En fjerdegradsligning og dens Galois-gruppe

Kent Holing

Statoil Forskningssenter
Arkitekt Ebbels veg 10
NO–7005 Trondheim
kho@statoil.com

Innledning

Vi skal for hele tall a og c bestemme Galois-gruppen G til fjerdegradsligningen

$$Q(x) = x^4 - 2cx^3 + (c^2 - 2a^2)x^2 + 2a^2cx - a^2c^2 = 0.$$

I alle tilfeller viser vi at dette kan gjøres ved bruk av enkle kriterier uttrykt ved a og c. Vi diskuterer også Galois-gruppen til en generalisering av ligningen.

For å bestemme Galois-gruppen (opp til isomorfi) til ligningen bruker vi algoritmene gitt i HOLING [1] og [2]. I tillegg trenger vi standard teori for fjerdegradsligningen (finnes i [1] og [2] og dets referanser) og en del resultater fra tallteori, som vi refererer til underveis. Galois-teori utover [1] og [2] er ikke nødvendig.[1]

Ligningen $Q(x) = 0$ er tidligere inngående studert i forbindelse med det såkalte *kvadratiske kasseproblemet*. Flere artikler i Normat de siste årene omhandler slike type problemer (problemene tilhører klassen av såkalte stigeproblemer) – se HOLING [3] med referanser. Se også [4] og [5], som er nyere enn [3].

La, som i [1], m og n være henholdsvis antall heltallsrøtter og klassisk konstruerbare røtter til ligningen $Q(x) = 0$, der røttene telles med multiplisitet og komplekse røtter inkluderes. Vi vet fra [1] at n er enkel å beregne ved hjelp av m og antallet heltallsrøtter til ligningen (fjerdegradsligningens kubiske resolvent)

$$R(t) = (t + 2a^2)(t^2 - c^2t + 2a^2c^2) = 0.$$

[1] For artikkelen er det tilstrekkelig med rene kokebokoppskrifter (algoritmer) på hvordan vi beregner Galois-gruppen til fjerdegradsligningen, og det finner vi i [1] og [2]. Hvis en ønsker en rask og konsis forklaring på hvordan Galois-teorien og fjerdegradsligningen er knyttet sammen, kan `http://planetmath.org/?op=getobj&from=objects&id=2825` være nyttig (forutsetter generell kjennskap til Galois-teori).

Vi definerer videre

$$
\begin{aligned}
C &= a^2 + c^2, \quad & E &= 2(D + c\sqrt{D} + 12a^2), \\
D &= c^2 - 8a^2, \quad & F &= 2(D - c\sqrt{D} + 12a^2).
\end{aligned} \tag{1}
$$

Vi skal se at størrelsene E og F brukes bare i de tilfeller D er et kvadrattall, slik at E og F begge er heltall.

Vi behandler de irredusible og redusible tilfellene av $Q(x)$ hver for seg. I [1] er det gitt en komplett algoritme til å bestemme Galois-gruppen for en monisk fjerdegradsligning med heltallskoeffisienter som er irredusibel over $\mathbb{Z}$, mens det i [2] er en tilsvarende algoritme for det redusible tilfellet for samme type fjerdegradsligning. Vi vil, som i [1] og [2], bruke standard gruppenotasjon for Galois-gruppene. Gruppene V og D_4 forekommer. Vi minner om at $V = \mathbb{Z}_2 \times \mathbb{Z}_2$ og D_4 er den dihedrale gruppen av orden 8 (symmetrigruppen til kvadratet).

Vi kan uten tap av generalitet anta at $a > 0$ og $c > 0$ når det gjelder bestemmelse av Galois-gruppen G til ligningen $Q(x) = 0$, da G ikke forandrer seg når a og c skifter fortegn og tilfellet $ac = 0$ er enkelt. (Vis selv at hvis $ac = 0$ så er $G = \{e\}$ hvis $a = 0$; ellers er $G = \mathbb{Z}_2$.)

Det er velkjent at diskriminanten til ligningen $Q(x) = 0$ spiller en viktig rolle når vi skal bestemme Galois-gruppen. Diskriminanten er lik $16a^4c^2C^2D$, så diskriminanten er et kvadrattall hvis og bare hvis D er et kvadrattall.

Til slutt, med et Pytagoreisk trippel (r, s, t) mener vi hele tall $r > 0$, $s > 0$ og $t > 0$ slik at $r^2 + s^2 = t^2$. Et slikt trippel (r, s, t) kalles primitivt hvis $\gcd(r, s, t) = 1$.

Fjerdegradsligningens Galois-gruppe

Setning 1 *Med a, c, m, C, D, E og F gitt som ovenfor og $ac \neq 0$ kan Galois-gruppen G til ligningen $Q(x) = 0$ bestemmes som følger:*

1. *Hvis C er et kvadrattall er $G = V$ om $m = 0$, og $G = \mathbb{Z}_2$ om $m \neq 0$.*
2. *Hvis C ikke er et kvadrattall gjelder:*
   - A. *$G = \mathbb{Z}_2$ om D og enten E eller F er kvadrattall,*
   - B. *$G = V$ om D, men verken E eller F, er kvadrattall, og*
   - C. *$G = D_4$ om D ikke er et kvadrattall.*

Vi viser setning 1 ved hjelp av hjelpesetningen nedenfor, som vises etter setningen.

Lemma 2 *Følgende gjelder:*

a) *$n = 4$.*
b) *Hvis C er et kvadrattall er $Q(x)$ redusibel.*
c) *Hvis C er et kvadrattall kan ikke D være et kvadrattall.*
d) *Bare når C er et kvadrattall kan $m > 0$, og da må $m = 2$.*
e) *Hvis C ikke er et kvadrattall så er $Q(x)$ redusibel hvis og bare hvis D er et kvadrattall og E eller F er et kvadrattall.*
f) *CD kan aldri være et kvadrattall.*

Bevis for setning 1: Av tilfellene i setningen er 1 og 2A redusible tilfeller mens 2B og 2C er irredusible tilfeller.

Vi viser 1: Anta at C er et kvadrattall. Da vet vi av lemma 2 b) at $Q(x) = 0$ er redusibel. Redusible fjerdegradsligninger uten heltallsrøtter (dvs. $m = 0$) har ifølge [2] Galois-gruppe G lik $\mathbb{Z}_2$ hvis diskriminanten er et kvadrattall; ellers er $G = V$. Vi ser av lemma 2 c) at diskriminanten ikke er et kvadrattall, så tilfellet med $m = 0$ er vist. Eneste gjenstående mulighet er da $m = 2$ ifølge lemma 2 d), men da er det trivielt at $G = \mathbb{Z}_2$.

Vi viser 2: Vi starter med det redusible tilfellet i del 2 av setningen, som vi skal se er tilfellet 2A. Anta altså at C ikke er et kvadrattall og $Q(x)$ er redusibel. Da må ifølge lemma 2 e) D være et kvadrattall og E eller F være et kvadrattall. Siden $m = 0$ ved lemma 2 d) må $G = \mathbb{Z}_2$ som ovenfor, og vi har vist tilfellet 2A.

Anta videre at $Q(x)$ er irredusibel. Siden $n = 4$ ved lemma 2 a), vet vi fra [1] at G må være enten V, $\mathbb{Z}_4$ eller D_4. Videre er $G = V$ hvis diskriminanten er et kvadrattall; ellers er G enten $\mathbb{Z}_4$ eller D_4. Anta nå at C ikke er et kvadrattall. Er D et kvadrattall så har vi altså at $G = V$, og vi har vist tilfellet 2B. Hvis D ikke er et kvadrattall må vi skille mellom gruppene $\mathbb{Z}_4$ og D_4. Om vi kan utelukke $\mathbb{Z}_4$ har vi også vist tilfellet 2C.

Vi må altså vise at Galois-gruppen ikke kan være $\mathbb{Z}_4$. Anta at verken C eller D er et kvadrattall. I [1] behandles $\mathbb{Z}_4/D_4$-tilfellet ved å innføre en hjelpeligning $P(x) = 0$. Denne ligningen blir i vårt tilfelle $P(x) = (x-c)^2(x^2+2a^2x-a^2c^2) = 0$. Vi har da at $G = \mathbb{Z}_4$ bare hvis røttene til $P(x) = 0$ alle ligger i rotkroppen til den kubiske resolventen $R(t) = 0$ til ligningen $Q(x) = 0$. Vi ser av uttrykkene for $Q(x)$ og $R(t)$ at rotkroppene til $P(x) = 0$ og $R(t) = 0$ er henholdsvis lik $\mathbb{Q}[\sqrt{C}]$ og $\mathbb{Q}[\sqrt{D}]$. Dette viser at $G = \mathbb{Z}_4$ bare kan inntre hvis CD er et kvadrattall (dette siste følger av [2] eller oppgave 2, noe som ikke kan skje ifølge lemma 2 f).

Setningen er dermed bevist, men se oppgave 2. □

Bevis for lemma 2: Del a og b: Det kan vises at for $k = \sqrt{C} > 0$ kan $Q(x)$ alltid faktoriseres som

$$Q(x) = p(x)q(x) = \big(x^2 - cx - a(a+k)\big)\big(x^2 - cx - a(a-k)\big). \tag{2}$$

Faktoriseringen kan bestemmes ved enten å observere direkte at $Q(x) = 0$ er ekvivalent med $(x^2 - cx - a^2)^2 = a^2k^2$ eller ved å bruke at den kubiske resolventen $R(t) = 0$ til $Q(x) = 0$ alltid har heltallsroten $-2a^2$.

Vi ser at (2) gir $n = 4$ og $Q(x) = 0$ er redusibel når k er heltallig (C er et kvadrattall). At $n = 4$ følger også av at resolventen $R(t) = 0$ har en heltallsrot, se [1].

Bevis for del c: Vi lar $k^2 = a^2 + c^2$ med $k > 0$ heltallig. Vi kan anta at (a, c, k) er et primitivt Pytagoreisk trippel. Hvis $D = k^2 - 9a^2$ er et kvadrattall må a være jamn og $\gcd(k - 3a, k + 3a) = 1$ (vises nedenfor). Siden a er jamn er $k - a$ og $k + a$ begge kvadrattall, og siden $k - 3a$ og $k + 3a$ er relativt primiske, er de også begge kvadrattall (produktet er jo et kvadrattall). Men da vil de 4 forskjellige kvadrattallene $k - 3a$, $k - a$, $k + a$ og $k + 3a$ være påfølgende tall i en aritmetisk rekke, noe som ikke kan være tilfelle etter et kjent teorem av Fermat, se Sierpinski [7]. (Se også [8].)

Til slutt, hvorfor er a jamn og $\gcd(k - 3a, k + 3a) = 1$ hvis D er et kvadrattall? At a er jamn kan vises ved kongruensregning modulo 16. At $\gcd(k-3a, k+3a) = 1$

følger av at $k+3a$ og $k-3a$ er odde, og ikke multipler av 3 (k er jo odde og ikke delelig med 3): En vilkårlig felles primtallsfaktor p av $k-3a$ og $k+3a$ vil da måtte gå opp i $2k$ og $6a$, og derfor gå opp i både k og a (da $p>3$) – noe som er umulig da k og a er relativt primiske.

Bevis for del d: Først ser vi av faktoriseringen (2) at hvis $m>0$ så er $m=2$ eller $m=4$ og k heltallig (C er et kvadrattall). Vi viser videre at vi heller ikke kan ha $m=4$, så $m=2$.[2] Er $m=4$ gir (2) at C er et kvadrattall. I tillegg er da også diskriminanten til $Q(x)=0$ et kvadrattall, så D er et kvadrattall. Men, det er som vi vet, ikke mulig at C og D samtidig er kvadrattall; så $m\neq 4$.[3]

Bevis for del e): At $Q(x)$ kan være redusibel selv om C ikke er et kvadrattall følger av at $Q(x)=(x^2-32x+204)(x^2-2x-51)$ når $a=6$ og $c=17$.

Med $Q(x)=p(x)q(x)$ fra (2), la røttene til ligningene $p(x)=0$ og $q(x)=0$ være henholdsvis x_1, x_2 og x_3, x_4. Da er $x_{1,2}=\frac{1}{2}(c\pm d_1)$ og $x_{3,4}=\frac{1}{2}(c\pm d_2)$, hvor $d_1=\sqrt{(k+3a)(k+a)}$ og $d_2=\sqrt{(k-3a)(k-a)}$.Vi kan også vise at $d_1+d_2=\sqrt{E}$ og $d_1-d_2=\sqrt{F}$ der E og F er gitt av (1) (om nødvendig, se Chrystal [9]).

Anta at C ikke er et kvadrattall og $Q(x)$ er redusibel. Siden $Q(x)=0$ ikke har heltallsrøtter ($m=0$ ifølge lemma 2 d) må $Q(x)$ kunne skrives som et produkt av to irredusible andregradsfaktorer med heltallskoeffisienter. Disse faktorene kan ikke være $p(x)$ og $q(x)$ da C ikke er et kvadrattall. Da må en av disse faktorene være $(x-x_1)(x-x_3)$ eller $(x-x_1)(x-x_4)$. Så enten må (i) x_1+x_3 og x_1x_3 begge være heltall, eller (ii) så må både x_1+x_4 og x_1x_4 være det.

Anta (i). Da er d_1+d_2 et heltall, så E er et kvadrattall. Også d_1d_2 er heltall. Siden $d_1d_2=c\sqrt{D}$ må D være et kvadrattall. Tilsvarende vil (ii) gi at D og F er kvadrattall.

Anta omvendt, når C ikke er et kvadrattall, at D og E er kvadrattall. Da er d_1d_2 og d_1+d_2 heltall. Dette gir at x_1+x_3 og x_1x_3 er rasjonale tall, som viser at $Q(x)$ er redusibel over $\mathbb{Q}$. Gauss' lemma[4] gir da at $Q(x)$ er redusibel over $\mathbb{Z}$, som skulle vises (det viser seg at også (i) må gjelde). Tilsvarende vises at $Q(x)$ er redusibel hvis D og F er kvadrattall ((ii) må også gjelde).

Til slutt, E og F kan ikke begge være kvadrattall (i så fall ville vi ha at $m=4$).

Bevis for del f: Vi kan anta at $\gcd(a,c)=1$. (Hvorfor?) Anta at CD er et kvadrattall. Ifølge lemma 2 c) kan da verken C eller D være kvadrattall, så C og D må ha en felles faktor $d>1$. En primtalldivisor av d må være lik 3, som gir at $C=3R^2$ og $D=3S^2$ for R og S heltall. Men $C=3R^2$ gir at både a og c må begge være jamne (bruk kongruensregning modulo 4), som er umulig. □

[2] Vi har tilfeller med $m=2$. Vi kan vise at for $a=rs$ og $c=(r+s)t$, der (r,s,t) er et Pytagoreisk trippel, er $m=2$. To av røttene til $Q(x)=0$ er da lik rt og st, så $m\geq 2$. Så enten er $m=2$ eller $m=4$. Nå er $Q(x)=(x^2-(r+s)tx+rst^2)q(x)$ der diskriminanten til $q(x)=x^2-(r+s)tx+rs(r+s)^2$ er lik $(r+s)^2(t^2+4rs)$. Siden t^2+4rs ikke er et kvadrattall (se [8]) ser vi at vi ikke kan ha $m=4$, så vi må ha $m=2$. Merk at vi kan også ha andre tilfeller med $m=2$ enn på denne formen, som for eksempel når $a=12$ og $c=5$.

[3] Vi kan også vise at $m=4$ ikke er mulig uten å bruke faktoriseringen (2): Det er nemlig slik at hvis $m=4$, så må (a,c) være proporsjonal med a og c gitt i fotnote 2 med (r,s,t) primitivt (se [4] og [5]), men da vet vi at $m\neq 4$.

[4] La $p(x)$ være et monisk polynom med heltallskoeffisienter. Da kan $p(x)$ skrives som et produkt av to moniske polynom av lavere grad med rasjonale koeffisienter hvis og bare hvis $p(x)$ kan skrives som et produkt av to moniske polynom av lavere grad med heltallskoeffisienter.

Vi avslutter med å utfordre leseren med to oppgaver.

Oppgave 1: La $a = 1$ og $c > 0$ være heltall.

a) Vis at fjerdegradsligningene $Q(x) = 0$ ovenfor for slike c alle har Galois-grupper, som – på ett unntak nær – er isomorfe.[5]

b) I motsetning til a), vis at hvis vi tillater c å være rasjonal, så kan alle tilfellene i setning 1 oppnås med $a = 1$.[6]

Oppgave 2: La $P(x) = 0$ være en monisk bikvadratisk ligning med heltallskoeffisienter. (En bikvadratisk ligning er en fjerdegradsligning $P(x) = 0$ som er en andregradsligning i x^2.)

Kappe & Warren [10] gir kriterier for når $P(x)$ er irredusibel og en metode for å bestemme Galois-gruppen G til ligningen $P(x) = 0$ når ligningen er irredusibel. Med $P(x) = x^4 + Ax^2 + B = 0$ er ifølge [10] $P(x)$ irredusibel hvis og bare hvis verken $A^2 - 4B$ eller $-A \pm 2\sqrt{B}$ er kvadrattall (teorem 2). Videre gir [10] at for $P(x)$ irredusibel så er $G = V$ hvis og bare hvis B er et kvadrattall, $G = \mathbb{Z}_4$ hvis og bare hvis $B(A^2 - 4B)$ er et kvadrattall; ellers er $G = D_4$ (teorem 3).

a) Vis at fjerdegradsligningen $Q(x) = 0$ kan transformeres til en monisk bikvadratisk ligning med heltallskoeffisienter.[7]

b) Bruk det ovenfor og lemma 2 til å vise 2B og 2C av setning 1.[8]

Et forsøk på generalisering

Vi skal nå se på en generalisering, og betrakter fjerdegradsligningen

$$Q(x) = x^4 - 2cx^3 + (c^2 - a^2 - b^2)x^2 + 2a^2cx - a^2c^2 = 0$$

for hele tall a, b og c. For $a = b$ har vi fjerdegradsligningen ovenfor. Merk at ligningen $Q(x) = 0$ for $a \neq b$ er relatert til det såkalte *ikkekvadratiske kasseproblemet*, se [3]–[6].

For å bestemme G (opp til isomorfi) av ligningen er det tilstrekkelig å anta $a > 0$, $b > 0$ og $c > 0$ siden fortegnsskifte på a, b og c ikke endrer G, og G er enkel å bestemme i tilfellene med $abc = 0$. Vi antar derfor videre at a, b og c er positive heltall. Vi kan uten tap av generalitet også anta at $a < b$ og $\gcd(a, b, c) = 1$.[9]

I det generelle tilfellet er det ikke lett å finne kriterier ut fra ligningens koeffisienter som bestemmer G slik det var når $a = b$, men vi har følgende:

[5] For $a = 1$ og $c > 0$ heltall er $C = c^2 + 1$ aldri kvadrattall. Vi kan også vise at $D = c^2 - 8$ er et kvadrattall hvis og bare hvis $c = 3$. For $a = 1$ og $c \neq 3$ er Galois-gruppene derfor alle isomorfe med D_4.

[6] Betegn $Q(x)$ med $Q(x; a, c)$ for rasjonale a og c. Ved å velge passende heltall $u > 0$ og $v > 0$ oppnås alle tilfeller i setning 1 for ligningen $Q(x; u, v) = 0$ (se tabell i appendiks). Siden vi har at $Q(x; u, v) = u^4 Q(x/u; 1, v/u) = 0$, kan vi velge $a = u/u = 1$ og $c = v/u$ da ligningene $Q(x; a, c) = 0$, $Q(x/u; 1, v/u) = 0$ og $Q(x; u, v) = 0$ alle har samme Galois-gruppe.

[7] Ligningen $Q(x) = 0$ kan transformeres til en monisk bikvadratisk ligning $P(x) = 0$ med heltallskoeffisienter ved å fjerne kubikkleddet til $Q(x)$ (standard metode). Det viser seg at den transformerte ligningen blir en bikvadratisk ligning da lineærleddet til $Q(x) = 0$ også fjernes. Det er lett å se at vi kan velge $P(x) = x^4 - 2(c^2 + 4a^2)x^2 + c^2(c^2 - 8a^2) = 0$.

[8] Ligningene $Q(x) = 0$ og $P(x) = 0$ har samme Galois-gruppe. Vi kan derfor bruke resultatet for $P(x) = 0$ til å bestemme Galois-gruppen til $Q(x) = 0$. Nå er $A = -2(c^2 + 4a^2)$ og $B = c^2 D$. Dette gir da at $A^2 - 4B = 8^2 a^2 C$, $-A + 2\sqrt{B} = E$, $-A - 2\sqrt{B} = F$ og $B(A^2 - 4B) = 8^2 a^2 c^2 CD$. Her ser vi hvordan C, D, E, F og CD fra setning 1 kommer inn.

[9] Med $Q(x; a, b, c) = Q(x)$ er $Q(c - x; b, a, c) = Q(x; a, b, c)$ og $Q(kx; ka, kb, kc) = k^4 Q(x; a, b, c)$.

Setning 3 *For ligningen ovenfor gjelder at hvis diskriminanten er lik* 0 *så er Galois-gruppen til ligningen* $G = \mathbb{Z}_2$.

Bevis: Det er kjent (se [4]–[6]) at hvis ligningen har en dobbelrot så er (a, b, c) proporsjonal med (r^3, s^3, t^3) der (r, s, t) er et primitivt Pytagoreisk trippel. Dobbelroten er heltallig i dette tilfellet. Det er derfor tilstrekkelig å la $a = r^3$, $b = s^3$ og $c = t^3$. Det er lett å vise at ligningen da har de to heltallsrøttene (dobbelroten) r^2t. De to andre røttene er gitt av $x^2 - 2s^2tx - r^2t^4 = 0$ med diskriminant lik $d = 4t^2(s^4 + r^2t^2)$.

Vi skal vise at d aldri kan være et kvadrattall, så $m = 2$ og $G = \mathbb{Z}_2$. Anta at d er et kvadrattall. Da er $s^4 + r^2t^2$ et kvadrattall. Men det gir at $r^4 - r^2t^2 + t^4$ også er et kvadrattall, noe som ikke er tilfelle: Det er kjent at den Diofantiske ligningen $x^4 - x^2y^2 + y^4 =$ et kvadrattall ikke har løsninger med $x \neq y$, se [7]. □

Avslutning

Vi vet at fjerdegradsligninger med heltallskoeffisienter bare kan ha følgende forskjellige (opp til isomorfi) Galois-grupper: S_4, A_4, V, $\mathbb{Z}_4$, D_4, S_3, A_3 , $\mathbb{Z}_2$ og $\{e\}$ (se [1] og [2]). Av disse opptrer de 5 første gruppene i det irredusible tilfellet mens V kan opptre også i det redusible tilfellet når ligningen ikke har heltallsrøtter og dens diskriminant ikke er et kvadrattall. Resten av gruppene opptrer bare i det redusible tilfellet hvor $\mathbb{Z}_2$ da kan opptre i to forskjellige tilfeller, enten når ligningen har to eller ingen heltallsrøtter (det siste når diskriminanten er et kvadrattall).

I tilfellet med $a = b$ har vi for $Q(x) = 0$ at $n = 4$ slik at vi trivielt kunne utelukke gruppene S_4 og A_4 (disse opptrer bare hvis $n = 0$) og S_3 og A_3 (disse opptrer bare hvis $n = 1$). Vi greide i tillegg å vise at gruppene $\mathbb{Z}_4$ og $\{e\}$ ikke kunne forekomme.

I det generelle tilfellet for $Q(x) = 0$ med $a \neq b$ og $abc \neq 0$ er det enkelt å finne eksempler på S_4, D_4, S_3 og V. Med litt mer arbeid finner vi også eksempler på A_4, A_3, $\mathbb{Z}_2$ (både med $m = 0$ og $m = 2$) og $\{e\}$ (se nedenfor). Vi har imidlertid ikke greid å avgjøre om gruppen $\mathbb{Z}_4$ kan forekomme.

I appendikset nedenfor er det gitt to tabeller over de forskjellige gruppetilfellene. Det er ifølge det ovenfor da ett hull i tabellen for $a \neq b$. Leseren utfordres til å finne eksempler på dette tilfellet (tilfelle med $\mathbb{Z}_4$) som mangler, eller å vise at dette tilfellet ikke kan forekomme.

For å finne eksempler med $m \geq 1$ bruker vi et resultat fra [5] som sier at hvis a, b og c er på formen

$$a = \alpha r, \quad b = (\beta - \alpha)s \quad \text{og } c = \beta t \tag{3}$$

for (r, s, t) et primitivt Pytagoreisk trippel, og α og β heltall med $\beta > \alpha \geq 1$, så har ligningen $Q(x) = 0$ heltallsroten αt.

Et tilfelle med $G = A_3$ krever at $m = 1$ og at diskriminanten er et kvadrattall (se eksempler nedenfor).

Tilfeller med $m \geq 2$ ($m = 2$ eller $m = 4$) kan genereres som følger: La (r, s, t) og (u, v, t) være to Pytagoreiske tripler med $r > u$. Med

$$a = r(v - s)u, \quad b = s(r - u)v \quad \text{og } c = (rv - us)t \tag{4}$$

vil ligningen $Q(x) = 0$ ha minst to heltallsrøtter, nemlig $r(v-s)t$ og $u(v-s)t$. De to andre røttene er røtter til $x^2 - (r-u)(s+v)tx - ru(rv-us)^2 = 0$. Vi har fire heltallsrøtter hvis og bare hvis $f = (r-u)^2(s+v)^2t^2 + 4ru(rv-us)^2$ er et kvadrattall. (f kan være et kvadrattall da f er kongruent 0 eller 1 modulo 4.) Vi vet ikke om både (r,s,t) og (u,v,t) kan velges primitive når $m = 4$.

Vi avslutter med enda en oppgave som utfordring til leseren.

Oppgave 3: La $a > 0$, $b > 0$ og $c > 0$ heltall, $a < b$ og $\gcd(a,b,c) = 1$. Anta at ligningen $Q(x) = 0$ har en triviell Galois-gruppe. Vis at det er 46 slike tilfeller med $a \leq 500\,000$. (*Hint*: Se BEILER [11].) I tabell 2 nedenfor er fem av disse tilfellene gitt.

Jeg vil rette en takk til Dave Rusin, James Buddenhagen og Allan MacLeod, som har bidratt med eksempler på A_4, A_3 , $\mathbb{Z}_2$ (med $m = 0$) og $\{e\}$.[10] Eksemplene på A_4 er generert ved hjelp av teori for elliptiske ligninger.

Appendiks

Eksempler på Galois-grupper $G = G[a,c]$ for $a = b$

Irredusible tilfeller	$G[a,c]$	Kommentar
V	$G[1,3]$	Tilfelle 2B (se oppgave 1)
D_4	$G[1,10]$	Tilfelle 2C (se oppgave 1)
Redusible tilfeller	$G[a,c]$	Kommentar
V	$G[5,12]$	Tilfelle 1 (m = 0)
$\mathbb{Z}_2$	$G[12,35]$	Tilfelle 1 (m = 2), på form som i fotnote 2
$\mathbb{Z}_2$	$G[6,17]$	Tilfelle 2A (E et kvadrattall)
$\mathbb{Z}_2$	$G[30,97]$	Tilfelle 2A (F et kvadrattall)

Eksempler på Galois-grupper $G = G[a,b,c]$ for $a \neq b$

Irredusible tilfeller	$G[a,b,c]$
S_4	$G[1,2,5]$
A_4	$G[5,333,365]$
V	$G[1,41,57]$
$\mathbb{Z}_4$	Ukjent
D_4	$G[1,7,17]$

[10] Se diskusjonen på (1) http://mathforum.org/epigone/sci.math.research/twomprendlex og (2) http://mathforum.org/epigone/sci.math.research/frizhempham. I (1) gis en interessant to-parameter familie av eksempler der Galois-gruppen $G = G[a,b,c] = G[a(S,T), b(S,T), c(S,T)]$ er undergrupper av A_4 for alle parametervalg (S,T). (Eksemplet er slik at diskriminanten til ligningen $Q(x) = 0$ alltid er et kvadrattall.) Det er ukjent om det finnes slike tilfeller med G en ekte undergruppe av A_4.

Redusible tilfeller	$G[a,b,c]$	Kommentar
S_3	$G[3,12,20]$	På form (3)
S_3	$G[4,9,10]$	Ikke på form (3)
A_3	$G[315,544,1885]$	Ikke på form (3)
A_3	$G[2480,39780,49793]$	På form (3) (se fotnote[11])
V	$G[9,16,37]$	
$\mathbb{Z}_2 \quad (m=0)$	$G[750,1482,3157]$	
$\mathbb{Z}_2 \quad (m=2)$	$G[27,64,125]$	Tilfelle som i setning 2
$\mathbb{Z}_2 \quad (m=2)$	$G[12,30,65]$	Ikke på form (4)
$\mathbb{Z}_2 \quad (m=2)$	$G[528,8568,10985]$	Konstruert ved hjelp av (4) (se fotnote[12])
$\{e\}$	$G[168,660,1105]$	Ikke på form (4) (oppgave 3)
$\{e\}$	$G[468,924,2125]$	Ikke på form (4) (oppgave 3)
$\{e\}$	$G[945,3520,6409]$	Konstruert ved hjelp av (4) (se fotnote[13] og oppgave 3)
$\{e\}$	$G[2688,17391,25625]$	Se oppgave 3
$\{e\}$	$G[3003,16320,33245]$	Se oppgave 3

Litteratur

[1] Kent Holing: Når har fjerdegradsligningen konstruerbare røtter? *Normat* **51**, 15–21 (2003).

[2] Kent Holing: Når har fjerdegradsligningen konstruerbare røtter? Tilleggskommentar om Galois-gruppen. *Normat* **51**, 80–82 (2003).

[3] Kent Holing: På gjengrodde stiger – Epilog. *Normat* **50**, 92–95 (2002).

[4] Problem 11050. *The American Mathematical Monthly* **110**, 957 (2003).

[5] Problem 1678. *Mathematics Magazine* **76**, 318 (2003) & **77**, 322–323 (2004).

[6] Oppgave 404. *Normat* **49**, 89 (2001) & **51**, 35–37 (2003).

[7] W. Sierpinski: Theory of Numbers, *Polska Akademia Nauk*, TOM 42, 1963, side 74.

[8] Oppgave 443. *Normat* **52**, 51 (2004).

[9] G. Chrystal: *Textbook of Algebra*, Vol. I, Seventh Edition, Chelsea Publishing Company, 1964 (opprinnelig 1886), s. 207–208.

[10] Luise-Charlotte Kappe and Bette Warren. An Elementary Test for the Galois Group of a Quartic Polynomial. *The American Mathematical Monthly* **96**, 133–137 (1989).

[11] A. H. Beiler: *Recreations in the Theory of Numbers. The Queen of Mathematics Entertains*, Second Edition, Dover, 1966 (1964), kapittel 14.

[11] På form (3) med $\alpha = 85$, $\beta = 101$ og $(r,s,t) = (468,155,493)$.

[12] På form (4) med $(r,s,t) = (53,56,65)$ og $(u,v,t) = (16,63,65)$ (skalert med $\gcd(a,b,c) = 7$) og f ikke kvadrattall.

[13] På form (4) med $(r,s,t) = (352,135,377)$ og $(u,v,t) = (260,273,377)$ (skalert med $\gcd(a,b,c) = 3588$) og $f = 39\,525\,408^2$ et kvadrattall.