Gjensyn med Abels og Ruffinis bevis for umuligheten av å løse den generelle n'tegradsligningen algebraisk når $n \geq 5$

Christian Skau

Institutt for matematikk og statistikk
Universitetet i Trondheim, AVH
N-7055 Dragvoll

1. Innledning

Et resultat som har fascinert generasjon etter generasjon av matematikere, er teoremet som sier at den generelle n'tegradsligningen ikke kan løses ved algebraiske operasjoner ("ved rotutdragninger") når $n \geq 5$. Men idag nevnes Niels Henrik Abels (1802–1829) berømte bevis fra 1824 [2] for denne umuligheten kun som en fotnote til den såkalte Galois-teorien. Denne teorien, som skyldes den bråmodne franske matematikeren Évariste Galois (1811–1832), drept 21 år gammel i en duell, representerer kvintessensen av en lang utvikling innen ligningsteorien der Lagrange (1736–1813), Ruffini (1765–1822) og Abel er sentrale navn. Galois' teorem gir en nødvendig og tilstrekkelig betingelse, via den såkalte Galois-gruppen, for når et polynom har røtter som kan uttrykkes ved algebraiske operasjoner. Selv lang tid etter Galois' banebrytende arbeid ble løsninger av (spesielle) ligninger ansett som det sentrale problem innen algebra, og dette synet var fremtredende gjennom mesteparten av det nittende århundret. Det var først etter en lang modningsprosess at perspektivet på Galois-teorien og på gruppebegrepet ble utvidet. Med Emil Artins innflytelsesrike forelesningsserie om Galois-teori i Hamburg sommeren 1926 ble kroppteoriaspektet ved Galois-teorien definitivt etablert, og Galois-gruppen ble definert via symmetrier til tallkroppen som naturlig er knyttet til det gitte polynomet [6]. (Se også [38].) Forbindelsen til ligningsteorien ble tonet ned betydelig. Alle moderne presentasjoner av Galois-teorien bygger på Artins fremstilling, som forøvrig er meget elegant. I oppbyggingen av denne teorien må en hel rekke abstrakte begreper innføres, og det kreves betydelig matematisk skolering og modenhet for tilegnelse av teorien. Etter å ha vært igjennom Galois-teorien for første gang opplever vel også mange det som et antiklimaks (selv om det burde være det motsatte!) når resultatet om uløsbarheten av femtegradsligningen presenteres som et korollar. Dette på grunn av ren utmattethet i anstrengelsen etter å absorbere denne omfattende teorien.

Det kunne derfor være av en viss interesse med et gjensyn med Abels opprinnelige bevis. Dette knytter seg til de enkleste prinsipper, slik som den Euklidske algoritmen og irredusibilitet av polynomer, samt symmetriske polynomer. Beviset er derfor også tilgjengelig for en større skare matematisk interesserte. I det hele

tatt er et av de mest fascinerende aspekter ved den klassiske ligningsteorien hvilke enkle betraktninger som ligger til grunn for denne.

La oss skissere Abels bevisidé: Først viser han at alle rotuttrykkene som forekommer i en algebraisk løsning av den generelle n'tegradsligningen er polynomer i de n røttene til denne ligningen. Dette gjøres ved at man arbeider seg suksessivt fra det "ytterste" (eller "siste") rottegnet som forekommer i løsningen, inn til det "innerste" (eller "første") rottegnet. Denne delen av beviset er blitt stående essensielt uforandret i ettertiden og gir et utmerket eksempel på Abels virtuose bruk av et polynoms irredusibilitet som middel til å resonnere. I dag er disse teknikkene "folklore" i algebra, men ifølge Sylow [30] var det Abel som først innførte irredusibilitet som prinsipp. Riktignok hadde Gauss (1777–1855) tidligere (1801) i sitt studium av sirkeldelingsligningen $x^n - 1 = 0$ definert begrepet irredusibelt polynom, men han bruker ikke irredusibiliteten som middel i sine videre utledninger.

Den andre delen av Abels bevis, den "substitusjonsteoretiske" (eller "gruppeteoretiske") delen, opptar to tredjedeler av hans publiserte bevis [3] og kan forenkles betydelig. Abel kjente ikke til den italienske legen og matematikeren Paolo Ruffinis forsøk på å bevise uløsbarheten av den generelle n'tegradsligningen i årene mellom 1799 og 1813 [27,28]. Ruffinis arbeider var meget uklare og vanskelige å tyde, blant annet fordi han benyttet seg av en meget komplisert notasjon. Samtidens matematikere reagerte stort sett negativt på hans påståtte bevis, unntatt Cauchy (1789–1857) som var positiv. I ettertid må man erkjenne at selv om Ruffinis bevis inneholder et stort gap, så er hans "gruppeteoretiske" betraktninger helt riktige og mye enklere enn Abels. Dette ble klargjort av Pierre Wantzel (1814–1848) i et arbeid fra 1845 [33], og det er Wantzels versjon av Ruffinis bevis vi skal presentere i stedet for andre delen av Abels eget bevis. Gapet i Ruffinis bevis var at han antok uten bevis det som Abel først beviste, nemlig at en algebraisk løsning av den generelle n'tegradsligningen kan bringes på en slik form at rotuttrykkene som forekommer, er polynomer i røttene til ligningen. Ruffinis "gruppeteoretiske" bevis starter med det "innerste" rottegnet i løsningen, og han viser ved en enkel betraktning at det må være en kvadratrot. Så viser han ved like enkle betraktninger at det neste rottegnet må være en kubikkrot dersom $n \geq 3$. På analog måte viser han at dette samme rottegnet må være en femterot dersom $n \geq 5$, og han har oppnådd en selvmotsigelse. Det er en bemerkelsesverdig symmetri i de to delene som beviset naturlig består av: I den ene delen starter man med det ytterste rottegnet og arbeider seg suksessivt innover mot det innerste; i den andre delen starter man med det innerste rottegnet og beveger seg utover.

Vi skal presentere en forholdsvis utførlig gjennomgåelse av ligningsteorien som leder opp til Abels og Ruffinis bevis. I den forbindelse gjennomgår vi også Lagranges analyse av de klassiske, kjente løsninger av tredje- og fjerdegradsligningene, og hans forsøk på ut fra denne analysen, å løse den generelle femtegradsligningen. Lagrange var den direkte inspirator for både Ruffini og Abel. Vi vil først presentere de klassiske løsningene av annen-, tredje- og fjerdegradsligningene idet vi poengterer det ved løsningene som peker mot Abels og Ruffinis resultater. Vi vil også skissere den klassiske ligningsteoriens to "pillarer". Den ene er "Lagrange-Ruffini-komponenten", som er teorien for polynomer i n variable, med drøfting av hvor mange forskjellige verdier disse antar under permutasjoner av de variable. Den andre er "Abel-komponenten", som består av den Euklidske algoritmen, største felles divisor til to polynomer, og irredusible polynomer, spesielt binomiske polynomer.

2. Grunnleggende begreper

Vi må presisere hva vi mener med "den generelle n'tegradsligningen" og hva det vil si å løse en ligning algebraisk ("ved rotutdragninger"). For dette trenger vi å introdusere noen nøkkelbegreper. Samtidig innfører vi en hendig notasjon. Vi vil hele tiden arbeide innenfor de komplekse tall $\mathbf{C}$, i stedet for å behandle kropper i almindelighet. Bevisene vi skal gi, kan imidlertid overføres ordrett til en mer generell situasjon, slik at tapet av generalitet bare er tilsynelatende. Vi mener at et slikt utgangspunkt har pedagogiske fordeler. En annen sak er at pionerene innen ligningsteorien — Lagrange, Ruffini, Abel og Galois — hadde det samme utgangspunktet (se **7**).

Tallkropp

Med en *tallkropp* (opprinnelig kalt "rasjonalitetsområde") forstår vi en delmengde E av $\mathbf{C}$ slik at 0 og 1 er med i E, og der addisjon, subtraksjon, multiplikasjon og divisjon (bortsett fra med 0), de såkalte rasjonale regningsarter, er utførbare innenfor E. Eksempler på tallkropper er de rasjonale tall $\mathbf{Q}$ og de relle tall $\mathbf{R}$. To andre eksempler er

$$E_1 = \{a + bi | a, b \in \mathbf{Q}\},$$

der i er den imaginære enheten, $i^2 = -1$, og

$$E_2 = \{a + b\sqrt{2} | a, b \in \mathbf{Q}\}.$$

Observer i forbindelse med E_2 at dersom $a + b\sqrt{2} \in E_2$ er forskjellig fra 0, så er $(a + b\sqrt{2})^{-1} \in E_2$. Vi rasjonaliserer nevneren ved et lite knep:

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in E_2 .$$

Vi skal senere se en betraktelig generalisering av denne rasjonaliseringen av nevneren i forbindelse med Abels analyse (se kommentar til korollar 2 i **4**).

Utvidelse av en tallkropp

La E være en tallkropp og la $b_1, \ldots, b_k$ være komplekse tall. Med $E(b_1, \ldots, b_k)$ forstår vi tallkroppen generert av $b_1, \ldots, b_k$ over E, det vil si den minste tallkroppen i $\mathbf{C}$ som inneholder E og $b_1, \ldots, b_k$. Vi sier at tallkroppen $E(b_1, \ldots, b_k)$ er en *utvidelse* av tallkroppen E. Hvis utvidelsen av E er generert av ett element, altså av formen $E(b)$, sier vi at vi har en *enkel* utvidelse av E.

Enhetsrøtter

Med en *primitiv* m'te enhetsrot vil vi forstå en løsning ω av ligningen $x^m - 1 = 0$, med den egenskap at de m røttene til denne ligningen er ω, ω^2, ω^3, ..., ω^{m-1}, $\omega^m = 1$. Eksempelvis er

$$\omega = e^{2\pi i/m} = \cos\frac{2\pi}{m} + i \sin\frac{2\pi}{m}$$

en primitiv m'te enhetsrot. Observer at dersom m er et primtall, så er enhver m'te enhetsrot ω forskjellig fra 1 en primitiv m'te enhetsrot. Mengden av alle enhetsrøtter i $\mathbf{C}$ vil vi betegne med $\mathcal{E}$.

Rene ligninger

En *ren* ligning er en ligning av formen $x^m - a = 0$. Dersom $x = r$ er en rot i denne ligningen, så er de m røttene gitt ved r, ωr, $\omega^2 r$, ..., $\omega^{m-1} r$, der ω er en primitiv m'te enhetsrot. Vi betegner en slik rot med det flertydige symbolet $r = \sqrt[m]{a}$ (eller $r = a^{1/m}$), og sier at r er en *m'te rot* av a.

Polynomer og rasjonale funksjoner over en tallkropp

Med et *polynom* i én variabel x over en tallkropp E mener vi et uttrykk av formen

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \,,$$

der koeffisientene $a_0, a_1, \cdots a_n$ er elementer i E. Vi sier at *graden* til $f(x)$ er n dersom $a_n \neq 0$. Dersom $a_n = 1$, sier vi at polynomet er *monisk*. Man betegner mengden av polynomer i x over E med $E[x]$. Med en *rasjonal funksjon* i x over E mener vi en kvotient mellom to polynomer av denne form.

Mer generelt får vi bruk for polynomer og rasjonale funksjoner i flere variable. Med et polynom $f(x_1, \ldots, x_n)$ i n variable x_1, ..., x_n over E mener vi en endelig sum av formen

$$f(x_1, \ldots, x_n) = \sum a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n} \,,$$

der koeffisientene $a_{i_1 i_2 \ldots i_n}$ ligger i E, og i_1, i_2, ..., i_n er hele tall ≥ 0. En rasjonal funksjon i x_1, ..., x_n over E defineres tilsvarende som en kvotient mellom to slike polynomer.

Den generelle n'tegradsligningen

Med en *generell* n'tegradsligning vil vi forstå en ligning av formen

$$x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0 \,, \tag{1}$$

der a_0, a_1, ..., a_{n-1} er komplekse tall som vi antar er *uavhengige* i betydningen algebraisk uavhengige over $\mathbf{Q}$. Dette betyr presist at dersom $f(a_0, a_1, \ldots, a_{n-1}) = 0$, der f er et polynom i n variable med koeffisienter fra $\mathbf{Q}$, så er f lik nullpolynomet. (Man kan vise at det er ekvivalent å anta algebraisk uavhengighet over tallkroppen $\mathbf{Q}(\mathcal{E})$, det vil si over den minste tallkroppen som inneholder $\mathbf{Q}$ og enhetsrøttene $\mathcal{E}$.)

Enhver ligning av n'te grad over $\mathbf{C}$ har n røtter i $\mathbf{C}$ (bevist av Gauss i 1799), og vi betegner røttene i (1) med x_1, ..., x_n. Røttene x_1, ..., x_n til (1) er igjen uavhengige hvis koeffisientene a_0, ..., a_{n-1} er det. Beviset for dette er ikke helt elementært. Som en alternativ måte å betrakte den generelle n'tegradsligning på kan en tenke seg at x_1, ..., x_n er n uavhengige komplekse tall som er røtter i en n'tegradsligning (1). Koeffisientene $a_0, \ldots, a_{n-1}$ i (1) er symmetriske polynomer i $x_1, \ldots, x_n$, og det følger da av fundamentalteoremet for symmetriske polynomer (se **4**) at $a_0, \ldots, a_{n-1}$ også er uavhengige.

Motsetningen til en generell ligning er en *spesiell* ligning. I en spesiell ligning er koeffisientene tall som er algebraisk avhengige over $\mathbf{Q}$. Et eksempel på en spesiell femtegradsligning er

$$x^5 - 2625x - 61500 = 0 \,.$$

Euler (1707–1783) studerte denne ligningen og fant at den hadde en rot $x = \alpha$ som kunne uttrykkes ved rotutdragninger:

$$\alpha = \sqrt[5]{75(5+4\sqrt{10})} + \sqrt[5]{225(35+11\sqrt{10})} + \sqrt[5]{225(35-11\sqrt{10})} + \sqrt[5]{75(5-4\sqrt{10})}.$$

Algebraisk løsning av ligninger

Med *algebraiske operasjoner* forstår vi de rasjonale operasjoner (addisjon, subtraksjon, multiplikasjon, divisjon) samt rotutdragninger. En foreløbig definisjon av begrepet "algebraisk løsning" av n'tegradsligningen (1) er følgende: Det fins en formel som inneholder kun de algebraiske operasjonene anvendt på koeffisientene $a_0, a_1, \ldots, a_{n-1}$ i (1), og som gir en rot i (1). Vi skal nå gi en presis definisjon: La $F = \mathbf{Q}(\mathcal{E}, a_0, a_1, \ldots, a_{n-1})$ være den minste tallkroppen i $\mathbf{C}$ som inneholder de rasjonale tallene $\mathbf{Q}$, enhetsrøttene $\mathcal{E}$, og koeffisientene $a_0, a_1, \ldots, a_{n-1}$. Tallkroppen F representerer det som er "kjent", de gitte "data", og oppgaven er å uttrykke røttene $x_1, \ldots, x_n$ til (1) ved hjelp av disse data. Med en *radikalutvidelse* K av F mener vi en kjede av enkle kropputvidelser der vi starter med F og ender med K :

$$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_{N-1} \subset F_N = K,$$

slik at $F_{i+1} = F_i(\eta_i)$, der η_i er rot i en ren ligning $x^{p_i} - \xi_i = 0$ hvor $\xi_i \in F_i$, p_i er et primtall, og $i = 0, 1, \ldots, N-1$. Altså er $\eta_i = \sqrt[p_i]{\xi_i} = \xi_i^{1/p_i}$.

Definisjon: n'tegradsligningen (1) kan *løses algebraisk* dersom det fins en radikalutvidelse K av F slik at minst én av røttene $x_1, \ldots, x_n$ til (1) ligger i K.

Kommentar 1. Antagelsen om at p_i'ene er primtall innebærer ikke noe tap av generalitet, idet $\sqrt[m_1]{\sqrt[m_2]{b}} = \sqrt[m_1]{\sqrt[m_2]{b}}$. Altså er enhver m'te rot en suksesjon av q_j'te røtter, der $m = q_1^{k_1} q_2^{k_2} \ldots q_l^{k_l}$ er primtallsfaktoriseringen av m.

Kommentar 2. Ifølge Abel (korollar til teorem 3 i **4**) kan et tall i F_{i+1} uttrykkes på formen

$$b_0 + b_1 \xi_i^{1/p_i} + b_2 \xi_i^{2/p_i} + \cdots + b_{p_i-1} \xi_i^{(p_i-1)/p_i},$$

der b'ene ligger i F_i for $i = 0, 1, \ldots, N-1$. La x_k være en rot til (1) som ligger i $K = F_N$, og uttrykk x_k ved tall i F_{N-1} som ovenfor. Ved gjentatte anvendelser av denne uttrykksformen helt til man kommer ned til $F = F_0$, får man en løsningsformel for roten x_k der enhetsrøtter og koeffisientene til (1) inngår, samt rotstørrelser bygget opp av disse. Dette er den presise forklaring på hva vi mener med at en rot i (1) kan gis som et algebraisk uttrykk i koeffisientene $a_0, a_1, \ldots, a_n$.

Kommentar 3. Dersom den generelle n'tegradsligningen (1) kan løses algebraisk så kan enhver spesiell n'tegradsligning løses algebraisk: Man innsetter de numeriske koeffisientene til den spesielle ligningen istedet for a_i-ene i formelen for roten. (Selv om dette synes intuitivt opplagt, så er det en subtil vanskelighet her som vi imidlertid ikke vil gå nærmere inn på.)

3. De klassiske løsningene av annen-, tredje- og fjerdegradsligningene

A. Den generelle annengradsligningen

Løsningen av den generelle annengradsligningen

$$x^2 + a_1 x + a_0 = 0$$

har vært kjent siden antikken. Som kjent er de to røttene x_1 og x_2 gitt ved

$$x_1 = -\frac{a_1}{2} + \frac{1}{2}\sqrt{a_1^2 - 4a_0}$$
$$x_2 = -\frac{a_1}{2} - \frac{1}{2}\sqrt{a_1^2 - 4a_0}\,.$$

Vi ser at $\sqrt{a_1^2 - 4a_0} = x_1 - x_2$.

Konklusjon: Rottegnet som forekommer i løsningen av den generelle annengradsligningen er en kvadratrot og kan uttrykkes som et polynom i røttene med rasjonale koeffisienter.

B. Den generelle tredjegradsligningen

Den første løsningen som ble funnet av den generelle tredjegradsligningen

$$(i) \qquad x^3 + a_2 x^2 + a_1 x + a_0 = 0$$

skyldes Scipione del Ferro (1465–1526), som var professor ved universitetet i Bologna til sin død. Løsningen ble senere uavhengig oppdaget av Nicolo Tartaglia (1505–1557). Vi skal presentere nedenfor den metoden som Gerolamo Cardano (1501–1576) gir i sin bok "Ars Magna", først trykket i Nürnberg i 1545. Cardano var forøvrig den første som introduserte komplekse tall $a + \sqrt{-b}$ i algebra, selv om han hadde store betenkeligheter med det. (Om alle intriger, kontroverser og hemmeligholdelser omkring tredje- og fjerdegradsligningene, se [32] og [36].)

Først fjerner man annengradsleddet i *(i)* ved å foreta substitusjonen $x = y - a_2/3$. Innsatt i *(i)* får man

$$(ii) \qquad y^3 + py + q = 0\,,$$

der $p = a_1 - (a_2^2/3)$, $q = (2a_2^3/27) - (a_2 a_1/3) + a_0$. Nå kommer det avgjørende knepet: Sett $y = u + v$ og innsett i *(ii)*:

$$(iii) \qquad u^3 + v^3 + (3uv + p)(u + v) + q = 0\,.$$

Man pålegger nå u og v betingelsen

$$(iv) \qquad 3uv = -p$$

(og altså $u^3v^3 = -p^3/27$.)

Av *(iii)* får man da

$$u^3 + v^3 = -q\,. \tag{v}$$

(iv) og *(v)* gir nå (se Viète-relasjonene i **4**) at u^3 og v^3 er røtter i annengradspolynomet

$$t^2 + qt - \frac{p^3}{27} = 0\,, \tag{vi}$$

og altså finner man

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \tag{vii}$$

$$v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\,.$$

Altså er løsningen av den generelle tredjegradsligningen tilbakeført til løsningen av en annengradsligning *(vi)* ("den kvadratiske resolventen til tredjegradsligningen") og til *rene* ligninger av tredje grad *(vii)*. Tar man i betraktning at $3uv = -p$ fra *(iv)*, og at kubikkrøtter kun er bestemt opp til en tredje enhetsrot, så får man av $y = u + v$ at de tre røttene y_1, y_2, y_3 til *(ii)* er gitt ved formlene:

$$y_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \tag{viii}$$

$$y_2 = \omega^2\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \omega\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

$$y_3 = \omega\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \omega^2\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\,.$$

Her er ω en primitiv 3dje enhetsrot. Løsningen *(viii)* kalles Cardanos formler. Ved å bruke at $1 + \omega + \omega^2 = 0$, så får man av *(viii)*:

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} = \frac{1}{3}(y_1 + \omega y_2 + \omega^2 y_3) \tag{ix}$$

$$\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} = \frac{1}{3}(y_1 + \omega^2 y_2 + \omega y_3)$$

Av *(ix)* utleder man nå lett at

$$\sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = \frac{1}{9}(\omega + \frac{1}{2})(y_1 - y_2)(y_1 - y_3)(y_2 - y_3) \tag{x}$$

Innsett nå i *(viii)*, *(ix)* og *(x)* for $y_i = x_i + (a_2/3) = x_i - (1/3)(x_1 + x_2 + x_3)$, $i = 1, 2, 3$, og for p og q uttrykt ved a_0, a_1, a_2.

Konklusjon: I den algebraiske løsningen av den generelle tredjegradsligningen *(i)* er det innerste rottegnet en kvadratrot og det neste rottegnet en kubikkrot. Rotutrykkene som forekommer i løsningen, er polynomer i røttene x_1, x_2, x_3 med koeffisienter i $\mathbf{Q}(\omega)$, der ω er en primitiv tredje enhetsrot.

C. Den generelle fjerdegradsligningen

Den algebraiske løsningen av den generelle fjerdegradsligningen ble funnet av Lodovico Ferrari (1522–1565), Cardanos sekretær og venn. Ferrari reduserer problemet med å finne løsningen av fjerdegradsligningen til å løse en tredjegradsligning, den såkalte "kubiske resolventen" til fjerdegradsligningen. Ferraris løsning står beskrevet i den ovenfor omtalte bok av Cardano. Vi skal her beskrive en løsningsmetode som skyldes Euler, og som er analog til den metoden vi benyttet for tredjegradsligningen.

Man fjerner først tredjegradsleddet i den generelle fjerdegradsligningen

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

ved å foreta substitusjonen $x = y - (a_3/4)$. Man får da *(i)* på den enklere formen

$$(ii) \qquad y^4 + py^2 + qy + r = 0\,,$$

der p, q, r er visse polynomer i a_0, a_1, a_2, a_3 som lett kan bestemmes. Man setter nå i analogi med tredjegradsligningen

$$(iii) \qquad y = \frac{1}{2}(u + v + w)\,.$$

Setter man *(iii)* inn i *(ii)*, så får man

$$(iv) \qquad (u^2 + v^2 + w^2)^2 + 4(uv + vw + wu)(u^2 + v^2 + w^2 + 2p)$$

$$+4p(u^2 + v^2 + w^2) + 8(uvw + q)(u + v + w) + 4(u^2v^2 + v^2w^2 + w^2u^2) + 16r = 0$$

Man pålegger nå følgende betingelser på u, v, w:

$$(v) \qquad u^2 + v^2 + w^2 = -2p$$

$$uvw = -q$$

(og altså $u^2v^2w^2 = q^2$).

Setter man *(v)* inn i *(iv)*, så får man

$$(vi) \qquad u^2v^2 + u^2w^2 + v^2w^2 = p^2 - 4r\,.$$

Av *(v)* og *(vi)* får man nå (se Viète-relasjonene i **4**) at u^2, v^2 og w^2 er de tre røttene til tredjegradspolynomet ("den kubiske resolventen")

$$(vii) \qquad t^3 + 2pt^2 + (p^2 - 4r)t - q^2 = 0\,.$$

La t_1, t_2 og t_3 være røttene i *(vii)*. Da er

$$(viii) \qquad u = \sqrt{t_1}\,, \quad v = \sqrt{t_2}\,, \quad w = \sqrt{t_3}$$

Fortegnene i *(viii)* bestemmes av $uvw = -q$ i *(v)*. Kun fire kombinasjoner er mulige og man finner de fire røttene y_1, y_2, y_3 og y_4 til (ii) ved å sette inn i *(iii)*:

$$(ix) \qquad \begin{aligned} y_1 &= \frac{1}{2}\left(\sqrt{t_1} + \sqrt{t_2} + \sqrt{t_3}\right) \\ y_2 &= \frac{1}{2}\left(\sqrt{t_1} - \sqrt{t_2} - \sqrt{t_3}\right) \\ y_3 &= \frac{1}{2}\left(-\sqrt{t_1} + \sqrt{t_2} - \sqrt{t_3}\right) \\ y_4 &= \frac{1}{2}\left(-\sqrt{t_1} - \sqrt{t_2} + \sqrt{t_3}\right) \end{aligned}$$

Av *(ix)* får vi lett at

$$(x) \qquad \sqrt{t_1} = y_1 + y_2\,, \quad \sqrt{t_2} = y_1 + y_3\,, \quad \sqrt{t_3} = y_1 + y_4\,.$$

Av *(x)* finner vi t_1, t_2 og t_3 som polynomer i y_1, y_2, y_3, y_4. Ved å bruke resultatene fra **B** får vi at rotuttrykkene som gir røttene t_1, t_2 og t_3 til *(vii)*, kan uttrykkes ved polynomer i t_1, t_2, t_3, og altså ved polynomer i y_1, y_2, y_3, y_4, med koeffisienter i $\mathbf{Q}(\omega)$, der ω er en tredje enhetsrot. Innsetter vi til slutt $y_i = x_i + (a_3/4), i = 1, 2, 3, 4$, der $a_3 = -(x_1 + x_2 + x_3 + x_4)$, så slutter vi følgende:

Konklusjon: I den algebraiske løsningen av den generelle fjerdegradsligningen *(i)* er det innerste rottegnet en kvadratrot og det neste rottegnet en kubikkrot. Rotuttrykkene som forekommer i løsningen, er polynomer i røttene x_1, x_2, x_3, x_4 med koeffisienter i $\mathbf{Q}(\omega)$, der ω er en primitiv tredje enhetsrot.

Vi skal se, når vi i **6** gjennomgår Ruffinis og Abels resultater om strukturen av en algebraisk løsning av den generelle n'tegradsligningen, at konklusjonene ovenfor for annen-, tredje- og fjerdegradsligningene passer inn i et mønster.

La oss bruke den algebraiske løsningen av den generelle tredjegradsligningen i **B**:

$$x^3 + a_2x^2 + a_1x + a_0 = 0,$$

som eksempel på en radikalutvidelse K av $F = \mathbf{Q}(\mathcal{E}, a_0, a_1, a_2)$, der $\mathcal{E}$ er enhetsrøttene, slik at en av røttene x_1, x_2, x_3, (faktisk alle tre!) ligger i K. Vi har nemlig

$$F = F_0 \subset F_1 \subset F_2 \subset F_3 = K\,,$$

der

$$F_1 = F_0\left(\sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\right),$$

$$F_2 = F_1\left(\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\right),$$

$$F_3 = F_2\left(\sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}\right),$$

og der $p = a_1 - (a_2^2/3)$, $q = (2a_2^3/27) - (a_2a_1/3) + a_0$.

4. Den klassiske ligningsteoriens to pillarer

A. Permutasjoner, polynomer i n variable, symmetriske polynomer

Vi tar utgangspunkt i sammenhengen mellom røttene til en n'tegradsligning og dens koeffisienter. Denne sammenhengen ble først påvist av den franske matematikeren François Viète (1540–1603), som forøvrig skapte den moderne algebraiske notasjonen. Han brukte bokstaver til å betegne ikke bare ukjente størrelser, men også kjente størrelser. Dessuten innførte han betegnelsene "polynom" og "koeffisient" i algebra.

La som før

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$$

være den generelle n'tegradsligningen og la røttene være $x_1, x_2, \cdots, x_n$. Da har vi faktoriseringen

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = (x - x_1)(x - x_2)\cdots(x - x_n)\,.$$

Multipliserer vi ut høyresiden og sammenligner koeffisienter, får vi *Viète-relasjonene*:

(i)
$$-a_{n-1} = x_1 + x_2 + \cdots + x_{n-1} + x_n = s_1$$

$$a_{n-2} = x_1x_2 + \cdots + x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n = \sum_{1\le i<j\le n} x_ix_j = s_2$$

$$\vdots$$

$$(-1)^n a_0 = x_1x_2\cdots x_{n-1}x_n = s_n\,.$$

$s_1, s_2, \ldots, s_n$ kalles de *elementære symmetriske* polynomer i de n variable $x_1, \ldots, x_n$. Et polynom $f(x_1, \ldots, x_n)$ i de n variable $x_1, \ldots, x_n$ over tallkroppen E kalles *symmetrisk* dersom

$$f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = f(x_1, x_2, \ldots, x_n)$$

for enhver permutasjon σ av symbolene 1, 2, ..., n. Vi innfører notasjonen $f_\sigma(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$. Betingelsen blir da $f_\sigma = f$ for enhver σ. Hva er så en permutasjon? En *permutasjon* av de n symbolene 1, 2, ..., n er en énentydig avbildning σ av mengden av disse symbolene på seg selv. Dersom $\sigma(1) = i_1$, $\sigma(2) = i_2$, ..., $\sigma(n) = i_n$, så bruker man følgende notasjon for σ :

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & & i_n \end{pmatrix}.$$

Denne notasjonen skyldes Cauchy [10], som forøvrig kalte permutasjoner for "substitusjoner". I sitt arbeide fra 1815 generaliserte han noen av de resultater Ruffini tidligere hadde oppnådd. Med *produktet* av to permutasjoner σ_1 og σ_2, betegnet

med $\sigma_1\sigma_2$, mener vi sammensetningen, eller komposisjonen, av σ_1 og σ_2. Det vil si først anvender vi avbildningen σ_2 og så σ_1.

Eksempel. La $n = 3$ og la

$$\sigma_1 = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix}.$$

Da er

$$\sigma_1\sigma_2 = \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix}.$$

Med den *inverse* permutasjonen til permutasjonen σ (vi betegner den inverse med σ^{-1}) mener vi simpelthen den inverse avbildningen til σ. Det er da klart at $\sigma\sigma^{-1} = \sigma^{-1}\sigma = id$, der id er identitetsavbildningen.

Eksempel. La $n = 3$ og la $\sigma = \left(\begin{smallmatrix} 1\,2\,3 \\ 2\,3\,1 \end{smallmatrix}\right)$. Da er $\sigma^{-1} = \left(\begin{smallmatrix} 1\,2\,3 \\ 3\,1\,2 \end{smallmatrix}\right)$ og $\sigma\sigma^{-1} = \sigma^{-1}\sigma = \left(\begin{smallmatrix} 1\,2\,3 \\ 1\,2\,3 \end{smallmatrix}\right) = id$.

Mengden av alle permutasjoner av n symboler med sammensetningsregelen er det første eksempelet på en *gruppe* som ble studert i matematikkens historie. Denne spesielle gruppen kalles den symmetriske gruppen på n symboler og betegnes med S_n. I Lagranges og Ruffinis studier av S_n er perspektivet helt sett ut fra lignings-teorien: Hva som var relevant for dem var å finne hvor mange forskjellige (formelle) verdier et polynom i n variable kunne anta under alle mulige permutasjoner av de variable. Man kan si at de studerte de mulige *indekser* undergrupper av S_n kunne ha, i stedet for undergruppene selv. Det var først med Cauchys [11] siste arbeider fra 1844–46 viet permutasjoner at gruppeperspektivet trer tydeligere frem. (Man må huske at Galois' arbeider enda ikke var publisert og alminnelig kjent.)

Vi vil innføre en alternativ notasjon for permutasjoner som også skyldes Cauchy og som skal vise seg å være hendig. Med en *k-sykel*, $1 < k \leq n$, mener vi en permutasjon σ i S_n som ombytter k symboler i $\{1, 2, \ldots n\}$ syklisk og fikserer de andre. Det vil si det finnes k distinkte symboler $i_1, i_2, \ldots, i_k$ i $\{1, 2, \ldots, n\}$ slik at $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_k) = i_1$, og de andre symbolene avbildes identisk på seg selv. Vi betegner σ med

$$\sigma = (i_1 i_2 \ldots i_k).$$

Observer at

$$\sigma^k = \sigma\sigma\cdots\sigma = id \qquad (k \text{ faktorer}).$$

Eksempel. La $n = 5$. Da er $\sigma = (123)$ en 3-sykel, og i vår tidligere notasjon skrives σ som $\sigma = \left(\begin{smallmatrix} 1\,2\,3\,4\,5 \\ 2\,3\,1\,4\,5 \end{smallmatrix}\right)$.

2-sykler inntar en spesiell stilling. De kalles for *transposisjoner*. Enhver permutasjon σ kan skrives som et produkt av transposisjoner. Dette vises enkelt ved først å påvise at σ kan skrives som et produkt av k-sykler og deretter at enhver k-sykel er et produkt av transposisjoner. For eksempel er $(efg\ldots pq) = (eq)(ep)\ldots(eg)(ef)$.

I Ruffinis "gruppeteoretiske" bevis for umuligheten av en algebraisk løsning av den generelle n'tegradsligningen for $n \geq 5$ er det to relasjoner mellom 3-sykler og

5-sykler som er fundamentale: La r, s, t, u, v være fem distinkte symboler i mengden $\{1, 2, \dots, n\}$. Da er

$$(ii) \qquad (rstuv) = (ruv)\,(rst)$$

$$(iii) \qquad (rst) = (rtsuv)\,(vusrt)\,,$$

noe man direkte verifiserer.

La oss nå returnere til polynomer i n variable. Et eksempel på et polynom f som *ikke* er symmetrisk, er:

$$(iv) \qquad f(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4\,.$$

Her er $n = 4$, og vi observerer at dersom

$$\sigma = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,3\,2\,4 \end{pmatrix}\,, \quad \tau = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,4\,3\,2 \end{pmatrix}\,,$$

så gir *(iv)*

$$f_\sigma(x_1, x_2, x_3, x_4) = f(x_1, x_3, x_2, x_4) = x_1x_3 + x_2x_4 \neq f(x_1, x_2, x_3, x_4)$$

og

$$f_\tau(x_1, x_2, x_3, x_4) = f(x_1, x_4, x_3, x_2) = x_1x_4 + x_2x_3 \neq f(x_1, x_2, x_3, x_4)\,.$$

Man overbeviser seg om at f antar nøyaktig tre forskjellige verdier ved alle mulige permutasjoner i S_4, nemlig de tre verdiene $f = f_{id}$, f_σ og f_τ.

Vi kommer nå til fundamentalteoremet for symmetriske polynomer. Dette teoremet ble bevist av den engelske matematikeren Waring (1734–1798) i 1762. Han presenterte et nytt bevis i 1770 [34], og det er dette siste beviset som vi finner i algebralærebøker senere. Beviset er helt elementært og var standard kost i alle eldre lærebøker i algebra, se for eksempel [23,29,35]. For en nyere referanse se [31].

Fundamentalteoremet for symmetriske polynomer. La $f(x_1, \dots, x_n)$ være et symmetrisk polynom i de n variable $x_1, \cdots, x_n$ over tallkroppen E. Da finnes et éntydig bestemt polynom $g(y_1, \dots, y_n)$ i de n variable $y_1, \dots, y_n$ over E slik at

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

der $s_1, \cdots, s_n$ er de elementære symmetriske polynomene i $x_1, \dots, x_n$.

Eksempel. La $n = 2$ og betrakt det symmetriske polynomet $f(x_1, x_2) = x_1^2 + x_2^2$. Da er

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

Altså er $f(x_1, x_2) = g(s_1, s_2)$, der $g(y_1, y_2) = y_1^2 - 2y_2$.

Korollar. Dersom $x_1, \dots, x_n$ er de n røttene til n'tegradsligningen

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0\,,$$

og $f(y_1, \dots, y_n)$ er et symmetrisk polynom i de n variable $y_1, \dots, y_n$ over tallkroppen E, så vil $f(x_1, \dots, x_n)$ være et element i tallkroppen $E(a_0, \dots, a_{n-1})$.

Bevis: Bruk Viète-relasjonene *(i)*.

B. Den Euklidske algoritmen, største felles divisor for to polynomer, irredusible polynomer, binomiske polynomer

La

$$g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0\,, \quad b_m \neq 0$$

$$h(x) = c_k x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c_0\,, \quad c_k \neq 0$$

være to polynomer i $E[x]$. Ved polynomdivisjon av $g(x)$ med $h(x)$ finner man polynomer $q(x)$ ("kvotienten") og $r(x)$ ("restleddet") i $E[x]$ slik at

$$(v) \qquad g(x) = q(x)h(x) + r(x)$$

$$\operatorname{grad}(r(x)) < \operatorname{grad}(h(x))\,.$$

Polynomene $q(x)$ og $r(x)$ er éntydig bestemt ved *(v)*. Dersom $r(x) = 0$, det vil si $r(x)$ er nullpolynomet, så sier vi at $h(x)$ er en *divisor* i $g(x)$. Som eksempel nevner vi det tilfellet at $g(\alpha) = 0$, det vil si $\alpha \in \mathbf{C}$ er en rot til $g(x)$. Settes da $h(x) = x - \alpha$, så ser man lett av *(v)* ved innsetting $x = \alpha$ at $r(x)$ er nullpolynomet. Altså er $x - \alpha$ en divisor i $g(x)$. På denne måten viser man at $g(x)$ kan skrives som $g(x) = b_m(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_m)$, der α_i'ene er røttene til $g(x)$.

Den Euklidske algoritmen fremkommer ved suksessive anvendelser av divisjonsalgoritmen ovenfor. Man får følgende skjema for den Euklidske algoritmen:

$$(vi) \qquad g(x) = q(x)h(x) + r(x)$$

$$h(x) = q_1(x)r(x) + r_1(x)$$

$$r(x) = q_2(x)r_1(x) + r_2(x)$$

$$r_1(x) = q_3(x)r_2(x) + r_3(x)$$

$$\vdots$$

$$r_{l-2}(x) = q_l(x)r_{l-1}(x) + r_l(x)$$

$$r_{l-1}(x) = q_{l+1}(x)r_l(x)\,.$$

Prosessen stopper når restleddet blir 0, noe som må inntreffe før eller siden da gradene til restleddene $r_i(x)$ avtar. Av skjemaet *(vi)* leser man nedenfra og opp først at $r_l(x)$ er en divisor i $r_{l-1}(x)$, så at $r_l(x)$ er en divisor i $r_{l-2}(x)$, og så videre. Konklusjonen er at $r_l(x)$ er en divisor i både $h(x)$ og $g(x)$. Men mer enn det: Dersom $s(x) \in E[x]$ er en divisor i både $h(x)$ og $g(x)$, så får man av skjemaet *(vi)* lest ovenfra og ned først at $s(x)$ er en divisor i $r(x)$, dernest at $s(x)$ er en divisor i $r_1(x)$, og så videre. Konklusjonen blir at $s(x)$ er en divisor i $r_l(x)$. Hvis vi normaliserer $r_l(x)$ til et monisk polynom ved å multiplisere med et passende tall i E, så har vi ved resonnementet ovenfor vist at to polynomer $h(x)$ og $g(x)$ i $E[x]$ har en éntydig bestemt *største felles divisor* i $E[x]$, ut fra følgende:

Definisjon. Største felles divisor til polynomene $h(x)$ og $g(x)$ i $E[x]$ er det éntydig bestemte moniske polynomet $d(x)$ i $E[x]$ med følgende egenskaper:

(i) $d(x)$ er en divisor i både $h(x)$ og $g(x)$.

(ii) Dersom $s(x)$ er en divisor i både $h(x)$ og $g(x)$, så er $s(x)$ en divisor i $d(x)$.

Vi betegner $d(x)$ med $(g(x), h(x))$.

Teorem 1. La $g(x)$ og $h(x)$ være to polynomer i $E[x]$ og la $d(x) = (g(x), h(x))$ være største felles divisor. Da finnes to polynomer $s(x)$ og $t(x)$ i $E[x]$ slik at

$$d(x) = s(x)g(x) + t(x)h(x)\,.$$

Bevis: Betrakt skjemaet *(vi)* ovenfra og ned. Av øverste linje får vi $r(x) = g(x) - q(x)h(x)$. Sett dette inn i neste linje og uttrykk $r_1(x)$ ved $g(x)$ og $h(x)$. Ved suksessivt å sette inn i påfølgende linje finner man til slutt at $r_l(x)$ kan uttrykkes på ønsket måte ved $g(x)$ og $h(x)$, og dermed $d(x)$ også ved å normalisere $r_l(x)$.

Definisjon. Et polynom $g(x) \in E[x]$ er *irredusibelt* over tallkroppen E dersom det er umulig å faktorisere $g(x) = g_1(x)g_2(x)$, der $g_1(x)$ og $g_2(x)$ er polynomer i $E[x]$, begge av grad ≥ 1.

Vi skal nå bevise et fundamentalteorem ved et helt elementært bevis som skyldes Abel. Han anvendte det med stor effekt i sine ligningteoretiske undersøkelser, blant annet i sitt bevis for umuligheten av å løse den generelle n'tegradsligningen algebraisk når $n \geq 5$. Dette fundamentalteoremet og dets umiddelbare konsekvenser, som vi formulerer som korollarer, inngår idag som "folklore" i Galois-teorien og kroppteorien, gjerne knyttet til begrepet "minimalpolynom".

Teorem 2 [4, s. 480]. La $h(x)$ være et irredusibelt polynom over tallkroppen E. La $g(x) \in E[x]$ ha en felles rot α med $h(x)$. Da er $h(x)$ en divisor i $g(x)$. Altså er alle røttene til $h(x)$ også røtter til $g(x)$.

Bevis: La $d(x) = (h(x), g(x))$. Siden $d(x)$ er en divisor i $h(x)$ og $h(x)$ er irredusibel, så må enten $d(x) = 1$ eller så er $d(x)$ lik $ah(x)$ for passende $a \in E$. Anta ad absurdum at $d(x) = 1$. Da finnes ifølge teorem 1 polynomer $s(x)$ og $t(x)$ i $E[x]$ slik at

$$1 = s(x)g(x) + t(x)h(x)\,.$$

Ved å sette $x = \alpha$ inn i denne ligningen får man en motsigelse idet høyresiden blir 0. Altså må $d(x) = ah(x)$ for passende $a \in E$. Siden $d(x)$ er en divisor i $g(x)$, er selvfølgelig også $h(x)$ en divisor i $g(x)$. Dette fullfører beviset.

Korollar 1. Dersom α er rot til et irredusibelt polynom $h(x)$ over tallkroppen E, så kan ikke α være rot til et polynom $g(x) \in E[x]$ av lavere grad enn $h(x)$ uten at $g(x)$ er nullpolynomet.

Bevis: Dersom $g(\alpha) = 0$, så er ifølge teoremet $h(x)$ en divisor i $g(x)$. Dette er kun mulig dersom $g(x) = 0$, da $\text{grad}(g(x)) < \text{grad}(h(x))$.

Korollar 2. La α være en rot til det irredusible polynomet $h(x) = x^k + c_{k-1}x^{k-1} + \cdots + c_1x + c_0$ over tallkroppen E. La $E(\alpha)$ være den enkle utvidelsen av E som α genererer over E. Da er

$$E(\alpha) = \{b_0 + b_1 + \cdots + b_{k-1}\alpha^{k-1} | b_0, \ldots, b_{k-1} \in E\}\,.$$

Dersom $\beta \in E(\alpha)$ og $\beta = b_0 + b_1\alpha + \cdots + b_{k-1}\alpha^{k-1}$, der b_i-ene er i E, så er disse entydig bestemt.

Bevis: Da $h(\alpha) = 0$, så er $\alpha^k = -(c_{k-1}\alpha^{k-1} + \cdots + c_1\alpha + c_0)$. Man kan bruke dette til å uttrykke $\alpha^{k+1}, \alpha^{k+2}$, etc. ved potenser α^i av α der $i \leq k-1$. Det er da klart at dersom β_1 og β_2 er to elementer i $A = \{b_0 + b_1\alpha + \cdots + b_{k-1}\alpha^{k-1} | b_0, \cdots, b_{k-1} \in E\}$, så er summen, differensen og produktet av β_1 og β_2 igjen i A. Dessuten er $E \subset A$ og $\alpha \in A$. Så det gjenstår kun å vise at dersom $\beta \in A, \beta \neq 0$, så er $\beta^{-1} \in A$. La nå $\beta = g(\alpha) \neq 0$, der $g(x) = b_0 + b_1 x + \cdots + b_{k-1}x^{k-1} \in E[x]$. Da må $(h(x), g(x)) = 1$, og altså finnes det ifølge teorem 1 polynomer $s(x)$ og $t(x)$ i $E[x]$ slik at

$$s(x)g(x) + t(x)h(x) = 1\,.$$

Sett $x = \alpha$. Siden $h(\alpha) = 0$, får vi at $s(\alpha)g(\alpha) = 1$, det vil si $\beta^{-1} = 1/g(\alpha) = s(\alpha)$. Dette betyr at $E(\alpha) = A$, som vi skulle vise.

Dersom $\beta \in E(\alpha)$ og

$$\beta = b_0 + b_1\alpha + \cdots + b_{k-1}\alpha^{k-1} = c_0 + c_1\alpha + \cdots c_{k-1}\alpha^{k-1}\,,$$

så er $(b_0 - c_0) + (b_1 - c_1) + \cdots + (b_{k-1} - c_{k-1})\alpha^{k-1} = 0$. Ifølge korollar 1 er da $b_0 = c_0, b_1 = c_1, \ldots b_{k-1} = c_{k-1}$. Dette viser entydigheten.

Kommentar. Et essensielt punkt i beviset for korollar 2 er den vidtrekkende generaliseringen av knepet med "rasjonalisering av nevneren" som vi møter i enkle situasjoner, for eksempel i tallkroppen $\mathbf{Q}(\sqrt{2})$. (Se **2.**)

Det irredusible polynomet vi eksklusivt skal møte i denne artikkelen er det *binomiske* polynomet $h(x) = x^p - a \in E[x]$, der p er et primtall. Vi presenterer nå Abels bevis for at dette er irredusibelt.

Teorem 3 [5, s. 228]. Det binomiske polynomet $x^p - a$, der a er et element i tallkroppen E og p er et primtall, har enten én rot i E, eller så er det irredusibelt over E.

Bevis: Anta $x^p - a$ ikke har noen rot i E, og anta ad absurdum at $x^p - a = f(x)g(x)$, der $f(x)$ og $g(x)$ er moniske polynomer i $E[x]$ av grad henholdsvis m og n, med $m, n \geq 1$ og $m + n = p$. Røttene i den rene ligningen $x^p - a = 0$ er $r, \omega r, \ldots, \omega^{p-1}r$, der ω er en primitiv p-te enhetsrot og r er én rot i $x^p - a = 0$. Da er

$$x^p - a = (x - r)(x - \omega r)\cdots(x - \omega^{p-1}r) = f(x)g(x)\,.$$

Herav får vi at konstantleddene A og B til henholdsvis $f(x)$ og $g(x)$ må være av formen $A = \omega^k r^m, B = \omega^l r^n$. Siden $m + n = p$ og p er primtall, er m og n relativt primiske. Altså finnes hele tall i og j slik at $im + jn = 1$. Altså får vi:

$$C = A^i B^j = \omega^{ik+jl} r^{im+jn} = \omega^{ik+jl} r\,.$$

Da blir $C^p = r^p = a$. Siden $C \in E$, har vi en motsigelse til at $x^p - a$ ikke har noen rot i E. Altså er $x^p - a$ irredusibel over E.

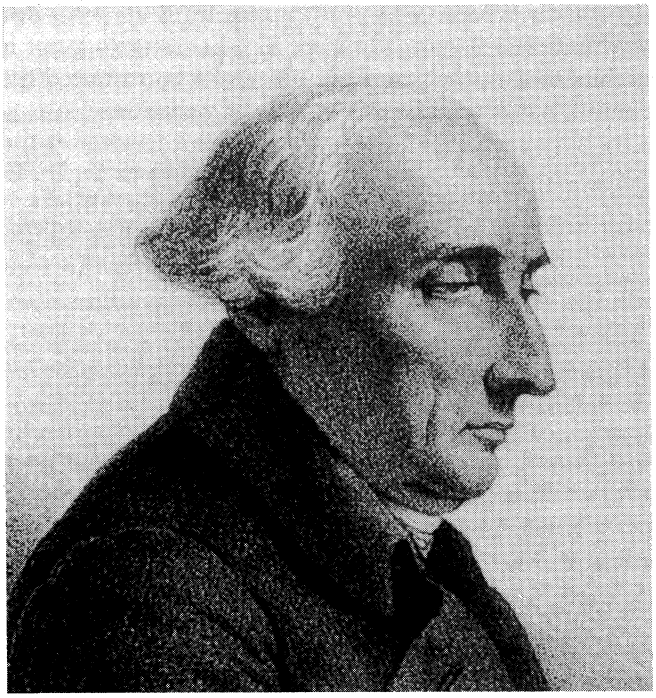
Korollar. Anta at det binomiske polynomet $x^p - a$, der a ligger i tallkroppen E og p er et primtall, ikke har noen rot i E. La $r = \sqrt[p]{a} = a^{1/p}$ være en rot til $x^p - a$. Da er

$$E(r) = \{b_0 + b_1 a^{1/p} + b_2 a^{2/p} + \cdots + b_{p-1}a^{(p-1)/p} | b_0, \ldots, b_{p-1} \in E\}\,.$$

Bevis: Dette følger umiddelbart av teoremet og korollar 2 til teorem 2.

5. Lagranges analyse av løsningene av tredje- og fjerdegradsligningene

Del Ferros og Ferraris algebraiske løsninger av henholdsvis den generelle tredje- og fjerdegradsligningen skjedde ved ad hoc kunstgrep. Man forsøkte i de neste 200 år med liknende kunstgrep å løse den generelle femtegradsligningen uten å lykkes. Viktige bidragsytere til ligningsteorien frem til året 1770, ved siden av Viète, var Tschirnhausen (1651–1708), Bezout (1730–1783) og selvfølgelig Euler. Året 1770 markerer et veiskille i ligningsteoriens historie. Ved et pussig sammentreff av tilfeldigheter ble det dette året offentliggjort fire betydelige arbeider alle viet ligningsteorien. Ved akademiene i Siena (Italia), London, Paris og Berlin ble det presentert avhandlinger av henholdsvis Malfatti (1731–1807), Waring, Vandermonde (1735–1796) og Lagrange [22]. Hver av disse avhandlingene inneholder viktige nye bidrag til ligningsteorien. Men det var Lagranges arbeid som hadde desidert størst spennvidde og perspektiv, og hans "Réflexions sur la résolution algébrique des équations" ble en hjørnesten for ligningsteorien. Ruffini, Abel og Galois står alle i stor gjeld til Lagranges analyse av og forklaring på hvorfor tredje- og fjerdegradsligningen lar seg løse algebraisk. Samtidig gir hans analyse den første indikasjon på hvorfor den generelle femtegradsligning ikke kan løses algebraisk. Vi skal nå gi et kort resymé av Lagranges arbeide.



Joseph Louis Lagrange
(1736–1813)

Lagrange observerte først at rotuttrykkene som forekommer i løsningen av de generelle tredje- og fjerdegradsligningene kunne uttrykkes som polynomer i røttene,

med koeffisienter bestående av rasjonale tall og enhetsrøtter. Ved å studere hvordan disse polyomene endret seg under permutasjoner av røttene fant han grunnen til at den algebraiske løsningen var mulig. Dette overbeviste ham om at nøkkelen til å finne den algebraiske løsningen til den generelle n'tegradsligningen

$$(*) \qquad x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

med røtter $x_1, \ldots, x_n$, var å undersøke om det fantes polynomer $f(x_1, \ldots, x_n)$ i røttene $x_1, \ldots, x_n$ over tallkroppen $\mathbf{Q}(\mathcal{E})$, som antok færre enn n verdier under alle mulige permutasjoner av x_i'ene. La nemlig $z_1 = f(x_1, \ldots, x_n)$, og anta at f antar verdiene $z_1, z_2, \ldots, z_m$ under alle mulige permutasjoner av x_i'ene. Da vil

$$(i) \qquad g(z) = (z - z_1)(z - z_2)\cdots(z - z_m)$$

være et m'tegradspolynom i z der koeffisientene er symmetriske polynomer i $x_1, \ldots, x_n$. Ifølge korollaret til fundamentalteoremet for symmetriske polynomer (**4 A**), ligger koeffisientene til $g(z)$ i tallkroppen $F = \mathbf{Q}(\mathcal{E}, a_0, a_1, \ldots, a_{n-1})$. Dersom $m < n$, har vi altså funnet et polynom av grad mindre enn n, som vi da ved induksjon kan tenke oss at vi kan løse algebraisk. Ligningen *(i)* kalles en *resolventligning* til (*). La oss nå demonstrere ved konkrete eksempler hvordan den generelle tredje- og fjerdegradsligningen kan løses på denne måten.

For den generelle tredjegradsligningen $x^3 + a_2x^2 + a_1x + a_0 = 0$ med røtter x_1, x_2, x_3, velges

$$z_1 = f(x_1, x_2, x_3) = (x_1 + \omega x_2 + \omega^2 x_3)^3,$$

der ω er en tredje enhetsrot. Man viser lett at f antar kun to verdier ved alle mulige permutasjoner av x_1, x_2, x_3, nemlig

$$(ii) \qquad \begin{aligned} z_1 &= (x_1 + \omega x_2 + \omega^2 x_3)^3 \\ z_2 &= (x_1 + \omega^2 x_2 + \omega x_3)^3 . \end{aligned}$$

Altså kan z_1 og z_2 bestemmes som røtter i en annengradsligning ("den kvadratiske resolventen til tredjegradsligningen"), der koeffisientene ligger i $F = \mathbf{Q}(\mathcal{E}, a_0, a_1, a_2)$, og altså er "kjente data". Å bestemme disse koeffisientene krever elementær, men tidkrevende, regning. Resolventligningen blir

$$z^2 + (2a_2^3 - 9a_2a_1 + 27a_0)z + (a_2^2 - 3a_1)^3 = 0 .$$

Av *(ii)* får man nå

$$(iii) \qquad \begin{aligned} x_1 + \omega x_2 + \omega^2 x_3 &= \sqrt[3]{z_1} \\ x_1 + \omega^2 x_2 + \omega x_3 &= \sqrt[3]{z_2} . \end{aligned}$$

(Kubikkrøttene i *(iii)* er ikke uavhengige idet man har $\sqrt[3]{z_1}\sqrt[3]{z_2} = a_2^2 - 3a_1$, noe man ser ved å multiplisere sammen venstresidene i *(iii)* og observere at dette produktet er et symmetrisk polynom i x_1, x_2, x_3.)

Av *(iii)* sammen med ligningen $x_1 + x_2 + x_3 = -a_2$ kan man lett bestemme røttene x_1, x_2, x_3, og man finner igjen Cardanos formler *(viii)* i **3** (når $a_2 = 0$).

For den generelle fjerdegradsligningen $x^4+a_3x^3+a_2x^2+a_1x+a_0=0$ med røtter x_1,x_2,x_3,x_4, velges

$$z_1=f(x_1,x_2,x_3,x_4)=(x_1+x_2-x_3-x_4)^2\,.$$

(Som Lagrange poengterer kunne man alternativt valgt $f=h\bar{h}$, der $\bar{h}$ er den komplekskonjugerte til $h(x_1,x_2,x_3,x_4)=x_1+ix_2+i^2x_3+i^3x_4$, $i^2=-1$.)

Man viser lett at f antar tre forskjellige verdier under alle mulige permutasjoner av x_1,x_2,x_3,x_4, nemlig

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

Altså er z_1,z_2,z_3 røtter i en tredjegradsligning ("den kubiske resolventen til fjerdegradsligningen"), med koeffisienter i tallkroppen $F=\mathbf{Q}(\mathcal{E},a_0,a_1,a_2,a_3)$. Man finner ved en del regning at resolventligningen blir

$$\begin{aligned} &z^3-(3a_3^2-8a_2)z^2+(3a_3^4-16a_3^2a_2+16a_2^2\\ &+16a_3a_1-64a_0)z-(a_3^3-4a_3a_2+8a_1)^2=0\,. \end{aligned}$$

Av *(iv)* får man

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

(Kvadratrøttene i *(v)* er ikke uavhengige, idet produktet av venstresidene i *(v)* er et symmetrisk polynom i x_1,x_2,x_3,x_4, og viser seg å være lik $-a_3^3+4a_3a_2-8a_1$.)

Relasjonen $x_1+x_2+x_3+x_4=-a_3$ sammen med (v) gir nå røttene x_1,x_2,x_3,x_4 til den generelle fjerdegradsligningen, akkurat som i **3**.

Hva med den generelle femtegradsligningen? Ifølge Lagranges filosofi skal man oppsøke et polynom $f(x_1,\dots,x_5)$ over tallkroppen $\mathbf{Q}(\mathcal{E})$ i de fem røttene $x_1,\dots,x_5$ slik at f antar færre enn fem verdier under alle permutasjoner av røttene. Dessuten, og det er en implisitt forutsetning, må $f(x_1,\dots,x_5)$ være av en slik beskaffenhet at man er i stand til å beregne røttene $x_1,\dots,x_5$ ut fra kjennskapet til f og de forskjellige verdier f antar. Det er nemlig lett å se at for *alle* $n>1$ finnes et polynom $g(x_1,\dots,x_n)$ med heltallige koeffisienter som antar *to* verdier under alle permutasjoner av $x_1,\dots,x_n$, nemlig

(vi)
$$g(x_1,\dots,x_n)=$$

$$(x_1-x_2)\,(x_1-x_3)\cdots(x_1-x_n)\,(x_2-x_3)(x_2-x_4)\cdots(x_{n-1}-x_n)$$

$$=\prod_{1\le i<j\le n}(x_i-x_j)\,.$$

Polynomet g antar verdiene $\pm\sqrt{D}$, der

$$D = \prod_{1\leq i<j\leq n} (x_i - x_j)^2 \in F = \mathbf{Q}(\mathcal{E}, a_0, \ldots a_{n-1})$$

er den såkalte *diskriminanten* til den generelle n'tegradsligningen (*). Men kjennskapet til g er ikke av særlig hjelp til å finne røttene $x_1, \ldots, x_n$. Når man ser bort fra polynomer av formen $c_1 + c_2 g$, der g er polynomet i *(vi)* og c_1 og c_2 er symmetriske polynomer i $x_1, \ldots, x_5$, var Lagrange ikke i stand til å finne et polynom $f(x_1, \ldots, x_5)$ i røttene til den generelle femtegradsligningen som antok færre enn fem verdier under alle mulige permutasjoner av $x_1, \ldots, x_5$. (Det var Ruffini [27] (1799) som først *beviste* at et slikt polynom ikke eksisterer, og Cauchy [10] (1815) utvidet dette resultatet for alle $n \geq 5$. I sitt første "bevis" for umuligheten av å løse den generelle femtegradsligningen algebraisk fra 1799 [27], bruker Ruffini dette resultatet. Abel benytter seg av det samme resultatet i den "substitusjonsteoretiske" delen av sitt bevis, og han krediterer Cauchy for dette.) Men selv om et slikt polynom ikke eksisterer, er enda ikke alt håp ute om å løse femtegradsligningen algebraisk: Dersom nemlig polynomet $z_1 = f(x_1, \ldots, x_n)$ i de n røttene til den generelle n'tegradsligningen (*) antar m forskjellige verdier under alle permutasjoner av $x_1, \ldots, x_n$, så kan godt $m \geq n$ dersom bare den tilhørende resolventligningen *(i)* av m'te grad er en *ren* ligning, det vil si av formen $g(z) = z^m - b = 0$, og altså $z_1 = \sqrt[m]{b}$.

Ut fra analogien med tredje- og fjerdegradsligningen, samt betraktningene vi har redegjort for ovenfor, ble Lagrange for den generelle n'tegradsligningen ledet til å betrakte følgende polynom

$$(vii) \qquad z_1 = f(x_1, \ldots, x_n) = x_1 + \omega x_2 + \cdots + \omega^{n-1} x_n,$$

der ω er en primitiv n'te enhetsrot. Det spesielle polynomet i *(vii)* kalles *Lagrange-resolventen* til den generelle n'tegradsligningen. Lagrange viste at for $n = 5$ vil denne være rot i en ren ligning $z^5 - b = 0$, der b igjen er et polynom, $b = g(x_1, \ldots, x_5)$, over $\mathbf{Q}(\mathcal{E})$ i røttene $x_1, \ldots, x_5$, og slik at g antar *seks* forskjellige verdier under alle permutasjoner av $x_1, \ldots, x_5$. Derimot er b *ikke* rot i en ren ligning. Dermed bryter Lagranges angrepsstrategi sammen for femtegradsligningen, den strategi som fungerte for tredje- og fjerdegradsligningene, idet man ledes til en resolventligning (som ikke er en ren ligning) av høyere grad enn fem. Selv om han uttrykker en viss tvil på grunn av dette, utelukker ikke Lagrange helt håpet om å kunne løse den generelle femtegradsligningen algebraisk.

I retrospekt kan man si at i det omtalte arbeidet til Lagrange finnes flere ansatser til Galois' senere definitive analyse av algebraisk løsbarhet av ligninger. Dersom man nemlig oversetter til "gruppespråket", så viser faktisk Lagrange den ene (og "letteste") implikasjonen i Galois' teorem anvendt på den generelle n'tegradsligningen: Hvis S_n er en oppløsbar gruppe, så er den generelle n'tegradsligningen algebraisk løsbar. (Se forøvrig drøftingen av dette punktet i [12].)

6. Abels og Ruffinis bevis for at den generelle n'tegradsligningen ikke kan løses algebraisk når $n \geq 5$

Abels teorem [3, s. 75]. Anta at den generelle n'tegradsligningen

$$(*) \qquad x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$$

kan løses algebraisk. La $F = \mathbf{Q}(\mathcal{E}, a_0, a_1, \ldots, a_{n-1})$ være tallkroppen generert av enhetsrøttene $\mathcal{E}$ og koeffisientene $a_0, a_1, \ldots, a_{n-1}$ over de rasjonale tall $\mathbf{Q}$. Da finnes en radikalutvidelse K av F :

$$(**) \qquad F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_{N-1} \subset F_N = K,$$

der $F_{i+1} = F_i(\eta_i)$, $\eta_i^{p_i} = \xi_i \in F_i$, p_i primtall, $i = 0, 1, \ldots, N-1$, slik at K inneholder minst én rot til (*), og der $\eta_0, \eta_1, \ldots, \eta_{N-1}$ kan uttrykkes som polynomer over $\mathbf{Q}(\mathcal{E})$ i røttene $x_1, x_2, \ldots x_n$ til (*).

Vi skal gjennomgå Abels bevis for dette teoremet til slutt. Først vil vi presentere Ruffinis "gruppeteoretiske" resonnement, som basert på Abels teorem gir et elegant bevis for umuligheten av å løse den generelle n'tegradsligningen algebraisk når $n \geq 5$. (Det er egentlig Wantzels [33] forenklede versjon av Ruffinis [28] siste bevisforsøk fra 1813 vi presenterer.)

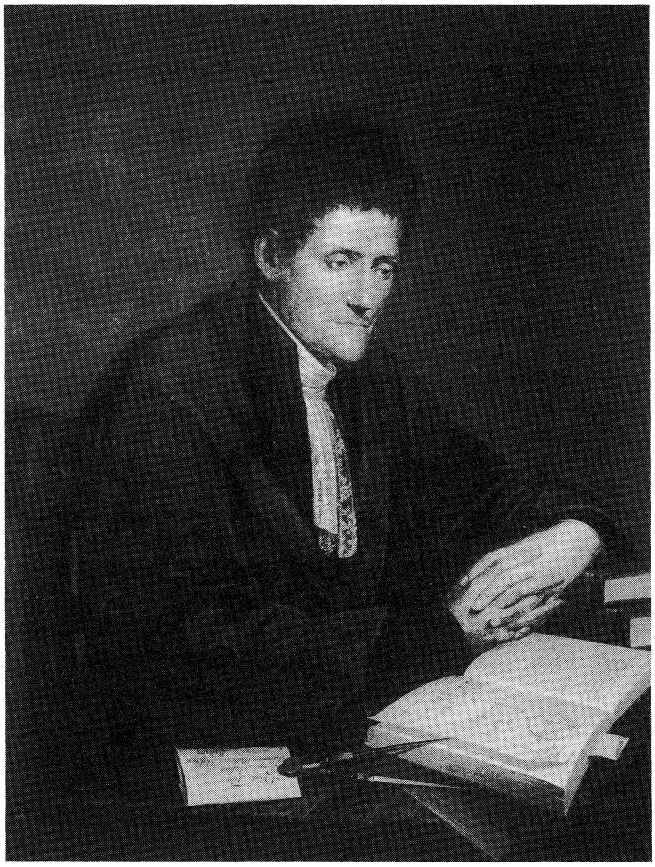
Teorem. (Abel og Ruffini). Den generelle n'tegradsligningen kan ikke løses algebraisk for $n \geq 5$.

Bevis: Anta ad absurdum at det finnes en algebraisk løsning. Vi tar utgangspunkt i radikalutvidelsen (**) som ifølge Abels teorem eksisterer med de nevnte egenskaper. (Vi kan selvfølgelig anta at $F_{i+1} \neq F_i$ for alle $i = 0, \ldots, N-1$, i (**).) La oss først betrakte den første radikalutvidelsen (det "innerste rottegnet") i (**): $F_0 \subset F_1$, det vil si $F \subset F(\eta_0)$, der η_0 er rot i den rene ligningen $x^{p_0} - \xi_0 = 0$. Her er $\xi_0 \in F$ og p_0 et primtall. La nå $\eta_0 = f(x_1, \ldots, x_n)$, der f er et polynom i røttene $x_1, \ldots, x_n$ til den generelle n'tegradsligningen (*) over tallkroppen $\mathbf{Q}(\mathcal{E})$. Da må f forandre verdi for minst én transposisjon, for ellers ville f være et symmetrisk poynom i $x_1, \ldots, x_n$, og følgelig $\eta_0 = f(x_1, \ldots, x_n) \in F$ ved korollaret til fundamentalteoremet for symmetriske polynomer i **4 A**. Vi minner om at enhver permutasjon kan skrives som et produkt av transposisjoner (**4 A**), og at man lett innser at $f_{\sigma\tau} = (f_\tau)_\sigma$ for $\sigma, \tau \in S_n$. Altså finnes en transposisjon τ, som vi kan anta (eventuelt etter renummerering av røttene $x_1, \ldots x_n$) er $\tau = (12)$, slik at $f \neq f_\tau$. Siden $\eta^{p_0} = \xi_0$, har vi

$$(i) \qquad f(x_1, x_2, \ldots, x_n)^{p_0} = \xi_0 \,.$$

Observer at høyresiden ξ_0 i *(i)* er en *symmetrisk rasjonal* funksjon i $x_1, \ldots, x_n$ over $\mathbf{Q}(\mathcal{E})$, idet $\xi_0 \in F = \mathbf{Q}(\mathcal{E}, a_0, a_1, \ldots, a_{n-1})$, og ethvert tall i F er en kvotient mellom to polynomer i $a_0, a_1, \ldots, a_{n-1}$ over $\mathbf{Q}(\mathcal{E})$. Anvend nå $\tau = (12)$ på begge sider av identiteten *(i)*:

$$(ii) \qquad f(x_2, x_1, \ldots, x_n)^{p_0} = \xi_0 \,.$$



Paolo Ruffini
(1765–1822)

Av *(ii)* ser vi at $f(x_2, x_1, \dots, x_n)$ er en rot i $x^{p_0} - \xi_0 = 0$, og altså er

$$(iii) \qquad f(x_2, x_1, \dots, x_n) = \omega\eta_0 = \omega f(x_1, x_2, \dots, x_n),$$

der ω er en primitiv p_0'te enhetsrot. Anvend nå $\tau = (12)$ på begge sider av identiteten *(iii)*:

$$f(x_1, x_2, \dots, x_n) = \omega f(x_2, x_1, \dots, x_n) = \omega^2 f(x_1, x_2, \dots, x_n).$$

Atså er $\omega^2 = 1$ og følgelig $p_0 = 2$. Med andre ord, det første ("innerste") rottegnet i en algebraisk løsning av den generelle n'tegradsligningen er en kvadratrot.

Vi påstår nå at $\eta_0 = f(x_1, \dots, x_n)$ er *invariant* under enhver 3-sykel $\sigma = (ijk)$, det vil si $f = f_\sigma$ for enhver 3-sykel σ. Anvend nemlig σ på begge sider av identiteten

$$(iv) \qquad f(x_1, \dots, x_n)^2 = \xi_0.$$

Da får vi $f_\sigma(x_1, \dots, x_n)^2 = \xi_0$, og altså er

$$(v) \qquad f_\sigma(x_1, \dots, x_n) = s\eta_0 = sf(x_1, \dots, x_n),$$

der s er +1 eller -1. Anvend σ suksessivt to ganger på begge sider av identiteten *(v)*, og bemerk at $\sigma^3 = id$:

$$f_{\sigma^2} = sf_\sigma = s^2 f$$

$$f = f_{\sigma^3} = s^2 f_\sigma = s^3 f\,.$$

Altså er $s^3 = 1$, og følgelig $s = +1$. Av *(v)* får vi $f_\sigma = f$, og påstanden er bevist.

Observasjon: I beviset for påstanden over har vi kun brukt at høyresiden i *(iv)* er invariant under enhver 3-sykel. Altså har vi også bevist: Hvis en rasjonal funksjon $h(x_1, \ldots, x_n)$ over $\mathbf{Q}(\mathcal{E})$ er invariant under enhver 3-sykel, og $g(x_1, \ldots, x_n)$ er et polynom over $\mathbf{Q}(\mathcal{E})$ slik at

$$g(x_1, \ldots, x_n)^2 = h(x_1, \ldots, x_n)\,,$$

så er også $g(x_1, \ldots, x_n)$ invariant under enhver 3-sykel.

Nå er $F_1 = F(\eta_0) = \{b_0 + b_1\eta_0 | b_0, b_1 \in F\}$, siden $\eta_0 = \sqrt{\xi_0}$, $\xi_0 \in F$. Altså er hvert tall i F_1 en rasjonal funksjon i $x_1, \ldots, x_n$ over $\mathbf{Q}(\mathcal{E})$ som er invariant under enhver 3-sykel. Av observasjonen ovenfor slutter vi nå at suksessive kvadratiske utvidelser av F_1 i radikalutvidelsen (**) gir opphav til tallkropper der hvert element er en rasjonal funksjon i $x_1, \ldots, x_n$ over $\mathbf{Q}(\mathcal{E})$ som er invariant under 3-sykler. Dette kan *ikke* lede til en algebraisk løsning av den generelle n'tegradsligningen når $n \geq 3$: Anta nemlig alle de enkle utvidelsene i (**) er kvadratiske og la $x_l \in F_N$, der $x_l \in \{x_1, \ldots, x_n\}$. Ifølge ovenstående er da $g(x_1, \ldots, x_n) = x_l$ invariant under 3-sykler, hvilket er absurd. Altså må det i (**) forekomme en *første* utvidelse $F_{i+1} = F_i(\eta_i)$, $\eta_i^{p_i} = \xi_i \in F_i, p_i$ primtall, slik at $\xi_i = h(x_1, \ldots, x_n)$ er en rasjonal funksjon i $x_1, \ldots, x_n$ over $\mathbf{Q}(\mathcal{E})$ som er invariant under 3-sykler, mens $\eta_i = g(x_1, \ldots, x_n)$ er et polynom i $x_1, \ldots, x_n$ over $\mathbf{Q}(\mathcal{E})$ som *ikke* er invariant under alle 3-sykler. (Spesielt må $p_i \neq 2$). Vi har altså

$$g(x_1, \ldots, x_n)^{p_i} = h(x_1, \ldots, x_n) = \xi_i\,. \tag{vi}$$

La σ være en 3-sykel slik at $g_\sigma \neq g$. Anvend σ på begge sider av identiteten *(vi)* og husk at høyresiden er invariant under σ :

$$g_\sigma(x_1, \ldots, x_n)^{p_i} = h(x_1, \ldots, x_n) = \xi_i.$$

Altså er $g_\sigma(x_1, \ldots, x_n)$ en rot i $x^{p_i} - \xi_i = o$, og følgelig

$$g_\sigma = \omega g\,, \tag{vii}$$

der ω er en primitiv p_i'te enhetsrot. Vi anvender σ suksessivt to ganger på identiteten *(vii)*, idet vi bemerker at $\sigma^3 = id$:

$$g_{\sigma^2} = \omega g_\sigma = \omega^2 g$$

$$g = g_{\sigma^3} = \omega^2 g_\sigma = \omega^3 g\,.$$

Altså er $\omega^3 = 1$, og følgelig $p_i = 3$.

Vi skal vise at dette fører til en selvmotsigelse når $n \geq 5$. Ifølge *(ii)* og *(iii)* i **4 A** kan en 5-sykel skrives som et produkt av to 3-sykler, og en 3-sykel kan skrives som et produkt av to 5-sykler. Dette medfører at et polynom (eller en rasjonal funksjon) $f(x_1, \ldots, x_n)$ er invariant under alle 3-sykler hvis og bare hvis $f(x_1, \ldots, x_n)$ er invariant under alle 5-sykler. Altså må det finnes en 5-sykel $\tau = (rstuv)$ slik at $g_\tau \neq g$. Dessuten må $h_\tau = h$. Av identiteten (formel *(vi)* der $p_i = 3$)

$$g_\tau(x_1, \ldots, x_n)^3 = h(x_1, \ldots, x_n) = \xi_i$$

får vi ved anvendelse av τ at

$$g_\tau(x_1, \ldots, x_n)^3 = h(x_1, \ldots, x_n) = \xi_i \,.$$

Altså er $g_\tau(x_1, \ldots, x_n)$ en rot i $x^3 - \xi_i = 0$. Følgelig må

$$g_\tau = \omega g \,, \tag{viii}$$

der ω er en primitiv tredje enhetsrot. Nå anvender vi 5-sykelen τ fire ganger på begge sider av identiteten *(viii)*, idet vi bemerker at $\tau^5 = id$:

$$g_{\tau^2} = \omega g_\tau = \omega^2 g$$

$$g_{\tau^3} = \omega^2 g\tau = \omega^3 g$$

$$g_{\tau^4} = \omega^3 g_\tau = \omega^4 g$$

$$g = g_{\tau^5} = \omega^4 g_\tau = \omega^5 g \,.$$

Altså er $\omega^5 = 1$, hvilket strider mot at ω er en primitiv tredje enhetsrot. Altså har vi oppnådd en motsigelse til antagelsen om at den generelle n'tegradsligningen kan løses algebraisk, og beviset for teoremet er fullført.

Kommentar. Av de to relasjonene

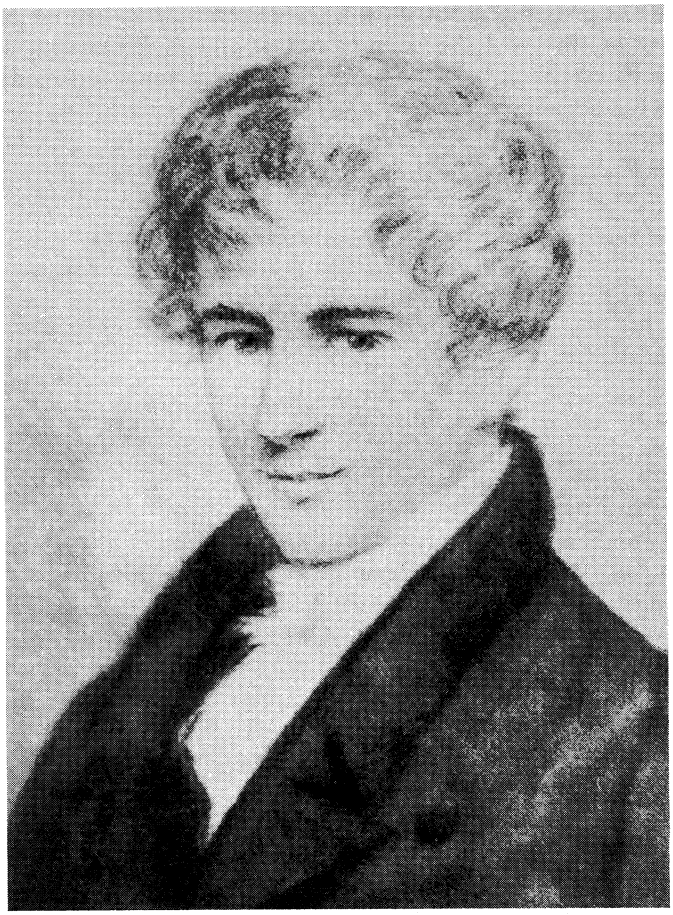
$$(rt)(rs) = (rst)$$

$$(tu)(rs) = (rst)(stu)$$

mellom 2-sykler (transposisjoner) og 3-sykler, der r, s, t, u er fire distinkte elementer i $\{1, 2, \ldots, n\}$, ser man at den *alternerende undergruppen* A_n av den symmetriske gruppen S_n er generert av alle 3-sykler i S_n. (A_n består av de permutasjoner i S_n som kan skrives som et produkt av et *like* antall transposisjoner.) Det er ikke vanskelig å bruke dette til å vise at en rasjonal funksjon $f(x_1, \ldots, x_n)$ i $x_1, \ldots, x_n$ over $\mathbf{Q}(\mathcal{E})$ som er invariant under alle 3-sykler, er av formen

$$f = b_0 + b_1 \Delta \,,$$

der $b_0, b_1 \in F$ og $\Delta = \prod_{1 \leq i < j \leq n}(x_i - x_j)$. Her er Δ kvadratroten av diskriminanten $D = \prod_{1 \leq i < j \leq n}(x_i - x_j)^2$ til (*). D er symmetrisk i x_i'ene og ligger følgelig i F. Dette viser at i radikalutvidelsen (**) vil $F_1 = F(\Delta)$, og når $n \geq 3$ har vi ifølge beviset ovenfor $F_2 = F_1(\eta_1)$, der η_1 er kubikkroten $\sqrt[3]{\xi_1}$ av et tall ξ_1 i F_1.



Niels Henrik Abel
(1802–1829)

Dette er helt i overensstemmelse med det vi vet om den algebraiske løsningen av den generelle annen-, tredje- og fjerdegradsligningen i **3**: Det innerste rottegnet er en kvadratrot, det neste er en kubikkrot.

Vi vender oss nå til beviset for Abels teorem. Det beviset vi skal presentere, er essensielt Abels oprinnelige bevis med en liten modifikasjon som skyldes Kronecker [21], idet man blant annet unngår Abels inndeling av rotuttrykkene etter grad og orden. Det siste viser seg å være unødvendig. La oss forøvrig bemerke at i Abels opprinnelige inndeling forekommer en feil [3, s. 72]. En så stor matematiker som W.R. Hamilton [15, s. 248] uttalte om dette punktet: "It renders it difficult to judge of the validity of his subsequent reasoning". Königsberger [19] viste hvordan Abels feil lett kan rettes opp, og forøvrig understreket han at Abels inndeling av rotuttrykkene etter orden og grad ikke har betydning for resultatet.

Bevis for Abels teorem. Ifølge hypotesen om at den generelle n'tegradsligningen (*) kan løses algebraisk, finnes en radikalutvidelse L av F :

$$(ix)\quad F \subset F(\alpha) \subset \cdots \subset F(\alpha, \ldots, \delta) \subset F(\alpha, \ldots, \delta, \eta) \subset F(\alpha, \ldots, \delta, \eta, \theta) = L\,,$$

slik at L inneholder en rot $x_1$til (*). Her er $\alpha, \ldots, \delta, \eta, \theta$ røtter i rene ligninger av

primtallsgrader over den foregående tallkroppen. Vi skal vise hvordan vi ut fra (ix) kan finne en ny radikalutvidelse K av F av type (**).

La θ i den siste kropputvidelsen $F(\alpha,\dots,\delta,\eta) \subset F(\alpha,\dots,\delta,\eta,\theta)$ (det "ytterste rottegnet") i *(ix)* være rot i den rene ligningen $x^p - a = 0$, der p er et primtall og $a \in F(\alpha,\dots,\delta,\eta)$. Vi kan anta at polynomet $x^p - a$ ikke har noen røtter i $F(\alpha,\dots,\delta,\eta)$. Ellers ville $\theta \in F(\alpha,\dots,\delta,\eta)$ siden F inneholder enhetsrøttene $\mathcal{E}$, og dermed ville den siste kropputvidelsen i *(ix)* være overflødig. Ifølge teorem 3 i **4 B** er $x^p - a$ irredusibel over $F(\alpha,\dots,\delta,\eta)$.

Ifølge korollar 2 til teorem 2 i **4 B** kan $x_1 \in L = F(\alpha,\dots,\delta,\eta,\theta)$ skrives éntydig på formen

$$(x) \qquad x_1 = b_0 + b_1\theta + \cdots + b_{p-1}\theta^{p-1}\,,$$

der b'ene ligger i $F(\alpha,\dots,\delta,\eta)$. Vi kan anta at ikke alle $b_1, b_2, \dots, b_{p-1}$ er 0, fordi ellers er den siste kropputvidelsen i *(ix)* overflødig. Sett uttrykket *(x)* for roten x_1 inn i (*). Vi får da

$$(xi) \qquad c_0 + c_1\theta + \cdots + c_{p-1}\theta^{p-1} = 0\,,$$

der c'ene ligger i $F(\alpha,\dots\delta,\eta)$, idet vi bruker relasjonen $\theta^p = a$ til å gjøre de forskjellige eksponentene til θ mindre enn p. Av korollar 2 til teorem 2 i **4 B** følger at $c_0 = c_1 = \cdots = c_{p-1} = 0$.

Erstatt så θ med $\omega^i\theta$ i *(x)*, for $i = 1, 2, \dots, p-1$, der ω er en primitiv p'te enhetsrot:

$$(xii) \qquad y_i = b_0 + b_1\omega^i\theta + \cdots + b_{p-1}\omega^{(p-1)i}\theta^{p-1}\,.$$

Setter man $x = y_i$ inn i venstresiden i (*), overbeviser man seg lett om at man får

$$c_0 + c_1\omega^i\theta + \cdots + c_{p-1}\omega^{(p-1)i}\theta^{p-1}\,,$$

der c'ene er de samme som i *(xi)*. Siden vi allerede har konstatert at $c_0 = c_1 = \cdots = c_{p-1} = 0$, så trekker vi følgende konklusjon: $y_1, y_2, \dots, y_{p-1}$ i *(xii)* er røtter i (*). Merk at ifølge korollar 2 til teorem 2 i **4 B** er y'ene parvis distinkte og også distinkte fra x_1. Ved eventuell renummerering av røttene $x_1, \dots, x_n$ til (*) kan vi anta $y_1 = x_2, \dots, y_{p-1} = x_p$. Vi har da følgende ligningssett:

$$(xiii) \qquad x_1 = b_0 + b_1\theta + \cdots + b_k\theta^k + \cdots + b_{p-1}\theta^{p-1}$$

$$x_2 = b_0 + b_1\omega\theta + \cdots + b_k\omega^k\theta^k + \cdots + b_{p-1}\omega^{p-1}\theta^{p-1}$$

$$\vdots$$

$$x_{i+1} = b_0 + b_1\omega^i\theta + \cdots + b_k\omega^{ki}\theta^k + \cdots + b_{p-1}\omega^{(p-1)i}\theta^{p-1}$$

$$\vdots$$

$$x_p = b_0 + b_1\omega^{p-1}\theta + \cdots + b_k\omega^{k(p-1)}\theta^k + \cdots + b_{p-1}\omega^{(p-1)^2}\theta^{p-1}\,.$$

La $k \in \{0, 1, \dots, p-1\}$. Multipliser x_{i+1} i *(xiii)* med ω^{-ki} og legg sammen høyre og venstre side i *(xiii)*. Man får da

$$b_k\theta^k = \frac{1}{p}\sum_{i=0}^{p-1}\omega^{-ki}x_{i+1}, \tag{xiv}$$

siden

$$\sum_{i=0}^{p-1}\omega^{li} = \frac{\omega^{lp}-1}{\omega^l - 1} = 0$$

dersom p ikke er en divisor i l.

For de $k \in \{1, 2, \dots, p-1\}$ der $b_k \neq 0$ setter vi nå

$$\nu_k = b_k\theta^k\,. \tag{xv}$$

Av *(xv)* får vi

$$\nu_k^p = b_k^p\theta^{pk} = b_k^p a^k \in F(\alpha, \dots, \delta, \eta)\,. \tag{xvi}$$

Av *(x)* får vi

$$x_1 = b_0 + \sum_{k\in J}\nu_k\,, \tag{xvii}$$

der $J = \{j \geq 1 | b_j \neq 0\}$. Dessuten viser *(xiv)* at b_0 og hver ν_k $(k \in J)$ kan uttrykkes som polynomer i $x_1, \dots, x_n$ over $\mathbf{Q}(\mathcal{E})$. Det er klart at $b_0 \in F(\alpha, \dots, \delta, \eta)$, og *(xvi)* sier at $\nu_k^p \in F(\alpha, \dots, \delta, \eta)$ for $k \in J$.

La $J = \{j_1, \dots, j_l\}$. Vi lager nå en ny radikalutvidelse L' av F ved å erstatte den siste utvidelsen $F(\alpha, \dots, \delta, \eta) \subset F(\alpha, \dots, \delta, \eta, \theta)$ i *(ix)* med l suksessive utvidelser, nemlig

$$F(\alpha, \dots, \delta, \eta) \subset F(\alpha, \dots, \delta, \eta, \nu_{j_1}) \subset \cdots \subset F(\alpha, \dots, \delta, \eta, \nu_{j_1}, \dots, \nu_{j_l}) = L'\,.$$

(Man kan lett vise at $L' = L$, men det behøves ikke.) Av *(xvii)* har vi at $x_1 \in L'$. La nå z_1 være enten b_0 eller en av $\nu_{j_1}^p, \dots, \nu_{j_l}^p$. Da er

$$z_1 = g(x_1, \dots, x_n)$$

for et passende polynom i $x_1, \dots, x_n$ over $\mathbf{Q}(\mathcal{E})$. La $z_1, \dots, z_m$ være de forskjellige verdiene g antar under alle permutasjoner av $x_1, \dots, x_n$. Da er z_1 en rot til ligningen

$$h(z) = (z - z_1)\cdots(z - z_m) = 0\,. \tag{xviii}$$

Man observerer at koeffisientene til $h(z)$ er symmetriske polynomer i $x_1, \dots, x_n$ over $\mathbf{Q}(\mathcal{E})$, og ifølge korollaret til fundamentalteoremet for symmetriske polynomer i **4 A** er $h(z)$ et polynom over F. Siden $z_1 \in F(\alpha, \dots, \delta, \eta)$ kan z_1 skrives éntydig på formen (korollar 2 til teorem 2 i **4 B**)

$$z_1 = d_0 + d_1\eta + \cdots + d_{q-1}\eta^{q-1}, \tag{xix}$$

der d'ene ligger i $F(\alpha, \ldots, \delta)$ og der η er rot i den rene ligningen $x^q - e = 0$, $e \in F(\alpha, \ldots, \delta)$, q primtall. (Vi antar at $\eta \notin F(\alpha, \ldots, \delta)$ slik at $x^q - e$ ifølge teorem 3 i **4 B** er irredusibel.)

Ved å resonnere på nøyaktig samme måte som ovenfor, idet ligningen *(xviii)* nå spiller samme rollen som ligningen (*) gjorde, finner man at $d_r\eta^r$, for $r \in \{0, 1, \ldots, q-1\}$, kan uttrykkes som polynom i $z_1, \ldots, z_m$ over $\mathbf{Q}(\mathcal{E})$, og følgelig også som polynom i $x_1, \ldots, x_n$ over $\mathbf{Q}(\mathcal{E})$. For de $r \in \{1, 2, \ldots, q-1\}$ der $d_r \neq 0$ setter vi $\mu_r = d_r\eta^r$. Da er $\mu_r^q \in F(\alpha, \ldots, \delta)$. Dessuten er $d_0 \in F(\alpha, \ldots, \delta)$. Denne prosedyren gjennomføres for alle b_0 og $\nu_{j_1}^p, \ldots, \nu_{j_l}^p$, og man erstatter så den nest siste utvidelsen $F(\alpha, \ldots, \delta) \subset F(\alpha, \ldots, \delta, \eta)$ i *(ix)* med en suksesjon av utvidelser basert på μ'ene, analogt det vi gjorde ovenfor med ν'ene. (Dersom det viser seg at $d_r = 0$ for alle $r \geq 1$ i de forskjellige uttrykkene *(xix)*, så kan utvidelsen $F(\alpha, \ldots, \delta) \subset F(\alpha, \ldots \delta, \eta)$ sløyfes helt).

Vi fortsetter den beskrevne prosedyren helt til vi (etter et endelig antall skritt) kommer til den første utvidelsen $F \subset F(\alpha)$ i *(ix)*. Vi har da oppnådd å finne en ny radikalutvidelse K av F av den ønskede formen (**), som beskrevet i teoremet.

Dette fullfører beviset for Abels teorem.

7. Sluttkommentar

Abel publiserte kun to arbeider utelukkende viet ligningsteorien før han døde. Det ene var det ovenfor omtalte beviset for umuligheten av å løse den generelle n'tegradsligningen algebraisk når $n \geq 5$. Det andre var en avhandling om en spesiell klasse ligninger som er algebraisk løsbare [4]. Et stort eksempelmateriale på denne type ligninger støtte Abel på i studiet av elliptiske funksjoner, spesielt "delingsligningen", som er analog til sirkeldelingsligningen $x^n - 1 = 0$ studert tidligere av Gauss. Etter Abels opprinnelige plan skulle avhandlingen, foruten de fem paragrafer den består av, ha minst to til som skulle omhandle anvendelser på elliptiske funksjoner, spesielt slike som tillater kompleks multiplikasjon. Foruten delingen av perioden til en elliptisk funksjon skulle den inneholde elliptiske transformasjonsformler og algebraiske anvendelser av disse. Det er sannsynligvis kappestriden mellom Abel og Jacobi på de elliptiske funksjoners område som gjorde at han ikke rakk å fullføre avhandlingen. Man finner forøvrig en innholdsfortegnelse gjengitt i [1,vol 2, s. 310–311]. De ligninger som Abel studerte i sin publiserte avhandling, ble senere av Kronecker og Jordan kalt for "abelske ligninger". Da det viser seg at disse nettopp er karakterisert ved at de tilhørende Galois-gruppene er kommutative, ble Abels navn på denne måten heftet til kommutative algebraiske strukturer.

Det som er nevnt ovenfor om Abels avhandling, er symptomatisk. Det er ingen vanntette skott i hans matematiske forskning, og ligningsteorien går igjen som en rød tråd i store deler av hans matematiske arbeider. Abel var først og fremst algebraiker, og han ga flere ganger uttrykk for at ligningsteorien var hans yndlingsstudium. I hans arbeider over elliptiske funksjoner trådte behandlingen av de forskjellige algebraiske ligninger, som denne teorien er så rik på, sterkt i forgrunnen. Hva mer er, ligningsteorien var i hans hånd det mest virksomme verktøy. For eksempel var det uten tvil den algebraiske løsningen av den elliptiske delingsligningen

som fra først av førte ham til den elliptiske transformasjonsteori. Også i beviset for det egentlige Abels teorem, det såkalte "addisjonsteoremet", spiller ligningsteorien en vesentlig rolle.

Évariste Galois
(1811–1832)

Et meget spennende og interessant emne, både matematisk og historisk, er spørsmålet om i hvilken grad Abels arbeider har bidratt til å muliggjøre Galois' definitive analyse av ligningsteorien, som topper seg i sistnevntes beundringsverdige fundamentalteorem [14]. Selv om Galois et sted sterkt benekter noen avhengighet av Abel, så er nok ikke det hele sannheten. Ingen har behandlet dette emnet så inngående og med så stor innsikt, såvidt artikkelforfatteren vet, som Sylow, som forøvrig sammen med Sohus Lie sto bak utgivelsen av den andre utgaven av Abels samlede verker i 1881 [1]. (Førsteutgaven kom i 1839 ved Holmboe.) Ved hundreårsjubileet for Abels fødsel i 1902 skrev Sylow en artikkel der han gjennomgår Abels matematiske testamente i detalj [30]. Det er to ting Sylow fremhever ved Abels arbeider, som må ha påvirket en så levende intelligens som Galois'. Det ene er den anvendelse Abel gjorde av et polynoms irredusibilitet, noe vi har sett flere eksempler på i denne artikkelen. Det andre er muligheten av å uttrykke alle røttene til et polynom ved en eneste størrelse, den man senere har kalt *Galois-resolventen*. Abel

anvender denne i sin siste avhandling om elliptiske funksjoner [1, s. 547] og tenker seg til og med det irredusible polynomet som har resolventen som rot, redusert ved å "adjungere" visse "irrasjonaliteter". Dette sted hos Abel har Galois sitert både i avhandlingen "Sur la théorie des nombres" og i den posthume "Mémoire sur les conditions de résolubilité des équations par radicaux" [14]. Det er nettopp ved den forente anvendelse av disse prinsipper og ved en slutningsmåte som er analog til Abels i avhandlingen om Abelske ligninger, at Galois beviser sitt epokegjørende fundamentalteorem.

Både Abel og Galois hadde et klart begrep om det vi idag kaller en kropp (tidligere kalt "rasjonalitetsområde"). I sine respektive arbeider om algebraiske løsninger av ligninger antar de at denne kroppen inneholder de rasjonale tall, altså er det vi idag kaller en kropp av karakteristikk 0. Når de snakker om rasjonalitetsområder generert eller bestemt av vilkårlige størrelser $x', x'', \ldots$, er det uklart om de mener at disse størrelsene er uspesifiserte komplekse tall. To argumenter for at de (implisitt) tenker seg alle størrelsene de betrakter, er komplekse tall er: (i) De tenker seg at komplekse enhetsrøtter er til deres disposisjon, og (ii) de tar for gitt at alle polynomer de betrakter, har røtter som ligger i et eventuelt større rasjonalitetsområde. Ifølge Gauss' bevis for algebraens fundamentalteorem er dette intet problem dersom størrelsene er komplekse tall. Beviset for at (ii) er riktig for kropper generelt, kom senere og skyldes Kronecker.

I Abels etterlatte skrifter finner vi et utkast til et større arbeid om algebraiske ligninger [5]. Her stiller han seg følgende problem: Finn formen som en algebraisk løsning til et irredusibelt polynom av gitt grad n må ha. Han stiller opp flere teoremer og antyder bevis for disse. Det ble Kronecker [20] som fullførte dette byggverket som Abel la fundamentet for. La oss som eksempel skrive ned den løsningen Abel selv meddeler for $n = 5$ over de rasjonale tall $\mathbf{Q}$. Dersom et irredusibelt polynom over $\mathbf{Q}$ av femte grad kan løses algebraisk, så må enhver rot ξ kunne skrives på følgende form:

$$\xi = A + P_0 k_0^{3/5} k_1^{4/5} k_2^{2/5} k_3^{1/5} + P_1 k_1^{3/5} k_2^{4/5} k_3^{2/5} k_0^{1/5}$$

$$+P_2 k_2^{3/5} k_3^{4/5} k_0^{2/5} k_1^{1/5} + P_3 k_3^{3/5} k_0^{4/5} k_1^{2/5} k_2^{1/5},$$

der

$$k_0 = C + B\sqrt{1+e^2} + \sqrt{h\left(1 + e^2 + \sqrt{1+e^2}\right)}$$

$$P_0 = A_1 + A_2 k_0 + A_3 k_2 + A_4 k_0 k_2 .$$

Her er $A, B, C, e, h, A_1, A_2, A_3, A_4$ rasjonale tall, og k_0, k_1, k_2, k_3 fremkommer av den gitte formelen for k_0 ved å ta alle mulige kombinasjoner av $\pm$ foran de to distinkte kvadratrottegnene som forekommer. Dessuten fremkommer P_0, P_1, P_2, P_3 av formelen for P_0 ved syklisk ombytting av k_0, k_1, k_2, k_3. Motsatt vil en ξ som er på formen ovenfor, være rot i et polynom over $\mathbf{Q}$ av femte grad. Se forøvrig [35] Band I, §196.

Av de formler Abel forøvrig stiller opp for det tilfellet at graden er et primtall, utleder han at røttene til et irredusibelt polynom av primtallsgrad som er algebraisk løsbart, kan skrives som et polynom over grunnkroppen i to vilkårlige av røttene [30, s. 21]. Han formoder at den motsatte implikasjonen er riktig. Galois beviste

dette ved å bruke sitt fundamentalteorem, og det inngår som den siste proposisjon i hans skjellsettende arbeid "Mémoire sur les conditions de résolubilité des équations par radicaux". (Dette arbeidet ble først publisert i 1846, fjorten år etter Galois' død, av Liouville i det matematiske tidsskriftet som sistnevnte grunnla [14].) Ved å bruke "Abel-delen" av det ovenfor omtalte resultatet til Abel og Galois, kan man lett vise at ingen polynomer over $\mathbf{Q}$ av formen

$$x^p + 2qx^2 - q\,,$$

der p er et primtall ≥ 5 og q er et vilkårlig primtall, kan løses algebraisk over $\mathbf{Q}$. Man viser nemlig at polynomet er irredusibelt over $\mathbf{Q}$ og antall reelle røtter er > 1 og $< p$. (Observer også at "Abel-delen" gir et nytt bevis for at den generelle femtegradsligningen ikke kan løses algebraisk.)

Sluttbemerkning. Ved en såkalt Tschirnhousen-transformasjon kan man redusere en femtegradsligning til en ligning av formen $x^5 + ax + b = 0$. For at en slik ligning over $\mathbf{Q}$ (forutsatt irredusibel) skal være algebraisk løsbar er det nødvendig og tilstrekkelig at koeffisientene er av formen

$$a = \frac{5\mu^4(4\lambda + 3)}{\lambda^2 + 1}$$

$$b = \frac{4\mu^5(4\lambda + 3)(2\lambda + 1)}{\lambda^2 + 1}$$

med $\lambda, \mu \in \mathbf{Q}$. For eksempel gir $\lambda = -24/7$ og $\mu = -5$ koeffisientene i Eulers ligning nevnt i **2**. (Se Netto [23].)

8. Litteratur

Heinrich Webers [35] monumentale trebindsverk "Lehrbuch der Algebra" fra 1895 gir en encyklopedisk oppsummering og et storslagent panorama over algebraens sentrale problemstillinger i det nittende århundret, med linjer tilbake til de tre foregående århundrene. Av Webers verk fremgår det hvilken sentral posisjon lignings-teorien hadde i algebra i det forrige århundret, der blant annet teorien for de elliptiske funksjoner ga et vell av eksempler på (spesielle) algebraiske ligninger som ble studert. Webers fremstilling av Galois-teorien står med én fot i det nittende århundret og én i de tyvende. Fortsatt er tilknytningen til ligningsteorien sterk, men gruppebegrepet er nå helt frigjort fra denne. Dessuten merker man Dedekinds innflytelse ved at de første steg tas i retning av å definere isomorfi mellom tallkropper som basis for definisjon av Galois-gruppen.

En forløper for Webers lærebøker i algebra er Camille Jordans [17] klassiske "Traité des substitutions et des équations algébriques" fra 1870. Med Jordans "Traité" ble Galois' ligningsteori den matematiske verdens fullstendige eiendom. Jordans verk gir den første originale fremstilling av Galois-teorien siden Galois selv. Hans bok kan samtidig betraktes som den første lærebok i gruppeteori, der blant annet kriterier for når en endelig gruppe er oppløsbar, drøftes inngående. Et stort eksempelmateriale av spesielle ligninger hentet fra teorien for elliptiske funksjoner gjennomgås.

Den første læreboken i algebra som behandlet Galois-teorien, var tredjeutgaven av Serrets [29] "Cours d'algèbre supérieure" fra 1866. (Førsteutgaven kom i 1849.) Presentasjonen av Galois-teorien er en parafrase av Galois' egen fremstilling, men med detaljerte bevis. Dessuten gir Serret i sin lærebok en grundig fremstilling av den klasiske ligningsteorien helt frem til Abel. Serrets læreverk kom i mange opplag og var en standardtekst og referanse i algebra så sent som 1900.

Ellers finnes det en omfattende litteratur som behandler forskjellige aspekter ved den klassiske ligningsteorien, og vi tar med i litteraturlisten nedenfor noen som er spesielt relevante for denne artikkelen. Når det gjelder historikk over ligningsteorien henviser vi til de meget lesverdige artiklene til Kiernan [18] og Ayoub [7], samt til bøkene [32], [39] og [40].

[1] N.H. Abel. *Oeuvres complètes.* Publiée par L. Sylow et S. Lie, 2 vols., Christiania (1881).

[2] N.H. Abel. *Mémoire sur les équations algébriques, ou l'on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré.* Oeuvres complètes, vol. 1, 28–33.

[3] N.H. Abel. *Démostration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré.* Oeuvres complètes, vol. 1, 66–87.

[4] N.H. Abel. *Mémoire sur une classe particulière d'équations résolubles algébriquement.* Oeuvres complètes, vol. 1, 478–507.

[5] N.H. Abel. *Sur la résolution algébrique des équationas.* Oeuvres complètes, vol. 2, 217–243.

[6] E. Artin. *Foundations of Galois theory.* New York University, Lecture notes, New York (1938).

[7] R.G. Ayoub. *Paolo Ruffini's contributions to the quintic.* Archive for History of Exact Sciences, 23 (1980), 253–277.

[8] O. Bolza. *On the theory of substitution-groups and its applications to algebraic equations.* American Journal of Mathematics, 13 (1891), 52–142.

[9] H. Burkhardt. *Die Anfänge der Gruppentheorie und Paolo Ruffini.* Zeitschrift für Mathematik und Physik, 37 (1892), 121–159.

[10] A. L. Cauchy. *Journal de l'École Polytechnique.* 10 (1815), 1–28, = Oeuvres, (2), 1, 64–90.

[11] A.L. Cauchy. *Oeuvres.* (1), Vols. 9, 10.

[12] E. Dehn. *Algebraic equations; An introduction to the theories of Lagrange and Galois.* Dover Publications (1960).

[13] H.M. Edwards. *Galois theory.* Springer Verlag, 1984.

[14] E. Galois. *Oeuvres mathématiques d'Évariste Galois. Préface par J. Lioville.* Journale de mathématique pures et appliquées, (1), 11 (1846), 381–444.

[15] W.R. Hamilton. *Transactions of the Royal Irish Academy.* Vol. 18, Part 2, Dublin (1839).

[16] O. Hölder. *Galois'sche Theorie mit Anwendungen.* Encyklopädie der Mathematische Wissenschaften. Vol. 1: Arithmetik und Algebra. Leipzig: Teubner (1898–1904).

[17] C. Jordan. *Traité des substitutions et des équations algébriques.* Paris: Gauthiers-Villars (1870).

[18] B.M. Kiernan. *The development of Galois theory from Lagrange to Artin.* Archive for History of Exact Sciences, 8 (1971), 40–154.

[19] L. Königsberger. *Berichtigung eines Satzes von Abel, die Darstellung der algebraischen Funktionen betreffend.* Mathematische Annalen, 1 (1869), 168–169.

[20] L. Kronecker. *Über die algebraisch auflösbaren Gleichungen.* Monatsberichte der Berl. Akademie (1853, 1856).

[21] L. Kronecker. *Einige Entwicklungen aus der Theorie der algebraischen Gleichungen.* Monatsbericht der Berl. Akademie (1879).

[22] J.L. Lagrange. *Réflexions sur la résolution algébrique des équations.* Nouveaux Memoires de l'Académie royale des Sciences et Belles-Lettres de Berlin (1770–1771).

[23] E. Netto. *Vorlesungen über Algebra.* 2 Bänder, Leipzig: Teubner (1896, 1900).

[24] S. Petersen. *De algebraiske ligningers teori.* København: Høst & Søns Forlag (1877).

[25] J. Pierpoint. *Lagrange's place in the theory of substitutions.* Bulletin of the American Mathematical Society, (2) 1 (1895), 196–204.

[26] J. Pierpoint. *On the Ruffini-Abelian theorem.* Bulletin of the American Mathematical Society, (2) 3 (1896), 200–221.

[27] P. Ruffini. *Teoria generale delle Equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grade superiore al quarto.* Bologna (1799). (Opere Matematiche, 3 vol., Bortolotti (ed.), Palermo (1915.)

[28] P. Ruffini. *Riflessioni interno alla soluzione delle equazioni algebraiche generali.* Modena (1813). (Opere Mathematiche.)

[29] J.A. Serret. *Cours d'algèbre supériure.* 3ième édition, 2 vol. (1866).

[30] L. Sylow. *Abels studier og hans opdagelser.* Festskrift ved hundreårsjubilæet for Niels Henrik Abels fødsel. Kristiania (1902).

[31] B.L. Van der Waerden. *Algebra I.* Achte Auflage, Springer-Verlag (1971).

[32] B.L. Van der Waerden. *A History of Algebra.* Springer-Verlag (1985).

[33] P.L. Wantzel. *Démonstration de l'impossibilité de résoudre toutes les équations algébriques avec des radicaux.* Nouvelles Annales de Mathématiques pures et appliqués, 4 (1845).

[34] E. Waring. *Meditationes Algebraicae.* Cambridge (1770).

[35] H. Weber. *Lehrbuch der Algebra.* 3 Bänder, Braunschweig: Druck und Verlag von Friedrich Vieweg und Sohn (1895–1896).

[36] L. Young. *Mathematicians and their Times.* Mathematics Studies 48, North Holland (1981).

[37] B. Holmboe. *Lærebog i den høiere Mathematik.* Christiania: Chr. Grøndahl (1849).

[38] B. L. Van der Waerden. *"Die Galois-Theorie von Heinrich Weber bis Emil Artin".* Archive for History of Exact Sciences, 9 (1972), 240–248.

[39] L. Nový. *"Origins of Modern Algebra".* Prague: Publishing House of the Czechoslovak Academy of Sciences (1973).

[40] J. P. Tignol. *"Galois' Theory of Algebraic Equations".* Longman Scientific & Technical (1988).