Elementär gruppteori, v.36

Elementär gruppteori, 5 sp, 272010.0

Kurstider: v. 36 – v. 42 (3.9 – 18.10)

- Föreläsningar : Må och Ti 10.15 - 12 i föreläsningssal Lindelöf.
- Demonstrationer: To 13.30 - 15 i Lindelöf, börjande vecka 37. Frivillig ikryssning av räknade hemtal. Bonuspoäng till tentamen 60%, 75% och 90% lösta hemtal ger 1, 2 respektive 3 bonuspoäng .

Kurslitteratur: Glader, Lindström: Diskret matematik, 2006. Kapitel 2.

Kurshemsida: http://web.abo.fi/fak/mnf/mate/kurser/algebrab/

Kurshemsidan på intranätet så man måste logga in dit först.

Kursmapp: Kopior av kursmaterial i datasalen Geologicum 127, (bredvid sal Lindelöf).

Kurstent: Tent: M 22.10 kl. 9-13 i Geologicum Aud I.

Kursinnehåll

- Algebraiska strukturer
- Grupper
- Permutationsgrupper
- Isomorfi
- Produkter av grupper
- Undergrupper
- Symmetri
- Lagranges sats
- Ekvivalensklasser
- Burnsides sats med tillämpningar på kombinatoriska problem och färgläggningsproblem

Algebraiska strukturer

Vi inleder detta kapitel med att definiera de grundläggande begreppen operation, algebraisk struktur, neutralt element, inverterbart element, associativ och kommutativ operation.

Definition. *En operation på en icke-tom mängd A är en avbildning från $A \times A$ till A. Om operationen betecknas $*$, så tillordnas varje ordnat par $(a, b) \in A \times A$ exakt ett element i A, vilket betecknas $a * b$.*

Med andra ord är $*$ en operation på A om och endast om villkoren (1) och (2) gäller:

(1) *$a * b$ är entydigt definierat för alla a och b i A;*

(2) *$a * b \in A$ för alla $a, b \in A$.*

Anmärkning. Villkoret (2) ovan, som förutsätter att (1) gäller, kan vi uttrycka med att säga att mängden A **är sluten under operationen** $*$.

Algebraiska strukturer

Exempel på operationer på de hela talens mängd $\mathbf{Z}$ är addition, subtraktion och multiplikation, varvid $a * b$ betyder $a + b$, $a - b$ respektive $a \cdot b$.

Division är inte en operation på $\mathbf{Z}$, eftersom division med 0 inte är definierat. Inte heller på $\mathbf{Z} \setminus \{0\}$ är division en operation, ty kvoten av två heltal behöver inte vara ett heltal, så villkor (2) är inte uppfyllt.

Däremot är division på $\mathbf{Q} \setminus \{0\}$ en operation, där $\mathbf{Q}$ betecknar de rationella talen.

Om $f : A \to A$ och $g : A \to A$ är funktioner, så skall vi med $f \circ g$ alltid avse **funktionssammansättningen**, dvs. den funktion från A till A som definieras av

$$(f \circ g)(x) = f(g(x)), \text{ för varje } x \in A.$$

Funktionssammansättningen $\circ$ är en operation på A^A. (Här betecknar A^A mängden av alla funktioner från A till A).

Algebraiska strukturer

Definition. *En (algebraisk) struktur är en mängd A försedd med en eller flera operationer. En mängd A med operationen $*$ bildar en struktur som betecknas $\langle A, * \rangle$. Vidare definierar vi ordningen för A som antalet element i mängden, beteckning $|A|$. Om A inte är ändlig säges A ha oändlig ordning.*

En struktur $\langle A, * \rangle$ är entydigt bestämd av mängden A och av att man för varje $a, b \in A$ känner produkten $a * b$. Om A är en ändlig mängd, strukturen kallas då också ändlig, kan man fullständigt beskriva strukturen med en kompositionstabell. (Cayley-tabell)

(A. Cayley, engelsk matematiker, 1821–1895)

Algebraiska strukturer

Definition. *Låt $\langle A, * \rangle$ vara en struktur. Ett neutralt element för $*$ är ett element $e \in A$ sådant att*

$$e * a = a * e = a, \text{ för varje } a \in A.$$

Ett element $a \in A$ är inverterbart med avseende på $*$ om det finns ett element $a' \in A$ sådant att

$$a' * a = a * a' = e\,.$$

Varje sådant element a' kallas invers till a.

Algebraiska strukturer

Vi skall nu visa att för en associativ operation har varje element högst en invers. Härvid säges en operation $*$, och även strukturen $\langle A, * \rangle$, vara **associativ** om

$$a * (b * c) = (a * b) * c, \text{ för alla } a, b, c \in A\,,$$

och **kommutativ** om

$$a * b = b * a, \text{ för alla } a, b \in A.$$

Sats 11. *Låt $\langle A, * \rangle$ vara en struktur.*

a) Då har operationen $*$ högst ett neutralt element i A;

b) om operationen $*$ på A är associativ med neutralt element, så har varje inverterbart element exakt en invers.

Bevis: a) Antag att e och e' är neutrala element. Då gäller:

$$e \text{ neutralt element } \Rightarrow e * e' = e' * e = e',$$

$$e' \text{ neutralt element } \Rightarrow e' * e = e * e' = e.$$

25

Alltså gäller det att $e = e'$.

b) Antag att $*$ är associativ med neutralt element e och att elementet $a \in A$ är inverterbart. Om u och v är inverser till a så gäller:

$$u = u * e = u * (a * v) = (u * a) * v = e * v = v,$$

alltså är $u = v$. $\square$

Anmärkning. Om elementet $a \in A$ är inverterbart med en entydigt bestämd invers, så betecknas denna a^{-1}.

Lights associativitetstest (F.W. Light 1949)

- Ändlig algebraisk struktur $\langle A, \cdot \rangle$ given av en Cayleytabell.
- Definiera operationerna $*$ och $\circ$ på A:

$$x * y = x \cdot (a \cdot y), \quad x \circ y = (x \cdot a) \cdot y$$

för alla $x, y \in A$ och fixerat $a \in A$.

- Om för varje fixerat $a \in A$ gäller att

$$x * y = x \circ y \quad \text{för alla } x, y \in A,$$

så är $\cdot$ associativ.

– Det gäller alltså att kolla att tabellerna för $\langle A, * \rangle$ och $\langle A, \circ \rangle$ är lika för alla $a \in A$.

Ex

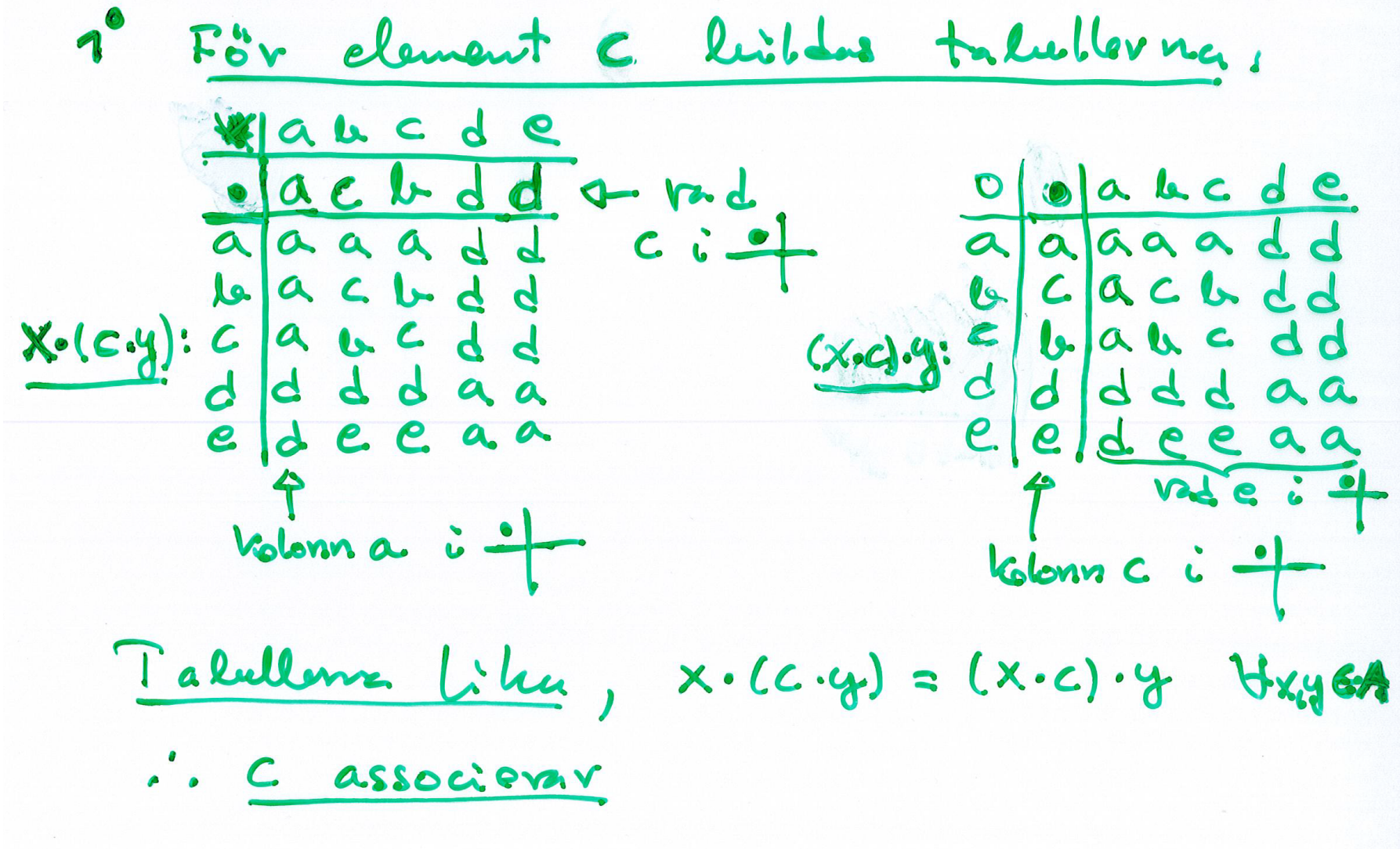
•	a	b	c	d	e
a	a	a	a	d	d
b	a	b	c	d	d
c	a	c	b	d	d
d	d	d	d	a	a
e	d	e	e	a	a

Nu är $a = e \cdot e$, $b = c \cdot c$ och $d = c \cdot e$, så det räcker att kolla associativiteten för c och e ($\{c, e\}$ genererar A).

Motivering: Om $a_1, a_2 \in A$ och $\begin{cases} x(a_1 y) = (x a_1) y \\ x(a_2 y) = (x a_2) y \end{cases}$

$\Rightarrow x((a_1 a_2) y) = x(a_1 (a_2 y)) = (x a_1)(a_2 y) = ((x a_1) a_2) y$

$= (x(a_1 a_2)) y$. $\therefore$ $a_1 \cdot a_2$ associerar med alla $x, y \in A$.


1° För element c bildas tabellerna:
X·(c·y):
(x·c)·y:
rad c i ·
kolonn a i ·
rad e i ·
kolonn c i ·
Tabellerna lika, x·(c·y) = (x·c)·y ∀x,y ∈ A
∴ c associerar

Algebraiska strukturer

2° För element e erhålls tabellerna:

$x \cdot (e \cdot y)$:

$*$	a	b	c	d	e
•	d	e	e	a	a
a	d	d	d	a	a
b	d	d	d	a	a
c	d	d	d	a	a
d	a	a	a	d	d
e	a	a	a	d	d

$(x \cdot e) \cdot y$

$\circ$	•	a	b	c	d	e
a	d	d	d	d	a	a
b	d	d	d	d	a	a
c	d	d	d	d	a	a
d	a	a	a	a	d	d
e	a	a	a	a	d	d

Tabellerna lika, $x \cdot (e \cdot y) = (x \cdot e) \cdot y$, $\forall x, y \in A$.

$\therefore$ e associerar

$\therefore\therefore$ c, e associerar och $\{c, e\}$ genererar A

$\Rightarrow$ • associativ operation i A.

Grupper

Ex] $\mathbb{R} = \{\text{reella tal}\}$, operation $+$

1°] $a, b \in \mathbb{R} \Rightarrow a+b \in \mathbb{R}$, $\mathbb{R}$ sluten under $+$

2°] $a, b, c \in \mathbb{R} \Rightarrow a+(b+c) = (a+b)+c$, $+$ associativ

3°] $\forall a \in \mathbb{R}: a+0 = 0+a = a$, 0 neutralt element

4°] $\forall a \in \mathbb{R}: a+(-a) = 0$, $-a$ invers till a

Grupper

$M_n = \{$ inverterbara $n \times n$-matriser $\}$, operation • matrismultiplikation

1° $A, B \in M_n \Rightarrow \underbrace{A \cdot B}_{n \times n} \in M_n$, M_n sluten under •

($\det A \neq 0, \det B \neq 0 \Rightarrow \det(A \cdot B) = \det A \cdot \det B \neq 0$)

2° $A, B, C \in M_n \Rightarrow A \cdot (B \cdot C) = (A \cdot B) \cdot C$, • associativ

3° $\forall A \in M_n : A \cdot I = I \cdot A = A$, I $n \times n$-enhetsmatrisen neutralt element

4° $\forall A \in M_n \; \exists A^{-1} \in M_n : A \cdot A^{-1} = A^{-1} \cdot A = I$,

A^{-1} invers till A

Grupper

$\mathcal{T} = \{f : A \to A : f \text{ bijektion}\}$, operation $\circ$ funktionssammansättning

1° $f, g \in \mathcal{T} \Rightarrow f \circ g \in \mathcal{T}$, $\mathcal{T}$ sluten under $\circ$

2° $f, g, h \in \mathcal{T} \Rightarrow f \circ (g \circ h) = (f \circ g) \circ h$, $\circ$ associativ

3° $\forall f \in \mathcal{T} : f \circ e = e \circ f = f$, $e(x) \equiv x$ neutralt element.

4° $\forall f \in \mathcal{T}\ \exists f^{-1} \in \mathcal{T} : f \circ f^{-1} = f^{-1} \circ f = e$

f^{-1} invers till f.

Grupper

Definition. *En grupp* $\langle G, * \rangle$ *är en algebraisk struktur som satisfierar följande axiom:*

(*i*) $a * (b * c) = (a * b) * c$, *för alla* $a, b, c \in G$;

(*ii*) *Det finns ett neutralt element* $e \in G$ *sådant att*

$e * a = a * e = a$ *för alla* $a \in G$;

(*iii*) *För varje* $a \in G$ *finns det ett element* $a^{-1} \in G$ *sådant att*

$a * a^{-1} = a^{-1} * a = e$.

Anmärkning. Med stöd av Sats 11 är e och a^{-1} i ovanstående definition entydigt bestämda.

Grupper

Om $|G| < \infty$, så är $\langle G, * \rangle$ en **ändlig grupp**. En ändlig grupp $\langle \{e, a_1, ..., a_n\}, * \rangle$ är fullständigt bestämd av sin kompositionstabell.

Exempel. (Se föreläsningsanteckningar).

Évariste Galois (1811–1832): "Undersökte vissa permutationsgrupper"

26

Grupper

Sats 12. *Låt a, b, c vara element i en grupp $\langle G, * \rangle$.*

(i) Då gäller strykningslagarna:

$$c * a = c * b \Rightarrow a = b;$$

$$a * c = b * c \Rightarrow a = b\,.$$

(ii) Då har ekvationen

$$a * x = b \qquad (y * a = b)$$

exakt en lösning $x = a^{-1} * b\,.$

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

Bevis: (i) Då c har inversen c^{-1} erhåller vi att

$$\begin{aligned} c * a = c * b &\Rightarrow c^{-1} * (c * a) = c^{-1} * (c * b) \\ &\Rightarrow (c^{-1} * c) * a = (c^{-1} * c) * b \\ &\Rightarrow e * a = e * b \\ &\Rightarrow a = b\,. \end{aligned}$$

Analogt bevis för den andra strykningslagen.

(ii) Vi har att $x = a^{-1} * b$ är en lösning, ty

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

Antag att både x_1 och x_2 är lösningar till ekvationen. Då är

$$a * x_1 = a * x_2\,(= b),$$

så del (i) ger att $x_1 = x_2$. Vi har således exakt en lösning. □

Grupper

Korollarium 13. *Om $\langle G, * \rangle$ är en ändlig grupp, så är varje rad och kolonn i kompositionstabellen en permutation av gruppens element.*

Exempel på viktiga grupper

(K4)

Exempel. **Kleins fyragrupp**. (Felix Klein, 1849-1925, tysk matematiker) (Se föreläsningsanteckningar).

Exempel. Gruppen av restklasser modulo n. Definiera för $n \geq 1$ mängden Z_n och operationen $+_n$ genom:

$$Z_n = \{0, 1, ..., n-1\},$$

$$i +_n j = \begin{cases} i + j, & \text{om } 0 \leq i + j \leq n-1; \\ i + j - n, & \text{om } i + j \geq n. \end{cases}$$

Strukturen $\langle Z_n, +_n \rangle$ har då kompositionstabellen

$+_n$	0	1	2	$\cdots$	$n-1$
0	0	1	2	$\cdots$	$n-1$
1	1	2	3	$\cdots$	0
$\vdots$		$\vdots$			$\vdots$
$n-1$	$n-1$	0	1	$\cdots$	$n-2$

Grupper

Strukturen $\langle Z_n, +_n \rangle$ har då kompositionstabellen

$+_n$	0	1	2	$\cdots$	$n-1$
0	0	1	2	$\cdots$	$n-1$
1	1	2	3	$\cdots$	0
$\vdots$		$\vdots$			$\vdots$
$n-1$	$n-1$	0	1	$\cdots$	$n-2$

så vi noterar att 0 är ett neutralt element och att inversen till elementet k ges av

$$k^{-1} = \begin{cases} n-k, & \text{om } k = 1, \ldots, n-1; \\ 0, & \text{om } k = 0. \end{cases}$$

Som hemuppgift lämnas beviset av att $\langle Z_n, +_n \rangle$ är en grupp.

28

Ex) $n = 10$

$5 +_n 2 = 7$, $5 +_n 9 = (\underbrace{5+9}_{\geq 10}) - 10 = 4$

Grupper

Anmärkning. Vi noterar att $|Z_n| = n$, så det finns grupper av godtycklig ändlig ordning. Vidare märker vi att kompositionstabellen i ovanstående exempel är symmetrisk kring diagonalen, dvs. $i +_n j = j +_n i$.

Definition. *En grupp* $\langle G, * \rangle$ *kallas Abelsk om* $a * b = b * a$ *för alla* $a, b \in G$. (dvs. Om $\langle G, * \rangle$ är Kommutativ)

Exempel på Abelska grupper är $\langle R, + \rangle$, $\langle Z, + \rangle$ och $\langle Z_n, +_n \rangle$. (Niels Henrik Abel, 1802-1829, norsk matematiker). (Även Kleins fyrgrupp, K_4 är Abelsk)!

Grupper

Exempel. **Den linjära gruppen** $GL(n, R)$ av inverterbara $n \times n$ matriser. (Se föreläsningsanteckningar).

$GL(n,\mathbb{R}) = \langle \{A : A \text{ reell } n \times n \text{ matris}, A^{-1} \text{ existerar}\}, \cdot \rangle$ matrismultiplikation

Grupper

Anmärkning. I fortsättningen betecknas en grupp $\langle G, * \rangle$ ofta med G och operationen $a * b$ med $a\,b$.

(hel tals)

Definition. *De positiva och negativa potenserna av ett element a i en grupp $\langle G, * \rangle$ definieras genom:*

$$a^0 := e,\ a^1 := a,\ a^n := a\,a^{n-1},\quad \textit{för } n \geq 2,$$
$$a^{-1} := a^{-1},\ a^{-m} := a^{-1}a^{-(m-1)},\quad \textit{för } m \geq 2.$$

Man kan då visa att för alla $m, n \in Z$ gäller:

$$a^m a^n = a^{m+n} \text{ och } (a^m)^n = a^{m\,n}.$$

(Se kursmappen)

$m = -1$: $(a^{-1})^n = a^{-n}$

$n = -1$: $(a^m)^{-1} = a^{-m}$ $(= (a^{-1})^m)$

$(a^m)^n = a^{mn} = a^{nm} = (a^n)^m$

Grupper

$a^0 = e$, $a^1 = a$, $a^n = a * a^{n-1}$, $n \geq 2$.

$a^{-1} = a^{-1}$, $a^{-m} = a^{-1} * a^{-(m-1)}$, $m \geq 2$.

Vi ser först: $a^{-n} = (a^{-1})^n$ för $n > 0$. (F)

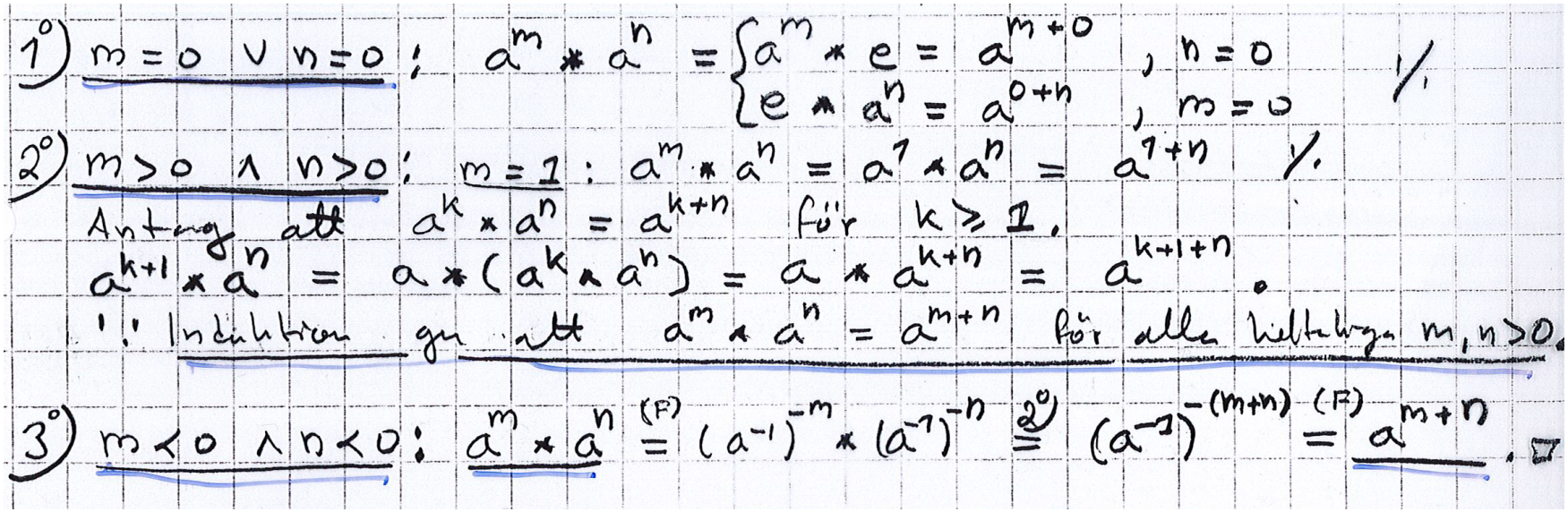
$n = 1$: $a^{-1} = (a^{-1})^1$ ⇒ formeln gäller.

Antag att $a^{-k} = (a^{-1})^k$ för $k \geq 1$. (Ind. ant.)

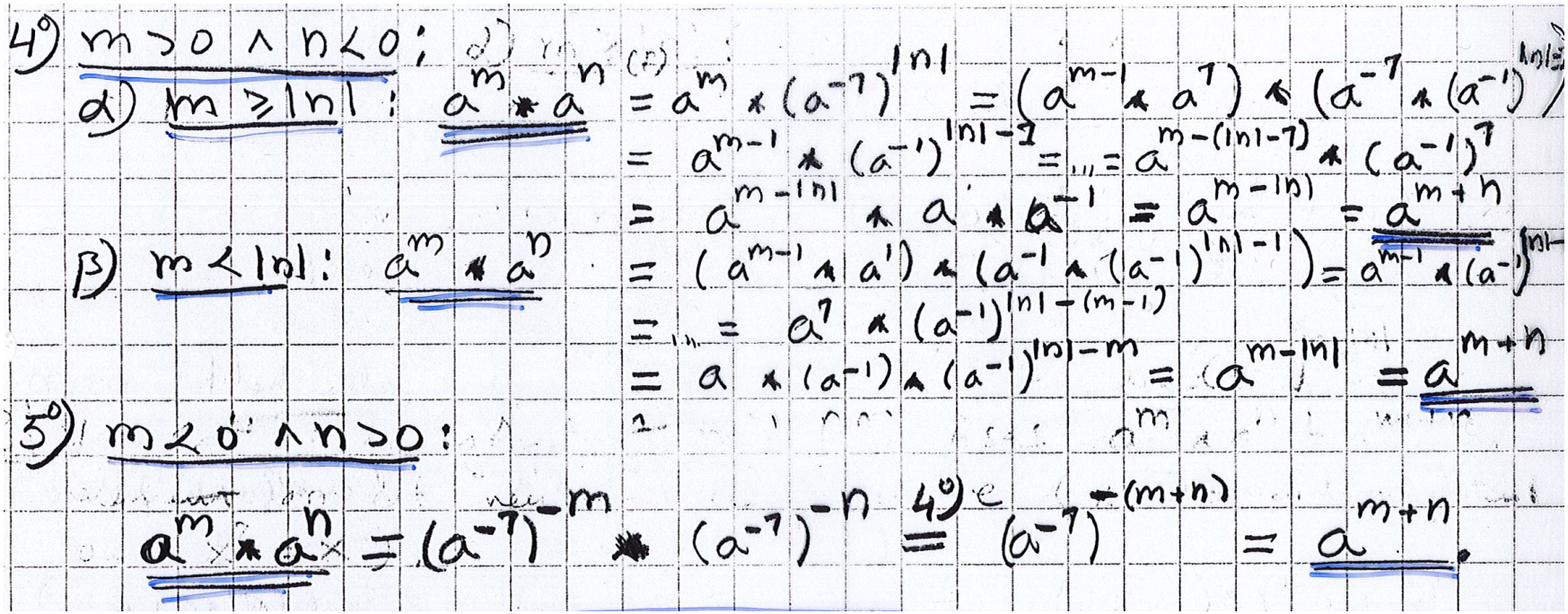
$a^{-(k+1)} = a^{-1} * a^{-k} = a^{-1} * (a^{-1})^k = (a^{-1})^{k+1}$

⇒ $a^{-n} = (a^{-1})^n$ för alla heltalen $n > 0$.

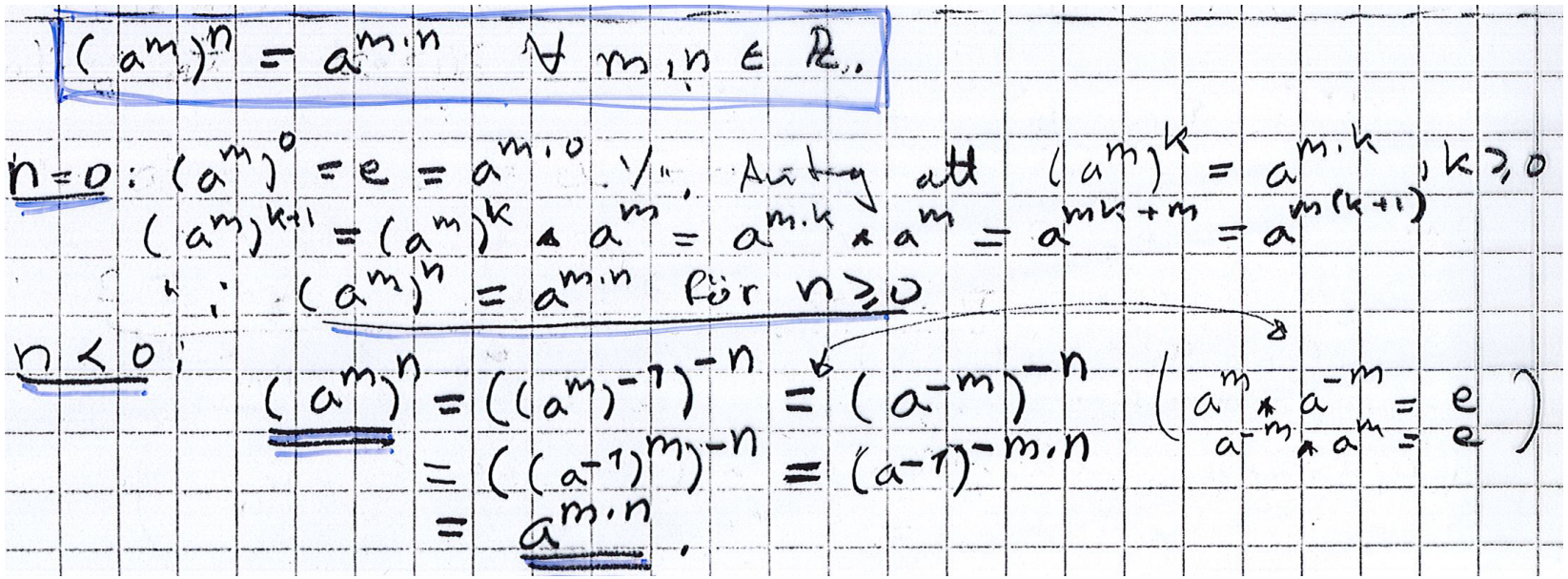
Grupper


1°) m = 0 ∨ n = 0 ;
2°) m > 0 ∧ n > 0 ;
m = 1 :
Antag att
för
Induktion
för alla heltalen
3°) m < 0 ∧ n < 0 ;
(F)
(F)

Grupper


4° m > 0 ∧ n < 0;
α) m ≥ |n|: a^m * a^n = a^m * (a^{-1})^{|n|} = (a^{m-1} * a^1) * (a^{-1} * (a^{-1})^{|n|-1}) = a^{m-1} * (a^{-1})^{|n|-1} = ... = a^{m-(|n|-1)} * (a^{-1})^1 = a^{m-|n|} * a * a^{-1} = a^{m-|n|} = a^{m+n}
β) m < |n|: a^m * a^n = (a^{m-1} * a^1) * (a^{-1} * (a^{-1})^{|n|-1}) = a^{m-1} * (a^{-1})^{|n|-1} = ... = a^1 * (a^{-1})^{|n|-(m-1)} = a * (a^{-1}) * (a^{-1})^{|n|-m} = a^{m-|n|} = a^{m+n}
5° m < 0 ∧ n > 0:
a^m * a^n = (a^{-1})^{-m} * (a^{-1})^{-n} 4° = (a^{-1})^{-(m+n)} = a^{m+n}.

Grupper


$(a^m)^n = a^{m\cdot n}$ $\forall\, m,n \in \mathbb{Z}$.
$n=0$: $(a^m)^0 = e = a^{m\cdot 0}$ V.
Antag att $(a^m)^k = a^{m\cdot k}$, $k \geq 0$
$(a^m)^{k+1} = (a^m)^k * a^m = a^{m\cdot k} * a^m = a^{mk+m} = a^{m(k+1)}$
$\therefore$ $(a^m)^n = a^{m\cdot n}$ för $n \geq 0$
$n < 0$:
$(a^m)^n = ((a^m)^{-1})^{-n} = (a^{-m})^{-n}$
$= ((a^{-1})^m)^{-n} = (a^{-1})^{-m\cdot n}$
$= a^{m\cdot n}$.
$a^m * a^{-m} = e$
$a^{-m} * a^m = e$

Grupper

Definition. *En grupp G kallas cyklisk om det finns ett element $a \in G$ sådant att*

$$G = \{a^k : k \in Z\}.$$

Exempel. Exempel på cykliska grupper. (Se föreläsningsanteckningar).

Sats 14. *Om gruppen G är cyklisk, så är den även Abelsk.*

Bevis: Antag att G är cyklisk med $G = \{a^k : k \in Z\}$ för något $a \in G$. Tag $b, c \in G$. Då finns det heltal m och n sådana att $a^m = b$ och $a^n = c$. Vidare gäller det att

$$b\,c = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = c\,b,$$

och därmed är G en abelsk grupp. □

Sats 14 kan inte omvändas, dvs. en Abelsk grupp behöver inte vara cyklisk, vilket följande exempel demonstrerar.