KTH Matematik

KTHs Matematiska Cirkel

Gruppteori

Joakim Arnlind

Andreas Enblom

Institutionen för matematik, 2006

Finansierat av Marianne och Marcus Wallenbergs Stiftelse

Innehåll

Några ord på vägen

Detta kompendium är skrivet för att användas som litteratur till KTHs Matematiska Cirkel under läsåret 2006–2007 och består av sju avsnitt. Kompendiet är inte tänkt att läsas enbart på egen hand, utan ska ses som ett skriftligt komplement till undervisningen på de sju träffarna.

Som den mesta matematik på högre nivå är kompendiet kompakt skrivet. Detta innebär att man i allmänhet inte kan läsa det som en vanlig bok. Istället bör man pröva nya satser och definitioner genom att på egen hand exemplifiera. Därmed uppnår man oftast en mycket bättre förståelse av vad dessa satser och deras bevis går ut på.

Övningsuppgifterna är fördelade i två kategorier. De med udda nummer har facit, och syftet med dessa är att eleverna ska kunna räkna dem och på egen hand kontrollera att de förstått materialet. De med jämna nummer saknar facit och kan användas som examination. Det rekommenderas dock att man försöker lösa även dessa uppgifter även om man inte examineras på dem. Om man kör fast kan man alltid fråga en kompis, en lärare på sin skola eller någon av oss.

Vi bör också nämna att få av uppgifterna är helt enkla. Kika därför inte i facit efter några få minuter (om du inte löst uppgiften), utan prata först med kompisar eller försök litet till. Alla uppgifter ska gå att lösa med hjälp av informationen i detta kompendium.

KTHs Matematiska Cirkel finasieras av Marianne och Marcus Wallenbergs Stiftelse. Vi tackar Dan Laksov och Roy Skjelnes, båda från Institutionen för Matematik vid KTH, för deras givande kommentarer om denna skrift.

Några ord om Cirkeln

KTHs Matematiska Cirkel, i dagligt tal benämnd Cirkeln, startade 1999. Dess ambition är att sprida kunskap om matematiken och dess användningsområden utöver vad eleverna får genom gymnasiekurser, och att etablera ett närmare samarbete mellan gymnasieskolan och högskolan. Cirkeln skall särskilt stimulera elevernas matematikintresse och inspirera dem till fortsatta naturvetenskapliga studier. Lärarna på cirkeln kan vid behov ge eleverna förslag på ämnen till projektarbeten vid gymnasiet.

Till varje kurs skrivs ett kompendium som distribueras gratis till eleverna. Detta material, liksom övriga uppgifter om KTHs Matematiska Cirkel, finns tillgängligt på

`http://www.math.kth.se/cirkel`

Sedan 2001 godkänns Cirkeln av Stockholms Stad som en 50-poängskurs eller som matematisk breddning. Det är upp till varje skola att godkänna Cirkeln som en kurs och det är lärarna från varje skola som sätter betyg på kursen. Lärarna är självklart också välkomna till Cirkeln och många har kommit överens med sin egen skola om att få Cirkeln godkänd som fortbildning eller som undervisning. Vi vill gärna understryka att föreläsningarna är öppna för alla gymnasieelever och lärare.

Vi har avsiktligt valt materialet för att ge eleverna en inblick i matematisk teori och tankesätt och presenterar därför både några huvudsatser inom varje område och bevisen för dessa resultat. Vi har också som målsättning att bevisa alla satser som används om de inte kan förutsättas bekanta av elever från gymnasiet. Detta, och att flera ämnen är på universitetsnivå, gör att lärarna och eleverna kan uppleva programmet som tungt, och alltför långt över gymnasienivån. Meningen är emellertid inte att lärarna och eleverna skall behärska ämnet fullt ut och att lära in det på samma sätt som gymnasiekurserna. Det viktigaste är att eleverna kommer i kontakt med teoretisk matematik och får en inblick i *matematikens väsen*. Vår förhoppning är att lärarna med denna utgångspunkt skall ha lättare att upplysa intresserade elever om KTHs Matematiska Cirkel och övertyga skolledarna om vikten av att låta både elever och lärare delta i programmet.

Några ord om betygssättning

Ett speciellt problem tidigare år har varit betygssättningen. Detta borde emellertid bara vara ett problem om lärarna använder sig av samma standard som de gör när de sätter betyg på ordinarie gymnasiekurser. Om utgångspunkten istället är att eleverna skall få insikt i matematiken genom att gå på föreläsningarna och att eleven gör sitt bästa för att förstå materialet och lösa uppgifterna, blir betygsättningen lättare. Självklart betyder det mycket vad eleverna har lärt av materialet i kursen, men lärarna kan bara förvänta sig att ett fåtal elever behärskar ämnet fullt ut. I det perspektivet blir det lätt att använda de officiella kriterierna:

Godkänd: Eleven har viss insikt i de moment som ingår i kursen och kan på ett godtagbart sätt redovisa valda delar av kursen såväl muntligt som skriftligt. Detta kan ske genom att eleven håller föredrag inför klassen, redovisar eller lämnar en rapport till sin matematiklärare.

Väl godkänd: Eleven har god insikt i flera moment från kursen. Eleven kan redovisa dessa moment både skriftligt och muntligt och dessutom uppvisa lösningar på problem som givits på kursen. Detta kan ske genom att eleven håller föredrag inför klassen, redovisar eller lämnar en rapport till sin matematiklärare.

Mycket väl godkänd: Eleven har mycket god insikt i flera moment av kursen och lämnar skriftliga redovisningar av flera delar av kursen eller lämnar lösningar på problem som givits på kursen. Detta kan ske genom att eleven håller föredrag inför klassen, redovisar eller lämnar en rapport till sin matematiklärare.

Det är också möjligt att skolorna samarbetar, så elever från en skola redovisar eller lämnar rapport för en lärare i en annan skola.

Författarna, augusti 2006

1 Mängdlära

1.1 Mängder

Låt oss börja med att titta på något av det mest grundläggande i matematiken, nämligen mängder. En mängd är helt enkelt en samling matematiska objekt. Matematiska objekt är ofta tal eller andra mängder och brukar kallas *element*. Det enklaste sättet att beskriva en mängd är att räkna upp dess element. Ett sådant exempel är

$$A = \{1, 3, a, 7\}. \tag{1.1}$$

Detta betyder att A är en mängd som innehåller elementen $1, 3, a$ och 7. Ett annat sätt att beskriva en mängd är att skriva $\{x \in D \,:\, \text{villkor på } x\}$. Med detta menar man mängden av alla element i D som uppfyller de givna villkoren. Som exempel tar vi

$$B = \{n \in \{1, 2, 3, \ldots\} \,:\, n \text{ är udda}\} \tag{1.2}$$

och

$$C = \{y \in \{1, 2, 3, 4\} \,:\, y > 2\}. \tag{1.3}$$

Mängden B innehåller alla udda positiva heltal, medan C innehåller alla element från mängden $\{1, 2, 3, 4\}$ som är större än 2. Alltså har vi

$$B = \{1, 3, 5, 7, 9, 11, \ldots\} \quad \text{och} \quad C = \{3, 4\}. \tag{1.4}$$

Vi bryr oss inte om i vilken ordning eller hur många gånger elementen räknas upp och därmed gäller till exempel

$$\{1, 2, 3, 4\} = \{3, 1, 4, 2\} = \{1, 3, 3, 1, 2, 4, 4, 1, 3, 2, 4\}. \tag{1.5}$$

Om A är en mängd och x är ett element i mängden A så skriver vi $x \in A$ och säger att x *tillhör* A. Exempelvis gäller $17 \in \{n \,:\, n \text{ är ett udda heltal}\}$ och $b \in \{a, b, 10, 3\}$. Att ett element x inte tillhör mängden A skrivs $x \notin A$. Den *tomma mängden* innehåller ingenting och betecknas $\emptyset$.

Exempel 1.1.1. Låt $A = \{4, 5, 8, 4711, 12, 18\}$ och $B = \{x \in A \,:\, x > 10\}$. Då är $B = \{12, 18, 4711\}$ medan $\{x \in A \,:\, x < 3\} = \emptyset$. ▲

Definition 1.1.2. Låt A och B vara mängder. Om alla element i mängden A också är element i mängden B så sägs A vara en *delmängd* till B. Detta betecknas $A \subseteq B$.

Exempel 1.1.3. Mängden $\{1, a\}$ är en delmängd till $\{1, 3, a\}$, eftersom alla element i $\{1, a\}$ finns i mängden $\{1, 3, a\}$. Vi skriver $\{1, a\} \subseteq \{1, 3, a\}$. ▲

Definition 1.1.4. Antag att A och B är mängder. *Unionen* av A och B består av de element som ligger i någon av mängderna och betecknas $A \cup B$. *Snittet* av A och B består av de element som ligger i båda mängderna och betecknas $A \cap B$.

Exempel 1.1.5. Låt $A = \{1, 3, 5, 6\}$ och $B = \{5, 8, 3, 4711\}$. Då har vi $A \cup B = \{1, 3, 5, 6, 8, 4711\}$ och $A \cap B = \{3, 5\}$. ▲

Det är dags att titta på några viktiga talmängder. Den mängd vi använder för att räkna föremål är de naturliga talen $\{0, 1, 2, 3, \dots\}$. Denna mängd betecknas $\mathbb{N}$. Tar vi med negativa tal får vi heltalen $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$. Beteckningen kommer från tyskans *zahl* som betyder tal. Slutligen betecknar vi med $\mathbb{R}$ de *reella talen*, det vill säga alla tal på tallinjen, exempelvis $0, -1, 3/2, -527/3, \sqrt{2}$ och π. Notera att $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{R}$.

Exempel 1.1.6. Vi har att $\mathbb{N} = \{n \in \mathbb{Z} : n \geqslant 0\}$. ▲

Exempel 1.1.7. Mängden $\{n \in \mathbb{Z} : n = 2 \cdot k \text{ för något } k \in \mathbb{Z}\}$ är mängden av alla jämna heltal. Denna mängd kan också skrivas som $\{2 \cdot k : k \in \mathbb{Z}\}$, eller som $\{\dots, -4, -2, 0, 2, 4, \dots\}$. ▲

1.2 Funktioner

Innan vi gör en ordentlig definition av vad en funktion är kan det vara på sin plats att titta på något välbekant, nämligen en formel som $f(x) = x^2 + 1$. Detta är ett exempel på en funktion. Formeln säger att om vi tar ett tal $x \in \mathbb{R}$ så får vi ett nytt tal $f(x) \in \mathbb{R}$ genom att göra beräkningen $x^2 + 1$. Mer konkret kan vi ta talet 2 och få fram ett nytt tal $f(2) = 5$. Vi säger att f är en funktion från de reella talen till de reella talen, eftersom både det vi stoppar in, x, och det vi får ut, $f(x)$, är reella tal. Vi brukar beteckna detta med $f : \mathbb{R} \to \mathbb{R}$.

Definition 1.2.1. Låt X och Y vara mängder. En *funktion* $\phi : X \to Y$ är ett sätt att till varje element $a \in X$ tilldela ett välbestämt element $b \in Y$. Vi skriver $\phi(a) = b$. Vi säger att a *avbildas* på b och att b är *bilden* av a.

Anmärkning 1.2.2. Ofta säger man att ϕ är en funktion från X till Y istället för att använda beteckningen $\phi : X \to Y$. Ett vanligt alternativ till ordet funktion är *avbildning*.

Exempel 1.2.3. Betrakta mängderna $A = \{1, 2, 3\}$ och $B = \{2, 4, 6\}$. Ett exempel på funktion $f : A \to B$ ges av $f(n) = 2n$ för $n \in A$. Vi har alltså att $f(1) = 2$, $f(2) = 4$ och $f(3) = 6$.

Här definieras funktionen f av formeln $f(n) = 2n$, men det är inte alls nödvändigt att det finns en formel som beskriver hur funktionen verkar. Om vi som här har en funktion från en *ändlig* mängd A kan man till exempel definera funktionen med hjälp av en tabell:

n	$f(n)$
1	2
2	4
3	6

(1.6)

Till sist, om det vore så att $B = \{1, 2, 3, 4, 5, 6, 7\}$ så skulle fortfarande f vara en funktion $A \to B$, eftersom elementen $f(1), f(2)$ och $f(3)$ alla tillhör B. ▲

Exempel 1.2.4. Låt $C = \{1, 3, b, \{a, 7, 13\}\}$ och $D = \{a, \{1, 3\}, 2\}$. Dessa mängder innehåller alltså både tal, bokstäver och mängder. Ett exempel på avbildning $g : C \to D$ ges av

x	$g(x)$
1	$\{1, 3\}$
3	a
b	2
$\{a, 7, 13\}$	$\{1, 3\}$

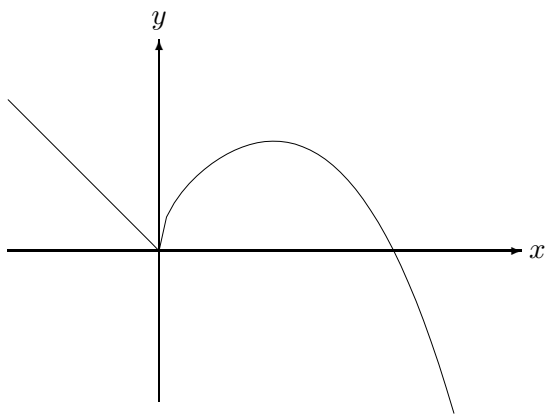
(1.7)

Exempelvis har vi alltså att $g(b) = 2$ och $g(\{a, 7, 13\}) = \{1, 3\}$. Eftersom mängden $\{a, 7, 13\}$ är ett element i C och g är en funktion från C till D så måste $g(\{a, 7, 13\})$ vara ett element i D. Att detta stämmer ser vi eftersom $g(\{a, 7, 13\}) = \{1, 3\}$ och eftersom mängden $\{1, 3\}$ är ett element i D. ▲

Exempel 1.2.5. Låt $h(x) = \sqrt{x} - x^3/3$. Då är h en funktion från mängden $\{x \in \mathbb{R} : x \geqslant 0\}$ till $\mathbb{R}$. Vi kan inte låta $x < 0$ eftersom $\sqrt{x}$ inte är väldefinerat i detta fall. Däremot skulle vi kunna definiera en funktion $\tilde{h} : \mathbb{R} \to \mathbb{R}$ genom att låta

$$\tilde{h}(x) = \begin{cases} \sqrt{x} - \frac{x^3}{3} & \text{om } x \geqslant 0 \\ -x & \text{om } x < 0. \end{cases} \tag{1.8}$$

Eftersom detta är en funktion $\mathbb{R} \to \mathbb{R}$ så kan vi symbolisera funktionen med grafen:



▲

1.3 Bijektioner

Definition 1.3.1. Låt X och Y vara mängder och $f : X \to Y$ en funktion. Funktionen f sägs vara en *injektion* om det är så att $f(x) \neq f(y)$ för alla $x, y \in X$ sådana att $x \neq y$. Vidare, om det för varje $y \in Y$ finns $x \in X$ så att $f(x) = y$ så är f en *surjektion*. Till sist, om f är både en injektion och en surjektion säger vi att f är en *bijektion*.

Låt oss fundera lite på vad detta betyder. Tag X, Y och f som i ovanstående definition. Att f är en injektion betyder att olika element i X avbildas på olika element i Y. Alltså, om vi har elementen $x, y \in X$ som är olika, det vill säga $x \neq y$, så måste $f(x)$ och $f(y)$ vara olika element i Y.

Exempel 1.3.2. Låt $X = \{1, 2, 3\}$ och $Y = \{1, 2, 3, 4, 5\}$. Definiera funktionen $f : X \to Y$ genom $f(x) = x + 1$. Detta är en injektion, eftersom $f(1), f(2)$ och $f(3)$ alla är olika. ▲

Exempel 1.3.3. Definiera funktionen $g : \mathbb{Z} \to \mathbb{Z}$ genom $g(n) = n^2$ för $n \in \mathbb{Z}$. Vi har exempelvis att $g(-2) = g(2) = 4$, och därmed är g inte en injektion. ▲

Exempel 1.3.4. Låt $A = \{a, b, c\}$ och $B = \{b, d\}$. Eftersom A innehåller 3 element men B bara 2 element så kan det inte finnas någon injektion $A \to B$. Detta kallas *Dirichlets lådprincip*: Om vi har k stycken lådor, och $k+1$ stycken bollar, måste minst en låda innehålla minst två bollar. Här har vi samma sak. Om vi har en funktion $h : A \to B$ så måste antingen b vara bilden av minst två element i A eller så måste d vara det. I varje fall är h inte en injektion. ▲

Att f är en surjektion betyder att varje element i Y är bilden av något element i X. Alltså, om y är ett element i Y så finns det ett element x i X så att y är bilden av x, det vill säga att $f(x) = y$.

Exempel 1.3.5. Låt $A = \{a, b, c\}$ och $B = \{a, c, d\}$. Betrakta funktionerna $f, g : A \to B$ som ges av tabellen

x	$f(x)$	$g(x)$
a	c	c
b	d	c
c	a	a

(1.9)

Eftersom $a = f(c), c = f(a)$ och $d = f(b)$ så är f en surjektion. Däremot finns det inte $x \in A$ så att $g(x) = d$, så g är inte en surjektion. ▲

Exempel 1.3.6. Funktionen i Exempel 1.3.2 är ingen surjektion, eftersom det inte finns $x \in X$ sådant att $f(x) = 1$ (och inte heller något element som avbildas på 5). ▲

En bijektion är alltså en funktion som är både en injektion och en surjektion. Det betyder att varje element i X motsvarar ett och endast ett element i Y, och tvärtom. Vi parar alltså ihop elementen i X och Y.

Exempel 1.3.7. Låt $A = \{10, 11, 22, 4711\}$ och $B = \{1, 2, 3, 4\}$. Betrakta funktionen $\rho : A \to B$ som ges av tabellen

x	$\rho(x)$
10	4
11	2
22	1
4711	3

(1.10)

Detta är en bijektion. Funktionen ρ parar ihop elementen som $10 \leftrightarrow 4$, $11 \leftrightarrow 2$, $22 \leftrightarrow 1$ och $4711 \leftrightarrow 3$, så varje element i A har en motsvarighet i B och tvärtom. Notera att A och B har lika många element. Detta hänger ihop med att det finns en bijektion mellan mängderna, se nedan. ▲

Exempel 1.3.8. Låt $\phi(x) = x - 3$ för $x \in \mathbb{Z}$. Då är ϕ en bijektion $\mathbb{Z} \to \mathbb{Z}$. ▲

1.4 Inversfunktioner

Betrakta två (inte nödvändigtvis olika) mängder X och Y, samt en bijektion $f : X \to Y$. Till varje $y \in Y$ finns exakt ett $x \in X$ sådant att $f(x) = y$. Det är just detta som utmärker en bijektion. Alltså kan vi definiera en ny funktion, $g : Y \to X$ genom att låta

$$g(y) \text{ vara det } x \in X \text{ som uppfyller att } f(x) = y, \tag{1.11}$$

för varje $y \in Y$. Notera nu att $f(g(y)) = y$ och att $g(f(x)) = x$ för alla $x \in X$ och $y \in Y$. När det är på detta sätt brukar vi säga att f och g är *inverser* till varandra. Vi skriver dessutom

$$g = f^{-1} \quad \text{och} \quad f = g^{-1}. \tag{1.12}$$

Inversen till en bijektion $h : X \to Y$ betecknas alltså med h^{-1} och uppfyller $h^{-1}(h(x)) = x$ och $h(h^{-1}(y)) = y$ för alla $x \in X$ och $y \in Y$.

Exempel 1.4.1. Låt $X = \{1, 2, 3\}$, och $Y = \{2, 3, 4\}$. Betrakta bijektionen $\phi : X \to Y$ definierad av $\phi(x) = x + 1$ för $x \in X$. Då har ϕ inversfunktionen ϕ^{-1} som uppfyller $\phi^{-1}(y) = y - 1$ för $y \in Y$. Detta eftersom $\phi^{-1}(\phi(x)) = \phi^{-1}(x + 1) = (x + 1) - 1 = x$ och $\phi(\phi^{-1}(y)) = \phi(y - 1) = (y - 1) + 1 = y$ för alla $x \in X$ och $y \in Y$. ▲

Det är nu viktigt att notera att det bara är bijektioner som har inverser. För andra funktioner är det alltid något i argumenten ovan som inte stämmer. Till exempel, om en funktion $f : X \to Y$ inte är en injektion så finns det $x, y \in X$ med $x \neq y$ men $f(x) = f(y)$. Låt nu $z = f(x) = f(y)$. Om det skulle vara så att det fanns en inversfunktion f^{-1} så skulle den uppfylla både $f^{-1}(z) = x$ och $f^{-1}(z) = y$. Men eftersom $x \neq y$ så är detta omöjligt.

Sats 1.4.2. *Låt $f : X \to Y$ vara en bijektion. Då är inversen $f^{-1} : Y \to X$ också en bijektion.*

Bevis. Vi visar först att f^{-1} är en injektion. Tag $u, v \in Y$ med $u \neq v$. Låt $x = f^{-1}(u)$ och $y = f^{-1}(v)$. Då har vi att $f(x) = u$ och $f(y) = v$. Antag att $x = y$. Då måste $u = f(x) = f(y) = v$ men vi vet att $u \neq v$ så detta är omöjligt. Alltså gäller $x \neq y$. Eftersom $u, v \in Y$ var godtyckliga så visar detta att $f^{-1}(u) \neq f^{-1}(v)$ för alla $u, v \in Y$ med $u \neq v$. Alltså är f^{-1} en injektion.

Vidare, tag $v \in X$. Låt $u = f(v)$. Då gäller $f^{-1}(u) = v$. Alltså finns det för varje $v \in X$ ett $u \in Y$ sådant att $f^{-1}(u) = v$. Detta betyder att f^{-1} är en surjektion.

Nu har det alltså visats att f^{-1} både är en injektion och en surjektion. Alltså är f^{-1} en bijektion. □

1.5 Storlekar på mängder

Låt X vara en mängd. Om det finns ett heltal n sådant att X innehåller exakt n element, så sägs X vara *ändlig*. I annat fall sägs mängden vara *oändlig*. Om X är en ändlig mängd så betecknar vi med $|X|$ antalet element i X. En ändlig mängd innehåller alltså ett ändligt antal element. Bijektioner kan användas för att jämföra ändliga mängder:

Sats 1.5.1. *Antag att n och m är positiva heltal. Låt A vara en mängd som innehåller n element och B en mängd som innehåller m element. Då har vi att $n = m$ om och endast om det finns en bijektion mellan A och B.*

Vi bevisar inte denna sats här. Men det är en lämplig övning för den intresserade läsaren.

Att det finns en bijektion mellan två ändliga mängder är alltså precis vad vi menar med att de innehåller lika många element. Men hur är det med oändliga mängder? Jo, det visar sig att oändliga mängder kan vara olika stora. Lite löst kan man säga att det finns olika stora oändligheter.

Exempel 1.5.2. Betrakta de oändliga mängderna $\mathbb{N}$, $\mathbb{Z}$ och $\mathbb{R}$. Det är lätt att hitta en bijektion mellan $\mathbb{N}$ och $\mathbb{Z}$, och därför anser vi att de är lika stora, trots att $\mathbb{N}$ är en delmängd till $\mathbb{Z}$ och att det finns element i $\mathbb{Z}$ som inte tillhör $\mathbb{N}$. Betrakta till exempel funktionen

$$\phi(n) = \begin{cases} -n/2 & \text{om } n \text{ är jämnt} \\ (n+1)/2 & \text{om } n \text{ är udda} \end{cases} \tag{1.13}$$

från $\mathbb{N}$ till $\mathbb{Z}$. Vi har att $\phi(0) = 0, \phi(1) = 1, \phi(2) = -1, \phi(3) = 2, \phi(4) = -2$ och så vidare. Notera att alla tal i $\mathbb{Z}$ kommer med i denna uppräkning, och alltså är ϕ en surjektion. Vidare ser vi att om $n, m \in \mathbb{N}$ och $n \neq m$ så är $\phi(n) \neq \phi(m)$, och därmed är ϕ en injektion. Alltså är ϕ ett exempel på en bijektion $\mathbb{N} \to \mathbb{Z}$.

Däremot kan man visa att det inte finns någon bijektion $\mathbb{N} \to \mathbb{R}$. Detta visades i förra årets Cirkel. Det finns gott om injektioner, men inga surjektioner, och därför inga bijektioner, från $\mathbb{N}$ till $\mathbb{R}$. För vissa känns detta helt naturligt, för andra väldigt konstigt, men så är det i alla fall. Vi brukar förklara detta fenomen med att $\mathbb{R}$ är större än $\mathbb{N}$, fast de båda är oändliga. ▲

Övning 1.1. Låt $A = \{1, 2, 3, 4, \ldots\}$, $B = \{1, 3, 5, 7, \ldots\}$, $C = \{2, 4, 6, 8, \ldots\}$ och $D = \{1, 4, 19, 36, 101\}$. Bestäm mängderna

1. $B \cup C$,
2. $B \cap C$,
3. $D \cap C$,
4. $\{x \in D : x \in B\}$,
5. $\{x \in A : x = y + 1 \text{ för något } y \in D\}$,
6. $\{x + 1 : x \in D\}$.

Övning 1.2. Låt $X = \{0, 2, 4, \ldots\}$ och definiera en funktion $f : X \to \mathbb{Z}$ genom $f(n) = n/2$. Visa att f är en injektion men ingen surjektion.

Övning 1.3. Låt $f(n) = n - 3$ för $n \in \mathbb{Z}$. Visa att $f : \mathbb{Z} \to \mathbb{Z}$ är en surjektion.

Övning 1.4. Låt X vara en mängd och definiera funktionen $\psi : X \to X$ genom att låta $\psi(x) = x$ för alla $x \in X$. Visa att ψ är en bijektion.

2 Grupper

2.1 Binära operationer

Låt X vara en mängd. Vi definierar nu den *kartesiska kvadraten* av X som mängden $\{(x, y) : x, y \in X\}$. Den kartesiska produkten består alltså av alla ordnade par (x, y), där $x, y \in X$. Vi betecknar den kartesiska kvadraten med $X \times X$ eller X^2.

Anmärkning 2.1.1. Om $x, y \in X$ och $x \neq y$ så är (x, y) och (y, x) olika element. Här har alltså ordningen på elementen betydelse. Vidare är det helt tillåtet att $x = y$.

Exempel 2.1.2. Låt $A = \{1, 2, 3\}$. Då gäller

$$A^2 = \{(1,1), (1,2), (1,3), (2,1), (2,2), (2,3), (3,1), (3,2), (3,3)\}. \tag{2.1}$$

För att förtydliga den ovanstående anmärkningen, notera exempelvis att $(1, 2) \neq (2, 1)$ och att $(1, 1) \in A^2$.

Vi ser att A^2 innehåller 9 element. Allmänt gäller att om X är en ändlig mängd med n element, så finns det n^2 element på mängden X^2. ▲

Exempel 2.1.3. Vi ser att $\mathbb{Z}\times\mathbb{Z}$ innehåller element som $(0, 0), (0, 1), (-3, 4711)$ och $(35, -2)$. ▲

Definition 2.1.4. Låt X vara en mängd. En *binär operation* B på X är en funktion $B : X \times X \to X$. Om $x, y \in X$ och B är en binär operation på X så skriver vi xBy istället för $B((x, y))$.

Exempel 2.1.5. Låt $X = \{a, c\}$. Då är $X \times X = \{(a, a), (a, b), (b, a), (b, b)\}$. Betrakta funktionen $B : X \times X \to X$ som ges av

ξ	$B(\xi)$
(a, a)	b
(a, b)	a
(b, a)	b
(b, b)	b

(2.2)

Detta är alltså en binär operation. Vi ser exempelvis att $aBb = a$. Ett mer naturligt sätt att beskriva denna binära operation är genom följande operationstabell:

B	a	b
a	b	a
b	b	b

(2.3)

Ur denna tabell läser vi att $aBa = b$, $aBb = a$, $bBa = b$ och $bBb = b$. Det vill säga, radindexet x står till vänster om B i xBy och kolumnindexet y står till höger om B. Notera att $aBb \neq bBa$ i detta exempel, och att det därmed är extra viktigt hur man läser tabellen. ▲

Exempel 2.1.6. För reella tal x och y, låt $x \circ y = x^2 - 3y^3$. Då är $\circ$ en binär operation på mängden $\mathbb{R}$. ▲

Exempel 2.1.7. Addition är en binär operation på mängden $\mathbb{Z}$. Vi vet ju att $n + m \in \mathbb{Z}$ för alla $n, m \in \mathbb{Z}$. Vi kan alltså se addition som en funktion

$$+ : \mathbb{Z}^2 \to \mathbb{Z}. \tag{2.4}$$

Här är det väldigt naturligt att skriva $n+m$ istället för $+((n, m))$. På samma sätt är multiplikation en binär operation i $\mathbb{Z}$. Här ser vi också det naturliga i att beskriva en binär operation med en operationstabell, i detta fall (ett urklipp ur) multiplikationstabellen:

$\cdot$	-1	0	1	2	3
-1	1	0	-1	-2	-3
0	0	0	0	0	0
1	-1	0	1	2	3
2	-2	0	2	4	6
3	-3	0	3	6	9

(2.5)

▲

2.2 Grupper

Nu är det dags att introducera grupper. Grupper är något som förekommer överallt i matematiken. En grupp är en mängd med en binär operation som uppfyller några få grundläggande villkor. Tanken med gruppteori är att utifrån dessa enkla villkor, som så många olika saker har gemensamt, kunna härleda en mängd användbara egenskaper en gång för alla. Vi börjar med den abstrakta definitionen, och fortsätter sedan med exempel.

Definition 2.2.1. Låt G vara en mängd. Antag att det finns en binär operation $\circ$ på mängden G. Den uppfyller, liksom alla binära operationer på G, att $x \circ y \in G$ för alla $x, y \in G$. Vi säger att G är *sluten* under operationen $\circ$. Antag också följande:

1. Vi har att $x \circ (y \circ z) = (x \circ y) \circ z$ för alla $x, y, z \in G$. Vi säger att operationen $\circ$ är *associativ* i G.

2. Det finns ett element $e \in G$ som uppfyller att $x \circ e = e \circ x = x$ för alla $x \in G$. Detta element kallas för en *identitet* eller ett *enhetselement* i G.

3. För varje element $x \in G$ finns ett element $x^{-1} \in G$ sådant att $x \circ x^{-1} = x^{-1} \circ x = e$. Elementet x^{-1} kallas en *invers* till x.

Då säger vi att G med operationen $\circ$ är en *grupp*. Egenskaperna 1 – 3 kallas för *gruppaxiomen*. För att poängtera att det är med operationen $\circ$ som G är en grupp, så brukar man ibland beteckna gruppen med $(G, \circ)$.

Exempel 2.2.2. Det mest naturliga exemplet på en grupp är heltalen $\mathbb{Z}$ med operationen $+$. Att addition är en binär operation har vi redan diskuterat, och det är välkänt att $x + (y + z) = (x + y) + z$ för alla heltal x, y, z. Vad är då en identitet hos heltalen? Jo, helt enkelt talet 0. Det uppfyller ju att $x + 0 = 0 + x = x$ för alla heltal x. Till sist, en invers till ett tal $x \in \mathbb{Z}$ är $-x$ eftersom $x + (-x) = (-x) + x = 0$. Vi sätter alltså $x^{-1} = -x$ och ser att $x + x^{-1} = x^{-1} + x = 0$. ▲

Exempel 2.2.3. De naturliga talen $\mathbb{N}$ med operationen $+$ är *inte* en grupp. De uppfyller visserligen 1 och 2 i Definition 2.2.1, men inte 3, eftersom elementen $-1, -2, -3, \ldots$ inte tillhör mängden $\mathbb{N}$. ▲

Exempel 2.2.4. De reella talen med addition är en grupp. Talet 0 är en identitet och en invers till x ges av $-x$. ▲

Exempel 2.2.5. Låt $G = \{x \in \mathbb{R} : x \neq 0\}$. Mängden G innehåller alltså alla reella tal förutom 0, och betecknas ofta $\mathbb{R} \setminus \{0\}$. Det visar sig att denna mängd är en grupp med vanlig multiplikation av tal som operation.

Att multiplikation av tal är en associativ binär operation på mängden G är klart. I denna mängd är det talet 1 som fungerar som en identitet. Vi har ju att $x \cdot 1 = 1 \cdot x = x$ för alla $x \in G$. Till sist, för $x \in G$ är en invers $x^{-1} = 1/x$. Detta eftersom $x \cdot (1/x) = (1/x) \cdot x = 1$.

Att en invers till x är $1/x$ är förklaringen till att vi måste ta bort talet 0 från de reella talen för att få en grupp under multiplikation. Det går ju inte att dividera med 0.

Jämför denna grupp med gruppen i Exempel 2.2.4. Vi ser att de reella talen har två olika naturliga gruppstrukturer. Dels den *additiva gruppen* $\mathbb{R}$ med operationen $+$, dels den *multiplikativa gruppen* $\mathbb{R} \setminus \{0\}$ med operationen $\cdot$. Vi brukar också säga att 0 är en *additiv identitet* i $\mathbb{R}$ och att 1 är en *multiplikativ idenititet* i $\mathbb{R}$. På samma sätt säger vi att en *additiv invers* till talet x är $-x$ och att en *multiplikativ invers* till x är $1/x$.

Slutligen kan vi notera att heltalen $\mathbb{Z}$ inte har någon multiplikativ grupp. Heltalen är en grupp under addition (se Exempel 2.2.2). Men heltalen är inte en grupp under multiplikation, inte ens om vi tar bort talet 0, eftersom $1/x$ inte är ett heltal för andra heltal än 1 och -1. Det krävs ju att en invers till ett element i en grupp också tillhör gruppen. ▲

Exempel 2.2.6. Låt $X = \{a, b\}$. Definiera en binär operation $\circ$ på X genom tabellen

$\circ$	a	b
a	a	b
b	b	a

(2.6)

Låt oss visa att X med operationen $\circ$ är en grupp. Vi har att

$$\begin{aligned}
a \circ (a \circ a) &= a \circ a = (a \circ a) \circ a \\
a \circ (a \circ b) &= a \circ b = (a \circ a) \circ b \\
a \circ (b \circ a) &= a \circ b = b = b \circ a = (a \circ b) \circ a \\
a \circ (b \circ b) &= a \circ a = a = b \circ b = (a \circ b) \circ b \\
b \circ (a \circ a) &= b \circ a = (b \circ a) \circ a \\
b \circ (a \circ b) &= b \circ b = (b \circ a) \circ b \\
b \circ (b \circ a) &= b \circ b = a = a \circ a = (b \circ b) \circ a \\
b \circ (b \circ b) &= b \circ a = b = a \circ b = (b \circ b) \circ b.
\end{aligned} \tag{2.7}$$

Alltså gäller $(x \circ y) \circ z = x \circ (y \circ z)$ för alla $x, y, z \in X$, så operationen $\circ$ är associativ. Vi ser också att

$$a \circ a = a \quad \text{och} \quad a \circ b = b \circ a = b. \tag{2.8}$$

Alltså gäller $x \circ a = a \circ x = x$ för alla $x \in X$. Det betyder att elementet a är en identitet i X. Till sist, eftersom $a \circ a = a$ och $b \circ b = a$, så ser vi att båda elementen a och b har inverser. I själva verket har vi att $a^{-1} = a$ och att $b^{-1} = b$. ▲

2.3 Egenskaper för grupper

Definition 2.3.1. Om gruppen G är en ändlig mängd, det vill säga innehåller ett ändligt antal element, så säger vi att G är en *ändlig grupp*. Vidare, om G är en ändlig grupp så säger vi att antalet element i G är *ordningen* av gruppen. Ordningen av G betecknas $|G|$.

Exempel 2.3.2. Gruppen $X = \{a, b\}$ i Exempel 2.2.6 är en ändlig grupp. Det är en grupp av ordning 2. Vi skriver $|G| = 2$. ▲

Det visar sig att en hel del av de egenskaper vi känner till för exempelvis heltal eller reella tal kan härledas för alla grupper endast utifrån gruppaxiomen. Här följer några sådana egenskaper.

Sats 2.3.3. *Låt G vara en grupp under operationen $\circ$. Låt $a, b, c \in G$. Då gäller följande:*

1. *Om $a \circ b = a \circ c$ så gäller $b = c$. Detta kallas för* vänstercancellation.
2. *Ekvationen*
$$a \circ x = b \tag{2.9}$$
har en unik lösning, nämligen $x = a^{-1} \circ b$.

Bevis.

1. Antag att $a \circ b = a \circ c$. Då följer $a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c)$. Använd nu att operationen $\circ$ är associativ och få $(a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c$. Eftersom $a^{-1} \circ a = e$ så får vi $e \circ b = e \circ c$. Därmed följer $b = c$ eftersom $e \circ b = b$ och $e \circ c = c$.

2. Låt oss först visa att det finns en lösning till ekvationen. Låt $x = a^{-1} \circ b$. Då gäller

$$a \circ x = a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b. \tag{2.10}$$

   Alltså har ekvationen minst en lösning, nämligen $x = a^{-1} \circ b$.

   Vidare, antag att både x och $\tilde{x}$ är lösningar till ekvationen, det vill säga att $a \circ x = b$ och att $a \circ \tilde{x} = b$. Då gäller $a \circ x = a \circ \tilde{x}$ och med hjälp av vänstercancellation får vi att $x = \tilde{x}$. Alltså finns det bara en lösning till ekvationen. □

Anmärkning 2.3.4. Att ekvationen $2x = 3$ går att lösa och har en unik lösning $x = 3/2$ vet alla. Detta är precis ekvation (2.9) i gruppen $\mathbb{R} \setminus \{0\}$ med multiplikation. Precis som i det ovanstående beviset är lösningen $x = 2^{-1} \cdot 3$.

Anmärkning 2.3.5. På liknande sätt som i Sats 2.3.3 kan man visa att *högercancellation* gäller, det vill säga att om $a \circ c = b \circ c$ så gäller $a = b$. Vidare kan man, också på liknande sätt som ovan, visa att ekvationen $x \circ a = b$ har en unik lösning. Det är en viktig skillnad mellan höger- och vänstercancellation samt mellan ekvationen $x \circ a = b$ och $a \circ x = b$. Det är nämligen inte nödvändigt att $x \circ y = y \circ x$ i en grupp. Vi vet visserligen att det gäller exempelvis i gruppen $\mathbb{Z}$ med operationen $\circ = +$, men det finns exempel på grupper där det inte gäller; se till exempel Avsnitt 3.1.

När vi nu kan använda cancellation och lösa ekvationer, kan vi bevisa två mycket centrala egenskaper hos grupper:

Följdsats 2.3.6. *Låt G med operationen $\circ$ vara en grupp. Då har G en unik identitet e. Vidare har varje element $a \in G$ en unik invers a^{-1}.*

Bevis. Antag att både e och f är identitetselement i G. Tag valfritt $a \in G$. Då gäller $a = a \circ e$ och $a = a \circ f$. Alltså har vi att $a \circ e = a \circ f$ och regeln om vänstercancellation ger oss att $e = f$. Alltså finns det bara ett identitetselement i G.

Vidare, tag $a \in G$. Eftersom en invers x till a löser ekvationen $a \circ x = e$ och eftersom denna ekvation har en unik lösning, så finns det en och endast en invers a^{-1} till elementet a. □

Sats 2.3.7. *Låt G vara en grupp med operationen $\circ$ och låt $a, b \in G$. Då gäller*

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1}. \tag{2.11}$$

Beviset för denna sats lämnas som övning.

2.4 Isomorfier

Definition 2.4.1. Antag att G är en grupp med operationen $\circ$ och att H är en grupp med operationen $*$. Om det finns en bijektion $\phi : G \to H$ sådan att

$$\phi(x \circ y) = \phi(x) * \phi(y) \quad \text{för alla } x, y \in G \tag{2.12}$$

så säger vi att G och H är *isomorfa*. Avbildningen ϕ kallas för en *isomorfi*.

Exempel 2.4.2. Låt $G = \{c, d\}$ och $H = \{0, 1\}$. Definiera de binära operationerna $\circ$ och $*$ via

$\circ$	c	d
c	d	c
d	c	d

$*$	0	1
0	0	1
1	1	0

(2.13)

Det är lätt att visa att $(G, \circ)$ och $(H, *)$ är grupper. Definiera en funktion $\phi : G \to H$ genom $\phi(c) = 1$ och $\phi(d) = 0$. Uppenbarligen är detta en bijektion. Dessutom uppfyller den

$$\begin{aligned}
\phi(c \circ c) &= \phi(d) = 0 = 1 * 1 = \phi(c) * \phi(c) \\
\phi(c \circ d) &= \phi(c) = 1 = 1 * 0 = \phi(c) * \phi(d) \\
\phi(d \circ c) &= \phi(c) = 1 = 0 * 1 = \phi(d) * \phi(c) \\
\phi(d \circ d) &= \phi(d) = 0 = 0 * 0 = \phi(d) * \phi(d).
\end{aligned} \tag{2.14}$$

Alltså har vi att $\phi(x \circ y) = \phi(x) * \phi(y)$ för alla $x, y \in G$. Det betyder att ϕ är en isomorfi mellan G och H.

Titta nu på grupperna, och framför allt på *grupptabellerna*, det vill säga de tabeller som definierar de binära operationerna för grupperna. Om vi i den första tabellen byter plats raderna och kolumnerna och sedan döper om d till 0 och c till 1 så får vi den andra tabellen. Alltså är G och H samma grupp, så när som på att vi bytt namn och plats på elementen. ▲

Att två grupper är isomorfa betyder alltså att de väsentligen är samma grupp, förutom att man eventuellt bytt namn och ordning på elementen i gruppen. Grupperna har alltså precis samma struktur och form, och därför betraktar vi dem som samma. Ordet isomorf kommer från grekiskans *isos* (=lika) och *morf* (=form).

Övning 2.1. Låt X och Y vara mängder. Antag att det finns en bijektion $\phi : X \to Y$. Visa att det finns en bijektion $X^2 \to Y^2$.

Övning 2.2. Bevisa Sats 2.3.7.

Övning 2.3. Låt G vara en grupp med operationen $\circ$. I Följdsats 2.3.6 visades det att varje element $x \in G$ har en unik invers x^{-1}. Gör ett nytt bevis för detta genom att använda vänstercancellation (Sats 2.3.3).

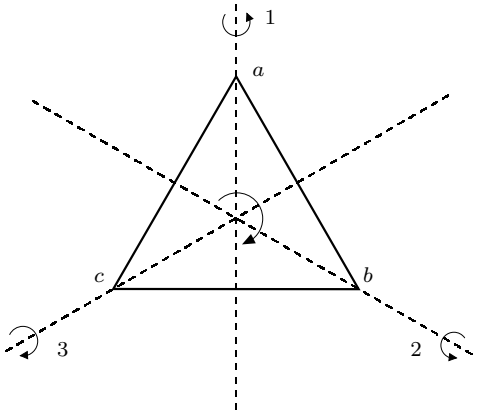
Övning 2.4. Låt oss använda beteckningen $z^2 = z \circ z$. Låt G vara en grupp och $x, y \in G$. Antag att $(x \circ y)^2 = x^2 \circ y^2$. Visa att $x \circ y = y \circ x$.

3 Delgrupper och cykliska grupper

3.1 Gruppen D_3

I de exempel på grupper som vi hittills har sett har gruppoperationen varit *kommutativ*, det vill säga att $a \circ b = b \circ a$ för alla element a och b i gruppen. Till exempel så har vi att $a + b = b + a$ för alla reella tal a och b. Nu vill vi visa ett exempel på en grupp där gruppoperationen *inte* är kommutativ, och en av de enklaste är symmetrigruppen för den liksidiga triangeln.

I figuren nedan ser vi en liksidig triangel.



Mångden D_3 består av de vridningar och vändningar efter vilka triangeln ser likadan ut som innan. Låt oss till exempel rotera trianglen 120° medurs kring den axel som går rakt genom mittpunkten, vinkelrätt mot pappret. Efter rotationen kommer bilden med triangeln att se precis likadan ut, bortsett från att hörnen har bytt plats; vi kan även rotera 240° utan att triangeln ändras. Vidare kan vi rotera 180° kring någon av axlarna $1, 2$ och 3 utan att ändra bilden; detta kallas för speglingar. Totalt har vi fem gruppelement: ρ, ρ^2, som betecknar rotation med 120° respektive 240° kring mittpunkten, samt $\sigma_1, \sigma_2, \sigma_3$ som betecknar spegling i axlarna 1,2 repsektive 3. Dessutom inför vi transformationen ϵ som inte gör någonting alls med triangeln. Dessa transformationer kallas för den liksidiga triangelns *symmetrier*.

Vi kan införa en binär operation på symmetrierna med hjälp av sammansättning. Alltså, $\rho \circ \sigma_1$ fås genom att först spegla triangeln i axel 1 och sedan rotera den 120° kring mittpunkten.

För att visa att detta är en grupp måste vi först kontrollera att mängden $\{\epsilon, \rho, \rho^2, \sigma_1, \sigma_2, \sigma_3\}$ är sluten under gruppoperationen, det vill säga att sammansättningen av två symmetrier lika gärna kan göras med endast en av dessa symmetrier. Låt oss beteckna hörnen i triangeln med a, b, c, i medurs riktning. Innan vi har gjort någon transformation kan vi alltså beskriva var hörnen befinner sig med symbolen (abc). Med denna notation verkar symmetrierna

som

$$\begin{aligned}\epsilon(abc) &= (abc)\\ \rho(abc) &= (cab)\\ \rho^2(abc) &= (bca)\\ \sigma_1(abc) &= (acb)\\ \sigma_2(abc) &= (cba)\\ \sigma_3(abc) &= (bac).\end{aligned} \tag{3.1}$$

Vi beskriver alltså hur symmetrierna verkar på triangeln genom att beskriva var hörnen befinner sig. Nu kan vi till exempel beräkna

$$(\rho \circ \sigma_1)(abc) = \rho(acb) = (bac) = \sigma_3(abc), \tag{3.2}$$

vilket visar att $\rho \circ \sigma_1 = \sigma_3$. På detta sätta kan vi beräkna alla möjliga sammansättningar och vi får tabellen

$\circ$	ϵ	ρ	ρ^2	σ_1	σ_2	σ_3
ϵ	ϵ	ρ	ρ^2	σ_1	σ_2	σ_3
ρ	ρ	ρ^2	ϵ	σ_3	σ_1	σ_2
ρ^2	ρ^2	ϵ	ρ	σ_2	σ_3	σ_1
σ_1	σ_1	σ_2	σ_3	ϵ	ρ	ρ^2
σ_2	σ_2	σ_3	σ_1	ρ^2	ϵ	ρ
σ_3	σ_3	σ_1	σ_2	ρ	ρ^2	ϵ

Från tabellen ser vi att det är naturligt att ha beteckningen ρ^2 eftersom $\rho \circ \rho = \rho^2$. Geometriskt förstår vi detta eftersom en rotation med $240°$ kan göras med två rotationer med $120°$.

Genom att inspektera denna tabell så ser vi att gruppoperationen i allmänhet inte är kommutativ; till exempel har vi att

$$\rho \circ \sigma_1 = \sigma_3 \neq \sigma_2 = \sigma_1 \circ \rho. \tag{3.3}$$

Då enhetselementet e finns med på varje rad i tabellen, så har varje element en invers, nämligen det element som står högst upp i kolumnen där e finns. Att operationen är associativ kommer vi att diskutera i ett senare kapitel, då vi talar om permutationer. Naturligtvis går det att kontrollera associativiteten direkt från tabellen ovan, men det skulle innebära en hel del arbete.

Gruppen som består av dessa symmetrier, tillsammans med den binära operation som innebär sammansättning av transformationer, betecknar vi med D_3.

3.2 Delgrupper

När vi diskuterar mängder talar vi ofta om delmängder, till exempel så är heltalen $\mathbb{Z}$ en delmängd till de reella talen $\mathbb{R}$, och på samma sätt är det naturligt att införa *delgrupper*. En delgrupp till en grupp G är en delmängd av

elementen i G tillsammans med gruppoperationen i G, så att detta par av mängd och operation uppfyller gruppaxiomen, det vill säga bildar en grupp.

Vi har tidigare diskuterat att de reella talen $\mathbb{R}$ är en grupp med addition som gruppoperation. Betrakta nu heltalen $\mathbb{Z}$ tillsammans med operationen addition; är detta en grupp? Det är klart att $\mathbb{Z}$ är sluten under addition eftersom summan av två heltal är ett heltal. Vidare så är enhetselementet $0 \in \mathbb{Z}$ och slutligen ligger inversen, $-n$, till ett heltal n i $\mathbb{Z}$. Eftersom addition av reella tal är associativ så är även addition av heltal associativ. Alltså är $\mathbb{Z}$ en delgrupp till $\mathbb{R}$ under addition. Låt oss nu skriva ned en ordentlig definition.

Definition 3.2.1. Låt mängden G med operationen $\circ$ vara en grupp och antag att delmängden $H \subseteq G$ är sluten under operationen $\circ$, d.v.s. om $h_1, h_2 \in H$ så är $h_1 \circ h_2 \in H$. Om H, tillsammans med $\circ$, är en grupp så säger vi att H är en *delgrupp* till G.

Exempel 3.2.2. Om vi väljer ut elementet a ur gruppen i Exempel 2.2.6, så utgör mängden $\{a\}$ en delgrupp till X. ▲

Exempel 3.2.3. Genom att inspektera tabellen för D_3, så ser vi att gruppen har fyra delgrupper: $\{\epsilon, \rho, \rho^2\}$, $\{\epsilon, \sigma_1\}$, $\{\epsilon, \sigma_2\}$ och $\{\epsilon, \sigma_3\}$. ▲

Som vi noterade i exemplet med heltalen och de reella talen, så följer associativiteten av att vi vet att operationen redan är en gruppoperation. Vi kan fråga oss hur mycket vi är tvungna att kontrollera för att fastställa att en delmängd är en delgrupp. Detta ger följande sats svar på.

Sats 3.2.4. *Låt G vara en grupp med gruppoperationen $\circ$, och låt H vara en delmängd till G. Då är H, tillsammans med $\circ$, en grupp om*

1. *H är sluten under $\circ$,*
2. *för alla element $g \in H$, så ligger inversen g^{-1} i H.*

Bevis. Låt oss kontrollera alla gruppaxiom. Enligt 1 så är H sluten under gruppoperationen och enligt 2 så finns inversen till varje element i mängden. Detta betyder att enhetselementet finns i mängden eftersom givet ett element $h \in H$ så finns $h^{-1} \in H$ och eftersom mängden är sluten så måste $h^{-1} \circ h = e$ ligga i H. Det återstår att visa att $\circ$ är associativ. Då $\circ$ är associativ för alla element i G så måste den också vara associativ för alla element i H, eftersom varje element i H också är ett element i G. □

Om gruppen är ändlig kan vi visa ett resultat som gör det tämligen enkelt att avgöra om en delmängd är den delgrupp.

Sats 3.2.5. *Låt G vara en ändlig grupp och antag att H är en delmängd till G. Om H är sluten under gruppoperationen så är H en delgrupp till G.*

Bevis. Vi antar, enligt satslydelsen, att H är sluten under gruppoperationen. Eftersom G är ändlig så är delmängden H ändlig, och vi kan skriva elementen i H som

$$H = \{h_1, h_2, \ldots, h_N\}, \tag{3.4}$$

där N är antalet element i H. Tag nu ett av dessa element i H, till exempel h_k, och skapa mängden

$$h_k H = \{h_k \circ h_1, h_k \circ h_2, \ldots, h_k \circ h_N\}, \tag{3.5}$$

där vi har opererat med h_k från vänster på alla element i H. Då vi har antagit att H är sluten under $\circ$ så måste $h_k H$ vara en delmängd till H. Vi vill visa att $h_k H = H$, och då vi har visat att $h_k H \subseteq H$ så räcker det att visa att $h_k H$ har N element.

Antag att $h_k H$ har färre än N element. Det betyder att det finns $h_i, h_j \in H$ sådana att $h_i \neq h_j$ och $h_k h_i = h_k h_j$. Enligt Sats 2.3.3 kan vi använda oss av vänstercancellation för att erhålla $h_i = h_j$, eftersom G är en grupp. Men detta motsäger att $h_i \neq h_j$ och vi drar slutsatsen att alla element $h_k h_1, \ldots, h_k h_N$ måste vara olika. Då $h_k H \subseteq H$ och $h_k H$ har lika många element som H så måste det gälla att $h_k H = H$.

Eftersom $h_k H = H$ så finns ett element $h_i \in H$ sådant att $h_k \circ h_i = h_k$. Denna likhet kan vi skriva som $h_k \circ h_i = h_k \circ e$ och från Sats 2.3.3 får vi att $h_i = e$. Alltså finns ett enhetselement i H. Med samma resonemang kan vi nu påstå att det måste finnas ett h_j sådant att $h_k \circ h_j = e$, vilket betyder att h_k^{-1} ligger i H. Då h_k är ett godtyckligt element så betyder det att inversen till alla element i H ligger i H. Enligt Sats 3.2.4 är H en delgrupp till G. □

Givet en grupp G och ett element $g \in G$ så kan vi ställa frågan om det finns någon delgrupp H till G, som innehåller g? Naturligtvis är G själv en delgrupp till G, men vi är intresserade av strikt mindre delgrupper. Det visar sig att det inte är så svårt att konstruera den minsta delgrupp som innehåller ett element g. Låt oss först införa lite notation som underlättar skrivarbetet. Låt g vara ett element i en grupp med gruppoperation $\circ$; då skriver vi

$$\begin{aligned} g^n &= \overbrace{g \circ g \circ \cdots \circ g}^{n} \\ g^0 &= e \\ g^{-n} &= \left(g^{-1}\right)^n. \end{aligned} \tag{3.6}$$

Detta skrivsätt tillåter att vi använder oss av de vanliga potenslagarna, det vill säga att

$$g^m \circ g^n = g^{m+n}. \tag{3.7}$$

Definition 3.2.6. Låt G vara en grupp med gruppoperationen $\circ$ och låt $g \in G$. Vi säger att mängden $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$ tillsammans med operationen $\circ$ är den *cykliska gruppen genererad av* g.

Vi lämnar som övning att visa att $\langle g \rangle$ verkligen är en grupp. Vi kan nu visa följande resultat.

Sats 3.2.7. *Låt G vara en grupp och låt $g \in G$. Då är $\langle g \rangle$ den minsta delgrupp som innehåller elementet g.*

Bevis. Låt oss visa att alla delgrupper som innehåller g även innehåller $\langle g \rangle$. Låt H vara en delgrupp och antag att $g \in H$. Eftersom H är sluten under gruppoperationen så måste även $g^n \in H$, för alla $n > 0$. Vidare måste enhetselementet finnas i H vilket ger att $g^0 = e \in H$. Slutligen måste även inversen g^{-1} ligga i H, och eftersom H är sluten under gruppoperationen så fås att $g^{-n} \in H$ för alla $n > 0$. Detta visar att $\langle g \rangle \subseteq H$ för alla delgrupper H som innehåller g; alltså är $\langle g \rangle$ den minsta grupp som innehåller elementet g. □

Det kan mycket väl vara så att givet ett element $g \in G$ så är $\langle g \rangle = G$. I detta fall säger vi att gruppen är *cyklisk*.

Exempel 3.2.8. Heltalen under addition är en cyklisk grupp som genereras av 1, det vill säga att $\langle 1 \rangle = \mathbb{Z}$. ▲

Exempel 3.2.9. Delgruppen $\{\epsilon, \rho, \rho^2\}$ till D_3 är en cyklisk grupp som genereras av ρ. ▲

Om G är en ändlig grupp så kan inte alla element i serien $g, g^2, g^3, \ldots$ vara olika, eftersom G i sådana fall inte vore ändlig. Alltså måste det finnas två olika heltal m_1 och m_2, sådana att $g^{m_1} = g^{m_2}$. Om vi antar att $m_2 > m_1$ så ger detta att

$$g^{m_2 - m_1} = e. \tag{3.8}$$

Alltså, för varje element g i en ändlig grupp, så finns det ett heltal $m > 0$ sådant att $g^m = e$. Detta gör följande definition meningsfull.

Definition 3.2.10. Låt G vara en ändlig grupp, tag ett element $g \in G$ och låt m vara det minsta positiva heltalet sådant att $g^m = e$. Då säger vi att m är *ordningen* av g.

Anmärkning 3.2.11. I Övning 3.5 ska du visa att $m = |\langle g \rangle|$, det vill säga att ordningen av g är ordningen av den cykliska gruppen genererad av g.

Exempel 3.2.12. I Exempel 2.2.6 har elementet b ordning 2, eftersom $b^2 = a$, som är enhetselementet i gruppen. ▲

Exempel 3.2.13. I gruppen D_3 har elementet ρ ordning 3 och elementen $\sigma_1, \sigma_2, \sigma_3$ har ordning 2. ▲

Övning 3.1. Låt G med operationen $\circ$ vara en grupp och låt $g \in G$. Vi inför notationen $g^n = \underbrace{g \circ \cdots \circ g}_{n}$ och $g^{-n} = \underbrace{g^{-1} \circ \cdots \circ g^{-1}}_{n}$ för positiva heltal n, samt $g^0 = e$. Visa att mängden $\{g^n : n \in \mathbb{Z}\}$ tillsammans med operationen $\circ$ är en grupp.

Övning 3.2. Visa att mängden $3\mathbb{Z} = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\}$ med operationen $+$ är en grupp.

Övning 3.3. Betrakta gruppen D_3 med notationen från detta kapitel. Visa att följande gäller

$$\sigma_1 \circ \rho = \sigma_2$$
$$\sigma_1 \circ \sigma_3 = \rho^2$$
$$\sigma_3 \circ \sigma_1 = \rho.$$

Övning 3.4. Visa att $\{\epsilon, \rho, \rho^2\}$ är en delgrupp till D_3 genom att använda Sats 3.2.5.

Övning 3.5. Låt G vara en grupp och låt m vara ordningen till elementet $g \in G$. Visa att $|\langle g \rangle| = m$.

4 Moduloräkning, $\mathbb{Z}_n$ och $\mathbb{U}_n$

4.1 Moduloräkning

Vi ska snart introducera ett viktigt exempel på en cyklisk grupp, och för detta behöver vi repetera ett par begrepp som rör heltalen.

Definition 4.1.1 (Delare)**.** Låt m och n vara heltal. Vi säger att m *delar* n om det finns ett heltal r sådant att $n = m \cdot r$. En *delare* till n är ett heltal som delar n.

Exempel 4.1.2. Vi har att 4 delar 12 eftersom vi kan välja $r = 3$ så att $12 = r \cdot 4 = 3 \cdot 4$. ▲

Definition 4.1.3. En *gemensam delare* till två heltal m och n är ett heltal som delar både m och n. Den *största gemensamma delaren*, sgd, till m och n är det största heltal r som är en gemensam delare till m och n. Vi skriver att $\text{sgd}(m, n) = r$. Två heltal sägs vara *relativt prima* om deras största gemensamma delare är 1.

Exempel 4.1.4. Talet 2 är en gemensam delare till 8 och 12, och 4 är den största gemensamma delaren; alltså är 8 och 12 *inte* relativt prima. Heltalen 8 och 9 är däremot relativt prima. ▲

Definition 4.1.5 (Primtal)**.** Ett positivt heltal p är ett *primtal* om det har exakt två positiva olika delare, nämligen 1 och p.

Exempel 4.1.6. Talet 1 är inget primtal eftersom det endast har en positiv delare, nämligen 1. Talet 2 är ett primtal eftersom 1 och 2 delar 2, och det finns inget annat positivt heltal som delar 2; talet 2 är för övrigt det enda jämna primtalet. De första 10 primtalen är: 2, 3, 5, 7, 11, 13, 17, 19, 23 och 29. ▲

Exempel 4.1.7. Talet 9 är inget primtal eftersom det har tre delare: 1, 3 och 9. ▲

Låt m och n vara två heltal och låt r vara ett heltal sådant att $m = qn + r$ för något heltal q. I detta fall skriver vi att

$$m \equiv r \pmod{n} \tag{4.1}$$

och säger att m *är kongruent med* r *modulo* n. Till exempel så uppfyller resten r då m divideras med n detta samband.

Exempel 4.1.8. Vi ser att $16 \equiv 2 \pmod{7}$, eftersom $16 = 2 \cdot 7 + 2$. Ett annat exempel är $8 \equiv 5 \pmod{3}$, eftersom $8 = 1 \cdot 3 + 2$. ▲

Vi noterar att man för varje heltal m, alltid kan välja ett heltal r så att $0 \leqslant r \leqslant n-1$ och $m \equiv r \pmod{n}$. På detta sätt definierar vi *addition modulo* n; för två heltal h och k beräknar vi deras summa modulo n genom att addera talen och sedan finna heltalet r $(0 \leqslant r \leqslant n-1)$ så att $h + k \equiv r \pmod{n}$. För addition modulo n inför vi symbolen $+_n$.

Exempel 4.1.9. Låt $n = 4$. Då har vi att $3 +_n 5 = 0$ och $7 +_n 4 = 3$. ▲

4.2 Gruppen $\mathbb{Z}_n$

Sats 4.2.1. *Låt $\mathbb{N}_n = \{0, 1, 2, \ldots, n-1\}$. Då är $\mathbb{N}_n$ tillsammans med $+_n$ en grupp och vi inför beteckningen $\mathbb{Z}_n$ för denna grupp.*

Bevis. Först och främst är det klart från definitionen av $+_n$ att givet två element $g, h \in \mathbb{N}_n$ så är $g +_n h \in \mathbb{N}_n$. Vidare så finns det ett enhetselement, nämligen 0, som uppfyller att $g +_n 0 = g$ för alla $g \in G$. Finns det en invers till varje element? Låt oss ta $g \in \mathbb{N}_n$ så att $g \neq 0$ och sätt $h = n - g \in \mathbb{N}_n$. Då får vi att $g +_n h = 0$, vilket visar att $h = g^{-1}$. Kom ihåg att enhetselementet, i detta fall 0, alltid har sig själv som invers.

Slutligen måste vi visa att $+_n$ är associativ, det vill säga att $g +_n (h +_n k) = (g +_n h) +_n k$ för alla $g, h, k \in \mathbb{N}_n$. Låt oss skriva $h + k = r_1 + l_1 n$ och $g + h = r_2 + l_2 n$, vilket ger oss att

$$g + r_1 + l_1 n = g + h + k = r_2 + l_2 n + k. \tag{4.2}$$

Detta visar att $g +_n r_1 = r_2 +_n k$, eftersom de två summorna endast skiljer sig åt med en multipel av n. Vi kan nu visa att

$$g +_n (h +_n k) = g +_n r_1 = r_2 +_n k = (g +_n h) +_n k.$$

□

Är nu $\mathbb{Z}_n$ en cyklisk grupp, som vi tidigare förutsåg? Vi ser att 1 genererar $\mathbb{Z}_n$ eftersom $1 +_n 1 = 2$, $1 +_n 1 +_n 1 = 3$, osv.

4.3 Gruppen $\mathbb{U}_n$

Kan vi på samma sätt definiera en grupp, där vi istället använder multiplikation modulo n som gruppoperation? Här måste vi vara lite mer försiktiga vilket följande exempel visar. Låt oss beteckna multiplikation av heltal modulo n med $\cdot_n$. Enhetselementet för multiplikation modulo n är heltalet 1. För det första så finns det inget heltal r sådant att $0 \cdot_n r = 1$, alltså saknar 0 en invers under denna operation. Således kan inte 0 vara ett element i en grupp med multiplikation modulo n. Låt $n = 6$ och låt $N = \{1, 2, 3, 4, 5\}$; är N tillsammans med operationen $\cdot_n$ en grupp? Nej, eftersom $2 \cdot_n 3 = 0$ så är inte mängden N sluten under $\cdot_n$. Låt oss ta $N = \{1, 2, 4, 5\}$ istället; får vi nu en grupp? I det här fallet är N sluten under operationen, men både 2 och 4 saknar invers. Väljer vi slutligen $N = \{1, 5\}$ så kan vi kontrollera att N tillsammans med $\cdot_n$ är en grupp. Det är ingen slump att vi tvingas välja endast de heltal som är relativ prima med 6, och vi ska visa att vi alltid får en grupp på detta vis. Först behöver vi dock ett lemma.

Lemma 4.3.1. *Antag att a och n är heltal sådana att $\text{sgd}(a, n) > 1$ och $n > 0$. Då finns det ett heltal $r > 0$ sådant att $r < n$ och $a \cdot_n r = 0$.*

Bevis. Låt oss sätta $c = \text{sgd}(a, n)$. Då finns det heltal m_1 och m_2 sådana att $n = cm_1$ och $a = cm_2$. Om vi sätter $r = m_1$ så får vi att

$$ar = cm_1m_2 = nm_2 \equiv 0 \pmod{n}. \tag{4.3}$$

Det är vidare klart att $r < n$ eftersom $c > 1$, samt att $r > 0$, vilket visar att $a \cdot_n r = 0$. □

Sats 4.3.2. *Låt n vara ett heltal och låt $N = \{r \in \mathbb{N} : 1 \leqslant r \leqslant n - 1$ och $\text{sgd}(r, n) = 1\}$. Då är N med operationen $\cdot_n$ en grupp. Vi betecknar denna grupp med $\mathbb{U}_n$.*

Bevis. Beviset för att $\cdot_n$ är associativ lämnas som en övning. Låt oss först visa att N är sluten under $\cdot_n$, det vill säga att produkten av två tal a och b, relativt prima med n, är igen relativt primt med n. Antag motsatsen, det vill säga att $\text{sgd}(a \cdot_n b, n) > 1$. Enligt Lemma 4.3.1 så finns det ett heltal $r < n$ sådant att $a \cdot_n b \cdot_n r = 0$.

Vi kommer upprepade gånger att använda oss av följande resultat: Om n delar ab och $\text{sgd}(n, a) = 1$, så är n en delare till b.

Från $a \cdot_n b \cdot_n r = 0$ följer det att eftersom b och n inte har någon gemensam delare ($\text{sgd}(b, n) = 1$), så betyder detta att n delar $a \cdot_n r$, det vill säga att $a \cdot_n r = 0$. Då $r < n$ och $r \neq 0$, så måste a och n ha en gemensam faktor om produkten skall vara delbar med n. Detta motsäger dock antagandet att $\text{sgd}(a, n) = 1$, vilket betyder att antagandet $\text{sgd}(a \cdot_n b, n) > 1$ måste vara falskt. Alltså är $\text{sgd}(a \cdot_n b, n) = 1$.

Låt oss nu ta ett element $a \in N$ och visa att $a^{-1} \in N$. Vi skriver elementen i N som

$$N = \{1, n_1, n_2, \ldots, n_k\}, \tag{4.4}$$

och inför mängden

$$N_a = \{a \cdot_n 1, a \cdot_n n_1, \ldots, a \cdot_n n_k\}. \tag{4.5}$$

Vi ska nu visa att $a \cdot_n n_i = a \cdot_n n_j$ om och endast om $i = j$, det vill säga att alla heltal i N_a är olika. Antag att $a \cdot_n n_i = a \cdot_n n_j$, vilket betyder att $an_i = an_j + nl$ för något heltal l. Detta ger oss att

$$a(n_i - n_j) = nl, \tag{4.6}$$

vilket betyder att $n_i - n_j = nl'$, för något heltal l', eftersom $\text{sgd}(a, n) = 1$. Men då $1 \leqslant n_i \leqslant n - 1$ för alla i, så måste $l' = 0$ vilket ger att $n_i = n_j$. Alltså består mängden N_a av lika många element som N, och eftersom N är sluten under multiplikation så måste $N_a = N$. Speciellt betyder detta att $1 \in N_a$, vilket säger att någon av produkterna $a \cdot_n 1, \ldots, a \cdot_n n_k$ är 1; alltså existerar det en invers till a. Vi har således visat att $\mathbb{U}_n$ är en grupp. □

Ett viktigt exempel fås då $n = p$ är ett primtal. I detta fall är alla positiva heltal mindre än p relativt prima med p och mängden $\{1, 2, \ldots, p-1\}$ med multiplikation modulo p är en grupp.

Övning 4.1. Låt n, m, a, b och p vara heltal sådana att

$$\begin{aligned} n &\equiv a \pmod{p} \\ m &\equiv b \pmod{p}. \end{aligned}$$

Visa att $n + m \equiv a + b \pmod{p}$.

Övning 4.2. Visa att multiplikation modulo n är associativ, det vill säga att

$$a \cdot_n \big(b \cdot_n c\big) = \big(a \cdot_n b\big) \cdot_n c.$$

för heltal a, b och c.

Övning 4.3. Betrakta gruppen $\mathbb{U}_5$ som består av mängden $\{1, 2, 3, 4\}$ tillsammans med operationen $\cdot_5$. Visa att elementen 2 och 3 genererar $\cdot_5$ och att $\mathbb{U}_5$ har en delgrupp av ordning 2.

Övning 4.4. Vilka element i $\mathbb{Z}_4$ genererar hela $\mathbb{Z}_4$?

5 Sidoklasser och Fermats lilla sats

5.1 Sidoklasser

I detta avsnitt ska vi bevisa två satser, Lagranges sats och Fermats lilla sats, som båda bygger på användandet av sidoklasser. Fermats lilla sats har till synes ingenting med gruppteori att göra och är därför ett första exempel på hur man, genom att använda en bakomliggande gruppstruktur, kan bevisa en sådan sats.

Definition 5.1.1. Låt H vara en delgrupp till G och låt $a \in G$. Vi kallar mängden $aH = \{ah : h \in H\}$ för den *vänstra sidoklassen* till H, som innehåller a. På samma sätt är $Ha = \{ha : h \in H\}$ den *högra sidoklassen* till H, som innehåller a.

Exempel 5.1.2. Det är enkelt att kontrollera att $H = \{0, 2\}$ är en delgrupp till $\mathbb{Z}_4$. Sidoklassen som innehåller 1 är $\{1, 3\}$ och sidoklassen som innehåller 2 är $\{2, 0\}$. Sidoklassen som innehåller 3 är $\{3, 1\}$. ▲

Anmärkning 5.1.3. I allmänhet är en sidoklass *inte* en delgrupp.

Anmärkning 5.1.4. Vänster och höger sidoklasser till en delgrupp är i allmänhet olika mängder. Resultaten vi kommer visa om sidoklasser gäller både höger och vänster sidoklasser även om beviset görs för endast ett av fallen.

Sats 5.1.5. *Låt H vara en delgrupp till G. Då har alla sidoklasser till H lika många element som H.*

Bevis. Ett vanligt sätt att visa att två mängder har lika många element är att konstruera en bijektion mellan mängderna. Kom ihåg att en bijektion mellan två mängder parar ihop varje element i den ena mängden med ett unikt element i den andra mängden, så att alla par i den senare mängden ingår i endast ett sådant par. Alltså, finns det en bijektion mellan två mängder, så har de lika många element. Låt oss konstruera en avbildning ϕ mellan H och en godtycklig sidoklass aH, för att sedan visa att ϕ är en bijektion. Vi sätter

$$\phi : H \to aH \quad \text{med} \quad \phi(h) = ah. \tag{5.1}$$

Vi visar först att ϕ är en injektion, d.v.s. om $h_1 \neq h_2$ så är $\phi(h_1) \neq \phi(h_2)$. Av definitionen får vi från $\phi(h_1) = \phi(h_2)$ att $ah_1 = ah_2$, och av vänstercancellation (Sats 2.3.3) fås att $h_1 = h_2$. Alltså är ϕ en injektion. För att visa att ϕ är en surjektion så tar vi ett godtyckligt element $g \in aH$ och visar att det finns ett element $h \in H$ så att $\phi(h) = g$. För varje element $g \in aH$ så finns det element $h_g \in H$ sådant att $g = ah_g$. Per definition betyder detta att $\phi(h_g) = ah_g = g$. Alltså är ϕ både en surjektion och en injektion, d.v.s. en bijektion. Då det finns en bijektion mellan mängderna H och aH drar vi slutsatsen att de har lika många element. □

Anmärkning 5.1.6. Notera att om en mängd, till exempel H ovan, har oändligt många element, så brukar man ta existensen av en bijektion som *definition* på att två mängder har lika många element.

Exempel 5.1.7. Vi noterar att sidoklasserna till $\mathbb{Z}_4$ i Exempel 5.1.2 alla har ordning 2. ▲

Sats 5.1.8. *Låt H vara en delgrupp till en ändlig grupp G. Då finns det element $a_1, a_2, \ldots, a_N$ sådana att*

$$G = a_1H \cup a_2H \cup \cdots \cup a_NH. \tag{5.2}$$

Bevis. Vi ska visa att det för varje element $g \in G$ existerar ett $a \in G$ och ett $h \in H$ sådana att $g = ah$. Om vi väljer ett godtyckligt $h \in H$ så säger Sats 2.3.3 att vi kan lösa ekvationen $g = ah$ genom att sätta $a = gh^{-1}$. Alltså ligger varje element i G i en sidoklass till H, och eftersom G är en ändlig grupp så kan vi finna element $a_1, a_2, \ldots, a_N$ sådana att

$$G = a_1H \cup a_2H \cup \cdots \cup a_NH.$$

□

Exempel 5.1.9. Låt $H = \{\epsilon, \rho, \rho^2\}$ vara en av delgrupperna till D_3. Då har vi att $D_3 = H \cup \sigma_1 H$. Väljer vi istället $H = \{\epsilon, \sigma_1\}$ så får vi att $D_3 = H \cup \rho H \cup \rho^2 H$ eller $D_3 = H \cup \sigma_2 H \cup \sigma_3 H$. ▲

Kan det vara så att ett element $g \in G$ ligger i två olika sidoklasser? Följande satser visar att två sidoklasser antingen har alla element eller inga element gemensamt.

Sats 5.1.10. *Antag att H är en delgrupp till G och antag att $a \in H$. Då är $aH = H$.*

Bevis. Eftersom H är en delgrupp, så är H sluten under gruppoperationen. Detta betyder att aH är en delmängd till H. Vi ska nu visa att varje element i H ligger i aH. Tag ett godtyckligt element $h \in H$. Då vill vi finna ett element $x \in H$ sådant att $ax = h$. Enligt Sats 2.3.3 så finns det ett sådant x, nämligen $x = a^{-1}h$. Alltså är $H \subseteq aH$ vilket, tillsammans med $aH \subseteq H$ visar att $aH = H$. □

Sats 5.1.11. *Låt H vara en delgrupp till G och låt a_1H och a_2H vara två sidoklasser. Då är antingen $a_1H = a_2H$ eller $a_1H \cap a_2H = \emptyset$.*

Bevis. Antag att det finns ett element $g \in G$ så att $g \in a_1H$ och $g \in a_2H$. Det betyder att det finns $b_1, b_2 \in H$ sådana att

$$g = a_1b_1 = a_2b_2, \tag{5.3}$$

vilket ger att

$$a_2 = a_1 b_1 b_2^{-1}. \tag{5.4}$$

Låt oss kalla $b_1 b_2^{-1}$ för h_0, alltså att $a_2 = a_1 h_0$. Detta ger oss att $a_2 H = \big(a_1 h_0\big) H = a_1\big(h_0 H\big)$. Enligt Sats 5.1.10 så är $h_0 H = H$ vilket ger oss att

$$a_2 H = a_1\big(h_0 H\big) = a_1 H. \tag{5.5}$$

Vi har således visat att givet att två sidoklasser har minst ett element gemensamt, så har de alla element gemensamt. □

5.2 Lagranges sats

Nu har vi de ingredienser vi behöver för att visa Lagranges sats.

Sats 5.2.1 (Lagranges sats)**.** *Låt H vara en delgrupp till en ändlig grupp G. Då är $|H|$ en delare till $|G|$.*

Bevis. Genom att kombinera Sats 5.1.8 och Sats 5.1.11 kan vi göra en uppdelning

$$G = a_1 H \cup a_2 H \cup \cdots \cup a_N H, \tag{5.6}$$

där $a_i H \cap a_j H = \emptyset$ då $i \neq j$. Detta betyder att antalet element i G är lika med summan av elementen i vardera sidoklass, det vill säga

$$|G| = |a_1 H| + |a_2 H| + \cdots + |a_N H|. \tag{5.7}$$

Eftersom varje sidoklass har lika många element som H, enligt Sats 5.1.5, så får vi att

$$|G| = N \cdot |H|. \tag{5.8}$$

Vi har således visat att $|H|$ delar $|G|$. □

Anmärkning 5.2.2. Lägg märke till att N i likheten $|G| = N \cdot |H|$ i beviset ovan är antalet olika vänster sidoklasser till H. Vi kommer senare att använda oss av detta då vi bevisar Burnsides lemma.

Exempel 5.2.3. I Exempel 5.1.2 så är $|\mathbb{Z}_4|$=4 och $|H| = |\{0, 2\}| = 2$. Alltså är $|H|$ en delare till $|\mathbb{Z}_4|$. ▲

Exempel 5.2.4. För D_3 gäller det att $|D_3| = 6$, och eftersom en delgrupp H har ordning 2 eller 3, så gäller det att $|H|$ delar $|D_3|$. ▲

Följdsats 5.2.5. *Låt G vara en ändlig grupp vars ordning p är ett primtal. Då är G cyklisk och G har inga undergrupper förutom G och $\{e\}$, där e är enhetselementet i G.*

Bevis. Eftersom ordningen av en undergrupp H delar p där p är ett primtal, så måste $|H| = 1$ eller $|H| = p$. Då varje undergrupp innehåller enhetselementet så är $\{e\}$ den enda undergruppen av ordning 1. Undergruppen av ordning p måste naturligtvis vara gruppen själv. Varför är nu denna grupp cyklisk? Tag ett godtyckligt element $g \in G$. Vad är ordningen till g? Om ordningen m av g vore mindre än p så skulle vi ha en undergrupp $\langle g \rangle$ av ordning m. Men eftersom den enda undergruppen av lägre ordning än p har ordning 1, så får vi att $|\langle g \rangle| = 1$. Som vi tidigare argumenterat så måste då $g = e$. Tar vi nu ett element $g \neq e$ så måste $|\langle g \rangle| = p$, vilket betyder att g genererar G. Alltså är G en cyklisk grupp. □

5.3 Fermats lilla sats

Genom att använda gruppstrukturen hos $\mathbb{U}_n$ tillsammans med Lagranges sats får vi följande resultat:

Sats 5.3.1 (Fermats lilla sats)**.** *Låt $a \in \mathbb{Z}$ och antag att p är ett primtal som inte delar a. Då gäller det att*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{5.9}$$

Bevis. Vi vet sedan tidigare att mängden $\{1, 2, \ldots, p-1\}$ tillsammans med multiplikation modulo p är en grupp, som vi betecknar $\mathbb{U}_p$. Eftersom p inte delar a så finns det ett element $b \in \mathbb{U}_p$ sådant att $b \equiv a \pmod{p}$. Enligt Lagranges sats så vet vi att ordningen n av b, det vill säga ordningen av gruppen $\langle b \rangle$, delar $|\mathbb{U}_p| = p - 1$. Alltså finns det ett positivt heltal r sådant att $p - 1 = nr$. Eftersom $b^n = 1$, enligt definitionen av ordning, så får vi att

$$\left(b^n\right)^r = 1^r \tag{5.10}$$

som ger att

$$b^{nr} = b^{p-1} = 1, \tag{5.11}$$

vilket enligt definitionen av $\cdot_n$ säger att $b^{p-1} \equiv 1 \pmod{p}$. Eftersom $a \equiv b \pmod{p}$, så gäller det även att $a^{p-1} \equiv 1 \pmod{p}$. □

Exempel 5.3.2. Vi kan enkelt visa att $7^{52} - 1$ inte är ett primtal, eftersom Fermats lilla sats säger oss att $7^{52} \equiv 1 \pmod{53}$, vilket betyder att $7^{52} - 1$ är delbart med 53. ▲

Exempel 5.3.3. Låt oss visa att $m = n^{33} - n$ är delbart med 5 för alla heltal n. Vi noterar först att $n^{33} - n = n(n^{32} - 1)$. Om n är delbart med 5 så är det klart att m är delbart med 5. Antag nu att n inte är delbart med 5. Fermats lilla sats säger oss då att

$$n^4 \equiv 1 \pmod{5}, \tag{5.12}$$

vilket vi kan använda för att visa

$$n^{32} = \left(n^4\right)^8 \equiv 1^8 = 1 \pmod 5. \tag{5.13}$$

Alltså är $n^{32} - 1 \equiv 0 \pmod 5$ vilket betyder att $n^{32} - 1$ är delbart med 5. Vi har följande resultat: Antingen är n delbart med 5, vilket direkt ger att $m = n\left(n^{32} - 1\right)$ är delbart med 5. Om n inte är delbart med 5 så har vi visat att $n^{32} - 1$ är delbart med 5. Detta visar att m alltid är delbart med 5. ▲

Fermats lilla sats nämner ingenting om grupper; ändock kan vi använda oss av den gruppteori som vi har utvecklat för att bevisa resultatet, genom att ta till vara på den gruppstruktur som heltalen med multiplikation modulo n besitter.

Övning 5.1. Vi har tidigare visat att $m = n^{33} - n$ är delbart med 5 för alla heltal n. Visa att det finns ett till heltal, mindre än 10, som alltid delar m.

Övning 5.2. Visa att det inte finns någon delgrupp till $\mathbb{Z}_{12}$ av ordning 5.

Övning 5.3. Finn en delgrupp H till $\mathbb{Z}_4$ och ett element $a \in \mathbb{Z}_4$ sådana att $H \neq \mathbb{Z}_4$ och $\mathbb{Z}_4 = H \cup aH$.

Övning 5.4. Om vi dividerar heltalet 8^{417} med 5 så får vi ett svar på formen

$$\frac{8^{417}}{5} = n + \frac{a}{5}$$

där n och a är två heltal och $0 \leqslant a \leqslant 4$. Bestäm a.

6 Grupper av permutationer

6.1 Permutationer

Definition 6.1.1. Låt X vara en ändlig mängd. En *permutation* σ av X är en bijektion $\sigma : X \to X$.

Låt oss kort fundera på vad det betyder att en funktion är en permutation. En bijektion mellan mängderna A och B parar som bekant ihop elementen i A med dem i B. Men en permutation är en bijektion från en mängd X till sig själv. Vi kan alltså se det som att en permutation byter ordning på elementen.

Exempel 6.1.2. Låt mängden X bestå av fem personer A, B, C, D, E som står på rad. Om vi ändrar ordningen på dessa människor så att de står som D, C, A, B, E så har vi *permuterat* (=kastat om) personerna. Själva omflyttningen av personerna är det vi kallar för en permutation. Permutationen flyttar alltså personerna som

$$A\,B\,C\,D\,E \longmapsto D\,C\,A\,B\,E. \tag{6.1}$$

Vi kan se permutationen som en funktion $\sigma : \{A, B, C, D, E\} \to \{A, B, C, D, E\}$ som ges av

$$\sigma(A) = D, \sigma(B) = C, \sigma(C) = A, \sigma(D) = B \text{ och } \sigma(E) = E. \tag{6.2}$$

Denna funktion är en bijektion från mängden $\{A, B, C, D, E\}$ till sig själv. ▲

Exempel 6.1.3. Låt $X = \{1, 2, 3\}$ och betrakta funktionen $\sigma : X \to X$ definierad av $\sigma(1) = 1, \sigma(2) = 3, \sigma(3) = 2$. Detta är uppenbarligen en bijektion, och därmed en permuation. Det är permutationen $1\,2\,3 \longmapsto 1\,3\,2$. ▲

För enkelhetens skull brukar vi ofta låta $X = \{1, 2, 3, \ldots, n\}$ för något positivt heltal n. Mängden av alla permutationer av denna mängd betecknas S_n. Exempelvis har vi att S_3 består av permutationerna

$$\begin{array}{lll} 1\,2\,3 \longmapsto 1\,2\,3 & 1\,2\,3 \longmapsto 1\,3\,2 & 1\,2\,3 \longmapsto 2\,1\,3 \\ 1\,2\,3 \longmapsto 2\,3\,1 & 1\,2\,3 \longmapsto 3\,2\,1 & 1\,2\,3 \longmapsto 3\,1\,2. \end{array} \tag{6.3}$$

Notera särskilt att även permutationen $1\,2\,3 \longmapsto 1\,2\,3$ som inte flyttar några element är en permutation. Denna permutation brukar kallas *identitetspermutationen.*

Anmärkning 6.1.4. Här har vi indirekt antagit att X är en *icke-tom* ändlig mängd. Att prata om permutationer av den tomma mängden $\emptyset$ är meningslöst. Alltså kommer vi fortsättningsvis antaga att de ändliga mängder X vi talar om är icke-tomma.

Låt oss nu använda begreppet *fakultet.* Vi definierar $n!$, uttalat n-fakultet, som produkten $1 \cdot 2 \cdot 3 \cdots n$. Exempelvis har vi att $1! = 1, 2! = 2, 3! = 6$ och $4! = 24$. Det visar sig att S_n består av $n!$ element:

Sats 6.1.5. *Låt n vara ett positivt heltal. Då finns det $n!$ olika permutationer av mängden $\{1, 2, 3, \ldots, n\}$.*

6.2 Sammansättning av permutationer

Låt X vara en ändlig mängd. För enkelhetens skull kan vi tänka på denna mängd som $\{1, 2, 3, \ldots, n\}$, men vilken ändlig mängd som helst går bra. Om ρ och σ är permutationer av X så betecknar vi med $\rho \circ \sigma$ funktionen $\tau : X \to X$ definierad av $\tau(x) = \rho(\sigma(x))$, och kallar detta *sammansättningen* av ρ och σ.

Funktionen $\rho \circ \sigma$ fungerar alltså så att vi *först* tar σ och *sedan* ρ på resultatet. Det gäller att komma ihåg att σ är först trots att den står till höger i $\rho \circ \sigma$. Men eftersom $(\rho \circ \sigma)(x) = \rho(\sigma(x))$ för alla $x \in X$ så är detta lätt att komma ihåg.

Exempel 6.2.1. Låt $X = \{1, 2, 3, 4\}$ och betrakta permutationerna

$$\rho : 1\,2\,3\,4 \longmapsto 2\,1\,4\,3 \quad \text{och} \quad \sigma : 1\,2\,3\,4 \longmapsto 3\,1\,2\,4. \tag{6.4}$$

Vi har alltså exempelvis att $\rho(2) = 1$ och att $\sigma(3) = 2$. Nu ges sammansättningen av ρ och σ av permutationen

$$\rho \circ \sigma : 1\,2\,3\,4 \longmapsto 4\,2\,1\,3 \tag{6.5}$$

eftersom

$$\begin{aligned} (\rho \circ \sigma)(1) &= \rho(\sigma(1)) = \rho(3) = 4 \\ (\rho \circ \sigma)(2) &= \rho(\sigma(2)) = \rho(1) = 2 \\ (\rho \circ \sigma)(3) &= \rho(\sigma(3)) = \rho(2) = 1 \\ (\rho \circ \sigma)(4) &= \rho(\sigma(4)) = \rho(4) = 3. \end{aligned} \tag{6.6}$$

I detta exempel ser vi att även sammansättningen av två permutationen är en permutation. Det är ingen tillfällighet. ▲

Sats 6.2.2. *Låt X vara en ändlig mängd och ρ och σ permutationer av X. Då är även sammansättningen $\rho \circ \sigma$ en permutation av X.*

Bevis. Vi ska alltså visa att sammansättningen av två bijektioner är en bijektion. Låt oss börja med att visa att $\rho \circ \sigma$ är en injektion. Tag $x, y \in X$ sådana att $x \neq y$. Låt $u = \sigma(x)$ och $v = \sigma(y)$. Eftersom σ är en bijektion så är σ även en injektion och alltså gäller $u \neq v$. Eftersom även ρ är en injektion så måste $\rho(\sigma(x)) = \rho(u) \neq \rho(v) = \rho(\sigma(y))$. Alltså gäller $(\rho \circ \sigma)(x) \neq (\rho \circ \sigma)(y)$ för alla $x, y \in X$ sådana att $x \neq y$. Alltså är $\rho \circ \sigma$ en injektion.

Låt oss nu visa att $\rho \circ \sigma$ är en surjektion. Tag $y \in X$. Eftersom ρ är en bijektion så är ρ även en surjektion och alltså finns $z \in X$ sådant att $\rho(z) = y$. Vidare är σ en surjektion, och alltså finns $x \in X$ sådant att $\sigma(x) = z$. Nu gäller alltså $\rho(\sigma(x)) = \rho(z) = y$, och därmed har vi visat att för varje $y \in X$ finns $x \in X$ sådant att $(\rho \circ \sigma)(x) = y$. Alltså är $\rho \circ \sigma$ en surjektion.

Eftersom $\rho \circ \sigma$ är både en injektion och en surjektion så är $\rho \circ \sigma$ en bijektion från X till sig själv. Alltså är $\rho \circ \sigma$ en permutation av mängden X. □

6.3 Gruppstruktur för permutationer

För en ändlig mängd X låter vi $Perm(X)$ beteckna mängden av alla permutationer av X. Exempelvis har vi alltså att $Perm(\{1, 2, 3, \ldots, n\}) = S_n$. Vi ska i detta avsnitt visa att $Perm(X)$ med operationen $\circ$ (sammansättning av permutationer) är en grupp.

Sats 6.3.1. *Låt X vara en ändlig mängd. Då är mängden $Perm(X)$ med operationen $\circ$ en grupp.*

Bevis. Att $\circ$ är en binär operation som uppfyller att $\rho \circ \sigma \in Perm(X)$ för alla $\rho, \sigma \in Perm(X)$ följer från Sats 6.2.2.

1. Tag nu permutationer $\rho, \sigma, \tau \in Perm(X)$. Betrakta permutationerna

$$\alpha_1 = \rho \circ (\sigma \circ \tau) \quad \text{och} \quad \alpha_2 = (\rho \circ \sigma) \circ \tau. \tag{6.7}$$

   Tag $x \in X$. Vi har att

$$\begin{aligned} \alpha_1(x) &= \rho((\sigma \circ \tau)(x)) \\ &= \rho(\sigma(\tau(x))) \\ &= (\rho \circ \sigma)(\tau(x)) \\ &= \alpha_2(x). \end{aligned} \tag{6.8}$$

   Eftersom $x \in X$ var godtycklig visar detta att $\alpha_1(x) = \alpha_2(x)$ för alla $x \in X$. Alltså gäller $\alpha_1 = \alpha_2$, det vill säga att

$$\rho \circ (\sigma \circ \tau) = (\rho \circ \sigma) \circ \tau \tag{6.9}$$

   för alla $\rho, \sigma, \tau \in Perm(X)$. Alltså är operationen $\circ$ associativ.

2. Låt $\epsilon : X \to X$ definieras av $\epsilon(x) = x$ för alla $x \in X$. Låt oss först visa att ϵ är en bijektion, det vill säga att $\epsilon \in Perm(X)$. Tag $x, y \in X$ med $x \neq y$. Då gäller $\epsilon(x) = x \neq y = \epsilon(y)$. Alltså är ϵ en injektion. Vidare, tag $y \in X$ och låt $x = y$. Då gäller $\epsilon(x) = y$. Alltså är ϵ en surjektion. Detta visar att ϵ är en bijektion.

   Tag $\sigma \in Perm(X)$ och $x \in X$. Vi har att $(\sigma \circ \epsilon)(x) = \sigma(\epsilon(x)) = \sigma(x)$ och att $(\epsilon \circ \sigma)(x) = \epsilon(\sigma(x)) = \sigma(x)$, och eftersom x var godtycklig så betyder detta att

$$\sigma \circ \epsilon = \epsilon \circ \sigma = \sigma. \tag{6.10}$$

   Alltså är ϵ en identitet i $Perm(X)$.

3. Tag $\sigma \in Perm(X)$. Eftersom σ är en bijektion $X \to X$ så finns det (se Avsnitt 1.4) en inversfunktion $\sigma^{-1} : X \to X$. Den är enligt Sats 1.4.2 också en bijektion. Alltså har vi att $\sigma^{-1} \in Perm(X)$. Nu återstår det att verifiera att σ^{-1} också är en invers i gruppteoretisk mening. Tag $x \in X$. Då gäller

$$(\sigma \circ \sigma^{-1})(x) = \sigma(\sigma^{-1}(x)) = x = \epsilon(x) \tag{6.11}$$

och

$$(\sigma^{-1} \circ \sigma)(x) = \sigma^{-1}(\sigma(x)) = x = \epsilon(x) \tag{6.12}$$

för alla $x \in X$. Alltså gäller

$$\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \epsilon. \qquad \square$$

Övning 6.1. Låt $X = \{1, 2, 3, 4, 5\}$ och definiera permutationerna

$$\rho : 1\,2\,3\,4\,5 \longmapsto 2\,1\,4\,3\,5 \quad \text{och} \quad \sigma : 1\,2\,3\,4\,5 \longmapsto 5\,4\,3\,2\,1. \tag{6.13}$$

Bestäm $\rho \circ \sigma$, $\sigma \circ \rho$ och $\rho \circ \rho$. Bestäm också ρ^{-1}.

Övning 6.2. En grupp G sägs vara *abelsk* om $x \circ y = y \circ x$ för alla $x, y \in X$. Är gruppen $Perm(\{1, 2\})$ abelsk?

Övning 6.3. Låt $X = \{1, 2, 3, 4\}$. Är gruppen $Perm(X)$ abelsk?

Övning 6.4. Låt X, Y vara ändliga mängder. Antag att det finns en bijektion $\phi : X \to Y$. Visa att grupperna $Perm(X)$ och $Perm(Y)$ är isomorfa.

Ledning: Definiera $\Phi(\sigma)(y) = \phi\left(\sigma(\phi^{-1}(y))\right)$ och visa att detta är en funktion $\Phi : Perm(X) \to Perm(Y)$. Visa sedan att Φ är en isomorfi.

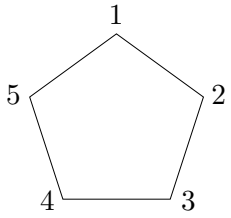
7 Burnsides lemma

7.1 Gruppverkan och banor

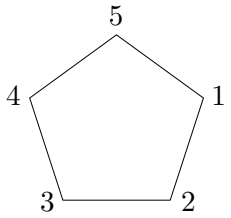
Vi har alltså sett att mängden $Perm(X)$ med operationen $\circ$ är en grupp. Denna grupp består alltså av alla permutationer av den ändliga mängden X.

Men vi kan också betrakta mindre permutationsgrupper, det vill säga delgrupper till $Perm(X)$. Låt X vara en ändlig mängd och G vara en delgrupp till $Perm(X)$. Det betyder att mängden G innehåller ett antal permutationer av X, men inte nödvändigtvis alla dessa permutationer. Ett element $g \in G$ är alltså en bijektion $X \to X$.

Exempel 7.1.1. Låt $X = \{1, 2, 3, 4, 5\}$ och betrakta pentagonen



Tänk dig nu att vi roterar pentagonen en femtedels varv medsols.

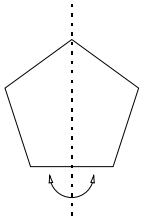


Då ser pentagonen fortfarande ut som från början, det vill säga hörnens positioner bibehålls, men numreringen har ändrats. Vi kan se denna rotation som en permutation av X, nämligen permutationen

$$1\,2\,3\,4\,5 \longmapsto 5\,1\,2\,3\,4. \tag{7.1}$$

Vi kan nu låta G bestå av de permutationer av mängden X som motsvarar en *symmetri* av pentagonen ovan. En symmetri är ett sätt att vrida och vända på pentagonen så att den fortfarande ser ut som från början.

De symmetrier som finns för pentagonen är 4 rotationer (1/5, 2/5, 3/5 och 4/5 varv medsols), 5 speglingar (se figuren nedan) och identitetspermutationen (att inte göra något alls med pentagonen).



Exempel på spegling

Alltså består G av tio specifika permutationer. Det återstår att övertyga sig om att detta verkligen är en delgrupp till S_5. Det är klart att om vi utför två symmetrier efter varandra så får vi en ny symmetri, alltså är G sluten under operationen $\circ$. Vidare är inversen till var och en av symmetrierna en symmetri i G. Detta eftersom identitetspermutationen är sin egen invers och likaså är speglingarna sina egna inverser (speglar man två gånger så kommer man tillbaka till ursprungsläget). Dessutom är rotation 1/5 och 4/5 varv varandras inverser (rotation 4/5 varv medsols är detsamma som rotation 1/5 varv *motsols*), precis som rotation 2/5 och 3/5 varv är varandras inverser.

Detta betyder att $g \circ h \in G$ för alla $g, h \in G$ och att $g^{-1} \in G$ för varje $g \in G$. Detta räcker som bekant för att visa att G är en delgrupp till S_5. ▲

Exempel 7.1.2. Gruppen D_3 från avsnitt 3.1 är en permutationsgrupp bestående av alla symmetrier av en liksidig triangel. Just i detta fall visar det sig dock att symmetrierna är alla permutationer av $\{a, b, c\}$ så i själva verket har vi att D_3 och $Perm(\{a, b, c\})$ är samma grupp. ▲

Definition 7.1.3. Låt X vara en ändlig mängd och G vara en delgrupp till $Perm(X)$. För $x \in X$ låter vi

$$Gx = \{y \in X \,:\, \sigma(x) = y \text{ för något } \sigma \in G\}, \tag{7.2}$$

och kallar denna mängd för *banan* till x.

Banan till x innehåller alltså de element som x avbildas på av någon permutation. Notera att $x \in Gx$ gäller för alla $x \in X$ eftersom $\sigma(x) = x$ när vi väljer $\sigma = \epsilon$, där ϵ är identitetspermutationen. Alltså är aldrig banan Gx tom.

Vi kan också se det som att vi utgår från elementet x. Sedan låter vi alla permutationer i G verka på x. Då får vi banan till x. Att banan skapas genom att låta hela G verka på x kan förklara beteckningen Gx.

Exempel 7.1.4. Låt $X = \{1, 2, 3, 4\}$ och låt G bestå av permutationerna

$$\epsilon : 1\,2\,3\,4 \longmapsto 1\,2\,3\,4 \quad \text{och} \quad \sigma : 1\,2\,3\,4 \longmapsto 1\,3\,2\,4. \tag{7.3}$$

Att detta verkligen är en delgrupp till $Perm(X)$ visas lätt (se Övning 7.2). Banorna som hör till G är

$$G1 = \{1\}, \quad G2 = G3 = \{2, 3\} \quad \text{och} \quad G4 = \{4\}. \tag{7.4}$$

Exempelvis har vi att $3 \in G2$ eftersom $\sigma(2) = 3$ och $1 \notin G2$ eftersom $\epsilon(2) \neq 1$ och $\sigma(2) \neq 1$. Det finns alltså tre olika banor i detta fall. ▲

Sats 7.1.5. *Låt $x, y \in X$. Då är banorna Gx och Gy antingen disjunkta eller identiska. Det vill säga, antingen gäller $Gx \cap Gy = \emptyset$ eller så gäller $Gx = Gy$.*

Bevis. Antag att $Gx \neq Gy$. Då finns minst ett $z \in X$ sådant att $z \in Gx$ men $z \notin Gy$. Detta betyder i synnerhet att det finns $\rho \in G$ sådant att $\rho(x) = z$.

Tag nu ett godtyckligt $w \in Gy$. Då finns $\sigma \in G$ sådant att $\sigma(y) = w$. Om det vore så att $w \in Gx$ så skulle det finnas $\tau \in G$ så att $\tau(x) = w$. Detta betyder alltså att $x = \tau^{-1}(w)$. Men då skulle

$$\rho(\tau^{-1}(\sigma(y))) = \rho(\tau^{-1}(w)) = \rho(x) = z, \tag{7.5}$$

och därmed har vi att permutationen $\rho \circ \tau^{-1} \circ \sigma \in G$ uppfyller $(\rho \circ \tau^{-1} \circ \sigma)(y) = z$, vilket motsäger att $z \notin Gy$. Alltså måste $w \notin Gx$ för alla $w \in Gy$. Detta betyder att $Gx \cap Gy = \emptyset$. □

7.2 Antalet banor

Återigen låter vi X vara en ändlig mängd. Vi räknar upp elementen i X som

$$X = \{x_1, x_2, \ldots, x_n\} \tag{7.6}$$

för något positivt heltal n. Talet n är alltså antalet element i X. Vidare låter vi G vara en grupp av permutationer av X. Alltså är G en delgrupp till $Perm(X)$. Eftersom G är en ändlig mängd kan vi räkna upp permutationerna i G som

$$G = \{\sigma_1, \sigma_2, \ldots, \sigma_N\} \tag{7.7}$$

för något positivt heltal N. Detta betyder att N är antalet permutationer i G. Observera att talen n och N inte har något sammanhang (förutom att $N \leqslant n!$ eftersom det totalt finns $n!$ permutationer av X, och G innehåller en del av dessa). Nu inför vi två stycken funktioner, $F : G \to \mathbb{N}$ och $f : X \to \mathbb{N}$ genom att låta

$$F(\sigma) \text{ vara antalet element } x \in X \text{ som uppfyller } \sigma(x) = x \tag{7.8}$$

och

$$f(x) \text{ vara antalet permutationer } \sigma \in G \text{ som uppfyller } \sigma(x) = x. \tag{7.9}$$

Funktionen $F(\sigma)$ räknar alltså hur många x som *fixeras* av permutationen σ (det vill säga att $\sigma(x) = x$), och $f(x)$ räknar hur många permutationer som *fixerar* ett givet element $x \in X$.

Givet en grupp G som verkar på en mängd X, kan vi fråga oss hur många *olika* banor som finns. Burnsides lemma talar om för oss hur vi kan beräkna antalet banor genom att använda oss av funktionen F. Innan vi bevisar denna sats så skall vi bevisa ett lemma.

Lemma 7.2.1. *För G och X som ovan så gäller det att*

$$|G| = f(x)|Gx|, \tag{7.10}$$

för alla $x \in X$.

Bevis. Låt oss för varje $x \in X$ införa mängden

$$H_x = \{\sigma \in G \,:\, \sigma(x) = x\}. \tag{7.11}$$

Från (7.9) ser vi direkt att $f(x)$ är antalet element i H_x. Mängden H_x är en delgrupp till G eftersom om $\sigma, \tau \in H_x$ så gäller det att $\big(\sigma \circ \tau\big)(x) = \sigma\big(\tau(x)\big) = \sigma(x) = x$. Alltså är $\sigma \circ \tau \in H_x$, och enligt Sats 3.2.5 så är H_x en delgrupp. I Anmärkning 5.2.2, till Lagranges sats, noterar vi att $|G| = N \cdot |H_x| = N \cdot f(x)$, där N är antalet disjunkta sidoklasser till H_x. Vi ska nu visa att $N = |Gx|$, vilket visar påståendet i lemmat.

För att visa att $N = |Gx|$ finner vi, som ett antal gånger tidigare, en bijektion mellan två mängder. Den ena mängden, som vi betecknar med K, består av alla sidoklasser till H_x och den andra mängden är banan till x. Låt oss nu konstruera bijektionen. Tag ett godtyckligt element $y \in Gx$. Från definitionen av banan till x vet vi att det finns ett $\sigma \in G$ sådant att $y = \sigma(x)$. Från detta definierar vi $\varphi : Gx \to K$ genom

$$\varphi(y) = \sigma H_x. \tag{7.12}$$

Är φ väldefinierad av detta samband? Vad händer om det finns ett $\sigma' \in G$ sådant att $y = \sigma'(x)$? Får vi samma sidoklass om vi använder σ' i definitionen ovan? Låt oss kontrollera detta. Antag att $y = \sigma'(x) = \sigma(x)$, vilket leder till att $\big(\sigma^{-1} \circ \sigma'\big)(x) = x$. Detta betyder att $\sigma^{-1} \circ \sigma' \in H_x$, eftersom $\sigma^{-1} \circ \sigma'$ fixerar x, och vi har därför att $\big(\sigma^{-1} \circ \sigma'\big) H_x = H_x$, vilket visar att $\sigma' H_x = \sigma H_x$. Alltså kan vi säga att φ är väldefinierad.

Låt oss nu visa att φ är en injektion. Antag att $y_1, y_2 \in Gx$ och att $\varphi(y_1) = \varphi(y_2)$. Vi vet att det finns element $\sigma_1, \sigma_2 \in G$ sådana att $y_1 = \sigma_1(x)$ och $y_2 = \sigma_2(x)$. Att $\varphi(y_1) = \varphi(y_2)$ betyder att $\sigma_1 H_x = \sigma_2 H_x$. Eftersom enhetselementet ϵ ligger i H_x så måste det finnas $\sigma \in H_x$ sådant att $\sigma_1 = \sigma_2 \circ \sigma$. Men detta visar att $y_1 = \sigma_1(x) = (\sigma_2 \circ \sigma)(x) = \sigma_2(x) = y_2$. Alltså är φ injektiv.

Låt oss nu visa att φ är en surjektion. Tag en godtycklig sidoklass σH_x. Om vi sätter $y = \sigma(x)$ så har vi att $y \in Gx$ och $\varphi(y) = \sigma H_x$. I och med detta har vi visat att φ är bijektiv och det har som konsekvens att antalet element i Gx är lika med antalet element i K, det vill säga antalet sidoklasser till H_x. Som tidigare nämnt så får vi sedan från Lagranges sats att $|G| = N|H_x| = |Gx|f(x)$. □

Sats 7.2.2 (Burnsides lemma)**.** *Antalet banor i G är*

$$\frac{F(\sigma_1) + F(\sigma_2) + \cdots + F(\sigma_N)}{N}. \tag{7.13}$$

Anmärkning 7.2.3. Vi kan alltså se det som att antalet banor i G är medelvärdet av antalet fixerade element.

Exempel 7.2.4. Låt oss återigen titta på Exempel 7.1.4. Här har vi alltså att $X = \{1, 2, 3, 4\}$ och att G består av permutationerna

$$\epsilon : 1\,2\,3\,4 \longmapsto 1\,2\,3\,4 \quad \text{och} \quad \sigma : 1\,2\,3\,4 \longmapsto 1\,3\,2\,4. \tag{7.14}$$

Här är alltså $G = \{\epsilon, \sigma\}$ så $N = 2$. Vi har att $F(\epsilon) = 4$ eftersom alla elementen $1, 2, 3$ och 4 fixeras av permutationen ϵ. Vidare har vi att $F(\sigma) = 2$ eftersom de element som fixeras av σ är 1 och 4. Alltså är antalet banor precis $(F(\epsilon) + F(\sigma))/2 = (2 + 4)/2 = 3$, vilket stämmer med det vi kom fram till i Exempel 7.1.4. ▲

Bevis av Sats 7.2.2. Vi ska visa Burnsides lemma genom att beräkna antalet element i mängden

$$M = \{(\sigma, x) \,:\, \sigma \in G, x \in X \text{ och } \sigma(x) = x\} \tag{7.15}$$

på två olika sätt. Mängden M består alltså av par av element från G och X sådana att elementet från G fixerar det från X. Vi vill nu visa att

$$|M| = f(x_1) + f(x_2) + \cdots f(x_n) \tag{7.16}$$

och att

$$|M| = F(\sigma_1) + F(\sigma_2) + \cdots F(\sigma_N). \tag{7.17}$$

Låt n vara antalet element i X och låt M_i vara mängden av de element (σ, x) i M för vilka $x = x_i$. Detta ger oss en uppdelning av M som

$$M = M_1 \cup M_2 \cup \cdots \cup M_n \tag{7.18}$$

där $M_i \cap M_j = \emptyset$ för $i \neq j$. Vi noterar att det i M_i finns ett element (σ, x_i) för varje $\sigma \in G$ som fixerar x_i; alltså är $|M_i| = f(x_i)$. Då mängderna $M_1, \ldots, M_n$ är disjunkta så kan vi beräkna storleken av M som i (7.16).

För att visa (7.17) definerar vi om M_i som mängden av alla element (σ, x) i M sådana att $\sigma = \sigma_i$. Detta ger oss en uppdelning

$$M = M_1 \cup \cdots \cup M_N \tag{7.19}$$

där $M_i \cap M_j = \emptyset$ för $i \neq j$. Nu inser vi att $|M_i| = F(\sigma_i)$ vilket ger oss (7.17).

Låt oss visa att $f(x_1) + \cdots + f(x_n) = (\text{antalet banor}) \cdot |G|$. Från Lemma 7.2.1 vet vi att $f(x) = |G|/|Gx|$ för alla $x \in X$, vilket ger oss att

$$f(x_1) + \cdots f(x_n) = |G|\left(\frac{1}{|Gx_1|} + \cdots + \frac{1}{|Gx_n|}\right). \tag{7.20}$$

Om x och y tillhör samma bana så är det klart att $|Gx| = |Gy|$. Låt oss därför gruppera termerna i summan ovan efter vilken bana de tillhör. Om vi betecknar antalet banor med r och låter $y_1, \ldots, y_r$ vara element från disjunkta banor så kan vi skriva summan i högerledet som

$$|G|\left(\frac{1}{|Gy_1|} + \cdots + \frac{1}{|Gy_1|} + \cdots + \frac{1}{|Gy_r|} + \cdots + \frac{1}{|Gy_r|}\right). \tag{7.21}$$

Nu noterar vi att

$$\frac{1}{|Gy_i|} + \cdots + \frac{1}{|Gy_i|} = |Gy_i|\frac{1}{|Gy_i|} = 1 \tag{7.22}$$

för alla y_i eftersom antalet termer precis är lika med antalet element i banan. Detta ger oss att

$$f(x_1) + \cdots + f(x_n) = |G|\big(\underbrace{1 + 1 + \cdots + 1}_{r}\big) = |G| \cdot r. \tag{7.23}$$

Nu återstår det bara att kombinera (7.16) och (7.17) för att erhålla

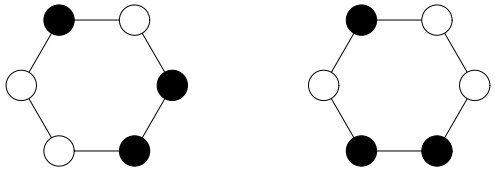
$$F(\sigma_1) + \cdots + F(\sigma_2) = f(x_1) + \cdots + f(x_n) = |G| \cdot r, \tag{7.24}$$

och då vi har betecknat antal element i G med N får vi slutligen

$$r = \frac{F(\sigma_1) + \cdots + F(\sigma_2)}{N}. \qquad \square$$

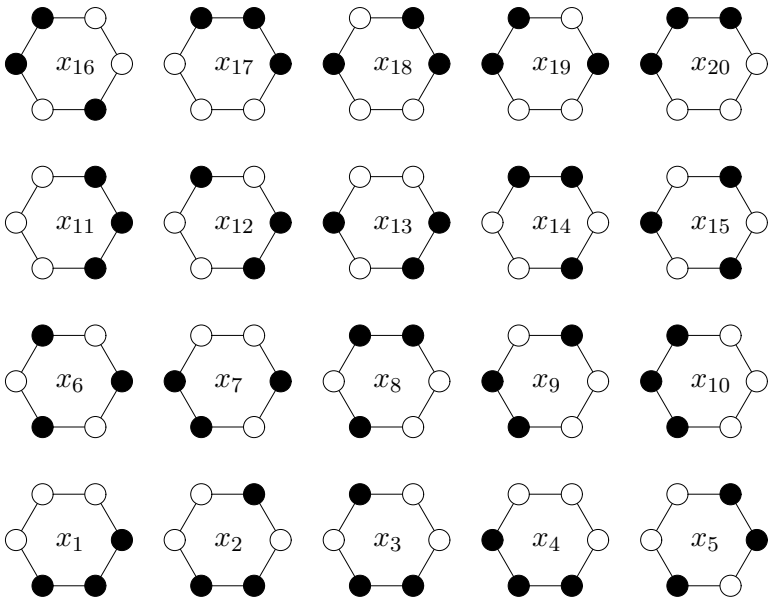
7.3 Tillämpning: Pärlhalsband

Hur många pärlhalsband med tre vita och tre svarta kulor finns det? Detta är en fråga som lätt besvaras med hjälp av Burnsides lemma. I själva verket kan vi använda nedanstående resonemang för att besvara denna fråga med ett godtyckligt antal svarta och vita kulor, men här tittar vi på ett konkret och enkelt exempel. Svårigheten med detta problem är att de två halsbanden



i själva verket är desamma. Om man roterar det vänstra halsbandet en sjättedels varv medsols och sedan speglar (det vill säga vänder på) det så får man halsbandet till höger.

Vi betraktar nu mängden X som består av följande 20 figurer:



Detta är samtliga *konfigurationer* av en hexagon med tre vita och tre svarta hörn. Vissa av dessa konfigurationer motsvarar samma halsband, eftersom man kan vrida och vända på halsbanden. Frågan är hur många olika halsband det finns.

Vi har alltså mängden $X = \{x_1, x_2, \ldots, x_{20}\}$ och ställer oss frågan vilka permutationer av denna mängd som motsvarar giltiga sätt att vrida och vända på halsbanden. Sådana permutationer kallas *symmetrier* och dem har vi talat om tidigare. En möjlig permutation är rotation en sjättedels varv medsols som exempelvis avbildar konfigurationen x_2 på konfigurationen x_7. Rotation en sjättedels varv medsols är alltså permutationen

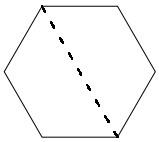
$$\rho_1 : x_1\, x_2\, x_3\, \cdots\, x_{20} \longmapsto x_4\, x_7\, x_9\, \cdots\, x_{17}. \tag{7.25}$$

Vi låter gruppen G bestå av alla symmetrier av konfigurationerna i X. Att G är en grupp är klart eftersom sammansättningen av två symmetrier är en ny symmetri, och eftersom inversen till en symmetri också är en symmetri. Detta betyder att

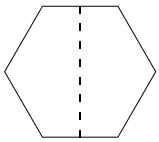
$$G = \{\epsilon, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5, \sigma_1, \sigma_2, \sigma_3, \tau_1, \tau_2, \tau_3\}, \tag{7.26}$$

där permutationerna beskrivs i nedanstående tabell:

Namn	Beskrivning
ϵ	Identitet
ρ_1	Rotation en sjättedels varv medsols
ρ_2	Rotation två sjättedels varv medsols
ρ_3	Rotation tre sjättedels varv medsols
ρ_4	Rotation fyra sjättedels varv medsols
ρ_5	Rotation fem sjättedels varv medsols
σ_1	Spegling i hörnaxel 1
σ_2	Spegling i hörnaxel 2
σ_3	Spegling i hörnaxel 3
τ_1	Spegling i kantaxel 1
τ_2	Spegling i kantaxel 2
τ_3	Spegling i kantaxel 3



Hörnaxel 1



Kantaxel 1

Notera nu att om $x, y \in X$ tillhör samma bana i G så motsvarar konfigurationerna x och y ett och samma halsband. Detta eftersom om de tillhör samma bana så finns det en symmetripermutation som avbildar x på y, och därmed finns det ett sätt att vrida och vända på x så att vi får y. Detta betyder att varje bana motsvarar ett unikt halsband, och därmed har vi att:

> Antalet banor är lika med antalet halsband. Alltså ska vi ta reda på antalet banor.

För att ta reda på antalet banor använder vi Burnsides lemma. Vi måste veta hur många konfigurationer som fixeras av varje permutation i G. Genom att tänka efter lite kommer vi fram till följande tabell:

Namn	Beskrivning	Fixerade konfigurationer	Antal
ϵ	Identitet	$x_1, x_2, \ldots, x_{20}$	20
ρ_1	Rotation en sjättedels varv	Inga	0
ρ_2	Rotation två sjättedels varv	x_6, x_{15}	2
ρ_3	Rotation tre sjättedels varv	Inga	0
ρ_4	Rotation fyra sjättedels varv	x_6, x_{15}	2
ρ_5	Rotation fem sjättedels varv	Inga	0
σ_1	Spegling i hörnaxel 1	x_1, x_6, x_{15}, x_{20}	4
σ_2	Spegling i hörnaxel 2	$x_6, x_{10}, x_{11}, x_{15}$	4
σ_3	Spegling i hörnaxel 3	x_4, x_6, x_{15}, x_{17}	4
τ_1	Spegling i kantaxel 1	Inga	0
τ_2	Spegling i kantaxel 2	Inga	0
τ_3	Spegling i kantaxel 3	Inga	0

Vi har alltså att

$$\begin{aligned} &F(\epsilon) = 20, \\ &F(\rho_1) = 0, F(\rho_2) = 2, F(\rho_3) = 0, F(\rho_4) = 2, F(\rho_5) = 0, \\ &F(\sigma_1) = 4, F(\sigma_2) = 4, F(\sigma_3) = 4, \\ &F(\tau_1) = 0, F(\tau_2) = 0, F(\tau_3) = 0. \end{aligned} \tag{7.27}$$

Därmed ges antalet banor av

$$\frac{20 + 0 + 2 + 0 + 2 + 0 + 4 + 4 + 4 + 0 + 0 + 0}{12} = \frac{36}{12} = 3. \tag{7.28}$$

Detta visar alltså att det finns tre olika pärlhalsband som innehåller tre vita och tre svarta kulor. De tre olika halsbanden är de som motsvaras av konfigurationerna x_1 (tre vita kulor i rad), x_2 (två vita kulor i följd, sedan en svart, sedan en vit) samt x_6 (varannan kula vit och varannan svart). Detta var kanske inte så svårt att se från början, men om antalet kulor är stort är ovanstående en mycket effektiv metod.

Övning 7.1. Låt $X = \{1, 2, 3, 4, 5, 6\}$ och σ vara permutationen $1\,2\,3\,4\,5\,6 \longmapsto 3\,2\,4\,6\,5\,1$. Bestäm $F(\sigma)$.

Övning 7.2. Låt $X = \{1, 2, 3, 4\}$ och låt G bestå av permutationerna

$$\epsilon : 1\,2\,3\,4 \longmapsto 1\,2\,3\,4 \quad \text{och} \quad \sigma : 1\,2\,3\,4 \longmapsto 1\,3\,2\,4. \tag{7.29}$$

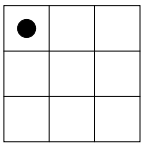
Visa att G är en delgrupp till $Perm(X)$.

Övning 7.3. Låt $X = \{a, b, c, d\}$ och låt G bestå permutationerna

$$\epsilon : a\,b\,c\,d \longmapsto a\,b\,c\,d, \quad \sigma : a\,b\,c\,d \longmapsto b\,c\,a\,d \quad \text{och} \quad \rho : a\,b\,c\,d \longmapsto c\,a\,b\,d. \tag{7.30}$$

Visa att $G = \langle\sigma\rangle$ (se Avsnitt 3.2), och dra slutatsen att G är en grupp. Bestäm banan Ga.

Övning 7.4. Gruppen D_4 består av symmetrierna till kvadraten och vi skriver $D_4 = \{e, \rho_1, \rho_2, \rho_3, \sigma_1, \sigma_2, \tau_1, \tau_2\}$, där ρ_1, ρ_2, ρ_3 är rotationer med $90°, 180°$ respektive $270°$ och σ_1, σ_2 samt τ_1, τ_2 är speglingar i de två hörnaxlarna repsektive kantaxlarna. Tag en kvadrat som består av 3x3 rutor och gör ett hål i en av rutorna; vi kallar detta ett hålkort.



Använd Burnsides lemma för att beräkna hur många *olika* hålkort det finns, när vi betraktar två hålkort som lika om man kan få det ena från det andra genom att verka med ett element ur D_4.

A Extra träning i mängdlära och bevisföring

Här kommer fyra tips på hur man visar saker om mängder:

1. Visa att $x \in A$.

   Här ska man alltså visa att x uppfyller de villkor som definierar vilka element som tillhör mängd A. Om exempelvis $A = \{1, 2, 3\}$ är det uppenbart att $2 \in A$, men om $A = \{x : \text{villkor på } x\}$ så måste man visa att x uppfyller de nämnda villkoren. Om $A = B \cap C$ så måste man visa att $x \in B$ och $x \in C$, medan om $A = B \cup C$ så räcker det att visa att $x \in B$ eller $x \in C$ (eller båda).

2. Visa att $A \subseteq B$.

   Tag ett godtyckligt element $x \in A$. Använd nu definitionen för mängden A för att skriva ner vilka villkor som finns på x. Visa sedan att $x \in B$. Eftersom x var godtyckligt så betyder detta att alla $x \in A$ uppfyller $x \in B$, det vill säga $A \subseteq B$.

3. Visa att $A = B$.

   Vi visar först $A \subseteq B$ och sedan $B \subseteq A$. Då har vi visat att alla element i A ligger i B och att alla element i B ligger i A. Det följer då naturligtvis att $A = B$.

4. Visa att $A = \emptyset$.

   Minns att $\emptyset$ betecknar denna tomma mängden, det vill säga en mängd som inte innehåller några element alls. Det som ska visas är alltså att det inte kan finnas några element i A.

   Antag till att börja med att $x \in A$. Använd definitionen av A för att skriva ner vilka villkor som då ställs på x. Visa att dessa villkor är omöjliga (att de leder till en motsägelse). Alltså kan det inte vara så att $x \in A$, oavsett vilket x vi väljer. Alltså innehåller inte A några element.

Låt Ω vara en godtycklig mängd. Vi kommer att antaga att alla mängder $A, B, C, \ldots$ är delmängder till Ω. Låt oss göra följande definitioner:

1. $A \setminus B = \{x \in A : x \notin B\}$
2. $A^c = \Omega \setminus A = \{x \in \Omega : x \notin A\}$
3. $A \Delta B = \{x \in \Omega : x \text{ tillhör en av } A \text{ och } B \text{ men inte båda}\}$

Övning A.1. Visa att $A \setminus B \subseteq A \Delta B$.

Övning A.2. Visa att $A \Delta B = (A \setminus B) \cup (B \setminus A)$.

Övning A.3. Två mängder B och C sägs vara *disjunkta* om de inte har några gemensamma element. Visa att B och C är disjunkta om och endast om $B \cap C = \emptyset$.

Övning A.4. Visa att A och A^c är disjunkta.

Övning A.5. Visa att $\Omega = A \cup A^c$.

Övning A.6. Symbolen $n!$ definieras som $n! = 1 \cdot 2 \cdot 3 \cdots n$ och kallas n-fakultet. Exempelvis har vi att $1! = 1$, $2! = 2$, $3! = 6$ och $5! = 120$. Låt $A_n = \{kn : k = 1, 2, 3, \ldots\}$. Visa att $n! \in A_1 \cap A_2 \cap \cdots \cap A_n$, för varje heltal $n \geqslant 1$, men att $A_1 \cap A_2 \cap A_3 \cap \cdots = \emptyset$.

Övning A.7. Låt $\mathbb{N} = \{0, 1, 2, \ldots\}$ och $B_n = \{1, 2, \ldots, n\}$ för $n = 1, 2, 3, \ldots$. Visa att $\mathbb{N} \setminus \{0\} = B_1 \cup B_2 \cup B_3 \cup \cdots$.

Övning A.8. Visa att $((A \cap C) \cup (B \cap C^c))^c = (A^c \cap C) \cup (B^c \cap C^c)$.

Lösningar

Övning A.1. Tag $x \in A \setminus B$. Det betyder att $x \in A$ och att $x \notin B$. Alltså tillhör x en av A och B, men inte båda, och därmed gäller $x \in A \Delta B$. Eftersom x var godtycklig betyder detta att $x \in A \Delta B$ för alla $x \in A \setminus B$, det vill säga att $A \setminus B \subseteq A \Delta B$.

Övning A.2. Tag $x \in A \Delta B$. Det betyder att x tillhör en av A och B men inte båda. Vi har två fall:

Till att börja med kan $x \in A$ och $x \notin B$. Då gäller per definition $x \in A \setminus B$. Eftersom $A \setminus B$ är en delmängd till $(A \setminus B) \cup (B \setminus A)$ så gäller även $x \in (A \setminus B) \cup (B \setminus A)$.

Det andra fallet är att $x \in B$ och $x \notin A$, det vill säga att $x \in B \setminus A \subseteq (A \setminus B) \cup (B \setminus A)$.

I båda fallen får vi alltså att $x \in (A \setminus B) \cup (B \setminus A)$, och eftersom x var godtycklig så betyder detta att $A \Delta B \subseteq (A \setminus B) \cup (B \setminus A)$.

Omvänt, tag $x \in (A \setminus B) \cup (B \setminus A)$. Det betyder att $x \in A \setminus B$ eller $x \in B \setminus A$. I båda fallen tillhör x en av A och B men inte båda. Alltså gäller $x \in A \Delta B$. Eftersom x var godtycklig så följer det att $(A \setminus B) \cup (B \setminus A) \subseteq A \Delta B$.

Nu har vi visat att $A \Delta B \subseteq (A \setminus B) \cup (B \setminus A)$ och att $(A \setminus B) \cup (B \setminus A) \subseteq A \Delta B$. Det betyder att $A \Delta B = (A \setminus B) \cup (B \setminus A)$.

Övning A.3. Antag att B och C är disjunkta. Antag att $x \in B \cap C$, det vill säga att $x \in B$ och $x \in C$. Men detta betyder att B och C har x som gemensamt element, vilket motsäger att B och C är disjunkta. Alltså måste $B \cap C = \emptyset$.

Omvänt, antag att $B \cap C = \emptyset$. Det betyder att det inte finns något element som tillhör både B och C. Alltså har B och C inga gemensamma element, det vill säga att B och C är disjunkta.

Nu har vi alltså visat två saker, dels att om B och C är disjunkta så gäller $B \cap C = \emptyset$, dels att om $B \cap C = \emptyset$ så är B och C disjunkta. Tillsammans betyder detta att B och C är disjunkta om och endast om $B \cap C = \emptyset$.

Övning A.4. Enligt föregående uppgift är det vi ska visa att $A \cap A^c = \emptyset$. Antag att $x \in A \cap A^c$. Det betyder att $x \in A$ och att $x \in A^c$. Det senare betyder per definition att $x \notin A$, vilket är en motsägelse. Alltså måste $A \cap A^c = \emptyset$.

Övning A.5. Tag $x \in \Omega$. Vi har två fall: $x \in A$ och $x \notin A$. I det först fallet gäller naturligtvis $x \in A \cup A^c$. I det andra fallet har vi per definition att $x \in A^c$, och därmed att $x \in A \cup A^c$. I båda fallen gäller alltså $x \in A \cup A^c$ och eftersom x var godtycklig så följer $\Omega \subseteq A \cup A^c$.

Omvänt, antag att $x \in A \cup A^c$. Vi vet att $A \subseteq \Omega$ och att $A^c \subseteq \Omega$. Alltså måste $x \in \Omega$. Detta visar att $A \cup A^c \subseteq \Omega$, och tillsammans med ovanstående får vi $\Omega = A \cup A^c$.

Övning A.6. Låt n vara ett heltal med $n \geqslant 1$. Tag ett heltal i med $1 \leqslant i \leqslant n$. Notera att $n! = ki$ där $k = 1 \cdot 2 \cdots (i-2) \cdot (i-1) \cdot (i+1) \cdot (i+1) \cdots (n-1) \cdot n \geqslant 1$. Alltså gäller $n! \in A_i$, och eftersom i var godyckligt så gäller $n! \in A_i$ för alla $i = 1, 2, \ldots, n$, det vill säga $n! \in A_1 \cap A_2 \cap \cdots \cap A_n$. Nu, eftersom n var godtyckligt så gäller $n! \in A_1 \cap \cdots \cap A_n$, för alla heltal $n \geqslant 1$.

Vidare, antag att $x \in A_1 \cap A_2 \cap \cdots$. Det betyder att $x \in A_n$ för alla heltal $n \geqslant 1$. I synnerhet gäller $x \in A_1 = \{1, 2, 3, \ldots\}$, det vill säga x är ett positivt heltal. Låt $m = x + 1$. Då gäller $x < m < 2m < 3m < \cdots$, och i synnerhet $x \neq km$ för $k = 1, 2, \ldots$, så $x \notin A_m$. Men detta motsäger ju att $x \in A_n$ för alla heltal $n \geqslant 1$. Alltså gäller $A_1 \cap A_2 \cap \cdots = \emptyset$.

Övning A.7. Tag $x \in \mathbb{N} \setminus \{0\}$. Det betyder att $x \in \mathbb{N} = \{0, 1, 2, \ldots\}$ och att $x \notin \{0\}$, det vill säga att x är något av talen $1, 2, 3, \ldots$. I synnerhet gäller $x \in \{1, 2, \ldots, x\} = B_x$ och därmed $x \in B_1 \cup B_2 \cup \cdots$. Eftersom x var godtycklig visar detta att $\mathbb{N} \setminus \{0\} \subseteq B_1 \cup B_2 \cup \cdots$.

Omvänt, antag att $x \in B_1 \cup B_2 \cup \cdots$. Det betyder att det finns ett heltal $n \geqslant 1$ så att $x \in B_n = \{1, 2, \ldots, n\}$. I synnerhet gäller $x \in \{0, 1, 2, \ldots\} = \mathbb{N}$ och $x \notin \{0\}$, det vill säga $x \in \mathbb{N} \setminus \{0\}$. Detta visar att $B_1 \cup B_2 \cup \cdots \subseteq \mathbb{N} \setminus \{0\}$.

Övning A.8. Tag $x \in ((A \cap C) \cup (B \cap C^c))^c$. Det betyder att $x \in \Omega$ och $x \notin (A \cap C) \cup (B \cap C^c)$. Alltså har vi att $x \notin A \cap C$ och $x \notin B \cap C^c$. Det finns nu två möjligheter: $x \in C$ och $x \notin C$.

I det första fallet, det vill säga $x \in C$, måste $x \notin A$ eftersom om $x \in A$ så skulle $x \in A \cap C$ vilket är falskt. Alltså gäller $x \in A^c$, vilket tillsammans med $x \in C$ ger att $x \in A^c \cap C$ i detta fall. I synnerhet har vi att $x \in (A^c \cap C) \cup (B^c \cap C^c)$.

I det andra fallet gäller $x \in C^c$ och då måste $x \in B^c$ eftersom om $x \in B$ så skulle $x \in B \cap C^c$ vilket är falskt. Alltså gäller $x \in B^c \cap C^c$, och i synnerhet $x \in (A^c \cap C) \cup (B^c \cap C^c)$.

I båda fallen gäller alltså $x \in (A^c \cap C) \cup (B^c \cap C^c)$, och eftersom x var godtycklig så visar detta att $((A \cap C) \cup (B \cap C^c))^c \subseteq (A^c \cap C) \cup (B^c \cap C^c)$.

Omvänt, tag $x \in (A^c \cap C) \cup (B^c \cap C^c)$. Då gäller $x \in A^c \cap C$ eller $x \in B^c \cap C^c$ (eller båda). Vi har alltså dessa två fall.

I det första fallet, det vill säga $x \in A^c \cap C$, har vi att $x \notin A$ och $x \notin C^c$. I synnerhet har vi att $x \notin A \cap C$ (eftersom $x \notin A$) och att $x \notin B \cap C^c$

(eftersom $x \notin C^c$). Alltså tillhör x varken $A \cap C$ eller $B \cap C^c$, vilket betyder att $x \in ((A \cap C) \cup (B \cap C^c))^c$.

I det andra fallet, det vill säga $x \in B^c \cap C^c$ har vi att $x \notin B$ och att $x \notin C$. Det följer att $x \notin A \cap C$ och att $x \notin B \cap C^c$. Alltså gäller $x \notin (A \cap C) \cup (B \cap C^c)$, vilket betyder att $x \in ((A \cap C) \cup (B \cap C^c))^c$.

I båda fallen har det alltså visats att $x \in ((A \cap C) \cup (B \cap C^c))^c$, och eftersom x var godtycklig visar detta att $(A^c \cap C) \cup (B^c \cap C^c) \subseteq ((A \cap C) \cup (B \cap C^c))^c$.

Vi har alltså visat att $((A \cap C) \cup (B \cap C^c))^c \subseteq (A^c \cap C) \cup (B^c \cap C^c)$ och att $(A^c \cap C) \cup (B^c \cap C^c) \subseteq ((A \cap C) \cup (B \cap C^c))^c$ och därmed att $((A \cap C) \cup (B \cap C^c))^c = (A^c \cap C) \cup (B^c \cap C^c)$.

Lösningar till udda övningsuppgifter

Övning 1.1.

1. $B \cup C = A$.
2. $B \cap C = \emptyset$.
3. $D \cap C = \{4, 36\}$.
4. $\{x \in D : x \in B\} = D \cap B = \{1, 19, 101\}$.
5. $\{x \in A : x = y + 1 \text{ för något } y \in D\} = \{2, 5, 20, 37, 102\}$.
6. $\{x + 1 : x \in D\} = \{2, 5, 20, 37, 102\}$.

Övning 1.3. Tag $m \in \mathbb{Z}$. Låt $n = m + 3$. Notera att $n \in \mathbb{Z}$. Nu gäller $f(n) = f(m + 3) = (m + 3) - 3 = m$. Eftersom m var godtyckligt betyder detta att det till varje $m \in \mathbb{Z}$ finns ett $n \in \mathbb{Z}$ sådant att $f(n) = m$. Alltså är f en surjektion.

Övning 2.1. Definiera funktionen $\psi : X^2 \to Y^2$ genom

$$\psi((x, y)) = (\phi(x), \phi(y)) \tag{1.1}$$

för alla $(x, y) \in X^2$. Låt oss visa att denna funktion är en bijektion.

Till att börja med, antag att $(x_1, y_1), (x_2, y_2) \in X^2$ uppfyller $(x_1, y_1) \neq (x_2, y_2)$. Det betyder att $x_1 \neq x_2$ eller $y_1 \neq y_2$ (eller både och). I fallet att $x_1 \neq x_2$ har vi att $\phi(x_1) \neq \phi(x_2)$ eftersom ϕ är en injektion. Alltså gäller i detta fall att $(\phi(x_1), \phi(y_1)) \neq (\phi(x_2), \phi(y_2))$. I det andra fallet, det vill säga att $y_1 \neq y_2$ har vi att $\phi(y_1) \neq \phi(y_2)$ eftersom ϕ är en injektion. Alltså gäller även här att $(\phi(x_1), \phi(y_1)) \neq (\phi(x_2), \phi(y_2))$. I båda fallen har vi att

$$\psi((x_1, y_1)) = (\phi(x_1), \phi(y_1)) \neq (\phi(x_2), \phi(y_2)) = \psi((x_2, y_2)). \tag{1.2}$$

Alltså är ψ en injektion.

Vidare, tag $(u, v) \in Y^2$. Då gäller $u, v \in Y$ och eftersom ϕ är en surjektion så finns $x, y \in X$ sådana att $\phi(x) = u$ och $\phi(y) = v$. Nu gäller

$$\psi((x, y)) = (\phi(x), \phi(y)) = (u, v). \tag{1.3}$$

Alltså finns det till varje $(u, v) \in Y^2$ ett element $(x, y) \in X^2$ sådant att $\psi((x, y)) = (u, v)$. Alltså är ψ en surjektion.

Övning 2.3. Tag $x \in G$. Antag att både y och z är inverser till x. Då har vi att $x \circ y = e$ och $x \circ z = e$. Nu följer $x \circ y = x \circ z$ och vänstercancellation ger oss att $y = z$. Alltså finns det bara en invers till x.

Övning 3.1. Först och främst har vi att

$$g^m \circ g^n = \big(\overbrace{g \circ g \circ \ldots \circ g}^{m}\big) \circ \big(\overbrace{g \circ g \circ \ldots \circ g}^{n}\big) = \big(\overbrace{g \circ g \circ \ldots \circ g}^{m+n}\big), \tag{1.4}$$

vilket visar att mängden är sluten under gruppoperationen. Då vi har definierat $g^0 = e$, så finns det ett enhetselement i mängden. Det är vidare klart att inversen till g^n är g^{-n}, som också ligger i mängden. Associativiteten följer direkt av att G är en grupp, eller genom att notera att

$$g^n \circ \big(g^m \circ g^k\big) = g^{n+m+k} = \big(g^n \circ g^m\big) \circ g^k. \tag{1.5}$$

Övning 3.3. Genom att använda oss av ekvationerna i (3.1) får vi att

$$\begin{aligned}
\sigma_1 \circ \rho(abc) &= \sigma_1(cab) = (cba) = \sigma_2(abc) \\
\sigma_1 \circ \sigma_3(abc) &= \sigma_1(bac) = (bca) = \rho^2(abc) \\
\sigma_3 \circ \sigma_1(abc) &= \sigma_3(acb) = (cab) = \rho(abc).
\end{aligned}$$

Övning 3.5. Vi ska alltså visa att antalet element i mängden $\{g^n : n \in \mathbb{Z}\}$ har lika många element som ordningen av elementet g. Ordningen m är det minsta positiva heltal sådant att $g^m = e$. Detta betyder att alla element $e, g, g^2, \ldots, g^{m-1}$ är olika, eftersom om $g^{n_1} = g^{n_2}$, där $n_1, n_2 \leqslant m$ och $n_1 < n_2$, så betyder det att

$$g^{n_2} \circ g^{-n_1} = g^{n_1} \circ g^{-n_1} \tag{1.6}$$

vilket ger att

$$g^{n_2 - n_1} = e. \tag{1.7}$$

Detta motsäger att m är det minsta positiva heltal sådant att $g^m = e$. Alltså är de m elementen $e, g, g^2, \ldots, g^{m-1}$ olika. Dessutom kan vi visa att elementet g^n där $n > m$ kan skrivas som

$$g^n = g^{qm} \circ g^{n-qm} = e^q \circ g^{n-qm} = e \circ g^{n-qm} = g^{n-qm} \tag{1.8}$$

där q är valt så att $0 \leqslant n - qm < m$, det vill säga att g^n redan finns i mängden $\{e, g, g^2, \ldots, g^{m-1}\}$. Detta visar att $\langle g \rangle$ har exakt m element.

Övning 4.1. Enligt antagandet att $n \equiv a \pmod{p}$ och $m \equiv b \pmod{p}$ så finns det heltal k och l sådana att

$$\begin{aligned}
n &= a + kp \\
m &= b + lp.
\end{aligned}$$

Detta ger oss att

$$n + m = a + b + (k + l)p$$

vilket enligt definitionen av modulo betyder att $n + m \equiv a + b \pmod{p}$.

Övning 4.3. Vi måste visa att för varje element $g \in \mathbb{U}_5$ så finns det heltal k och l sådana att $2^k \equiv g \pmod 5$ och $3^l \equiv g \pmod 5$. Vi beräknar de första potenserna av 2 och 3. Kom ihåg att vår notation betyder $g^n = \underbrace{g \cdot_5 g \cdot_5 \cdots \cdot_5 g}_{n}$.

$$\begin{aligned} &2^0 = 1; \quad 2^1 = 2; \quad 2^2 = 4; \quad 2^3 = 3; \quad 2^4 = 1 \\ &3^0 = 1; \quad 3^1 = 3; \quad 3^2 = 4; \quad 3^3 = 2; \quad 3^4 = 1. \end{aligned}$$

Detta betyder att $\langle 2 \rangle = \langle 3 \rangle = \mathbb{U}_5$. Låt oss se vilken cyklisk grupp som 4 genererar:

$$4^1 = 4; \quad 4^2 = 1.$$

Alltså är $\{1, 4\}$ en delgrupp till $\mathbb{U}_n$.

Övning 5.1. Vi visar att 3 alltid delar $m = n^{33} - n = n(n^{32} - 1)$. Om n är delbart med 3, så är det klart att m är delbart med 3. Antag nu att n inte är delbart med 3. Fermats lilla sats säger oss då att

$$n^2 \equiv 1 \pmod 3.$$

Detta ger oss att

$$m = n\big((n^2)^{16} - 1\big) \equiv n(1 - 1) = 0 \pmod 3.$$

Vi har således visat att m alltid är delbart med 3.

Övning 5.3. Vi kan kontrollera att $\{0, 2\}$ är en delgrupp till $\mathbb{Z}_4$. Mängden är sluten eftersom $2 +_4 2 = 0$, och vi ser att $2^{-1} = 2$. Sidoklassen som innehåller 1 är $\{1, 3\}$. Vi får då att

$$\mathbb{Z}_4 = H \cup 1H.$$

Övning 6.1. Kom ihåg att $\rho \circ \sigma$ betyder först σ sedan ρ. Vi får att

$$\begin{aligned} &\rho \circ \sigma : 1\,2\,3\,4\,5 \longmapsto 5\,3\,4\,1\,2 \\ &\sigma \circ \rho : 1\,2\,3\,4\,5 \longmapsto 4\,5\,2\,3\,1 \\ &\rho \circ \rho : 1\,2\,3\,4\,5 \longmapsto 1\,2\,3\,4\,5. \end{aligned} \tag{1.9}$$

Eftersom $\rho \circ \rho = \epsilon$ så ser vi att $\rho^{-1} = \rho$.

Övning 6.3. Nej, gruppen $Perm(X)$ är inte abelsk eftersom exempelvis permuationerna

$$\rho : 1\,2\,3\,4 \longmapsto 2\,1\,3\,4 \quad \text{och} \quad \sigma : 1\,2\,3\,4 \longmapsto 1\,3\,2\,4 \tag{1.10}$$

uppfyller

$$\rho \circ \sigma : 1\,2\,3\,4 \longmapsto 2\,3\,1\,4 \quad \text{och} \quad \sigma \circ \rho : 1\,2\,3\,4 \longmapsto 3\,1\,2\,4. \tag{1.11}$$

Alltså har vi att $\rho \circ \sigma \neq \sigma \circ \rho$.

Övning 7.1. Eftersom $\sigma(2) = 2$ och $\sigma(5) = 5$ men $\sigma(x) \neq x$ för alla andra $x \in X$, så är det alltså två element i X som fixeras av σ. Alltså är svaret att $F(\sigma) = 2$.

Övning 7.3. Vi ser att

$$\begin{aligned}(\sigma \circ \sigma)(a) &= \sigma(\sigma(a)) = \sigma(b) = c \\ (\sigma \circ \sigma)(b) &= \sigma(\sigma(b)) = \sigma(c) = a \\ (\sigma \circ \sigma)(c) &= \sigma(\sigma(c)) = \sigma(a) = b \\ (\sigma \circ \sigma)(d) &= \sigma(\sigma(d)) = \sigma(d) = d.\end{aligned} \tag{1.12}$$

Därmed gäller $\sigma^2 = \sigma \circ \sigma = \rho$. På liknande sätt visas det att $\sigma^3 = \epsilon$. Nu ser vi att $\sigma^4 = \sigma \circ \sigma^3 = \sigma \circ \epsilon = \sigma$, och på samma sätt att

$$\sigma^5 = \rho, \quad \sigma^6 = \epsilon, \quad \sigma^7 = \sigma, \quad \sigma^8 = \rho, \tag{1.13}$$

och så vidare. Alltså har vi att

$$\langle \sigma \rangle = \{\sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \ldots\} = \{\sigma, \rho, \epsilon\} = G. \tag{1.14}$$

Vi ser att G är den cykliska gruppen genererad av σ. I synnerhet är G en grupp.

För att bestämma banan till a: Notera att $\epsilon(a) = a, \sigma(a) = b$ och att $\rho(a) = c$. Alltså har vi att $a, b, c \in Ga$. Men det finns ingen permutation $\tau \in G$ sådan att $\tau(a) = d$. Alltså måste $d \notin Ga$. Vi har alltså visat att

$$Ga = \{a, b, c\}. \tag{1.15}$$

För övrigt gäller $Gb = Gc = Ga$ och $Gd = \{d\}$.

Sakregister