Kapitel 3

Fundamental Aritmetik

I det følgende præsenteres en undersøgende tilgang til elementære operationer på de hele tal. Nærmere bestemt vil vi tage udgangspunkt i fundamentale egenskaber ved addition på de hele tal, for derefter kort at diskutere multiplikation. Helt centralt for undervisningsmaterialet er introduktionen af potensudtryk og potensregneregler, og i halen stiller vi det oplagte spørgsmål: Hvis multiplikation kan forstås som gentagen addition, og eksponentiering kan forstås som gentagen multiplikation, findes der så en operation, der kan forstås som gentagen eksponentiering - og hvorfor har jeg aldrig hørt om den? Det fagelige indhold orienterer sig mod grundlæggende algebraisk forståelse af operationer på tal, og placeres naturligt i 1.g, som et dels repeterende, dels undersøgende forløb om potensregning.

Vi vil i det følgende forudsætte, at læseren er bekendt med *associativitet* og *kommutativitet* for addition af hele tal, altså

$$a + (b + c) = (a + b) + c, \qquad a + b = b + a$$

for alle $a, b, c \in \mathbb{Z}$. Desuden forudsættes bekendthed med subtraktion og forståelse af subtraktion som invers til addition.

3.1 Kernestof

For fuldstændighed og klarhed af den røde tråd introduceres multiplikation med hele tal som gentagen addition, hvilket er præciseret herunder.

Definition 3.1.1. Lad $a \in \mathbb{Z}$ og $m \in \mathbb{N}$. Da defineres *multiplikation* $\cdot$ ved

$$a \cdot m \coloneqq \underbrace{a + a + \ldots + a}_{m \text{ gange}}, \qquad a \cdot 0 \coloneqq 0, \qquad \text{og} \qquad a \cdot (-m) \coloneqq -\underbrace{(a + a + \ldots + a)}_{m \text{ gange}} = -a \cdot m$$

For $m \in \mathbb{Z}$ indfører vi konventionen, at

$$\underbrace{a + a + \ldots + a}_{m \text{ gange}} \coloneqq \operatorname{sign}(m) \underbrace{(a + a + \ldots + a)}_{|m| \text{ gange}}, \qquad \operatorname{sign}(m) \coloneqq \begin{cases} 1, & \text{hvis } m > 0, \\ 0, & \text{hvis } m = 0, \\ -1, & \text{hvis } m < 0 \end{cases}$$

som betyder, at vi kan definere $a \cdot m \coloneqq \underbrace{a + a + \ldots + a}_{m \text{ gange}}$ for alle $m \in \mathbb{Z}$.

For at forsimple mere komplekse udregninger indfører vi det sædvanlige regnehierarki, så for $a, b \in \mathbb{Z}$ og $m, n \in \mathbb{Z}$ defineres

$$a \cdot m + b \cdot n \coloneqq (a \cdot m) + (b \cdot n),$$

så vi med andre ord multiplicerer *før* vi adderer.

Vi fortsætter i samme spor og introducerer følgende genkendelige regneregler, som beskriver samspillet mellem operationerne $+$ og $\cdot$ i de hele tal. Læseren opfordres til at lægge særligt mærke til den principielle nødvendighed af et bevis samt udformningen af samme for følgende resultat.

Sætning 3.1.2. Lad $a, b \in \mathbb{Z}$ og $m, n \in \mathbb{Z}$. Da gælder

a) $a \cdot m + a \cdot n = a \cdot (m + n)$.
c) $a \cdot m + b \cdot m = (a + b) \cdot m$.
e) $(a \cdot m) \cdot n = a \cdot (m \cdot n)$.
b) $a \cdot m - a \cdot n = a \cdot (m - n)$.
d) $a \cdot m - b \cdot m = (a - b) \cdot m$.
f) $m \cdot n = n \cdot m$.

Bevis for a). Lad $a \in \mathbb{Z}$ og $m, n \in \mathbb{N}$. Da haves

$$a \cdot m + a \cdot n = \underbrace{a + a + \ldots + a}_{m \text{ gange}} + \underbrace{a + a + \ldots + a}_{n \text{ gange}} = \underbrace{a + a + \ldots + a}_{m+n \text{ gange}} = a \cdot (m + n)\,,$$

hvor første og sidste lighedstegn følger af definitionen af multiplikation.

Da samtlige punkter a)-f) har ensartede beviser udelades disse fra noten her. □

Parallelt til introduktionen af multiplikation som gentagen addition vil vi nu indføre eksponering af heltal som gentagen multiplikation, hvilket er præciseret i definitionen herunder.

Definition 3.1.3. Lad $a \in \mathbb{Z}$ og $m \in \mathbb{N}$. Da defineres *eksponering* $\wedge$ ved

$$a \wedge m \coloneqq \underbrace{a \cdot a \cdot \ldots \cdot a}_{m \text{ gange}},$$

og for $a \neq 0$ defineres desuden

$$a \wedge 0 \coloneqq 1, \qquad \text{og} \qquad a \wedge (-m) \coloneqq \frac{1}{\underbrace{a \cdot a \cdot \ldots \cdot a}_{m \text{ gange}}} = \frac{1}{a \wedge m}$$

Vi kalder a for *grundtallet*, m for *eksponenten* og hele udtrykket $a \wedge m$ for en *potens*.

Med mildt misbrug af notationen indfører vi indfører vi konventionen, at for alle $m \in \mathbb{Z}$ haves

$$\underbrace{a \cdot a \cdot \ldots \cdot a}_{m \text{ gange}} \coloneqq \underbrace{(a \cdot a \cdot \ldots \cdot a)}_{|m| \text{ gange}}^{\operatorname{sign}(m)},$$

hvor $x^1 = x$, $x^0 = 1$ og $x^{-1} = \frac{1}{x}$. Det betyder, at vi kan skrive $a \wedge m = \underbrace{a \cdot a \cdot \ldots \cdot a}_{m \text{ gange}}$ for alle $m \in \mathbb{Z}$.

Igen for at forsimple mere komplekse udregninger udbygger vi det sædvanlige regnehierarki, så for $a, b \in \mathbb{Z}$ og $m, n \in \mathbb{Z}$ defineres

$$a \wedge m + b \wedge n \coloneqq (a \wedge m) + (b \wedge n)\,, \qquad a \wedge m \cdot b \wedge n \coloneqq (a \wedge m) \cdot (b \wedge n)\,,$$

så vi med andre ord eksponerer vi *før* vi adderer og multiplicerer.

Inspireret af vores tidligere etablerede regneregler, som beskriver samspillet mellem addition og multiplikation, formulerer og beviser vi nu følgende regneregler, som beskriver samspillet mellem multiplikation og eksponering. Læserens opmærksomhed henledes på den slående lighed mellem beviserne for Sætning 3.1.2 og Sætning 3.1.4.

Sætning 3.1.4. Lad $a, b \in \mathbb{Z}$ og $m, n \in \mathbb{Z}$. Da gælder

a) $a \wedge m \cdot a \wedge n = a \wedge (m + n)$.
c) $a \wedge m \cdot b \wedge m = (a \cdot b) \wedge m$.
e) $(a \wedge m) \wedge n = a \wedge (m \cdot n)$.
b) $\dfrac{a \wedge m}{a \wedge n} = a \wedge (m - n)$.
d) $\dfrac{a \wedge m}{b \wedge m} = \left(\dfrac{a}{b}\right) \wedge m$.

hvor b) og d) forudsætter $b \neq 0$.

Bevis for a). Lad $a \in \mathbb{Z}$ og $m, n \in \mathbb{Z}$. Da haves

$$a \wedge m \cdot a \wedge n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{m \text{ gange}} \cdot \underbrace{a \cdot a \cdot \ldots \cdot a}_{n \text{ gange}} = \underbrace{a \cdot a \cdot \ldots \cdot a}_{m+n \text{ gange}} = a \wedge (m+n)\,,$$

hvor første og sidste lighedstegn følger af definitionen af eksponering. □

Indtil nu har vi brugt en utraditionel notation for at undstrege, at eksponering er en operation, som konstrueres fra multiplikation helt analogt til hvordan multiplikation konstrueres fra addition. Symbolet for multiplikation $\cdot$ undertrykkes ofte i matematiske udsagn; vi taler om et underforstået multiplikationssymbol, så $ab \coloneqq a \cdot b$ for alle $a, b \in \mathbb{Z}$. Tilsvarende undertrykkes symbolet for eksponering $\wedge$ på følgende vis.

Notation 3.1.5. Lad $a, m \in \mathbb{Z}$. Da noteres eksponering ved

$$a^m \coloneqq a \wedge m$$

hvor a er *grundtallet*, m er *eksponenten* og udtrykket a^m kaldes en *potens*.

Til fremtidig reference reformulerer vi indholdet af Sætning 3.1.4 herunder udtrykt i den traditionelle notation.

Sætning 3.1.6. Lad $a, b \in \mathbb{Z}$ og $m, n \in \mathbb{Z}$. Da gælder

a) $a^m \cdot a^n = a^{m+n}$.

b) $\dfrac{a^m}{a^n} = a^{m-n}$.

c) $a^m \cdot b^m = (a \cdot b)^m$.

d) $\dfrac{a^m}{b^m} = \left(\dfrac{a}{b}\right)^m$.

e) $(a^m)^n = a^{m \cdot n}$.

hvor b) og d) forudsætter henholdsvis $a \neq 0$ og $b \neq 0$.

3.1.1 Persepektivering: Knuth's pil op ↑

Vi så først, hvordan multiplikation kan defineres som gentagen addition, hvorefter vi definerede eksponering som gentagen multiplikation. I naturlig forlængelse heraf undersøger vi nu definitionen af en operation, der noterer gentagen eksponering. Vi bemærker dog først, at eksponering $\wedge$ *ikke* er associativ, altså at ligheden

$$(a \wedge m) \wedge n \stackrel{?}{=} a \wedge (m \wedge n)\,, \qquad a, m, n \in \mathbb{Z}$$

ikke gælder generelt, se eventuelt Sætning 3.1.4e), hvorfor parenteserne i følgende udsagn er nødvendige for at sikre definitionens entydighed.

Definition 3.1.7. Lad $a \in \mathbb{Z}$ og $m \in \mathbb{N}$. Da defineres *Knuth's pil op* $\uparrow$ ved

$$a \uparrow m \coloneqq \underbrace{a \wedge (a \wedge (\ldots \wedge a))}_{m \text{ gange}}\,.$$

Bemærkning. Vi definerer ikke Knuth's pil op for $m \in \mathbb{Z}$, da en sådan udviddelse faktisk ikke er kendt.

Det er centralt at bemærke, at fordi $\wedge$ ikke er associativ, så er vi nødt til at udføre operationerne i en bestemt rækkefølge angivet af placeringen af parenteser. Det betyder også, at vi ikke kan udlede regneregler for samspillet mellem $\uparrow$ og $\wedge$, eksempelvis har vi

$$a \uparrow m \wedge a \uparrow n = \underbrace{(a \wedge (a \wedge (\ldots \wedge a)))}_{m \text{ gange}} \wedge \underbrace{(a \wedge (a \wedge (\ldots \wedge a)))}_{n \text{ gange}} \stackrel{?}{=} \underbrace{(a \wedge (a \wedge (\ldots \wedge a)))}_{m \star n \text{ gange}} = a \uparrow (m \star n)\,,$$

hvor $\star$ er en pladsholder for $+$, $\cdot$ eller $\wedge$, men uanset hvad ville ligheden ikke gælde generelt. Intuitionen er således, at eftersom vi i definitionen af $\uparrow$

3.1.2 Persepektivering: Generalisering til de Rationale Tal $\mathbb{Q}$

For fuldstændighed og klarhed af den røde tråd introduceres først division som den inverse operation til multiplikation, hvilket er præciseret i definitionen herunder.

Definition 3.1.8. Lad $a, b \in \mathbb{Z}$. Da defineres *division* / ved

$$a/b \coloneqq a \cdot \frac{1}{b},$$

hvor $\frac{1}{b} \in \mathbb{Q}$ noterer det tal, som opfylder $b \cdot \frac{1}{b} = 1$ for $b \in \mathbb{Z}$. Eksistens og entydighed af et sådant tal vil vi ikke diskutere nærmere her.

Med observationen at subtraktion og division som operationer er modsætninger til henholdsvis addition og multiplikation, vil vi motivere definitionen af m'te rødder som modsætning til m'te potens.

Definition 3.1.9. Lad $a \in \mathbb{Q}_+$ og $m \in \mathbb{N}$. Da er den *m'te rod af a*, noteret $\sqrt[m]{a}$, det positive tal, som opfylder

$$\left(\sqrt[m]{a}\right)^m = a$$

Eksistens og entydighed af den m'te rod af a nævnes uden bevis, dog kan særligt entydighed retfærdiggøres med et argument som følgende. Lad $a, b \in \mathbb{Q}_+$ og $m \in \mathbb{N}$. Da haves

$$a^m = b^m \quad \Leftrightarrow \quad \frac{a^m}{b^m} = 1 \quad \Leftrightarrow \quad \left(\frac{a}{b}\right)^m = 1 \quad \overset{(\dagger)}{\Leftrightarrow} \quad \frac{a}{b} = 1 \quad \Leftrightarrow \quad a = b$$

hvor vi postulerer, at det eneste positive tal multipliceret med sig selv m gange, der giver 1, er tallet 1 selv. Eksistens af m'te rødder kræver en grundig introduktion af reelle tal, som vi på ingen måde forudsætter her. Vi viser nu, at den m'te rod faktisk er modsætning til m'te potens.

Sætning 3.1.10. Lad $a \in \mathbb{Q}_+$ og $m \in \mathbb{N}$. Da gælder

$$\sqrt[m]{a^m} = a = \left(\sqrt[m]{a}\right)^m$$

Bevis. Vi udnytter først definitionen af den m'te rod, hvilket efterfølges af elementære omskrivninger.

$$\left(\sqrt[m]{a^m}\right)^m = a^m \quad \Leftrightarrow \quad \frac{\left(\sqrt[m]{a^m}\right)^m}{a^m} = 1 \quad \overset{(\dagger)}{\Leftrightarrow} \quad \left(\frac{\sqrt[m]{a^m}}{a}\right)^m = 1 \quad \Leftrightarrow \quad \frac{\sqrt[m]{a^m}}{a} = 1 \quad \Leftrightarrow \quad \sqrt[m]{a^m} = a$$

hvor (†) gør brug af Sætning 3.1.6(4)[1]. Dette viser den første lighed, mens den anden lighed ganske simpelt følger af defintiionen af den m'te rod. □

Vi fortsætter den pedantiske grundighed med definitionen af multiplikation med et rationalt tal, igen for at sikre den røde tråd.

Definition 3.1.11. Lad $a \in \mathbb{Q}$, $m \in \mathbb{Z}$ og $n \in \mathbb{N}$. Da defineres *multiplikation* $\cdot$ ved

$$a \cdot \frac{m}{n} \coloneqq \frac{a \cdot m}{n}$$

Vi bemærker således, at multiplikation med et rationalt tal er defineret som sædvanlig multiplikation med tælleren efterfulgt af division med nævneren.

Med henvisning til ovenstående defineres eksponering med rationale tal.

Definition 3.1.12. Lad $a \in \mathbb{Q}_+$, $m \in \mathbb{Z}$ og $n \in \mathbb{N}$. Da defineres *eksponering* ved

$$a^{m/n} \coloneqq \sqrt[n]{a^m}$$

[1] Principielt er argumentet ugyldigt, da vi ikke ved at $\sqrt[m]{a^m}$ er et rationalt tal.

På samme måde som med multiplikation er eksponering med et rationalt tal blot den sædvanlige eksponering med tælleren efterfulgt af den modsatte operation med nævneren, nemlig at tage den n'te rod.

Vi så tidligere, at eksponering med hele tal opfylder en række regneregler. Da vi nu har udviddet definitionen til at dække eksponering med rationale tal, er vi nødt til at bevise disse regneregler i det generelle tilfælde. For at understrege de tekniske krav til et sådant bevis, bemærker vi at den viste regneregel er det simpleste tilfælde, og selv her er der skridt, vi ikke kan argumentere for fyldestgørende.

Sætning 3.1.13. Lad $a, b \in \mathbb{Q}$ og $m, n \in \mathbb{Q}$. Da gælder

a) $a^m \cdot a^n = a^{m+n}$.

b) $\dfrac{a^m}{a^n} = a^{m-n}$.

c) $a^m \cdot b^m = (a \cdot b)^m$.

d) $\dfrac{a^m}{b^m} = \left(\dfrac{a}{b}\right)^m$.

e) $(a^m)^n = a^{m \cdot n}$.

Bevis for c). Lad $m \in \mathbb{Q}$ og $p \in \mathbb{Z}$ og $q \in \mathbb{N}$, så $m = p/q$. Da haves for $a, b \in \mathbb{Q}$, at

$$a^m \cdot b^m = a^{p/q} \cdot b^{p/q} = \left(\sqrt[q]{a}\right)^p \left(\sqrt[q]{b}\right)^p \overset{(\dagger_1)}{=} \left(\sqrt[q]{a} \cdot \sqrt[q]{b}\right)^p \overset{(\dagger_2)}{=} \left(\sqrt[q]{a \cdot b}\right)^p = (a \cdot b)^{p/q} = (a \cdot b)^m ,$$

hvor $(\dagger_1)$ kræver generaliseringen af Sætning 3.1.6(c) for $a, b \in \mathbb{R}$, hvilket vi ikke har vist (og end ikke defineret - overvej, hvad det egentlig sige at multiplicere reelle tal?). Ligheden markeret med $(\dagger_2)$ følger, da der findes netop ét tal, som opløftet i q'te potens giver ab, nemlig $\sqrt[q]{ab}$ og da

$$\left(\sqrt[q]{a}\sqrt[q]{b}\right)^q = \sqrt[q]{a}^q \cdot \sqrt[q]{b}^q = ab,$$

så kan vi konkludere $\sqrt[q]{a}\sqrt[q]{b} = \sqrt[q]{ab}$. □