ÖVNING 6

ÖVNINGENS SYFTE

- ATT UTFORSKA STRUKTUREN HOS TALSYSTEMEN UNDER ADDITION RESP. MULTIPLIKATION SAMT SAMBANDET MELLAN DEN ADDITIVA OCH MULTIPLIKATIVA STRUKTUREN.
- ATT INTRODUCERA GRUPPER, RINGAR, KROPPAR

A1 SKRIV UPP ALLA FORMLER OCH EGENSKAPER DU/NI KÄNNER TILL SOM HANDLAR OM ADDITION, SUBTRAKTION, MULTIPLIKATION OCH DIVISION. (TILLSAMMANS BÖR NI KOMMA PÅ MÅNGA!)

EX. $a+0=a$, $-(-a)=a$, $a(b+c)=ab+ac$, ...

DÄR a,b,c BETECKNAR TAL UR NÅGON TALMÄNGD.

VILKA TALMÄNGDER KÄNNER DU TILL? VAD SKILJER DESSA TALMÄNGDER? VAD ÄR ETT TAL? VAD ÄR ADDITION, SUBTRAKTION, MULTIPLIKATION OCH DIVISION?

A2 DESSA FORMLER ÄR INTE OBEROENDE AV VARANDRA. HÄRLED SÅ MÅNGA DU KAN UR DE ÖVRIGA! TILL SLUT ÅTERSTÅR NÅGRA SOM DU INTE KAN REDUCERA BORT, VILKA ÄR DET?

RÅD: BETRAKTA FORMLER MED + OCH − FÖR SIG FÖRST, OCH DÄREFTER FORMLER MED MULTIPLIKATION OCH DIVISION

DEN ADDITIVA STRUKTUREN

ANTAG ATT VI HAR KVAR FÖLJANDE FORMLER FÖR EN TALMÄNGD M:

(1) $a+b=b+a \quad \forall a,b\in M$

(2) $(a+b)+c=a+(b+c) \quad \forall a,b,c\in M$

(3) $\exists\, 0\in M : \forall a\in M : \; a+0=a$

(4) $\forall a\in M\ \exists -a\in M : \; a+(-a)=0$

UR DESSA FORMLER KAN VI VISA T.EX.

(5) $0+a=a \quad \forall a\in M$

(6) $(-a)+a=0 \quad \forall a\in M$

(7) $a+x=a+y \Rightarrow x=y$

(8) $-(-a)=a$

(9) EKVATIONERNA $a+x=b$ OCH $x+a=b$ ÄR ENTYDIGT LÖSBARA FÖR ALLA a OCH b SOM LIGGER I M.

(10) $-(a+b)=(-a)+(-b) \quad \forall a,b\in M$

B1 BEVISA ATT FORMLERNA (5)–(10) FÖLJER UR ENBART FORMLERNA (1)–(4).

DE FORMLER SOM NI NU BEVISAT UTGÖR SATSER I EN TEORI SOM HAR FORMLERNA (1)–(4) SOM AXIOM. TÄNK EFTER VILKA AXIOM SOM NI ANVÄNT.

B2 HUR KAN MAN I DENNA TEORI DEFINIERA SUBTRAKTION $a-b$ DÄR $a,b \in M$?

- VAD ÄR SKILLNADEN MELLAN MINUS-TECKNET I DE TVÅ SAMMANHANGEN

  $-a$ OCH $a-b$?

- DISKUTERA FORMELN

  $$a-b = a+(-b)$$

  ÄR DETTA EN <u>SATS</u> ELLER EN <u>DEFINITION</u> ELLER BEROR DET PÅ NÅGOT ?

MULTIPLIKATIVA STRUKTUREN

ANTAG NU ATT VI HAR FÖLJANDE FORMLER:

(1)′ $a \cdot b = b \cdot a \quad \forall a,b \in M$

(2)′ $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a,b,c \in M$

(3)′ $\exists 1 \in M \; \forall a \in M : \; a \cdot 1 = a$

(4)′ $\forall a \in M \setminus \{0\} \; \exists a^{-1} \in M : \; a \cdot a^{-1} = 1$

C1 VISA FÖLJANDE FORMLER (5)′–(10)′ MED HJÄLP AV <u>ENBART</u> FORMLERNA (1)′–(4)′.

(5)′ $1 \cdot a = a \quad \forall a \in M$

(6)′ $a^{-1} a = 1 \quad \forall a \in M, a \neq 0$

(7)′ $a \neq 0 \wedge a \cdot x = a \cdot y \Rightarrow x = y$

(8)′ $(a^{-1})^{-1} = a \quad \forall a \in M, a \neq 0$

(9)′ EKVATIONERNA $a \cdot x = b$ OCH $x \cdot a = b$ ÄR ENTYDIGT LÖSBARA FÖR ALLA a OCH b DÄR $a \neq 0$.

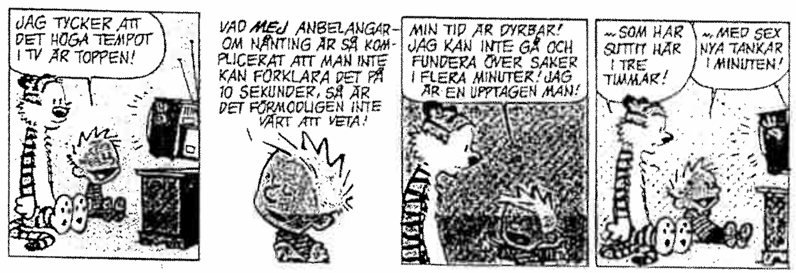
(10)′ $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1} \quad \forall a,b \in M$

C2 HUR KAN MAN DEFINIERA DIVISION a/b DÄR $a,b \in M$ OCH $b \neq 0$? VARFÖR FÅR INTE b VARA 0? JÄMFÖR MED DISKUSSIONEN I B2 OVAN. VILKA LIKHETER OCH SKILLNADER FINNS ?

C3 FÖR VILKA TALMÄNGDER $(\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C})$ GÄLLER FORMLERNA (1)–(4) RESP. (1)′–(4)′ ?

C4 BLAND DE FORMLER SOM VI BETRAKTAT I SAMBAND MED DEN ADDITIVA OCH DEN MULTIPLIKATIVA STRUKTUREN SAKNAS VISSA TYPER AV FORMLER. VILKA ? VAD UTMÄRKER DEM ?

Kalle och Hobbe



© Bill Watterson, Europa Press

GRUPPER, RINGAR, KROPPAR

D1 VI HAR HITTILLS BEGRÄNSAT VÅRT INTRESSE TILL TALMÄNGDER, NÄMLIGEN

$$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}.$$

DISKUTERA VAD SOM HÄNDER OM MAN UTFÖR NÅGON OPERATION, DVS OM a OCH b LIGGER I M, VAR LIGGER $a+b$, $a-b$, $a\cdot b$, a/b ?

DEF: EN MÄNGD M SÄGS VARA SLUTEN UNDER OPERATIONEN $*$ OM FÖLJANDE GÄLLER:

$$a, b \in M \Rightarrow a*b \in M$$

D2 UNDER VILKA OPERATIONER, $+, -, \cdot, /$, ÄR TALMÄNGDERNA $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$, RESP $\mathbb{C}$ SLUTNA?

DEF: EN MÄNGD M (INTE NÖDVÄNDIGTVIS TALMÄNGD) FÖRSEDD MED EN OPERATION $*$ KALLAS EN (ABELSK) GRUPP OM FÖLJANDE GÄLLER

(0) $\forall a,b \in M: a,b \in M \Rightarrow a*b \in M$ (SLUTENHET)

(1) $\forall a,b \in M: a*b = b*a$ (KOMMUTATIVITET)

(2) $\forall a,b,c \in M: (a*b)*c = a*(b*c)$ (ASSOCIATIVITET)

(3) $\exists e \in M: \forall a \in M: a*e = e*a = a$ (NEUTRALT EL.)

(4) $\forall a \in M: \exists a' \in M: a*a' = a'*a = e$ (INVERST ELEMENT)

VI SKRIVER $\langle M, * \rangle$ FÖR ATT BETECKNA MÄNGDEN M FÖRSEDD MED OPERATIONEN $*$.

D3 LÅT M VARA NÅGON AV TALMÄNGDERNA $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. I VILKA FALL ÄR $\langle M, + \rangle$ EN GRUPP? VILKET ELEMENT ÄR NEUTRALT? VAD INNEBÄR INVERST ELEMENT?

D4 BETRAKTA NU RESTKLASSER MODULO 4,

$$\mathbb{Z}_4 = \{[0], [1], [2], [3]\}.$$

LÅT OPERATIONEN $\oplus$ VARA ADDITION MODULO 4

DVS. $[0] \oplus [2] = [2]$

$[2] \oplus [3] = [5] = [1]$

O.S.V.

VI KAN GÖRA EN "ADDITIONSTABELL":

$\oplus$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]*	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

*HÄR STÅR ALLTSÅ $[1] \oplus [2]$

- VISA ATT $\langle \mathbb{Z}_4, \oplus \rangle$ ÄR EN GRUPP. EGENSKAPERNA (1), (3) OCH (4) KAN MAN SE "DIREKT" I TABELLEN. HUR?
- OPERATIONEN $\oplus$ ÄR VÄLDEFINIERAD GENOM TABELLEN OVAN. OM VI ISTÄLLET DEFINIERAR $\oplus$ GENOM $[a] \oplus [b] = [a+b]$, VAD MÅSTE VI DÅ VISA FÖR ATT VETA ATT OPERATIONEN ÄR VÄLDEFINIERAD?

D5 VISA ATT FÖLJANDE SATSER ALLTID ÄR SANNA I EN GRUPP $\langle M, * \rangle$

- $a * x = a * y \Rightarrow x = y \quad \forall a,x,y \in M$
- $(a')' = a \quad \forall a \in M$
- $(a * b)' = a' * b' \quad \forall a,b \in M$
- EKVATIONERNA $a * x = b$ OCH $x * a = b$ ÄR ENTYDIGT LÖSBARA FÖR ALLA $a, b \in M$.

OBS: SKRIV BEVISEN NOGA OCH MARKERA I VARJE STEG VILKET GRUPPAXIOM (0)–(4) SOM ANVÄNDS.

JÄMFÖR DESSA BEVIS MED BEVISEN DU/NI GJORDE I UPPGIFTERNA B1 OCH C1.

D6 VISA ATT I EN GRUPP $\langle M, * \rangle$ FINNS BARA ETT NEUTRALT ELEMENT.
VISA OCKSÅ ATT FÖR VARJE ELEMENT $a \in M$ FINNS BARA ETT INVERST ELEMENT a'.

D7 VISA ATT FÖR TALMÄNGDERNA

$$M_1 = \mathbb{Q} \setminus \{0\}, \quad M_2 = \mathbb{R} \setminus \{0\}, \quad M_3 = \mathbb{C} \setminus \{0\}$$

GÄLLER ATT

$$\langle M_1, \cdot \rangle, \quad \langle M_2, \cdot \rangle, \quad \langle M_3, \cdot \rangle$$

ÄR GRUPPER, DVS. $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$ ÄR GRUPPER UNDER MULTIPLIKATION.
VARFÖR HAR VI TAGIT BORT NOLLAN?
VILKET ELEMENT ÄR NEUTRALT?
VAD INNEBÄR INVERST ELEMENT?

"INVERSA OPERATIONER"

I EN GRUPP $\langle M, * \rangle$ KAN MAN ALLTID DEFINIERA EN S.K. INVERS OPERATION. LÅT OSS GÖRA DET DÅ OPERATIONEN $*$ ÄR ANTINGEN ADDITION $+$ ELLER MULTIPLIKATION.

I ADDITION: LÅT $\langle M, + \rangle$ VARA EN GODTYCKLIG GRUPP DÄR OPERATIONEN KALLAS ADDITION, $+$. DET NEUTRALA ELEMENTET BRUKAR DÅ KALLAS NOLLA OCH BETECKNAS 0. OM $a \in M$ SÅ KALLAS DET INVERSA ELEMENTET a' FÖR MOTSATT ELEMENT OCH SKRIVS $-a$.
DEN INVERSA OPERATIONEN KALLAS SUBTRAKTION, $-$, OCH KAN DEFINIERAS T.EX. GENOM

$$a - b \overset{\text{def}}{=} a + (-b)$$

II MULTIPLIKATION: LÅT NU $\langle M, \cdot \rangle$ VARA EN GODTYCKLIG GRUPP DÄR OPERATIONEN KALLAS MULTIPLIKATION, $\cdot$. DET NEUTRALA ELEMENTET KALLAS DÅ FÖR EN ETTA OCH BETECKNAS 1. DET INVERSA ELEMENTET a' SKRIVS OFTA a^{-1}.
DEN INVERSA OPERATIONEN KALLAS DIVISION, $/$, OCH KAN DEFINIERAS GENOM

$$a/b \overset{\text{def}}{=} a \cdot b^{-1}$$

VI HAR HITTILLS STUDERAT ADDITIVA OCH MULTIPLIKATIVA STRUKTURER VAR FÖR SIG. FÖR ATT T.EX. FÅ VÅRT VANLIGA TALSYSTEM MÅSTE VI KOPPLA IHOP DE BÅDA STRUKTURERNA. DETTA SKER MED HJÄLP AV <u>DEN DISTRIBUTIVA LAGEN</u>. VI FÅR DÅ NEDANSTÅENDE UPPSÄTTNING AV FORMLER UR VILKA VI KAN HÄRLEDA ALLA FORMLER MED +, − OCH ·. DESSA FORMLER KALLAS <u>RINGAXIOMEN</u> OCH DEN STRUKTUR SOM UPPFYLLER DESSA KALLAS EN <u>RING</u>.
OM VI ÄVEN VILL HA MED DIVISION KRÄVS YTTERLIGARE ETT AXIOM; VI FÅR DÅ EN <u>KROPP</u>.

DEF $\langle M, +, \cdot \rangle$ KALLAS EN RING OM FÖLJANDE ÄR UPPFYLLT:

I <u>AXIOM OM ADDITION</u>

(0) $\forall a,b \in M: \quad a,b \in M \Rightarrow a+b \in M$
(1) $\forall a,b \in M: \quad a+b = b+a$
(2) $\forall a,b,c \in M: \quad (a+b)+c = a+(b+c)$
(3) $\exists\, 0 \in M\ \forall a \in M: \quad a+0 = \mathbf{0+a=a}$
(4) $\forall a \in M\ \exists -a \in M: \quad a+(-a) = \mathbf{(-a)+a=0}$

II <u>AXIOM OM MULTIPLIKATION</u>

(0) $\forall a,b \in M: \quad a,b \in M \Rightarrow a\cdot b \in M$
(1) $\forall a,b \in M: \quad a\cdot b = b\cdot a$
(2) $\forall a,b,c \in M: \quad (a\cdot b)\cdot c = a\cdot(b\cdot c)$
(3) $\exists\, 1 \in M\ \forall a \in M: \quad a\cdot 1 = \mathbf{1\cdot a = a}$

III <u>ADDITION OCH MULTIPLIKATION; DISTRIBUTIVA LAGEN</u>

$$\forall a,b,c \in M: \quad a\cdot(b+c) = (a\cdot b)+(a\cdot c)$$

E1 KOLLA VILKA AV DE VANLIGA TALMÄNGDERNA $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ SOM ÄR RINGAR.

E2 VISA ATT $\langle \mathbb{Z}_4, \oplus, \odot \rangle$ ÄR EN RING OM $\odot$ ÄR MULTIPLIKATION MODULO 4, DVS.

$$[a]\odot[b] \overset{df}{=} [ab].$$

FÖRST: KONTROLLERA ATT $\odot$ ÄR VÄLDEFINIERAD, DVS. ATT $[ab]=[a'b']$ OM $[a]=[a']$ OCH $[b]=[b']$. GÖR GÄRNA EN MULTIPLIKATIONSTABELL!

E3 VISA ATT I EN RING $\langle M, +, \cdot \rangle$ GÄLLER FÖLJANDE

(i) $a\cdot 0 = 0 \quad \forall a \in M$
(ii) $(-1)\cdot(-1) = 1$
(iii) $-(-a) = a \quad \forall a \in M$
(iv) $(-a)\cdot b = -(a\cdot b) \quad \forall a,b \in M$
(v) $(-a)(-b) = a\cdot b \quad \forall a,b \in M$

<u>OBS</u>: MARKERA I VARJE STEG VILKET AXIOM SOM ANVÄNDS NÄR DU BEVISAR LIKHETERNA (i) − (v).

E4 VISA ATT I EN RING $\langle M, +, \cdot \rangle$ MED MINST TVÅ ELEMENT SÅ ÄR $0 \neq 1$.

SOM SAGT, FÖR ATT KUNNA DIVIDERA OCKSÅ BEHÖVS YTTERLIGARE ETT AXIOM; VI HAR FÖLJANDE DEFINITION.

DEF $\langle M,+,\cdot\rangle$ ÄR EN <u>KROPP</u> OM

(1) $\langle M,+,\cdot\rangle$ ÄR EN RING OCH

(2) $\forall a \in M\setminus\{0\}\ \exists a^{-1} : a\cdot a^{-1} = a^{-1}a = 1$

F1 VILKA AV TALMÄNGDERNA $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ ÄR KROPPAR ?

F2 VISA ATT $\langle M\setminus\{0\}, \cdot\rangle$ ÄR EN GRUPP OM $\langle M,+,\cdot\rangle$ ÄR EN KROPP.

F3 ANTAG NU ATT $\langle M,+,\cdot\rangle$ ÄR EN GODTYCKLIG KROPP. DÅ KAN VI DEFINIERA DE INVERSA OPERATIONERNA :

$$a-b \overset{\text{def}}{=} a+(-b) \qquad \forall\, a,b\in M$$

$$\left(\tfrac{a}{b} =\right) a/b \overset{\text{def}}{=} a\cdot b^{-1} \qquad \forall\, a,b\in M,\ b\neq 0$$

VISA ATT FÖLJANDE GÄLLER :

(1) $(a-b)+(c-d) = (a+c)-(b+d)$

(2) $\frac{a}{b}\cdot\frac{c}{d} = \frac{a\cdot c}{b\cdot d}$, $b\neq 0, d\neq 0$

(3) $(a-b)-(c-d) = (a+d)-(b+c)$

(4) $\frac{a/b}{c/d} = \frac{a\cdot d}{b\cdot c}$, $b\neq 0, c\neq 0, d\neq 0$

(5) $\frac{a}{b}+\frac{c}{d} = \frac{a\cdot d + b\cdot c}{b\cdot d}$

P.S. GLÖM INTE ATT I VARJE LED MARKERA VILKET AV KROPPSAXIOMEN SOM ANVÄNDS !

F4 JÄMFÖR FORMEL (1) OCH (2) SAMT FORMEL (3) OCH (4) I FÖREGÅENDE UPPGIFT. VAD SER NI DÅ ?

TILL SIST, I MÅN AV TID :

G1 VISA ATT $\langle \mathbb{Z}_4, \oplus, \odot\rangle$ INTE ÄR EN KROPP.

DETTA KAN DU SE I MULTIPLIKATIONSTABELLEN FÖR $\langle \mathbb{Z}_4, \odot\rangle$ OM DU GJORDE EN SÅDAN I UPPGIFT E2. HUR ?

G2 VISA ATT $\langle \mathbb{Z}_3, \oplus, \odot\rangle$ ÄR EN KROPP.

G3 VISA ATT $\langle \mathbb{Z}_n, \oplus, \odot\rangle$ ÄR EN RING FÖR ALLA $n = 2, 3, 4, \ldots$ VILKA ÄR KROPPAR ?