Hvad søgte de og hvad fandt de?

Kombinatoriske løsningsformler til algebraiske ligninger – fra Cardano til Cauchy – Del 2*

Uffe Thomas Jankvist og Neslihan Sağlanmak

Institut for Matematik og Fysik
Roskilde Universitetscenter
Box 260
DK–4000 Roskilde
utj@ruc.dk, neslihan@ruc.dk

7 Lagranges store analyse

Joseph Louis Lagranges (1736–1813) *Reflexions sur la résolution algébrique des équations* [23] fra 1770–71 står som en milepæl i den algebraiske ligningsløsningsteori. I stedet for direkte at springe ud i at udvikle en – eller arbejde videre med en allerede opfundet – metode til løsning af n'tegradsligningen, analyserer Lagrange de allerede etablerede metoder til tredje-, og fjerdegradsligningens løsning. Lagrange betegner sin tilgang til problemet som en *a priori* tilgang, i modsætning til en *a posteriori* tilgang. Således er Lagranges mål ikke at finde en metode der virker, hvilket var den tilgang matematikere før Lagrange fortrinsvist havde benyttet sig af. Hensigten med Lagranges *a priori* tilgang er derimod at finde ud af, hvorfor og hvordan metoder som Cardanos, Ferraris, Tschirnhaus', Bezouts og Eulers giver en løsning til generelle tredje- og fjerdegradsligninger, og hvorfor de fejler med hensyn til den generelle femtegradsligning. *A priori* tilgangen består i, at Lagrange så at sige arbejder »baglæns«, det vil sige, at han bestemmer rødderne til hjælpeligningen som rationale funktioner af rødderne til den oprindelige ligning. Hermed

*Artiklen er grundet dens længde og omfang delt i to. Første del og litteraturlisten er trykt i forrige nummer af Normat.

bliver egenskaberne ved hjælpeligningens rødder åbenlyse og viser klart, hvorfor disse rødder giver rødderne til den oprindelige ligning. Lagrange viser altså, at problemet med ligningsløsning afhænger af egenskaberne ved de rationale funktioner i rødderne.

Lagrange begynder med en udlægning af Cardanos metode til løsning af den generelle tredjegradsligning

$$x^3 + px + q = 0. \tag{1}$$

Ved substitutionen $x = u + v$ fås

$$u^3 + v^3 + q + (u + v)(3uv + p) = 0, \tag{2}$$

som underlægges betingelsen

$$3uv + p = 0 \quad \Rightarrow \quad v = -\frac{p}{3u}. \tag{3}$$

Indsættes nu udtrykket for v i ligning (2), som herefter ganges igennem med u^3, fås en sjettegradsligning i u

$$u^6 + qu^3 - \left(\frac{p}{3}\right)^3 = 0. \tag{4}$$

Dette er hjælpeligningen som Cardanos formel bygger på, og som Lagrange i sin afhandling kalder den *reducerede ligning* (la réduite).

I stedet for at gå direkte til beregningen af løsningen,[11] altså bestemme rødderne x_i til (1) som funktion af u_i, rødderne til (4), så bestemmes u_i som funktion af x_i. Da (4) er en sjettegradsligning har den seks rødder, altså ender man med seks rødder til den oprindelige tredjegradsligning. Til al »held« er disse seks rødder $u_1, \ldots, u_6$ parvis ens, hvilket Lagrange viser på essentielt følgende vis: Da (4) er en andengradsligning i u^3, antager de seks rødder opløftet i tredje potens $u_1^3, \ldots, u_6^3$ kun to værdier; y_1 og y_2, hvor $y_1 y_2$ ifølge Viète-relationerne er lig det konstante led $-(\frac{1}{3}p)^3$. Man kan, eventuelt ved omnummerering, antage at

$$u_1^3 = u_2^3 = u_3^3 = y_1 \quad \text{og} \quad u_4^3 = u_5^3 = u_6^3 = y_2.$$

Kaldes u_1, u_2, u_3 for »1. gruppe« er således de tre løsninger til $u^3 = y_1$

$$\sqrt[3]{y_1}, \quad \omega\sqrt[3]{y_1}, \quad \omega^2\sqrt[3]{y_1},$$

i en eller anden rækkefølge, hvor ω er en primitiv enhedsrod. Kaldes u_4, u_5, u_6 »2. gruppe«, er de tre løsninger til $u^3 = y_2$

$$\sqrt[3]{y_2}, \quad \omega\sqrt[3]{y_2}, \quad \omega^2\sqrt[3]{y_2},$$

i en eller anden rækkefølge. Altså haves at

$$u_2 = \omega u_1, \;\; u_3 = \omega^2 u_1, \;\; u_5 = \omega u_4, \;\; u_6 = \omega^2 u_4. \tag{5}$$

[11] Hvilket er muligt da (4) er en andengradsligning i u^3.

Da man fra Viète-relationerne har at $y_1y_2 = -(\frac{1}{3}p)^3$, må nogle af produkterne af et u_i fra 1. gruppe og et u_j fra 2. gruppe være lig $-\frac{1}{3}p$; antag, evt. efter omnummerering indenfor de to grupper, at $u_1u_4 = -\frac{1}{3}p$. Dette bevirker, at også $u_2u_6 = \omega^3u_1u_4 = -\frac{1}{3}p$ og ligeledes at $u_3u_5 = -\frac{1}{3}p$. Da man ifølge (3) har, at $uv = -\frac{1}{3}p$, haves, hvis man lader v_i betegne den værdi af v som korresponderer med u_i, at

$$v_1 = u_4,\ \ v_2 = u_6,\ \ v_3 = u_5,\ \ v_4 = u_1,\ \ v_5 = u_3,\ \ v_6 = u_2.$$

Følgeligt er der altså kun tre forskellige værdier af $u_i + v_i$, nemlig

$$u_1 + u_4,\ \ u_2 + u_6 = \omega u_1 + \omega^2 u_4,\ \ u_3 + u_5 = \omega^2 u_1 + \omega u_4,$$

som altså er tre rødder til den oprindelige tredjegradsligning (1)

$$x_1 = u_1 + u_4,\ \ x_2 = \omega u_1 + \omega^2 u_4,\ \ x_3 = \omega^2 u_1 + \omega u_4. \tag{6}$$

Men tilbage til bestemmelsen af $u_1, \ldots, u_6$ som funktioner af rødderne x_1, x_2, x_3. Dette gøres nemt, hvis man benytter, at $\omega^2 + \omega + 1 = 0$ og ganger anden ligning af (6) med ω^2 henholdsvis ω og tredje ligning med ω henholdsvis ω^2, og dernæst lægger disse til den første ligning i (6). Herved får man

$$x_1 + \omega^2 x_2 + \omega x_3 = 3u_1 + (1 + \omega + \omega^2)u_4$$

henholdsvis

$$x_1 + \omega x_2 + \omega^2 x_3 = 3u_4 + (1 + \omega + \omega^2)u_1.$$

Altså er

$$u_1 = \frac{1}{3}(x_1 + \omega^2 x_2 + \omega x_3) \quad \text{og} \quad u_4 = \frac{1}{3}(x_1 + \omega x_2 + \omega^2 x_3).$$

Den reducerede lignings resterende rødder følger direkte af udtrykkene i (5)

$$u_2 = \frac{1}{3}(\omega x_1 + x_2 + \omega^2 x_3), \qquad u_3 = \frac{1}{3}(\omega^2 x_1 + \omega x_2 + x_3),$$
$$u_5 = \frac{1}{3}(\omega x_1 + \omega^2 x_2 + x_3), \qquad u_6 = \frac{1}{3}(\omega^2 x_1 + x_2 + \omega x_3).$$

Lagrange ser altså, at man kan udtrykke alle rødderne til hjælpeligningen (4), som altså med rette også kan kaldes en resolvent, ved at permutere rødderne x_1, x_2, x_3 i udtrykket

$$\frac{1}{3}(x_1 + \omega x_2 + \omega^2 x_3),$$

hvilket er et rationalt[12] udtryk i x_1, x_2, x_3.

[12]Med rational menes implicit, her og i det følgende, rationalt over et koefficientlegeme; her indeholdende n'te enhedsrødderne.

Pointen i at løse den reducerede ligning er at bestemme nogle, og dermed alle, u_i. Deraf drager Lagrange følgende sindrige konklusioner: *A priori* forklarer det, hvorfor hjælpeligningen har grad 6. Da hjælpeligningens koefficienter er rationale funktioner af koefficienterne i den oprindelige ligning, hvis koefficienter er de elementære symmetriske polynomier, er hjælpeligningens koefficienter symmetriske i x_1, x_2, x_3. Derved gælder, at hvis et udtryk i x_1, x_2, x_3 er en rod til hjælpeligningen, så er samtlige permutationer af x_1, x_2, x_3 i udtrykket også en rod til hjælpeligningen. Da eksempelvis $3u_4 = x_1 + \omega x_2 + \omega^2 x_3$ ved permutation af rødderne har seks forskellige værdier[13], gælder at disse er rødder til den reducerede ligning, som derfor må have grad 6. Yderligere forklarer Lagrange ved dette, hvorfor hjælpeligningen er en andengradsligning i u^3. F.eks. antager u_4^3 kun to forskellige værdier ved de $3! = 6$ permutationer af rødderne, hvilket ses på følgende vis: Da

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

så gælder

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

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

hvilket giver, at

$$\left(\frac{1}{3}\right)^3 (x_1 + \omega^2 x_2 + \omega x_3)^3 \quad \text{og} \quad \left(\frac{1}{3}\right)^3 (x_1 + \omega x_2 + \omega^2 x_3)^3$$

er rødderne til en ligning, der altså har grad 2. Generelt vil Lagranges observation kunne formuleres som

Proposition 1 *Lad f være et rationalt udtryk i n ubekendte $x_1, \ldots, x_n$. Hvis f antager m forskellige værdier $f_1, f_2, \ldots, f_m$ ved alle permutationer af $x_1, \ldots, x_n$, så er f en rod i en monisk ligning $\theta(t) = 0$ af grad m*

$$\theta(t) = (t - f_1)(t - f_2) \cdots (t - f_m),$$

hvis koefficienter er symmetriske i $x_1, \ldots, x_n$ og altså kan udtrykkes som rationale funktioner af de elementære symmetriske polynomier. Yderligere gælder, at hvis f er rod i en anden ligning $\phi = 0$ med koefficienter symmetriske i $x_1, \ldots, x_n$ så er graden af $\phi \geq m$.

Proposition 1 er dermed et første skridt på vejen til en generel metode til at finde rødderne til et n'tegradspolynomium. Hvis man finder et rationalt udtryk i de n rødder, $f(x_1, \ldots, x_n)$, som antager færre end n værdier ved permutation, så kan alle $f_{\sigma_i}(x_1, \ldots, x_n)$ bestemmes som rødder til $\theta(t) = 0$, hvor $\theta(t)$'s koefficienter kan bestemmes rationalt ved koefficienterne i den oprindelige ligning. Hvordan $\theta(t)$'s

[13] Med en værdi mener Lagrange udtrykkets formelle værdi og ikke den numeriske værdi [23]. Han antager implicit, at addition og multiplikation er kommutative, det vil sige, at $ab = ba$ og $a + b = b + a$ [18].

koefficienter bestemmes i koefficienterne til den oprindelige ligning er i og for sig irrelevant; pointen er, at det kan gøres ved rationale operationer. Derudover gælder selvfølgelig, at $f(x_1, \ldots, x_n)$ er af en sådan beskaffenhed, at man kan beregne $x_1, \ldots x_n$ ud fra f og dets værdier ved permutation af rødderne.

Efter yderligere at have taget Tschirnhaus', Eulers og Bezouts metoder til løsning af tredjegradsligningen samt Ferraris løsning af fjerdegradsligningen under behandling, når Lagrange frem til en konklusion. Nemlig den, at samtlige af metoderne går ud på at finde funktioner af rødderne til den oprindelige ligning på en sådan måde at; (1) den resulterende ligning (eller ligninger) er af mindre grad end den oprindelige ligning eller kan splittes op i andre ligninger af mindre grad end denne, og (2) værdierne af de søgte rødder nemt kan udledes fra dem. Lagrange stiller dernæst spørgsmålet om, hvorvidt det altid vil være muligt at bestemme sådanne funktioner for ligninger af enhver grad, det vil sige et vilkårligt antal rødder, hvorefter han påpeger, at det lader til at være særdeles svært at besvare dette spørgsmål generelt. For ligninger af grad ≤ 4 kan de simpleste funktioner, som afslører disses rødder skrives på følgende form

$$x_1 + \omega x_2 + \omega^2 x_3 + \ldots + \omega^{n-1} x_n,$$

hvor $x_1, x_2, x_3, \ldots, x_n$ er rødderne til den oprindelige ligning. Det ville på baggrund af dette, fortsætter Lagrange, være nærliggende ved induktion at konkludere, at en hvilken som helst ligning af vilkårlig grad ville kunne løses ved hjælp af en resulterende ligning, hvis rødder kan repræsenteres på samme form

$$x_1 + \omega x_2 + \omega^2 x_3 + \omega^3 x_4 + \ldots$$

Bemærk iøvrigt, at udtryk som ovenstående er de såkaldte Lagrange-resolvente.

Forsøget med at løse femtegradsligningen ud fra en generalisering af ovenstående vil gå ud på at finde et polynomium

$$f_1 = f(x_1, \ldots, x_5) = x_1 + \omega x_2 + \ldots + \omega^4 x_5,$$

hvor $x_1, \ldots, x_5$ er rødderne og ω er en primitiv femte enhedsrod. Ved permutation af rødderne er der i alt $5! = 120$ forskellige værdier $(f_1, f_2, \ldots, f_{120})$, men man observerer også, at der for f_i gælder, at også ωf_i, $\omega^2 f_i$, $\omega^3 f_i$ og $\omega^4 f_i$ er indeholdt i mængden af de 120 værdier. Sammenholdt med denne observation fås af proposition 1, at $\theta(t)$ indeholder faktoren[14]

$$(t - f_1)(t - \omega f_1)(t - \omega^2 f_1)(t - \omega^3 f_1)(t - \omega^4 f_1) = t^5 - f_1^5,$$

hvor θ i alt vil indeholde 24 af ovenstående udtryk hvert med forskelligt f_i. Dette giver, at θ er et polynomium af grad 24 i t^5. Hvis man kan finde rødder til dette specielle polynomium af grad 24, viser Lagrange, at man derudaf kan bestemme rødderne $x_1, \ldots, x_5$. Problemet er imidlertid, at det ikke er muligt for ham at bestemme de 24 rødder og det på trods af at han ved et genialt ræsonnement yderligere formår at reducere hjælpeligningen til en ligning af grad 6 [30] [6].

[14] Lighedstegnet indses ved at $(x-1)(x-\omega)(x-\omega^2)(x-\omega^3)(x-\omega^4) = 0$.

Lagrange koncentrerer sig på bemærkelsesværdig vis om de essentielle egenskaber for en lignings løsbarhed; det vil sige *a priori* studiet af funktioner $f(x_1, \ldots, x_n)$ og deres værdier ved samtlige permutationer af $x_1, \ldots, x_n$. Lagrange kalder selv denne procedure for »ligningernes metafysik«. Således er Lagrange altså at betragte som en pioner med hensyn til eksplicit brug af permutationer inden for algebraen, omend heller ikke han kommer med en streng definition af en permutation. Desværre for gruppeteoriens udvikling ligger Lagranges opmærksomhed ved udtrykket $f(x_1, \ldots, x_n)$ og ikke ved selve permutationen. Lagrange opfandt af den årsag en ad hoc notation til at betegne, om et udtryk blev ændret ved en permutation eller ej, i stedet for at besvære sig med at opfinde en notation for selve permutationen[15] [18].

Lagrange indser det fundamentale i at klassificere udtryk efter den indvirkning en permutation har på dem, men af ovenstående grund er de af Lagranges sætninger, som i dag er en del af gruppeteorien, formuleret med udgangspunkt i de algebraiske udtryk og ikke permutationerne selv. Et andet og vigtigt eksempel på Lagranges bidrag til gruppeteorien (og dermed permutationsteorien), som udsprang af hans søgen efter at kunne klassificere udtrykkene $f(x_1, \ldots, x_n)$, er hans sætning om, at graden af θ i proposition 1, altid er $n!$ eller en divisor i $n!$.[16] For Lagrange tjener denne sætning primært til at få begreb om, hvilke grader en resolvent kan have i forhold til graden n af den oprindelige ligning, men det er ikke desto mindre denne sætning, som i en mere generel gruppeteoretisk kontekst er navngivet efter Lagrange.[17] Dermed er denne sætning et biprodukt af en af Lagranges andre sætninger, som kan siges at være en udvidelse af proposition 1, hvor to funktioner sammenholdes relativt til hinanden. Her gengives den i en moderne version.

Sætning 1 *Lad ϕ og ψ være rationale funktioner i rødderne $x_1, \ldots, x_n$ til den oprindelige ligning. Hvis ϕ antager m forskellige værdier ved de permutationer som lader ψ invariant, så er ϕ en rod i en ligning af grad m, hvis koefficienter er rationale udtryk i ψ og i koefficienterne i den oprindelige ligning. Specielt gælder, hvis ϕ er invariant ved de permutationer som lader ψ invariant, at ϕ kan udtrykkes rationalt i ψ og koefficienterne i den oprindelige ligning.*[18]

Eftersom Lagrange ikke eksplicit udtaler sig om, hvorvidt han tror femtegradsligningen kan løses algebraisk eller ej, er der således blandt nutidige matematikere delte opfattelser om netop dette. Den mest gængse opfattelse har dog været, at Lagrange ikke troede på løsbarheden af femtegradsligningen, men man kan ikke underbygge det ud fra hans arbejde, og spørgsmålet er, om ikke det er den store anseelse Lagrange nyder, der har præget tolkningen af hans vage udtalelser omkring emnet [25]. Faktum er i hvert fald, at han lader begge muligheder stå åbne.

[15] I denne notation betyder $f[(x_1)(x_2)(x_3)]$, at f ændrer værdi ved alle permutioner på nær identiteten, og $f[(x_1, x_2)(x_3)]$ at f forbliver uændret ved permutationen (angivet i cykelnotation ved x'ernes fodtegn) (12)(3), men ændres af enhver permutation som substituerer x_1 eller x_2 med x_3.

[16] Mere præcist viser Lagrange at $m = n!/|I(f)|$, hvor $I(f)$ er stabilisatoren til f, det vil sige undergruppen af permutationer som lader f invariant.

[17] Lagranges sætning: *I en endelig gruppe vil ordnen af en undergruppe altid være en divisor i gruppens orden.*

[18] Selve sætningen er hos Lagrange meget løst formuleret, og det fremgår først præcist, hvad den implicerer, når beviset for den gennemgås [23].

Fra et Galoisteoretisk synspunkt ser vi, at Lagrange (og Vandermonde) med Lagrange-resolventene tager et skridt i Galois' retning. Og oversætter man til gruppeteoretisk terminologi, har man den letteste implikation i Galois' sætning anvendt på den generelle n'tegradsligning: Hvis S_n er en opløselig gruppe, så er den generelle n'tegradsligning algebraisk løsbar [30] [25].

Det er først rigtigt med Lagrange og Vandermonde, at permutations- og invariansbetragtninger bliver en etableret del af den algebraiske ligningsløsningsteori. Deres, om man så må sige, genistreg er, at de projicerer den gamle alkymistiske kombinationstanke over på udtryk i rødderne og indser, at det netop er sådanne udtryk samt deres værdier ved samtlige permutationer, der er ligningsløsningens »metafysik«. I begges arbejder er der ligheder til Cauchys permutationer, omend der stadig er nogen vej endnu, da de behandler udtryk i rødderne og ikke selve permutationerne.

8 Anvendelsen af permutationer

Som vi så i foregående afsnit, studerede matematikere som f.eks. Vandermonde og Lagrange permutationer af rødderne i et polynomium. Deres studium af permutationer var dog altid knyttet til en bestemt kontekst, nemlig den af polynomier, og deres notation var ikke altid lige bekvem.

Ruffini anvendte permutationerne på en mere direkte vis, omend stadig i forbindelse med ligningsløsning, i sine afhandlinger (1799–1813). I Ruffinis bevis forekommer tilmed elementer af, hvad vi i dag vil betegne som gruppeteori. Med Cauchys artikel fra 1815 blev der sat fokus på selve permutationerne, der blev udviklet »regneregler« for disse, en mere sindrig notation og i det hele taget blev permutationsteorien i højere grad en selvstændig disciplin.

Paolo Ruffini (1765–1822)

Augustin Louis Cauchy (1789–1857)

Først en for det efterfølgende vigtig definition.

Definition 1 *Med en* cykel *menes en permutation σ af elementerne $x_1, x_2, \ldots, x_k$, hvorom der gælder at $\sigma(x_1) = x_2, \ldots, \sigma(x_{k-1}) = x_k, \sigma(x_k) = x_1$.*

8.1 Ruffinis permutationsbegreb

Det kan diskuteres, hvorvidt Paolo Ruffini (1765–1822) var den første matematiker, der var overbevist om den generelle femtegradslignings uløselighed, men han er den første som søger at bevise det, hvilket han gør i sit værk fra 1799.[19] Imidlertid er der ingen af hans samtidige kollegaer som vil anerkende beviset, og Ruffini kæmper således en forgæves kamp i årene fra 1799 til 1813, hvor han løbende udgiver nye udgaver af sit bevis [29]. Heller ikke forsøget på at optage en korrespondance med Lagrange fører til noget, idet Lagrange ikke lader høre fra sig. Vi skal ikke her redegøre i detaljer for Ruffinis bevis eller dets eventuelle mangler,[20] men derimod skitsere nogle af de biprodukter, der opstod som følge af hans bevis.

Ruffini søger i sit værk, med udgangspunkt i Lagranges arbejde omhandlende funktioners opførsel ved permutation af variablene (rødderne), at bestemme samtlige sådanne permutationer af variablene, som lader funktionerne invariante. Ruffinis permutationsbegreb er dog anderledes end det i dag udbredte, men forstås alligevel bedst ved brug af moderne termer [32]: Hvis f er en given funktion i n variable, forstår Ruffini med en *permutazione* en mængde G af omarrangementer (nutidens permutationer) fra den symmetriske gruppe S_n, hvorom der gælder

$$\forall \sigma \in G: \quad f \circ \sigma = f,$$

for et givet f. Vi vil nedenfor referere til Ruffinis *permutazione* som permutationsgruppen[21] G til f.

Ruffini deler sine permutationsgrupper op i to hovedtyper; *simple* (semplice) og *sammensatte* (composte) permutationsgrupper. Med en simpel permutationsgruppe forstår han en mængde af permutationer, som er frembragt ved potensopløftning af et enkelt element. Simple permutationsgrupper kan ifølge Ruffini være af to typer; enten er de potenser af en permutation, som består af én cykel, eller også er de potenser af en permutation, som er et produkt af flere cykler. De sammensatte permutationsgrupper er frembragt af flere end en permutation og er derfor ikkecykliske. Disse inddeles i to hovedtyper, som svarer til transitive og intransitive undergrupper.

Definition 2 *En permutationsgruppe G kaldes* intransitiv*, hvis der eksisterer to værdier a og b i mængden af argumenter for $f(x_1, \ldots, x_n)$, hvorom det gælder, at*

$$\forall \sigma \in G: \quad \sigma(a) \neq b,$$

og transitiv *hvis et sådant par (a, b) ikke eksisterer.*

De transitive permutationsgrupper kan være henholdsvis *primitive* eller *imprimitive.*

Definition 3 *En transitiv gruppe G kaldes* imprimitiv*, såfremt der eksisterer en ikke-triviel delmængde H af de n argumenter, hvis billede under enhver permutation σ i gruppen G er enten H selv eller disjunkt med H, det vil sige*

$$\forall \sigma \in G: \quad \sigma(H) = H \quad \vee \quad \sigma(H) \cap H = \emptyset,$$

[19] *Teoria generale delle equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto.*

[20] En sådan gennemgang kan findes i [30].

[21] Fremover vil vi nøjes med at betegne denne som G.

og primitiv *hvis en sådan delmængde ikke eksisterer.*

Ruffinis inddeling i de ovennævnte fem typer kan anskueliggøres ved tabel 1 [32].

simple permutationsgrupper (*permutazioni semplici*)	• potenser af en cykel • potenser af en ikke-cykel
sammensatte permutationsgrupper (*permutazioni composte*)	• intransitive • transitive, imprimitive • transitive, primitive

Tabel 1: Ruffinis klassifikation af permutationsgrupper [32]. Med en ikke-cykel menes en permutation, som er et produkt af flere cykler.

Efter at have klassificeret permutationsgrupperne går Ruffini i gang med sit bevis. Vi vil her blot gennemgå et par af elementerne i dette bevis. Ruffini viser, at der for den generelle femtegradsligning ikke eksisterer nogen resolvent af mindre grad end 5. Mere præcist viser han, at der ikke eksisterer et rationalt udtryk i de n objekter, som kun antager 3, 4 eller 8 værdier under permutationerne af de n rødder, når $n > 4$. Til dette benytter Ruffini Lagranges resultat; antallet af forskellige værdier, som et udtryk i n variable kan antage, er en divisor i $n!$. Ruffinis idé er at bestemme, hvilke divisorer af $n!$ der i dette tilfælde er mulige – altså hvilke grader femtegradsligningens resolvent ifølge Langranges proposition 1 kan antage. Til dette formål definerer han *graden af ækvivalens* (grado de uguaglianza) af en funktion f i de n rødder af en ligning, som antallet af de forskellige permutationer, der ikke ændrer f; altså antallet af permutationer i permutationsgruppen til f. Hvis p betegner graden af ækvivalens, haves således ifølge Lagranges resultat, at p er en divisor i $n!$, og at $n!/p$ er antallet af forskellige værdier af f. Med udgangspunkt i dette bestemmer Ruffini de mulige værdier af p for alle de fem typer af permutationsgrupper (jf. tabel 1) ved omstændelige udregninger, og han viser, at værdien af p ikke kan være et multiplum af 5. Det vil sige, at for femtegradsligningen, $n = 5$, haves

$$\frac{n!}{p} = 5k,$$

hvor $k \in \mathbf{N}$, altså $n!/p \geq 5$, og ifølge proposition 1 er resolventen således mindst en femtegradsligning.

Ruffini antager uden bevis, at et hvilket som helst algebraisk udtryk indeholdt i en antaget løsning kan udtrykkes rationalt i rødderne af ligningen og n'te enhedsrødderne.[22] En mulighed er, at udtrykket f giver en resolvent, som er en ren femtegradsligning

$$z^5 - r = 0.$$

Lad os sige, at $(f_1, \ldots, f_{120})$ er værdierne af f under permutation af rødderne $x_1, \ldots, x_5$. Ruffini undersøger alle disse og observerer, at enten er alle f_i'er ens (hvilket kan udelukkes da $z^5 - r = 0$ i hvert fald har fem forskellige rødder), eller at f antager fem forskellige værdier. Er det sidste tilfældet, viser Ruffini, at r ikke er rational i rødderne, hvilket er i modstrid med hans ovenstående korrekte antagelse

[22] Det er denne antagelse uden bevis som er »hullet« i Ruffinis bevis af femtegradsligningens algebraiske uløselighed og som først vises af Abel i ca. 1824 [32].

[18]. For en mere indgående gennemgang af Ruffinis bevis henvises til [29] samt moderne fremstillinger i [9], [28] og [30].

Historien om Ruffinis kamp for at få anerkendt sit bevis for femtegradsligningens algebraiske uløselighed må siges at være lidt af en matematisk tragedie. Måske var sandheden i virkeligheden den, at datidens matematikmiljø ikke rigtig ville eller var modent til at indse uløseligheden af femtegradsligningen. En af de eneste som tog en interesse i Ruffinis arbejde var ironisk nok Cauchy, da han ellers var kendt for at være en af de værste matematikere med hensyn til det at give andre kredit og anerkendelse. Men Cauchy var inspireret af Ruffini, og i sit arbejde om permutationer fra 1815 generaliserer han da også netop nogle af Ruffinis resultater, samtidig med at han præsenterer en helt ny notationsform. Dette er måske den eneste måde, hvorpå Ruffinis arbejde kom til at spille en rolle i udviklingen af matematikken [2].

8.2 Cauchys »substitutioner«

Augustin Louis Cauchys (1789–1857) i særdeleshed vigtigste bidrag til gruppeteorien er hans sætning om, at hvis p er et primtal som deler ordenen af gruppen G, så findes der i G en undergruppe af orden p. Denne sætning førte senere Sylow til en generalisering, kendt som Sylows tre sætninger, som fortsat er en af milepælene indenfor gruppeteorien.[23]

I nærværende artikel vil vi imidlertid koncentrere os om Cauchys tidlige arbejde med gruppeteoretiske elementer i hans artikel[24] [11] fra 1815. Cauchys primære formål med denne artikel er at bevise følgende sætning:

Sætning 2 *Antallet af forskellige værdier R, som et ikke-symmetrisk udtryk K, i n ubekendte antager, kan ikke være mindre end det største primtal p, som ikke overstiger n, med mindre $R = 2$.*

Cauchy deler beviset for denne sætning op i beviserne af de følgende tre propositioner:

1. Hvis $R < p$, så vil enhver værdi af K ikke kunne ændres ved en permutation[25] af orden p.

2. Hvis en værdi K er invariant ved en permutation af orden p, så forbliver den uændret under enhver 3-cykel.

3. Hvis en værdi K er invariant under enhver 3-cykel, så er K enten symmetrisk i dets variable eller antager præcis to værdier under samtlige permutationer.

Cauchy pointerer, at dette er en generalisering af et af Ruffinis resultater; umuligheden af at have et udtryk i fem eller flere variable, som antager netop tre eller fire forskellige værdier. Vi skal også her koncentrere os om biprodukterne af Cauchys bevis; bidrag til den i dag kendte permutationsteori. For en gennemgang af beviset se foruden [11] f.eks. [18].

[23] Moderne formuleringer af Cauchys og Sylows sætninger kan bl.a. findes i [21].

[24] *Mémoire sur le nombre des valeurs qu'une function peut acquérir, lorsqu'on y permute de toutes les manières possibles les quantités qu'elle renferme.*

[25] Ved permutation menes det som Cauchy kalder en substitution (se senere).

Cauchy bevæger sig i sin artikel ud over permutationers tilknytning til ligningsløsningsteorien og nævner kun i forbifarten, at variablene kan anses som værende rødder i et eller andet polynomium. Hans egen motivation, påpeger han, for sit studium af permutationer stammer fra talteorien, som han har sammenkædet med Ruffinis arbejde. Bemærkelsesværdigt er det ligeledes, at Cauchy i sit bevis af ovenstående sætning introducerer begreber og notationer som stadig benyttes i moderne terminologi. F.eks. benytter han to-rækkersnotationen for en permutation, hvilket han er den første der gør; en sådan findes hverken hos Lagrange eller Ruffini. Tager vi f.eks. de fire objekter $1, 2, 4, 3$ i given rækkefølge, og lader $2, 4, 3, 1$ være permutationen af disse, så etablerer Cauchy for denne permutation »loven«

$$1 \mapsto 2, \qquad 2 \mapsto 4, \qquad 4 \mapsto 3, \qquad 3 \mapsto 1.$$

Dette er den samme lov, som man også benytter for permutationer i dag, nemlig en bijektiv afbildning af mængden $\{1, 2, \ldots, n\}$ på sig selv. Cauchy kalder denne lov for en *substitution* – altså det der for os er en permutation – og han skriver den som[26]

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

Altså er en substitution en to-liniers notation; øverste linie er objekternes oprindelige rækkefølge, og nederste linie er billederne af objekterne. Med en *permutation* mener han derimod en en-linies notation, det vil sige rækkefølgen af objekterne a_1, $a_2, \ldots, a_n$, f.eks. som før 2, 4, 3, 1. Cauchy er dog udmærket klar over, at rækkefølgen, hvori de fire objekter bliver omarrangeret, ikke har nogen betydning for hans definition af en permutation (en permutation af n objekter kan således opskrives på $n!$ forskellige måder). F.eks. gælder at

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

Cauchy begrænser sig dog ikke til kun fire objekter, men forsøger at håndtere et vilkårligt antal objekter, men selv om han foreslår en generel notation

$$\begin{pmatrix} a & b & c & \ldots & l \\ \alpha & \beta & \gamma & \ldots & \lambda \end{pmatrix}$$

for en vilkårlig permutation, er det klart at dette »billede« kun er praktisk for et mindre antal af objekter. Selv benytter han derfor den forkortede notation

$$\begin{pmatrix} A_1 \\ A_2 \end{pmatrix},$$

hvor A_1 og A_2 er vilkårlige permutationer af de pågældende objekter.

I relation til ovenstående redegørelse af Cauchys arbejde skal det påpeges, som eksempelvis sætning 2 antyder, at Cauchys abstraktionsniveau ikke er mere vidtløftigt end, at han tager udgangspunkt i netop et udtryk i n variable, samt hvilke

[26] Cauchy benyttede punktum og ikke mellemrum mellem objekterne, hvorfor han f. eks. skriver (1 2 4 3) som (1.2.4.3).

egenskaber dette måtte have under den symmetriske gruppe S_n. Dette er ikke meget forskelligt fra f.eks. Lagranges tilgang, men Cauchy indser altså, at det essentielle i udtrykket er variablenes indbyrdes placering, hvorfor udtrykket udmærket kan erstattes af en »pladsholder« – det han kalder en permutation, og det er netop disse, og ikke udtrykkene selv, som Cauchy grupperer i forhold til visse egenskaber. Derved tager Cauchy et stort skridt fremad i udviklingen af den generelle permutations- og gruppeteori, da han ligeledes har udviklet regneregler for disse.

Cauchys måske vigtigste bidrag i sin 1815-artikel er sammensætningen (le produit) af to permutationer. Ved sammensætningen $\binom{A_2}{A_3}\binom{A_4}{A_5}$ skal forstås den substitution, der fremkommer ved først at foretage substitutionen $\binom{A_2}{A_3}$ og derefter $\binom{A_4}{A_5}$. Han definerer, at $\binom{A_2}{A_3}\binom{A_4}{A_5}$ anvendt på A_1 giver en ny »permutation« A_6, med samme resultat som når A_6 anvendes på A_1. Altså

$$\binom{A_1}{A_6} = \binom{A_2}{A_3}\binom{A_4}{A_5}.$$

Lad os illustrere dette med et eksempel. Vi vælger A_1 og A_2 ligesom Cauchy gør, A_3, A_4 og A_5 vælger vi selv, da Cauchy ikke giver eksempler på disse. Lad os f.eks. antage, at vi har »permutationerne«

$$A_1 = (1\ 2\ 4\ 3) \qquad A_2 = (2\ 4\ 3\ 1) \qquad A_3 = (4\ 3\ 2\ 1)$$
$$A_4 = (3\ 4\ 1\ 2) \qquad A_5 = (4\ 1\ 2\ 3).$$

Vi har nu at

$$\begin{aligned}\binom{A_2}{A_3}\binom{A_4}{A_5} &= \begin{pmatrix}2&4&3&1\\4&3&2&1\end{pmatrix}\begin{pmatrix}3&4&1&2\\4&1&2&3\end{pmatrix}\\ &= \begin{pmatrix}2&4&3&1\\4&3&2&1\end{pmatrix}\begin{pmatrix}4&3&2&1\\1&4&3&2\end{pmatrix}\\ &= \begin{pmatrix}2&4&3&1\\1&4&3&2\end{pmatrix}.\end{aligned} \tag{7}$$

Når (7) anvendes på A_1 får vi, ifølge Cauchys betragtning,

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

som vi altså døber A_6,

$$A_6 = (2\ 1\ 4\ 3).$$

Ligeledes har vi at

$$\binom{A_1}{A_6} = \begin{pmatrix}1&2&4&3\\2&1&4&3\end{pmatrix} = \begin{pmatrix}2&4&3&1\\1&4&3&2\end{pmatrix}, \tag{8}$$

hvorfor vi altså, i overensstemmelse med Cauchy, har at (7) er lig (8).

Cauchy viser også, at der altid findes et naturligt tal N, således at[27]

$$\begin{pmatrix} A_1 \\ A_t \end{pmatrix}^N = \begin{pmatrix} A_1 \\ A_1 \end{pmatrix}$$

og betegner herefter det mindste N som *graden* (degré) af substitutionen. Han definerer også en cyklisk permutation, dennes potenser samt en transposition.

Med Ruffini og Cauchy bliver der sat et helt andet fokus på permutationerne. Måderne hvorpå Ruffini og Cauchy indfører deres permutationer er dog som set vidt forskellige. Cauchys permutationer, altså substitutionerne, svarer til vore dages permutationer, hvorimod Ruffinis permutationer (permutazioni) svarer til, hvad vi i dag vil betegne som en stabilisator G_f af f, det vil sige $G_f = \{g \in S_n \mid g(f) = f\}$. Karakteriseringen af disse undergrupper G_{f_i} i forskellige typer er alle meget grundigt behandlet hos Ruffini. Dette er ikke det eneste »forklædte« element fra gruppeteorien i Ruffinis arbejde, også hans »grad af ækvivalens« kan oversættes til et moderne gruppebegreb, nemlig det af indexet af en permutationsgruppe. Man kan således argumentere for, at Ruffini i sit arbejde benytter sig af vore dages gruppeteori, eller i alt fald elementer af denne. Ruffini er således den første, der introducerer, hvad der svarer til stabilisatoren, indexet, cykelopløsningen af en permutation (permutationsgruppe) samt primitive og imprimitive permutationer. Derudover viser han, at S_5 ikke indeholder nogen undergrupper af index 3 eller 4.

Cauchys behandling af permutationer som en selvstændig disciplin og ikke kun som et virkemiddel på et udtryk i flere variable er af stor vigtighed. Med dette fulgte regneregler så som sammensætning og potensopløftning af permutationer, som i forhold til tidligere notationsformers kunnen medførte klart nemmere beregninger, og man kan ikke overvurdere disse værktøjers betydning for udviklingen af f.eks. Galoisteorien.

Også eksempler på brugen af invarians og symmetri kan findes i teksterne. Hos Ruffini har vi tilfældet med en transitiv imprimitiv gruppe indeholdende delmængden H, hvorom det gælder, at den kan være invariant overfor en permutation $\sigma \in S_n$; $\sigma(H) = H$. Hos Cauchy har vi underinddelingen af sætning 2 i de tre propositioner, i hvis formuleringer der indgår såvel udtryk der er invariante overfor permutationer som udtryk der er symmetriske i deres variable, samtidig med at der i selve sætningen (sætning 2) optræder udtrykket K, som er ikke-symmetrisk i de n ubekendte.

Cauchys to-liniers substitutionsbegreb lider af ikke at være entydigt. Men man må formode, at denne opskrivning for fremtidige matematikere har haft den fordel, at gruppestrukturen, det vil sige aksiomerne om lukkethed, associativitet samt eksistens af et inverst element og identiteten, har været mere åbenlys end, hvis Cauchy i et hug havde opfundet cykelnotationen.

9 Konklusion

Formålet med nærværende artikel har været at vise, at Galois' banebrydende indarbejdelse af gruppeteori i teorien for algebraiske ligninger ikke markerede en så

[27] Med notationen $\binom{A_1}{A_t}^N$ skal forstås sammensætningen af N substitutioner lig substitutionen $\binom{A_1}{A_t}$.

pludselig overgang, som man måske kunne tro, men at ligningsløsningsteorien derimod har været underlagt en mere kontinuerlig udvikling med adskillige frugtbare tiltag i de ca. 300 års forskning før Abels og Galois' arbejder. Disse tidligere tiltag og angrebsmetoder til løsningen af den generelle n'tegradsligning har, med sit indhold af kombinatoriske og gruppeteoretiske elementer, såsom permutations- og invariansbetragtninger, i større eller mindre omfang, ledt mere eller mindre naturligt frem til Galois' resultater.

Selve udviklingen af de matematiske begreber kombination, permutation og invarians kan derimod ikke beskrives som værende en kontinuert proces, den er som sådan mere sporadisk. F.eks. er udviklingen af kombinationsbegrebet en i særdeleshed spredt affære, hvilket et opslag under »Combination« i Krügels *Mathematisches Wörterbuch* fra 1803 da også viser [20]. Udviklingen af kombinationer finder sted inden for så forskellige discipliner som lykkespil, forsikring, kryptering, musik med flere, hvilket rækker langt ud over denne artikels problemfelt. Målet i denne artikel har dog også kun været at se på, hvorledes de tre ovennævnte begreber har influeret på ligningsløsningsteorien i kraft af de forskellige tilgange til denne, og hvilken udvikling begreberne herunder har gennemgået.

Overordnet kan man sige, at tiden fra Cardano til Cauchy er karakteriseret ved tre forskellige tilgange i metoderne til den algebraiske løsning af ligninger; (1) symmetriske udtryk i rødderne, (2) substitutioner, variabelskift og elimination og (3) brugen af n'terødder og Lagrange-resolvente.

Brugen af symmetriske udtryk i rødderne finder vi først og fremmest hos Viète og Girard i forbindelse med formuleringen af Viète-relationerne. Symmetriske udtryk i rødderne findes også hos Waring og Vandermonde i forbindelse med hovedsætningen for symmetriske polynomier. I Vandermondes elegante løsning af andengradsligningen v.h.a. de elementære symmetriske polynomier anvendes ligeledes symmetribetragtninger.

Cardano anvender substitution i sin løsningsformel for tredjegradsligningen. Variabelskift og elimination af de mellemliggende led i en ligning er bærende elementer i Tschirnhaus' metode (og Eulers lignende metode). Bezouts metode bygger ligeledes på elimination. Det overordnede sigte her er, at substitution, variabelskift og elimination skal føre til en ny ligning. Denne ligning skal være af lavere grad end den oprindelige, og dens rødder skal indgå i udtrykket for rødderne til den oprindelige ligning.

Brugen af n'terødder finder vi først hos Bezout, idet han som den første anvender disse eksplicit. Også Vandermonde anvender n'terødder i sit forsøg på at opstille en funktion for den generelle n'tegradsligning. Såvel Vandermonde som Lagrange benytter sig af resolvente. Brugen af n'terødder er et vigtigt element i Lagranges gennemgang af metoderne samt i de såkaldte Lagrange-resolvente. Ruffini tager udgangspunkt i Lagranges arbejde, nærmere bestemt proposition 1, hvorfor brugen af resolvente også er et bærende element i hans bevis; Ruffini viser jo, at der for den generelle femtegradsligning ikke findes en resolvent af grad ≤ 5.

I de ca. 200 år fra Cardano til Lagrange, forsøgte matematikerne uden held, ved hjælp af ovennævnte tre tilgange, at finde algebraiske løsninger til højeregradsligninger. Man kan måske derfor ved første øjekast mene, at matematikerne i denne periode ikke var synderlig succesfulde, da ingen af dem jo nåede deres mål – at løse den generelle n'tegradsligning algebraisk. Imidlertid skulle selve rejsen vise sig at være vigtigere end destinationen, da det var ud af biprodukterne af periodens

kontinuerlige søgen, at de første optrin til gruppeteorien opstod, f.eks. i form af den i artiklen beskrevne alkymistiske kombinationstanke. Disse ca. 200 år kan derfor på ingen måde siges at have været sløve, faktisk var det i denne periode at grundlaget for Vandermondes og Lagranges store arbejder blev grundlagt, hvorfor disse års betydning for Abels og Galois' resultater heller ikke kan overvurderes.

Lagranges arbejde har som bekendt haft en enorm betydning for Abel og Galois, som de også selv påpegede, og hele permutationsbetragtningen for at bestemme Galoisgruppen i moderne abstrakt algebra stammer fra netop Lagrange og Vandermonde. Ligeledes er Ruffinis og især Cauchys arbejde om permutationer i den efterfølgende periode[28] enkeltstående og har således også været en uundgåelig kilde til inspiration for den næste generations matematikere, såvel Abel som Galois.

10 Taksigelser til . . .

Tak til David Heiberg Backchi for sin medvirken i udarbejdelsen af den rapport[29] som ligger til grund for nærværende artikel. Tak til Bernhelm Booß-Bavnbek for flittig vejledning og rådgivning i forbindelse med såvel rapport som artikel. Tak til Tinne Hoff Kjeldsen for hjælp undervejs samt ideen om at lave rapporten til en artikel. Ligeledes tak til Kirsti Andersen og Henrik Kragh Sørensen for henholdsvis kommentarer og inspiration til den oprindelige rapport.

[28] Cauchy udgiver ikke selv noget nyt omhandlende permutationer førend i 1844, hvor han vender tilbage til sit 1815-arbejde og videreudvikler dette. [25]

[29] Nærværende artikel er baseret på en projektrapport [7] udført på kandidatoverbygningen ved Roskilde Universitetscenter. Rapporten kan anskaffes via http://mmf.ruc.dk/