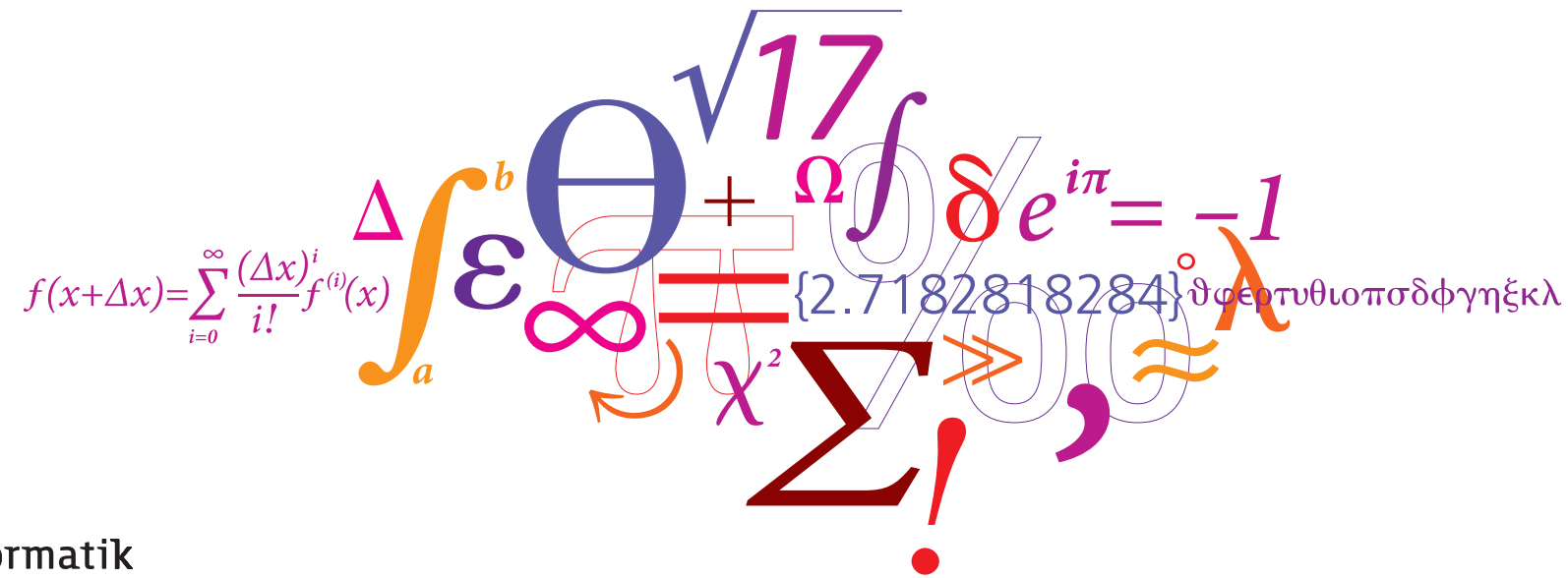
Formelle systemer og aksiomatisk mængdelære

Thomas Bolander, DTU Informatik

Matematik: Videnskaben om det uendelige 2
Folkeuniversitetet i København, efteråret 2011



DTU Informatik
Institut for Informatik og Matematisk Modellering

Lidt om kurset

- Hjemmeside for kurset:
  `http://matematikfilosofi.ruc.dk/vodu2.html`
- Hjemmesiden vil blive opdateret løbende med kursusmateriale—primært slides og links til online-materiale.
- Kurset udgør emnemæssigt/historisk en fortsættelse af kurset *Matematik: Videnskaben om det uendelige 1*.
- I nærværende kursus er der fokus på udviklingen af den moderne matematik i det 20. århundrede: formelle systemer, moderne mængdelære, Hilberts matematikfilosofi, Gödels ufuldstændighedssætninger, beregnelighedsbegrebet, matematikkens "urimelige" effektivitet i fysikken m.m.

Underviserne

Thomas Bolander
Lektor, ph.d.
Datalogi på DTU

Klaus Frovin Jørgensen
Lektor, ph.d.
Filosofi på RUC

Stig Andur Pedersen
Professor
Filosofi på RUC

Vi deler alle en tværfaglig interesse i logik og matematikkens historie, filosofi og grundlag.

Lidt om mig selv

- Thomas Bolander, lektor ved DTU Informatik, Danmarks Tekniske Universitet (siden 2007).
- Studieleder for Matematik ved Folkeuniversitetet i København.
- Forskningsområder: logik og kunstig intelligens.
- Aktuelt: Forskning i hvordan man giver kunstig intelligens-systemer (robotter o.lign.) sociale kompetencer i kraft af evnen til at "sætte sig i andres sted".

Hvad er matematik?

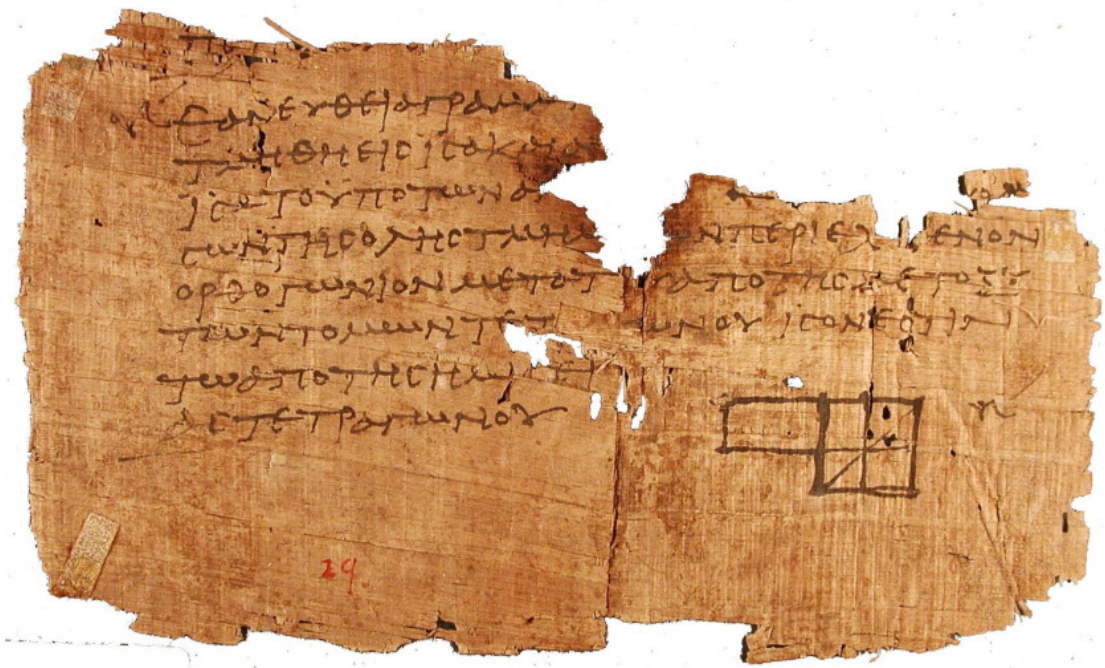
Opvarmningsspørgsmål:

På hvilke måder adskiller matematik sig fra andre videnskaber?

Matematikkens "absolutte sikkerhed"

Matematikken har alle dage brøstet sig af at skaffe *absolut sikkerhed* for sine påstande igennem matematiske beviser.

Eksempel. Euklids *Elementer* om geometri fra det 3. århundrede f.Kr. har været benyttet som lærebog og reference-værk helt op til det 20. århundrede og opfattes stadig i dag som *fuldstændigt* fejlfri. Ikke mange bøger med 2000 år på bagen opfattes stadig i dag som perfekte og fejlfri.



Den aksiomatiske metode

Euklids Elementer benytter den **aksiomatiske metode**. Denne metode er formodentlig er den græske antiks vigtigste bidrag til matematikkens grundlag.

Ideen er følgende: Der er et antal basale matematiske sandheder som kaldes **aksiomer**, udfra hvilke andre sandheder kan udledes i et endeligt antal skridt. Det kan kræve stor snilde at opdage et bevis, men der bør være muligt at tjekke rent mekanisk, skridt for skridt, hvorvidt et påstået bevis er korrekt (moderne formulering).

På denne vis er det muligt at *verificere* beviser, og dermed *garantere* korrektheden af deres konklusioner (givet de valgte aksiomer). Altså "den absolutte sikkerhed".

Aksiomerne fra Euklids Elementer

Euklids aksiomer.

Lad det være forudsat:

1. At man kan trække en ret Linie fra et hvilketsomhelst Punkt til et hvilketsomhelst Punkt.

2. At man kan forlænge en begrænset ret Linie i ret Linie ud i eet.

3. At man kan tegne en Cirkel med et hvilketsomhelst Centrum og en hvilkensomhelst Radius.

4. At alle rette Vinkler ere ligestore.

5. At, naar en ret Linie skærer to rette Linier, og de indvendige Vinkler paa samme Side ere mindre end to rette, saa mødes de to Linier, naar de forlænges ubegrænset, paa den Side, hvor de to Vinkler ligge, der ere mindre end to rette.

Alle de matematiske sætninger i Euklids Elementer er udledt af blot disse 5 aksiomer (postulater).

Aksiomerne opfattes som "åbenlyse sandheder".

Aksiomerne er taget fra Thyre Eibes danske oversættelse af Elementer fra 1897.

Trussel mod den absolutte sikkerhed

Omkring 1900 begyndte tilliden til matematikkens absolutte sikkerhed at vakle.

Det skete da der blev opdaget **paradokser** i **mængdelæren**.

Mængdelære er den del af matematikken der omhandler mængder.

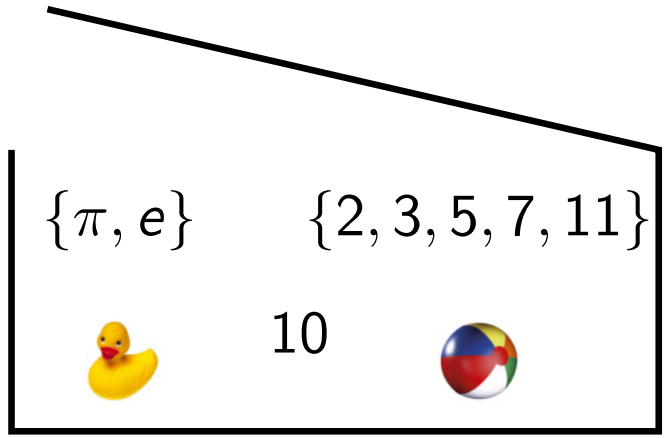
Eksempler på mængder.

$\{1, 2, 3\}$
$\{0, 2, 4, 6, 8, 10\}$
$\{0, 2, 4, 6, 8, 10, \dots\}$
$\{0, -123.453, \pi, 1 - e^{\pi}, \{0, 2, 4, 6, \dots\},$  ,  ,  $\}$

Det naive mængdebegreb

Intuitivt kan en mængde bestå af vilkårlige matematiske objekter: tal, funktioner, geometriske objekter, ligninger, andre mængder osv.

Intuitivt er en mængde således bare en slags matematisk **rodekasse**, som vi kan putte hvad vi nu har lyst til ned i, for at holde samling på det.



Dette afspejles i mængdebegrebet som formuleret af mængdelærens fader, Georg Cantor, i 1895:

> *Unter einer 'Menge' verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objecten m unsrer Anschauung oder unseres Denkens (welche die 'Elemente' von M genannt werden) zu einem Ganzen.*

Paradokser

Desværre viser Cantors mængdebegreb sig at lede til alvorlige problemer for matematikken. Det leder til *paradokser*.

Paradoks: Et tilsyneladende korrekt ræssonement der, baseret på tilsyneladende korrekte antagelser, leder til en modstrid.

Det mest berømte af mængdelærens paradokser er *Russells paradoks*...

Russells paradoks

Russells paradoks (1901). Mængden U af alle mængder er et eksempel på en mængde som indeholder sig selv (altså $U \in U$). Mængden $\mathbb{N}$ af naturlige tal er derimod et eksempel på en mængde som *ikke* indeholder sig selv (altså $\mathbb{N} \notin \mathbb{N}$).

Betragt nu mængden R af **alle mængder som ikke indeholder sig selv**, det vil sige, lad $R = \{x \mid x \notin x\}$.

Spørgsmålet er nu: indeholder R sig selv eller ej?

Antag først at R indeholder sig selv. Da må den per definition af R være en af de mængder som ikke indeholder sig selv, hvilket er en modstrid.

Antag modsat at R *ikke* indeholder sig selv. Da opfylder den R's definition og må derfor være element i R. Konklusionen er så at R er element i R, hvilket igen er en modstrid. Uafhængigt af vores antagelse omkring R ledes vi altså frem til en modstrid. Denne modstrid kaldes *Russells paradoks*.

I matematisk notation: $R \in R \Leftrightarrow R \in \{x \mid x \notin x\} \Leftrightarrow R \notin R$.

Barberens paradoks

Russell giver selv følgende analogi til sit paradoks:

> *Forestil dig en landsby med en enkel barber. Det er her naturligt at forestille sig at* **barberen er den som barberer alle som ikke barberer sig selv**. *Spørgsmålet er nu: barberer barberen sig selv eller ej?*

Hvordan kan vi undslippe dette paradoks?

Pinocchios paradoks

Konsekvenser af paradokserne

Russells paradoks rystede matematikkens grundvold i starten af det 20. århundrede, fordi man ikke kunne finde nogen let måde at undslippe det på.

Det er klart at man ikke kan tillade en matematik bygget på et fundament som indeholder paradokser, for så har man reelt ikke sikkerhed for noget som helst længere.

Normalt vil man jo vide at hvis et udsagn er gyldigt (f.eks. $2 + 2 = 4$) er det modsatte udsagn ugyldigt (f.eks. $2 + 2 \neq 4$), men det bryder sammen i paradokserne ($R \in R$ er gyldig hvis og kun hvis $R \notin R$ er det).

Paradokserne leder derfor til en reel matematisk *grundlagskrise* i starten af det 20. århundrede, og man føler at hele matematikkens fundament er ved at brase sammen.

Løsning af paradokserne

Det viser sig at være ikke helt ligetil at løse paradokserne. Russell skriver i sin selvbiografi følgende om sit forsøg på at løse sit paradoks:

> *"I was trying hard to solve the contradiction mentioned above. Every morning I would sit down before a blank sheet of paper. Throughout the day, with a brief interval for lunch, I would stare at the blank sheet. Often when evening came it was still empty."*

Det ledende synspunkt i starten af det 20. århundrede var at grundlagskrisen skabt af Russells paradoks skulle løses ved at antage en *formalistisk* tilgang til matematikken: forsøge at genopbygge matematikken fra grunden ved hjælp af meget en strikt variant af den aksiomatiske metode (streng symbolmanipulation).

Mere præcist: Ideen var at genopbygge matematikken indenfor et *formelt system*...

Formelle systemer

Formelle systemer er opbygget af *formler*, *aksiomer* og *slutningsregler*. Formlerne er tegnstrenge opbygget efter mekaniske regler.

Eksempler på formler kunne være: $x + 1 = 3$, $x + y + z = x \cdot x + 117$ og $\forall x \exists y (y > x)$.

Aksiomerne i et formelt system er en udvalgt delmængde af formlerne (de "oplagt sande" formler, jvf. Euklids aksiomer).

Eksempel på aksiom: $1 + 3 = 3 + 1$, eller mere generelt $x + y = y + x$.

En **slutningsregel** er et princip, der på rent formel, mekanisk måde angiver, hvordan man fra en eller flere formler kan udlede en ny formel.

Eksempel på slutningsregel: Udfra φ og $\varphi \to \psi$ sluttes ψ (*modus ponens*).

Et **formelt bevis**, eller blot et **bevis**, er en endelig sekvens af formler. Et bevis starter med et eller flere *aksiomer*, og enhver formel skal (hvis den ikke selv er et aksiom) fremkomme af de foregående formler i sekvensen ved brug af en *slutningsregel*. (Sammenlign Euklid).

Eksempel på formelt system

Et formelt system kan siges at *modellere* en del af verden. Som eksempel vil vi nu prøve at skabe et lille formelt system som kan modellere det lille overfyldte bord på billedet.

Eksempler på mulige *formler* i systemet: `på(mandarin,lille_bog)` og `på(x,y)` $\Rightarrow$ `på(y,x)`. Vi udvælger nu *aksiomer* og *slutningsregler*:

- **Aksiomer**:
  - (A1) `på(mandarin,lille_bog)`
  - (A2) `på(lille_bog,store_bog)`
  - (A3) `på(x,y)` $\Rightarrow$ `over(x,y)`
  - (A4) `over(x,y)` $\wedge$ `over(y,z)` $\Rightarrow$ `over(x,z)`

- **Slutningsregler**:
  - (S1) ψ udfra $\varphi \Rightarrow \psi$ og φ.
  - (S2) $\varphi \wedge \psi$ udfra φ og ψ.
  - (S3) $\varphi(k_1, \ldots, k_n)$ udfra $\varphi(x_1, \ldots, x_n)$, hvor k_i'erne er konstanter.

Eksempel på formelt bevis

Følgende er et (formelt) *bevis* i det konstruerede formelle system:

1.	`på(mandarin,lille_bog)`	aksiom (A1)
2.	`på(lille_bog,store_bog)`	aksiom (A2)
3.	`på(x,y)` $\Rightarrow$ `over(x,y)`	aksiom (A3)
4.	`på(mandarin,lille_bog)` $\Rightarrow$ `over(mandarin,lille_bog)`	regel (S3) på 3.
5.	`over(mandarin,lille_bog)`	regel (S1) på 1.,4.
6.	`på(lille_bog,store_bog)` $\Rightarrow$ `over(lille_bog,store_bog)`	regel (S3) på 3.
7.	`over(lille_bog,store_bog)`	regel (S1) på 2.,6.
8.	`over(mandarin,lille_bog)` $\wedge$ `over(lille_bog,store_bog)`	regel (S2) på 5.,7.
9.	`over(x,y)` $\wedge$ `over(y,z)` $\Rightarrow$ `over(x,z)`	aksiom (A4)
10.	`over(mandarin,lille_bog)` $\wedge$ `over(lille_bog,store_bog)` $\Rightarrow$ `over(mandarin,store_bog)`	regel (S3) på 9.
11.	`over(mandarin,store_bog)`	regel (S1) på 8.,10.

som beviser at mandarinen ligger over den store bog...

Formelle systemer for matematik

Men nu handler matematik jo mere om tal og mængder end om mandariner og bøger... Så de formelle systemer man normalt er interesseret i indenfor matematik er formelle systemer for talteori, mængdelære, osv.

Ideen er at finde et passende sæt aksiomer og slutningsregler indenfor hvilke vi kan bevise alle matematikkens sætninger på et mere solidt grundlag.

Men det at forsøge at "mekanisere" matematikken igennem formelle systemer er ikke i sig selv nogen garanti for at vi får et mere solidt grundlag. Vi kan eksempelvis let komme i problemer hvis vi laver et formelt system indeholdende aksiomer og slutningsregler svarende til Cantors naive mængdebegreb som vi introducerede tidligere...

En formalisering af den naive mængdelære

Cantors naive mængdebegreb (1895) kan formuleres på følgende måde:

> *Ethvert prædikat (enhver egenskab) bestemmer en* **mængde** *bestående at de objekter som opfylder prædikatet (egenskaben).*

Lidt mere formelt:

> *Ethver prædikat P bestemmer en* **mængde** *M_P for hvilken der gælder $\forall x(P(x) \Leftrightarrow x \in M_P)$.*

Mængden M_P bestemt af P betegner vi normalt $\{y \mid P(y)\}$.
Ovenstående kan derfor omskrives til:

> *For ethvert prædikat P findes mængden $\{y \mid P(y)\}$ og der gælder $\forall x(P(x) \Leftrightarrow x \in \{y \mid P(y)\})$.*

Det leder direkte frem til følgende *aksiom* som formaliserer det naive mængdebegreb:

UC $\forall x(\varphi(x) \Leftrightarrow x \in \{y \mid \varphi(y)\})$, for enhver formel φ.

En formalisering af den naive mængdelære

Betragt igen aksiomet som formaliserer det naive mængdebegreb:

UC $\forall x(\varphi(x) \Leftrightarrow x \in \{y \mid \varphi(y)\})$, for enhver formel φ.

Vi kan opnå et formelt system ved til dette aksiom at tilføje følgende slutningsregel:

S Udfra $\forall x\psi(x)$ sluttes $\psi(t)$, for enhver formel ψ og ethvert mængde-udtryk t.

I dette formelle system kan vi rekonstruere Russells paradoks...

En formalisering af Russells paradoks

Betragt igen formaliseringen af den naive mængdelære:

UC $\varphi(x) \Leftrightarrow x \in \{y \mid \varphi(y)\}$, for alle formler φ (ubegrænset komprehension).

S Udfra $\varphi(x)$ sluttes $\varphi(t)$, hvor t er et vilkårligt udtryk på formen $\{x \mid x \in \psi\}$ (substitution).

Vi kan nu rekonstruere Russells paradoks *indenfor* det formelle system på følgende måde. Lad $\varphi(x)$ være formlen $x \notin x$. Da fås af UC:

$$x \notin x \Leftrightarrow x \in \{y \mid y \notin y\}.$$

Vi kan nu benytte slutningsreglen S til at substitutere x med $\{y \mid y \notin y\}$:

$$\{y \mid y \notin y\} \notin \{y \mid y \notin y\} \Leftrightarrow \{y \mid y \notin y\} \in \{y \mid y \notin y\}.$$

Lader vi R betegne udtrykket $\{y \mid y \notin y\}$ reducerer dette til:

$$R \notin R \Leftrightarrow R \in R.$$

Bemærk at R netop betegner den mængde som blev introduceret i Russells paradoks!

En formalisering af Russells paradoks

Den beviste formel $R \notin R \Leftrightarrow R \in R$ er naturligvis en modstrid. Vi må konkludere at enten gælder både $R \notin R$ og $R \in R$ eller også gælder ingen af dem. Førstnævnte mulighed svarer til begrebet *inkonsistens* i forbindelse med formelle systemer.

Et formelt system kaldes **inkonsistent** hvis der findes en formel φ, så både φ og ikke-φ kan bevises. Inkonsistenser svarer til paradokser.

Antag vi til vores formelle system UC+S tilføjer følgende naturlige aksiom (udelukkede tredjes princip):

UTP $x \in y \vee x \notin y$.

Vi kan nu konkludere at det formelle system UC+UTP+S er inkonsistent (paradoksfyldt). Hvordan?

Mod en ny mængdelære

Konklusionen på ovenstående argument er: Cantors naive mængdebegreb er inkonsistent, ikke kun i en uformel sædvanlig matematisk ramme, men også i en strengt formaliseret ramme.

Formalisering er altså ikke i sig selv nok til at redde matematikken, men den gør det tydeligt hvor problemerne er. Problemet er her aksiomet UC som tillader os at definere "farlige" mængder såsom Russell-mængden.

En mulig løsning på problemet er at *begrænse* aksiomet UC, så det ikke kan lede til inkonsistenser. Det kan gøres ved at *relativisere* aksiomet:

ZF8 $\forall x(\varphi(x) \wedge x \in M \Leftrightarrow x \in \{y \in M \mid \phi(y)\})$, for enhver mængde M og enhver formel φ.

Nu siger aksiomet at givet en mængde M og et prædikat P kan vi altid udtage mængden af de elementer i M som opfylder P. Det oprindelige aksiom er blevet *relativiseret* til M.

I denne form er aksiomet blevet til et **delmængdeaksiom**: Vi kan udtage vilkårlige delmængder af givne mængder.

Opbygning af mængder

Betragt igen delmængdeaksiomet:

ZF8 $\forall x(\varphi(x) \wedge x \in M \Leftrightarrow x \in \{y \in M \mid \phi(y)\})$, for enhver mængde M og enhver formel φ.

Delmængdeaksiomet leder ikke i sig selv til paradokser og inkonsistens. Men det leder heller ikke i sig selv til en mængdeteori: Hvorfra skal vi få de mængder som vi skal bruge delmængdeaksiomet til at udtage delmængder af? Indtil videre har vi *ingen*.

Vi må tilføje nogen aksiomer som vi kan *opbygge* mængder med. Vi kan starte helt blødt med at erklære eksistensen af en **tom mængde** $\emptyset$:

ZF3 $\forall x(x \notin \emptyset)$

Men den tomme mængde giver jo heller ikke i sig selv så meget sjov. Vi må have fat i nogen lidt større mængder...

Mere om opbygning af mængder

Potensmængder: En standard-måde at opbygge en større mængde fra en mindre på. Potensmængden af en mængde M er mængden af dens delmængder, betegnet $\mathcal{P}(M)$.

Eksempel: Hvis $M = \{1, 2\}$ er $\mathcal{P}(M) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.

Vi kan altså få opbygget en hel del mængder ved at hævde eksistensen af potensmængden af enhver mængde:

ZF7 $\forall x(x \in \mathcal{P}(M) \Leftrightarrow x \subseteq M)$, for enhver mængde M.

Dette er **potensmængdeaksiomet**.

Potensmængdeaksiomet + den tomme mængde giver eksistensen af *uendeligt mange forskellige mængder*:

$$\emptyset, \mathcal{P}(\emptyset), \mathcal{P}(\mathcal{P}(\emptyset)), \mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))), \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))), \mathcal{P}^5(\emptyset), \mathcal{P}^6(\emptyset), \ldots$$

Mere om opbygning af mængder

Potensmængdeaksiomet + den tomme mængde giver:

$$\emptyset, \mathcal{P}(\emptyset), \mathcal{P}(\mathcal{P}(\emptyset)), \mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))), \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset)))), \mathcal{P}^5(\emptyset), \mathcal{P}^6(\emptyset), \ldots$$

Men alle disse mængder har hver især kun *endeligt mange elementer*.

For at kunne generere *uendelige mængder* bliver vi nødt til *eksplicit* at hævde eksistensen af en **uendelig mængde**:

ZF4 $\exists I(\emptyset \in I \wedge \forall x \in I(x \cup \{x\} \in I))$

Ovenstående kaldes **uendelighedsaksiomet** og betegnes ofte *Inf*.

Zermelo-Fraenkel mængdelære, ZF: Ovenstående aksiomer (ZF3, ZF4, ZF7, ZF8) + et par yderligere helt naturlige aksiomer + en enkelt slutningsregel (modus ponens).

Zermelo-Fraenkel mængdelære (ZF & ZFC)

Zermelo-Fraenkel mængdelære, ZF, er et alternativ til Cantors naive mængdelære. Forskelle:

- **Konsistens**. ZF formodes at være konsistent. Ingen inkonsistenser kendt, Cantors og Russells paradokser kan ikke umiddelbart formaliseres i ZF (hvorfor ikke?).
- **Opbygning af mængder nedefra**. I ZF bygges mængder op nedefra: starter med den tomme mængde og bygger mere og mere komplekse mængder op derfra.
- **Kompleksitet**. ZF er et komplekst system af ikke-trivielle aksiomer. Den naive mængdelære kunne potentielt have klaret sig med UC + meget lidt mere.

Udvalgsaksiomet kan tilføjes til ZF hvorved man får ZFC. Næste uges lektion handler netop om udvalgsaksiomet og dets konsekvenser.

ZFC er i dag det tætteste vi er kommet på et alment accepteret formelt **grundlag for matematikken**.

ZFC og den sædvanlige matematik

Formalisering. Al "mainstream" matematik kan (øjensynligt) formaliseres i ZFC. Meget af den er allerede blevet formaliseret igennem computer-genererede eller computer-assisterede beviser.

Forventning: hvis man kan bevise et matematisk resultat med "sædvanlige midler", kan man også bevise det rent formelt i ZFC.

Bemærk dog: der kan være ret stor forskel på det "almindelige" bevis og dets formaliserede sidestykke (formelle beviser er bl.a. altid *ufatteligt* lange).

Konklusion. ZFC synes at være en passende formalisering af matematikken.

MEN: Historien slutter ikke her. Ideen om ZFC som en formalisering af matematikken og det endegyldige sikre grundlag for den viser sig at have en række uventede konsekvenser. Disse vil blive afdækket lidt efter lidt i løbet af kurset...

Opsummering

- Cantors intuitive mængdebegreb viser sig at lede til paradokser. Et af dem er *Russells paradoks*.
- Paradokser truer *matematikkens grundlag*.
- Den foreslåede løsning er en *formalisering* af matematikken, dvs. en genopbygning af matematikken igennem *formelle systemer*.
- Formelle systemer er dog ikke automatisk garanteret at være paradoksfrie: Cantors mængdebegreb kan også formaliseres, og leder til *inkonsistens*.
- Løsningen er et nyt formelt system, hvori mængder bygges op nedefra.
- Dette leder til mængdelæren ZFC, det bedste bud på et moderne grundlag for matematikken.

En "lille" hjemmeopgave

En lille udfordring, så I har noget at tænke over på vej hjem herfra (eller til at holde jer søvnløse natten igennem):

Hyperspilsparadokset (Zwicker, 1987). Et to-personers spil kaldes **endeligt**, hvis det altid vil blive afsluttet i løbet af et endeligt antal træk. Turneringsskak er et eksempel på et endeligt spil.

Vi definerer nu **hyperspillet** som det spil hvori spiller 1 i sit første træk vælger et endeligt spil som skal spilles, og spiller 2 dernæst foretager det første træk i spillet. Alle resterende træk er da træk i det valgte spil.

Ethvert hyperspil vil således vare præcist ét træk mere end et af de endelige spil, og **hyperspillet må derfor være endeligt**.

Men hvis hyperspillet er endeligt, må det også være et af de spil som kan vælges i det første træk i hyperspillet! Det vil sige, spiller 1 kan vælge hyperspillet i sit første træk, spiller 2 kan igen vælge hyperspillet i det efterfølgende træk, og de 2 spillere kan fortsætte med at vælge hyperspillet *ad infinitum*. **Hyperspillet kan derfor ikke være endeligt**.

Hvad er løsningen på dette paradoks?