KTH Matematik
Bengt Ek
April 2006

Kompletteringsmaterial till kursen 5B1928 Logik för D1:

K1 Något om axiomatisering och Peanos axiomsystem

Dessa sidor berör delar av logiken som är lite mer teoretiska, och kanske "svårare", än de vi hittills sysslat med. Vi har tidigare i kursen lärt oss hur man kan härleda sentenser ur andra sentenser och att bestämma sanningsvärden för sentenser i en given tolkning. Man kan säga att vi nu skall "höja oss" lite och betrakta egenskaper under härledning hos sentensmängder och modeller för sentensmängder, dvs tolkningar som gör alla sentenserna sanna. För oss är axiomen för linjärt ordnade mängder och Peanos axiomsystem de viktigaste exemplen, se nedan.

Som tidigare i kursen (men inte i Forbes bok) kommer vi att använda predikatlogik med **n-ställiga funktionssymboler**. Vi påminner oss att det då i det logiska språket finns, utöver n-ställiga predikatsymboler och individkonstanter (vilka kan betraktas som 0-ställiga funktionssymboler) som vi haft tidigare, också funktionssymboler $f, g, ...$, var och en med sin "ställighet". Om f t.ex. är en 2-ställig funktionssymbol är $f(a,b), f(a,a), f(x,c), f(f(x,y),x)$ alla **termer**, dvs de kan stå i samma positioner i predikatlogiska formler som individkonstanter och individvariabler. En tolkning $\mathfrak{I}$ tillordnar symbolen f en funktion $f^{\mathfrak{I}}$ (som vi också kan kalla $\mathrm{Ref}(f)$) av två variabler i domänen D, med värden i D.

Begreppen modell och teori:

Definition:
En tolkning $\mathfrak{I}$ är en **modell** för en mängd sentenser Δ om $\mathfrak{I}$ ger alla sentenser i Δ sanningsvärdet 1.
Vi kan också uttrycka detta som att $\mathfrak{I}$ **satisfierar** Δ.
(Δ behöver inte vara ändlig, vi kan också ha en oändlig mängd sentenser.)

Definition:
En mängd sentenser $\mathcal{T}$ som är sluten under härledning kallas för **en teori**.

Villkoret är alltså att varje sentens som kan härledas (med naturlig deduktion, säg) från sentenser i $\mathcal{T}$ tillhör $\mathcal{T}$. Med symboler: $\mathcal{T} \vdash q \Rightarrow q \in \mathcal{T}$. Speciellt

ingår alla teorem i alla teorier (teorem är ju sentenser som kan härledas från vilken sentensmängd som helst).

Definitionen tar bara fasta på vilka sentenser som teorin påstår gälla, inte "innehållet", vad det handlar om.

Exempel på teorier:

- Mängden av **alla** välformade sentenser i något predikatlogiskt språk är sluten under härledning. Den utgör alltså en teori (teorin som säger att allt gäller, "anything goes").
- För en tolkning $\mathfrak{I}$ finns en motsvarande teori $\mathcal{T}_{\mathfrak{I}}$ som består av alla sentenser som är sanna i $\mathfrak{I}$. Sundhetssatsen för naturlig deduktion medför ju att alla sentenser som kan härledas från sentenser som är sanna i $\mathfrak{I}$ också är sanna i $\mathfrak{I}$, så $\mathcal{T}_{\mathfrak{I}}$ är en teori.
- Om man utgår från en godtycklig mängd sentenser $\mathcal{A}$ och låter $\mathcal{T}_{\mathcal{A}}$ vara alla sentenser som kan härledas från $\mathcal{A}$, $\mathcal{T}_{\mathcal{A}} = \{q : \mathcal{A} \vdash q\}$, blir detta en teori. (Allt som kan härledas från sådant som kan härledas från $\mathcal{A}$ kan ju härledas från $\mathcal{A}$.)

Viktiga **egenskaper för teorier:**

- $\mathcal{T}$ är **konsistent** omm $\curlywedge \notin \mathcal{T}$, dvs precis om det inte för någon sentens p gäller att både p och $\sim p$ ligger i $\mathcal{T}$. Den enda teori (över ett givet språk) som inte är konsistent är teorin som innehåller alla välformade sentenser i språket (varför?). Enligt sundhets- och fullständighetssatsen är en teori konsistent om och endast om den har en modell, dvs en satisfierande tolkning.
- $\mathcal{T}$ är **fullständig** om det för varje sentens p gäller att (minst) en av p och $\sim p$ tillhör $\mathcal{T}$. Det finns alltså inga sentenser i språket som teorin "saknar åsikt om". Alla modeller för en fullständig teori ger samma sanningsvärden till alla sentenser i språket.
- $\mathcal{T}$ är **axiomatiserbar** omm det finns en **avgörbar** mängd sentenser $\mathcal{A}$ så att $\mathcal{T} = \{q : \mathcal{A} \vdash q\}$. $\mathcal{A}$ kallas ett **axiomsystem** för teorin, sentenserna i $\mathcal{A}$ kallas **axiom**. Att $\mathcal{A}$ är *avgörbar* betyder att det finns en algoritm för att avgöra om en given sentens tillhör $\mathcal{A}$ eller inte. Vi ger här inte en exakt definition av vad en algoritm är.

Ett axiomsystem kallas konsistent eller fullständigt om motsvarande teori är konsistent respektive fullständig. Axiomen i $\mathcal{A}$ sägs vara **oberoende** om det inte går att härleda något av dem från de övriga, dvs om

$$\mathcal{A} \setminus \{p\} \nvdash p \text{ för alla } p \in \mathcal{A}.$$

För att visa detta räcker det enligt sundhetssatsen att finna en tolkning som satisfierar $\mathcal{A} \setminus \{p\}$ men inte p.

Exempel på axiomsystem:

1. Axiomen för en linjärt (strikt) ordnad mängd:

Språk:
en tvåställig relationssymbol $<$
(som vanligt i matematiken skriver vi $x < y$ i stället för $<xy$.)

Axiom:

<1	$\forall x \sim x < x$	$<$ är irreflexiv, inget element är mindre än sig själv
<2	$\forall x \forall y \forall z ((x < y \,\&\, y < z) \rightarrow x < z)$	$<$ är transitiv
<3	$\forall x \forall y (x < y \vee x = y \vee y < x)$	av två olika element är alltid ett mindre än det andra

[Att mängden är *linjärt* (även kallat *totalt*) ordnad innebär just att tolkningen satisfierar <3. <1 och <2 är axiomen för en **partiellt** (strikt) ordnad mängd.]

Exempel på linjärt ordnade mängder (dvs modeller för <1 – <3):

- $D = \mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$, heltalen, med $<$ tolkad som "mindre än"
- $D = [0, 2] = \{x \in \mathbb{R} : 0 \leq x \leq 2\}$, alla reella tal mellan och med 0 och 2, $<$ åter tolkad som "mindre än"
- $D = \mathbb{R}_0 \cup \mathbb{Z}_1$, där $\mathbb{R}_0$ och $\mathbb{Z}_1$ är två "disjunkta kopior" av $\mathbb{R}$ och $\mathbb{Z}$ (dvs $\mathbb{R}_0$ och $\mathbb{Z}_1$ "ser ut" precis som $\mathbb{R}$ och $\mathbb{Z}$, men $\mathbb{R}_0 \cap \mathbb{Z}_1 = \varnothing$) och $a < b$ precis om $a \in \mathbb{R}_0$ och $b \in \mathbb{Z}_1$ eller $a < b$ i $\mathbb{R}_0$ eller $\mathbb{Z}_1$

Exempel på partiellt ordnade mängder är de ovanstående och:

- $D = \mathbb{N} = \{0, 1, 2, \dots\}$, de naturliga talen, med $a < b$ tolkad som "a är en delare till b och $a \neq b$"

Övningar

$<$1. Vilka av följande tolkningar satisfierar axiomen <1 – <3?
a) $D = \mathbb{N} = \{0, 1, 2, 3, ...\}$, de naturliga talen, $<$ tolkat som "större än".
b) $D = \{\alpha, \beta, \gamma\}$, $\mathrm{Ext}(<) = \{\langle\alpha, \beta\rangle, \langle\beta, \gamma\rangle, \langle\gamma, \alpha\rangle\}$.
c) $D = \mathbb{N} \setminus \{0\} = \{1, 2, 3, ...\}$, de positiva heltalen, $a < b$ tolkat som "$a \neq b$ och b är (jämnt) delbart med a.
$<$2. Visa att axiomen <1 – <3 är oberoende. [Ledning: för att visa att ett axiom är oberoende av de övriga, dvs inte kan härledas från dem, räcker det att finna en modell för de övriga som gör det falskt.]
$<$3. Visa att sentensen $\forall x \forall y (x < y \rightarrow \sim y < x)$ följer ur axiom <1 och <2. En (total eller partiell) ordningsrelation är alltså asymmetrisk.
$<$4. Är teorin som ges av axiomen <1 – <3 fullständig?
$<$5. Visa att om $\mathfrak{A} = (A, <_a), \mathfrak{B} = (B, <_b)$ är två modeller för axiomen <1 – <3, med domänerna A och B disjunkta, är $\mathfrak{A}+\mathfrak{B} = (A \cup B, <)$ också en modell om $<$ definieras enligt: $x < y$ precis om någon av följande gäller 1) $x \in A$ och $y \in B$, 2) $x, y \in A$ och $x <_a y$ eller 3) $x, y \in B$ och $x <_b y$. Ordningen innebär alltså att "först kommer A och sedan kommer B".
$<$6. Låt åter $\mathfrak{A} = (A, <_a), \mathfrak{B} = (B, <_b)$ vara två modeller för axiomen <1 – <3 och definiera $\mathfrak{A} \times \mathfrak{B}$ till att vara den tolkning som har domän $A \times B = \{\langle a, b\rangle \mid a \in A, b \in B\}$ och $\langle a_1, b_1\rangle < \langle a_2, b_2\rangle$ precis om antingen $b_1 <_b b_2$ eller $b_1 = b_2$ och $a_1 <_a a_2$.
Visa att $\mathfrak{A} \times \mathfrak{B}$ också är en modell för axiomen <1 – <3.

2. Axiomen för en grupp:

Språk:
en individkonstant (dvs en 0-ställig funktionssymbol) e
en 1-ställig funktionssymbol $^{-1}$ (vi skriver t.ex. x^{-1} i stället för $^{-1}(x)$.)
en 2-ställig funktionssymbol $*$ (vi skriver t.ex. $x * y$ i stället för $*(x, y)$.)

Axiom:

G1	$\forall x \forall y \forall z\, (x * y) * z = x * (y * z)$	associativitet
G2	$\forall x\, (x * e = x \,\&\, e * x = x)$	e är identitetselement
G3	$\forall x\, (x * x^{-1} = e \,\&\, x^{-1} * x = e)$	$^{-1}$ ger en invers

Exempel på grupper:

- $D = \mathbb{Z} = \{..., -2, -1, 0, 1, 2, 3, ...\}$, med $\mathrm{Ref}(e) = 0$, addition som $*$ och teckenbyte som $^{-1}$
- $D = \{$alla inverterbara $n \times n$ - matriser$\}$, med e tolkad som I, enhetsmatrisen, $*$ som matrismultiplikation och $^{-1}$ som matrisinvers
- $D = \{$alla stela avbildningar som avbildar en kvadrat på sig själv$\}$, med e tolkad som identitetsavbildningen, $*$ som sammansättning av avbildningar och $^{-1}$ som invers avbildning

Övningar
G1. Vilka av följande är grupper (dvs modeller för gruppaxiomen)?
a) $D = \{1, i, -1, -i\}$, e tolkad som 1, $*$ tolkad som multiplikation av komplexa tal, $^{-1}$ tolkad som invertering av tal.
b) $D = \mathbb{Z}$, e tolkad som 1, $*$ tolkad som multiplikation av hela tal.
c) $D = \{1\}$, $e, *, ^{-1}$ tolkade på de enda sätt som går.
G2. Visa att sentensen $\forall x \forall y \exists z\, x * z = y$ följer ur gruppaxiomen, dvs att den är sann i alla grupper. Man kan alltså dividera godtyckliga element från vänster i en grupp (och också från höger).
G3. Visa att axiom G3 är oberoende av de övriga axiomen. [Ledning: övning G1b.]
G4. Är teorin som ges av axiomen G1 – G3 fullständig? [Ledning: kan sentensen $\forall x \forall y\, x * y = y * x$ eller dess negation härledas från axiomen?]

Om isomorfi mellan tolkningar

Exempel
Betrakta tolkningarna $\mathfrak{I}_1$ med domän $D_1 = \{0, 3, 17\}$, $<$ tolkat som "mindre än" och $\mathfrak{I}_2$ med domän $D_2 = \{\varnothing, \{\beta, \zeta\}, \{\alpha, \beta, \delta, \zeta\}\}$, $<$ tolkat som $\subset$. Dessa tolkningar är tydligen båda modeller för axiomen <1 – <3, men dessutom är de "väldigt lika", varje element i D_1 kan paras ihop med precis ett element i D_2 (nämligen $0 \mapsto \varnothing, 3 \mapsto \{\beta, \zeta\}, 17 \mapsto \{\alpha, \beta, \delta, \zeta\}$) så att motsvarande element har motsvarande relationer i de olika tolkningarna (t.ex. motsvarar $3 < 17$ och $\{\beta, \zeta\} \subset \{\alpha, \beta, \delta, \zeta\}$ varandra).

Då vi talar om *olika* tolkningar av ett logiskt språk menar vi ofta *väsentligen olika*, dvs om två tolkningar har domäner där elementen motsvarar varandra enentydigt och samma relationer, funktionssamband etc gäller mellan motsvarande element i tolkningarna, vill vi ofta inte skilja mellan dem. Detta görs exakt i det matematiska begreppet **isomorfi**.

Definition:
Två tolkningar $\mathfrak{I}_1$ och $\mathfrak{I}_2$ av samma logiska språk med domäner D_1 och D_2 sägs vara **isomorfa**, $\mathfrak{I}_1 \cong \mathfrak{I}_2$, om det finns en *isomorfi* mellan dem, dvs en *bijektion* $\varphi : D_1 \to D_2$ som "bevarar strukturen":

(1) För varje n-ställig relationssymbol R i språket och $\alpha_1, \ldots, \alpha_n \in D_1$,
$$R^{\mathfrak{I}_1}\alpha_1 \ldots \alpha_n \;\Leftrightarrow\; R^{\mathfrak{I}_2}\varphi(\alpha_1) \ldots \varphi(\alpha_n)$$

(2) För varje n-ställig funktionssymbol f i språket och $\alpha_1, \ldots, \alpha_n \in D_1$,
$$\varphi(f^{\mathfrak{I}_1}(\alpha_1, \ldots, \alpha_n)) = f^{\mathfrak{I}_2}(\varphi(\alpha_1), \ldots, \varphi(\alpha_n))$$

(3) För varje individkonstant c i språket,
$$\varphi(c^{\mathfrak{I}_1}) = c^{\mathfrak{I}_2}$$

Här står $R^{\mathfrak{I}}, f^{\mathfrak{I}}, c^{\mathfrak{I}}$ för tolkningarna av R, f, c i tolkningen $\mathfrak{I}$ och att φ är en **bijektion** betyder att varje element i D_2 är $\varphi(\alpha)$ för exakt ett $\alpha \in D_1$, dvs φ "parar ihop" elementen i D_1 enentydigt med elementen i D_2.

Idén är alltså att elementen i D_1 har samma samband som definieras av tolkningen som motsvarande element i D_2, de kan ses som två olika representanter för samma "abstrakta tolkning". Ett svenskt ord för isomorfi (relationen, inte funktionen) är *strukturlikhet*.
Det är inte svårt att inse att isomorfa tolkningar ger samma sanningsvärden till alla sentenser i språket. Mindre klart är kanske att det omvända inte gäller, man kan ha olika, icke-isomorfa, tolkningar som ger samma sanningsvärden till alla sentenser (sådana tolkningar kallas **ekvivalenta**, betecknat $\mathfrak{I}_1 \equiv \mathfrak{I}_2$. $\mathfrak{I}_1 \cong \mathfrak{I}_2$ är alltså ett **starkare** villkor än $\mathfrak{I}_1 \equiv \mathfrak{I}_2$.).

Relationen $\cong$ mellan tolkningar är *reflexiv* (isomorfi mellan $\mathfrak{I}$ och $\mathfrak{I}$: identitetsfunktionen $I(\alpha) = \alpha$), *symmetrisk* (om φ ger isomorfin $\mathfrak{I}_1 \cong \mathfrak{I}_2$ ger den inversa funktionen φ^{-1} isomorfin $\mathfrak{I}_2 \cong \mathfrak{I}_1$) och *transitiv* (om φ ger isomorfin $\mathfrak{I}_1 \cong \mathfrak{I}_2$ och ψ ger isomorfin $\mathfrak{I}_2 \cong \mathfrak{I}_3$, ger sammansättningen $\psi\varphi$ isomorfin $\mathfrak{I}_1 \cong \mathfrak{I}_3$). $\cong$ är alltså en **ekvivalensrelation** mellan tolkningar. Då vi studerar en teori är vi oftast bara intresserade av **ekvivalensklasser** av tolkningar.

För att visa att två tolkningar är isomorfa räcker det att finna en isomorfi φ (och visa att den verkligen är en isomorfi).
För att visa att två tolkningar inte är isomorfa är det tillräckligt att finna en sentens som är sann i den ena tolkningen men inte i den andra. Enligt ovan finns det fall när detta inte är möjligt, nämligen om två tolkningar är ekvivalenta utan att vara isomorfa.

Exempel på isomorfa tolkningar:

- $\mathfrak{I}_1$, $\mathfrak{I}_2$ och $\mathfrak{I}_3$ givna av $D_1 = \mathbb{N} = \{0, 1, 2, \dots\}$, $D_2 = 2\mathbb{N} = \{0, 2, 4, \dots\}$, $D_3 = \{2, 8, 18, 32, \dots\}$ och $<$ tolkad som "mindre än" i alla tre fallen, är tre isomorfa modeller för axiomen <1 – <3. Isomorfier $\varphi : D_1 \to D_2$ och $\psi : D_1 \to D_3$ ges av $\varphi(n) = 2n, \psi(n) = 2(n+1)^2$, man ser ju att φ är en bijektion från D_1 till D_2 och att $m < n \Leftrightarrow \varphi(m) < \varphi(n)$ och motsvarande för ψ.
- $\mathfrak{I}_1$ och $\mathfrak{I}_2$ givna av $D_1 = \mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}, D_2 = \mathbb{R}$, de reella talen, med e tolkat som 1 respektive 0, $^{-1}$ enligt $x^{-1} = \frac{1}{x}$ respektive $-x$, $*$ som $\times$ respektive $+$ är isomorfa grupper, dvs isomorfa modeller för axiomen G1 – G3. En isomorfi ges av $\varphi(x) = \log x$. T.ex. är ju $\varphi(x_1 *^{\mathfrak{I}_1} x_2) = \log(x_1 x_2) = \log x_1 + \log x_2 = \varphi(x_1) *^{\mathfrak{I}_2} \varphi(x_2)$ och $\varphi(e^{\mathfrak{I}_1}) = \varphi(1) = \log 1 = 0 = e^{\mathfrak{I}_2}$.
- Om $\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{B}_1, \mathfrak{B}_2$ är modeller för axiomen <1 – <3, sådana att $\mathfrak{A}_1 \cong \mathfrak{A}_2$ och $\mathfrak{B}_1 \cong \mathfrak{B}_2$, gäller också att $\mathfrak{A}_1 + \mathfrak{B}_1 \cong \mathfrak{A}_2 + \mathfrak{B}_2$. Om φ_a och φ_b ger isomorfierna mellan $\mathfrak{A}_1, \mathfrak{A}_2$ respektive $\mathfrak{B}_1, \mathfrak{B}_2$, ges en isomorfi mellan $\mathfrak{A}_1 + \mathfrak{B}_1$ och $\mathfrak{A}_2 + \mathfrak{B}_2$ av φ, given av $\varphi(x) = \varphi_a(x)$ om $x \in A_1$ och $\varphi(x) = \varphi_b(x)$ om $x \in B_1$. Man kan verifiera att $x <_1 y \Leftrightarrow \varphi(x) <_2 \varphi(y)$.
  Genom att använda detta kan man också definiera $\mathfrak{A} + \mathfrak{B}$ (på isomorfi när) även om A och B inte är disjunkta, ersätt t.ex. $\mathfrak{A}$ med en isomorf tolkning vars domän A är disjunkt med $\mathfrak{B}$:s domän B.

Övningar

Iso1. Visa att $\mathfrak{I}_1$ och $\mathfrak{I}_2$ är isomorfa grupper, och ange en isomorfi φ mellan dem.
$\mathfrak{I}_1$ ges av $D_1 = \{1, i, -1, -i\}$, e tolkad som 1, $*$ tolkad som multiplikation av komplexa tal, $^{-1}$ tolkad som invertering av tal.
$\mathfrak{I}_2$ ges av $D_2 = \{\pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \pm \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\}$, e tolkad som $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $*$ tolkad som matrismultiplikation och $^{-1}$ tolkad som matrisinvers.

Iso2. Låt $\mathfrak{A} = (A, <_a), \mathfrak{B} = (B, <_b)$ vara som i övning <5 ovan. Visa med ett motexempel att $\mathfrak{A} + \mathfrak{B}$ och $\mathfrak{B} + \mathfrak{A}$ inte alltid är isomorfa.
[Går det med ändliga mängder A, B?]

Iso3. Betrakta åter $\mathfrak{A}, \mathfrak{B}$ som i <5,6.
Visa med ett motexempel att $\mathfrak{A} \times \mathfrak{B}$ och $\mathfrak{B} \times \mathfrak{A}$ inte alltid är isomorfa.

Peanos axiom för de naturliga talen

Peanos axiom beskriver de naturliga talen. Då vi studerar dem har vi alltså en viss tolkning (**standardmodellen** $\mathbb{N}$) i tankarna. Vi vill härleda egenskaper för de naturliga talen ur axiomen, därmed slipper vi att syssla explicit med den oändliga domänen. Helst vill vi förstås att alla satser som gäller för naturliga tal skall kunna bevisas med dessa axiom, dvs att det skall vara ett fullständigt axiomsystem.

Peanos axiom

Språk (tolkningen i standardmodellen inom [ ]):
en 0-ställig funktionssymbol (dvs en individkonstant) 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	$\forall z_1 ... \forall z_n((\phi 0\ \&\ \forall x\,(\phi x \rightarrow \phi S(x))) \rightarrow \forall x\, \phi x)$	induktionsaxiom

I P7 är ϕx en godtycklig formel med alla fria variabler bland $x, z_1, ..., z_n$. P7 är alltså egentligen ett oändligt antal axiom, ett s.k. **axiomschema**. Vi kommer bara att behöva fallet $n = 0$.

Övningar

P1. Visa med Peanos axiom (eller Q-axiomen, se nedan) och naturlig deduktion att $1 + 1 = 2$. (1 betyder $S(0)$ och 2 betyder $S(1)$.)
P2. Visa att följande följer ur Peanos axiom (det krävs inte ett formellt bevis med naturlig deduktion, det kan bli för långt)
a) $\forall x\, 0 + x = x$.
b) $\forall x \forall y\, y + S(x) = S(y) + x$.
c) $\forall x \forall y\, x + y = y + x$.
d) $\forall x\,(x \neq 0 \rightarrow \exists y\, x = S(y))$, dvs axiom Q7 nedan.
e) $\forall x\, S(0) * x = x$.
Man får i varje deluppgift anta att de föregående i listan redan visats.

Ett svagare axiomsystem för de naturliga talen

Ett svagare system av axiom än Peanos är de s.k. **Q-axiomen**. De är svagare än Peanos axiom i betydelsen att allt som kan visas med dem också kan visas med Peanos axiom (dvs alla Q-axiomen kan härledas från Peanos axiom), men inte tvärtom. Q-axiomen kommer vi att stöta på igen då vi talar om Gödels ofullständighetssats.

Q-axiomen

Språk: som för Peano

Axiom:

Q1	$\forall x\,\forall y\,(S(x)=S(y)\rightarrow x=y)$	=P1
Q2	$\forall x\,S(x)\neq 0$	=P2
Q3	$\forall x\,x+0=x$	=P3
Q4	$\forall x\,\forall y\,x+S(y)=S(x+y)$	=P4
Q5	$\forall x\,x*0=0$	=P5
Q6	$\forall x\,\forall y\,x*S(y)=(x*y)+x$	=P6
Q7	$\forall x\,(x\neq 0\rightarrow\exists y\,x=S(y))$	alla utom 0 är efterföljare

Övningar

Q1) Visa att följande **inte** följer ur Q-axiomen:

a) $\forall x\,x\neq S(x)$

b) $\forall x\forall y\,x+y=y+x$

c) $\forall x\forall y\forall z\,x+(y+z)=(x+y)+z$

d) $\forall x\,0+x=x$

e) $\forall x\,0*x=0$

f) $\forall x\forall y\forall z\,x*(y+z)=(x*y)+(x*z)$

Ledning: betrakta tolkningen $D=\mathbb{N}\cup\{\alpha,\beta\},\quad \alpha\neq\beta,\quad \alpha,\beta\notin\mathbb{N}$

x	$S(x)$
n	$n+1$
α	α
β	β

$n\in\mathbb{N}$

$+$	n	α	β
m	$m+n$	β	α
α	α	β	α
β	β	β	α

$m,n\in\mathbb{N}$

$*$	0	j	α	β
0	0	0	α	β
i	0	$i\cdot j$	α	β
α	0	β	β	β
β	0	α	α	α

$i,j\in\mathbb{N};\ i,j\neq 0$

Om välordnade mängder

Detta avsnitt ingår inte i "A-delen" av kursen

Vi låter i fortsättningen ω, ζ, η beteckna de naturliga talen $\mathbb{N}$, heltalen $\mathbb{Z}$ och de rationella talen $\mathbb{Q}$ betraktade som **linjärt ordnade mängder** med den vanliga ordningsrelationen $<$.

Exempel
ω och ζ är inte isomorfa, ty t.ex. är $\exists x \forall y\,(x \neq y \rightarrow x < y)$ sann i ω och falsk i ζ. Sentensen säger ju att det finns ett minsta element, vilket det gör i ω (nämligen 0) men inte i ζ.

Låt A vara den linjärt ordnade mängden $\{x \mid x \in \mathbb{Q},\ x \geq 0\}$. Då har A ett minsta element (0), men ω och A är inte isomorfa, ty för ω gäller att varje delmängd har ett minsta element, men det har inte t.ex. delmängden $\{x \mid x \in \mathbb{Q},\ x > 0\}$ till A.

Den senare egenskapen har visat sig vara så viktig att man har gett den ett eget namn, **välordning**. Vi kommer att använda den då vi skall tala om mängdlära senare i kursen.

Definition:
En linjärt ordnad mängd X säges vara **välordnad** (eng. well-ordered) om varje icke-tom delmängd till X innehåller ett minimalt element.

Definitionen säger alltså att för alla delmängder A till X gäller

$$\exists x\, x \in A \rightarrow \exists x\,(x \in A\ \&\ \forall y\,(y < x \rightarrow y \notin A)).$$

Vi skall se i avsnittet om kompakthetssatsen att det inte går att uttrycka detta villkor helt som en sentens i första ordningens predikatlogik, uttrycket "för alla delmängder A" kräver ett "starkare språk".

Anmärkning: Med en **"välgrundad"** (eng. well-founded) (partiell) ordning, menar vi en (partiell) ordning sådan att varje icke-tom delmängd till den ordnade mängden har ett minimalt element.
En välordning är alltså detsamma som en välgrundad linjär ordning.
I en välordnad mängd har varje icke-tom delmängd ett unikt *minsta* element, dvs ett som är mindre än alla andra i delmängden. I en linjärt ordnad mängd är ju ett minimalt element detsamma som ett minsta element (enligt ax <3).

ω är välordnad, men det är varken ζ eller η.

Varje **ändlig** linjärt ordnad mängd är välordnad (visas t.ex. med induktion över antalet element).
I själva verket är varje delmängd till en välordnad mängd välordnad. Om $Y \subseteq X$, X välordnad, är ju en icke-tom delmängd till Y också en icke-tom delmängd till X och har alltså ett minimalt element.

Om X är en linjärt ordnad mängd och $a \in X$ kallas mängden $X_a = \{x \in X \mid x < a\}$ ett (inledande) **segment** av X. Om X är välordnad är X_a enligt ovan också välordnad.

Om X är en **oändlig** välordnad mängd, kan vi definiera en funktion $\varphi : \omega \to X$ enligt $\varphi(0) = X$:s minsta element, $\varphi(1) =$ det minsta elementet i $X \setminus \{\varphi(0)\}$, $\varphi(2) =$ det minsta elementet i $X \setminus \{\varphi(0), \varphi(1)\}$ etc. Eftersom X är oändlig "tar det inte slut", vi får en funktion definierad på hela ω.
Om varje element i X är $\varphi(n)$ för något $n \in \omega$, ger φ en isomorfi mellan ω och X. Annars finns det ett minsta element $u \in X$ (välordning!) som inte är $\varphi(n)$ för något n. Då ger φ en isomorfi mellan ω och segmentet X_u. I båda fallen är alltså ω isomorf med "början" av X, antingen hela X eller ett segment av den.
Om ω är isomorf med ett segment av X och resten av X också är oändlig, kan man på samma sätt se att X "innehåller" två kopior av ω som inledning etc. Detta leder oss också till en oändlig välordnad mängd som inte är isomorf med ω. Låt ω' vara $\omega \cup \{\odot\}$ med $<$ definierad som vanligt på ω och med $n < \odot$ för alla $n \in \omega$. ω' är då välordnad, ty om A är en icke-tom delmängd till ω' och $A \neq \{\odot\}$ är det minsta elementet i $\omega \cap A$ också det minimala elementet i A och om $A = \{\odot\}$ är $\odot$ minimalt i A. ω' är inte isomorf med ω, ty ω' har ett **största** element ($\odot$), men det har inte ω.

Ett viktigt skäl till intresset för välordnade (och välgrundat partiellt ordnade) mängder är att **induktion** och **rekursion** fungerar på dem:

Sats: (Induktion på en välordnad mängd)
Låt X vara en välordnad mängd och P en egenskap på X.
Om det för alla $a \in X$ gäller $\forall x\,(x < a \to Px) \to Pa$,
så gäller Px för alla $x \in X$.

Bevis: Enligt förutsättningen kan $\{x \in X \mid \sim Px\}$, mängden $x \in X$ så att Px inte gäller, inte ha ett minimalt element. Om a vore ett sådant skulle ju Px gälla för alla x som är mindre än a, dvs $\forall x\,(x < a \to Px)$ skulle gälla, så enligt förutsättningen Pa, motsägelse. Den betraktade mängden är alltså tom (X är ju välordnad) och P gäller för alla $x \in X$. □

Anmärkning: Av beviset framgår att induktion fungerar på varje välgrundat (partiellt) ordnad mängd.

Observera att vi inte behöver någon särskild "bas" för induktionen, om z är det minsta elementet i X (ett minimalt element om X bara är partiellt ordnad) är $x < z$ falsk för alla $x \in X$, så $\forall x\,(x < z \to Px)$ sann. Således följer Pz ur förutsättningen.
Vi **kan** heller inte för en godtycklig välordnad mängd formulera villkoret som vi brukar för induktion över de naturliga talen. Visserligen finns det för alla element $x \in X$ utom det sista (om det finns ett sista) en efterföljare $S(x)$ (det **minsta** elementet som är större än x), men eftersom inte alla element behöver vara efterföljare till något räcker det **inte** att förutsätta Pz och $\forall x\,(Px \to PS(x))$, för att få $\forall x\,Px$. I ω' ovan t.ex. kan vi inte dra slutsatsen $P\odot$.

Antagandet om välordning är viktigt. Om $X = \{x \in \eta \mid x \geq 0\}$ är X inte välordnad och t.ex. $Px : x \leq 1$ uppfyller villkoret, men inte slutsatsen, i satsen (tänk efter!).

För naturliga tal är vi vana vid att definiera funktioner rekursivt.
Om vi har någon regel (en funktion) som bestämmer $f(n)$ så snart vi vet alla tidigare värden för f (speciellt vet vi $f(0)$), så bestäms f entydigt för alla $n \in \mathbb{N}$.
Motsvarande visar sig gälla för alla välordnade mängder:

Sats: (Rekursion på en välordnad mängd)
Låt X vara en välordnad mängd och Y en mängd.
Givet en funktion g som till ett element $c \in X$ och en funktion definierad på segmentet X_c ordnar ett element i Y, finns en unik funktion $f : X \to Y$ som uppfyller

$$(*) \qquad f(c) = g(c, f\,|_{X_c}), \quad \text{för alla } c \in X.$$

Här betecknar $f\,|_{X_c}$ **restriktionen** av f till segmentet X_c, dvs den funktion på X_c som för $x \in X_c$ tar värdet $f(x)$.

Bevis: Låt för $a \in X$ (tillfälligt) ${}_aX = X_a \cup \{a\} = \{x \in X \mid x \leq a\}$ och Pa betyda "det finns en funktion $f_a : {}_aX \to Y$ som uppfyller $(*)$ för $c \in {}_aX$".
(Detta är meningsfullt eftersom $c \in {}_aX$ (dvs $c \leq a$) medför $X_c \subset {}_aX$.)
Beviset sker sedan i fyra steg:
i) Entydigheten:
Låt $f_1, f_2 : X \to Y$ båda uppfylla $(*)$ för alla $c \in X$.
Om $f_1\,|_{X_c} = f_2\,|_{X_c}$ fås $f_1(c) = g(c, f_1\,|_{X_c}) = g(c, f_2\,|_{X_c}) = f_2(c)$.
Med induktion över X fås att $f_1(x) = f_2(x)$ för alla $x \in X$.
ii) Om Pa och $b \leq a$, så Pb och $f_b = f_a\,|_{{}_bX}$:
$f_a\,|_{{}_bX}$ uppfyller $(*)$ på ${}_bX$, så Pb, och enligt *i)* (på den välordnade mängden ${}_bX$) är lösningen entydig, så $f_b = f_a\,|_{{}_bX}$.
iii) Funktionen $f(x) = f_x(x)$, definierad för alla x med Px, uppfyller $(*)$:
Om Pa och $b \leq a$ så (gäller Pb och) är $f(b) = f_b(b) = f_a\,|_{{}_bX}(b) = f_a(b)$, så $f\,|_{{}_aX} = f_a$ och $(*)$ är uppfylld enligt definitionen av f_a.
iv) Px gäller för alla $x \in X$:
Antag att Px gäller för alla $x \in X_a$ och definiera $f_a(x) = f_x(x)$ för $x \in X_a$ och $f_a(a) = g(a, f_a\,|_{X_a})$. Då är f_a definierad på ${}_aX$ och uppfyller $(*)$, enligt *iii)* (på X_a) och definitionen (för a), så Pa.
Med induktion över X fås att Px gäller för alla $x \in X$.
Påståendet i satsen följer. □

Med samma bevis ses att rekursion fungerar på varje välgrundat ordnad mängd.

Övningar

Vo1) Visa att en linjärt ordnad mängd X är välordnad om och endast om varje strikt avtagande följd av element i X är ändlig.
Vo2) En linjär ordning $<$ på en mängd X kallas **tät** om det för två godtyckliga olika element i X finns ett element strikt mellan dem, dvs $\forall x\,\forall y\,(x < y \to \exists z\,(x < z \;\&\; z < y))$. Visa att en tät ordning på en mängd med minst två element inte kan vara en välordning.
Vo3) Visa att om X, Y är välordnade är $X + Y$ (definierat i övning <5) också välordnad.
Vo4) Visa att om X, Y är välordnade är $X \times Y$ (definierat i övning <6) också välordnad.

Svar och anvisningar till övningarna

Ö <1. a) Ax <1 ok, inget tal är större än sig själv. Ax <2 ok, om a är större än b och b är större än c är a större än c. Ax <3 ok, för alla tal a och b gäller antingen att de är lika eller att ett av dem är större än det andra.
b) Ax <1 ok, ty $\langle \xi, \xi \rangle \notin \mathrm{Ext}(<)$ för $\xi = \alpha, \beta, \gamma$ i denna tolkning. Ax <3 ok, för varje par av olika element i D gäller olikhet åt ett håll. Men ax <2 är **inte** satisfierat i denna tolkning: $a < b$ och $b < c$, men inte $a < c$.
c) Ax <1 ok enligt tolkningen av <. Ax <2 ok, om a är en delare till b som är en delare till c, är a också en delare till c. Men ax <3 är **inte** satisfierat i denna tolkning: 2 och 3 är olika element i D, men ingen av dem är en delare till den andra.
Ö <2. Tolkningen $D = \{\alpha\}$, $\mathrm{Ext}(<) = \{\langle \alpha, \alpha \rangle\}$ satisfierar ax <2 och ax <3, men inte ax <1, så ax <1 är oberoende av de övriga.
Tolkningarna i ö <1 b) och c) visar att ax <2 respektive ax <3 är oberoende av de andra två.
Ö <3. Antag att $a < b$ och $b < a$. Då vore enligt ax <2 också $a < a$, vilket motsäger ax <1. Således gäller $a < b \rightarrow \sim b < a$.
Ö <4. Sentensen $p : \exists x \, \forall y \, (y = x \vee x < y)$, dvs "det finns ett minsta element i tolkningen", är sann i tolkningen $D = \mathbb{N}$, $<$ tolkas som "mindre än" och falsk i tolkningen $D = \mathbb{Z}$, $<$ tolkas som "mindre än". Således är varken $\sim p$ eller p en logisk följd av axiomen och kan då inte heller härledas från dem. Axiomen är alltså inte fullständiga.
Ö <5. Ax <1 ok, ty $a < a$ strider mot ax <1 i antingen $\mathfrak{A}$ (om $a \in A$) eller i $\mathfrak{B}$ (om $a \in B$). Ax <2 ok, ty antag att $a < b$ och $b < c$. Om då $a \in B$ fås $b, c \in B$ och $a < c$ följer från ax <2 för $\mathfrak{B}$ och pss om $c \in A$ fås $a, b \in A$ och $a < c$ från ax <2 för $\mathfrak{A}$. I det återstående fallet $a \in A$, $c \in B$ gäller också $a < c$ enligt definitionen av $<$ i $\mathfrak{A} + \mathfrak{B}$. Ax <3 ok, ty om $a, b \in A$ eller $a, b \in B$ fås det ur ax <3 i $\mathfrak{A}$ respektive $\mathfrak{B}$ och annars gäller $a < b$ eller $b < a$.
Ö <6. Ax <1 ok, ty om $\langle a, b \rangle < \langle a, b \rangle$ måste $b <_b b$ eller (eftersom $b = b$) $a <_a a$, båda omöjliga enligt ax <1 i $\mathfrak{B}$ och $\mathfrak{A}$. Ax <2 ok, ty om $\langle a_1, b_1 \rangle < \langle a_2, b_2 \rangle$ och $\langle a_2, b_2 \rangle < \langle a_3, b_3 \rangle$ gäller antingen $b_1 = b_2$ eller $b_1 < b_2$ och antingen $b_2 = b_3$ eller $b_2 < b_3$; om $b_1 = b_2 = b_3$ måste $a_1 < a_2$ och $a_2 < a_3$, så $a_1 < a_3$ enligt ax <2 för $\mathfrak{A}$, annars (dvs om $b_1 < b_2$ eller $b_2 < b_3$) fås $b_1 < b_3$ enligt ax <2 för $\mathfrak{B}$ eller "=E" — i båda fallen gäller $\langle a_1, b_1 \rangle < \langle a_3, b_3 \rangle$. Ax <3 ok, ty betrakta $\langle a_1, b_1 \rangle$ och $\langle a_2, b_2 \rangle$. Om $b_1 <_b b_2$ gäller $\langle a_1, b_1 \rangle < \langle a_2, b_2 \rangle$ och om $b_2 <_b b_1$ gäller $\langle a_2, b_2 \rangle < \langle a_1, b_1 \rangle$. Enligt ax <3 i $\mathfrak{B}$ måste annars $b_1 = b_2$ och om då $a_1 <_a a_2$ gäller $\langle a_1, b_1 \rangle < \langle a_2, b_2 \rangle$ och om $a_2 <_a a_1$ gäller $\langle a_2, b_2 \rangle < \langle a_1, b_1 \rangle$ — enda återstående fallet är enligt ax<3 i $\mathfrak{A}$ att $a_1 = a_2$ så $\langle a_1, b_1 \rangle = \langle a_2, b_2 \rangle$

Ö G1. a) Det givna ger verkligen en tolkning, ty $1 \in D$, produkten av två tal i D ligger i D, liksom det inverterade värdet till ett tal i D. Ax G1 ok, ty multiplikation av komplexa tal är associativ. Ax G2 ok, 1 gånger $a = a$ gånger $1 = a$ för alla komplexa tal. Ax G3 ok på samma sätt.
b) Den givna tolkningen satisfierar ax G1 och ax G2, men man kan inte finna en tolkning av $^{-1}$ så att ax G3 är uppfyllt, för $2 \in \mathbb{Z}$ finns t.ex. inget $n \in \mathbb{Z}$ så att $2 \cdot n = 1$.
c) Tydligen måste det gälla $\mathrm{Ref}(e) = 1$, $e * e = e$ och $e^{-1} = e$. Det är lätt att se att ax G1, G2 och G3 satisfieras av tolkningen.
Ö G2. För godtyckliga a och b gäller $a*(a^{-1}*b) \overset{\text{ax G1}}{=} (a*a^{-1})*b \overset{\text{ax G3}}{=} e*b \overset{\text{ax G2}}{=} b$. Detta visar att den givna sentensen följer ur gruppaxiomen (för givna x, y ges z av $x^{-1} * y$).
Ö G3. För tolkningen i ö G1b är ax G1 och ax G2 satisfierade. Om vi definierar $^{-1}$ på något sätt, t.ex. som funktionen som tar det konstanta värdet 1, får vi en modell för ax G1 och ax G2 som inte satisfierar ax G3. Det kan således inte härledas från de andra axiomen, det är oberoende av dem.
Ö G4. Sentensen $p : \forall x \forall y\, x * y = y * x$ (som säger att $*$ är kommutativ) är satisfierad i tolkningen i ö G1a, men dess negation satisfieras av tolkningen i det andra exemplet på grupper (kvadratiska matriser). Då kan varken p eller $\sim p$ härledas från axiomen, så teorin är inte fullständig.

Ö Iso1. En isomorfi ges av $\varphi(\pm 1) = \pm \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\varphi(\pm i) = \pm \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, ty φ är en bijektion $D_1 \to D_2$ (varje element i D_2 är bild av exakt ett element i D_1) och villkoren för en isomorfi är uppfyllda; (1) ok, ty det finns inga relationer här. (3) ok, ty $\varphi(e^{\mathfrak{I}_1}) = \varphi(1) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = e^{\mathfrak{I}_2}$. Att (2) är uppfyllt, dvs att $\varphi(a^{-1}) = \varphi(a)^{-1}$ och $\varphi(a *_1 b) = \varphi(a) *_2 \varphi(b)$ för alla $a, b \in D_1$, ses av att multiplikation med elementen i D_1 svarar mot rotation av det komplexa talplanet $\mathbb{C}$ och multiplikation med motsvarande element i D_2 svarar mot samma rotation av planet beskrivet som $\mathbb{R}^2$. Man kan också direkt konstatera att både $\mathfrak{I}_1$ och $\mathfrak{I}_2$ är isomorfa med $\mathfrak{I}_3$, gruppen av rotationer vinklarna $0, \frac{\pi}{2}, \pi, -\frac{\pi}{2}$ av planet kring ett origo. $\mathfrak{I}_1 \cong \mathfrak{I}_3$ och $\mathfrak{I}_2 \cong \mathfrak{I}_3$ ger $\mathfrak{I}_1 \cong \mathfrak{I}_2$, ty $\cong$ är en ekvivalensrelation.
Ö Iso2. Med $\mathfrak{A} = \omega$ och $B = \{\odot\}$, $<_b$ tom, är $\mathfrak{A}+\mathfrak{B}$ och $\mathfrak{B}+\mathfrak{A}$ inte isomorfa, ty $\mathfrak{A} + \mathfrak{B}$ har ett sista element ($\odot$), men det har inte $\mathfrak{B} + \mathfrak{A}$ (som är isomorf med ω). Sentensen $\exists x \forall y\, (x = y \vee y < x)$ är alltså sann i $\mathfrak{A} + \mathfrak{B}$ men falsk i $\mathfrak{B} + \mathfrak{A}$.
Om A och B är ändliga är både $\mathfrak{A} + \mathfrak{B}$ och $\mathfrak{B} + \mathfrak{A}$ isomorfa med den unika (på isomorfi när) linjärt ordnade mängden med $|A| + |B|$ element.
Ö Iso3. Med $\mathfrak{A} = \omega$ och $\mathfrak{B} = (\{0, 1\}, <)$ är $\mathfrak{A} \times \mathfrak{B}$ och $\mathfrak{B} \times \mathfrak{A}$ inte isomorfa, ty $\mathfrak{A} \times \mathfrak{B}$ består av två "kopior" av ω efter varandra ($\langle 0,0\rangle < \langle 1,0\rangle < \langle 2,0\rangle < \cdots < \langle 0,1\rangle < \langle 1,1\rangle < \langle 2,1\rangle < \dots$), medan $\mathfrak{B} \times \mathfrak{A}$ består av ett oändligt antal kopior av $\{0, 1\}$ efter varandra ($\langle 0,0\rangle < \langle 1,0\rangle < \langle 0,1\rangle < \langle 1,1\rangle < \langle 0,2\rangle < \langle 1,2\rangle < \langle 0,3\rangle < \dots$, den är isomorf med ω).
Sentensen $\exists x\, (\exists y\, y < x \,\&\, \forall y\, (y < x \to \exists z\, (y < z \,\&\, z < x)))$, som säger att det finns ett element som inte är det minsta och som saknar närmaste föregångare, är alltså sann i $\mathfrak{A} \times \mathfrak{B}$ och falsk i $\mathfrak{B} \times \mathfrak{A}$.

Ö P1. Vi skall visa: $1+1=2$, dvs $S(0)+S(0)=S(S(0))$

1	(1)	$\forall x \forall y\, x+S(y)=S(x+y)$	P4 = Q4	
1	(2)	$\forall y\, S(0)+S(y)=S(S(0)+y)$	1	$\forall$E
1	(3)	$S(0)+S(0)=S(S(0)+0)$	2	$\forall$E
4	(4)	$\forall x\, x+0=x$	P3 = Q3	
4	(5)	$S(0)+0=S(0)$	4	$\forall$E
1,4	(6)	$S(0)+S(0)=S(S(0))$	3,5	=E

Eftersom sentensen på rad 6 bara beror av premisserna (dvs axiomen P3 och P4) på raderna 4 och 1 är beviset klart.

Ö P2. Övningar med induktion:

a) Låt ϕx vara $0+x=x$.
Då gäller $\phi 0 : 0+0=0$ enligt ax P3.
Antag ϕa.
Då får man $0+S(a) \overset{\text{ax P4}}{=} S(0+a) \overset{\phi a}{=} S(a)$, dvs $\phi S(a)$. Eftersom a var godtyckligt gäller $\forall x\,(\phi x \rightarrow \phi S(x))$.
Ax P7 ger $\forall x\, \phi x$, dvs det sökta resultatet.

b) Låt ϕx vara $\forall y\, y+S(x)=S(y)+x$.
Eftersom $b+S(0) \overset{\text{ax P4}}{=} S(b+0) \overset{\text{ax P3}}{=} S(b) \overset{\text{ax P3}}{=} S(b)+0$, gäller $\phi 0$.
Antag ϕa.
Då får man $b+S(S(a)) \overset{\text{ax P4}}{=} S(b+S(a)) \overset{\phi a}{=} S(S(b)+a) \overset{\text{ax P4}}{=} S(b)+S(a)$, dvs (med $\forall$I) $\phi S(a)$.
Ax P7 ger $\forall x\, \phi x$.

c) Låt ϕx vara $\forall y\, x+y=y+x$.
$\phi 0 : \forall y\, 0+y=y+0$ följer från a) ovan och ax P3.
Antag ϕa.
Man finner att $S(a)+b \overset{\text{b) ovan}}{=} a+S(b) \overset{\text{ax P4}}{=} S(a+b) \overset{\phi a}{=} S(b+a) \overset{\text{ax P4}}{=} b+S(a)$, dvs (med $\forall$I) $\phi S(a)$.
Som i a) följer $\forall x\, \phi x$.

d) Låt ϕx vara $x \neq 0 \rightarrow \exists y\, x=S(y)$.
$\phi 0$ gäller då trivialt.
För alla a gäller $\exists y\, S(a)=S(y)$, så (SI(PMI)) $\phi S(a)$ gäller (utan induktionsantagande!).
Som förut får vi $\forall x\, \phi x$.

e) Låt ϕx vara $S(0)*x=x$.
Då gäller $\phi 0 : S(0)*0=0$ enligt ax P5.
Antag ϕa.
Då får man $S(0)*S(a) \overset{\text{ax P6}}{=} (S(0)*a)+S(0) \overset{\phi a}{=} a+S(0) \overset{\text{ax P4}}{=} S(a+0) \overset{\text{ax P3}}{=} S(a)$, dvs $\phi S(a)$. Eftersom a var godtyckligt gäller $\forall x\,(\phi x \rightarrow \phi S(x))$.
Ax P7 ger $\forall x\, \phi x$, saken är klar.

Ö Q1) Först gäller det att visa att tolkningen som beskrivs i ledningen är en modell för Q-axiomen.
Axiomen Q1, Q2, Q3, Q5 och Q7 ses enkelt vara satisfierade i tolkningen.
Ax Q4: vi skall verifiera $c+S(d)=S(c+d)$ för alla $c,d \in D$. Om $c,d \in \mathbb{N}$ gäller det förstås. Om d är α eller β är $c+S(d)=c+d=S(c+d)$, eftersom $c+d$ också är α eller β. Om c är α eller β och d är ett naturligt tal är $c+S(d)=c=S(c)=S(c+d)$, allt enligt tabellerna för S och addition i tolkningen. Därmed är alla fall täckta, så ax Q4 satisfieras av tolkningen.
Ax Q6: nu gäller det att visa $c*S(d)=(c*d)+c$ för alla $c,d \in D$. Om $c,d \in \mathbb{N}$ gäller det förstås. Om c är α eller β är $c*S(d)$ och $(c*d)+c$ båda

β respektive α (den som c inte är). Om slutligen c är ett naturligt tal och d är α eller β, är $c * S(d) = c * d = (c * d) + c$. Ax Q6 satisfieras alltså av den givna tolkningen.
Om man visar att de givna sentenserna inte satisfieras är saken klar.
a) $\forall x\, x \neq S(x)$ är falsk, ty $\alpha = S(\alpha)$.
b) $\forall x \forall y\, x + y = y + x$ är falsk, ty $\alpha + \beta = \alpha, \quad \beta + \alpha = \beta$.
c) $\forall x \forall y \forall z\, x + (y + z) = (x + y) + z$ är falsk, ty

$$(\alpha + \alpha) + \beta = \beta + \beta = \alpha, \quad \alpha + (\alpha + \beta) = \alpha + \alpha = \beta.$$

d) $\forall x\, 0 + x = x$ är falsk, ty $0 + \alpha = \beta$.
e) $\forall x\, 0 * x = 0$ är falsk, ty $0 * \alpha = \alpha$.
f) $\forall x \forall y \forall z\, x * (y + z) = (x * y) + (x * z)$ är falsk, ty

$$\alpha * (\alpha + \beta) = \alpha * \alpha = \beta, \quad \alpha * \alpha + \alpha * \beta = \beta + \beta = \alpha.$$

Vo1) Låt X vara en linjärt ordnad mängd.
Om X är välordnad och $\cdots < a_{n+1} < a_n < \cdots < a_2 < a_1 < a_0$ en strikt avtagande följd i X, betrakta den icke-tomma delmängden $A = \{a_0, a_1, \dots\}$ till X. A har ett minimalt element, a_k säg. Men då kan inte följden fortsätta efter a_k ($a_{k+1} < a_k$ är omöjligt eftersom a_k är minimalt), följden är alltså ändlig.
Om å andra sidan X inte är välordnad, finns en icke-tom delmängd B som saknar minimalt element. Tag ett $b_0 \in B$. Eftersom det inte är minimalt i B finns $b_1 \in B$ med $b_1 < b_0$, men b_1 är inte heller minimalt i B, så vi finner $b_2 \in B$ med $b_2 < b_1$ och sedan ständigt mindre $b_3, b_4, \dots$ i en oändlig strikt avtagande följd i X. Om varje strikt avtagande följd är ändlig är alltså X välordnad.
Motsvarande resonemang visar att samma villkor gäller om och endast om en godtycklig ordning (ev. partiell) är välgrundad.
Vo2) Låt $(X, <)$ vara en tät linjärt ordnad mängd med $a_0, b \in X,\ b < a_0$.
Eftersom ordningen är tät finns $a_1 \in X$ med $b < a_1 < a_0$, men då finns $a_2 \in X$ med $b < a_2 < a_1$ etc. Vi får en oändlig strikt avtagande följd. Som i ö Vo1 saknar delmängden $\{a_0, a_1, a_2, \dots\}$ till X ett minimalt element, så X är inte välordnad.
Vo3) Att $X + Y$ är linjärt ordnad visades i ö <5. För att visa välordningsegenskapen, låt A vara en icke-tom delmängd till $X \cup Y$ (vi kan anta att X och Y är disjunkta). Om A innehåller något element i X finns det ett minimalt sådant (ty X är välordnad), det är också minimalt i A. Om A inte innehåller något element i X, måste den innehålla ett element i Y och, eftersom Y är välordnad, ett minimalt sådant. Det är då minimalt i A. I båda de möjliga fallen har A alltså ett minimalt element, så $X + Y$ är välordnad.
Vo4) Att $X \times Y$ är linjärt ordnad visades i ö <6. För att visa välordningsegenskapen, låt A vara en icke-tom delmängd till $X \times Y$. Mängden $B = \{b \in Y \mid \text{det finns } x \in X \text{ så att } \langle x, b\rangle \in A\}$ är då en icke-tom delmängd till Y, kalla ett minimalt element i den (finns eftersom Y är välordnad) b_0. Mängden $C = \{a \in X \mid \langle a, b_0\rangle \in A\}$ är då en icke-tom delmängd till X, kalla ett minimalt element (X välordnad) a_0. Då är $\langle a_0, b_0\rangle \in A$ ett minimalt element i A, $X \times Y$ är alltså välordnad.