Gruppteori *

Ilyas Ahmed och Qusay Naji†

23 maj 2007

*Tack till professor Dan Laksov

†I samarbete med Kungilga Tekniska Högskolan (KTH)

Contents

1 INTRODUKTION

Som sista års gymnasieelever har vi, liksom alla andra tredje års gymnasister, fått arbeta med ett projektarbete som omfattar 100 gymnasiepoäng. Inom projektarbetet har vi fått fördjupa oss inom ett specifikt ämne som vi sedan fått att arbeta med kontinuerligt. Av det starka intresset för matematik blev det ett självklart val skriva ett projektarbete inom detta väldigt teoretiska ämne. Idèn till att vi skulle arbeta med matematik kom redan under vårt andra gymnasieår 2006. Då hade vi tänkt oss att arbeta med differenser och derivator, men efter ett flertal diskussioner beslutade vi tillslut att byta område något till mer abstrakt, nämligen gruppteori. Under arbetets gång pågick det en matematikkurs på Kungliga Tekniska Högkolan (KTH) för gymnasielever. Som en sammanträffande, handlade denna kurs också om gruppteori och som hjälp till vårt skrivande gick vi på kursens föreläsningar på KTH varje månad.

Självaste projektarbetet har gått ut på att skriva om gruppteori på ett förenklat så att andra gymnasielever kan förstå gruppterions grunder. Ett flertal förändringar och rättningar har gjorts under skrivandets gång. Trots att vi har försökt kraftigt förenkla både språk och definitioner kan innehållet i detta kompendium vara djupt hjärnansträngande. Nya främmande symboler och begrepp kan göra läsaren förvirrad men trots det tror vi att man väl kan åtminstone ytligt förstå vad gruppteori handlar om.

Gruppteori är ett fundamentalt område inom matematiken. Den ingår mer eller mindre tydligt i de flesta grenar av matematiken. Grupper ger det naturliga språket för att beskriva alla slags symmetrier, vilket är förklaringen till att användingsområdet av gruppteorin är enorm både inom matematik, naturvetenskap och teknik.

1.1 Tacksägelse

Vi vill speciellt tacka professor Dan Laksov för projektidèn och den hjälp han givit oss under arbetets gång. Dan Laksov har också tipsat oss om typsättningssystemet TEX, som har låtit oss lyckas att få ett snyggt arbete. Vi vill också tacka vår handledare Agneta Gisle, inom projektarbetet för all hjälp, stöd och den tid hon givit oss.

Ilyas Ahmed och Qusay Naji
24 maj 2007

2 GRUNDER

För att kunna förstå gruppteori, måste man först ha några grunder i bakhuvudet. Det som gör matematiken så unik, är att när man väl har förstått någonting, så sitter den alltid kvar. Vi ska nu beskriva en viktig egenskap inom matematiken som de flesta faktiskt redan har stött på i A-kursen i matematik men nog inte varit medvetna om det.

2.1 Mängdlära

Mängdlära nog den viktigaste delen inom matematiken. Det är synd att att man inte läser i den svenska skolan om mängdlära på grundligt sätt förr än i gymnasiet på kursen Diskret Matematik. Eftersom mängdlära bygger grunden för alla våra tal, så är det väldigt viktigt att kunna ha ett grepp om teorin för att kunna gå vidare till den högre matematiken. Låt oss nu ta en titt påvad en mängd är. En mängd kan tänkas vara en påse med saker i. Dessa saker i påsen kallas för element. Sättet att skriva en mängd i matematisk form ser ut såhär:

$$A = \{\clubsuit, \heartsuit, 3\}$$

Denna mängd som vi kallar för A har tre element: en klöver, ett hjärta och siffran tre. En mängd behöver alltså inte endast innehålla siffror. Det är tillåtet för elementen att vara saker och ting. Här har vi fler exempel på mängder:

$$B = \{1, 5, 8, 58\} \qquad C = \{4.5, 2\} \qquad D = \{\frac{1}{3}, \pi, \frac{4}{9}\} \qquad E = \{\frac{2}{3}, x, y, \sqrt{3}\}$$

2.2 Välkända Mängder

Mängden $\mathbb{Z}$ omfattar alla heltal:

$$\mathbb{Z} = \{-n \ldots -3, -2, -1, 0, 1, 2, 3, 4 \ldots n\}$$

Mängden $\mathbb{N}$ omfattar alla naturliga tal:

$$\mathbb{N} = \{0, \ldots 4, \ldots 7, \ldots n\}$$

Mängden $\mathbb{Q}$ omfattar alla rationella tal:

$$\mathbb{Q} = \{\text{alla tal } \frac{a}{b}, \text{ där a,b} \in \mathbb{Z} \text{ och b} \neq 0\}$$

Irrationella tal är speciella tal som har en förmåga att inte kunna skrivas påformen $\frac{a}{b}$ som till exempel $\sqrt{2}$, π och e. Mängden $\mathbb{R}$ omfattar de reella talen, där alla rationella och irrationella tal också ingår. De komplexa talen betecknas med $\mathbb{C}$ och består av alla tal $a + bi$ där a, b är reella. Alla dessa mängder är de absolut grundläggande begrepp som finns inom matematiken. För att förstå hur man kan tillämpa dessa mängder måste vi först ta en titt på några grundläggande operationer för mängder.

2.3 Grundläggande operationer för mängder

Nu när du vet vad en mängd är så inleder vi några grundläggande operationer för mängder.

Definition 2.3.1. Låt A och B vara mängder. *Unionen* av A och B, som skrivs $A \cup B$ är mängden som består av de element som tilhör antigen A eller B (eller båda). *Snittet* av A och B som skrivs $A \cap B$ är mängden som består av de element som tillhör både A och B.

Exempel 2.3.2. Låt mängden $A = \{1, 2, 3, 4, \ldots\}$, mängden $B = \{1, 3, 5, 7, \ldots\}$ och mängden $C = \{2, 4, 6, 8, \ldots\}$. Unionen av B och C består av de element som ligger i någon av mängderna. Detta medför att $B \cup C = A$ eftersom det finns element i B och C som också finns i A. Snittet av B och C är mängden av element som ligger i de båda mängderna. I detta fall blir snittet, $B \cap C = \emptyset$, det vill säga den tomma mängden.

2.4 Funktioner

Det finns ett till viktigt begrepp som krävs för förståelse om gruppteorin. Det begreppet är funktioner. Funktioner är allmänt väldigt välkända och nästan alla vet vad en funktion är.

Definition 2.4.1. Låt X och Y vara mängder. En funktion $f : X \longmapsto Y$ associerar till varje element $x \in X$ ett unikt element $y \in Y$.

Exempel 2.4.2. Den kanske mest kända funktionen är $y = kx + m$ eller om vi vill vara mer petiga så är y en funktion av x:

$$y = f(x) = kx + m$$

Vad säger den här funktionen egentligen? Det den säger är att om vi lägger in ett tal från x-planet i funktionen $f(x)$, så får vi ett nytt tal i y-planet. Om vi tar ett annat exempel och låter funktinen $f : \mathbb{R} \longmapsto \mathbb{R}$ och $f(x) = x^3 + 1$. Funktionen säger att om man tar ett element $x \in \mathbb{R}$ och lägger in det i funktionen, så får vi ett nytt element $f(x) \in \mathbb{R}$ som är en bild av x.

Anmärkning 2.4.3. Ofta säger man att f är en funktion från X till Y och kan skrivas som $f : X \longmapsto Y$. Man säger att funktionen *avbildar* ett element från X till Y. Vidare i det här kompendiet kommer vi att använda oss av skrivsättet $f : X \longmapsto Y$ och definiera funktionen.

Exempel 2.4.4. Vi tar ett exempel på en funktion som går från en ändlig mängd till en ändlig mängd. Vi låter mängderna $A = \{1, 2, 3\}$ och $B = \{2, 4, 6\}$. Betrakta funktionen $f : A \longmapsto B$ så att den definieras av $f(n) = 2n$ för $n \in A$. Vi har att: $f(1) = 2$, $f(2) = 4$ och $f(3) = 6$. Exemplet visar att elementen $n \in A$ och resultaten av funktionen visar att de tillhör B, vilket bevisar att funktionen går från A till B $f : A \longmapsto B$.

2.5 Injektion, surjektion och bijektion

Nu kommer vi till det som är väldigt viktigt att förstå och det är *bijektioner*. Inom gruppteorin måste man ha bijektioner för att någonting kan definieras som en grupp.

Definition 2.5.1 Om X och Y är mängder och $f : X \longmapsto Y$ en funktion så är funktionen f en *injektion* om det är så att $f(x) \neq f(y)$ för alla $x, y \in X : x \neq y$ Vidare, om det för varje element $y \in Y$ finns precis ett element $x \in X$ så att $f(x) = y$, det vill säga att när varje element i mängden Y är en bild av precis ett element i mängden X så är funktionen f en *surjektion*. Slutligen, om f är både en injektion och surjektion så är funktionen f en *bijektion*.

Exempel 2.5.2. Låt $X = \{1, 2, 3\}$ och $Y = \{1, 2, 3, 4, 5\}$. Vi definierar funktionen $f : X \longmapsto Y$ som $f(x) = x + 1$. Då är:

$$f(1) = 1 + 1 = 2$$
$$f(2) = 1 + 2 = 3$$
$$f(3) = 1 + 3 = 4$$

vilket visar att $f : X \longmapsto Y$ är en injektion eftersom $f(1)$, $f(2)$ och $f(3)$ är alla olika och avbildningarna är också olika.

Exempel 2.5.3. Låt $X = \{1, 2, 3\}$ och $Y = \{4, 8, 12\}$. Vi definierar funktionen $f : X \longmapsto Y$ som $f(x) = 4x$. Då har vi:

$$f(1) = 4 \times 1 = 4$$
$$f(2) = 2 \times 4 = 8$$
$$f(3) = 3 \times 4 = 12$$

Detta visar att varje element i Y är en bild av ett element i X, vilket betyder att funktionen är en surjektion. Denna funktion är också en injektion för att alla elementen i X är olika och deras avbildningar är också olika. Funktionen $f : X \longmapsto Y$ är en bijektion.

Notering 2.5.4. Funktionen i Exempel 2.5.2 är inte en surjektion eftersom elementen 1 och 5 i mängden Y har inte avbildningar i mängden X och därmed är det inte en bijektion.

2.6 Inversfunktioner

För varje bijektion finns en inversfunktion. Låt X och Y vara mängder och $x \in X$ och $y \in Y$. Betrakta bijektionen $f : X \longmapsto Y$. Vi kan definiera en funktion $f^{-1} : Y \longmapsto X$ sådant att till varje $y \in Y$ associerar det entydiga element $x \in X$ sådan att $f(x) = y$. Om vi låter $f^{-1}(y)$ vara det x som uppfyller att $f(x) = y$, så säger man att f och f^{-1} är inverser till varandra sådan att $f(f^{-1}(y)) = f(x) = y$ och $f^{-1}(f(x)) = f^{-1}(y) = x$

Sats 2.6.1. Om $f : X \longmapsto Y$ är en bijektion, så är inversen $f^{-1} : Y \longmapsto X$ också en bijektion.

Bevis 2.6.2. Ta $u, v \in Y : u \neq v$. Låt $f^{-1}(u) = x$ och $f^{-1}(v) = y$. Vi vet att $f(x) = u$ och att $f(y) = v$. Om $x = y$ så måste $f^{-1}(u) = f^{-1}(v)$ och $u = f(x) = f(y) = v$. Men eftersom $u = v$ så är $x \neq y$ som medför att $f^{-1}(u) \neq f^{-1}(v)$ och därmed visar att inversen en injektion. Vidare för varje $f(x) = y$ finns inversen $f^{-1}(y) = x : x \in X$ och $y \in Y$. Alltså för varje element $x \in X$ finns precis ett element $y \in Y$. Inversfunktionen är en surjektion och är därmed en bijektion. ■

3 GRUPPTEORI

Gruppteori har en väldigt unik ställning inom matematiken eftersom grupper inte endast uppstsår inom matematiken, utan i hela universum. Det är också möjligt att hitta grupper i exempelvis kemi och fysik. En grupp är en mängd med en binär operation $\circ$ som uppfyller några grundläggande villkor. Utifrån dessa villkor, som så många olika saker har gemensamt, kan man härleda en mängd användbara egenskaper. De villkoren, eller reglerna, som ger upphov till en grupp är alltså strikt kravsättande.

3.1 Vad kännetecknar en Grupp?

För att få en enkel och abstrakt förståelse av en grupps villkor kan man sammanfatta definitionen på följande sätt:

Definition 3.2.1. Låt G vara en mängd med operationen $\circ$. Liksom alla binära operationer på G, gäller att $x \circ y \in G$ för alla $x, y \in G$. Man säger att G är sluten under $\circ$ och skrivs ofta som $(G, \circ)$. Vidare gäller följande:

(i) $(G, \circ)$ är associativ enligt $x \circ (y \circ z) = (x \circ y) \circ z$ för alla $x, y, z \in G$

(ii) Det finns ett enhetselement $e \in G$ till x som uppfyller att $x \circ e = e \circ x = x$

(iii) För varje element $x \in G$ finns en invers $x^{-1} \in G : \ x \circ x^{-1} = x^{-1} \circ x = e$

Dessa tre egenskaper kallas för *gruppaxiomen* och bildar gruppen $(G, \circ)$. Observera att $\circ$ är en binär operation som kan vara allt från multiplikation, addition, subtraktion, division eller någon annan operation som man kan definiera.

3.2 Definitioner och exempel på olika Grupper

Inom gruppteorin är definitionen för en operation viktig, eftersom om vi inte har en operation, kan vi inte få någon grupp. Nedan visar vi ett flertar definitioner och exempel på mängder slutna till en viss operation, vilket sedan bildar grupper eller ej visas i exemplen.

Definition 3.2.2. Vi betraktar operationen *addition* för mängderna $\mathbb{Z}$, $\mathbb{Q}$ och $\mathbb{R}$. Om det finns tre element $m, n, p \in \mathbb{Z}$; $m, n, p \in \mathbb{Q}$; och $m, n, p \in \mathbb{R}$, då gäller:

1. $(m + n) + p = m + (n + p)$

2. $0 + m = m = m + 0$

3. $m + (-m) = 0 = -m + m$

Exempel 3.2.3. Vi undersöker om $(\mathbb{Z}, +)$ enligt defenition bildar en grupp och låter $m = -2$, $n = 5$ och $p = 3$. Då har vi att:

1. $(-2 + 5) + 3 = 3 + 3 = 6 = -2 + 8 = -2 + (5 - 3)$

2. $0 + (-2) = -2 = -2 + 0$

3. $-2 - (-(-2)) = 0 = (-(-2)) + (-2)$

Alltså är $(\mathbb{Z}, +)$ en grupp, eftersom den har uppfyllt alla tre gruppaxiomen.

Exempel 3.2.4. Om vi låter elementen för $(\mathbb{Q}, +)$ vara $m = \frac{1}{5}$, $n = \frac{2}{3}$ och $p = \frac{1}{3}$, så gäller:

1. $\left(\frac{1}{5} + \frac{1}{3}\right) + \frac{1}{2} = \frac{8}{15} + \frac{1}{2} = \frac{31}{30} = \frac{1}{5} + \frac{5}{6} = \frac{1}{5} + \left(\frac{1}{3} + \frac{1}{2}\right)$

2. $0 + \frac{1}{5} = \frac{1}{5} = \frac{1}{5} + 0$

3. $\frac{1}{5} + (-\frac{1}{5}) = 0 = -\frac{1}{5} + \frac{1}{5}$

Vi ser här också att $(\mathbb{Q}, +)$ är en grupp.

Exempel 3.2.5. För $(\mathbb{R}, +)$ låter vi $m = 4$, $n = 3$ och $p = -1$. Då gäller:

1. $(4 + 3) + (-1) = 6 = 4 + (3 + (-1))$

2. $0 + 4 = 4 = 4 + 0$

3. $-4 + 4 = 0 = 4 + (-4)$

Alltså är $(\mathbb{R}, +)$ också en grupp.

Exempel 3.2.6 Nu undersöker vi om $(\mathbb{N}, +)$ är en grupp. Vi låter $m = 1$, $n = 2$ och $p = 3$. D gäller:

1. $(1 + 2) + 3 = 6 = 1 + (2 + 3)$
2. $0 + 1 = 1 = 1 + 0$
3. $-1 + 1 = 0 = 1 + (-1)$

Här ser vi att inversen till $m = 1$ måste vara -1, men eftersom talet inte finns med i de naturliga talen $\mathbb{N}$, uppfyller $(\mathbb{N}, +)$ inte alla tre gruppaxiomen, vilket medför att $(\mathbb{N}, +)$ *inte* är en grupp!

Vi har nu visat några exempel på hur en mängd med operationen addition bildar en grupp och ett exempel på hur den inte bildar en grupp. Nästa steg är att definiera operationen *multiplikation* i en grupp.

Definition 3.2.7. Vi betraktar operationen multiplikation för mängderna $\mathbb{Q}$ och $\mathbb{R}$. Om det finns tre element $a, b, c \in \mathbb{Q} \setminus \{0\}$ och $a, b, c \in \mathbb{R} \setminus \{0\}$, alltså man bortser från noll i båda mängderna så gäller:

1. $(a \times b) \times c = a \times (b \times c)$
2. $1 \times a = a = a \times 1$
3. $\frac{1}{a} \times a = 1 = a \times \frac{1}{a}$

Exempel 3.2.8. För $a, b, c \in \mathbb{Q} \setminus \{0\} = \{a, b, c \in \mathbb{Q} \colon a \neq 0\}$ låter vi $a = \frac{1}{2}$, $b = \frac{1}{3}$ och $c = \frac{1}{4}$. Då gäller:

1. $\left(\frac{1}{2} \times \frac{1}{3}\right) \times \frac{1}{4} = \frac{1}{6} \times \frac{1}{4} = \frac{1}{24} = \frac{1}{2} \times \frac{1}{12} = \frac{1}{2} \times \left(\frac{1}{3} \times \frac{1}{4}\right)$
2. $1 \times \frac{1}{2} = \frac{1}{2} = \frac{1}{2} \times 1$
3. $2 \times \frac{1}{2} = 1 = \frac{1}{2} \times 2$

$(\mathbb{Q}, \times)$ är en grupp om och endast om vi bortser nollan från mängden, eftersom $\frac{1}{a}$ är inte definierat för $a = 0$ och då kan vi inte heller hitta en invers till $(\mathbb{Q}, \times)$, då den måste vara $\frac{1}{a}$. Notera att inversen $\frac{1}{a}$ för $a = \frac{1}{2}$ är lika med 2.

Exempel 3.2.9. För $a, b, c \in \mathbb{R} \setminus \{0\} = \{a, b, c \in \mathbb{R} \colon a \neq 0\}$ sätter vi $a = 2$, $b = 0,5$ och $c = -3$. Då gäller:

1. $(2 \times 0,5) \times (-3) = 1 \times (-3) = -3 = 2 \times (-1,5) = 2 \times (0,5 \times (-3))$
2. $1 \times 2 = 2 = 2 \times 1$
3. $2 \times 2^{-1} = 1 = 2^{-1} \times 2$

På samma sätt är $(\mathbb{R}, \times)$ en grupp om och endast om $a \neq 0$. Observera att i denna grupp är inversen $2^{-1} = \dfrac{1}{2}$

Nu ska vi ta en speciell operation som vi själva definierar. Eftersom vi vet att $\circ$ är en binär operation som kan vara vilken operation som helst så definierar vi $\circ$ på ett nytt sätt.

Definition 3.3.10. Låt $a \circ b = a + b - ab$. Om det finns tre element $a, b, c \in \mathbb{R} \setminus \{1\}$ och $a, b, c \in \mathbb{Q} \setminus \{1\}$, så gäller:

1. $(a \circ b) \circ c = a \circ (b \circ c)$
2. $0 \circ a = a \circ 0$
3. $\dfrac{-a}{1-a} \circ a = a \circ \dfrac{-a}{1-a}$

Exempel 3.3.11. Om vi nu använder oss av de reella talen sådan att $\mathbb{R} \setminus \{1\} = \{a \in \mathbb{R} \colon a \neq 0\}$ och låter $a = 5$, $b = -2$ och $c = 0$. Då gäller:

1. $(5 \circ -2) \circ 0 = (5 \circ -2) + 0 - (5 \circ -2) \times 0 = (5 + (-2) - (-10)) + 0 - (5 + (-2)) - (-10)) \times 0 = 0 = 5 \circ (-2 \circ 0)$
2. $0 \circ 5 = 0 + 5 - 5 \times 5 = 5 = 5 \circ 0$
3. $\dfrac{-5}{1-5} \circ 5 = \dfrac{-5}{-4} + 5 - \left(\dfrac{-5}{-4} \times 5\right) = \dfrac{5+20}{4} - \dfrac{25}{4} = \dfrac{25}{4} - \dfrac{25}{4} = 0 = 5 \circ \dfrac{-5}{1-5}$

Exempel 3.3.12. Vidare kan vi visa att de rationella talen följer exakt samma regler som elementen i de reella talen. För $\mathbb{Q} \setminus \{1\} = \{a \in \mathbb{Q} \colon a \neq 0\}$ låter vi $a = \dfrac{1}{2}$, $b = 2$ och $c = 3$. Då gäller:

1. $\left(\frac{1}{2} \circ 2\right) \circ 3 = \left(\frac{1}{2} \circ 2\right) + 3 - \left(\frac{1}{2} \circ 2\right) \times 3 = \left(\frac{1}{2} + 2 - \frac{1}{2} \times 2\right) + 3 - \left(\frac{1}{2} + 2 - \frac{1}{2} \times 2\right) \times 3 = \frac{1}{2} + 2 + 3 - \frac{1}{2} \times 2 - \frac{1}{2} \times 3 - 2 \times 3 + \frac{1}{2} \times 2 \times 3 = \frac{1}{2} + 5 - 1 - \frac{3}{2} - 6 + 3 = \frac{1}{2} \circ (2 \circ 3)$
2. $0 \circ \frac{1}{2} = 0 + \frac{1}{2} - 0 \times \frac{1}{2} = \frac{1}{2} = \frac{1}{2} \circ 0$
3. $\frac{-\frac{1}{2}}{1 - \frac{1}{2}} \circ \frac{1}{2} = \frac{-\frac{1}{2}}{1 - \frac{1}{2}} + \frac{1}{2} - \left(\frac{-\frac{1}{2}}{1 - \frac{1}{2}} \times \frac{1}{2}\right) = \frac{-\frac{1}{2}}{\frac{1}{2}} + \frac{1}{2} - \left(\frac{-\frac{1}{4}}{\frac{1}{2}}\right) = -1 + \frac{1}{2} + \frac{1}{2} = 0 = \frac{1}{2} \circ \frac{-\frac{1}{2}}{1 - \frac{1}{2}}$

Vi ser att både $\mathbb{R}$ och $\mathbb{Q}$ med vår egen definierad binär operation $\circ$ bildar en grupp. Det spelar alltså ingen roll vilken operatioin det är, utan *hur* vi definierar operationen. Det är det som gör matematiken unik i jämförelse med fysik eller kemi, att om vi definierar exempelvis en viss formel på ett sådant sätt den funkar, så kan man inte säga att operationen är fel eftersom definitionen säger att den är korrekt. Nu när vi bevisat gruppaxiom med olika operationer för olika mängder kan vi ta ett nästa steg och det är hur vi kan tillämpa gruppteorin i t.ex. vardagslivet. Nästa del handlar om *permutationer*.

4 GRUPPER AV PERMUTATIONER

I denna del kommer vi att visa möjligheten på tillämpning av gruppteorin. Det som vi har visat tidigare är bara grunden och det är inte förräns här gruppteorin börjar bli väldigt spännande.

4.1 Permutationer

Definition 4.1.1. En *permutation* ϕ av en mängd, låt oss säga X är en bijektion $\phi : X \longmapsto X$.

Exempel 4.1.2. Som en notering innan vi går vidare. Med permutation menas att man *kastar om* ordningen av element i en mängd. Vi låter exempelvis mängden $X = \{A, B, C\}$ och låter $\phi : X \longmapsto X$. Antag att elementen A, B, C är 3 personer som står på rad enligt mängden X. Om vi nu ändrar ordningen, eller permuterar dessa personer till från ABC till ACB, så har vi en funktion $\phi : ABC \longmapsto ACB$. Detta kan ges av $\phi(A) = A$, $\phi(B) = C$ och $\phi(C) = B$. Vidare kan vi visa att det finns totalt 6 stycken permutationer eftersom det finns 3 element som kan permuteras $3! = 1 \times 2 \times 3 = 6$ gånger:

$$\begin{array}{lll} ABC \longmapsto ABC & ABC \longmapsto ACB & ABC \longmapsto BCA \\ ABC \longmapsto BAC & ABC \longmapsto CAB & ABC \longmapsto CBA \end{array}$$

Lägg märke till att även $ABC \longmapsto ABC$ är en permutation som kallas för *identitetspermutation* och vi beteknar det med ϵ. Varje permutation är uppenbarligen en bijektion till sig själv.

4.2 Sammansättning av permutationer

Hur kan en permutation då bilda grupper? Vi har bara permuterat och använt oss av funktioner men inte sett någon gruppstruktur. En permutationsgrupp består av alla bijektioner på en mängd X tillsammans med operationen $\circ$ som är en sammansättning av bijektioner.

Exempel 4.2.1. Låt mängden $X = \{2, 4, 6, 8\}$. Vi låter unktionerna $\rho : X \longmapsto X$ och $\sigma : X \longmapsto X$ betraktas som $\rho : 2468 \longmapsto 4268$ och $\sigma : 2468 \longmapsto 8246$. Enligt betraktelsen har vi exempelvis att:

$$\rho(2) = 4 \qquad \sigma(8) = 6 \qquad \rho(4) = 2$$

Det vi gör här är att vi sammansätter permutationerna ρ och σ med operationen $\circ$, alltså $\rho \circ \sigma$ så får vi:

$$(\rho \circ \sigma)(2) = \rho(\sigma(2)) = \rho(8) = 8$$
$$(\rho \circ \sigma)(4) = \rho(\sigma(4)) = \rho(2) = 4$$
$$(\rho \circ \sigma)(6) = \rho(\sigma(6)) = \rho(4) = 2$$
$$(\rho \circ \sigma)(8) = \rho(\sigma(8)) = \rho(6) = 6$$

Vi har att sammansättningen $\rho \circ \sigma$ ger permutationen $\rho \circ \sigma : 2468 \longmapsto 8426$

Det är faktiskt så att sammansättningen av permutationer är en bijektion, det vill säga att sammansättningen av två bijektioner är en bijektion. Om vi antar att X är en ändlig mängd och ρ, σ är permutationer av X och vi sammansätter dem. Om vi har två element $x, y \in X$ sådan att $x \neq y$ och låter $\sigma(x) = m$ och $\sigma(y) = n$ så ser vi att $m \neq n$ vilket tyder på att det är en injektion. Det visar sig också att för varje element i permutationen σ finns precis ett element i permutationen ρ efter sammansättningen, vilket visar att det är en surjektion.

4.3 Gruppstruktur för permutationer

Vi ska nu unersöka om de tre egenskaper som gäller för att en grupp ska uppstå gäller också för sammansättning av permutationer. $Perm(X)$ innefattar alla de möjliga permutationer för mängden X. Vi ska alltså undersöka om de tre gruppaxiomen gäller även här om $Perm(X)$ är accosiativ enligt $\rho \circ (\sigma \circ \varphi) = (\rho \circ \sigma) \circ \varphi$, om det finns en identitetspermutation sådan att $\sigma \circ \epsilon = \epsilon \circ \sigma = \sigma$ som tillhör $Perm(X)$ och om det finns en invers sådan att $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = \epsilon$. Låt oss nu bevisa att $Perm(X)$ faktiskt är en grupp:

Sats 4.3.1. Anta att X är en ändlig mängd. $Perm(X)$ är alla permutationer för mängden X. Då är $\circ$ en binär operation som sammansätter permutationerna. Mängden $Perm(X)$ tillsammans med $\circ$ är en grupp.

Bevis 4.3.2. Låt σ, ρ och φ vara permutationer som tillhör $Perm(X)$ och vi sammansätter permutationerna med operationen $\circ$. Nu så gäller att bevisa de tre gruppaxiomen:

1. Vi måste bevisa att $\rho \circ (\sigma \circ \varphi) = (\rho \circ \sigma) \circ \varphi$. Om vi låter $x \in X$ och antar permutationerna $y_1 = \rho \circ (\sigma \circ \varphi)$ och $y_2 = (\rho \circ \sigma) \circ \varphi$. När vi

sätter elementet x i y_1, måste vi få samma permutation som när man sätter x i y_2. Alltså måste $y_1 = y_2$. Då gäller:

$$y_1 = \rho((\sigma \circ \varphi)(x)) = \rho(\sigma(\varphi(x))) = (\rho \circ \sigma)(\varphi(x)) = y_2$$

Vilket i sin tur bevisar att permutationsgruppen är associativ.

2. Nu visar vi att det finns en identitespermutation. En identitetspermutation är en sådan permutation som sammansätter med vilken permutation som helst och i slutskedet får man samma ordning som för den andra permutationen. Låt $\epsilon : X \longmapsto X$ definieras av $\epsilon(x) = x$ för alla $x \in X$. För att bevisa att ϵ är en permutation som tillhör $Perm(X)$ måste vi bevisa att det är en bijektion. Vi har att ϵ är en injektion om $x, y \in X$ och $x \neq y$. Då gäller att:

$$\epsilon(x) = x \neq y = \epsilon(y)$$

Vidare är ϵ en surjektion om det finns bara en bild $y : y \in X$ för varje x och $x = y$. Vi har att:

$$\epsilon(x) = y$$

vilket visar att ϵ är en bijektion. Om vi nu låter $\sigma \in Perm(X)$ och $x \in X$ så har vi att $(\sigma \circ \epsilon)(x) = \sigma(\epsilon(x)) = \sigma(x)$ och att $(\epsilon \circ \sigma)(x) = \epsilon(\sigma(x)) = \sigma(x)$. Detta medför att:

$$\sigma \circ \epsilon = \epsilon \circ \sigma = \sigma$$

och då visar det sig att ϵ är identiteten i $Perm(X)$

3. Slutligen har vi inversen. I detta fall vet vi att för varje bijektion finns en annan inversfuktion (enligt Sats 2.6.1.) Denna funktion är också en permutation som tillhör $Perm(X)$ och resultatet av en permutation utfört med en binär operation med dess invers är ϵ. Vad vi egentligen menar med detta är att i $Perm(X)$ finns alla möjliga permutationer och att det för varje permutation finns en permutation sådan att vi får identitetspermutationen ϵ. Vi låter $\varphi \in Perm(X)$, då gäller:

$$\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = \epsilon$$

som slutligen visar att permutationsgruppen uppfyller de grundläggande gruppaxiomen och kan därför definieras som en grupp. ■

Exempel 4.3.3. Vi använder oss av permutationerna $\rho : 2468 \longmapsto 4268$ och $\sigma : 2468 \longmapsto 8246$ från exempel 4.2.1 samt lägger till en permutation $\varphi : 2468 \longmapsto 2486$. Det första gruppaxiomen är associativitet. Då gäller:

1. Vi permuterar alla element i ordningen 2468 och börjar med 2:an, alltså har vi att

$$V.L. = \rho \circ (\sigma \circ \varphi)(2) = \rho(\sigma(2)) = \rho(8) = 8$$
$$H.L = (\rho \circ \sigma)(\varphi(2)) = (\rho \circ \sigma)(2) = \rho(\sigma(2)) = \rho(8) = 8$$
$$V.L = H.L$$

   vidare för element 4,

$$V.L = \rho \circ (\sigma \circ \varphi)(4) = \rho(\sigma(4)) = \rho(2) = 4$$
$$H.L = (\rho \circ \sigma)(\varphi(4)) = (\rho \circ \sigma)(4) = \rho(\sigma(4)) = \rho(2) = 4$$
$$V.L = H.L$$

   vidare för element 6,

$$V.L = \rho \circ (\sigma \circ \varphi)(6) = \rho(\sigma(8)) = \rho(6) = 6$$
$$H.L = (\rho \circ \sigma)(\varphi(6)) = (\rho \circ \sigma(8)) = \rho(\sigma(8)) = \rho(6) = 6$$
$$V.L = H.L$$

   slutligen för element 8 har vi

$$V.L = \rho \circ (\sigma \circ \varphi)(8) = \rho(\sigma(6)) = \rho(4) = 2$$
$$H.L = (\rho \circ \sigma)(\varphi(8)) = (\rho \circ \sigma(6)) = \rho(\sigma(6)) = \rho(4) = 2$$
$$V.L = H.L$$

   alltså är permutationsgruppen är associativ.

2. Nu visar vi att det finns en identitetspermutation. Man får identitetspermutationen på ett sådant sätt att om man sätter elementet x i funktionen (permutationen) så får man tillbaka x som resultat. Vi har att:

$$\rho \circ \rho(2) = \rho(4) = 2$$
$$\rho \circ \rho(4) = \rho(2) = 4$$
$$\rho \circ \rho(6) = \rho(6) = 6$$
$$\rho \circ \rho(8) = \rho(8) = 8$$

   och vi vet också att permutationen $\rho \circ \rho = \epsilon$ är identitetspermutationen där $\epsilon : 2468 \longmapsto 2468$ som i princip inte gör någon permutation alls. Det finns alltså en identitetspermutation.

3. Varje permutation har en invers som resulterar i permutationen ϵ. Exempelvis är permutationen $\rho \circ \rho = \epsilon$, det vill säga att ρ är invers till sig självt. Vi tar exempelvis funktionen $\delta : 2468 \longmapsto 4682$ som är inversen till σ. Då gäller:

$$(\sigma \circ \delta)(2) = \sigma(4) = 2$$
$$(\sigma \circ \delta)(4) = \sigma(6) = 4$$
$$(\sigma \circ \delta)(6) = \sigma(8) = 6$$
$$(\sigma \circ \delta)(8) = \sigma(2) = 8$$

vi har nu visat att vi får då identitetspermutationen ϵ, vilket i sin tur bevisar att permutationsgruppen uppfyller de grundläggande gruppaxiomen och kan därfor definieras som en grupp.

5 Referenser

1. J. Arlind, A. Enblom, *Gruppteori*, Kungliga Tekniska Högskolan (KTH), Institutionen för Matematik, 2006

2. C.C. Pinter, *Book of Abstract Algebra*, McGraw-Hill Math, 1990

3. T. Rowland, Group, *http://mathworld.wolfram.com/Group.html*

4. Group theory, *http://en.wikipedia.org/wiki/Grouptheory*