En Introduktion till

Abstrakt Algebra

Jonathan Nilsson

Senast uppdaterad den 9 mars 2019

Introduktion

Den här texten utgör en kortfattad introduktion till abstrakt algebra. Tanken är främst att texten ska ge perspektiv på mer avancerad matematik med fokus på algebraiska strukturer utan att vi ska behöva gå in för mycket på detaljer. Denna del av kursen blir alltså mer en upptäcksfärd inom algebrans värld, där vi gör lite kortare beräkningar här och där men inte gräver ned oss i så mycket bevis.

Efter en inledande repetition om mängder och funktioner går vi igenom relationer, binära operationer, grupper, ringar, och kroppar. Vi tittar lite djupare på några specifika exempel såsom den symmetriska gruppen, polynomringar, och Gaussiska heltal.

Jag har försökt färgkoda texten: viktiga eller större definitioner skrivs i blå rutor, och exempel i gröna. Ord som definieras är fetstilade. Varje del har också ett antal tillhörande övningsuppgifter.

När jag själv läste min första kurs i algebraiska strukturer kändes det på något vis befriande - man är inte bunden vid de reella talen eller alla deras regler, och man inser att det finns massor av intressanta och användbara nya sätt att räkna på!

Jag hoppas att denna text ska ge samma upplevelse, och att ni tar med er dessa tankar till er egen undervisning.

Kapitel 1

Mängder, funktioner, relationer

1.1 Mängder

Inom grundläggande matematik arbetar man mest med mängder bestående av tal, t.ex.

$\mathbb{N} = \{1, 2, 3, \ldots\}$	Naturliga tal[1]
$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$	Heltal
$\mathbb{Q} = \{\frac{a}{b} \mid a, b \in \mathbb{Z}; b \neq 0\}$	Rationella tal
$\mathbb{R}$ = alla tal med decimalutveckling	Reella tal
$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$	Komplexa tal

En mängd kan dock bestå av vilken sorts objekt som helst, till och med andra mängder. Låt till exempel

$F = \{$  $\}$ $\qquad S = \Big\{\{a, b, c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a\}, \{b\}, \{c\}, \{\}\Big\}.$

Här är F en mängd frukter medan S består av alla delmängder till mängden $\{a, b, c\}$. Observera att S har åtta element, även om var och en av dessa i sig är mängder.

De två mängderna ovan har ändligt många element, och vi har definierat dem genom att lista alla deras element. Man kan dock även definiera mängder med hjälp av villkor, t.ex.

$$P = \{p \in \mathbb{N} \mid p \text{ är ett primtal}\}.$$

Detta är en väldefinierad mängd: varje naturligt tal är antingen ett primtal eller inte, men det är svårare att se om ett givet tal, t.ex. 50587 tillhör mängden P eller inte. Om man inte läst någon talteori är inte ens självklart huruvida P är en ändlig eller oändlig mängd!

Kom ihåg att om x tillhör en mängd M så skriver vi $x \in M$ och kallar x för ett **element** i M. Här följer en lista över annan användbar notation som vi använder för mängder A och B. Vi skriver

$A \subset B$ om A är en **delmängd** av B, d.v.s. $x \in A \Rightarrow x \in B$

$A \cup B$ för **unionen** av A och B: mängden av element som tillhör antingen A eller B (eller båda).

$A \cap B$ för **snittet** av A och B: mängden av element som tillhör både A och B

$A \times B =$ för **produkten** av A och B, alla par av element (a, b) där $a \in A$ och $b \in B$

$A \backslash B$ för mängden av element i A som inte ligger i delmängden B.

[1] Vi kommer att skriva $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$, i vissa böcker kallas denna mängd för de naturliga talen.

1.2 Funktioner

En funktion består av tre delar: en **definitionsmängd** D, en **målmängd** M, och en **regel** som för varje element i D ger ett entydigt element i M. Denna data kan sammanfattas som:

$$f : D \to M \qquad x \mapsto f(x),$$

alltså "f är en funktion från D till M som omvandlar x till $f(x)$".

Inom envariabelsanalys har de flesta funktionerna formen $f : \mathbb{R} \to \mathbb{R}$; de tar ett reellt tal och omvandlar det till ett annat reellt tal. Till exempel har vi studerat kvadreringsfunktionen

$$f : \mathbb{R} \to \mathbb{R} \qquad f : x \mapsto x^2.$$

Regeln $x \mapsto x^2$ skrivs kanske vanligare som $f(x) = x^2$.

Inom linjär algebra och flervariabelanalys studerar man främst funktioner av typen $f : \mathbb{R}^n \to \mathbb{R}^m$, alltså funktioner som tar n stycken reella tal som indata och producerar m stycken reella tal.

Ett exempel är funktionen

$$g : \mathbb{R}^2 \to \mathbb{R}^3, \qquad g(x, y) = (x^2 + y, x - y, e^x).$$

Här har vi till exempel $g(0, 1) = (1, -1, 1)$.

Ett typisk funktion från linjär algebra är

$$T : \mathbb{R}^2 \to \mathbb{R}^2, \qquad T(x, y) = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$$

Till exempel har vi $T(1, 0) = (0, 1)$ och $T(3, 5) = (-5, 3)$.

Reglerna som säger hur vi beräknar funktionsvärdena i funktionerna ovan tar formen av algebraiska uttryck, men så behöver det inte vara. Det räcker att regeln på ett entydigt sätt säger vad funktionsvärdet är. Ta t.ex. funktionen

$$F : \{\text{Mängden av alla djur}\} \to \mathbb{N}_0 \qquad x \mapsto \text{antal ben som } x \text{ har.}$$

Detta är en helt vanlig funktion [2], vi har t.ex.

$$F(\text{katt}) = 4 \qquad F(\text{spindel}) = 8 \qquad F(\text{orm}) = 0.$$

Om definitionsmängden till en funktion är ändlig är det ibland lättast att beskriva alla funktionens värden. Vi har t.ex. en funktion

$G : \{$  $\} \to \{$  $\}$

$G($  $) =$  $\quad G($  $) =$  $\quad G($  $) =$  $\quad G($  $) =$ 

[2] Här kan man i och för sig fråga sig exakt vad definitionen av "djur" och "ben" är, men om vi antar att vi är överens om dessa begrepp så är funktionen väldefinierad.

1.2.1 Injektivitet och surjektivitet

En funktion $f : A \to B$ kallas **injektiv** om $f(x) = f(y)$ endast när $x = y$. Detta är ekvivalent med att säga att $x \neq y \Rightarrow f(x) \neq f(y)$, det vill säga att olika element i A avbildas på olika element i B. Funktionen G ovan är till exempel *inte* injektiv, eftersom både 🍌 och 🍊 avbildas på samma element. Om A är en delmängd till B finns det en naturlig injektiv funktion som avbildar varje element på sig själv, t.ex.

$$h : \{1, 3, 5\} \to \{1, 2, 3, 4, 5\} \text{ där } h(1) = 1, h(3) = 3, h(5) = 5.$$

Här kan man tänka att f "stoppar in" eller "injicerar" mängden A i mängden B, därav namnet injektiv.

En funktion $f : A \to B$ kallas **surjektiv** om $\{f(x) \mid x \in A\} = B$, det vill säga varje element i målmängden B är en bild av något (eller några) element i A. Mängden $\{f(x) | x \in A\}$ kallas **värdemängden** till f och är alltid en delmängd i målmängden. Av funktionerna ovan är G surjektiv men inte h. "Sur" betyder "på" så man kan komma ihåg att en surjektiv funktion avbildar definitionsmängden "på hela målmängden".

En funktion $f : A \to B$ kallas **bijektiv** om f är både injektiv och surjektiv. Detta betyder att f precis parar ihop alla element i A med alla element i B. Prefixet "Bi" betyder två, så man kan komma ihåg innebörden genom att tänka att en bijektiv funktion har "båda två" av egenskaperna injektiv och surjektiv.

En **invers** till en funktion $f : A \to B$ är en annan funktion $g : B \to A$ så att

$$g(f(a)) = a \text{ och } f(g(b)) = b \text{ för alla } a \in A, b \in B.$$

Om vi skriver $\mathrm{id_M}$ för *identitetsfunktionen* $M \to M$ som avbildar varje element på sig själv så kan detta villkor skrivas

$$g \circ f = \mathrm{id}_A \text{ och } f \circ g = \mathrm{id}_B.$$

När detta är fallet skriver vi $g = f^{-1}$ och $f = g^{-1}$ och säger att f och g är varandras inverser. En funktion $f : A \to B$ har en **invers** om och endast om f är bijektiv. Här är ett exempel: Låt $f : \{a, b, c\} \to \{1, 2, 3\}$ där $f(a) = 2$, $f(b) = 3$, och $f(c) = 1$. Funktionen f är då bijektiv. Inversen till f ges av

$$f^{-1} : \{1, 2, 3\} \to \{a, b, c\} \text{ där } f^{-1}(1) = c,\ f^{-1}(2) = a,\ f^{-1}(3) = b.$$

1.3 Relationer

Att förstå relationer kan vara krångligt, så vi börjar med ett konkret exempel. Vi inför en symbol $\sim$ på följande vis: för två naturliga tal $x, y \in \mathbb{N}$ så bestämmer vi att vi skriver $x \sim y$ om x och y har lika många siffror. Då gäller t.ex. $103 \sim 289$ och vi säger att 103 är relaterat till 289 via relationen $\sim$. Vad vi just har gjort är att definiera en **relation** $\sim$ på de naturliga talen $\mathbb{N}$.

Föregående är endast ett exempel, man kan definiera relationer på vilka mängder som helst, och med vilken regel som helst, det enda som krävs är att varje par av element i mängden antingen är relaterade eller inte.

Mer formellt kan man definiera en **relation** på en mängd M som en *delmängd* $R \subset M \times M$. För $x, y \in M$ så skriver vi sedan xRy om och endast om $(x, y) \in R$ och vi säger då att x och y är *relaterade* via R, och annars skriver vi $x \not R y$. Oftast används dock andra symboler för relationer, t.ex. $\sim$. Här är några exempel på relationer.

Låt $M = \{a, b, c\}$ och definiera $R = \{(a, a), (a, c), (b, c), (c, b)\}$. Då har vi alltså aRa, aRc, bRc, och cRb men inga andra element är relaterade. Lägg också märke till att t.ex. $c \not R a$, i relationer spelar det alltså roll vilket element som står på vänster/höger sida om relationstecknet. När M är en ändlig mängd kan man definiera en relation genom att markera vilka element som är relaterade i en tabell. I detta exempel ser denna tabell för relationen R ut så här:

R	a	b	c
a	•		•
b			•
c		•	

I ovanstående exempel listade vi alla element i R, men vi vet ju att mängder även kan beskrivas på mer abstrakta sätt. Ett annat klassiskt exempel på en relation på heltalen $\mathbb{Z}$ är $|$ eller "delar". Här säger vi att "a delar b" och vi skriver $a|b$ om och endast om det finns ett heltal c så att $ac = b$. Vi har t.ex. $3|12$ och $5 \nmid 3$ och $5|0$. Vill man skriva relationen $|$ som en delmängd av $\mathbb{Z} \times \mathbb{Z}$ så har man

$$| = \{(a, ca) | a, c \in \mathbb{Z}\}.$$

Här kommer ytterligare tre exempel på relationer:

Exempel 1.1

- "Är större än" eller ">" är en vanligt förekommande relation på de reella talen $\mathbb{R}$.
- "Är syskon med" är en relation S på mängden människor. Här definierar man aSb om personerna a och b har samma föräldrar.
- Relationen "$\subset$" eller "är en delmängd av" är en relation på mängden av alla mängder [3]. Här definierar man (som bekant) $A \subset B$ när $x \in A \Rightarrow x \in B$.

1.3.1 Ekvivalensrelationer

Låt $\sim$ vara en relation på en mängd M.

Definition 1.1

Vi säger att relationen $\sim$ är

Reflexiv	om $a \sim a$ för alla $a \in M$.
Symmetrisk	om $a \sim b \Rightarrow b \sim a$ för alla $a, b \in M$.
Transitiv	om ($a \sim b$ och $b \sim c$) $\Rightarrow a \sim c$ för alla $a, b, c \in M$.

En relation $\sim$ som har alla dessa tre egenskaper kallas för en **ekvivalensrelation**.

[3] Ett sidospår här är att "mängden av alla mängder" är egentligen inte en mängd, ett klassiskt problem inom mängdläran som belyses i "Russels paradox". Man kan undgå dessa teoretiska problem genom att istället betrakta mängden av alla delmängder till en stor men fix mängd U, ett såkallat "universum".

Exempel 1.2

Relationen >, "större än" är *inte reflexiv*: det är ju exempelvis inte sant att $5 > 5$.
Relationen är *inte symmetrisk* heller: bara för att $3 > 2$ kan man inte dra slutsatsen att den omvända olikheten $2 > 3$ gäller.
Men relationen *är transitiv*: Om $a > b$ och $b > c$ så är också $a > c$.

Exempel 1.3

Relationen "är syskon" är symmetrisk: om A är syskon med B så är ju också B syskon med A. Relationen är också transitiv: om A och B har samma föräldrar och B och C har samma föräldrar så har ju också A och C samma föräldrar. Reflektionen är faktiskt också reflexiv: alla är sykon med sig själv enligt vår definition, eftersom vi definierade att vara syskon som att ha samma föräldrar! Alltså är relationen en ekvivalensrelation.

Ekvivalensrelationer är mycket användbara inom så gott som alla matematiska områden. Att ha en ekvivalensrelation R på en mängd M motsvarar nämligen precis att dela upp M i ett antal "block" där varje block består av element som alla är relaterade till varandra. En sådan uppdelning av M kallas även för en partition.

Definition 1.2

Låt $\sim$ vara en ekvivalensrelation på M. För $x \in M$ definierar vi då

$$[x] = \{m \in M \mid m \sim x\}.$$

Alltså är $[x]$ mängden av alla element som är relaterade till x. Här kallas $[x]$ för **ekvivalensklassen** för x, och x kallas för en **representant** för denna ekvivalensklass. Vi skriver också $M/\sim$ för *mängden av alla ekvivalensklasser*.

Genom att välja representanter $x_1, \ldots, x_n$, en från varje ekvivalensklass har vi alltså $M/\sim = \{[x_1], [x_2], \ldots, [x_n]\}$.

Nu ska vi se ett antal exempel på dessa begrepp. Vi börjar med ett litet exempel.

Exempel 1.4

Tag $M = \{a, b, c\}$ och definierar relationen $\sim$ genom $a \sim a$, $b \sim b$, $c \sim c$, $a \sim b$, och $b \sim a$. Tabellen för relationen blir alltså

$\sim$	a	b	c
a	•	•	
b	•	•	
c			•

Relationen $\sim$ är då reflexiv, symmetrisk, och transitiv så $\sim$ är en ekvivalensrelation. Här ser vi att $[a] = \{a, b\} = [b]$ och $[c] = \{c\}$. Det finns alltså två ekvivalensklasser: $\{a, b\}$ och $\{c\}$. Genom att välja en representatnt i varje ekvivalensklass kan vi då t.ex. skriva $\{a, b, c\}/\sim = \{[a], [c]\}$.

Exempel 1.5

I detta exempel tittar vi på det bekanta begreppet *delbarhet* i termer av relationer. Vi definierar en relation på heltalen $\mathbb{Z}$ så här: definiera $a \sim b$ om och endast om $3|a-b$, alltså om $a-b$ är delbart med 3. Man kan snabbt verifiera att detta är en ekvivalensrelation: reflexivitet $a \sim a$ är ju det samma som $3|a-a$ alltså $3|0$ vilket är sant. Om $a \sim b$ har vi $3|a-b$ betyder ju att $3n = a-b$ för något heltal n, men då gäller ju också $3(-n) = b-a$ så $3|b-a$ också, och vi har $b \sim a$ och vi har visat att $\sim$ är symmetrisk. Slutligen visar vi transitivitet. Låt $a \sim b$ och $b \sim c$ - detta betyder att det finns heltal n och m så att $3n = a-b$ och $3m = b-c$. Adderar vi dessa två ekvationer får vi $3n+3m = a+-b+b-c$, alltså $3(n+m) = a-c$ vilket visar att $3|a-c$ och vi har $a \sim c$. Vi har alltså visat att $\sim$ är en ekvivalensrelation.
Nu undersöker vi ekvivalensklasserna. Vilka element i $\mathbb{Z}$ är ekvivalenta med 0 via relationen $\sim$? Att $a \sim 0$ betyder ju att $3|a$ så vi har

$$[0] = \{3n \mid n \in \mathbb{Z}\} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}.$$

Härnäst undersöker vi vilka tal som är ekvivalenta med 1. $a \sim 1 \Leftrightarrow 3|a-1 \Leftrightarrow 3n = a-1$ för något n alltså $a = 3n+1$ för något n. Vi får alltså

$$[1] = \{3n+1 \mid n \in \mathbb{Z}\} = \{\ldots, -8, -5, -2, 1, 4, 7, 10, \ldots\}.$$

Med liknande argument får vi

$$[2] = \{3n+2 \mid n \in \mathbb{Z}\} = \{\ldots, -7, -4, -1, 2, 5, 8, 11, \ldots\}.$$

Men nu har vi faktiskt hittat alla ekvivalensklasser: varje heltal tillhör någon av ekvivalensklasserna $[0]$, $[1]$, eller $[2]$. Vi drar alltså slutsatsen att $\mathbb{Z}/\sim = \{[0], [1], [2]\}$. Man kan såklart även välja andra representanter för ekvivalensklasserna. Det gäller t.ex. att $[-1] = [2]$ och $[301] = [1]$. I allmännhet är ju $[a] = [b]$ om och endast om $a \sim b$.

Ett annat vanligt exempel kommer från linjär algebra när man definierar begreppet *vektorer* geometriskt. Här definierar man en riktad sträcka som ett par punkter (P, Q) där $P, Q \in \mathbb{R}^n$ och vi tänker oss detta som en sträcka från P till Q. Men här vill vi betrakta två riktade sträckor som lika om de har samma längd och riktning, oberoende av var i rummet de är belägna. Vi definierar därför en relation $\sim$ på mängden riktade sträckor, genom att säga att $(P, Q) \sim (R, S)$ om och endast om $Q - P = R - S$ (koordinatvis subtraktion av element i $\mathbb{R}^n$). Detta är en ekvivalensrelation, och vi kallar ekvivalensklasserna för *vektorer*. Varje vektor är alltså egentligen en ekvivalensklass $[(P, Q)]$ bestående av alla riktade sträckor med samma längd om riktning som den riktade sträckan (P, Q). Oftast ser man annan notation för dessa ekvivalensklasser $[(P, Q)]$, till exempel $\overline{PQ}$.

Exempel 1.6

I detta exempel låter vi A och B vara två mängder. Vi definierar $A \sim B$ om och endast om det finns en bijektion $f : A \to B$. Detta är också en ekvivalensrelation. Om $A \sim B$ säger vi att A och B har samma *kardinalitet*. Ekvivalensklasserna kallas *kardinaltal*. Om A är en ändlig mängd består klassen $[A]$ av alla mängder som har lika många element som A, och man kan identifiera sådana kardinaltal med de naturliga talen. Men det finns även högre kardinaltal. Här finns många användbara och förvånande reslutat [a], det gäller till exempel att

$$[\mathbb{N}] = [\mathbb{Z}] = [\mathbb{Q}] \neq [\mathbb{R}] = [\mathbb{R} \times \mathbb{R}].$$

[a] Om du är nyfiken på denna typ av matematik kan du till exempel söka efter "Hilberts hotell", "Cantors sats", "kontinuumhypotesen", eller "Gödels ofullständighetssatser".

Hur definierar man de rationella talen $\mathbb{Q}$ från heltalen $\mathbb{Z}$? Om endast heltalen finns kan vi inte tala om tal på formen $\frac{a}{b}$ eftersom sådan division är odefinierad, $\frac{3}{5}$ är ju inte ett heltal. Inom abstrakt algebra definierar man därför de rationella talen på följande vis: Låt $M = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \neq 0\}$. Mängden M består alltså av alla heltalspar (a, b) där b inte är 0. Vi ska här tänka på (a, b) som "(a, b)". Vi är dock inte klara här, vi vill ju också att t.ex. $\frac{8}{12}$ och $\frac{2}{3}$ ska representera *samma rationella tal*. Därför inför vi en ekvivalensrelation på M genom att bestämma att $(a, b) \sim (c, d)$ om och endast om $ad = bc$. Därefter definierar vi $\mathbb{Q} = M/\sim$. Formellt sett är alltså varje rationellt tal en klass av heltalspar.

Relationer av typen "Kan omformas till" är en vanlig relation inom matematik. Till exempel är "likformighet" en användbar relation på trianglar, "isotopi" är en relation på knutar, och "homeomorfi" är en relation på topologiska rum. Ett klassiskt exempel är t.ex. att topologer betraktar en kaffemugg och en munk som samma objekt: de tillhör samma ekvivalensklass under relationen "homeomorfi".

Övningsuppgifter

1.1 Låt

$$A = \left\{ \text{🍎}, \text{🍌}, \text{🍉} \right\} \quad \text{och} \quad B = \left\{ \text{🐯}, \text{🐰} \right\}$$

Besvara följande frågor, motivera dina svar!

(a) Finns det några injektiva funktioner $A \to B$?

(b) Finns det några surjektiva funktioner $A \to B$?

(c) Finns det några bijektiva funktioner $A \to B$?

(d) Finns det några funktioner $A \to B$ som är varken injektiva eller surjektiva?

(e) Besvara ovanstående frågor för funktioner $B \to A$.

1.2 Följande övning visar att oändliga mängder ibland kan bete sig kontra-intuitivt!

(a) Ge ett exempel på en funktion $\mathbb{N} \to \mathbb{N}$ som är injektiv men inte surjektiv.

(b) På *Hilbert's hotell* finns det oändligt många rum som är numrerade $1, 2, 3, \ldots$. Du tänker checka in men får höra att det är fullt - alla rum är upptagna. Vad ska hotellvärden meddela de andra gästerna för att göra plats för dig på hotellet utan att slänga ut någon?

(c) Om det kommer oändligt många nya människor till det fulla hotellet, kan man fortfarande checka in alla?

(d) Om det kommer oändligt många bussar, var och en med oändligt många människor, kan man fortfarande checka in alla?

1.3 Vilka av följande relationer är reflexiva? Symmetriska? Transitiva? Ekvivalensrelationer?

(a) Relationen "är halvsyskon" på mängden människor. Vi definierar här alltså $a \sim b$ om a och b har precis en gemensam förälder.

(b) Relationen $\geq$ på $\mathbb{R}$.

(c) Relationen $\parallel$ alltså "är parallell med" på mängden vektorer i planet.

(d) Relationen $\perp$ alltså "är vinkelrät mot" på mängden vektorer i planet.

(e) Relationen "gränsar till" på mängden länder.

(f) Relationen $\subset$ eller "är delmängd av".

1.4 Ge i varje deluppgift ett exempel[4] på en relation som är

(a) Reflexiv men inte symmetrisk.

(b) Symmetrisk men inte reflexiv.

(c) Reflexiv och symmetrisk men inte transitiv.

1.5 Definiera följande relation på planet $\mathbb{R} \times \mathbb{R}$: $(a, b) \sim (c, d)$ om och endast om $a + b = c + d$.

(a) Visa att relationen $\sim$ är en ekvivalensrelation.

(b) Hitta alla element i ekvivalensklassen $[(1, 3)]$. Beskriv alltså alla (x, y) så att $(x, y) \sim (1, 3)$.

(c) Ekvivalensklasserna är delmängder i planet. Hur kan man beskriva de olika ekvivalensklasserna geometriskt?

1.6 En relation $\sim$ på mängden $\{a, b, c\}$ beskrivs av följande tabell

R	a	b	c
a	•		•
b			•
c	•	•	

(a) Är relationen $\sim$ reflexiv?

(b) Är relationen $\sim$ symmetrisk?

(c) Är relationen $\sim$ transitiv?

[4] Om du har problem med att hitta på relationer kan du t.ex. ta mängden $\{a, b, c\}$ och definiera en relation genom att skriva ned en tabell precis som i kapitlet om relationer.

Kapitel 2

Binära operationer och Magma

2.1 Introduktion

De reella talen är bra till mycket. Med deras hjälp kan man mäta avstånd, hastigheter, beräkna räntekostnader, förändringshastigheter och så vidare. I vissa sammanhang behöver man dock räkna på andra sätt.

Vad är klockan är 75893498 timmar till exempel? Adderar vi 24 timmar visar ju klockan samma sak, så i denna situation hade det varit bättre att ha ett talsystem där $24 = 0$. Här kan man utföra beräkningarna i *gruppen* $(\mathbb{Z}_{24}, +)$, mer om detta senare i detta kapitel.

De komplexa talen är ett välbekant talsystem som har många tillämpningar, de är exempelvis speciellt användbara inom signalbehandling, kontrollteori, elektromagnetism, kvantmekanik, och fluidmekanik.

Inom en del av kemin räknar man med en typ av *symmetrigrupper* för att analysera kristaller. Här består varje "tal" av en symmetri, och två sådana symmetrier kan kombineras för att forma nya symmetrier.

Kvaternioner är ett talsystem som påminner om de komplexa talen, fast istället för en imaginär enhet i så har man tre olika, i, j, k. Kvaternionerna kan användas för att beskriva rotationer i rummet och har därför tillämpats för beräkningar inom bland annat flygdynamik, navigation, datorgrafik, och molekylärdynamik.

För att förstå dessa typer av talsystem, eller *algebraiska strukturer* måste man glömma mycket som man tar för givet vid räkning med reella tal.

2.2 Binära operationer

Definition 2.1

En **binär operation** på en mängd M är en funktion $f : M \times M \to M$.

En binär operationen tar alltså två stycken element i M och producerar ett tredje element i M. Man brukar införa en symbol som t.ex. $\star$ för den binära operationen och sedan skriva $a \star b$ istället för $f(a, b)$.

Vanlig addition, subtraktion, och multiplikation är exempel på binära operationer på $\mathbb{R}$. Här kan man också ersätta $\mathbb{R}$ med $\mathbb{Z}$, $\mathbb{Q}$, eller $\mathbb{C}$. Notera dock att vi inte kan definiera operationen "subtraktion" på de naturliga talen $\mathbb{N}$ - en binär operation på $\mathbb{N}$ ska ju för varje par av element i $\mathbb{N}$ ge ett nytt element i $\mathbb{N}$, men vi har t.ex. $3 - 5 \notin \mathbb{N}$.

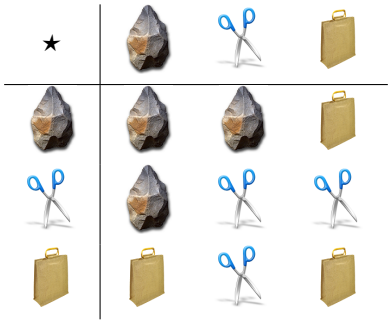
En mängd M tillsammans med en binär operation $\star$ kallas ibland för en **magma**, och vi skriver $(M,\star)$ för magman för att poängtera att den består *både* av en mängd och en binär operation på mängden. Det händer också att man har två olika binära operationer på samma mängd: t.ex. är "heltalen med addition" $(\mathbb{Z},+)$ en annan algebraisk struktur än "heltalen med multiplikation" $(\mathbb{Z},\cdot)$. Man kallar ofta binära operationener för "multiplikation" även om den inte behöver ha något med vanlig multiplikation att göra.

Ett enkelt exempel är "sten-sax-påse magman" nedan. Vår mängd består här av tre element:

$M =$  .

Vi definierar en binär operatinen $\star$ på M genom att bestämma att produkten av två element är vinnaren i sten-sax-påse, t.ex.  . Det kan ju också bli oavgjort, så vi definierar även  och så vidare.

Om mängden M är ändlig kan man precis som med vanlig multiplikation beskriva operationen $\star$ med hjälp av en "multiplikationstabell" här skriver vi elementet $a\star b$ i a's rad och b's kolonn. Så här ser multiplikationstabellen ut för sten-sax-påse-magman:



2.3 Binära operationers egenskaper

Lägg märke till att ett uttryck av formen $a\star b\star c$ saknar entydig betydelse: en binär operation tar ju två element i mängden och producerar ett tredje, så vi kan antingen beräkna $a\star(b\star c)$ *eller* $a\star(b\star c)$ - det kan hända att dessa faktiskt ger olika resultat. Notera t.ex. att i sten-sax-påse magman så har vi

 ,

här blir ju vänsterledet  medan högerledet blir  . Detta är en ganska ovanlig egenskap bland matematiska objekt.

Definition 2.2

En binär operation på M kallas **associativ** om

$$(a\star b)\star c = a\star(b\star c) \text{ för alla } a,b,c\in M.$$

Man säger då också att magman är associativ. I en associativ magma kan man alltså skriva $a \star b \star c$ utan att det blir otydligt eftersom det då inte spelar någon roll var man sätter parenteserna.

Magman $(\mathbb{Z}, +)$ är associativ och vi kan skriva ett uttryck som $1 + 5 + 7$ utan parenteser eftersom $(1 + 5) + 7 = 1 + (5 + 7)$.

Å andra sidan är magman $(\mathbb{Z}, -)$ inte associativ. Ett uttryck av formen $8 - 3 - 2$ saknar entydig betydelse [1] eftersom $3 = (8 - 3) - 2 \neq 8 - (3 - 2) = 7$.

Definition 2.3

En binär operation på M kallas **kommutativ** eller **abelsk**[2]om

$$a \star b = b \star a \text{ för alla } a, b \in M.$$

Sten-sax-påse magman ovan är faktiskt kommutativ. Vi är mest vana att räkna med kommutativa operationer: t.ex. är $(\mathbb{R}, +)$ och $(\mathbb{R}, \cdot)$ kommutativa. Men vi känner också till flera exempel på icke-kommutativa operationer. Subtraktion och division är t.ex. inte kommutativa, och matrismultiplikation från linjär algebra är inte heller kommutativ.

Definition 2.4

Antag att $\star$ är en binär operation på M. Om det finns ett element e i M som uppfyller $e \star x = x = x \star e$ för alla $x \in M$ så kallas e för ett **identitetselement** i $(M, \star)$.

När vi betraktar heltalen med multiplikation $(\mathbb{Z}, \cdot)$ så är heltalet 1 ett identitetselement eftersom $1 \cdot x = x = x \cdot 1$ för alla heltal x.

Om vi istället betraktar heltalen med addition $(\mathbb{Z}, +)$ så är heltalet 0 ett identitetselement eftersom $0 + x = x = x + 0$ för alla heltal x.

Från linjär algebra vet vi att i $(\mathrm{Mat}_{2\times 2}(\mathbb{R}), \cdot)$, alltså mängden av alla reella 2×2-matriser med matrismultiplikation så är $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ ett identitetselement.

Nu tittar vi på en rent abstrakt struktur $(\{$🍏, 🍉, 🍊$\}, \star)$ där $\star$ beskrivs av multiplikationstabellen nedan

★	🍏	🍉	🍊
🍏	🍊	🍏	🍉
🍉	🍏	🍉	🍊
🍊	🍉	🍊	🍏

Här kan vi utläsa från tabellen att 🍉 är ett identitetselement: att multiplicera ett element x med 🍉 ger alltid resultat x.

Sten-sax-påse magman är ett exempel på en algebraisk struktur som inte har något identitetselement.

[1] Det är dock vanligt att man ändå inför *konventioner* för hur uttryck av formen $8 - 3 - 2$ ska beräknas. En dator beräknar exempelvis sådana uttryck från vänster till höger, alltså $(8 - 3) - 2$.

[2] Efter den norska matematikern Niels Henrik Abel (1802-1829) som bland annat studerade denna typ av algebraiska strukturer.

Sats 2.1

Det kan aldrig finnas mer än ett identitets-element i en för en binär operation.

Bevis

Vi gör ett motsägelsebevis. Antag att e och f är olika identitetselement i $(M,\star)$. Då gäller

$$e = f \star e = f,$$

i första likheten använde vi att f är ett identiteselement, och i andra likheten att använde vi att e är ett identitetselement. Alltså är $e = f$ vilket är en motsägelse. Alltså kan det inte finnas mer än ett identitetselement.

Definition 2.5

Antag att e är ett identitetselement i $(M,\star)$, och låt $a \in M$. En **invers** till a är ett element $b \in M$ så att $a \star b = e = b \star a$.

Om b är en invers till a så blir ju automatiskt också a in invers till b enligt definitionen, vi säger att a och b är *varandras inverser*. Oftast använder man notationen a^{-1} för inversen till a, om den binära operationen är relaterad till vanlig addition så skriver man ibland istället $-a$ för inversen till a.

Här följer ett antal exempel.

Exempel 2.1

- I $(\mathbb{Z},+)$ är 0 identitetselement. Inversen av ett heltal a är $-a$ eftersom $a+(-a) = 0$. Varje heltal har alltså en invers under operationen $+$.
- I $(\mathbb{Z},\cdot)$ är 1 identitetselement. Här gäller $1^{-1} = 1$ och $-1^{-1} = -1$, men alla andra heltal saknar inverser under $\cdot$.
- I $(\mathbb{Q},\cdot)$ är 1 identitetselement. Här gäller $(\frac{a}{b})^{-1} = \frac{b}{a}$ eftersom $\frac{a}{b} \cdot \frac{b}{a} = 1$. Detta innebär att alla element utom 0 har en invers i $(\mathbb{Q},\cdot)$.

Precis som man kan prata om identitets-element för en binär operation kan man också prata om *noll-element*. Vi säger att n är ett *noll-element* för en binär operation $*$ på M om $x * n = n$ och $n * x = n$ för alla $x \in M$.

Exempelvis ser vi att 0 är ett noll-element i $(\mathbb{Z},\cdot)$, och noll-matrisen är noll-element i $(\mathrm{Mat}_{2\times 2}(\mathbb{R}),\cdot)$. Å andra sidan är $(\mathbb{Z},+)$ och sten-sax-påse-magman exempel där noll-element inte existerar.

Övningsuppgifter

2.1 I den här övningen ska vi träna på att räkna med abstrakta binära operationer. Betrakta därför sten-sax-påse magman från kaptitlets början.

(a) Beräkna ✂ $\star\big($(✂ $\star$ 👜)$\star$ 🪨$\big)$.

(b) Fundera på vad det det innebär att lösa en ekvation i en magma. Lös därefter ekvationen (✂ $\star X)\star$ 👜 = ✂ .

(c) Visa att man genom att sätta ut parenteser på olika vis i uttrycket

kan få resultatet att bli både  ,  , och  .

(d) Finns det några identitetselement eller nollelement i denna magma?

2.2 Låt M vara mängden av 2×2-matriser där summan i varje rad och kolonn är 1. Med andra ord har vi

$$M = \left\{ \begin{bmatrix} a & 1-a \\ 1-a & a \end{bmatrix} \mid a \in \mathbb{R} \right\}$$

(a) Visa att matrismultiplikation är en binär operation på M. Kontrollera alltså att om $A, B \in M$ så har vi också $A \cdot B \in M$.

(b) Är $(M, \cdot)$ associativ?

(c) Har $(M, \cdot)$ ett identitetselement?

(d) Har varje element i M en invers?

(e) Finns det ett noll-element i $(M, \cdot)$?

2.3 De *utvidgade reella talen* $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, \infty\}$ kan vara användbara när man exempelvis räknar på gränsvärden.

(a) Hur ska man definiera en binär operation $+$ på $\overline{\mathbb{R}}$ så att den överensstämmer med vanlig addition för reella tal, och så att identitetselement och inverser fortfarande finns? Blir operationen kommutativ? Associativ? Finns ett noll-element?

(b) Samma fråga fast för multiplikation på $\overline{\mathbb{R}}$.

(c) Utifrån de binära operationerna du valt i de föregående deluppgifterna, gäller då den "distributiva lagen" $a \cdot (b + c) = a \cdot b + a \cdot c$ i $\overline{\mathbb{R}}$?

2.4 För varje deluppgift nedan, ange om den givna magman är associativ, kommutativ, har identitestelement, ett nollelement, och vilka element som har inverser.

(a) $(\mathbb{R}, \star)$ där $a \star b = ab + 1$.

(b) $(\mathbb{R}, \bullet)$ där $a \bullet b = a^b$.

(c) $(\mathbb{R}, \square)$ där $a \square b = \frac{a+b}{2}$, alltså medelvärdet av a och b.

(d) $(\mathbb{R} \cup \{-\infty, \infty\}, \uparrow)$ där $a \uparrow b = \max(a, b)$, produkten av två tal är alltså det största av talen.

2.5 Vilka av följande binära operationer är kommutativa?

(a) $(\mathbb{R}^+, /)$ alltså positiva reella tal med division.

(b) Sten-sax-påse magman.

(c) Den binära operationen $\star$ med följande tabell:

$\star$			
			
			
			

.

(d) $(\{f : \mathbb{R} \to \mathbb{R}\}, \cdot)$ alltså mängden funktioner $\mathbb{R} \to \mathbb{R}$ med punktvis multiplikation: $(f \cdot g)(x) := f(x)g(x)$.

(e) $(\{f : \mathbb{R} \to \mathbb{R}\}, \circ)$ alltså mängden funktioner $\mathbb{R} \to \mathbb{R}$ med sammansättning: $(f \circ g)(x) := f(g(x))$.

Kapitel 3

Grupper

Definition 3.1

En **grupp** $(G, \star)$ är en mängd G tillsammans med en binär operation $\star$ på G som uppfyller följande tre villkor:

- Operationen $\star$ är associativ, d.v.s. $(a \star b) \star c = a \star (b \star c)$ för alla $a, b, c \in G$.
- Det existerar ett identitetselement för $\star$ d.v.s. det existerar ett $e \in G$ så att $e \star a = a = a \star e$ för alla $a \in G$.
- Varje element i G har en invers d.v.s. för alla $a \in G$ så existerar $a^{-1} \in G$ med $a \star a^{-1} = e = a^{-1} \star a$.

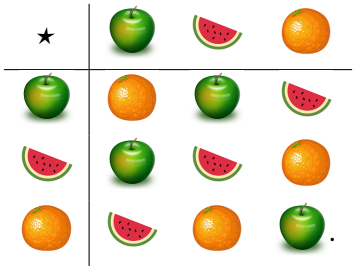
Ibland inkluderar man också villkoret att $(G, \star)$ ska vara **sluten**, alltså att $g \star h \in G$ för alla $g, h \in G$, men egentligen följer det av det faktum att $\star$ är en binär operation på G. Om det är underförstått vilken binär operation $\star$ man pratar om säger man också att G är en grupp när man menar $(G, \star)$.

Som exempel noterar vi att $(\mathbb{Z}, +)$ och $(\mathbb{R}, +)$ och $(\mathbb{Q}, +)$ alla är grupper. Addition är associativ i samtliga fall, identitetselementet är 0 i samtliga fall, och inversen av ett element a är $-a$.

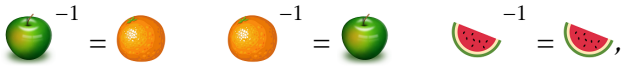
$(\mathbb{R}, \cdot)$ är *inte* en grupp: associativitet gäller och identitetselement finns, men 0 saknar invers: inget element multiplicerat med 0 kan bli 1.

Tar vi bort nollan får vi dock en grupp, det vill säga $(\mathbb{R}\backslash\{0\}, \cdot)$ är en grupp.

Vårt frukt-exempel från tidigare utgör också en grupp:

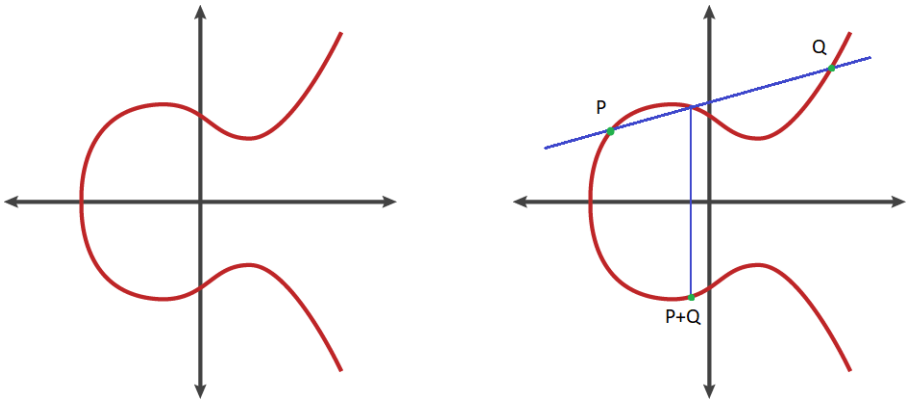


Här ser vi direkt från tabellen att  är ett identitetselement och att



så alla element har inverser. Associativitet gäller också, men det är svårare att se direkt ur tabellen.

En annan grupp med många praktiska[1] och teoretiska[2] tillämpningar är *gruppen associerad med en elliptisk kurva*. Grafen till kurvan $y^2 = x^3 - x + 1$ visas nedan. Man kan definera summan av två punkter P och Q på kurvan enligt följande: dra en linje mellan P och Q, den skär kurvan i en tredje punkt - spegla denna punkt i x-axeln för att få $P + Q$. Denna struktur utgör en grupp[3]!



3.1 Heltal modulo n

En binär operation man ofta studerar inom t.ex. talteori är "addition modulo n". Vi börjar med att titta på ett tidigare exempel.

I förra sektionen tittade vi på en ekvivalensrelation $\sim$ på heltalen där $a \sim b$ när $3|a - b$. Detta gav upphov till tre ekvivalensklasser:

$$\mathbb{Z}/\sim = \{[0], [1], [2]\}$$

där vi valt *representanter* $0, 1, 2$ för de tre klasserna.

Vi definierar nu en binär relation $+$ på $\mathbb{Z}/\sim$ enligt:

$$[a] + [b] := [a + b].$$

Här kan notationen vara förvirrande: det vänstra $+$-teckenet är den nya operationen vi definierar, och $+$-tecknet på högersidan är vanlig addition av heltal. Vår regel säger alltså att för att kombinera två ekvivalensklasser så väljer vi en representant för varje klass, adderar dessa, och tar detta elements ekvivalensklass. Exempelvis har vi $[2] + [2] = [1]$ eftersom $[2] + [2] := [2 + 2] = [4]$ och $[4] = [1]$ eftersom 1 och 4 representerar samma ekvivalensklass. Skriver vi ned tabellen för $(\mathbb{Z}/\sim, +)$ får vi

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

Faktum är att $(\mathbb{Z}/\sim, +)$ också är en grupp. Associativitet innebär ju att $[a] + ([b] + [c]) = ([a] + [b]) + [c]$ vilket är ekvivalent med att $[a + (b + c)] = [(a + b) + c]$. Men detta är ju

[1] Elliptiska kurvor över ändliga kroppar används för bland annat kryptering och heltalsfaktorisering.
[2] Teorin för elliptiska kurvor utgjorde ett viktigt steg i beviset av Fermats stora sats.
[3] Egentligen måste vi också introducera en oändlighetspunkt som blir vårt identitetselement på kurvan.

sant eftersom vanlig addition är associativ. $[0]$ är identitetselement och varje element $[a]$ har inversen $[-a]$. När man vet vad sammanhanget är låter man ofta bli att skriva ut hakparenteserna.

Om vi ersätter 3 med ett annat positivt heltal n får vi samma typ av algebraiska struktur: Vi definierar en ekvivalensrelation på $\mathbb{Z}$ genom $a \sim b$ när $n|a-b$ och får då n stycken ekvivalensklasser $\{[0],[1],[2],\ldots,[n-1]\}$. Här definierar vi på samma vis $[a]+[b]=[a+b]$. Operationen vi definierat kallas också för *addition modulo n*. Vi adderar alltså två tal vanligt och tar resten vid division med n. I många böcker används också notationen

$$a \equiv b \pmod{n} \qquad \text{eller} \qquad a \equiv_n b \qquad \text{istället för} \qquad [a]=[b],$$

fördelen med detta kan vara att man håller reda på vilket talet n är. Man brukar också skriva $\mathbb{Z}_n$ istället för $\mathbb{Z}/\sim$.

Sammanfattningsvis skriver vi alltså $(\mathbb{Z}_n,+)$ för mängden $\{[0],[1],[2],\ldots,[n-1]\}$ där addition är definierat modulo n.

Det är inte svårt att se att $(\mathbb{Z}_n,+)$ är en grupp: associativitet följer från associativiteten hos heltalsaddition, $[0]$ är ett identitetselement, och inversen av $[a]$ är $[-a]=[n-a]$.

Vi kan också betrakta $(\mathbb{Z}_n,\cdot)$ där operationen $\cdot$ definieras via $[a]\cdot[b]:=[ab]$. Detta är ingen grupp eftersom 0 inte har någon invers.

Sats 3.1

Ett element $[a]$ i $(\mathbb{Z}_n,\cdot)$ har en invers om och endast om a och n är relativt prima, det vill säga största gemensamma delaren för heltalen a och n är 1.

Bevis

Antag först att största gemensamma delaren för a och n är 1. Enligt Euklides algoritm betyder detta att det finns heltal x och y så att $xa+yn=1$. Men då gäller i sin tur $[x]\cdot[a]=[xa]=[1-yn]=[1]-[yn]=[1]$ eftersom $yn \equiv 0 \mod n$. På samma vis gäller $[a]\cdot[x]=[1]$, så $[x]$ är inversen till $[a]$.
Vi visar nu också omvändningen: vi antar att största gemensamma delaren för n och a inte är 1. Men då saknas lösningar till den diofantiska ekvationen $ax+ny=1$, vilket betyder att det saknas lösningar till $ax \equiv 1 \mod n$, vilket är ekvivalent med att det saknas lösningar x till $[a]\cdot[x]=[1]$, och a saknar därför invers.

Sats 3.2

$(\mathbb{Z}_n\backslash\{[0]\},\cdot)$ är en grupp om och endast om n är ett primtal.

Bevis

Enligt Sats 3.1 är $[a]$ inverterbart om och endast om $\gcd(a,n)=1$. Detta är sant för alla a i intervallet $1 \le a \le n-1$ om och endast om n är ett primtal.

3.2 Undergrupper

Kan man ha en grupp innuti en annan grupp?

Definition 3.2

Låt $(G,\star)$ vara en grupp. Om $H \subset G$ är en delmängd så att $(H,\star)$ själv är en grupp så kallas denna för en **undergrupp** till G.

Om $(G,\star)$ är en grupp, och $H \subset G$ är en delmängd, när är då $(H,\star)$ en grupp? En sak som kan hända är att h_1 och h_2 ligger i H, men deras produkt $h_1 \star h_2$ ligger inte längre i H, om detta är fallet säger man att $(H,\star)$ inte är *sluten*. Som exempel kan vi ta $G = (\mathbb{Z},+)$ och $H = \{-2,-1,0,1,2\}$. Då är $(H,+)$ inte en grupp: 1 och 2 ligger i H, men inte $1+2$, operationen $+$ är inte sluten på H.

Ett annat problem uppstår om vi tar delmängden $\mathbb{N}$ i samma grupp. Här är $\mathbb{N}$ en delmängd som är sluten under addition, men $(\mathbb{N},+)$ är ändå ingen grupp för den *saknar nämligen inverser*.

Vi sammanfattar i en sats:

Sats 3.3

Låt $(G,\star)$ vara en grupp. En (icke tom) delmängd $H \subset G$ ger en undergrupp $(H,\star)$ om och endast om för alla $h,h' \in H$:

- $h \star h' \in H$
- $h^{-1} \in H$

Bevis

För att $(H,\star)$ ska vara en grupp krävs att den är sluten, associativitet, ett identitetselement, och inverser. Associativitet följer automatiskt eftersom $(G,\star)$ är associativ. Att identitetselementet $e \in G$ också tillhör H följer från de listade egenskaperna. $h \in H$ har en invers $h^{-1} \in h$, och $e = h \star h^{-1} \in H$ eftersom H var sluten.

Varje grupp $(G,\star)$ har två tråkiga undergrupper: dels är hela gruppen själv tekniskt sett en undergrupp eftersom $G \subset G$. Å andra sidan är också $\{e\}$ en undergrupp, alltså gruppen bestående av endast identitetselementet e.

Exempel 3.1

Låt $G = (\mathbb{Z}_6,+)$. Vi ska hitta alla undergrupper i G. Gruppen har 6 element $\{[0],[1],[2],[3],[4],[5]\}$ (vi kommer att skippa hakparenteserna framöver). Vi vet att två undergrupper är G själv, och $\{0\}$. Du kan också verifiera att $H_2 = \{0,2,4\}$ och $H_3 = \{0,3\}$ är undergrupper! Dessa 4 är faktiskt alla: så fort en undergrupp innehåller 1 kan vi ju ta $1+1$, och $1+1+1$, o.s.v tills vi har hela G. Samma sak gäller om $5 \in H$ eftersom $5+5+5+5+5 = 1$.

Vi såg i exemplet att storlekarna på undergruppern var $1,2,3,6$, detta är inte en slump, utan ett exempel på Lagranges sats, som vi tyvärr inte hinner bevisa här:

Sats 3.4

Lagrange's sats: Om $H \subset G$ är en undergrupp så gäller $|H|\big||G|$, alltså antalet element i H delar antalet element i G.

3.3 Produkter av grupper

Det finns ett naturligt sätt att kombinera två grupper till en större grupp.

Definition 3.3

Låt $(G,\star)$ och $(H,\bullet)$ vara två grupper. Vi definierar **produkten** av G och H som

$$G \times H = \{(g,h) \mid g \in G, h \in H\}$$

där den nya binära operationen $\cdot$ ges av

$$(g_1,h_1)\cdot(g_2,h_2) := (g_1 \star g_2, h_1 \bullet h_2).$$

Det är lätt att verifiera att $G \times H$ är en grupp: associativitet följer av associativitet i grupperna G och H, identitetselementet i $G \times H$ är (e,e) och inversen till (g,h) är (g^{-1},h^{-1}).

Exempel 3.2

Vi undersöker gruppen $\mathbb{Z}_3 \times \mathbb{Z}_2$ (där operationerna är addition modulo 3 respektive 2). Den har 6 element:

$$(0,0),\quad (0,1),\quad (1,0),\quad (1,1),\quad (2,0),\quad (2,1)$$

Nu kan vi t.ex. beräkna

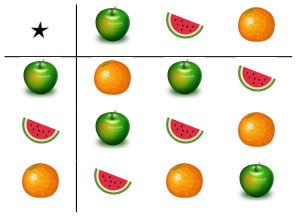
$$(2,1)\cdot(1,0) = (2+1, 1+0) = (0,1)$$

eller

$$(1,1)^{-1} = (1^{-1}, 1^{-1}) = (2,1).$$

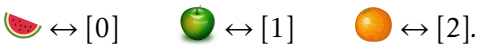
3.4 Samband mellan grupper

Ibland kan saker som ser olika ut egentligen fungera på precis samma sätt. Den observante läsaren kanske har märkt att vi har sett två exempel på grupper med tre element som ser ganska lika ut: $(M,\star)$ och $(\mathbb{Z}_3,+)$ med följande tabeller:



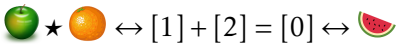
$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

Från en matematisk synvinkel är dessa i själva verket *samma* algebraiska struktur! Allt vi har gjort är att "byta namn" på elementen, de binära operationerna är egentligen lika. För att se detta kan man para ihop



Då ser man att multiplikationstabellen för $\star$ och $+$ är exakt lika (även om ordningen i raderna och kolonnerna är skiftade).

Om vi känner till denna ihopparning kan vi nämligen beräkna frukt-multiplikationen med hjälp av den högra tabellen så här:



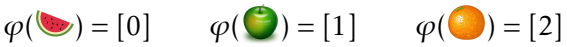
så  vilket stämmer med den vänstra tabellen. Detta är ett exempel på något som inom matematiken kallas för *isomorfi* av grupper.

Nu ska vi definiera dessa begrepp lite mer ordentligt.

Definition 3.4

Låt $(G,\star)$ och $(H,*)$ vara två grupper. En **homomorfi** från G till H är en funktion $\varphi : G \to H$ så att $\varphi(a\star b) = \varphi(a)*\varphi(b)$ för alla $a,b \in G$. En bijektiv homomorfi kallas för en **isomorfi**, och om en sådan existerar så säger man att G och H är *isomorfa*.

Enligt vårt inledande exempel är de två grupperna $(M,\star)$ och $(\mathbb{Z}_3,+)$ isomorfa, eftersom funktionen φ med



är en isomorfi.

Homomorfier sägs vara "strukturbevarande" eftersom de översätter operationen på G till operationen på H. Homo betyder "lika", och iso betyder "samma".

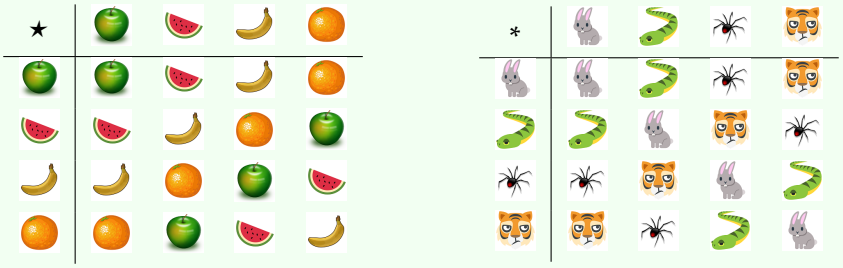
Isomorfa objekt är exakt samma från ett matematiskt perspektiv. En homomorfi som inte är bijektiv pekar ofta på några gemensamma egenskaper mellan de två objekten.

Definiera exempelvis $\varphi : (\mathbb{Z},+) \to (\mathbb{Z}_2,+)$ genom $\varphi(k) = [k]$. Detta är en homomorfi eftersom $\varphi(a+b) = [a+b] = [a]+[b] = \varphi(a)+\varphi(b)$. Här gäller det med andra ord att $\varphi(k) = [0]$ om k är jämnt och $\varphi(k) = [1]$ om k är udda. Funktionen φ håller alltså reda på vilka tal som är jämna eller udda och struntar i resten av strukturen. Att φ är en homomorfi kan alltså med ord sammanfattas som att "udda gånger udda är udda", "jämnt gånger jämnt är jämnt", och "udda gånger jämnt är udda".

Vi tittar nu på ett annat exempel.

Exempel 3.3

Låt $(G,\star)$ och $(H,*)$ ha följande multiplikationstabeller:



Man kan verifiera att båda dessa är grupper. Är de isomorfa? Detta kan verka svårt att svara på, det finns ju väldigt många funktioner $\varphi : G \to H$, så vi kan inte rimligtvis testa allihopa. Men i det här fallet kan vi ändå visa att grupperna *inte* är isomorfa. Vi ser nämligen att $x * x =$  för alla $x \in H$. Så om $\varphi : G \to H$ vore en isomorfi skulle således både

$$\varphi(\text{🍌}) = \varphi(\text{🍉} \star \text{🍉}) = \varphi(\text{🍉}) * \varphi(\text{🍉}) = \text{🐰}$$

och

$$\varphi(\text{🍏}) = \varphi(\text{🍏} \star \text{🍏}) = \varphi(\text{🍏}) * \varphi(\text{🍏}) = \text{🐰}.$$

Men detta är en motsägelse, för φ skulle ju vara en bijektion, så  och  kan inte avbildas på samma objekt.

Faktum är att de två grupperna i exemplet är de enda två olika grupperna med fyra element. Gruppen med frukt är isomorf med $(\mathbb{Z}_4,+)$ och gruppen med djur kallas *Kleins fyrgrupp*. Den senare är isomorf med gruppen $(\mathbb{Z}_2,+)\times(\mathbb{Z}_2,+)$, alltså mängden av alla par av element i $\mathbb{Z}_2$, där additionen är modulo 2 elementvis:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(1,0),(0,1),(1,1)\} \text{ med } (a,b)+(c,d) = (a+c,b+d).$$

Om vi skriver $e = (0,0)$, $a = (0,1)$, $b = (1,0)$, och $d = (1,1)$ får vi följande tabeller för dessa två grupper:

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Man kan bevisa att varje grupp med fyra element är isomorf med en av dessa två grupper.

Övningsuppgifter

3.1 Ingen av följande exempel på binära operationer utgör grupper. Förklara vad som saknas i vart fall!

(a) $(\mathbb{N},+)$, alltså de naturliga talen med addition.

(b) $(\mathbb{Z},-)$, alltså de naturliga talen med subtraktion.

(c) $(\mathbb{Z}, \cdot)$, alltså heltalen med multiplikation.

(d) Mängden av 2×2-matriser med matrismultiplikation.

(e) $(\mathbb{N}_0, \#)$ där $a\#b = |a - b|$.

(f) Operationen $*$ på $\{a, b\}$ med följande multiplikationstabell

*	a	b
a	a	a
b	a	b

3.2 Verifiera att följande strukturer alla är grupper.

(a) Mängden reella 2×2-matriser med determinant 1 under matrismultiplikation.

(b) Mängden bijektiva funktioner $\{1, 2, 3\} \to \{1, 2, 3\}$ under sammansättning.

3.3 Skriv ned en multiplikationstabellen för en grupp med två element på så vis att de tre villkoren i definitionen av en grupp är uppfyllda. Det finns väsentligen en enda grupp med två element, fundera på vad detta påstående betyder mer precist.

3.4 Låt $(G, \star)$ vara en grupp.

(a) Bevisa att det bara finns en enda invers till varje $g \in G$.

(b) Bevisa att om $(G, \star)$ är en grupp och $g, h \in G$ så har vi $(g \star h)^{-1} = h^{-1} \star g^{-1}$.

3.5 (a) Hitta 120^{-1} i $(\mathbb{Z}_{431}, \cdot)$.

(b) Hitta alla lösningar till ekvationen $452x = 214$ i $\mathbb{Z}_{943}$.

3.6 Låt H vara den minsta *undergruppen* av $(\mathbb{Z}, +)$ som innehåller talen 6 och 10. Vilka tal tillhör H? Försök hitta en så enkel beskrivning som möjligt av H!

3.7 Antag att vi har en grupp med 4 element a, b, c, d. Hur kan vi avgöra om gruppen är isomorf med $\mathbb{Z}_4$ eller $\mathbb{Z}_2 \times \mathbb{Z}_2$?

3.8 Bevisa att $\mathbb{Z}_3 \times \mathbb{Z}_2$ är isomorf med $\mathbb{Z}_6$!

3.9 I kapitlet visade vi hur gruppen associerad med en elliptisk kurva fungerade.

(a) Är gruppen associerad med en elliptisk kommutativ?

(b) Är gruppen associativ? Prova att välja tre punkter P, Q, R i bilden i detta kapitel och beräkna $(P + Q) + R$ respektive $P + (Q + R)$.

3.10 Visa att en homomorfi $G \to H$ måste skicka identitetselementet i G till identitetselementet i H!

3.11 Låt $U = \{1, -1, i, -i\}$. Visa att $(U, \cdot)$ är en undergrupp av $(\mathbb{C}\backslash\{0\}, \cdot)$. Visa sedan att $(U, \cdot)$ är isomorf med $(\mathbb{Z}_4, +)$.

3.12 Vi definierar en funktion

$$\varphi : \mathbb{C} \to \mathrm{Mat}_{2\times2}(\mathbb{R}) \quad \text{genom} \quad \varphi(a + bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

(a) Är φ injektiv? surjektiv? bijektiv?

(b) Visa att φ är en grupp-homomorfism från $(\mathbb{C}, +)$ till $(\mathrm{Mat}_{2\times2}(\mathbb{R}), +)$

(c) Visa att $\varphi(z \cdot w) = \varphi(z) \cdot \varphi(w)$ för alla $z, w \in \mathbb{C}$.

Kapitel 4

Den symmetriska gruppen S_n

En grupp som ofta dyker upp inom olika matematiska och andra naturvetenskapliga områden är den såkallade *symmetriska gruppen*.

Definition 4.1

För varje $n \in \mathbb{N}$ definierar vi den **symmetriska gruppen** S_n som

$$S_n = \{\sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \mid \sigma \text{ bijektiv.}\}$$

där grupp-operationen är $\circ$, sammansättning av funktioner. Elementen i S_n kallas också **permutationer**

Hur kan man beskriva ett element i S_n? Lättast är att beskriva alla dess funktionsvärden. Vi har t.ex. en funktion σ på $\{1, 2, 3, 4, 5\}$ som uppfyller

$$\sigma(1) = 3 \quad \sigma(2) = 1 \quad \sigma(3) = 2 \quad \sigma(4) = 5 \quad \sigma(5) = 4.$$

Det är enkelt att verifiera att σ är bijektiv: alla tal $1-5$ avbildas på olika siffror så σ är injektiv, och varje siffra $1-5$ förekommer till höger om ett likhetstecken så σ är surjektiv[1]. Alltså tillhör σ den symmetriska gruppen S_5. Det är ganska omständigt att skriva ut σ på ovanstående vis. Därför inför vi följande notation för vårt σ ovan:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$$

Översta raden är alltså $1, 2, 3, 4, 5$ och nedre raden är $\sigma(1), \sigma(2), \sigma(3), \sigma(4), \sigma(5)$.

Nästa fråga är hur man beräknar grupp-produkten av element i denna form. Vi illustrerar med ett exempel:

[1] På ändliga mängder är dessa villkor ekvivalenta så det räcker att testa det ena.

Exempel 4.1

Låt σ och τ vara element i S_4 som ges av:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Vi ska beräkna $\sigma \circ \tau$ som också kommer att bli ett element i S_4. Precis som vid vanlig sammansättning av funktioner är det den *högra* funktionen som appliceras först. har $(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(3) = 3$ detta kan ses direkt från matris-notationen. På samma vis har vi $(\sigma \circ \tau)(2) = \sigma(\tau(2)) = \sigma(4) = 2$, och $(\sigma \circ \tau)(3) = \sigma(1) = 4$ och $(\sigma \circ \tau)(4) = \sigma(2) = 1$. Sammanfattningsvis har vi alltså

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

När vi gör den analoga uträkningen för $\tau \circ \sigma$ får vi resultatet

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix},$$

så speciellt noterar vi att $\tau \circ \sigma \neq \sigma \circ \tau$. Detta illustrerar att symmetriska gruppen alltså *inte är kommutaiv* (för $n > 2$).

Vi har ännu inte verifierat att S_n är en grupp. Associativiteten i S_n följer direkt från associativiteten hos funktionssammansättning. Identitetselementet i S_n är (såklart) identitetsfunktionen på $\{1, 2, \ldots, n\}$. I vår notation skrivs denna

$$e = \begin{pmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \end{pmatrix}.$$

Eftersom bijektiva funktioner har inverser, så existerar inverser i S_n. För att hitta inversen till en permutation i vår notation måste vi byta plats raderna, och sedan sortera om kolonnerna så att övre raden blir ordnad $1, 2, \ldots, n$.

Om

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix} \text{ så har vi } \sigma^{-1} = \begin{pmatrix} 3 & 1 & 2 & 5 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}.$$

Nu kan du lätt testa att verkligen $\sigma \circ \sigma^{-1} = e = \sigma^{-1} \circ \sigma$ (vi kommer i fortsättningen inte alltid skriva ut $\circ$-tecknet). Vi har nu visat att S_n är en grupp!

Exempel 4.2

Vi ska nu skriva ned hela grupptabellen för S_3. Elementen i S_3 är:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad r_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad r_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Räknar vi ut alla produkter av dessa 6 element får vi följande multiplikationstabell för gruppen S_3:

$\circ$	e	r_1	r_2	σ_1	σ_2	σ_3
e	e	r_1	r_2	σ_1	σ_2	σ_3
r_1	r_1	r_2	e	σ_3	σ_1	σ_2
r_2	r_2	e	r_1	σ_2	σ_3	σ_1
σ_1	σ_1	σ_2	σ_3	e	r_1	r_2
σ_2	σ_2	σ_3	σ_1	r_2	e	r_1
σ_3	σ_3	σ_1	σ_2	r_1	r_2	e

Varför kallas S_n egentligen symmetrisk? Ordet kommer från det faktum att man kan se varje element i S_n som en symmetri - ett sätt att avbilda någonting på sig självt (i vårt fall mängden $\{1, 2, \ldots, n\}$).

För S_3 kan man faktiskt tolka detta geometriskt: Om vi tar en liksidig triangel och döper hörnen till $1, 2, 3$ så kan varje element i S_3 ses om ett sätt att *flytta triangeln till sig själv*. Titta exempelvis på r_1 ovan. Den flyttar hörn $1 \mapsto 2 \mapsto 3 \mapsto 1$, och motsvarar alltså en *rotation* av triangeln. r_2 roterar åt motsatt håll. σ_1 skiftar hörn 2 med hörn 3, så σ_1 *speglar* triangeln i linjen som går från hörn 1 till mitten på sidan mellan 2 och 3. σ_2 och σ_3 är två andra speglingar, och identitestelementet e är operationen som inte flyttar något alls. Gruppoperationen motsvarar här att utföra flyttningarna efter varandra. Vi ser t.ex. från tabellen att $r_1 \circ (r_1 \circ r_1) = e$ och detta stämmer ju - roterar vi triangeln tre gånger kommer vi tillbaka till utgångsläget!

4.1 Cykel-notation

Det finns ett ännu mer kompakt sätt att skriva element i S_n. Vi illustrerar med ett exempel: Låt

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 6 & 5 & 1 \end{pmatrix}$$

Om vi börjar med ett element från $\{1, \ldots, 6\}$ och applicerar σ om och om igen så kommer vi tillslut tillbaka till elementet där vi började. Börjar vi t.ex. med 1 så har vi $\sigma(1) = 4$, $\sigma(4) = 6$, och $\sigma(6) = 1$. Vi har alltså en "cykel"$1 \mapsto 4 \mapsto 6 \mapsto 1$. I cykel-notation skrivs denna $(1, 4, 6)$, den kallas en 3-cykel. Vi har också andra cykler: vi har $2 \mapsto 3 \mapsto 2$ så $(2, 3)$ är en 2-cykel och slutligen skickas ju 5 till 5, så (5) är en 1-cykel. I **cykel-notation** skrivs därför

$$\sigma = (1, 4, 6)(2, 3)(5)$$

Man struntar ofta att skriva ut 1-cykler eftersom de är underförstådda, så man kan också skriva $\sigma = (1, 4, 6)(2, 3)$. Här är det fortfarande lätt att läsa ut vad σ gör: varje tal skickas till nästa i cykeln, där sista elementet i en cykel skickas tillbaka till det första.

Lägg märke till att cykeln $(1,4,6)$ också kan skrivas som $(4,6,1)$ eller $(6,1,4)$, cykler kan alltså roteras"cykliskt. Elementet $(4,1,6)$ är dock en annan cykel!

Identitetselementet består ju bara av 1-cykler så ibland skriver man $()$ eller (1) för identitetselementet.

Elementet $\begin{pmatrix}1&2&3&4&5&6\\1&5&3&4&2&6\end{pmatrix}$ i S_6 blir i cykel-notationen helt kort $(2,5)$. Element av denna form, som bara byter plats på två element och lämnar resten kallas för **transpositioner**.

Sats 4.1

Varje element i S_n kan skrivas som produkt av transpositioner. Om σ är en produkt av ett *jämnt* antal transpositioner så säger vi att σ är jämn, och vi skriver $\operatorname{sgn}(\sigma) = 1$. Annars, om σ är en produkt av ett *udda* antal transpositioner så säger vi att σ är udda, och vi skriver $\operatorname{sgn}(\sigma) = -1$.

För att se att det första påståendet är sant räcker det att visa att varje *cykel* i σ är en produkt av transpositioner. Detta är inte svårt att inse: Exempelvis har vi i S_4:

$$(1,3,4,2) = (1,2) \circ (1,4) \circ (1,3).$$

För att testa att detta stämmer kan man t.ex. testa att verkligen $3 \mapsto 4$ i högerledet:

$$(1,2) \circ (1,4) \circ (1,3)(3) = (1,2) \circ (1,4)(1) = (1,2)(4) = 4.$$

Detta fungerar därför att vi alltid kan sortera om en lista genom att upprepat byta plats på det första elementet och andra element.

Eftersom $(1,3,4,2) \in S_4$ kan skrivas som en sammansättning av 3 - alltså ett udda antal transpositioner, så $\operatorname{sgn}(1,3,4,2) = -1$.

Exempel 4.3

Vi löser en exempeluppgift: Skriv elementet $\sigma \in S_9$ som en produkt av transpositioner. Är σ jämn eller udda?

$$\sigma = \begin{pmatrix}1&2&3&4&5&6&7&8&9\\8&9&5&1&4&6&2&3&7\end{pmatrix}$$

Lösning: Vi börjar med att skriva σ i cykel-notation. Vi ser att $1 \mapsto 8 \mapsto 3 \mapsto 5 \mapsto 4 \mapsto 1$, så $(1,8,3,5,4)$ är en 5-cykel i σ. Vi har också en 3-cykel $(2,9,7)$ och en 1-cykel (6). I cykelnotation blir därför

$$\sigma = (1,8,3,5,4) \circ (2,9,7).$$

Nu skriver vi var och en av dessa som en produkt av transpositioner:

$$(1,8,3,5,4) = (1,4) \circ (1,5) \circ (1,3) \circ (1,8) \quad \text{och} \quad (2,9,7) = (2,7) \circ (2,9)$$

Så alltså blir

$$\sigma = (1,4) \circ (1,5) \circ (1,3) \circ (1,8) \circ (2,7) \circ (2,9)$$

och $\operatorname{sgn}(\sigma) = 1$.

En tillämpning av symmetriska grupper kommer i linjär algebra när man definierar *determinanter*. Många böcker definierar determinanten med hjälp av rad-och kolonnutveckling, d.v.s. man ger en formel för 2×2 eller 3×3 fallet och visar sedan hur man

successivt kan räkna ut större determinanter. Men finns det en formel som gäller för alla matrisstorlekar? Svaret är ja!

Definition 4.2

Låt $A = (a_{i,j})$ vara en $n \times n$-matris. Då definierar vi determinanten av A som:

$$\det(A) = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \cdots a_{n,\sigma(n)}.$$

Vi verifierar att formeln fungerar i 2×2-fallet. Låt $A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix}$. I formeln ovan ska vi nu summera över S_2. Denna har bara 2 element: identitetselementet e och elementet $(1,2)$ som skiftar 1 och 2. $\operatorname{sgn}(e) = 1$ och $\operatorname{sgn}(1,2) = -1$ så vi får

$$\det(A) = \operatorname{sgn}(e) a_{1,e(1)} a_{2,e(2)} + \operatorname{sgn}(1,2) a_{1,(1,2)(1)} a_{2,(1,2)(2)} = a_{1,1} a_{2,2} - a_{1,2} a_{2,1},$$

vilket stämmer med vad vi lärt oss i linjär algebra. Utför vi räkningarna för 3×3-fallet får vi den såkallade *Sarrus regel*.

4.2 Den alternerande gruppen A_n

Den symmetriska gruppen S_n har en undergrupp A_n som består av *alla jämna element* i S_n. Vi definierar

$$A_n = \{\sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1\}.$$

Detta kallas den **alternerande gruppen**. Vi verifierar att detta är en undergrupp. Först och främst är operationen $\circ$ sluten på A_n; om σ och τ båda kan skrivas med ett jämnt antal transpositioner, så gäller ju också detta för deras produkt. Identitetselementet är jämnt och ligger därför i A_n. Slutligen, om $\sigma \in A_n$ så gäller också $\sigma^{-1} \in A_n$; inversen till en produkt av transpositioner får vi genom att vända ordningen på transpositionerna. Exempelvis gäller för $\sigma = (1,3) \circ (1,2)$ att $\sigma^{-1} = (1,2) \circ (1,3)$ vilket man ser genom att multiplicera ihop dem:

$$\sigma \circ \sigma^{-1} = (1,3) \circ (1,2) \circ (1,2) \circ (1,3) = (1,3) \circ e \circ (1,3) = (1,3) \circ (1,3) = e$$

Övningsuppgifter

4.1 Låt

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix} \quad \text{och} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$$

Beräkna $\sigma\tau$ och $\tau\sigma$ och $\sigma\sigma$ och τ^{-1}.

4.2 Låt σ och τ vara som i föregående uppgift.

(a) Skriv σ och τ i cykel-notation.

(b) Skriv τ som en en produkt av transpositioner.

(c) Är σ respektive τ jämna eller udda?

4.3 Hur många element har S_5? Hur många av dessa är transpositioner? Hur många innehåller exakt en 3-cykel?

4.4 Låt

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \in S_5$$

(a) Beräkna $\sigma^2, \sigma^3, \sigma^4, \sigma^5, \sigma^6$.

(b) Visa att $H = \{\sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \sigma^6\}$ är en undergrupp i S_5.

(c) Gruppen H har sex element. Är H isomorf med S_3 eller $\mathbb{Z}_6$? Motivera ditt svar!

4.5 Låt

$$a = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \text{och } b = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Visa att $(\{a, b\}, \cdot)$ är isomorf med S_2.

4.6 Visa att A_3 är isomorf med $(\mathbb{Z}_3, +)$.

4.7 Vi säger att i är en *fix-punkt* för $\sigma \in S_n$ när $\sigma(i) = i$. Låt

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 2 & 1 & 3 & 6 & 3 \end{pmatrix}$$

(a) Hur många fix-punkter har σ?

(b) Hur många fix-punkter har σ^2?

(c) Hur många element i S_4 saknar fix-punkter?

4.8 Vi säger att $\sigma = (1,2,5)(3,6)(4)(7)(8,9) \in S_9$ (cykel-notation) har *cykel-typ* $(2,2,1)$ eftersom den består av två 1-cykler, två 2-cykler och en 3-cykel. Vilka cykel-typer finns i S_3, och hur många element av varje cykeltyp finns det?

4.9 Hur många element av varje cykel-typ finns det i S_4?

Kapitel 5

Ringar och Kroppar

Heltalen $\mathbb{Z}$ är ju utrustade med två stycken binära operationer, både addition och multiplikation. Dessa är dessutom *kompatibla* i den meningen att bland annat $a(b+c) = ab+ac$. Ringar och kroppar är algebraiska strukturer som generaliserar dessa koncept till andra mängder och binära operationer.

5.1 Ringar

Definition 5.1

En **ring** $(R, \oplus, \otimes)$ är en mängd R tillsammans med två olika binära operationer $\oplus$ och $\otimes$ på R, så att följande gäller:

- $(R, \oplus)$ är en abelsk grupp.
- operationen $\otimes$ är associativ och har ett identitetselement.
- $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ och $(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$.

Identitetselementet för $\otimes$ brukar skrivas som 1, eller 1_R när man vill poängtera vilken ring man pratar om. Reglerna i punkt 3 kallas för de *distributiva lagarna*.

När man arbetar med ringar brukar man skriva $-a$ för den *additiva inversen* för a, alltså a's invers i gruppen $(R, \oplus)$. Den multiplikativa inversen för a, alltså a's invers i $(R, \otimes)$ skrivs a^{-1} *om den existerar*. Precis som med vanliga tal skriver man också a^n för produkten $a \otimes a \otimes \cdots \otimes a$ (med n faktorer), men nu är ju produkten i vår ring R.

Vanligtvis brukar man använda de vanligare symbolerna + istället för $\oplus$ och $\cdot$ istället för $\otimes$ när man räknar med ringar, men vi använder andra symboler här i definitionen för att förtydliga att våra binära operationer inte behöver ha någonting att göra med vanlig addition och multiplikation.

Det finns många exempel på ringar. Vi tittar på ett par:

Exempel 5.1

Heltalen med vanlig addition och multiplikation $(\mathbb{Z}, +, \cdot)$ är en ring. Villkoren i definitionen av en ring är här räknelagar som vi är vana att använda.

Exempel 5.2

$\mathbb{Z}_n$ är ett till exempel på en ring för alla $n \geq 2$. Här definierar vi som som bekant $[a]+[b] = [a+b]$ och $[a]\cdot[b] = [ab]$. För $\mathbb{Z}_3$ kan vi t.ex. beskriva dessa två operationer med hjälp av två tabeller:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Här har vi inte skrivit ut hakparenteser för att det ska bli lättare att läsa.

Exempel 5.3

Ringen $(\mathbb{Z}[x], +, \cdot)$, alltså ringen av alla polynom med heltalskoefficienter. Här ges operationerna av vanlig addition och multiplikation av polynom. Om t.ex. $p(x) = x+3$ och $q(x) = 2x-1$ så är $(p+q)(x) = 3x+2$ och $(p\cdot q)(x) = (x+3)(2x-1) = 2x^2+5x-3$. Mer generellt, om $(R, +, \cdot)$ är vilken ring som helst så blir också $(R[x], +, \cdot)$ en ring, alltså polynomringen med koefficienter i ringen R.

Exempel 5.4

Ringen av alla 2×2-matriser med reella koefficienter brukar skriva $\mathrm{Mat}_{2\times 2}(\mathbb{R})$. Här räknar vi med addition och multiplikation av matriser. Mer generellt kan man titta på $\mathrm{Mat}_{n\times n}(S)$ där $n \in N$ och S är vilken ring som helst.

Vi vet ju att $0 \cdot x = 0$ för alla heltal x. Detta är faktiskt något som gäller i *alla* ringar. Vi formulerar detta som en sats.

Sats 5.1

Låt $\mathbf{0}$ vara identitetselementet i $(R, \oplus)$. Då gäller $\mathbf{0} \cdot x = \mathbf{0}$ och $x \cdot \mathbf{0} = \mathbf{0}$ för alla $x \in R$.

Bevis

För alla $a, b \in R$ har vi

$$a \otimes b = (a \oplus \mathbf{0}) \otimes b = (a \otimes b) \oplus (\mathbf{0} \otimes b)$$

Första likheten ovan använder att $\mathbf{0}$ är identitetselement för $\oplus$, andra likheten är den distributiva lagen. Vi vill nu "subtrahera" $a \otimes b$ från båda sidor. Detta gör vi genom att addera den additiva inversen till $a \otimes b$ på bägge sidor. Då får vi

$$\mathbf{0} = -(a\otimes b)\oplus(a\otimes b) = -(a\otimes b)\oplus\Big((a\otimes b)\oplus(\mathbf{0}\otimes b)\Big) = \Big(-(a\otimes b)\oplus(a\otimes b)\Big)\oplus(\mathbf{0}\otimes b) = \mathbf{0}\oplus(\mathbf{0}\otimes b) = \mathbf{0}\otimes b$$

Vi har visat att $\mathbf{0} \otimes b = \mathbf{0}$ för alla $b \in R$. På helt analogt vis kan man även visa att $b \otimes \mathbf{0} = \mathbf{0}$ för alla $b \in R$.

5.2 Delringar och Produkter av ringar

Delringar är den ring-teoretiska motsvarigheten till undergrupper.

Definition 5.2

Om $(R,+,\cdot)$ är en ring, och $S \subset R$ är en delmängd så att $(S,+,\cdot)$ fortfarande är en ring, så säger vi att S är den **delring** av R.

Exempel 5.5

- $\mathbb{Z}$, $\mathbb{Q}$ och $\mathbb{R}$, är alla delringar av $\mathbb{C}$.
- Låt $J = \{2a \mid a \in \mathbb{Z}\}$ och $U = \{2a+1 \mid a \in \mathbb{Z}\}$ vara de jämna respektive udda heltalen. Då är varken J eller U delringar av $\mathbb{Z}$. J är inte en delring eftersom den saknar ett multiplikativt identitetselement (1). U är inte en delring eftersom den inte är sluten under addition: summan av två udda i U ligger inte i U!
- Mängden reella övertriangulära 2×2-matriser utgör en delring av hela matrisringen:

$$\left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \,\middle|\, a,b,c \in \mathbb{R} \right\} \text{ är en delring av } \mathrm{Mat}_{2\times 2}(\mathbb{R}).$$

Precis som för grupper kan man också definiera produkten av två ringar:

Definition 5.3

Låt $(R,+,\cdot)$ och $(S,+,\cdot)$ vara två ringar. Vi definierar **produktringen** av R och S som mängden $R\times S$ med följande operationer:

$$(r_1,s_1)+(r_2,s_2) := (r_1+r_1, s_1+s_2)$$

$$(r_1,s_1)\cdot(r_2,s_2) := (r_1\cdot r_1, s_1\cdot s_2).$$

Notera att +tecknet betyder tre olika saker i definitionen! Det finns en operation + i R, en i S, och en i $R\times S$. På samma vis har tecknet $\cdot$ tre olika betydelser.

Lägg också märke till att om 1_R och 1_S är de multiplikativa identitetselementen i R respektive S, så kommer $(1_R,1_S)$ att bli multiplikativt identitetselementet i $R\times S$ eftersom $(1_R,1_S)\cdot(r,s) = (1_R\cdot r, 1_S\cdot s) = (r,s)$.

5.3 Polynomringar och matrisringar

Om $(R,+,\cdot)$ är vilken ring som helst så kan vi definiera *polynomringen* $R[x]$ med koefficienter i R. Detta är mängden polynom av form

$$r_0 + r_1x + r_2x^2 + \cdots + r_nx^n \quad \text{med } r_0,r_1,r_2,\ldots,r_n \in R.$$

Här betraktar vi x som en variabel, precis som för vanliga polynom. Med hjälp av operationerna + och $\cdot$ i ringen R går att addera och multiplicera polynom precis som vid vanlig polynomräkning, och därför blir $R[x]$ också en ring! Notera att $R \subset R[x]$ blir en delring - mängden konstanta polynom. Precis som med vanliga polynom skriver man x^k istället för $1x^k$, och man skriver inte ut termer av formen $0x^k$ alls.

Exempel 5.6

Vi tar nu $R = \mathbb{Z}_3$, och räknar ut en summa och en produkt i $\mathbb{Z}_3[x]$. Som exempel: Tag

$$p(x) = x^2 + x + 2 \in \mathbb{Z}_3[x] \quad \text{och} \quad q(x) = 2x + 2 \in \mathbb{Z}_3[x]$$

Då får vi summan av p och q genom att addera polynomens koefficienter, precis som vid vanlig polynomräkning, men koefficienterna ligger nu i $\mathbb{Z}_3$!

$$p(x) + q(x) = (x^2 + x + 2) + (2x + 2) = (1 + 0)x^2 + (2 + 1)x + (2 + 2) = 1x^2 + 0x + 1 = x^2 + 1$$

Multiplicerar vi p och q får vi istället:

$$p(x) \cdot q(x) = (x^2 + x + 2) \cdot (2x + 2) = (x^2 + x + 2) \cdot 2x + (x^2 + x + 2) \cdot 2$$

$$= (2x^3 + 2x^2 + x) + (2x^2 + 2x + 1) = 2x^3 + x^2 + 1$$

Med en liknande konstruktion kan man konstruera en *matrisring* med koefficienter i en annan ring. Betrakta mängden $n \times n$-matriser där elementen på raderna och kolonnerna alla är element i en ring $(R, +, \cdot)$. När man beräknar produkten av två matriser behöver man ju ta produkter och summor av elementen i matriserna, och eftersom dessa operationer kan beräknas i ringen R så blir denna mängd av matriser en ring.

Matrisringen med koefficienter i R skrivs $\mathrm{Mat}_{n\times n}(R)$.

Exempel 5.7

Vi tar åter $R = \mathbb{Z}_3$, och räknar ut en summa och en produkt i $\mathrm{Mat}_{2\times 2}(\mathbb{Z}_3)$. Som exempel: Tag

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 2 \end{bmatrix} \quad \text{och} \quad B = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}$$

Då har vi

$$A + B = \begin{bmatrix} 1+0 & 1+2 \\ 0+1 & 2+2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \quad \text{och} \quad A \cdot B = \begin{bmatrix} 1\cdot 0 + 2 \cdot 1 & 1 \cdot 1 + 2 \cdot 2 \\ 0 \cdot 0 + 2 \cdot 1 & 0 \cdot 1 + 2 \cdot 2 \end{bmatrix} = \begin{bmatrix} 2 & 2 \\ 2 & 1 \end{bmatrix}$$

5.4 Inverterbara element

Med *inversen* till ett element i en ring $(R, +, \cdot)$ menar man den multiplikativa inversen, alltså inversen i magman $(R, \cdot)$ om en sådan existerar. Vi skriver alltså precis som tidigare $b = a^{-1}$ om $b \cdot a = 1_R = a \cdot b$.

Två grundläggande frågor vi borde reda ut är följande: har alla element i en ring en invers? Och kan ett element ha mer än en invers? På den första frågan är svaret nej - nollan (identitetselementet i $(R, +)$) kan ju inte ha en invers eftersom $0 \cdot b = 0 \neq 1$ för alla $b \in R$. I själva verket kan också andra element sakna invers.

Vad det gäller den andra frågan så är också svaret nej: ett element $a \in R$ kan ha *högst* en invers. För antag att både b och c är två olika inverser till a. Då gäller

$$b \cdot a = 1 \Rightarrow (b \cdot a) \cdot c = c \Rightarrow b \cdot (a \cdot c) = c \Rightarrow b \cdot 1 = c \Rightarrow b = c,$$

vilket är en motsägelse. Alltså är inverser unika, och istället för att säga att "b är en invers till a" kan vi med gott samvete säga att "b är inversen till a".

Exempel 5.8

Vi tittar på ett par exempel på inverser i olika ringar.

- I ringen $\mathbb{Q}$ av rationella tal, så har alla tal utom 0 en invers. Inversen till $\frac{a}{b}$ är $\frac{b}{a}$ eftersom $\frac{a}{b}\frac{b}{a} = 1$.
- I ringen $\mathbb{Z}$ har vi $1^{-1} = 1$ och $(-1)^{-1} = (-1)$, men *inget* annat element har invers.
- I ringen $\mathbb{Z}_{17}$ är 5 inversen till 7, eftersom $7 \cdot 5 = 1$ i ringen. Mer allmänt så bevisade vi ju tidigare att i ringen $\mathbb{Z}_p$ har alla element utom 0 en invers.
- I ringen $\mathbb{Z}_5 \times \mathbb{Z}_7$ är ett element (a, b) inverterbart så länge $a \neq 0$ och $b \neq 0$. Vi har t.ex. $(2,3)^{-1} = (3,5)$ eftersom $(2,3) \cdot (3,5) = (1,1) = 1$.
- I ringen $\mathrm{Mat}_{2\times 2}(\mathbb{R})$ av reella 2×2-matriser så har vi exempelvis

$$\begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix}^{-1} = \begin{bmatrix} -5 & 2 \\ 3 & -1 \end{bmatrix} \quad \text{eftersom} \quad \begin{bmatrix} 1 & 2 \\ 3 & 5 \end{bmatrix} \cdot \begin{bmatrix} -5 & 2 \\ 3 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 1.$$

  Från linjär algebra minns vi att inversen existerar för alla matriser som inte har determinant 0!
- I polynomringen $\mathbb{R}[x]$ så saknar polynomet $(x + 3)$ invers: vad man än multiplicerar med kan man inte få 1. Mer allmänt så existerar inverser för alla konstanter (utom 0), men inga andra polynom har invers.

5.5 Faktorisering och Primtal

Kan man prata om "primtal" i en annan ring än $\mathbb{Z}$? Det ska vi försöka reda ut i det här avsnittet.

I ringen $(\mathbb{Z}, +, \cdot)$ är $15 = 3 \cdot 5$ en primtalsfaktorisering: vi har brutit upp talet 15 i så små delar som möjligt.

Helt analogt kan man fråga sig om det går att faktorisera element i en annan ring. Tag till exempel ringen $(\mathbb{R}[x], +, \cdot)$ bestående av polynom med reella koefficienter med vanlig addition och multiplikation av polynom. Polynomet $2x^2 + 10x + 12$ kan faktoriseras som en produkt av två polynom:

$$2x^2 + 10x + 12 = (2x + 4) \cdot (x + 3),$$

och här fungerar $(2x + 4)$ och $(x + 3)$ som "primtal" fast i ringen $\mathbb{R}[x]$!

Vi är nu redo att definiera dessa begrepp mer ordentligt.

Definition 5.4

Låt $(R, +, \cdot)$ vara en ring.

- För $a, b \in R$ så skriver vi $a|b$ och säger att a **delar** b om det finns något $c \in R$ så att $a \cdot c = b$.
- Vi kallar $a \in R$ **irreducibelt** om det enda sättet att faktorisera a är $a = b \cdot (b^{-1}a)$ där b är ett inverterbart elementen i R.

Här är ett par exempel på vårt nya delbarhetsbegrepp:

Exempel 5.9

- I ringen $\mathbb{Z}$ har vi $3|54$, för $3 \cdot 17 = 54$.
- I ringen $\mathbb{R}[x]$ så har vi $(x+1)|(x^2+3x+2)$, för $(x+1)(x+2) = x^2+3x+2$.
- I ringen $\mathbb{Z}_6$ har vi $2|0$ eftersom t.ex. $2 \cdot 3 = 0$.

Irreducibla element är en motsvarighet till primtal i ringar. Man brukar dela upp de nollskilda ringelementen i tre typer: *inverterbara element*, *irreducibla element*, och de övriga kallas *reducibla*.

För heltalsringen är $\{1, -1\}$ de enda inverterbara elementen, de irreducibla är primtalen (och deras negativer), och de reducibla är de sammansatta talen.

Men varifrån kommer villkoret att de enda delarna är inverterbara element? Talet 7 är ju ett primtal, men ändå kan sju skrivas som t.ex. $(-1)\cdot(-7)$ eller $1 \cdot 7$. I dessa faktoriseringar är dock ena faktorn ett inverterbart element i $\mathbb{Z}$, så 7 räknas ändå som irreducibelt.

På samma vis är $(x+3)$ irreducibelt i ringen $\mathbb{R}[x]$. Förvisso kan vi faktorisera $(x+3) = 7\cdot(\frac{1}{7}x+\frac{3}{7})$, men ena faktorn 7 är ju inverterbar i ringen $\mathbb{R}[x]$, så $(x+3)$ är ändå irreducibelt.

Vi bör också ignorera inverterbara element när vi tittar på faktoriseringar av andra ringelement. Vi har en primtalsfaktorisering $15 = 5 \cdot 3$ men vi kan också exempelvis skriva $15 = (-3) \cdot (-5)$. Dessa två sätt att skriva 15 betraktas ändå som samma faktorisering, eftersom om man byter plats på faktorerna och multiplicerar varje faktor med det *inverterbara* talet -1 i ringen, så får man den gamla faktoriseringen.

Analogt kan vi i $\mathbb{R}[x]$ skriva både

$$2x^2 + 10x + 12 = (2x+4)\cdot(x+3) \quad \text{och} \quad 2x^2 + 10x + 12 = (2x+6)(x+2),$$

men dessa kan ändå betraktas som samma faktorisering, eftersom de bara skiljer sig via omflyttning av faktorer och multiplikation med inverterbara element.

Exempel 5.10

- I ringen $\mathbb{Z}$ är 13 irreducibelt, och 35 är reducibelt.
- I ringen $\mathbb{R}[x]$ så är $(x+5)$ irreducibelt. Alla polynom av form $ax+b$ är faktiskt irreducibla.
- I ringen $\mathbb{C}[x]$ är polynomet x^2+1 reducibelt eftersom $x^2+1 = (x+i)(x-i)$. I ringen $\mathbb{R}[x]$ är dock polynomet x^2+1 irreducibelt!
- I ringen $\mathbb{Z}_2[x]$ är polynomet x^2+x+1 irreducibelt.

Men i vissa ringar kan man faktiskt faktorisera samma element på olika sätt! Om vi exempelvis tittar på ringen $(\mathbb{Z}_6, +, \cdot)$ så kan 4 skrivas på två sätt:

$$2 \cdot 2 = 4 = 2 \cdot 5$$

Dessa sätt är verkligen olika eftersom man inte kan få ena faktorn 2 till vänster genom att multiplicera 5 med ett inverterbart element.

De felsta ringar vi ska titta på är dock **ringar med entydig faktorisering**: ringar där varje reducibelt element kan skrivas på ett *unikt sätt* som en produkt av irreducibla element (upp till multiplikation med inverterbara element och omordning av faktorer).

5.6 Gaussiska heltal

Definition 5.5

Vi definierar de **Gaussiska heltalen** som följande delmängd av $\mathbb{C}$:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

Vi definierar addition och multiplikation av Gaussiska heltal precis som för komplexa tal.

Eftersom $\mathbb{C}$ själv är en ring så räcker det att testa att operationerna $+$ och $\cdot$ är slutna på $\mathbb{Z}[i]$, vilket är lätt att testa. Det följer att de Gaussiska heltalen är en ring.

Endast fyra element i $\mathbb{Z}[i]$ är inverterbara: $\{1, -1, i, -i\}$.

Man kan också bevisa att $\mathbb{Z}[i]$ är en ring med entydig faktorisering.

De irreducibla elementen i $\mathbb{Z}[i]$ kallas *Gaussiska primtal*.

Exempel 5.11

Vanliga primtal behöver inte vara Gaussiska primtal! Exempelvis är talet 5 irreducibelt i $\mathbb{Z}$, men 5 är inte irreducibelt i $\mathbb{Z}[i]$ eftersom vi har en faktorisering av 5 som en produkt av två Gaussiska primtal: $5 = (2 + i) \cdot (2 - i)$.

Sats 5.2

Ett vanligt primtal $p \in N$ är ett Gaussiskt primtal om och endast om $p \equiv 3 \mod 4$.

Bevis

Vi visar endast ena riktningen av satsen: att om p är 1 modulo 4 så är p reducibelt i $\mathbb{Z}[i]$. Antag alltså att $p \equiv 1 \mod 4$. Ett resultat från talteori säger att primtalet p då kan skrivas som en summa av två kvadrater: $p = x^2 + y^2$ där x och y är heltal. Men då har vi en motsvarande faktorisering $p = (x + iy) \cdot (x - iy)$ i $\mathbb{Z}[i]$ så p är inget Gaussiskt primtal.

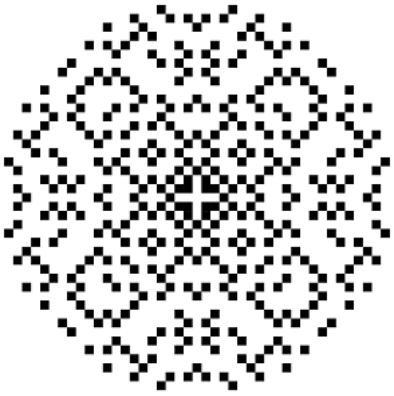
Vi formulerar en beskrivning av alla Gaussiska primtal utan bevis.

Sats 5.3

Satsen om Gaussiska primtal
Varje Gaussiskt primtal ligger i en av följande kategorier:

1. Låt p vara ett primtal i $\mathbb{N}$ som är 3 modulo 4. Då är $p, -p, ip$, och $-ip$ Gaussiska primtal.
2. När både a och b är nollskilda så är $a + bi$ är ett Gaussiskt primtal om och endast om $a^2 + b^2$ är ett vanligt primtal i $\mathbb{N}$.

I bilden nedan har vi markerat alla Gaussiska primtal z med $|z| < 20$ i det komplexa talplanet:



Exempel 5.12

Säg att vi vill primtalsfaktorisera $182 - 182i$. Vi ser snabbt att vi har

$$182 - 182i = 182(1 - i) = 2 \cdot 7 \cdot 13 \cdot (1 - i).$$

Härifrån behandlar vi faktorerna separat. 7 är ett gaussiskt primtal enligt satsen. Eftersom $2 = 1^2 + 1^2$ så har vi också $2 = (1 + i)(1 - i)$ och dessa båda faktorer är Gaussiska primtal enligt satsen. På samma vis har vi $13 = 3^2 + 2^2$ och därför är $13 = (3 + 2i)(3 - 2i)$ en primtalsfaktorisering i $\mathbb{Z}[i]$. Till slut har vi $(1 - i) = -i(1 + i)$ alltså ett inverterbart element multiplicerat med ett primtal - alltså är $(1 - i)$ ett Gaussiskt primtal. Vår slutsats blir att

$$182 - 182i = (1 + i) \cdot (1 - i) \cdot 7 \cdot (3 + 2i) \cdot (3 - 2i) \cdot (1 - i)$$

är en faktorisering med Gaussiska primtal.

5.7 Algebraiska heltal

Definition 5.6

Ett komplext tal α kallas för ett **algebraiskt heltal** om det finns ett polynom $p(x) \in \mathbb{Z}[x]$ med heltalskoefficienter och där högstagradskoefficienten är 1, så att $p(x) \in \mathbb{Z}[x]$ som uppfyller $p(\alpha) = 0$.

Polynom där högstagradskoefficienten är 1 kallas också *moniska* polynom. Man kan visa att de algebraiska heltalen utgör en delring av $\mathbb{C}$.

Exempel 5.13

- 5 är ett algebraiskt heltal eftersom 5 är ett nollställe till polynomet $x - 5$.
- $\sqrt{3}$ är ett algebraiskt heltal eftersom $\sqrt{3}$ är ett nollställe till $x^2 - 3$.
- π är *inte* ett algebraiskt heltal. Man kan bevisa att $p(\pi) \neq 0$ för alla polynom p (utom det konstanta noll-polynomet såklart).

Exempel 5.14

Är $\sqrt{3+\sqrt{5}}$ ett algebraiskt heltal?

Låt $\alpha = \sqrt{3+\sqrt{5}}$. Vi försöker hitta ett polynom som har α som nollställe. Vi har $\alpha^2 = 3+\sqrt{5}$, så $\alpha^2 - 3 = \sqrt{5}$ och $(\alpha^2-3)^2 = 5$, och $0 = (\alpha^2-3)^2 - 5 = \alpha^4 - 6\alpha^3 + 4$. Så om vi tar $p(x) = x^4 - 6x^3 + 4$ så har vi $p(\alpha) = 0$ och därför är $\alpha = \sqrt{3+\sqrt{5}}$ ett algebraiskt heltal.

5.8 Kroppar

Definition 5.7

En **kropp** är en ring $(K, \oplus, \otimes)$ där multiplikationen $\otimes$ är kommutativ och alla element utom det additiva identitetselementet har en multiplikativ invers. Det sista villkoret är samma sak som att säga att $(K\backslash\{\mathbf{0}\}, \otimes)$ är en grupp.

Vanliga exempel på kroppar är $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, och $\mathbb{Z}_p$ där p är ett primtal.

Mycket matematik kan utföras oberoende av vilket kropp man arbetar med. Om K är en kropp kan vi exempelvis studera alla polynom med koefficienter i K. Vi kan också studera $\mathrm{Mat}_{n\times n}(K)$, alltså mängden av $n\times n$-matriser vars koefficienter tillhör K. Eftersom alla element utom 0 har multiplikativ invers så kan man alltid lösa ekvationer av formen $ax = b$ i K.

Övningsuppgifter

5.1 Utför följande räkningar i ringen $\mathbb{Z}\times\mathbb{Z}_3$:

(a) Beräkna $(13, 2) + (5, 2)$

(b) Beräkna $(3, 2) \cdot (1, 2)$

(c) Beräkna $(2, 2)^5$

5.2 Utför följande räkningar i polynomringen $\mathbb{Z}_5[x]$.

(a) Beräkna $(x^5 + 2x^4 + 3x^2 + 4x + 3) + (2x^4 + 2x^3 + x^2 + 2x + 4)$

(b) Beräkna $(2x^2 + 3x + 4) \cdot (3x + 2)$

(c) Beräkna $(x + 1)^5$

5.3 Vi tittar på ringen $\mathrm{Mat}_{2\times 2}(\mathbb{Z}_5)$ och två av dess element:

$$A = \begin{bmatrix} 2 & 3 \\ 2 & 0 \end{bmatrix} \quad \text{och} \quad B = \begin{bmatrix} 4 & 1 \\ 3 & 1 \end{bmatrix}.$$

Beräkna $A + B$ och $A \cdot B$ och $B \cdot A$.

5.4 Hur många element har ringen $\mathrm{Mat}_{2\times 2}(\mathbb{Z}_2)$? Vilka av elementen är *inverterbara*?

5.5 Ett element a in ring kallas för en *idempotent* om $a \cdot a = a$.

(a) Hitta alla idempotenter i $\mathbb{C}$.

(b) Hitta fyra olika idempotenter i ringen $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$, alltså ringen av 2×2-matriser med heltalskoefficienter.

5.6 Det finns totalt åtta tredjegradspolynom i $\mathbb{Z}_2[x]$. Skriv ned dessa och ta reda på vilka av dem som är irreducibla.

5.7 Visa att $\alpha = \sqrt{2} + \sqrt{3}$ är ett algebraiskt heltal genom att hitta ett polynom $p(x) \in \mathbb{Z}[x]$ som uppfyller $p(\alpha) = 0$. *Tips*: börja med att kvadrera α!

5.8 I en ring gäller att $r|0$ för alla r i ringen eftersom $0 \cdot r = 0$ (0 är alltså det additiva identitetselementet i R). Men om det finns två *nollskilda* $a, b \in R$ så att $a \cdot b = 0$, så kallas a och b för **nolldelare**.

(a) Hitta en nolldelare i $\mathrm{Mat}_{2\times 2}(\mathbb{R})$.

(b) Hitta alla nolldelare i $\mathbb{Z}_{15}$.

5.9 Lista alla Gaussiska heltal $|z|$ i första kvadranten som uppfyller $|z| \leq 5$, och ta reda på vilka av dessa som är Gaussiska primtal. Med andra ord, hitta alla $a + bi$ där $a^2 + b^2 \leq 25$ och $a > 0$ och $b \geq 0$). Ta reda på vilka av dessa som är Gaussiska primtal.

5.10 Faktorisera följande Gaussiska heltal som produkter av Gaussiska primtal. *Tips:* prova eventuellt att dividera med Gaussiska primtal från förra övningen!

(a) $10i$

(b) $4 + 3i$

(c) $5 + 5i$

5.11 *Karaktäristiken* $\mathrm{char}(R)$ för en ring R är det minsta antalet ettor (alltså identitetselementet i R) som man kan addera så att resultatet blir 0. Om resultatet aldrig blir 0 skriver man $\mathrm{char}(R) = 0$. Bestäm karaktäristiken för följande ringar:

(a) Heltalen $\mathbb{Z}$

(b) Polynomringen $\mathbb{R}[x]$

(c) Heltal modulo femton, $\mathbb{Z}_{15}$

(d) Ringen $\mathbb{Z}_4 \times \mathbb{Z}_6$

5.12 Ett vanligt misstag för nybörjare inom matematik är att skriva $(a + b)^n = a^n + b^n$. Misstaget är så vanligt att det på engelska börjat kallas "Freshman's dream". Bevisa att om n är ett primtal så är drömmen verklighet i ringen $\mathbb{Z}_n$!

5.13 Det finns en kropp $(K, +, \cdot)$ med fyra element $K = \{\heartsuit, \diamondsuit, \spadesuit, \clubsuit\}$. Operationerna ges i följande tabeller:

$+$	$\clubsuit$	$\heartsuit$	$\spadesuit$	$\diamondsuit$
$\clubsuit$	$\clubsuit$	$\heartsuit$	$\spadesuit$	$\diamondsuit$
$\heartsuit$	$\heartsuit$	$\clubsuit$	$\diamondsuit$	$\spadesuit$
$\spadesuit$	$\spadesuit$	$\diamondsuit$	$\clubsuit$	$\heartsuit$
$\diamondsuit$	$\diamondsuit$	$\spadesuit$	$\heartsuit$	$\clubsuit$

$\cdot$	$\clubsuit$	$\heartsuit$	$\spadesuit$	$\diamondsuit$
$\clubsuit$	$\clubsuit$	$\clubsuit$	$\clubsuit$	$\clubsuit$
$\heartsuit$	$\clubsuit$	$\heartsuit$	$\spadesuit$	$\diamondsuit$
$\spadesuit$	$\clubsuit$	$\spadesuit$	$\diamondsuit$	$\heartsuit$
$\diamondsuit$	$\clubsuit$	$\diamondsuit$	$\heartsuit$	$\spadesuit$

I den här uppgiften ska vi öva på att räkna i denna kropp.

(a) Beräkna $\diamondsuit \cdot (\diamondsuit + ((\diamondsuit + \clubsuit) \cdot \spadesuit))$.

(b) Har $(K, +)$ ett identitetselement? Ett nollelement?

(c) Har $(K, \cdot)$ ett identitetselement? Ett nollelement?

(d) Hitta de additiva inverserna $-\clubsuit$, $-\heartsuit$, $-\spadesuit$, och $-\diamondsuit$ i $(K, +)$.

(e) Hitta de multiplikativa inverserna $\heartsuit^{-1}$, $\spadesuit^{-1}$, och $\diamondsuit^{-1}$ i $(K, \cdot)$.

(f) Det går att räkna med matriser med koefficienter i K på precis samma vis som med vanliga matriser. Beräkna $\begin{bmatrix} \clubsuit & \heartsuit \\ \spadesuit & \diamondsuit \end{bmatrix} \cdot \begin{bmatrix} \heartsuit \\ \spadesuit \end{bmatrix}$.

(g) Vilket är identitetselementet i $(\mathrm{Mat}_{2\times 2}(K), \cdot)$, alltså mängden 2×2-matriser med koefficienter i K med matrismultiplikation?

(h) Lös ekvationen $\spadesuit(x + \heartsuit) = \diamondsuit$. Beskriv hur du hittar lösningen!

(i) "Roten ur" är något vi bara definierat för reella tal. Hur skulle du välja att definiera "roten ur" på K? Vad blir då $\sqrt{\clubsuit}$, $\sqrt{\heartsuit}$, $\sqrt{\spadesuit}$, och $\sqrt{\diamondsuit}$?

(j) Se om förra deluppgiften kan användas för att lösa ekvationen $x^2 + \heartsuit = \spadesuit$.