Kapitel 1

Kardinalitet

Den här texten är tagen från boken **Diskret matematik** *av Asratian–Björn–Turesson (och delvis modifierad). Av den anledningen finns det visa hänvisningar på en del ställen som är ersatta med "??".*

1.1. Fördjupning: Jämförelse av oändliga mängder

1.1.1. Bakgrund och motivering

Att avgöra vilken av två ändliga mängder som är störst är (i princip) inte svårt: Man räknar helt enkelt antal element i var och en av mängderna och får på så sätt veta om en av mängderna är större än den andra eller om mängderna är lika stora. Så kan man naturligtvis inte göra med oändliga mängder eftersom det då finns oändligt många element att räkna.

Ändå är det ofta intressant att jämföra två oändliga mängder för att avgöra vilken av mängderna som är störst eller om mängderna i någon mening är lika stora. Följande exempel ger oss en viss vägledning om hur man kan gå tillväga utan att räkna elementen.

Exempel 1.1.1. Antag att vi vill ta reda på om det finns flest personer eller stolar i ett rum eller om det möjligen finns lika många. Vi ber då helt enkelt personerna att ta var sin stol (eller sätta sig på varsin stol). Om det blir stolar över, finns det fler stolar än personer; om stolarna inte räcker, finns det fler personer än stolar; om varje person får en stol och det inte blir några stolar över, finns det lika många personer som stolar.

Precis som i exemplet kan man para ihop elementen i två mängder om man vill jämföra deras storlekar. Vi kan också beskriva detta tillvägagångssätt med funktioner.

Exempel 1.1.2. (Fortsättning på exempel 1.1.1.) Låt P och S beteckna mängderna av personer respektive stolar i förra exemplet.[1] I fallet då $|P| = |S|$ finns det en bijektion mellan P och S, nämligen den funktion som avbildar en person på den

[1] Här ser vi stolarna som olika. Man kan t.ex. skilja dem åt genom deras placering i rummet.

stol som han eller hon valt. I fallet då $|P| < |S|$ är denna funktion injektiv, men inte surjektiv, och i fallet då $|P| > |S|$ finns det en injektiv funktion från S till P som inte är surjektiv.

1.1.2. Samma kardinalitet

Vi definierar nu vad vi menar med att två mängder ”är lika stora” eller – som vi kommer att säga – ”har samma kardinalitet”.

Definition 1.1.3. Vi säger att två mängder A och B har **samma kardinalitet** om det finns en bijektion från A till B. Detta förhållande betecknas $A \sim B$.

Exempel 1.1.4. Det är klart att en mängd A är ändlig om och endast om A är tom eller $A \sim \{1, 2, \dots, n\}$ för något $n \geq 1$.

Exempel 1.1.5.

a) Vi har att $\mathbf{N} \sim \mathbf{Z}_+$. Här ges en bijektion av $f(n) = n + 1,\ n \in \mathbf{N}$.

b) Vi har också att $2\mathbf{Z}_+ \sim \mathbf{Z}_+$, där $2\mathbf{Z}_+$ betecknar mängden av alla jämna, positiva heltal, d.v.s. talen $2, 4, 6, \dots$. Detta följer då funktionen $f : 2\mathbf{Z}_+ \to \mathbf{Z}_+$ som ges av $f(n) = n/2,\ n \in 2\mathbf{Z}_+$, uppenbarligen är en bijektion.

c) Vidare gäller att $\mathbf{Z} \sim \mathbf{Z}_+$. Definiera nämligen $f : \mathbf{Z} \to \mathbf{Z}_+$ genom

$$f(n) = \begin{cases} 2n + 1 & \text{om } n \geq 0, \\ -2n & \text{om } n < 0. \end{cases}$$

Alltså är

$$f(0) = 1,\ f(1) = 3,\ f(2) = 5, \dots, f(-1) = 2,\ f(-2) = 4,\ f(-3) = 6 \dots .$$

Visa själv som övning att f är en bijektion!

d) Till sist gäller att $]0, 1[\sim \mathbf{R}$. Definiera nämligen $f :]0, 1[\to \mathbf{R}$ genom

$$f(x) = \frac{1}{x} + \frac{1}{x - 1}, \quad x \in]0, 1[.$$

Då är f kontinuerlig, strängt avtagande och har gränsvärdena $\pm\infty$ i ändpunkterna, vilket innebär att f antar varje reellt värde precis en gång.

Sats 1.1.6. *För alla mängder A, B och C gäller att*

(1) $A \sim A$,

(2) *om* $A \sim B$, *är även* $B \sim A$,

(3) *om* $A \sim B$ *och* $B \sim C$, *så är* $A \sim C$.

Bevis. (1) Detta följer av att den funktion $f : A \to A$ som ges av $f(x) = x,\ x \in A$, är en bijektion.

(2) Om $f : A \to B$ är en bijektion, är även $f^{-1} : B \to A$ en bijektion, enligt sats **??**.

(3) Om $f : A \to B$ och $g : B \to C$ är bijektioner, är även $g \circ f : A \to C$ en bijektion, enligt sats **??**. □

1.1.3. Uppräkneliga och överuppräkneliga mängder

I avsnitt **??** definierade vi numrerbara mängder: En mängd A kallas **numrerbar** om den är oändlig och dess element kan räknas upp i en följd $a_1, a_2, a_3, \ldots$.

Man visar oftast att en mängd är numrerbar genom att åberopa följande sats.

Sats 1.1.7. *En mängd A är numrerbar om och endast om $A \sim \mathbf{Z}_+$.*

Detta innebär att alla numrerbara mängder har samma kardinalitet. Man betecknar ofta denna kardinalitet med $\aleph_0$, där $\aleph$ (”alef”) är den första bokstaven i det hebreiska alfabetet.

Bevis. Antag först att $A \sim \mathbf{Z}_+$ och låt f vara en bijektion från $\mathbf{Z}_+$ till A. Om vi sätter $a_j = f(j),\ j = 1, 2, \ldots$, så är $A = \{a_1, a_2, \ldots\}$, och alltså är A numrerbar. Om vi omvänt har att $A = \{a_1, a_2, \ldots\}$, så definieras en bijektion $f : \mathbf{Z}_+ \to A$ genom att sätta $f(j) = a_j$ för $j = 1, 2, \ldots$, och därför är $A \sim \mathbf{Z}_+$. □

Exempel 1.1.8. Vi ser att mängden $\mathbf{Z}_+$ är numrerbar eftersom $\mathbf{Z}_+ \sim \mathbf{Z}_+$. Vidare är, enligt exempel 1.1.5, mängderna $\mathbf{N},\ 2\mathbf{Z}_+$ och $\mathbf{Z}$ numrerbara.

Definition 1.1.9. En mängd A kallas

(1) **uppräknelig** om A är ändlig eller numrerbar,

(2) **överuppräknelig** för övrigt.

Det är lätt att visa att unionen och snittet av två uppräkneliga mängder är uppräkneliga. Följande resultat, som visades av Cantor, är ibland användbart för att visa att en mängd är numrerbar.

Sats 1.1.10. *Om A_j är uppräknelig för $= 1, 2, \ldots$, är $\bigcup_{j=1}^{\infty} A_j$ uppräknelig.*

Bevis. Vi antar först att varje mängd A_j är oändlig: $A_j = \{a_{j1}, a_{j2}, \ldots\}$ (för ett element a_{jk} betecknar indexet j att $a_{jk} \in A_j$ och indexet k att a_{jk} har nummer k

i A_j). Vi skriver sedan upp mängderna i en oändlig kvadrat:

$$\begin{array}{ccccccccccc}
a_{11} & & a_{12} & \to & a_{13} & & a_{14} & \to & a_{15} & & \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow & & & \\
a_{21} & & a_{22} & & a_{23} & & a_{24} & & a_{25} & & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & & & & \\
a_{31} & & a_{32} & & a_{33} & & a_{34} & & a_{35} & & \cdots \\
\downarrow & \nearrow & & \swarrow & & & & & & & \\
a_{41} & & a_{42} & & a_{43} & & a_{44} & & a_{45} & & \cdots \\
\vdots & & \vdots & & \vdots & & \vdots & & & &
\end{array}$$

Om vi nu går igenom kvadraten, som pilarna visar, får vi listan

$$a_{11},\ a_{21},\ a_{12},\ a_{13},\ a_{22},\ a_{31},\ a_{41},\ a_{32},\ a_{23},\ a_{14},\ a_{15},\ a_{24},\ a_{33},\ a_{42},\ldots,$$

och vi får en uppräkning av $\bigcup_{j=1}^{\infty} A_j$ om vi bara tar med varje element i listan en gång och stryker eventuella upprepningar. I fallet då en eller flera mängder A_j är ändliga, är beviset det samma med den enda skillnaden att en eller flera av raderna i kvadraten innehåller ett ändligt antal element. $\square$

Nästa resultat är möjligen något överraskande.

Sats 1.1.11. *Mängden* $\mathbf{Q}$ *av rationella tal är numrerbar.*

Bevis. Låt $A_j = \{\frac{k}{j} : k \in \mathbf{Z}\}$, $j = 1, 2, \ldots$. Då gäller för varje j att $A_j \sim \mathbf{Z}$ och därför att A_j är numrerbar. Härav följer att $\mathbf{Q} = \bigcup_{j=1}^{\infty} A_j$ är numrerbar. $\square$

Vi visar nu att intervallet $]0,1[$ är överuppräkneligt. Lägg märke till att härav följer att även de reella talen är överuppräkneliga eftersom $\mathbf{R} \sim\ ]0,1[$. Satsen är ett resultat av Cantor från 1874. Beviset nedan är också Cantors, men från 1891.

Sats 1.1.12. *Intervallet* $]0,1[$ *är överuppräkneligt.*

I beviset nedan kommer vi att utnyttja decimalutvecklingarna för talen i $]0,1[$. Varje sådant tal kan ju skrivas på formen $0{,}a_1a_2a_3a_4a_5a_6\ldots$. Alla tal med ändlig decimalutveckling kan skrivas på två sätt, t.ex. kan 0,25 skrivas som 0,250000... eller som 0,249999... . Alla övriga tal (d.v.s. de som inte kan skrivas med ändlig decimalutveckling) kan bara skrivas på ett sätt.

Bevis. I det här beviset fyller vi ut ändliga decimalutvecklingar med nollor (och får därmed inga tal som slutar med en oändlig följd 9:or). För att få en motsägelse antar vi att mängden $]0,1[$ är numrerbar, d.v.s. att alla tal i $]0,1[$ kan skrivas i en oändlig följd $a_1, a_2, \ldots$. Vi skriver nu upp decimalutvecklingarna av talen i följden i en tabell:

$$\begin{aligned}
a_1 &= 0{,}a_{11}a_{12}a_{13}a_{14}a_{15}a_{16}\ldots,\\
a_2 &= 0{,}a_{21}a_{22}a_{23}a_{24}a_{25}a_{26}\ldots,\\
a_3 &= 0{,}a_{31}a_{32}a_{33}a_{34}a_{35}a_{36}\ldots,\\
a_4 &= 0{,}a_{41}a_{42}a_{43}a_{44}a_{45}a_{46}\ldots,\\
a_5 &= 0{,}a_{51}a_{52}a_{53}a_{54}a_{55}a_{56}\ldots,\\
&\ \vdots
\end{aligned}$$

där $a_{jk} \in \{0, \dots, 9\}$ för alla $j, k \in \mathbf{Z}_+$. Bilda nu talet $b = 0{,}b_1b_2b_3b_4b_5b_6\dots$, där vi väljer

$$b_j = \begin{cases} 1 & \text{om } a_{jj} \neq 1, \\ 2 & \text{annars,} \end{cases} \qquad j \in \mathbf{Z}_+.$$

Eftersom b varken slutar med oändligt många nollor eller nior, kan b bara skrivas på ett sätt. Vi har att $b \in \,]0,1[$ och $b \neq a_n$ för varje $n \in \mathbf{Z}_+$ eftersom $a_{nn} \neq b_n$. Alltså finns b inte med bland de uppräknade talen. Detta är en motsägelse mot antagandet att vår följd innehöll alla reella tal i $]0,1[$. Detta visar att $]0,1[$ inte är numrerbar. $\square$

Den bevismetod vi just använt kallas för *Cantors diagonalförfarande* och förekommer ofta i matematiska bevis. Fundera själv på varför man inte med samma metod kan visa att mängden av rationella tal mellan 0 och 1 är överuppräknelig!

Exempel 1.1.13. Ett reellt tal x kallas **algebraiskt** om det löser en polynomekvation

$$a_nx^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0,$$

där koefficienterna i ekvationen är heltal och $a_n \neq 0$, och annars **transcendent**. Att ge exempel på algebraiska tal är lätt; exempelvis är $x = \sqrt{2-\sqrt{3}}$ algebraiskt eftersom $x^4 - 4x^2 + 1 = 0$ (övning). Att det överhuvudtaget finns transcendenta tal är däremot inte alls klart från början.

Låt A_j, $j = 1, 2, \dots$, beteckna mängden av reella tal x som löser en polynomekvation på formen ovan, där $|a_n| + |a_{n-1}| + \dots + |a_1| + |a_0| \leq j$ och $n \leq j$. Det är lätt att se att varje mängd A_j är ändlig. Härav följer att mängden av algebraiska tal är numrerbar eftersom den är unionen av mängderna A_j.

Den sista observationen har långtgående konsekvenser. Då $\mathbf{R}$ är överuppräknelig och mängden av algebraiska tal är numrerbar, måste mängden av transcendenta tal också vara överuppräknelig. Det finns alltså gott om reella tal som inte är lösningar till någon polynomekvation med heltalskoefficienter. Lägg märke till att vi har visat detta utan att ge något som helst exempel på ett transcendent tal.

Lyckligtvis går det att ge sådana exempel. Liouville[2] gav 1851 första exemplet på ett transcendent tal:

$$\sum_{n=1}^{\infty} 10^{-n!} = 0{,}110001000000000000000000100\dots.$$

Redan 1844 gav han första beviset för att att transcendenta tal existerar (d.v.s. flera årtionden innan Cantor).

1873 bevisade Hermite[3] att talet e är transcendent. Några år senare, nämligen 1882, visade Lindemann[4] att π är transcendent. En konsekvens av Lindemanns upptäckt är att problemet som kallas **cirkelns kvadratur** är olösbart. Cirkelns kvadratur är ett av de klassiska konstruktionsproblemen med anor från det antika Grekland.[5] Problemet innebär att man ska konstruera en kvadrat med samma area som en given cirkel; de enda tillåtna hjälpmedlen är en passare och en ograderad linjal (d.v.s. en linjal utan markeringar).

[2] Joseph Liouville (1809–82), fransk matematiker.
[3] Charles Hermite (1822–1901), fransk matematiker.
[4] Ferdinand von Lindemann (1852–1939), tysk matematiker.
[5] De övriga är kubens fördubbling och vinkelns tredelning.

1.1.4. Mindre kardinalitet

Definition 1.1.14. Låt A och B vara två mängder. Vi säger att A har

(1) **samma eller mindre kardinalitet** som B om det finns en injektiv funktion från A till B; detta förhållande betecknas $A \precsim B$,

(2) **mindre kardinalitet** än B om det finns en injektiv men ingen bijektiv funktion från A till B; detta förhållande betecknas $A \prec B$.

Det är klart att $A \precsim B$ om och endast om A har samma kardinalitet som en delmängd till A; ty om $f : A \to B$ är injektiv så är $A \sim f(A) \subseteq B$.

Exempel 1.1.15. Vi har att $\mathbf{Z} \precsim \mathbf{R}$ eftersom den funktion $f : \mathbf{Z} \to \mathbf{R}$ som ges av $f(n) = n,\ n \in \mathbf{Z}$, är injektiv. Då $\mathbf{Z}$ är numrerbar medan $\mathbf{R}$ är överuppräknelig, finns det ingen bijektiv funktion från $\mathbf{Z}$ till $\mathbf{R}$, d.v.s. i själva verket är $\mathbf{Z} \prec \mathbf{R}$.

Relationen ”samma eller mindre kardinalitet” fungerar som en ordningsrelation[6] på mängder. Bland annat har vi följande resultat.

Sats 1.1.16. *För alla mängder A, B och C gäller att*

(1) $A \precsim A$,

(2) *om* $A \precsim B$ *och* $B \precsim C$, *så är* $A \precsim C$.

Bevis. (1) Funktionen $f : A \to A$ som ges av $f(x) = x,\ x \in A$, är injektiv.

(2) Om $f : A \to B$ och $g : B \to C$ är injektiva, så är även $g \circ f : A \to C$ injektiv, enligt sats **??**. □

Nästa sats visar att ”samma eller mindre kardinalitet” verkligen fungerar som en ordningsrelation. Satsen bevisades oberoende av varandra av Schröder[7] 1896 och Bernstein[8] 1898. Vi väntar med beviset till avsnitt 1.1.7.

Sats 1.1.17. (Schröder–Bernsteins sats) *Om A och B är två mängder sådana att $A \precsim B$ och $B \precsim A$, så gäller att $A \sim B$.*

Exempel 1.1.18. Eftersom $]0,1[\ \subset [0,1]$ och $[0,1] \subset \mathbf{R}$, har vi att $]0,1[\ \precsim [0,1]$ och $[0,1] \precsim \mathbf{R}$. Vidare är $\mathbf{R} \precsim\ ]0,1[$ eftersom $\mathbf{R} \sim\ ]0,1[$. Vi har alltså att $\mathbf{R} \precsim [0,1]$ och $[0,1] \precsim \mathbf{R}$. Schröder–Bernsteins sats ger därför att $[0,1] \sim \mathbf{R}$.

Följande sats, som bevisades av Cantor 1890–91, visar att potensmängden till en mängd alltid är ”större” än mängden själv; jämför detta med vad som gäller för ändliga mängder.

[6] Egentligen en partiell ordningsrelation, se definition **??** och kapitel **??**.
[7] Ernst Schröder (1841–1902), tysk matematiker.
[8] Felix Bernstein (1878–1956), tysk matematiker.

Sats 1.1.19. *För varje mängd A gäller att $A \prec \mathcal{P}(A)$.*

Bevis. Eftersom $\mathcal{P}(\varnothing) = \{\varnothing\}$ är satsen sann om $A = \varnothing$, så vi kan anta att $A \neq \varnothing$ i resten av beviset. Låt $f : A \to \mathcal{P}(A)$ definieras av $f(a) = \{a\}$ för $a \in A$. Då är f injektiv och alltså är $A \precsim \mathcal{P}(A)$.

Vi visar nu att det inte finns någon bijektion från A till $\mathcal{P}(A)$. Antag motsatsen, d.v.s. att det finns en bijektion $g : A \to \mathcal{P}(A)$. Låt $B = \{a \in A : a \notin g(a)\}$. Eftersom $B \subseteq A$, är $B \in \mathcal{P}(A)$ (B är ju en av A:s delmängder), och eftersom g är surjektiv, finns det ett element $b \in A$ sådant att $g(b) = B$. Det måste då antingen gälla att $b \in B$ eller att $b \notin B$.

Om $b \in B$, gäller enligt definitionen av B att $b \notin g(b) = B$, vilket är en motsägelse. Å andra sidan, om $b \notin B$, gäller det fortfarande att $b \in A$, och eftersom $b \notin B$, gäller det att $b \in g(b) = B$, vilket också är en motsägelse. Detta visar att det inte kan finnas någon bijektion från A till $\mathcal{P}(A)$. $\square$

Med hjälp av sats 1.1.19 kan vi få en följd av mängder med större och större kardinalitet:

$$\mathbf{Z} \prec \mathcal{P}(\mathbf{Z}) \prec \mathcal{P}(\mathcal{P}(\mathbf{Z})) \prec \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbf{Z}))) \prec \mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathbf{Z})))) \prec \dots .$$

Det är inte alltför svårt att bevisa att ”mängden” av alla oändliga kardinaliteter inte är uppräknelig. Faktum är att de oändliga kardinaliteterna är för många för att kunna bilda en mängd inom vår axiomatiska mängdlära **ZFC** som vi studerade i avsnitt **??**. Kardinaliteter kallas också kardinaltal.

Sats 1.1.20. *Det finns ingen mängd innehållande alla kardinaltal.*

Bevis. Antag att vi har en mängd M bestående av kardinaliteter. Vi ska visa att den inte kan innehålla alla kardinaliteter. Låt för varje kardinalitet $\alpha \in M$, mängden A_α vara en mängd med kardinalitet α.

Substitutionsaxiomet i Zermelo–Fraenkels mängdlära försäkrar oss om att vi kan bilda en ny mängd

$$B = \bigcup_{\alpha \in M} A_\alpha.$$

Eftersom $A_\alpha \subseteq B$ så är $A_\alpha \preceq B$ för alla $\alpha \in M$. Men då $B \prec \mathcal{P}(B)$ (enligt sats 1.1.19) så kan inte kardinaliteten för $\mathcal{P}(B)$ tillhöra mängden M. Följaktligen innehåller inte M alla kardinaltal. $\square$

Följande sats är intressant. Vi lämnar den utan bevis, med den intresserade läsaren uppmanas att försöka ge ett eget bevis, se övningarna i slutet av kapitlet.

Sats 1.1.21. *Låt $F = \{f : \mathbf{Z}_+ \to \mathbf{Z}_+\}$ vara mängden av alla funktioner $f : \mathbf{Z}_+ \to \mathbf{Z}_+$. Då är*

$$F \sim \mathcal{P}(\mathbf{Z}_+) \sim \mathbf{R} \sim \mathbf{R}^2.$$

Den sista delen av satsen, att $\mathbf{R} \sim \mathbf{R}^2$, kan tyckas mycket förvånande då den säger att det finns lika många punkter på tallinjen $\mathbf{R}$ som det gör i planet $\mathbf{R}^2$.

1.1.5. En datalogisk tillämpning av kardinalitet

Varje datorprogram kan kodas binärt, och om vi lägger till en etta först så får vi ett unikt positivt heltal för varje program på en given dator. I en idealiserad dator kan vi tänka oss att vi tillåter godtyckligt stora program (men ett givet program måste ha ändlig längd). Det finns alltså en injektion mellan mängden *Prog* av alla datorprogram och $\mathbf{Z}_+$. Eftersom vi enkelt kan skapa längre och längre program så är *Prog* oändlig, och alltså måste vi ha $\mathit{Prog} \sim \mathbf{Z}_+$.

I samma idealiserade situation tänker vi oss att ett datorprogram tar indata i form av en binär sträng (d.v.s. en följd av ettor och nollor) och ger utdata som en binär sträng. Genom att lägga till ettor först kan vi anse att programmet är en funktion från $\mathbf{Z}_+$ till $\mathbf{Z}_+$. (Även här tillåter vi godtyckligt långa indata och utdata, som dock måste vara ändliga. Vi tänker oss också att programmen faktiskt alltid stannar, d.v.s. aldrig hamnar i oändliga loopar.)

Enligt sats 1.1.21 har mängden $F = \{f : \mathbf{Z}_+ \to \mathbf{Z}_+\}$ större kardinalitet än *Prog*. Vi kan alltså dra slutsatsen att inte alla funktioner från $\mathbf{Z}_+$ till $\mathbf{Z}_+$ kan programmeras.

1.1.6. Kontinuumhypotesen

Vi har ovan sett att mängderna $\mathbf{N}$ och $\mathbf{Z}$ har samma kardinalitet som $\mathbf{Z}_+$. Vi har också sett att $]0,1[$ och $[0,1]$ har samma kardinalitet som $\mathbf{R}$. En naturlig fråga inställer sig nu: Är det sant att varje oändlig delmängd till $\mathbf{R}$ antingen har samma kardinalitet som $\mathbf{Z}_+$ eller som $\mathbf{R}$? Cantor trodde att så var fallet och formulerade den så kallade **kontinuumhypotesen** i en artikel 1878. Man kan formulera denna hypotes på följande sätt: Det finns ingen delmängd X till $\mathbf{R}$ sådan att $\mathbf{Z}_+ \prec X \prec \mathbf{R}$. Senare gav Hilbert[9] problemet att bevisa eller motbevisa kontinuumhypotesen som det första av sina 23 berömda problem.

Först 1938 togs det första steget mot en lösning på detta problem. Då visade nämligen Gödel[10] att om Zermelo–Fraenkels axiomsystem **ZFC** är motsägelsefritt, så är även det axiomsystem som man får om man lägger till kontinuumhypotesen motsägelsefritt. Det går alltså inte att motbevisa kontinuumhypotesen inom **ZFC**. Senare visade Cohen[11] 1963 att **ZFC** fortfarande är motsägelsefritt om man lägger till negationen av kontinuumhypotesen till axiomsystemet. Detta innebär att det inte går att bevisa kontinuumhypotesen i detta axiomsystem. En konsekvens är att kontinuumhypotesen är oberoende av axiomsystemet. Man kan jämföra kontinuumhypotesens roll med parallellaxiomets i vanlig euklidisk geometri; parallellaxiomet kan ju varken bevisas eller motbevisas med hjälp av de övriga axiomen.

1.1.7. Bevis för Schröder–Bernsteins sats

Vi avslutar kapitlet med att ge ett bevis för Schröder–Bernsteins sats.

[9] David Hilbert (1862–1943), tysk matematiker. Hilbert är kanske mest känd för de 23 ”Hilbertproblemen” som han formulerade vid matematikernas världskongress i Paris år 1900.

[10] Kurt Gödel (1906–78), logiker född i Brno, Tjeckien, då en del av kejsardömet Österrike–Ungern, från 1940 verksam i USA. Förutom detta resultat är Gödel mest känd för sitt bevis av predikatlogikens fullständighet (1930) och för sin ofullständighetssats (1931).

[11] Paul Cohen (1934–2007), amerikansk matematiker.

Bevis av Schröder–Bernsteins sats (sats 1.1.17). Enligt förutsättningarna har vi injektioner $f : A \to B$ och $g : B \to A$.

Varje element $a \in A$ har högst en urbild $b \in B$ (under avbildningen g), som i sin tur har högst en urbild i A (under avbildningen f), o.s.v. där processen tar slut om man kommer till ett element som saknar urbild. Fortsätter man bakåt så hamnar man i (exakt) ett av följande tre fall:

a) Man stannar på ett element i A utan urbild.

b) Man stannar på ett element i B utan urbild.

c) Man kan fortsätta bakåt hur länge som helst.

Vilket fall vi hamnar i beror givetvis på vilket element i A vi börjar med.

Vi kan dela upp A i tre disjunkta delmängder A_a, A_b och A_c enligt dessa fall. På samma sätt kan B delas in i de tre disjunkta delmängderna B_a, B_b och B_c, beroende på om man slutar med ett element i mängden A eller B eller om slut saknas.

Då har alla element i B_a en (entydig) urbild i A_a, och alla element i A_a har en (entydig) bild i B_a, det ger att f är en bijektion från A_a till B_a. Vi får på samma sätt att f är en bijektion från A_c till B_c, och att g är en bijektion från B_b till A_b och från B_c till A_c. Definierar vi nu $h : A \to B$ som

$$h(a) = \begin{cases} f(a), & a \in A_a, \\ g^{-1}(a), & a \in A_b, \\ f(a), & a \in A_c, \end{cases}$$

så blir h en bijektion. $\square$