt $e_n = 1/n$ för $n = 1, 2, \ldots$ och sätt

$$E = \{e_1, e_2, e_3, \ldots\}. \tag{4.18}$$

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 $\inf_{\mathbb{Q}} E = 0$.
Ledning: Använd Övning 4.6.

Övning 4.9 ($\star\star\star$)**.** Låt $\alpha > 0$ och $\beta > 0$ vara två snitt. Visa att $\alpha \cdot \beta$ är ett snitt.

Övning 4.10 ($\star\star$)**.** Låt α och β vara två snitt. Visa att $\alpha + \beta$ är ett snitt.

Övning 4.11 ($\star\star\star$)**.** Låt A vara en delmängd av $\mathbb{R}$ sådan att $A \neq \emptyset$ och A är uppåt begränsad. Definiera γ som

$$\gamma = \bigcup_{\alpha \in A} \alpha. \tag{4.19}$$

Visa att γ är ett snitt.

Övning 4.12 ($\star\star\star$)**.** Sätt

$$\alpha = \{q \in \mathbb{Q} \mid q > 0 \text{ och } q^2 < 2\} \cup \{q \in \mathbb{Q} \mid q \leqslant 0\}. \tag{4.20}$$

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

Övning 4.13 ($\star\star\star$)**.** Låt X vara en icke-tom uppåt begränsad delmängd av $\mathbb{R}$ och låt $\alpha \in \mathbb{R}$. Låt $\alpha + X = \{\alpha + x \mid x \in X\}$. Visa att $\alpha + X$ är icke-tom och uppåt begränsad och att $\sup(\alpha + X) = \alpha + \sup X$.

Övning 4.14 ($\star\star\star$)**.** Låt c vara ett positivt reellt tal och låt X vara en icke-tom uppåt begränsad delmängd av $\mathbb{R}$. Definiera mängden $c \cdot X$ genom

$$c \cdot X = \{c \cdot x \mid x \in X\}.$$

Visa att $c \cdot X$ är icke-tom och uppåt begränsad och att

$$\sup_{\mathbb{R}}(c \cdot X) = c \cdot \sup_{\mathbb{R}} X.$$

Ledning: Övning 3.11 kan vara till hjälp.

5 Decimalutvecklingar

I kapitel 4 konstruerade vi de reella talen som Dedikindsnitt. Precis som att vi inte tänker på heltal eller rationella tal som ekvivalensklasser, så kommer vi från och med detta kapitel inte längre att tänka på reella tal som snitt, utan helt enkelt som element i den väsentligen unika (se Sats 4.0.10) ordnade kroppen med supremumegenskapen. Vi kommer ägna kapitlet åt att definiera och undersöka ett välbekant sätt att representera reella tal, nämligen decimalutvecklingar. De ger oss ett sätt att skriva reella tal, på samma sätt som kvotuttrycken $\frac{a}{b}$ gav oss ett sätt att skriva rationella tal. Att använda sig av decimaltal är ofta praktiskt, det är exempelvis enkelt att jämföra storleken på olika tal när de är skrivna som decimalutvecklingar. Men vad menar vi egentligen med ett uttryck som $0,333\ldots$, och varför är det lika med $\frac{1}{3}$? Kan alla reella tal skrivas som ett unikt decimaltal? Dessa frågor kommer att besvaras i detta kapitel. Vi inleder dock med ett avsnitt om den Arkimediska egenskapen.

5.1 Den Arkimediska egenskapen

Genom att utnyttja supremumegenskapen ska vi nu visa att $\mathbb{R}$ har en (intuitivt uppenbar) egenskap som kallas för den Arkimediska egenskapen. Denna egenskap kommer att behövas senare i kapitlet då vi studerar decimalutvecklingar.

Sats 5.1.1. *För varje $\alpha \in \mathbb{R}$ finns det ett naturligt tal n sådant att $\alpha < n$.*

Bevis. Vi använder oss av ett motsägelsebevis. Antag att det finns ett $\alpha \in \mathbb{R}$ sådant att $n \leqslant \alpha$ för alla $n \in \mathbb{N}$. Det skulle innebära att $\mathbb{N}$ är en icke-tom och uppåt begränsad delmängd av $\mathbb{R}$. Supremumegenskapen ger därmed att det finns ett $\beta \in \mathbb{R}$ sådant att $\beta = \sup_{\mathbb{R}} \mathbb{N}$. Vi ska nu visa att detta leder till en motsägelse. Eftersom β är en övre begränsning till $\mathbb{N}$ har vi för varje $n \in \mathbb{N}$ att $(n+1) \leqslant \beta$, vilket medför att $n \leqslant (\beta - 1)$. Detta innebär att även $\beta - 1$ är en övre begränsning till $\mathbb{N}$, men det strider mot att β är den minsta övre begränsningen till $\mathbb{N}$. □

Den Arkimediska egenskapen kan i ord uttryckas som att det inte finns reella tal som är "oändligt stora". Följdsatsen nedan visar att det inte heller finns positiva reella tal som är "oändligt nära noll".

Följdsats 5.1.2. *För varje positivt reellt tal α finns det ett naturligt tal n sådant att $\frac{1}{n} < \alpha$.*

Bevis. Tag $\alpha > 0$. Sats 5.1.1 medför att det finns ett $n \in \mathbb{N}$ sådant att

$$\frac{1}{\alpha} < n. \tag{5.1}$$

Vi noterar nu att $\frac{\alpha}{n} > 0$. Därmed gäller det att

$$\frac{1}{n} = \frac{\alpha}{n} \cdot \frac{1}{\alpha} < \frac{\alpha}{n} \cdot n = \alpha \tag{5.2}$$

□

Vi ska nu bevisa att det mellan två olika reella tal alltid finns ett rationellt tal.

Sats 5.1.3. *Låt α och β vara reella tal sådana att $\alpha < \beta$. Då finns det ett rationellt tal q sådant att*

$$\alpha < q < \beta.$$

Bevis. Vi delar upp beviset i tre fall:

$$\text{(i)}\ \ 0 \leqslant \alpha < \beta$$

$$\text{(ii)}\ \ \alpha < 0 < \beta$$

$$\text{(iii)}\ \ \alpha < \beta \leqslant 0$$

Antag först att (i) gäller. Eftersom $\alpha < \beta$ så har vi att $\beta - \alpha > 0$. Följdsats 5.1.2 förser oss därför med ett naturligt tal n sådant att

$$\frac{1}{n} < \beta - \alpha. \tag{5.3}$$

Betrakta mängden

$$A = \left\{ k \in \mathbb{N} \;\middle|\; \frac{k}{n} < \beta \right\}.$$

Notera att A är icke-tom eftersom den till exempel innehåller det naturliga talet 0. Dessutom är A uppåt begränsad av till exempel $n \cdot \beta$. Därmed kan vi definiera ett naturligt tal m genom

$$m = \max A.$$

Vi påstår nu att

$$\alpha < \frac{m}{n} < \beta.$$

Eftersom m tillhör A har vi att $\frac{m}{n} < \beta$ och det kvarstår därför endast att visa att $\alpha < \frac{m}{n}$. Antag att detta inte gäller, det vill säga antag att $\frac{m}{n} \leqslant \alpha$. Då har vi att

$$\frac{m+1}{n} = \frac{m}{n} + \frac{1}{n} < \alpha + (\beta - \alpha) = \beta.$$

Detta innebär att $m + 1 \in A$, vilket strider mot att m är det maximala elementet i A. Vårt antagande att $\frac{m}{n} \leqslant \alpha$ måste därför vara falskt och vi kan sluta oss till att $\alpha < \frac{m}{n} < \beta$. Beviset av satsen för fallen (ii) och (iii) lämnas till läsaren i Övning 5.3.

□

5.2 Definition av decimalutvecklingar

Decimaltalen använder sig av ett positionssystem byggt på heltalet 10. Om a_0 är ett icke-negativt heltal och $a_1, a_2, \dots$ är heltal mellan noll och nio, så är $a_0{,}a_1a_2a_3\dots$ intuitivt lika med följande "oändliga summa" av rationella tal[9]

$$a_0 + \frac{a_1}{10} + \frac{a_2}{100} + \frac{a_3}{1000} + \cdots \tag{5.4}$$

Notera att detta inte duger som en strikt matematisk definition - vi har ju inte definierat vad vi menar med en oändlig summa. Vi ska ge ge en strikt definition av decimaltal nedan, men innan dess behöver vi följande Hjälpsats.

Hjälpsats 5.2.1. *Låt $a_0, a_1, a_2, \dots$ vara heltal sådana att $a_0 \geqslant 0$ och $0 \leqslant a_k \leqslant 9$ för $k = 1, 2, \dots$. Följande mängd är uppåt begränsad*

$$\left\{ a_0 + \frac{a_1}{10} + \cdots + \frac{a_k}{10^k} \;\middle|\; k = 0, 1, 2, \dots \right\}. \tag{5.5}$$

Bevis. Vi kommer att använda oss av formeln för geometriska summa, se appendix E.

Låt C vara ett reellt tal sådant att $a_0 \leqslant C$ och $9 \leqslant C$. Då har vi att

$$\begin{aligned} a_0 + \frac{a_1}{10} + \cdots + \frac{a_k}{10^k} &\leqslant C \cdot \left(1 + \frac{1}{10} + \cdots + \frac{1}{10^k}\right) \\ &= C \cdot \frac{1 - \frac{1}{10^{k+1}}}{1 - \frac{1}{10}} \\ &\leqslant C \cdot \frac{1}{1 - \frac{1}{10}} \\ &= C \cdot \frac{10}{9} \end{aligned}$$

Således har vi att $a_0 + \frac{a_1}{10} + \cdots + \frac{a_k}{10^k} \leqslant C\frac{10}{9}$, oberoende av vad k är, och därmed är mängden (5.5) uppåt begränsad. □

Nu är vi redo att definiera decimaltalsutecklingar.

Definition 5.2.2. Låt $a_0, a_1, a_2, \dots$ vara heltal sådana att $0 \leqslant a_0$ och $0 \leqslant a_k \leqslant 9$ för $k = 1, 2, \dots$ och låt α vara ett reellt tal. Vi säger att $a_0, a_1, a_2, \dots$ är en *decimalutveckling* för α och skriver

$$\alpha = a_0{,}a_1a_2\dots \tag{5.6}$$

om det gäller att

$$\alpha = \sup_{\mathbb{R}} \left\{ a_0 + \frac{a_1}{10} + \cdots + \frac{a_k}{10^k} \;\middle|\; k = 0, 1, 2, \dots \right\}. \tag{5.7}$$

[9] För enkelhetens skull kommer vi i detta kompendium samla ihop alla siffror till vänster om kommatecknet i ett enda heltal a_0, som därmed tillåts vara större än nio.

Notera att mängden i högerledet ovan är en icke-tom mängd av rationella tal eftersom varje element är en ändlig summa av rationella tal. Då mängden är och uppåt begränsad enligt Hjälpsats 5.2.1, så existerar supremum av mängden enligt Hjälpsats 4.3.10. Alltså är högerledet i (5.7) ett reellt tal.

Exempel 5.2.3. Om endast ett ändligt antal av decimalerna a_k är nollskilda så blir resultatet förstås ett rationellt tal. Till exempel har vi att:

$$0.125 = \sup_{\mathbb{R}} \left\{ 0, \frac{1}{10}, \frac{12}{100}, \frac{125}{1000} \right\} = \frac{125}{1000}. \tag{5.8}$$

Här är alltså $a_k = 0$ för $k \geqslant 4$. ▲

Omvänt så kan vi för varje givet reellt tal α ge en konstruktion av heltal a_0,$a_1, a_2, \ldots$ sådana att a_0,$a_1 a_2 \cdots = \alpha$. För $\alpha > 0$ låt a_0 vara det största heltalet sådant att $a_0 \leqslant \alpha$. Att ett sådant heltal a_0 finns följer från att $\mathbb{R}$ har den Arkimediska egenskapen. Låt sedan a_1 vara det största heltalet sådant att $a_0 + \frac{a_1}{10} \leqslant \alpha$. Generellt låter vi a_k, för $k = 0, 1, 2, \ldots$, vara det största heltalet sådant att

$$a_0 + \frac{a_1}{10} + \cdots + \frac{a_{k-1}}{10^{k-1}} + \frac{a_k}{10^k} \leqslant \alpha. \tag{5.9}$$

Hjälpsats 5.2.4. *Låt $a_0, a_1, a_2, \ldots$ vara konstruerade från det reella talet α, som ovan. Då är $0 \leqslant a_0$, $0 \leqslant a_k \leqslant 9$ för $k \geqslant 1$ och a_0,$a_1 a_2 \cdots = \alpha$.*

Bevis. Vi börjar med att visa att

$$a_0 \geqslant 0, \quad 0 \leqslant a_k \leqslant 9 \text{ för } k \geqslant 1.$$

Att $a_0 \geqslant 0$ är klart från definitionen av a_0, eftersom $\alpha > 0$. Låt nu $k \geqslant 1$. Per definition av $a_0, a_1 \ldots, a_{k-1}$ gäller det då att

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

Därmed är det givetvis även sant att

$$a_0 + \frac{a_1}{10} + \cdots + \frac{a_{k-1}}{10^{k-1}} + \frac{0}{10^k} \leqslant \alpha,$$

vilket visar att $a_k \geqslant 0$. För att visa att $a_k \leqslant 9$ för $k \geqslant 1$ använder vi oss av ett motsägelsebevis. Vi antar därför att det finns ett $k \geqslant 1$ sådant att $a_k \geqslant 10$. Då följer det att

$$\begin{aligned} a_0 + \frac{a_1}{10} + \cdots + \frac{a_{k-1}+1}{10^{k-1}} &= a_0 + \frac{a_1}{10} + \cdots + \frac{a_{k-1}}{10^{k-1}} + \frac{10}{10^k} \\ &\leqslant a_0 + \frac{a_1}{10} + \cdots + \frac{a_{k-1}}{10^{k-1}} + \frac{a_k}{10^k} \\ &\leqslant \alpha \end{aligned}$$

Detta strider mot att a_{k-1} är det minsta heltalet sådant att

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

Därmed måste antagandet att $a_k \geqslant 10$ vara falskt.

Vi visar nu att

$$a_0{,}a_1a_2\cdots = \alpha.$$

Låt oss definiera talen e_k genom

$$e_k = a_0 + \frac{a_1}{10} + \cdots + \frac{a_k}{10^k} \tag{5.10}$$

för $k = 0, 1, 2, \ldots$, och låt mängden E vara given som

$$E = \{e_0, e_1, e_2, \ldots\}. \tag{5.11}$$

Vi vill visa att α är den minsta övre begränsningen till mängden E. Att α är en övre begränsning till E är klart från definitionen av talen a_k, så det kvarstår endast att visa att α är den minsta övre begränsningen. Vi måste därför visa att om $\beta < \alpha$, så är β inte en övre begränsning till E. Tag $\beta < \alpha$ och låt $\gamma = \alpha - \beta$. Då är $\gamma > 0$, eftersom $\beta < \alpha$. Tag nu ett heltal N sådant att $10^{-N} < \gamma$. Att det finns ett sådant heltal N är en konsekvens av Följdsats 5.1.2. I Övning 5.1 ombeds läsaren att visa att konstruktionen av a_k medför att

$$\alpha - e_k < \frac{1}{10^k}. \tag{5.12}$$

Från olikheten (5.12) får vi att

$$\beta = \alpha - \gamma < \alpha - \frac{1}{10^N} < e_N. \tag{5.13}$$

Alltså kan inte β vara en övre begränsning till E. Detta visar att α är den minsta övre begränsningen, det vill säga supremum, till E. □

5.3 Två grundläggande egenskaper hos decimalutvecklingar

Hjälpsatsen nedan visar att ”man kan plocka ut en ändlig delsumma från ett decimaltal”.

Hjälpsats 5.3.1.

$$a_0{,}a_1a_2\cdots = a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_n}{10^n} + \underbrace{0{,}00\ldots0}_{n+1\ 0:or}a_{n+1}a_{n+2}\ldots \tag{5.14}$$

Bevis. Låt $e_0, e_1, e_2, \ldots$ vara som ovan. Vi har per definition att

$$a_0{,}a_1a_2\cdots = \sup_{\mathbb{R}}\{e_0, e_1, e_2, \ldots\}.$$

Övning 5.2 visar att vi även har att

$$a_0{,}a_1a_2\cdots = \sup_{\mathbb{R}}\{e_{n+1}, e_{n+2}, e_{n+3}, \ldots\}.$$

För alla $j \geqslant n+1$ gäller det att

$$e_j = e_n + \frac{a_{n+1}}{10^{n+1}} + \frac{a_{n+2}}{10^{n+2}} + \cdots + \frac{a_j}{10^j}.$$

Vi kan därmed använda oss av resultatet från Övning 4.13 för att sluta oss till att

$$a_0,a_1a_2\ldots = e_n + \sup_{\mathbb{R}} \left\{ \frac{a_{n+1}}{10^{n+1}} + \cdots + \frac{a_j}{10^j} \;\middle|\; j \geqslant n+1 \right\} \tag{5.15}$$

$$= e_n + \sup_{\mathbb{R}} \left\{ 0 + \frac{0}{10} + \cdots + \frac{0}{10^n} + \frac{a_{n+1}}{10^{n+1}} + \cdots + \frac{a_j}{10^j} \;\middle|\; j \geqslant n+1 \right\} \tag{5.16}$$

$$= a_0 + \frac{a_1}{10} + \frac{a_2}{10^2} + \cdots + \frac{a_n}{10^n} + \underbrace{0{,}00\ldots0}_{n+1\ 0\text{:or}} a_{n+1}a_{n+2}\ldots \tag{5.17}$$

Därmed är beviset klart. □

Nästa Hjälpsats visar att den välkända räkneregeln att decimaltecknet flyttas vid multiplikation med heltalspotenser av tio är korrekt.

Hjälpsats 5.3.2. *För varje heltal $n \geqslant 0$ gäller det att*

$$10^n \cdot a_0,a_1a_2\cdots = c,a_{n+1}a_{n+2}\ldots, \tag{5.18}$$

där $c = 10^n \cdot a_0 + 10^{n-1} \cdot a_1 + \cdots + a_n$.

Bevis. Precis som i beviset av Hjälpsats 5.3.1, kommer vi även i detta bevis att använda oss av resultaten från Övning 5.2 och Övning 4.13. Dessutom kommer vi också behöva resultatet från Övning 4.14. Följande likheter gäller:

$$\begin{aligned}
10^n \cdot a_0,a_1a_2\ldots &= 10^n \cdot \sup_{\mathbb{R}}\{e_0, e_1, \ldots\} \\
&= 10^n \cdot \sup_{\mathbb{R}}\{e_n, e_{n+1}, \ldots\} \\
&= \sup_{\mathbb{R}}\{10^n e_n, 10^n e_{n+1}, \ldots\} \\
&= \sup_{\mathbb{R}}\left\{c, c + \frac{a_{n+1}}{10}, c + \frac{a_{n+1}}{10} + \frac{a_{n+2}}{10^2}, \ldots\right\} \\
&= c,a_{n+1}a_{n+2}\ldots
\end{aligned}$$

Därmed är beviset klart. □

5.4 Periodiska decimalutvecklingar

Definition 5.4.1. Ett reellt tal $\alpha > 0$ har *periodisk decimalutveckling* om det finns heltal $n \geqslant 1$, $k \geqslant 0$ och heltal $a_1, a_2, a_3, \ldots, a_n, b_0, b_1, b_2, \ldots, b_k$ så att

$$\alpha = b_0,b_1\ldots b_k a_1a_2\ldots a_n a_1a_2\ldots a_n\ldots \tag{5.19}$$

Sats 5.4.2. *Antag att $\alpha > 0$ har periodisk decimalutveckling. Då är α ett rationellt tal.*

Bevis. Antag att ekvation (5.19) är uppfylld. Låt oss införa beteckningarna

$$\begin{aligned} A &= 10^{n-1} \cdot a_1 + 10^{n-2} \cdot a_2 + \cdots + a_n \\ B &= 10^k \cdot b_0 + 10^{k-1} \cdot b_1 + \cdots + b_k \\ \beta &= 0{,}a_1 a_2 \ldots a_n a_1 a_2 \ldots a_n \ldots \end{aligned}$$

Hjälpsats 5.3.2 och Hjälpsats 5.3.1 ger tillsammans att

$$10^n \cdot \beta = A + \beta,$$

vilket vi även kan uttrycka som

$$\beta = \frac{A}{10^n - 1}. \tag{5.20}$$

Från detta uttryck för β är det klart att β är ett rationellt tal. Vidare har vi, återigen från Hjälpsats 5.3.2 och Hjälpsats 5.3.1, att

$$10^k \cdot \alpha = B + \beta.$$

Det följer därför att

$$\alpha = \frac{1}{10^k} \cdot (B + \beta), \tag{5.21}$$

vilket visar att även α är rationellt. □

Anmärkning 5.4.3. Man kan även visa att omvändningen till satsen ovan är sann, det vill säga att varje rationellt tal q har periodisk decimalutveckling.

Exempel 5.4.4. Beviset av Sats 5.4.2 visar hur vi kan skriva ett tal α med periodisk decimalutveckling på formen $\frac{n}{m}$, där n och m är heltal. Exempelvis gäller det att

$$\frac{1}{3} = 0{,}333\ldots$$

Ty, med beteckningar som i Sats 5.4.2 har vi:

$$\begin{aligned} n &= 1 \\ k &= 0 \\ a_1 &= 3 \\ b_0 &= 0 \\ \alpha = \beta &= 0{,}333\ldots \\ A &= a_1 = 3 \\ B &= b_0 = 0 \end{aligned}$$

och med ekvation (5.20) får vi:

$$\beta = \frac{A}{10^1 - 1} = \frac{3}{9} = \frac{1}{3}.$$

Därmed har vi visat att

$$\frac{1}{3} = 0{,}333\ldots$$

▲

5.5 Kan ett reellt tal ha flera decimalutvecklingar?

Vi har visat att vi till varje reellt tal kan konstruera ett decimaltal och för alla val av a_k så är $a_0{,}a_1a_2\ldots$ ett reellt tal. Man kan nu fråga sig om två olika decimalutvecklingar $a_0{,}a_1a_2\ldots$ och $b_0{,}b_1b_2\ldots$, det vill säga där det finns ett k sådant att $a_k \neq b_k$, kan representera samma reella tal? I detta avsnitt ska vi besvara denna fråga. Vi börjar med en definition som är relevant i detta sammanhang.

Definition 5.5.1. Låt $\alpha > 0$ vara ett reellt tal. En decimalutveckling $a_0, a_1, a_2\ldots$ för α innehåller *återkommande nior* om det finns något $k \geqslant 0$ sådant att $a_l = 9$ för alla $l > k$. Detta medför att

$$\alpha = a_0{,}a_1a_2\ldots a_k999\ldots. \tag{5.22}$$

Notera att om α har en decimalutveckling med återkommande nior, så har α en periodisk decimalutveckling (jämför ekvation (5.19)). Vi kan därför använda resultaten från föregående avsnitt i vår analys av decimalutvecklingar med återkommande nior.

Vi ska nu visa att om $b_k \leqslant 8$ så är

$$b_0{,}b_1b_2\ldots b_k999\cdots = b_0{,}b_1\ldots(b_k+1)000\ldots \tag{5.23}$$

Med beteckningar som i Sats 5.4.2 har vi

$$\begin{aligned}
\alpha &= b_0{,}b_1b_2\ldots b_k999\ldots\\
A &= a_n = a_1 = 9\\
B &= 10^k\cdot b_0 + 10^{k-1}\cdot b_1 + \cdots + a_k\\
\beta &= 0{,}a_1a_1a_1\cdots = 0{,}999\ldots
\end{aligned}$$

Från ekvation (5.20) och (5.21) får vi nu

$$\begin{aligned}
\alpha &= \frac{1}{10^k}\cdot(B+\beta)\\
&= \frac{1}{10^k}\cdot\left(10^k\cdot b_0 + 10^{k-1}\cdot b_1 + \cdots + b_k + \beta\right)\\
&= \frac{1}{10^k}\cdot\left(10^k\cdot b_0 + 10^{k-1}\cdot b_1 + \cdots + b_k + \frac{A}{10^n-1}\right)\\
&= \frac{1}{10^k}\cdot\left(10^k\cdot b_0 + 10^{k-1}\cdot b_1 + \cdots + b_k + \frac{9}{9}\right)\\
&= b_0 + \frac{b_1}{10} + \cdots + \frac{b_{k-1}}{10^{k-1}} + \frac{b_k+1}{10^k}\\
&= b_0{,}b_1\ldots(b_k+1)000\ldots
\end{aligned}$$

Exempel 5.5.2. Från ekvation (5.23) får vi till exempel följande likheter:

$$0{,}999\cdots = 1 \tag{5.24}$$

$$1{,}2999\cdots = 1{,}3 \tag{5.25}$$

▲

Att det finns flera olika decimaltal som representerar samma reella tal är inte så farligt då vi kan visa att fallet med återkommande nior är det enda exemplet. Innan vi visar detta ska vi bevisa ett starkare resultat, som visar hur ordningsrelationen på $\mathbb{R}$ kan uttryckas i termer av decimalutvecklingar.

Hjälpsats 5.5.3. *Låt $\alpha, \beta \in \mathbb{R}$ och låt $a_0{,}a_1a_2\ldots$ och $b_0{,}b_1b_2\ldots$ vara decimalutvecklingar utan återkommande nior för α respektive β. Antag att $a_j \neq b_j$ för något $j \in \mathbb{N}$ och låt k vara det minsta naturliga talet sådant att $a_k \neq b_k$. Då gäller det att $\alpha < \beta$ om och endast om $a_k < b_k$.*

Bevis. Antag att $a_k < b_k$. Eftersom $a_0, a_1, a_2\ldots$ inte innehåller återkommande nior kan vi välja $m > k \geqslant 0$ sådant att $a_m \neq 9$. Låt oss införa beteckningen

$$s = a_0 + \frac{a_1}{10} + \cdots + \frac{a_{k-1}}{10^{k-1}}.$$

Eftersom $a_j = b_j$ för alla $j \leqslant k$, så har vi enligt Hjälpsats 5.3.1 att

$$\beta = s + \frac{b_k}{10^k} + \underbrace{0{,}00\ldots0}_{k+1\ \text{0:or}} b_{k+1}b_{k+2}\ldots$$

Notera speciellt att detta medför att $s + \frac{b_k}{10^k} \leqslant \beta$.

Vi har nu följande kedja av likheter och olikheter:

$$\begin{aligned}
\alpha &= s + \frac{a_k}{10^k} + \frac{a_{k+1}}{10^{k+1}} + \cdots + \frac{a_m}{10^m} + \underbrace{0{,}00\ldots0}_{m+1\ \text{0:or}} a_{m+1}a_{m+2}\ldots \\
&\leqslant s + \frac{b_k - 1}{10^k} + \frac{9}{10^{k+1}} + \cdots + \frac{9-1}{10^m} + \underbrace{0{,}00\ldots0}_{m+1\ \text{0:or}} 999\ldots \\
&= s + \frac{b_k}{10^k} - \frac{1}{10^k} - \frac{1}{10^m} + \frac{9}{10^{k+1}} + \cdots + \frac{9}{10^m} + \underbrace{0{,}00\ldots0}_{m+1\ \text{0:or}} 999\ldots \\
&= s + \frac{b_k}{10^k} - \frac{1}{10^k} - \frac{1}{10^m} + \underbrace{0{,}00\ldots0}_{k+1\ \text{0:or}} 999\ldots \\
&= s + \frac{b_k}{10^k} - \frac{1}{10^k} - \frac{1}{10^m} + \frac{1}{10^k} \\
&\leqslant \beta - \frac{1}{10^m} \\
&< \beta
\end{aligned}$$

Vi har nu visat att $a_k < b_k$ medför att $\alpha < \beta$. Antag nu istället att $\alpha < \beta$. Beviset ovan visar då att vi inte kan ha att $b_k < a_k$. Eftersom $a_k \neq b_k$ måste det därför gälla att $a_k < b_k$ och beviset är därmed avslutat. □

Följdsats 5.5.4. *Låt $a_0, a_1, a_2\ldots$ och $b_0, b_1, b_2\ldots$ vara decimaltalsutvecklingar som ej innehåller återkommande nior. Antag att det existerar ett $k \geqslant 0$ sådant att $a_k \neq b_k$. Då är $a_0{,}a_1a_2\cdots \neq b_0{,}b_1b_2\ldots$.*

Bevis. Låt k vara det minsta naturliga talet sådant att $a_k \neq b_k$. Om $a_k < b_k$ har vi att $a_0{,}a_1a_2\cdots < b_0{,}b_1b_2\ldots$ och om $b_k < a_k$ har vi att $b_0{,}b_1b_2\cdots < a_0{,}a_1a_2\ldots$. I båda fallen gäller det att $a_0{,}a_1a_2\cdots \neq b_0{,}b_1b_2\ldots$. Eftersom någon av olikheterna $a_k < b_k$ eller $b_k < a_k$ måste vara uppfylld, så måste det vara så att $a_0{,}a_1a_2\cdots \neq b_0{,}b_1b_2\ldots$. □

Detta visar att om två decimalutvecklingar utan återkommande nior inte innehåller exakt samma siffror, så kan de inte representera samma reella tal.

5.6 Utvecklingar i andra baser

Som vi nämnt bygger decimaltal på ett positionssystem baserat på talet tio. Ett tal skrivet på decimalform sägs vara uttryckt i *basen* 10. I själva verket har vi även arbetat med denna bas när vi i detta kompendium skrivit heltal som till exempel ”100”. Strikt taget definieras detta uttryck genom $100 = 1 \cdot 10^2 + 0 \cdot 10^0 + 0 \cdot 10^0$ [10].

Det är dock inget speciellt med just talet 10; alla heltal $n > 1$ duger lika bra som bas. Faktum är att alla definitioner och satser från avsnitt 5.2 till 5.5 gäller även för andra baser än tio (vissa små modifikationer av formuleringarna och bevisen är nödvändiga.) Exempelvis har vi följande definition för utveckling av tal i bas två:

Definition 5.6.1. Låt $a_0{,}a_1, a_2, \ldots$ vara heltal sådana att $a \geqslant 0$ och $0 \leqslant a_k \leqslant 1$ för $k = 1, 2, \ldots$. Vi definierar uttrycket $[a_0{,}a_1a_2a_3\ldots]_2$ som[11]

$$[a_0{,}a_1a_2a_3\ldots]_2 = \sup_{\mathbb{R}} \left\{ a_0 + \frac{a_1}{2} + \cdots + \frac{a_k}{2^k} \;\middle|\; k = 0, 1, 2, \ldots \right\}$$

En utveckling av ett tal i bas två kallas för en *binär utveckling*.

Exempel 5.6.2. Precis som i fallet med decimaltal, så kommer en ändlig binär utveckling, det vill säga en binär utveckling där endast ett ändligt antal av talen a_k är nollskilda, att ge ett rationellt tal. Till exempel definieras $[0{,}1101]_2$ av

$$[0{,}1101]_2 = \sup_{\mathbb{R}} \{e_0, e_1, \ldots\},$$

där $e_k = a_0 + \frac{a_1}{2} + \cdots + \frac{a_k}{2^k}$. I detta exempel är $a_k = 0$ för $k \geqslant 5$ och därför gäller det att

$$\{e_0, e_1, \ldots\} = \{e_0, e_1, e_2, e_3, e_4\}.$$

[10] 100 definieras alltså *inte* av $100 = 99 + 1$, utan denna likhet kräver egentligen ett bevis.

[11] Som tidigare samlar vi alla siffror till vänster om kommatecknet i heltalet a_0, vilket är skälet till att vi tillåter att a_0 är större än ett.

Eftersom $e_j \leqslant e_4$ för $0 \leqslant j \leqslant 4$ får vi därför

$$\begin{aligned}
[0{,}1101]_2 &= \sup_{\mathbb{R}}\{e_0, e_1, \dots\} \\
&= \{e_0, e_1, e_2, e_3, e_4\} \\
&= e_4 \\
&= 0 + \frac{1}{2} + \frac{1}{4} + \frac{0}{8} + \frac{1}{16} \\
&= \frac{13}{16}.
\end{aligned}$$

▲

Övningar

Övning 5.1 ($\star\star\star$)**.** Bevisa olikheten (5.12).

Övning 5.2 ($\star\star\star$)**.** Låt $a_0, a_1, a_2, \dots$ vara heltal sådana att $a_0 \geqslant 0$ och $0 \leqslant a_k \leqslant 9$ för $k = 1, 2, \dots$. Som tidigare definierar vi en följd rationella tal e_k genom

$$e_k = a_0 + \frac{a_1}{10} + \cdots + \frac{a_k}{10^k}. \tag{5.26}$$

Låt $n \in \mathbb{N}$ och visa att

$$\sup_{\mathbb{R}}\{e_0, e_1, e_2, \dots\} = \sup_{\mathbb{R}}\{e_n, e_{n+1}, e_{n+2}, \dots\}. \tag{5.27}$$

Övning 5.3 ($\star\star\star$)**.** Slutför beviset av Sats 5.1.3.

Övning 5.4 ($\star\star$)**.** Använd metoden från Exempel 5.4.4 för att visa att

(a) $\frac{1}{6} = 0{,}166\dots$

(b) $\frac{1}{111} = 0{,}009009\dots$

Övning 5.5 ($\star$)**.** Låt $\alpha = [0{,}01101]_2$. Bestäm heltal n och m så att $\alpha = \frac{n}{m}$.

Övning 5.6 ($\star$)**.** Finn en binär utveckling av $\alpha = \frac{3}{4}$.

Övning 5.7 ($\star$)**.** Finn en binär utveckling av $\alpha = \frac{1}{2}$.

6 Egenskaper för de reella talen

Vi fortsätter vårt studium av de reella talen. Det viktigaste resultatet i kapitlet är att $\mathbb{R}$, till skillnad från $\mathbb{Q}$, ej är en uppräknelig mängd. Vi inleder dock med att visa att supremumegenskapen hos $\mathbb{R}$ ser till att vi fått med det tal vi saknade i $\mathbb{Q}$, det vill säga $\sqrt{2}$.

6.1 $\sqrt{2} \in \mathbb{R}$

Exempel 6.1.1. 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

$$A = \{x \in \mathbb{R} \mid x > 0 \text{ och } x^2 < 2\}. \tag{6.1}$$

Enligt Övning 6.2 är mängden A uppåt begränsad och icke-tom. Vi kan därför göra följande definition

$$y = \sup_{\mathbb{R}} A. \tag{6.2}$$

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

$$h < \frac{2 - y^2}{2y + 1}. \tag{6.3}$$

Då gäller det att

$$\begin{aligned}(y + h)^2 &= y^2 + h(2y + h) < y^2 + h(2y + 1) \\ &< y^2 + \frac{2 - y^2}{2y + 1}(2y + 1) = y^2 + 2 - y^2 = 2.\end{aligned} \tag{6.4}$$

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

$$k = \frac{y^2 - 2}{2y}. \tag{6.5}$$

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

$$\begin{aligned}(y - k)^2 &= y^2 + k^2 - 2yk > y^2 - 2yk = y^2 - 2y\frac{y^2 - 2}{2y} \\ &= y^2 - (y^2 - 2) = 2.\end{aligned} \tag{6.6}$$

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 $y^2 = 2$.

Vi har nu konstruerat ett reellt tal y med egenskapen att $y^2 = 2$. Det är klart från vår definition av y att $y > 0$.

Vi skulle nu vilja göra definitionen att $\sqrt{2}$ är lika med det positiva reella tal vars kvadrat är lika med två. För att denna definition ska vara meningsfull måste vi dock bevisa att det finns ett *unikt* positivt reellt tal vars kvadrat är lika med två. Att bevisa detta är lämnat åt läsaren i Övning 6.5.

▲

Anmärkning 6.1.2. Genom att generalisera argumentet i exemplet ovan kan man visa att $\sqrt[n]{x} \in \mathbb{R}$ för alla heltal $n > 0$ och reella tal $x > 0$.

6.2 Kardinaliteten av $\mathbb{R}$

Vi behandlar nu ett av de vid första anblicken mera förvånande resultaten i matematiken, nämligen att de reella talen inte är uppräkneliga (och således finns det olika stora oändligheter!). Detta bevisades först av den tyska matematikern Georg Cantor i 1874. Beviset vi presenterar kallas Cantors diagonalbevis[12]. Det publicerades 1891 och är en bevismetod som har använts i bevisen av flera berömda satser, exempelvis Gödel's ofullständighetssatser samt Turing's lösning till "avgörbarhetsproblemet".

Sats 6.2.1. *Mängden $\mathbb{R}$ av alla reella tal är överuppräknelig*[13].

Bevis. Från föregående avsnitt vet vi att vi från varje reellt tal x kan konstruera ett decimaltal sådant att

$$x = a_0{,}a_1a_2a_3\ldots. \tag{6.7}$$

Vi kan anta att $a_0, a_1, a_2 \ldots$ inte kommer att innehålla återkommande nior.

Vi ska nu konstruera ett motsägelsebevis; det vill säga 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

$$\mathbb{R} = \{x^{(0)}, x^{(1)}, x^{(2)}, x^{(3)}, \ldots\} \tag{6.8}$$

[12]Det första diagonalbeviset presenterades dock trots namnet år 1875 av Paul du Bois-Reymond.

[13]Se Definition 3.2.4.

där

$$\begin{aligned} x^{(0)} &= a_{00},a_{01}a_{02}a_{03}\dots \\ x^{(1)} &= a_{10},a_{11}a_{12}a_{13}\dots \\ x^{(2)} &= a_{20},a_{21}a_{22}a_{23}\dots \\ x^{(3)} &= a_{30},a_{31}a_{32}a_{33}\dots \\ &\vdots \end{aligned} \tag{6.9}$$

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

$$y = c_0,c_1c_2c_3\dots \tag{6.10}$$

där vi definierar c_k som

$$c_k = \begin{cases} 1 & \text{om } a_{kk} = 0 \\ 0 & \text{om } a_{kk} \in \{1,2,3,4,5,6,7,8,9\}. \end{cases} \tag{6.11}$$

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 (6.9) 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 således från antagandet att $\mathbb{R}$ kan räknas upp konstruerat ett reellt tal som ej finns med i uppräkningen. Detta är en motsägelse och antagandet att $\mathbb{R}$ är uppräknelig måste därför vara falskt. Således måste $\mathbb{R}$ vara överuppräknelig. □

Anmärkning 6.2.2. Genom att modifiera beviset ovan lite grann kan man även visa att det öppna enhetsintervallet

$$(0,1) = \{\gamma \in \mathbb{R} \mid 0 < \gamma < 1\}$$

är överuppräkneligt.

Anmärkning 6.2.3. Vi har sett i det föregående kapitlet att det mellan varje par av två olika reella tal finns ett rationellt tal. Detta kan måhända kännas motsägelsefullt givet Sats 3.2.9 och Sats 6.2.1. Det finns dock ingen logisk motsättning här. Vad denna skenbara motsägelse visar är istället att vi inte kan lita på vår intuition när vi resonerar kring oändligheten.

Sats 6.2.1 medför även att det finns ett irrationellt tal mellan varje par av olika reella tal:

Följdsats 6.2.4. *Låt α och β vara reella tal sådana att $\alpha < \beta$. Då finns det ett irrationellt tal γ sådant att*

$$\alpha < \gamma < \beta.$$

Bevis. Beviset är lämnat åt läsaren i Övning 6.7 □

6.3 Algebraiska tal

Definition 6.3.1. Ett *polynom* $p(x)$ i variabeln x är en summa på formen

$$p(x) = \sum_{k=0}^{n} a_k x^k = a_n x^n + a_n x^{n-1} + \cdots + a_1 x + a_0 \tag{6.12}$$

för något heltal $n \geqslant 0$ och $a_0, a_1, \ldots, a_k \in \mathbb{R}$. 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 6.3.2. Ett reellt tal y är *algebraiskt* om det existerar ett nollskilt heltalspolynom $p(x)$ sådant att

$$p(y) = a_n y^n + a_n y^{n-1} + \cdots + a_1 y + a_0 = 0. \tag{6.13}$$

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

Anmärkning 6.3.3. Vi noterar att alla rötter till ett polynom p med rationella koefficienter också är algebraiska, ty om $a_n = b_n/c_n, \ldots, a_0 = b_0/c_0$ är rationella, kan vi multiplicera polynomet med produkten $c = c_n c_{n-1} \ldots c_0$ och erhålla ett polynom $q(x) = cp(x)$ med heltalskoefficienter och samma rötter som p.

Exempel 6.3.4. Alla rationella tal är algebraiska. Tag ett rationellt tal $y = \frac{a}{b}$; då uppfyller y en ekvation av typen (6.13) där $n = 1$, $a_1 = b$ och $a_0 = -a$. Alltså

$$a_1 y + a_0 = b\frac{a}{b} - a = a - a = 0. \tag{6.14}$$

▲

Exempel 6.3.5. Talet $y = \sqrt{2}$ är algebraiskt. Tag $n = 2$, $a_2 = 1, a_1 = 0$ och $a_0 = -2$. Detta ger

$$a_2 y^2 + a_1 y + a_0 = \left(\sqrt{2}\right)^2 - 2 = 2 - 2 = 0. \tag{6.15}$$

▲

Anmärkning 6.3.6. 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 6.3.2 betyder att det finns *minst* ett sådant polynom.

Sats 6.3.7. *De algebraiska talen är uppräkneliga.*

Bevis. Enligt Algebrans fundamentalsats (Sats 7.1.7) så gäller det särskilt att ett polynom endast har 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; varje algebraiskt tal måste vara en rot till ett heltalspolynom och

en uppräknelig union av ändliga mängder är igen uppräknelig (se Övning 3.3). Vi ska därför nu visa att mängden av alla heltalspolynom är uppräknelig. Definiera *rangen* N av ett heltalspolynom som

$$N = n + |a_0| + |a_1| + \cdots + |a_n|. \tag{6.16}$$

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

$$p_{N,1}, p_{N,2}, \ldots, p_{N,k_N}. \tag{6.17}$$

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

$$p_{1,1}, \ldots, p_{1,k_1}, p_{2,1}, \ldots, p_{2,k_2}, \ldots \tag{6.18}$$

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

6.4 Transcendenta tal

Definition 6.4.1. 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 6.4.2. *Mängden av transcendenta tal är överuppräknelig.*

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 Övning 3.3. □

Anmärkning 6.4.3. Notera att detta betyder att de allra flesta reella tal är transcendenta. De flesta talen dyker alltså inte upp som lösningar till de ekvationer som vi oftast jobbar med.

Det är i allmänhet ganska svårt att hitta exempel på transcendenta tal, vilket känns tämligen olustigt då de flesta reella tal är transcendenta. Två exempel på transcendenta tal som läsaren kanske känner igen är talen π och e. Bevisen för att de verkligen är transcendenta är ganska svåra och utelämnas från detta kompendium.[14] Ett sätt att hitta ett transcendent tal är att med en slumptalsgenerator generera en oändlig decimalutveckling, ty det går att visa att det resulterande talet med sannolikhet exakt 1 måste vara transcendent. Nackdelen är att det kommer att ta oändlig lång tid, och fordrar att slumptalsgeneratorn är perfekt slumpmässig, vilket i praktiken är en icke-verifierbar egenskap.

[14] Beviset för att e är transcendent kan hittas i kompendiet till 2005 års matematiska cirkel som finns att hitta på kurshemsidan till den kursomgången.

6.5 Multiplikativa normer

Följande stycke ger en kort introduktion till normer på mängder med multiplikation och addition. De kommer att spela än större i kapitel 7 än i detta kapitel.

Ett exempel på en norm på $\mathbb{R}$ ges av absolutbeloppet:

Definition 6.5.1. Låt $x \in \mathbb{R}$. *Absolutbeloppet* $|x|$ av x definieras som

$$|x| = \begin{cases} x & \text{om } x \geq 0, \\ -x & \text{om } x < 0. \end{cases}$$

Från definitionen följer att $|x| \geq 0$ för alla $x \in \mathbb{R}$, med likhet precis då $x = 0$. Till exempel gäller att $|2| = 2$ och $|-4| = 4$, och generellt att $|x| = |-x|$ för alla $x \in \mathbb{R}$. Man kan nämligen tolka absolutbeloppet $|x|$ som avståndet på tallinjen från x till punkten 0, och för ett tal x gäller att x och $-x$ har samma avstånd till 0.

Absolutbeloppet kan ses som en funktion från kroppen $\mathbb{R}$ till de icke-negativa reella talen $\mathbb{R}_{\geqslant 0}$. För att mäta storleken på element i en godtycklig talmängd så behöver vi generalisera absolutbeloppet.

Definition 6.5.2. Givet en mängd $\mathbb{D}$ med en multiplikation och addition, säger vi att en funktion $N : \mathbb{D} \to \mathbb{R}_{\geq 0}$ är en *multiplikativ norm* på $\mathbb{D}$ om

(i) $N(x) = 0$ endast om $x = 0$

(ii) $N(xy) = N(x)N(y)$ för alla $x, y \in \mathbb{D}$

(iii) $N(x + y) \leqslant N(x) + N(y)$ för alla $x, y \in \mathbb{D}$ (*triangelolikheten*)

Att en talmängd är utrustad med en multiplikativ norm betyder alltså i synnerhet att sättet vi mäter storleken på element hänger samman med sättet vi multiplicerar element: storleken på en produkt är lika med produkten av faktorernas storlekar.

Vi ska nu visa att absolutbeloppet är en multiplikativ norm på $\mathbb{R}$.

Sats 6.5.3. *Absolutbeloppet* $|\cdot|$ *är en multiplikativ norm på* $\mathbb{R}$.

Bevis. Det är klart från definitionen att $|x| \geqslant 0$ för alla x och $|x| = 0$ om och endast om $x = 0$.

För att visa att absolutbeloppet uppfyller ekvation (ii) i Definition 6.5.2 observerar vi att det finns tre fall att undersöka:

(i) $x, y \geq 0$

(ii) $x, y < 0$

(iii) $x \geq 0, y < 0$ eller $x < 0, y \geq 0$

Vi visar här det sista fallet och lämnar de första två åt läsaren.

Om fall (iii) gäller kan vi av symmetriskäl anta att $x \geq 0$ och $y < 0$. Då gäller att $xy \leq 0$. Därmed följer att $|x| \cdot |y| = x \cdot (-y) = -(xy) = |xy|$, vilket skulle visas.

Vi bevisar nu att absolutbeloppet uppfyller ekvation (iii) i Definition 6.5.2. Från definitionen av absolutbeloppet gäller att $x \leq |x|$ och $y \leq |y|$. Genom att addera dessa olikheter får vi att

$$x + y \leq |x| + |y|.$$

Definitionen av absolutbeloppet ger även att $-x \leq |x|$ och $-y \leq |y|$. Adderar vi dessa två olikheter får vi

$$-x - y \leq |x| + |y|.$$

Eftersom $|x + y|$ är lika med antingen $x + y$ eller $-(x + y) = -x - y$ får vi, oavsett tecknet på $x + y$, att

$$|x + y| \leq |x| + |y|. \qquad \square$$

Övningar

Övning 6.1 ($\star\star$)**.** För ett polynom av grad n definierar vi rangen N som

$$N = n + |a_0| + |a_1| + \cdots + |a_n|. \tag{6.19}$$

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

Övning 6.2 ($\star$)**.** Visa att mängden $A = \{x \in \mathbb{R} \mid x > 0 \text{ och } x^2 < 2\}$ är icke-tom och uppåt begränsad.
Ledning: Denna övning påminner mycket om Övning 4.3. För att visa att A är uppåt begränsad kan resultatet från Övning 4.2 vara användbar.

Övning 6.3 ($\star$)**.** Låt $\beta = \sqrt{2} + 1$. Visa att $\beta \in \mathbb{A}$.

Övning 6.4 ($\star\star$)**.** Låt $\beta = \sqrt{2} + \sqrt{3}$. Visa att $\beta \in \mathbb{A}$.

Övning 6.5 ($\star$)**.** Visa att om x, y är positiva reella tal sådana att $x^2 = 2$ och $y^2 = 2$, så är $x = y$.
Ledning: Använd resultatet från Övning 4.2.

Övning 6.6 ($\star\star\star$)**.** Låt $\alpha, \beta \in \mathbb{R}$ vara sådana att $\alpha < \beta$. I Anmärkning 6.2.2 påstod vi att det öppna enhetsintervallet $(0, 1)$ är en överuppräknelig mängd. Använd detta för att visa att det öppna intervallet

$$(\alpha, \beta) = \{\gamma \in \mathbb{R} \mid \alpha < \gamma < \beta\}$$

är överuppräkneligt.
Ledning: Konstruera en bijektion från $(0, 1)$ till (α, β).

Övning 6.7 ($\star\star\star$)**.** Låt $\alpha, \beta \in \mathbb{R}$ vara sådana att $\alpha < \beta$. Visa att det finns ett irrationellt tal γ sådant att

$$\alpha < \gamma < \beta.$$

Ledning: Använd Sats 3.2.9 och resultatet från Övning 6.6.

Övning 6.8 ($\star\star\star$)**.** Visa att de transcendenta talen $\mathbb{T}$ ej är slutna under addition det vill säga visa att det finns $x, y \in \mathbb{T}$, så att $x + y \notin \mathbb{T}$.

Övning 6.9 ($\star$)**.** Låt N vara en multiplikativ norm på en kropp K med multiplikativt enhetselement 1. Visa att $N(1) = 1 \in \mathbb{R}$.

Övning 6.10 ($\star$)**.** Låt N vara en multiplikativ norm på en kropp K. Låt $A = \{x \in K \mid N(x) = 1\}$. Visa att A är sluten under multiplikation, det vill säga för alla $x, y \in A$ så gäller det att $xy \in A$.

7 Komplexa tal, kvaternioner och oktonioner

I detta kapitel går vi vidare och utforskar fler typer av tal. Återigen kommer vi delvis vara motiverade av att utvidga mängden av ekvationer som vi kan lösa.

7.1 Komplexa tal

År 1545 publicerade den Italienska matematikern Gerolamo Cardano en bok som innehöll en formel för att lösa tredjegradsekvationer, det vill säga ekvationer på formen

$$w_3x^3 + w_2x^2 + w_1x + w_0 = 0, \tag{7.1}$$

där $w_i \in \mathbb{R}$, för $j = 0, 1, 2, 3$. Han gav en formel som liknar formeln för lösningen av en andragradsekvation

$$w_2x^2 + w_1x + w_0 = 0, \tag{7.2}$$

nämligen

$$x = \frac{-w_1/w_2}{2} \pm \sqrt{\left(\frac{w_1/w_2}{2}\right)^2 - \frac{w_0}{w_2}}. \tag{7.3}$$

I de fall då (7.2) har reella lösningar, så ges lösningarna av formeln (7.3). Ibland händer det dock att $\left(\frac{w_1/w_2}{2}\right)^2 - \frac{w_0}{w_2} < 0$ vilket leder till att man i formeln (7.3) är tvungen att ta kvadratroten av ett negativt tal. Men om det för $0 < a, b \in \mathbb{R}$ gäller att $a = \sqrt{-b}$ så har vi att $a^2 = -b < 0$, vilket är omöjligt i $\mathbb{R}$, som konsekvens av Definition 3.5.2 och Hjälpsats 3.5.4.

Denna problematik uppstår dock enbart då ekvation (7.2) fullständigt saknar reella lösningar (se Övning 7.2), vilket gjorde att man på den tiden kunde avfärda situationen som någon sorts meningslös konsekvens av lösningsformeln. I Cardanos formel för lösningen av tredjegradsekvationer ingår dock ett tal i med den, på den tiden, chockerande egenskapen att

$$i^2 = -1$$

även då alla tre rötter till (7.1) är reella! Så formeln ger meningsfulla lösningar, men vägen dit går via "tal" som har till synes motsägelsefulla egenskaper. Talet i kallades av det skälet imaginärt.

Tal på formen $a+bi$ med $a, b \in \mathbb{R}$ visade sig dock vara användbara, och började med tiden accepteras. De kallas komplexa tal, då dom är sammansatta av såväl en reell del a och en så kallad imaginär del bi. Det dröjde dock ända till 1799 innan normannen Caspar Wessel insåg att komplexa tal kan betraktas som punkter i ett plan.

Det är den idé som vi kommer att följa när vi konstruerar mängden $\mathbb{C}$ av de komplexa talen.

Definition 7.1.1. Det reella talplanet $\mathbb{R}^2$ är mängden av ordnade par av reella tal:

$$\mathbb{R}^2 = \{(a, b) \mid a, b \in \mathbb{R}\}. \tag{7.4}$$

Ett vanligt sätt att representera planet är genom ett koordinatsystem med två koordinataxlar, där den horisontella axeln representerar värdet av a och vertikala axeln representerar värdet av b i punkten (a, b), se Figur 7.1.

Definition 7.1.2. De *komplexa talen* är mängden

$$\mathbb{R}^2 = \{(a, b) \mid a, b \in \mathbb{R}\}$$

tillsammans med operationerna:

- addition: $(w_1, z_1) + (w_2, z_2) = (w_1 + w_2, z_1 + z_2)$,
- multiplikation: $(w_1, z_1) \cdot (w_2, z_2) = (w_1 w_2 - z_1 z_2, w_1 z_2 + z_1 w_2)$,

för alla $w_1, z_1, w_2, z_2 \in \mathbb{R}$. Vi betecknar mängden av de komplexa talen med $\mathbb{C}$.

Anmärkning 7.1.3. Notera att konstruktionen av de komplexa talen är mycket enklare än konstruktionen av $\mathbb{R}$, $\mathbb{Q}$ och $\mathbb{Z}$. De komplexa talen är inte på något sätt mer "mystiska" eller mer abstrakta än de reella talen.

Anmärkning 7.1.4. Att $\mathbb{C}$ är sluten under addition och multiplikation följer av att $\mathbb{R}$ är sluten under addition och multiplikation.

För alla $a, b \in \mathbb{R}$ skriver vi $(a, 0) = a$ och $(0, b) = bi$. Ett komplext tal (a, b) skrivs därmed

$$(a, b) = (a, 0) + (0, b) = a + bi.$$

I allmänhet har vi att multiplikationen från Definition 7.1.2 fungerar som vanlig produkt av parenteser, såsom

$$\begin{aligned}(w_1 + z_1 i) \cdot (w_2 + z_2 i) &= w_1 w_2 + w_1 z_2 i + z_1 w_2 i + z_1 z_2 i^2 \\ &= (w_1 w_2 - z_1 z_2) + (w_1 z_2 + z_1 w_2) i.\end{aligned}$$

Notera att varje punkt $(a, b) \in \mathbb{R}^2$ kan skrivas $(a, b) = (a, 0) + (0, b)$. Vi kan se $\mathbb{R}$ som en delmängd av $\mathbb{C}$ genom att identifiera ett tal $a \in \mathbb{R}$ med punkten $(a, 0)$. Det gäller även att $(w_1, 0) + (w_2, 0) = (w_1 + w_2, 0)$ och $(w_1, 0) \cdot (w_2, 0) = (w_1 w_2, 0)$, så additionen och multiplikationen i $\mathbb{C}$ är kompatibel med multiplikationen i $\mathbb{R}$.

Det additiva enhetselementet i $\mathbb{C}$ är $0 = (0, 0)$ och det multiplikativa enhetselementet är $1 = (1, 0)$, det vill säga de vanliga reella enhetselementen under identifikationen av reella tal med tal på formen $(a, 0)$ ovan.

Fördelen med ovanstående definition av komplexa tal är att till exempel i nu är något så enkelt som en punkt i ett koordinatsystem, nämligen punkten $(0, 1)$. Detta är varken mer abstrakt eller onaturligt än vanliga reella tal – protester mot att vi bara "hittat på" talet i är således inte längre aktuella.

Sats 7.1.5. *Talet i uppfyller att $i^2 = -1$.*

Bevis. Enligt definitionen av multiplikation har vi att

$$i^2 = (0, 1)^2 = (0, 1) \cdot (0, 1) = (0 \cdot 0 - 1 \cdot 1, 0 \cdot 1 + 1 \cdot 0) = (-1, 0) = -1. \quad \square$$

Alla kroppsaxiomen verifieras enkelt för $\mathbb{C}$, och vi lämnar dessa verifikationer som en frivillig räkneövning åt läsaren (för den multiplikativa inversen, se ekvation (7.8)). Däremot har Sats 7.1.5 som följd att egenskapen att vara ordnad försvinner när vi går från $\mathbb{R}$ till $\mathbb{C}$.

Sats 7.1.6. *Det finns ingen ordning på $\mathbb{C}$ så att $\mathbb{C}$ är en ordnad kropp.*

Bevis. Antag att det finns en ordning $<$ på $\mathbb{C}$ som gör $\mathbb{C}$ till en ordnad kropp. Då gäller det antingen att $0 < i$ eller $i < 0$. Anta att det första fallet gäller. Eftersom $i^2 = -1$ så måste det enligt Definition 3.5.2 (O2) gälla att $0 < -1$. Vi kan multiplicera denna olikhet med i och får då $0 < -i$, igen enligt (O2). Men enligt Hjälpsats 3.5.3 så medför $0 < i$ att $-i < 0$, så vi har en motsägelse. Fallet $i < 0$ hanteras på liknande sätt. □

Sats 7.1.5 innebär att vi nu kan lösa alla andragradsekvationer fullständigt, ty om $a < 0$ så har vi att $-a > 0$ och $\sqrt{a} = i\sqrt{-a}$. Därför medför

$$\left(\frac{w_1/w_2}{2}\right)^2 - \frac{w_0}{w_2} < 0 \tag{7.5}$$

i (7.3) att

$$\sqrt{\left(\frac{w_1/w_2}{2}\right)^2 - \frac{w_0}{w_2}} = i\sqrt{-\left(\left(\frac{w_1/w_2}{2}\right)^2 - \frac{w_0}{w_2}\right)}, \tag{7.6}$$

vilket ger oss två rötter i (7.3). Faktum är att detta resultat endast är ett specialfall av en allmän sats:

Sats 7.1.7 (Algebrans fundamentalsats)**.** *Låt $1 \leq n \in \mathbb{N}$ och $w_j \in \mathbb{C}$ för $0 \leq j \leq n$. Antag att $w_n \neq 0$. Då gäller att polynomet*

$$w_n x^n + w_{n-1}x^{n-1} + \cdots + w_1 x + w_0, \tag{7.7}$$

har n rötter (räknat med multiplicitet[15]) i $\mathbb{C}$.

Definition 7.1.8. En talmängd med egenskapen att alla polynomekvationer med koefficienter i talmängden är fullständigt lösbara kallas *algebraisk sluten.*

Den uppmärksamma läsaren har kanske noterat att även för $w_j \in \mathbb{R}$ i (7.7) så gäller det ej att rötterna är reella – ekvationen $x^2 + 1 = 0$ är ett exempel. För $w_j \in \mathbb{C}$ säger däremot satsen att alla rötter finns i $\mathbb{C}$. De komplexa talen är således den naturliga talmängden för studiet av polynomekvationer, medan en algebraiker som enbart jobbar med reella tal lever farligt.

Anmärkning 7.1.9. Vi ber läsaren notera att Sats 7.1.7 inte säger något om hur rötterna kan bestämmas, utan talar enbart om att de finns. I själva verket bevisades det redan år 1824 av den norska matematikern Niels Henrik Abel att det för $n \geq 5$ inte finns någon lösningsformel för rötterna som enbart använder

[15]Exempelvis har polynomet $p(x) = x^2$ en dubbelrot i noll och $p(x)$ har därför två rötter räknat med multiplicitet.

sig av de fyra räknesätten samt rotutdragning. För en konkret ekvationen med $n \geq 5$ är man således ofta tvungen att approximera rötterna numeriskt med hjälp av en dator istället för att bestämma dem exakt.

Beviset för Sats 7.1.7 fordrar teori som ligger bortom detta kompendium. Den nyfikna läsaren uppmanas att inskriva sig på kurser i matematik vid KTH eller SU.

Vi visar nu att $\mathbb{C}$ kan utrustas med en multiplikativ norm.

Definition 7.1.10. Låt $z = a + bi \in \mathbb{C}$. *Absolutbeloppet* av z är

$$|z| = \sqrt{a^2 + b^2}.$$

Anmärkning 7.1.11. Pythagoras sats visar att ovanstående definition motsvarar vår vanliga intuition om hur avstånd mäts i planet.

Sats 7.1.12. *Absolutbeloppet på $\mathbb{C}$ är en multiplikativ norm.*

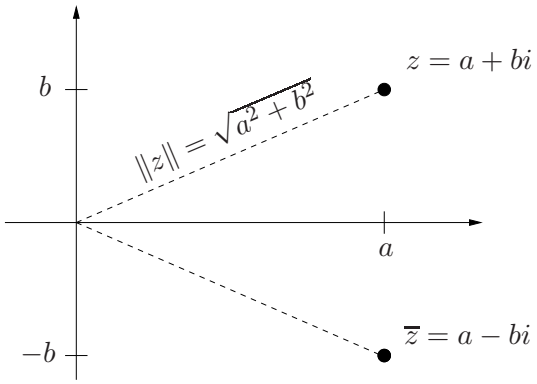
Bevis. Att $|z| = 0$ om och endast om $z = 0$ är klart från definitionen. Per definition av multiplikationen på $\mathbb{C}$ har vi att

$$\begin{aligned}
|(a+bi)(c+di)| &= |(ac-bd)+(ad+bc)i| = \sqrt{(ac-bd)^2+(ad+bc)^2} \\
&= \sqrt{a^2c^2 - 2abcd + b^2d^2 + a^2d^2 + 2abcd + b^2d^2} \\
&= \sqrt{a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2} = \sqrt{(a^2+b^2)(c^2+d^2)} \\
&= \sqrt{a^2+b^2}\sqrt{c^2+d^2} = |a+bi||c+di|.
\end{aligned}$$

Att absolutbeloppet uppfyller att $|z_1 + z_2| \leqslant |z_1| + |z_2|$ följer[16] från anmärkning 7.1.11 samt den vanliga triangelolikheten i planet: att det kortaste avståndet mellan två punkter är en rak linje. □

Följande operation är användbar för att skriva normer och multiplikativa inverser på ett kompakt sätt:

Definition 7.1.13. Låt $z = a + bi \in \mathbb{C}$. Det *komplexa konjugatet* av z är det komplexa talet $\overline{z} = a - bi$.



Figur 7.1: Den geometriska tolkningen av absolutbeloppet av $z = a + bi$ är som avståndet från punkten (a, b) till origo. Den geometriska tolkningen av det komplexa konjugatet av z är som speglingen av punkten (a, b) i x-axeln.

[16] Identiteten kan även visas rent algebraiskt.

Vi har att $z\overline{z} = (a+bi)(a-bi) = a^2 - abi + bia - b^2i^2 = a^2 + b^2 = |z|^2$, så att

$$\sqrt{z\overline{z}} = |z|,$$

och speciellt har vi att $z\overline{z} \in \mathbb{R}_{\geqslant 0}$ (se Definition 6.5.2). Vidare har vi för $z \neq 0$ att

$$\frac{\overline{z}}{|z|^2} z = \frac{\overline{z}}{z\overline{z}} z = \frac{\overline{z}z}{z\overline{z}} = 1,$$

så vi kan uttrycka den multiplikativa inversen till z genom

$$z^{-1} = \frac{\overline{z}}{|z|^2}. \tag{7.8}$$

7.2 Kvaternioner

Hittills i detta kompendium har vi i varje steg motiverat införandet av nya talmängder med önskemålet om att kunna lösa en större klass av ekvationer. Vi behövde snabbt negativa och rationella tal, och vid lite eftertanke insåg vi även behovet av reella tal. Komplexa talen visade sig genom algebrans fundamentalsats att vara den naturliga talmängden för studiet av polynomekvationer. I detta och i det följande avsnittet kommer vi införa två nya talmängder, men målet är inte längre att utvidga klassen av ekvationer som går att lösa.

De reella talen och de rationella talen kan ses som endimensionella. De komplexa talen beskrivs med hjälp av $\mathbb{R}^2$, det vill säga talplanet, och kan därför ses som tvådimensionella. Ett första skäl att vilja konstruera högredimensionella talmängder är ren nyfikenhet: går det, och i så fall hur? Ett annat skäl är att de komplexa talen har visat sig vara användbara för geometriska operationer i planet: rotationer ges av multiplikation med komplexa tal med norm lika med ett, det vill säga med komplexa tal på enhetscirkeln. Den skotska matematikern William Rowan Hamilton insåg att geometriska operationer i tre dimensioner – i rummet – kanske skulle kunna beskrivas med hjälp av någon form av tredimensionell talmängd, och försökte därför konstruera en sådan, dock utan framgång. Skälet till att Hamilton misslyckades är att det inte går att konstruera en talmängd med vettiga egenskaper i tre dimensioner. Däremot fick han under en promenad längs Royal Canal i centrala Dublin den 16 Oktober 1843 plötsligt insikten att ekvationen

$$i^2 = j^2 = k^2 = ijk = -1, \tag{7.9}$$

skulle ge upphov till en talmängd i fyra dimensioner med önskvärda egenskaper. Han ristade därefter in ekvationen i Broom Bridge, där det idag finns en stenskylt med ekvation (7.9). Hamiltons egen text ska enligt utsaga från sökande matematiker vara svårhittad då han inte var den enda personen som klottrade på bron.

Definition 7.2.1. *Kvaternionerna* $\mathbb{H}$ är mängden

$$\mathbb{R}^4 = \{(w_0, w_1, w_2, w_3) \mid w_0, \ldots, w_3 \in \mathbb{R}\},$$

av fyrtupplar utrustade med följande multiplikation:

$$\begin{aligned} & (w_0, w_1, w_2, w_3)(z_0, z_1, z_2, z_3) \\ = \; & (w_0z_0 - w_1z_1 - w_2z_2 - w_3z_3, w_0z_1 + w_1z_0 + w_2z_3 - w_3z_2, \\ & w_0z_2 - w_1z_3 + w_2z_0 + w_3z_1, w_0z_3 + w_1z_2 - w_2z_1 + w_3z_0), \end{aligned} \tag{7.10}$$

samt med additionen

$$(w_0, w_1, w_2, w_3) + (z_0, z_1, z_2, z_3) = (w_0 + z_0, w_1 + z_1, w_2 + z_2, w_3 + z_3).$$

Anmärkning 7.2.2. Att $\mathbb{H}$ är sluten under addition och multiplikation följer av att $\mathbb{R}$ är sluten under addition och multiplikation. Vidare är $\mathbb{H}$ algebraiskt sluten, se Definition 7.1.8.

Liksom med komplexa talen skriver vi $(w_0, w_1, w_2, w_3) = w_0 + w_1i + w_2j + w_3k$. Att visa att multiplikationen i (7.10) då sammanfaller med multiplikationen som följer av (7.9) och distributiva lagen är Övning 7.5. Vi kan identifiera $\mathbb{C}$ med mängden

$$\{w \in \mathbb{H} \mid w_2 = w_3 = 0\},$$

och vi lämnar åt läsaren att verifiera att multiplikationen i $\mathbb{C}$ är kompatibel med multiplikationen i $\mathbb{H}$ under denna identifikation.

Eftersom en kvaternion w har fyra komponenter, så är det naturligt att betrakta kvaternionerna som en fyrdimensionell talmängd. Att vi inte skriver talkropp beror på följande:

Sats 7.2.3. *Kvaternionerna $\mathbb{H}$ är inte kommutativa: det existerar $a, b \in \mathbb{H}$ så att $ab \neq ba$.*

Att visa detta är Övning 7.3.

Anmärkning 7.2.4. Att $\mathbb{H}$ inte är kommutativ betyder i synnerhet att $\mathbb{H}$ inte är en kropp.

Alla återstående axiom för kroppar är uppfyllda. Det additiva enhetselementet i $\mathbb{H}$ är naturligtvis $0 = (0, 0, 0, 0)$, och det multiplikativa enhetselementet är $1 = (1, 0, 0, 0)$. Att verifiera detta är Övning 7.4. Att verifiera associativa lagen samt den distributiva lagen är lite omständligt, och lämnas som frivillig övning åt läsaren.

Definition 7.2.5. Låt $w = w_0 + w_1i + w_2j + w_3k \in \mathbb{H}$. Då är absolutbeloppet

$$|w| = \sqrt{w_0^2 + w_1^2 + w_2^2 + w_3^2}.$$

Detta är en generalisering av sättet att mäta avstånd i tre dimensioner. Följande sats innebär således att även kvaternionerna har egenskapen att storleken av en produkt är lika med produkten av storlekarna:

Sats 7.2.6. *Absolutbeloppet på $\mathbb{H}$ är en multiplikativ norm.*

Bevis. Beviset är väsentligen identiskt med beviset för Sats 7.1.12 och lämnas som frivillig övning. □

Definition 7.2.7. Konjugatet i $\mathbb{H}$ ges av $\overline{w} = (w_0, -w_1, -w_2, -w_3)$.

Vi har då att $w\overline{w} = |w|^2$, vilket vi uppmanar läsaren att verifiera. Vi kan då, på samma sätt som i $\mathbb{C}$, hitta multiplikativa inverser i $\mathbb{H}$:

Sats 7.2.8. *Låt $0 \neq w = (w_0, w_1, w_2, w_3) \in \mathbb{H}$. Då har w en multiplikativ invers w^{-1} som uppfyller*

$$w^{-1}w = 1 = ww^{-1}$$

och som ges av

$$w^{-1} = \overline{w}/|w|^2 = \frac{1}{w_0^2 + w_1^2 + w_2^2 + w_3^2}(w_0, -w_1, -w_2, -w_3).$$

Bevis. Beviset är lämnat åt läsaren i Övning 7.7. □

Vi har nu konstruerat kvaternionerna och visat att de åtminstone har en uppsättning talliknande egenskaper, även om avsaknaden av kommutativitet är otillfredsställande. Men är de alls användbara? Hamilton var ju motiverad av tillämpningar i tredimensionell geometri, men lyckades istället konstruera en fyrdimensionell talmängd. Intressant nog så kan kvaternioner användas för att beskriva rotationer i rummet. En kvaternion med absolutbelopp lika med ett kallas för en *enhetskvaternion*. Låt w vara en enhetskvaternion, och z en godtycklig kvaternion. Vi kan nu bilda en ny kvaternion z' genom att sätta

$$z' = wzw^{-1}.$$

Denna operation kallas konjugering med w. Eftersom $z = z_0 + z_1 i + z_2 j + z_3 k$ så får vi via tillämpning av distributiva lagen att

$$z' = wz_0w^{-1} + wz_1iw^{-1} + wz_2jw^{-1} + wz_3kw^{-1}.$$

Men $wz_0w^{-1} = ww^{-1}z_0 = z_0$, eftersom alla kvaternioner kommuterar med reella tal (se Övning 7.6). Så

$$z' = z_0 + wz_1iw^{-1} + wz_2jw^{-1} + wz_3kw^{-1},$$

det vill säga första komponenten i z bevaras under konjugering med w. Således är det endast de återstående tre komponenterna som kan förändras, och det går att visa[17] att operationen här motsvarar en rotation, samt att varje sådan rotation motsvaras av en enhetskvaternion. Men mer än så är sant: givet två rotationer α och β runt origo i $\mathbb{R}^3$, så fås en tredje rotation γ genom att först utföra rotationen β och därefter utföra rotationen α (jämför sammansättning

[17]Beviset är inte särskilt svårt, men kräver lite kunskap i linjär algebra, och ryms således inte i detta kompendium.

av funktioner: $f \circ g(x) = f(g(x)))$. Givet kvaternioner w_α och w_β som representerar rotationerna α respektive β så ges w_γ som produkten

$$w_\alpha w_\beta = w_\gamma,$$

så multiplikationen i $\mathbb{H}$ återspeglar sammansättningen av rotationer i $\mathbb{R}^3$, vilket är ytterst praktiskt i tillämpningar.

Det finns ett antal andra sätt att räkna på rotationer i rummet, men kvaternioner är av flera skäl praktiska i tillämpningar. De fordrar endast 4 reella tal – jämfört 9 reella tal om man använder metoder från linjär algebra – och de avrundningsfel som oundvikligen uppstår vid datorberäkningar är synnerligen lätta att hantera när man använder sig av kvaternioner. Därför används kvaternioner idag i såväl datorspel som vid styrning av satelliter[18].

7.3 Oktonioner

Man kan nu fråga sig om det går att fortsätta: kan vi hitta en talmängd i en ännu högre dimension än dimension fyra? Den frågan ställde sig även John T. Graves, en vän till Hamilton. Svaret gav han – samma år som Hamiltons upptäckt av kvaternionerna – i ett brev till Hamilton, där han beskrev den talmängd som senare fick namnet oktonionerna.

Definition 7.3.1. Oktonionerna $\mathbb{O}$ är mängden

$$\mathbb{R}^8 = \{(w_0, \ldots, w_7) \mid w_k \in \mathbb{R}, 0 \leq k \leq 7\},$$

utrustad med multiplikation och addition enligt nedan. Låt

$$(w_1, \ldots, w_7) = w_0 + w_1 i_1 + \cdots + w_7 i_7,$$

multiplikationen ges då av följande relationer:

$\cdot$	$\boldsymbol{i_1}$	$\boldsymbol{i_2}$	$\boldsymbol{i_3}$	$\boldsymbol{i_4}$	$\boldsymbol{i_5}$	$\boldsymbol{i_6}$	$\boldsymbol{i_7}$
$\boldsymbol{i_1}$	-1	i_3	$-i_2$	i_5	$-i_4$	$-i_7$	i_6
$\boldsymbol{i_2}$	$-i_3$	-1	i_1	i_6	i_7	$-i_4$	$-i_5$
$\boldsymbol{i_3}$	i_2	$-i_1$	-1	i_7	$-i_6$	i_5	$-i_4$
$\boldsymbol{i_4}$	$-i_5$	$-i_6$	$-i_7$	-1	i_1	i_2	i_3
$\boldsymbol{i_5}$	i_4	$-i_7$	i_6	$-i_1$	-1	$-i_3$	i_2
$\boldsymbol{i_6}$	i_7	i_4	$-i_5$	$-i_2$	i_3	-1	$-i_1$
$\boldsymbol{i_7}$	$-i_6$	i_5	i_4	$-i_3$	$-i_2$	i_1	-1

samt $1 \cdot i_j = i_j = i_j \cdot 1$, för $1 \leq j \leq 7$.

Additionen ges av

$$(w_0, \ldots, w_7) + (z_0, \ldots, z_7) = (w_0 + z_0, \ldots, w_7 + z_7).$$

[18] Se till exempel J. B. Kuipers (1999) Quaternions and rotation Sequences: a Primer with Applications to Orbits, Aerospace, and Virtual Reality, Princeton University Press.

Anmärkning 7.3.2. Att $\mathbb{O}$ är sluten under addition och multiplikation följer av att $\mathbb{R}$ är sluten under addition och multiplikation. Vidare är $\mathbb{O}$ algebraiskt sluten.

Som vanligt kan vi identifiera $\mathbb{H}$ med delmängden

$$\{w \in \mathbb{O} \mid w_4 = w_5 = w_6 = w_7 = 0\},$$

och vi lämnar åt läsaren att verifiera att multiplikationen och additionen i $\mathbb{H}$ är kompatibel med multiplikationen och additionen i $\mathbb{O}$. En omedelbar konsekvens av detta och Sats 7.2.3 är

Sats 7.3.3. Oktonionerna $\mathbb{O}$ *är inte en kropp.*

Precis som $\mathbb{H}$ är $\mathbb{O}$ inte kommutativ. Men situationen är värre än så, oktonionerna har nämligen den konstiga egenskapen att multiplikationen inte ens är associativ!

Sats 7.3.4. $\mathbb{O}$ *är inte associativ, det vill säga det finns* $w, y, z \in \mathbb{O}$ *så att*

$$w(yz) \neq (wy)z.$$

Bevis. Det räcker att hitta 3 element i $\mathbb{O}$ så att deras produkt inte är associativ. Detta är Övning 7.8. □

Definition 7.3.5. Låt $w \in \mathbb{O}$. Då är absolutbeloppet $|w|$ definierat som

$$|w| = \sqrt{\sum_{k=0}^{7} w_k^2}.$$

Anmärkning 7.3.6. Precis som för $\mathbb{H}$ och $\mathbb{C}$ så har vi ett konjugat, som ges av $\overline{w} = (w_0, -w_1, \ldots, -w_7)$, och $|w|^2 = w\overline{w}$. Som förväntat ges inverser som $w^{-1} = \overline{w}/|w|^2$ och vi har återigen att normen är multiplikativ:

Sats 7.3.7. *Absolutbeloppet på* $\mathbb{O}$ *är en multiplikativ norm.*

Beviset liknar beviset för Sats 7.1.12 men utelämnas av pappersbesparande skäl.

Oktonionernas bristande associativitet samt även i övrigt ganska otympliga multiplikation har som konsekvens att de betraktas som något av ett kuriosum av många matematiker, och de används inte aktivt i praktiska tillämpningar så som kvaternionerna[19]. Deras popularitet har dock tilltagit senaste decennierna, och aktiv forskning om oktonioner bedrivs bland annat vid Uppsala Universitet.

Vi har nu konstruerat en hel uppsättning olika talmängder, och även sett hur de ryms i varandra. För att repetera har vi följande inklusioner:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O}.$$

Vi sammanfattar de olika stegen på vägen:

[19] Man skulle kunna misstänka att oktonioner kan representera rotationer i ett sjudimensionellt rum. Så är dock inte fallet då sammansättning av rotationer – i vilket rum som helst – måste vara associativ.

- Vi får $\mathbb{Z}$ från $\mathbb{N}$ genom att lägga till additiva inverser.
- Vi får $\mathbb{Q}$ från $\mathbb{Z}$ genom att lägga till multiplikativa inverser.
- Vi får $\mathbb{R}$ från $\mathbb{Q}$ genom att "fylla igen hålen i tallinjen."
- Från $\mathbb{R}$ till $\mathbb{C}$ får vi lösningar till alla polynomekvationer, men $\mathbb{C}$ är inte en *ordnad* kropp.
- Från $\mathbb{C}$ till $\mathbb{H}$ förlorar vi kommutativiteten. Med andra ord, det finns element $a, b \in \mathbb{H}$ så att $ab \neq ba$.
- Från $\mathbb{H}$ till $\mathbb{O}$ förlorar vi associativiteten. Med andra ord, det finns element $a, b, c \in \mathbb{O}$ så att $a(bc) \neq (ab)c$.

Matematiker blir förstås nyfikna och vill ta reda på om det går att fortsätta så. Finns det 16-dimensionella talmängder, etc.? Listan ovan visar att det inte är orimligt att tänka sig att vi förlorar än flera egenskaper om vi försöker bilda multiplikationer i högre dimensioner, och så är även fallet.

Sedenionerna $\mathbb{S}$ är mängden $\mathbb{R}^{16}$ utrustad med en multiplikation och addition så att man kan identifiera $\mathbb{O}$ med de element i $\mathbb{R}^{16}$ vars sista 8 komponenter är noll. Men i detta steg händer det något konstigt. Ty om multiplikation och addition på $\mathbb{R}^{16}$ uppfyller (A1)-(A5) samt (M1),(M4),(M5) och (D) på sidan 28 och 29, och även har egenskapen att reella tal kommuterar med alla element i $w \in \mathbb{R}^{16}$, så kommer det att finnas element

$$0 \neq z, w \in \mathbb{R}^{16} \quad \text{så att} \quad z \cdot w = 0.$$

Vi kan således utvidga listan ovan:

- Från $\mathbb{O}$ till $\mathbb{S}$ händer något absurt! Det finns nämligen "tal" $z, w \in \mathbb{S}$ som inte är noll, men där $zw = 0$.

Detta medför speciellt att sedenionerna inte kan utrustas med en multiplikativ norm, eftersom $N(z)N(w) = N(zw) = N(0) = 0$ medför att produkten av de nollskilda reella talen $N(z)$ och $N(w)$ är noll, vilket är omöjligt.

Om en mängd har en multiplikation som är varken kommutativ, associativ eller bevarar storleken på elementen, då kanske det inte är rimligt att kalla elementen för "tal" heller. Författarna till detta kompendium tycker inte det och väljer därför att sätta punkt här.

Övningar

Övning 7.1 ($\star\star$)**.** Visa att för $z, w \in \mathbb{C}$ gäller att $\overline{z+w} = \overline{z} + \overline{w}$, samt $\overline{zw} = \overline{z} \cdot \overline{w}$.

Övning 7.2 ($\star\star\star$)**.** Antag att en andragradsekvation $a_2x^2 + a_1x + a_0 = 0$ med reella koefficienter a_2, a_1 och a_0 har en lösning x_0 sådan att $x_0 \notin \mathbb{R}$, det vill säga $x_0 = a + bi$ med $b \neq 0$. Visa att då har ekvationen även en annan lösning x_1 sådan att $x_1 \notin \mathbb{R}$.
Ledning: Använd resultatet från Övning 7.1.

Övning 7.3 ($\star\star$)**.** Visa att multiplikationen i $\mathbb{H}$ ej är kommutativ, det vill säga hitta åtminstone två element $a, b \in \mathbb{H}$ så att $ab \neq ba$.

Övning 7.4 ($\star$)**.** Visa att $(0,0,0,0)$ är det additiva enhetselementet i $\mathbb{H}$ och visa att $(1,0,0,0)$ är det multiplikativa enhetselementet i $\mathbb{H}$.

Övning 7.5 ($\star\star\star$)**.** Sätt $(w_0, w_1, w_2, w_3) = w_0 + w_1 i + w_2 j + w_3 k$. Visa att multiplikationen i ekvation (7.10) då sammanfaller med multiplikationen som följer av ekvation (7.9) och den distributiva lagen.

Övning 7.6 ($\star\star$)**.** Låt $a \in \mathbb{R}$. Visa att a kommuterar med alla $w \in \mathbb{H}$, det vill säga att $aw = wa$ för alla $w \in \mathbb{H}$.

Övning 7.7 ($\star\star$)**.** Bevisa Sats 7.2.8.

Övning 7.8 ($\star$)**.** Visa att multiplikationen i $\mathbb{O}$ ej är associativ.

Lösningar till udda övningsuppgifter

Övning 1.1.

(i) $B \cup C = A$.

(ii) $B \cap C = \emptyset$.

(iii) $D \cap C = \{4, 36\}$.

(iv) $\{x \in D \mid x \in B\} = D \cap B = \{1, 19, 101\}$.

(v) $\{x \in A \mid x = y + 1 \text{ för något } y \in D\} = \{2, 5, 20, 37, 102\}$.

(vi) $\{x + 1 \mid x \in D\} = \{2, 5, 20, 37, 102\}$.

Övning 1.3. Tag $x \in \mathbb{N}$, det vill säga att x är något av talen $0, 1, 2, 3, \ldots$. I synnerhet gäller $x \in \{0, 1, 2, \ldots, x\} = B_x$ och därmed $x \in B_0 \cup B_1 \cup B_2 \cup \ldots$. Eftersom x var godtycklig visar detta att $\mathbb{N} \subseteq B_0 \cup B_1 \cup B_2 \cup \ldots$.

Omvänt, antag att $x \in B_0 \cup B_1 \cup B_2 \cup \ldots$. Det betyder att det finns ett heltal $n \geqslant 1$ så att $x \in B_n = \{0, 1, 2, \ldots, n\}$. I synnerhet gäller $x \in \{0, 1, 2, \ldots\} = \mathbb{N}$. Detta visar att $B_0 \cup B_1 \cup B_2 \cup \ldots \subseteq \mathbb{N}$.

Eftersom båda inklusioner $\mathbb{N} \subseteq B_0 \cup B_1 \cup B_2 \cup \ldots$ och $B_0 \cup B_1 \cup B_2 \cup \ldots \subseteq \mathbb{N}$ gäller kan vi dra slutsatsen att $\mathbb{N} = B_0 \cup B_1 \cup B_2 \cup \ldots$.

Övning 1.5. Alla utom ”Mängden av de naturliga talen” är påståenden. Det enda påståendet för vilket vi kan avgöra om det är sant eller falskt är ”Varje mängd innehåller minst ett element”, och detta påstående är falskt eftersom den tomma mängden inte innehåller något element.

Övning 1.7. Vi har (i) $\iff$ (ix) och (ii) $\iff$ (vi). Dessutom gäller att (iii) $\iff$ (viii) (observera att $A \cap B \subseteq B$). Man ser också att (v) $\iff B \subseteq A \iff$ (x).

Slutligen påstår vi att (iv) och (vii) är ekvivalenta. Antag först att $A = \emptyset$. I så fall är $x \in A$ ett falskt påstående oavsett vad x är för något. Men ett falskt påstående implicerar varje annat påstående, så alltså gäller att $x \in A \implies x \notin A$. Antag omvänt att $x \in A \implies x \notin A$, vi vill bevisa att $A = \emptyset$. Antag motsatsen, så att det finns något x med $x \in A$. Enligt implikationen vi antagit gäller nu också $x \notin A$, en motsägelse, vilket bevisar att $A = \emptyset$.

Övning 1.9. Lösningen till denna uppgift är i stort sätt identiskt med beviset av Sats 1.3.1. Vi antar alltså motsatsen till det vi vill visa, det vill säga vi antar att det faktiskt finns heltal a, b så att ekvation (1.3) gäller, och härleder en motsägelse. Därifrån drar vi slutsatsen att a, b med den egenskapen ej kan finnas.

Vi kan anta att a är det minsta möjliga positiva tal så att ekvation (1.3) är uppfylld. Ekvation (1.3) är ekvivalent med ekvationen $a^2 = 3b^2$, och eftersom högerledet i den senare ekvationen är delbar med tre, så måste a^2 vara delbar med tre, vilket medför att a är delbar med tre, så $a = 3c$ för något positivt tal c. Vi erhåller då ekvationen $3^2c^2 = 3b^2$ vilket ger $3c^2 = b^2$. Eftersom vänsterledet

nu är delbart med tre, måste då även högerledet vara delbart med tre, och vi får att $b = 3d$ för något d. Vi får då att $3c^2 = 3^2d^2$ vilket ger

$$\left(\frac{c}{d}\right)^2 = 3 = \left(\frac{a}{b}\right)^2.$$

Men $3c = a$, så $c < a$ och detta är en motsägelse, för vi antog ju att a var det minsta positiva tal så att (1.3) är uppfylld.

Övning 2.1. Att $y, z \in [x]$ betyder att xRy och xRz. Eftersom R är symmetrisk så följer yRx. Nu vet vi alltså att yRx och att xRz och eftersom R är transitiv så följer yRz.

Övning 2.3. Antag att $[x] \cap [y] \neq \emptyset$, vilket betyder att det finns ett $z \in A$ som uppfyller $z \in [x]$ och $z \in [y]$. Vi har alltså att xRz och att yRz. Eftersom R är symmetrisk så följer zRy. Använd nu transitiviteten hos R för att få att xRy, vilket betyder att x är relaterad till y. Men vi vet att x inte är relaterad till y så detta är en motsägelse, och därmed måste $[x] \cap [y] = \emptyset$.

Övning 2.5. Vi måste visa att multiplikationen är väldefinierad. Låt

$$[(a,b)]R[(a_1,b_1)], \quad \text{det vill säga} \quad a + b_1 = a_1 + b,$$

och

$$[(c,d)]R[(c_1,d_1)], \quad \text{det vill säga} \quad c + d_1 = c_1 + d.$$

Vi måste då visa att $[(a,b)][(c,d)]R[(a_1,b_1)][(c_1,d_1)]$, det vill säga

$$[(ac+bd, ad+bc)]R[(a_1c_1 + d_1d_1, a_1d_1 + b_1c_1)].$$

Vi visar först att $[(ac+bd, ad+bc)]R[(a_1c + b_1d, a_1d + b_1c)]$, det vill säga att

$$ac + bd + a_1d + b_1c = ad + bc + a_1c + b_1d. \tag{7.11}$$

Observera att $a + b_1 = a_1 + b$ medför att

$$ac + b_1c = a_1c + bc, \quad \text{samt att} \quad ad + b_1d = a_1d + bd.$$

Adderar vi högerledet i första ekvationen med vänsterledet i andra, och vänsterledet i första med högerledet i andra, så får vi

$$ac + b_1c + a_1d + bd = a_1c + bc + ad + b_1d,$$

vilket är ekvation (7.11). Genom att använda $c + d_1 = c_1 + d$ kan man på liknade sätt visa att

$$[(a_1c + b_1d, a_1d + b_1c)]R[(a_1c_1 + b_1d_1, a_1d_1 + b_1c_1)].$$

Eftersom R är en ekvivalensrelation och således transitiv får vi att

$$[(ac+bd, ad+bc)]R[(a_1c_1 + d_1d_1, a_1d_1 + b_1c_1)],$$

vilket skulle visas.

Övning 2.7. Eftersom $0 < m$ så finns det ett $a \in \mathbb{N}$ så att $m = [(a, 0)]$ och då $n < 0$ så finns det ett $b \in \mathbb{N}$ så att $n = [(0, b)]$. Då har vi att

$$mn = [(a, 0)][(0, b)] = [(0a + 0b, 0 + ab)] = [(0, ab)],$$

och då $m, n \neq 0$ och därför även $a, b \neq 0$ och således $ab \neq 0$, har vi att $[(0, ab)] < 0$.

Övning 2.9. Den kommutativa lagen för addition i $\mathbb{Z}$ följer av att

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

där vi använde den kommutativa lagen för addition i $\mathbb{N}$.

På liknade sätt följer den associativa lagen för addition

$$\begin{aligned}([(a, b)] + [(c, d)]) + [(e, f)] &= [((a + c) + e, (b + d) + f)] \\ &= [(a + (c + e), b + (d + f)] \\ &= [(a, b)] + ([(c, d)] + [(e, f)]).\end{aligned}$$

Den kommutativa lagen för multiplikation följer av

$$\begin{aligned}[(a, b)][(c, d)] &= [(ac + bd, ad + bc)] = [(ca + db, da + cb)] \\ &= [(ca + db, cb + da)] = [(c, d)][(a, b)].\end{aligned}$$

Den associativa lagen för multiplikation följer av

$$\begin{aligned}[(a, b)]\,([(c, d)][(e, f)]) &= [(a, b)][(ce + df, cf + de)] \\ &= [(a(ce + df) + b(cf + de), a(cf + de) + b(ce + df))] \\ &= [(ace + adf + bcf + bde, acf + ade + bce + bdf)] \\ &= [((ac + bd)e + (ad + bc)f, (ac + bd)f + (ad + bc)e)] \\ &= [(ac + bd, ad + bc)][(e, f)] \\ &= ([(a, b)][(c, d)])\,[(e, f)]\end{aligned}$$

Den distributiva lagen följer från att

$$\begin{aligned}[(a, b)]([(c, d)] + [(e, f)]) &= [(a, b)][(c + e, d + f)] \\ &= [(a(c + e) + b(d + f), a(d + f) + b(c + e))] \\ &= [(ac + ae + bd + bf, ad + af + bc + be)] \\ &= [(ac + bd, ad + bc)] + [(ae + bf, af + be)] \\ &= [(a, b)][(c, d)] + [(a, b)][(e, f)].\end{aligned}$$

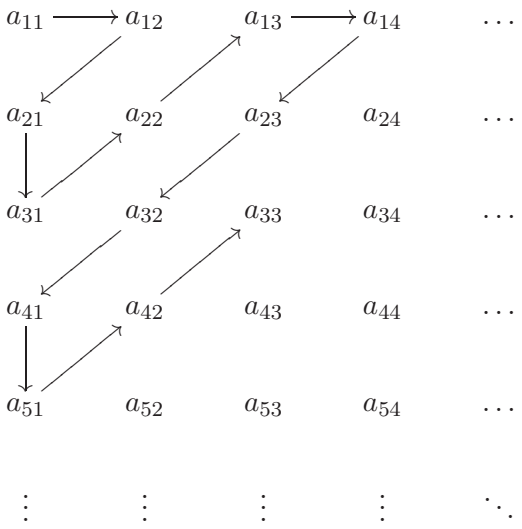
Övning 2.11. Vi har att $(1, 2)S(0, 0)$ och att $(0, 0)S(1, 3)$ men däremot inte att $(1, 2)S(1, 3)$ vilket betyder att S inte är transitiv.

Övning 2.13. Enligt identifikationen av n med $[(n,1)]$ så har vi att

$$\begin{aligned} n\cdot[(a,b)] &= [(n,1)]\cdot[(a,b)] = [(na,b)] = [(\underbrace{a+a+\cdots+a}_{n\text{ gånger}},b)] \\ &= [(a,b)] + [(\underbrace{a+a+\cdots+a}_{n-1\text{ gånger}},b)] \\ &= [(a,b)] + [(a,b)] + [(\underbrace{a+a+\cdots+a}_{n-2\text{ gånger}},b)] \\ &\vdots \\ &= \underbrace{[(a,b)] + [(a,b)] + \cdots + [(a,b)]}_{n\text{ gånger}}. \end{aligned}$$

Övning 3.1. Ett exempel ges av funktionen f definierad genom $f(1) = A$, $f(2) = B$, $f(3) = C$, $f(4) = B$. Vi kan välja $f(k)$ fritt bland A, B och C för $k = 1, 2, 3, 4$. Alltså ska vi välja ett av tre alternativ fyra gånger, så vi får totalt $3^4 = 81$ möjliga funktioner.

Övning 3.3. Eftersom mängderna $A_1, A_2, A_3, \ldots$ är uppräkneliga kan vi skriva $A_n = \{a_{n1}, a_{n2}, a_{n3}, \ldots\}$ för $n = 1, 2, 3, \ldots$. Alltså kan vi skriva upp elementen i $A = A_1 \cup A_2 \cup A_3 \cup \ldots$ enligt följande:



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

$$b_0 = a_{11}, \quad b_1 = a_{12}, \quad b_2 = a_{21}, \quad b_3 = a_{31}, \ldots \tag{7.12}$$

som uppfyller att $A = \{b_0, b_1, b_2, \ldots\}$. Alltså är A uppräknelig.

Övning 3.5. Antag att $a, b \in K$ har egenskapen att $a + x = x$ och $b + x = x$ för alla $x \in K$. Då får vi att $a = b + a = a + b = b$, så $a = b$, vilket visar att det additiva enhetselementet är unikt.

Antag att $c, d \in K$ har egenskapen att $c \cdot x = x$ och $d \cdot x = x$ för alla $x \in K$. Då får vi att $c = d \cdot c = c \cdot d = d$, så $c = d$, vilket visar att det multiplikativa enhetselementet är unikt.

Övning 3.7. Enligt antagande har vi att $ad = bc$. Antag att $0 < \frac{a}{b}$. 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 $0 < \frac{c}{d}$.

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

Övning 3.9. Relationen $<$ för rationella tal definierades genom

$$\frac{a}{b} > 0 \qquad \text{om} \qquad ab > 0, \tag{7.13}$$

och för $p, q \in \mathbb{Q}$ så är

$$p > q \qquad \text{om} \qquad p - q > 0. \tag{7.14}$$

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

$$p - q = \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd} > 0. \tag{7.15}$$

Enligt (7.13) gäller detta om

$$bd(ad - bc) > 0. \tag{7.16}$$

För att visa att $<$ är en ordning så måste vi kontrollera att $<$ uppfyller kraven i Definition 2.3.12. För alla $x, y, z \in \mathbb{Q}$ skall följande gälla:

(i) Endast en av följande gäller: $x < y$, $y < x$ eller $x = y$.

(ii) Om $x < y$ och $y < z$ så är $x < z$.

Sätt

$$x = \frac{a}{b}, \quad y = \frac{c}{d} \qquad \text{och} \qquad z = \frac{e}{f}. \tag{7.17}$$

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

$$x < y: \qquad bd(bc - ad) > 0 \tag{7.18}$$
$$y < x: \qquad bd(ad - bc) > 0 \tag{7.19}$$
$$x = y: \qquad bd(bc - ad) = 0. \tag{7.20}$$

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 $x < z$, det vill säga $z - x > 0$. Sätt

$$p = y - x \qquad \text{och} \qquad q = z - y. \tag{7.21}$$

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 $p=\frac{s}{t}$ och $q=\frac{u}{v}$ och antag att $p,q>0$, det vill säga $st>0$ och $uv>0$. Vi beräknar

$$p+q=\frac{sv+tu}{tv}. \tag{7.22}$$

Nu vill vi visa att $p+q>0$, det vill säga att

$$tv(sv+tu)=stv^2+uvt^2>0. \tag{7.23}$$

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 3.11. Antagandet att $x<y$ medför att $y-x>0$. Eftersom vi även antagit att $z>0$ ger egenskap $(O2)$ i definition 3.5.2 att

$$z(y-x)>0$$

Från denna olikhet följer den sökta olikheten med hjälp av (D) och (O1).

Övning 3.13. Vi visar endast att $q<\frac{q+r}{2}$, beviset av att $\frac{q+r}{2}<r$ är helt analogt. Eftersom $q<r$ ger (O1) att

$$q+r<r+r=2r \tag{7.24}$$

Övning 3.11 ger nu att

$$\frac{q+r}{2}=\frac{1}{2}\cdot(q+r)<\frac{1}{2}\cdot 2r=r \tag{7.25}$$

Övning 4.1. Vi måste visa att $\alpha_0\subseteq\alpha_1$ och $\alpha_0\neq\alpha_1$. Låt $q\in\alpha_0$. Då gäller att $q<0<1$, så $q\in\alpha_1$. Alltså gäller det att $\alpha_0\subseteq\alpha_1$. Dessutom har vi $\frac{1}{2}\in\alpha_1$, ty $\frac{1}{2}<1$, men $\frac{1}{2}\notin\alpha_0$, ty $0<\frac{1}{2}$. Alltså gäller det att $\alpha_0\neq\alpha_1$.

Övning 4.3. Vi visar att 2 är en övre begränsning till A. Vi ska alltså visa att $a\leqslant 2$ för alla $a\in A$. Låt b vara ett rationellt tal sådant att $b>2$. Vi ska visa att $b\notin A$. Resultatet från Övning 4.2 medför att

$$b^2>2^2=4.$$

Eftersom $4>2$ har vi att $b^2>2$, vilket innebär att det inte gäller att $b^2\leqslant 2$. Eftersom $b>2>0$ visar detta att $b\notin A$. Således måste det gälla att $a\leqslant 2$ för alla $a\in A$, vilket medför att A är uppåt begränsad.

Övning 4.5. Det är klart att 1 är en övre begränsning till $(0,1)$. Det kvarstår därför endast att visa att 1 är den minsta övre begränsningen till $(0,1)$. Antag att $r<1$ är en övre begränsning till $(0,1)$. Då är det klart att $0<r$. Enligt Övning 3.13 har vi att $0<r<\frac{1+r}{2}<1$. Alltså gäller det att $\frac{1+r}{2}\in(0,1)$ och att $r<\frac{1+r}{2}$. Detta är en motsägelse eftersom vi antog att r var en övre begränsning till $(0,1)$. Därmed gäller det att $\sup_{\mathbb{R}}(0,1)=1$.

Övning 4.7. Eftersom $1/n > 0$ för alla $n \geqslant 1$ så är $e_n < 1$ för alla $n \geqslant 1$. Alltså är 1 en övre begränsning till E. Låt oss visa att ett rationellt tal $z < 1$ inte kan vara en övre begränsning, vilket visar att 1 är den minsta övre begränsningen till E. Tag $z < 1$ och sätt $d = 1 - z > 0$. Välj ett heltal n_0 sådant att $n_0 > 1/d$, vilket ger att $d > 1/n_0$. Vi får då att

$$e_{n_0} = 1 - \frac{1}{n_0} > 1 - d = z. \tag{7.26}$$

Eftersom $e_{n_0} \in E$ så kan z inte vara en övre begränsning. Alltså är $\sup_{\mathbb{Q}} E = 1$.

Övning 4.9. Vi påminner oss om definitionen av $\alpha \cdot \beta$ för positiva snitt

$$\alpha \cdot \beta = \{q \in \mathbb{Q} \mid q \leqslant rs \text{ för några } r \in \alpha, s \in \beta \text{ där } r > 0, s > 0\}. \tag{7.27}$$

Vi visar att (R1)–(R3) i Definition 4.2.1 är uppfyllda.

(R1) Mängden $\alpha \cdot \beta$ är inte tom eftersom $\alpha \neq \emptyset$ och $\beta \neq \emptyset$. Då α och β är uppåt begränsade så finns det ett rationellt tal q sådant att $p < q$ för alla $p \in \alpha$ eller $p \in \beta$. Då är $q^2 \notin \alpha \cdot \beta$ vilket ger att $\alpha \cdot \beta \neq \mathbb{Q}$.

(R2) Detta följer direkt från definitionen eftersom om $q \in \alpha \cdot \beta$ så innehåller $\alpha \cdot \beta$ alla rationella tal mindre än q.

(R3) Låt $a \in \alpha \cdot \beta$. Vi vill visa att det finns ett $r \in \alpha \cdot \beta$ sådant att $r > a$. Om $a \leqslant 0$ är det klart att det finns sådana r; antag att $a > 0$. Då $a \in \alpha \cdot \beta$ så finns det två positiva tal $p \in \alpha$ och $q \in \beta$ sådana att $a \leqslant pq$. Eftersom α är ett snitt så vet vi att det finns ett $u \in \alpha$ sådant att $u > p$. Om vi sätter $r = au/p$ så är $r > a$ och

$$r = a\frac{u}{p} \leqslant pq\frac{u}{p} \leqslant uq. \tag{7.28}$$

Eftersom $u \in \alpha$ och $q \in \beta$ så är $r \in \alpha \cdot \beta$.

Övning 4.11. Vi verifierar egenskaperna (R1)–(R3) i Definition 4.2.1.

(R1) Mängden $\gamma \neq \emptyset$ eftersom A enligt antagande innehåller minst ett snitt. Eftersom A är uppåt begränsad så finns det ett snitt β sådant att $\alpha < \beta$ för alla $\alpha \in A$. Låt q vara övre begränsning till β. 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 4.13. Eftersom X är icke-tom finns det minst ett element $x \in X$. Då har vi att $(\alpha + x) \in \alpha + X$ och därmed är $\alpha + X$ icke-tom. Eftersom X är icke-tom och uppåt begränsad så existerar $\sup_{\mathbb{R}} X$. För varje $y \in \alpha + X$ finns

det $x \in X$ sådant att $y = \alpha + x$. Vi noterar nu att $x \leqslant \sup_{\mathbb{R}} X$ för alla $x \in X$ och därför har vi att

$$y = \alpha + x \leqslant \alpha + \sup_{\mathbb{R}} X. \tag{7.29}$$

Det visar att $\alpha + \sup_{\mathbb{R}} X$ är en övre begränsning till $\alpha + X$. Det kvarstår nu endast att visa att $\alpha + \sup_{\mathbb{R}} X$ är den minsta övre begränsningen till $\alpha + X$. Antag att β är en övre begränsning till $\alpha + X$. Det innebär att vi för varje $x \in X$ har att $\alpha + x \leqslant \beta$ vilket är ekvivalent med att $x \leqslant \beta - \alpha$. Eftersom x i den sista olikheten ovan är godtycklig, så är $\beta - \alpha$ en övre begränsning till X. Eftersom $\sup_{\mathbb{R}} X$ är den *minsta* övre begränsningen till X har vi därför att $\sup_{\mathbb{R}} X \leqslant \beta - \alpha$ vilket ger att $\alpha + \sup_{\mathbb{R}} X \leqslant \beta$. Det följer att $\alpha + \sup_{\mathbb{R}} X$ är den minsta övre begränsningen till $\alpha + X$.

Övning 5.1. Vi kommer att bevisa denna olikhet med ett motsägelsebevis. Vi antar därför att det finns ett heltal $k \geqslant 0$ sådant att olikheten $\alpha - e_k < \frac{1}{10^k}$ inte är uppfylld, det vill säga vi antar att $\alpha - e_k \geqslant \frac{1}{10^k}$, vilket är ekvivalent med att $e_k + \frac{1}{10^k} \leqslant \alpha$. Detta innebär att

$$a_0 + \cdots + \frac{a_k + 1}{10^k} \leqslant \alpha,$$

vilket är en motsägelse eftersom a_k per definition är det *största* heltalet sådant att

$$a_0 + \cdots + \frac{a_k}{10^k} \leqslant \alpha.$$

Därför måste vårt antagande att det fanns ett heltal $k \geqslant 0$ sådant att $\alpha - e_k \geqslant \frac{1}{10^k}$ vara falskt, det vill säga det måste vara sant att $\alpha - e_k < \frac{1}{10^k}$ för alla $k \geqslant 0$. Därmed är beviset klart.

Övning 5.3. Vi betraktar först det enklaste fallet, nämligen fall (ii). Låt $q = 0$. Då gäller det givetvis att $q \in \mathbb{Q}$ och att $\alpha < q < \beta$.

Vi betraktar nu istället fall (iii). Eftersom $\beta - \alpha > 0$, så har vi att

$$\alpha - \beta = -(\beta - \alpha) < 0.$$

Det följer att

$$-\beta < -\alpha.$$

Eftersom $\beta \leqslant 0$ så har vi även att $(-\beta) \geqslant 0$. Sammantaget har vi att

$$0 \leqslant -\beta < -\alpha.$$

Vi kan nu använda oss av att vi redan bevisat fall (i) i Sats 5.1.3. Vi vet nämligen att det finns ett $q \in \mathbb{Q}$ sådant att

$$-\beta < q < -\alpha.$$

Vi får således att

$$\alpha < -q < \beta.$$

Därmed är beviset klart även för fall (iii).

Övning 5.5. Med samma metod som i Exempel 5.6.2 får vi
$\alpha = [0{,}01101]_2 = 0 + \frac{0}{2} + \frac{1}{4} + \frac{1}{8} + \frac{0}{16} + \frac{1}{32} = \frac{13}{32}$. Vi kan således ta $n = 13$ och $m = 32$.

Övning 5.7. Vi noterar att

$$[0{,}1]_2 = \sup_{\mathbb{R}} \left\{ 0, \frac{1}{2} \right\} = \frac{1}{2}.$$

(Här är alltså $a_k = 0$ för $k \geqslant 2$.)
En binär utveckling av $\alpha = \frac{1}{2}$ ges därför av $[0{,}1]_2$.

Övning 6.1. Då graden av polynomet är 2 och rangen är 4 så har vi sambandet

$$4 = 2 + |a_0| + |a_1| + |a_2| \tag{7.30}$$

vilket ger

$$|a_0| + |a_1| + |a_2| = 2. \tag{7.31}$$

På hur många sätt kan vi välja tre tal större eller lika med noll, sådana att summan är två? Vi gör en liten tabell:

$\lvert a_0 \rvert$	$\lvert a_1 \rvert$	$\lvert a_2 \rvert$
2	0	0
0	2	0
0	0	2
0	1	1
1	0	1
1	1	0

Märk nu att detta är fallen för *beloppet* av koefficienterna. För det första fallet, till exempel, så kan vi välja koefficienterna på två sätt: $(a_0, a_1, a_2) = (2, 0, 0)$ och $(a_0, a_1, a_2) = (-2, 0, 0)$. Detsamma gäller för de följande två fallen. För fallet då $(|a_0|, |a_1|, |a_2|) = (0, 1, 1)$ kan vi faktiskt göra fyra val: $(0, 1, 1), (0, 1, -1), (0, -1, 1)$ och $(0, -1, -1)$. Totalt har vi alltså $3 \cdot 2 + 3 \cdot 4 = 18$ olika val. Resultatet är att det finns 18 polynom av grad 2 och rang 4.

Övning 6.3. Vi måste visa att det finns ett heltalspolynom $p(x)$ som uppfyller $p(\beta) = 0$. Låt $p(x) = x^2 - 2x - 1$. Då har vi

$$\begin{aligned} p(\beta) &= \beta^2 - 2\beta - 1 \\ &= (\sqrt{2} + 1)^2 - 2\sqrt{2} - 2 - 1 \\ &= 2 + 2\sqrt{2} + 1 - 2\sqrt{2} - 3 \\ &= 0. \end{aligned}$$

Därmed har vi per definition av $\mathbb{A}$ att $\beta \in \mathbb{A}$.

Övning 6.5. Antag att x och y är som i uppgiftens lydelse. Antag att $x \neq y$. Då gäller det att $x < y$ eller $y < x$. Låt oss anta att $x < y$. Övning 4.2 ger då att $x^2 < y^2$. Det är en motsägelse eftersom vi antog att $x^2 = 2 = y^2$. På samma sätt får vi en motsägelse om $y < x$. Därmed måste antagandet att $x \neq y$ vara falskt, vilket visar att $x = y$.

Övning 6.7. Eftersom $\mathbb{Q}$ är en uppräknelig mängd enligt Sats 3.2.9, kan det endast finnas uppräkneligt många rationella tal i mängden (α, β). Övning 6.6 visar å andra sidan att det öppna intervallet (α, β) är en överuppräknelig mängd. Därför måste det finnas ett irrationellt tal $\gamma \in (\alpha, \beta)$ (i själva verket visar detta att det måste finnas överuppräkneligt många irrationella tal i (α, β)). Per definition av (α, β) innebär det att $\alpha < \gamma < \beta$. Beviset är därmed klart.

Övning 6.9. Vi har att $N(1) = N(1 \cdot 1) = N(1)N(1)$ och eftersom $1 \neq 0$ så gäller att $N(1) \neq 0$. Vi kan därför dela med $N(1)$ och får därför $1 = N(1)$.

Övning 7.1. Sätt $z = a + bi, w = c + di$. Vi har då att

$$\begin{aligned}\overline{z} + \overline{w} &= \overline{a + bi} + \overline{c + di} = a - bi + c - di = a + c - (b + d)i \\ &= \overline{a + c + (b + d)i} = \overline{z + w}.\end{aligned}$$

För multiplikationen har vi

$$\begin{aligned}\overline{z} \cdot \overline{w} &= (a - bi)(c - di) = ac - bd - bci - adi = ac - bd - (bc + ad)i \\ &= \overline{ac - bd + (bc + ad)i} = \overline{(a + bi)(c + di)} = \overline{zw}.\end{aligned}$$

Övning 7.3. Enligt (7.10) har vi att $(0, 1, 0, 0)(0, 0, 1, 0) = (0, 0, 0, 1)$, men $(0, 0, 1, 0)(0, 1, 0, 0) = (0, 0, 0, -1) \neq (0, 0, 0, 1)$.

Övning 7.5. Multiplikation av två kvarternioner $w = w_0 + w_1 i + w_2 j + w_3 k$ och $z = z_0 + z_1 i + z_2 j + z_3 k$ ger via distributiva lagen upphov till produkterna

$$i^2, j^2, k^2, ij, ji, jk, kj, ik, ki. \tag{7.32}$$

Vi kan bestämma dessa från ekvationen

$$i^2 = j^2 = k^2 = ijk = -1. \tag{7.33}$$

De tre första produkterna i (7.32) är då $i^2 = j^2 = k^2 = -1$. Efter multiplikation med k från höger ger sista likheten i (7.33) att $-ij = -k$ så

$$ij = k.$$

Efter multiplikation med ji från vänster ger sista likheten i (7.33) att $ji(ijk) = -ji$. Men $ji(ijk) = j(ii)jk = -1(jj)k = k$. Så $-ji = k$ och därmed

$$ji = -k.$$

Multiplikation från vänster med i i sista likheten i (7.33) ger $i(ijk) = -i$ men $i(ijk) = (ii)(jk) = -jk$ så

$$jk = i.$$

Multiplikation med kj från höger i sista likheten i (7.33) ger att $ijk(kj) = -kj$ men $ijk(kj) = ij(kk)j = -ijj = i$, så

$$kj = -i.$$

Vi har redan visat att $ji = -k$. Detta ger att $jik = 1$ och därmed att $-ik = j$ så

$$ik = -j.$$

Sist har vi att $ijk = -1$ och därför $ji(ijk) = -ji$ och därför att $k = -ji$ och därför att

$$ki = j.$$

Då har vi bestämt alla produkter i (7.32) och kan därför multiplicera och förenkla alla produkter i (7.32)

$$\begin{aligned}
wz &= (w_0 + w_1 i + w_2 j + w_3 k)(z_0 + z_1 i + z_2 j + z_3 k) \\
&= (w_0 z_0 + w_0 z_1 i + w_0 z_2 j + w_0 z_3 k) \\
&\quad + (w_1 z_0 i + w_1 z_1 i^2 + w_1 z_2 ij + w_1 z_3 ik) \\
&\quad + (w_2 z_0 j + w_2 z_1 ji + w_2 z_2 j^2 + w_2 z_3 jk) \\
&\quad + (w_3 z_0 k + w_3 z_1 ki + w_3 z_2 kj + w_3 z_3 k^2) \\
&= (w_0 z_0 + w_0 z_1 i + w_0 z_2 j + w_0 z_3 k) \\
&\quad + (w_1 z_0 i - w_1 z_1 + w_1 z_2 k - w_1 z_3 j) \\
&\quad + (w_2 z_0 j - w_2 z_1 k - w_2 z_2 + w_2 z_3 i) \\
&\quad + (w_3 z_0 k + w_3 z_1 j - w_3 z_2 i - w_3 z_3).
\end{aligned}$$

Vi har nu endast kvar termer som antingen är reella eller endast har en förekomst av i, j eller k. Vi samlar ihop termerna ovan och får då att

$$\begin{aligned}
wz &= (w_0 z_0 - w_1 z_1 - w_2 z_2 - w_3 z_3) \\
&\quad + (w_0 z_1 i + w_1 z_0 i + w_2 z_3 i - w_3 z_2 i) \\
&\quad + (w_0 z_2 j - w_1 z_3 j + w_2 z_0 j + w_3 z_1 j) \\
&\quad + (w_0 z_3 k + w_1 z_2 k - w_2 z_1 k + w_3 z_0 k) \\
&= (w_0 z_0 - w_1 z_1 - w_2 z_2 - w_3 z_3) \\
&\quad + (w_0 z_1 + w_1 z_0 + w_2 z_3 - w_3 z_2) i \\
&\quad + (w_0 z_2 - w_1 z_3 + w_2 z_0 + w_3 z_1) j \\
&\quad + (w_0 z_3 + w_1 z_2 - w_2 z_1 + w_3 z_0) k \\
&= (w_0 z_0 - w_1 z_1 - w_2 z_2 - w_3 z_3, w_0 z_1 + w_1 z_0 + w_2 z_3 - w_3 z_2, \\
&\quad w_0 z_2 - w_1 z_3 + w_2 z_0 + w_3 z_1, w_0 z_3 + w_1 z_2 - w_2 z_1 + w_3 z_0),
\end{aligned}$$

där sista likheten kommer från identifikationen som infördes i övningen. En jämförelse visar att detta är samma multiplikation som i (7.10).

Övning 7.7. Vi måste visa att för alla $w \neq 0$ så är $w\overline{w}/|w|^2 = 1$, samt

$(\overline{w}/|w|^2)w = 1$. Enligt definitionen av multiplikation (7.10) har vi då

$$\begin{aligned}
w\overline{w}/|w|^2 &= (w_0, w_1, w_2, w_3)\frac{1}{w_0^2 + w_1^2 + w_2^2 + w_3^2}(w_0, -w_1, -w_2, -w_3) \\
&= \frac{1}{w_0^2 + w_1^2 + w_2^2 + w_3^2}(w_0, w_1, w_2, w_3)(w_0, -w_1, -w_2, -w_3) \\
&= \frac{1}{w_0^2 + w_1^2 + w_2^2 + w_3^2}(w_0w_0 + w_1w_1 + w_2w_2 + w_3w_3, \\
&\quad - w_0w_1 + w_1w_0 - w_2w_3 + w_3w_2, -w_0w_2 + w_1w_3 + w_2w_0 - w_3w_1, \\
&\quad - w_0w_3 - w_1w_2 + w_2w_1 + w_3w_0) \\
&= \frac{1}{w_0^2 + w_1^2 + w_2^2 + w_3^2}(w_0^2 + w_1^2 + w_2^2 + w_3^2, 0, 0, 0) \\
&= (1, 0, 0, 0) = 1.
\end{aligned}$$

Notera att vi använde Övning 7.6 i andra likheten, det vill säga vi använde att

$$\frac{1}{w_0^2 + w_1^2 + w_2^2 + w_3^2} \in \mathbb{R}$$

kommuterar med alla $w \in \mathbb{H}$. Uttrycket efter tredje likheten ovan är lika med $(\overline{w}/|w|^2)w$, vilket visar att vi även har $(\overline{w}/|w|^2)w = 1$.

A Träning i bevisföring

Då man i gymnasiet inte är van vid att göra bevis och liknande övningar som de vi ger i detta kompendium så har vi lagt med detta avsnitt som en träning i hur man kan tänka.

En av de viktigaste lärdomarna man ska ta med sig härifrån är att när man ställs inför ett problem så är den första frågan man ska ställa sig:

"Vad är definitionerna av objekten som ingår i frågan?"

Nedan ger vi några mer specifika tips på olika bevismetoder.

A.1 Tekniker i mängdlära

Ska man visa någonting om mängder är följande tips användbara. Här är A och B godtyckliga mängder, och x ett godtyckligt element.

(i) Visa att $x \in A$.

Här ska man alltså visa att x uppfyller de villkor som definierar vilka element som tillhör mängden A. Om exempelvis $A = \{1, 2, 3\}$ är det uppenbart att $2 \in A$, men om $A = \{x \mid \text{villkor på } x\}$ så måste man visa att x uppfyller de nämnda villkoren. Om $A = B \cap C$ så måste man visa att $x \in B$ och $x \in C$, medan om $A = B \cup C$ så räcker det att visa att $x \in B$ eller $x \in C$ (eller båda).

(ii) Visa att $A \subseteq B$.

Tag ett godtyckligt element $x \in A$. Använd nu definitionen för mängden A för att skriva ner vilka villkor som finns på x. Visa sedan att detta medför att $x \in B$. Eftersom x var godtyckligt så betyder detta att alla element i A även ligger i B, det vill säga att $A \subseteq B$.

(iii) Visa att $A = B$.

Visa först att $A \subseteq B$ och sedan att $B \subseteq A$. Då har vi visat att alla element i A ligger i B och att alla element i B ligger i A. Det måste betyda att $A = B$.

(iv) Visa att $A = \emptyset$.

Minns att $\emptyset$ betecknar den tomma mängden, det vill säga en mängd som inte innehåller några element alls. Det som ska visas är alltså att det inte kan finnas några element i A.

Antag till att börja med att $x \in A$. Använd definitionen av A för att skriva ner vilka villkor som då ställs på x. Visa att dessa villkor är omöjliga (att de leder till en motsägelse). Alltså kan det inte vara så att $x \in A$, oavsett vilket x vi väljer, så A innehåller inga element.

Exempel A.1.1. Låt A vara en mängd och låt B vara en delmängd av en annan mängd C. Visa att $A \cap B \subseteq C$.

Lösning. Vi vill här visa att en mängd är en delmängd av en annan mängd så vi använder tips (ii) ovan. Tag ett godtyckligt $x \in A \cap B$. Definitionen av snitt av mängder (Definition 1.1.5) säger att $A \cap B$ består av de element som ligger i både A och B. Speciellt gäller att alla element i $A \cap B$ ligger i B, så det följer att $x \in B$. Då B är en delmängd av C gäller enligt definitionen för delmängd (Definition 1.1.2) att alla element i B även ligger i C. Speciellt måste då $x \in C$. Alltså, om $x \in A \cap B$ så gäller att $x \in C$. Eftersom x var godtycklig så har vi visat att $A \cap B \subseteq C$. □

Exempel A.1.2. Låt $A = \{x \in \mathbb{R} \mid x > 3\}$ och låt $B = \{x \in \mathbb{R} \mid x^2 - 1 = 0\}$. Visa att $A \cap B = \emptyset$.

Lösning. Här använder vi tips (iv). Tag ett $x \in A \cap B$. Definitionen av snittet säger då att $x \in A$ och att $x \in B$. Att $x \in B$ betyder att x uppfyller $x^2 - 1 = 0$ vilket endast är sant om $x = \pm 1$. Eftersom både 1 och -1 är mindre än 3 så kan inte $x \in A$, vilket betyder att x inte ligger i $A \cap B$. Eftersom x var godtycklig följer det att $A \cap B = \emptyset$. □

A.2 Tekniker i logik och bevisföring

Här ger vi tips på tekniker för att visa saker i logik. Vi skriver P och Q för två godtyckliga påståenden.

(i) Visa att $P \implies Q$.

Anta att P är sann. Om vi från detta kan skapa en följd av implikationer som visar att Q är sann så är vi klara.

(ii) Visa att $P \iff Q$.

Här ska vi visa att påståendena P och Q är ekvivalenta. Detta görs genom att visa att både $P \implies Q$ och $Q \implies P$.

(iii) Visa att P är falskt.

En teknik för att visa att ett påstående är falskt är att anta motsatsen och visa att detta skapar en motsägelse. Med andra ord antar vi att påståendet P är sant och visar att detta implicerar ett påstående Q som vi vet är falskt såsom $1 = 0$. Vi kan då dra slutledningen att antagandet att P är sant inte kan stämma så P måste vara falskt.

Exempel A.2.1. Visa att om n är ett jämnt heltal så är $n^2 + 1$ udda.

Lösning. Vi börjar med att fråga oss vad definitionen för udda och jämna tal är. (*Författarna: Eftersom vi inte gett någon definition för detta tidigare i kompendiet ger vi en här*).

Definition A.2.2. Ett tal $n \in \mathbb{Z}$ är *jämnt* om det finns ett $m \in \mathbb{Z}$ så att $n = 2m$. Vi kallar n *udda* om det finns ett $m \in \mathbb{Z}$ så att $n = 2m + 1$.

Lösning (forts.) Nu när vi vet definitionerna så kan vi börja lösa uppgiften. Vi vill alltså visa påståendet "n är jämnt" implicerar påståendet "$n^2 + 1$ är udda". Detta gör vi genom att använda teknik (i) ovan. Antag att n är jämnt. Då finns per definition ett heltal m så att $n = 2m$. Det följer därmed att $n^2 = 4m^2$ så $n^2 + 1 = 4m^2 + 1 = 2 \cdot (2m^2) + 1$. Eftersom $k = 2m^2$ är ett heltal ser vi att $n^2 = 2k + 1$ med $k \in \mathbb{Z}$. Alltså är $n^2 + 1$ udda om n är jämnt. □

B Naturliga talen

I kapitel två visade vi hur man kan konstruera heltalen från de naturliga talen, men vi tog existensen av de naturliga talen for givet. Vi kommer här visa hur man kan konstruera de naturliga talen direkt ur mängdläran.

År 1889 publicerade den italienska matematikern Giuseppe Peano en samling axiom, (P1)-(P5), som skulle formalisera de naturliga talens fundamentala egenskaper:

(P1) 0 är ett naturligt tal.

(P2) För varje naturligt tal a är a's efterföljare $S(a)$ ett naturligt tal.

(P3) 0 är inte efterföljare till något tal.

(P4) Två olika tal har aldrig samma efterföljare.

(P5) Om P är en egenskap sådan att 0 har denna egenskap, och om det att ett tal n har egenskapen P medför att efterföljaren $S(n)$ har egenskapen P, så har varje tal egenskapen P (induktionsaxiomet).

De första fyra axiomen bör kännas naturliga för läsaren. Efterföljaren $S(0)$ skrivs oftast med tecknet "1" och är såklart inte efterföljare till något annat tal än just 0. Men vilken egenskap är det som det femte axiomet formaliserar? Säg att vi har en matematisk egenskap P, och vi har lyckats verifiera att 0 har egenskapen, vilket vi skriver som $P(0)$. Om P nu har den egenskapen att $P(n)$ medför att även $P(S(n))$ då kan vi nu dra slutsatsen att $P(1)$, ty $S(0) = 1$. Men då kan vi upprepa resonemanget och dra slutsatsen att $P(2)$, och därmed även $P(3)$, och så vidare. Vi kan upprepa resonemanget så många gånger vi har lust – i den matematiska världen finns ingen tidsbegränsning – så vi drar slutsatsen att P måste vara sant för varje efterföljare till 0. Axiom (5) säger att P måste gälla för varje naturligt tal, så det formaliserar intuitionen att de naturliga talen just är de elementen som uppstår som efterföljare till 0, det vill säga $S(0), S(S(0)), \ldots$

Vår uppgift är således att konstruera en mängd med element som uppfyller ovanstående axiom, särskilt måste vi konstruera ett objekt som vi kallar 0 samt definiera vad vi menar med $S(n)$ givet n.

B.1 Konstruktionen

Från och med nu tar vi inte existensen av tal som matematiska objekt för givet, utan det är vår uppgift att konstruera dem ur mängdläran. Vi börjar således helt från grunden, där det enda som vi antar existerar är den tomma mängden Ø samt mängdoperationerna som behandlades i kapitel 1.

Vilka objekt inom mängdläran finns det då som kan motsvara tal? Naturliga talen är ju de tal som vi räknar antal med, så informellt skulle vi vilja att ett naturligt tal, säg 3, representerar alla mängder med exakt 3 element, till exempel genom att sätta $3 = \{A : A \text{ har 3 element}\}$ och detta är även den första moderna definitionen av naturliga tal som gavs av den tyska logikern Gottlobb Frege på 1870-talet. Denna definition har vissa tekniska brister som gör att den inte fungerar i modern axiomatisk mängdlära[20], och vi kommer istället att presentera en konstruktion som först föreslogs av den ungersk-amerikanska matematikern John von Neumann.

Ett av axiomen för mängdläran är existensen av den tomma mängden $\emptyset = \{\}$, det vill säga mängden som inte har några element. Läsaren bör observera att detta även är den enda konkreta mängden vi i nuläget känner till: alla de andra exempel på mängder i Kapitel 1 förutsätter existensen av de naturliga talen, men de har vi ju ännu inte konstruerat. Eftersom antalet element i tomma mängden är noll, så är det intuitivt att definiera tecknet 0 genom att sätta $0 = \emptyset = \{\}$. Vi vill nu bilda talet 1. En vettig kandidat är en mängd med just ett element, och ett naturligt val är att sätta $1 = \{\emptyset\} = \{\{\}\}$, det vill säga mängden som endast innehåller tomma mängden (notera att $\{\emptyset\} \neq \emptyset$: en påse som innehåller en tom påse är inte tom!). Nu har vi två objekt att jobba med, nämligen objekten 0 och 1, och vi sätter därför $2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\} = \{\{\}, \{\{\}\}\}$. Metoden är nu klar, ty i allmänhet definierar vi $n + 1 = n \cup \{n\}$, för n är en mängd som innehåller n stycken objekt, så $n \cup \{n\}$ måste innehålla $n + 1$ stycken objekt. Vi är nu redo för vår första definition i detta kapitel:

Definition B.1.1. Givet ett tal naturligt tal n definieras n's *efterföljare* $S(n)$ genom att sätta $S(n) = n \cup \{n\}$, vi skriver även $n + 1 = S(n)$. En mängd A sägs vara *sluten* under S om det för varje element $n \in A$ gäller att $S(n) \in A$.

Givet n är $S(n)$ således den mängden som innehåller alla element i n samt även innehåller n som ett element!

Definition B.1.2. De *naturliga talen* $\mathbb{N}$ är den minsta mängden som innehåller $0 = \emptyset$ och som är sluten under S.[21]

Anmärkning B.1.3. Med 'minsta' menas att om A är en annan mängd som uppfyller $0 \in A$ och A är sluten under S, så gäller det att $\mathbb{N} \subset A$. Kravet att $\mathbb{N}$ är den *minsta* mängden som innehåller 0 och är sluten under S säkerställer att inga andra element än de icke-negativa heltalen som bildas av den ovan beskrivna metoden finns i $\mathbb{N}$. Vi ber även läsaren observera att även fast $\emptyset \subset A$

[20] En presentation av ett axiomatisk fundament för mängdläran ryms tyvärr inte inom detta kompendium, utan vi nöjer oss med den beskrivning som ges i Kapitel 1.

[21] Existensen av denna oändliga mängd är ett axiom i mängdläran.

för varje mängd A, så är det ej sant att $\emptyset \in A$ för varje mängd A – exempelvis gäller att $\emptyset \notin \emptyset$.

Vi kan nu verifiera att mängden $\mathbb{N}$ uppfyller axiomen (1)-(4). Vi har per konstruktion att $0 = \{\emptyset\} \in \mathbb{N}$, och per definition är $\mathbb{N}$ sluten under S, så Axiom (2) är uppfyllt. 0 är inte efterföljare till något tal, ty $S(n) \neq \emptyset = 0$, per definition av S. Att visa att $n \neq m$ medför $S(n) \neq S(m)$ lämnas som en (svår) övning åt läsaren.

Axiom (5) är uppfyllt på grund av av kravet $\mathbb{N}$ är den minsta mängden som innehåller 0 och är sluten under S, ty om 0 har en egenskap P och det att n har egenskapen P medför att $S(n)$ har egenskapen P, då är mängden

$$\{m \in \mathbb{N} \mid m \text{ uppfyller } P\}$$

en delmängd av $\mathbb{N}$ som innehåller 0 och är sluten under S. Men eftersom $\mathbb{N}$ är den minsta mängden som uppfyller det villkoret så måste

$$\mathbb{N} = \{n \in \mathbb{N} \mid m \text{ uppfyller } P\}.$$

Vi har således lyckats med att konstruera en konkret mängd $\mathbb{N}$ som har de grundläggande egenskaper som de naturliga talen bör ha, det vill säga axiom (1)-(5). Vi inför nu additionen på mängden genom följande *rekursiva definition*.

Definition B.1.4. Givet två element $a, b \in \mathbb{N}$ definieras summan $a + b$ enligt följande

$$a + 0 = a \tag{B.1}$$
$$a + S(b) = S(a + b). \tag{B.2}$$

Exempel B.1.5. Enligt Definition B.1.4 har vi att $1 + 1 = 1 + S(0) = S(1 + 0) = S(1) = 1 \cup \{1\} = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\} = 2$. ▲

Exempel B.1.6. Att definitionen är rekursiv betyder att ett givet steg är definierat via tidigare steg. För att räkna ut exempelvis vad $a+2 = a+S(1) = S(a+1)$ är, är vi tvungna att bestämma $a+1$. Men $a+1 = a+S(0) = S(a+0)$ så vi måste bestämma $a+0$. Detta är dock det "första steget" och är definierat som a. Då har vi att $a + 1 = S(a + 0) = S(a)$. Således har vi att $a + 2 = S(a + 1) = S(S(a))$, så addition med 2 motsvarar att gå två steg fram i naturliga talen, ett resultat som kanske inte överraskar läsaren, men indikerar att vår definition av addition motsvarar den vanliga additionen som alla är förtrogna med. ▲

Anmärkning B.1.7. Elementen a, b är mängder, men notera att i kapitel 1 definierades det inte en operation "+" för mängder. Unionen $\cup$ av två mängder definierades där, men den sammanfaller inte med + i definition B.1.4. Exempelvis så är $a \cup a = a$ för alla mängder a, medan $a + a \neq a$, för alla nollskillda element $a \in \mathbb{N}$.

Definition B.1.8. Givet två element $a, b \in \mathbb{N}$ definieras produkten $a \cdot b$ (vi skriver även ab) genom att sätta

$$a \cdot 0 = 0 \tag{B.3}$$
$$a \cdot S(b) = a + a \cdot b. \tag{B.4}$$

Exempel B.1.9. Enligt Definition B.1.8 har vi att

$$a \cdot 1 = a \cdot S(1) = a + a \cdot 0 = a + 0 = a,$$

för varje $a \in \mathbb{N}$, där vi använde (B.3) i näst sista steget och (B.1) i sista steget. ▲

Vi har följande uppsättning räknelagar.

Sats B.1.10 (Räknelagar för $\mathbb{N}$)**.** *För alla $a, b, c \in \mathbb{N}$ gäller det att*

$$\begin{aligned} a + b &= b + a, \textit{ kommutativa lagen för addition} \\ (a + b) + c &= a + (b + c), \textit{ associativa lagen för addition} \\ a \cdot b &= b \cdot a, \textit{ kommutativa lagen för multiplikation} \\ a \cdot (b \cdot c) &= (a \cdot b) \cdot c, \textit{ associativa lagen för multiplikation} \\ a \cdot (b + c) &= (a \cdot b) + (a \cdot c), \textit{ distributiva lagen.} \end{aligned}$$

Bevis. Bevisen bygger på induktion, det vill säga vi kommer använda oss av axiom (5). Vi visar associativa lagen för addition och lämnar resten som frivillig övning åt läsaren. Välj två godtyckliga $a, b \in \mathbb{N}$. Enligt (B.1) så får vi att

$$(a + b) + 0 = a + (b + 0). \tag{B.5}$$

Detta är egenskapen $P(0)$: att $a, b, 0$ bildar en associativ trippel som i (B.5). Vi visar nu att om det för ett givet c gäller att $P(c)$, då följer det att $P(S(c))$. Så antag att $P(c)$, det vill säga att $(a + b) + c = a + (b + c)$ gäller för något $c \in \mathbb{N}$. Vi måste visa att $(a + b) + S(c) = a + (b + S(c))$, det vill säga $P(S(c))$. Men vi har att

$$(a+b)+S(c) = S((a+b)+c) = S(a+(b+c)) = a+S(b+c) = a+(b+S(c)),$$

där (B.4) användes i första, tredje och fjärde likheten, och antagandet $(a + b) + c = a + (b + c)$ användes i andra likheten. Enligt induktionsaxiomet måste det då för a, b gälla att $(a + b) + c = a + (b + c)$ för alla $c \in \mathbb{N}$ och eftersom a, b var godtyckliga gäller det för alla $a, b, c \in \mathbb{N}$. □

Vi kan nu lämna den ganska otympliga mängdnotationen ovan och helt enkelt skriva $0, 1, 2, \ldots$. Ovanstående genomgång visar att de naturliga talen *går* att konstruera ur mängdläran så att Peano axiomen och räknelagarna är giltiga. Exakt vilken mängd ett givet tal n är har liten betydelse för oss i detta kompendium.

C Definitioner av delkropp, homomorfi och isomorfi

Låt K_1 och K_2 vara två kroppar, med räkneoperationer $+_1, \cdot_1$ respektive $+_2, \cdot_2$. K_1 sägs vara en delkropp till K_2 om varje $\alpha \in K_1$ kan tillordnas ett unikt $\beta_\alpha \in K_2$, så att additiva och multiplikativa enhetselement tillordnas varandra, och så att räkneoperationerna är bevarade:

$$\beta_{\alpha_1 +_1 \alpha_2} = \beta_{\alpha_1} +_2 \beta_{\alpha_2}$$

och

$$\beta_{\alpha_1 \cdot_1 \alpha_2} = \beta_{\alpha_1} \cdot_2 \beta_{\alpha_2}.$$

Mera exakt så kan vi definiera

Definition C.0.11. Låt K_i vara kroppar med räkneoperationer $+_i, \cdot_i$, enhetselement $0_i, 1_i$ och ordningar $<_i$ för $i = 1, 2$. K_1 är en *delkropp* till K_2 om det finns en funktion $f : K_1 \to K_2$, så att följande gäller för alla $x, y \in K_1$

(i) $x \neq y$ medför $f(x) \neq f(y)$ (unik tillordning),

(ii) $\begin{cases} f(x +_1 y) = f(x) +_2 f(y) \\ f(x \cdot_1 y) = f(x) \cdot_2 f(y) \end{cases}$ (kompatibla räkneoperationer),

(iii) $f(0_1) = 0_2, \quad f(1_1) = 1_2,$ (enhetselement bevaras).

K_1 är en ordnad delkropp av K_2 om även följande villkor gäller för alla $x, y \in K_1$

(iv) $x <_1 y$ medför att $f(x) <_2 f(y)$.

En funktion $f : K_1 \to K_2$ som uppfyller villkoren (ii) och (iii) ovan kallas för en *homomorfi* av kroppar. En homomorfi av kroppar som även uppfyller villkoret (iv) kallas för en homomorfi av ordnade kroppar. Homomorfi är ett modernt ord bildat ur grekiska *homo* som betyder samma, och *morfe* som betyder form eller utseende.

Definition C.0.12. Två (ordnade) kroppar K_1 och K_2 är *isomorfa* om det existerar en homomorfi $f : K_1 \to K_2$ av (ordnade) kroppar, så att f som funktion är en bijektion mellan K_1 och K_2 (se Definition 3.1.5). En sådan funktion f kallas för en isomorfi av (ordnade) kroppar.

D Det finns bara en ordnad kropp med supremumegenskapen

I detta avsnitt ska vi *skissa* ett bevis följande Sats. [22]

Sats D.0.13. *Alla ordnade kroppar med supremumegenskapen är isomorfa*[23].

[22] Läsare som är intresserade av att se ett fullständigt bevis kan finna ett sådant exempelvis i läroboken *Calculus* av Michael Spivak.

[23] Se appendix C för en definition av begreppet isomorfi.

Innan vi börjar med bevisskissen är följande anmärkning på sin plats:

Anmärkning D.0.14. Tidigare i detta kompendium har vi nämnt att det finns flera sätt att *konstruera* de reella talen. Kanske undrar läsaren hur detta kan vara förenligt med påståendet i rubriken till detta avsnitt. Poängen är att det räcker med att visa att alla ordnade kroppar med supremumegenskapen är isomorfa, ty det innebär att de delar alla "intressanta" egenskaper med varandra. Det är i denna bemärkelse det endast finns en ordnad kropp med supremumegenskapen.

Skiss av ett bevis av Sats D.0.13. Låt K vara en ordnad kropp med supremumegenskapen. Vårt mål är att konstruera en funktion $f : \mathbb{R} \to K$ som är en isomorfi av ordande kroppar.

Låt $+_K$ och $\cdot_K$ beteckna operationerna i K, låt $<_K$ beteckna ordningen i K samt låt 0_K och 1_K beteckna enhetselementen i K.

Till att börja med definierar vi $f(0) = 0_K$ och $f(1) = 1_K$. Vidare definierar vi för varje heltal $n > 0$

$$f(n) = \underbrace{1_K + 1_K + \cdots + 1_K}_{\text{n termer}} \tag{D.1}$$

samt $f(-n) = -f(n)$.

Definitionen ovan kan på ett naturligt sett utvidgas till de rationella talen genom att för alla $n, m \in \mathbb{Z}$, $m \neq 0$ göra definitionen

$$f\left(\frac{n}{m}\right) = f(n) \cdot_K f(m)^{-1} \tag{D.2}$$

Anmärkning D.0.15. Här behöver man visa att f är väldefinierad, det vill säga att $f\left(\frac{n}{m}\right) = f\left(\frac{s}{t}\right)$ om $\frac{n}{m} = \frac{s}{t}$.

Slutligen definierar vi f på hela $\mathbb{R}$ genom

$$f(x) = \sup_K \{f(q) \mid q \in \mathbb{Q},\ q < x\} \tag{D.3}$$

Anmärkning D.0.16. Det är inte särskilt svårt att visa att mängden $\{f(q) \mid q \in \mathbb{Q},\ q < x\}$ är en icketom och uppåt begränsad delmängd av K. Eftersom K är en ordnad kropp med supremumegenskapen har denna mängd därför ett (unikt) supremum i K.

Anmärkning D.0.17. Man kan visa att definitionerna (D.2) och (D.3) överensstämmer i det fall då $x \in \mathbb{Q}$.

Nu är definitionen av f färdig, men det kvarstår att visa att f är en isomorfi mellan de ordnade kropparna $\mathbb{R}$ och K. Den grundläggande idén för att vissa detta är att först visa att villkoren (ii) och (iv) i Definition C.0.11 är uppfylla då $x, y \in \mathbb{Q}$ och med hjälp av detta visa att dessa villkor även gäller för godtyckliga $x, y \in \mathbb{R}$. Slutligen kan även visa att f är en bijektion.

□

E Geometrisk summa

Låt $a \in \mathbb{R}$ med $|a| < 1$ och betrakta talföljden $a, a^2, a^3, \ldots$. Det är inte svårt att visa – och ganska intuitivt – att $\lim_{n\to\infty} a^n = 0$. Den ändliga summan

$$s_n = 1 + a + a^2 + \ldots + a^n$$

kallas för en *geometrisk summa*. Med *summasymbolen* Σ kan vi skriva detta som

$$\sum_{i=0}^{n} a^i = 1 + a + a^2 + \ldots + a^n.$$

Notationen betyder att vi tar summan av alla termer a^i för alla heltal i från 0 till n. Symbolen Σ är ursprungligen en grekisk bokstav som uttalas "sigma".

Notera nu att $as_n = a + a^2 + \ldots + a^{n+1}$. Därmed gäller att

$$s_n - as_n = (1 + a + a^2 + \ldots + a^n) - (a + a^2 + \ldots + a^n + a^{n+1}) = 1 - a^{n+1}.$$

Eftersom vi kan skriva $s_n - as_n = (1 - a)s_n$ har vi att $(1 - a)s_n = 1 - a^{n+1}$. Då $a \neq 1$, och därmed $1 - a \neq 0$, kan vi dividera båda sidorna med $1 - a$ och få följande formel för den geometriska summan:

$$\sum_{i=0}^{n} a^i = s_n = \frac{1 - a^{n+1}}{1 - a}.$$

F Några bevis av satser från Kapitel 4

Bevis av (A4),(A5) och (O1) i Hjälpsats 4.3.5.

(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 α och att varje element i α 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 β 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 α, eftersom $-q > -q - r$. Alltså har vi att $p < -q$ eftersom α 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 det klart att $w > 0$. Eftersom w är ett positivt rationellt tal och α 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

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

Vi ser vidare att

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

Eftersom v var ett godtyckligt 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 $\alpha + \beta < \alpha + \gamma$, det vill säga $\alpha + \beta \subseteq \alpha + \gamma$ 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 $\alpha + \beta \neq \alpha + \gamma$. □

Bevis av (M5) och (D) i Hjälpsats 4.3.9.

(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, det vill säga genom att visa de två inklusionerna $\alpha \cdot \alpha^{-1} \subseteq 1$ och $1 \subseteq \alpha \cdot \alpha^{-1}$. Att bevisa att α^{-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 $q \in \alpha^{-1}$, det vill säga $\alpha \cdot \alpha^{-1} \subseteq 1$.

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 $\frac{1}{z} > 1$. Låt oss först anta att $\frac{1}{z} \in \alpha$. Eftersom $\frac{1}{z} > 1$ och α är uppåt begränsad så måste (se Anmärkning F.0.18) det finnas ett positivt heltal k sådant att

$$x = \left(\frac{1}{z}\right)^k \in \alpha \qquad \text{och} \qquad y = \left(\frac{1}{z}\right)^{k+1} \notin \alpha. \tag{F.3}$$

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

$$z = \frac{z^{k+1}}{z^k} = \frac{\frac{1}{z^k}}{\frac{1}{z^{k+1}}} = x\frac{1}{y}. \tag{F.4}$$

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

$$x'\frac{1}{y'} = \frac{x'x}{yx'} = \frac{x}{y} = z. \tag{F.5}$$

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

$$x = z^{k+1} \in \alpha \qquad \text{och} \qquad y = z^k \notin \alpha. \tag{F.6}$$

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 α. Låt oss anta att detta är avklarat och att $\frac{1}{y} \in \alpha^{-1}$. Vi får

$$z = \frac{z^{k+1}}{z^k} = \frac{x}{y} = x \cdot \frac{1}{y}. \tag{F.7}$$

Då $x \in \alpha$ och $\frac{1}{y} \in \alpha^{-1}$ 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 α, β, γ så gäller det att $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$. Vi gör detta genom att bevisa de två inklusionerna

$$\alpha(\beta + \gamma) \subseteq \alpha\beta + \alpha\gamma \qquad \text{och} \qquad \alpha\beta + \alpha\gamma \subseteq \alpha(\beta + \gamma). \tag{F.8}$$

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

$$r = x(y + z) \tag{F.9}$$

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

$$r = x_1 y + x_2 z \tag{F.10}$$

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

$$\frac{x_1}{x_2} y \leqslant y \quad \text{vilket medför att} \quad \frac{x_1}{x_2} y \in \beta. \tag{F.11}$$

Vi kan skriva r som

$$r = x_1 y + x_2 z = x_2 \left(\frac{x_1}{x_2} y + z \right). \tag{F.12}$$

Eftersom $x_2 \in \alpha, x_1 \frac{y}{x_2} \in \beta$ 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

$$\alpha(\beta + \gamma) = -\alpha\big[-(\beta + \gamma)\big] = -\Big[\alpha(-\beta - \gamma)\Big]. \tag{F.13}$$

Nu är alla tre snitt, det vill säga $\alpha, -\beta, -\gamma$, positiva och vi kan använda resultatet för positiva snitt för att erhålla

$$\alpha(\beta + \gamma) = -\Big[\alpha(-\beta - \gamma)\Big] = -\Big[-\alpha\beta - \alpha\gamma\Big] = \alpha\beta + \alpha\gamma. \tag{F.14}$$

(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

$$\alpha\gamma = \alpha\Big[(\beta + \gamma) + (-\beta)\Big]. \tag{F.15}$$

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

$$\alpha\gamma = \alpha\Big[(\beta + \gamma) + (-\beta)\Big] = \alpha(\beta + \gamma) - \alpha\beta \tag{F.16}$$

vilket medför att

$$\alpha\gamma + \alpha\beta = \alpha(\beta + \gamma). \tag{F.17}$$

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

$$-\alpha\beta = \alpha\Big[-(\beta + \gamma) + \gamma\Big]. \tag{F.18}$$

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

$$-\alpha\beta = \alpha\Big[-(\beta + \gamma) + \gamma\Big] = -\alpha(\beta + \gamma) + \alpha\gamma \tag{F.19}$$

vilket medför att

$$\alpha(\beta + \gamma) = \alpha\gamma + \alpha\beta. \tag{F.20}$$

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

Anmärkning F.0.18. Antag att $q > 1$ är rationellt. För varje positivt heltal n gäller att

$$\begin{aligned} q^n &= \Big(1 + (q-1)\Big)^n \\ &= 1 + n(q-1) + \frac{n(n-1)}{2}(q-1)^2 + \cdots + (q-1)^n \\ &\geqslant 1 + n(q-1). \end{aligned} \tag{F.21}$$

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.

Bevis av påståendena (i),(iii) och (iv) i Hjälpsats 4.3.11.

Bevis av ekvation (iv):
Antag att $p < r$. Tag $q \in \alpha_p$. Då är $q < p < r$, så $q \in \alpha_r$. Därmed är det klart att $\alpha_p \subseteq \alpha_r$. Det kvarstår att visa att $\alpha_p \neq \alpha_r$. Detta följer från att $p \notin \alpha_p$, men $p \in \alpha_r$.

Bevis av ekvation (iii):
Vi betraktar endast fallet $p, r > 0$ och lämnar de övriga fallen till läsaren att visa. Ekvation (iv) som vi nyss bevisat medför att $p, r > 0$ ger att $\alpha_p, \alpha_r > 0$. Tag $q \in \alpha_p \cdot \alpha_r$. Då har vi att det finns $0 < p', r'$ sådana att $p' < p, r' < r$ och $q \leqslant p' \cdot r'$. Det ger att $q \leqslant p' \cdot r' < pr$ och därmed att $q \in \alpha_{p \cdot r}$. Tag nu $q \in \alpha_{p \cdot r}$. Om $q \leqslant 0$ så är inte svårt att se att $q \in \alpha_{p \cdot r}$. Vi antar därför att $q > 0$. Då är $q < p \cdot r$, vilket ger att $\frac{q}{p \cdot r} < 1$. Tag nu $a \in \mathbb{Q}$ sådant $\frac{q}{p \cdot r} < a < 1$ och låt $b = \frac{q}{a \cdot p \cdot r}$. Vi noterar att $0 < b < 1$. Vi har att $\frac{q}{p \cdot r} = a \cdot b$ och därmed att $q = (a \cdot p) \cdot (b \cdot r)$. Eftersom $0 < a \cdot p < p$ och $0 < b \cdot r < r$ har vi därför att $q \in \alpha_p \cdot \alpha_r$. Vi har bevisat inklusionerna $\alpha_p \cdot \alpha_r \subseteq \alpha_{p \cdot r}$ och $\alpha_{p \cdot r} \subseteq \alpha_p \cdot \alpha_r$. Därmed följer ekvation (iii).

Bevis av ekvation (i):
Antag att $p \neq r$. Då gäller det att $p < r$ eller $r < p$. Om $p < r$ har vi att $\alpha_p < \alpha_p$ och om $r < p$ har vi att $\alpha_r < \alpha_p$. I båda fallen är alltså $\alpha_p \neq \alpha_r$.

□

Sakregister