MAT1140

Plenumsregning 19/10

H18 Notat Peano: Vi starter med litt bakgrunnsstoff fra notatet:

$\mathbb{Z}$ er en mengde som inneholder $\mathbb{N}$ og som er utstyrt med en avbildning $-: \mathbb{Z} \to \mathbb{Z}$ slik at $- \circ - = id_{\mathbb{Z}}$ (dvs. at $-(-n) = n$ for alle $n \in \mathbb{Z}$. Har vi

$$-\mathbb{N} = \{-n : n \in \mathbb{N}\},$$

får vi

$$\mathbb{N} \cup -\mathbb{N} = \mathbb{Z} \qquad (1)$$

$$\mathbb{N} \cap -\mathbb{N} = \{0\} \qquad (2)$$

Prop 1.7: For $k \in \mathbb{Z}$ er $k = -k$ hvis og bare hvis $k = 0$.

Vi utvider etterfølgerfunksjonen S på $\mathbb{N}$ til en etterfølgerfunksjon $s: \mathbb{Z} \to \mathbb{Z}$ ved å sette

$$s(k) = \begin{cases} S(k) & \text{hvis } k \in \mathbb{N} \\ -(S^{-1}(k)) & \text{ellers} \end{cases} \qquad (3)$$

Prop 1.8: $- \circ s \circ - \circ s = id_{\mathbb{Z}}$, dvs $-s(-s(n)) = n$ for alle $n \in \mathbb{Z}$.

Observer at dette medfører at $-(-s(-s(n))) = -n$, dvs

$$s(-s(n)) = -n \qquad (4)$$

Vi har nå kommet til den første oppgaven vi skal løse, nemlig å bevise

<u>Prop 1.9</u> La P være en egenskap definert på $\mathbb{Z}$. Anta $P(0)$ og at for alle $k \in \mathbb{Z}$

$$P(k) \Leftrightarrow P(s(k)) \qquad (5)$$

Da er $P(k)$ for alle $k \in \mathbb{Z}$.

<u>Bevis:</u> Vi skal først vise $P(k)$ for alle $k \in \mathbb{N}$ og deretter for alle $k \in -\mathbb{N}$.

Vi observerer først at siden $s(k) = S(k)$ for $k \in \mathbb{N}$, så følger det fra (5) at

$$P(k) \Rightarrow P(S(k))$$

Siden vi også har $P(0)$, følger det fra vanlig induksjon (Aksiom 1.1) at $P(k)$ for alle $k \in \mathbb{N}$.

Det gjenstår å vise $P(k)$ for alle $k \in -\mathbb{N}$, altså $P(-n)$ for alle $n \in \mathbb{N}$. Ved vanlig induksjon holder det å vise at $P(-0) = P(0)$ og at $P(-n) \Rightarrow P(-S(n))$. Siden $P(0)$ er gitt, holder det å vise induksjons-trinnet. Ifølge formel (4) er $-n = s(-s(n))$, og dermed har vi

$$P(n) \Leftrightarrow P(s(-s(n))) \xLeftrightarrow{\text{antagelsen}} P(-s(n)) \Leftrightarrow P(-S(n)).$$

Dette viser induksjonstrinnet og dermed har vi $P(-n)$ for alle $n \in \mathbb{N}$.

Neste oppgave er å vise entydigheten i dette teoremet.

<u>Teorem 1.10</u>: La A være en mengde, $x \in A$ et element og $f: A \to A$ en bijeksjon. Da finnes den én og bare én avbildning $u: \mathbb{Z} \to A$ slik at $u_0 = x$ og $u_{s(n)} = f(u_n)$ for alle $n \in \mathbb{Z}$.

<u>Bevis for entydighet</u>: Anta for motsigelse at det finnes to slike funksjoner u og v. Vi skal vise ved <u>utvidet</u> <u>induksjon</u> (dvs. Prop 1.9) at $u_n = v_n$ for alle $n \in \mathbb{Z}$. La

$$P_k : u_k = v_k$$

Vi skal bruke Prop 1.9 på denne påstanden. Observer først at vi har P_0 siden $u_0 = x = v_0$. Det gjenstår å vise $P_k \Leftrightarrow P_{s(k)}$. Vi ser først implikasjonen $P_k \Rightarrow P_{s(k)}$. Vi har

$$P_k \Leftrightarrow u_k = v_k \Rightarrow f(u_k) = f(v_k) \Rightarrow u_{s(k)} = v_{s(k)} \Leftrightarrow P_{s(k)}$$

Anta omvendt at vi har $P_{s(k)}$. Da er

$$f(u_k) = u_{s(k)} = v_{s(k)} = f(v_k),$$

dvs $f(u_k) = f(v_k)$. Siden f er injektiv, betyr dette at $u_k = v_k$, dvs at vi har P_k. $\square$

Det neste resultatet i notatet innfører addisjon ~~[illegible]~~ gjennom følgende teorem:

<u>Teorem 1.11</u>: Det fines én og bare én avbildning $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ slik at

$$k + 0 = k \tag{6}$$

$$k + s(l) = s(k+l) \tag{7}$$

for alle $k, l \in \mathbb{Z}$.

Vår neste oppgave er å vise

<u>Teorem 1.12</u>: For alle $k, l, m \in \mathbb{Z}$ har vi

$$(k+l)+m = k+(l+m) \tag{8}$$

$$k+0 = 0+k = k \tag{9}$$

$$k+l = l+k \tag{10}$$

$$k+(-k) = (-k)+k = 0 \tag{11}$$

<u>Bevis</u>: Vi starter med å bevise (8). Vi holder k og l fast og viser følgende påstand ved utvidet induksjon

$$P(m): \quad (k+l)+m = k+(l+m)$$

Vi observerer først at $P(0)$ holder siden vi på venstre side av likhetstegnet har

$$(k+l)+0 \overset{(6)}{=} k+l$$

og på høyre side har

$$k+(l+0) \overset{(6)}{=} k+l.$$

For å fullføre induksjonen må vi vise at

~~[illegible]~~

$P(s(m)) \Leftrightarrow P(m)$. Vi har

$$P(s(m)) \iff (k+l)+s(m) = k+(l+s(m))$$
$$\Updownarrow \text{ (ved (7) på begge sider)}$$
$$s((k+l)+m) = k+s(l+m)$$
$$\Updownarrow \text{ (bruker (7) på høyre side)}$$
$$s((k+l)+m) = s(k+(l+m))$$
$$\Updownarrow \text{ (fordi } s \text{ er injektiv)}$$
$$(k+l)+m = k+(l+m)$$
$$\Updownarrow$$
$$P(m).$$

Dette viser at $P(s(m)) \Leftrightarrow P(m)$ og ifølge Prop 1.9 gjelder da $P(m)$ for alle m.

Vi ser nå på ligning (9). Den ene påstanden, at $k+0=k$, er identisk med (6) og dermed allerede etablert. Vi viser den andre påstanden ved entydet induksjon. La

$$P(k): \quad 0+k=k.$$

Vi sjekker først $P(0)$. På venstre side har vi $0+0=0$ ifølge (6), mens vi på høyre side bare har 0. Dermed er $P(0)$ ok. Det gjenstår å vise at $P(k) \Leftrightarrow P(s(k))$. Vi har

$$P(s(k)) \iff 0+s(k) = s(k)$$
$$\Updownarrow \text{ (7)}$$
$$s(0+k) = s(k)$$
$$\Updownarrow \text{ (s er injektiv)}$$
$$0+k=k$$
$$\Updownarrow$$
$$P(k)$$

Vi har dermed bevist (a) og går løs på (b) 6

Her viser jeg først et lemma:

Lemma A: For alle $k \in \mathbb{Z}$ har vi
$$s(0)+k = k+s(0) = s(k)$$

Bevis for lemma A: Den siste likheten følger direkte fra (6) og (7):
$$k+s(0) \overset{(7)}{=} s(k+0) \overset{(6)}{=} s(k).$$

For å vise likheten $s(0)+k = s(k)$ bruker vi utvidet induksjon på påstanden

~~$P(k): k+s(0) = s(k)$~~
$$P(k):\ s(0)+k = s(k)$$

Vi observerer først at $P(0)$ holder siden vi på venstre side har $s(0)+0 \overset{(6)}{=} s(0)$ og på høyre side har $s(0)$. Følgende argument avslutter beviset ved å vise at $P(k) \Leftrightarrow P(s(k))$:

$$P(s(k)) \Leftrightarrow s(0)+s(k) = s(s(k))$$
$$\Updownarrow \text{ (bruker (7) på høyre side)}$$
$$s(s(0)+k) = s(s(k))$$
$$\Updownarrow \ s \text{ er injektiv}$$
$$s(0)+k = s(k)$$
$$\Updownarrow$$
$$P(k)$$

$\square$

Vi går nå tilbake til ligning (10):

$$k + l = l + k$$

Vi holder k fast og viser påstanden ved utvidet induksjon på l, dvs vi bruker induksjonshypotesen

$$P(l): \quad k + l = l + k.$$

For $l = 0$ blir dette $k + 0 = 0 + k$, som holder ifølge (9). Det gjenstår å vise at $P(l) \Rightarrow P(s(l))$. Vi får

$$
\begin{aligned}
P(s(l)) \Leftrightarrow k + s(l) &= s(l) + k \\
&\Updownarrow \text{(bruker (10)) (lemma A)} \\
s(k+l) &= (l + s(0)) + k \\
&\Updownarrow \text{(bruker (8))} \\
s(k+l) &= l + (s(0) + k) \\
&\Updownarrow \text{(lemma A)} \\
s(k+l) &= l + s(k) \\
&\Updownarrow \text{(bruker (7))} \\
s(k+l) &= s(l+k) \\
&\Updownarrow \text{(s er injektiv)} \\
k + l &= l + k \\
&\Updownarrow \\
&P(l)
\end{aligned}
$$

Dermed er (10) vist.

Før vi viser (11), trenger vi et lemma til

<u>Lemma B</u>: For alle $k \in \mathbb{Z}$ er $-s(k) = -k + s^{-1}(0)$.

<u>Bevis for lemma B</u>: Vi tar s av begge sider. På venstre siden får vi

$$s(-s(k)) = -k \quad \text{ved formel (4)}$$

På høyre side får vi

$$s(-k + s^{-1}(0)) \overset{(7)}{=} -k + s(s^{-1}(0)) = -k + 0 = -k.$$

Siden s er injektiv, betyr dette at

$$-s(k) = -k + s^{-1}(0). \qquad \square$$

For å vise (11) foretar vi først følgende regnestykke:

$$s(k) + (-s(k)) \overset{\text{Lemma A, B}}{=} (k + s(0)) + (-k + s^{-1}(0))$$

$$\overset{(10)}{=} (k + s(0)) + (s^{-1}(0) - k) \overset{(8)}{=} [(k + s(0)) + s^{-1}(0)] + (-k)$$

$$\overset{(8)}{=} [k + (s(0) + s^{-1}(0))] + (-k)$$

$$\overset{(10)}{=} [k + (s^{-1}(0) + s(0))] + (-k)$$

$$\overset{(7)}{=} [k + (s(s^{-1}(0)) + 0)] + (-k)$$

$$= [k + (0 + 0)] + (-k)$$

$$= k + (-k).$$

Dette viser at $s(k) + (-s(k)) = k + (-k)$ for alle k.

Vi fullfører nå beviset for (11) ved å bruke ekvidelt induksjon på følgende utsagn

$P(k): k + (-k) = 0.$

Vi ser først at $P(0)$ holder ved å observere at $0 + (-0) = 0 + 0 = 0$. Siden vi allerede har vist at $k + (-k) = s(k) + (-s(k))$, ser vi at $P(k) \Leftrightarrow P(s(k))$, og dermed er (11) bevist.

Dette avslutter beviset for teorem 1.12 $\square$

Vi innfører en relasjon $\leq$ på $\mathbb{Z}$ ved

$$k \leq l \Leftrightarrow l - k \in \mathbb{N}.$$

Vår neste oppgave er å bevise teorem 1.13 som vi deler opp i to deler.

Teorem 1.13A: $\leq$ er en total ordning på $\mathbb{Z}$.

Bevis: Vi sjekker først at $\leq$ tilfredsstiller de tre kravene til en ordning:

(i) Refleksiv: Siden $k - k = k + (-k) = 0 \in \mathbb{N}$, er $k \leq k$, som betyr at $\leq$ er refleksiv.

~~(ii) Symmetrisk: Vi må vise at hvis k≤l og l≤k~~

(ii) Antisymmetri: Vi må vise at hvis $k \leq l$ og $l \leq k$, så er $l = k$. Dette betyr at $l - k \in \mathbb{N}$ og $k - l \in \mathbb{N}$. Et lite regnestykke som assosiative og kommutative lover (formlene (8) og (10)) viser at

$$(l - k) + (k - l) = (l + (-k)) + (k + (-l)) = 0.$$

Siden $l - k, k - l \in \mathbb{N}$, betyr dette at $l + (-k) = 0$ (dette krever egentlig et eget argument).

Siden vi også har $l+(-l)=0$, betyr dette at $l+(-k)=l+(-l)$. Forkortningsregelen (formel (17) i notatet) kan lett utvides til $\mathbb{Z}$, og dermed får vi $(-k)=(-l)$. Siden

se side 18

funksjonen $-$ er injektiv er dermed $k=l$, og antisymmetri er bevist.

(iii) <u>Transitivitet</u>: Anta $k\leq l$ og $l\leq m$. Da er $l-k\in\mathbb{N}$ og $m-l\in\mathbb{N}$, og følgelig er $(l-k)+(m-l)\in\mathbb{N}$. Ved litt regning ser vi at

$$(l-k)+(m-l)=(l+(-k))+(m+(-l))$$
$$=(l+(-l))+(m+(-k))=m-k.$$

Dermed ~~...~~ m-k ∈ N, dvs $k\leq m$, som viser transitiviteten.

Det gjenstår å vise at ordningen er total. Anta at $k,l\in\mathbb{Z}$. Et regnestykke viser at $(l-k)=-(k-l)$. Dette hvis ikke $l-k$ er i $\mathbb{N}$, så er $k-l$ det. Vi har altså enten $l-k\in\mathbb{N}$ eller $k-l\in\mathbb{N}$, dvs enten $l\geq k$ eller $k\geq l$. Dette viser at ordningen er total og beviset er dermed fullført.

Teorem 1.13 B: Hver ikke-tomme delmengde av $\mathbb{Z}$ som har en nedre skranke har et minste element. Hver ikke-tomme delmengde av $\mathbb{Z}$ som har en övre skranke har et största element.

Bevis: Jeg viser den första delen. Ideen er å føre problemet til velordningsprinsippet (teorem 1.6 i notatet). Anta at A er mengden vår og at a er en nedre skranke. Da er

$$B = \{x - a : x \in A\}$$

en delmengde av $\mathbb{N}$ ifølge teorem 1.6 har B et minste element $x_0 - a$, der $x_0 \in A$. Da er x_0 det minste elementet i A.

Beviset for den andre delen er tilsvarende. $\square$

Vi skal nå se på multiplikasjon:

Teorem 1.14 Det finnes én og bare én avbildning $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ slik at for alle $k, l \in \mathbb{Z}$:

$$k \cdot 0 = 0 \qquad (12)$$

$$k \cdot s(l) = k \cdot l + k \qquad (13)$$

Bevis: For hver k lar vi $f_k : \mathbb{Z} \to \mathbb{Z}$ ved $f_k(l) = l + k$. Bruker vi teorem 1.10 på denne og initialbetingelsen $u_k(0) = 0$, får vi en funksjon $u_k : \mathbb{Z} \to \mathbb{Z}$ slik at $u_k(s(\ell)) = f_k(u_k(\ell))$ $= u_k(\ell) + k$. Denne funksjonen er entydig bestemt. Setter vi $k \cdot \ell = u_k(\ell)$, får vi $k \cdot s(\ell) = k\ell + k$, akkurat som vi ønsket oss $\square$

Vi skal dele opp det lange teorem 1.15 i to deler. Vi definerer $1 = S(0)$.

<u>Teorem 1.15A</u> For alle $k, l, m \in \mathbb{Z}$ har vi

$$(k \cdot l) \cdot m = k(l \cdot m) \tag{14}$$

$$k \cdot 1 = 1 \cdot k = k \tag{15}$$

$$k \cdot l = l \cdot k \tag{16}$$

$$(k + l) \cdot m = km + lm \tag{17}$$

$$m(k+l) = m \cdot k + m \cdot l \tag{18}$$

<u>Bevis</u>: Prøver man å bevise (14), oppdager man fort at man trenger distributivitet og vi begynner derfor med (18)

<u>(18)</u> Vi holder m og k fast og bruker utvidet induksjon til å vise

$P(\ell)$: $m(k+\ell) = m \cdot k + m \cdot \ell$

Vi ser først at $P(0)$ holder siden begge sider er lik $m \cdot k$. Det er dermed nok å vise at $P(\ell) \Leftrightarrow P(s(\ell))$. Vi har

$$P(s(l)) \Leftrightarrow m\cdot(k+s(l)) = m\cdot k + m\cdot s(l)$$

$$(17) \Updownarrow (13)$$

$$m\cdot s(k+l) = m\cdot k + (m\cdot l + m)$$

$$(13) \Updownarrow \text{ assosiativ lov for addisjon}$$

$$m\cdot(k+l) + m = (m\cdot k + m\cdot l) + m$$

$$\Updownarrow \text{ forkortingsregel}$$

$$m\cdot(k+l) = m\cdot k + m\cdot l$$

$$\Updownarrow$$

$$P(l)$$

<u>14</u> Vi kan må bevise (14) med samme teknikk.
Vi holder fast k og l, og bruker induksjon
på

$$P(m):\quad (k\cdot l)\cdot m = k\cdot(l\cdot m)$$

Vi ser at $P(0)$ holder siden begge sider blir 0,
og det gjenstår dermed å vise $P(m) \Leftrightarrow P(s(m))$.
Vi har:

$$P(s(m)) \Leftrightarrow (k\cdot l)\cdot s(m) = k\cdot(l\cdot s(m))$$

$$\Updownarrow (13)$$

$$(k\cdot l)\cdot m + k\cdot l = k\cdot(l\cdot m + l)$$

$$\Updownarrow (18)$$

$$(k\cdot l)\cdot m + k\cdot l = k(l\cdot m) + k\cdot l$$

$$\Updownarrow \text{ forkortingsregelen.}$$

$$(k\cdot l)\cdot m = k(l\cdot m)$$

$$\Updownarrow$$

$$P(m).$$

Dermed er (14) bevist.

(15) Den ene likheten er enkel:

$$k \cdot 1 = k \cdot s(0) = k \cdot 0 + k = k.$$

For å vise at $1 \cdot k = k$ bruker vi induksjon på

$$P(k) : 1 \cdot k = k.$$

$P(0)$ holder siden begge sider er 0, og følgende resonnement viser at $P(k) \Leftrightarrow P(s(k))$

$$P(s(k)) \Leftrightarrow 1 \cdot s(k) = s(k)$$

$$\Updownarrow \text{ Lemma A}$$

$$1 \cdot k + 1 = k + s(0)$$

$$\Updownarrow \text{ def. av } +$$

$$1 \cdot k + 1 = k + 1$$

$$\Updownarrow \text{ forkortningsregel}$$

$$1 \cdot k = k$$

$$\Updownarrow$$

$$P(k)$$

(17). Vi trenger denne før vi beviser (16). Vi bruker utvidet induksjon på

$$P(m) : (k+l) \cdot m = k \cdot m + l \cdot m$$

$P(0)$ holder siden begge sider er 0. Følgende argument viser at $P(m) \Leftrightarrow P(s(m))$

$$P(s(m)) \Leftrightarrow (k+l) \cdot s(m) = k \cdot s(m) + l(s(m))$$

$$\Updownarrow$$

$$(k+l)m + (k+l) = (k \cdot m + k) + (l \cdot m + l)$$

$$\Updownarrow$$

$$(k+l)m + (k+l) = (k \cdot m + l \cdot m) + (k+l)$$

$$\Updownarrow \text{ forkortningsregel}$$

$$(k+l) \cdot m = k \cdot m + l \cdot m \Leftrightarrow P(m)$$

(16) Vi bruker utvidet induksjon på

$P(\ell)$: $k \cdot \ell = \ell \cdot k$

$P(0)$ holder siden begge sider er 0 (vi trenger egentlig et eget induksjonsbevis for å vise at $0 \cdot k = 0$, men det overlates til leseren). Følgende argument viser at $P(\ell) \Leftrightarrow P(s(\ell))$:

$$
\begin{aligned}
P(s(\ell)) \Leftrightarrow k \cdot s(\ell) &= s(\ell) \cdot k \\
&\Updownarrow \text{(13)} \quad \text{Lemma A} \\
k \cdot \ell + k &= (\ell + 1) \cdot k \\
&\Updownarrow \text{(17)} \\
k \cdot \ell + k &= \ell \cdot k + k \\
&\Updownarrow \\
k \cdot \ell &= \ell \cdot k \\
&\Updownarrow \\
&P(\ell)
\end{aligned}
$$

$\square$

Før vi beviser resten av teorem 1.14, er det et par andre ting vi bør ta oss av

<u>Lemma C</u>: For alle $k, \ell \in \mathbb{Z}$ har vi

$$(-k) \cdot \ell = k(-\ell) = -(k\ell) \qquad (19)$$

og

$$(-k) \cdot (-\ell) = k \cdot \ell. \qquad (20)$$

Bevis: Siden vi nå har etablert at multiplikasjon er kommutativ (16), holder det å ~~[illegible]~~ bevise den ene likheten i (19). Vi observerer først at $k \cdot l + k(-l) = k \cdot (l + (-l)) = k \cdot 0 = 0$. På den annen side er $k \cdot l + (-(kl)) = 0$. Siden begge sider er null, har vi dermed

$$k \cdot l + k \cdot (-l) = k \cdot l + (-(kl)),$$

som ved forkortningsregelen gir $k \cdot (-l) = -(kl)$.

For å bevise (20) observerer vi at

$$(-k)(-l) = -(k(-l)) = -(-(k \cdot l)) = k \cdot l$$

ved to ganger bruk av (19) $\square$

<u>Lemma D</u>: Hvis $k, l > 0$ (dvs $k, l \in \mathbb{N}_+$), så er $k \cdot l > 0$.

<u>Bevis</u>: Vi holder fast $k > 0$ og viser ved vanlig induksjon at

$P(l)$: $l = 0$ eller $k \cdot l > 0$.

Siden $P(0)$ åpenbart er sann, holder det å vise at $P(l) \Rightarrow P(s(l))$. Anta derfor at $P(l)$ holder. Da er $k \cdot s(l) = k \cdot l + k > k \cdot l \geq 0$. Dette viser at $P(s(l))$ holder.

Vi er nå klar til å vise de siste delene av teorem 1.15:

<u>Teorem 1.15 B</u>: For alle $k, l \in \mathbb{Z}$ gjelder

$$k \cdot l = 0 \Rightarrow k = 0 \vee l = 0 \qquad (21)$$

For alle $m \in \mathbb{Z}$

$$k \leq l \Leftrightarrow k + m \leq l + m \qquad (22)$$

$$k \geq 0 \wedge l \geq 0 \Rightarrow k \cdot l \geq 0 \qquad (23)$$

<u>Bevis</u>: Vi beviser den kontrapositive versjonen av (21) som sier at hvis $k \neq 0$ og $l \neq 0$, så er $k \cdot l \neq 0$. Hvis k, l er positive, vet vi dette fra lemma D. De andre mulighetene er at én eller begge faktorene k, l er negativ, f. eks $k = -m$ der $m \in \mathbb{N}_+$, eller $k = -m, l = -n$ der $m, n \in \mathbb{N}_+$. Da følger resultatet fra lemma C og det vi allerede har vist.

For å vise (22) observerer vi at

$$(l+m) - (k+m) = (l+m) + (-(k+m))$$
$$= (l+m) + ((-k) + (-m)) = l - k$$

etter endel bruk av assosiativitet og kommutativitet (vi har også brukt at $-(k+m) = (-k) + (-m)$ som bør vises separat)

Dermed har vi

$$k \leq l \Leftrightarrow l-k \geq 0 \Leftrightarrow (l+m)-(k+m) \geq 0$$
$$\Updownarrow$$
$$(k+m) \leq (l+m).$$

Det siste punktet, (23), følger fra lemma D.

Appendiks: Bevis for forkortningsregelen.

Jeg glemte å ta med et bevis for denne regelen der jeg burde:

Forkortningsregelen: For alle $k, l, m \in \mathbb{Z}$ gjelder

$$k+m = l+m \Rightarrow k = l$$

Bevis: Vi starter med følgende lille observasjon som bygger på at s er injektiv:

$$(*) \quad k+m = l+m \Longleftrightarrow s(k+m) = s(l+m) \Longleftrightarrow k+s(m) = l+s(m)$$

For å bevise setningen bruker vi utvidet induksjon på påstanden

$$P(m): \ \forall k, l \in \mathbb{Z} \ (k+m = l+m \Rightarrow k = l)$$

$P(0)$ er åpenbar sann siden $k+0=k$ og $l+0=l$.

For å bevise $P(m) \Rightarrow P(s(m))$, antar vi at $P(m)$ holder og at $k+s(m) = l+s(m)$. Ifølge $(*)$ er da $k+m = l+m$, og siden $P(m)$ holder, betyr dette at $k = l$. Dette viser at $P(s(m))$ holder.

Bevisel for at $P(s(m)) \Rightarrow P(m)$ er tilsvarende. Anta at $P(s(m))$ holder og at $k + m = l + m$. Ifølge (*) er da $k + s(m) = l + s(m)$, og siden $P(s(m))$ holder, betyr dette at $k = l$. Dermed holder $P(m)$ og beviset er fullført. $\square$