Kapitel 10

TALBEGREPPET *

Vi har redan mött olika typer av tal: naturliga, hela, rationella, reella och komplexa, betecknade med $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ resp. $\mathbb{C}$. Vad är det som skiljer olika talmängder? Finns det andra typer av tal? Vad menas egentligen med ett tal? Vi skall försöka svara på dessa frågor genom att analysera olika egenskaper hos olika talmängder. Men svaren är inte alltid enkla, och riktigt tillfredsställande svar kräver ibland djupare kunskaper som först är tillgängliga i senare kurser.

Vi har $\mathbb{N} = \{0, 1, 2, 3, ...\}$, $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, ...\}$, $\mathbb{Q} = \{\frac{m}{n} : m, n \in \mathbb{Z},\ n \neq 0\}$. Det är inte lika lätt att beskriva alla reella och komplexa tal. Vi skall försöka göra det i detta avsnitt och visa hur och varför man definierar olika typer av tal.

Alla tal kan adderas och multipliceras. Detta betyder att om a och b är två tal så kan man bilda deras summa $a + b$ och deras produkt ab. Det är mycket viktigt att om X betecknar något av talområdena ovan så

$$a, b \in X \Rightarrow a + b,\ ab \in X, \tag{1}$$

dvs summa och produkt av två tal av samma typ är av samma typ. Hur är det med de två andra räknesätten – subtraktion och division? Om man kräver att

$$a, b \in X \Rightarrow a - b \in X, \tag{2}$$

så är det inte möjligt att välja $X = \mathbb{N}$, ty trots att t ex $2, 3 \in \mathbb{N}$ så $2 - 3 = -1 \notin \mathbb{N}$. Däremot kan X vara lika med $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Hur är det med

$$a, b \in X \Rightarrow \frac{a}{b} \in X? \tag{3}$$

*LMA100, ht 02

Först och främst måste man tillägga att $b \neq 0$ (varför?). Det är klart att $\mathbb{N}$ och $\mathbb{Z}$ saknar egenskapen (3) ty t ex $2, 3 \in \mathbb{Z}$, men $\frac{2}{3} \notin \mathbb{Z}$. De andra talområdena $\mathbb{Q}$, $\mathbb{R}$ och $\mathbb{C}$ uppfyller villkoret (3) (med $b \neq 0$). Man säger att $\mathbb{Q}$, $\mathbb{R}$ och $\mathbb{C}$ är slutna med avseende på de fyra räknesätten. $\mathbb{Z}$ är inte sluten med avseende på division, och $\mathbb{N}$ är inte sluten med avseende på subtraktion eller division. Det visar sig att just slutenheten med avseende på olika operationer (här de fyra räknesätten) har en stor betydelse när det gäller skillnader mellan olika talområden. Av den anledningen har man infört följande begrepp:

(10.1) Definition. Man säger att en talmängd K är en **talkropp** om $1 \in K$ och K är sluten m a p de fyra räknesätten, dvs om $a, b \in K$ så $a \pm b$, $ab \in K$, och i fall $b \neq 0$, $\frac{a}{b} \in K$. □

Som exempel kan vi nämna kroppen av de rationella talen $\mathbb{Q}$, de reella talen $\mathbb{R}$ och de komplexa talen $\mathbb{C}$. Finns det andra talkroppar? Svaret är att det finns många fler, t o m oändligt många. Innan vi konstruerar andra talkroppar låt oss tänka en stund på $\mathbb{N}$ och $\mathbb{Z}$ som inte är kroppar men ändå måste anses som mycket viktiga talmängder. Heltalen är den enklaste talmängd som kallas för ring:

(10.2) Definition. Man säger att en talmängd R är en **talring** om $1 \in R$ och R är sluten m a p addition, subtraktion och multiplikation, dvs om $a, b \in R$ så $a \pm b$, $ab \in R$. □

Heltalen $\mathbb{Z}$ är en talring. Det är också klart att varje talkropp är en talring. $\mathbb{N}$ är inte en talring.

Hur kan man konstruera talringar och talkroppar? Vi visar en enkel sats som är ett specialfall av en mycket allmän konstruktion av talringar och talkroppar.

(10.3) Sats. *Låt R vara en talring och låt α vara ett tal sådant att $\alpha \notin R$ men $\alpha^2 \in R$. Då bildar alla tal*

$$a + b\alpha, \text{ där } \ a, b \in R,$$

en talring som betecknas med $R[\alpha]$. Om R är en kropp så är också $R[\alpha]$ en kropp.

Innan vi bevisar satsen låt oss titta på några intressanta exempel:

(10.4) Exempel. (a) Låt $R = \mathbb{Z}$ och låt $\alpha = \sqrt{2}$. Då har vi $\sqrt{2} \notin \mathbb{Z}$ och $(\sqrt{2})^2 = 2 \in \mathbb{Z}$. Satsen säger att talen

$$a + b\sqrt{2}, \quad \text{där} \quad a, b \in \mathbb{Z},$$

bildar en ring. Om vi i stället för $\mathbb{Z}$ väljer $R = \mathbb{Q}$ får vi att talen

$$a + b\sqrt{2}, \quad \text{där} \quad a, b \in \mathbb{Q},$$

bildar en kropp. Detta betyder bl a att kvoten av två tal $a + b\sqrt{2}$ och $c + d\sqrt{2} \neq 0$ med $c, d \in \mathbb{Q}$ måste kunna skrivas som $e + f\sqrt{2}$, där $e, f \in \mathbb{Q}$. Låt oss pröva:

$$\frac{1+\sqrt{2}}{3+2\sqrt{2}} = \frac{(1+\sqrt{2})(3-2\sqrt{2})}{(3+2\sqrt{2})(3-2\sqrt{2})} = -1 + \sqrt{2}.$$

Det här kan inte vara någon överraskning – det finns många liknande exempel i grundskolans läroböcker!

(b) I stället för $\alpha = \sqrt{2}$ kan man välja $\alpha = \sqrt{a}$, där a är ett godtyckligt heltal sådant att $\sqrt{a} \notin \mathbb{Q}$. På så sätt får vi oändligt många ringar $\mathbb{Z}[\sqrt{a}\,]$ och kroppar $\mathbb{Q}[\sqrt{a}\,]$. Är de verkligen olika? Det är ganska lätt att visa att för olika primtal p är kropparna $\mathbb{Q}[\sqrt{p}\,]$ olika (se övning B). Alltså existerar oändligt många olika kroppar eftersom primtalen bildar en oändlig mängd.

(c) En mycket intressant ring får man då man väljer $R = \mathbb{Z}$ och $\alpha = i$. Vi har $i^2 = -1 \in \mathbb{Z}$. Enligt satsen bildar talen

$$a + bi, \quad \text{där} \quad a, b \in \mathbb{Z},$$

en ring. Tal av denna typ kallas **Gaussiska heltal** [†]. De spelar en viktig roll i algebraisk talteori. □

Låt oss nu bevisa satsen:

Bevis av (10.3): Låt $x = a + b\alpha$, $y = c + d\alpha \in R[\alpha]$. Vi vill visa att $R[\alpha]$ är en ring, dvs att $x \pm y$, $xy \in R[\alpha]$. Vi har

$$x \pm y = (a + b\alpha) \pm (c + d\alpha) = (a \pm c) + (b \pm d)\alpha \in R[\alpha]$$

samt

$$xy = (a + b\alpha)(c + d\alpha) = (ac + bd\alpha^2) + (ad + bc)\alpha \in R[\alpha] \text{ ty } \alpha^2 \in R.$$

Om R är en kropp, vill vi visa att $x, y \in R[\alpha]$ och $y \neq 0$ ger $x/y \in R[\alpha]$. Detta är lite svårare. Här har vi:

[†] C.F. Gauss (30/4 1777 - 23/2 1855) var en tysk matematiker – en av de mest betydelsefulla i matematikens historia.

$$\frac{x}{y} = \frac{a+b\alpha}{c+d\alpha} = \frac{(a+b\alpha)(c-d\alpha)}{(c+d\alpha)(c-d\alpha)} = \frac{ac-bd\alpha^2}{c^2-d^2\alpha^2} + \frac{bc-ad}{c^2-d^2\alpha^2}\alpha = e + f\alpha,$$

där

$$e = \frac{ac-bd\alpha^2}{c^2-d^2\alpha^2} \in R \quad \text{och} \quad f = \frac{bc-ad}{c^2-d^2\alpha^2} \in R$$

ty R är en kropp. Alltså $x/y \in R[\alpha]$.

Beviset kan te sig avslutat men det finns en punkt som kräver eftertanke. Vi vet att $c + d\alpha \neq 0$ och vi förlänger bråket x/y med $c - d\alpha$. Får vi göra det? Med andra ord, är $c - d\alpha \neq 0$? Antag motsatsen, dvs att $c - d\alpha = 0$. Om $d \neq 0$, får vi $\alpha = c/d \in R$ vilket strider mot antagandet om α. Om $d = 0$, så ger $c - d\alpha = 0$ att $c = 0$, vilket betyder att $c + d\alpha = 0$ – en motsägelse igen! Alltså är $c - d\alpha \neq 0$ och vårt bevis är fullständigt. □

Låt oss återkomma till allmänna funderingar över talen och deras egenskaper. Våra kunskaper om olika talområden bygger på vår förmåga att hantera talen. I praktiken betyder det att vi följer olika regler när vi utför olika räkneoperationer. Vad är det för regler? Du kan säkert nämna eller skriva ut sådana regler som t ex associativiteten för addition: $a + (b + c) = (a + b) + c$, eller kommutativiteten för multiplikation: $ab = ba$. Hur många sådana regler finns det? Är alla lika viktiga? När kan man vara säker på att man har alla nödvändiga regler? Sådana frågor har sysselsatt många människor och svaren på dem bygger på matematisk forskning under en ganska lång tidsperiod. Här följer en förteckning över de viktigaste räknelagarna i en talmängd R i vilken de kan vara uppfyllda eller ej – allt beror på hur man väljer R :

(10.5) Egenskaperna hos addition och multiplikation:

Addition:

(a) slutenhet:	$\forall a, b \in R$	$a, b \in R \Rightarrow a + b \in R$,
(b) associativitet:	$\forall a, b, c \in R$	$(a + b) + c = a + (b + c)$,
(c) kommutativitet:	$\forall a, b \in R$	$a + b = b + a$,
(d) neutralt element:	$\exists\, 0 \in R\, \forall a \in R$	$0 + a = a$,
(e) motsatt element:	$\forall a \in R\, \exists m(a) \in R$	$a + m(a) = 0$ ($m(a)$ betecknas med $-a$).

Multiplikation:

(f) slutenhet:	$\forall a, b \in R$	$a, b \in R \Rightarrow ab \in R$,
(g) associativitet:	$\forall a, b, c \in R$	$(ab)c = a(bc)$,
(h) kommutativitet:	$\forall a, b \in R$	$ab = ba$,
(i) neutralt element:	$\exists\, 1 \in R\, \forall a \in R$	$1a = a$,
(j) inverst element:	$\forall a \in R \setminus \{0\}\, \exists i(a) \in R$	$a\, i(a) = 1$ ($i(a)$ betecknas med a^{-1}).

Addition och multiplikation:

(k) distributivitet: $\forall a, b, c \in R \quad a(b+c) = ab + ac$.

Alla dessa regler gäller då R är en talkropp t ex $\mathbb{Q}$, $\mathbb{R}$ eller $\mathbb{C}$. Om $R = \mathbb{Z}$ så gäller alla räknelagar med undantag av (j) – t ex $2 \in \mathbb{Z}$, men $1/2 \notin \mathbb{Z}$. Egenskapen (j) ger just skillnaden mellan en talkropp och en talring. I en talkropp gäller alla räknelagarna (a) – (k), medan i en talring gäller alla utom (j).

Räknelagarna (a) – (k) är grunden för all manipulation med talen och man måste vara medveten om deras giltighet i det talområde man vill arbeta med. Andra räknelagar som t ex

(i) $a0 = 0$ då $a \in R$,

(ii) $-(-a) = a$ då $a \in R$,

(iii) $(-1)a = -a$ då $a \in R$,

(iv) $(-a)b = -ab$ då $a, b \in R$,

(v) $(-a)(-b) = ab$ då $a, b \in R$,

kan man bevisa om man vet att R är en ring (se övningar). I själva verket kan man definiera allmänna begrepp *ring* och *kropp* i vilka dessa räknelagar kan härledas:

(10.6) Definition. Man säger att en mängd R vars element kan adderas under en operation ”$+$” och multipliceras under en operation ”$\cdot$” är en **ring** om dessa operationer har alla egenskaper (10.5) (a) – (k) med undantag av (j). Om alla egenskaper (a) – (k) gäller så säger man att R är en **kropp**. □

Vi har redan mött andra ringar och kroppar än talringar och talkroppar i avsnitten om restaritmetiker och polynomringar.

I samband med definitionerna av begreppen ring och kropp har du säkert observerat att man inte nämner subtraktion och division. Förklaringen är att subtraktion och division kan definieras i efterhand med hjälp av addition och multiplikation:

(10.7) Definition. (a) Om R är en ring och $a, b \in R$ så säger man att

$$a - b = a + (-b)$$

är **skillnaden** eller **differensen** mellan a och b.

(b) Om R är en kropp och $a, b \in R$, $b \neq 0$, så säger man att

$$a : b = ab^{-1}$$

är **kvoten** av a genom b. Kvoten betecknas också med $\frac{a}{b}$. □

Vårt syfte i detta avsnitt är att förklara hur man definierar talbegreppet. Som vi redan vet finns det oändligt många olika talringar och talkroppar. På vilket sätt intar $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ och $\mathbb{C}$ en särställning bland dem? Ett kort svar som kräver många förklaringar är följande: $\mathbb{Z}$ är den minsta talringen, $\mathbb{Q}$ är den minsta talkroppen, $\mathbb{R}$ är den största talkroppen som tillåter ordningsrelationen $\leq$ och $\mathbb{C}$ är den största talkroppen överhuvudtaget. Man inser säkert att alla dessa svar förutsätter att man vet vad ett tal är. Svaret på den frågan är inte enkelt och det tog en mycket lång tid i mänsklighetens utveckling innan man kunde komma till ett tillfredsställande svar. Trots det har man sedan en lång tid tillbaka kunnat räkna med alla typer av tal och utveckla vetenskapliga teorier som bygger på beräkningar och som framgångsrikt beskriver världen runt omkring oss. De naturliga talen är med all säkerhet lika gamla som den mänskliga civilisationen, rationella tal (åtminstone positiva) är nästan lika gamla, negativa tal (hela, rationella och reella) användes för ungefär 1000 år sedan, och komplexa tal introducerades under 1500-talet. Därför finns det inte någon större anledning till oro om våra svar inte visar sig bli fullständiga. Vi skall försöka förklara olika aspekter av talbegreppet utan att förutsätta några större förkunskaper. Mera tillfredsställande förklaringar väntar den som läser fortsättningskurser i matematik.

Det finns två möjligheter att introducera talbegreppet. Den ena är att börja med de naturliga talen och försöka steg för steg konstruera andra typer av tal. Den metoden ter sig naturlig och tilltalande men den är mycket arbetsam och, tyvärr, ganska lång om man vill kontrollera alla detaljer. Vi skall berätta om den senare i detta avsnitt.

Den andra möjligheten utgår från att man kan hantera talen om man vet vilka regler som styr deras användning. Det räcker om man kommer överens om dessa regler och följer dem för att kunna använda talen, men man behöver inte bry sig om hur de är konstruerade. En sådan inställning till talen är mycket praktisk, men en matematiker vill gärna veta hur talen konstrueras (och alla andra som använder talen måste tro på möjligheten av dessa konstruktioner). Man kan jämföra den inställningen med inställningen till tekniken – om man har läst en instruktionsbok till en TV-apparat så vet man hur man använder den utan att behöva veta hur den är konstruerad (eller att den finns). En beskrivning av en programvara är troligen ännu bättre som jämförelse – man får en förteckning över kommandon och deras effekt utan att behöva veta hur programvaran är konstruerad eller om den finns tillgänglig.

Vi skall försöka beskriva de egenskaper som karakteriserar de reella talen. Valet av dessa egenskaper är ett resultat av matematisk forskning huvudsakligen under 1800-talet. De reella talen spelar en mycket central roll. Å ena sidan har alla människor en intuitiv uppfattning om dessa tal som kommer från erfarenheten av att räkna och mäta i vardagslivet. Å andra sidan bygger alla vetenskaper, och bland dem matematiken själv, på de reella talens egenskaper.

Som vi redan vet bildar de reella talen en kropp. Men det finns många kroppar så man måste välja egenskaper som utmärker just den. En viktig egenskap är att man kan jämföra de reella talen med hjälp av $\leq$ – de reella talen bildar en ordnad kropp. Låt oss definiera helt allmänt vad detta betyder:

(10.8) Definition. Man säger att en kropp K är **ordnad** om den innehåller en delmängd P sådan att:

(a) om $x \in K$ så gäller exakt ett av de tre alternativen: $x \in P$ eller $x = 0$ eller $-x \in P$,

(b) om $x, y \in P$ så gäller att $x + y \in P$ och $xy \in P$.

Man säger att P är mängden av de positiva elementen i K. □

Det är klart att i $K = \mathbb{R}$ kan vi välja P = alla positiva reella tal. Detta betyder att $\mathbb{R}$ är en ordnad kropp. $\mathbb{Q}$ är också ordnad eftersom vi kan välja P = alla positiva rationella tal. Vi skall senare visa att $\mathbb{C}$ inte är en ordnad kropp (det följer av att $i^2 = -1$).

Vi skall uppehålla oss en stund vid definitionen (10.8). Man kan definiera:

$$x > y \quad (\text{eller } \ y < x) \quad \text{om} \quad x - y \in P. \tag{10.9}$$

Man brukar också skriva $x \geq y$ (eller $y \leq x$) om $x > y$ eller $x = y$. Detta är en ordningsrelation enligt vår tidigare definition. $x > 0$ betyder att $x - 0 \in P$, dvs $x \in P$; $x < 0$ betyder att $0 - x \in P$, dvs $-x \in P$.

Om K är en ordnad kropp så kan man definiera de naturliga och de rationella talen i K. Först observerar vi att $1 > 0$ ($1 \in K$ är neutralt för multiplikation). Vi vet att $1 \neq 0$ så att $1 \in P$ eller $-1 \in P$. Antag att $-1 \in P$. Då är $1 = (-1)(-1) \in P$ enligt (b) i (10.8). Detta ger att både 1 och -1 tillhör P vilket strider mot (a) i (10.8). Därför måste $1 \in P$. De naturliga talen i K får vi som

$$0, 1, 1 + 1, 1 + 1 + 1, 1 + 1 + 1 + 1, \ldots$$

vilka definitionsmässigt betecknas med 0,1,2,3,4,.... Observera att $0 < 1 < 2 < 3 < 4$... eftersom $2 - 1 = 1 > 0$, $3 - 2 = 1 > 0$, $4 - 3 = 1 > 0$ osv. Heltalen i K definieras som: alla naturliga tal x och deras motsatta tal $-x$, dvs 0, ± 1, ± 2, ± 3, ± 4, ... De rationella talen definieras som alla kvoter ab^{-1} , där a, b är hela och $b \neq 0$ (se (10.7)).

Både $\mathbb{Q}$ och $\mathbb{R}$ är ordnade kroppar så en definition av de reella talen måste bygga på en annan egenskap (utöver det att $\mathbb{R}$ är ordnad). Innan vi formulerar en lämplig egenskap, låt oss återkomma för en stund till definitionen av en ordnad kropp. I en sådan kropp kan man definiera absolutbelopp:

$$|x| = \begin{cases} x & \text{om } x \geq 0, \\ -x & \text{om } x < 0. \end{cases} \tag{10.10}$$

Man kan också säga vad det betyder att en följd x_1, x_2, x_3, ... går mot 0. Man säger så om det för varje naturligt tal n finns ett N sådant att $|x_i| < \frac{1}{n}$ då $i > N$. Nu kan vi formulera en grundläggande

egenskap som skiljer $\mathbb{Q}$ från $\mathbb{R}$. Låt $x_1, x_2, ..., x_i, ...$ vara en växande och begränsad följd av rationella tal, dvs $x_1 \leq x_2 \leq ... \leq x_i \leq ...$ och det finns ett tal B så att $x_i \leq B$ då $i = 1, 2, ...$ Vad kan man säga om gränsvärdet $\lim_{i\to\infty} x_i$? I analyskurser visas att gränsvärdet existerar. Är gränsvärdet ett rationellt tal? Låt oss betrakta ett exempel. Definiera

$$x_n = 1, a_1 a_2 ... a_n, \quad n \geq 1,$$

där a_i är i :te siffran i decimalutvecklingen av $\sqrt{2}$, dvs

$x_1 = 1, 4,$
$x_2 = 1, 41,$
$x_3 = 1, 414,$
$x_4 = 1, 4142,$
. . .

Det är klart att alla x_n är rationella och att följden är växande och begränsad. Ändå är det också klart att $\lim_{n\to\infty} x_n = \sqrt{2}$, dvs följden konvergerar mot ett icke-rationellt tal $\sqrt{2}$. Men gränsvärdet är ett reellt tal och det är sant helt allmänt att en växande och begränsad följd av reella tal konvergerar mot ett reellt tal. Man säger att de reella talen bildar en fullständig kropp[‡]. Allmänt har man följande begrepp:

(10.11) Definition. En ordnad kropp kallas **fullständig** om varje växande och begränsad följd av kroppens element konvergerar mot ett element i kroppen. □

Mera exakt, om K är en ordnad kropp så är den fullständig om för varje följd $x_1 \leq x_2 \leq ... \leq x_n \leq ...$ sådan att $x_n \in K$ och det finns $B \in K$ så att $x_n \leq B$ då $n = 1, 2, ...$ man kan hitta $x \in K$ så att $\lim_{n\to\infty} x_n = x$.

Nu kan vi definiera de reella talen:

(10.12) Definition. Med **reella tal** menar man elementen i en ordnad och fullständig kropp K. □

Dessa få ord döljer ett ganska sammansatt matematiskt innehåll: K är en kropp, dvs uppfyller villkoren (a) – (k) på sidan 4, K är ordnad, dvs upfyller (a) och (b) i (10.8), och slutligen är K fullständig, dvs uppfyller (10.11). Nu kan man ställa två frågor:

Finns det en ordnad och fullständig kropp?
Hur många ordnade och fullständiga kroppar finns det?

[‡]Detta bevisas i analyskurser med hjälp av supremumaxiomet som är ekvivalent med den egenskapen.

Man behöver inte veta svaret på dessa två frågor för att kunna räkna med de reella talen eftersom (10.12) är en exakt förteckning över alla grundläggande egenskaper hos dessa tal och det räcker att följa dem och deras logiska konsekvenser. Men svaren på dessa två frågor är mycket viktiga inte bara för en matematiker (en matematiker vill dessutom se själv hur man kommer fram till svaren). De är följande: Det finns ordnade och fullständiga kroppar. Om K_1 och K_2 är två sådana så finns det en bijektiv funktion $f : K_1 \to K_2$ (dvs enentydig och på hela K_2) som uppfyller $f(a+b) = f(a)+f(b)$, $f(ab) = f(a)f(b)$ och om $a > 0$ så är $f(a) > 0$[§]. Intuitivt säger existensen av f att K_1 och K_2 skiljer sig bara när det gäller beteckningar, dvs om $a \in K_1$ så kan $f(a)$ uppfattas som ett annat namn på a. Addition och multiplikation i K_1 översätter man med hjälp av f till addition och multiplikation i K_2. Likaså positiva element ur K_1 övergår med hjälp av f i positiva element i K_2. I den meningen är kroppen av de reella talen entydig.

Vi vet redan att om vi har de reella talen så kan vi definiera de naturliga, hela och rationella. På så sätt har vi en möjlighet att tillfredsställa vårt behov av någorlunda ordentlig presentation av talbegreppet. Men även om den för många ändamål är helt tillfredsställande, går vi ett steg längre och försöker beskriva konstruktioner av olika talmängder. Behovet av sådana konstruktioner insåg man under 1800-talet då utvecklingen av matematiken gick så långt att intuitiva föreställningar om talen inte längre var tillräckliga. Man försökte konstruera olika talområden genom att utgå från de naturliga talen och successivt gå till de hela, rationella, reella och komplexa. Den vägen är ganska lång, arbetsam (man måste kontrollera många detaljer), och det värsta, rätt så tråkig om man bortser från mera allmänna principer som styr dessa konstruktioner och har betydelse i andra sammanhang. Därför behövs möjligen ett varningens ord att inte fördjupa sig i alla detaljer och läsa det följande mera kursivt.

(10.13) De naturliga talen. De äldsta talen är de naturliga (och de är mest naturliga eftersom de är de äldsta). Varifrån kommer de? En stor tysk matematiker L. Kronecker sade någon gång att ”Gud skapade de naturliga talen, allt annat är människans skapelse”. Det vore för enkelt med detta svar men det är mycket djupsinnigt. Den enda möjligheten att definiera de naturliga talen är den metod som vi tidigare använde för att definiera de reella: Man kan beskriva deras grundläggande egenskaper. Varifrån kommer de egenskaper som betraktas som grundläggande? Svaret är att de kommer från mänsklighetens erfarenhet av experimentell hantering av talen och det faktum att de regler som man har följt under en mycket lång tid ger en bild av verkligheten som överensstämmer med våra observationer. En analys av sådana regler kunde göras enbart av matematiker. Det var R. Dedekind [¶] och G. Peano [‖] som föreslog ett urval av sådana grundläggande regler under senare delen av 1800-talet. Den mest kända definitionen kommer från Peano och låter så här:

(10.14) Definition. Med **naturliga tal** menar man elementen i en mängd $\mathbb{N}$ som satisfierar följande villkor:

(a) det finns ett utvalt element $0 \in \mathbb{N}$;

(b) det finns en injektiv funktion som mot varje element $n \in \mathbb{N}$ ordnar ett element $n^* \in \mathbb{N}$ så att $n^* \neq 0$;

[§] En sådan funktion f kallas isomorfism och man säger att K_1 och K_2 är isomorfa ordnade kroppar.

[¶] Richard Dedekind (1831-1916), tysk matematiker.

[‖] Giuseppe Peano (1858-1932), italiensk matematiker.

(c) om $X \subseteq \mathbb{N}$ och

(c_1) $0 \in X$,

(c_2) $\forall n\ (n \in X \Rightarrow n^* \in X)$,

så är $X = \mathbb{N}$. □

Intuitivt betyder n^* talet $n + 1$ (n^* kallas efterföljaren till n, och 1 definieras som 0^*). Sista villkoret (c) kallas ofta ”induktionsaxiometöch är grunden för matematisk induktion. Lägg märke till att man inte nämner addition och multiplikation i definitionen. De definieras i efterhand. Peanos definition överenstämmer väl med vår intuition, den är lätt att förstå, den är kort och elegant. Den uppfyller många av de kriterier som man vill uppfylla när man definierar ett matematiskt objekt. Vidare kan man ur den definitionen härleda alla kända egenskaper hos de naturliga talen.

Men hur är det egentligen med existensen och entydigheten av den mängden? När det gäller entydigheten är svaret enkelt: Man kan visa att om N_1 och N_2 är två mängder som uppfyller villkoren i definitionen (10.14) så är de isomorfa vilket betyder att det finns en bijektiv funktion $f : N_1 \to N_2$ sådan att $f(1) = 1$ samt $f(n^*) = f(n)^*$ (jämför ett liknande påstående om de reella talen på sidan 9). Existensen av de naturliga talen vilar på vår övertygelse om att åtminstone en mängd av de naturliga talen existerar – nämligen den som under mänsklighetens historia så troget och framgångsrikt har tjänat till att räkna, resonera och dra korrekta slutsatser om världen runt omkring oss. Med andra ord är existensen av de naturliga talen ett axiom. Här har vi närmat oss matematikens grunder som har mycket gemensamt med vetenskapernas filosofi.

Alla andra talområden kan nu successivt konstrueras: De hela talen från de naturliga, de rationella från de hela, de reella från de rationella och de komplexa från de reella. När vi tidigare sade att det går att bevisa existensen av de reella talen så menade vi just att det var möjligt att konstruera dessa tal från de naturliga.

Nu skall vi börja vår vandring från de naturliga talen genom rationella och reella till de komplexa. Vi utelämnar många detaljer och begränsar oss till allmänna idéer.

Det finns två huvudorsaker till att talbegreppet utvidgades. Det första var behov i samband med mätningar. Man upptäckte mycket tidigt att det behövdes bråktal för att uttrycka dimensioner (längder och areor) av jordlotter. Men icke-rationella tal dök upp även i samband med mätningar (vi får se det i samband med konstruktionen av de reella talen). Den andra orsaken har en mera abstrakt karaktär. Nya typer av tal behövdes för att kunna lösa ekvationer. Ett typiskt exempel är de komplexa talen. På 1500-talet kände man till formeln

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

för lösningar till andragradsekvationen $x^2+px+q=0$. Löser man ekvationen $x^2-3x+2=0$ så får man enligt den formeln $x_1=1$ och $x_2=2$. Tar man i stället $x^2-2x+2=0$ så blir $x_1=1+\sqrt{-1}$ och $x_2=1-\sqrt{-1}$. En del människor skulle kanske säga att ekvationen $x^2-2x+2=0$ i så fall saknar lösningar eftersom $\sqrt{-1}$ är helt utan mening. Andra skulle acceptera symbolen $\sqrt{-1}$, tillskriva den egenskapen att $(\sqrt{-1})^2=-1$ och sätta in $1+\sqrt{-1}$ i ekvationen $x^2-2x+2=0$. Då är

$$(1+\sqrt{-1})^2-2(1+\sqrt{-1})+2=1+2\sqrt{-1}+(-1)-2-2\sqrt{-1}+2=0$$

dvs $1+\sqrt{-1}$ är en lösning till ekvationen. Så gjorde några italienska matematiker under 1500-talet. Om man anser att $1+\sqrt{-1}$ bör uppfattas som en lösning till ekvationen $x^2-2x+2=0$ så bör man också ha en bra förklaring till varför. Det gäller att motivera användningen av $\sqrt{-1}$. Det tog 300 år innan man kunde ge en tillfredsställande förklaring och rent formellt konstruera de komplexa talen. Men exakt samma situation som med de komplexa talen har man med de hela, rationella och reella. Om man frågar ett barn om x sådant att $2+x=3$ så får man svaret $x=1$. Tar man istället $3+x=2$ riskerar man att bli utskrattad. Ekvationen $2+x=3$ kan lösas i mängden av de naturliga talen, men $3+x=2$ kräver ett nytt talområde – de hela talen (i synnerhet de negativa). På liknande sätt går det att dela 4 i två lika delar (dvs lösa $2x=4$) i heltalen, men det går inte att dela 3 i två lika delar i den mängden (dvs lösa $2x=3$) – det behövs rationella tal för att göra det. Slutligen kan man hitta ett rationellt tal som multiplicerat med sig självt ger 4 (dvs lösa $x^2=4$), men det går inte att hitta ett rationellt tal som multiplicerat med sig självt ger 2 (dvs lösa $x^2=2$) – för att göra det behövs ett nytt talområde. Det naturliga önskemålet att polynomekvationer alltid skall gå att lösa, tvingar oss således att successivt utvidga talområden. Om det finns en slutstation för denna utvidgningsprocess får vi veta lite senare. Så låt oss börja!

(10.15) Från de naturliga talen till de hela. Ekvationen $3+x=5$ definierar $x=2$ som sin lösning. Samma lösning ger $4+x=6$, $5+x=7$ osv. Man kan uppfatta 2 som paret (5,3) eller (6,4) eller (7,5) osv. Paret (a,b) ger lösningen till $b+x=a$ med $a>b$. Paren (a,b) och (c,d) ger samma x om $a-b=c-d$, dvs $a+d=b+c$. Men det finns par (a,b) med $a=b$ och $a<b$. Har de en liknande tolkning? T ex kan (3,5) uppfattas som lösningen till $5+x=3$. En sådan lösning finns inte bland de naturliga talen men själva tolkningen ger en idé hur man kan definiera heltalen.

Låt oss betrakta alla par (a,b) där $a,b\in\mathbb{N}$. Vi säger att $(a,b)\sim(c,d)$ då och endast då $a+d=b+c$. Man verifierar lätt att detta är en ekvivalensrelation, och vi definierar heltalen $\mathbb{Z}$ som mängden av dess ekvivalensklasser. Vi inför också följande skrivsätt för ekvivalensklassen $[(a,b)]$:

$$[(a,b)]=\begin{cases} a-b & \text{om } a\geq b,\\ -(b-a) & \text{om } a<b.\end{cases}$$

T ex är $[(1,3)]=-(3-1)=-2$ och paren (1,3), (2,4), (3,5) osv tillhör samma klass. Vidare definierar man addition och multiplikation av heltal:

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

$$[(a,b)][(c,d)] = [(ac+bd,\, ad+bc)].^{**}$$

Här måste man kontrollera att dessa operationer är väldefinierade, dvs att om $(a,b) \sim (a',b')$ och $(c,d) \sim (c',d')$ så $(a+c,b+d) \sim (a'+c',b'+d')$ och $(ac+bd,ad+bc) \sim (a'c'+b'd',a'd'+b'c')$, dvs summan och produkten beror inte på vilken representant för respektive ekvivalensklass man använder. Detta kallas också för att $\sim$ är en *kongruensrelation* med avseende på addition och multiplikation (betraktade som operationer på $\mathbb{N} \times \mathbb{N}$).

Nu kan man kontrollera att heltalen bildar en ring men att gå igenom alla detaljer är ganska omständligt. Lägg också märke till att $\mathbb{N}$ kan betraktas som delmängd av $\mathbb{Z}$ så att det verkligen är korrekt att införa skrivsättet ovan: t ex är 2 både ett naturligt tal och en beteckning för klassen $[(5,3)]$.

(10.16) Från de hela talen till de rationella. Konstruktionen är nästan identisk med den förra. Ekvationen $2x = 1$ definierar $1/2$. Samma lösning ger $4x = 2$, $6x = 3$ osv. Vi kan uppfatta $1/2$ som paren (1,2), (2,4), (3,6) osv. $-1/2$ får man som t ex $(-1,2)$, $(-2,4)$ osv. Allmänt kan lösningen till $bx = a$ uppfattas som paret (a,b). Observera att $b \neq 0$. Två par (a,b) och (c,d) ger samma rationella tal om $\frac{a}{b} = \frac{c}{d}$. Men vi vill undvika bråk (de skall ju definieras!). Därför skriver vi villkoret på formen $ad = bc$. Nu kan vi starta vår konstruktion.

Betrakta alla par (a,b) sådana att $a,b \in \mathbb{Z}$ och $b \neq 0$. Man säger att $(a,b) \sim (c,d)$, $d \neq 0$, om $ad = bc$. Detta är en ekvivalensrelation och vi inför beteckningen

$$[(a,b)] = \frac{a}{b} \text{ (eller } a:b)$$

för ekvivalensklasserna. T ex är $[(1,3)] = \frac{1}{3}$ och paren (1,3), (2,6), (3,9) tillhör samma klass (definierar samma rationella tal). Nu kan vi definiera addition och multiplikation av rationella tal:

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad+bc}{bd}, \\ \frac{a}{b}\frac{c}{d} &= \frac{ac}{bd}, \end{aligned}$$

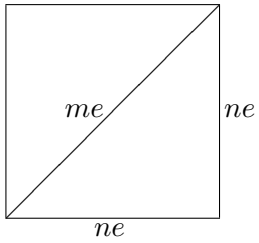
och kontrollera att dessa är väldefinierade och att man verkligen får en kropp (se övningar). Observera att:

$$\begin{aligned} \frac{a}{1} + \frac{c}{1} &= \frac{a+c}{1}, \\ \frac{a}{1}\frac{c}{1} &= \frac{ac}{1}, \end{aligned}$$

**Tänk på $[(a,b)]$ och $[(c,d)]$ som $a-b$ och $c-d$. Då är$(a-b)(c-d) = (ac+bd)-(ad+bc) = [(ac+bd,ad+bc)]$.

dvs talen $\frac{a}{1}$ adderas och multipliceras precis som heltalen a. Man kommer överens om att skriva $\frac{a}{1} = a$ så att de vanliga heltalen kan betraktas som en delmängd till de rationella talen.

(10.17) Från de rationella talen till de reella. Den biten av vägen är lite annorlunda och utgör ett mycket större steg än de två föregående. Först och främst hittar man lätt ekvationer med rationella koefficienter som saknar rationella lösningar, t ex $x^2 = 2$. Sådana ekvationer kräver en utvidgning av de rationella talen. Men det finns en annan mycket viktig anledning till att man inser behovet av nya tal. Man upptäckte mycket tidigt att rationella tal inte är tillräckliga för att kunna mäta längder av sträckor. Följande klassiska exempel spelade en mycket viktig roll i matematikens utveckling. Betrakta en kvadrat och anta att man har fixerat en enhet e sådan att kvadratens sida rymmer exakt n enheter och dess diagonal m enheter (m och n är naturliga tal).



Nu vet vi att $(ne)^2 + (ne)^2 = (me)^2$ så att $2n^2 = m^2$, dvs $\sqrt{2} = \frac{m}{n}$. Detta visar att om e finns så är $\sqrt{2}$ ett rationellt tal. Pythagoras [††] och hans elever visste mycket väl att det inte var fallet. Sin upptäckt om förhållandet mellan kvadratens sida och dess diagonal betraktade de som något som stred mot naturens ordning och försökte hemlighålla under en tid. Men konsekvensen blev att Euklides [‡‡] kort därefter kunde utveckla geometrin och läran om reella tal som mått på sträckor.

Hur visar man att $\sqrt{2}$ inte är rationellt? Vi skall visa det genom att utnyttja entydigheten av primfaktoruppdelningar av de naturliga talen. Antag att $\sqrt{2}$ är rationellt, dvs att

$$\sqrt{2} = \frac{m}{n}\,,$$

där m, n är naturliga tal. Då är $2n^2 = m^2$. Eftersom m^2 och n^2 är kvadrater av heltal innehåller de ett jämnt antal primfaktorer 2 (möjligen 0 sådana faktorer). Alltså förekommer 2 som primfaktor i $2n^2$ ett udda antal gånger, medan i m^2 ett jämnt antal gånger så att $2n^2 \neq m^2$. Detta motsäger likheten $2n^2 = m^2$ och visar att $\sqrt{2}$ inte kan vara rationellt.

Låt oss nu konstruera de reella talen. Vi kan inte längre använda oss av tekniken med par av rationella tal. Men vi kan utnyttja följder av rationella tal. Reella tal (enligt gymnasiekunskaper) är decimaltal av typen $A = a, a_1a_2...a_n...$, där a är heltalsdelen och $0, a_1a_2...a_n...$ är decimaldelen av A. Varje sådant tal kan approximeras med rationella tal – följden

[††] Pythagoras (572-500 f Kr)
[‡‡] Euklides (ca 350 f Kr)

$x_1 = a, a_1$,
$x_2 = a, a_1 a_2$,
$x_3 = a, a_1 a_2 a_3$,
...
$x_n = a, a_1 a_2 a_3 ... a_n$,
...

består av rationella tal och konvergerar mot A, dvs $\lim_{n\to\infty} x_n = A$. T ex är för $A = \pi$:

$x_1 = 3, 1$,
$x_2 = 3, 14$,
$x_3 = 3, 141$,
...
$x_8 = 3, 14159265$,
...

Låt nu A vara ett positivt tal. Följden $\{x_1, x_2, ..., x_n, ...\} = \{x_n\}_1^\infty$ består då av rationella tal, den är växande och begränsad (ty $x_n \leq A$ för alla n). Vi vet att en sådan följd alltid har ett gränsvärde. Två följder $\{x_n\}$ och $\{x'_n\}$ har samma gränsvärde då och endast då deras skillnad går mot 0, dvs $\lim_{n\to\infty}(x_n - x'_n) = 0$. Positiva reella tal är alltså gränsvärden av växande och begränsade följder av rationella tal och två följder definierar samma reella tal som sitt gränsvärde om deras skillnad går mot 0. Men vi kan inte definiera reella tal som gränsvärden av sådana följder så länge de reella talen inte är konstruerade eftersom en sådan definition skulle förutsätta att de reella talen (dvs gränsvärdena) är kända. Ändå identifierar vi varje reellt tal med ett gränsvärde på följande sätt. (Här börjar den formella definitionen.)

Betrakta alla växande och begränsade följder $\{x_1, x_2, ..., x_n, ...\} = \{x_n\}_1^\infty$, där x_n är positiva rationella tal. Man säger att två följder $\{x_n\}_1^\infty$ och $\{x'_n\}_1^\infty$ är ekvivalenta (definierar samma reella tal) om deras skillnad $\{x_n - x'_n\}_1^\infty$ konvergerar mot 0, dvs $\lim_{n\to\infty}(x_n - x'_n) = 0$. Alla följder som tillhör klassen av $\{x_n\}_1^\infty$ betecknas med $[\{x_n\}_1^\infty]$. En sådan klass kallar man för ett positivt reellt tal. Nu kan man definiera addition och multiplikation av de positiva reella talen (väldefinition måste kontrolleras):

$$[\{x_n\}_1^\infty] + [\{x'_n\}_1^\infty] = [\{x_n + x'_n\}_1^\infty],$$

$$[\{x_n\}_1^\infty][\{x'_n\}_1^\infty] = [\{x_n x'_n\}_1^\infty].$$

För att nu konstruera de negativa reella talen och talet 0 måste man upprepa samma konstruktion som ledde oss från de naturliga talen till de hela: Man betraktar alla par (a, b), där a och b är positiva reella tal, och man identifierar (a, b) med (c, d) om $a + d = b + c$. Kontrollen att man får en kropp och att den är ordnad och fullständig är ganska lång men inte särskilt svår (detaljerna behandlas närmare i fortsättningskurser i matematik [†]).

[†] Vanligen brukar man i stället för växande och begränsade följder betrakta godtyckliga följder av rationella tal $x_1, x_2, ..., x_n, ...$ sådana att avståndet mellan talen x_i och x_j går mot 0 då i och j växer, dvs $|x_i - x_j| \to 0$ då $i, j \to \infty$.

(10.18) Från de reella talen till de komplexa. Vi vet redan att behovet av de komplexa talen upptäcktes i samband med andragradsekvationer med reella koefficienter. En så enkel ekvation som $x^2 = -1$ saknar reella lösningar. Antag att vi har en kropp K som innehåller de reella talen $\mathbb{R}$ och sådan att det finns $\alpha \in K$ som satisfierar ekvationen $x^2 = -1$, dvs $\alpha^2 = -1$. Man kontrollerar utan större svårigheter (se (10.3)) att talen

$$a + b\alpha, \text{ där } \quad a, b \in \mathbb{R}\,,$$

bildar en kropp. Det finns en mycket lång tradition att α betecknas med i (ibland j) [‡]. I den kroppen har vi:

$$\begin{aligned} (a+bi)+(c+di) &= (a+c)+(b+d)i\,, \\ (a+bi)(c+di) &= (ac-bd)+(ad+bc)i. \end{aligned} \tag{10.19}$$

Än så länge har vi inte någon formell konstruktion av de komplexa talen (vi sade ju ”Antag att vi har en kropp K...”). Men vi har i alla fall en klar bild av hur en kropp som innehåller lösningen till $x^2 = -1$ måste se ut. Konstruktionen är mycket enkel. Idén är (som flera gånger tidigare) att uppfatta nya tal som par av redan kända: $a + bi$ kan uppfattas som (a, b), där $a, b \in \mathbb{R}$.

(10.20) Definition. Med **komplexa tal** menar man alla par (a, b), där $a, b \in \mathbb{R}$, som adderas och multipliceras på följande sätt:

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

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

Mängden av de komplexa talen betecknas med $\mathbb{C}$. □

Beteckningen (a, b) är lite omständlig. Därför observerar man att:

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

Följder av den typen kallas Cauchyföljder.

[‡] ”i” kommer från ordet ”imaginär”. Det finns ett mycket intressant val av terminologi när det gäller nya typer av tal. De naturliga talen bland de hela kallas positiva, de övriga negativa. Bråktalen bland de reella kallas rationella, de övriga irrationella. Komplexa talen $a + bi$ har realdel a och en imaginärdel b. Alltså var allt nytt negativt, irrationellt och imaginärt (samt en lång tid impopulärt).

$$(a,0)(b,0) = (ab,0),$$

dvs paren $(a,0)$ adderas och multipliceras precis som vanliga reella tal a. Man kommer överens om att skriva $(a,0) = a$ så att $\mathbb{R} \subset \mathbb{C}$. Därefter noterar man att $(0,1)(0,1) = (-1,0) = -1$. Man betecknar $(0,1) = i$. Nu har vi $(0,b) = (b,0)(0,1) = bi$ så att

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

och vi får våra gamla beteckningar (10.19). Det som återstår är kroppstrukturen:

(10.21) Sats. *De komplexa talen $a + bi$, där $a, b \in \mathbb{R}$ och $i^2 = -1$, bildar en kropp.*

Satsen visas lätt, men beviset tar lite tid eftersom man måste kontrollera alla villkor (a) – (k) på sidan 4.

Innan vi tittar på möjligheten att gå vidare med liknande konstruktioner låt oss summera våra kunskaper. **Nu kan vi säga att med ett tal menar man alltid ett komplext tal.** I synnerhet kan det vara fråga om ett naturligt, helt, rationellt eller reellt tal. Med en talring (eller talkropp) menas alltid en ring (eller kropp) bestående av tal.

$\mathbb{Z}$ är den minsta talringen därför att om R är en talring så gäller att $1 \in R$ vilket ger att $1 + 1$, $1 + 1 + 1, ... \in R$, dvs R innehåller de naturliga talen. Vidare måste $0 \in R$ och $-x \in R$ om $x \in R$ så att R innehåller $\mathbb{Z}$. $\mathbb{Q}$ är den minsta talkroppen eftersom varje talkropp K innehåller $\mathbb{Z}$ och därmed också alla tal $\frac{a}{b}$, där $a, b \in \mathbb{Z}$ och $b \neq 0$, dvs $K \supseteq \mathbb{Q}$.

De reella talen bildar den största ordnade talkroppen. Låt oss först konstatera att $\mathbb{C}$ inte är ordnad. Antag nämligen att man kan välja en mängd P av positiva element i $\mathbb{C}$. Då är $i \in P$ eller $-i \in P$. I varje fall är $(\pm i)^2 = -1 \in P$ vilket är omöjligt ty redan $1 \in P$ (se (10.8)). Man visar (men det är inte helt banalt) att om en talkropp kan ordnas så kan den inte innehålla något komplext tal $a + bi$ med $b \neq 0$, dvs den ligger i $\mathbb{R}$. I den meningen är $\mathbb{R}$ den största ordnade talkroppen.

De komplexa talen bildar den största talkroppen. I vilken mening? Man kan fråga sig som tidigare om det finns polynomekvationer, nu med komplexa koefficienter, som inte kan lösas i det komplexa talområdet. Svaret på den frågan kommer från C.F. Gauss som år 1799 visade följande sats:

(10.22) Polynomalgebrans fundamentalsats. *Varje polynomekvation av positiv grad med komplexa koefficienter har en komplex lösning.*

Satsen säger att om $p(X) = a_n X^n + ... + a_1 X + a_0$, där $a_i \in \mathbb{C}$, $n > 0$ och $a_n \neq 0$ så är $p(z) = 0$ för ett komplext tal $z \in \mathbb{C}$. Man säger också att kroppen av de komplexa talen är algebraiskt sluten. Det finns flera olika bevis för den satsen men alla kräver lite större förkunskaper [§].

[§] Beviset ges i kursen ”Analytiska funktioner”. Ett nästan rent algebraiskt bevis i ”Galoisteori”.

(10.23) Finns något bortom de komplexa talen? Den sista satsen säger att det inte finns något vidare behov att utvidga den komplexa talkroppen p g a olösbara polynomekvationer. I den meningen bildar de komplexa talen den största talkroppen. Men en lång tid innan man var medveten om detta, upptäckte man matematiska objekt som kunde användas till att beskriva och utforska naturen och som i många avseenden liknade talen. Exempel på sådana begrepp är vektor, matris, kvaternion och tensor. Vektorer och matriser är uppsättningar av tal som också kan adderas och multipliceras på ett lämpligt sätt. De ger en möjlig generalisering av talbegreppet. **Kvaternioner**, som enklast kan beskrivas med hjälp av matriser, är ett annat exempel på en algebraisk struktur som ligger mycket nära de komplexa talen. Vi skall avsluta detta avsnitt genom att säga några ord om just kvaternioner.

W.R. Hamilton [¶] som gav en formell definition av komplexa tal i form av reella talpar försökte gå vidare med sin idé och betrakta par av komplexa tal. Han ville definiera addition och multiplikation av sådana par och möjligen få en ny kropp. Faktum är att det finns många kroppar som innehåller de komplexa talen, men de måste alltid innehålla element som inte uppfyller någon icke-trivial polynomekvation med komplexa koefficienter (t ex kroppen $\mathbb{C}(X)$ av alla rationella funktioner med komplexa koefficienter, dvs alla bråk $\frac{p(X)}{q(X)}$, där $p(X)$ och $q(X)$ är polynom med komplexa koefficienter – variabeln X är inte ett nollställe till något nollskilt polynom med komplexa koefficienter). Därför är det inte längre möjligt att konstruera en kropp större än $\mathbb{C}$ vars element uppfyller polynomekvationer med komplexa koefficienter. Hamilton lyckades dock att konstruera en struktur som har den egenskapen och som uppfyller alla räknelagar för en kropp med bara ett undantag. På Brougham Bridge i Dublin där Hamilton bodde finns idag en tavla med följande text: ”Here as he walked by on the 16th of October 1843 Sir William Rowan Hamilton in a flash of genius discovered the fundamental formula for quaternion multiplication $i^2 = j^2 = k^2 = ijk = -1$ and cut it in on a stone of this bridge”. Han publicerade sina resultat år 1853. Konstruktionen av kvaternioner, som spelar en mycket viktig roll i många matematiska och fysikaliska teorier, är följande. Betrakta alla par (z_1, z_2), där z_1, z_2 är komplexa tal. Definiera

$$(z_1, z_2) + (z_1', z_2') = (z_1 + z_1', z_2 + z_2'),$$

och

$$(z_1, z_2)(z_1', z_2') = (z_1 z_1' - z_2 \bar{z}_2', z_1 z_2' + \bar{z}_1' z_2),$$

där $\bar{z} = a - bi$ (z konjugat) om $z = a + bi$. Man observerar att

$$(z_1, 0) + (z_1', 0) = (z_1 + z_1', 0),$$

och

$$(z_1, 0)(z_1', 0) = (z_1 z_1', 0).$$

Detta visar att de komplexa talen kan identifieras med paren $(z, 0)$. Därför skriver vi $(z, 0) = z$. Beteckna också $(0, 1) = j$ och $(0, i) = k$. Vi har $j^2 = (0, 1)(0, 1) = (-1, 0) = -1$ och $k^2 = (0, i)(0, i) = (-1, 0) = -1$. Dessutom har vi $(0, c + di) = (0, c) + (0, di) = (c, 0)(0, 1) + (d, 0)(0, i) = cj + dk$. Därför kan vi skriva:

$$q = (a + bi, c + di) = (a + bi, 0) + (0, c + di) = a + bi + cj + dk.$$

Detta är en typisk kvaternion. Dess *konjugat* är $\bar{q} = a - bi - cj - dk$ och dess *belopp* är kvadratroten ur $q\bar{q} = a^2 + b^2 + c^2 + d^2$.

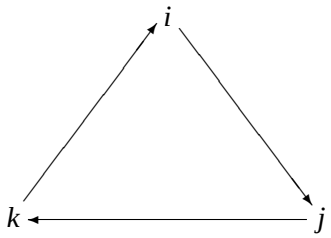
[¶] W.R. Hamilton (1805-1865).

För att snabbt kunna räkna med kvaternioner är det bäst att kontrollera följande multiplikationsregler:

ij = -*ji* = *k*,

jk = -*kj* = *i*,

ki = -*ik* = *j*.



Vi ser att multiplikation av kvaternioner inte är kommutativ. Låt oss sammanfatta**:**

(10.24) Sats. *Alla kvaternioner* $a + bi + cj + dk$*, där* $i^2 = j^2 = k^2 = -1$ *och* $ij = -ji = k$*, bildar en algebraisk struktur* $\mathbb{H}$ *som uppfyller alla villkor i definitionen av en kropp med undantag av multiplikationens kommutativitet. Dessutom uppfyller varje kvaternion en andragradsekvation med reella koefficienter.*

För det sista påståendet i satsen se övningen om kvaternioner. Ibland säger man att $\mathbb{H}$ är en icke-kommutativ kropp, men termerna **skevkropp** eller **divisionsring** är mera vanliga. Satsen är inte svår att bevisa.