Om ideale elementer i matematikken

Klaus Frovin Jørgensen

7. september 2011

I artiklen "Über das Unendliche" beskriver David Hilbert (1862-1943) i ret udførlige detaljer sin matematikfilosofi og mere specifikt sit program i forhold til at komme vanskelighederne vedrørende matematikkens grundlag til livs. (Hilbert, 1926).

Det uendelige spiller naturligvis en stor rolle i matematikken, og Hilbert mener, at matematikken på mange måder nærmest er karakteriseret ved at være studiet af det uendelige. Som Hilbert beskriver det, er det uendelige ikke realiseret i den fysiske verden. Det er kun inden for matematikken, at vi ved hjælp af idealiseringer kan håndtere det uendelige. Men det er selvfølgelig på ingen måde selvindlysende eller på anden måde simpelt, hvordan dette skal gøres, og Hilbert er opmærksom på, at de problemer man stødt på med hensyn til matematikkens grundlag meget vel kan skyldes, at man endnu ikke helt har forstået det uendeliges natur og rolle i matematikken.

På et overordnet plan mener Hilbert, at den matematiske metode helt generelt består af en regressiv og en progressiv del. Den progressive del giver anledning til nye objekter og begreber i matematikken. Matematikken ekspanderer som videnskab, men det er på baggrund af den regressive metode, at vi skal sikre, at det ikke går galt. Centralt i den progressive metode står det, som Hilbert kalder, introduktionen af *ideale elementer*.

Hilbert mente at de ideale elementer grundlæggende har til opgave at: Systematisere, generalisere, skabe sammenhæng, fuldstændiggøre og afslutte matematikken. Men de spiller også en central rolle i forbindelse med opdagelser og forklaringer.

Nedenfor gennemgås en længere række eksempler på brugen og introduktionen af ideale elementer i matematikken. Det kan – for at komme en forståelse af ideale elementer nærmere – være relevant at kigge på disse eksempler samt diskutere, hvorledes eksemplerne illustrerer de ideale elementers rolle i forbindelse med udviklingen af matematisk viden:

Eksemplerne er:

1. Brugen af indivisibler i den førmoderne matematik.
2. Introduktionen af reelle og komplekse tal.
3. Projektiv geometri, som fuldstændiggørelsen af euklidisk geometri.
4. Udvalgsaksiomet.
5. Frembringende funktioner.

1 Indivisibler

Introduktionen af *indivisibler* kan på flere måder ses som en introduktion af et idealt element. I dag ved vi, at i antikken benyttede i hvert fald Archimedes (ca. 287-212 f.Kr) sig af indivisibler, selv om dette ikke fandt vej til de mere 'officielle' tekster. Men brugen af indivisibler bryder på flere måder med det, vi kunne kalde for Det græske paradigme. Ikke desto gjorde man altså brug af indivisibler i antikken.

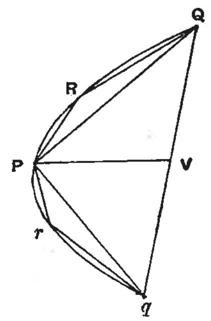
Vi skal i dette eksempel se, hvordan Archimedes på to forskellige måder finder arealet under en parabel. Den første måde findes i den 'officielle tekst', *Parablens kvadratur* (Archimedes, 1897, 233-252), og gør brug af det, vi kalder for et udtømningsbevis. Det andet bevis findes i teksten *Om metoden* (Archimedes, 1912). Det er værd at bemærke det elegante og den direkte tilgang, som de sidste bevis har. Og det er også værd at bide mærke i Archimedes' egen kommentar: Det er ved brug af denne anden metode, at resultaterne rent faktisk findes.

1.1 Archimedes' udtømningsbevis

Archimedes' 'officielle' tekst gør ikke brug af indivisibler, og det holder sig derved inden for det græske paradigme. Lad os først se, hvordan parablens kvadratur løses uden brug af indivisibler. Bagefter kigger vi på brugen af indivisibler til løsningen.

Den oprindelige teksten er *Parablens kvadratrur'*, og den ender med følgende sætning:

> **Proposition 24.** Every segment bounded by a parabola and a chord Qq is equal to four-thirds of the triangle which has the same base as the segment and equal height.



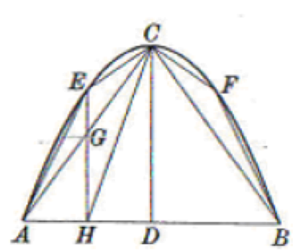
(Archimedes, 1897, 251)

Et vigtigt lemma for beviset af parablens kvadratur er sætning 23, som siger at givet en følge af arealer $A, B, C, D, \ldots, Z$, hvor A er det største og alle arealerne er fire gange så stor, som det næste areal i følgen, så gælder der følgende lighed:

$$A + B + C + \ldots + Z + {}^{1}\!/\!_{3}Z = {}^{4}\!/\!_{3}A.$$

Vi beviser ikke sætning 23 her, men et bevis for sætning 24 (parablens kvadratur) er følgende:

Dan $\triangle ABC$ og del den i de to rette trekanter $\triangle ADC$ og $\triangle BDC$ (se nedenstående figur). Kald midten af AD for H og konstruér midtnormalen HE.



Keglesnitslæren siger $EG = {}^{1}\!/\!_{2}GH$. Dette medfører at forholdet mellem $\triangle AEG$ og $\triangle AGH$ er ${}^{1}\!/\!_{2}$, hvilket også gør sig gældende for forholdet mellem $\triangle GEC$ og $\triangle HGC$. Dette giver

$$\triangle AEC = \frac{1}{2}\triangle AHC = \frac{1}{8}\triangle ABC$$

Af symmetri-grunde har vi:

$$\triangle AEC + \triangle BFC = \frac{1}{4}\triangle ABC.$$

Hvis vi fortsætter denne måde at halvere korden på, får vi en samling trekanter, hvis arealer vi kan skrive op som en følge:

$$\triangle ABC, \frac{1}{4}\triangle ABC, \frac{1}{4^2}\triangle ABC, \ldots \tag{1}$$

Lad Σ betegne det efterspurgte areal, det vil sige Σ er parablens kvadratur. Yderligere sætter Archimedes K til at være $\frac{4}{3}\triangle ABC$. Heraf kan vi trivielt slutte:

$$K < \Sigma \text{ eller } K = \Sigma \text{ eller } K > \Sigma.$$

Men nu 'gætter' Archimedes på, at K faktisk er lig Σ. At dette faktisk også er tilfældet vises nu ved et et dobbelt-modstrids-bevis; altså han viser, at hverken den første eller den sidste mulighed gælder.

Antag $\Sigma < K$. Ovenfor så vi, hvordan det at halvere korden gav anledning til følge af arealer (se formel 1). Lad nu S_n være den n-te sum af denne følge. Denne sum består af arelaer, som ligger under parablen. Vi har altså:

$$S_n = \triangle ABC + \frac{1}{4}\triangle ABC + \cdots + \frac{1}{4^n}\triangle ABC < \Sigma.$$

Vælg en følge S_n, sådan at det sidste led, kald det X, i følgen er mindre end forskellem mellem K og Σ, dvs:

$$K - \Sigma > X$$

Fra lemmaet (sætning 23) har vi, at

$$K = \frac{4}{3}\triangle ABC = \triangle ABC + \frac{1}{4}\triangle ABC + \cdots + X + \frac{1}{3}X.$$

Men herved kommer $\triangle ABC + \frac{1}{4}\triangle ABC + \cdots + X = S_n$ til at overstige Σ, hvilket er en umulighed, da afsnitssummen altid ligger indenfor parablen.

På lignende giver antagelsen om $K < \Sigma$ også en modstrid.

Derved kan Archimedes slutte, at $\Sigma = K = \frac{4}{3}\triangle ABC$.

1.2 Archimedes' bevis ved brug af indivisibler

Lad os nu kigge nærmere på, hvordan Archimedes' bevis ved brug af indivisibler forløber. I 'forordet' til teksten *Om metoden* skriver Archimedes til Erastosthenes (en elev af Archimedes):

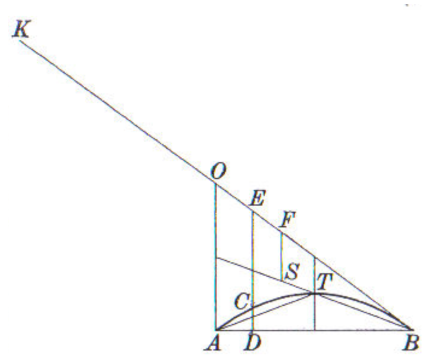
> I sent you on a former occasion some of the theorems discovered by me, merely writing out the enunciations and inviting you to discover the proofs, which at the moment I did not give. The enunciations of the theorems which I sent were as follows.
>
> (Archimedes, 1912, 13)

I teksten præsenterer Archimedes en 'metode' til sin elev, og denne metode kan siges at være karakteriseret ved følgende:

1. Brug af et vægtstangsprincip, så arealer kan 'vejes'.

2. Arealet af en figur i planen forstås som (samlingen) af alle parallelle linjestykker, der så at sige udgør figuren.

Lad os se, hvordan denne metode bliver brugt i Archimedes' bevis for parablens kvadratur



Lad parabelbuen AB være givet og konstruér tangenten til B. Forlæng denne til K, sådan at O bliver midtpunkt til BK ($OK = OB$). Konstruér DE parrallel til AO. Fra keglesnitslæren har vi:

$$CD : ED = AD : AB$$

$$CD : ED = OE : OB$$

Dette medfører:

$$CD : ED = OE : OK$$

'Hæng' nu CD ud på K. Ved vægtstangsprincippet er CD nu i ligevægt med ED (ophængt i E).

Gør nu det samme for alle ordinaterne. Derved får vi, at hænges alle 'stykkerne' under parabelbuen op i K, så balanceres dette af $\triangle BOA$.

Da S er medianernes skæringspunkt, kan vi se S som ligevægtspunktet for $\triangle BOA$. Derved kan vi forstå $\triangle BOA$ som ophængt i F. Archimedes kan nu relativt simpelt konstatere at $OK = 3OF$ og at $\triangle BOA = 4\triangle ATB$, hvor man får

$$\Sigma = \frac{1}{3}\triangle BOA = \frac{4}{3}\triangle ATB.$$

Bemærk, hvor simpelt, elegant og direkte indivisibel-beviset er. Bemærk også, at Archimedes nævner, at det netop er indivisblerne, som har en afgørende betydning i forhold til at *opdage* sætningerne.

1.3 Torricellis tragt

Torricellis tragt er et andet godt eksempel på indivisblernes elegance. Toricellis tragt er en uendelig figur med et endeligt volume men en uendelig overflade. Der er to forskellige beviser for, at dette faktisk er tilfældet: Et bevis, som benytter indivisibler (og det såkaldte Cavalieris princip) og så et udtømningsbevis. Se (Mancosu og Vailati, 1991) for en gennemgang af dette.

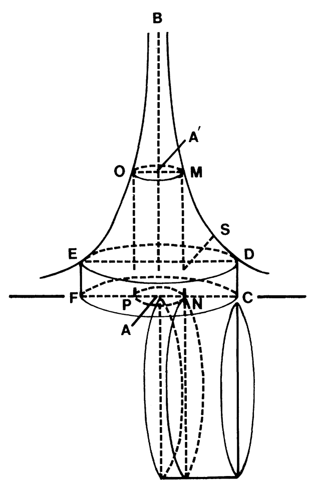


Figure 2

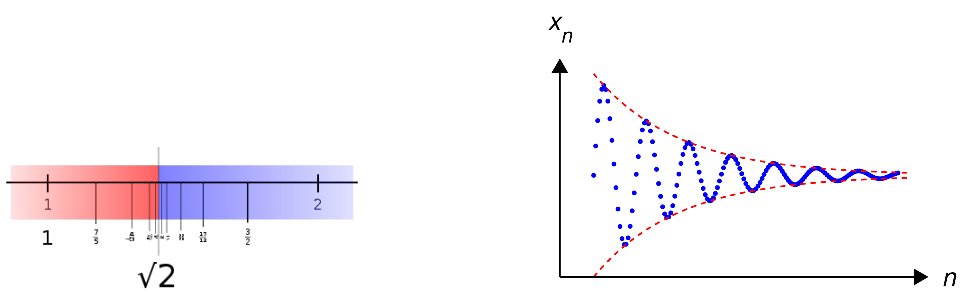
Figur fra (Mancosu og Vailati, 1991, 54)

2 De reelle og komplekse tal

Matematisk fik man imidlertid aldrig helt styr på indivisiblerne. Men de var gode til generelt at skabe orden og sammenhæng i de betragtninger, man gjorde sig inden for rækkerudviklingen og inden for integral- og differentialregningen. Konvergensbetragtningerne gik op. Men matematisk set fik man ikke de præcise formuleringer på plads, og man måtte ty til forskellige mulige (og umulige) intuitioner.

Med den såkaldte *aritmetisering* af de reelle tal kom grundlaget for disse i den sidste halvdel 1800-tallet endeligt på plads. Konvergensbetragtninger på baggrund af de reelle tal sendte indivisiblerne på pension og sikrede brugen af eksempelvis uendelige rækker. De reelle tal skabte i den grad orden.

De reelle tal introduceres typisk som Dedekindsnit eller som Cauchyfølger.



Dedekindsnit og Cauchyfølge. Illustrationer fra Wikipedia.

Lad os kigge på eksemplet med Cauchyfølger. En følge af rationelle tal $x_1, x_2, \dots$ er en *Cauchyfølge*, hvis der for ethvert ε eksisterer et N således, at for alle $n, m > N$

$$|x_n - x_m| < \varepsilon$$

Vi danner nu klassen **Cau** af alle Cauchyfølger, og på baggrund af denne klasse kan vi konstruere de reelle tal, som ækvivalensklasser af Cauchyfølger. Vi har således brug for ækvivalensrelation[1] mellem Cauchyfølger. Vi siger, at to Cauchyfølger (a_n) og (b_n) er ækvivalente, hvis deres forskel er 0 i grænsen; altså:

$$(a_n) \sim (b_n) \Leftrightarrow \lim(a_n - b_n) = 0$$

Fra klassen **Cau** af Cauchy-følger konstrueres de reelle tal som ækvivalensklasser:

$$[(a_n)] = \{(b_n) \in \mathbf{Cau} \mid (a_n) \sim (b_n)\}.$$

[1] Vi siger, at $\sim$ er en *ækvivalensrelation* over D, når den er refleksiv, symmetrisk og transitiv, dvs. hvis det for alle elementer i D gælder at:

i) $x \sim x$

ii) $x \sim y$ medfører $y \sim x$

iii) $x \sim y$ og $y \sim z$ medfører $x \sim z$

Bemærk, et reelt tal er generelt en ret uendelig størrelse: Dels er enhver repræsentant[2] for et reelt tal en uendelige følge, dels har hver ækvivalensklasse uendeligt mange elementer.

Vi definerer regneregler på de reelle tal. Lad x og y være reelle tal. Vælg (a_n) i x og (b_n) i y; vi definerer da

$$\begin{aligned} x+y &= [(a_n+b_n)] \\ x\cdot y &= [(a_n b_n)] \\ 0 &= [(0)] \\ 1 &= [(1)] \end{aligned}$$

Vi kan ligeledes definere $<$ for de reelle tal. Og derved bliver det muligt at bevise, selv om det er langt bevis, at

$$\mathbf{R} = (\mathbf{Cau}/\!\sim, +, \cdot, <)$$

er et fuldstændigt ordnet arkimedisk legeme. Altså *fuldstændigt, uden infinitisimaler med* $\mathbf{Q}$ *tæt i* $\mathbf{R}$.

Vi har lige set et eksempel på det, man inden for algebraen kalder for den generiske metode: Man konstruerer på baggrund af nogle allerede givne objekter (i dette tilfælde de rationelle tal) nogle nye objekter (i dette tilfælde de reelle tal) ved at lave en kvotientstruktur. På denne måde konstrueres de reelle tal nede fra og op. Det er derfor det kaldes for aritmetiseringen af analysen.

Generelt opstår objekter som ækvivalensklasser af mere simple objekter. Vi kan konstruere de hele tal, de rationelle tal, de reelle tal, de imaginære tal på denne måde.

Ækvivalensrelationer står således centralt og enhver ækvivalensrelation $\sim$ har en *karakteristisk funktion*:

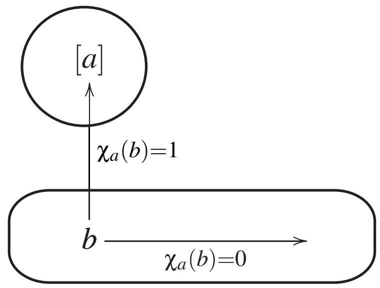
$$\chi(a,b) = \begin{cases} 1, & \text{hvis } a \sim b, \\ 0, & \text{ellers.} \end{cases}$$

Vi kan parametrisere χ:

$$\chi_a(b) = \begin{cases} 1, & \text{hvis } a \sim b, \\ 0, & \text{ellers.} \end{cases}$$

Således kan vi forstå χ_a som en funktion, der netop sender alle b over i a's ækvivalensklasse, dersom b er ækvivalent med a.. Dette kan illustreres på følgende måde:

[2] En repræsentant er i dette tilfælde en Cauchyfølge, som så at sige generere en ækvivalensklasse.



På denne led kan vi (intensionelt) forstå en ækvivalensklasse som genereret af et *i)* paradigmatisk eksempel samt *ii)* den tilhørende karakteristiske funktion. Så når vi generelt inden for algebraen konstruerer nye objekter ved hjælp af den skitserede kvotientkonstruktion, så kan vi forstå de nye objekter – i vores tilælde de nye tal – som bestående af:

1. Et *prototypisk* eksempel,

2. Den tilhørende *karakteristiske funktion*.

Det afgørende i dette tilfælde er følgende. Når vi konstruerer **Z** og **Q** på denne måde, så er de karakteristiske funktioner *afgørbare*. Det vil sige, at der findes en algoritme sådan at givet eksempelvis to rationelle tal q_1 og q_2, så afgør algoritmen i et endeligt tidsrum om q_1 er lig q_2 eller ej. Men i modsætning til de naturlige og rationelle tal, så er lighedsrelationen mellem reelle tal *ikke* afgørbar. Og dette skyldes netop det faktum at vi generelt forstår reelle tal som nogle uendelige størrelser. Og som sådan er de altså også at forstå som ideale elementer.

Det følgende er et eksempel på et umiddelbart uafgørbart spørgsmål vedrørende reelle tal. Lad $R(n)$ stå for: "De $n-99$ til n decimaler i π er alle 9-taller". Det vil sige, hvis der eksisterer et n sådan at $R(n)$ faktisk er sand, så eksisterer der 100 9-taller i træk et sted i decimaltalsudviklingen af π. Man ved i dag ikke, om dette faktisk er tilfældet eller ej. Definér nu:

$$a_n = \begin{cases} 2^{-n} & \text{hvis} \quad \forall k \leq n \neg R(k) \\ 2^{-k} & \text{hvis} \quad k \leq n \text{ og } R(k) \text{ og } \forall p < k \neg R(p) \end{cases}$$

Vi kan nu faktisk ikke afgøre om (a_n) er element i 0 eller ej. Ækvivalensklassen til 0 kan vi med andre ord ikke skarpt afgrænse. Således er de karakteristiske funktioner til ækvivalensklasserne i **R** ikke – som i tilfældene **N**, **Z** og **Q** – afgørbare.

De reelle tal er altså selv ideale elementer. De er uendelige og det er ikke alle egenskaber ved dem, vi generelt kan afgøre. Men de skaber en sammenhæng og fuldstændiggører: Vi kan lave følger af rationelle tal, som ikke konvergerer til noget rationelt tal, men som kun konvergerer til et reelt tal. Der findes altså 'huller' i **Q**. Tilføjer vi derimod de irrationelle tal fuldstændiggøres tallene: En hvilken som helst konvergent følge af reelle tal konvergerer til et reelt tal. Tallegemet afsluttes med tilføjelsen af de reelle tal.

2.1 De komplekse tal

Hilbert nævner selv de komplekse – eller som de også hedder *imaginære* tal som et eksempel på ideale elementer. Når vi introducerer de komplekse tal bliver teorierne pæne og harmoniske, og tingene går så at sige op. De komplekse tal konstrueres ud fra de reelle. Lad **C** er mængden af alle komplekse tal hvilke har formen $a+bi$, hvor a og b er reelle tal og $i=\sqrt{-1}$. Med de komplekse tal bliver det muligt, eksempelvis, at vise:

Algebraens hovedsætning. Ethvert polynomium af grad n

$$p(x) = x^n + a_1x^{m_1} + a_2x^{m_2} + \cdots + a_{k-1}x + a_k$$

har n rødder i **C**.

3 Projektiv geometri som fuldstændiggørelsen af euklidisk geometri

Vi kan forstå projektiv geometri som en fuldstændiggørelse af euklidisk geometri. Punkter og linjer i det uendelige tilføjes, hvorved det frugtbare dualitetsprincip kan bevises.

Den projektive geometri opstod blandt andet på baggrund af de diskussioner man i matematikhistorien havde omkring det euklidiske parallelaksiom. Lad os prøve at kigge på teorierne i en moderne formulering og derfor introducerer vi det affine plan og dets aksiomer. Dette plan forstår vi, i første omgang, som et euklidisk plan, bare uden begreberne afstand, vinkel og koordinator.

Vi arbejder med linjer og punkter og et punkt A ligger enten på l eller også gør det ikke. To linjer er *parallelle*, hvis de ingen punkter har tilfælles, og to eller flere punkter er *kolineære* hvis der findes en linje, hvorpå punkterne ligger. To eller flere linjer siges at være *konkurrente*, hvis de alle har et punkt tilfælles.

Den affine plan består af punkter og linjer, samt en bestemt relation imellem disse. Punkterne udgør en mængde og linjerne er delmængder af denne mængde. Den affine plan opfylder tre aksiomer:

A1 Givet to punkter A og B eksisterer der netop en linje, som indeholder A og B.

A2 Givet en linje l og et punkt A, som ikke ligger på l, da eksisterer der netop en linje, som er parallel med l og som indeholder A.

A3 Der eksisterer tre punkter, som ikke er kolineære.

Den mindste (og endelige) affine plan består af fire punkter A,B,C og D og linjerne imellem disse punkter. Det vil sige linjerne AB,AC,AD,BC,BD,CD. Det er ikke svært at overbevise sig selv om, at denne konfiguration af punkter og linjer opfylder aksiomerne $A1$–$A3$; f.eks. er AC og BD parallelle.

Den projektive plan kan ses som fuldstændiggørelsen af den affine plan. Det får vi at se om lidt. Men lad os først give aksiomerne for den projektive plan.

P1 Givet to punkter A og B eksisterer der netop en linje, som indeholder A og B.

P2 To linjer l og m mødes altid i et punkt.

P3 Der eksisterer tre punkter, som ikke er kolineære.

P4 Alle linjer består af mindst tre punkter.

Givet den mindste affine plan, som vi så ovenfor, så kan vi nu konstruere den mindste projektive plan på baggrund heraf. Vi bibeholder de fire punkter A,B,C og D. Men en linje i den projektive plan består af mindst tre punkter. Derfor tilføjer vi til linjen BA punktet P. Linjen hedder så BAP. I den affine plan var BA og CD parallelle. Men i den projektive plan har to linjer et punkt tilfælles. Derfor forlænger vi, så at sige, CD til P, sådan at den 'nye' linje i den projektive plan hedder CDP. Fra den affine plan har vi linjerne AD og BC, som der var parallelle. Dem forlænger vi i den projektive plan til R. AD og BC var parallelle i den affine plan. Men lad dem mødes i et 'nyt' punkt Q. Den konstruerede konfiguration består af syv punkter og syv linjer. Alle linjer har tre punkter og alle punkter tilhører tre linjer. Og det er ikke svært at tjekke, at konfigurationen opfylder aksiomerne P1–P4.

Man kan forstå det affine plan som det projektive plan minus en linje. Rent faktisk giver ethvert projektiv plan anledning til en affin plan, når man trækker en men kun en linje ud af den projektive plan.

Sætning. En projektiv plan minus en linje er en affin plan.

Lad en projektiv plan π være givet. Vi så i det foregående eksempel at π mindst indeholder syv linjer; kald de tre af dem for l,m og n. Givet P2 har vi, at l skærer alle linjer i et punkt, og derfor vil alle linjer miste et punkt, når vi skærer l ud af π. Lad os sige, at A er skæringspunktet mellem m og l i π. Vi efterviser nu A1–A3.

A1. Da π opfylder P1 så opfylder $\pi - l$ også P1, som er det samme som A1.

A2. Lad P være et punkt i $\pi - l$, sådan at P ikke ligger på m. Vi skal vise, at der findes en linje i $\pi - l$, sådan at denne linje er parallel til m. I π er punktet A der hvor m og l skærer hinanden. Dan nu i π linjen AP. Denne har mindst tre punkter, kald det tredje Q. Når vi skærer l ud af π, så er PQ en linje i $\pi - l$, blot uden punktet A. PQ er parallel til m, da deres eneste skæringspunkt i π er skåret ud i $\pi - l$.

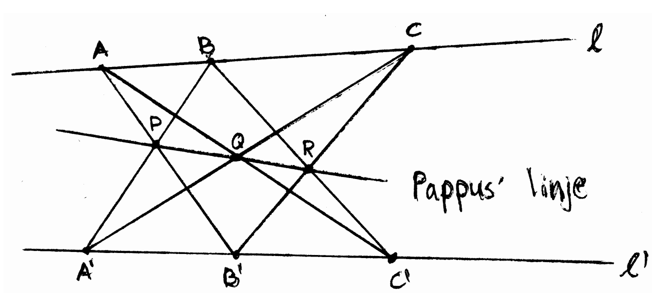
A3. Da to linjer m og n ifølge P1 består af mindst to punkter hver ikke på l, eksisterer der tre ikke-kolineære punkter i $\pi - l$.

3.1 Dualitetsprincippet

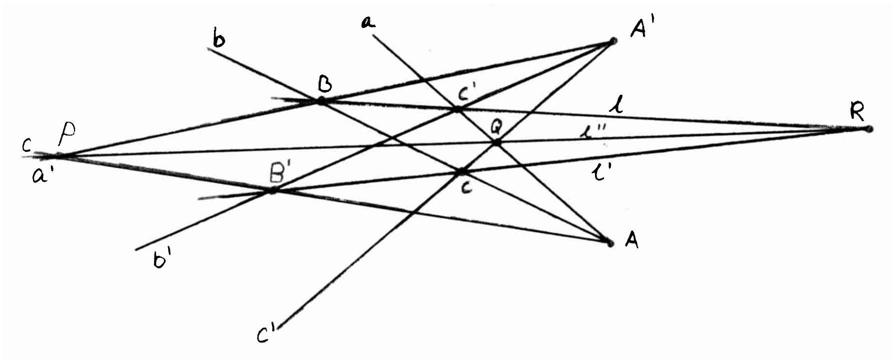
Vi kan altså forstå den projektive plan som den affine plan tilføjet en ekstra linje: En linje vi kunne kalde for linjen i det uendelige. På denne led 'afsluttes' den affine plan på en særlig måde, hvilket giver den en ganske særlig egenskab, som kommer til udtryk i det, man kalder for dualitetsprincippet. Hvis man i et geometrisk udsagn α inden for den projektive geometri bytter om på punkt og linje og vender relationerne om, så får man det man kalder det duale udsagn kaldet $\alpha*$. I α bytter man altså "punkt" ud med "linje", og "linje" ud med "punkt", "konkurrens" ud med "kolinearitet", "ligger på" ud med "indeholder" osv. så får man altså det duale udsagn $\alpha*$. Man kan vise, at hvis α gælder i den projektive geometri, så gælder $\alpha*$. Det er for eksempel relativt nemt at tjekke, at de duale udsagn til aksiomerne gælder.

Princippet er selvfølgelig et meget brugbart og frugtbart princip: Når man har bevist en sætning, har man i virkeligheden bevist to.

Pappus' sætning, som siger, at givet to linjer l og l' med tripler af punkter (A,B,C) og (A',B',C') respektivt; givet linjer til de modstående 'alternerende' punkter (se figur), så vil skæringspunkterne P,Q,R være kolineare.



Pappus' sætning gælder ikke i alle projektive geometrier. Men i de geometrier, som den gælder, der gælder det duale udsagn også.



Den duale Pappus-konfiguration.

4 Udvalgsaksiomet

I 1904 introducerede den tyske matematiker Ernst Zermelo (1871-1953) *udvalgs-aksiomet*. Zermelo arbejdede i Göttingen og var under stærk indflydelse fra Hilbert. Udvalgsaksiomet var forsåvidt blevet brugt, omend implicit, af matematikere før Zermelo, men Zermelo var den første til at indse aksiomets fundamentale betydning, idet Zermelo påviste, at aksiomet var nødvendigt for at bevise, at enhver mængde kan velordnes (velordningssætning). Tidligere, i 1883, havde Georg Cantor (1845-1918) hævdet, at sætningen om velordning var en gyldigt princip, men det lykkedes aldrig for Cantor at bevise princippet. Det var Zermelos fortjeneste at formulere det generelt yderst frugtbare udvalgsaksiom samt vise, hvorledes velordning baserer sig på udvalgsaksiomet. Som vi kan se på nedenstående liste af konsekvenser af aksiomet, er dette virkelig et aksiom, som er frugtbart og som afslutter og gør 'tingene' pæne.

Udvalgsaksiomet siger, at til en samling af ikke-tomme mængder, så kan vi udplukke netop et element fra hvert af mængderne. Eller sagt lidt mere formelt: Give Figur fra wikipedia: "Banach-Tarski Paradox". t en samling $\{S_i \mid i \in I\}$ af ikke-tomme mængder, eksisterer der en valgfunktion f sådan at

$$f : I \longrightarrow \bigcup_i S_i, \quad f(i) \in S_i, \text{ for alle } i \in I.$$

Konsekvenser af Udvalgsaksiomet:

- Enhver mængde kan velordnes.
- Ordning efter kardinalitet er en total ordning. Altså: givet to mængder A og B så er kardinaliteten af de to enten den samme, eller også er kardinaliteten af den ene mindre end den anden.

- Ethvert vektorrum har en basis.

- Hahn-Banachs sætning: En lineær funktional, defineret på et delrum af et vektorrum, som er begrænset af en seminorm, kan udvides til en lineær funktional, begrænset af samme seminorm, på hele rummet.

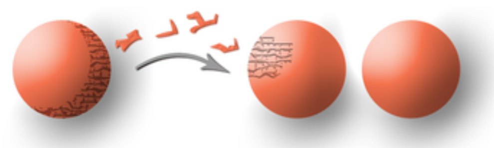
- Zorns Lemma: Alle partielt ordnede mængder A, hvor enhver kæde (dvs. totalt ordnet delmængde) har en øvre grænser i A, indeholde mindst et maksimalt element x. At $x \in A$ er maksimalt vil sige, at for alle $y \in A$ gælder der, at $x \leq y$ medfører $x = y$..

- Ethvert legeme har en algebraisk udvidelse, som er algebraisk afsluttet. At et legeme K er algebraisk afsluttet vil sige, at ethvert polynomium i en variabel af grad ≥ 1 med koefficienter i K har rødder i K.

- Tychonoffs Sætning. Produktet af enhver samling af kompakte topologiske rum er kompakt.

Det er værd at bemærke, at Udvalgsaksiomet således har helt centrale resultater spredt bredt udover matematikken: Generel mængdelære, funktionalanalyse, topologi, algebra. Mange andre matematiske discipliner nyder også godt af aksiomet.

Men man skal også vide, at der følger også såkaldte paradokser, eksempelvis det såkaldte Banach-Tarski paradoks.



Figur fra wikipedia: "Banach-Tarski Paradox".

5 Frembringende funktioner

Lad os forestille os, at vi er givet en følge af tal $a_0, a_1, a_2, \ldots$. Spørgsmålet er nu: Hvordan kan vi pakke alle disse tal ned i et objekt, som så at sige husker alle disse tal? Et svar på spørgsmålet kunne være *frembringende funktioner* Frembringende funktioner går tilbage til Laplace.

At frembringende funktioner er et eksempel på de idealer elementer er ikke et eksempel, som Hilbert giver. Men det kunne det lige så godt have været. Eksemplet berører nemlig noget helt centralt og noget meget generelt ved *den matematiske metode*: Indlejring af 'simple´ problemer i en 'kompleks´kontekst', hvorved det simple problem **løses**.

Frembringende funktioner benyttes mange steder i matematikken. Blandt andet inden for: talteori, sandsynlighedsregning, kombinatorik, kombinatorisk analyse. Imidlertid er det essentielle, at indlejre et simpelt problem i et mere komplekst.

Definition. Hvis (a_k) er en følge af tal, så er *den frembringende funktion* for (a_k) den (formelle) potensrække:

$$P(z) := \sum_{k=0}^{\infty} a_k z^k \ := \big(\sum_{k=0}^{n} a_k z^k \big)_{n \geq 0}$$

hvor z typisk er kompleks.

Bemærk, at definitionen skal forstås som en uendelig følge af endelige summer. Dette er det *formelle* aspekt af 'objektet': Vi vil sådan set undgå spørgsmålet vedrørende om rækken er konvergent eller ej. Det er ikke det, som er det relevante i denne sammenhæng. . Det centrale er altså, at det er en *formel potensrække*. Det er ikke det, at der skulle være noget funktions-agtigt over udtrykket, ej heller, at der skulle være noget frembringende over det — men det er udelukkende det, at der er tale om en følge af endelige summer (og derved bekymrer vi os ikke det fjerneste om konvergens). Det er dette aspekt, som er det metodiske trick her. Så i mange tilfælde vil man betragte $P(z)$ som et *formelt* (eller blot et *symbolsk*) objekt.

Det helt generelle problem, som man kunne være interesseret i at løse med de formelle potensrækker – altså med de frembringende funktioner er: Lad (a_k) være en rekursiv følge, dvs.:

$$a_k = q_1 a_{k-1} + q_2 a_{k-2} + \cdots + q_d a_{k-d}.$$

Problemet består nu i, at finde et såkaldt lukket udtryk for a_k; dvs. hvordan når vi frem til en funktion g, sådan, at $g(k) = a_k$, og sådan at g direkte giver dette, uden at skulle regne alle de forgående tal i følgen ud.

Motivation for at finde et sådan udtryk kunne være:

- Hvad er følgens sammenhæng til resten af matematikken?
- Hvad er følgens asymptotiske opførsel?
- Ønsket om en mere effektiv beregning af det k-te element.

Lad os give et eksempel på brugen af frembringende funktioner. Fibonacci [Leonardo af Pisa (1175–1250)] tallene beskriver ideelle populationer:

0	1	2	3	4	5	6	7	$\cdots$	10	$\cdots$	14	$\cdots$	20	$\cdots$
0	1	1	2	3	5	8	13	$\cdots$	55	$\cdots$	377	$\cdots$	6765	$\cdots$

Lad f være den elementære talteoretiske Fibonacci-funktion:

$$f(0)=0, f(1)=1 \text{ og for } n \geq 2, f(n)=f(n-1)+f(n-2).$$

Dette er en rekursiv definition af Fibonaccitallene, og spørgsmålet går nu ud på, at finde et lukket udtryk for $f : \mathbf{N} \longrightarrow \mathbf{N}$. Problemet er selvfølgelig: Hvordan finder man lige på det? Løsningen – som vi straks skal se – er kompliceret. Og det er et godt spørgsmål, hvordan man finder frem til den løsning.

Sæt $\phi = \frac{1+\sqrt{5}}{2}$ og $\hat{\phi} = \frac{1-\sqrt{5}}{2}$. Så er J. Binets formel fra 1843 er:

$$f(n) = \frac{1}{\sqrt{5}}(\phi^n - \hat{\phi}^n).$$

Induktionsbevis. $f(0)=0$ og $f(1)=1$. Lad nu $n>0$. Bemærk, at $\phi^2 = \phi+1$ og $\hat{\phi}^2 = \hat{\phi}+1$. Således har vi

$$\begin{aligned} f(n+1) &= f(n)+f(n-1) \\ &= \tfrac{1}{\sqrt{5}}\big(\phi^n - \hat{\phi}^n\big) + \tfrac{1}{\sqrt{5}}\big(\phi^{n-1} - \hat{\phi}^{n-1}\big) \\ &= \tfrac{1}{\sqrt{5}}\big((\phi^n + \phi^{n-1}) - (\hat{\phi}^n + \hat{\phi}^{n-1})\big) \\ &= \tfrac{1}{\sqrt{5}}\big(\phi^{n+1} - \hat{\phi}^{n+1}\big) \end{aligned}$$

Men det vanskelige spørgsmål er nu: Hvordan finder man frem til Binets formel?

Det er klart, at induktionsbeviset viser, at Binets formel er korrekt, men det giver ikke megen information, som kan fortælle om *opdagelsen*. Eller som kan fortælle os *hvorfor* er formlen korrekt? Dertil har vi brug for de frembringende funktioner – de ideale elementers metode. Og til dette er de frembringende funktioner *storslåede*.

Vi definerer først på hele $\mathbf{Z}$.

Lad $[n=1]$ være karakteristisk funktion for "n er lig 1", dvs:

$$[n=1] = \begin{cases} 1, & \text{hvis } n=1, \\ 0, & \text{ellers,} \end{cases}$$

Lad $[n>0]$ være en tilsvarende karakteristisk funktion. Vi kan nu definere f på een formel, sådan at for alle hele tal n:

$$f(n) = [n>0]\big(f(n-1)+f(n-2)+[n=1]\big).$$

Lad os danne den frembringende funktion for f:

$$F(z) = \sum_{n=0}^{\infty} f(n) z^n, \qquad z \in \mathbf{C}.$$

Og brug så en-linjes-definitionen af f.

$$\begin{aligned}
F(z) &= \sum_{n=0}^{\infty} \Big([n>0](f(n-1)+f(n-2)+[n=1])\Big)z^n \\
&= \sum_{n=0}^{\infty} f(n-1)z^n \ + \ \sum_{n=0}^{\infty} f(n-2)z^n \ + \ \sum_{n=0}^{\infty}[n=1]z^n \\
&= \sum_{n=0}^{\infty} f(n)z^{n+1} \ + \sum_{n=0}^{\infty} f(n)z^{n+2} \ + z \\
&= z\sum_{n=0}^{\infty} f(n)z^n \ + \ z^2\sum_{n=0}^{\infty} f(n)z^n \ + \ z \\
&= F(z)(z+z^2)+z.
\end{aligned}$$

Isolering af $F(z)$ giver:

$$F(z) = \frac{z}{1-z-z^2}$$

Vi rækkeudvikler nu F. Og smider alle de komplekse udtryk væk. Det vil sige, vi går fra det komplekse tal tilbage til de reelle. Dermed får vi hurtigt vores ønskede lukkede udtryk.

Lad ϕ og $\hat{\phi}$ være som før. Da $F(z)$ er en rationel funktion, kan den (for $|z|$ tæt på 0) udvikles som partialbrøk:

$$F(z) = \frac{1}{\sqrt{5}}\left(\frac{1}{1-\phi z} - \frac{1}{1-\hat{\phi}z}\right).$$

De to indre brøker kan udvikles som geometriske rækker:

$$\frac{1}{1-\phi z} = \sum_{n=0}^{\infty}(\phi z)^n, \qquad \frac{1}{1-\hat{\phi}z} = \sum_{n=0}^{\infty}(\hat{\phi}z)^n.$$

Dermed får vi:

$$F(z) = \sum_{n=0}^{\infty}\frac{1}{\sqrt{5}}\big(\phi^n - \hat{\phi}^n\big)z^n.$$

Binets formel blev fundet i en tid hvor man netop var begyndt at bruge analytiske metoder inden for talteori og kombinatorik: Først Euler (1707-1783), siden Dirichlet (1805-1859). Men lad os kigge lidt på den aymptotiske udvikling af udtrykket.

Binets formel fortæller os, at:

$$f(n) \longrightarrow \frac{\phi^n}{\sqrt{5}}, \ \text{når} \ n \longrightarrow \infty.$$

Eksempelvis:

$$f(10) = 55, \quad \text{hvor} \quad \frac{\phi^{10}}{\sqrt{5}} \simeq 55,0036$$

$$f(11) = 89, \quad \text{hvor} \quad \frac{\phi^{11}}{\sqrt{5}} \simeq 88,998.$$

Vi introducerede Fibonaccitallenes frembringende funktion ved at indlejre et simpelt problem i en kompleks sammenhæng omkring en følge af endelige summer, hvor vi netop undlod at bekymre os om konvergens og på sin vis blot betragtede udtrykket som et formelt udtryk. Denne indlejring muliggjorde *opdagelsen* af udtrykket og dermed Fibonaccifølgens sammenhæng med eksempelvis det gyldne snit og analysen generelt. Og udtrykket er virkelig frugtbart: Det var ved hjælp af dette lukkede udtryk, at Matiyasevich i 1970 til løsningen af Hilberts såkaldte tiende problem.

Man kan diskutere i hvilken udstrækning, der findes forklaringer i matematikken. Men det virker imidlertid klart nok, at hvis vi søger en forklaring på, *hvorfor* Fibonaccifølgen har det lukkede udtryk, som den faktisk har, så er det ikke induktionsbeviset vi skal kigge på. Dette bevis giver os ingen forklaringer – men man kunne hævde at det komplekse bevis via den frembringende funktion var et skridt på vejen.

En generel sætning

I tilfældet med rekursive følger, giver frembringende funktioner os faktisk en generel metode, som i princippet altid virker:

1. Skriv ned i en enkelt ligning den rekursive følge g_n.
2. Opskriv den frembringende funktion $G(z)$ med udgangspunkt i 1.
3. Udvikl $G(z)$ i en formel potensrække og aflæs koefficienterne til z^n.

Den generelle sætning siger, at et lukket udtryk kan findes til en hvilken som helst rekursiv følge.

Dette viser virkelig en styrke ved den ideale metode med anvendelse af kompleks analyse til at løse problemer vedrørende rekursive følger er natulige tal

Litteratur

Archimedes (1897). *The Works of Archimedes*, Cambridge University Press, London. Redigeret og kommenteret af T.L. Heath.

Archimedes (1912). *The Method of Archimedes*, Cambridge University Press, London. Redigeret og introduceret af T.L. Heath. Bogen findes på internetadressen: http://www.archive.org/details/cu31924005730563.

Hilbert, D. (1926). Über das Unendliche, *Matematische Annalen* **95**: 161–190. Page references are given to the English translation found *in* van Heijenoort, J., *From Frege to Gödel*, Harvard University Press, pp. 369–392.

Mancosu, P. og Vailati, E. (1991). Rorricelli's Infinitely Long Solid and Its Philosophical Reception in the Seventeenth Century, *ISIS* **82**: 50–70.