saadaan polynomin kertoimista rationaalisilla laskutoimituksilla ja juurenotoilla (ajattele toisen asteen yhtälön ratkaisukaavaa).

Kutakin n:n arvoa kohti voidaan muodostaa sellainen polynomi $p(x)$, johon liittyvä ryhmä G_p on koko S_n. Nähdään siis, että on olemassa n:nnen asteen yhtälön *yleinen ratkaisukaava* jos ja vain jos ryhmä S_n on ratkeava. Edellinen esimerkki osoittaa, että näin on silloin ja vain silloin, kun $n < 5$.

Tämän tuloksen saavuttivat Abel ja Galois 1800-luvun alkupuolella. Se ratkaisi matemaatikkoja satoja vuosia askarruttaneen kysymyksen ja merkitsi samalla ryhmäteorian alkua.

Cayleyn lauseen todistuksessa (edellinen pykälä) liitettiin ryhmän $G = \{x_1, x_2, \ldots, x_n\}$ kuhunkin alkioon x joukon $\{1, 2, \ldots, n\}$ permutaatio α_x. Olkoon V n-ulotteinen (kompleksikertoiminen) vektoriavaruus ja olkoon $\{B_1, \ldots, B_n\}$ sen kiinnitetty kanta. Kun sovelletaan permutaatiota α_x kantavektoreihin, saadaan säännöllinen lineaarikuvaus $V \to V$. Tätä puolestaan vastaa säännöllinen $n \times n$-matriisi A_x. Näin muodostuu kuvaus

$$G \longrightarrow GL_n(\mathbb{C}), \qquad x \mapsto A_x,$$

joka on ryhmähomomorfismi. Tätä kuvausta – tai G:n homomorfisena kuvana näin saatua matriisiryhmää – sanotaan ryhmän G *säännölliseksi esitykseksi*. Matriisiryhmän $GL_n(C)$ asemesta voidaan yhtä hyvin tarkastella sen kanssa isomorfista kuvausryhmää

$$GL(V) = \{\, t : V \longrightarrow V \mid t \text{ on säännöllinen lineaarikuvaus } \}.$$

Yleisesti mitä tahansa ryhmähomomorfismia

$$G \longrightarrow GL_n(\mathbb{C}) \qquad \text{tai} \qquad G \longrightarrow GL(V)$$

sanotaan ryhmän G *esitykseksi* (representation). Esitysten avulla ryhmiä voidaan tutkia matriisien tai lineaarikuvausten teoriaa käyttäen. Tämä ns. ryhmien esitysteoria on osoittautunut hyvin hyödylliseksi sekä itse ryhmäteoriassa että sen sovelluksissa.

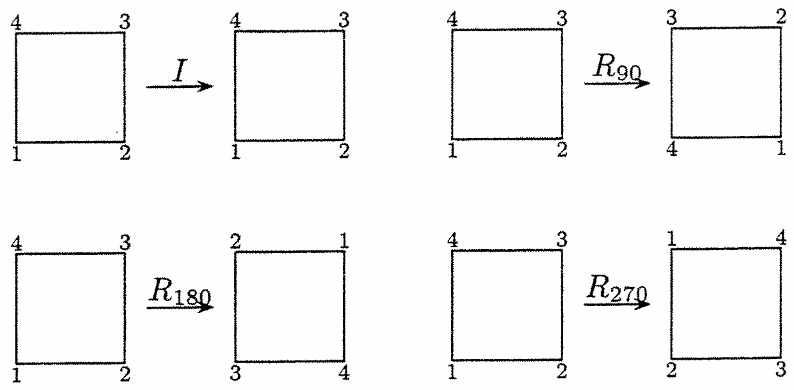
ESIMERKKI 3. Määritetään syklisen ryhmän C_3 säännöllinen (matriisi)esitys.

IV.6 Neliön symmetriaryhmä eli diedriryhmä D_4

Tässä pykälässä havainnollistetaan luvuissa III ja IV esitettyä teoriaa tutkimalla tarkemmin diedriryhmää D_4. Tarkastellaan siis neliötä ${}^d_a\square^c_b$ tason pistejoukkona sekä niitä tason kiertoja ja peilauksia, jotka kuvaavat neliön itselleen. (Katso myös liitteet Symmetriaryhmät ja Matematiikan monet kasvot.)

1. Kierrot

Neliö (tason pistejoukkona) kuvautuu itselleen seuraavissa kierroissa: kulman α kierto neliön keskipisteen ympäri, missä $\alpha = 0,\ \frac{\pi}{2},\ \pi,\ \frac{3\pi}{2}$. Merkitään näitä kiertoja $I = R_0$ (identtinen kuvaus), R_{90}, R_{180}, R_{270}. Merkitsemällä kärkiä 1, 2, 3, 4 saadaan yhteys neljän alkion permutaatioihin: esim. $R_{90} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \in S_4$. Tässä käytetään kuitenkin havaintoon perustuvaa geometrista tarkastelua:



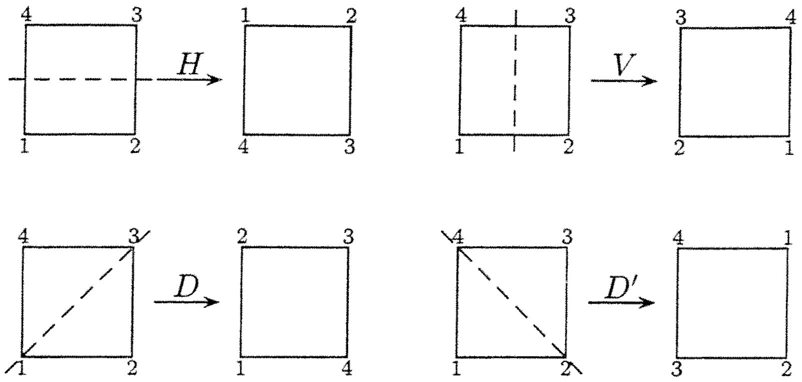
Laskutoimituksena on kuvausten yhdistäminen, esim. $(R_{180}, R_{90}) \mapsto R_{180} \circ R_{90} = R_{270}$. Tällöin on muistettava, että $A \circ B$ tarkoittaa yhdistettyä kuvausta, jossa ensin tehdään B, sitten A. Tämä on tunnetusti assosiatiivinen, neutraalialkio on identtinen kuvaus I, kuvauksilla I, R_{90}, R_{180}, R_{270} on käänteisalkiot (esim. $R_{270}^{-1} = R_{90}$, koska $R_{270} \circ R_{90} = R_{90} \circ R_{270} = I$). Siis $(\{I, R_{90}, R_{180}, R_{270}\}, \circ)$ on ryhmä. Tarkista oheinen kertotaulu ja totea, että siitä näkyy myös ryhmän kommutatiivisuus (taulukko on symmetrinen lävistäjän suhteen). Kertotaulumerkintä on pykälässä III.2 esitetyn mukainen.

	h	g
h		$h \circ g$
g	$g \circ h$	

$\circ$	I	R_{90}	R_{180}	R_{270}
I	I	R_{90}	R_{180}	R_{270}
R_{90}	R_{90}	R_{180}	R_{270}	I
R_{180}	R_{180}	R_{270}	I	R_{90}
R_{270}	R_{270}	I	R_{90}	R_{180}

2. Peilaukset

Neliöllä on täsmälleen neljä symmetria-akselia (ks. kuva) ja se kuvautuu itselleen peilauksissa niiden suhteen: H on peilaus vaaka-akselin suhteen, V peilaus pystyakselin suhteen, D peilaus kärkien 1 ja 3 kautta kulkevan lävistäjän suhteen ja D' peilaus kärkien 2 ja 4 kautta kulkevan lävistäjän suhteen.



Esimerkiksi $(\{I, H\}, \circ)$ muodostaa ryhmän, jonka kertotaulu on

$\circ$	I	H
I	I	H
H	H	I

Vertaa tätä ryhmään $(\mathbb{Z}_2, +)$. Muodostaako $(\{I, H, D\}, \circ)$ ryhmän?

Yhdistämällä em. peilauksia saadaan esim. $H \circ V = R_{180}$ (tarkista seuraamalla, miten kärkipisteet kuvautuvat – montako kärkipistettä riittää?). Peilaukset eivät siis muodosta ryhmää, mutta $(\{I, R_{90}, R_{180}, R_{270}, H, V, D, D'\}, \circ)$ on ryhmä, *neliön symmetriaryhmä* eli *diedriryhmä* D_4 ja sille saadaan kertotaulu:

$\circ$	I	R_{90}	R_{180}	R_{270}	H	V	D	D'
I	I	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	I	D	D'	V	H
R_{180}	R_{180}	R_{270}	I	R_{90}	V	H	D'	D
R_{270}	R_{270}	I	R_{90}	R_{180}	D'	D	H	V
H	H	D'	V	D	I	R_{180}	R_{270}	R_{90}
V	V	D	H	D'	R_{180}	I	R_{90}	R_{270}
D	D	H	D'	V	R_{90}	R_{270}	I	R_{180}
D'	D'	V	D	H	R_{270}	R_{90}	R_{180}	I

Tämä ryhmä ei ole kommutatiivinen (esim. $H \circ R_{270} = D$, $R_{270} \circ H = D'$). Kuvauksia I, R_{90}, R_{180}, R_{270}, H, V, D_1, D' sanotaan neliön *symmetrioiksi.*

Neliön kiertojen ryhmä $G = (\{I, R_{90}, R_{180}, R_{270}\}, \circ)$ on D_4:n aliryhmä, esim. siksi että G todettiin edellä ryhmäksi ja $G \subset D_4$.

3. D_4:n aliryhmät

a) Tutkitaan ensin neliön kiertojen muodostamaa aliryhmää G. Vertaamalla allaolevia taulukoita todetaan, että $(\mathbb{Z}_4, +)$ on isomorfinen ryhmän $(G, \circ)$ kanssa:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

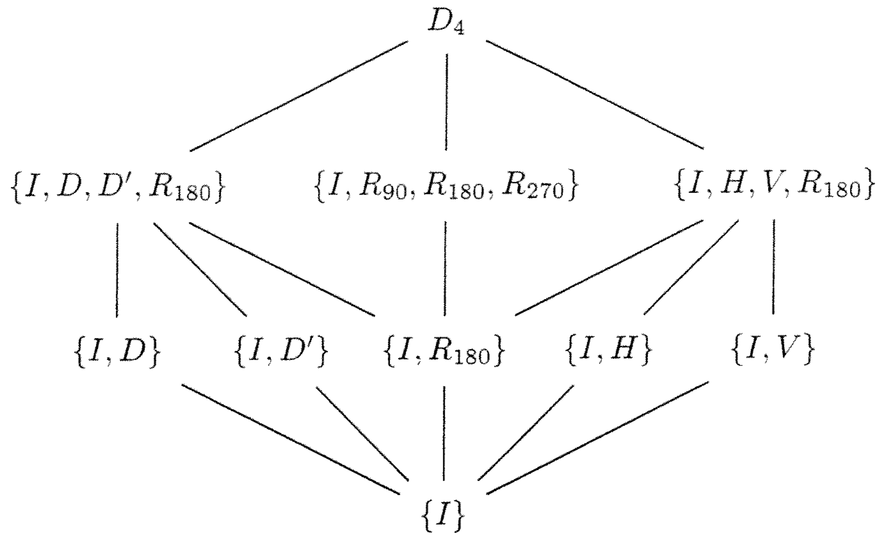
$\circ$	I	R_{90}	R_{180}	R_{270}
I	I	R_{90}	R_{180}	R_{270}
R_{90}	R_{90}	R_{180}	R_{270}	I
R_{180}	R_{180}	R_{270}	I	R_{90}
R_{270}	R_{270}	I	R_{90}	R_{180}

Kuvaus $f : 0 \mapsto I,\ 1 \mapsto R_{90},\ 2 \mapsto R_{180},\ 3 \mapsto R_{270}$ on bijektio $\mathbb{Z}_4 \to G$ ja ryhmähomomorfismi, koska kaikilla $a,\ b \in \mathbb{Z}_4$ on $f(a+b) = f(a) \circ f(b)$. Huomaa myös kaavan $f(x^{-1}) = f(x)^{-1}$ tulkinta (tässä $f(-x) = f(x)^{-1}$), esim. $-3 = 1$ (koska $3+1=0$) ja $f(-3) = f(1) = R_{90} = R_{270}^{-1} = f(3)^{-1}$.

b) G on esimerkki syklisestä ryhmästä, esim. R_{270} virittää sen: käyttämällä tavallista merkintää $R_{270}^2 = R_{270} \circ R_{270}$ saadaan $R_{270}^2 = R_{180}$; $R_{270}^3 = R_{90}$, $R_{270}^4 = I$. Myös R_{90} virittää ryhmän G : $(R_{90})^2 = R_{180}$, $(R_{90})^3 = R_{270}, (R_{90})^4 = I$. Huomaa myös geometria: R_{270} on kulman $-\frac{\pi}{4}$ kierto ja R_{90} on kulman $\frac{\pi}{4}$ kierto, siis R_{270} on kierto negatiiviseen suuntaan ("myötäpäivään"), R_{90} positiiviseen suuntaan ("vastapäivään").

c) D_4:n aliryhmät. Etsitään kaikki D_4:n aliryhmät käyttämättä apuna geometriaa. Helpointa on aloittaa tutkimalla, mitkä ovat D_4:n sykliset aliryhmät, ts. tyyppiä $\{a^n \mid n \in \mathbb{Z}\}$ olevat aliryhmät. Joka tapauksessa ryhmällä on yhden alkion syklinen aliryhmä $\{I\}$. Kahden alkion sykliset D_4:n aliryhmät saadaan ottamalla identtisen kuvauksen lisäksi jokin peilaus tai kierto π:llä (tapaukset, joissa kuvauksen kertaluku on 2 eli kuvaus on oma käänteiskuvauksensa): $\{I, D\}$, $\{I, D'\}$, $\{I, R_{180}\}$, $\{I, H\}$, $\{I, V\}$. (Totea tämä kertotaulusta ja vertaa sitä luvun III.1 harjoitustehtävään 6.) Kolmen alkion syklisiä aliryhmiä ei tässä tapauksessa ole, mutta G on neljän alkion syklinen aliryhmä. Muita syklisiä aliryhmiä ei ole. (Käyttämällä hyväksi tietoa $\#D_4 = 8 = 2\cdot2\cdot2$ saataisiin suoraan tulos, että D_4:llä voi olla vain aliryhmiä, joissa on 1, 2, 4 tai 8 alkiota.)

Kokeilemalla tutkitaan, mitkä ovat D_4:n aliryhmät, jotka eivät ole syklisiä mutta jotka saadaan kahden alkion virittäminä. Olkoon S alkioiden a ja b virittämä. Silloin on oltava a^n, $b^n \in S$ ja $a^i b^j \in S$ aina kun $n, i, j \in \mathbb{Z}$, ja toisaalta näistä alkioista saadaan tässä tapauksessa aliryhmä. Aliryhmän $\{I, D, D', R_{180}\}$ virittäjät ovat D, D' tai D, R_{180} tai D', R_{180}. Aliryhmän $\{I, H, V, R_{180}\}$ virittäjät ovat R_{180}, H tai H, V tai R_{180}, V. Ryhmän D_4 virittäjät ovat R_{270}, H tai D, H tai D', H.



D_4:n aliryhmät järjestettyinä sisältymisrelaation suhteen, eli ryhmän D_4 Hassen kaavio.

Tarkastellaan vielä lähemmin väitettä, että D_4:n virittävät R_{270} ja H:

$$R_{270}^0 = I,\ R_{270} = R_{270},\ R_{270}^2 = R_{180},\ R_{270}^3 = R_{90},\ H = H,$$
$$R_{270} \circ H = D',\ R_{270}^2 \circ H = V,\ R_{270}^3 \circ H = D,$$
$$R_{270}^4 = I,\ H^2 = I.$$

Kaikki ryhmän D_4 alkiot voidaan esittää yksikäsitteisesti muodossa

$$R_{270}^j H^i, \qquad j = 0, 1, 2, 3, \quad i = 0, 1.$$

Tämän varmistamiseksi on huomattava, että

$$H \circ R_{270} = R_{270}^3 \circ H, \quad R_{270}^4 = I, \quad H^2 = I$$

(ns. *relaatiot*). Esim.

$$\begin{aligned} V \circ D' &= (R_{270}^2 \circ H) \circ (R_{270} \circ H) = R_{270}^2 \circ (H \circ R_{270}) \circ H \\ &= R_{270}^2 \circ R_{270}^3 \circ H \circ H = R_{270} \circ H^2 = R_{270} \circ I = R_{270} \end{aligned}$$

.

4. Sivuluokat

Määritetään suoraan laskemalla, nojautumatta yleiseen teoriaan, mitkä ovat aliryhmän $S = \{I, H\}$ vasemmanpuoleiset sivuluokat. Nämä ovat siis tyyppiä $x \circ S$, $x \in D_4$:

$$
\begin{aligned}
I \circ \{I, H\} &= \{I, H\}, \\
R_{180} \circ \{I, H\} &= \{R_{180} \circ I, R_{180} \circ H\} = \{R_{180}, V\}, \\
R_{270} \circ \{I, H\} &= \{R_{270}, R_{270} \circ H\} = \{R_{270}, D'\}, \\
R_{90} \circ \{I, H\} &= \{R_{90}, R_{90} \circ H\} = \{R_{90}, D\}, \\
H \circ \{I, H\} &= \{H, I\}, \ V \circ \{I, H\} = \{V, R_{180}\}, \\
D \circ \{I, H\} &= \{D, R_{90}\}, \ D' \circ \{I, H\} = \{D', R_{270}\}.
\end{aligned}
$$

Siis S:n vasemmanpuoleiset sivuluokat ovat $\{I, H\}$, $\{R_{180}, V\}$, $\{R_{270}, D'\}$ ja $\{R_{90}, D\}$. S ei ole normaali, koska esim. $R_{270} \circ \{I, H\} = \{R_{270}, D'\}$ ja $\{I, H\} \circ R_{270} = \{R_{270}, H \circ R_{270}\} = \{R_{270}, D\}$.

Lopuksi todetaan, että on saatu ryhmän D_4 ositus neljään sivuluokkaan, joissa kussakin on kaksi alkiota. Koska $2 \cdot 4 = 8$, näin pitääkin olla. (Minkä lauseen perusteella?)

5. D_4:n keskus

Määritetään joukko $N = \{x \in D_4 \mid x \circ y = y \circ x \quad \forall y \in D_4\}$. Kertotaulusta nähdään, että $N = \{I, R_{180}\}$. N on normaali aliryhmä, koska $y \circ N = N \circ y$, $\forall y \in D_4$. Nyt sivuluokat ovat

$$
\begin{aligned}
I \circ N &= R_{180} \circ N = \{I, R_{180}\}, \\
R_{270} \circ N &= R_{90} \circ N = \{R_{270}, R_{90}\}, \\
H \circ N &= V \circ N = \{H, V\}, \\
D \circ N &= D' \circ N = \{D, D'\}
\end{aligned}
$$

ja esim. $R_{270} \circ \{I, R_{180}\} = \{R_{270}, R_{90}\} = \{I, R_{180}\} \circ R_{270}$. Koska $\{I, R_{180}\}$ on normaali aliryhmä, voidaan muodostaa tekijäryhmä

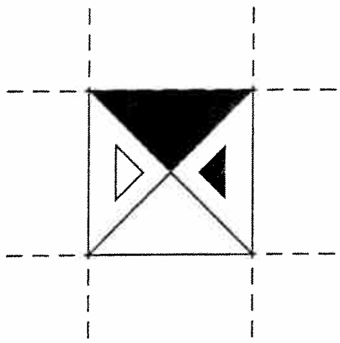
$$D_4/N = \big\{\{R_{270}, R_{90}\}, \{H, V\}, \{D, D'\}, \{I, R_{180}\}\big\}.$$

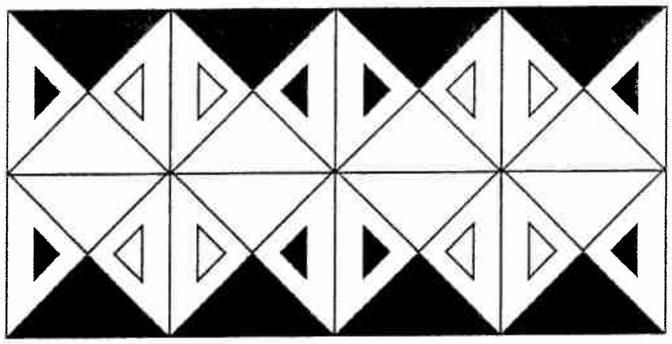
Laskutoimitus on $(x \circ N) \circ (y \circ N) = (x \circ y) \circ N$.

(Esim. $\{R_{270}, R_{90}\} \circ \{H, V\} = (R_{270} \circ N) \circ (H \circ N) = (R_{270} \circ H) \circ N = D' \circ N = \{D, D'\}$.)
Projektio $\pi : D_4 \to D_4/N$ on homomorfismi, $\pi(x) = x \circ N$, $\quad \mathrm{Ker}(\pi) = N$.

6. Ornamentit

Säännöllisten geometristen kuvioiden symmetriaryhmiä käytetään mm. ornamenttikoristelussa.

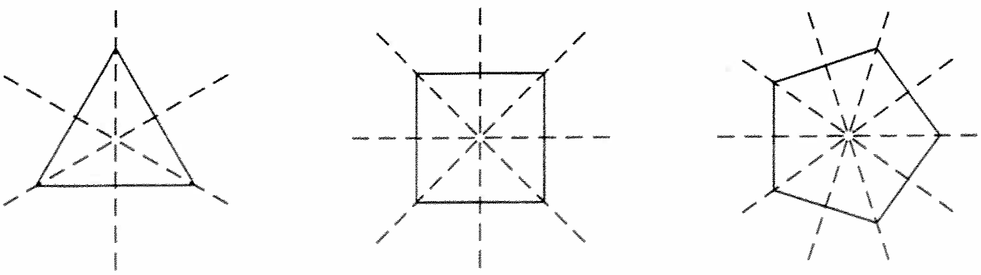




Peilaamalla neliön sivujen suhteen (peilausakselit merkitty pilkkuviivoilla), saadaan taso peitetyksi ylläolevalla tavalla neliönkuvilla. Huomaa, että yhdistämällä peilaukset vaaka- ja pystyakselin suhteen saadaan kulman π suuruinen kierto neliön kärjen ympäri (edellä $H \circ V = V \circ H = R_{180}$).

7. D_n ja C_n

D_n on säännöllisen n-kulmion symmetriaryhmä, kun $n \geq 3$. Ryhmällä D_n on syklinen aliryhmä C_n, jonka virittää kierto R kulman $2\pi/n$ verran n-kulmion keskipisteen ympäri; siis $R^n = I$. Lisäksi ryhmään D_n kuuluvat peilaukset n-kulmion symmetria-akselien suhteen.



$n = 3$ $n = 4$ $n = 5$

Jos merkitään peilausta jonkin symmetria-akselin suhteen H:lla, niin ryhmässä D_n ovat voimassa relaatiot $H^2 = I$, $R^n = I$ ja kuvaukset H ja R virittävät ryhmän D_n.