Matematik 1c

Daniel Bosk

E-mail address: dbosk@kth.se
URL: http://www.bosk.se/

Innehåll

KAPITEL 1

Introduktion

MATEMATIKEN HAR FUNNITS i mer än 5000 år, men började utvecklas i riktning mot dagens matematik först omkring 300 f.Kr. i antikens Grekland. Innan dess var matematiken endast räkning, ett verktyg för att beräkna skatter och konstruera byggnadsverk.

Ordet matematik har sitt ursprung i grekiskans *μάθημα (máthēma)* som betyder *lärande, studier, vetenskap*. Det är i det antika Grekland som dagens matematik har sitt ursprung. De studerade främst geometri och gjorde detta genom att sätta upp några grundläggande antaganden, kallade postulat eller axiom, som de var övertygade om att de stämde överens med verkligheten. Dessa var enkla antaganden, såsom att två parallella linjer aldrig kommer att skära varandra. Utifrån dessa enkla postulat härledde de olika geometriska resultat och de kunde bevisa att det måste vara på ett visst sätt. Även om de kunde se genom några enkla experiment hur saker förhöll sig till varandra nöjde de sig inte utan ett bevis utifrån postulaten och tidigare bevisade resultat.

Detta har verkat som inspiration för matematiker genom historien och är den drivkraft som verkat för att matematiken utvecklats till det som den är idag. Dagens matematik bygger likt grekernas på några enkla grundantaganden som vi kallar för axiom. Vidare måste begrepp som vi använder definieras tydligt så att vi vet exakt vad som menas med dem. Detta var drivkraften bakom axiomatiseringen av de naturliga talen som vi kommer att se i Kapitel 4, bakom grundläggningen av de hela talen i Kapitel 5 och de övriga talen. Länge hade matematikerna tagit talen som självklara, men vid 1800-talets mitt behövde de veta tydligare vad ett tal var för att kunna gå vidare.

I en definition av ett objekt eller egenskap sätter vi upp regler för hur ett objekt som är av denna typ eller har denna egenskap ska bete sig. Om vi kan visa att ett objekt uppfyller reglerna i definitionen, då måste objektet också vara av den typen eller ha den egenskapen. Då vet vi exakt, vi kan bevisa att ett objekt är av en specifik typ. Vi kan också göra det omvända, om ett objekt är av denna typen uppfyller det de givna reglerna. Då när vi bevisar saker kan vi utgå från enbart dessa regler.

1.1. Vad är då matematik?

MATEMATIKEN KAN BESKRIVAS som studiet av abstrakta konstruktioner. Med abstrakta konstruktioner menar vi saker som endast finns i vårt sinne. Vi sätter upp axiomen och definitionerna, spelreglerna, och undersöker sedan vad dessa spelregler ger upphov till.

Historiskt har matematiken ofta varit sammankopplad med studiet av verkligheten. Vi har kunnat studera verkligheten med hjälp av matematiken genom att våra grundregler varit grundläggande principer för verkligheten[1]. Men trots detta är matematiken skild från verkligheten. De axiom vi utgår ifrån behöver inte vara principer från verkligheten. Det finns matematiska konstruktioner som kan te sig så verklighetsfrånkopplade att icke-matematiker ifrågasätter varför

[1]Se exempelvis Euklides postulat för geometrin.

de studeras, och detta för oss in på ett viktigt konstaterande. Många matematiker genom historien studerade matematiken enbart för den rena matematikens skull – för att den var vacker, inte för att den gick att tillämpa på verkligheten. Exempel på sådana är Pierre de Fermat (ca 1607-1650) som är upphovsman till den kända *Fermats stora sats*. Han var advokat och amatörmatematiker. *Fermats stora sats* eller *Fermats sista sats* säger att ekvationen $x^n + y^n = z^n$, där x, y och z är heltal, saknar lösningar för heltal n större än två. Fermat lämnade en anteckning i marginalen av sin kopia av Diophantus *Arithmetica* att han hade ett bevis för detta, men att marginalen var för liten för att rymma det. Det tog matematiker ända fram till år 1994 att bevisa satsen, så möjligen hade Fermat inte ett korrekt bevis för satsen. Han hade däremot ett korrekt bevis för sin *lilla sats* som säger att om p är ett primtal, då ger a^{p-1} alltid resten 1 vid division med p. Leonard Euler (1707-1783) generaliserade Fermats lilla sats till att gälla även sammansatta tal, och denna generalisering är känd som *Fermat-Eulers sats* eller bara *Eulers sats*. Resultaten för dessa hade inget tillämpningsvärde för tiden utan drivkraften var att utforska matematikens vackra värld och finna vackra resultat som dessa. År 1978 publicerade Ronald Rivest (1947-), Adi Shamir (1952-) och Leonard Adleman (1945-) ett krypteringssystem sedermera känt som RSA. RSA-systemet bygger på Fermat-Eulers sats och systemet ligger till grunden för mycket av den säkra kommunikationen som sker på Internet idag. Det dröjde alltså ca 300 år innan en tillämpning dök upp. Detta visar vikten av den så kallade grundforskningen, den forskning som inte har någon omedelbar tillämplighet. Denna är inte viktig bara för matematiken utan alla vetenskaper. För vi kan ställa oss frågan om vi hade haft säker kommunikation på Internet idag om vi bara utforskat det som verkat direkt tillämpbart?

KAPITEL 2

Logik och bevis

MATEMATIKEN HAR SIN grund i logiken. Det är logiken som ger matematiken möjligheten till ett resonemang och möjligheten till härledning. Matematiken utgår från några få grundläggande antaganden, kallade *axiom*, från vilka alla matematiska resultat härleds. En matematiker nöjer sig således inte med att undersöka några exempel – eller göra experiment – inte ens tusen- eller miljontals exempel duger. Det är detta som skiljer matematiken från exempelvis fysiken och kemin, trots att dessa till mycket stor omfattning använder matematiken som hjälpmedel. Vi har inga grundläggande principer för fysiken och kemin som vi känner till, utan det är dessa vi försöker att finna. Vi känner däremot till alla grundläggande principer för matematiken, detta för att matematiken är skapad av oss – det är vi som bestämt dessa principer.

2.1. Logik

ALL MATEMATISK ARGUMENTATION består av *utsagor*. Dessa är deklarativa meningar som kan klassificeras som antingen *sanna* eller *falska*. Vi behöver inte alltid veta precis vilket, men det måste vara den ena eller den andra – aldrig båda. Detta kallas *Lagen om det uteslutna tredje*. Om vi tittar på följande meningar:

(1) Denna text är skriven på svenska.
(2) Grön är en fin färg.
(3) Denna mening är falsk.
(4) Det finns oändligt många primtalstvillingar.
(5) $x^2 + 1 = 0$

Den första meningen är en utsaga, och den är sann. Den andra är ej en utsaga i logisk bemärkelse, det är en smaksak. Den tredje meningen är ej en utsaga, den kan varken vara sann eller falsk eftersom att det leder till motsägelsefulla slutsatser. Den fjärde meningen är en utsaga, ingen vet dock om den är sann eller falsk. Den femte och sista symbolföljden är en utsaga, men vi vet inte vad x är så vi kan inte uttala oss om den skulle vara sann eller falsk. Detta visar vikten av att tydligt specificera alla delar av en utsaga, så att det är alldeles klart vad vi menar. Den femte utsagan skulle behöva ändras till exempelvis ”det finns ett komplext tal x sådant att $x^2 + 1 = 0$” för att den skulle vara sann. Om vi istället ändrat den till ”det finns ett heltal x sådant att $x^2 + 1 = 0$” skulle den vara falsk oavsett hur vi väljer x eftersom att det inte finns ett sådant heltal. En utsaga som alltid är falsk kallar vi för *motsägelse* eller *kontradiktion*. En utsaga som alltid är sann kallar vi för *tautologi*.

Två utsagor P och Q sägs vara logiskt ekvivalenta om P är sann precis när Q är sann och följdaktligen om P är falsk precis när Q är falsk. Vi skriver detta som $P \equiv Q$.

2.1.1. Kombinerade utsagor. Vi vill också kunna forma nya utsagor från redan kända, detta genom att kombinera och modifiera dem. Om P är en utsaga, då säger vi att *negationen* av P, betecknad $\neg P$ eller icke P, är falsk precis när P är sann och sann precis när P är falsk. Vi kommer då fram till

Lagen om dubbelnegation. Om vi funderar på vad som händer om vi tar $\neg(\neg P)$ så kommer vi fram till att $P \equiv \neg(\neg P)$.

Exempel 2.1. Ett exempel på negation, låt P vara utsagan "vi befinner oss i Sverige". Då blir $\neg P$ "vi befinner oss ej i Sverige".

Exempel 2.2. Vi kan också titta på följande utsaga, "alla svenskar tycker om surströmming". Negationen av den utsagan är *inte* att ingen svensk tycker om surströmming, utan den är "inte alla svenskar tycker om surströmming". Det räcker då med att det finns någon svensk som inte tycker om surströmming – detta är en viktig skillnad att inte ta fel på!

Vi kan också kombinera utsagor genom *konjunktioner*. Om P och Q är utsagor, då betecknar vi konjunktionen som P och Q eller $P \wedge Q$. Konjunktionen är sann då både P och Q båda är sanna och falsk annars.

Exempel 2.3. Låt P vara utsagan "jag bor i Sverige" och Q vara utsagan "jag har en Internetuppkoppling". Då kan vi skapa den nya utsagar $P \wedge Q$ som blir "jag bor i Sverige *och* jag har en Internetuppkoppling".

Övning 2.4. När är de olika utsagorna P, Q och $P \wedge Q$ i Exempel 2.3 sanna respektive falska?

Vi har också *disjunktionen* som betecknas P eller Q eller $P \vee Q$. Disjunktionen är sann om antingen P eller Q eller båda är sanna, och är således falsk endast när P och Q båda är falska. Konjunktionen och disjunktionen sammanfattas i en sanningstabell i Tabell 1.

TABELL 1. Sanningstabell för konjunktionen och disjunktionen. S betyder sant och F betyder falskt.

P	Q	$P \wedge Q$	$P \vee Q$
S	S	S	S
S	F	F	S
F	S	F	S
F	F	F	F

Övning 2.5. Vilken av följande logiska utsagor passar bäst för ett klassiskt tårtkalas? På ett kalas

(1) äts tårta *och* dricks saft *och* äts kakor *och* dricks kaffe *och* dricks te.
(2) äts tårta *eller* dricks saft *eller* äts kakor *eller* dricks kaffe *eller* dricks te.

Övning 2.6. Testa att kombinera negationen, konjunktionen och disjunktionen, går det att forma några logiskt ekvivalenta utsagor?

2.1.2. Implikationer. Implikation är synonymt med ordet *medför*. Om P och Q är utsagor säger vi att P *implicerar* Q eller *om* P, *då* Q. Vi ska undersöka när denna sammansatta utsaga bör vara sann och när den bör vara falsk. Låt oss formulera ett exempel.

Exempel 2.7. Låt P vara utsagan "jag vinner pengar" och Q vara utsagan "jag köper nya böcker till skolan". Utsagan $P \implies Q$ blir då "*om* jag vinner pengar, *då* jag köper nya böcker till skolan".

Implikationen är uppenbart falsk om jag vinner pengar men inte köper böcker till skolan, men sann om jag köper böcker. Annars, om jag inte vinner pengar, då har jag heller inte lovat att köpa böcker till skolan. Då måste utsagan

TABELL 2. Sanningstabell för implikationen och dess logiskt ekvivalenta former. S betyder sant och F betyder falskt.

P	Q	$P \implies Q$	$\neg(P \wedge \neg Q)$	$\neg Q \implies \neg P$	C	$(P \wedge \neg Q) \implies C$
S	S	S	S	S	F	S
S	F	F	F	F	F	F
F	S	S	S	S	F	S
F	F	S	S	S	F	S

vara sann i det fallet. Men att jag inte vinner pengar hindrar mig ju inte att köpa böcker till skolan ändå, följdaktligen borde utsagan vara sann även i det fallet. Implikationens olika sanningsvärden sammanfattas i Tabell 2.

Vi kan naturligtvis vända på implikationen, om P och Q är utsagor och $P \implies Q$ då säger vi att dess *omvändning* är $Q \implies P$. Omvändningen för en implikation är inte nödvändigtvis logiskt ekvivalent med implikationen. Ett exempel får illustrera.

Exempel 2.8. Låt P vara utsagan "vi är i Stockholm" och Q vara utsagan "vi är i Sverige". Då blir $P \implies Q$ utsagan "om vi är i Stockholm, då är vi i Sverige". Dess omvändning $Q \implies P$, "om vi är i Sverige, då är vi i Stockholm", är däremot inte sann eftersom att vi skulle kunna vara i exempelvis Sundsvall, Göteborg eller Kiruna som också är städer i Sverige.

Om vi däremot tittar på utsagan $\neg Q \implies \neg P$, det vill säga "om inte vi är i Sverige, då är vi inte i Stockholm". Denna kallas för den *kontrapositiva* utsagan.

Om $P \implies Q$ och $Q \implies P$ båda skulle vara sanna, då skriver vi detta som $P \iff Q$. Utsagan $P \iff Q$ kallas för *dubbelimplikation* eller *ekvivalens* och är sann då P och Q båda är sanna och då de båda är falska. Den utläses som P *om och endast om* Q.

Vi ska nu avsluta med en viktig logisk ekvivalens till implikationen. Denna ligger till grund för motsägelsebevis. Utsagan $(P \wedge \neg Q) \implies C$, där C är en motsägelse och därmed alltid är falsk, är logiskt ekvivalent med $P \implies Q$. Detta ses tydligast i en sanningstabell, och den är given i Tabell 2 tillsammans med implikationen och dess kontrapositiva utsaga. Implikationen $P \implies Q$ är bara falsk när P är sann och Q är falsk. Konjunktionen $P \wedge \neg Q$ är sann endast när P är sann och Q är falsk. Om C alltid är falsk, då kommer $P \wedge \neg Q \implies C$ att vara falsk endast när $P \wedge \neg Q$ är sann. Men det är ju precis när P är sann och Q är falsk, det vill säga när $P \implies Q$ är falsk. Följdaktligen måste de vara logiskt ekvivalenta.

2.2. Axiom

FÖR ATT DET ska kunna gå att härleda någonting måste det finnas några grundläggande utsagor som en grund att bygga på. Dessa utsagor kallar vi för *axiom*, och de är från dessa alla matematiska härledningar utgår. Vi har också definitioner som indirekt kan specificera axiom. Axiomen kan ej härledas eftersom att de utgör startpunkter för all härledning.

Vi har ovan redan sett några axiom, nämligen de logiska axiomen. Vi var dock inte tydliga med detta eftersom att vi inte visste vad ett axiom var. Vi ska i kommande kapitel ta upp de matematiska axiomen. Det finns axiom som gäller för hela matematiken, dessa är axiomen för mängdläran, och det finns olika axiomuppsättningar inom specifika områden inom matematiken. Axiomen för mängdläran ligger dock på en högre nivå än den som avses för denna text. Vi kommer att nöja oss med en definition av begreppet mängd och sedan utgå

från en annan uppsättning axiom, Peanos axiom för de naturliga talen, som duger för våra ändamål.[1]

2.3. Satser och bevis

GRUNDEN MÅ VARA viktig att stå på, men möjligheten att ta oss vidare till nya resultat – satser – är också av yttersta vikt. Faktum är ju att vi tidigare behövde logiken för att kunna resonera och dra slutsatser, för att kunna bevisa nya resultat. Nya resultat, som är implikationer eller dubbelimplikationer, sammanfattas i något som kallas för *satser*. En sats ges oftast på formen "om dessa villkor P är uppfyllda, då gäller även Q", där P och Q är utsagor. Men en sats kan inte bara presenteras utan vidare, den kräver alltid ett *bevis*. Ett bevis är en logisk härledning som utgår från axiomen och andra tidigare bevisade satser för att visa att om P är sann då måste även Q vara sann precis då.

Satsen är huvudbegreppet, men vi har även andra typer av satser. Vi har *lemman*, som är hjälpsatser. Dessa behöver vi för att visa ett mindre resultat för att beviset för en annan sats inte ska bli onödigt långt. Vi har även *korollarier*, som är följdsatser. Detta är satser som följer mer eller mindre direkt från en annan sats och har därför ett mycket kort bevis.

Vi ska nu titta på några vanliga bevismetoder. När ett bevis genomförs och presenteras brukar detta avslutas med Q.E.D., som är en förkortning för latinets *Quod Erat Demonstrandum* och betyder "vilket skulle visas". Detta är ett arv från tiden då latin var det vetenskapliga språket och mer eller mindre all vetenskaplig kommunikation skedde på latin.

2.3.1. Motexempelbevis. Vi börjar med den enklaste bevismetoden. Om någon skulle påstå att "alla svenskar tycker om surströmming", då räcker det med att vi hittar en svensk som inte tycker om surströmming för att motbevisa påståendet. Det vill säga, vi hittar ett motexempel. Kom ihåg från tidigare att negationen av utsagan "alla svenskar tycker om surströmming" är "det finns åtminstone en svensk som inte tycker om surströmming" och att det är denna utsaga som vi bevisar genom att finna en sådan svensk.

2.3.2. Direkta bevis. Vi låter P och Q vara utsagor. För att hypotesen P ska implicera konklusionen Q måste P vara sann precis när Q är sann. Vi åstadkommer detta genom konstruktionen av en kedja av implikationer

$$P \implies R_1, R_1 \implies R_2, \ldots, R_n \implies Q.$$

Enligt *Lagen om syllogism* måste då $P \implies Q$. Karakteristiskt för denna bevismetod är att det bara är att "räkna på" för att komma fram till konklusionen.

2.3.3. Kontrapositiva bevis. Låt P och Q vara utsagor. Eftersom att vi tidigare, i Tabell 2, sett att den kontrapositiva implikationen $\neg Q \implies \neg P$ är logiskt ekvivalent med $P \implies Q$ kan vi likväl bevisa den kontrapositiva implikationen som $P \implies Q$. Vi vill kunna göra detta för att detta ibland kan vara lättare än att visa att P medför Q.

[1]Faktum är att om mängdlärans axiom används, då härledes Peanos axiom från mängdläran och Peanos axiom blir då satser istället för axiom.

2.3.4. Motsägelsebevis. Motsägelsebeviset och det direkta beviset är kanske de bevismetoder som används flitigast i detta kompendium. Motsägelsebeviset är effektivt och kan ofta vara enklare att använda än att konstruera ett direkt bevis. Metoden använder en logisk ekivalens, precis som föregående metod, nämligen att $(P \wedge \neg Q) \implies C$ är logiskt ekvivalent med $P \implies Q$ när C är en motsägelse. Den säger att vi ska anta vår hypotes P och även anta motsatsen $\neg Q$ till vår önskade konklusion Q. Om dessa antaganden tillsammans leder till en utsaga som alltid är falsk, det vill säga en motsägelse C, då har vi visat att P implicerar Q eftersom att detta är logiskt ekvivalent.

KAPITEL 3

Mängder

MÄNGDER ÄR KANSKE det mest grundläggande begreppet inom matematik. Ja, kanske till och med mer grundläggande än talen. En mängd kan beskrivas som ett matematiskt objekt som är en samling av andra matematiska objekt. Med andra ord, en mängd kan ses som en abstrakt påse som vi kan stoppa matematiska saker i. Och likt en påse som kan innehålla andra påsar kan även en mängd innehålla andra mängder.

I slutet av 1800-talet tillkom mängdläran till matematiken. Äran för denna upptäkt tilldelas Georg Cantor (1845-1918). Cantor är också utan tvekan den som bidragit mest till utvecklingen av mängdteorin. Under sin livstid gjorde han en uttömmande utforskning av mängder och gav häpnansväckande resultat. Cantor fokuserade sina studier mot oändliga mängder och han fann bland annat att det finns fler än en oändlighet. Heltalen och de reella talen är båda oändligt många, men Cantor visade att de reella talen var fler än de hela talen. År 1877 ställde Cantor upp sin välkända hypotes kallad *Konintuumhypotesen*[1]. Cantors kontiuumhypotes säger följande.

> Det finns ingen mängd vars kardinalitet är strikt mellan dem för heltalen och de reella talen.

Med andra ord, det finns ingen oändlighet större än antalet heltal men mindre än antalet reella tal. Cantor kunde aldrig bevisa sin hypotes och faktum är att den fortfarande står obevisad, ingen har kunnat visa om den är sann eller falsk. År 1963 bevisade Paul Cohen (1934-) med hjälp av ett resultat från 1940 av Kurt Gödel (1906-1978) att Cantors kontinuumhypotes inte går att bevisa eller motbevisa inom mängdteorin själv utan att det krävs ett axiom som antingen godtar eller förkastar den.

3.1. Begreppet mängd

DET ÄR NU DAGS att vi utforskar mängdbegreppet lite mer. Även om Cantors definition av mängd inte längre används är den tillräcklig för våra ändamål. Idag har Cantors definition ersatts av en uppsättning axiom för mängdteorin, kallade Zermelo-Fraenkels axiom efter matematikerna Ernst Zermelo (1871-1953) och Abraham Fraenkel (1891-1965). Dessa är dock onödigt avancerade för den grunda studie som vi ska göra, de behövs dock för många djupare matematiska resultat.

Definition 3.1 (Cantors mängdbegrepp)**.** En *mängd* är en samling av objekt. Objekt som *tillhör* mängden sägs vara *element* i mängden.

En mängd kan ibland också kallas för *samling*.

En mängd anses vara bestämd, eller *väldefinierad*, endast om man för varje objekt kan avgöra om det ingår i mängden eller inte. Vi säger att ett objekt *tillhör* eller *ej tillhör* en mängd. Om M är en mängd och x är ett element i M, då skriver vi detta som $x \in M$. För ett objekt y som ej tillhör mängden M skriver vi $y \notin M$.

[1] *Eng.* continuum hypothesis.

Om vi vill beskriva en mängd kan vi gå tillväga på olika sätt. Vi kan lista mängdens alla element och på så vis säga precis vad som utgör mängden. Detta kan bli problematiskt för mycket stora mängder, vi kan därför nöja oss med en exakt beskrivning av vilka element som tillhör mängden.

Exempel 3.2. Låt M vara en mängd innehållandes elementen A, B och C. Då skriver vi detta som $M = \{A, B, C\}$.

Exempel 3.3. Låt N vara mängden av alla namn kortare än fem bokstäver. Vi kan då skriva

$$N = \{\text{alla namn kortare än fem bokstäver}\}$$

eller

$$N = \{n : n \text{ är ett namn kortare än fem bokstäver}\}$$

som utläses N är mängden av alla n sådana att n är ett namn kortare än fem bokstäver. Denna mängd är väldefinierad för vi kan enkelt avgöra om ett element tillhör mängden eller inte. Om ett objekt ej är ett namn, då tillhör det heller inte mängden. Om ett objekt är ett namn och om det också är kortare än fem bokstäver tillhör det mängden, annars inte.

Exempel 3.4. Den tomma mängden som inte har några element betecknas med $\emptyset$. Vi har följdaktligen att $\emptyset = \{\}$.

Vi kan nu skapa mängder och tala om vilka element de innehåller, men hur kan vi jämföra två mängder? Hur vet vi om två mängder är lika?

Definition 3.5. Vi säger att två mängder A och B är *lika* om varje element i A även tillhör B och varje element i B även tillhör A. Om A och B är lika skriver vi $A = B$, annars skriver vi $A \neq B$.

Övning 3.6. Undersök vad detta innebär, vilka mängder är egentligen lika? Är $\{1, 2, 3\}$ lika med $\{1, 1, 3, 3, 2, 3, 2, 1\}$?

Övning 3.7. I inledning sades att en mängd kan innehålla andra mängder. En mängd X som tillhör en mängd M är då ett element som alla andra i mängden M. Om $X = \{1, 2\}$ och $M = \{X, 2, 3\} = \{\{1, 2\}, 2, 3\}$, vilka av följande utsagor är sanna och vilka är falska: $1 \in M$, $2 \in M$ och $3 \in M$ samt $\{1\} \in M$, $\{2\} \in M$ och $\{1, 2\} \in M$.

Övning 3.8. På hur många sätt kan man egentligen matematiskt beskriva den tomma mängden?

Vi fortsätter med ett annat viktigt begrepp.

Definition 3.9. Två mängder A och B sägs vara *disjunkta* om varje element i A ej är ett element i B.

Övning 3.10. Om A och B är mängder, betyder det samma sak att $A \neq B$ som att A och B är disjunkta?

3.2. Operationer på mängder

Efter att ha tittat på vad en mängd är och hur vi kan avgöra om två mängder är lika ska vi nu titta på hur vi kan skapa nya mängder genom att kombinera mängder som vi redan har.

Definition 3.11. Låt A och B vara mängder. Vi låter mängden $A \cup B$ av alla element i A och alla element i B kallas för *unionen* av A och B. Det vill säga, $A \cup B = \{x : x \in A \text{ eller } x \in B\}$.

Övning 3.12. Utforska unionsbegreppet, finns det några intressanta resultat om detta?

Definition 3.13. Låt A och B vara mängder. Vi låter mängden $A \cap B$ av alla element i A som också tillhör B kallas för *snittet* mellan A och B. Det vill säga, $A \cap B = \{x : x \in A \text{ och } x \in B\}$.

Övning 3.14. Utforska snittbegreppet, finns det några intressanta resultat om detta?

Övning 3.15. Hur förhåller sig union- och snittoperationerna? Exempelvis, spelar det någon roll om vi tar snittet av två unioner eller om vi tar unionen av två snitt?

Definition 3.16. Låt A och B vara mängder. Vi låter mängden $A \setminus B$ av alla element i A som inte tillhör B kallas för *differensen* mellan A och B. Det vill säga, $A \setminus B = \{x : x \in A \text{ och } x \notin B\}$.

Övning 3.17. Finns det några intressanta resultat om differensen? Hur förhåller sig denna operation gentemot operationerna union och snitt?

Definition 3.18. Låt M och N vara mängder. Mängden $\{(m, n) : m \in M \text{ och } n \in N\}$ av alla ordnade par med första element i M och andra element i N kallas för den *kartesiska produkten* av M och N och skrivs $M \times N$.

Namnet kartesisk produkt kommer från den franske matematikern och filosofen René Descartes (1596-1650) vars latinska namn var Renatus Cartesius. Descartes matematiska studier gav upphov till denna typ av begrepp och därför är den kartesiska produkten i efterhand uppkallad efter honom.

Övning 3.19. Låt V vara mängden av alla valörer i en kortlek, det vill säga $V = \{2, 3, 4, 5, 6, 7, 8, 9, 10, \text{knekt}, \text{dam}, \text{kung}, \text{ess}\}$. Låt också F vara mängden av färger i en kortlek, det vill säga $F = \{\spadesuit, \clubsuit, \heartsuit, \diamondsuit\}$. Vad blir $F \times V$ och vad skulle denna mängd kunna användas för att representera?

3.3. Delmängder

Härnäst ska vi titta på delar av mängder, eller mängder vars element utgör en del av de element som finns i en annan mängd. Detta är intressant för att det är inte alltid som vi är intresserade av hela mängden, det är inte heller alltid som vi bara är intresserade av enbart ett element. Ibland kan det vara intressantare att titta på en del av elementen i en mängd, och från dessa skapa en ny mängd. Vi ger därför följande definition.

Definition 3.20. Låt A och B vara mängder. Vi säger att A är en *delmängd* av B om varje element i A även tillhör B. Vi skriver detta som $A \subseteq B$ och utläser det som att A *är inkluderad i* B. Vi kan likvärdigt skriva $B \supseteq A$ och utläser detta som att B *inkluderar* A. Om dessutom $A \neq B$ är A en *äkta* eller *proper delmängd* av B och detta skrivs $A \subset B$ respektive $B \supset A$.

Övning 3.21. Vad skulle det innebära om A är en delmängd av B och B är en delmängd av A, det vill säga $A \subseteq B$ och $B \subseteq A$? Är detta ens möjligt? Det är faktiskt så att det är en vanlig bevismetod inom matematiken att först visa $A \subseteq B$ och sedan visa $B \subseteq A$.

Vi fortsätter med en annan definition med koppling till delmängdsbegreppet.

Definition 3.22. Låt A vara en delmängd till mängden B. Vi kallar mängden $A^{\complement} = B \setminus A$ för *komplementet* till A i mängden B.

Övning 3.23. Vad är det för skillnad mellan begreppen komplement och differens?

Exempel 3.24. Låt $M = \{1, 2, 3\}$ och $A = \{1, 2\}$ vara två mängder. Då har vi att $A \subseteq M$, det vill säga A är en delmängd till M, och faktiskt $A \subset M$, det vill säga A är en äkta delmängd till M. Vi har dessutom att komplementet till A är $A^{\complement} = M \setminus A = \{3\}$.

Nu när vi har delmängder till en mängd M, då kan det vara skönt att ha ett enkelt notationssätt för mängden av alla delmängder till M. Denna mängd som innehåller alla delmängder till M som element kallas *potensmängd* och definieras härnäst.

Definition 3.25. Låt M vara en mängd. Vi kallar mängden av alla delmängder till M för *potensmängden* av M. Vi betecknar potensmängden till M som $\mathcal{P}(M)$.

Övning 3.26. Undersök hur potensmängden av en mängd M förhåller sig till mängden M själv.

3.4. Relationer

VI SKA NU titta på hur vi kan upprätta relationer mellan elementen i en mängd. I tidigare avsnitt har vi redan stött på en relation – likheten mellan två mängder.

Definition 3.27. En *binär relation* R på en mängd M är en delmängd till den kartesiska produkten $M \times M$. Om $(x, y) \in M \times M$ tillhör R skriver vi xRy som utläses *x är relaterat till y via R.*

Anmärkning 3.28. Mängden R är följdaktligen en delmängd till den kartesiska produkten $M \times M$.

Enligt denna definition skulle likhetsrelationen mellan mängder vara en relation på mängden av alla mängder och två mängder i denna mängd är relaterade om de uppfyller kraven i Definition 3.5. Vi ska titta på ett mindre abstrakt exempel.

Exempel 3.29. Låt S vara mängden av alla personer som är skrivna på en adress i Sverige. Två personer $p \in S$ och $q \in S$ är relaterade via relationen G om de bor på samma gata. Om p bor på "Gatuvägen 1, 123 45 Kommunen" och q bor på "Gatuvägen 3, 123 45 Kommunen", då gäller att pGq eftersom att båda bor på "Gatuvägen".

Vi kan då också beskriva G på följande vis. Låt V_i vara mängden av alla personer som är skriva på någon väg i. Då är G unionen av $V_i \times V_i$ för alla vägar i i Sverige.

Övning 3.30. Använd mängderna som definieras i Övning 3.19 och definiera en relation för någon dessa. Inspiration: Du kan utgå från ditt favoritkortspel och definiera en eller flera lämpliga relationer mellan kort eller mängder av kort.

3.4.1. Ekvivalensrelation och ekvivalensklass.

Vi ska nu titta på en speciell typ av relation – ekvivalensrelationen. Ekvivalensrelationen har en särskild struktur för hur element är relaterade till varandra. Den har sitt namn från att den påminner om likhetsbegreppet som vi tagit upp tidigare.

Definition 3.31. En binär relation R på en mängd M som uppfyller att

(1) för alla $x \in M$ gäller att xRx (reflexivitet),
(2) för alla $x, y \in M$ gäller att om xRy då gäller även yRx (symmetri),
(3) för alla $x, y, z \in M$ gäller att om xRy och yRz då gäller även att xRz (transitivitet),

kallas för *ekvivalensrelation*.

Övning 3.32. Undersök vilka relationer du känner till som är reflexiva, symmetriska och transitiva, och följdaktligen är ekvivalensrelationer.

En ekvivalensrelation *partitionerar* en mängd M i disjunkta delmängder kallade partitioner. Dessa partitioner utgörs av något som brukar kallas för ekvivalensklasser.

Definition 3.33. Låt R vara en ekvivalensrelation definierad på mängden M. Om a är ett element i M, då kallar vi mängden $\{x \in M : xRa\}$ för *ekvivalensklassen* för a och betecknar denna som $[a]_R$, elementet a sägs vara en *representant* för ekvivalensklassen.

Om det är klart under vilken relation ekvivalensklassen gäller räcker det med att skriva $[a]$ istället för $[a]_R$.

På samma sätt som att det går att skapa en partition genom att införa en ekvivalensrelation på mängden går det också att skapa en ekvivalensrelation på mängden genom att partitionera den.

Exempel 3.34. Låt F vara mängden av alla fåglar. Vi inför en relation A där två fåglar x och y är relaterade via A om de tillhör samma fågelart. Är detta en ekvivalensrelation? Om x är en berguv (*Bubo bubo*), då måste xAx eftersom att x tillhör samma fågelart som sig själv. Således är relationen reflexiv. Om x är en berguv och om xAy, då måste även y vara en berguv och följdaktligen yAx. Relationen är därför symmetrisk. Om x är en berguv och xAy, då måste y vara en berguv. Om dessutom yAz måste z också vara en berguv. Eftersom både x och z är berguvar gäller att xAz. Då är relationen transitiv. Relationen uppfyller kraven för en ekvivalensrelation och måste därför vara en ekvivalensrelation.

Eftersom att relationen A är en ekvivalensrelation innebär det att den partitionerar mängden F av alla fåglar. Varje partition, eller ekvivalensklass, är en mängd av alla fåglar inom samma art. Exempelvis är mängden av alla berguvar en ekvivalensklass.

Mängden av alla ekvivalensklasser hos M under relationen $\sim$ brukar betecknas $M/\sim$ och kallas för *kvotmängden av M och $\sim$*. Om m är ett element i M, då är $[m]_\sim$ ett element i kvotmängden $M/\sim$.

3.5. Avbildningar

Vi ska nu införa ett annat väldigt centralt begrepp inom matematiken. Vi ska titta på avbildningar, eller funktioner som kanske är det mer kända namnet. Funktioner kommer att komma tillbaka senare i kursen. Vi börjar med att definiera vad en funktion är.

Definition 3.35. Låt A och B vara mängder. En *funktion*, eller *avbildning*, $f\colon A \to B$ tilldelar till varje $a \in A$ ett välbestämt $b \in B$. Vi skriver $f(a) = b$ eller $a \mapsto b$ och säger att a *avbildas* på b eller att b är *bilden* av a. Mängden A sägs vara funktionens *definitionsmängd* och mängden B sägs vara funktionens *värdemängd*.

Anmärkning 3.36. Notera att varje funktion $f\colon A \to B$ ger en funktionsgraf G_f som är en delmängd till den kartesiska produkten $A \times B$. Det vill säga, $G_f = \{(a, b) \in A \times B : f(a) = b\}$. Då är $(a, b) \in G_f$ om $f(a) = b$, eller $a \mapsto b$.

Exempel 3.37. Låt $A = \{1, 2, 3\}$ och $B = \{x, y, z\}$ vara mängder. Vi låter $f : A \to B$ vara en funktion från A till B. Vi låter $1 \mapsto x$, $2 \mapsto z$ och $3 \mapsto y$. Vi har då exempelvis att 2 avbildas på $f(2) = z$.

Övning 3.38. Skulle en funktion kunna ses som en relation?

I de flesta fall är det inte lämpligt att lista alla avbildningarna för funktionen, det vill säga ge dess funktionsgraf, som vi gjorde ovan. Istället är det bättre att ge en beskrivning av hur elementen ska avbildas. Vi ska illustrera med två exempel.

Exempel 3.39. Låt M vara mängden av alla människor i Sverige och P vara mängden av alla geografiska platser på jorden. Låt $p\colon M \to P$ vara en avbildning från M till P. Vi avbildar då varje människa i M på den geografiska plats i P där den föddes.

Exempel 3.40. Låt $f\colon M \to M$ vara en avbildning från mängden $M = \{0, 1, 2, 3, \ldots\}$ till sig själv, och låt x avbildas på $f(x) = x + 1$.

Vi ska nu införa en egenskap för avbildningar. Vi vill kunna beskriva en funktion som avbildar element på ett särskilt vis.

Definition 3.41. Låt f vara en funktion från en mängd A till en mängd B. Vi säger att f är *injektiv* om för varje $x \in A$ och $y \in A$ gäller att om $f(x) = f(y)$ då är även $x = y$.

Exempel 3.42. Låt $A = \{1, 2, 3\}$ och $B = \{a, b\}$ vara mängder samt låt f vara en funktion från A till B. Vi låter $f(1) = a$, $f(2) = b$ och $f(3) = b$. Då är f inte injektiv eftersom att $f(2) = f(3)$ men $2 \neq 3$.

Exempel 3.43. Låt $A = \{1, 2\}$ och $B = \{a, b, c\}$ vara mängder samt låt f vara en funktion från A till B. Vi låter $f(1) = a$ och $f(2) = b$. Då är f injektiv eftersom att det för alla element $x \in A$ gäller att om $f(x) = f(y)$ då är $x = y$.

Vi ska införa en till egenskap likt den ovan.

Definition 3.44. Låt f vara en funktion från en mängd A till en mängd B. Vi säger att f är *surjektiv* om det för varje $b \in B$ existerar ett $a \in A$ sådant att $b = f(a)$.

Exempel 3.45. Funktionen f i Exempel 3.42 är surjektiv eftersom att det för varje element $y \in B$ finns ett element i $x \in A$ sådant att $f(x) = y$.

Exempel 3.46. Funktionen f i Exempel 3.43 är ej surjektiv eftersom att det finns ett element i B, nämligen c, sådant att $f(x) \neq c$ för alla $x \in A$.

Definition 3.47. En avbildning som är både injektiv och surjektiv sägs vara *bijektiv*.

3.6. Kardinalitet

Vi kan avgöra om två mängder är lika genom att undersöka om alla element finns med i båda mängderna, om de gör det så är mängderna lika. Om det däremot saknas element kan vi i nuläget inte säga mycket mer än att mängderna är olika. Det kan dock vara intressant att kunna se hur två disjunkta mängder förhåller sig till varandra. Till exempel genom att bestämma hur stora de är.

När vi avgör hur stort någonting är, med avseende på antal, brukar vi räkna antalet objekt. Om vi exempelvis skulle avgöra hur många personer vi ser just nu börjar vi med att peka på en person och säga *ett*, peka på en annan person och säga *två*, och så vidare tills att vi har pekat på samtliga personer vi kan se. Det vi egentligen gör när vi räknar på detta vis är att upprätta en avbildning från talen $1, 2, 3, \ldots$ till objekten vi räknar. Vi kan utifrån denna idé definiera storleken för mängder, kallad en mängds *kardinalitet*, på följande vis.

Definition 3.48. Om A och B är mängder säger vi att de har samma *kardinalitet* om det finns en bijektiv avbildning mellan A och B. Vi skriver då att $\operatorname{card} A = \operatorname{card} B$. Om A har samma kardinalitet som mängden $\{1, 2, 3, \ldots, n\}$ för något heltal n skriver vi $\operatorname{card} A = n$. Den tomma mängden $\emptyset$ har kardinalitet $\operatorname{card} \emptyset = 0$.

Exempel 3.49. Mängderna $M = \{a, b, c\}$ och $N = \{1, 2, 3\}$ har samma kardinalitet, nämligen 3. Detta eftersom att avbildningen $f\colon M \to N$ sådan att $f(a) = 1$, $f(b) = 2$ och $f(c) = 3$ är bijektiv.

Anledningen till att vi definierar kardinalitet på detta vis och inte nöjer oss med att bara räkna elementen i mängden är för att det inte längre går att räkna elementen när mängderna blir oändligt stora. Men trots att de är oändligt stora vill vi fortfarande kunna jämföra dem. Det var just detta som Cantor gjorde, och vi har redan i inledningen nämnt några av de resultat som han kom fram till.

KAPITEL 4

De naturliga talen

DE NATURLIGA TALEN är de tal som vi använder för att ordna och räkna saker. Talen $1, 2, 3, \ldots$ är naturliga tal och det är dessa tal som människan använt längst i historien. Talet noll kom väldigt sent i historien, så sent som på 800-talet i Indien, medan de andra talen använts sedan årtusenden tillbaka i tiden. Vi ska ändå ta med talet 0 bland våra naturliga tal. Mängden av naturliga tal betecknas $\mathbb{N}$, det vill säga $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$. Då dessa tal funnits länge i människans historia har de också betraktats som självklara, självklara att den tyske matematikern Leopold Kronecker (1823-1891) sade "Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk", på svenska "Den käre Gud har skapat de hela talen, allt annat är människans verk."

Under 1800-talet blev dock matematikerna uppmärksamma på att det behövdes en stadigare grund att bygga matematiken på. Det gick inte längre att anta talen som självklara. Hittills hade de naturliga talen (detta kapitel), heltalen (Kapitel 5) och de reella talen (Kapitel **??**) ansetts vara självklara. Men nu började självklarheten att ifrågasättas.

I detta kompendium kommer grunden att läggas först och sedan fortsätter vi vår väg uppåt. Det vill säga, vi börjar med de naturliga talen och går sedan vidare till de hela talen, de rationella talen och slutligen de reella talen. Att döma av det historiska förloppet grundades matematiken egentligen i omvänd ordning. Det vill säga, de reella talen grundades först. Sedan se rationella talen, de hela talen och sist de naturliga talen. Vi ska nu i kommande avsnitt titta närmare på de axiom som ligger till grund för de naturliga talen.

4.1. Peanos axiom för de naturliga talen

UNDER 1800-TALETS slut och början av 1900-talet grundades de delar av matematiken som redan använts sedan årtusenden tillbaka. De naturliga talen fick sin axiomatiska grund när Richard Dedekind (1831-1916) år 1888 publicerade ett antal axiom för de naturliga talen. Året efter publicerade dock Giuseppe Peano (1858-1932) en förbättring av dessa axiom och det är Peanos förbättrade axiom som godtagits och används idag, om än i lite annorlunda formulering.

Vi ska nu titta på Peanos axiom för de naturliga talen. Börja med att släppa taget om allt du tror dig känna till om matematiken. När du fortsätter efter denna mening ska din "matematikvärld" vara helt tom. Därefter kan du fylla den med axiomen alltefter de presenteras i texten. Vi börjar nu med det första axiomet.

Axiom 4.1. 0 är ett naturligt tal.

Det första axiomet, Axiom 4.1, säger helt enkelt att det finns åtminstone ett naturligt tal. Det säger ingenting mer om 0 än att det är ett naturligt tal och vi vet inte ännu vilka egenskaper som nollan besitter. Detta är allt som nu finns i vår matematikvärld – "noll är ett naturligt tal". Vi går vidare till nästa axiom.

Axiom 4.2. För alla naturliga tal a existerar en efterföljare betecknad $S(a)$ som är ett naturligt tal.

För ett naturligt tal n, låter vi dess efterföljare betecknas med $S(n)$. På samma sätt låter vi $S(S(n))$ beteckna efterföljaren till efterföljaren till n, och så vidare. Notera att vi vet ännu inte vad som menas med en efterföljare. Det enda vi vet är att alla naturliga tal har en efterföljare som är ett naturligt tal. Vi kan därmed fylla upp vår matematikvärld med en lång rad efterföljare och efterföljare till efterföljare och så vidare.

Axiom 4.3. För alla naturliga tal n gäller att 0 inte är dess efterföljare.

Vi kommer att återkomma till de två senaste axiomen. Men låt oss först gå vidare med vad vi menar med likhet och att två naturliga tal är lika. Vi betecknar likhet med tecknet $=$.

Axiom 4.4 (Reflexivitet)**.** För alla naturliga tal n gäller att n är lika med sig själv. Detta betecknas $n = n$.

Vi kan nu också konstatera i vår matematikvärld att $0 = 0$, och vi vet att $S(0) = S(0), S(S(0)) = S(S(0)), \ldots, S(S(\ldots S(0))) = S(S(\ldots S(0)))$.

Axiom 4.5 (Symmetri)**.** För alla naturliga tal a och b gäller att om a är lika med b då är även b lika med a. Det vill säga, om $a = b$ då är $b = a$.

Axiom 4.6 (Transitivitet)**.** För alla naturliga tal a, b och c gäller att om $a = b$ och $b = c$ då är $a = c$.

Axiom 4.7 (Slutenhet under likhet)**.** För alla naturliga tal a gäller att om $a = b$ för något b då måste b också vara ett naturligt tal.

Axiom 4.4, 4.5, 4.6 och 4.7 behandlar begreppet likhet (=). Axiom 4.4 säger att ett naturligt tal måste vara lika med sig självt. Denna egenskap kallas reflexivitet. Axiom 4.5 säger att om ett naturligt tal är lika med ett annat, då måste även omvändningen gälla. Denna egenskap kallas symmetri. Axiom 4.6 säger att om vi får en kedja med likheter, då måste ändarna av kedjorna vara lika. Exempelvis, om $a = b$ och $b = c$ får vi att $a = b = c$ och $a = c$ måste då gälla. Denna egenskap kallas transitivitet. Axiom 4.7 säger att om ett naturligt tal är lika med någonting, då måste detta någonting också vara ett naturligt tal. Denna egenskap kallas slutenhet, hur vi än använder likhet kan vi inte komma utanför de naturliga talen. Vi vet nu hur begreppet likhet och $=$ ska fungera och vad det betyder.

Vi ska nu gå tillbaka till Axiom 4.2 och Axiom 4.3. Vi ska dock först introducera ytterligare ett axiom som vi vill kombinera med dessa två axiom.

Axiom 4.8. För alla naturliga tal a och b gäller att om deras efterföljare är lika måste även a och b vara lika. Det vill säga, om $S(a) = S(b)$ då är $a = b$.

Axiom 4.8 säger att två olika tal kan inte ha samma efterföljare. Detta betyder att vi inte kan få exempelvis grenstruktur eller ”öglor”. Utan strukturen som måste uppstå är en linje där varje naturligt tal är en efterföljare till ett unikt annat naturligt tal – med undantag för noll (0) som enligt Axiom 4.3 inte är efterföljare till något naturligt tal. Axiom 4.2 säger att ett naturligt tals efterföljare alltid är ett naturligt tal och att en sådan alltid existerar. Dessa två axiom säger tillsammans med Axiom 4.8 att det finns oändligt många naturliga tal. Om vi har ett naturligt tal kan vi alltid ta dess efterföljare enligt Axiom 4.2, men oavsett hur många efterföljare vi tar kommer vi enligt Axiom 4.3 aldrig tillbaka dit vi startade vid 0. Vi vet att inget naturligt tal kan ha 0 som efterföljare, men $S(0)$ då? Om vi låter $S(S(0))$ ha $S(0)$ som efterföljare, då får

vi en ögla trots att det inte har 0 som efterföljare. Därför behöver vi Axiom 4.8 som säger att då måste $S(S(0))$ och 0 vara samma naturliga tal – vilket inte är sant och följdaktligen kan vi inte få några öglor.

Vi tittar nu på det sista axiomet.

Axiom 4.9 (Induktionsaxiomet)**.** Låt M vara en samling av objekt sådan att 0 tillhör M och har egenskapen att det för alla naturliga tal n gäller att om n tillhör samlingen M då tillhör även efterföljaren $S(n)$ samlingen M. Då innehåller M alla naturliga tal.

Det sista axiomet, Axiom 4.9, beskriver induktionsprincipen, de naturliga talen i sig och även mängden av alla naturliga tal. Det säger att om 0 tillhör en samling och efterföljaren till varje naturligt tal i samlingen finns med, då innehåller mängden alla naturliga tal. Noll (0) är ett naturligt tal, då finns efterföljaren $S(0)$ också med. Eftersom att efterföljaren $S(0)$ till 0 är ett naturligt tal, då måste även $S(S(0))$ vara med i denna samling. Då säger vi att samlingen måste innehålla alla naturliga tal. Det följer också från detta axiom att alla naturliga tal är på formen $S(S(\dots S(0)))$. Det är detta axiom som ligger till grund för bevismetoden induktion, därav axiomets namn.

Vi ska nu införa några välbekanta symboler.

Definition 4.10. Låt följande symboler beteckna de olika efterföljarna.

$$1 = S(0), \quad 2 = S(1), \quad 3 = S(2), \quad \dots$$

Låt dessutom $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ beteckna mängden av alla naturliga tal.

Anmärkning 4.11. Märk väl att $1, 2$ och 3 enbart utgör symboler för

$$S(0), S(S(0)) \text{ respektive } S(S(S(0))).$$

Vi vet inte hur dessa förhåller sig till varandra genom addition och multiplikation eftersom vi inte vet vad addition och multiplikation är ännu. Vi vet inte ens om dessa objekt som symbolerna representerar går att räkna med ännu. Ännu utgör dessa bara en oordnad ansamling av symboler.

Vi ska nu göra en definition som kommer att förenkla vår notation avsevärt.

Definition 4.12. Om n är ett naturligt tal och $n = S(S(\cdots S(0)))$. Då skriver vi $S^n(0) = n$. Om $n = 0$ skriver vi $S^0(0) = 0$.

4.2. Aritmetik

Ordet aritmetik kommer från grekiskans *ἀριθμός*, som betyder tal, och *ἀριθμητική*, som betyder konsten att räkna. Aritmetiken kan beskrivas som läran om att kombinera tal. De delar av aritmetiken vi ska behandla i detta avsnitt är operationerna addition ($+$) och multiplikation ($\cdot$). Det vill säga, vi ska i detta avsnitt bestämma hur man räknar med de naturliga talen.

Innan vi går vidare till att titta på addition och multiplikation behöver vi en definition.

Definition 4.13. En *binär operation* $\diamond$ på en mängd M är en funktion $\diamond\colon M \times M \to M$ som tar två element x och y i M och parar dessa med ett element $\diamond(x, y)$ i M. Vanligtvis betecknas $\diamond(x, y)$ med $x \diamond y$. Det vill säga, $(x, y) \mapsto x \diamond y$.

4.2.1. Addition. Den första av de aritmetiska operationerna vi ska ta upp är addition. Den definition vi använder oss av i detta kompendium är samma definition som gavs av Peano år 1889. Peanos definition av addition bygger även den på induktionsprincipen och kan därför till en början kanske upplevas lite underlig och svårförståelig, men vi ska diskutera den efteråt.

Definition 4.14 (Summa)**.** För varje par av naturliga tal a och b definieras en *summa* $a+b$ som är ett naturligt tal. Delarna a och b av en summa kallas för summans *termer*. Vi definierar först

$$a+0=a. \tag{4.1}$$

Om summan $a+b$ är definierad låter vi

$$a+S(b)=S(a+b). \tag{4.2}$$

Den första delen av definitionen är tämligen enkel. Allt (4.1) säger är att om vi adderar noll från höger till ett tal så får vi talet självt. Det vill säga, det händer ingenting vid addition med noll från höger. Detta är dock väldigt viktigt, och vi kommer att se varför alldeles strax.

Den andra delen kan upplevas lite svårare. Det (4.2) säger är att ett tal adderat med efterföljaren till ett annat är samma sak som efterföljaren till de båda talens summa. Men hur hjälper det oss? Det visas lättast med ett exempel.

Exempel 4.15. Vi vill finna summan för talen 2 och 3. Alla tal kan skrivas som en kedja av efterföljare till noll, vi vet från Definition 4.10 att $2=S(S(0))$ och $3=S(S(S(0)))$. Om vi skriver summan $2+3$ på formen från (4.2) har vi $2+S(S(S(0)))=S(2+S(S(0)))$. Men då fick vi ett nytt uttryck $2+S(S(0))$ som är på samma form, summan av ett tal och efterföljaren till ett tal. Om vi använder (4.2) igen får vi $S(2+S(S(0)))=S(S(2+S(0)))$. Nu har vi återigen ett uttryck på samma form. Upprepning ger oss $S(S(2+S(0)))=S(S(S(2+0)))$. Nu fick vi dock inte en summa av ett tal och en efterföljare, utan vi fick summan av ett tal och noll. Men vi vet ju från (4.1) att $2+0=2$ och då får vi $S(S(S(2)))$. Det är just detta som gör (4.1) så viktig, förr eller senare kommer vi fram till en summa där ena termen är noll och då måste vi veta vad det är. Utöver detta vi vet också att $2=S(S(0))$, om vi sätter in detta får vi $S(S(S(S(S(0)))))$ som vi enligt definition betecknar med 5. Följdaktligen är $2+3=5$.

Denna typ av återupprepande användning av sig själv kallas för *rekursion*.

Övning 4.16. Visa att om a är ett naturligt tal, då är $a+1=S(a)$.

Övning 4.17. Visa att om a och b är naturliga tal, då är $a+b=S^b(a)$.

Notera att $a+0$ per definition är lika med a, detta säger tyvärr ingenting om $0+a$.

Övning 4.18. Är $0+a$ också lika med a? Bevisa ditt påstående.

Om vi studerar summan ser vi att $+$ är en binär operation på mängden av naturliga tal. Vi kallar denna operation för *addition*.

Definition 4.19 (Addition)**.** Additionsoperatorn $+$ är en funktion $+\colon \mathbb{N}\times\mathbb{N}\to\mathbb{N}$ sådan att varje par av naturliga tal (a,b) avbildas på summan $a+b$, som är ett naturligt tal som vi finner genom Definition 4.14.

4.2.2. Identitetselementet. När vi nu sett nollans speciella betydelse är det dags att ge dess viktiga egenskap ett namn. Detta gör vi i följande definition.

Definition 4.20. Givet en mängd M med en definierad binär operation $\diamond : M\times M\to M$. Ett element e kallas *identitetselement* om det för alla element x i mängden uppfyller att $x\diamond e=e\diamond x=x$.

Exempel 4.21. Det naturliga talet 0 är det additiva identitetselementet för de naturliga talen.

Man kan nu undra varför vi vill ha en sådan definition enbart för nollan? Anledningen är att det finns andra tal bland de naturliga talen som beter precis som nollan, fast för en annan operation än addition. Vi kommer att stöta på ett identitetselement till i nästa avsnitt.

4.2.3. Multiplikation. Multiplikation är den andra aritmetiska operationen vi ska titta på i detta kapitel. Även definitionen av multiplikation är den Peano gav år 1889. Dessutom bygger även den på rekursion, precis som definitionen för addition.

Definition 4.22 (Produkt)**.** För varje par av naturliga tal a och b definierar vi en *produkt* $a \cdot b$ som är ett naturligt tal. Delarna a och b av en produkt kallas för produktens *faktorer*. Vi definierar först

$$a \cdot 0 = 0. \tag{4.3}$$

Om produkten $a \cdot b$ är definierad låter vi

$$a \cdot S(b) = a + (a \cdot b). \tag{4.4}$$

Produkten $a \cdot b$ skrivs vanligen som ab.

Likt summan ger även produkten en binär operation.

Definition 4.23 (Multiplikation)**.** Multiplikationsoperatorn $\cdot$ är en funktion $\cdot \colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ sådan att varje par av naturliga tal (a, b) avbildas på produkten $a \cdot b$, som är ett naturligt tal som vi finner genom Definition 4.22. Denna operation kallar vi för *multiplikation*.

Övning 4.24. Vilket element är identitetselementet för multiplikation av de naturliga talen? Visa att så är fallet.

Övning 4.25. Visa att om a och b är naturliga tal, då är

$$a \cdot b = \underbrace{a + a + \cdots + a}_{b}.$$

Övning 4.26. Visa att $0 \cdot a = 0$. Notera att $a \cdot 0$ per definition är lika med 0, $0 \cdot a = 0$ fordrar dock ett bevis.

4.3. Likhet och olikhet

DET ÄR NU DAGS att introducera ett sätt att jämföra tal som ej är lika. Vi har redan sett likhet, som vi betecknade med $=$ och utläste *är lika med*. Likheter är väldigt intressanta, men det finns många saker som inte är lika. Exempelvis har vi de naturliga talen, de är oändligt många och inget av dem är lika med något annat. Därför definierar vi här en annan relation på de naturliga talen.

Definition 4.27 (Olikhet)**.** Låt a och b vara naturliga tal. Då säger vi att a är *mindre än eller lika med* b om det finns ett naturligt tal n sådant att $a + n = b$, vi skriver detta som $a \leq b$. Vi kan också säga att b är *större än eller lika med* a och beteckna detta genom $b \geq a$. Om vi ej tillåter n att vara noll, då skriver vi $a < b$ respektive $b > a$. Vi utläser dessa som a är *strikt mindre än* b respektive b är *strikt större än* a.

Exempel 4.28. Vi kan nu säga att $0 < 1 < 2 < 3$ och så vidare. Det vill säga, vi har nu infört en form av ordning av de naturliga talen.

Exempel 4.29. Låt x vara ett naturligt tal sådant att $0 < x$ och $x < 5$, det vill säga $0 < x < 5$. Vi menar då att x kan vara något av talen $1, 2, 3$ eller 4.

Övning 4.30. Är $<$, $\leq$, $>$ och $\geq$ relationer?

4.4. Additionens algebraiska egenskaper

ORDET ALGEBRA KOMMER från arabiskans *al-jabr* genom Muhammad ibn Mūsā al-Khwārizmīs (ca. 780-ca. 850) bok *Al-Kitāb al-mukhtaṣar fī ḥīsāb al-ğabr wa'l-muqābala*, på svenska *Den sammanfattande boken om beräkning genom komplettering och balansering*[1]. Ordet *al-jabr* betyder ordagrant *återställande*. Algebra kan beskrivas som matematikens studium av operationer och regler. Vi ska nu titta närmare på hur den aritmetiska operationen addition beter sig.

Innan vi tittar på additionens algebraiska egenskaper behöver vi några hjälpsatser. Vi börjar med en mycket enkel hjälpsats som säger att om man adderar talet ett till ett tal får man dess efterföljare.

Lemma 4.31. *Om a är ett naturligt tal, då är $a+1$ dess efterföljare.*

BEVIS. Om vi tittar på additionen $a+1$ har vi per definition att $a+1 = a+S(0)$. Från (4.2) får vi att $a+S(0) = S(a+0)$. Vi har från (4.1) att $a+0 = a$. Vi får då att

$$a+1 = a+S(0) = S(a+0) = S(a). \tag{4.5}$$

Således är $a+1$ efterföljaren $S(a)$ till a. Q.E.D.

Exempel 4.32. Om vi vidare tittar på additionen $a+2$ har vi att

$$a+2 = a+S(1) = S(a+1).$$

Vi har från Lemma 4.31 att $a+1 = S(a)$ och vi får att

$$a+2 = S(S(a)) = (a+1)+1.$$

Vi kan nu formulera en vidareutveckling av resultatet i exemplet genom följande hjälpsats.

Lemma 4.33. *Om a och n är naturliga tal gäller att*

$$a+n = S^n(a). \tag{4.6}$$

BEVIS. Vi har enligt Definition 4.10 att $n = S^n(0)$. Då har vi att $a+n = a+S^n(0)$. Enligt (4.2) är $a+S^n(0) = S(a+S^{n-1}(0))$, där $n-1$ får beteckna det naturliga tal sådant att $S(n-1) = n$. Men enligt (4.2) är $a+S^{n-1}(0) = S(a+S^{n-2}(0))$, där $n-2$ är det naturliga tal sådant att $S^2(n-2) = n$. Vi har nu att

$$a+n = S(S(a+S^{n-2}(0))) = S^2(a+S^{n-2}(0)).$$

Således har vi $S^k(a+S^{n-k}(0))$ för $k \leq n$. När $k = n$ får vi $S^n(a+S^{n-n}(0)) = S^n(a+0) = S^n(a)$. Q.E.D.

Övning 4.34. Visa att $S^a(S^b(0)) = S^{b+a}(0)$.

Vi kan nu börja titta på vilka egenskaper som addition har. En fråga som vi kan ställa oss, spelar det någon roll i vilken ordning vi adderar? Spelar det någon roll om vi adderar först 1 och 2 och sedan adderar 3? Följande sats besvarar just den frågan.

Sats 4.35 (Associativitet)**.** *Om a, b och c är naturliga tal, då gäller att $a+(b+c) = (a+b)+c$.*

[1]Egen översättning från "The Compendious Book on Calculation by Completion and Balancing".

BEVIS. Vi börjar med att titta på $a+(b+c)$. Enligt Lemma 4.33 har vi att $b+c = S^c(b)$. Enligt Definition 4.10 är $b = S^b(0)$ och vi får att $b+c = S^c(S^b(0))$. Vi har då kvar $a + (b + c) = a + S^c(S^b(0))$. Enligt Lemma 4.33 igen har vi

$$a + S^c(S^b(0)) = S^c(S^b(a)) = S^c(S^b(S^a(0))). \tag{4.7}$$

Vi fortsätter med att kolla på $(a + b) + c$. Då har vi $a + b = S^b(a)$ och således

$$S^b(a) + c = S^c(S^b(a)) = S^c(S^b(S^a(0))). \tag{4.8}$$

Vi ser att (4.7) och (4.8) är lika och således har vi även att

$$a + (b + c) = (a + b) + c.$$

Q.E.D.

Exempel 4.36. Vi vill addera talen $1, 2$ och 3 genom $1 + 2 + 3$. Enligt Sats 4.35 spelar det ingen roll om vi först adderar $1 + 2 = 3$ och sedan adderar 3, det vill säga $3 + 3 = 6$, eller om vi först adderar $2 + 3 = 5$ och sedan adderar $1 + 5 = 6$. Som vi ser är $(1 + 2) + 3 = 3 + 3 = 6$ och $1 + (2 + 3) = 1 + 5 = 6$ båda lika med 6.

Vidare kan vi fråga oss, spelar det någon roll om vi adderar 1 med 2 eller om vi adderar 2 med 1?

Sats 4.37 (Kommutativitet)**.** *Om a och b är naturliga tal, då gäller att $a+b = b + a$.*

BEVIS. Vi har från Lemma 4.33 att $a + b = S^b(a) = S^b(S^a(0))$. Men

$$S^b(S^a(0)) = \underbrace{S(S(S(\cdots(S}_{b}\underbrace{(S(S(S(\cdots(S}_{a}(0)))))))))). \tag{4.9}$$

På samma sätt har vi att $b + a = S^a(b) = S^a(S^b(0))$ och

$$S^a(S^b(0)) = \underbrace{S(S(S(\cdots(S}_{a}\underbrace{(S(S(S(\cdots(S}_{b}(0)))))))))). \tag{4.10}$$

Eftersom att (4.9) och (4.10) är lika måste vi ha $a + b = b + a$. Q.E.D.

Exempel 4.38. Vi vill addera talen 1 och 2. Enligt Sats 4.37 spelar det ingen roll om vi gör detta genom $1 + 2$ eller $2 + 1$. I båda fallen kommer vi fram till att $1 + 2 = 2 + 1 = 3$.

4.5. Multiplikationens algebraiska egenskaper

PRECIS SOM FÖR addition undrar vi nu hur multiplikation beter sig. Spelar det någon roll i vilken ordning vi multiplicerar naturliga tal? En ytterligare fråga som uppstår nu är dock: hur förhåller sig multiplikation till addition? Vi ska börja med att besvara denna fråga, sedan fortsätter vi med att undersöka associativiteten och kommutativiteten som vi gjorde för addition.

Sats 4.39 (Distributivitet)**.** *Om a, b och c är naturliga tal gäller att $a\cdot(b+c) = a \cdot b + a \cdot c$ och $(a + b) \cdot c = a \cdot c + b \cdot c$.*

BEVIS. Vi har först från Lemma 4.33 att $b + c = S^c(S^b(0))$. Således får vi att $a \cdot (b + c) = a \cdot (S^c(S^b(0)))$. Från Definition 4.23 får vi då att

$$a\cdot(b+c) = a\cdot(S^c(S^b(0))) = \underbrace{a + a + \cdots + a}_{c} + a\cdot S^b(0) = \underbrace{a + a + \cdots + a}_{c} + \underbrace{a + a + \cdots + a}_{b}. \tag{4.11}$$

Om vi tittar på de enskilda delarna av uttrycket längst till höger. Då har vi enligt definitionen för produkten att

$$\begin{aligned}\underbrace{a+a+\cdots+a}_{b} &= \underbrace{a+a+\cdots+a}_{b-1}+a\cdot S(0)\\ &= \underbrace{a+a+\cdots+a}_{b-2}+a\cdot S(1)\\ &= \underbrace{a+a+\cdots+a}_{b-3}+a\cdot S(2)\\ &\vdots\\ &= a\cdot b.\end{aligned}$$

Vi har på samma sätt att

$$\underbrace{a+a+\cdots+a}_{c}=a\cdot c.$$

Om vi använder detta i (4.11) får vi att

$$a\cdot(b+c)=\underbrace{a+a+\cdots+a}_{b}+\underbrace{a+a+\cdots+a}_{c}=a\cdot b+a\cdot c,$$

vilket visar första delen av satsen.

Om vi tittar på $(a+b)\cdot c$ får vi att

$$(a+b)\cdot c=\underbrace{(a+b)+(a+b)+\cdots+(a+b)}_{c}.$$

Eftersom att additionen är associativ och kommutativ kan vi byta plats på termerna och får då

$$\underbrace{(a+b)+(a+b)+\cdots+(a+b)}_{c}=\underbrace{a+a+\cdots+a}_{c}+\underbrace{b+b+\cdots+b}_{c}.$$

På samma sätt som ovan får vi att detta är $a\cdot c+b\cdot c$. Då har vi visat att $(a+b)\cdot c=a\cdot c+b\cdot c$ och vi har visat satsen. Q.E.D.

Övning 4.40. Gäller det också att $a\cdot(b_1+b_2+\cdots+b_n)=a\cdot b_1+a\cdot b_2+\cdots+a\cdot b_n$?

Vi vet nu hur multiplikationen förhåller sig till additionen och kan då gå vidare till att undersöka om multiplikationen har de associativa och kommutativa egenskaperna som additionen har. Vi börjar med associativiteten.

Sats 4.41 (Associativitet)**.** *Om a och b är naturliga tal, då gäller att $a\cdot(b\cdot c)=(a\cdot b)\cdot c$.*

Bevis. Vi tittar först på $a\cdot(b\cdot c)$ och får enligt definitionen för multiplikation att

$$a\cdot(b\cdot c)=a\cdot(\underbrace{b+b+\cdots+b}_{c}).$$

Eftersom att multiplikationen är distributiv (Sats 4.39) får vi att

$$a\cdot(\underbrace{b+b+\cdots+b}_{c})=\underbrace{a\cdot b+a\cdot b+\cdots+a\cdot b}_{c}. \tag{4.12}$$

Vi tittar nu på $(a\cdot b)\cdot c$. Enligt definitionen för multiplikation är

$$(a\cdot b)\cdot c=\underbrace{a\cdot b+a\cdot b+\cdots+a\cdot b}_{c}. \tag{4.13}$$

Eftersom att (4.12) och (4.13) är lika har vi visat satsen. Q.E.D.

Sats 4.42 (Kommutativitet)**.** *Om a och b är naturliga tal, då gäller att $a \cdot b = b \cdot a$.*

BEVIS. Beviset använder induktion. Låt a vara ett naturligt tal. Vi vill visa att $a \cdot b = b \cdot a$ för alla naturliga tal b. För $b = 0$ är det klart att multiplikationen är kommutativ. För $b = 1$ har vi att

$$a \cdot 1 = a + a \cdot 0 = a. \tag{4.14}$$

Vi har också att

$$1 \cdot a = \underbrace{1 + 1 + \cdots + 1}_{a}.$$

Enligt Lemma 4.31 och att additionen är associativ (Sats 4.35) får vi att

$$\underbrace{1 + 1 + \cdots + 1}_{a} = S^a(0) = a. \tag{4.15}$$

Eftersom att (4.14) och (4.15) är lika måste också $a \cdot 1 = 1 \cdot a$.

Antag att multiplikationen är kommutativ för alla b mindre än k. Vi har då att $a \cdot k = k \cdot a$. Vi vill nu visa att då måste multiplikationen vara kommutativ även för $b = k+1$. Eftersom att multiplikation är distributiv över addition (Sats 4.39) har vi att $a \cdot (k+1) = a \cdot k + a \cdot 1$. Vi har redan konstaterat att $a \cdot k = k \cdot a$ och att $a \cdot 1 = 1 \cdot a$, och följdaktligen är $a \cdot (k+1) = a \cdot k + a \cdot 1 = k \cdot a + 1 \cdot a$. Vi har från distributiviteten igen att $k \cdot a + 1 \cdot a = (k+1) \cdot a$. Således är multiplikationen kommutativ även för $b = k + 1$ och den måste därför vara kommutativ för alla naturliga tal. Q.E.D.

Övning 4.43. Vilka likheter finns mellan beviset ovan och induktionsaxiomet för de naturliga talen?

Övning 4.44. Visa att $(a + b)(c + d) = ac + ad + bc + bd$.

4.6. Algebraiska egenskaper för de naturliga talen

DET ÄR NU DAGS att sammanfatta de algebraiska egenskaperna för de naturliga talen. Vi har i tidigare avsnitt visat att de naturliga talen har följande egenskaper.

Algebraiska egenskaper för de naturliga talen. *På mängden $\mathbb{N}$ av hela tal definieras två binära operationer, addition ($+$) och multiplikation ($\cdot$). För addition gäller följande:*

> **Kommutativitet:** $a + b = b + a$ *för alla* $a, b \in \mathbb{N}$.
> **Associtivitet:** $(a + b) + c = a + (b + c)$ *för alla* $a, b, c \in \mathbb{N}$.
> **Additivt identitetselement:** *Det finns ett element* $0 \in \mathbb{N}$ *sådant att för alla* $a \in \mathbb{N}$ *gäller att* $0 + a = a + 0 = a$.

För multiplikation gäller följande:

> **Kommutativitet:** $a \cdot b = b \cdot a$ *för alla* $a, b \in \mathbb{N}$.
> **Associtivitet:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *för alla* $a, b, c \in \mathbb{N}$.
> **Multiplikativt identitetselement:** *Det finns ett element* $1 \in \mathbb{N}$ *sådant att för alla* $a \in \mathbb{N}$ *gäller att* $1 \cdot a = a \cdot 1 = a$.

Utöver detta gäller även

> **Multiplikativ distributivitet över addition:** $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$ *och* $(b + c) \cdot a = (b \cdot a) + (c \cdot a)$ *för alla reella tal* $a, b, c \in \mathbb{N}$.

4.7. Potenser

DET KAN BLI tröttsamt i längden att skriva ut många faktorer i en produkt. För additionen kunde vi istället för att skriva $a+a+\cdots+a$ multiplicera a med antalet a-termer i summan, på så vis behöver vi inte skriva ut alla a-termer utan det räcker med att vi vet vilken term och hur många vi ska addera. Vi vill naturligtvis kunna göra liknande för multiplikation. Istället för att skriva ut alla b-faktorer i en produkt $b \cdot b \cdots b$ räcker det med att vi skriver faktorn och antalet av denna faktor. Då skriver vi produkten $b \cdot b \cdots b$ med n faktorer som a^n. Detta åstadkommer vi med potenser som definieras enligt följande.

Definition 4.45. Låt a och n vara naturliga tal. Låt $a^1 = a^{S(0)} = a$. Om a^n är definierad låter vi $a^{S(n)} = a \cdot a^n$. Vi kallar a^n för en *a-potens* med *exponenten* n.

Anmärkning 4.46. Notera att a^0 ej är definierad för något naturligt tal a. Vi återkommer till detta i Kapitel **??** som handlar om rationella tal.

Exempel 4.47. Vi har produkten $2 \cdot 2 \cdot 2$ som består av tre termer som alla är 2. Vi kan då skriva produkten som en 2-potens, nämligen 2^3. Enligt definitionen är $2^3 = 2 \cdot 2^2 = 2 \cdot 2 \cdot 2^1 = 2 \cdot 2 \cdot 2$.

Exempel 4.48. Talet 72 kan skrivas som produkten $8 \cdot 9 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$. Om vi använder potensform får vi att $72 = 2^3 \cdot 3^2 = 2^3 3^2$.

Exempel 4.49. Talet 4 kan skrivas som en 4-potens, nämligen 4^1. Det kan också skrivas som en 2-potens, nämligen $4 = 2 \cdot 2 = 2^2$.

4.7.1. Några resultat om potenser. Vi ska nu titta på några enkla resultat som följer av vår definition av potenser. En första fråga kan vara, vad händer om vi adderar två potenser?

Exempel 4.50. Vi vill addera potenserna a^n och b^m där a och b är naturliga tal och n och m är naturliga tal skilda från noll. Om vi adderar dem får vi

$$a^n + b^m = \underbrace{a \cdot a \cdots a}_{n} + \underbrace{b \cdot b \cdots b}_{m}.$$

Vi kan inte komma särskilt mycket längre och vi kan konstatera att detta var ett föga intressant resultat.

Om vi istället testar att multiplicera två potenser.

Exempel 4.51. Vi vill multiplicera potenserna a^n och b^m där a och b är naturliga tal och n och m är naturliga tal skilda från noll. Vi får då att

$$a^n \cdot b^m = a^n b^m = \underbrace{a \cdot a \cdots a}_{n} \cdot \underbrace{b \cdot b \cdots b}_{m}.$$

Detta verkar mer lovande, vad händer om $a = b$?

Om $a = b$ får vi att

$$a^n b^m = a^n a^m = \underbrace{a \cdot a \cdots a}_{n} \cdot \underbrace{a \cdot a \cdots a}_{m} = \underbrace{a \cdot a \cdots a}_{n} \cdot a^m = a^{S^n(m)} = a^{n+m}. \quad (4.16)$$

Detta är ett intressant resultat och vi sammanfattar det som följande sats.

Sats 4.52. *Om a, $n \neq 0$ och $m \neq 0$ är naturliga tal, då är $a^n a^m = a^{n+m}$.*

BEVIS. Satsen följer direkt från (4.16). Q.E.D.

Exempel 4.53. Vi vill multiplicera potenserna 2^3 och 2^5. Vi får då enligt Sats 4.52 att

$$2^3 2^5 = 2^{3+5} = 2^8.$$

Om vi kontrollerar ser vi att $2^3 = 8$ multiplicerat med $2^5 = 32$ faktiskt är $2^8 = 256$.

Eftersom att det fungerar att addera exponenterna ter det sig naturligt att fråga om vi även kan multiplicera exponenterna och vad det skulle betyda.

Exempel 4.54. Om $a, n \neq 0$ och $m \neq 0$ är naturliga tal kan vi skapa potensen a^{nm}. Vi vet att

$$nm = \underbrace{n + n + \cdots + n}_{m}$$

och således att

$$a^{nm} = a^{n+n+\cdots+n} = \underbrace{a^n a^n \cdots a^n}_{m}. \tag{4.17}$$

Men vi har nyss definierat potenser för att förenkla skrivandet av sådana produkter. Följdaktligen får vi att

$$a^n a^n \cdots a^n = (a^n)^m. \tag{4.18}$$

Vi sammanfattar resultatet i följande sats.

Sats 4.55. *Låt $a, n \neq 0$ och $m \neq 0$ vara naturliga tal. Då gäller att $(a^n)^m = a^{nm}$.*

Bevis. Satsen följer från Exempel 4.54. Q.E.D.

Vi har nu visat att vi har addition och multiplikation av exponenter. Följande sats visar också att multiplikation av exponenter är distributiv över addition av exponenter.

Sats 4.56. *Om $a, b, n \neq 0$, $m \neq 0$ och $p \neq 0$ är naturliga tal, då är $(a^n b^m)^p = a^{np} b^{mp}$.*

Bevis. Om vi tittar på vad $(a^n b^m)^p$ faktiskt betyder, så finner vi att

$$(a^n b^m)^p = \underbrace{(a^n b^m)(a^n b^m) \cdots (a^n b^m)}_{p}.$$

Eftersom att multiplikation är associativ och kommutativ får vi att

$$\underbrace{(a^n b^m)(a^n b^m) \cdots (a^n b^m)}_{p} = \underbrace{a^n a^n \cdots a^n}_{p} \underbrace{b^m b^m \cdots b^m}_{p} = (a^n)^p (b^m)^p.$$

Vi har från Exempel 4.54 att $(a^n)^p (b^m)^p = a^{np} b^{mp}$. Och därför är $(a^n b^m)^p = a^{np} b^{mp}$. Q.E.D.

Vi avslutar avsnittet med ett exempel som nyttjar de båda satserna.

Exempel 4.57. Vi vill multiplicera 4^3 och 12^2. Vi vet att $4 = 2 \cdot 2$, det vill säga $4 = 2^2$, samt att $12 = 3 \cdot 4 = 3 \cdot 2^2$. Om vi använder detta och tittar på vad vi hade från början, 4^3 är således $(2^2)^3 = 2^{2\cdot 3} = 2^6$. 12^2 blir då $(3 \cdot 2^2)^2$ och således $12^2 = 3^{1\cdot 2} 2^{2\cdot 2} = 3^2 2^4$. Om vi multiplicerar dem får vi

$$(\underbrace{2^6}_{4^3} \cdot \underbrace{3^2 2^4}_{12^2}) = 2^6 2^4 3^2 = 2^{6+4} 3^2 = 2^{10} 3^2.$$

Övning 4.58. Visa att addition av exponenter och multiplikation av exponenter båda är associativa och kommutativa operationer.

4.8. Avslutande reflektion

SOM EN AVSLUTANDE reflektion till detta kapitel ges följande övningsuppgifter. Tanken med dessa övningar är att reflektera över matematikens existens, hur den förhåller sig till verkligheten etc.

Övning 4.59. Diskutera förhållandet mellan matematiken och verkligheten. En inledande fråga i diskussionen kan vara: Grundar sig matematiken i verkligheten eller är den oberoende av verkligheten? Diskutera.

Övning 4.60. a) Om matematiken är oberoende av verkligheten, hur kan den användas för att utforska och förutsäga verkligheten? Och om verkligheten såg annorlunda ut, skulle matematiken se likadan ut?

b) Om matematiken grundar sig i verkligheten, hur kan den användas för att förutsäga verkligheten när den behöver verkligheten för att visas vara sann?

KAPITEL 5

De hela talen

Vi är nu välbekanta med de naturliga talen, $\mathbb{N} = \{0, 1, 2, \ldots\}$. Vi har operationerna addition och multiplikation och vet hur dessa fungerar. I detta kapitel kommer vi att utöka de naturliga talen med avseende på addition.

Om vi adderar två tal a och b får vi ett tredje tal c, vi skriver detta som $a + b = c$. Det finns dock inget sätt att ta oss tillbaka till a, det vill säga det finns inget naturligt tal d sådant att $c + d = a + b + d = a$. Ett annat sätt att säga det på är att det finns inga naturliga tal n och m sådana att deras summa $n+m = 0$ är lika med identitetselementet noll. Detta är dock en väldigt intressant och önskvärd egenskap. Vi ska förtydliga vad vi menar och ge denna egenskap ett namn.

Definition 5.1. Givet en mängd M med en definierad binär operation $\diamond : M \times M \to M$ och ett identitetselement e. Ett element b kallas för *inversen till* ett element a om $a \diamond b = b \diamond a = e$.

Övning 5.2. Utforska inversbegreppet. Frågor att inspirera: I Definition 5.1, är a inversen till något element? Hur många inverser kan ett element ha? Har alla element en invers?

Vi ska i detta kapitel tillföra denna egenskap till additionen för de naturliga talen. Resultatet är vad som kallas de hela talen, och mängden av de hela talen betecknas[1] $\mathbb{Z}$.

5.1. Utökningen av de naturliga talen

Låt oss nu skapa de hela talen. Det enda vi har att tillgå är de naturliga talen, dessa vet vi att de existerar och hur de fungerar. Vi börjar med att låta mängden $M = \mathbb{N} \times \mathbb{N} = \{(a, b) : a \text{ och } b \text{ är naturliga tal}\}$ vara mängden av alla ordnade par av naturliga tal.

Exempel 5.3. Vi har exempelvis att $(1, 2) \in M$ och $(2, 1) \in M$ samt att $(1, 2) \neq (2, 1)$.

Låt oss nu införa en relation $\sim$ på denna mängd. Om (a, b) och (c, d) är ordnade par av naturliga tal, det vill säga element i mängden M, då vill vi att $(a, b) \sim (c, d)$ ska vara sant precis när $a + d = b + c$. Denna relation $\sim$ är faktiskt en ekvivalensrelation. För att visa detta kollar vi att relationen uppfyller axiomen i Definition 3.31 för en ekvivalensrelation. Additionen är kommutativ och eftersom att $a+b = b+a$ har vi $(a, b) \sim (a, b)$, och följdaktligen är den reflexiv. Om $(a, b) \sim (c, d)$ då är $a + d = b + c$ och således

$$\begin{aligned} c + b &= b + c, \\ d + a &= a + d \text{ och} \\ c + b &= d + a. \end{aligned}$$

[1] Anledningen till att de betecknas med $\mathbb{Z}$ är tyskans *Zahlen* som betyder tal.

Den sista ekvationen ger precis $(c,d) \sim (a,b)$. Relationen måste då vara symmetrisk. Om $(a,b) \sim (c,d)$ och $(c,d) \sim (e,f)$, då har vi först att

$$a + d = b + c \tag{5.1}$$

och sedan att

$$c + f = d + e. \tag{5.2}$$

Detta ger

$$a + d + f = b + c + f = b + d + e.$$

Eftersom att additionen är kommutativ får vi $a + f + d = b + e + d$ och följdaktligen att $a + f = b + e$ som betyder att $(a,b) \sim (e,f)$. Eftersom att relationen då även är transitiv är relationen en ekvivalensrelation.

Vi betecknar ekvivalensklasserna på följande sätt: Om (a,b) är ett element i M, då är $[(a,b)] = \{(x,y) \in M : (a,b) \sim (x,y)\}$. Det vill säga, $[(a,b)]$ innehåller alla talpar i M som uppfyller ekvivalensrelationen med talparet (a,b).

Exempel 5.4. Vi har att $(0,0) \sim (1,1)$ eftersom att $0+1 = 0+1$. Följdaktligen har vi $[(0,0)] = [(1,1)]$ och $(1,1) \in [(0,0)]$, men naturligtvis även $(0,0) \in [(0,0)]$.

Anmärkning 5.5. Kom ihåg att det inte spelar någon roll om vi väljer $(0,0)$ eller $(1,1)$ som representant för ekvivalensklassen $[(0,0)] = [(1,1)]$ eftersom att det är samma ekvivalensklass.

Exempel 5.6. Vi har däremot $(0,0) \nsim (1,0)$ eftersom att $0 + 0 \neq 0 + 1$, och följdaktligen $(1,0) \notin [(0,0)]$.

Låt oss nu definiera en binär operation $+$ som vi kallar för addition och en binär operation $\cdot$ som vi kallar för multiplikation på mängden av ekvivalensklasser hos M. Vi låter $[(a,b)]+[(c,d)] = [(a+c, b+d)]$ och $[(a,b)] \cdot [(c,d)] = [(ac+bd, ad+bc)]$. Vi måste dock visa att dessa är väldefinierade. Om $(a,b) \sim (a',b')$ och $(c,d) \sim (c',d')$, då vill vi visa att $(a+c, b+d) \sim (a'+c', b'+d')$. Vi har från $(a,b) \sim (a',b')$ att $a+b' = b+a'$ och från $(c,d) \sim (c',d')$ att $c+d' = d+c'$. Om vi adderar vänsterleden i de båda ekvationerna, då måste detta vara lika med summan av högerleden. Det vill säga, $(a + b') + (c + d') = (b + a') + (d + c')$. Eftersom att additionen är associativ och kommutativ får vi att

$$a + c + b' + d' = b + d + a' + c',$$

och således måste $(a + c, b + d) \sim (a' + c', b' + d')$.

Övning 5.7. Visa att multiplikationen också är väldefinierad.

Exempel 5.8. Om vi adderar $[(1,2)]$ och $[(2,4)]$ får vi

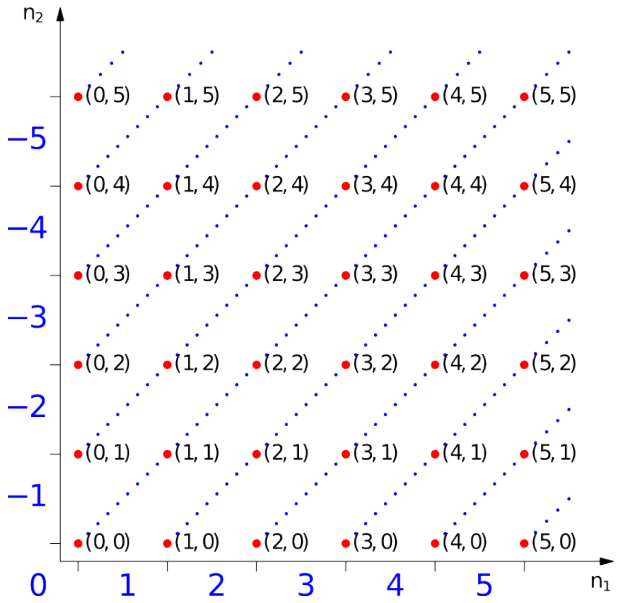
$$[(1,2)] + [(2,4)] = [(1+2, 2+4)] = [(3,6)] = [(0,3)].$$

Exempel 5.9. Om vi multiplicerar $[(1,2)]$ och $[(2,4)]$ får vi

$$[(1,2)] \cdot [(2,4)] = [(1 \cdot 2 + 2 \cdot 4, 1 \cdot 4 + 2 \cdot 2)] = [(10,8)] = [(2,0)].$$

Vi har nu objekt med egenskaperna att de beter sig som de naturliga talen, men vi kan även addera dem för att få identitetselementet. Identitetselementet för addition måste vara ekvivalensklassen $[(0,0)]$. Eftersom att $[(a,b)]+[(0,0)] = [(a+0, b+0)] = [(a,b)]$ och $[(0,0)] + [(a,b)] = [(0+a, 0+b)] = [(a,b)]$ måste $[(0,0)]$ vara identitetselementet för addition.

Övning 5.10. Hur skulle de naturliga talen kunna representeras med dessa objekt?



FIGUR 1. Ekvivalensklasser för par av naturliga tal (n_1, n_2) under relationen $\sim$.

Den additiva inversen till $[(a,b)]$ är $[(b,a)]$ eftersom att $[(a,b)] + [(b,a)] = [(a+b, b+a)] = [(a+b, a+b)]$. Eftersom att $0 + (a+b) = 0 + (a+b)$ har vi enligt ekvivalensrelationen att $(0,0) \sim (a+b, a+b)$ och därför måste de tillhöra samma ekvivalensklass. Detta innebär att $[(a,b)]$ och $[(b,a)]$ måste vara varandras inverser under addition.

Övning 5.11. Kan ett tal ha fler än en invers?

Vi sammanfattar detta avsnitt med följande definitioner. Vi börjar med att definiera vad de hela talen är.

Definition 5.12 (Heltalen)**.** Låt $M = \mathbb{N} \times \mathbb{N}$ vara mängden av alla naturliga talpar och $\sim$ vara ekvivalensrelationen på mängden M sådan att $(a,b) \sim (c,d)$ är uppfylld för elementen (a,b) och (c,d) i M om $a + d = b + c$.

Låt $\mathbb{Z} = M/\sim = \{[(a,b)] : (a,b) \in M\}$ vara mängden av alla ekvivalensklasser för M under ekvivalensrelationen $\sim$. Varje element n i $\mathbb{Z}$ kallar vi ett *heltal*.

Låt också 0 beteckna $[(0,0)] \in \mathbb{Z}$, 1 beteckna $[(1,0)] \in \mathbb{Z}$ och a beteckna $[(a,0)] \in \mathbb{Z}$ för alla naturliga tal a. Beteckna också den additiva inversen $[(0,a)] \in \mathbb{Z}$ till $[(a,0)]$ med $-a$.

De nya beteckningarna och ekvivalensklasserna visas i Figur 1.

När vi nu vet vad ett heltal är kan det vara passande att införa aritmetiska operationer för dem. Vi börjar med additionen, vi tar multiplikationen senare.

Definition 5.13 (Addition)**.** Låt $x = [(a,b)]$ och $y = [(c,d)]$ vara heltal och $+$ en binär operation på $\mathbb{Z}$, kallad *addition*, sådan att $x + y = [(a,b)] + [(c,d)]$ är lika med $[(a+c, b+d)]$.

Övning 5.14. I Exempel 5.8, vilka tal adderades och vilket blev resultatet?

Övning 5.15. I Exempel 5.9, vilka tal multiplicerades och vilket blev resultatet?

Nu när vi kan addera heltal är det lämpligt att vi tittar på hur vi kan jämföra dem annat än med likhet. Olikheter infördes med hjälp av additionen för de naturliga talen, det är inte förvånande att vi gör detsamma för heltalen.

Definition 5.16 (Olikhet)**.** Låt $x = [(a, b)]$ och $y = [(c, d)]$ vara heltal. Vi säger att x *är mindre än* y, betecknat $x < y$, om $a + d < b + c$ enligt relationen $<$ för de naturliga talen. Vi kan också säga att y *är större än* x och skriver då $y > x$. Vi säger att x *är mindre än eller lika med* y om $a + d \leq b + c$, detta betecknas $x \leq y$. Vi kan också säga att y *är större än eller lika med* x och betecknas $y \geq x$.

Nu när vi kan ordna de hela talen är den naturliga efterföljande definitionen denna.

Definition 5.17. Låt oss kalla ett tal mindre än noll för ett *negativt* tal, och låt oss kalla ett tal större än noll för ett *positivt* tal.

Vi har nu infört olika namn för talen på båda sidorna om talet noll. Nu till inverserna.

Definition 5.18. Om $x = [(a, b)]$ är ett heltal, då är $-x = -[(a, b)] = [(b, a)]$ dess *additiva invers*. Denna kallas även för *negationen* av x.

Anmärkning 5.19. Låt a och b vara heltal och $-b$ den additiva inversen till b. Normalt skriver vi $a + (-b)$ som $a - b$ för att spara in på några tecken. Vi benämner $a - b$ som *subtraktionen* av b från a. Ur en matematisk synvinkel är subtraktion inte en egen operation utan vi adderar den additiva inversen för b till a.

Övning 5.20. Visa att ett nollskilt naturligt tal är ett positivt tal.

Övning 5.21. Visa att den additiva inversen för ett nollskilt naturligt tal är ett negativt tal.

Den andra aritmetiska operationen, multiplikation, ger vi i den sista definitionen.

Definition 5.22 (Multiplikation)**.** Låt $x = [(a, b)]$ och $y = [(c, d)]$ vara heltal och $\cdot$ en binär operation på $\mathbb{Z}$, kallad *multiplikation*, sådan att $x \cdot y = [(a, b)] \cdot [(c, d)]$ är lika med $[(ac + bd, ad + bc)]$. Vi skriver ofta xy istället för $x \cdot y$.

Vi ska nu visa ett lemma som vi kommer att behöva i kommande avsnitt. Lemmat talar om att produkten av ett helt tal och noll blir noll.

Lemma 5.23. *För alla heltal* a *gäller att* $a \cdot 0 = 0 \cdot a = 0$.

Bevis. Antag att $a = [(b, c)]$ där b och c är naturliga tal. Vi har per definition att $a \cdot 0 = [(b, c)] \cdot [(0, 0)] = [(b \cdot 0 + c \cdot 0, a \cdot 0 + c \cdot 0)] = [(0, 0)] = 0$. På samma sätt får vi att $0 \cdot a = [(0, 0)] \cdot [(b, c)] = [(0 \cdot b + 0 \cdot c, 0 \cdot c + 0 \cdot b)] = [(0, 0)] = 0$. Q.E.D.

Övning 5.24. Är additionen kommutativ för de hela talen?

Övning 5.25. Är additionen associativ för de hela talen?

Övning 5.26. Är multiplikationen kommutativ för de hela talen?

Övning 5.27. Är multiplikationen associativ för de hela talen?

Övning 5.28. Är multiplikationen distributiv över additionen för de hela talen?

Övning 5.29. De naturliga talens ordning är $0 < 1 < 2 < 3 < \ldots$, enligt relationen $<$ definierad för de naturliga talen. Gäller denna ordning även för relationen $<$ definierad för hela tal? Hur ordnas de hela talen?

5.2. Algebraiska egenskaper för de hela talen

DET ÄR NU DAGS att sammanfatta de algebraiska egenskaperna för de hela talen. De hela talen bygger på de naturliga talen och ska vara en utökning av dessa. Vi hade för avsikt att de hela talen skulle ha samma algebraiska egenskaper som vi visat att de naturliga talen har. Vi fortsätter därför härnäst med en sammanfattning av de algebraiska egenskaper som de hela talen måste ha. Dessa är desamma som för de naturliga talen förutom tillägget om att varje tal a har en additiv invers $-a$.

Algebraiska egenskaper för de hela talen. *På mängden $\mathbb{Z}$ av hela tal definieras två binära operationer, addition $(+)$ och multiplikation $(\cdot)$. För addition gäller följande:*

Kommutativitet: $a+b=b+a$ *för alla* $a,b\in\mathbb{Z}$.
Associtivitet: $(a+b)+c=a+(b+c)$ *för alla* $a,b,c\in\mathbb{Z}$.
Additivt identitetselement: *Det finns ett element* $0\in\mathbb{Z}$ *sådant att för alla* $a\in\mathbb{Z}$ *gäller att* $0+a=a+0=a$.
Additiv invers: *För alla* $a\in\mathbb{Z}$ *finns ett element* $-a\in\mathbb{Z}$ *sådant att* $a+(-a)=(-a)+a=0$.

För multiplikation gäller följande:

Kommutativitet: $a\cdot b=b\cdot a$ *för alla* $a,b\in\mathbb{Z}$.
Associtivitet: $(a\cdot b)\cdot c=a\cdot(b\cdot c)$ *för alla* $a,b,c\in\mathbb{Z}$.
Multiplikativt identitetselement: *Det finns ett element* $1\in\mathbb{Z}$ *sådant att för alla* $a\in\mathbb{Z}$ *gäller att* $1\cdot a=a\cdot 1=a$.

Utöver detta gäller även

Multiplikativ distributivitet över addition: $a\cdot(b+c)=(a\cdot b)+(a\cdot c)$ *och* $(b+c)\cdot a=(b\cdot a)+(c\cdot a)$ *för alla hela tal* $a,b,c\in\mathbb{Z}$.

5.3. Algebraiska egenskaper för de negativa talen

VI ÄR REDAN bekanta med de naturliga talen, och därmed också den delen av de hela talen som motsvarar de naturliga talen. Därför ska vi i detta avsnitt fokusera på de nya talen, de heltal $a<0$ som är mindre än noll – eller de negativa talen.

Låt oss börja med ett av de fundamentala resultaten, nämligen att ett heltal a multiplicerat med -1 ger dess invers $-a$. Vi formulerar detta som en sats.

Sats 5.30. *Låt a vara ett heltal. Då är a multiplicerat med -1 inversen $-a$ till a. Det vill säga, $(-1)\cdot a=-a$.*

BEVIS. Vi har att $1+(-1)=0$. Om vi multiplicerar noll med ett tal får vi enlingt Lemma 5.23 fortfarande noll. Följdaktligen får vi att $a(1+(-1))=0$ eftersom att vi då multiplicerar a med noll. Eftersom att multiplikation är distributiv över addition får vi då att

$$a(1+(-1))=1\cdot a+(-1)a=a+(-1)a=0.$$

Då måste $(-1)a$ vara inversen $-a$ till a. Q.E.D.

Anmärkning 5.31. Notera att detta och följande resultat även kan härledas direkt från talparskonstruktionen i avsnitt 5.1 trots att vi i detta bevis väljer att använda oss av de algebraiska egenskaperna givna i avsnitt 5.2.

Vi fortsätter med kanske det mest häpnanväckande resultatet, som är en följdsats till föregående.

Korollarium 5.32. *Den additiva inversen -1 till heltalet ett multiplicerad med sig själv är ett. Det vill säga $(-1)(-1)=1$.*

BEVIS. Eftersom att -1 är ett heltal följer det från Sats 5.30 att om vi multiplicerar det med -1 får vi dess invers. Inversen för -1 är 1 och således har vi att $(-1)(-1) = 1$. Q.E.D.

Övning 5.33. Om a och b är heltal, gäller då att $(-a)(-b) = ab$ för alla heltal a och b?

Låt oss avsluta med ett exempel om addition av två negativa tal.

Exempel 5.34. Om vi adderar -1 och -1, vad får vi då? Eftersom att vi adderar två lika termer kan vi skriva additionen som multiplikationen $2 \cdot (-1) = (-1) + (-1)$. Vi vet från Sats 5.30 att ett heltal multiplicerat med -1 är dess invers, då får vi $(-1) + (-1) = 2 \cdot (-1) = -2$.

Exempel 5.35. Vi kan också beräkna summan $(-1)+(-1)$ genom att använda heltalens distributiva egenskap. Eftersom att $(-1) = (-1) \cdot 1$ och att multiplikation är distributiv över addition får vi att $(-1) + (-1) = (-1)(1 + 1) = (-1)(2) = -2$.

Övning 5.36. Om a och b är heltal, gäller generellt att $(-a)+(-b) = -(a+b)$?

Övning 5.37. Utred vad $-(a - b)$ egentligen betyder.

5.3.1. Potenser för heltalen. Vi ska nu införa potenser för de hela talen, likt de vi införde för de naturliga talen. Vi definierar potenser enligt följande definition.

Definition 5.38. Låt a vara ett heltal. Vi definierar att $a^1 = a$. Om a^n är definierat för något naturligt tal n, då är $a^{n+1} = a \cdot a^n$. Vi utläser a^n som en *a-potens* med *exponenten n*.

Övning 5.39. Utforska potenser för de hela talen. Finns det några intressanta resultat om dessa potenser?

KAPITEL 6

Talsystem

Vi vet sedan tidigare avsnitt att tal existerar och att det finns olika typer av tal; naturliga tal, hela tal, rationella tal och irrationella tal. Vi vet dessutom att det finns oändligt[1] många tal av varje typ samt att de går att räkna med på olika sätt. Men vad är egentligen ett tal?

Ett tal är inom matematiken ett *abstrakt objekt* som följer givna regler, som vi sett i kapitlen om de naturliga (Kapitel 4) och de hela talen (Kapitel 5). Är då 123 ett tal? Nej, 123 är bara en *representation* av talet vi *benämner* etthundratjugotre. Ett talsystem, eller talbeteckningssystem, tillhandahåller ett entydigt sätt att representera dessa abstrakta tal på. Detta görs genom olika tecken och teckenkombinationer. De tecken vi är vana vid i västkulturerna är siffrorna 0 till 9. Vi behöver här skilja på ett tal och en siffra. Siffror är tecken som används för att representera tal. Det vill säga, talet 123 representeras av sammansättningen av de tre siffrorna $1, 2$ och 3.

Genom historien har det använts många olika talsystem, varav några finns kvar än idag. I Tabell 1 ges några representationer av etthundratjugotre i olika talsystem.

Tabell 1. Olika representationer av etthundratjugotre i olika talsystem.

Binära talsystemet	1111011
Decimala talsystemet	123
Hexadecimala talsystemet	$7B$
Romerska talsystemet	CXXIII

Övning 6.1. Lista alla sätt du känner till att representera tal på.

Övning 6.2. Hitta på ett eget sätt att representera tal på.

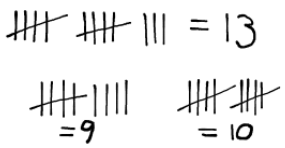
Det talsystem som är vanligast idag är det *decimala talsystemet*, där tecknen som används är siffrorna $0, 1, 2, 3, 4, 5, 6, 7, 8$ och 9.

Anmärkning 6.3. Märk väl skillnaden mellan ett decimalt tal och ett decimaltal. Ett decimalt tal är ett tal representerat med det decimala talsystemet. Ett decimaltal är ett tal med decimalkomma och decimaler, exempelvis 1.2.

Andra vanliga talsystem är det binära, med siffrorna 0 och 1, och det hexadecimala, med 16 olika siffror. Dessa två används flitigt inom datateknik. Det decimala, det binära och det hexadecimala talsystemen är av en speciell typ av talsystem som kallas *positionssystem*. Anledningen till namnet är att en siffras position har betydelse för dess värde.

Exempel 6.4. I 111 betyder den första ettan 100 medan den andra ettan betyder 10 och den sista betyder 1. Det vill säga, samma siffra har olika betydelse beroende på vilken position den har i representationen som den befinner sig i.

[1]Med detta är det inte sagt att de olika mängderna har samma kardinalitet.



FIGUR 1. Tecknen i ett enkelt teckenvärdessystem.

Positionssystemen behandlas i detalj i ett kommande avsnitt.

Det romerska talsystemet är däremot inte ett positionssystem, utan är en modifikation av typen *teckenvärdessystem*. Det romerska systemet behandlas i nästa avsnitt.

6.1. Det romerska talsystemet

DET ROMERSKA TALSYSTEMET är baserat på en modifikation av ett *teckenvärdessystem*. I ett teckenvärdessystem har varje tecken ett speciellt värde. Detta till skillnad från positionssystemet där positionen är avgörande för tecknets värde. I ett mycket enkelt teckenvärdessystem, som används idag, representerar ett streck talet ett, två streck representerar talet två, och så vidare till och med talet fyra. Det vill säga, samma tecken har alltid samma värde och upprepningar adderas tillsammans för att få talet de representerar. Talet fem representeras däremot med fyra streck, som ovan, och ett femte streck snett över de fyra andra strecken. Detta bildar ett nytt tecken även om det är logiskt uppbyggt från tidigare tecken. Systemet består således av två tecken, ett tecken som har värdet ett och ett tecken som har värdet fem. Se Figur 1.

Det romerska systemet är en modifiering av detta system. Tecknen och deras betydelse i det romerska talsystemet ges i Tabell 2.

TABELL 2. De romerska siffrorna.

I	V	X	L	C	D	M
1	5	10	50	100	500	1000

Det romerska talsystemt fungerar nästan på samma sätt som ett teckenvärdessystem. Den väsentliga skillnaden är att i teckenvärdessystemet summeras alla tecknens värden medan det i det romerska systemet även finns subtraktion. I det romerska systemet subtraheras ett tecken av lägre värde som står före ett tecken med högre värde. Exempelvis, IV ger 4 eftersom att en etta står före en femma. VI ger däremot 6 eftersom att tecknens värde summeras. Talen 1-10 ges i Tabell 3 och några andra större tal finns i Tabell 4.

TABELL 3. Talen 1-10 i det decimala och det romerska talsystemen.

Decimala talsystemet	1	2	3	4	5	6	7	8	9	10
Romerska talsystemt	I	II	III	IV	V	VI	VII	VIII	IX	X

Som kan ses i Tabell 4 är det eftersträvansvärt att så få tecken som möjligt används vid subtraktion. Exempelvis kan tänkas att 487 är 500 minus 13 och därför skulle kunna skrivas som XIIID. Det blir dock enklare att se om man istället använder C, eller 100, för subtraktionen av D, eller 500, och sedan lägger till tecknen för 87 som vanligt.

Övning 6.5. Undersök och diskutera hur enkelt det är att räkna med och representera tal med det romerska talsystemet.

2011	MMXI	$1000 + 1000 + 10 + 1$
1999	MCMXCIX	$1000 + (1000 - 100) + (100 - 10) + (10 - 1)$
1998	MCMXCVIII	$1000 + (1000 - 100) + (100 - 10) + 5 + 1 + 1 + 1$
587	DLXXXVII	$500 + 50 + 10 + 10 + 10 + 5 + 1 + 1$
487	CDLXXXVII	$(500 - 100) + 50 + 10 + 10 + 10 + 5 + 1 + 1$

TABELL 4. Några tal skrivna med det romerska talsystemet.

Övning 6.6. Med utgångspunkt i föregående övning, hur tror du att romarna bidragit till matematikhistorien?

Övning 6.7. Hur är det med talet noll och negativa tal i det romerska talsystemet?

6.2. Positionssystem

SOM NÄMNTS TIDIGARE innebär ett positionssystem att samma tecken har olika betydelse eller värde beroende på vilken position tecknet innehar. Systemet har en *talbas*. Det decimala talsystemet har basen 10 och varje position motsvarar en unik 10-potens. Siffran på denna position ger koefficienten för denna potens.

Exempel 6.8. Det decimala talsystemet har basen 10. Talet etthundratjugotre representeras i detta system som 123. Vi har då

$$1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0 = 100 + 20 + 3 = 123.$$

Exempel 6.9. Det binära talsystemet har basen 2. Således representeras talet etthundratjugotre som 1111011. Vi har då

$$1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 123.$$

Exempel 6.10. Om ett positionssystem har basen b används då b antal siffror, dessa har värdena $0, 1, 2, \ldots, b-1$. För att representera ett tal används summor av b-potenser där siffrans position avgör exponenten. Siffrans värde avgör koefficienten för, det vill säga hur många av, den specifika b-potensen som ska adderas. Det vill säga talet vars värde beräknas som

$$d_1 b^{n-1} + d_2 b^{n-1} + \cdots + d_{n-1} b^1 + d_n b^0$$

representeras som $d_1 d_2 \cdots d_n$ i basen b.

Det finns även andra talsystem, exempelvis babyloniernas sexagesimala positionssystem som hade basen 60. Spår av detta kan vi idag se i hur vi räknar tid, att en minut har 60 sekunder och en timme har 60 minuter. Vi använder dock inte 60 olika tecken för att representera våra sekunder och minuter utan tar istället hjälp av det decimala talsystemet. Det babylonska sexagesimalsystemet är det äldsta kända användandet av ett positionssystem och härstammar från Babylonien[2] omkring 3100 f.Kr.

Kan då alla naturliga tal verkligen representeras med en godtycklig bas på detta sätt? Följande sats visar att sådant är fallet.

Sats 6.11. *Låt $b > 1$ vara ett naturligt tal större än ett. För varje naturligt tal $x \in \mathbb{N}$ existerar ett naturligt tal $n > 0$ strikt större än noll och naturliga tal $d_i < b$, där $1 \leq i \leq n$, strikt mindre än b sådana att x kan skrivas som*

$$x = d_1 b^{n-1} + d_2 b^{n-2} + \cdots + d_{n-1} b^1 + d_n b^0.$$

Denna presentation är unik upp till ordningen av termerna.

[2]Babylonien låg i södra delen av Mesopotamien, ungefär i dagens Irak.

För att kunna bevisa detta behöver vi först följande lemma.

Lemma 6.12. *Låt $b > 0$ vara ett naturligt tal större än noll, m och n naturliga tal och $c = c_1b^{n-1} + c_2b^{n-2} + \cdots + c_{n-1}b + c_n$, där $0 < c_1 < b$ och $0 \leq c_i < b$ för $i = 2, 3, \ldots, n$, och $d = d_1b^{m-1} + d_2b^{m-2} + \cdots + d_{m-1}b + d_m$, där $0 < d_1 < b$ och $0 \leq d_j < b$ för $j = 2, 3, \ldots, m$. Då gäller att $c - d = 0$ endast om $n = m$ och $c_i = d_i$ för $i = 1, 2, 3, \ldots, n$.*

BEVIS. Låt oss anta att $n = m + k$ för något naturligt tal k. Vi har då att

$$c - d = c_1b^{n-1} + \cdots + c_{k-1}b^{n-k+1} + (c_k - d_0)b^m + \cdots + (c_n - d_m) = 0.$$

Men $c_1b^{n-1} \neq 0$ och då måste $n = m$.

Då har vi att

$$c - d = (c_1 - d_1)b^{n-1} + \cdots + (c_{n-1} - d_{n-1})b + (c_n - d_n) = 0.$$

Låt oss anta att $c_n - d_n \neq 0$, om inte delar vi med b tills att vi får en nollskild term utan en faktor b. Då får vi att

$$(c_0 - d_0)b^n + \cdots + (c_{n-1} - d_{n-1})b = -(c_n - d_n). \tag{6.1}$$

Eftersom att vänsterledet i (6.1) är delbart med b måste även högerledet vara detta eftersom att de är lika. Men eftersom att $c_i < b$ och $d_i < b$ har vi att $-b < c_i - d_i < b$ för $i = 0, 1, 2, \ldots, n$. Då är $-(c_n - d_n)$ delbar med b endast om $-(c_n - d_n) = 0$, vilket är en motsägelse. Då måste alla termer $c_i - d_i = 0$ för $i = 1, 2, 3, \ldots, n$. Q.E.D.

Nu är vi redo att visa satsen.

BEVIS SATS 6.11. Vi börjar med att visa att summan existerar. Om vi delar x med b får vi en kvot q_1 och en restterm r_1 sådana att $x = q_1b + r_1$ och $0 \leq r_1 < b$. Om vi på samma vis delar q_1 med b får vi en kvot q_2 och en restterm r_2 sådana att $q_1 = q_2b + r_2$ och $0 \leq r_2 < b$. Upprepas detta förfarande får vi att $q_i = q_{i+1}b + r_{i+1}$, $i \in \mathbb{N}$. Från Övning **??** har vi att $q_{i+1} < q_i$ eftersom att $b > 1$. Vi får då från välordningsprincipen för de naturliga talen att $q_n = 0$ för något $n \in \mathbb{N}$. Vi nu sätter ihop dessa resultat enligt följande idé. Vi hade först att $x = q_1b + r_1$, men $q_1 = q_2b + r_2$ och följdaktligen är

$$x = (q_2b + r_2)b + r_1.$$

Eftersom att $q_i = q_{i+1}b + r_{i+1}$ får vi att

$$\begin{aligned} x &= ((((q_nb + r_n)b + r_{n-1})b + \cdots + r_3)b + r_2)b + r_1 \\ &= r_nb^{n-1} + r_{n-1}b^{n-2} + \cdots + r_3b^2 + r_2b^1 + r_1b^0. \end{aligned}$$

Om vi låter $d_1 = r_n, d_2 = r_{n-1}, \ldots, d_{n-1} = r_2, d_n = r_1$ ser vi att vi får en summa på korrekt form.

Antag att det för ett naturligt tal x finns två olika representationer $c_1c_2 \cdots c_n$ och $d_1d_2 \cdots d_m$, båda med basen b. Detta innebär att

$$c_1b^{n-1} + c_2b^{n-2} + \cdots + c_nb^0 = x = d_1b^{m-1} + d_2b^{m-2} + \cdots + d_mb^0.$$

Då måste

$$c_1b^{n-1} + c_2b^{n-2} + \cdots + c_n - d_1b^{m-1} + d_2b^{m-2} + \cdots + d_m = 0,$$

men enligt Lemma 6.12 kan detta ej vara sant och vi har en motsägelse. Då måste det vara samma representation.

Q.E.D.

Övning 6.13. Diskutera innebörden av denna sats och dess bevis.

Exempel 6.14. Det kan nu vara av intresse med ett exempel där representationen ej är unik. Ett tydligt exempel är det romerska talsystemet där 99 skulle kunna representeras av både IC och XCIX. Representationen för tal i det romerska systemet är därmed inte unik.

Eftersom att vi enligt Sats 6.11 kan representera alla naturliga tal i en godtycklig bas $b > 1$ större än ett och att denna representation är unik kan vi med säkerhet definiera ett positionssystem enligt följande.

Definition 6.15 (Positionssystem[3])**.** Ett *positionssystem*, eller positionsvärdesystem, har en *talbas* $b \in \mathbb{N} \setminus \{0, 1\}$, siffrorna $S = \{s \in \mathbb{N} : s < b\}$ och representerar ett tal $x \in \mathbb{N}$ som $d_1 d_2 \cdots d_n$, där $d_i \in S$ är siffran på position i, och

$$x = d_1 b^{n-1} + d_2 b^{n-2} + \ldots + d_{n-1} b^1 + d_n b^0.$$

Exempel 6.16. Det decimala talsystemet har basen $b = 10$ och använder siffrorna $S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.

Exempel 6.17. Det binära talsystemet har basen $b = 2$ och använder siffrorna $S = \{0, 1\}$.

Exempel 6.18. Det hexadecimala talsystemet har basen $b = 16$. När ett talsystem har basen $b > 10$ används vanligtvis bokstäver från alfabetet som siffror för värdena 10, 11 och så vidare. Det hexadecimala talsystemet använder vanligtvis siffrorna

$$S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\},$$

där $A = 10$, $B = 11$, $\ldots$, $F = 15$.

För att kunna urskilja vilken talbas ett tal representeras med brukar basen anges som ett subskript. Exempelvis talet 123 skrivet med det decimala systemet anges som 123_{10}. Det blir då lättare att förstå $123_{10} = 1111011_2$ som betyder att 123 i bas 10 skrivs som 1111011 i bas 2. Vanligtvis, när basen är självklar, brukar den utelämnas. I de första 9 åren i grundskolan är det uteslutande det decimala talsystemet som används och det har därför aldrig varit nödvändigt att där specificera att basen varit 10.

Övning 6.19. Enligt Definition 6.15 används inte talen 0 och 1 som baser, försök att förklara varför.

Övning 6.20. Vidareutveckla Definition 6.15 till att även omfatta rationella tal.

Övning 6.21. Visa att alla rationella tal kan representeras med en godtycklig bas $1 < b \in \mathbb{N}$ enligt den nya definitionen från Övning 6.20.

Övning 6.22. Det rationella talet $\frac{1}{3} = 0.333\ldots$ skrivs som en oändlig decimalutveckling i bas 10. Är det så i alla baser $1 < b \in \mathbb{N}$?

Övning 6.23. Försök att formulera en metod för att byta talbas för ett tal.

6.3. Byte av talbas

Eftersom att Sats 6.11 säger att alla naturliga tal kan representeras i alla baser innebär detta att samma tal har en unik representation i varje bas. Det kan då vara intressant att se ett tals olika representationer i olika baser. Hur detta basbyte går till och att det fungerar framgår av beviset för satsen. Metoden illustreras här med nedan givna exempel.

[3] *Eng.* positional system, place-value system

Exempel 6.24. Talet $123_{10} = 1111011_2$, detta finner vi genom följande:

$$\begin{aligned} 123 &= 61 \cdot 2 + 1 \\ 61 &= 30 \cdot 2 + 1 \\ 30 &= 15 \cdot 2 + 0 \\ 15 &= 7 \cdot 2 + 1 \\ 7 &= 3 \cdot 2 + 1 \\ 3 &= 1 \cdot 2 + 1 \\ 1 &= 0 \cdot 2 + 1 \end{aligned}$$

Då får vi

$$\begin{aligned} &1 + 2 \cdot (1 + 2 \cdot (0 + 2 \cdot (1 + 2 \cdot (1 + 2 \cdot (1 + 2 \cdot (1 + 0)))))) \\ &\quad = 1 \cdot 2^6 + 1 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 \\ &\quad = 1111011_2 = 123_{10}. \end{aligned} \tag{6.2}$$

Exempel 6.25. Talet $123_{10} = 7B_{16}$, detta finner vi genom följande:

$$\begin{aligned} 123 &= 7 \cdot 16 + 11 \\ 7 &= 0 \cdot 16 + 7 \end{aligned}$$

Således får vi siffrorna 7 och B samt att

$$(0 + 7) \cdot 16 + 11 = 7 \cdot 16^1 + 11 \cdot 16^0 = 7B_{16} = 123_{10}.$$

Detta betyder att $7B_{16} = 123_{10}$ och därför är $7B$ hexadecimalt samma tal som 123 är decimalt.

Övning 6.26. Vilket tal representerar 123 när det hexadecimala talsystemet används? Det vill säga, hur representeras 123_{16} med basen 10?

Övning 6.27. Inom datateknik är baserna $2 = 2^1$, $8 = 2^3$ och $16 = 2^4$ väldigt populära, men bas $10 = 2 \cdot 5$ är däremot inte lika populär. Datorns interna representation av tal sker i form av *bitar* som kan anta värdena *på* och *av*, eller 1 och 0. Detta motsvarar precis det binära talsystemet, det vill säga basen $2 = 2^1$, detta förklarar basens popularitet. Försök att förklara varför baserna $8 = 2^3$ och $16 = 2^4$ är populära, medan bas $10 = 2 \cdot 5$ inte är det.

6.4. En additionsalgoritm

POSITIONENS BETYDELSE för siffrornas värde i positionssystemet gör att tal representerade i detta talsystem blir väldigt enkla att räkna med. Vi ska i detta avsnitt undersöka varför.

Vi inleder först med en illustration av algoritmen genom följande exempel.

Exempel 6.28. Vi vill addera talen 123_{10} och 253_{10} i basen 10. Vi skriver dem då ovanför varandra och får då steg `a)` nedan.

```
a)   1 2 3   b)   1 2 3  c)   1 2 3  d)   1 2 3
   + 2 5 3      + 2 5 3     + 2 5 3     + 2 5 3
   -------      -------     -------     -------
                      6         7 6       3 7 6
```

Vi fortsätter genom att addera siffrorna i den sista kolumnen, det vill säga entalen. Vi får då 3 och 3, och totalt har vi 6. Detta tal skriver vi under raden och hamnar då i steg `b)`. Vi fortsätter på samma sätt i stegen `c)` och `d)`. I steg `c)` adderar vi tiotalen och i steg `d)` adderar vi hundratalen. Summan av de två talen är talet som står under raden, det vill säga $123 + 253 = 376$.

Exempel 6.29. Vi vill nu addera talen 123_{10} och 999_{10}, fortfarande i basen 10. Vi gör då som ovan och får steg `a)` nedan.

```
                    1          1 1        1 1 1        1 1 1
a)   1 2 3   b)   1 2 3  c)   1 2 3  d)   1 2 3  e)   1 2 3
   + 9 9 9     + 9 9 9    + 9 9 9    + 9 9 9    + 9 9 9
   -------     -------    -------    -------    -------
                     2        2 2      1 2 2      1 1 2 2
```

Vi fortsätter genom att addera siffrorna i den sista kolumnen, det vill säga entalen 3 och 9, och får då 12. Eftersom att vi får 12 ental innebär detta att vi får ett tiotal och två ental. Tiotal adderas tillsammans med tiotal och vi skriver 1 ovanför kolumnen med tiotal. Vi hamnar då i steg `b)`. I steg `c)` adderar vi kolumnen med talen $1, 2$ och 9, det vill säga alla tiotal. Vi får åter 12 och gör som i steg `b)` eftersom att 12 tiotal innebär att vi har ett hundratal och två tiotal. I steg `c)` när vi adderar $1, 1$ och 9 får vi 11. Detta innebär att vi får ett hundratal och ett tusental. Eftersom att det inte fanns några tusental i de båda termerna skriver vi tusentalet ovanför den tomma kolumnen till vänster, detta visas i steg `d)`. I steg `e)` adderar vi $1, 0$ och 0 och får 1 som skrivs under raden. Då får vi att $123 + 999 = 1122$.

Anmärkning 6.30. Notera att tiotalet ges av kvoten vid heltalsdivision med basen som nämnare, dessutom ges entalet av resten vid denna heltalsdivision.

Vi vill nu titta på det generella fallet med en godtycklig bas $b > 1$. När vi ovan adderar kolumnerna kan vi få ett en- eller tvåsiffrigt tal som resultat. Till exempel när vi i Exempel 6.29 steg `b)` adderar 3 och 9 får vi det tvåsiffriga talet 12. Om $b > 1$ är basen i ett talsystem, $s < b$ och $t < b$ är två siffror i detta talsystem. Då är summan $0 \leq s + t \leq 2(b - 1)$. Om summan $s + t$ är strikt mindre än b följer det av Sats 6.11 att summan är ensiffrig. Följande lemma fastställer att om summan $s + t$ är större än b och mindre än $2(b - 1)$ då är summan exakt tvåsiffrig.

Lemma 6.31. *Ett naturligt tal x i intervallet $b \leq x \leq 2(b - 1)$ kan skrivas som en summa $x = d_1 b^1 + d_2 b^0$, där $1 \leq d_1 \leq b - 1$ och $0 \leq d_2 \leq b - 1$.*

Bevis. Det är klart från Sats 6.11 att x kan skrivas som en summa på formen $d_1 b^{n-1} + \cdots + d_n b^0$ och att denna är unik. Det som återstår att visa är att den består av enbart två termer, det vill säga att $n = 2$.

Om vi tittar på fallet $x = b$ får vi vid heltalsdivision kvoten $x/b = 1$ och resttermen 0. Det vill säga, vi har $d_1 = 1$, $d_2 = 0$ och således $x = 1 \cdot b + 0$. Då måste vi ha minst två termer.

Om vi tittar på fallet $x = 2(b - 1)$ ser vi att $2(b - 1) = b + (b - 2)$. Heltalsdivisionen x/b ger då kvoten $b/b = 1$ och resttermen $b - 2$. Vi har således $d_1 = 1$, $d_2 = b - 2$ och följdaktligen $x = 1 \cdot b + (b - 2)$.

Då har vi exakt två termer. Q.E.D.

Övning 6.32. Diskutera innebörden av detta lemma och dess bevis.

Innan vi går vidare till satsen som visar att denna additionsmetod fungerar måste vi ha lite notation för att underlätta formuleringarna. Låt q_b vara en funktion sådan att den ger kvoten vid heltalsdivisionen t/b och beteckna denna som $q_b(t)$. Låt också r_b vara en funktion sådan att den ger resten vid heltalsdivisionen t/b och beteckna denna som $r_b(t)$. Då har vi att $t = q_b(t) \cdot b + r_b(t)$.

Exempel 6.33. Vi har att $q_5(7) = 7/5 = 1$ och $r_5(7) = 7 - q_5(7) \cdot 5 = 2$.

Exempel 6.34. Vi har att $q_{10}(7) = 7/10 = 0$ och $r_{10}(7) = 7 - q_{10}(7) \cdot 10 = 7$.

Följande sats visar att denna additionsmetod fungerar för godtyckligt långa tal $x = x_1 x_2 \cdots x_n$ och $y = y_1 y_2 \cdots y_m$ representerade i samma talbas $b > 1$.

Sats 6.35 (Additionsalgoritm)**.** *Låt $x = x_1x_2\cdots x_n$ och $y = y_1y_2\cdots y_m$ vara två tal representerade i ett positionssystem med basen $b > 1$, x_i och y_i vara identiskt noll för $i < 1$ och $N = \max\{n, m\}$. Låt också $q_b(t) = t/b$ vara kvoten och $r_b(t)$ vara resten vid heltalsdivisionen t/b. Summan $x+y$ kan då fås genom*

$$\begin{aligned} x + y = {} & q_b(x_{n-N} + y_{m-N})b^N + \\ & \left(r_b(x_{n-N} + y_{m-N}) + q_b(x_{n-N+1} + y_{m-N+1})\right) b^{N-1} + \\ & \left(r_b(x_{n-N+1} + y_{m-N+1}) + q_b(x_{n-N+2} + y_{m-N+2})\right) b^{N-2} + \\ & \cdots + \left(r_b(x_{n-1} + y_{m-1}) + q_b(x_n + y_m)\right) b^1 + r_b(x_n + y_m)b^0. \end{aligned} \tag{6.3}$$

Bevis. Låt oss först antaga att $n = m + k$. Om vi tittar på $x = x_1b^{n-1} + x_2b^{n-2} + \cdots + x_nb^0$ och $y = y_1b^{m-1} + y_2b^{m-2} + \cdots + y_mb^0$ får vi att

$$\begin{aligned} x + y = {} & x_1b^{n-1} + \cdots + x_{k-1}b^{n-k+1} + (x_k + y_1)b^m + \\ & (x_{k+1} + y_2)b^{m-1} + \cdots + (x_{n-1} + y_{m-1})b^1 + (x_n + y_m)b^0 \end{aligned}$$

Vi fortsätter med att titta på en av termerna $(x_{i+k} + y_i)b^{n-k-i}$ och vi ser att $0 \le x_{i+k} + y_i \le b - 2$. Vi har från Lemma 6.31 att om $b \le x_{i+k} + y_i \le 2(b-1)$ är $x_{i+k} + y_i = d_1b + d_2$ med $1 \le d_1 < b$ och $0 \le d_2 < b$ och $x_{i+k} + y_i = d < b$ annars.

Vi tittar på det första fallet. Vi får då att

$$(x_{i+k} + y_i)b^{n-k-i} = (d_1b + d_2)b^{n-k-i} = d_1b^{n-k-i+1} + d_2b^{n-k-i}.$$

Vi har att $q_b(d_1b + d_2) = d_1$ och att $r_b(d_1b + d_2) = d_2$ och således att

$$(x_{i+k} + y_i)b^{n-k-i} = q_b(x_{i+k} + y_i)b^{n-k-i+1} + r_b(x_{i+k} + y_i)b^{n-k-i}.$$

Om $x_{i+k} + y_i < b$ har vi att $q_b(x_{i+k} + y_i) = 0$ och $r_b(x_{i+k} + y_i) = x_{i+k} + y_i$ och då får vi även med det andra fallet.

Vi ser i (6.3) att båda dessa termer finns med. $q_b(x_{i+k} + y_i)$ finns med som en del i $b^{n-k-i+1}$-potensen och $r_b(x_{i+k} + y_i)$ finns med som en del i b^{n-k-i}-potensen.

Vi kan således konstatera att likheten i (6.3) är korrekt. Q.E.D.

Övning 6.36. Diskutera innebörden av denna sats och dess bevis.

Med detta har vi visat att additionsmetoden fungerar för en godtycklig bas $b > 1$ i ett positionssystem. Alla q_b-termerna motsvarar tiotalet som skrivs ovanför vänstervarande kolumn om summan blir för stor. Om summan inte blir för stor blir q_b-termen noll. Alla r_b-termerna motsvarar entalet som alltid skrivs under strecket.

Övning 6.37. Undersök om den välkända multiplikationsalgoritmen, som elever lär sig i den svenska grundskolan, även den fungerar för alla baser $1 < b \in \mathbb{N}$.

Övning 6.38. Bevisa ditt resultat från Övning 6.37.

Litteraturförteckning

Arnlind, Joakim, Ekholm, Tomas, och Enblom, Andreas. Reella tal. URL `http://www.kth.se/sci/institutioner/math/gymnasie/matcirkel/`. 2005.

Bartle, Robert Gardner och Sherbert, Donald R. *Introduction to real analysis*. Wiley, New York, 3 utgåvan, 2000. ISBN 0-471-32148-6.

Greger, Karl. *Matematik. 1, Mängder, funktioner och tal : Lågstadielärarlinjens grundkurs : Mellanstadielärarnas grundkurs*. Almqvist & Wiksell, Stockholm, 1971.

Grillet, Pierre A. *Abstract algebra*. Springer, New York, 2 utgåvan, 2007. ISBN 978-0-387-71567-4 (acid-free paper).

Kiselman, Christer O. och Mouwitz, Lars. *Matematiktermer för skolan*. Nationellt centrum för matematikutbildning (NCM), Göteborgs universitet, Göteborg, 1 utgåvan, 2008. ISBN 978-91-85143-12-2 (inb.).

Kline, Morris. *Mathematical thought from ancient to modern times. Vol. 1*. Oxford Univ. Press, New York, 1990a. ISBN 0-19-506135-7.

Kline, Morris. *Mathematical thought from ancient to modern times. Vol. 3*. Oxford Univ. Press, New York, 1990b. ISBN 0-19-506137-3.

Oxford English Dictionary. The Oxford Dictionary of English Etymology, November 2010. URL `http://www.oed.co.uk`.

Figurer

Tabeller

Sakregister