

Matematik, KTH

Bengt Ek

februari 2015

MATERIAL TILL KURSEN
SF1662, DISKRET MATEMATIK:

Lite om bevis i matematiken

Inledning

Bevis är centrala i all matematik. Utan (exakta definitioner och) bevis riskerar man att ledas vilse av förutfattade meningar och illa underbyggd intuition.

Ett exempel från analysen: om man tänker på begreppet **kontinuerlig funktion** som att "grafan kan ritas utan att man lyfter pennan från papperet", är det lätt att dra slutsatsen att en funktion som är kontinuerlig i en punkt måste vara kontinuerlig i något (litet) intervall omkring punkten. Men med en exakt definition av begreppet kontinuitet kan man faktiskt konstruera en funktion $f(x)$ som är kontinuerlig för alla irrationella x , men inte för något rationellt x .

Vi skall här se på ett par sätt att formalisera resonemang och bevisföring (i första hand för matematik, men vi tar ibland mer "vardagliga" exempel). I matematiska läroböcker och artiklar används så gott som alltid en mer informell form av bevis, men det är då underförstått att resonemangen "i princip" kan formaliseras och det överlämnas åt läsaren att förvissa sig om detta. Anledningen till att man i praktiken undviker strikt formella bevis är att de oftast skulle bli otympligt långa och "pedantiska", men det lönar sig ändå att studera hur de är uppbyggda för att lära sig att använda riktiga typer av resonemang och tvärtom undvika dem som leder fel.

Man kan skilja på **semantiska** (som ser till betydelsen) och **syntaktiska** (som ser till formen) resonemang. Först måste vi dock ge en mer exakt, formell beskrivning av de påståenden vi vill bevisa och grunda våra resonemang på.

Påståenden

Komplicerade påståenden kan ofta delas upp i mindre delar. Tydligen "innehåller" t.ex.

om det är lördag, läser Lisa diskret matte

de enklare påståendena 'det är lördag' och 'Lisa läser diskret matte'. För att visa **hur** det större påståendet byggs upp av de mindre använder man s.k. **konnektiv**. Om vi låter A betyda 'det är lördag' och B betyda 'Lisa läser

diskret matte', kan det sammansatta påståendet skrivas

$$A \rightarrow B$$

Med olika konnektiv kan man med samma A och B uttrycka t.ex.

$\neg A$	'det är inte lördag'
$A \wedge B$	'det är lördag och Lisa läser diskret matte'
$A \vee B$	'det är lördag eller Lisa läser diskret matte (eller båda)'
$B \rightarrow A$	'det är lördag om Lisa läser diskret matte'
$A \leftrightarrow B$	'det är lördag om och endast om Lisa läser diskret matte'

De olika konnektiven kallas

negation 'inte' ($\neg$),
 konjunktion 'och' ($\wedge$),
 disjunktion 'eller' ($\vee$),
 implikation 'endast om' ($\rightarrow$) och
 dubbel implikation 'om och endast om', 'omm' ($\leftrightarrow$).

Uttryck bildade på detta sätt kallas **satslogiska sentenser** och A , B är exempel på **atomära sentenser**. En sentens är alltså en följd av symboler, en följd som kan uttrycka olika påståenden beroende på vilken **tolkning** (se nedan) vi betraktar (lite som att bokstavsföljden 'rolig' betyder olika saker om vi tolkar den som ett danskt eller som ett svenskt ord).

Det kan fortsättas:

Ex. Om den atomära sentensen C står för 'Det är tentapub på kåren', kan den komplicerade utsagan

'Det är inte tentapub på kåren om det är så att det inte är lördag om och endast om det både är så att Lisa läser diskret matte om det är lördag och att det är tentapub på kåren'

(enligt ett sätt att uppfatta den) **stegvis** översättas till en sentens enligt " $\neg C$ om det är så att ($\neg A$ om och endast om både (B om A) och C)"

så: $(\neg A \leftrightarrow ((A \rightarrow B) \wedge C)) \rightarrow \neg C$

I den första kursboken (DM), avsnitt 7.2, står betydligt mer om satslogik, men allt det ingår inte i vår kurs.

Ett mera uttrycksfullt logiskt språk (och ett som normalt är det man behöver i matematiken) ges av (första ordningens) **predikatlogik**.

Om vi t.ex. vill uttrycka att både Lisa och Olle läser diskret matte, kan vi låta D betyda 'Olle läser diskret matte' och skriva $B \wedge D$. Men i så fall missar vi det väsentliga att det är två personer som gör samma sak, i motsats till i fallet $A \wedge B$.

Predikatlogiken tillåter att vi inför ett **predikat** L , säg, med betydelsen 'läser diskret matte'. Om man också inför **namnen** a för Lisa och b för Olle, kan vi uttrycka att båda sköter sina studier som

$$La \wedge Lb$$

(ibland (som i bokens avsnitt 7.3, som behandlar predikatlogik) skrivs $L(a)$ i stället för La .)

I matematik är det ju normalt väsentligt att man talar om flera matematiska objekt, som tal, funktioner eller liknande. Med predikaten P för 'är primtal', U för 'är udda' och S för 'är större än' (ett s.k. tvåställt predikat) kan vi

uttrycka att alla primtal utom det minsta är udda som

$$\forall x \forall y ((Px \wedge Py) \rightarrow (Sxy \rightarrow Ux))$$

och att för varje udda primtal finns ett mindre primtal som

$$\forall x ((Px \wedge Ux) \rightarrow \exists y (Py \wedge Sxy))$$

$\forall x$ och $\exists x$ kan här läsas "för alla x " och "för något x ".

$\forall$ och $\exists$ kallas **kvantifikatorer** (all- och existens-).

$\forall x Px$ betyder alltså påståendet "alla objekt är primtal". Det är falskt om det handlar om alla heltal, men sant om det bara handlar om talen 3, 17 och 29.

Det för oss till frågan om vilka påståenden som uttrycks av våra sentenser och vad vi skall mena med att de är sanna eller falska.

Tolkningar, sanningsvärden

Om ett påstående som 'det är lördag och Lisa läser diskret matte' ($A \wedge B$ ovan) är sant, beror förstås helt av om det är sant att det är lördag och om det är sant att Lisa läser diskret matte.

Med en **tolkning** av ett satslogiskt språk menar vi en tilldelning av **sanningsvärden** till alla atomära sentenser. Vi betecknar här **sant** med 1 och **falskt** med 0 och kan beskriva betydelsen av de olika konnektiven med tabeller:

p	$\neg p$	p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$
1	0	1	1	1	1	1	1
0	1	1	0	0	1	0	0
'inte'		0	1	0	1	1	0
		0	0	0	0	1	1
				'och'	'eller'	'medför'	'omm'
				'men'	'bara om'		

p och q står här för godtyckliga sentenser, så vi kan upprepa (rekursion!) användningen av tabellerna för att finna sanningsvärden för mer komplicerade sentenser, t.ex. sentensen i exemplet ovan

$$(\neg A \leftrightarrow ((A \rightarrow B) \wedge C)) \rightarrow \neg C$$

som får sanningsvärdestabellen (en rad för varje möjlig tolkning av språket som bara innehåller de atomära sentenserna A , B och C)

A	B	C	$(\neg A \leftrightarrow ((A \rightarrow B) \wedge C)) \rightarrow \neg C$				
1	1	1	0	0	1	1	1
1	1	0	0	1	1	0	1
1	0	1	0	1	0	0	0
1	0	0	0	1	0	0	1
0	1	1	1	1	1	1	0
0	1	0	1	0	1	0	1
0	0	1	1	1	1	1	0
0	0	0	1	0	1	0	1

(Under konnektiven står sanningsvärdet i de olika tolkningarna för motsvarande delar. Under $\rightarrow$ i $A \rightarrow B$ står t.ex. sanningsvärdena för $A \rightarrow B$. Inramat, under det högsta konnektivet, står hela sentensens sanningsvärden.)

En tolkning av ett predikatlogiskt språk kräver lite mer. En tolkning ges av en

mängd, **universum** för tolkningen, och för varje predikat ges ett sanningsvärde för varje element (par av element etc) i universum. T.ex. är då

$$\forall x (Px \vee Qx)$$

sann i en tolkning precis om det för varje element i dess universum gäller att minst ett av predikaten P och Q är sant för det.

Med hjälp av tolkningar kan vi definiera att en sentens p är en **logisk följd** eller **semantisk följd** av en uppsättning sentenser $\Gamma = \{q_1, q_2, \dots, q_n\}$:

$$\Gamma \models p$$

betyder precis att varje tolkning som gör **alla** sentenser i Γ sanna också gör p sann. p följer alltså i så fall säkert av de förutsatta q :na och vi kan säga att vi har bevisat p med hjälp av $q_1, \dots, q_n$ om vi visar ovanstående.

I det satslogiska fallet går det bra att göra så, särskilt om antalet ingående atomära sentenser inte är för stort – ställ upp en sanningsvärdestabell för alla $q_1, \dots, q_n, p$ och kontrollera om p är sann i alla de tolkningar (rader i tabellen) där alla q_i är sanna. T.ex. får man (oftast skrivs A, B i stället för $\{A, B\}$)

$$A, B \models (\neg A \leftrightarrow ((A \rightarrow B) \wedge C)) \rightarrow \neg C.$$

I det predikatlogiska fallet går det inte lika lätt, där finns det ju alltid oändligt många olika tolkningar (olika universa)!

Lösningen på det problemet kan vara ett syntaktiskt **härledningssystem**, t.ex.

Naturlig deduktion

I stället för att betrakta betydelser, tolkningar, kan man hålla sig till sentenserna, dvs strängarna av symboler, och formulera regler för vad som kan härledas ur vad.

T.ex. bör man ur $A \rightarrow B$ och A kunna härleda B (vi inser det genom att betrakta sanningsvärden, men kan se det som en regel som tillåter oss att skriva B på nästa rad om vi har $A \rightarrow B$ och A på tidigare rader i en härledning). Härledning brukar skrivas med symbolen $\vdash$, t.ex.

$$A \rightarrow B, A \vdash B$$

(eller $\{A \rightarrow B, A\} \vdash B$).

På de två sista sidorna finns ett antal regler som räcker för att härleda alla logiska följder. Det visar vi inte, men det är det som gör att vi kan använda naturlig deduktion som härledningsmetod. **Gödels fullständighetssats** säger (fast Gödel använde ett annat härledningssystem) att

$$\Gamma \models p \Leftrightarrow \Gamma \vdash p$$

dvs p är en logisk följd av Γ om och endast om det finns en härledning av p från Γ . Implikationen åt vänster ($\Leftarrow$) säger att härledningsmetoden är **sund** (vi kan bara härleda sådant som verkligen är en logisk följd) medan implikationen åt höger ($\Rightarrow$) säger att härledningsmetoden är **fullständig** (vi kan härleda allt som är en logisk följd). Lite förenklat uttryckt, "något kan bevisas om och endast om det är sant".

I huvudsak finns två regler för varje konnektiv, en "E-regel" (för att "eliminera" en förekomst av konnektivet) och en "I-regel" (för att "introducera" konnektivet). Dessutom krävs en regel som tillåter oss att göra **antaganden** på vägen och en regel som låter oss dra slutsatsen p om vi har $\neg\neg p$.

Reglerna skall tolkas så att den sista raden kan skrivas upp med åberopande av regeln i fråga om raderna över redan finns (i någon ordning) bland våra rader. $p, q, \dots$ kan då vara vilka sentenser som helst och $g, h, \dots, a_1, \dots, b_1, \dots$ godtyckliga radnummer.

För att visa hur en härledning i naturlig deduktion skall se ut, ser vi på några exempel. Som antytts ovan skrivs härledningen upp i ett antal "rader", med flera kolumner där det är helt bestämt vad som skall stå. Tanken är just att det inte skall krävas någon fantasi av läsaren för att kontrollera om en härledning är korrekt. En dator skulle klara det. (Att komma på hur något skall härledas, däremot, kan kräva både fantasi och kreativitet.)

Ex. För att visa att $A \rightarrow B$, $A \vdash B$ skriver vi

1	(1)	$A \rightarrow B$	premiss
2	(2)	A	premiss
1,2	(3)	B	1,2 $\rightarrow E$

På de två första raderna står **premisserna**, de sentenser som står till vänster om $\vdash$ -symbolen, och den tredje raden innehåller vår önskade slutsats, som i det här fallet fickas med bara en regelanvändning.

Den andra kolumnen är en numrering av raderna, för att vi skall kunna hänvisa till dem. I den första kolumnen står numren för de rader vi behövt för att härleda radens sentens (som finns i kolumn tre). Som framgår av reglerna kan det i första kolumnen bara stå radnummer för premisser och antaganden (det finns inga regler som placerar andra nummer där). Den tredje raden ovan betyder alltså att B kan härledas (eller har härletts) ur sentenserna (premisserna) på raderna 1 och 2. De två sista kolumnerna talar om vilken regel vi åberopar för att skriva upp sentensen på raden, precis som det står formulerat i reglerna.

Vi tar ett exempel till, där det behövs mer än ett steg i själva härledningen:

Ex. Vi visar att $A \rightarrow \neg B \vdash B \rightarrow \neg A$

1	(1)	$A \rightarrow \neg B$	premiss
2	(2)	B	antagande (för $\rightarrow I$)
3	(3)	A	antagande (för $\neg I$)
1,3	(4)	$\neg B$	1,3 $\rightarrow E$
1,2,3	(5)	$\perp$	4,2 $\neg E$
1,2	(6)	$\neg A$	3,5 $\neg I$
1	(7)	$B \rightarrow \neg A$	2,6 $\rightarrow I$

Eftersom slutsatsen på rad 7 bara beror av premissen på rad 1, är saken klar. Observera att de antaganden vi gör (enligt sin regel, förstås) är precis som när vi resonerar informellt. Slutsatsen på sista raden får inte bero av antaganden, de "tas bort" av vissa regler (här står som förklaring t.ex. "(för $\rightarrow I$)" vid ett antagande; det hör egentligen inte till, utan är bara för att förklara varför vi gjort antagandet). I t.ex. $\rightarrow I$ -regeln står vid sista raden (1) att den beror av $\{a_1, \dots, a_n\}/j$. Det betyder att antagandet på rad j skall tas bort från $\{a_1, \dots, a_n\}$ (om det finns med).

$\perp$ på rad 5 är en sentens som alltid är falsk, en motsägelse, kallad **falsum** (den

kallas ibland ett "0-ställigt konnektiv"). Här har vi härlett $\perp$ från raderna 1, 2 och 3 (A), vilket enligt principen för ett motsägelsebevis ju betyder att 1 och 2 leder till 6 ($\neg A$), negationen till antagandet 3 (dessutom leder 1 och 3 till negationen av 2, $\neg B$, men det behöver vi inte här). På liknande sätt följer av att 1 och 2 (B) leder till 6 ($\neg A$) att 1 leder till 7 ($B \rightarrow \neg A$).

Rader som står åtskilda i en regel kan vara identiska (regeln skall alltså tolkas som att var och en av dess rader över den sista måste finnas bland våra redan härledda), t.ex. kan vi visa att det alltid gäller att A medför A så:

Ex. Vi visar $\vdash A \rightarrow A$

- | | | | |
|---|-----|-------------------|---------------------|
| 1 | (1) | A | antagande |
| | (2) | $A \rightarrow A$ | 1,1 $\rightarrow$ I |

Slutsatsen på rad 2 beror inte av något, så härledningen är klar. En sentens p som kan härledas från ingenting, $\vdash p$, brukar kallas ett **teorem**. Enligt Gödels fullständighetssats som vi nämnde ovan är det ekvivalent med att p är sann i alla tolkningar, $\models p$, att p är en **tautologi**.

Andra exempel på teorem/tautologier är

$$A \vee \neg A, A \rightarrow (B \rightarrow A) \text{ och } (\neg A \rightarrow A) \rightarrow A.$$

För vår kurs räcker det att man kan göra enklare härledningar i naturlig deduktion för satslogik, ungefär som i exemplen ovan och dem som finns bland exemplen för övning 3. Meningen är att det skall ge förståelse för hur man kan resonera också då man gör informella bevis.

Bland reglerna finns också sådana som bara används i predikatlogik (regler för $\forall$, $\exists$ och $=$). Flera av dem innehåller olika villkor, som t.ex. att för att man ur Pa skall kunna dra slutsatsen $\forall x Px$ måste a vara ett namn som inte förekommer på angivna rader i härledningen. Det svarar mot att man för att visa att något gäller för alla tal, måste visa det för ett "godtyckligt" tal – det räcker inte att visa det för π , 0 eller $\sqrt{7}$.

$\exists$ E-regeln är nog den mest subtila. Det kan vara något att fundera över varför villkoren i den ser ut som de gör och varför den precis motsvarar vårt sätt att resonera då vi använder $\exists x Px$. Man kan jämföra med $\forall$ E-regeln, som också den kan tåla lite eftertanke.

För att illustrera kvantifikatorreglerna ger vi ett sista

Ex. Vi visar att $\exists x \forall y Qxy \vdash \forall y \exists x Qxy$ (t.ex. "om det finns ett största tal, så finns det för varje tal ett tal som är $\geq$ det")

- | | | | |
|---|-----|---------------------------|---|
| 1 | (1) | $\exists x \forall y Qxy$ | premiss |
| 2 | (2) | $\forall y Qay$ | antagande |
| 2 | (3) | Qab | 2 $\forall$ E |
| 2 | (4) | $\exists x Qxb$ | 2 $\exists$ I |
| 1 | (5) | $\exists x Qxb$ | 1,2,4 $\exists$ E (a finns inte på raderna 1, 4) |
| 1 | (6) | $\forall y \exists x Qxy$ | 5 $\forall$ I (b finns inte på rad 1) |

Observera att det omvända inte gäller, $\forall y \exists x Qxy \not\vdash \exists x \forall y Qxy$. Tänk på $\mathbb{N}$ med $\geq$ som Q . Varför skulle ett liknande bevis för det inte fungera?

Härledningsregler för naturlig deduktion (2 sidor)

Regel för premiss

$$j \quad (j) \quad p \quad \text{premiss}$$

Regel för antagande

$$j \quad (j) \quad p \quad \text{antagande}$$

Regel för $\wedge E$:

$$\begin{array}{c} a_1, \dots, a_n \quad (j) \quad p \wedge q \\ \vdots \\ a_1, \dots, a_n \quad (k) \quad p \quad j \quad \wedge E \\ \text{(eller } q) \end{array}$$

Regel för $\rightarrow E$:

$$\begin{array}{c} a_1, \dots, a_m \quad (j) \quad p \rightarrow q \\ \vdots \\ b_1, \dots, b_n \quad (k) \quad p \\ \vdots \\ a_1, \dots, a_m, b_1, \dots, b_n \quad (l) \quad q \quad j, k \quad \rightarrow E \end{array}$$

Regel för $\neg E$:

$$\begin{array}{c} a_1, \dots, a_m \quad (j) \quad \neg p \\ \vdots \\ b_1, \dots, b_n \quad (k) \quad p \\ \vdots \\ a_1, \dots, a_m, b_1, \dots, b_n \quad (l) \quad \perp \quad j, k \quad \neg E \end{array}$$

Regel för $\vee E$:

$$\begin{array}{c} a_1, \dots, a_m \quad (g) \quad p \vee q \\ \vdots \\ h \quad (h) \quad p \quad \text{antagande} \\ \vdots \\ b_1, \dots, b_n \quad (i) \quad r \\ \vdots \\ j \quad (j) \quad q \quad \text{antagande} \\ \vdots \\ c_1, \dots, c_u \quad (k) \quad r \\ \vdots \\ X \quad (l) \quad r \quad g, h, i, j, k \quad \vee E \end{array}$$

där $X =$

$= \{a_1, \dots, a_m\} \cup \{b_1, \dots, b_n\} / h \cup \{c_1, \dots, c_u\} / j$

DN-regeln

$$\begin{array}{c} a_1, \dots, a_n \quad (j) \quad \neg \neg p \\ \vdots \\ a_1, \dots, a_n \quad (k) \quad p \quad j \quad \text{DN} \end{array}$$

Regel för $\wedge I$:

$$\begin{array}{c} a_1, \dots, a_m \quad (j) \quad p \\ \vdots \\ b_1, \dots, b_n \quad (k) \quad q \\ \vdots \\ a_1, \dots, a_m, b_1, \dots, b_n \quad (l) \quad p \wedge q \quad j, k \quad \wedge I \end{array}$$

Regel för $\rightarrow I$:

$$\begin{array}{c} j \quad (j) \quad p \quad \text{antagande} \\ \vdots \\ a_1, \dots, a_n \quad (k) \quad q \\ \vdots \\ \{a_1, \dots, a_n\} / j \quad (l) \quad p \rightarrow q \quad j, k \quad \rightarrow I \end{array}$$

Regel för $\neg I$:

$$\begin{array}{c} j \quad (j) \quad p \quad \text{antagande} \\ \vdots \\ a_1, \dots, a_n \quad (k) \quad \perp \\ \vdots \\ \{a_1, \dots, a_n\} / j \quad (l) \quad \neg p \quad j, k \quad \neg I \end{array}$$

Regel för $\vee I$:

$$\begin{array}{c} a_1, \dots, a_n \quad (j) \quad p \\ \vdots \\ a_1, \dots, a_n \quad (k) \quad p \vee q \quad j \quad \vee I \\ \text{(eller } q \vee p) \end{array}$$

Regel för $\leftrightarrow E$:

$$\begin{array}{c}
 a_1, \dots, a_m \quad (j) \quad p \leftrightarrow q \\
 \text{(eller } a_1, \dots, a_m \quad (j) \quad q \leftrightarrow p) \\
 \vdots \\
 b_1, \dots, b_n \quad (k) \quad p \\
 \vdots \\
 a_1, \dots, a_m, b_1, \dots, b_n \quad (l) \quad q \quad j, k \quad \leftrightarrow E
 \end{array}$$
Regel för $\forall E$:

$$\begin{array}{c}
 a_1, \dots, a_n \quad (j) \quad \forall \nu \phi \nu \\
 \vdots \\
 a_1, \dots, a_n \quad (k) \quad \phi t \quad j \quad \forall E
 \end{array}$$

ϕt är $\phi \nu$ med **alla** ν ersatta med t

Regel för $\exists E$:

$$\begin{array}{c}
 a_1, \dots, a_m \quad (j) \quad \exists \nu \phi \nu \\
 \vdots \\
 k \quad (k) \quad \phi t \quad \text{antagande} \\
 \vdots \\
 b_1, \dots, b_n \quad (l) \quad \psi \\
 \vdots \\
 X \quad (m) \quad \psi \quad j, k, l \quad \exists E
 \end{array}$$

där $X = \{a_1, \dots, a_m\} \cup \{b_1, \dots, b_n\}/k$
 ϕt är $\phi \nu$ med **alla** ν ersatta med t
namnet t förekommer inte på
någon av raderna $j, l, \{b_1, \dots, b_n\}/k$

Regel för $= E$:

$$\begin{array}{c}
 a_1, \dots, a_m \quad (j) \quad t_1 = t_2 \\
 \vdots \\
 b_1, \dots, b_n \quad (k) \quad \phi t_1 \\
 \vdots \\
 X \quad (l) \quad \phi t_2 \quad j, k \quad = E
 \end{array}$$

ϕt_2 är ϕt_1 med **godtyckligt antal** t_1 ersatta med t_2

Regel för $\leftrightarrow I$:

$$\begin{array}{c}
 g \quad (g) \quad p \quad \text{antagande} \\
 \vdots \\
 a_1, \dots, a_m \quad (h) \quad q \\
 \vdots \\
 j \quad (j) \quad q \quad \text{antagande} \\
 \vdots \\
 b_1, \dots, b_n \quad (k) \quad p \\
 \vdots \\
 X \quad (l) \quad p \leftrightarrow q \quad g, h, j, k \quad \leftrightarrow I
 \end{array}$$

där $X = \{a_1, \dots, a_m\}/g \cup \{b_1, \dots, b_n\}/j$

Regel för $\forall I$:

$$\begin{array}{c}
 a_1, \dots, a_n \quad (j) \quad \phi t \\
 \vdots \\
 a_1, \dots, a_n \quad (k) \quad \forall \nu \phi \nu \quad j \quad \forall I
 \end{array}$$

där t inte finns på rad $a_1, \dots, a_n$
 $\phi \nu$ är ϕt med **alla** t ersatta med ν
variabeln ν finns inte i ϕt

Regel för $\exists I$:

$$\begin{array}{c}
 a_1, \dots, a_n \quad (j) \quad \phi t \\
 \vdots \\
 a_1, \dots, a_n \quad (k) \quad \exists \nu \phi \nu \quad j \quad \exists I
 \end{array}$$

$\phi \nu$ är ϕt med ett **godtyckligt antal** t ersatta med ν

Regel för $= I$:

$$(j) \quad t = t \quad =I$$

Om axiomatisering

Som vi sett ovan kan vissa sentenser bevisas (härledas) ”från ingenting”, t.ex. $\vdash A \rightarrow A$, men för att få intressanta satser om verkligt ”matematiska” begrepp måste man utgå från något. Man ställer då upp ett antal sentenser (s.k. **axiom**) som skall fånga egenskaperna hos objekten (tal, punkter, mängder, gruppelement, ...) och härleder sentenser från dem. De sentenserna uttrycker då påståenden som blir sanna för alla objekt som uppfyller axiomen.

I allmänhet har man en av två olika avsikter då man studerar en uppsättning axiom, ett **axiomsystem**. Antingen vill man beskriva en viss mängd objekt och dess egenskaper, t.ex. de naturliga talen eller punkter och linjer i planet (geometri), eller så vill man undersöka gemensamma egenskaper för alla mängder av en viss typ (nämligen de som uppfyller axiomen), t.ex. alla partialordnade mängder eller alla grupper (som vi kommer att tala om längre fram i kursen).

Som ett exempel (som man inte behöver lära sig) på en axiomatisering av den första typen ger vi ett ofta använt system av axiom för de naturliga talen, **Peanos axiom**. Vi är här intresserade av en viss tolkning, **standardmodellen** $\mathbb{N}$, även om det kan finnas andra tolkningar som uppfyller alla axiomen.

Som ofta i matematiska sammanhang är det praktiskt (nästan nödvändigt) att införa **funktioner** i vårt logiska språk. En funktionssymbol f svarar då i en tolkning mot en viss funktion (av ett visst antal (**ställigheten** för f) element från tolkningens universum).

PEANOS AXIOM

Språk (tolkningen i standardmodellen inom []):

en 0-ställig funktionssymbol (dvs en individkonstant, ett namn) 0 [talet 0]

en 1-ställig funktionssymbol S [nästa tal]

två 2-ställiga funktionssymboler $+$ och $*$ [addition och multiplikation]

(vi skriver t.ex. $x + y$ och $x * y$ i stället för $+(x, y)$ och $*(x, y)$.)

Axiom:

P1	$\forall x \forall y (S(x) = S(y) \rightarrow x = y)$	olika tal har olika efterföljare
P2	$\forall x S(x) \neq 0$	0 är inte efterföljare
P3	$\forall x x + 0 = x$	rekursiv definition av $+$, bas
P4	$\forall x \forall y x + S(y) = S(x + y)$	rekursiv definition av $+$, steg
P5	$\forall x x * 0 = 0$	rekursiv definition av $*$, bas
P6	$\forall x \forall y x * S(y) = (x * y) + x$	rekursiv definition av $*$, steg
P7	$\forall z_1 \dots \forall z_n ((\phi 0 \wedge \forall x (\phi x \rightarrow \phi S(x))) \rightarrow \forall x \phi x)$	induktionsaxiom

I P7 är ϕx en godtycklig formel med alla fria variabler bland $x, z_1, \dots, z_n$. P7 är alltså egentligen ett oändligt antal axiom, ett s.k. **axiomschema**.

Med P7 (oftast med $n = 0$) kan vi genomföra **induktionsbevis** i $\mathbb{N}$.

Kurt Gödel visade 1931 (vilket vi inte gör här) att P1–P7 ”inte räcker” för att beskriva de naturliga talen fullständigt, dvs det finns satser som är sanna för de naturliga talen men ändå inte kan härledas från dessa axiom. Och, starkare, hur man än lägger till axiom (på något sätt så att man entydigt kan avgöra om en given sentens är ett axiom) kommer det alltid att finnas satser som är sanna i $\mathbb{N}$ men inte kan bevisas med de axiomen (**Gödels (första) ofullständighetssats**, en av logikens mest berömda satser).

Som exempel på en axiomatisering av den andra typen, där man oftast är intresserad av alla tolkningar som uppfyller axiomen, ger vi

AXIOM FÖR PARTIALORDNINGAR

Språk: en 2-ställig relationssymbol $\preceq$.

Axiom:

$$\begin{array}{ll} \forall x \, x \preceq x & \text{reflexivitet} \\ \forall x \, \forall y \, ((x \preceq y \wedge y \preceq x) \rightarrow x = y) & \text{antisymmetri} \\ \forall x \, \forall y \, \forall z \, ((x \preceq y \wedge y \preceq z) \rightarrow x \preceq z) & \text{transitivitet} \end{array}$$

Från dem kan man härleda alla egenskaper som är gemensamma för **alla** partialordnade mängder. Däremot kan man inte härleda allt som gäller för någon speciell partialordnad mängd, t.ex. gäller ju $\forall x \, \forall y \, (x \preceq y \vee y \preceq x)$ för de naturliga talen $\mathbb{N}$, med $\preceq$ tolkad som $\leq$, men det kan inte visas från axiomen ovan (eftersom axiomen är uppfyllda även för partialordningar som inte är totalordningar, t.ex. $\mathcal{P}(\{0, 1\}) = \{\emptyset, \{0\}, \{1\}, \{0, 1\}\}$ med $\preceq$ tolkad som $\subseteq$).