2. Gruppteori

Vi inleder detta kapitel med att definiera de grundläggande begreppen operation, algebraisk struktur, neutralt element, inverterbart element, associativ och kommutativ operation.

Grupper

Definition. *En operation på en icke-tom mängd A är en avbildning från $A \times A$ till A. Om operationen betecknas $*$, så tillordnas varje ordnat par $(a, b) \in A \times A$ exakt ett element i A, vilket betecknas $a * b$.*

Med andra ord är $*$ en operation på A om och endast om villkoren (1) *och* (2) *gäller:*

(1) *$a * b$ är entydigt definierat för alla a och b i A;*

(2) *$a * b \in A$ för alla $a, b \in A$.*

Anmärkning. Villkoret (2) ovan, som förutsätter att (1) gäller, kan vi uttrycka med att säga att mängden A **är sluten under operationen** $*$.

Exempel på operationer på de hela talens mängd $\mathbf{Z}$ är addition, subtraktion och multiplikation, varvid $a * b$ betyder $a + b$, a-b respektive $a \cdot b$.

Division är inte en operation på $\mathbf{Z}$, eftersom division med 0 inte är definierat. Inte heller på $\mathbf{Z} \setminus \{0\}$ är division en operation, ty kvoten av två heltal behöver inte vara ett heltal, så villkor (2) är inte uppfyllt. Däremot är division på $\mathbf{Q} \setminus \{0\}$ en operation, där $\mathbf{Q}$ betecknar de rationella talen.

Om $f : A \to A$ och $g : A \to A$ är funktioner, så skall vi med $f \circ g$ alltid avse **funktionssammansättningen**, dvs. den funktion från A till A som definieras av

$$(f \circ g)(x) = f(g(x)), \text{ för varje } x \in A.$$

Funktionssammansättningen $\circ$ är en operation på A^A. (Här betecknar A^A mängden av alla funktioner från A till A).

Definition. *En (algebraisk) struktur är en mängd A försedd med en eller flera operationer. En mängd A med operationen $*$ bildar en struktur som betecknas $\langle A, * \rangle$. Vidare definierar vi ordningen för A som antalet element i mängden, beteckning $|A|$. Om A inte är ändlig säges A ha oändlig ordning.*

En struktur $\langle A, * \rangle$ är entydigt bestämd av mängden A och av att man för varje $a, b \in A$ känner produkten $a * b$. Om A är en ändlig mängd, strukturen kallas då också ändlig, kan man fullständigt beskriva strukturen med en kompositionstabell.

Exempel. Om $A = \{a, b\}$, $a * a = b * a = b * b = a$ och $a * b = b$, så har kompositionstabellen utseendet

$*$	a	b
a	a	b
b	a	a

Definition. *Låt $\langle A, * \rangle$ vara en struktur. Ett neutralt element för $*$ är ett element $e \in A$ sådant att*

$$e * a = a * e = a, \text{ för varje } a \in A.$$

Ett element $a \in A$ är inverterbart med avseende på $*$ om det finns ett element $a' \in A$ sådant att

$$a' * a = a * a' = e\,.$$

Varje sådant element a' kallas invers till a.

Vi skall nu visa att för en associativ operation har varje element högst en invers. Härvid säges en operation $*$, och även strukturen $\langle A, * \rangle$, vara **associativ** om

$$a * (b * c) = (a * b) * c, \text{ för alla } a, b, c \in A\,,$$

och **kommutativ** om

$$a * b = b * a, \text{ för alla } a, b \in A.$$

Sats 11. *Låt $\langle A, * \rangle$ vara en struktur.*

a) Då har operationen $*$ högst ett neutralt element i A;

b) om operationen $*$ på A är associativ med neutralt element, så har varje inverterbart element exakt en invers.

Bevis: a) Antag att e och e' är neutrala element. Då gäller:

$$e \text{ neutralt element } \Rightarrow e * e' = e' * e = e',$$
$$e' \text{ neutralt element } \Rightarrow e' * e = e * e' = e\,.$$

Alltså gäller det att $e = e'$.

b) Antag att $*$ är associativ med neutralt element e och att elementet $a \in A$ är inverterbart. Om u och v är inverser till a så gäller:

$$u = u * e = u * (a * v) = (u * a) * v = e * v = v,$$

alltså är $u = v$. □

Anmärkning. Om elementet $a \in A$ är inverterbart med en entydigt bestämd invers, så betecknas denna a^{-1}.

Definition. *En grupp $\langle G, * \rangle$ är en algebraisk struktur som satisfierar följande axiom:*

(*i*) $a * (b * c) = (a * b) * c$, *för alla* $a, b, c \in G$;

(*ii*) *Det finns ett neutralt element* $e \in G$ *sådant att* $e * a = a * e = a$ *för alla* $a \in G$;

(*iii*) *För varje* $a \in G$ *finns det ett element* $a^{-1} \in G$ *sådant att* $a * a^{-1} = a^{-1} * a = e$.

Anmärkning. Med stöd av Sats 11 är e och a^{-1} i ovanstående definition entydigt bestämda.

Om $|G| < \infty$, så är $\langle G, * \rangle$ en **ändlig grupp**. En ändlig grupp $\langle \{e, a_1, ..., a_n\}, * \rangle$ är fullständigt bestämd av sin kompositionstabell.

Exempel.

1) $\langle \mathbf{R}, + \rangle$ är en grupp med $e = 0$ och $a^{-1} = \text{-}a \ \ \forall\ a \in \mathbf{R}$.

$\langle \mathbf{Z}, + \rangle$ är en grupp med $e = 0$ och $a^{-1} = \text{-}a \ \ \forall\ a \in \mathbf{Z}$

$\langle \{0, 1, 2, \ldots\}, + \rangle$ är inte en grupp, eftersom $e = 0$ men $a > 0$ saknar invers.

$\langle \{0, \pm 2, \pm 4, \pm 6, \ldots\}, + \rangle$ är en grupp med $e = 0$ och $a^{-1} = \text{-}a$.

$\langle \underbrace{\{0, \pm 1, \pm 2\}}_{A}, + \rangle$ är inte en grupp. Vi har $e = 0$ och $a^{-1} = \text{-}a$, men A är ej sluten under $+$, exempelvis så gäller att $2 + 2 \notin A$.

2) $\langle \mathbf{R}, \bullet \rangle$ är inte en grupp, ty den är associativ och $e = 1$, men 0 saknar invers.

$\langle \mathbf{R} \setminus \{0\}, \bullet \rangle$ är en grupp med $e = 1$ och $a^{-1} = \frac{1}{a} \ \ \forall\ a \in \mathbf{R} \setminus \{0\}$.

3) Låt $\langle \{a, b, c\} \rangle, * \rangle$ vara en grupp med

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

där a är ett neutralt element, $e = a$.

$$\begin{cases} b * c = a \\ c * b = a \end{cases} \Rightarrow \begin{cases} b^{-1} = c \\ c^{-1} = b \end{cases}$$

Det är klart att $(a^{-1} = a)$.

4) Kan följande tabell vara kompositionstabellen till en grupp $\langle \{a, b, c\}, * \rangle$?

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

Antites: Tabellen är kompositionstabellen till gruppen. Då är $e = b$ och vidare gäller att

$$b = e = c * c^{-1} = \overbrace{(c * c)}^{c} * c^{-1} = c * (c * c^{-1}) = c * e = c$$

Vi har nu konstaterat att $b = c$ vilket är en motsägelse. Antitesen är alltså falsk och tabellen kan inte vara en kompositionstabell till $\langle \{a, b, c\}, * \rangle$.

Sats 12. *Låt a, b, c vara element i en grupp $\langle G, * \rangle$.*

(i) Då gäller strykningslagarna:

$$c * a = c * b \Rightarrow a = b;$$

$$a * c = b * c \Rightarrow a = b\,.$$

(ii) Då har ekvationen

$$a * x = b$$

exakt en lösning $x = a^{-1} * b$.

Bevis: (i) Då c har inversen c^{-1} erhåller vi att

$$\begin{aligned} c * a = c * b &\Rightarrow c^{-1} * (c * a) = c^{-1} * (c * b) \\ &\Rightarrow (c^{-1} * c) * a = (c^{-1} * c) * b \\ &\Rightarrow e * a = e * b \\ &\Rightarrow a = b\,. \end{aligned}$$

Analogt bevis för den andra strykningslagen.

(ii) Vi har att $x = a^{-1} * b$ är en lösning, ty

$$a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b\,.$$

Antag att både x_1 och x_2 är lösningar till ekvationen. Då är

$$a * x_1 = a * x_2\,(= b),$$

så del (i) ger att $x_1 = x_2$. Vi har således exakt en lösning. □

Korollarium 13. *Om $\langle G, * \rangle$ är en ändlig grupp, så är varje rad och kolonn i kompositionstabellen en permutation av gruppens element.*

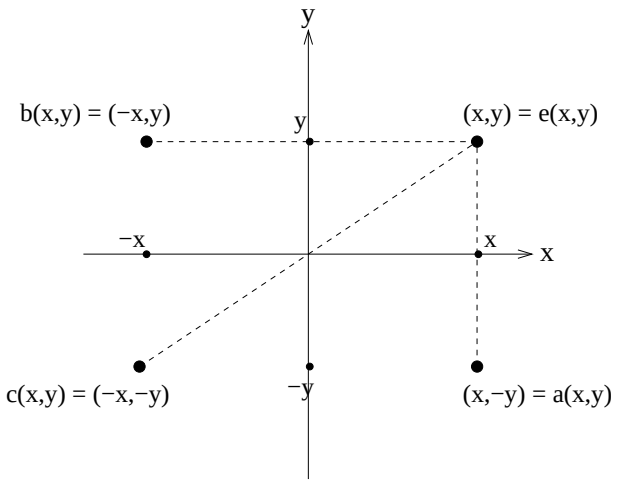
Bevis: (Hemuppgift)

Exempel på viktiga grupper

Exempel. Kleins fyragrupp. (Felix Klein, 1849-1925, tysk matematiker)

Betrakta $\mathbf{R}^2 = \{(x, y) : x, y \in \mathbf{R}\}$. Låt G bestå av fyra avbildningar:

$$\begin{cases} e = \text{identiska avbildningen}, \\ a = \text{spegling i x-axeln}, \\ b = \text{spegling i y-axeln}, \\ c = \text{spegling i origo}. \end{cases}$$



Figur 1.

Låt $\circ$ svara mot funktionssammansättningen. Då erhålls gruppen $\langle G, \circ \rangle$, **Kleins fyragrupp**, med kompositionstabellen

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Exempel. Gruppen av restklasser modulo n. Definiera för $n \geq 1$ mängden Z_n och operationen $+_n$ genom:

$$Z_n = \{0, 1, ..., n\text{-}1\},$$
$$i +_n j = \begin{cases} i + j, & \text{om } 0 \leq i + j \leq n\text{-}1; \\ i + j\text{-}n, & \text{om } i + j \geq n\,. \end{cases}$$

Strukturen $\langle Z_n, +_n \rangle$ har då kompositionstabellen

$+_n$	0	1	2	$\cdots$	n-1
0	0	1	2	$\cdots$	n-1
1	1	2	3	$\cdots$	0
$\vdots$		$\vdots$			$\vdots$
n-1	n-1	0	1	$\cdots$	n-2

så vi noterar att 0 är ett neutralt element och att inversen till elementet k ges av

$$k^{-1} = \begin{cases} n \Leftrightarrow k, & \text{om } k = 1, ..., n \Leftrightarrow 1; \\ 0, & \text{om } k = 0. \end{cases}$$

Som hemuppgift lämnas beviset av att $\langle Z_n, +_n \rangle$ är en grupp.

Anmärkning. Vi noterar att $|Z_n| = n$, så det finns grupper av godtycklig ändlig ordning. Vidare märker vi att kompositionstabellen i ovanstående exempel är symmetrisk kring diagonalen, dvs. $i +_n j = j +_n i$.

Definition. *En grupp $\langle G, * \rangle$ kallas Abelsk om $a * b = b * a$ för alla $a, b \in G$.*

Exempel på Abelska grupper är $\langle R, + \rangle$, $\langle Z, + \rangle$ och $\langle Z_n, +_n \rangle$. (Niels Henrik Abel, 1802-1829, norsk matematiker).

Exempel. Den linjära gruppen $GL(n, R)$ av inverterbara $n \times n$ matriser kan skrivas

$$GL(n, \mathbf{R}) = \langle \{A : A \text{ är en } n \times n\text{-matris med reella element och } A^{-1}\text{existerar}, \}, \bullet \rangle$$

där $\bullet$ är operationen matrismultiplikation. $GL(n, \mathbf{R})$ är sluten under $\bullet$, ty

$$\begin{aligned} A, B \text{ är inverterbara matriser} &\Rightarrow \det A \neq 0 \neq \det B \\ &\Rightarrow \det(A \bullet B) = \det A \cdot \det B \neq 0 \\ &\Rightarrow A \bullet B \text{ inverterbar } n \times n \text{ matris.} \end{aligned}$$

(i) $A \bullet (B \bullet C) = (A \bullet B) \bullet C$, dvs $\bullet$ är associativ.
(ii) $I \bullet A = A \bullet I = A$, där det neutrala elementet är enhetsmatrisen I.
(iii) $A \bullet A^{-1} = A^{-1} \bullet A = I$, där A^{-1} är en entydig invers.

$GL(n, \mathbf{R})$ är alltså en grupp. Om $n > 1$ är i regel $A \bullet B \neq B \bullet A$. Den linjära gruppen $GL(n, \mathbf{R})$ är alltså inte abelsk om $n > 1$. ($GL(1, \mathbf{R}) = \langle \mathbf{R} \setminus \{0\}, \bullet \rangle$)

Anmärkning. I fortsättningen betecknas en grupp $\langle G, * \rangle$ ofta med G och operationen $a * b$ med $a\,b$.

Definition. *De positiva och negativa potenserna av ett element a i en grupp $\langle G, * \rangle$ definieras genom:*

$$\begin{aligned} &a^0 = e,\ a^1 = a,\ a^n = a\,a^{n-1}, \quad \textit{för } n \geq 2, \\ &a^{-1} = a^{-1},\ a^{-m} = a^{-1}a^{-(m-1)}, \quad \textit{för } m \geq 2. \end{aligned}$$

Man kan då visa att för alla $m, n \in Z$ gäller:

$$a^m a^n = a^{m+n} \text{ och } (a^m)^n = a^{m\,n}\,.$$

Definition. *En grupp G kallas cyklisk om det finns ett element $a \in G$ sådant att*

$$G = \{a^k : k \in Z\}.$$

Exempel. Exempel på cykliska grupper.

a) $\langle \mathbf{Z}, + \rangle$ är en cyklisk grupp, ty med $a = 1$ erhåller vi

$$\begin{cases} a^k = 1^k = \underbrace{1 + 1 + \ldots + 1}_{\text{k st.}} = k, \quad \forall\ k \in \mathbf{Z}_+ \\ a^0 = 1^0 = e = 0 \\ a^{-k} = 1^{-k} = (1^{-1})^k = \overbrace{(\text{-}1) + (\text{-}1) + \ldots + (\text{-}1)}^{\text{k st.}} = \text{-}k, \quad \forall k \in \mathbf{Z}_+ \end{cases}$$

Vi har alltså $\langle \mathbf{Z}, + \rangle = \langle \{1^k : k \in \mathbf{Z}\}, + \rangle$.

b) $\langle \mathbf{Z}_n, +_n \rangle$ är cyklisk, ty

$$\begin{aligned} 1^0 &= e = 0 \\ 1^1 &= 1 \\ 1^2 &= 1 +_n 1 = 2 \\ 1^3 &= 1 +_n 1 +_n 1 = 3 \\ &\vdots \\ 1^{n-1} &= 1 +_n 1 +_n \ldots +_n 1 = n\text{-}1 \\ 1^n &= 1 +_n 1 +_n \ldots +_n 1 = 0 \qquad (n\text{-}n) \\ 1^{n+1} &= 1^1 +_n 1^n = 1 +_n 0 = 1 \\ &\vdots \end{aligned}$$

Man kan visa att $\langle \mathbf{Z}_n, +_n \rangle$ och $\langle \mathbf{Z}, + \rangle$ är "de enda" cykliska grupperna.

Sats 14. *Om gruppen G är cyklisk, så är den även Abelsk.*

Bevis: Antag att G är cyklisk med $G = \{a^k : k \in Z\}$ för något $a \in G$. Tag $b, c \in G$. Då finns det heltal m och n sådana att $a^m = b$ och $a^n = c$. Vidare gäller det att

$$b\,c = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = c\,b,$$

och därmed är G en Abelsk grupp. □

Sats 14 kan inte omvändas, dvs. en Abelsk grupp behöver inte vara cyklisk, vilket följande exempel demonstrerar.

Exempel. Kleins fyragrupp (K4)

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Vi vet att $a^{-1} = a, b^{-1} = b, c^{-1} = c$. Gruppen är Abelsk, symmetrisk m.a.p. diagonalen.

$$\begin{aligned} &e^k = e, \quad \forall k \in \mathbf{Z} \\ &a^k \in \{e, a\}, \quad \forall k \in \mathbf{Z} \qquad (a^{-k} = (a^{-1})^k = a^k) \\ &b^k \in \{e, b\}, \quad \forall k \in \mathbf{Z} \qquad (b^{-k} = (b^{-1})^k = b^k) \\ &c^k \in \{e, c\}, \quad \forall k \in \mathbf{Z} \qquad (c^{-k} = (c^{-1})^k = c^k) \end{aligned}$$

$\nexists$ element $d \in G : G = \{d^k : k \in \mathbf{Z}\}$. G är därför ej cyklisk. (Abelsk $\not\Rightarrow$ cyklisk)

Permutationsgrupper

Definition. *Låt M vara en icke-tom mängd. En bijektiv avbildning $f : M \to M$ kallas en permutation av M. Gruppen av permutationer av M, betecknad* $\mathrm{Sym}(M)$, *definieras av*

$$\mathrm{Sym}(M) = \langle \{f : M \to M, \ \textit{sådana att } f \textit{ är en permutation av } M\}, \circ \rangle ,$$

där operationen $\circ$ betecknar funktionssammansättning.

Påstående: $\mathrm{Sym}(M)$ är en grupp.

Bevis: Om f, g är permutationer så är de bijektiva avbildningar från M till M. Då är även $f \circ g$ en bijektiv avbildning från M till M (Algebra A), vilket ger att $f \circ g$ är en permutation. Därmed är $\mathrm{Sym}(M)$ sluten under operationen $\circ$.

(i) För varje $x \in M$ gäller att

$$(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = ((f \circ g) \circ h)(x) .$$

Då är $f \circ (g \circ h) = (f \circ g) \circ h$ och $\circ$ är associativ.

(ii) Definiera avbildningen $id : M \to M$ genom $id(x) = x$ för alla $x \in M$. Då är id det neutrala elementet, ty för alla $x \in M$ är

$$f(x) = (f \circ id)(x) = (id \circ f)(x),$$

så $f \circ id = id \circ f = f$ för alla $f \in \mathrm{Sym}(M)$.

(iii) Om f är en permutation så är f en bijektiv avbildning från M till M. Då är även f^{-1} en bijektiv avbildning från M till M och därmed en permutation. Vidare gäller för alla $x \in M$ att $(f \circ f^{-1})(x) = (f^{-1} \circ f)(x) = x = id(x)$, så $f \circ f^{-1} = f^{-1} \circ f = id$.

Därmed är $\mathrm{Sym}(M)$ en grupp. □

Definition. *För* $M = \{1, 2, ..., n\}$, $n \geq 1$, *definierar vi*

$$S_n = \mathrm{Sym}(M) = \mathrm{Sym}(\{1, 2, ..., n\}) .$$

S_n kallas symmetriska gruppen av grad n.

Observera att elementen i S_n är permutationer, inte talen $1, 2, ..., n$. En permutation $f \in S_n$ kan representeras som

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix} ,$$

varvid det neutrala elementet e och inversen f^{-1} representeras som

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \text{ och } f^{-1} = \begin{pmatrix} f(1) & f(2) & \cdots & f(n) \\ 1 & 2 & \cdots & n \end{pmatrix} .$$

Exempel. Om $n \geq 3$ så är S_n **inte en Abelsk grupp.**

För $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$ och $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ i S_4 gäller

$$f \circ g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

Alltså är $f \circ g \neq g \circ f$ och S_4 är ej Abelsk.

För S_n, $n \geq 3$, definieras:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 1 & 3 & 2 & 4 & \ldots & n \end{pmatrix}, \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & \ldots & n \\ 2 & 1 & 3 & 4 & \ldots & n \end{pmatrix}$$

$(f \circ g)(1) = 3 \neq 2 = (g \circ f)(1)$

Detta ger nu att S_n inte är Abelsk då $n \geq 3$.

Med stöd av föregående exempel och Sats 14 erhåller vi att om $n \geq 3$ så är S_n **inte en cyklisk grupp.**

Antalet permutationer av $\{1, 2, ..., n\}$ är $n!$, dvs. $|S_n| = n!$ ($|S_1| = 1, |S_2| = 2, |S_3| = 6, |S_4| = 24, ...$).

Definition. *Om en permutation $g \in S_n$ permuterar de r olika elementen $k_1, k_2, ..., k_r$ cykliskt, vilket betyder att*

$$g(k_1) = k_2, g(k_2) = k_3, ..., g(k_{r-1}) = k_r, g(k_r) = k_1$$

och om de övriga elementen i $\{1, 2, ..., n\}$ *lämnas fixa, så kallas* g *en cykel och betecknas*

$$g = (k_1\ k_2\ ...\ k_r)\,.$$

Exempel. Låt $f \in S_5$ vara given av

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

Vi ser att $1 \to 4 \to 3 \to 1$ och $2 \to 5 \to 2$, dvs. (1 4 3) och (2 5) är cykler. Varje cykel ger en permutation:

$$(1\ 4\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix}, \qquad (2\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}.$$

Låt oss se hur f kan rekonstrueras från sina cykler (1 4 3) och (2 5). Vi inför först begreppet disjunkta cykler.

Definition. *Två cykler i* S_n *kallas disjunkta om de inte innehåller något gemensamt element.*

Exempelvis är (123) och (45) disjunkta, men inte (123) och (35).

Lemma 15. *Om* f *och* g *är disjunkta cykler i* S_n*, så gäller* $f \circ g = g \circ f$*.*

Bevis: Tag godtyckligt $k \in \{1, 2, ..., n\}$. Ett av tre fall kan inträffa:
Fall 1: Antag att $f(k) = i \neq k$. Då är $g(k) = k$ och $g(i) = i$, varför

$$(g \circ f)(k) = g(f(k)) = f(k) = f(g(k)) = (f \circ g)(k)\,.$$

Fall 2: Antag att $g(k) = j \neq k$. Analogt med Fall 1.
Fall 3: Antag att $f(k) = k$ och $g(k) = k$. Då är

$$(g \circ f)(k) = g(f(k)) = g(k) = k = f(k) = f(g(k)) = (f \circ g)(k)\,.$$

Därmed är $f \circ g = g \circ f$ för disjunkta cykler i S_n. □

Låt oss nu fortsätta med vårt tidigare exempel. Emedan cyklerna är disjunkta är ordningsföljden irrelevant och vi får

$$(143) \circ (25) = (25) \circ (143) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix} = f\,.$$

Exempel. Rekonstruera $f \in S_6$ från dessa cykler

$$(1\ 6\ 5) \qquad (2\ 3) \qquad (4)$$

Cyklerna är **disjunkta** och ger följande permutationer:

$$(1\ 6\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 3 & 4 & 1 & 5 \end{pmatrix}, \quad (2\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 5 & 6 \end{pmatrix}, \quad (4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

Vi får (ordningsföljden är irrelevant):

$$\begin{aligned}(1\ 6\ 5) \circ (2\ 3) \circ (4) &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 3 & 4 & 1 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 5 & 6 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 2 & 4 & 1 & 5 \end{pmatrix} = f.\end{aligned}$$

Emedan $(4) = e$, skriver vi $f = (1\ 6\ 5) \circ (2\ 3)$ och oftast endast $f = (1\ 6\ 5)(2\ 3)$.

Sats. *Varje $f \in S_n$ är antingen en cykel eller produkten av disjunkta cykler i S_n.*

Observera att en permutation som är en cykel kan framställas med flera olika cykelbeteckningar, exempelvis för $f = (1423)$ i S_4 gäller det att

$$f = (4231) = (2314) = (3142) = (1423)\,.$$

Neutrala elementet i S_n kan skrivas som

$$e = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix} = (1)(2)...(n) = (1) = (2) = ... = (n)\,.$$

Vi avslutar detta avsnitt med ett antal exempel.

Exempel. Bestäm inversen till $(1\ 4\ 3\ 6)$ i S_6.

$$(1\ 4\ 3\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 6 & 3 & 5 & 1 \end{pmatrix}, \text{ varför } \quad (1\ 4\ 3\ 6)^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 2 & 4 & 1 & 5 & 3 \end{pmatrix} = (6\ 3\ 4\ 1)$$

Exempel. Bestäm inversen till $(1\ 3\ 7)(2\ 5)$ i S_7

Det gäller att $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$ (Algebra A). Då erhålls:

$$((1\ 3\ 7) \circ (2\ 5))^{-1} = (2\ 5)^{-1} \circ (1\ 3\ 7)^{-1} = (5\ 2) \circ (7\ 3\ 1) = (7\ 3\ 1) \circ (5\ 2).$$

eftersom disjunkta cykler kommuterar.

Exempel. Betrakta icke-disjunkta cykler i S_5:

$$(1\ 2\ 4)(2\ 3\ 5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 1 & 4 \end{pmatrix} = (1\ 2\ 3\ 5\ 4), \text{ en cykel.}$$

$$(2\ 3\ 5)(1\ 2\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix} = (1\ 3\ 5\ 2\ 4), \text{ en cykel.}$$

$(1\ 2\ 3\ 5\ 4) \neq (1\ 3\ 5\ 2\ 4)$, icke-disjunkta cykler behöver ej kommutera, dvs. ordningsföljden är viktig.

Exempel. Antag att vi har 13 spaderkort och Jokern med bildsidan nedåt i ordningen $A, 2, \ldots, 10, Kn, D, K, J$. Antag att vi utför perfekta omblandningar, dvs. delar korthögen i två delar med sju kort var och blandar korten turvis om varandra så att A alltid är underst och J alltid överst i packen. Hur många omblandningar krävs för att återställa den ursprungliga ordningen?

Lösning: Betrakta S_{14}

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 1 & 3 & 5 & 7 & 9 & 11 & 13 & 2 & 4 & 6 & 8 & 10 & 12 & 14 \end{pmatrix} = (1)(14)(2\ 3\ 5\ 9\ 4\ 7\ 13\ 12\ 10\ 6\ 11\ 8),$$

där 1 motsvarar A, 11 motsvarar Kn, 12 motsvarar D, 13 motsvarar K och 14 motsvarar J. Vi söker nu det minsta $k \geq 1$ sådant att $f^k = e$ (ett sådant existerar enligt Lemma 19).

$$f^k(1) = 1 \text{ och } f^k(14) = 14 \quad \forall\, k \geq 1$$

$$f^{12}(j) = j \text{ för } j = 2, \ldots, 13.$$

Svar: Tolv perfekta omblandningar.

Isomorfa grupper

När är två grupper väsentligen lika? Denna fråga kan besvaras med hjälp av begreppet isomorfi för grupper. Först skall vi dock införa begreppet homomorfi för algebraiska strukturer:

Definition. *Antag att $\langle G, * \rangle$ och $\langle H, \diamond \rangle$ är algebraiska strukturer och att $f : G \to H$. Då kallas f en homomorfi om det för alla $a, b \in G$ gäller att*

$$f(a * b) = f(a) \diamond f(b)\,.$$

Homomorfivillkoret betyder att varje likhet $z = x * y$ i G medför likheten $f(z) = f(x) \diamond f(y)$ i H.

Exempelvis är avbildningen $f : Z \setminus \{0\} \to Z_+$ given av $f(x) = x^2$ en homomorfi mellan de algebraiska strukturerna $\langle Z \setminus \{0\}, \cdot \rangle$ och $\langle Z_+, \cdot \rangle$, ty $f(x\,y) = (x\,y)^2 = x^2 y^2 = f(x)\,f(y)$.

Definition. *Två grupper $\langle G, * \rangle$ och $\langle H, \diamond \rangle$ är isomorfa, vilket betecknas $\langle G, * \rangle \cong \langle H, \diamond \rangle$, om det finns en bijektion $\varphi : G \to H$ sådan att för alla $a, b \in G$ gäller att*

$$\varphi(a * b) = \varphi(a) \diamond \varphi(b)\,.$$

Då säger vi att φ är en isomorfism.

Exempel. Låt oss jämföra $\mathbf{Z}_2$ och S_2.

$$\underline{S_2}: \qquad e = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \qquad f = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

$\circ$	e	f
e	e	f
f	f	e

$$\underline{\mathbf{Z}_2}: \qquad \langle \{0,1\}, +_2 \rangle$$

$+_2$	0	1
0	0	1
1	1	0

Definierar nu: $\varphi : \mathbf{Z}_2 \mapsto S_2$ genom $\begin{cases} \varphi(0) = e \\ \varphi(1) = f \end{cases}$.

φ är alltså en bijektiv avbildning.

$$\begin{cases} \varphi(0 +_2 0) = \varphi(0) = e = e \circ e = \varphi(0) \circ \varphi(0) \\ \varphi(0 +_2 1) = \varphi(1) = f = e \circ f = \varphi(0) \circ \varphi(1) \\ \varphi(1 +_2 0) = \varphi(1) = f = f \circ e = \varphi(1) \circ \varphi(0) \\ \varphi(1 +_2 1) = \varphi(0) = e = f \circ f = \varphi(1) \circ \varphi(1) \end{cases}$$

φ är en isomorfism och $\mathbf{Z}_2 \cong S_2$.

Det gäller att $|S_3| = |Z_6| = 6$. Är grupperna isomorfa? Vi har tidigare noterat att Z_6 är Abelsk men inte S_3. Med stöd av följande lemma kan vi ge ett nekande svar på frågan.

Lemma 16. *Om gruppen $\langle G, * \rangle$ är Abelsk och $\langle G, * \rangle \cong \langle H, \diamond \rangle$, så är även $\langle H, \diamond \rangle$ en Abelsk grupp.*

Bevis: Låt $\varphi : G \to H$ vara en isomorfism. Tag godtyckliga $x, y \in H$. Då finns det element $a, b \in G$ sådana att $\varphi(a) = x$ och $\varphi(b) = y$. Vidare gäller det att

$$x \diamond y = \varphi(a) \diamond \varphi(b) = \varphi(a * b) = \varphi(b * a) = \varphi(b) \diamond \varphi(a) = y \diamond x\,,$$

så $\langle H, \diamond \rangle$ är en Abelsk grupp. $\square$

Produkter av grupper

Det är ofta fördelaktigt att framställa en komplicerad grupp G som en direkt produkt av enklare grupper $H_1, ..., H_n$, eller visa att G är isomorf med en dylik produkt, $G \cong H_1 \times H_2 \times ... \times H_n$. Bekant från analysen är den naturliga produkten $\langle R^n, + \rangle$ av ordnade n-tipler försedda med addition

$$(a_1, ..., a_n) + (b_1, ..., b_n) = (a_1 + b_1, ..., a_n + b_n)\,.$$

Definition. *Antag att vi har grupperna $\langle G, * \rangle$ och $\langle H, \diamond \rangle$. Då definieras den direkta produkten $G \times H$ av G och H som mängden av ordnade elementpar (a, b), där $a \in G$ och $b \in H$, försedd med operationen*

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 * a_2, b_1 \diamond b_2) \in G \times H\,.$$

Anmärkning. a) Analog definition för n stycken grupper.

b) Om G och H är av ändlig ordning gäller $|G \times H| = |G|\,|H|$.

Påstående: $G \times H$ är en grupp.

Bevis: Antag att $(a_1, b_1), (a_2, b_2) \in G \times H$. Då erhålls att

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 * a_2, b_1 \diamond b_2) \in G \times H\,.$$

så $\cdot$ är en operation på $G \times H$.

(i) Nu gäller kalkylerna

$$\begin{aligned}(a_1, b_1) \cdot ((a_2, b_2) \cdot (a_3, b_3)) &= (a_1, b_1) \cdot (a_2 * a_3, b_2 \diamond b_3) = (a_1 * (a_2 * a_3), b_1 \diamond (b_2 \diamond b_3)) \\ &= ((a_1 * a_2) * a_3, (b_1 \diamond b_2) \diamond b_3) = (a_1 * a_2, b_1 \diamond b_2) \cdot (a_3, b_3) \\ &= ((a_1, b_1) \cdot (a_2, b_2)) \cdot (a_3, b_3)\,,\end{aligned}$$

så operationen $\cdot$ är associativ.

(ii) Låt e och e' vara neutrala element i G respektive H. För $(a, b) \in G \times H$ gäller

$$\begin{aligned}(e, e') \cdot (a, b) &= (e * a, e' \diamond b) = (a, b), \\ (a, b) \cdot (e, e') &= (a * e, b \diamond e') = (a, b),\end{aligned}$$

och därmed är (e, e') det neutrala elementet i $G \times H$.

(iii) Tag nu $(a, b) \in G \times H$ och betrakta likheterna

$$\begin{aligned}(a^{-1}, b^{-1}) \cdot (a, b) &= (a^{-1} * a, b^{-1} \diamond b) = (e, e'), \\ (a, b) \cdot (a^{-1}, b^{-1}) &= (a * a^{-1}, b \diamond b^{-1}) = (e, e'),\end{aligned}$$

som ger att $(a, b)^{-1} = (a^{-1}, b^{-1})$.

Då har vi visat att $G \times H$ är en grupp. $\square$

Exempel. $Z_6 \cong Z_2 \times Z_3$. (Hemuppgift).

I allmänhet gäller det **inte** att $Z_{m\,n} \cong Z_m \times Z_n$.

Exempel. Betrakta $Z_2 \times Z_2$ och Kleins fyragrupp.

$K4$:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$Z_2 \times Z_2$:

$\bullet$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Definierar nu $\varphi : \{e, a, b, c\} \mapsto \{(0,0), (0,1), (1,0), (1,1)\}$ genom:

$$\varphi(e) = (0,0),\ \varphi(a) = (0,1),\ \varphi(b) = (1,0),\ \varphi(c) = (1,1)$$

Denna definition ger att φ är en bijektion. Då är φ en isomorfi, eftersom $d_1, d_2 \in K_4 \Rightarrow \varphi(d_1 \circ d_2) = \varphi(d_1) \bullet \varphi(d_2)$. Ett exempel på detta är $\varphi(a \circ b) = \varphi(c) = (1,1) = (0,1) \bullet (1,0) = \varphi(a) \bullet \varphi(b)$. Vi vet nu att $K4 \cong Z_2 \times Z_2$ och då $K4$ ej är cyklisk så är inte $Z_2 \times Z_2$ det heller (Hemuppgift). Vi vet dock att Z_4 är cyklisk och kan därmed konstatera att $Z_2 \times Z_2 \ncong Z_4$.

Undergrupper

Betrakta grupperna $\langle R, + \rangle$ och $\langle Z, + \rangle$ försedda med samma operation (addition). Då $Z \subset R$ är det naturligt att kalla $\langle Z, + \rangle$ en delgrupp av $\langle R, + \rangle$.

Definition. *Antag att vi har en grupp $\langle G, * \rangle$. Om $H \subseteq G$ och $\langle H, * \rangle$ är en grupp, så kallas $\langle H, * \rangle$ en undergrupp (delgrupp) till gruppen $\langle G, * \rangle$.*

Anmärkning. a) $\langle G, * \rangle$ och $\langle \{e\}, * \rangle$ kallas de triviala undergrupperna till $\langle G, * \rangle$.

b) Om e och e' är de neutrala elementen i $\langle G, * \rangle$ respektive $\langle H, * \rangle$, så gäller $e' * e' = e' = e' * e$, vilket enligt Sats 12 (i) medför att $e' = e$. Vi har därmed samma neutrala element i båda grupperna.

Sats 17. *Givet en grupp $\langle G, * \rangle$ och $H \subseteq G$. Då är $\langle H, * \rangle$ en undergrupp till $\langle G, * \rangle$ om och endast om både 1) och 2) gäller:*

1) $H \neq \emptyset$;

2) $\forall\ a, b \in H \Rightarrow a * b^{-1} \in H$, *där* b^{-1} *är inversen till* b *i* G.

Bevis: (Hemuppgift).

Speciellt för **ändliga** grupper gäller:

Sats 18. *Givet en ändlig grupp $\langle G, * \rangle$ och $H \subseteq G$. Då är $\langle H, * \rangle$ en undergrupp till $\langle G, * \rangle$ om $H \neq \emptyset$ och $a, b \in H \Rightarrow a * b \in H$.*

För beviset behövs ett hjälpresultat:

Lemma 19. *Låt a vara ett element i den ändliga gruppen $\langle G, * \rangle$. Då finns det ett minsta positivt heltal n med $a^n = e$. Vidare gäller det att gruppelementen $a = a^1,\ a^2,\ a^3, ...,\ a^{n-1},\ a^n = e$ är olika.*

Bevis: Klart om $a = e$. Antag att $a \neq e$ och betrakta i G elementföljden $a, a^2, a^3, \ldots$. Då G är ändlig måste följden ha element som upprepar sig. Välj en sådan upprepning:

$$a^p = a^q$$

med $p > q$. Multiplikation av båda leden med a^{-q} ger:

$$a^{p-q} = e,$$

där p-$q > 0$. Alltså $a^m = e$ för $m = p$-$q > 0$. Låt n vara det minsta positiva heltal med denna egenskap. (Ett sådant tal existerar). Nu är alla element $a, a^2, ..., a^n$ olika, ty om $a^i = a^j$ för $1 \leq j < i \leq n$ så gäller det att $a^{i-j} = e$ med $1 \leq i$-$j < n$, vilket strider mot definitionen av n. □

Bevis av Sats 18: Tag $a \in H$. Upprepad användning av antagandet $a, b \in H \Rightarrow a * b \in H$ ger att

$$a^k \in H \text{ för alla } k \geq 1\,. \qquad (*)$$

Om $H = \{e\}$, så är H en undergrupp av G. Om $H \neq \{e\}$, så väljer vi $a \in H$ sådant att $a \neq e$. Då G är en ändlig grupp ger Lemma 19 att det finns ett $k_0 > 1$ med

$$a^{k_0} = e\,.$$

Multiplicera med a^{-1} och erhåll: $a^{k_0 - 1} = a^{-1}$. Emedan k_0-$1 \geq 1$ ger nu $(*)$ att

$$a \in H \Rightarrow a^{-1} = a^{k_0 - 1} \in H\,.$$

Tag nu $a, c \in H$. Då gäller det att $a, c^{-1} \in H$ och vidare att $a * c^{-1} \in H$, (med stöd av antagandet $a, b \in H \Rightarrow a * b \in H$). Men då ger Sats 17 att $\langle H, * \rangle$ är en undergrupp till $\langle G, * \rangle$. □

Symmetri

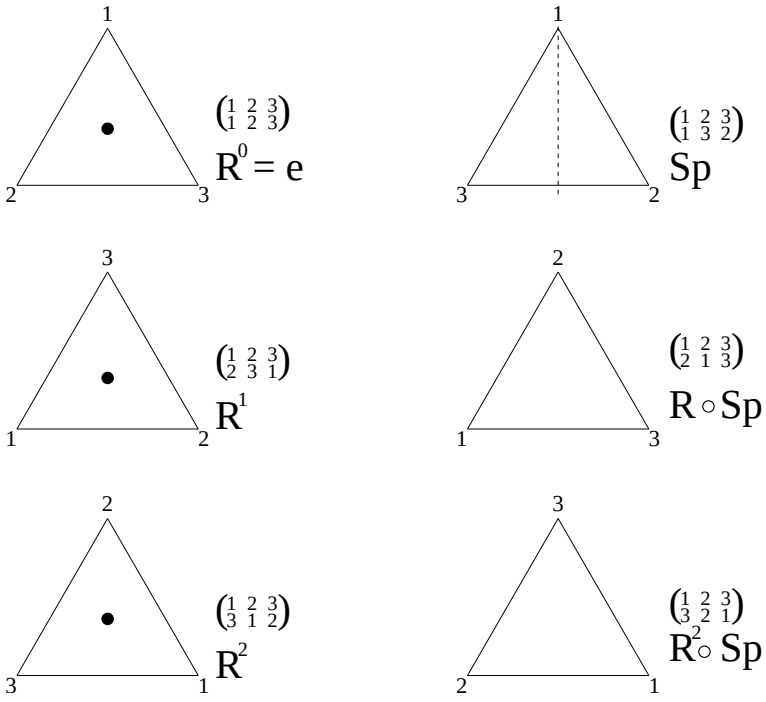
Allmänt uttryckt är **symmetrin av ett objekt** en omordning av objektet så att alla dess väsentliga grunddrag bevaras. Hos månghörningar betyder detta att hörn omplaceras till hörn och sidor till sidor.

Symmetrin hos regelbundna månghörningar och polyedrar kan med fördel studeras med hjälp av permutationsgrupper.

Låt oss betrakta en regelbunden n-hörning M för vilken vi numrerar hörnen moturs med talen $1, 2, ..., n$ och antar att $n \geq 3$. Symmetrierna hos M ges då av rotationer moturs samt speglingar i symmetriaxlar.

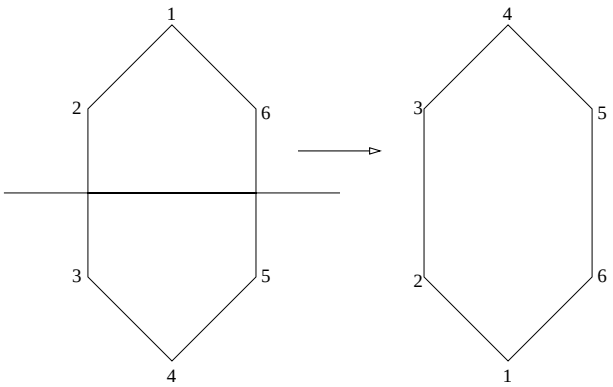
Exempel. Fallet $n = 3$:

Symmetrierna hos M ges av rotationer $\frac{360^\circ}{n}$ moturs ($\equiv R$), samt speglingar i diagonalen genom hörnet 1 ($\equiv Sp$) efterföljt av rotationer.



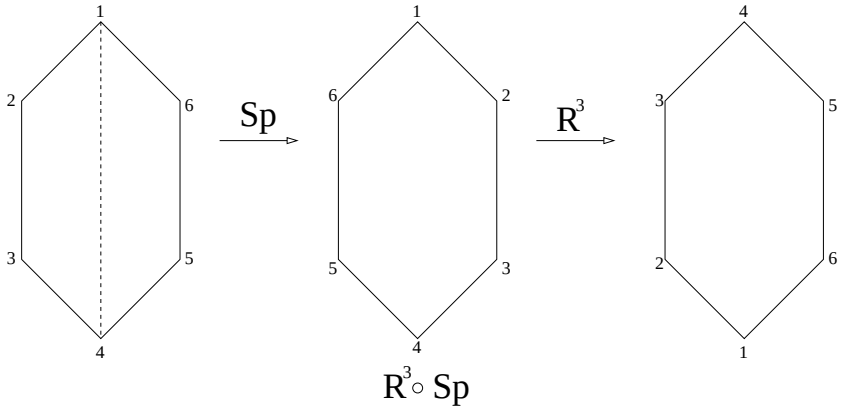
Figur 2.

Obs! För jämnt n även spegling i diagonalen genom mittpunkter på motsatta sidor:



Figur 3.

Erhålls med Sp och R som:



Figur 4.

Definiera nu permutationerna $R, Sp \in S_n$ genom

$$R = \begin{pmatrix} 1 & 2 & 3 & \cdots & n\text{-}1 & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix},$$
$$Sp = \begin{pmatrix} 1 & 2 & 3 & \cdots & n\text{-}1 & n \\ 1 & n & n\text{-}1 & \cdots & 3 & 2 \end{pmatrix}.$$

Då gäller

$$R^k \circ Sp = Sp \circ R^{-k}, \qquad (*)$$

för $k = 0, 1, ..., n\text{-}1$. (Hemuppgift).

Alla "tänkbara placeringar av M" fås genom att upprepa R och Sp, (Sp vänder på M, R roterar på M). Definiera nu

$$H = \{R^l,\ R^k \circ Sp : l = 0, ..., n\text{-}1,\ k = 0, ..., n\text{-}1\} \subseteq S_n.$$

Påstående: $\langle H, \circ \rangle$ *är en grupp.*

Bevis: Vi betraktar fyra fall och utnyttjar formel $(*)$ ovan.

1) Betrakta $R^{l_1} \circ R^{l_2}$. Om $l_1 + l_2 \leq n$-1 gäller det att $R^{l_1} \circ R^{l_2} = R^{l_1+l_2} \in H$. Om $l_1 + l_2 \geq n$ har vi $R^{l_1} \circ R^{l_2} = R^{n+(l_1+l_2-n)} = e \circ R^{l_1+l_2-n} \in H$.

2) Betrakta $(R^k \circ Sp) \circ R^l$. Vi antar att k-$l \geq 0$ och tillämpar $(*)$: $(R^k \circ Sp) \circ R^l = (Sp \circ R^{-k}) \circ R^l = Sp \circ R^{l-k} = R^{k-l} \circ Sp \in H$. Om vi antar att k-$l < 0$ erhålls $(R^k \circ Sp) \circ R^l = (Sp \circ R^{-k}) \circ R^l = Sp \circ R^{n+(l-k-n)} = Sp \circ e \circ R^{l-k-n} = R^{n+k-l} \circ Sp \in H$.

3) $R^l \circ (R^k \circ Sp) = (R^l \circ R^k) \circ Sp = R^{l+_n k} \circ Sp \in H$.

4) $(R^{k_1} \circ Sp) \circ (R^{k_2} \circ Sp) = R^{k_1} \circ Sp \circ (Sp \circ R^{-k_2}) = R^{k_1} \circ R^{-k_2}$. Om k_1-$k_2 \geq 0$ så är det sista ledet lika med $R^{k_1-k_2} \in H$. Om k_1-$k_2 < 0$ så får vi efter sammansättning med $e = R^n$ att det sista ledet är lika med $R^{n+(k_1-k_2)} \in H$.

Vi har alltså visat att $a, b \in H \Rightarrow a \circ b \in H$ och då ger Sats 18 att H är en undergrupp till S_n. □

Alla symmetrier av M bildar då gruppen $D_n = \langle H, \circ \rangle$ som kallas **diedergruppen**. Denna grupp av permutationer är en **undergrupp till** S_n.

Ordningen för diedergruppen är $|D_n| = 2n$, ty vi har $2n$ olika permutationer, n rotationer R^k och n stycken sammansättningar av speglingen Sp med rotationen R^k, dvs $R^k \circ Sp$.

Vi observerar att D_n är en **äkta** (icke-trivial) undergrupp av S_n då $n \geq 4$, ty då är $2n = |D_n| < |S_n| = n!$. Vidare noterar vi att D_n "byggs upp" av R och Sp, dvs. D_n genereras av $\{R, Sp\}$.

Generering av grupper

Låt $\langle G, * \rangle$ vara en grupp och tag en icke-tom delmängd M av G. Tag snittet av alla undergrupper H till G som innehåller M. Beteckna detta snitt med $\langle M \rangle$, alltså

$$\langle M \rangle = \bigcap_{\substack{M \subseteq H \\ H \text{ delgr.}}} H \, .$$

Påstående. *$\langle \langle M \rangle, * \rangle$ är en undergrupp till G.*

Bevis: Vi har att $e \in \langle M \rangle \neq \emptyset$, ty $e \in H$ för varje undergrupp H av G.

Tag $a, b \in \langle M \rangle$. Detta medför att $a, b \in H$ för alla undergrupper H sådana att $M \subseteq H$. Då gäller det att $a, b^{-1} \in H$ för alla undergrupper H sådana att $M \subseteq H$. Av detta följer att $a * b^{-1}$ tillhör alla undergrupper H sådana att $M \subseteq H$. Därmed gäller det att $a * b^{-1} \in \langle M \rangle$. Då ger Sats 17 att $\langle \langle M \rangle, * \rangle$ är en undergrupp till G. □

Anmärkning. $\langle M \rangle$ är den minsta undergruppen till G som innehåller M.

Definition. *Givet en grupp $\langle G, * \rangle$ och en icke-tom delmängd M av G. Då kallas $\langle M \rangle$ undergruppen till G genererad av M* och *M kallas generator för undergruppen $\langle M \rangle$.*

Sats 20. *Elementen i $\langle M\rangle$ är de element i G som kan skrivas som $a_1a_2...a_k$, där $a_i \in M$ eller $a_i^{-1} \in M$, för $k = 1, 2, ...$*

Bevis: Definiera

$$H = \{a_1a_2...a_k : a_i \in M \text{ eller } a_i^{-1} \in M,\ k = 1, 2, ...\}.$$

Klart att $M \subseteq H$ och att $H \neq \emptyset$. Tag $a = a_1 \cdot a_2 \cdot ... \cdot a_k \in H$ och $b = b_1 \cdot b_2 \cdot ... \cdot b_l \in H$. Då är $a^{-1} = a_k^{-1} \cdot a_{k-1}^{-1} \cdot ... \cdot a_2^{-1} \cdot a_1^{-1} \in H$. Därmed gäller det att $b\,a^{-1} = b_1 \cdot b_2 \cdot ... \cdot b_l \cdot a_k^{-1} \cdot a_{k-1}^{-1} \cdot ... \cdot a_1^{-1} \in H$. Sats 17 ger då att H är en undergrupp till G. Vidare gäller att $\langle M\rangle \subseteq H \subseteq G$. Definitionen på H ger att $H \subseteq \langle M\rangle$, ty $a_1 \cdot a_2 \cdot ... \cdot a_k$ tillhör varje undergrupp som M är delmängd av, och därmed även snittet $\langle M\rangle$. Alltså gäller det att $H = \langle M\rangle$. □

Exempel. $Z \times Z = \langle\{(1,0),(0,1)\}\rangle$ då operationen är addition.

Det är klart att $\langle\{(1,0),(0,1)\}\rangle \subseteq Z \times Z$. Om $(a,b) \in Z \times Z$ så gäller:

$$(a,b) = (a,0) + (0,b) = (1,0)^a + (0,1)^b \overset{\text{Sats20}}{\in} \langle\{(1,0),(0,1)\}\rangle$$

vilket innebär att $Z \times Z \subseteq \langle\{(1,0),(0,1)\}\rangle$. Vi kan då konstatera att $Z \times Z = \langle\{(1,0),(0,1)\}\rangle$.

$\underline{a > 0:}$ $\quad (1,0)^a = \overbrace{(1,0) + \ldots + (1,0)}^{\text{a st.}}$

$\underline{a = 0:}$ $\quad (1,0)^0 = e = (0,0)$

$\underline{a < 0:}$ $\quad (1,0)^a = ((1,0)^{-1})^{|a|} = \overbrace{(\text{-}1,0) + \ldots + (\text{-}1,0)}^{\text{|a| st.}}$

Detta gäller analogt för $(0,1)^b$.

Anmärkning. Om G är en cyklisk grupp så finns det ett element $a \in G$ sådant att $G = \{a^k : k \in Z\}$. Med andra ord gäller $G = \langle a\rangle$, dvs. den undergrupp som genereras av a är hela G, a är därmed generator för G.

Definition. *Om $G = \langle M\rangle$ och M är en ändlig mängd, dvs. $M = \{a_1, ..., a_n\}$, så kallas G en ändligt genererad grupp, $G = \langle\{a_1, ..., a_n\}\rangle$.*

En cyklisk grupp är då ändligt genererad (av ett element), men en ändligt genererad grupp behöver inte vara cyklisk, jämför $Z \times Z$ i ovanstående exempel.

Exempel. Några ändligt genererade grupper.

a) $\mathbf{Z} = \langle\mathbf{Z}, +\rangle = \langle 1\rangle = \langle\text{-}1\rangle$, men $\mathbf{Z} \neq \langle 2\rangle$. $\quad(\langle 2\rangle = \{2z : z \in \mathbf{Z}\},\ \langle 0\rangle = \{0\} = \{e\})$

b) $\mathbf{Z}_5 = \langle\mathbf{Z}_5, +_5\rangle = \langle 1\rangle = \langle 2\rangle = \langle 3\rangle = \langle 4\rangle$. $\quad(\langle 0\rangle = \{0\})$

c) $\mathbf{Z}_6 = \langle \mathbf{Z}_6, +_6 \rangle = \langle 1 \rangle = \langle 5 \rangle$. $(\langle 3 \rangle = \{0,3\}, \langle 2 \rangle = \{0,2,4\}, \langle 0 \rangle = \{e\})$

d) Kleins fyragrupp K4:

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Gruppen är ej cyklisk, men den är ändligt genererad av $\langle \{a,b\} \rangle = \{e,a,b,c\} = \langle \{a,c\} \rangle = \langle \{b,c\} \rangle$. $(\langle a \rangle = \{e,a\}, \langle b \rangle = \{e,b\}, \langle c \rangle = \{e,c\})$

e) $S_3 = \langle \{a,b\} \rangle$, där $\begin{cases} a = (1\ 2\ 3) & (= R) \\ b = (2\ 3) & (= Sp) \end{cases}$, ty

$$\left.\begin{aligned} a^2 &= (1\ 2\ 3)(1\ 2\ 3) = (1\ 3\ 2) \\ a^3 &= (1\ 2\ 3)(1\ 3\ 2) = (1) = e \\ ab &= (1\ 2\ 3)(2\ 3) = (1\ 2) \\ a^2b &= (1\ 2\ 3)(1\ 2) = (1\ 3) \\ a &= (1\ 2\ 3) \\ b &= (2\ 3) \end{aligned}\right\} = S_3$$

Sats 21. *Låt $\langle G, * \rangle$ vara en ändlig grupp och antag att $e \neq a \in G$. Vi definierar ordningen för elementet a som det minsta positiva heltal n för vilket det gäller att $a^n = e$. Då är $n = |\langle a \rangle|$.*

Bevis: (Klart att satsen gäller även för $a = e$, $n = 1$ och $\langle a \rangle = \{e\}$). Lemma 19 ger att det finns ett n med $a^n = e$, $a^k \neq e$, $k = 1, ..., n$-1, och elementen $a^1, ..., a^n = e$ är alla olika. Alltså $\{a, a^2, ..., a^n = e\} = \langle a \rangle$, (Sats 20), och $|\langle a \rangle| = n$. □

Sidoklasser och Lagranges sats

I exempelvis $\langle Z_6, +_6 \rangle$ gäller det att $|\langle 2 \rangle| = 3$ och $|\langle 3 \rangle| = 2$. Båda dessa tal är faktorer i $|Z_6| = 6$. Detta är ingen tillfällighet, vilket inses såsnart vi har bevisat Lagranges sats!

Definition. *Antag att G är en grupp och att H är en undergrupp till G. Då definieras för varje $a \in G$ (vänster)sidoklassen aH och (höger)sidoklassen Ha genom*

$$aH = \{a\,h : h \in H\} \text{ och } Ha = \{h\,a : h \in H\}\,.$$

Påstående:

(*i*) $G = \bigcup_{a \in G} aH$;

(*ii*) *Sidoklasserna är disjunkta, $aH \cap bH \neq \emptyset \Rightarrow aH = bH$.*

Bevis: (i) Klart att

$$\bigcup_{a\in G} aH \subseteq G\,.$$

Tag godtyckligt $a \in G$. För $e \in H$ gäller $a = a\,e$, vilket medför att $a \in aH$. Alltså har vi att

$$G \subseteq \bigcup_{a\in G} aH$$

och därmed gäller påståendet (i).

(ii) Om $aH \cap bH \neq \emptyset$, så finns det $h_1, h_2 \in H$ sådana att $a\,h_1 = b\,h_2$. Då är $a = b\,h_2\,h_1^{-1}$ och för varje $h \in H$ är $a\,h = b\,h_2\,h_1^{-1}\,h \in bH$, så $aH \subseteq bH$. Vidare är $b = a\,h_1\,h_2^{-1}$, så för varje $h \in H$ gäller att $b\,h = a\,h_1\,h_2^{-1}\,h \in aH$, vilket ger att $bH \subseteq aH$. Alltså $aH = bH$ om $aH \cap bH \neq \emptyset$. □

Med stöd av (i) och (ii) är då mängden av sidoklasser $\{aH : a \in G\}$ en **partition** av G. Denna partition betecknas G/H,

$$G/H = \{aH : a \in G\}\,.$$

Sats 22. *Om H är en undergrupp till G, så är G/H en partition av G med $|H| = |aH|$ för alla $a \in G$.*

Bevis: Tag godtyckligt $a \in G$. Definiera $\varphi : H \to aH$ genom $\varphi(h) = a\,h$ för alla $h \in H$.

(i) Funktionen φ är **surjektiv**, ty för godtyckligt $a\,h \in aH$ gäller att $\varphi(h) = a\,h$.

(ii) Funktionen φ är **injektiv**, ty $\varphi(h_1) = \varphi(h_2) \Rightarrow a\,h_1 = a\,h_2 \Rightarrow h_1 = h_2$.

Därmed är φ en bijektion och $|H| = |aH|$. □

Partitionen G/H av G i delmängder som alla har lika många element ger att

$$|G| = |H|\,|G/H|\,.$$

$|G/H|$ brukar kallas **index** för undergruppen H i G. Nu kan vi formulera Lagranges viktiga sats. (Joseph-Louis Lagrange (1736-1813)).

Sats 23. (Lagrange). *Om H är en undergrupp till en ändlig grupp G, så är $|G|$ delbar med $|H|$.*

Satserna 23 och 21 ger att ordningen för ett element i en ändlig grupp G alltid delar $|G|$:

Sats 24. *För varje $a \in G$ i en ändlig grupp G är $|G|$ delbar med ordningen för a. Speciellt gäller $a^{|G|} = e$.*

Bevis: Sats 23 ger att $|\langle a\rangle|$ delar $|G|$. Ordningen för a ges av $n = |\langle a\rangle|$, (Sats 21). Då finns det ett heltal $m > 0$ sådant att $|G| = m \cdot n$, vilket medför att $a^{|G|} = a^{m\,n} = (a^n)^m = e^m = e\,.$ □

Varje grupp av primtalsordning är cyklisk:

Sats 25. *Antag att G är en ändlig grupp och att $|G|$ är ett primtal. Då är G cyklisk med $G = \langle a \rangle$ för alla $a \in G$ med $a \neq e$, och vidare gäller:*

$$G = \{a, a^2, ..., a^{|G|-1}, e\}\,.$$

Bevis: Antag att $|G| = p$, där p är ett primtal. Låt $a \in G$ och antag att $a \neq e$. Då är $a^1 \neq e$, så $|\langle a \rangle| > 1$. Sats 24 ger att $a : s$ ordning $n = |\langle a \rangle|$ delar $|G|$. Därmed gäller det att $|\langle a \rangle| = |G| = p$. Lemma 19 ger att elementen $a^1, a^2, ..., a^p = e$ är alla olika. Då gäller det att

$$G = \{a, a^2, ..., a^{|G|-1}, a^{|G|} = e\},$$

så G är cyklisk med $G = \langle a \rangle$. □

Det finns väsentligen en grupp av primtalsordning:

Sats 26. *Om gruppen G är av primtalsordning p, så är är $G \cong Z_p$.*

Bevis: Antag att $|G| = p$, där p är ett primtal. Tag $a \in G$ sådant att $a \neq e$. Definiera $\varphi : Z_p \to G$ genom

$$\varphi(k) = a^k, \quad \text{för } k \in \{0, 1, ..., p\text{-}1\}\,.$$

Då är φ en bijektion, ty $G = \langle a \rangle$ (Sats 25) och $a, a^2, ..., a^p = e$ är alla olika (Lemma 19). Vidare gäller

$$\varphi(k_1 +_p k_2) = a^{k_1 +_p k_2} = a^{k_1}\, a^{k_2},$$

ty om $k_1 + k_2 \leq p$-1, så gäller det att $a^{k_1 +_p k_2} = a^{k_1 + k_2} = a^{k_1}\, a^{k_2}$. Om $k_1 + k_2 \geq p$, så gäller det att $a^{k_1 +_p k_2} = a^{k_1 + k_2 - p} = a^{k_1}\, a^{k_2}\, a^{-p} = a^{k_1}\, a^{k_2}\, (a^p)^{-1} = a^{k_1}\, a^{k_2}\, e^{-1} = a^{k_1}\, a^{k_2}$. Alltså har vi att

$$\varphi(k_1 +_p k_2) = a^{k_1}\, a^{k_2} = \varphi(k_1)\, \varphi(k_2),$$

och således gäller det att $Z_p \cong G$. □

Vi avslutar detta avsnitt med ett hjälpresultat.

Lemma 27. *Om H är en undergrupp av G så gäller det att*

$$aH = \{b \in G : aH = bH\}$$

för alla $a \in G$.

Bevis: Visar att $b \in aH \Leftrightarrow aH = bH$.

(i) ($\Rightarrow$). Antag att $b \in aH$. Då $b = b\,e \in bH$, gäller det att $b \in aH \cap bH$. Alltså $aH = bH$, ty $\{aH : a \in G\}$ är en partition av G.

(ii) ($\Leftarrow$). Antag att $aH = bH$. Då har vi att $b \in bH \Rightarrow b \in aH$. □

Ekvivalensklasser

Genom att dela in elementen i en mängd X i mängder bestående av "ekvivalenta" element erhåller vi en partition av X i ekvivalensklasser. För att kunna göra detta bör vi införa en generalisering av begreppet likhet, nämligen en ekvivalensrelation på X. Först definierar vi begreppet relation.

Definition. *Givet en mängd X. En relation R på X är en delmängd av $X \times X$. Om $(x, y) \in R$ så säger vi att x står i relationen R till y och betecknar detta med $x\,R\,y$.*

Exempel. Att $x \leq y$ för x, y reella är en relation på mängden av reella tal.

Definition. *En relation R på en mängd X är en ekvivalensrelation om för alla $x, y, z \in X$ gäller:*

1. $x\,R\,x$ *(den reflexiva egenskapen)*;
2. $x\,R\,y \Leftrightarrow y\,R\,x$ *(den symmetriska egenskapen)*;
3. $x\,R\,y$ *och* $y\,R\,z \Rightarrow x\,R\,z$ *(den transitiva egenskapen)*.

Exempel. Ekvivalensrelationer

a) Relationen $x \leq y$ på de reella talens mängd är reflexiv och transitiv, men inte symmetrisk, så "$\leq$" är inte en ekvivalensrelation.

b) Exempel på en ekvivalensrelation; Låt $R \subseteq \mathbf{C} \times \mathbf{C}$ definierad genom

$$z_1 R z_2 \Leftrightarrow |z_1| = |z_2|. \quad (\mathbf{C} = \{\text{komplexa tal}\})$$

1) $\forall z \in \mathbf{C} : |z| = |z| \Leftrightarrow zRz$, R är reflexiv.
2) $\forall z_1, z_2 \in \mathbf{C} : |z_1| = |z_2| \Leftrightarrow |z_2| = |z_1|$, $z_1 R z_2 \Leftrightarrow z_2 R z_1$, R är symmetrisk.
3) $\forall z_1, z_2, z_3 \in \mathbf{C} : (|z_1| = |z_2| \text{ och } |z_2| = |z_3|) \Rightarrow |z_1| = |z_3|$, $(z_1 R z_2 \text{ och } z_2 R z_3) \Rightarrow z_1 R z_3$, R är transitiv.

Punkterna 1-3 ger oss att R är en ekvivalensrelation.

Definition. *Låt R vara en ekvivalensrelation på en mängd X. För varje $x \in X$ bildar vi mängden $[x]$ bestående av alla element som är relaterade till x,*

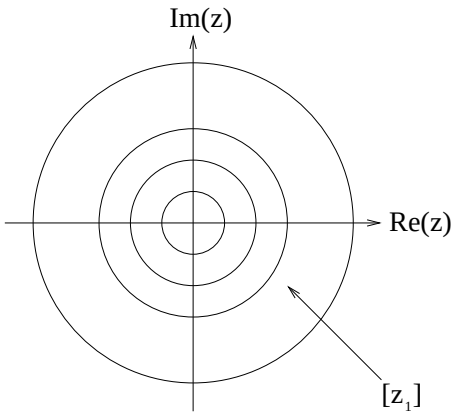
$$[x] = \{y : x\,R\,y\},$$

som kallas en ekvivalensklass med avseende på R. Alltså $y \in [x] \Leftrightarrow x\,R\,y$.

Exempel. (forts. på föregående exempel) För $z_1 R z_2 \Rightarrow |z_1| = |z_2|$ i $\mathbf{C}$ ger $z_1 = 1 + i$ ekvivalensklassen

$$[z_1] = \{z \in \mathbf{C} : |z| = |z_1| = |1 + i| = \sqrt{2}\}.$$

Därmed består $[z_1]$ av alla punkter på cirkeln $|z| = \sqrt{2}$. Ekvivalensklasserna bildar origocentrerade cirklar med radie ≥ 0. Ekvivalensklasserna bildar även en partition av $\mathbf{C}$.



Figur 5.

Påstående: *Givet en grupp G med undergruppen H. Definiera en relation R på G genom $a\,R\,b \Leftrightarrow aH = bH$. Då är R en ekvivalensrelation med ekvivalensklasserna givna av sidoklasserna, $[a] = aH$.*

Bevis: (i) För alla $a \in G$ gäller att $aH = aH$, så $a\,R\,a$.

(ii) För alla $a, b \in G$ gäller att $aH = bH \Leftrightarrow bH = aH$, så $a\,R\,b \Leftrightarrow b\,R\,a$.

(iii) För alla $a, b, c \in G$ gäller att ($aH = bH$ och $bH = cH$) $\Rightarrow aH = cH$, så $a\,R\,b$ och $b\,R\,c$ medför att $a\,R\,c$.

Därmed är R en ekvivalensrelation på G. Vidare gäller för varje $a \in G$ att $[a] = \{b \in G : a\,R\,b\} = \{b \in G : aH = bH\} = aH$, där den sista likheten ges av Lemma 27. □

Anmärkning. Vi har tidigare visat att $\{aH : a \in G\}$ utgör en partition av G. Detta gäller alltid för mängden av ekvivalensklasser.

Sats. (Algebra A). *Om R är en ekvivalensrelation på mängden X, så utgör ekvivalensklasserna en partition av X. Omvänt, om man har en partition av mängden X, så kan man införa en ekvivalensrelation R vars ekvivalensklasser genererar partitionen.*

Nu inför vi en viktig ekvivalensrelation, kallad G-ekvivalens, på en mängd X:

Sats 28. *Låt X vara en mängd och G en undergrupp av gruppen* $\mathrm{Sym}(X)$ *av permutationer på X. Definiera relationen $\sim$ på X genom $x \sim y \Leftrightarrow$ det finns en permutation $g \in G$ sådan att $y = g(x)$. Då är $\sim$ en ekvivalensrelation, som kallas G-ekvivalens på X.*

Bevis: (i) Det neutrala elementet i $\langle G, \circ \rangle$ är $id : X \to X$ given av $id(x) = x$ för alla $x \in X$. Då har vi att $x \sim x$ för alla $x \in X$ och då är $\sim$ reflexiv.

(ii) Följande utredning visar att $x \sim y \Rightarrow y \sim x$,

$$\begin{aligned} x \sim y &\Rightarrow \exists\, g \in G : y = g(x) \\ &\Rightarrow \exists\, g^{-1} \in G : g^{-1}(y) = g^{-1}(g(x)) = x \\ &\Rightarrow y \sim x\,. \end{aligned}$$

Analogt visas att $y \sim x \Rightarrow x \sim y$. Alltså gäller $x \sim y \Leftrightarrow y \sim x$, så $\sim$ är symmetrisk.

(iii) Följande implikationer påvisar transitiviteten,

$$\begin{aligned} x \sim y \text{ och } y \sim z &\Rightarrow \exists\, g, h \in G : g(x) = y \text{ och } h(y) = z \\ &\Rightarrow h \circ g \in G \text{ och } z = (h \circ g)(x) \\ &\Rightarrow x \sim z\,. \end{aligned}$$

Därmed är $\sim$ en ekvivalensrelation. □

Definition. *Ekvivalensklassen* $[x] = \{y \in X : x \sim y\}$ *kallas G-ekvivalensklassen av* x *eller banan av* x.

Således gäller det att X är unionen av disjunkta G-ekvivalensklasser.

Exempel.

1) Låt g vara en permutation på en ändlig mängd X, $|X| = n$, dvs. $g \in S_n$. Sätt $G = \langle g \rangle$ = undergrupp av S_n och tag $x \in X$. Då gäller enligt Sats 28 att

$$[x] = \{y \in X : \exists \text{ permutation } h \in G \text{ med } y = h(x)\}.$$

Emedan $G = \{g^i : 0 \le i \le |\langle g \rangle| = g\text{:s ordning}\}$, så är

$$[x] = \{\underbrace{x}_{g^0(x)}, g(x), g^2(x), \ldots, \underbrace{g^{|\langle g \rangle|}(x)}_{= x = g^0(x)}\}$$

Vi kan härmed konstatera att $[x] = \{$alla element i samma cykel som x$\}$.

2) Låt $X = \{A, B, C, D\}$, $g = (A\ B\ C)(D)$ och $G = \langle g \rangle \subseteq S_4$. Då är:

$$\begin{cases} [A] = [B] = [C] = \{A, B, C\} \\ [D] = \{D\} \end{cases}$$

Exempel.

Låt $X = \{1, 2, \ldots, 6\}$ och $\langle G, \circ \rangle \subseteq S_6$ med

$$G = \{e = (1), f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 5 & 6 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 6 & 3 & 4 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 3 & 4 & 5 \end{pmatrix}\}$$

Kollar som följande att: $f_1 \circ f_2 = f_3 = f_2 \circ f_1$, $f_1 \circ f_3 = e = f_3 \circ f_1$, $f_2 \circ f_3 = f_1 = f_3 \circ f_2$, $f_1 \circ f_1 = f_2$, $f_2 \circ f_2 = e$, $f_3 \circ f_3 = f_2$. Sats 18 ger nu att $\langle G, \circ \rangle$ är en undergrupp av S_6.

$$\begin{cases} e = (1) \\ f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 5 & 6 & 3 \end{pmatrix} = (1\ \ 2)\,(3\ \ 4\ \ 5\ \ 6) \\ f_2 = (3\ \ 5)\,(4\ \ 6) \\ f_3 = (1\ \ 2)\,(3\ \ 6\ \ 5\ \ 4) \end{cases}$$

Då är G-ekvivalensklasserna följande:

$$[1] = \{1, 2\} = [2]$$
$$[3] = \{3, 4, 5, 6\} = [4] = [5] = [6]$$

Vi har endast två disjunkta G-ekvivalensklasser, $X = [1] \cup [3]$

Definition. *Antag att* $\langle G, \circ \rangle$ *är en grupp av permutationer på en mängd* X *och att* $g \in G$. *Då kallas mängden*

$$X_g = \{x \in X : g(x) = x\}$$

fixpunktmängden för g *i* X. *För givet* $x \in X$ *kallas mängden*

$$\text{stab}(x) = \{g \in G : g(x) = x\}$$

stabilisatorn till x.

Sats 29. stab(x) *är en undergrupp till* $\langle G, \circ \rangle$.

Bevis: Eftersom $e = id \in \text{stab}(x)$ så är stab$(x) \neq \emptyset$. Tag $f, g \in \text{stab}(x)$. Då är $f(x) = x$ och $g(x) = x$, varför $x = g^{-1}(g(x)) = g^{-1}(x)$, så $g^{-1} \in \text{stab}(x)$. Nu gäller $(f \circ g^{-1})(x) = f(g^{-1}(x)) = f(x) = x$, så $f \circ g^{-1} \in \text{stab}(x)$. Då ger Sats 17 att stab(x) är en undergrupp till $\langle G, \circ \rangle$. □

Exempel. Betrakta igen $X = \{1, 2, \ldots, 6\}$ och $\langle G, \circ \rangle$ med

$$G = \{e = (1), f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 5 & 6 & 3 \end{pmatrix}, f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 6 & 3 & 4 \end{pmatrix}, f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 3 & 4 & 5 \end{pmatrix}\}$$

Då gäller att $X_e = X$, $X_{f_1} = \oslash$, $X_{f_2} = \{1, 2\}$, $X_{f_3} = \oslash$ och vidare att

$$\text{stab}(1) = \{e, f_2\}$$
$$\text{stab}(2) = \{e, f_2\}$$
$$\text{stab}(3) = \{e\} = \text{stab}(4) = \text{stab}(5) = \text{stab}(6).$$

Varje delgrupp G till gruppen Sym(X) av alla permutationer av en mängd $X \neq \emptyset$ kallas en **permutationsgrupp** eller en **grupp av permutationer**. Låt $|X_g|$ beteckna antalet element i g:s fixpunktmängd X_g och låt $|[x]|$ beteckna antalet element i G-ekvivalensklassen av x. Dessutom må $|\text{stab}(x)|$ beteckna antalet element i stabilisatorn till x.

Sats 30. *Låt* $\langle G, \circ \rangle$ *vara en ändlig delgrupp av* Sym(X). *För* $x \in X$ *gäller då att*

$$|G| = |[x]| \, |\text{stab}(x)| \, .$$

Bevis: Sats 29 ger att stab(x) är en undergrupp till G. Nu har vi att

$$G/\text{stab}(x) = \{g\text{stab}(x) : g \in G\},$$

där $g\text{stab}(x) = \{g \circ h : h \in \text{stab}(x)\}$. Nu ger Sats 23 att

$$|G| = |G/\text{stab}(x)|\,|\text{stab}(x)|\,.$$

Vidare gäller det att

$$[x] = \{y \in X : x \sim y\} = \{g(x) : g \in G\}\,.$$

Vi skall visa att det finns en bijektion $\varphi : G/\text{stab}(x) \to [x]$. Definiera därför φ för alla $g \in G$ genom

$$\varphi(g\text{stab}(x)) = g(x)\,.$$

(i) Funktionen φ är väldefinierad, ty om $g\text{stab}(x) = h\text{stab}(x)$ ger Lemma 27 att $g \in h\text{stab}(x)$, dvs. $g = h \circ s$ där $s \in \text{stab}(x)$. Alltså $g(x) = h(s(x)) = h(x)$, ty $s(x) = x$.

(ii) Funktionen φ är injektiv, ty $\varphi(g\text{stab}(x)) = \varphi(h\text{stab}(x)) \Rightarrow g(x) = h(x) \Rightarrow (h^{-1} \circ g)(x) = (h^{-1} \circ h)(x) = x \Rightarrow h^{-1} \circ g \in \text{stab}(x)$. Sätt nu $s = h^{-1} \circ g$. Då är $g = h \circ s$, vilket medför att $g \in h\text{stab}(x)$. Lemma 27 ger då att $h\text{stab}(x) = g\text{stab}(x)$ och därmed är φ injektiv.

(iii) Funktionen φ är surjektiv, ty antag att $y \in [x]$, dvs. $x \sim y$. Då finns det ett $g \in G$ sådant att $y = g(x)$. Alltså har vi att $\varphi(g\text{stab}(x)) = g(x) = y$, så φ är surjektiv.

Därmed är φ en bijektion och $|G/\text{stab}(x)| = |[x]|$. Då har vi att $|G| = |[x]|\,|\text{stab}(x)|$. □

Exempel. Betrakta åter $X = \{1, 2, ..., 6\}$ och låt gruppen $\langle G, \circ\rangle$ bestå av följande permutationer på X: $e = (1)$, $f_1 = (12)(3456)$, $f_2 = (35)(46)$ och $f_3 = (12)(3654)$. Vi har:

x	$[x]$	$\lvert[x]\rvert$	$\text{stab}(x)$	$\lvert\text{stab}(x)\rvert$
1	$\{1,2\}$	2	$\{e, f_2\}$	2
2	$\{1,2\}$	2	$\{e, f_2\}$	2
3	$\{3,4,5,6\}$	4	$\{e\}$	1
4	$\{3,4,5,6\}$	4	$\{e\}$	1
5	$\{3,4,5,6\}$	4	$\{e\}$	1
6	$\{3,4,5,6\}$	4	$\{e\}$	1

Sats 30 ger att $|G| = |[X]| \cdot |\text{stab}(x)| = 4$.

Korollarium 31. *Om $y \in [x]$, så är $|\text{stab}(x)| = |\text{stab}(y)|$.*

Bevis: Då $y \in [x]$, så är $[y] = [x]$. Alltså:

$$|\text{stab}(x)| = |G|/|[x]| = |G|/|[y]| = |\text{stab}(y)|,$$

och korollariet är bevisat. □

Exempel. Vi fortsätter med föregående exempel. Vi har $X = \{1, 2, \ldots, 6\}$ och $\langle G, \circ\rangle$ är en permutationsgrupp på X med uppbyggnaden

$$G = \{e, f_1 = (12)(3456), f_2 = (35)(46), f_3 = (12)(3654)\}$$

Då gäller

g	X_g	$\lvert X_g\rvert$
e	X	6
$(12)(3456)$	$\oslash$	0
$(35)(46)$	$\{1,2\}$	2
$(12)(3654)$	$\oslash$	0

och vi får

$$\sum_{g\in G}|X_g| = 8 = \sum_{x=1}^{6}|\mathrm{stab}(x)|, \qquad |G| = 4$$

Antalet olika G-ekvivalensklasser är är alltså $\frac{8}{4} = 2$.

Låt oss nu **allmänt** beräkna antalet olika G-ekvivalensklasser för en given permutationsgrupp G på en mängd X.

Varje G-ekvivalensklass utgör en delmängd av X vars element inte kan urskiljas under gruppoperationer och följaktligen är antalet G-ekvivalensklasser exakt antalet skiljbara, olika typer av objekt i X.

Antalet olika G-ekvivalensklasser ges av Burnsides sats. (William Burnside 1852-1927).

Sats 32. (Burnsides sats). *Låt $\langle G, \circ\rangle$ vara en ändlig delgrupp av* $\mathrm{Sym}(X)$. *Låt k beteckna antalet olika G-ekvivalensklasser. Då gäller*

$$k = \frac{1}{|G|}\sum_{g\in G}|X_g|\,.$$

Bevis: Låt $n =$ antalet par $(g,x) \in G \times X$ med $g(x) = x$. Då $X_g = \{x \in X : g(x) = x\}$, får vi att

$$n = \sum_{g\in G}|X_g|\,.$$

Emedan $\mathrm{stab}(x) = \{g \in G : g(x) = x\}$, gäller det att

$$n = \sum_{x\in X}|\mathrm{stab}(x)|\,.$$

Nu får vi med stöd av Korollarium 31 och Sats 30 att

$$\sum_{x\in[y]}|\mathrm{stab}(x)| = |[y]|\,|\mathrm{stab}(y)| = |G|\,. \qquad (*)$$

Alltså om $[y_1], ..., [y_k]$ är de k olika G-ekvivalensklasserna, så erhålls att

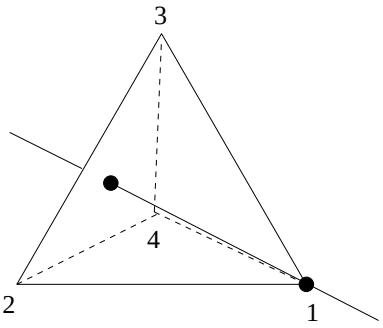
$$\sum_{g\in G}|X_g| = n = \sum_{x\in X}|\mathrm{stab}(x)| = \sum_{x\in[y_1]}|\mathrm{stab}(x)| + ... + \sum_{x\in[y_k]}|\mathrm{stab}(x)| = k\,|G|,$$

där den sista likheten följer med stöd av $(*)$, varför vi erhåller $k = \frac{1}{|G|}\sum_{g\in G}|X_g|\,.$ □

Låt en rymdfigur i R^3, t.ex. en kub, vara given och betrakta alla rotationer av rymdfiguren kring olika symmetriaxlar. Mängden av alla sådana rotationer som överför rymdfiguren på sig själv bildar en grupp, dvs. vi får gruppen bestående av rotationssymmetrier av rymdfiguren.

Låt oss betrakta ett exempel i form av en regulär tetraeder i R^3.

Exempel. Låt T vara en regulär tetraeder i $\mathbf{R}^3$, dvs



Figur 6.

Bestäm ordningen av gruppen som består av rotationssymmetrier av T.

Låt G vara gruppen av permutationer av hörnen som svarar mot rotationssymmetrierna. Vi tillämpar Sats 30 och betraktar hörn 1. Nu gäller

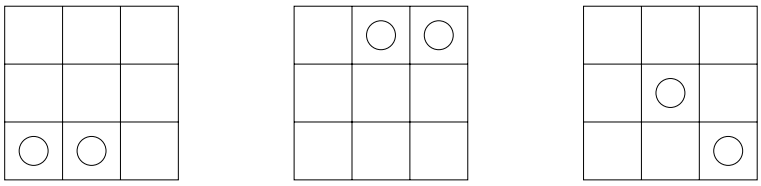
$$[1] = \{1, 2, 3, 4\}, \qquad |[1]| = 4$$

ty hörn 1 kan roteras till vilket hörn som helst. Betrakta hörn 1 och symmetriaxeln α genom hörn 1. Vi har

$$\begin{aligned} \text{stab}(1) &= \{\text{rot}0^\circ, \text{rot}120^\circ, \text{rot}240^\circ \text{ kring } \alpha\} \\ &= \text{rotationssymmetrier som bibehåller hörn 1 fixerad.} \\ |\text{stab}(1)| &= 3 \end{aligned}$$

Sats 30 ger att $|G| = |[1]|\,|\text{stab}(1)| = 4 \cdot 3 = 12$.

Exempel. Antag att vi vill tillverka ID-kort utav plastkvadrater som är markerade med ett 3×3 rutnät på båda sidorna av korten och stansade med två hål, såsom i följande figur:



Figur 7.

Emedan det finns 9 lägen och 2 hål, så är antalet sätt att stansa hålen

$$\binom{9}{2} = \frac{9!}{7!2!} = \frac{9 \cdot 8}{2} = 36\,.$$

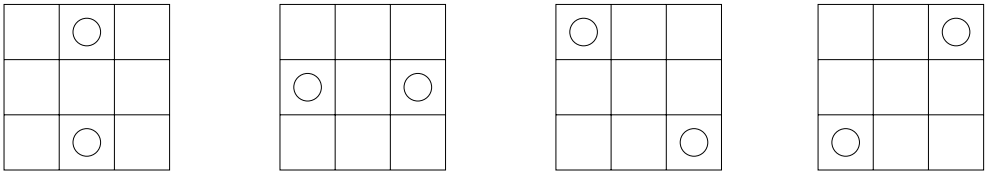
Vi kommer att hänvisa till dessa som **konfigurationer**. Notera att man inte kan skilja på alla konfigurationer, ty korten kan roteras och speglas.

Den grupp G som opererar här är **diedergruppen** D_n med $n = 4$, som består av symmetrierna av kvadraten.

Vi måste betrakta D_4 opererande på mängden X som består av 36 konfigurationer istället för de fyra hörnen, dvs. vi har 8 permutationer av dessa 36 konfigurationer. Då är antalet G-ekvivalensklasser på X exakt antalet skiljbara olika identitetskort.

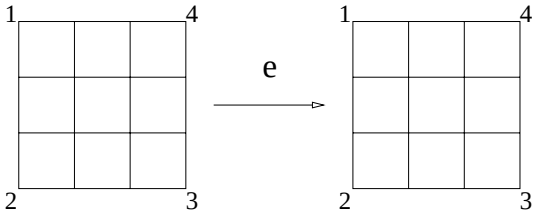
Vi använder Burnsides sats. För var och en av de 8 symmetrierna g behöver vi endast beräkna $|X_g|$, dvs. antalet konfigurationer fixerade av g.

Exempelvis då g är rotation med 180 grader har vi fyra fixerade konfigurationer:

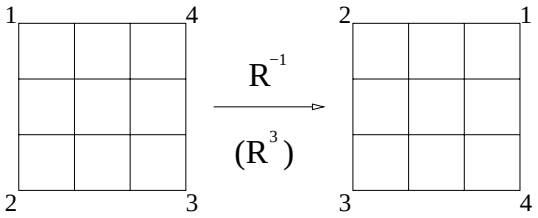


Figur 8.

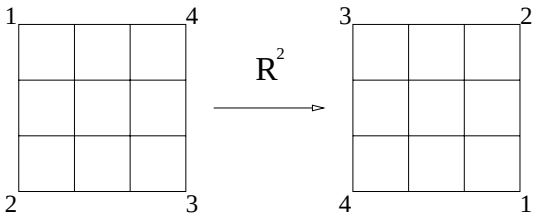
Låt oss först börja med att skriva ut de 8 permutationerna:



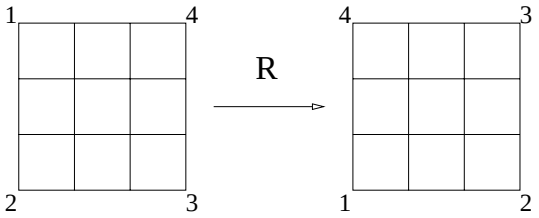
$$e = h_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1)(2)(3)(4), \quad |X_{h_1}| = 36 \qquad (\text{rot}0^\circ)$$



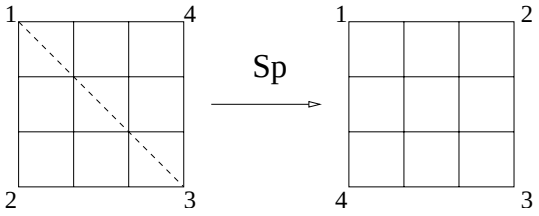
$$h_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234), \quad |X_{h_2}| = 0 \qquad (\text{rot}270^\circ)$$



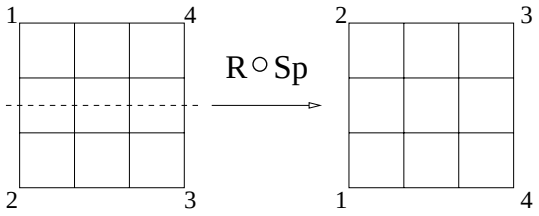
$$h_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24), \quad |X_{h_3}| = 4 \qquad (\text{rot}180^\circ)$$



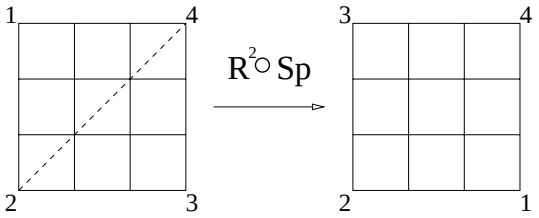
$$h_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1432), \quad |X_{h_4}| = 0 \qquad (\text{rot}90^\circ)$$



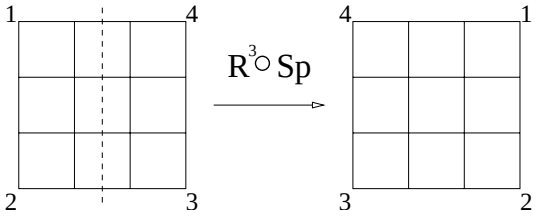
$$h_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (1)(24)(3), \quad |X_{h_5}| = 6$$



$$h_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34), \quad |X_{h_6}| = 6$$



$$h_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (13)(2)(4), \quad |X_{h_7}| = 6$$



$$h_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23), \quad |X_{h_8}| = 6$$

Nu ger Burnsides sats att

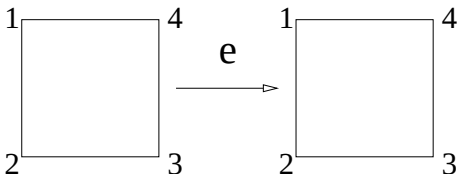
$$k = \frac{1}{|G|} \sum_{i=1}^{8} |X_{h_i}| = \frac{1}{8}(36 + 0 + 4 + 0 + 6 + 6 + 6 + 6) = 64/8 = 8,$$

så vi har 8 **olika** ID-kort.

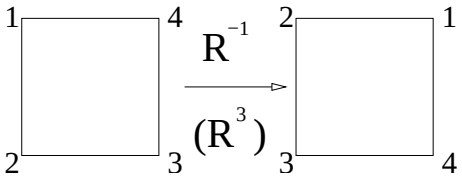
Det är klart att i detta speciella fall skulle det inte vara alltför svårt att bestämma de åtta korten genom försök och misstag. Men i mera allmänna situationer och vid lösning av problem gällande symmetri är Sats 32 ytterst användbar. Därom mera i följande avsnitt.

Tillämpning på färgläggningsproblem

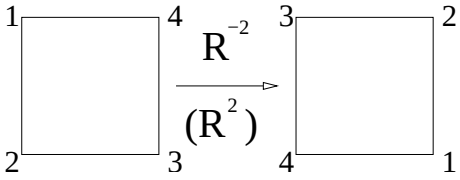
Exempel. På hur många sätt kan hörnen (eller sidorna) hos en kvadrat färgläggas med 2 olika färger om man inte skiljer på fall som kan överföras på varandra genom rotationer eller speglingar? Gruppen som opererar här är diedergruppen D_4 som har 8 element.



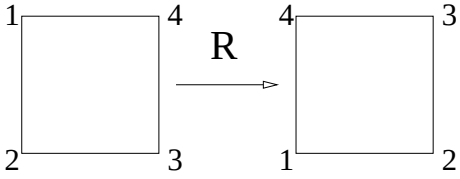
$$e = h_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1)(2)(3)(4)$$



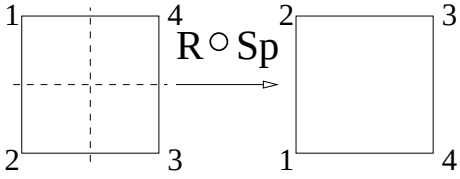
$$h_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1234)$$



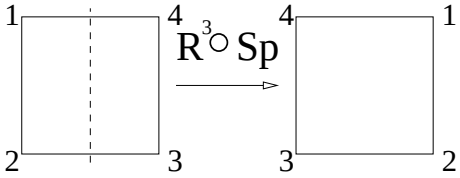
$$h_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24)$$



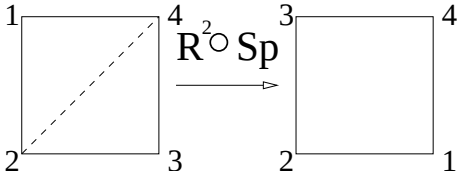
$$h_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} = (1432)$$



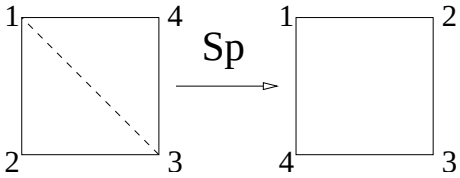
$$h_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$$



$$h_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23)$$



$$h_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = (13)(2)(4)$$



$$h_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = (1)(24)(3)$$

Vi har alltså $X = \{1, 2, 3, 4\}$, $G = D_4 \subset S_4$ och $Y =$ mängden av olika färger. En färgläggning av hörnen är en funktion $f : X \to Y$. Vi skiljer **inte** på elementen $f \circ g$ då $g \in D_4$.

Låt oss i fortsättningen resonera allmänt med $G \subseteq S_n$ och $X = \{1, 2, ..., n\}$.

Problem: *Hur många olika mängder* $\{f \circ g : g \in G\}$ *finns det då* f *genomlöper mängden*

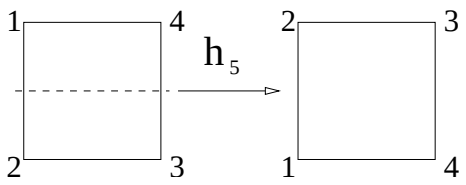
$$\mathcal{F} = Y^X = \{f : X \to Y\} = \{\text{alla färgläggningar}\}?$$

Definition. *För varje* $g \in G$ *definieras avbildningen* $g' : \mathcal{F} \to \mathcal{F}$ genom

$$g'(f) = f \circ g\,,$$

för varje $f \in \mathcal{F}$. Vidare definieras $G' = \{g' : g \in G\}$.

Exempel. Betrakta $h_5 = (12)(34) \in G$, $G = D_4$. Vidare är $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ V & R & R & R \end{pmatrix} \in \mathcal{F}$ (V = vit, R = röd)
Då är $h_5' = f \circ h_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ V & R & R & R \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ R & V & R & R \end{pmatrix}$



Figur 9.

Lemma 33. *Avbildningen* $g' : \mathcal{F} \to \mathcal{F}$ *är en permutation.*

Bevis: (i) Avbildningen g' är surjektiv, ty tag godtyckligt $f_1 \in \mathcal{F}$ och sätt $f_2 = f_1 \circ g^{-1} \in \mathcal{F}$. Då gäller $g'(f_2) = f_2 \circ g = f_1 \circ g^{-1} \circ g = f_1$.

(ii) Avbildningen g' är injektiv, ty låt $g'(f_1) = g'(f_2)$, dvs. $f_1 \circ g = f_2 \circ g$. Då gäller $f_1(g(x)) = f_2(g(x))$ för alla $x \in X$. Då g är en permutation så är den surjektiv och därmed gäller det att $f_1(x) = f_2(x)$ för alla $x \in X$, så $f_1 = f_2$, vilket ger att g' är injektiv.

Alltså har vi att g' är en bijektion och därmed en permutation. □

Anmärkning. Vi observerar att $G = D_n$ är en undergrupp av $\mathrm{Sym}(X)$ och att G' är en delmängd av $\mathrm{Sym}(\mathcal{F})$.

Sats 34. *Strukturen* $\langle G', \circ \rangle$, *där* $G' = \{g' : g \in G\}$, *är en undergrupp av* $\mathrm{Sym}(\mathcal{F})$.

Bevis: Klart att $G' \neq \emptyset$. Tag $h', g' \in G'$. Vi bör visa att $h' \circ g' \in G'$, (Sats 18), ty $|\mathcal{F}| < \infty$. För varje $f \in \mathcal{F}$ gäller

$$(h' \circ g')(f) = h'(g'(f)) = h'(f \circ g) = (f \circ g) \circ h = f \circ (g \circ h)$$
$$= (g \circ h)'(f)\,.$$

Alltså: $h' \circ g' = (g \circ h)' \in G'$, ty $g \circ h \in G$. □

Påstående: *Avbildningen* $' : G \to G'$ *som avbildar* g *på* g' *är bijektiv, varför* $|G| = |G'|$.

Bevis: Vi har att $G' = \{g' : g \in G\}$.

(i) Klart att $'$ är surjektiv.

(ii) Visar injektiviteten. Antag att $|Y| \geq 2$. För alla $f \in \mathcal{F}$ gäller

$$g' = h' \Rightarrow g'(f) = h'(f) \Rightarrow f \circ g = f \circ h\,. \qquad (*)$$

Antites: $g \neq h$.

Då finns det ett $i \in X : j_1 = g(i) \neq h(i) = j_2$. Vidare finns det då ett $f \in \mathcal{F}$ sådant att $f(j_1) \neq f(j_2)$. Då gäller

$$(f \circ g)(i) = f(g(i)) = f(j_1) \neq f(j_2) = f(h(i)) = (f \circ h)(i),$$

men detta ger en motsägelse till $(*)$! Antitesen är falsk och $g = h$. Därmed är $'$ injektiv.

Vi har då att $' : G \to G'$ är en bijektion, vilket ger att $|G| = |G'|$. □

Då g' är en permutation på $\mathcal{F}$ för varje $g' \in G'$ (Lemma 33), så erhålls G'-ekvivalensklassen, (med avseende på gruppen G'), för $f \in \mathcal{F}$ med stöd av Sats 28 av

$$[f] = \{g'(f) : g' \in G'\}\,.$$

Alltså gäller det att

$$\{f \circ g : g \in G\} = \{g'(f) : g \in G\} = \{g'(f) : g' \in G'\} = [f]\,.$$

Därmed tillhör alla element $f \circ g$ för $g \in G$ samma G'-ekvivalensklass av f, med andra ord ger dessa element upphov till färgläggningar som vi **inte** skiljer på.

Vi är alltså intresserade av **antalet** G'-ekvivalenklasser i $\mathcal{F}$ med avseende på G'. Nu ger Sats 32 (Burnside) och ovanstående påstående att antalet olika G'-ekvivalensklasser är

$$\frac{1}{|G'|} \sum_{g \in G} |\mathcal{F}_{g'}| = \frac{1}{|G|} \sum_{g \in G} |\mathcal{F}_{g'}|\,,$$

där

$$\mathcal{F}_{g'} = \{f \in \mathcal{F} : g'(f) = f\} = \{f \in \mathcal{F} : f \circ g = f\}\,.$$

Exempel. Vi återgår till det tidigare exemplet med kvadraten. Vi har $G = \{h_1, h_2, \ldots, h_8\} = D_4$ vilket ger oss $|G| = 8$.

$$\begin{aligned} h_1 &= (1)(2)(3)(4), & h_5 &= (12)(34), \\ h_2 &= (1234), & h_6 &= (14)(23), \\ h_3 &= (13)(24), & h_7 &= (13)(2)(4), \\ h_4 &= (1432), & h_8 &= (1)(24)(3). \end{aligned}$$

Vi har $\mathcal{F}_{h_1'} = \{f \in \mathcal{F} : f \circ h_1 = f \circ e = f\} = \{f \in \mathcal{F} : f = f\} = \mathcal{F}$, varför $|\mathcal{F}_{h_1'}| = 2^4 = 16$.

Vidare gäller att $\mathcal{F}_{h_2'} = \{f \in \mathcal{F} : f \circ h_2 = f\} = \{f \in \mathcal{F} : f(1) = f(2), f(2) = f(3), f(3) = f(4), f(4) = f(1)\} = \{f \in \mathcal{F} : f(1) = f(2) = f(3) = f(4)\}$

En färgläggning f tillhör alltså $\mathcal{F}_{h_2'}$ endast då hörnen 1,2,3 och 4 alla har samma färg. Vi kan välja denna färg på två sätt, varför $|\mathcal{F}_{h_2'}| = 2$.

Låt oss, innan vi fortsätter med vårt exempel, beskriva ett lämpligt sätt att beräkna $|\mathcal{F}_{g'}|$ då $g \in G \subseteq S_n$ och G' opererar på $\mathcal{F} = Y^X = \{\text{alla färgläggningar}\}$, där $Y =$ mängden av alla färger, antalet olika färger $= q = |Y|$ och $X = \{1, 2, ..., n\}$.

Om $g \in G$ skrivs som en produkt av disjunkta cykler så skriver vi alltid ut också cykler av formen (k). Vi inför nu begreppet **cykelindex**:

Definition. *Antalet disjunkta cykler i permutationen $g \in G$ betecknas med* cyc$g$ *och kallas cykelindexet för g.*

Om exempelvis $f \in S_7$ och $f = (23)(567) = (1)(23)(4)(567)$, så är cyc$f = 4$.

Exempel. Betrakta $g = (14)(357) \in S_7$. Då skriver vi $g = (14)(2)(357)(6)$. Om q färger är tillgängliga i Y, så påstår vi att

$$|\mathcal{F}_{g'}| = q^4.$$

Om vi låter $f \in \mathcal{F}$ vara given, så gäller

$$f \in \mathcal{F}_{g'} \Leftrightarrow f \circ g = f \Leftrightarrow \begin{cases} f(1) = f(4) \text{ och} \\ f(3) = f(5) = f(7). \end{cases}$$

Då finns det q val för var och en av färgerna:

$$f(1) = f(4),\ f(2),\ f(3) = f(5) = f(7) \text{ och } f(6).$$

Således finns det q^4 möjliga avbildningar $f \in \mathcal{F}$.

Om vi generaliserar resonemanget i föregående exempel till $g \in G \subseteq S_n$, så erhåller vi att

$$|\mathcal{F}_{g'}| = q^{\mathrm{cyc}\, g}.$$

Vi återgår till exemplet med kvadraten:

$$|\mathcal{F}_{h_1'}| = 2^4 = 16, \quad |\mathcal{F}_{h_2'}| = 2^1 = 2, \quad |\mathcal{F}_{h_3'}| = 2^2 = 4$$
$$|\mathcal{F}_{h_4'}| = 2^1 = 2, \quad |\mathcal{F}_{h_5'}| = 2^2 = 4 = |\mathcal{F}_{h_6'}|, \quad |\mathcal{F}_{h_7'}| = 2^3 = 8 = |\mathcal{F}_{h_8'}|$$

Sats 32 ger antalet olika G'-ekvivalensklasser (olika färgläggningar):

$$\frac{1}{|G'|} \sum_{g' \in G'} |\mathcal{F}_{g'}| = \frac{1}{8}(16 + 2 + 4 + 2 + 4 + 4 + 8 + 8) = 6.$$

Allmänt kan sägas om q st. färger:

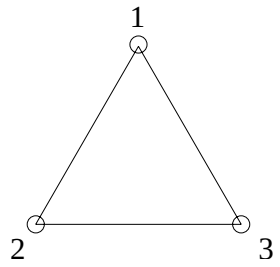
$$\text{antal färgläggningar } = \frac{1}{8}(q^4 + 2q + 3q^2 + 2q^3) = \frac{q}{8}(q+1)(q^2+q+2).$$

Vi sammanfattar våra utredningar i följande sats:

Sats 35. *Låt G vara en undergrupp av S_n, $X = \{1, 2, ..., n\}$ och Y en mängd av q stycken färger. Då är antalet av G inducerade G'-ekvivalensklasser, (olika färgläggningar), på $\mathcal{F} = Y^X = \{$alla färgläggningar$\}$ givet av*

$$\frac{1}{|G|} \sum_{g \in G} |\mathcal{F}_{g'}| = \frac{1}{|G|} \sum_{g \in G} q^{\mathrm{cyc}\, g}.$$

Exempel. En molekyl har atomerna placerade i hörnen av en liksidig triangel. På hur många sätt kan man färglägga atomerna med q stycken givna färger?



Figur 10.

$$X = \{1, 2, 3\}$$

a) Här opererar diedergruppen $G = D_3 = S_3$. Vi har $|G| = 6$ och

$$G = \{(1)(2)(3),\ (123),\ (132),\ (1)(23),\ (12)(3),\ (13)(2)\}$$

Sats 35 ger att

$$k = \frac{1}{|G|}\sum_{g\in G} q^{\mathrm{cyc}g} = \frac{1}{6}(q^3 + q^1 + q^1 + q^2 + q^2 + q^2) = \frac{q}{6}(q^2 + 3q + 2) = \frac{q}{6}(q+1)(q+2).$$

b) Vid enbart rotation, $H_1 = \{(1)(2)(3),\ (123),\ (132)\}$ som är en undergrupp av $G = D_3$, gäller

$$k = \frac{1}{|H_1|}\sum_{g\in H_1} q^{\mathrm{cyc}g} = \frac{1}{3}(q^3 + 2q) = \frac{q}{3}(q^2 + 2).$$

c) Vid enbart spegling, $H_2 = \{(1)(2)(3),\ (1)(23)\}$ som är en undergrupp av $G = D_3$, gäller

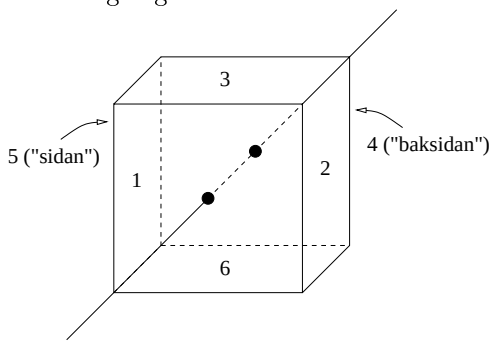
$$k = \frac{1}{2}(q^3 + q^2) = \frac{q^2}{2}(q+1).$$

d) För $H_3 = \{(1)(2)(3)\}$ som är en undergrupp av $G = D_3$ gäller

$$k = \frac{1}{1}\cdot q^3 = q^3.$$

Exempel. Rotationsgruppen till en kub. Låt G vara gruppen av permutationer av sidorna som består av rotationssymmetrier av kuben. På hur många sätt kan sidorna för kuben färgläggas med q stycken färger?

Sidorna numreras $1, \ldots, 6$ och vi får $X = \{1, 2, \ldots, 6\}$. Vi bestämmer först $|G|$ ($G \subseteq S_6$. Vi fixerar sida 1 med axeln α genom sida 1 och sida 4 enligt figuren:



Figur 11.

Nu gäller att $[1] = \{1, 2, \ldots, 6\} = X$, ty sida 1 kan roteras till vilken annan sida som helst om vi beaktar även andra symmetriaxlar utöver α. Vi har alltså

$$|[1]| = 6$$

Vidare gäller att

$$\mathrm{stab}(1) = \{\mathrm{rot}0^\circ,\ \mathrm{rot}\frac{\pi}{2},\ \mathrm{rot}\pi \text{ och } \mathrm{rot}\frac{3\pi}{2} \text{ kring } \alpha\},\ \text{och } |\mathrm{stab}(1)| = 4.$$

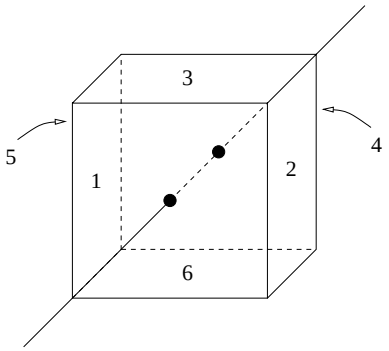
Sats 30 ger

$$|G| = |[1]| \cdot |\mathrm{stab}(1)| = 6 \cdot 4 = 24.$$

Sats 35 säger

$$k = \frac{1}{|G|} \sum_{g \in G} q^{\mathrm{cyc}g}.$$

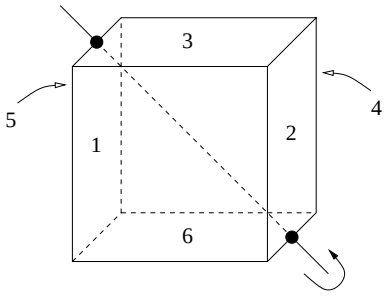
$$h_1 = e = (1)(2)(3)(4)(5)(6),\ q^{\mathrm{cyc}h_1} = q^6$$
$$h_2 = \mathrm{rot}\frac{\pi}{2} = (1)(2356)(4),\ q^{\mathrm{cyc}h_2} = q^3$$
$$h_3 = \mathrm{rot}\pi = (1)(25)(36)(4),\ q^{\mathrm{cyc}h_3} = q^4$$
$$h_4 = \mathrm{rot}\frac{3\pi}{2} = (1)(2653)(4),\ q^{\mathrm{cyc}h_4} = q^3$$



Figur 12.

Liknande rotationer kring axeln genom sidorna 2 och 5 samt genom 3 och 6 finns. Bidrag $= 3(2q^3 + q^4) = 6q^3 + 3q^4$.

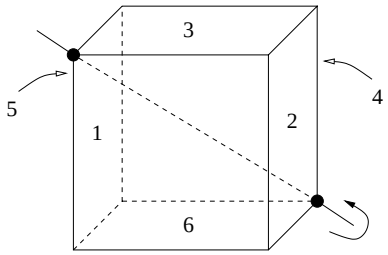
$$h_{11} = \mathrm{rot}\pi = (14)(26)(35),\ q^{\mathrm{cyc}h_2} = q^3$$



Figur 13.

Det finns 5 liknande rotationer (axel genom kant). Bidrag $= 6q^3$.

$$h_{17} = \mathrm{rot}\frac{2\pi}{3} = (135)(246),\ q^{\mathrm{cyc}h_{17}} = q^2$$
$$h_{18} = \mathrm{rot}\frac{4\pi}{3} = (153)(264),\ q^{\mathrm{cyc}h_{18}} = q^2$$



Figur 14.

Det finns 3 liknande rotationer (axel genom hörn). Bidrag $= 4(2q^2) = 8q^2$.

Vi får alltså

$$k = \frac{1}{|G|}\sum_{g\in G} q^{\mathrm{cyc}\, g} = \frac{1}{24}(q^6 + 3q^4 + 12q^3 + 8q^2).$$

Exempel. Antag att vi har kuber sådana att alla sidorna är målade med **olika** färger. Om $q \geq 6$ färger är tillgängliga, hur många olika kuber har vi?

Lösning: Låt $X = \{1, 2, ..., 6\}$ och låt Y vara mängden av q färger, (såsom tidigare).

Emedan sidorna har olika färger, så är färgläggningen i detta fall en **injektiv** avbildning

$$f : X \to Y\,.$$

Låt $\mathcal{G} \subseteq \mathcal{F} = Y^X$ beteckna mängden av alla sådana avbildningar. Låt vidare G beteckna rotationsgruppen till kuben. Då vet vi att $|G| = 24$.

Om $g \in G$ och $f \in \mathcal{G}$, så är $g'(f) = f \circ g$ en injektiv avbildning. Alltså $g'(f) \in \mathcal{G}$ och $g' : \mathcal{G} \to \mathcal{G}$.

Antag att $g \in G$ med $g \neq e$. Då är $\mathcal{G}_{g'} = \{f \in \mathcal{G} : f \circ g = f\}$. Om $f_1 \in \mathcal{G}_{g'}$, dvs. $f_1 \circ g = f_1$, så följer det från $g(i) = j$ att

$$f_1(i) = f_1(g(i)) = f_1(j)\,.$$

Emedan f_1 är injektiv följer det att $i = j$ för varje $i \in X$. Då $g \neq e$ är detta omöjligt, varför $\mathcal{G}_{g'} = \emptyset$ då $g \neq e$. Alltså

$$|\mathcal{G}_{g'}| = 0, \quad \text{då } g \neq e\,.$$

Nu gäller

$$\mathcal{G}_{e'} = \{f \in \mathcal{G} : f = f\} = \mathcal{G}\,.$$

Vidare är antalet ordnade delmängder till Y bestående av 6 stycken element givet av

$$(q)_6 = \frac{q!}{(q\text{-}6)!},$$

ty den första färgen kan väljas på q olika sätt, den andra på q-1 olika sätt osv., alltså:

$$(q)_6 = q(q\text{-}1)(q\text{-}2)(q\text{-}3)(q\text{-}4)(q\text{-}5) = \frac{q!}{(q\text{-}6)!}\,.$$

Därmed är

$$|\mathcal{G}_{e'}| = \frac{q!}{(q\text{-}6)!}\,.$$

Sats 35 ger då att antalet olika färgläggningar är

$$n = \frac{1}{|G|}\sum_{g\in G}|\mathcal{G}_{g'}| = \frac{|\mathcal{G}_{e'}|}{|G|} = \frac{q!}{24\,(q\text{-}6)!}\,.$$

Om $q = 6$ (det minimala antalet olika färger), så får vi att

$$n = \frac{6!}{24} = 30\,.$$

Kopplingsfunktioner

En **kopplingsfunktion** i n-variabler är en funktion från alla binära n-tipler till mängden $\{0,1\}$ av binära 1-tipler, dvs. en avbildning

$$f : \{0,1\}^n \to \{0,1\}$$

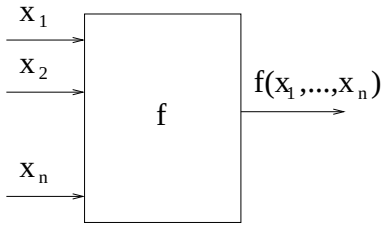
är en kopplingsfunktion. ($\{0,1\}^n = \{0,1\} \times \{0,1\} \times ... \times \{0,1\}$ (produkt med n faktorer)).

Låt

$$\mathcal{F}_n = \{f : \{0,1\}^n \to \{0,1\}\} = \{0,1\}^{\{0,1\}^n}\,.$$

Sätt $X = \{0,1\}^n$ och $Y = \{0,1\}$. Då är $\mathcal{F}_n = Y^X$.

Namnet kopplingsfunktion kommer från att vi tänker oss ha en elektrisk krets som accepterar INPUT av n stycken variabler av binära tal och producerar OUTPUT av en variabel. Outputen beror endast av inputen, dvs. kretsen har inget minne.



Figur 15.

Nu frågar vi oss hur många funktioner f finns det?

$$|\mathcal{F}_n| = |Y^X| = |Y|^{|X|},\ |X| = 2^n,\ |Y| = 2\,,$$

så vi erhåller

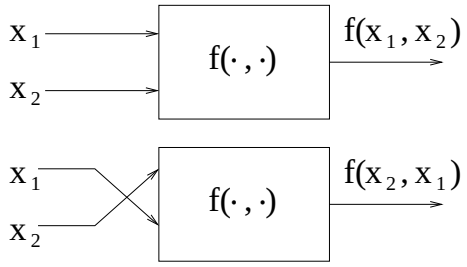
$$|\mathcal{F}_n| = 2^{2^n} .$$

Exempelvis om $n = 3$ så är $|\mathcal{F}_3| = 256$ och om $n = 4$ så är $|\mathcal{F}_4| = 65536$.

För $n = 2$ finns det $2^{2^2} = 16$ kopplingsfunktioner:

x_1	x_2	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Hur många $f \in \mathcal{F}_n$ behövs för att "täcka" alla möjligheter om inputvariablerna kan permuteras?



Figur 16.

Man kan säga att $f, g \in \mathcal{F}_2$ är **ekvivalenta** om g kan erhållas från f genom en permutation av variablerna x_1 och x_2. Alltså om $g(x_1, x_2) = f(x_2, x_1)$, så är $f \sim g$ via permutationen

$$(x_1 x_2) = \begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix} .$$

Notera att $f \sim f$ via identitetspermutationen.

Låt oss bestämma alla ekvivalensklasser av funktioner i $\mathcal{F}_2$. Varje permutation av variablerna inducerar en permutation av $\mathcal{F}_2$. Permutationen $(x_1 x_2)$ på $\{0, 1\}$ ger permutationen

$$h = (f_2 f_4)(f_3 f_5)(f_{10} f_{12})(f_{11} f_{13}) \text{ av } \mathcal{F}_2 ,$$

dvs. $h = (f_0)(f_1)(f_2 f_4)(f_3 f_5)(f_6)(f_7)(f_8)(f_9)(f_{10} f_{12})(f_{11} f_{13})(f_{14})(f_{15})$. Alltså 12 stycken disjunkta cykler. Dessa är ekvivalensklasserna av funktioner i $\mathcal{F}_2$. Således har vi 12 ekvivalensklasser.

Låt oss nu se hur man kan använda Sats 35 för liknande problem av mer komplicerad art.

Exempel. Hur många "icke-ekvivalenta" kopplingsfunktioner i tre variabler finns det om permuterade variabler ger ekvivalenta kopplingsfunktioner?

Vi har $n = 3$, sätt $x = x_1$, $y = x_2$ och $z = x_3$. Vi får då att $X = \{0,1\}^3$, $Y = \{0,1\}$. Vi har 8 tillstånd för inputvariablerna (x, y, z), dvs

$$\underbrace{(0,0,0)}_{1},\ \underbrace{(0,0,1)}_{2},\ \underbrace{(0,1,0)}_{3},\ \underbrace{(0,1,1)}_{4},\ \underbrace{(1,0,0)}_{5},\ \underbrace{(1,0,1)}_{6},\ \underbrace{(1,1,0)}_{7},\ \underbrace{(1,1,1)}_{8}.$$

Då är $X = \{1, 2, \ldots, 8\}$ och $\mathcal{F}_3 = \{f : X \to \{0,1\}\}$.

Det finns 6 permutationer av variablerna $\{x, y, z\}$ och var och en av dessa permutationer inducerar en permutation av X:

$$\begin{aligned}
e &\Leftrightarrow (1)(2)(3)(4)(5)(6)(7)(8),\ 8 \text{ cykler.}\\
(xy) &\Leftrightarrow (1)(2)(35)(46)(7)(8),\ 6 \text{ cykler.}\\
(xz) &\Leftrightarrow (1)(25)(3)(47)(6)(8),\ 6 \text{ cykler.}\\
(yz) &\Leftrightarrow (1)(23)(4)(5)(67)(8),\ 6 \text{ cykler.}\\
(xyz) &\Leftrightarrow (1)(253)(467)(8),\ 4 \text{ cykler.}\\
(xzy) &\Leftrightarrow (1)(235)(476)(8),\ 4 \text{ cykler.}
\end{aligned}$$

Man kan visa att dessa permutationer bildar en undergrupp G av S_8.

$$|G| = 6,\ Y = \{0,1\} = 2 \text{ st. variabler, } q = |Y| = 2.$$

Sats 35 ger antalet olika G-ekvivalensklasser:

$$\frac{1}{|G|}\sum_{g\in G} q^{\mathrm{cyc}\, g} = \frac{1}{6}(2^8 + 2^6 + 2^6 + 2^6 + 2^4 + 2^4) = 80.$$

Det finns alltså väsentligen 80 olika kopplingsfunktioner av tre variabler, eller det behövs endast 80 st. vid permutering av inputvariablerna för att "täcka" alla.

Låt oss avslutningsvis kontrollera fallet $n = 2$. Sätt $x = x_1$ och $y = x_2$, samt $X = \{0,1\}^2$, $Y = \{0,1\}$. Vi har 4 tillstånd för inputvariablerna (x, y). Om dessa betecknas med $1, 2, 3, 4$ har vi:

$$1 \leftrightarrow (0,0),\ 2 \leftrightarrow (0,1),\ 3 \leftrightarrow (1,0),\ 4 \leftrightarrow (1,1)\,.$$

Då är $X = \{1, 2, 3, 4\}$ och $\mathcal{F}_2 = \{f : X \to \{0,1\}\}$. Det finns 2 permutationer av variablerna x och y, och var och en av dessa permutationer inducerar en permutation av X:

$$\begin{aligned}
e &\Leftrightarrow (1)(2)(3)(4) \quad 4 \text{ cykler,}\\
(xy) &\Leftrightarrow (1)(23)(4) \quad 3 \text{ cykler.}
\end{aligned}$$

Alltså har vi $|G| = 2$ och $q = |Y| = 2$ variabler. Då ger Sats 35 att antalet olika ekvivalensklasser är:

$$\frac{1}{|G|}\sum_{g\in G} q^{\mathrm{cyc}\, g} = \frac{1}{2}(2^4 + 2^3) = 12.$$