26/8 - 13

MAT 2400

Bevis

Mange matematiske utsagn er av formen

"Det eksisterer ...." $\exists x\, A(x)$

eller

"For alle ....." $\forall x\, A(x)$

For å bevise utsagn av typen $\exists x A(x)$ er det nok å finne eller konstruere en x som oppfyller A. For å bevise utsagn av typen $\forall x A(x)$ må vi argumentere for at $A(x)$ holder for alle x i det domenet vi tenker på

For å motbevise utsagn av typen $\exists x A(x)$ må vi vise at det ikke finnes noen x slik at $A(x)$ er sann, dvs. vi må vise at $A(x)$ er usann for alle x (husk $\sim \exists x A(x) \Leftrightarrow \forall x \sim Ax$ er en tautologi)
For å motbevise utsagn av typen $\forall x A(x)$ er det nok å finne én x slik at $A(x)$ ikke holder, dvs. en x slik at $\sim A(x)$ er sann (husk at $\sim \forall x A(x) \Leftrightarrow \exists x \sim A(x)$ er en tautologi)

Eksempel: Her er et enkelt eksistensbevis. Vi skal vise at dersom x, y er to reelle tall og

$x<y$, så finnes det et reelt tall z slik at $x<z<y$.

Idéen er at midtpunktet $z=\frac{x+y}{2}$ må være et slikt punkt. La oss sjekke: Siden $x<y$, er $\frac{x}{2}<\frac{y}{2}$ og følgelig

$$x=\frac{x}{2}+\frac{x}{2}<\frac{x}{2}+\frac{y}{2}=\frac{x+y}{2}=z$$

$$y=\frac{y}{2}+\frac{y}{2}>\frac{x}{2}+\frac{y}{2}=\frac{x+y}{2}=z$$

Kontrapositive bevis

Mange matematiske setninger er på formen "Hvis A, så B", dvs $A\Rightarrow B$. Som regel er det en underforstått allkvantor i slike utsagn, slik at det man egentlig ønsker å vise, er

(*) $\quad \forall x\,(A(x)\Rightarrow B(x))$

dvs "for alle x er det slik at hvis $A(x)$ er sann, så er også $B(x)$ sann". Vi må altså vise at dersom $A(x)$ er sann, så er $B(x)$ det også.

Siden $A\Rightarrow B$ er logisk ekvivalent med $\neg B\Rightarrow\neg A$, er (*) logisk ekvivalent med

(**) $\quad \forall x\,(\neg B(x)\Rightarrow \neg A(x))$

Beviser vi (**), har vi dermed også bevist (*). I en

Det tilfellet er det lettere å bevise (**) enn (*) fordi det er enklere å utnytte kraften i premissen $\sim B$ enn i A. La oss se på et eksempel.

Setning: Hvis n^2 er et partall, så er n det også.

Bemerkning: Formelt kan vi skrive dette utsagnet som

$$(*) \qquad \forall n \in \mathbb{N} \, (P(n^2) \Rightarrow P(n))$$

der P er predikatet: $P(x) =$ "x er et partall".

Bevis: Det kontrapositive utsagnet er

$$(**) \qquad \forall n \in \mathbb{N} (\sim P(n) \Rightarrow \sim P(n^2))$$

Siden negasjonen av å være partall er å være oddetall, sier (**)

"Hvis n er et oddetall, så er n^2 det også"

Dette er lett å vise: Hvis n er et oddetall, er det på formen $n = 2k+1$. Men da er

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

som åpenbart er et oddetall. Dermed er setningen bevist.

Bemerkning: Beviset illustrerer hvorfor det ofte er lurt å argumentere kontrapositivt — premissen

"n er et oddetall"

er mye enklere å utnytte enn premissen

"n^2 er et partall"

Motsigelsesbevis

En annen bevisform som er nyttig å vite om, er motsigelsesbevis. Her ønsker vi å bevise en påstand A, men istedenfor å gjøre dette direkte, antar vi isteden $\sim A$ og viser at denne antagelsen fører til en selvmotsigelse. Siden selvmotsigelsen umulig kan være sann, betyr dette at vi må forkaste hypotesen $\sim A$, og dermed har vi vist at A er sann.

Rent logisk betyr en selvmotsigelse at vi kan bevise både et utsagn B og dets negasjon $\sim B$. I et motsigelses bevis viser vi altså

$$\sim A \Rightarrow (B \wedge \sim B)$$

Dette utsagnet har samme sannhetsverditabell som A, og dermed får vi en "logisk sjekk" på argumentet vårt ovenfor:

A	B	$\sim B$	$B \wedge \sim B$	$\sim A$	$\sim A \Rightarrow (B \wedge \sim B)$
T	T	F	F	F	T
T	F	T	F	F	T
F	T	F	F	T	F
F	F	T	F	T	F

La oss se på et eksempel. Husk at et reelt tall r er rasjonalt dersom det kan skrives som en brøk $r = \frac{m}{n}$ av to hele tall m og n.

Setning: $\sqrt{2}$ er irrasjonal (dvs. ikke rasjonal)

Bevis: Vi bruker et motsigelsesbevis og antar derfor at $\sqrt{2}$ er rasjonal og håper at dette vil lede til en misforståelse. Hvis $\sqrt{2}$ er rasjonal, kan den åpenbart skrives som en brøk

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

der m og n er positive og ikke har felles faktorer (hvis ikke forkorter vi bare bort de felles faktorene). Opphøyer vi begge sider i annen, får vi

$$2 = \frac{m^2}{n^2} \quad \text{dvs} \quad m^2 = 2n^2$$

Dette betyr at m^2 er et ~~[illegible]~~ partall, og dermed er m også et partall, dvs $m = 2k$ for et helt tall k. Setter vi dette inn i formelen $m^2 = 2n^2$, får vi

$$(2k)^2 = 2n^2 \Leftrightarrow 4k^2 = 2n^2 \Leftrightarrow n^2 = 2k^2$$

Dette betyr at n^2, og dermed n, er et partall. Vi har dermed vist at både m og n er partall, og det strider mot forutsetningen at de ikke har felles faktorer. Dermed må vi forkaste antagelsen om at $\sqrt{2}$ er rasjonal og setningen er bevist.

Eksistensbevis og konstruktive bevis

Anta at vi skal bevise at noe eksisterer, dvs et utsagn av typen

$$\exists x A(x)$$

I noen bevis gjør man å regne ut eller konstruere et element x som oppfyller A, og disse kalles konstruktive bevis. I andre tilfeller – f. eks. når vi bruker motsigelsesbevis – viser vi bare at det må finnes en slik x uten "å finne" den. Slik bevis kaller vi gjerne (vene) eksistensbevis. For de fleste matematikere er det ikke noen logisk forskjell på de to bevistypene, men konstruktive bevis gir selvfølgelig mer informasjon å arbeide videre med.

Spillteori gir noen slående eksempler på rene eksistensbevis. Det finnes spill der man har bevist at den ene spilleren har en gevinststrategi, men der ingen aner hva den strategien er.

Jeg kan ikke motstå fristelsen til å vise frem et morsomt (men utypisk) eksistensbevis.

Setning: Det finnes irrasjonale tall a, b slik at a^b er rasjonal.

Bevis: La først $a = \sqrt{2}$, $b = \sqrt{2}$. Hvis $\sqrt{2}^{\sqrt{2}}$ er rasjonal, er vi ferdig. Hvis ikke, kan vi sette $a = \sqrt{2}^{\sqrt{2}}$ og $b = \sqrt{2}$ og få

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{\sqrt{2}\cdot\sqrt{2}} = \sqrt{2}^2 = 2$$

Vi vet dermed at setningen holder enten for $a = \sqrt{2}, b = \sqrt{2}$ eller for $a = \sqrt{2}^{\sqrt{2}}, b = \sqrt{2}$, men ikke hvilken av disse det er!

Bemerkning: Siden man har vist at $\sqrt{2}^{\sqrt{2}}$ er irrasjonal, er det det andre eksemplet som faktisk gjelder. Dette er det imidlertid svært vanskelig å vise!