Abel och lösbara ekvationer av primtalsgrad

Lars Gårding

Matematiska Institutionen
Universitetet i Lund
Box 725
S-220 07 Lund

Niels Henrik Abel visade 1824 att den allmänna ekvationen av grad 5 inte kan lösas med rotutdragningar och rationella operationer. Två år senare ger han i ett brev till Crelle rotuttryck för rötterna till en femtegradsekvation som kan lösas på detta sätt och skriver dessutom att han utsträckt resultatet till ekvationer av primtalsgrad. Hans bevis finns bara delvis i det efterlämnade manuskriptet [5] om lösbara ekvationer och deras rötter. Det har en utförlig inledning och början, men slutet, som handlar om ekvationer av primtalsgrad, är en oredigerad skiss.

För Abel var målet att finna rötternas form hos lösbara ekvationer. För hans yngre rival, Évariste Galois, var målet ett annat: att finna de möjliga symmetrigrupperna eller Galoisgrupperna för lösbara ekvationer. Båda avled innan de kunnat skriva färdiga arbeten. Galois kunde lösa sitt problem för ekvationer av primtalsgrad medan Abel inte hann fullborda sitt mera ambitiösa projekt.

Via Christian Skaus intressanta artikel [10] i Normat (1990) och en uppsats [9] av den svenska matematikern Malmsten (Crelle 1847) där Abels ofullbordade manuskript [5] bearbetas, har jag kommit att läsa manuskriptet och de arbeten som följde efter av Kronecker [8] och Weber [12].

Abels manuskript slutar med en explicit men okommenterad formel för rötterna hos en lösbar ekvation. Samma formel finns hos Kronecker och Weber som emellertid inte citerar Abel på denna punkt. Det betyder att Abel visste eller gissade sitt slutresultat, som dessutom implicit och i viss form innehåller en berömd sats av Galois. Men beviset har luckor, vilket också utretts av Abels kommentator Sylow. Avsikten med denna artikel är att fylla ut bevisen på ett sätt som harmonierar med Abels manuskript.

Vad det rör sig om mera i detalj är lätt att förstå med tillgång till några av den nutida algebrans basbegrepp. Trots att läsaren beräknas känna till dem, räknar jag upp dem i ett inledande avsnitt.

Carl Johan Malmsten blev 1841 professor i matematik i Uppsala och skrev under 1840-talet många anmärkningsvärda arbeten. Han var efter Klingenstierna den förste matematiker i Sverige som både följde med sin tid och bidrog till den. Den unge professorns framställningskonst gjorde matematiken till ett modeämne i 1840-talets Uppsala. Han var en ofta anlitad talare, och hans goda hand med språket syns också i de arbeten han skrev på svenska. Då han presenterade sig för en större publik, blev språket franska eller latin. Malmsten var först och främst analytiker

och var kanske den förste i Sverige som förstod vad konvergens är för något. Före Riemann fann han funktionalekvationer för funktioner analoga med ζ-funktionen, dock utan att använda dem, och han var den förste med en sträng teori för kedjebråk. Liksom de flesta matematiker läste han Abels arbeten, särskilt det posthuma [5] om ekvationer som kan lösas genom rotutdragning, senare kallade metacykliska. Läsningen avsatte det intressanta arbetet [9] (Crelle 1847). Det citeras av Kronecker [8] några år senare och har antagligen haft en viss betydelse för dennes arbeten om rötternas struktur som senare generaliserades av Heinrich Weber och finns tillgängliga i t.ex. Weber [12].

Till slut vill jag tacka Christian Skau för hans tålamod och de lärorika diskussioner han fört med mig om Abels manuskript.

1. Algebraiska förberedelser

Jag antar att läsaren vet vad en kropp är. Mängden av polynom

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m$$

i en obestämd x med koefficienter i en kropp K betecknas med $K[x]$. Genom multiplikation av polynom blir $K[x]$ en ring och samtidigt ett linjärt rum av oändlig dimension över K. Då $a_m \neq 0$ sägs $f(x)$ ha grad m. Man har $\operatorname{grad} f(x)g(x) = \operatorname{grad} f(x) + \operatorname{grad} g(x)$ för icke försvinnande polynom. I $K[x]$ har man entydig faktoruppdelning modulo multiplikation med element i $K \setminus 0$. Polynom utan faktorer av positiv grad sägs vara irreducibla. Då t är ett element i en kropp innehållande K, låter vi $K(t)$ beteckna alla $f(t)/g(t)$ med $f(x)$, $g(x) \in K[x]$, $g(t) \neq 0$. Analogt för $K(t_1, \ldots, t_n)$.

En bijektion $U : K \to L$ mellan kroppar sägs vara en isomorfism om $U(ab) = UaUb$ och $U(a \pm b) = Ua \pm Ub$ för alla a, $b \in K$. Då $L = K$ säger man att U är en automorfism. Alla automorfismer $L \to L$ bildar en grupp under sammansättning som vi kallar $\operatorname{Aut} L$. Med $\operatorname{Aut}(L/K)$ ska vi mena den undergrupp i $\operatorname{Aut} L$ som är identiteten på en del K av L.

Ett element t i en överkropp till en kropp K sägs vara algebraiskt av grad m över K om $1, t, \ldots, t^{m-1}$ är linjärt oberoende över K och t^m ligger i deras linjära hölje. Det betyder att det finns ett polynom $f(x) \in K[x]$ av minsta grad m sådant att $f(t) = 0$. Vi säger att $f(x)$ är ett minimalpolynom till t och att m är graden av t över K. Det är klart att varje minimalpolynom är irreducibelt och bestämt på en konstant när. Vi kan då bilda kvotringen $K[x]$ mod $f(x)$ som visar sig vara isomorf med $K(t)$. Om $K \to K'$ är en isomorfism och $f'(x)$ är bilden av ett irreducibelt polynom $f(x) \in K[x]$, så är motsvarande kvotringar isomorfa. Om t, t' är rötter till motsvarande ekvationer följer alltså att

(*) *varje isomorfism $K \to K'$ kan fortsättas till en isomorfism $K(t) \to K'(t')$.*

Algebraiska talkroppar erhåller man genom att successivt adjungera algebraiska tal. En upprepad användning av (*) visar

Fortsättningssats. Om $K \subset L$ är algebraiska talkroppar kan varje isomorfism från K fortsättas till en isomorfism från L.

Galoiskroppar, Galoisgrupper

Två rötter till ett och samma irreducibla polynom sägs vara konjugerade till varandra. Om $f(x) \in K[x]$ är irreducibel av grad n med rötterna $\alpha_1, \ldots, \alpha_n$, så sägs $L = K(\alpha_1, \ldots, \alpha_n)$ vara sönderfallskroppen till $f(x)$. Vi skriver då också $L = K(f)$ och $\mathrm{Aut}(L/K) = \mathrm{Aut}(f/K)$.

Om $U \in \mathrm{Aut}(f/K)$ och $f(\alpha) = 0$, är också $f(U\alpha) = 0$, dvs α och $U\alpha$ är konjugerade. Dessutom, om α, β är rötter kan enligt $(*)$ isomorfismen $K(\alpha) \to K(\beta)$ utvidgas till en isomorfism i $\mathrm{Aut}(f/K)$. Denna grupp överför alltså varje rot i varje annan rot.

En algebraisk kropp $L \supset K$ sägs vara en Galoiskropp över K då $UL = L$ för varje isomorfism $U : L \to UL$ som är identiteten på K. Varje sönderfallskropp $L = K(\alpha_1, \ldots, \alpha_n)$ över K har denna egenskap, ty $U\alpha_1, \ldots$ är då lika med rötterna $\alpha_1, \ldots$ i någon ordning. Alltså är $\mathrm{Aut}(f/K)$ isomorf med en undergrupp av alla permutationer av n element. Följaktligen är antalet element i $\mathrm{Aut}(f, K)$ en delare till $n!$.

Det följer av $(*)$ att om L är en Galoiskropp över K, $v, w \in L$, och $Uv = v$ medför att $Uw = w$ för varje $U \in \mathrm{Aut}(L/K)$, så är w ett polynom i v med koefficienter i K.

2. Radikalutvidgningar

Enkla radikalutvidgningar

Varje kropp i det följande antas innehålla de rationella talen. En kropp L sägs vara en enkel radikalutvidgning av grad n av en kropp K då K innehåller en primitiv n^{te} enhetsrot ω och $L = K(s)$, där s är nollställe till ett irreducibelt polynom $h(x) = x^n - a \in K[x]$. Alla rötter har då formen $\omega^k s$ för $k = 0, \ldots, n-1$. Speciellt är $K(s)$ en Galoiskropp över K, elementen har formen

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

gruppen $\mathrm{Aut}(K(s)/K)$ är cyklisk av grad n och alstras av $s \to s\omega$. De konjugerade till u över K har alltså formen

$$u_j = a_0 + a_1 \omega^j s + \cdots + a_{n-1} (\omega^j s)^{n-1}. \tag{1'}$$

Inför man Lagranges resolventer

$$(\omega^k, u) = \sum_0^{n-1} \omega^{-kj} u_j, \tag{2}$$

får man av (1') att

$$n a_k s^k = (\omega^k, u). \tag{3}$$

Lemma 1. Om $K(s)$ är en enkel radikalutvidgning av primtalsgrad p av en kropp K och $s' = bs^k$ där $0 < k < p$ och $0 \neq b \in K$, så är $K(s) = K(s')$ och potenserna $s, \ldots, s^{p-1}$ är permutationer av motsvarande potenser av s' multiplicerade med tal ur K.

Anmärkning: Om s är rot till $x^p - a \in K[x]$, är s' rot till $x^p - b^p a^k \in K[x]$, där båda polynomen är irreducibla.

Bevis: Med $kj' \equiv j \bmod p$ är $s^j = b_j s'^{j'}$ för något $b_j \in K$, ty $s^p \in K$. Vidare är $j \to j'$ en permutation av $1, \dots, p-1 \bmod p$. Härav följer uppenbarligen att $K(s) = K(s')$.

Sats 1. Låt

$$K \subset L \subset L(s)$$

vara kroppar och antag att $L(s)$ är en enkel radikalutvidgning av L av primtals grad p och att K innehåller en primitiv p^{te} enhetsrot ω. Låt vidare M vara en Galoiskropp över K. Då är $M \cap L(s) = M \cap L$, eller också finns ett $s' \in (M \cap L)(s)$ sådant att $L(s') = L(s)$ och

$$(L \cap M) \subset (L \cap M)(s') = L(s') \cap M$$

är en enkel radikalutvidgning av grad p.

Bevis: Eftersom $L(s) \supset L$ behöver vi bara betrakta det senare fallet $M \cap L(s) \neq M \cap L$. Då finns ett $u \in L(s) \setminus L$ som också ligger i M. Det har då formen (1) där något $a_k s^k \neq 0$ och $k > 0$. Fixera ett sådant u och sätt $s' = a_k s^k$. Då är enligt lemmat $L(s) = L(s')$ och, om vi uttrycker u som polynom i s', får u formen (1) där koefficienten för s' är lika med 1. Vi kan alltså från början anta att $s' = s$ och $a_1 = 1$ för vårt speciella u.

Eftersom $u \in M$ är alla dess konjugerade $u_0, \dots, u_{p-1}$ över $L \supset K$ en del av de konjugerade över K och ligger alltså i M. Detsamma gäller resolventerna, och eftersom $a_1 = 1$, följer att $s = (\omega, u)/p$ ligger i M. Vi kan nu upprepa resonemanget med ett godtyckligt

$$v = b_0 + b_1 s + \cdots + b_{p-1} s^{p-1}$$

i $L(s) \setminus L$ som ligger i M. Dess konjugerade och resolventer ligger i M och eftersom $s \in M$ ser vi att koefficienterna $b_0, \dots$ också ligger i M. Det betyder att $(M \cap L)(s)$ är en enkel radikalutvidgning av primtalsgrad p av $L \cap M$, och satsen är bevisad.

Sammansatta och primära radikalutvidgningar

Då n är en produkt mk kan man sönderlägga en enkel radikalutvidgning $K \subset K(s)$ i två,

$$K \subset K(s^m) \subset K(s).$$

Man säger att L är en radikalutvidgning av K om det finnes en kedja enkla radikalutvidgningar

$$K \subset K_1 \subset \cdots \subset L \tag{4}$$

som slutar med L. Enligt det som sagts ovan kan man anta att varje kropp i kedjan har primtalsgrad över den föregående. Då alla dessa primtal är lika säger vi att L är en *primär* radikalutvidgning av K.

Sats 2. Låt L vara en Galoiskropp över en kropp K. Varje enkel radikalutvidgning $L \subset L(s)$ av primtalsgrad p kan utvidgas till en primär radikalutvidgning $L \subset M$, där M är den minsta Galoiskropp över K som innehåller $L(s)$.

Bevis: Låt $s_1, \dots, s_k$ med $s = s_1$ vara alla konjugerade till s över K och $x^p - c_1$, $\dots$, $x^p - c_k$ motsvarande polynom i $L[x]$. I sviten

$$L \subset L(s_1) \subset L(s_1, s_2) \subset \cdots \subset L(s_1, \dots, s_k)$$

är varje kropp antingen identisk med den föregående eller en enkel radikalutvidgning av grad p, och den sista kroppen är den minsta Galoiskropp över K som innehåller $L(s)$.

Ekvationslösning genom rotutdragning

Låt $f(x) \in K[x]$ vara ett irreducibelt polynom med koefficienter i en kropp K, som antas innehålla alla enhetsrötter. Att ekvationen $f(x) = 0$ är lösbar med successiva rotutdragningar och rationella operationer betyder att det finns en svit enkla radikalutvidgningar

$$K \subset L_1 \subset \cdots \subset L_{n-1} \subset L_n \tag{5}$$

där L_n innehåller en rot till $f(x) = 0$, dvs ett element i sönderfallskroppen $K(f)$ av $f(x)$ över K. Enligt Sats 1 är då $K(f) \cap L_n = K(f) \cap L_{n-1}$, eller också är $L_n \cap K(f)$ en enkel radikalutvidgning av $L_{n-1} \cap K(f)$ som i sin tur osv. Vi kan alltså anta att alla kropparna i sviten efter vissa strykningar är innehållna i $K(f)$.

Vi kan nu visa en kompletterande sats som liksom de två tidigare finns mer eller mindre implicit hos Abel.

Sats 3. Om $f(x) \in K[x]$ är ett irreducibelt polynom och ekvationen $f(x) = 0$ är lösbar med successiva rotutdragningar och rationella operationer, finns en svit av Galoiskroppar över K,

$$K \subset L_1 \subset \cdots \subset K(f) \tag{6}$$

där var och en är en primär radikalutvidgning av den föregående.

Bevis: Vi vet att det finns en radikalutvidgning (5) av K, där varje kropp $L_{k+1} = L_k(s_k)$ har primtalsgrad över den föregående, alla är innehållna i $K(f)$, och L_n innehåller en rot till $f(x) = 0$. Här är redan L_1 en Galoiskropp över K. Enligt Sats 2 finns en primär radikalutvidgning $L_1 \subset L_2'$ med L_2' en Galoiskropp över K innehållen i $K(f)$ som har $L_1 \subset L_2$ som första led. Om L_2' innehåller en rot til $f(x) = 0$, är $L_2' = K(f)$. I annat fall, om $s_3 \in L_2'$, så också $L_3 = L_2(s_3) \subset L_2'$ osv. Alltså, om s_k är ett första s_j utanför L_2', så är $L_2'(s_k)$ en enkel radikalutvidgning av L_2' som i sin tur är första ledet i en primär radikalutvidgning av L_2' till en Galoiskropp innehållen i $K(f)$. Efter ett ändligt antal sådana steg får vi en svit av det önskade slaget som slutar med en Galoiskropp L_j' över K som är identisk med $K(f)$. Det bevisar satsen.

Att Abel verkligen föreställt sig sviten i Sats 3 kan man sluta av Sylows kommentar i [1] II s. 333 där Abels uppställning av de i ordning adjungerade rotuttrycken återfinns nederst på sidan.

För Abel tedde sig Sats 3 i konkret form så att rötterna till $f(x) = 0$ kunde uttryckas genom superponerade rotuttryck och rationella operationer. Det betyder att om en rot fixeras, så får man de andra genom att de ingående kvadrat-, kubik- osv rötterna antar alla sina värden genom att multipliceras med potenser av motsvarande primitiva enhetsrötter. Antar man att alla enhetsrötter som ingår finns med i grundkroppen K, får man alla operationer i $\mathrm{Aut}(f/K)$ på detta sätt. Detta påstående följer omedelbart av fortsättningssatsen. Vi kan alltså sluta att antalet element i $\mathrm{Aut}(f/K)$ är produkten av de primtalspotenser som i (6) uttrycker en kropps grad över den följande. Av detta följer ett påpekande av Sylow i dennes kommentar till Abels manuskript ([1] II s. 335) som kan uttryckas som följer:

Lemma 2. Om $f(x)$ har primtalsgrad p, uppträder p bara en gång bland de successiva gradtalen i (6) och då med potensen 1.

Bevis: Eftersom gruppen $\mathrm{Aut}(f/K)$ permuterar p objekt, måste dess ordning dela $p!$.

3. Lösbara ekvationer av primtalsgrad

Innan vi går in på en analys av Abels manuskript ska vi kort bevisa en huvudsats med två följdsatser, en om Galoisgruppen och en om rötternas form. Tillsammans innehåller de det Abel visste och ville visa om lösbara ekvationer av primtalsgrad.

Huvudsatsen

Sats 4. Låt K vara en kropp och $f(x) \in K[x]$ ett irreducibelt polynom av primtalsgrad p. Om ekvationen $f(x) = 0$ är lösbar och K innehåller enhetsrötterna av grad p, finns en radikalsvit

$$K \subset L \subset L(t) = K(f)$$

där $L(t)$ har grad p över L och

(i) $K(f) = K(t)$,

(ii) $L = K(s)$, $s = t^p$, är en Galoiskropp över K,

(iii) rötterna till $f(x) = 0$ har formen

$$x_k = \sum_0^{p-1} a_j \omega^{jk} t^j \tag{7}$$

där $a_j = a_j(s)$ med $a_j(x) \in K[x]$, $a_1 = 1$ och ω är en primitiv p^{te} enhetsrot.

Bevis: Betrakta en svit enligt sats 3, och sönderlägg den i enkla radikalutvidgningar. Första gången $f(x)$ sönderfaller i faktorer kommer dessa faktorer att bilda en bana för en grupp av primtalsordning. Det betyder att antalet faktorer och den permuterande gruppens ordning båda är lika med p. Alltså sönderfaller $f(x)$ i linjära faktorer. Vi har alltså en radikalutvidgning $K \subset L \subset L(t)$ där rötterna $x_0, \ldots, x_{p-1}$ har formen (7) med koefficienter $a_j \in L$. Lemma 1 visar så att vi kan välja t så att $a_1 = 1$, och Lemma 2 visar att L är en Galoiskropp över K. Under denna förutsättning är det lätt att visa att $K(t) = K(f)$. Ty antag att $U \in \mathrm{Aut}(f/K)$ lämnar $t = (\omega, x)/p$ invariant. Då är $UL = L$ och $Ux_k = x_j$ för något j samtidigt som

$$Ux_k = b_0 + \omega^k t + \cdots + b_{p-1}\omega^{k(p-1)} t^{p-1}$$

där $b_0, \ldots, b_{p-1} \in L$. En jämförelse av koefficienterna för t i x_j visar då att $\omega^k = \omega^j$ varav $j = k$ så att U är identiteten. Enligt Galoisteorins grunder betyder det att alla element i $K(f)$ ligger i $K(t)$. Eftersom L består av alla element i $K(t)$ som är invarianta under $T : t \to \omega t$, följer nu att $L = K(t^p) = K(s)$, och med detta har vi visat (i), (ii) och (iii).

Anmärkning: Som tidigare kan vi införa Lagranges resolventer

$$(\omega^k, x) = \sum_0^{p-1} \omega^{-kj} x_j,$$

och vi får som tidigare $a_j t^j = (\omega^j, x)/p$. Alltså är de icke försvinnande resolventerna linjärt oberoende över $K(s)$. Enligt (7) är

$$px_k = \sum_0^{p-1} \omega^{jk} (\omega^j, x).$$

Observera också att (7) visar att $Tx_i = x_{i+1}$, så att $T(\omega^j, x) = \omega^j(\omega^j, x)$ där index räknas mod p.

Galoisgruppen

Med vissa luckor finns första delen av den sats som nu följer bevisad hos Abel och Malmsten. Den andra delen finns ofullständig hos Malmsten. Avsnittets rubrik motiveras av den anmärkning som följer efter satsens bevis.

Följdsats 1. Till varje $U \in \mathrm{Aut}(f/K)$ finns ett $k \not\equiv 0 \bmod p$ och ett $a(s) \in K(s)$ så att

$$Ut = a(s)t^k \tag{8}$$

och så att

$$U(\omega^j, x) = \omega^{ljk}(\omega^{jk}, x) \tag{9}$$

om $Ux_0 = x_l$ och vänstra sidan inte är noll.

Anmärkning: Eftersom $K(s) = K(t^p)$ är gruppen $\mathrm{Aut}(K(s)/K)$ isomorf med $\mathrm{Aut}(f/K)$ mod T, dvs enligt (9) med den undergrupp G av $\mathrm{Aut}(f/K)$ vars element V lämnar x_0 invariant, $Vx_0 = x_0$. Enligt (9) med $l = 0$ permuterar gruppens element V de icke försvinnande resolventerna cykliskt. Alltså är G isomorf med en undergrupp av den multiplikativa gruppen $Z_p \setminus 0$, dvs den är cyklisk och alstras av ett element U av ordning r som delar $p-1$. Vi skriver

$$U(\omega^j, x) = (\omega^{jg}, x) \tag{9'}$$

där $U^g = 1$, dvs $g^r \equiv 1 \bmod p$.

Bevis: Låt som tidigare $Tt = \omega t$. Elementen TUt och Ut har samma p^{te} potens, nämligen $(TUt)^p = TUt^p = TUs = Us$, ty $UK(s) = K(s)$ eftersom $K(s)$ är en Galoiskropp. De löser alltså båda en ekvation $x^p - c = 0$ där $c \in K(s)$. Det följer att $TUt = \omega^k Ut$ för något k. Eftersom också $Ut = c_0 + c_1 t + \cdots + c_{p-1}t^{p-1}$ med koefficienter i $K(s)$, så följer att $Ut = c_k t^k$ varav (8).

Låt oss nu betrakta resolventerna

$$(\omega^j, x) = \sum_0^{p-1} \omega^{-ji} x_i = p a_j(s) t^j, \tag{10}$$

den sista likheten enligt (7). Eftersom U permuterar rötterna och resolventerna är linjärkombinationer av dem, inducerar U en linjär transformation

$$U(\omega^j, x) = \sum c_{ji}(\omega^i, x)$$

av resolventerna där $c_{ij} \in K$. Men enligt (10) är (ω^j, x) ett egenelement till T med egenvärdet ω^j, och enligt (8) är $U(\omega^j, x)$ ett egenelement till T med egenvärdet ω^{kj}. Det följer då av den sista ekvationen att

$$U(\omega^j, x) = d_j(\omega^{kj}, x) \tag{11}$$

där $d_j \neq 0$ då $(\omega^j, x) \neq 0$. Nu är

$$px_0 = \sum_0^{p-1}(\omega^j, x), \qquad px_i = \sum_0^{p-1} \omega^{ij}(\omega^j, x)$$

varav enligt (11)

$$\sum d_j(\omega^{jk}, x) = \sum \omega^{lj}(\omega^j, x).$$

Alltså är $d_j = \omega^{ljk}$ så att (9) följer.

Anmärkning: Av (9) följer efter någon räkning hur $\mathrm{Aut}(f/K)$ opererar på rötterna, men det är enklast att utgå från (8). Man får $T^{1/k}Ut = \omega a(s)t^k = UTt$ varav samma likhet applicerad på $K(t) = K(f)$. Med $kk' \equiv 1 \bmod p$ får vi alltså

$$UTU^{-1} = T^{k'},$$

och genom iterationer $UT^jU^{-1} = T^{jk'}$ varav

$$Ux_j = UT^jx_0 = T^{k'j}Ux_0 = x_{k'j+l}$$

om $Ux_0 = x_l$ och indices räknas mod p.

Om Γ är gruppen av affina bijektioner $j \to ij + l$ av Z_p, och vi noterar att $\mathrm{Aut}(f/K)$ innehåller $T : x_k \to x_{k+1}$, ser vi alltså att

$\mathrm{Aut}(f/K)$ *är isomorf med en undergrupp av* Γ *som innehåller translationen* $k \to k + 1$.

Följdsatsen 1 är ett specialfall av en sats av Galois ([7]) som säger detsamma om $\mathrm{Aut}(f/K)$ då $f(x) \in K[x]$ är irreducibel av primtalsgrad p och det finns en svit av kroppar

$$K \subset K_1 \subset \cdots \subset K_{n+1} = K(f)$$

sådan att var och en är normal över den föregående, $\mathrm{Aut}(K_{j+1}/K_j)$ är cyklisk för alla j, och $f(x)$ är irreducibel i K_n. Man säger att ekvationen $f(x) = 0$ är metacyklisk. Galois' bevis är enkelt och utnyttjar att endast translationerna i Γ har perioden p. Som ovan ser man att $\mathrm{Aut}(K(f)/K_n)$ alstras av ett T som är cyklisk av ordning p. Om vi antar att $\mathrm{Aut}(K(f)/K_{j+1})$ har den önskade egenskapen att innehålla translationerna och vara isomorf med en undergrupp av Γ, och antar att $U \in \mathrm{Aut}(K(f)/K_j)$, är $V = UTU^{-1}$ identiteten på K_{j+1} och har perioden p. Alltså är V en potens av T, och man kan resonera som tidigare och visa att $\mathrm{Aut}(K(f)/K_j)$ också har den önskade egenskapen.

Rötternas form

Den andra följdsatsen uttrycker i modern terminologi det resultat som var Abels huvudmål. Genom att applicera $\mathrm{Aut}(f/K)$ på formeln

$$px_0 = (\omega^0, x) + (\omega, x) + \cdots + (\omega^{p-1}, x) \tag{12}$$

får man alla rötter x_k uttryckta som summor av p^{te} rötter ur element i $K(s)$. Dessa rötter kan emellertid inte väljas oberoende av varandra. Vi ska se nedan att de är rationella funktioner av en av dem.

Enligt anmärkningen efter Följdsats 1 permuteras termerna i (12) cykliskt av en undergrupp G i $\mathrm{Aut}(f/K)$ som alstras av ett element U med ordning r givet av (9′) där r delar $p-1$ och $g^r \equiv 1 \bmod p$. Låt $(\omega^i, x) = pa_i t^i \neq 0$ och betrakta motsvarande bana under U,

$$B_i = \bigcup_0^{r-1} (\omega^{ig^k}, x).$$

Alla ig^k är här skilda mod p eftersom r är det minsta tal $k > 0$ för vilket $g^k \equiv 1 \bmod p$. Alltså har varje bana r element. Välj $I \subset (1, \ldots, p-1)$ så att

$$\bigcup_{i \in I} \bigcup_0^{r_i - 1} B_i \tag{13}$$

är en uppdelning av alla icke försvinnande resolventer utom (ω^0, x) i banor under U.

Vi kan nu återge det slutresultat som Abel eftersträvade.

Följdsats 2. Det finns ett element $U \in \mathrm{Aut}(f/K)$ sådant att

$$Ut = a(s)t^g, \qquad Us = a(s)^p s^g \tag{14}$$

och att rötterna till $f(x) = 0$ ges av

$$px_0 = a_0 + \sum_{i \in I} \sum_0^{r-1} c_{ik} (\sqrt[p]{s})^{ig^k} \tag{15}$$

med $c_{ik} \in K(s)$ då $\sqrt[p]{s}$ antar sina p värden.

Anmärkning: Observera att vi har valt t så att $(\omega, x) = pt$. Satsen finns explicit i Abels manuskript. Formel (15) ovan återfinns hos Abel i en uppställning överst på s. 240 där varje rad är en bana under G medan möjligheten att en bana är noll inte nämns explicit.

Bevis: Vi har

$$(\omega^i, x) = pa_i(s)t^i$$

och upprepningar av (14) visar att elementen i banan B_i har formen

$$c_{ik}(s)t^{ig^k}$$

varav (15). Då $t \to \omega^j t$ får man px_j på vänster sida av (15). Det visar satsen.

Anmärkning: Vi kan också räkna ut koefficienterna $c_{ik}(s)$ i (15) mera systematiskt, men för enkelhetens skull bara för den första banan

$$t, \quad Ut, \quad \dots, \quad U^{r-1}t.$$

Vi anmärker till att börja med att vi kan ersätta (14) med

$$Ut = a(s)s^{-k}t^{g+kp}$$

där k är ett heltal. Om $g^r \equiv 1 + jp \bmod p^2$ kan vi alltså genom att byta g mot $g + kp$ med ett lämpligt k anta att $j = -1$ så att

$$g^r = 1 - p + qp^2$$

för något heltal q. Enligt (14) får vi sviten

$$\begin{aligned} t, \quad Ut = a(s)t^g, \quad U^2t = a(Us)a(s)^g t^{g^2}, \\ \dots, \quad U^{r-1}t = a(U^{r-2}s)\dots a(s)^{g^{r-2}} t^{g^{r-1}}. \end{aligned} \tag{16}$$

Med ett steg till får man $t = B(s)t^{g^r}$ där

$$B(s) = a(U^{r-1}s)a(U^{r-2}s)^g \dots a(s)^{g^{r-1}}. \tag{17}$$

Det följer att $t^{1-g^r} = t^{p-qp^2} = B$ så att

$$t = A(s)\sqrt[p]{B}, \qquad A(s) = s^q \tag{18}$$

varav

$$t + Ut + \cdots + U^{r-1}t = \sum_0^{r-1} A(U^i s)\sqrt[p]{B(U^i s)}, \tag{19}$$

vilket är helt analogt med den formel för rötterna till en lösbar ekvation av grad 5 som Abel gav i sitt brev [6] till Crelle. Man observerar att U opererar på B genom att exponenterna förskjuts cykliskt, och att det följer av (17) att

$$\sqrt[p]{B(Us)} = C(s)\sqrt[p]{B^g}, \qquad C(s) = a(s)^{1-qp}$$

helt analogt med $Ut = a(s)t^g$. Motsvarande formler finns för alla banor i (15) genom att man ersätter $t = s^{1/p}$ med (18).

4. Abels manuskript

Redan i början av den del av manuskriptet som handlar om lösbara ekvationer av primtalsgrad, $f(x) = 0$, $f(x) \in K[x]$, $\operatorname{grad} f(x) = p$, skriver Abel upp rötterna enligt (7) som

$$x_k = \sum_0^{p-1} a_j(\omega^k t)^j, \qquad k = 0, \ldots, p-1,$$

där koefficienterna ligger i en kropp $L \supset K$ och t är rot till ett irreducibelt polynom $x^p - s \in L[x]$. Sedan undersöker han konjugerade $t' = Ut$, $s' = Us$ till t, s. A priori är s' ett polynom i t med koefficienter i L, och Abel vill att bara den konstanta koefficienten kan vara skild från noll, dvs att L är en Galoiskropp. Men hans otåliga argumentering håller inte. Om han hade tänkt på sin uppställning av hur radikalutvidgningen gått till (vår Sats 3), hade beviset som hos Sylow och oss varit lätt. Med antagandet att L är en Galoiskropp, visar sedan Abel fullt korrekt att

$$t' = at^k, \qquad a \in L, \qquad k \not\equiv 0 \bmod p. \tag{20}$$

Här använder han implicit ett $T \in \operatorname{Aut}(K(f)/L)$ definierat av $t \to \omega t$, dvs $Tx_k = x_{k+1}$. Hans bevis finns i förkortad upplaga i beviset av Följdsats 1.

Abels nästa steg är att visa att $L = K(s)$ varav $K(f) = K(t)$ i vår beteckning. Beviset är inte invändningsfritt, men Abel kan nu anta att elementet a i (20) har formen $a(s), a(x) \in K[x]$.

Abel säger sedan att $\operatorname{Aut}(K(s)/K)$ borde alstras av (20) upphöjt till p, dvs

$$s \to s' = a(s)^p s^k. \tag{21}$$

Han skriver upp iterationerna och drar slutsatsen att operationens ordning delar $p-1$, eftersom $k^r \equiv 1 \bmod p$ medför att r delar $p-1$. Han betraktar så en annan bijektion (20) och drar därefter outsagt den i sammanhanget omotiverade slutsatsen att $\operatorname{Aut}(K(s)/K)$ är cyklisk av en ordning r som delar $p-1$ och skriver upp alla konjugerade till s som

$$s, \quad \theta s, \quad \theta^2 s, \quad \ldots, \quad \theta^{r-1} s, \quad \theta^r s = s.$$

Vi kan inte dra denna slutsats utan att som i Följdsats 1 också utnyttja att varje $U \in \operatorname{Aut}(f/K)$ permuterar rötterna och alltså inducerar en linjär transformation av resolventerna. Men just detta måste han ha underförstått, ty omedelbart efteråt, på s. 240, följer en framställning av x_0 som en summa som frånsett beteckningarna är densamma som vår formel (15) i Följdsats 2. I de följande raderna itereras den cykliska permutation som U inducerar på högra sidan. Nederst på den föregående sidan 239 skriver Abel i våra beteckningar upp de första termerna i vår formel (16), och nederst på s. 240 står alla termerna i summan i vår formel (19) med B enligt (17). Det betyder att Abel trots sina ofullständiga bevis hade det slutliga resultatet i Följdsats 2.

De tre följande sidorna som avslutar manuskriptet verkar ha att göra med en utvidgning av de vunna resultaten till lösbara ekvationer av grad p^m, resultat som i allmän formulering finns utlovade i början av arbetet.

5. Malmsten, Kronecker, Weber

Malmstens arbete [9] följer den allmänna delen av Abel [5] ganska noga med vissa preciseringar. När det kommer till lösbara ekvationer av primtalsgrad accepterar Malmsten att koefficienterna i

$$x_0 = a_0 + a_1 t + \cdots + a_{p-1} t^{p-1}$$

är polynom i $s = t^p$ men tillför också något nytt, nämligen att $\mathrm{Aut}(f/K)$ transformerar resolventerna linjärt, vilket inte finns explicit hos Abel. Av detta drar han den ofullständiga slutsatsen att $\mathrm{Aut}(f/K)$ permuterar de p^{te} potenserna av icke försvinnande resolventerna $(\omega, x), \ldots, (\omega^{p-1}, x)$ (men han vet inte att de permuteras cykliskt). Det följer av detta att deras produkt ligger i grundkroppen. Malmsten applicerar detta resultat på en allmän ekvation av grad p där rötterna $x_0, \ldots, x_{p-1}$ kan betraktas som obestämda. I så fall visar han att invariansen under en enda transposition är möjlig bara då $p \leq 3$. Malmsten ser här ett allmänt och begripligt resonemang som visar att allmänna ekvationer av primtalsgrad > 3 inte kan lösas med rotutdragningar och rationella operationer.

I inledningen till sin första artikel [8a] citerar Kronecker Malmsten och tillkännager – utan bevis – sin upptäckt att $\mathrm{Aut}(f/K)$ permuterar resolventernas p^{te} potenser cykliskt. Han tycks då bara ha tänkt på fallet då resolventernas p^{te} potenser bildar en enda bana för $\mathrm{Aut}\, K(s)/K)$. Man kan anta att han fullföljt Malmsten på denna punkt utan att se att man måste bevisa att den näst sista kroppen L är en Galoiskropp. Som vi har sett finns det fullständiga resultatet uttalat hos Abel, men Kronecker citerar i sin inledning bara två formler i [5] där detta inte framgår. Det kan förklaras av att han föredragit Malmstens klara och rediga framställning framför Abels manuskript. Kronecker uttalar vår Följdsats 2 om rötternas form inklusive (18) och (19), nu med en hänvisning till Abels arbete [4] om Abelska ekvationer. Artikeln slutar med en sats som utförd närmare i [8b] som säger att rötterna till en lösbar ekvation med hela koefficienter och kommutativ Galoisgrupp är polynom i enhetsrötter med rationella koefficienter. Kronecker har också funnit att en lösbar irreducibel ekvation av udda primtalsgrad p med reella koefficienter har antingen en eller p reella rötter. Beviset är mycket enkelt: konjugering av rötterna är en operation i $\mathrm{Aut}(f/K)$ där K är en reell kropp, och en sådan kan inte fixera två rötter utan att vara identiteten.

Hela teorin för lösbara ekvationer av primtalsgrad togs upp i Webers lärobok [12]. Nyheten där är att Galois' sats används som genväg till Galoisgruppens aktion på resolventerna. Därmed försvinner problemet att visa att den näst sista kroppen L är en Galoiskropp ur litteraturen.

Bibliografi

[1] N.H. Abel. *Œuvres complètes I, II.* Publiés par L. Sylow et S. Lie. Christiania (1881).

[2] N.H. Abel. *Mémoire sur les équations algébriques où l'on démontre l'impossibilité de la résolution de l'équation générale du cinqième degré.* Œuvres complètes, vol. I, 28–33.

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

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

[5] N.H. Abel. *Sur la résolution algébrique des équations.* Œuvres complètes, vol. II, 217–243.

[6] N.H. Abel. *Brev till Crelle.* Œuvres complètes, vol. II, 266.

[7] É. Galois. *Mémoire sur les conditions de résolubilité des équations par radicaux.* Œuvres mathématiques d'Évariste Galois. Préface par J. Liouville. Journal de mathématiques pures et appliqués, (1), **11** (1846), 381–384.

[8] L. Kronecker. *Über die algebraisch auflösbaren Gleichungen.* Monatshefte Berl. Akademie (1853, 1856).

[9] Johan Malmsten. *In solutionem aequationum algebraicarum disquisitio.* Crelle **34** (1847), 30–45.

[10] C. Skau. *Gjensyn med Abels og Ruffinis bevis for umuligheten av å løse den generelle n'tegradsligningen algebraisk når* $n \geq 5$. Normat **38**, 2 (1990), 53–84.

[11] B.L. v.d. Waerden. *Moderne Algebra I.* Grundlehren, Bd. XXXIII, J. Springer, Berlin (1937).

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