Aksel Bertelsen

OM AT PERMUTERE

Version 2, december 2023.

Indhold

Forord

For nogle år siden skrev jeg en artikel, *Ruffinis umulighedsbeviser og ikosaederet*, som nåede at udkomme i det allersidste nummer af det matematiske tidsskrift *Normat*. Artiklen begyndte således: Jeg har ofte fortalt elever i gymnasiet, at der udover formlen for andengradsligningen, findes formler til løsning af tredje- og fjerdegradsligninger, men at man kan bevise, at der ikke kan laves en tilsvarende formel for femtegradsligningen. Når en elev har undret sig og gerne har villet se bare antydningen af et bevis, har jeg måtte skuffe vedkommende og sagt, at det er for kompliceret, og at sådanne beviser fylder flere hundrede sider.

Artiklen var et forslag til, hvordan man måske alligevel kunne forklare eller i hvert fald give en ide om, hvorfor det er umuligt at lave en formel til løsning af femtegradsligninger. Den var især henvendt til gymnasielærere, men nu har jeg fået lyst til at give en fremstilling, som vil være nemmere at læse for elever med interesse for emnet. Det betyder bl.a. andet, at der er lagt ekstra vægt på forståelse af regning med permutationer, og de første kapitler kan bruges som en introduktion til at arbejde med permutationer.

Noterne handler ikke så meget om at beregne antal permutationer som i kombinatorikken, men mere om de algebraiske strukturer man møder, når man regner med permutationer. Der forudsættes stort set kun kendskab til funktionsbegrebet, vektorer i en plan og ligninger af højest anden grad.

Inden det sidste nummer udkom, havde *Normat* skrantet i adskillige år, og mængden af abonnenter var skrumpet voldsomt, så der var ikke mange, som fik mulighed for at læse min artikel. Ved at lægge disse noter ud på nettet bliver artiklen, om end i en lidt anden form, tilgængelig for en større kreds.

Aksel Bertelsen, Tjæreby 2021.

Billedet på første side er en gengivelse af *Interiør med kortspillende børn* malet af Hugo Salmson (1843-1894).

1. PERMUTATIONER

Ordene permutation og at permutere er dagligdags ord på andre sprog som f.eks. engelsk, fransk og italiensk, hvor de betyder omplacering og at omplacere, eller ombytning og at bytte rundt på. Det var matematikere fra disse lande, der begyndte at arbejde systematisk med permutationer i slutningen af 1700-tallet.

I begyndelsen blev ordene brugt i deres dagligdags betydning, og man kunne f.eks. skrive: hvis man i udtrykket

$$x + xy - z^2$$

permuterer de variable x og z, får man udtrykket

$$z + zy - x^2.$$

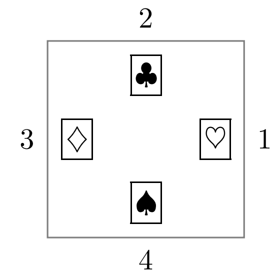
Her er meningen klar nok: man bytter om på x og z. Man kan imidlertid bytte rundt på de variable på andre måder end ved bare at ombytte to af dem, og så var tingene ikke altid helt så enkle. Princippet bag ombytningerne blev ikke altid klart formuleret, og det er stadigvæk sådan, at man kan komme ud i problemer, hvis man ikke gør sig klart, hvad sådanne ombytninger består i.

Hvordan man fra at arbejde med ombytninger i en dagligdags betydning af ordet kommer frem til en præcis definition af, hvad en permutation skal betyde i matematik, vil blive illustreret i dette første kapitel.

Operationer, der flytter rundt på nogle matematiske objekter, lærer de fleste tidligt at kende i geometrien, hvor man arbejder med f.eks. at spejle og at parallelforskyde punkter. Disse geometriske operationer kaldes under ét for afbildninger. Afbildningsbegrebet er også centralt i forbindelse med permutationer, men man bruger normalt kun ordet permutation, når man afbilder *endelige* mængder på sig selv.

Opstillinger

Vi ser på en situation, hvor fire kortspillere sidder ved et bord, hver med ét kort i hånden. Spillerne sidder på pladser med numrene 1, 2, 3 og 4. De fire kort er esserne i hjerter, klør, ruder og spar, og de er placeret som vist på figuren nedenfor til venstre.



$p:$

$\heartsuit$	$\clubsuit$	$\diamondsuit$	$\spadesuit$
1	2	3	4

Fordelingen af kortene kan også angives ved tabellen ovenfor til højre. Denne tabel kan opfattes som en forskrift for en *afbildning* p, der til hvert af de fire kort knytter den plads, hvor kortet sidder. En sådan afbildning vil vi kalde en *opstilling* af kortene.

Vi vil kun interessere os for kortfordelinger, hvor der på hver plads sidder netop ét kort, hvilket betyder, at den tilhørende opstilling er en *bijektiv* afbildning.

Hvis A er en vilkårlig mængde med n elementer, defineres en *opstilling* af elementerne i A som en bijektiv afbildning p af A på $\{1, 2, , \dots, n\}$, altså en afbildning p, der til hvert element x i A knytter et tal $p(x)$ i mængden $\{1, 2, , \dots, n\}$, således at der ikke er to forskellige elementer x og y for hvilke $p(x) = p(y)$. Tallet $p(x)$ kaldes *billedet* af x.

Når vi arbejder med opstillinger, vil vi kalde elementerne i A for *genstande*, og tallene $1, 2, , \dots, n$ for *pladser*. At $p(x) = y$ skal altså forstås sådan, at genstanden x befinder sig på plads y.

Af og til vil en opstilling blive angivet ved kun at vise en række af n genstande, og da vil det være underforstået, at de står på pladserne $\{1, 2, , \dots, n\}$. I tabellen for p i korteksemplet kunne man altså nøjes med den øverste række. I stedet for at sætte kasser om genstandene kan man også skrive opstillingen som vist nedenfor.

$$p : (\heartsuit, \clubsuit, \diamondsuit, \spadesuit)$$

Samtlige opstillinger af A udgør en mængde, der betegnes $O(A)$. Af multiplikationsprincippet følger, at antallet af opstillinger i $O(A)$ er $n!$, altså $n(n-1)(n-2)\ldots 2\cdot 1$. Der er nemlig n muligheder for, hvad der kan stå på plads 1, og dernæst $n-1$ muligheder for hvad der kan stå på plads 2, da der ikke må stå den samme genstand som på plads 1, osv.

Mens $p(x)$ angiver, hvor en genstand befinder sig, angiver $p^{-1}(y)$ hvilken genstand, der befinder sig på plads y.

Permutationer

Vi forestiller os nu, at kortene omfordeles ved, at hver spiller giver sit kort til naboen til højre. Den oprindelige opstilling p bliver derved erstattet af en ny opstilling q:

p:

$\heartsuit$	$\clubsuit$	$\diamondsuit$	$\spadesuit$
1	2	3	4

q:

$\spadesuit$	$\heartsuit$	$\clubsuit$	$\diamondsuit$
1	2	3	4

Hvordan man kommer fra p til q kan beskrives matematisk ved hjælp af en funktion σ defineret ved, at $\sigma(i)$ er lig med den plads, som kortet på plads i flyttes hen til. Nedenfor er vist en tabel med funktionsværdierne for σ.

i	1	2	3	4
$\sigma(i)$	2	3	4	1

Når f.eks. $\sigma(1) = 2$ vil man med sprogbrug for afbildninger kort sige, at 1 går over i 2, men i den konkrete praktiske situation betyder det altså, at kortet på plads 1 kommer hen på plads 2.

Funktionen σ kan kaldes en *permutation*, idet en permutation generelt defineres på følgende måde:

> En *permutation* er en bijektiv afbildning af en endelig mængde på sig selv.

Vi kommer næsten udelukkende til at beskæftige os med permutationer af tallene $1, 2, , \ldots, n$. Disse permutationer udgør en mængde, der kaldes S_n, eller *den symmetriske gruppe*, og vi vender tilbage til denne betegnelse på side 32.

Af multiplikationsprincippet følger, at antallet af permutationer i S_n er $n!$, altså $n(n-1)(n-2)\ldots 2\cdot 1$. Der er nemlig n muligheder for, hvad billedet af 1 kan være, og dernæst $n-1$ muligheder for hvad billedet af 2 kan være, osv.

I stedet for at angive en funktionstabel med kasser som på forrige side, bruger man i forbindelse med permutationer følgende, lidt kortere, skrivemåde:

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

Man siger, at permutationen på denne måde angives ved brug af *tabelnotation.* Det bemærkes, at man får samme forskrift, hvis man bytter rundt på søjlerne i funktionstabellen. For eksempel kan σ også angives som

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

Definitionen ovenfor siger ikke noget om, hvad en permutation gør ved en given opstilling, men fortæller bare hvilken slags matematisk størrelse, der er tale om.

Vi skal nu se, hvordan man rent matematisk kort kan udtrykke, hvordan man ud fra en given opstilling p i $O(A)$ og en given permutation σ i S_n kan få en ny opstilling i $O(A)$.

Da både p og σ er bijektive, vil den sammensatte afbildning $\sigma \circ p$ også være bijektiv, og den vil afbilde A på $\{1, 2, , \dots, n\}$. Afbildningen $\sigma \circ p$ vil altså være en ny opstilling i $O(A)$. Denne afbildning vil vi for det meste bare betegne σp.

I eksempel med kortspillerne havde vi:

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

p :

♡	♣	♢	♠
1	2	3	4

Ved at udregne $\sigma p(x) = \sigma \circ p(x) = \sigma(p(x))$ for alle x får man:

σp :

♡	♣	♢	♠
2	3	4	1

Man kan ordne søjlerne i forskriften, så tallene i anden række står i stigende orden:

σp :

♠	♡	♣	♢
1	2	3	4

Man siger, at man får σp ved at permutere p med σ, eller at man *anvender* σ på p, eller at man lader permutationen σ *virke* på p.

Når vi generelt går fra en opstilling p til opstillingen σp, vil man i praksis kunne sige, at

$$\boxed{\sigma \text{ fører genstanden på plads } i \text{ hen på plads } \sigma(i).}$$

Hvis nemlig $p(x) = i$, vil der gælde, at $\sigma p(x) = \sigma(p(x)) = \sigma(i)$.

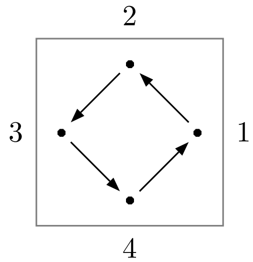
Når en opstilling er angivet på formen (a, b, c, d), og σ er som i korteksemplet, kan man bare skrive

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} (a, b, c, d) = (d, a, b, c),$$

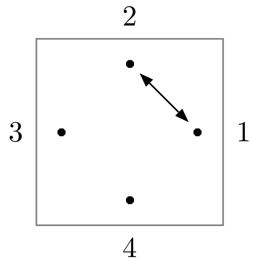
altså uden mellemregninger, idet man i praksis bruger, at σ fører genstanden på plads i hen på plads $\sigma(i)$, så genstanden på plads 1 kommer hen på plads 2, osv.

Pilefigurer

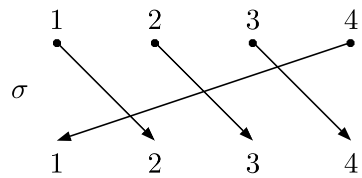
Permutationen σ i korteksemplet kan illustreres med en *pilefigur* som vist nedenfor. Der går en pil fra i til j, hvis $\sigma(i) = j$, og det betyder i praksis, at kortet på plads i flyttes hen til plads j.



En anden permutation π af kortene kunne ske ved, at spillerne på plads 1 og 2 bytter kort, mens de to andre spillere beholder deres kort. Denne permutation kan illustreres med følgende pilefigur, hvor der er lavet et isoleret punkt, når $\pi(i) = i$.



Der kan laves andre typer af pilefigurer. F.eks. kan permutationen σ illustreres på følgende måde:



Pilefigurer er som regel kun nyttige, når der er relativt få pladser, ellers bliver de let uoverskuelige.

Produkt af permutationer

Man kan sammensætte to permutationer σ og π i S_n ligesom man sammensætter afbildninger. Det vil sige, at man får en ny permutation $\pi\circ\sigma$ givet ved:

$$\pi\circ\sigma(i) = \pi(\sigma(i)).$$

I stedet for $\pi\circ\sigma$ skriver man ofte bare $\pi\sigma$, og kalder $\pi\sigma$ for et *produkt* af π og σ. Ser vi f.eks. på

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

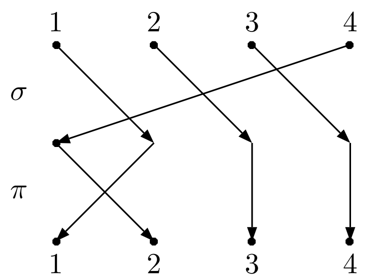
kan vi udregne $\pi\sigma(1)$ på følgende måde

$$\pi\sigma(1) = \pi\circ\sigma(1) = \pi(\sigma(1)) = \pi(2) = 1.$$

Med andre ord går 1 først over i 2 ved σ, og så går 2 over i 1 ved π. Samlet får man

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

I korteksemplet vil $\pi\sigma$ svare til at der laves en rotation af kortene på pladserne 2, 3 og 4.



Man kan illustrere sammensætningen af permutationerne ved brug af to pilefigurer, som vist ovenfor.

Produktet er ikke *kommutativt*, da der ikke altid gælder, at $\sigma\pi$ er lig med $\pi\sigma$. Udregnes i eksemplet $\sigma\pi$, får man

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

altså noget andet end $\pi\sigma$.

Den *associative* lov gælder imidlertid, d.v.s. at

$$(\mu\pi)\sigma = \mu(\pi\sigma), \tag{1}$$

for alle σ, π og μ i S_n, da loven gælder for sammensætning af funktioner generelt. Man kan altså undlade parenteserne og bare skrive $\mu\pi\sigma$, når man ganger tre permutationer.

Blandt permutationerne i S_n er der en, hvor alle tal går over i sig selv. Denne permutation kaldes den *neutrale permutation* eller *identiteten*. Den svarer i praksis til, at man lader alle genstande blive på deres plads, og det kan virke forkert at tale om en permutation, når der ikke sker ændringer, men vi skal se, at det er nyttigt at inddrage den type. Den neutrale permutation vil vi kalde ϵ. F.eks. har vi S_4:

$$\epsilon = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

Navnet neutral permutation kommer af, at når man ganger en vilkårlig permutation σ med ϵ, får man igen σ:

$$\epsilon\sigma = \sigma\epsilon = \sigma \tag{2}$$

Til enhver permutation σ hører en *invers* permutation σ^{-1}, der løst sagt gør det omvendte af σ i den forstand, at de to ophæver hinanden. Mere præcist skal gælde, at $\sigma\sigma^{-1} = \epsilon$ og $\sigma^{-1}\sigma = \epsilon$. Forskriften for σ^{-1} får man ved at bytte om på de to rækker i forskriften for σ, som i det følgende eksempel.

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

Vi får ofte brug for, at der generelt gælder, at

$$(\pi\sigma)^{-1} = \sigma^{-1}\pi^{-1} \tag{3}$$

Dette følger af, at $\pi\sigma\sigma^{-1}\pi^{-1} = \epsilon$, da der både gælder, at $\sigma\sigma^{-1}$ er lig med ϵ, og at $\pi\pi^{-1}$ er lig med ϵ.

Opstillingspar

Når man har et par af opstillinger (p, q), hvor p og q begge tilhører $O(A)$, kan vi finde en permutation σ i S_n, så $\sigma p = q$. Ganges nemlig fra højre med p^{-1} på begge sider får man, at

$$\sigma = qp^{-1} \tag{4}$$

som er en bijektiv afbildning, der afbilder $\{1, 2, , \dots, n\}$ på sig selv, og som derfor tilhører S_n. Ser vi som eksempel igen på

p :

$\heartsuit$	$\clubsuit$	$\diamondsuit$	$\spadesuit$
1	2	3	4

q :

$\spadesuit$	$\heartsuit$	$\clubsuit$	$\diamondsuit$
1	2	3	4

får vi følgende permutation, som vi har mødt nogle gange:

$$qp^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Generelt vil vi sige, at et ordnet par (p, q) af opstillinger fra $O(A)$ udgør et *opstillingspar*.

Forskellige opstillingspar kan give samme permutation. Som eksempel kan man tage

p_1 :

$\diamondsuit$	$\clubsuit$	$\heartsuit$	$\spadesuit$
1	2	3	4

q_1 :

$\spadesuit$	$\diamondsuit$	$\clubsuit$	$\heartsuit$
1	2	3	4

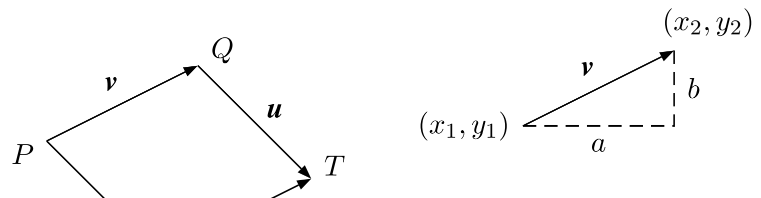
Dette opstillingspar giver samme permutation som p og q ovenfor, nemlig en cyklisk forskydning med en plads til højre.

Permutationer og vektorer

Sammenhængen mellem opstillinger, opstillingspar og permutationer har mange lighedspunkter med relationerne mellem punkter, pile og *vektorer* i geometrien. I dette afsnit laves en sammenligning af de to områder, som forhåbentligt kan tydeliggøre permutationernes rolle.

Vi vil lade opstillinger svare til punkter i en plan. I vektorregningen kaldes et ordnet par af punkter for en *pil*, og parret bliver også illustreret med en sådan. Når to opstillinger svarer til to punkter, vil et opstillingspar svare til en pil. En vektor defineres i geometrien som en mængde af pile, der er ensrettede og lige lange. Det svarer til, at en permutation kan opfattes som mængden af opstillingspar (p, q) med en vis fælles egenskab, nemlig at de har samme qp^{-1}.

I vektorregningen kaldes en pil for en *repræsentant* for en vektor, og et opstillingspar kan på tilsvarende måde kaldes en repræsentant for en permutation.

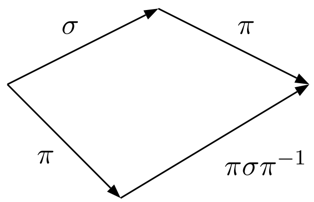


$$\boldsymbol{v} = \begin{pmatrix} a \\ b \end{pmatrix}$$

En pil angives ved to koordinatsæt, nemlig koordinaterne til begyndelses- og slutpunktet, mens den vektor, som pilen repræsenterer, angives ved et koordinatsæt, der fortæller, hvordan man kommer fra det ene punkt til det andet. Tilsvarende har man til et opstillingspar to tabeller, mens den tilhørende permutation angives ved bare en tabel, der fortæller, hvordan man kommer fra den ene opstilling til den anden.

For punkter og vektorer gælder følgende regel om hjørnerne P, Q, S og T i et parallelogram (se figur forrige side): Hvis pilen fra P til Q er en repræsentant for en vektor $\boldsymbol{v}$, og pilen fra S til T også er en repræsentant for $\boldsymbol{v}$, så vil pilen fra P til S og pilen fra Q til T begge være repræsentanter for en vektor $\boldsymbol{u}$. Reglen hænger sammen med, at den kommutative lov gælder for sum af vektorer.

En tilsvarende regel gælder ikke for to opstillingspar, da den kommutative lov ikke gælder for produkt af permutationer. Det tætteste, man kan komme, er følgende.



For givne σ og π kan man finde en permutation μ, så $\mu\pi = \pi\sigma$ ved at isolere μ, hvilket giver $\mu = \pi\sigma\pi^{-1}$. Man siger, at $\pi\sigma\pi^{-1}$ er den *konjugerede* af σ ved π, og at $\pi\sigma\pi^{-1}$ og σ er konjugerede.

Nedenfor er vist et eksempel, hvor σ er (12)(34), og π er (23).

$$\begin{tikzcd}
(\heartsuit, \clubsuit, \diamondsuit, \spadesuit) \arrow[r, "1 \leftrightarrow 2\,,\, 3 \leftrightarrow 4"] \arrow[d, "2 \leftrightarrow 3"'] & (\clubsuit, \heartsuit, \spadesuit, \diamondsuit) \arrow[d, "2 \leftrightarrow 3"] \\
(\heartsuit, \diamondsuit, \clubsuit, \spadesuit) \arrow[r, "1 \leftrightarrow 3\,,\, 2 \leftrightarrow 4"] & (\clubsuit, \spadesuit, \heartsuit, \diamondsuit)
\end{tikzcd}$$

I næste kapitel vises, hvad to konjugerede permutationer har til fælles.

Andre anvendelser af ordet permutation

Ordet permutation bruges desværre på flere forskellige måder i matematik. I kombinatorik er en permutation oftest bare en konkret opstilling af nogle genstande i rækkefølge, altså det vi har kaldt en opstilling, som f.eks. (b, d, a, c).

Kombinatorikkens permutationer kaldes nogle steder *passive permutationer*, i modsætning til de *aktive* permutationer, som vi har set på, hvor en permutation beskriver en proces, der frembringer en opstilling ud fra en given opstilling.

Permutationer baseret på genstande

Når det drejer sig om aktive permutationer kan man også arbejde med flere forskellige typer. Indtil nu har vi set på permutationer baseret på pladser, men man kan også arbejde med permutationer baseret på genstande. Som eksempel kan vi i situationen med de fire kortspillere forestille os, at spilleren med hjerter beder om at få byttet kort med den spiller, der har en ruder, ligegyldigt hvor hjerteren og ruderen sidder.

Permutationer baseret på genstande kan på mange måder behandles ligesom permutationer baseret på pladser, men for at undgå at blande tingene sammen, holder vi os for det meste til permutationer baseret på pladser.

I opgave 1.7 er en kort introduktion til permutationer baseret på genstande, og det fremgår heraf, at hvis man nummererer genstandene med tallene $1, 2, \ldots, n$ kan disse permutationer også udtrykkes ved permutationer i S_n.

Det er kun, når man lader permutationer virke på opstillinger, at der er forskel på om permutationerne er baseret på pladser eller genstande. Ser man på regning med permutationerne selv er der ingen forskel; her bruges bare, at der er tale om en bijektiv afbildning af en endelig mængde på sig selv.

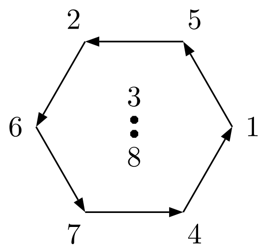
2. CYKLER OG GRUPPER

Vi skal i første del af dette kapitel se, at der findes en særlig simpel type permutationer, *cykler*, som er byggesten for samtlige permutationer. At cyklerne er byggesten betyder, at enhver permutation kan skrives som et produkt af cykler. Ved at arbejde med cykler kan man forenkle både opskrivning af permutationer og regning med permutationer.

Et eksempel på en cykel er følgende permutation i S_8:

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

Vi kan placere tallene således, at man får en pilefigur af σ som vist på figuren nedenfor.



De to *fixpunkter*, altså de to tal, der afbildes over i sig selv ved σ, er placeret i centrum. De øvrige tal er placeret på en cirkel, et hjul, således at man ser, at σ laver en rotation med én plads i positiv omløbsretning, altså mod uret.

De tal, der ikke er fixpunkter, kan vi indicere således

1	5	2	6	7	4
c_1	c_2	c_3	c_4	c_5	c_6

Der gælder da, at $\sigma(c_i) = c_{i+1}$ for alle i fra 1 til 5, og $\sigma(c_6) = c_1$. Det er denne egenskab, der karakteriserer cykler, og den, der giver en pilefigur af samme type som ovenfor.

Generelt kaldes en permutation σ i S_n for en *m-cykel* eller en *cykel af længde m*, hvis de tal, der ikke er fixpunkter, udgør en mængde C, der kan skrives $C = \{c_1, c_2, \dots, c_m\}$, således at

$$\sigma(c_1) = c_2,\ \sigma(c_2) = c_3,\ \dots, \sigma(c_{m-1}) = c_m,\ \sigma(c_m) = c_1$$

En sådan permutation vil vi skrive i den såkaldte *cykelnotation* som $(c_1\ c_2\ \dots c_m)$, og σ i eksemplet bliver så til

$$\sigma = (\,1\,5\,2\,6\,7\,4\,).$$

Man kan illustrere σ med en pilefigur som den nedenfor

$$1 \to 5 \to 2 \to 6 \to 7 \to 4 \to 1$$

Da permutationen er en rotation, er det ligegyldigt, hvilket tal, der står først, så man kan også skrive f.eks. $\sigma = (\,6\,7\,4\,1\,5\,2\,)$.

Fixpunkterne indgår ikke i cykelnotationen, så en 3-cykel som $(\,1\,3\,2\,)$ kan tilhøre S_3, men også f.eks. S_5, idet 4 og 5 så er fixpunkter. Med de tal, der *indgår* i en given cykel, menes dem, der ikke er fixpunkter.

I en 1-cykel er alle tal fixpunkter, så det er en neutral permutation. En sådan har vi kaldt ϵ, men bruges cykelnotation, kan den også betegnes (1). En 2-cykel ombytter to tal, og den kaldes en *transposition*.

For en m-cykel σ vil der gælde, at $\sigma^m = (1)$. Tager man nemlig udgangspunkt i et vilkårligt i på den tilhørende pilefigur, er det klart, at $\sigma^r(i)$ vil gennemløbe hele cyklen, når r løber fra 0 til $m-1$, og at $\sigma^m(i) = i$.

Den inverse til en m-cykel $\gamma = (c_1\ c_2\ \dots\ c_m)$ vil være

$$\gamma^{-1} = (c_m\ c_{m-1}\ \dots\ c_2\ c_1),$$

idet produktet af $(c_1\ c_2\ \dots\ c_m)$ og $(c_m\ c_{m-1}\ \dots\ c_2\ c_1)$ er (1) ligegyldigt hvilken faktor, der står først. Specielt er γ^{-1} altså også en m-cykel.

Opspaltning i disjunkte cykler

To cykler i S_n kaldes *disjunkte*, hvis der ikke er noget tal, der indgår i begge cykler. Der gælder følgende sætning:

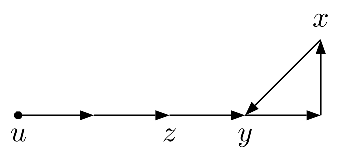
Enhver permutation kan skrives som et produkt af disjunkte cykler.

Det følgende eksempel viser, hvordan man får skrevet en permutation i S_8 som et produkt af disjunkte cykler, men forklarer samtidigt hvorfor det generelt vil kunne lade sig gøre. Vi sætter

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

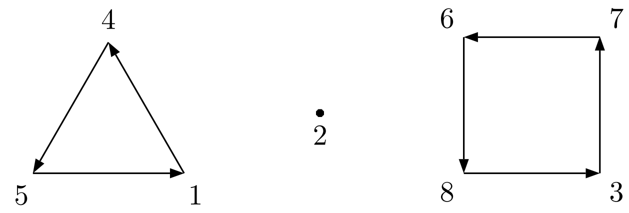
Man tager udgangspunkt i tallet 1, og ser at $\sigma(1) = 4$. Dernæst ser man, at $\sigma(4) = 5$, og at $\sigma(5) = 1$, således at man er tilbage ved udgangspunktet. Vi har på denne måde fået cyklen $(1\ 4\ 5)$, og vi kan sige, at 1 *frembringer* denne cykel. Den består af tal af formen $\sigma^r(1)$, hvor $r{=}1, 2, 3$.

Ligegyldigt hvilket udgangspunkt u, der vælges, vil man efter et endeligt antal trin være tilbage ved udgangspunktet, når man bevæger sig frem i talfølgen $\sigma^r(u)$ med $r = 0, 1, 2, \ldots$. Man kan nemlig ikke blive ved med at få et nyt tal, da mængden af mulige talværdier er endelig, så på et tidspunkt vil man have et x og $y = \sigma(x)$, hvor y er et af de tal, som man har haft.



Hvis y ikke er tallet u, vil der undervejs være et z, så $\sigma(z) = y$. Men så er $\sigma(z) = \sigma(x)$, hvilket er umuligt, da σ er bijektiv. Altså er $y{=}u$, så man når tilbage til udgangspunktet.

Blandt de resterende tal vælges det mindste, som er 2. Dette tal frembringer en 1-cykel. Det mindste tal blandt de resterende er nu 3, som frembringer 4-cyklen $(3\ 7\ 6\ 8)$. Vi har da cyklerne:



Man kan skrive σ som et produkt af disse tre cykler:

$$\sigma = (145)(2)(3768) \tag{5}$$

men meget ofte udelader man 1-cyklerne, som er neutrale, så:

$$\sigma = (145)(3768) \tag{6}$$

Enhver permutation σ kan på denne måde skrives som et produkt af disjunkte cykler. De disjunkte cykler, der indgår i produktet, kan kun vælges på én måde, og de er altså entydigt bestemt. Man kan derfor tale om *cykelfremstillingen*, altså i bestemt form, af en permutation. Det skal dog bemærkes, at faktorerne kan skrives i forskellig rækkefølge, og at 1-cykler både kan indgå eller udelades.

At faktorerne kan skrives i forskellig rækkefølge hænger sammen med, at to disjunkte cykler γ og δ kommuterer, dvs at $\gamma\delta = \delta\gamma$. Dette følger umiddelbart af, at der bortset fra fixpunkter ikke er nogen fælles tal i de to disjunkte cykler. I eksemplet ovenfor har man f.eks. også, at $\sigma = (3768)(145)$.

Antallet af cykler i en cykelfremstilling af σ med samtlige cykler, altså også 1-cykler, kaldes $c(\sigma)$. I eksemplet ovenfor får man altså $c(\sigma) = 3$.

Regning med cykler

Når man ganger to permutationer ud fra deres cykelfremstillinger, er det naturligt også at angive produktet ved en cykelfremstilling. Dette opnår man som vist i det følgende eksempel, hvor

$$\pi = (125)(34) \qquad \sigma = (13)(24)$$

Først finder vi billedet af 1 ved $\pi\sigma$ ved at starte med det 1-tal, der står bagerst. Vi noterer, at det går over i 3. Dernæst finder vi 3 i den nærmest foranstående cykel og noterer, at det går over i 4. Der er ikke noget foranstående 4-tal, så ved $\pi\sigma$ går 1 over i 4. På tilsvarende måde får man, at 4 ved $\pi\sigma$ går over i 5, at 5 går over i 1, at 3 går over i 2, og endeligt at 2 går over i 3. Så

$$\pi\sigma = (145)(23)$$

Ofte vil man udregne produkter ud fra cykelfremstillinger, fordi de er pladsbesparende og overskuelige.

Permutationer som produkt af transpositioner

Enhver cykel $\gamma = (c_1\ c_2\ \cdots\ c_m)$, hvor $m \geq 2$, kan skrives som et produkt af transpositioner på følgende måde

$$(c_1\ c_2\ c_3\ \cdots\ c_m) = (c_1\ c_2)(c_2\ c_3)\ldots(c_{m-1}\ c_m).$$

Dette kan man kontrollere ved at se efter, hvad der sker med hvert c_i på begge sider af lighedstegnet. Det betyder, at en rotation af m genstande i en cirkel i praksis kan laves ved $m-1$ parvise ombytninger.

Da enhver permutation kan skrives som et produkt af cykler, kan enhver permutation altså også skrives som et produkt af transpositioner. Faktorerne i dette produkt er imidlertid ikke entydigt bestemt.

Cykelstruktur

Ved *cykelstrukturen* af en permutation σ forstås en angivelse af længden af de cykler, der fremkommer i cykelfremstillingen, hvor samtlige cykler indgår. Længderne vil vi skrive adskilt med kommaer i kantede parenteser i aftagende orden. For eksempel vil (125)(367)(49) have cykelstrukturen [3,3,2,1] i S_9.

Samtlige permutationer i S_n kan opdeles i klasser bestående af de permutationer, der har samme cykelstruktur. I S_3 vil der være 3 klasser svarende til cykelstrukturerne [1,1,1], [2,1] og [3] med henholdsvis 1, 3 og 2 permutationer.

Lige og ulige permutationer

Man kan lave en endnu grovere opdeling af permutationerne i S_n i kun to typer. Opdelingen er baseret på tallet

$$k = n - c(\sigma), \tag{7}$$

altså n minus det samlede antal cykler i cykelfremstillingen.

En permutation σ kaldes *lige*, hvis k er lige, ellers er den *ulige*. Når man ganger permutationer, gælder de samme regler som ved multiplikation af hele tal: lige gange lige giver lige, ulige gange ulige giver lige, og lige gange ulige giver ulige. Der er et bevis i W. Phillips: On the definition of even and odd permutations.

For en m-cykel σ i S_n er $c(\sigma)$ lig med $1+n-m$, idet $n-m$ er antallet af 1-cykler. Derfor er $k = n-(1+n-m) = m-1$, så

$$\boxed{\text{En } m\text{-cykel er lige, hvis } m \text{ er ulige.}}$$

Specielt gælder, at en transposition er ulige, en 3-cykel er lige, og at en 1-cykel, altså identiteten, er lige.

Ved *fortegnet*, $\text{sign}(\sigma)$, af en permutation σ forstås tallet 1, hvis σ er lige, og -1, hvis σ er ulige.

Konjugering

Brug af cykelfremstillinger gør det let at finde den konjugerede til en permutation σ ved permutationen π, altså finde $\pi\sigma\pi^{-1}$. Antag først, at σ er en cykel: $\sigma = (c_1\ c_2\ \dots\ c_n)$. Da er

$$\pi\sigma\pi^{-1} = (\pi(c_1)\ \pi(c_2)\ \dots\ \pi(c_n)) \tag{8}$$

Det kan vises på følgende måde. Vi sætter $c_{n+1} = c_1$, og lader i være et af tallene $1, 2, \dots n$. Der gælder da, at

$$\pi\sigma\pi^{-1}(\pi(c_i)) = \pi\sigma(c_i) = \pi(c_{i+1}),$$

hvilket kan illustreres som vist på figuren nedenfor:

$$\begin{tikzcd}
c_1 \arrow[r] & \cdots \arrow[r] & c_i \arrow[r, "\sigma"] & c_{i+1} \arrow[r] \arrow[d, "\pi"] & \cdots \arrow[r] & c_n \arrow[r] & c_1 \\
& & \pi(c_i) \arrow[u, "\pi^{-1}"] \arrow[r] & \pi(c_{i+1}) & & &
\end{tikzcd}$$

Specielt ses, at $\pi\sigma\pi^{-1}$ også er en cykel af længde n.

Hvis $\sigma = \sigma_1\sigma_2\dots\sigma_k$ er en vilkårlig permutation skrevet som et produkt af disjunkte cykler, kan vi omskrive $\pi\sigma\pi^{-1}$ således:

$$\pi\sigma\pi^{-1} = \pi\sigma_1\pi^{-1}\pi\sigma_2\pi^{-1}\dots\pi\sigma_k\pi^{-1}.$$

Permutationerne $\pi\sigma_i\pi^{-1}$ kan udregnes ved brug af (8), hvorved man får cykelfremstillingen af $\pi\sigma\pi^{-1}$. Specielt ses, at

$$\boxed{\pi\sigma\pi^{-1} \text{ har samme cykelstruktur som } \sigma.}$$

Der gælder omvendt, at permutationer med samme cykelstruktur er konjugerede; beviset overlades til læseren i opgave 2.9.

Konjugering blev indført på side 17 i kapitel 1, og eksempler på anvendelser er givet i opgaverne 2.10 og 3.8.

Grupperne S_n

Anden del af dette kapitel handler om de grundlæggende algebraiske egenskaber ved multiplikation af permutationer. Kendskabet til disse egenskaber gør det mere overskueligt, hvad man kan og ikke kan, når man laver manipulationer med permutationer.

Generelt er der $n!$ permutationer i S_n. De udgør sammen med regneoperationen gange en *algebraisk struktur*, hvilket vil sige, at hvis man ganger to permutationer i S_n, så får man igen en permutation i S_n.

Da der kun er endeligt mange permutationer, kan man i princippet opstille en *kompositionstavle*, der viser resultaterne af samtlige mulige multiplikationer. Som eksempel ser vi på S_3, der består af 6 permutationer, og vi nummererer dem således:

$$\sigma_1 : (1) \qquad \sigma_2 : (12) \qquad \sigma_3 : (123)$$
$$\sigma_4 : (13) \qquad \sigma_5 : (132) \qquad \sigma_6 : (23)$$

Multiplikationerne giver følgende kompositionstavle:

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_1	σ_6	σ_5	σ_4	σ_3
σ_3	σ_3	σ_4	σ_5	σ_6	σ_1	σ_2
σ_4	σ_4	σ_3	σ_2	σ_1	σ_6	σ_5
σ_5	σ_5	σ_6	σ_1	σ_2	σ_3	σ_4
σ_6	σ_6	σ_5	σ_4	σ_3	σ_2	σ_1

(9)

Det er klart, at sådanne kompositionstavler bliver uoverskuelige, når n er større end 3, men der er egenskaber ved rækkerne og søjlerne i tavlerne, som gør det lettere at forstå de algebraiske egenskaber ved produktet. F.eks. ser man, at hver række og hver søjle indeholder alle seks permutationer, og at der ikke er nogen af de seks, der står i samme række eller søjle.

Vi har i kapitel 1 set, at multiplikation med permutationer opfylder den associative lov, at der er et neutralt element, og at enhver permutation har netop ét inverst element. Disse egenskaber kendetegner de algebraiske strukturer, der kaldes grupper, som generelt defineres på følgende måde:

Ved en *gruppe* forstås en mængde G med en regneoperation, også kaldet en *komposition*, der til to vilkårlige elementer a og b i G knytter et element $a * b$ i G, så følgende tre betingelser er opfyldt for elementer fra G:

1) For alle a, b og c gælder, at $(a * b) * c = a * (b * c)$.
2) Der findes et element e, så $a * e = e * a = a$ for alle a.
3) For alle a findes et element a^{-1}, så $a * a^{-1} = a^{-1} * a = e$.

En gruppe behøver ikke at være endelig, og f.eks. udgør de positive reelle tal med multiplikation en uendelig gruppe.

Vi skal nu se, hvordan de tre gruppeegenskaber kan bruges ved løsning af et par algebraiske problemer. Vi ser igen på S_n.

Enhver ligning af formen $\alpha\sigma = \beta$, hvor σ er ukendt, de andre kendte, kan løses på følgende måde. Man kan gange fra venstre på begge sider af lighedstegnet med α^{-1}, og man får så, at $\alpha^{-1}(\alpha\sigma) = \alpha^{-1}\beta$. Den associative lov giver så $(\alpha^{-1}\alpha)\sigma = \alpha^{-1}\beta$. Dernæst giver den tredje gruppeegenskab, at $(1)\sigma = \alpha^{-1}\beta$, og endelig får man $\sigma = \alpha^{-1}\beta$ ved brug af den anden gruppeegenskab. Der kan altså højst være denne ene løsning, og ved indsættelse kan man eftervise, at den virkelig er en løsning.

På lignende måde ser man, at der gælder følgende *forkortningsregel*: Hvis $\alpha\sigma = \alpha\tau$ så er $\sigma = \tau$. Det er dette, der viser sig ved, at alle permutationer i en række i en kompositionstavle er forskellige. Den i'te række er nemlig

$$\sigma_i\sigma_1 \quad \sigma_i\sigma_2 \quad \dots \quad \sigma_i\sigma_n$$

og forkortningsreglen giver, at to af disse ikke kan være ens, for så ville to af permutationerne i S_n være ens.

Undergrupper

En delmængde H af S_n kaldes *stabil*, hvis produktet af to vilkårlige permutationer i H også ligger i H. En stabil delmængde H af S_n kaldes også en *undergruppe*, da den i sig selv vil udgøre en gruppe, som det fremgår af opgave 2.16.

De lige permutationer i S_n udgør en undergruppe A_n, der kaldes den *alternerende* gruppe. F.eks. er $A_3 = \{(1), (123), (132)\}$.

Som et andet eksempel kan man se på alle permutationer i S_4, hvor 4 er fixpunkt. Disse permutationer udgør en undergruppe, der på oplagt måde svarer til S_3.

Frembringere for undergrupper

Man siger, at en undergruppe H af S_n er *frembragt* af delmængden F, hvis hvert element i H kan udtrykkes som et produkt af elementer fra F, og F kaldes da for et *frembringersæt* for H. Dette er ensbetydende med, at H er den mindste undergruppe, der indeholder F.

Enhver m-cykel σ frembringer en undergruppe i S_n, som består af potenserne σ^r, hvor $r = 0, 1, \dots, m-1$. En sådan cyklisk undergruppe er altså frembragt af en enkelt permutation.

Hele S_3 kan frembringes af to permutationer, f.eks. (12) og (123). De øvrige fire permutationer kan nemlig udtrykkes ved disse to på følgende måde:

$$\begin{aligned} (1) &= (12)(12) & \qquad (23) &= (12)(123) \\ (13) &= (123)(12) & \qquad (132) &= (12)(123)(12) \end{aligned}$$

I de følgende kapitler bliver det afgørende at bestemme de mulige undergrupper i S_n, eller mere præcist at bestemme antallet af permutationer i de mulige undergrupper, og her kan det være en hjælp at arbejde med frembringersæt.

3. ABBATIS FORMEL

I de følgende tre kapitler forklares med moderne skrivemåder, hvorfor man begyndte at arbejde med permutationer inden for matematikken i slutningen af 1700-tallet.

Permutation af en funktions variable

I forbindelse med forsøget på at finde en formel til løsning af femtegradsligninger studerede man af grunde, som bliver forklaret i kapitel 5, hvad der sker med forskriften for en funktion i flere variable, når de variable permuteres.

Hvis de variable kaldes x_1, x_2, …, x_n vil funktionen blive skrevet $f(\boldsymbol{x})$, hvor $\boldsymbol{x} = (x_1, \ldots, x_n)$. Som eksempel kan vi tage

$$f(x_1, x_2, x_3, x_4) = x_1^2 + x_2^2 - x_3x_4 - x_4.$$

Hvis man bytter om på x_1 og x_4, får man forskriften

$$f(x_4, x_2, x_3, x_1) = x_4^2 + x_2^2 - x_3x_1 - x_1.$$

De to højresider ovenfor er ikke ens, da f.eks. $\boldsymbol{x} = (1, 0, 0, 0)$ giver 1 i den ene, men -1 i den anden.

Bytter man derimod om på x_1 og x_2 i $f(\boldsymbol{x})$, får man

$$f(x_2, x_1, x_3, x_4) = x_2^2 + x_1^2 - x_3x_4 - x_4.$$

Selv om denne højreside umiddelbart ser anderledes ud end højresiden for $f(\boldsymbol{x})$, er de to højresider ens på den måde, at de giver samme værdi for alle $\boldsymbol{x}$, da $x_1^2 + x_2^2$ er lig med $x_2^2 + x_1^2$.

Man var interesseret i at finde ud af, om man kunne sige noget generelt om hvor mange *forskellige* forskrifter, man kan få frem ved at permutere de variable i en given forskrift.

For at kunne besvare dette spørgsmål må vi indføre lidt notation ved brug af begreberne fra kapitel 1.

Et talsæt $\boldsymbol{x} = (x_1, \ldots, x_n)$ i R^n kan opfattes som en opstilling p i $O(A)$, hvor $A = \{x_1, x_2, \ldots, x_n\}$, og $p(x_i) = i$:

$$p : \begin{array}{|c|c|c|c|} \hline x_1 & x_2 & \ldots & x_n \\ \hline 1 & 2 & \ldots & n \\ \hline \end{array}$$

Vi lader en permutation σ i S_n virke på $\boldsymbol{x}$ på samme måde som σ virker på p, dvs. at

$$\sigma\boldsymbol{x} = \sigma p.$$

Det betyder, at σ virker på $\boldsymbol{x}$ ved at koordinaten på plads i flyttes hen på plads $\sigma(i)$.

Hvis f.eks. $\sigma = (12)(34)$, vil man få

$$\sigma(x_1, x_2, x_3, x_4) = (x_2, x_1, x_4, x_3).$$

Vi tænker os nu, at vi først permuterer $\boldsymbol{x}$ med σ, og at vi dernæst permuterer resultatet med π i S_n. Da den associative lov gælder for sammensætning af afbildninger, har vi, at $\pi(\sigma p) = (\pi\sigma)p$, hvilket betyder, at

$$\pi(\sigma\boldsymbol{x}) = (\pi\sigma)\boldsymbol{x}. \tag{10}$$

Heraf følger, at vi kan skrive $\pi\sigma\boldsymbol{x}$ uden at sætte parenteser.

Vi vender tilbage til en vilkårlig funktion $f(\boldsymbol{x})$ af n variable, og lader σ være en permutation i S_n. Vi vil sige, at $f(\sigma\boldsymbol{x})$ har samme *værdi* som $f(\boldsymbol{x})$, hvis de to forskrifter giver samme værdi for alle $\boldsymbol{x}$, og vi skriver så $f(\sigma\boldsymbol{x}) = f(\boldsymbol{x})$.

I undersøgelserne af, hvor mange forskellige værdier $f(\sigma\boldsymbol{x})$ kan give, når σ gennemløber S_n, vil vi ofte bruge følgende:

$$\boxed{\text{Hvis } f(\boldsymbol{x}) = f(\sigma\boldsymbol{x}), \text{ så er } f(\pi\boldsymbol{x}) = f(\sigma\pi\boldsymbol{x}),}$$

hvor π er en vilkårlig permutation i S_n. Da ligningen til venstre i rammen gælder for alle $\boldsymbol{x}$, kan vi indsætte $\pi\boldsymbol{x}$ i stedet for $\boldsymbol{x}$ i denne ligning, hvilket giver ligningen til højre.

Eksempler med tre variable

Når der kun er 3 variable er det mere overskueligt, at kalde de variable f.eks. a, b og c, og sætte $\boldsymbol{x} = (a, b, c)$. Vi ser først på

$$f(\boldsymbol{x}) = f(a, b, c) = a^2 + ab - c.$$

For hver permutation σ i S_3 vil vi finde forskriften for $f(\sigma\boldsymbol{x})$. Hvis f.eks. $\sigma = (123)$, får vi, at $\sigma\boldsymbol{x} = (c, a, b)$, og dermed

$$f(\sigma\boldsymbol{x}) = c^2 + ca - b.$$

Nedenfor er $f(\sigma\boldsymbol{x})$ vist for hver af de 6 permutationer i S_3.

σ	$f(\sigma\boldsymbol{x})$
(1)	$a^2 + ab - c$
(12)	$b^2 + ba - c$
(123)	$c^2 + ca - b$

σ	$f(\sigma\boldsymbol{x})$
(13)	$c^2 + cb - a$
(132)	$b^2 + bc - a$
(23)	$a^2 + ac - b$

Her giver $f(\sigma\boldsymbol{x})$ seks forskellige værdier, når σ gennemløber S_3.

I det næste eksempel er der permutationer, der bevarer funktionens værdi. Vi ser her på følgende funktion

$$f(a, b, c) = a + b - c^2.$$

De seks permutationer i S_3 giver følgende værdier af $f(\sigma\boldsymbol{x})$:

σ	$f(\sigma\boldsymbol{x})$
(1)	$a + b - c^2$
(13)	$c + b - a^2$
(23)	$a + c - b^2$

σ	$f(\sigma\boldsymbol{x})$
(12)	$b + a - c^2$
(132)	$b + c - a^2$
(123)	$c + a - b^2$

Her er $f(\boldsymbol{x}) = f((12)\boldsymbol{x})$, og det ses, at udtryk med samme værdi kommer i par. Det skyldes, at værdien af funktionen ikke ændres ved at bytte om på første- og andenkoordinaten, ligegyldigt hvad de er. Det følger også af følgende ræsonnement. Når $f(\boldsymbol{x}) = f((12)\boldsymbol{x})$, kan vi erstatte $\boldsymbol{x}$ med $(13)\boldsymbol{x}$, så vi får at

$$f((13)\boldsymbol{x}) = f((12)(13)\boldsymbol{x}).$$

Da (12)(13)=(132), får vi, at de to udtryk i linje 2 i tabellen må have samme værdi.

Som det sidste eksempel med 3 variable ser vi på funktionen

$$f(a, b, c) = a^2 + b^2 + c^2.$$

Her er $f(\sigma\boldsymbol{x}) = f(\boldsymbol{x})$ for alle σ, så funktionen antager kun én værdi ved samtlige permutationer af de variable. En sådan funktion kaldes *symmetrisk*. Betegnelsen den *symmetriske* gruppe for S_n stammer antageligt netop fra, at en symmetrisk funktion er uændret ved alle permutationer af de variable.

Abbatis formel

Vi ser nu på et større eksempel, der også bliver brugt senere. Her er f følgende førstegradspolynomium af fire variable:

$$f(x_1, x_2, x_3, x_4) = x_1 + x_2 - x_3 - x_4.$$

Funktionen kan antage 6 værdier ved de 24 permutationer i S_4 af de variable. De to plustegn kan nemlig placeres på seks forskellige måder, således at man får følgende værdier

$$\begin{aligned} y_1 &= x_1 + x_2 - x_3 - x_4 & \qquad y_4 &= x_3 + x_4 - x_1 - x_2 \\ y_2 &= x_1 + x_3 - x_2 - x_4 & y_5 &= x_4 + x_2 - x_3 - x_1 \\ y_3 &= x_1 + x_4 - x_3 - x_2 & y_6 &= x_3 + x_2 - x_1 - x_4 \end{aligned}$$

Værdien af $f(x_1, x_2, x_3, x_4)$ bliver bevaret ved følgende permutationer af $\boldsymbol{x}$, hvor $\boldsymbol{x} = (x_1, x_2, x_3, x_4)$:

$$\sigma_1 : (1) \qquad \sigma_2 : (12) \qquad \sigma_3 : (34) \qquad \sigma_4 : (12)(34)$$

Værdien y_2 får man for eksempel ved permutationen $\pi = (23)$ af $\boldsymbol{x}$, som giver

$$f(x_1, x_3, x_2, x_4) = x_1 + x_3 - x_2 - x_4 = y_2.$$

For alle i er $f(\boldsymbol{x}) = f(\sigma_i \boldsymbol{x})$, og derfor er $f(\pi \boldsymbol{x}) = f(\sigma_i \pi \boldsymbol{x})$. Permutationerne $\sigma_1\pi$, $\sigma_2\pi$, $\sigma_3\pi$ og $\sigma_4\pi$ af $\boldsymbol{x}$ giver derfor alle værdien y_2. De fire permutationer er (23), (123), (243) og (1243).

Til hver af de seks mulige værdier vil man på denne måde finde fire forskellige permutationer af $\boldsymbol{x}$, der giver den pågældende værdi. Samtlige 24 permutationer i S_4 kan derfor opstilles i et rektangulært skema som vist nedenfor, hvor række i består af de permutationer af $\boldsymbol{x}$, der giver y_i.

(1)	(12)	(34)	(12)(34)
(23)	(123)	(243)	(1243)
(24)	(124)	(234)	(1234)
(13)(24)	(1324)	(1423)	(14)(23)
(14)	(142)	(134)	(1342)
(13)	(132)	(143)	(1432)

Fremgangsmåden kan uden videre overføres til en vilkårlig funktion $f(x_1, \ldots, x_n)$ i n variable, så man får følgende formel, som vi her kalder *Abbatis formel*:

> Hvis k er antallet af forskellige værdier, som en funktion af n variable kan antage ved samtlige permutationer af de variable, og hvis m er antallet af permutationer, der bevarer funktionens værdi, gælder, at
>
> $$n! = mk.$$
>
> Antallet af permutationer i S_n er altså m gange k.

Pietro Abbati (1768-1842) lavede i 1803 som den første et generelt bevis for denne formel. Nogle få andre havde tidligere anvendt formlen, men kun argumenteret for den ved hjælp af nogle eksempler. Vi vender tilbage til Abbati i kapitel 6.

Bevis. Vi lader $\sigma_1, \ldots, \sigma_m$ være de permutationer, der bevarer $f(\boldsymbol{x})$. De tænkes opstillet i en række. Hvis $f(\boldsymbol{x})$ ikke er symmetrisk, findes en permutation π_2 så $f(\pi_2 \boldsymbol{x}) \neq f(\boldsymbol{x})$. Permutationerne $\sigma_1\pi_2, \ldots, \sigma_m\pi_2$ er forskellige ifølge forkortningsreglen. De kan altså opstilles som en anden række under den første.

Anden række vil indeholde samtlige permutationer μ, for hvilke $f(\mu \boldsymbol{x})$ er lig med $f(\pi_2 \boldsymbol{x})$. Hvis nemlig $f(\mu \boldsymbol{x}) = f(\pi_2 \boldsymbol{x})$, så er $f(\mu\pi_2^{-1}\boldsymbol{x}) = f(\boldsymbol{x})$, og da første række indeholder samtlige permutationer, der bevarer værdien af $f(\boldsymbol{x})$, må der findes i så $\mu\pi_2^{-1} = \sigma_i$. Der vil altså gælde $\mu = \sigma_i\pi_2$, så μ ligger i række 2.

Hvis de to rækker indeholder hele S_n er vi færdige, ellers vælges π_3, der ikke allerede er i skemaet, og man kan lave en ny række som med π_2. Værdien af permutationerne i række 3 er forskellig fra værdien af dem i række 1 og 2, da række 3 indeholder samtlige med værdien $f(\pi_3 \boldsymbol{x})$. Specielt er der ingen permutation i række 3, der tilhører en af de to første rækker.

Således fortsættes indtil alle permutationer i S_n er brugt. Der vil ikke være to rækker med samme værdi, og hver permutation vil indgå netop én gang i skemaet, da argumenterne ovenfor viser, at alle permutationer i samme række er forskellige, og at alle permutationer i to forskellige rækker er forskellige. Hele skemaet består af $n!$ permutationer, og da der er m rækker og k søjler må der gælde, $n! = mk$. Hermed er formlen bevist.

Stabilisatorgruppen for f

De permutationer $\sigma_1, \ldots, \sigma_m$ i S_n, der bevarer værdien af en funktion f af n variable, udgør en *stabil* mængde H, altså en undergruppe i S_n.

Antag nemlig, at σ_i og σ_j tilhører H. Da er $f(\sigma_i \boldsymbol{x}) = f(\boldsymbol{x})$, hvilket giver $f(\sigma_i\sigma_j \boldsymbol{x}) = f(\sigma_j \boldsymbol{x})$, og da $f(\sigma_j \boldsymbol{x}) = f(\boldsymbol{x})$, får vi så $f(\sigma_i\sigma_j \boldsymbol{x}) = f(\boldsymbol{x})$. Altså er $\sigma_i\sigma_j$ også med i H.

Undergruppen H kaldes *stabilisatorgruppen* for f, og antallet af permutationer i H er lig med tallet m i Abbatis formel.

Man kan bl.a. anvende Abbatis formel i situationer, hvor man vil vide *om* der findes funktioner, der antager et givet antal værdier ved samtlige permutationer af de variable. I stedet kan man så undersøge, om der findes en undergruppe i S_n af en vis størrelse, hvilket ofte vil være et mere overskueligt problem. Der er nemlig kun endeligt mange mulige undergrupper, mens der er uendeligt mange mulige funktioner.

Antal kombinationer

En meget brugt formel i kombinatorikken er formlen for antal kombinationer, dvs. antal delmængder på r elementer, der kan udtages fra en mængde på n elementer. Dette antal betegnes normalt $K(n, r)$, og formlen lyder

$$K(n,r) = \frac{n!}{r! \cdot (n-r)!} \tag{11}$$

Denne formel kan udledes ved brug af Abbatis formel. Vi ser først på et eksempel, hvor $n = 5$ og $r = 3$, og lader $f(\boldsymbol{x})$ være

$$f(x_1, x_2, x_3, x_4, x_5) = x_1 + x_2 + x_3 - x_4 - x_5.$$

Ved permutation af de variable kan man få 5! funktionsudtryk. To af disse vil have samme værdi, netop hvis det er de samme tre variable, der står forrest, altså som ikke står efter et minustegn. Antal forskellige værdier for denne funktion er altså lig med antal delmængder på 3, der kan udtages af de 5 variable, dvs. $K(5, 3)$.

Vi kan finde dette antal ved i stedet at finde antallet af permutationer, der bevarer værdien af $f(\boldsymbol{x})$. En permutation bevarer værdien af $f(\boldsymbol{x})$, hvis den er sammensat af en permutation af de første tre variable og en permutation af de sidste to variable. Antallet af permutationer af den første slags er 3!, og af den

anden slags 2!. Ifølge multiplikationsprincippet er der så $3! \cdot 2!$ permutationer, der bevarer $f(\boldsymbol{x})$. Abbatis formel giver så

$$K(5,3) = \frac{5!}{3! \cdot 2!}$$

Fremgangsmåden i eksemplet kan umiddelbart generaliseres. Det bemærkes, at man i kombinatorikken ofte beviser formlen for $K(n, r)$ ved at opstille et rektangulært skema ligesom i beviset for Abbatis formel. Abbatis formel kan altså opfattes som en udvidelse af formlen for $K(n, r)$.

Netop to værdier

Når $n \geq 2$ kan man finde funktioner af n variable, der antager netop to forskellige værdier ved de mulige permutationer af de variable. Generelle fremgangsmåder til at konstruere sådanne forskrifter bliver illustreret i tilfældet, hvor $n = 3$.

Man kan finde en funktion $f(x_1, x_2, x_3)$, der antager 3! forskellige værdier ved de mulige permutationer af de variable, f.eks. $f(x_1, x_2, x_3) = x_1^2 x_2$. Summen g af de funktioner man får ved at permutere de variable med alle de *lige* permutationer er

$$f((1)(x_1, x_2, x_3)) + f((123)(x_1, x_2, x_3)) + f((132)(x_1, x_2, x_3)),$$

så $g(x_1, x_2, x_3) = x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1$, og stabilisatorgruppen består af de tre lige permutationer, så Abbatis formel giver, at $k = 2$.

En anden fremgangsmåde består i at se på produktet h af alle faktorer af formen $x_i - x_j$, hvor $i < j$. For $n = 3$ får man

$$h(x_1, x_2, x_3) = (x_1 - x_2) \cdot (x_1 - x_3) \cdot (x_2 - x_3).$$

Enhver transposition af to af de variable vil ændre fortegnet af h, og da enhver permutation er et produkt af transpositioner, vil h altså kun antage 2 værdier ved samtlige permutationer af de variable.

Funktioner af fire variable

For funktioner af fire variable vil det ifølge Abbatis formel kun være muligt at få k-værdierne $\{1, 2, 3, 4, 6, 8, 12, 24\}$, da k skal gå op i 4!, altså gå op i 24. Det er ikke på forhånd givet, at man til hvert af disse tal faktisk kan finde en funktion, hvor k er lig med det pågældende tal, men i skemaet nedenfor er angivet eksempler på funktioner, der viser, at det er muligt.

k	$f(\boldsymbol{x})$
24	$x_1^3 x_2^2 x_3$
12	$x_1^2 + x_2^2 - x_3 x_4 - x_4$
8	$x_1^3 x_2^2 x_3 + x_3^3 x_1^2 x_2 + x_2^3 x_3^2 x_1$
6	$x_1 + x_2 - x_3 - x_4$
4	x_1
3	$(x_1 + x_2 - x_3 - x_4)^2$
2	$(x_1 - x_2) \cdot (x_1 - x_3) \cdot (x_1 - x_4) \cdot (x_2 - x_3) \cdot (x_2 - x_4) \cdot (x_3 - x_4)$
1	$x_1 + x_2 + x_3 + x_4$

På side 32 så vi, at $x_1 + x_2 - x_3 - x_4$ giver 6 værdier, $y_1, \ldots, y_6$, men da $y_4 = -y_1$, $y_5 = -y_2$ og $y_6 = -y_3$ vil $(x_1 + x_2 - x_3 - x_4)^2$ kun give 3 forskellige værdier. Disse tre værdier, som vi skal bruge i kapitel 5, kalder vi henholdsvis z_1, z_2 og z_3.

Af Abbatis formel følger, at det foregående også kan udtrykkes således: Til ethvert helt tal m, der går op i 4!, findes en funktion af 4 variable med en stabilisatorgruppe bestående af m permutationer. Det er så nærliggende at tro, at noget tilsvarende gælder for alle n. Det gælder da også for alle $n \leq 4$, men ikke for $n = 5$, som vi skal se i næste kapitel.

4. RUFFINIS OPDAGELSER

Da italieneren Paolo Ruffini (1765–1822) begyndte at studere matematik, regnede man stadig med, at det var muligt at finde en formel til løsning af femtegradsligninger. Det gjorde han uden tvivl også, og han har nok oprindeligt arbejdet på at finde en sådan formel. Dette kapitel handler om, hvad det var for en opdagelse, der fik ham overbevist om, at det ikke ville være muligt at løse problemet.

Han arbejdede med funktioner af fem variable x_1, x_2, x_3, x_4 og x_5, og fandt ud af, at de på nogle afgørende punkter adskiller sig fra funktioner af 4 eller færre variable. De fem variable kan permuteres på 120 måder, og hvis funktioner af fem variable skulle opføre sig som funktioner af fire variable, skulle der til ethvert helt tal m, der går op i 120, findes en funktion med en stabilisatorgruppe bestående af m permutationer.

Ruffini kunne imidlertid 1799 bevise nogle resultater, hvoraf man bl.a. får følgende:

> Stabilisatorgruppen for en funktion af fem variable kan ikke bestå af 30 permutationer.

Det følgende bevis for påstanden er meget kortere end det, Ruffini lavede i 1799. Hans eget bevis vender vi tilbage til senere.

Bevis for påstanden

Beviset er *indirekte*, idet vi antager, at der findes en funktion $f(\boldsymbol{x})$ af fem variable $(x_1, \ldots, x_5)$ med en stabilsatorgruppe på 30 permutationer. Lad H være stabilisatorgruppen, altså de permutationer σ i S_5, for hvilke $f(\sigma\boldsymbol{x}) = f(\boldsymbol{x})$.

Beviset falder i tre dele, og første del består i at vise, at enhver 5-cykel σ vil ligge i H. Dette kan indses på følgende måde.

Ifølge Abbatis formel antager $f(\sigma\boldsymbol{x})$ fire værdier, når σ gennemløber S_5, da 120 divideret med 30 er 4. Der er fem potenser af σ, nemlig (1), σ, σ^2, σ^3 og σ^4, og de 5 funktionsudtryk $f(\sigma^i\boldsymbol{x})$, hvor $i = 0, 1, \ldots, 4$, kan derfor ikke alle være forskellige. Der findes altså to forskellige eksponenter u og v, hvor $u < v$, så $f(\sigma^u\boldsymbol{x}) = f(\sigma^v\boldsymbol{x})$. Ved at erstatte $\boldsymbol{x}$ med $\sigma^{-u}\boldsymbol{x}$, og benytte en potensregneregel, får vi så, at $f(\boldsymbol{x}) = f(\sigma^{v-u}\boldsymbol{x})$. Det vil sige, at σ^{v-u} tilhører H. Der findes altså et tal q, $q \in \{1, 2, 3, 4\}$, så σ^q ligger i H.

For hver af de fire mulige værdier 1, 2, 3 og 4 af q er det let at finde hele tal s og t, så

$$1 = s \cdot p + t \cdot q,$$

hvor $p = 5$, se eventuelt opgave 4.1. Da $\sigma^p = (1)$ får man så

$$\sigma = \sigma^{s\cdot p+t\cdot q} = (\sigma^p)^s(\sigma^q)^t = (\sigma^q)^t.$$

Da sidstnævnte udtryk ligger i H, eftersom σ^q ligger i H, må σ altså tilhøre H.

Andel del i beviset bygger på, at enhver 3-cykel kan skrives som et produkt af to 5-cykler, idet for eksempel

$$(a\,b\,c) = (a\,c\,b\,d\,e)(e\,d\,b\,a\,c).$$

Da alle 5-cykler ligger i H, må alle 3-cykler derfor ligge i H.

I tredje og sidste del af beviset tælles antallet af 3-cykler og 5-cykler. Antallet af 3-cykler er K(5,3) gange 2, altså 20. De tre tal i cyklen kan nemlig vælges på K(5,3) måder, og ud fra tre givne tal kan man lave 2 cykler. Antallet af 5-cykler er som tidligere nævnt 4!, altså 24. I alt er der altså 44 3- og 5-cykler i H, som derfor ikke kan bestå af 30 permutationer. Hermed er påstanden bevist.

Ruffinis bevis

Ruffini beviser først et resultat, som med moderne matematiske begreber kan formuleres således:

S_5 har ingen undergrupper med 30 permutationer.

Han laver et *direkte* bevis, hvor han systematisk finder antallet af permutationer i hver eneste mulig type af undergruppe i S_5. Han undersøger ikke alle de mulige konkrete undergrupper, men inddeler dem i typer, som kan behandles ens. Denne typeinddeling er først og fremmest baseret på cykelstrukturen af permutationer, der frembringer undergruppen.

Den simpleste type undergruppe er en, der er frembragt af en cykel σ. Alle undergrupper, der er frembragt af en m-cykel består af m permutationer, nemlig potenserne σ^u, $u = 0, 1, \ldots, m-1$. Der eksisterer altså undergrupper i S_5 bestående af hhv. 1, 2, 3, 4 og 5 permutationer.

Den næstsimpleste type er en, der er frembragt af en cykel σ og en anden permutation π. Ruffini opdeler undersøgelsen af disse i specialtilfælde svarende til forskellige typer af π.

Som eksempel kan vi se på det tilfælde, hvor σ er en 5-cykel, og π er et produkt af to disjunkte 2-cykler.

$$\sigma = (12345), \qquad \pi = (14)(23).$$

En stabil mængde med σ og π må indeholde følgende 10 permutationer af formen σ^u eller $\sigma^u\pi$, hvor $u \in \{0, 1, 2, 3, 4\}$:

(1)	(12345)	(13524)	(14253)	(15432)
(14)(23)	(15)(24)	(25)(34)	(12)(35)	(13)(45)

Man kan regne efter, at de udgør en stabil mængde ved simpelthen at udregne samtlige mulige produkter, men det går meget nemmere, hvis man bare udregner $\pi\sigma$ og ser, at man får $\sigma^4\pi$. Heraf får man f.eks., da $\sigma^5 = (1)$ og $\pi^2 = (1)$, at

$$\sigma^2\pi\sigma\pi = \sigma^2\sigma^4\pi\pi = \sigma.$$

Det ses på denne måde ret let, at man har en stabil mængde, så σ og π frembringer altså en undergruppe med 10 permutationer. Selvom han formulerer det noget anderledes, er det den samme teknik Ruffini bruger til at vise, at mængden er stabil.

Som det sidste eksempel kan nævnes, at hvis σ er 5-cyklen (12345) og π er 2-cyklen (12), så vil σ og π frembringe hele S_5 med 120 permutationer. De nærmere detaljer er formuleret som øvelser i opgave 4.2.

Tilsvarende gennemføres for alle de øvrige principielt forskellige slags frembringersæt for undergruppen. Det er meget omstændeligt og fylder over 4 tætskrevne sider hos Ruffini, men han kommer frem til, at ingen undergruppe består af 15, 30 eller 40 permutationer.

At der ikke kan være undergrupper med 15 eller 40 permutationer er ikke relevant for den del af Ruffinis arbejde med femtegradsligningerne, som vi skal se på i næste kapitel.

Abbatis formel giver, at Ruffinis resultat også kan udtrykkes:

> En funktion af fem variable kan ikke antage netop 4 værdier ved samtlige permutationer af de variable.

En af Ruffinis afgørende ideer var altså at vise, at det er umuligt at lave *undergrupper* med visse givne egenskaber, i stedet for at vise, at det er umuligt at lave *forskrifter* med visse givne egenskaber. Ved at se på undergrupper får man som tidligere nævnt et mere begrænset problem, forstået på den måde, at der kun er *endeligt* mange undergrupper, mens der er uendeligt mange forskrifter.

5. FEMTEGRADSLIGNINGEN

Dette kapitel handler om, hvad Ruffinis opdagelser om permutationsgruppen S_5 har at gøre med at løse *femtegradsligninger*, altså ligninger af formen

$$x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0, \qquad (12)$$

hvor x er ubekendt, og ligningen koefficienter a_i opfattes som kendte tal. Ved en *konkret* ligning forstås en ligning som f.eks.

$$x^5 + 4x - 5 = 0,$$

hvor talværdierne af koefficienterne er givet. En *rod* eller en løsning er et tal x_0, som passer i ligningen, d.v.s. at venstresiden bliver 0, når x_0 indsættes i stedet for x. F.eks. er 1 rod i ligningen ovenfor. At løse ligningen betyder at finde samtlige rødder. Det er ikke så svært at vise, at en femtegradsligning højst kan have fem rødder, men beviset er ikke væsentligt i denne sammenhæng.

For ligninger af grad mindre end 5 findes der *generelle formler* til udregning af løsningerne. For en andengradsligning

$$x^2 + a_1x + a_0 = 0$$

har man f.eks. følgende løsningsformel

$$x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0}}{2} \qquad (13)$$

Disse generelle formler udregner løsningerne ved hjælp af ligningens koefficienter og brug af de sædvanlige 4 regneoperationer og roduddragning. I formlerne kan også indgå faste kendte tal, som 2 og 4 i (13). Ved roduddragning forstås ikke bare kvadratrod, men også kubikrod, osv.

Det er en formel i samme stil, der tænkes på, når man taler om at finde en formel til løsning af femtegradsligninger. For bedre at forstå problemet med at finde en sådan formel, kan man tænke sig, at man kender rødderne, som kaldes x_1, x_2,..., x_5. Man kan så opstille følgende ligning, der vil have rødderne x_1, x_2,..., x_5:

$$(x - x_1)(x - x_2)(x - x_3)(x - x_4)(x - x_5) = 0 \tag{14}$$

Ganges parenteser ud, får man en ligning som (12), hvor koefficienterne er polynomier i rødderne, f.eks. er

$$a_4 = -(x_1 + x_2 + x_3 + x_4 + x_5) \quad \text{og} \quad a_0 = -x_1x_2x_3x_4x_5.$$

Spørgsmålet er, om man ved brug af disse relationer mellem koefficienter og rødder kan gå baglæns og finde rødderne ud fra koefficienterne ved hjælp af de sædvanlige 4 regneoperationer og roduddragning.

Andengradsligninger

Problemerne med løsning af femtegradsligninger bliver tydeligere, hvis vi først ser på, hvordan man kan løse de tilsvarende ligninger af lavere grad. *Andengradsligningen* skriver vi som nævnt

$$x^2 + a_1x + a_0 = 0. \tag{15}$$

Man kan lave en ligning med rødder x_1 og x_2 på følgende måde:

$$(x - x_1)(x - x_2) = 0.$$

Ved at gange parenteser ud får man en ligning af formen (15). Sammenhængen mellem ligningens koefficienter og rødder kan udtrykkes ved relationerne:

$$-a_1 = x_1 + x_2 \tag{16}$$

$$a_0 = x_1x_2 \tag{17}$$

En algebraisk løsningsformel til andengradsligningen er to ligninger, hvor henholdsvis x_1 og x_2 er udtrykt ved a_0 og a_1 ved

hjælp af de fire grundlæggende regneoperationer og roduddragning. Vi vil nu komme frem til en sådan løsningsformel på en lidt anderledes måde end den sædvanlige.

I (16)-(17) er a_0 og a_1 *symmetriske* funktioner af rødderne. En løsningsformel med x_1 på venstresiden vil ikke have en symmetrisk funktion på venstresiden. Det betyder, at højresiden må indeholde en roduddragning; hvis den ikke gjorde, ville højresiden være symmetrisk i rødderne, da de fire sædvanlige regneoperationer bevarer symmetrien.

Hvis man for en ikke-symmetrisk funktion $f(x_1, x_2)$ kan finde en potens $f(x_1, x_2)^n$, der er symmetrisk, kan man ved roduddragning få $f(x_1, x_2)$ udtrykt ved a_0 og a_1. En ikke-symmetriske funktion med denne egenskab er $x_1 - x_2$, idet $(x_1 - x_2)^2$ er symmetrisk. Ombytter man nemlig x_1 og x_2 skifter størrelsen i parentesen nemlig bare fortegn, men det ophæves, når der kvadreres. For at udtrykke $(x_1 - x_2)^2$ ved a_0 og a_1 kan vi bruge, at

$$(x_1 - x_2)^2 = x_1^2 + x_2^2 - 2x_1x_2.$$

Denne højreside kan igen ved brug af en kvadratsætning udtrykkes ved de symmetriske funktioner $x_1 + x_2$ og x_1x_2:

$$x_1^2 + x_2^2 - 2x_1x_2 = (x_1 + x_2)^2 - 4x_1x_2 = a_1^2 - 4a_0.$$

Hvoraf vi alt i alt får, at $(x_1 - x_2)^2$ er lig med $a_1^2 - 4a_0$, så

$$x_1 - x_2 = \pm\sqrt{a_1^2 - 4a_0}.$$

Addition af ovenstående ligning og relationen (16) giver

$$2x_1 = -a_1 \pm \sqrt{a_1^2 - 4a_0}.$$

Til sidst får man så løsningsformlen (13) ved division med 2.

At $(x_1 - x_2)^2$ kan udtrykkes som et polynomium i koefficienterne er ingen tilfældighed; det gælder ethvert symmetrisk polynomium ifølge en fundamental sætning om symmetriske polynomier, som vi nu vil se på.

Viète-relationerne

Relationerne mellem en n'tegradslignings koefficienter og rødder giver nogle symmetriske polynomier, som er særligt simple. Ud fra et eksempel med $n = 4$ kan man udlede, hvordan disse simple polynomier ser ud. Vi danner fjerdegradsligningen

$$(x - x_1)(x - x_2)(x - x_3)(x - x_4) = 0,$$

og ganger parenteserne ud. Man får en sum af produkter, der er dannet ved fra hver af parenteserne at vælge enten x eller $-x_i$. I alle de produkter, hvor der er j x'er, sættes x^j uden for en parentes, og hvis udtrykket i parentesen kaldes a_j, får man

$$a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0.$$

Koefficienterne a_i er givet ved de såkaldte *Viète-relationer*:

$$\begin{aligned}
a_4 &= 1\\
-a_3 &= x_1 + x_2 + x_3 + x_4\\
a_2 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4\\
-a_1 &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4\\
a_0 &= x_1x_2x_3x_4
\end{aligned}$$

Polynomierne på højresiderne kaldes de *elementarsymmetriske* polynomier af fire variable, og de benævnes her ovenfra og ned s_0, s_1, s_2, s_3 og s_4.

På tilsvarende måde har man elementarsymmetriske polynomier s_0, s_1,..., s_n af n variable, og

s_i er summen af alle produkter af i af de variable.

for $i \geq 1$, og $s_0 = 1$. Det er underforstået, at der i hvert produkt kun indgår *forskellige* variable. Relationerne er opkaldt efter Francois Viète (1540–1603).

Fundamentalsætningen om symmetriske polynomier

De elementarsymmetriske polynomier udgør en slags basis for samtlige symmetriske polynomier forstået på følgende måde:

Hvis $f(x_1, \ldots, x_n)$ er et symmetrisk polynomium, findes netop ét polynomium g i n variable, for hvilket

$$f(x_1, \ldots, x_n) = g(s_1, \ldots, s_n),$$

hvor $s_1, \ldots, s_n$ er de elementarsymmetriske polynomier.

Sætningen blev først bevist af Waring (1734-1798), men havde været kendt af bl.a. Newton i mindst hundrede år før.

Eksempel. Ved brug af en kvadratsætning ses, at

$$x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2 = s_1^2 - 2s_2.$$

Vi får brug for fundamentalsætningen i følgende situation. Antag, at $h(\boldsymbol{x})$ er et ikke-symmetrisk polynomium, der antager k værdier $z_1, \ldots, z_k$ ved samtlige permutationer af de variable, og at s er en symmetrisk funktion af k variable. Da vil $s(z_1, \ldots, z_k)$ være en symmetrisk funktion af de n variable $x_1, \ldots, x_n$. En permutation af de variable $x_1, \ldots, x_n$ vil nemlig give en permutation af de variable $z_1, \ldots, z_k$, hvilket ikke ændrer værdien af s, da den er symmetrisk. Fundamentalsætningen giver så, at man kan skrive $s(z_1, \ldots, z_k)$ som et polynomium af de elementarsymmetriske polynomier af n variable.

Eksempel. Vi har på side 36 set, at $h(a, b, c) = a^2b + b^2c + c^2a$ antager værdierne $z_1 = a^2b + b^2c + c^2a$ og $z_2 = ab^2 + bc^2 + ca^2$ ved samtlige permutationer af a, b og c. Funktionen $s(z_1, z_2) = z_1 + z_2$ er derfor symmetrisk, og man finder at

$$s(z_1, z_2) = (a + b + c)(ab + ac + bc) - 3abc = s_1s_2 - 3s_3.$$

Der findes systematiske metoder til at bestemme g, men det er ikke noget. som vi får brug for her. I opgave 5.1 er der eksempler, der illustrerer metoden.

Tredje- og fjerdegradsligningerne

Tredje- og fjerdegradsligningerne kan løses ved en fremgangsmåde, som i princippet er den, der blev brugt i forbindelse med andengradsligningerne. Da det er fremgangsmåden, der er det afgørende, nøjes vi her med at se på fjerdegradsligningerne, mens tredjegradsligningerne indgår i opgave 5.3. Fjerdegradsligningen har formen

$$x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = 0 \tag{18}$$

Som vist tidligere side 37 antager polynomiet $(x_1+x_2-x_3-x_4)^2$ følgende tre værdier ved samtlige permutationer af de variable.

$$\begin{aligned} z_1 &= (x_1 + x_2 - x_3 - x_4)^2 \\ z_2 &= (x_1 - x_2 + x_3 - x_4)^2 \\ z_3 &= (x_1 - x_2 - x_3 + x_4)^2 \end{aligned}$$

Disse værdier er løsning til en tredjegradsligning

$$(z - z_1)(z - z_2)(z - z_3) = 0.$$

Tredjegradsligningen har formen

$$z^3 + b_2z^2 + b_1z + b_0 = 0 \tag{19}$$

og koefficienterne er symmetriske polynomier i z_1, z_2 og z_3. Det betyder, at de også er symmetriske polynomier i x_1, x_2, x_3 og x_4, som forklaret på forrige side.

Ifølge fundamentalsætningen om symmetriske polynomier kan koefficienterne i tredjegradsligningen udtrykkes ved de elementarsymmetriske funktioner i x_i'erne og dermed ved koefficienterne i fjerdegradsligningen. Man får

$$\begin{aligned} b_2 &= -(3a_3^2 - 8a_2) \\ b_1 &= 3a_3^4 - 16a_3^2a_2 + 16a_2^2 + 16a_3a_1 - 64a_0 \\ b_0 &= -(a_3^3 - 4a_3a_2 + 8a_1)^2 \end{aligned}$$

Når vi har en formel til løsning af tredjegradsligningen kan vi altså bestemme værdierne af z_1, z_2 og z_3. Sammen med værdien af a_3 giver det følgende ligningssystem til bestemmelse af x_i'erne:

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= -a_3 \\ x_1 + x_2 - x_3 - x_4 &= \sqrt{z_1} \\ x_1 - x_2 + x_3 - x_4 &= \sqrt{z_2} \\ x_1 - x_2 - x_3 + x_4 &= \sqrt{z_3} \end{aligned}$$

Ligningssystemet kan løses, og man får

$$\begin{aligned} x_1 &= \tfrac{1}{4}(-a_3 + \sqrt{z_1} + \sqrt{z_2} + \sqrt{z_3}) \\ x_2 &= \tfrac{1}{4}(-a_3 + \sqrt{z_1} - \sqrt{z_2} - \sqrt{z_3}) \\ x_3 &= \tfrac{1}{4}(-a_3 - \sqrt{z_1} + \sqrt{z_2} - \sqrt{z_3}) \\ x_4 &= \tfrac{1}{4}(-a_3 - \sqrt{z_1} - \sqrt{z_2} + \sqrt{z_3}) \end{aligned}$$

Eksempel. Fjerdegradsligningen

$$x^4 + 2x^3 - 13x^2 - 14x + 24 = 0 \tag{20}$$

giver ved brug af formlerne øverst på siden

$$z^3 - 116z^2 + 1600z = 0.$$

Denne ligning har rødderne 0, 16 og 100, som svarer til z_1, z_2 og z_3. Ved indsættelse i formlerne ovenfor for $x_1, \ldots, x_4$ får man så, at rødderne i fjerdegradsligningen bliver 1, -2, 3 og -4.

Vi kan nu opsummere en række fællestræk ved den metode til løsning af n-tegradsligninger, som er brugt, når $n \leq 4$. Den overordnede idé er at lave en formel til løsning af en n'tegradsligning ved hjælp af en formel til løsning af $(n-1)$'tegradsligninger.

Fremgangsmåden er at finde en funktion $f(\boldsymbol{x})$ af rødderne og en potens $f(\boldsymbol{x})^p$, som kun antager $n-1$ forskellige værdier ved samtlige permutationer af de variable. Disse $n-1$ værdier kan så bestemmes ved at løse en $(n-1)$'tegradsligning.

Funktionerne $f(\boldsymbol{x})$ var i alle tilfælde førstegradspolynomier, og når man havde $(n-1)$ førstegradspolynomier af rødderne, kunne man supplere med den Viète-relation, der handler om et førstegradspolynomium i rødderne. Man har så et lineært ligningssystem med n-ligninger med n ubekendte, der kan løses.

Tilbage til femtegradsligningerne

Som forklaret i forrige kapitel, viste Ruffinis undersøgelser af S_5, at man ikke vil kunne finde funktioner af de fem rødder, som vil give 4 værdier ved samtlige permutationer af rødderne. Det ville altså ikke være muligt at komme frem til løsningerne af en femtegradsligning ved hjælp af formlerne for løsning af fjerdegradsligningerne ved en fremgangsmåde i lighed med den, der virker for ligningerne af lavere grad.

At man ikke kan komme frem til en formel på denne måde, var nok det, der i første omgang ledte Ruffini på sporet af, at det ikke ville være muligt overhovedet at opstille en formel til løsning af femtegradsligninger.

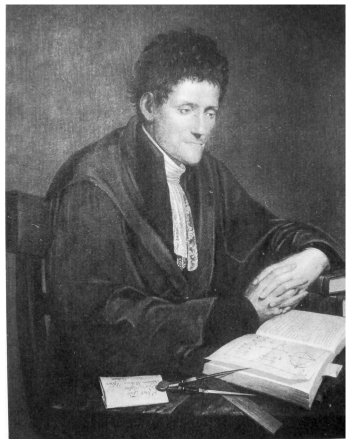
At man ikke kan komme frem til en formel på én bestemt måde udelukker ikke, at man ikke vil kunne komme frem til en formel på en anden måde, og er dermed ikke noget bevis for, at der ikke vil kunne laves en sådan formel. Det var Ruffini også godt klar over, og han forsøgte at gøre beviset fuldstændigt ved en række supplerende argumenter.

Hans udledninger blev imidlertid så komplicerede, at de er svære at gennemskue, og det er først Niels Henrik Abel (1802-1829), der laver et bevis, som bliver alment accepteret.

6. PERMUTATIONERNES HISTORIE

Efter at Cardano (1501–1576) i 1545 havde publiceret sine formler til løsning af tredje- og fjerdegradsligninger, gik der over 200 år før nogen for alvor gjorde fremskridt med hensyn til femtegradsligningerne. Ved brug af permutationer af en funktions variable opdagede Lagrange (1736-1813), at man kunne udlede formlerne til løsning af ligningerne af lavere grad end 5 ved fremgangsmåder med en række *fælles træk*, som omtalt i kapitel 5. Indtil da havde man udledt disse formler på ret forskellig måde. Lagranges opdagelse gav ham håb om, at en lignende fremgangsmåde ville kunne bruges i forbindelse med femtegradsligninger. Han var imidlertid ikke i stand til at kopiere teknikken.

Ruffini, der er portrætteret nedenfor, fortsatte Lagranges arbejde med permutationer, men gik langt videre i sine undersøgelser af permutationernes egenskaber.



Det var disse undersøgelser, der som omtalt i kapitel 4, førte Ruffini frem til, hvad der forhindrede, at man kunne anvende Lagranges metoder på femtegradsligningerne.

Ruffinis og Abbatis formuleringer

Permutationer er i det foregående blevet beskrevet ved brug af matematiske betegnelser, der er kommet til efter Ruffini. Det kan derfor være interessant at se et konkret eksempel på, hvordan Ruffini rent faktisk formulerer sig, bl.a. for at se hvordan indførelse af nye begreber og skrivemåder kan forenkle de matematiske beskrivelser.

Som eksempel bruges et par sætninger fra § 273 i Ruffinis værk fra 1799, hvor han første gang publicerede sine resultater om femtegradsligningen. Ruffini benytter her, ligesom i mange andre af sine beregninger med permutationer, en tabel, der som udgangspunkt har et udtryk af formen $f(x^i)(x^{ii})(x^{iii})(x^{iv})(x^v)$, og som indeholder alle de 120 mulige udtryk, man får ved at permutere de variable.Tabellen er vist på siderne 53-55. I tabellen er de 120 udtryk nummererede; vi får her kun brug for 4 af dem:

$$\begin{array}{ll} 1^\circ\ f(x^i)(x^{ii})(x^{iii})(x^{iv})(x^v) & 3^\circ\ f(x^{ii})(x^{iii})(x^i)(x^{iv})(x^v) \\ 25^\circ\ f(x^{ii})(x^{iii})(x^{iv})(x^v)(x^i) & 28^\circ\ f(x^i)(x^{ii})(x^{iv})(x^v)(x^{iii}) \end{array}$$

I paragraf 273 skriver Ruffini følgende (i oversættelse)

> ... man antager så resultatet
>
> $$1^\circ = 3^\circ = 10^\circ = 28^\circ = 38^\circ = 80^\circ.$$
>
> Ved at anvende den tredje permutation på resultatet 3° kommer heraf $3^\circ = 25^\circ$....

At for eksempel $1^\circ = 3^\circ$ betyder med vores moderne betegnelser, at $f(\boldsymbol{x}) = f((132)\boldsymbol{x})$. Med *den tredje permutation* mener Ruffini den, der svarer til $1^\circ = 28^\circ$, altså (354).

Når Ruffini skriver, at han udfører den tredje permutation på 3°, vil det sige, at han i $f(x^{ii})(x^{iii})(x^i)(x^{iv})(x^v)$ flytter det på

plads 3 hen på plads 5, det på plads 5 hen på plads 4 og det på plads 4 hen på plads 3; han får derfor $f(x^{ii})(x^{iii})(x^{iv})(x^v)(x^i)$, som er 25°.

Ruffinis udregning kan vi med moderne notation skrive på følgende måde: Hvis man har, at $f(\boldsymbol{x}) = f((354)\boldsymbol{x})$, gælder også, at $f((132)\boldsymbol{x}) = f((354)(132)\boldsymbol{x})$, så $f((132)\boldsymbol{x}) = f((15432)\boldsymbol{x})$.

Ruffini kunne ikke arbejde med udtryk som (354)(132), fordi han ikke klart definerede permutationer som selvstændige matematiske objekter med en tilhørende kompositionsregel.

Pietro Abbati, der ligesom Ruffini boede i Modena i Italien og var ven med Ruffini, forenklede nogle af Ruffinis argumenter, og gav nogle mere generelle beviser, som for eksempel det, der er omtalt i kapitel 3. Desuden definerede Abbati permutationer på en måde, som er tæt på at gøre dem til selvstændige matematiske objekter. Han skriver

> ... har man noteret de pladser, eller rum, hvor rødderne kommer fra og hvor de kommer hen, når de bevæger sig fra (A') til (A''), og givet navnet ***permutation*** til en sådan observation...

suppleret med bl.a. følgende eksempel:

$$(A')\ \ f(x^i)(x^{ii})(x^{iii})(x^{iv})(x^v) = (A'')\ \ f(x^{iii})(x^i)(x^{iv})(x^v)(x^{ii})$$

At notere sig de pladser, hvor rødderne, kommer fra og hvor de kommer hen, svarer jo til at opstille et skema af formen

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

men Abbati går ikke så langt som at indføre en fast notation.

På de følgende tre sider er Ruffinis tabel gengivet.

1° $f(x^{i})(x^{ii})(x^{iii})(x^{iv})(x^{v})$,

2° $f(x^{ii})(x^{i})(x^{iii})(x^{iv})(x^{v})$,

3° $f(x^{ii})(x^{iii})(x^{i})(x^{iv})(x^{v})$,

4° $f(x^{iii})(x^{i})(x^{ii})(x^{iv})(x^{v})$,

5° $f(x^{i})(x^{iii})(x^{ii})(x^{iv})(x^{v})$,

6° $f(x^{iii})(x^{ii})(x^{i})(x^{iv})(x^{v})$,

7° $f(x^{ii})(x^{iii})(x^{iv})(x^{i})(x^{v})$,

8° $f(x^{iii})(x^{iv})(x^{i})(x^{ii})(x^{v})$,

9° $f(x^{iv})(x^{i})(x^{ii})(x^{iii})(x^{v})$,

10° $f(x^{i})(x^{iii})(x^{iv})(x^{ii})(x^{v})$,

11° $f(x^{iii})(x^{iv})(x^{ii})(x^{i})(x^{v})$,

12° $f(x^{iv})(x^{ii})(x^{i})(x^{iii})(x^{v})$,

13° $f(x^{iii})(x^{i})(x^{iv})(x^{ii})(x^{v})$,

14° $f(x^{i})(x^{iv})(x^{ii})(x^{iii})(x^{v})$,

15° $f(x^{iv})(x^{ii})(x^{iii})(x^{i})(x^{v})$,

16° $f(x^{i})(x^{ii})(x^{iv})(x^{iii})(x^{v})$,

17° $f(x^{ii})(x^{iv})(x^{iii})(x^{i})(x^{v})$,

18° $f(x^{iv})(x^{iii})(x^{i})(x^{ii})(x^{v})$,

19° $f(x^{iii})(x^{ii})(x^{iv})(x^{i})(x^{v})$,

20° $f(x^{ii})(x^{iv})(x^{i})(x^{iii})(x^{v})$,

21° $f(x^{iv})(x^{i})(x^{iii})(x^{ii})(x^{v})$,

22° $f(x^{ii})(x^{i})(x^{iv})(x^{iii})(x^{v})$,

23° $f(x^{i})(x^{iv})(x^{iii})(x^{ii})(x^{v})$,

24° $f(x^{iv})(x^{iii})(x^{ii})(x^{i})(x^{v})$,

25° $f(x^{ii})(x^{iii})(x^{iv})(x^{v})(x^{i})$,

26° $f(x^{i})(x^{iii})(x^{iv})(x^{v})(x^{ii})$,

27° $f(x^{iii})(x^{i})(x^{iv})(x^{v})(x^{ii})$,

28° $f(x^{i})(x^{ii})(x^{iv})(x^{v})(x^{iii})$,

29° $f(x^{iii})(x^{ii})(x^{iv})(x^{v})(x^{i})$,

30° $f(x^{ii})(x^{i})(x^{iv})(x^{v})(x^{iii})$,

31° $f(x^{iii})(x^{iv})(x^{i})(x^{v})(x^{ii})$,

32° $f(x^{iv})(x^{i})(x^{ii})(x^{v})(x^{iii})$,

33° $f(x^{i})(x^{ii})(x^{iii})(x^{v})(x^{iv})$,

34° $f(x^{iii})(x^{iv})(x^{ii})(x^{v})(x^{i})$,

35° $f(x^{iv})(x^{ii})(x^{i})(x^{v})(x^{iii})$,

36° $f(x^{ii})(x^{i})(x^{iii})(x^{v})(x^{iv})$,

37° $f(x^{i})(x^{iv})(x^{ii})(x^{v})(x^{iii})$,

38° $f(x^{iv})(x^{ii})(x^{iii})(x^{v})(x^{i})$,

39° $f(x^{ii})(x^{iii})(x^{i})(x^{v})(x^{iv})$,

40° $f(x^{ii})(x^{iv})(x^{iii})(x^{v})(x^{i})$,

41° $f(x^{iv})(x^{iii})(x^{i})(x^{v})(x^{ii})$,

42° $f(x^{iii})(x^{i})(x^{ii})(x^{v})(x^{iv})$,

43° $f(x^{ii})(x^{iv})(x^{i})(x^{v})(x^{iii})$,

44° $f(x^{iv})(x^{i})(x^{iii})(x^{v})(x^{ii})$,

45° $f(x^{i})(x^{iii})(x^{ii})(x^{v})(x^{iv})$,

46° $f(x^{i})(x^{iv})(x^{iii})(x^{v})(x^{ii})$,

47° $f(x^{iv})(x^{iii})(x^{ii})(x^{v})(x^{i})$,

48° $f(x^{iii})(x^{ii})(x^{i})(x^{v})(x^{iv})$,

49° $f(x^{iii})(x^{iv})(x^{v})(x^{i})(x^{ii})$,

50° $f(x^{iii})(x^{iv})(x^{v})(x^{ii})(x^{i})$,

51° $f(x^{i})(x^{iv})(x^{v})(x^{ii})(x^{iii})$,

52° $f(x^{ii})(x^{iv})(x^{v})(x^{iii})(x^{i})$,

53° $f(x^{ii})(x^{iv})(x^{v})(x^{i})(x^{iii})$,

54° $f(x^{i})(x^{iv})(x^{v})(x^{iii})(x^{ii})$,

55° $f(x^{iv})(x^{i})(x^{v})(x^{ii})(x^{iii})$,

56° $f(x^{i})(x^{ii})(x^{v})(x^{iii})(x^{iv})$,

57° $f(x^{ii})(x^{iii})(x^{v})(x^{iv})(x^{i})$,

58° $f(x^{iv})(x^{ii})(x^{v})(x^{i})(x^{iii})$,

59° $f(x^{ii})(x^{i})(x^{v})(x^{iii})(x^{iv})$,

60° $f(x^{i})(x^{iii})(x^{v})(x^{iv})(x^{ii})$,

61° $f(x^{iv})(x^{ii})(x^{v})(x^{iii})(x^{i})$,

62° $f(x^{ii})(x^{iii})(x^{v})(x^{i})(x^{iv})$,

63° $f(x^{iii})(x^{i})(x^{v})(x^{iv})(x^{ii})$,

64° $f(x^{iv})(x^{iii})(x^{iv})(x^{i})(x^{ii})$,

65° $f(x^{iii})(x^{i})(x^{v})(x^{ii})(x^{iv})$,

66° $f(x^{i})(x^{ii})(x^{v})(x^{iv})(x^{iii})$,

67° $f(x^{iv})(x^{i})(x^{v})(x^{iii})(x^{ii})$,

68° $f(x^{i})(x^{iii})(x^{v})(x^{ii})(x^{iv})$,

69° $f(x^{iii})(x^{ii})(x^{v})(x^{iv})(x^{i})$,

70° $f(x^{iv})(x^{iii})(x^{v})(x^{ii})(x^{i})$,

71° $f(x^{iii})(x^{ii})(x^{v})(x^{i})(x^{iv})$,

72° $f(x^{ii})(x^{i})(x^{v})(x^{iv})(x^{iii})$,

73° $f(x^{iv})(x^{v})(x^{i})(x^{ii})(x^{iii})$,

74° $f(x^{iv})(x^{v})(x^{ii})(x^{i})(x^{iii})$,

75° $f(x^{iv})(x^{v})(x^{ii})(x^{iii})(x^{i})$,

76° $f(x^{iv})(x^{v})(x^{iii})(x^{i})(x^{ii})$,

77° $f(x^{iv})(x^{v})(x^{i})(x^{iii})(x^{ii})$,

78° $f(x^{iv})(x^{v})(x^{iii})(x^{ii})(x^{i})$,

79° $f(x^{i})(x^{v})(x^{ii})(x^{iii})(x^{iv})$,

80° $f(x^{ii})(x^{v})(x^{iii})(x^{iv})(x^{i})$,

81° $f(x^{iii})(x^{v})(x^{iv})(x^{i})(x^{ii})$,

82° $f(x^{ii})(x^{v})(x^{i})(x^{iii})(x^{iv})$,

83° $f(x^{i})(x^{v})(x^{iii})(x^{iv})(x^{ii})$,

84° $f(x^{iii})(x^{v})(x^{iv})(x^{ii})(x^{i})$,

85° $f(x^{ii})(x^{v})(x^{iii})(x^{i})(x^{iv})$,

86° $f(x^{iii})(x^{v})(x^{i})(x^{iv})(x^{ii})$,

87° $f(x^{i})(x^{v})(x^{iv})(x^{ii})(x^{iii})$,

88° $f(x^{iii})(x^{v})(x^{i})(x^{ii})(x^{iv})$,

89° $f(x^{i})(x^{v})(x^{ii})(x^{iv})(x^{iii})$,

90° $f(x^{ii})(x^{v})(x^{iv})(x^{iii})(x^{i})$,

91° $f(x^{i})(x^{v})(x^{iii})(x^{ii})(x^{iv})$,

92° $f(x^{iii})(x^{v})(x^{ii})(x^{iv})(x^{i})$,

93° $f(x^{ii})(x^{v})(x^{iv})(x^{i})(x^{iii})$,

94° $f(x^{iii})(x^{v})(x^{ii})(x^{i})(x^{iv})$,

95° $f(x^{ii})(x^{v})(x^{i})(x^{iv})(x^{iii})$,

96° $f(x^{i})(x^{v})(x^{iv})(x^{iii})(x^{ii})$, 97° $f(x^v)(x^i)(x^{ii})(x^{iii})(x^{iv})$,

98° $f(x^v)(x^{ii})(x^i)(x^{iii})(x^{iv})$,

99° $f(x^v)(x^{ii})(x^{iii})(x^i)(x^{iv})$,

100° $f(x^v)(x^{iii})(x^i)(x^{ii})(x^{iv})$,

101° $f(x^v)(x^i)(x^{iii})(x^{ii})(x^{iv})$,

102° $f(x^v)(x^{iii})(x^{ii})(x^i)(x^{iv})$,

103° $f(x^v)(x^{ii})(x^{iii})(x^{iv})(x^i)$,

104° $f(x^v)(x^{iii})(x^{iv})(x^i)(x^{ii})$,

105° $f(x^v)(x^{iv})(x^i)(x^{ii})(x^{iii})$,

106° $f(x^v)(x^i)(x^{iii})(x^{iv})(x^{ii})$,

107° $f(x^v)(x^{iii})(x^{iv})(x^{ii})(x^i)$,

108° $f(x^v)(x^{iv})(x^{ii})(x^i)(x^{iii})$,

109° $f(x^v)(x^{iii})(x^i)(x^{iv})(x^{ii})$,

110° $f(x^v)(x^i)(x^{iv})(x^{ii})(x^{iii})$

111° $f(x^v)(x^{iv})(x^{ii})(x^{iii})(x^i)$,

112° $f(x^v)(x^i)(x^{ii})(x^{iv})(x^{iii})$,

113° $f(x^v)(x^{ii})(x^{iv})(x^{iii})(x^i)$,

114° $f(x^v)(x^{iv})(x^{iii})(x^i)(x^{ii})$,

115° $f(x^v)(x^{iii})(x^{ii})(x^{iv})(x^i)$,

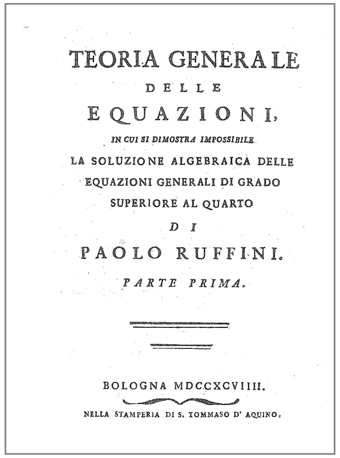
116° $f(x^v)(x^{ii})(x^{iv})(x^i)(x^{iii})$,

117° $f(x^v)(x^{iv})(x^i)(x^{iii})(x^{ii})$,

118° $f(x^v)(x^{ii})(x^i)(x^{iv})(x^{iii})$,

119° $f(x^v)(x^i)(x^{iv})(x^{iii})(x^{ii})$,

120° $f(x^v)(x^{iv})(x^{iii})(x^{ii})(x^i)$,


TEORIA GENERALE
DELLE
EQUAZIONI,
IN CUI SI DIMOSTRA IMPOSSIBILE
LA SOLUZIONE ALGEBRAICA DELLE
EQUAZIONI GENERALI DI GRADO
SUPERIORE AL QUARTO
DI
PAOLO RUFFINI.
PARTE PRIMA.

BOLOGNA MDCCXCVIIII.
NELLA STAMPERIA DI S. TOMMASO D' AQUINO.

Ovenfor ses titelbladet på Ruffinis værk fra 1799. Teksten er:

Generel teori
om ligninger,
hvor det vises,
at det er umuligt
algebraisk at løse
en ligning af grad
større end fire.
Af Paolo Ruffini.
Første del.
Bologna 1799.
Trykt af S. Tommaso
D'Aquino.

Cauchys bidrag

Franskmanden Augustin Louis Cauchy (1789-1857), udgav i 1815 en artikel, hvor han arbejdede videre med nogle af Ruffinis resultater angående antallet af forskellige værdier, som en funktion kan antage, når de variable permuteres. De første ord af artiklens ret lange titel er *Memoire Sur le Nombre des Valeurs*, og selve artiklen har følgende indledning.

> MM. Lagrange og Vandermonde er, tror jeg, de første, der betragtede funktioner af flere variable med hensyn til antallet af værdier de kan give, når de variable byttes rundt. De viste flere interessante sætninger angående dette emne i to artikler publiceret i 1771, den ene i Berlin, den anden i Paris. Siden dengang har nogle italienske matematikere med succes haft travlt med at komme videre på dette område, især M. Ruffini, som gengav resultaterne af sin forskning i Volume XII af Memoirs fra det Italienske Selskab, og i hans *Teori om Numeriske Ligninger*. En af de mest bemærkelsesværdige konsekvenser af disse matematikeres arbejde er, at med et givent antal bogstaver kan man ikke altid danne en funktion, der antager et forudbestemt antal værdier.

Med nutidens øjne er det ikke Cauchys resultat, der er det væsentligste, men den notation og de begreber han indfører i arbejdet med permutationer.

Cauchy bruger i første omgang en funktion af fire variable som eksempel, nemlig en funktion K med en forskrift af formen

$$a_1 a_2^m \cos(a_4) + a_4 \sin(a_3).$$

Ud fra funktionsudtrykket opstiller han de variable i rækkefølge som 1.2.4.3, idet han kun angiver indices for de variable, og skriver dem i den rækkefølge, man møder dem, når man går fra venstre mod højre, og kun skriver hver variabel én gang. En sådan opstilling kalder han en *permutation*. Han indfører så begrebet en *substitution* som et udtryk af formen

$$\begin{pmatrix} 1.2.4.3 \\ 2.4.3.1 \end{pmatrix},$$

og skriver, at det skal forstås sådan, at man ved denne substitution anvendt på K får et nyt funktionsudtryk K' ved at erstatte index 1 med index 2, index 2 med index 4, index 4 med index 3, og index 3 med index 1. Dvs. man får

$$K' = a_2 a_4^m \cos(a_3) + a_3 \sin(a_1).$$

Det, som vi tidligere har kaldt opstilling og permutation, er altså hos Cauchy i 1815 henholdsvis permutation og substitution.

Idet han kalder de to permutationer for A_1 og A_2, indfører han følgende skrivemåde:

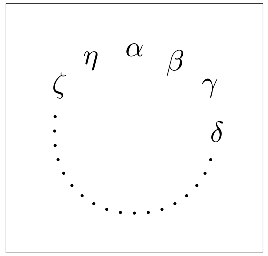
> Så, hvis man kalder permutationen 1.2.4.3 for A_1 og permutationen 2.4.3.1 for A_2 så bliver substitutionen $\begin{pmatrix} 1.2.4.3 \\ 2.4.3.1 \end{pmatrix}$ angivet på følgende måde $\begin{pmatrix} A_1 \\ A_2 \end{pmatrix}$

Ved at indføre en fast notation og navngive substitutionerne gør Cauchy dem til selvstændige objekter, og han går dermed et skridt videre end f.eks. Abbati.

Med moderne betegnelser er Cauchys substitutioner permutationer baseret på *genstande*, ikke på pladser. En permutation som den øverst på siden i linje 5 ville vi opfatte som en afbildning γ, der til hvert tal i den øverste række knytter tallet, der står lige under i den nederste række. Genstandene er de variable a_i, og man permuter en opstilling som f.eks. K med γ ved at *erstatte* genstanden a_i med genstanden $a_{\gamma(i)}$.

Cauchy arbejder med cykler og transpositioner. Den generelle form af en cykel angives som nedenfor til venstre, og illustreres som nedenfor til højre.

$$\begin{pmatrix} \alpha & \beta & \gamma & \cdots & \zeta & \eta \\ \beta & \gamma & \delta & \cdots & \eta & \alpha \end{pmatrix}$$



Her bruger han altså ikke prikker mellem symbolerne. Transpositioner skriver han også som vi på én linje, f.eks. (α, β).

Han indførte et *produkt* af substitutioner således:

> Jeg vil sige, at en substitution er *produktet* af flere andre, når man får samme resultat ved at anvende de andre efter hinanden. For eksempel, hvis man på permutationen A_1 anvender substitutioner $\begin{pmatrix} A_2 \\ A_3 \end{pmatrix}$ og $\begin{pmatrix} A_4 \\ A_5 \end{pmatrix}$ efter hinanden, og man som resultat får permutationen A_6; så er substitutionen $\begin{pmatrix} A_1 \\ A_6 \end{pmatrix}$ ækvivalent med produktet af de to andre, og jeg vil angive denne ækvivalens på følgende måde
>
> $$\begin{pmatrix} A_1 \\ A_6 \end{pmatrix} = \begin{pmatrix} A_2 \\ A_3 \end{pmatrix} \begin{pmatrix} A_4 \\ A_5 \end{pmatrix}$$

Det bemærkes, at han skriver den substitution, der udføres først, forrest, hvor vi gør det omvendt.

Hans formål med artiklen fra 1815 var at vise en generalisering af Ruffinis resultat om, at en funktion i fem variable ikke kan antage 3 eller 4 værdier ved permutation af de variable. Han viser, at antallet af forskellige værdier, som en funktion af n variable kan antage, ikke både kan være større end 2 og mindre end det største primtal p, der er mindre eller lig med n. Han opstiller desuden den formodning, at dette antal ikke både kan være større end 2 og mindre end n, når $n \geq 5$. Formodningen blev bevist i 1845 af Joseph Bertrand (1822-1900).

Efter en pause genoptager Cauchy omkring 1845 sit arbejde med permutationer, og han skriver en artikel, der udover at indføre inverse permutationer indeholder meget af det, der er omtalt i kapitel 2. F. eks. opspaltning i disjunkte cykler, konjugerede permutationer og frembringere for undergrupper af permutationer.

Man fik et nyt redskab i arbejdet med permutationer, da man i anden halvdel af 1800-tallet begyndte at bruge *matricer*. Den første egentlige teori om matricer kom i 1858, da Arthur Cayley (1821-1895) udgav *A Memoir on the Theory of Matrices*. Matricer og hvordan de kan anvendes i forbindelse med permutationer bliver omtalt i det følgende kapitel.

7. PERMUTATIONER OG MATRICER

Vi ser i dette kapitel på en bestemt type afbildninger, der til ethvert talsæt $(x_1, x_2, \cdots, x_n)$ bestående af n tal knytter et talsæt af samme type. Mængden af sådanne talsæt betegnes R^n. For nemheds skyld antages fra starten at $n = 3$, men der kan uden problemer generaliseres til vilkårligt n. Talsættene vil både blive skrevet vandret og lodret.

Ved en *lineær afbildning* forstås en afbildning f, der til ethvert talsæt (x, y, z) knytter et talsæt $f(x, y, z)$, således at

$$f\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a_{11}x + a_{12}y + a_{13}z \\ a_{21}x + a_{22}y + a_{23}z \\ a_{31}x + a_{32}y + a_{33}z \end{pmatrix}.$$

Koefficienterne a_{ij} kan opstilles i en 3 gange 3 *matrix* A:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}.$$

Forskriften for afbildningen f kan så skrives

$$f\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Højresiden skal opfattes som en kortere og mere overskuelig skrivemåde for forskriften, og man kan så sige, at den udregnes som prikproduktet af hver række i matricen A og (x, y, z).

Som eksempler på lineære afbildninger i rummet kan nævnes spejlinger i en plan og drejninger om en linje. F.eks. vil en spejling f i xy-planen have forskriften $f(x, y, z) = (x, y, -z)$, og den tilhørende matrix er

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Permutationsmatricer

Lineære afbildninger omfatter imidlertid også permutationer, idet enhver permutation af koordinaterne i (x, y, z) fremkommer ved et passende valg af tallene a_{ij}. F.eks. vil en ombytning af x og y svare til

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Matricen kaldes en *permutationsmatrix*. I permutationsmatricer er der i hver række og hver søjle netop ét 1-tal, mens der på de øvrige pladser står 0. Der er 6 af den slags 3 gange 3 matricer, og de svarer altså til de 6 permutationer i S_3.

Regning med matricer

Vi ser nu på to matricer A og B, der svarer til lineære afbildninger f og g:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}, \qquad B = \begin{pmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{pmatrix}.$$

Hvis man sammensætter de to lineære afbildninger, således at billedet af et talsæt (x, y, z) er lig med $f(g(x, y, z))$, får man en ny afbildning $f \circ g$. Ved at udregne $f(g(x, y, z))$ ses, at $f \circ g$ har en forskrift af formen

$$(f \circ g) \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} c_{11}x + c_{12}y + c_{13}z \\ c_{21}x + c_{22}y + c_{23}z \\ c_{31}x + c_{32}y + c_{33}z \end{pmatrix},$$

hvor koefficienterne c_{ij} udregnes således

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} \tag{21}$$

Afbildningen $f \circ g$ er altså også lineær, og den tilhørende matrix betegnes AB. Man kalder AB for produktet af A og B.

Af (21) ses, at c_{ij} bestemmes ved at udregne prikproduktet af række i i A og søjle j i B. Denne form for multiplikation kaldes *række-søjle multiplikation*, og den er illustreret nedenfor ved udregning af $c_{21} = 2 \cdot 1 + 1 \cdot 1 + 3 \cdot 2 = 9$.

$$\begin{pmatrix} 0 & 1 & 2 \\ \boxed{2 \;\; 1 \;\; 3} \\ 1 & 0 & 4 \end{pmatrix} \begin{pmatrix} \boxed{\begin{matrix} 1 \\ 1 \\ 2 \end{matrix}} & \begin{matrix} 0 \\ 1 \\ 0 \end{matrix} & \begin{matrix} 2 \\ 3 \\ 0 \end{matrix} \end{pmatrix} = \begin{pmatrix} 5 & 1 & 3 \\ \boxed{9} & 1 & 7 \\ 9 & 0 & 2 \end{pmatrix}$$

For sammensætning af to afbildninger f og g gælder ikke generelt, at $f \circ g = g \circ f$. Den kommutative lov gælder derfor ikke ved multiplikation af matricer; generelt er AB ikke lig med BA.

De to matricer A og B kan også adderes, og dette sker på den simplest tænkelige måde, nemlig ved bare at addere tal på de samme positioner, så hvis $A + B$ kaldes C, gælder, at

$$c_{ij} = a_{ij} + b_{ij}.$$

Matricer kan altså opfattes som selvstændige objekter, der kan adderes og ganges, og regneoperationerne kan laves ved hjælp af cas-værktøjer.

Regning med permutationsmatricer

Et produkt af to permutationer har vi jo indtil nu fundet ved helt konkret at lave nogle ombytninger, men ved brug af permutationsmatricer kan et sådant produkt bestemmes ved at lave egentlige udregninger med tal. Som eksempel kan vi se på produktet af matricerne, der svarer til (123) og (12):

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Resultatet bliver den matrix, som svarer til (123)(12), altså til permutationen (13).

Hvis $m(\sigma)$, $m(\tau)$ og $m(\sigma\tau)$ er de permutationsmatricer, der svarer til permutationerne σ, τ og $\sigma\tau$, gælder generelt, at

$$m(\sigma)m(\tau) = m(\sigma\tau). \tag{22}$$

Da der til hver permutationsmatrix svarer netop en permutation, og matrixmultiplikation kan laves ved hjælp af et cas-værktøj, kan man altså bestemme produktet af to permutationer via deres permutationsmatricer ved hjælp af et cas-værktøj.

Til den identiske permutation σ_1 svarer den lineære afbildning $f(x, y, z) = (x, y, z)$, så dens permutationsmatrix er

$$E = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

For en vilkårlig permutation σ får man af (22), at

$$m(\sigma)m(\sigma^{-1}) = E, \qquad m(\sigma^{-1})m(\sigma) = E,$$

da $\sigma\sigma^{-1} = \sigma^{-1}\sigma = \sigma_1$. Permutationsmatricen for σ^{-1}, altså $m(\sigma^{-1})$, kaldes den *inverse matrix* til $m(\sigma)$, og den betegnes $m(\sigma)^{-1}$. Når man kender matricen $m(\sigma)$, kan $m(\sigma)^{-1}$ bestemmes ved brug af et cas-værktøj.

Standardrepræsentationen

Vi ser nu på permutationer på mængden V af talsæt (x, y, z), hvor $x + y + z = 0$. Elementerne kan skrives $(x, y, -x - y)$. Der gælder f.eks.

$$\sigma_3(x, y, -x - y) = (-x - y, x, y).$$
$$\sigma_2(x, y, -x - y) = (y, x, -x - y).$$

Man kan nøjes med at angive de to første koordinater, og skrive

$$\sigma_3(x, y) = (-x - y, x), \qquad \sigma_2(x, y) = (y, x),$$

da summen af de tre koordinater er 0.

Permutationerne σ_i definerer på denne måde nogle lineære afbildninger af R^2 på R^2, og til disse hører matricer $m(\sigma_i)$, der er vist nedenfor:

$$\boxed{\begin{array}{lll} \sigma_1 : \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \sigma_2 : \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \sigma_3 : \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \\ \sigma_4 : \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix} & \sigma_5 : \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} & \sigma_6 : \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix} \end{array}}$$

Disse matricer er ikke permutationsmatricer, så man kan ikke direkte udføre permutationer ved hjælp af dem, men de har samme algebraiske struktur som permutationerne, d.v.s. at man kan finde produktet af to permutationer ved hjælp af de tilhørende matricer, idet (22) også gælder i dette tilfælde.

Når man til enhver permutation σ i S_3 kan knytte en matrix $m(\sigma)$, således at (22) gælder, siger man, at man har en *matrixrepræsentation*, eller bare en *repræsentation* af S_3. Afbildningen m behøver ikke være enentydig.

Matrixrepræsentationer for en vilkårlig permutationsgruppe blev grundigt studeret i 1900-tallet, og resultaterne er bl.a. blevet anvendt inden for kemi og kvantemekanik. Disse matrixrepræsentationer og deres anvendelser vil ikke blive omtalt yderligere her, da man så ville bevæge sig ind på et ret snævert område, der ikke passer ind i en introduktion til permutationer, som disse noter er tænkt at skulle være.

OPGAVER

Til kapitel 1

1.1 Nedenfor er vist en permutation σ i S_5 og en opstilling p af bogstaverne a, b, c, d og e.

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

p :

e	b	a	d	c
1	2	3	4	5

Bestem opstillingen σp.

1.2 Nedenfor er vist to permutationer σ og π i S_5.

$$\sigma : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \qquad \pi : \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

Bestem hvert af produkterne $\sigma\pi$ og $\pi\sigma$, og angiv σ^{-1}.

1.3 Nedenfor er vist to permutationer α og β i S_4.

$$\alpha : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \qquad \beta : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Løs ligningerne $\sigma\alpha = \beta$ og $\alpha\sigma = \beta$, hvor den ubekendte σ er en permutation i S_4.

1.4 Nedenfor er vist to opstillinger p og q af bogstaverne a, b, c, d, e og f på seks pladser med numrene 1, 2, 3, 4, 5 og 6.

p :

c	b	f	a	d	e
1	2	3	4	5	6

q :

e	b	a	d	f	c
1	2	3	4	5	6

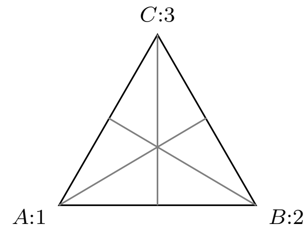
Angiv den permutation σ i S_6 for hvilken $\sigma p = q$.

1.5 Nedenfor er vist to permutationer σ og π i S_4.

$$\sigma : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \qquad \pi : \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

Find den konjugerede til σ ved π.

1.6 Tre genstande A, B og C er placeret i punkter med numrene 1, 2 og 3, der udgør hjørnerne i en ligesidet trekant. Vi vil se på følgende seks afbildninger, der permuterer genstandene. Tre drejninger f_1, f_3 og f_5 på henholdsvis 0, 120 og 240 grader i positiv omløbsretning om midtnormalernes skæringspunkt M; og de tre spejlinger f_2, f_4 og f_6 i midtnormalerne gennem henholdsvis punkt 1, 2 og 3.



Opskriv permutationerne i S_3, der hører til hver af de seks afbildninger.
Find permutationen, der hører til $f_2 \circ f_3$.

1.7 Til hvert opstillingspar (p, q), hvor p og q tilhører $O(A)$, kan man definere en bijektiv afbildning γ af A på sig selv ved

$$\boxed{\gamma(x) \text{ er den genstand i } q\text{, der har erstattet } x \text{ i } p.}$$

At $\gamma(x)$ erstatter x betyder, at de befinder sig på samme plads i hhv. q og p. Man kalder γ en permutation baseret på genstande.

Udtryk γ ved p og q i stil med (4), og udtryk q ved γ og p.

Angiv den permutation γ baseret på genstande, der svarer til

$$p : (\heartsuit, \clubsuit, \diamondsuit, \spadesuit) \qquad q : (\spadesuit, \heartsuit, \clubsuit, \diamondsuit),$$

idet hjerter, klør, ruder og spar betegnes h, k, r og s.

Angiv $\alpha\gamma$, hvor α er permutationen, der ombytter klør og ruder.

Til kapitel 2 om cykler

2.1 Givet permutationen

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

Skriv σ og σ^{-1} som produkter af disjunkte cykler.

2.2 Skriv permutationen $(1374)(15763)(12)(142)$ som produkt af disjunkte cykler.

2.3 Angiv de mulige cykelstrukturer af permutationerne i S_5.

2.4 Skriv permutationen

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

som et produkt af transpositioner.

2.5 Bestem fortegnet for permutationen

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

2.6 Angiv for S_4 de mulige cykelstrukturer, og angiv antallet af permutationer af hver type.

2.7 Løs ligningen $(124)\sigma = (13)(24)$, hvor $\sigma \in S_4$.

2.8 Ved *ordenen* af en permutation σ i S_n forstås det mindste naturlige tal p, for hvilket $\sigma^p = (1)$.

Bestem ordenen af $(124)(35)$ i S_5.

2.9 Vis, at to cykler, $\sigma = (a_1\ a_2\ \ldots\ a_n)$ og $\mu = (b_1\ b_2\ \ldots\ b_n)$, er konjugerede ved π, hvis $\pi(a_i) = b_i$ for $i = 1, 2, \ldots, n$.

Vis dernæst, at to permutationer med samme cykelstruktur er konjugerede.

2.10 Vis, at to konjugerede permutationer σ og μ har samme orden. Ordenen af en permutation blev defineret i opgave 2.8.

Til kapitel 2 om grupper

2.11 Nedenfor er vist fire permutationer fra S_4:

$$\sigma_1 = (1) \qquad \sigma_2 = (12)(34) \qquad \sigma_3 = (13)(24) \qquad \sigma_4 = (14)(23)$$

Vis, at de fire permutationer udgør en undergruppe i S_4 og lav en kompositionstavle for undergruppen.

Gør rede for, at undergruppen er kommutativ.

Angiv et minimalt frembringersæt for undergruppen, altså et frembringersæt, hvor ingen af permutationerne kan undværes.

2.12 Vis, at S_3 er frembragt af (12) og (13).

2.13 Det oplyses, at (1234) og (13) frembringer en undergruppe H i S_4 bestående af otte permutationer.

Bestem disse otte permutationer.

2.14 Vis at undergruppen i S_4 bestående af samtlige lige permutationer frembringes af (123) og (234).

2.15 Gør rede for, at en gruppe H er frembragt af F, netop hvis H er den mindste undergruppe, der indeholder F.

2.16 Lad H være en stabil delmængde af en endelig gruppe G.

Vis, at H i sig selv er en gruppe. Vink: For et vilkårligt element a i H vil potenserne a^p være en endelig mængde, da H er endelig, så der findes to forskellige eksponenter p og q så $a^p = a^q$. Man kan bruge dette til at vise, at det neutrale element i G ligger i H, og at det inverse element til a ligger i H.

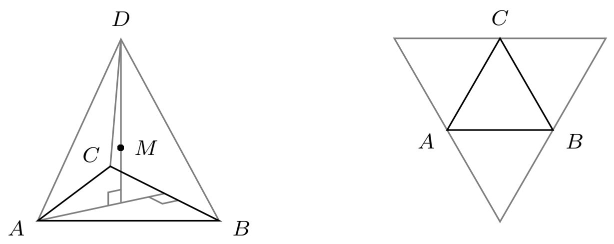
2.17 For en givet permutation α i S_n ser vi på mængden

$$H = \{\sigma \in S_n \,|\, \sigma\alpha = \alpha\sigma\}.$$

Gør rede for, at H er en undergruppe i S_n.

Bestem H, når $\alpha = (12)$ i S_4.

2.18 Et regulært tetraeder har fire hjørner, og fire sideflader, som består af ligesidede trekanter. Gennem hvert hjørne går der en linje vinkelret på den modstående sideflade, og disse fire linjer skærer hinanden i et punkt M, der kaldes tetraederets midtpunkt. Det regulære tetraeder kan udfoldes til en plan figur som vist på illustrationen nedenfor til højre.



Vi tænker os, at de fire hjørner er givet ved koordinaterne til punkter i et 3-dimensionalt koordinatsystem, og at disse er nummereret 1, 2, 3 og 4. Desuden forstiller vi os, at der i hjørnerne befinder sig bevægelige punkter, eller genstande, som her kaldes A, B, C og D. Som udgangspunkt befinder A, B, C og D sig i punkterne 1, 2, 3 og 4.

Til hver permutation σ i S_4 svarer en permutation af A, B, C og D. Hvis σ ikke er en 4-cykel fremkommer σ ved en rumlig afbildning, der enten er en drejning om en linje eller en spejling i en plan.

Beskriv for hver af de cykelstrukturer, der ikke er 4-cykler, en drejning eller en spejling, der giver en permutation af den pågældende type.

Skriv 4-cyklen (1234) som et produkt af en 3-cykel og en 2-cykel, og find derved en drejning og spejling, som kan sammensættes til en afbildning, der giver en permutation, der svarer til (1234).

Hvilke afbildninger svarer de lige permutationer til?

Til kapitel 3

3.1 Sæt $\boldsymbol{x} = (x_1, x_2, x_3, x_4)$, $\sigma = (1243)$ og

$$f(x_1, x_2, x_3, x_4) = x_1^2 x_3 + x_2 - x_4$$

Find $\sigma\boldsymbol{x}$ og $f(\sigma\boldsymbol{x})$.

3.2 Gør rede for, at

$$\sigma(x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}),$$

for en vilkårlig permutation σ i S_n

3.3 En funktion af 4 variable a, b, c og d har forskriften

$$ab + cd$$

Bestem antal forskellige værdier, som funktionen kan antage ved permutation af de variable.

3.4 En funktion af 8 variable har forskriften

$$x_1^2 + x_2 + x_3 - x_4 + x_5^2 - x_6 + x_7 - x_8.$$

Bestem antal forskellige værdier, som funktionen kan antage.

3.5 Lad f være den funktion af fire variable, der har forskriften

$$(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4).$$

Vis, at f skifter fortegn ved enhver transposition.

Find antallet af værdier som f antager ved samtlige permutationer af de variable.

3.6 Find en funktion af fem variable, der antager 40 værdier ved permutation af de variable.

3.7 Angiv stabilisatorgrupperne for funktionerne i skemaet på side 37 sidst i kapitel 3.

3.8 Lad f være funktionen $f(a,b,c,d) = (a-b)(c-d)$. Hvis man behandler denne funktion helt som funktionen i eksemplet på side 32-33 får man et skema som nedenfor.

(1)	(12)(34)	(13)(24)	(14)(23)
(12)	(34)	(1324)	(1423)
(123)	(134)	(243)	(142)
(13)	(1234)	(24)	(1432)
(132)	(234)	(124)	(143)
(23)	(1342)	(1243)	(14)

Af cykelstrukturen på permutationerne i den øverste række i skemaet ses, at stabilisatorgruppen H er en *normal undergruppe* i S_4, det vil sige, at hvis en permutation h tilhører H, så vil enhver konjugeret til h i S_4 også tilhøre H. For enhver permutation p i S_4 vil php^{-1} altså også tilhøre H. Undergruppen i den øverste række af tabellen på side 33 er ikke normal i S_4.

De 6 rækker i skemaet kaldes *sideklasser*. De 2 spørgsmål øverst på næste side går ud på at vise, at hvis a_1 og a_2 ligger i samme sideklasse, og b_1 og b_2 ligger i samme sideklasse, så vil a_1b_1 og a_2b_2 også ligge i samme sideklasse.

$\cdots$	a_1	$\cdots$	a_2	$\cdots$
$\cdots$	b_1	$\cdots$	b_2	$\cdots$
$\cdots$	a_1b_1	$\cdots$	a_2b_2	$\cdots$

Først bemærkes, at hvis to permutationer c_1 og c_2 ligger i samme række, så har de formen $c_1 = qp_1$ og $c_2 = qp_2$, hvor q er første permutation i sideklassen, og p_1 og p_2 tilhører H.

Gør rede for, at c_1 og c_2 tilhører samme sideklasse, netop hvis $c_2 = c_1h_c$ for et h_c i H.

Der gælder altså specielt, at $a_2 = a_1h_a$ og $b_2 = b_1h_b$, hvor h_a og h_b tilhører H.

Vis, at a_2b_2 ligger i samme sideklasse som a_1b_1 ved at benytte at H er normal i S_4, hvilket betyder at der findes h i H, således at $h_ab_1 = b_1h$.

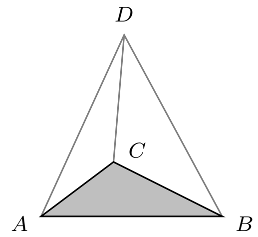
Udregn a_1b_1 og a_2b_2, når $a_1 = (24)$, $a_2 = (1432)$, $b_1 = (34)$ og $b_2 = (1324)$.

Man kan altså regne med sideklasser ved at regne med repræsentanter for sideklasserne.

Giv et eksempel på, at det tilsvarende ikke gælder for permutationerne i tabellen på side 33.

3.9 Denne opgave skal give en geometrisk illustration af Abbatis formel, hvor funktioner er erstattet af geometriske figurer. Vi ser som i opgave 2.18 på et regulært tetraeder, og på de permutationer og afbildninger, der er omtalt i den opgave.

Ved en permutation σ i S_4 af A, B, C og D vil trekant ABC blive afbildet over i enten sig selv eller en af de andre sideflader.



Angiv de permutationer, der gør, at ABC føres over i en trekant, der som punktmængde er lig ABC, og angiv antallet af forskellige punktmængder man kan få af ABC ved at permutere de fire hjørner på samtlige 24 mulige måder.

Til kapitel 4

4.1 Find hele tal s og t, så $sp + tq = 1$, når $p = 5$, og q er henholdsvis 1, 2, 3 og 4.

Det kan bemærkes, at man på side 39 kunne man have brugt Bézouts identitet: Hvis p og q er to hele tal med største fælles divisor d, findes der to hele tal s og t, så $sp + tq = d$. Det kan så også bemærkes, at der findes generelle metoder baseret på Euklids algoritme til at bestemme s og t, men her kan man altså let finde s og t ved at prøve sig frem.

4.2 Formålet med denne opgave er at vise, at S_5 er lig med undergruppen H frembragt af $\sigma = (12345)$ og $\pi = (12)$. Fremgangsmåden er at vise, at alle transpositioner i S_5 er med i H. Da enhver permutation kan skrives som et produkt af transpositioner, vil enhver permutation så også være med i H.

Vis ved direkte udregning, at alle permutationerne $\sigma^i\pi\sigma^{-i}$ er transpositioner bestående af naboer, altså af formen $(a\,b)$, hvor $b = a + 1$.

Udregn (12)(23)(12), og vis, at alle transpositioner af formen $(a\,b)$, hvor $b = a + 2$, er med i H.

Vis at alle transpositioner er med i H.

4.3 Lad H betegne undergruppen i S_5 frembragt af de to permutationer σ og π, hvor

$$\sigma = (12345), \quad \text{og} \quad \pi = (2354).$$

Gør rede for, at enhver permutation af formen $\sigma^i\pi^j$ må tilhøre H, og angiv antallet af den slags permutationer.

Vis, at der findes en potens σ^i således at $\pi\sigma = \sigma^i\pi$, og benyt dette til at vise, at permutationerne $\sigma^i\pi^j$ udgør en stabil mængde, som altså må være lig med undergruppen H.

Til kapitel 5

5.1 Denne opgave går ud på at finde frem til, hvordan forskellige symmetriske polynomier $f(x, y)$ af to variable kan udtrykkes som polynomier af de to elementarsymmetriske polynomier

$$s_1(x, y) = x + y \qquad s_2(x, y) = xy.$$

Udtryk $x^2 + y^2$ og $x^2y + xy^2$ ved s_1 og s_2.

Udtryk $g(x, y) = x^3 + y^3$ ved s_1 og s_2, f.eks. ved at udregne $g(x, y) - (x + y)^3$ og bruge det foregående resultat.

Et vilkårligt symmetrisk tredjegradspolynomium af x og y har formen $a+b(x+y)+cxy+d(x^2+y^2)+e(x^2y+xy^2)+f(x^3+y^3)$; udtryk et sådant polynomium ved s_1 og s_2.

Udtryk x^2y^2, $x^3y + xy^3$ og $x^4 + y^4$ ved s_1 og s_2.

5.2 Omskriv følgende funktion af tre variable

$$x^3 + y^3 + z^3 - (x + y + z)^3$$

ved at hæve parentesen, og brug dette resultat til at udtrykke $x^3 + y^3 + z^3$ ved hjælp af de elementarsymmetriske funktioner i tre variable.

5.3 Denne opgave handler om, hvordan løsningerne til en tredjegradsligning kan udledes ved brug af den fremgangsmåde, der på side 47-48 blev brugt til at løse fjerdegradsligninger. Dog med den forskel, at der i denne opgave bruges komplekse tal. Tredjegradsligningen skrives på formen

$$x^3 + a_2x^2 + a_1x + a_0 = 0 \tag{23}$$

Lad ω være det komplekse tal med længden 1 og et argument på 120 grader, altså tallet $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

Gør rede for, at $\omega^3 = 1$.

Vi sætter $\boldsymbol{x} = (x_1, x_2, x_3)$ og ser på funktionen

$$f(\boldsymbol{x}) = (x_1 + \omega x_2 + \omega^2 x_3)^3$$

Vis, at $f(\sigma \boldsymbol{x})$ kun antager to værdier, nemlig

$$z_1 = (x_1 + \omega x_2 + \omega^2 x_3)^3 \qquad z_2 = (x_1 + \omega x_3 + \omega^2 x_2)^3$$

ved alle permutationer σ i S_3. Vink: Bruges ikke et cas-værktøj, kan man f.eks. benytte omskrivninger af følgende type

$$\omega^3(x_1 + \omega x_2 + \omega^2 x_3)^3 = (\omega(x_1 + \omega x_2 + \omega^2 x_3))^3.$$

Værdierne z_1 og z_2 er løsninger til ligningen $(z - z_1)(z - z_2) = 0$, altså til andengradsligningen

$$z^2 - (z_1 + z_2)z + z_1 z_2 = 0 \tag{24}$$

Gør rede for, at koefficienterne $b_1 = z_1 + z_2$ og $b_0 = z_1 z_2$ er symmetriske funktioner af x_1, x_2 og x_3, og at de derfor kan udtrykkes ved koefficienterne i tredjegradsligningen.

Vis, at $b_0 = (a_2^2 - 3a_1)^3$.

Det er forholdvis besværligt at bestemme b_1, men det oplyses, at andengradsligningen bliver

$$z^2 + (2a_2^3 - 9a_2 a_1 + 27a_0)z + (a_2^2 - 3a_1)^3 = 0$$

Når man kender z_1 og z_2, har man ligningssystemet

$$x_1 + \omega x_2 + \omega^2 x_3 = \sqrt[3]{z_1} \tag{25}$$
$$x_1 + \omega^2 x_2 + \omega x_3 = \sqrt[3]{z_2} \tag{26}$$
$$x_1 + x_2 + x_3 = -a_2 \tag{27}$$

til bestemmelse af x_1, x_2 og x_3.

Løs ligningssystemet ved bl.a. at benytte, at $1 + \omega + \omega^2 = 0$.

Til kapitel 6

6.1 Denne opgave går ud på at gennemskue, hvordan Ruffini har opbygget tabellen over S_5 på siderne 53-55.

Hvilke permutationer består første søjle af?

Hvordan er søjle 2, 3, 4 og 5 konstrueret ud fra søjle 1?

Brug principperne i de to foregående spørgsmål til at lave tabeller som Ruffinis over S_2 og S_3.

Forklar, hvordan første søjle i Ruffinis tabel er konstrueret.

6.2 Nedenfor er vist en oversættelse af paragraf 267 i Ruffinis bog *Teoria generale delle Equazioni* fra 1799. Hvad Ruffini forstår ved "en sammensat permutation af første slags"er ikke væsentligt i denne sammenhæng.

> 267. Af dette følger klart, at hvis en funktion
>
> $$y = f(x^i)(x^{ii})(x^{iii})(x^{iv})(x^v)$$
>
> har en sådan form, at man har
>
> $$f(x^i)(x^{ii})(x^{iii})(x^{iv})(x^v) = f(x^{ii})(x^i)(x^{iv})(x^v)(x^{iii})$$
>
> kan dette ske ved en sammensat permutation af første slags, og derfor er også
>
> $$f(x^i)(x^{ii})(x^{iii})(x^{iv})(x^v) = f(x^{ii})(x^i)(x^{iii})(x^{iv})(x^v)$$

Hvilken permutation σ i S_5 er der tale om i linje 4?

Forklar, hvordan man kan udlede linje 7 ud fra linje 4.

6.3 Lad $f(\boldsymbol{x})$ være en funktion, der svarer til 1° i Ruffinis tabel, og lad σ være permutationen (1532).

Angiv numrene på de funktioner i Ruffinis tabel, der svarer til funktionerne $f(\sigma\boldsymbol{x})$, $f(\sigma^2\boldsymbol{x})$, $f(\sigma^3\boldsymbol{x})$ og $f(\sigma^4\boldsymbol{x})$.

6.4 I kapitel 2 blev to permutationer σ og μ kaldt konjugerede, hvis der findes en permutation π så $\pi\sigma = \mu\pi$, og senere blev det så vist, at to konjugerede permutationer har samme cykelstruktur. Cauchy går omvendt frem i *Mémoir sur les arrangements que l'on peut former avec des lettres données* fra 1845. Han kalder først to permutationer for konjugerede, hvis de har samme cykelstruktur og løser så i det viste uddrag følgende problem.

> Problem I. - Idet der er givet n variable x, y, z $\cdots$ og to konjugerede permutationer P, Q dannet med disse variable, skal man finde en tredje permutation R, som er løsning til den lineære ligning
>
> $$RP = QR.$$
>
> Løsning. - Udtryk permutationen P ved hjælp af sine cykliske faktorer, idet alle de variable vises, skriv derefter permutationen Q under permutationen P, præsenteret på samme måde som P. Fjern dernæst parenteserne og kommaerne, der er placeret mellem de variable. De to permutationer Q, P vil så være omformet til opstillinger, som repræsenterer de to led af permutationen R.

Hans navne for konjugerede og permutationer er *semblables* og *substitutions*, men her er de gengivet med nutidige betegnelser.

Brug Cauchys opskrift ovenfor til at finde en permutation π så $\pi\sigma = \mu\pi$, når

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

Sammenlign denne løsningsmetode med den, der er skitseret i opgave 2.9.

Til kapitel 7

7.1 Angiv matricerne A og B, der svarer til de lineære afbildninger, som man får ved at permutere et talsæt (x_1, x_2, x_3, x_4) ved permutationerne (124) og (13)(24) i S_4.

Bestem matricen AB, og angiv cykelstrukturen af den tilhørende permutation.

Angiv de inverse matricer til A og B.

7.2 Ved den *transponerede* matrix til en 4 gange 4 matrix A forstås den matrix B for hvilken $b_{ij} = a_{ji}$. Denne matrix betegnes også A'. For eksempel har man

$$A = \begin{pmatrix} 4 & 9 & 0 & 1 \\ 7 & 3 & 2 & 2 \\ 1 & 8 & 0 & 5 \\ 0 & 3 & 1 & 6 \end{pmatrix}, \qquad A' = \begin{pmatrix} 4 & 7 & 1 & 0 \\ 9 & 3 & 8 & 3 \\ 0 & 2 & 0 & 1 \\ 1 & 2 & 5 & 6 \end{pmatrix}.$$

I det følgende kan benyttes, at $(AB)'$ er lig med $B'A'$ og at $(AB)^{-1}$ er lig med $B^{-1}A^{-1}$ for alle A og B.

Lad nu A være en 4 gange 4 permutationsmatrix svarende til en permutation σ.

Beskriv udseendet af A, når σ er en transposition, og gør rede for, at $A^{-1} = A' = A$ i dette tilfælde.

Benyt, at en vilkårlig permutation σ kan sammensættes af transpositioner til at vise, at der for en vilkårlig permutationsmatrix A gælder, at $A^{-1} = A'$.

7.3 Ved standardrepræsentationen af S_4 repræsenteres en permutation σ ved den matrix, der svarer til den lineære afbildning, som man får ved at se på de første 3 koordinater, når et talsæt $(x_1, x_2, x_3, -x_1 - x_2 - x_3)$ permuteres ved σ.

Bestem matricerne A og B, der ved standardrepræsentationen svarer til (124) og (13)(24), og angiv A^{-1} og B^{-1}.

Det græske alfabet

De små bogstaver

α	alfa	ι	iota	ρ	rho
β	beta	κ	kappa	σ	sigma
γ	gamma	λ	lambda	τ	tau
δ	delta	μ	my	υ	ypsilon
ϵ	epsilon	ν	ny	ϕ	fi
ζ	zeta	ξ	ksi	χ	ki
η	eta	o	omikron	ψ	psi
θ	teta	π	pi	ω	omega

De store bogstaver

Γ	gamma	Ξ	ksi	Φ	fi
Δ	delta	Π	pi	Ψ	psi
Θ	teta	Σ	sigma	Ω	omega
Λ	lambda	Υ	ypsilon		

Indeks