Noen eksempler på hvordan man fører et bevis

Nedenfor følger noen forslag om hvordan man kan føre et bevis, avhengig av påstanden man skal vise. OBS: Dette er ikke en strikt oppskrift man skal følge, men mer en veiledning om hvordan man kan angripe problemet. I de fleste tilfeller kan man gå frem på forskjellige måter.

Vi ser på følgende bevisteknikker:

- Bevis per induksjon
- Direkte bevis
- Indirekte bevis
- Bevis ved kontraposisjon
- Bevis for likhet av mengder
- Bevis for ekvivalenser
- Bevis ved moteksempler

1. Bevis per induksjon

Denne bevistypen kan vi bruke når vi skal vise noe for alle naturlige tall.

Eksempel 1.1. *Seksjon 0, Oppgave 17:*
La A være en endelig mengde, $|A| = s$. Hva er verdien til $|\mathcal{P}(A)|$? Bevis din formodning.
Løsning: Vi har $|\mathcal{P}(A)| = 2^s$. (*)

Bevis per induksjon over s:

Induksjonsstart: $s = 0$: $A = \emptyset$, $\mathcal{P}(A) = \{\emptyset\}$, $|\mathcal{P}(A)| = 1 = 2^0$, så dette er OK.

Induksjonstrinn: Vi antar nå at vår formodning (*) er sann for alle mengder med s elementer. Vi må da vise at formodningen er sann for en vilkårlig mengde med $s+1$ elementer.

La altså A være en mengde med $s+1$ elementer, la $a \in A$ og $A' = A \backslash \{a\}$. Da har A' s elementer, og ved induksjonshypotesen består $\mathcal{P}(A')$ av 2^s elementer. Vi har $\mathcal{P}(A) = \mathcal{P}(A') \cup \{B \cup \{a\} | B \in \mathcal{P}(A')\}$. Dermed er $|\mathcal{P}(A)| = |\mathcal{P}(A')| + |\mathcal{P}(A')| = 2^s + 2^s = 2 \cdot 2^s = 2^{s+1}$, og påstanden er vist.

Eksempel 1.2. *En annen formel man kan vise med induksjon, og som du kanskje har sett før, er den binomiske formelen:*
La a og b være vilkårlige reelle tall. Da er

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

for alle naturlige tall n.

Bevis per induksjon over n:

Induksjonsstart: $n = 0$: $(a+b)^0 = 1 = a^0b^0 = \sum_{i=0}^{0} \binom{0}{i} a^i b^{0-i}$, så dette er OK.

Induksjonstrinn: Anta nå at $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$. Vi må da vise at $(a+b)^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} a^i b^{n+1-i}$:

$$(a+b)^{n+1} = (a+b)(a+b)^n = (a+b)\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

$$= a\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} + b\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} = \sum_{i=0}^{n} \binom{n}{i} a^{i+1} b^{n-i} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i+1}$$

$$= \sum_{i=1}^{n+1} \binom{n}{i-1} a^i b^{n-(i-1)} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n+1-i} = \sum_{i=1}^{n} \binom{n}{i-1} a^i b^{n+1-i} + a^{n+1}$$

$$+ \sum_{i=1}^{n} \binom{n}{i} a^i b^{n+1-i} + b^{n+1} = \sum_{i=1}^{n} (\binom{n}{i-1} + \binom{n}{i}) a^i b^{n+1-i} + a^{n+1} + b^{n+1}$$

$$= \sum_{i=1}^{n} \binom{n+1}{i} a^i b^{n+1-i} + a^{n+1} + b^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} a^i b^{n+1-i}.$$

2. Direkte bevis

Eksempel 2.1. *Seksjon 4, Oppgave 32:*
La $(G, *)$ være en gruppe med identitetselement e og slik at $x * x = e$ for alle $x \in G$. Vis at G er abelsk.

Vi må altså vise at $a * b = b * a$ for alle $a, b \in G$. Her kan vi starte med $a * b$ og komme direkte frem til at dette er lik $b * a$: Siden $x * x = e$, så er $x^{-1} = x$ for alle $x \in G$. Da får vi for alle $a, b \in G$ (siden $a * b$ er igjen i G):

$$a * b = (a * b)^{-1} = b^{-1} * a^{-1} = b * a.$$

Eksempel 2.2. *Seksjon 5, Oppgave 51:*
La G være en gruppe og $a \in G$ fiksert. Vis at $H_a = \{x \in G | xa = ax\}$ er en undergruppe i G.

Bevis: Vi bruker Teorem 5.14. Vi må vise følgende tre ting:

(1) *H_a er lukket.*
(2) *Identitetselementet e i G er i H_a.*
(3) *For alle $x \in H_a$, $x^{-1} \in H_a$.*

ad (1): La $x, y \in H_a$. Vi må da vise at produktet xy ligger igjen i H_a:

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy).$$

Dermed kommuterer xy med a, og xy ligger i H_a.

ad(2): $e \in H_a$, siden $ea = a = ae$.

ad(3): Vi må vise at dersom $x \in G$ slik at $ax = xa$, så er $ax^{-1} = x^{-1}a$. Her kan vi ikke bruke samme teknikk som i (1), dvs. vi kan ikke starte med ax^{-1} og komme frem til at dette er lik $x^{-1}a$. Vi starter med det vi kjenner (nemlig $ax = xa$), og så kommer vi etter noen operasjoner frem til det vi vil ha (nemlig $x^{-1}a = ax^{-1}$):

$$\begin{aligned} ax &= xa && \text{ganger med } x^{-1} \text{ fra venstre siden} \\ x^{-1}ax &= x^{-1}xa \\ x^{-1}ax &= ea = a && \text{ganger med } x^{-1} \text{ fra høyre siden} \\ x^{-1}axx^{-1} &= ax^{-1} \\ x^{-1}a &= ax^{-1} \end{aligned}$$

3. Indirekte bevis

Når vi skal bevise noe ut ifra gitte forutsetninger, da er det av og til enklest å anta at det vi skal vise er feil, og så komme frem til noe som motsier forutsetningene. Da vet vi at vår antagelse må ha vært feil, og dermed er den opprinnelige påstanden riktig.

Eksempel 3.1. *La G være en ikke-abelsk gruppe og G' være en abelsk gruppe. Vis at det ikke kan finnes en isomorfi mellom G og G'.*

Bevis: Anta at det finnes en isomorfi mellom G og G'. La $\phi : G \to G'$ være en slik isomorfi. Da gjelder for alle $a, b \in G$: $\phi(ab) = \phi(a)\phi(b) = \phi(b)\phi(a) = \phi(ba)$ p.g.a. homomorfi-egenskapen. Dermed altså $\phi(ab) = \phi(ba)$, og siden ϕ er $1-1$, så er $ab = ba$. Men dette motsier at G ikke er abelsk (a og b var jo vilkårlige her). Dermed var vår antagelse feil, og det finnes ingen isomorfi fra G til G'.

Eksempel 3.2. *Vis at det finnes uendelig mange primtall.*

Bevis (Beviset går tilbake til Euklid): Anta at det finnes bare endelig mange primtall, la $p_1, \ldots, p_n$ være alle primtall. Se på $q = p_1 \cdot \cdots \cdot p_n + 1$. Enten er q selv prim (da har vi funnet et primtall som er forskjellig fra alle p_i, $i = 1, ..., n$) eller q har en primfaktor som er forskjellig fra primtallene $p_1, ..., p_n$: Anta nemlig at en p_i, $i \in \{1, ..., n\}$, er en primfaktor i q. Da har vi altså $p_i | p_1 \cdot \cdots \cdot p_n$ og $p_i | q$, og da må vi også ha at $p_i | (q - p_1 \cdot \cdots \cdot p_n) = 1$. Men dette er åpenbart en motsigelse, siden p_i er et primtall og dermed $\neq 1, -1$. Men dermed har vi funnet et primtall som ikke er en av $p_1, \ldots, p_n$. Altså kan ikke $p_1, \ldots, p_n$ være alle primtall, og dermed finnes det uendelig mange primtall.

4. Bevis ved kontraposisjon

Når vi skal vise at et utsagn A impliserer et utsagn B, så kan vi like godt vise at $\neg B$ impliserer $\neg A$. ($\neg B \Rightarrow \neg A$ kalles det *kontrapositive* til $A \Rightarrow B$). Av og til er det lettere å vise det kontrapositive.

Eksempel 4.1. *Vis at hvis $p \geq 3$ er et primtall, så er $p = 4k+1$ eller $p = 4k-1$ for en $k \in \mathbf{N}$.*

Bevis: Vi viser at dersom p ikke er på formen $4k+1$ eller $4k-1$, så er p ikke et primtall:

Dersom p ikke er på formen $4k+1$ eller $4k-1$, så er p på formen $4k$ eller $4k+2$ for en $k \in \mathbf{N}$.

Hvis $p = 4k$, da er $p = 2 \cdot 2k$ ikke prim.

Hvis $p = 4k+2$, da er $p = 2(2k+1)$ ikke prim.

5. Hvordan skal man vise likhet av mengder?

Noen ganger må man vise at en mengde A er lik en mengde B. Da er det oftest lurt å dele inn beviset i to deler:

(1) Vis at $A \subseteq B$, dvs. du må ta et vilkårlig element i A og vise at det ligger i B.
(2) Vis at $B \subseteq A$, dvs. for et vilkårlig element i B må du vise at elementet ligger i A.

6. Hvordan skal man vise ekvivalenser?

6.1. Når du skal vise at $A \Leftrightarrow B$ ("Utsagnet A er ekvivalent med utsagnet B"), kan du av og til starte med A og så omformulere utsagnet A endelig mange ganger på en ekvivalent måte for så til slutt å komme frem til utsagnet B. Dvs. du går frem på følgende måte:

$$\begin{aligned} & A \\ \Leftrightarrow\ & \ldots \\ \Leftrightarrow\ & \ldots \\ & \vdots \\ \Leftrightarrow\ & \ldots \\ \Leftrightarrow\ & B \end{aligned}$$

Men noen ganger kan du ikke gå frem på denne måten, men du må dele opp beviset i to bevis:

(1) Vis at $A \Rightarrow B$ ("A impliserer B")
(2) Vis at $B \Rightarrow A$ ("B impliserer A")

6.2. Noen ganger må du vise at flere utsagn er ekvivalente med hverandre, for eksempel at $A \Leftrightarrow B \Leftrightarrow C$. Da er det ofte enklest å "gå i ring", dvs. å vise at $A \Rightarrow B$, $B \Rightarrow C$, $C \Rightarrow A$.

7. Moteksempler

Noen ganger må du vise at et utsagn ikke er sant, eller avgjøre om noe er en ekvivalensrelasjon, en gruppe osv. Når du skal vise at noe ikke er sant, da må du komme med et **konkret** moteksempel som motsier utsagnet!

Eksempel 7.1. *Seksjon 0, Oppgave 30*

Avgjør om følgende er en ekvivalensrelasjon: For $x, y \in \mathbf{R}$, $x\mathcal{R}y$ *dersom* $x \geq y$.

Løsning: Denne relasjonen er ikke symmetrisk, dermed er den ikke en ekvivalensrelasjon.

Moteksempel: La $x = 2$, $y = 1$. *Da er* $x \geq y$, *og dermed* $x\mathcal{R}y$, *men* $y \ngeq x$, *dermed står ikke* y *i relasjon med* x.

(Utarbeidet av Andrea Hofmann, Vår 2007)