MATEMATIK 4AL

Christian U. Jensen

Matematisk Afdeling
Institut for Matematiske Fag
Københavns Universitet
2001

Indhold

1 Symmetriske polynomier

Lad i det følgende R være en kommutativ ring (uden nuldivisorer) med ét-element.

Definition 1.1. Et polynomium $f(X_1,\ldots,X_n) \in R[X_1,\ldots,X_n]$ kaldes *symmetrisk* hvis f går over i sig selv ved enhver permutation af $X_1,\ldots,X_n$, dvs.

$$f(X_{\sigma(1)},\ldots,X_{\sigma(n)}) = f(X_1,\ldots,X_n)\,, \quad \forall \sigma \in S_n\,.$$

Eksempel 1.2. Polynomierne

$$\begin{aligned}
s_1 &= X_1 + \cdots + X_n && (n \text{ Led})\\
s_2 &= X_1X_2 + X_1X_3 + \cdots + X_{n-1}X_n && \left(\binom{n}{2} \text{ led}\right)\\
s_3 &= X_1X_2X_3 + \cdots + X_{n-2}X_{n-1}X_n && \left(\binom{n}{3} \text{ led}\right)\\
&\vdots\\
s_n &= X_1X_2X_3\ldots X_n && (1 \text{ led})
\end{aligned}$$

er symmetriske, da

$$(T-X_1)(T-X_2)\ldots(T-X_n) = T^n - s_1T^{n-1} + s_2T^{n-2} - \cdots + (-1)^n s_n\,.$$

$s_1, s_2, \ldots, s_n$ kaldes de *elementær-symmetriske polynomier* i $X_1, X_2, \ldots, X_n$.

Sætning 1.3. (Hovedsætning for symmetriske polynomier). *Ethvert symmetrisk polynomium i $R[X_1,\ldots,X_n]$ kan på én og kun én måde skrives som et polynomium i $s_1,\ldots,s_n$.*

Inden beviset giver vi først nogle forberedelser.

Lad $f(X_1,\ldots,X_n) = \sum a_{i_1\ldots i_n} X_1^{i_1}\ldots X_n^{i_n} \in R[X_1,\ldots,X_n]$. Ved *graden af et led* $a_{i_1\ldots i_n}X_1^{i_1}\ldots X_n^{i_n}$ med $a_{i_1\ldots i_n} \neq 0$ forstås $i_1+\cdots+i_n$.

Ved *graden af et egentligt polynomium* f forstås den højeste forekommende grad af leddene med koefficient $\neq 0$.

Graden af leddene er ikke nok til at bestemme en ordning af leddene. Derfor indføres begrebet signatur. Ved *signaturen af et led* $a_{i_1\ldots i_n}X_1^{i_1}\ldots X_n^{i_n}$ med $a_{i_1\ldots i_n} \neq 0$ forstås talsættet $i = (i_1,\ldots,i_n)$. Mængden af signaturer ordnes ved, at man først ordner efter grad og derefter inden for hver grad ordner lexikografisk, dvs. for to forskellige signaturer $(i_1,\ldots,i_n)$ og $(j_1,\ldots,j_n)$ haves

$$(i_1,\ldots,i_n) < (j_1,\ldots,j_n)$$

hvis enten $i_1+\cdots+i_n < j_1+\cdots+j_n$ eller $i_1+\cdots+i_n = j_1+\cdots+j_n$ og $i_\nu < j_\nu$ for det mindste ν for hvilket $i_\nu \neq j_\nu$.

Ved *signaturen af et egentligt polynomium* forstås den højeste forekommende signatur.

Lemma 1.4. *Produktet af to egentlige polynomier i $R[X_1, \ldots, X_n]$ er egentligt, og leddet af højeste signatur i produktet er produktet af leddene af højeste signatur i de to polynomier.*

Bevis. Øvelse. □

Nu vender vi tilbage til hovedsætningen.

Bevis (for Hovedsætningen om symmetriske polynomier).

Først eksistens

Lad $f \in R[X_1, \ldots, X_n]$ være symmetrisk. Kan antage $f \neq 0$. Lad $cX_1^{i_1} \ldots X_n^{i_n}$ være leddet af højeste signatur. Da f er symmetrisk må $i_1 \geq i_2 \geq \cdots \geq i_n$.

Betragtes specielt de elementær-symmetriske polynomier $s_1, \ldots, s_n$ har disse som led af højeste signatur henholdsvis $X_1, X_1X_2, \ldots, X_1 \ldots X_n$.

På grund af Lemma 1.4 vil polynomiet $s_1^{j_1} s_2^{j_2} \ldots s_n^{j_n}$ for vilkårligt hele tal $j_1, \ldots, j_n \geq 0$ som led af højeste signatur have

$$X_1^{j_1}(X_1X_2)^{j_2} \ldots (X_1 \ldots X_n)^{j_n},$$

hvis signatur er

$$(j_1 + j_2 + \cdots + j_n, j_2 + \cdots + j_n, \ldots, j_n).$$

Vælger vi $j_1 = i_1 - i_2, j_2 = i_2 - i_3, \ldots, j_{n-1} = i_{n-1} - i_n, j_n = i_n$ bliver dette netop signaturen $(i_1, \ldots, i_n)$.

Differencen

$$f - cs_1^{j_1} s_2^{j_2} \ldots s_n^{j_n}$$

vil derfor enten være nulpolynomiet eller et symmetrisk polynomium af lavere signatur end f. Fortsættes med dette, må vi efter endeligt mange skridt få nulpolynomiet.

Entydighed:

Hertil er det nok at vise, at for $g = g(Y_1, \ldots, Y_n) \in R[Y_1, \ldots, Y_n]$ gælder

$$g \neq 0 \implies g(s_1, \ldots, s_n) = g(X_1 + \cdots + X_n, X_1X_2 + \cdots + X_{n-1}X_n, X_1 \ldots X_n) \neq 0.$$

Lad $dY_1 \ldots Y_n$ med $d \neq 0$ være et led i g. Indsættes heri for $Y_1, \ldots, Y_n$ de elementær-symmetriske polynomier $s_1, \ldots, s_n$ fås i følge det foregående, et polynomium i $X_1, \ldots, X_n$ i hvilket leddet af højeste signatur er

$$dX_1^{t_1}(X_1X_2)^{t_2} \ldots (X_1 \ldots X_n)^{t_n}.$$

Signaturen af dette led er

$$(t_1 + \cdots + t_n, t_2 + \cdots + t_n, \ldots, t_n).$$

Betragtes nu først de led i g for hvilke $t_1 + \cdots + t_n$ er størst, derefter blandt disse de led, for hvilke $t_2 + \cdots + t_n$ er størst osv., får vi i g udskilt et bestemt led $dY_1^{t_1} \ldots Y_n^{t_n}$ med den

egenskab, at det og kun det ved indsætning af de elementær-symmetriske polynomier fører til et led med nævnte signatur

$$(t_1 + \cdots t_n, t_2 + \cdots t_n, \ldots, t_n)\,.$$

Dette led kan ikke forkortes med noget andet, hvorfor

$$g(X_1 + \cdots X_n, X_1X_2 + \cdots + X_{n-1}X_n, \ldots, X_1 \ldots X_n) \neq 0\,.$$

□

- - - - - - - - - - -

I anvendelser spiller polynomiet

$$\Delta(X_1, \ldots, X_n) = \prod_{n \geq i > j \geq 1} (X_i - X_j) = \begin{vmatrix} 1 & X_1 & \cdots & X_1^{n-1} \\ 1 & X_2 & \cdots & X_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & X_n & \cdots & X_n^{n-1} \end{vmatrix} \tag{1}$$

en vigtig rolle.

Åbenbart gælder

$$\Delta(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = \begin{cases} \Delta(X_1, \ldots, X_n) & \text{for } \sigma \text{ lige} \\ -\Delta(X_1, \ldots, X_n) & \text{for } \sigma \text{ ulige}\,. \end{cases}$$

Specielt er

$$d(X_1, \ldots, X_n) = (\Delta(X_1, \ldots, X_n))^2$$

et symmetrisk polynomium. Alment kaldes et polynomium $f(X_1, \ldots, X_n)$ *skævsymmetrisk*, hvis

$$f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = \begin{cases} f(X_1, \ldots, X_n) & \text{for } \sigma \text{ lige} \\ -f(X_1, \ldots, X_n) & \text{for } \sigma \text{ ulige}\,. \end{cases}$$

Bemærkning 1.5. f er skævsymmetrisk såfremt $f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = -f(X_1, \ldots, X_n)$ for enhver transposition σ.

Vi viser nu

Sætning 1.6. *Lad R være et legeme af karakteristik $\neq 2$, og lad $f(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$. Da gælder*

$$f(X_1, \ldots, X_n) \text{ er skævsymmetrisk } \iff f(X_1, \ldots, X_n) = \Delta(X_1, \ldots, X_n) g(X_1, \ldots, X_n)\,,$$

hvor $g(X_1, \ldots, X_n)$ er symmetrisk.

Bevis. "⇐": klar.

"⇒": Lad $1 \leq i, j \leq n$ og $i > j$.

Vi skriver $f = \sum_{\mu,\nu} c_{\mu\nu} X_i^\mu X_j^\nu$, hvor

$$c_{\mu\nu} \in R[X_1, \ldots, X_{j-1}, X_{j+1}, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]\,.$$

Ved at anvende transpositionen $\begin{pmatrix} i & j \\ j & i \end{pmatrix}$ ses, at $c_{\mu\nu} = -c_{\nu\mu} \forall \mu, \nu$; specielt er $c_{\mu\mu} = 0$. Hvis f.eks. $\nu \leq \mu$ fås

$$\begin{aligned} c_{\mu\nu} X_i^\mu X_j^\nu + c_{\nu\mu} X_i^\nu X_j^\mu &= c_{\mu\nu} X_i^\mu X_j^\mu (X_j^{\nu-\mu} - X_i^{\nu-\mu}) \\ &= c_{\mu\nu} X_i^\mu X_j^\mu (X_j - X_i)(x_j^{\nu-\mu-1} + \cdots + X_i^{\nu-\mu-1}) \,. \end{aligned}$$

Heraf ses, at f er delelig med $X_i - X_j$.

Da de $\binom{n}{2}$ polynomier $X_i - X_j$, $1 \leq j < i \leq n$ er ikke-associerede irreducible elementer i $R[X_1, \ldots, X_n]$, der har entydig primfaktoropløsning, ses, at $f = \Delta g$, hvor $g \in R[X_1, \ldots, X_n]$.

g bliver automatisk symmetrisk, da både f og Δ er skævsymmetriske. □

Opgave: Lad $f(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$ og antag, at man ved anvendelse af de $n!$ permutationer af de variable $X_1, \ldots, X_n$ højst får to forskellige polynomier. Vis, at f kan skrives

$$f = g + \Delta h \,,$$

hvor g og h er symmetriske polynomier i $R[X_1, \ldots, X_n]$.

- - - - - - - - - -

Da $d(X_1, \ldots, X_n) = (\Delta(X_1, \ldots, X_n))^2$ er symmetrisk, kan d fremstilles som polynomium i $s_1, \ldots, s_n$. Hertil får vi brug for *Newtons Formler for Potenssummer*. Vi sætter

$$\begin{aligned} P_1 &= X_1 + \cdots + X_n \\ P_2 &= X_2^2 + \cdots + X_n^2 \\ &\vdots \\ P_\nu &= X_1^\nu + \cdots + X_n^\nu \,. \end{aligned}$$

Vi betragter $F(T, X_1, \ldots, X_n) = \prod_{i=1}^n (T - X_i) = T^n - s_1 T^{n-1} + s_2 T^{n-2} - \cdots + (-1)^n s_n = T^n + a_1 T^{n-1} + a_2 T^{n-2} + \cdots + a_n$, hvor $a_i = (-1)^i s_i$; vi har $F(T, X_1, \ldots, X_n) \in R[X_1, \ldots, X_n][T]$. Vi anvender formel differentiation med hensyn til T

$$F'(T) = nT^{n-1} + (n-1)a_1 T^{n-2} + \cdots + a_{n-1} = \frac{F(T)}{T - X_1} + \cdots + \frac{F(T)}{T - X_n} \,. \qquad (2)$$

Nu er $\frac{F(T)}{T-X_i} = \frac{F(T)-F(X_i)}{T-X_i} = \frac{T^n - X_i^n}{T-X_i} + a_1 \frac{T^{n-1} - X_i^{n-1}}{T-X_i} + \cdots a_{n-1} \frac{T - X_i}{T - X_i} =$

$$\begin{aligned} &(T^{n-1} + X_i T^{n-2} + X_i^2 T^{n-3} + \cdots + X_i^{n-1}) \\ &+ a_1 (T^{n-2} + X_i T^{n-3} + \cdots + X_i^{n-2}) \\ &+ a_2 (T^{n-3} + \cdots + X_i^{n-3}) \\ &\vdots \\ &+ a_{n-1} \,. \end{aligned}$$

Ved addition fås et udtryk for $F'(T)$, som sammenholdt med (2), giver

$$\begin{aligned}
P_1 + na_1 &= (n-1)a_1\\
P_2 + a_1P_1 + na_2 &= (n-2)a_2\\
P_3 + a_1P_2 + a_2P_1 + na_3 &= (n-3)a_3\\
\vdots &\quad\vdots\\
P_{n-1} + a_1P_{n-2} + a_2P_{n-3} + a_3P_{n-4} + \cdots + a_{n-2}P_1 + na_{n-1} &= a_{n-1}\,.
\end{aligned}$$

Nu er

$$X_i^n + a_1X_i^{n-1} + \cdots + a_{n-1}X_i + a_n = 0\,.$$

Ved addition fås

$$P_n + a_1P_{n-1} + \cdots + a_{n-1}P_1 + na_n = 0\,.$$

Endvidere er for $k = 1, 2, \ldots$

$$X_i^{n+k} + a_iX_i^{n+k-1} + \cdots + a_{n-1}X_i^{k+1} + a_nX_i^k = 0\,.$$

Ved addition fås

$$P_{n+k} + a_1P_{n+k-1} + \cdots + a_{n-1}P_{k+1} + a_nP_k = 0\,.$$

- - - - - - - - - -

De udledte formler kaldes for Newtons Formler for Potenssummer:

$$\begin{aligned}
P_1 + a_1 &= 0\\
P_2 + a_1P_1 + 2a_2 &= 0\\
P_3 + a_1P_2 + a_2P_1 + 3a_3 &= 0\\
\vdots &\quad\vdots\\
P_{n-1} + \cdots + a_{n-3} + a_{n-2}P_1 + (n-1)a_{n-1} &= 0\\
P_n + a_1P_{n-1} + \cdots + a_{n-2}P_2 + a_{n-1}P_1 + na_n &= 0
\end{aligned}$$

og for $q > n$ haves

$$P_q + a_1P_{q-1} + \cdots a_{n-1}P_{q-n+1} + a_nP_{q-n} = 0\,.$$

Hvis vi sætter $a_\ell = 0$ for $\ell > n$ kan Newtons formler skrives ensartet:

$$P_q + a_1P_{q-1} + a_2P_{q-2} + \cdots + a_{q-1}P_1 + qa_q = 0\,.$$

Af disse formler kan $P_1, P_2, \ldots$ beregnes:

$$\begin{aligned}
P_1 &= -a_1\\
P_2 &= a_1^2 - 2a_2\\
P_3 &= -a_1^3 + 3a_1a_2 - 3a_3\\
P_4 &= a_1^4 - 4a_1^2a_2 + 4a_1a_3 + 2a_2^2 - 4a_4
\end{aligned}$$

Et alment eksplicit udtryk er:

$$P_q = \begin{vmatrix} 1 & 0 & 0 & \cdots & 0 & -a_1 \\ a_1 & 1 & 0 & \cdots & 0 & -2a_2 \\ a_2 & a_1 & 1 & \cdots & 0 & -3a_3 \\ \vdots & & \vdots & & & \vdots \\ a_{q-1} & a_{q-2} & a_{q-3} & \cdots & a_1 & -qa_q \end{vmatrix}$$

Potenssummerne $P_1, P_2, \ldots$ spiller en central rolle, når vi vil udtrykke $d(X_1, \ldots, X_n)$ ved $s_1, \ldots, s_n$.

Ud fra (1) fås, idet determinantens kvadrat udregnes ved søjle-søjle multiplikation

$$d = \Delta^2 = \begin{vmatrix} n & P_1 & P_2 & \cdots & P_{n-1} \\ P_1 & P_2 & P_3 & \cdots & P_n \\ P_2 & P_3 & P_4 & \cdots & P_{n+1} \\ \vdots & & \vdots & & \vdots \\ P_{n-1} & P_n & P_{n+1} & \cdots & P_{2n-2} \end{vmatrix}$$

For $n = 1, 2, 3, 4, 5$ fås

$\underline{n=2}$: $F(T, X_1, X_2) = T^2 + a_1 T + a_2$

$$d = \begin{vmatrix} 2 & P_1 \\ P_1 & P_2 \end{vmatrix} = \begin{vmatrix} 2 & -a_1 \\ -a_1 & a_1^2 - 2a_2 \end{vmatrix} = a_1^2 - 4a_2.$$

$\underline{n=3}$: $F(T, X_1, X_2, X_3) = T^3 + a_1 T^2 + a_2 T + a_3$

$$d = \begin{vmatrix} 3 & P_1 & P_2 \\ P_1 & P_2 & P_3 \\ P_2 & P_3 & P_4 \end{vmatrix} = a_1^2 a_2^2 - 4a_2^3 - 4a_1^3 a_3 - 27a_3^2 + 18a_1 a_2 a_3.$$

$\underline{n=4}$: $F(T, X_1, \ldots, X_4) = T^4 + a_1 T^3 + a_2 T^2 + a_3 T + a_4$

$d = 256a_4^3 - 192a_4^2 a_3 a_1 - 128a_4^2 a_2^2 + 144a_4^2 a_2 a_1^2 - 27a_4^2 a_1^4 + 144a_4 a_3^2 - 6a_4 a_3^2 a_1^1$
$-80a_4 a_3 a_2^2 a_1 + 18a_4 a_3 a_2 a_1^3 + 16a_4 a_2^2 - 4a_4 a_2^2 - 4a_4 a_2^3 a_1^2 - 27a_3^4 + 18a_3^2 a_2 a_1 - 4a_3^3 a_1^3$
$4a_3^2 a_2^3 + a_3^2 a_2^2 a_1.$

$\underline{n=5}$: $F(T, X_1, \ldots, X_5) = T^5 + a_1 X^4 + a_2 T^3 + a_3 T^2 + a_4 T + a_5$

d bliver ret kompliceret, men til vores formål er følgende tilstrækkeligt:
$d = 4^4 a_4^5 + 5^5 a_5^4 + a_1$ (heltalspol. i $a_1, \ldots, a_5$) $+ a_2$ (heltalspol. i $a_1, \ldots, a_5$)
$+a_3$ (heltalspol. i $a_1, \ldots, a_5$).

2 Aut (S_n)

Forberedelser

Definition 2.1. En permutation $\sigma \in S_n$ siges at have *cykeltype* $(\ell_1, \ldots, \ell_t)$, hvor $n = \ell_1 + \cdots + \ell_t$, hvis længderne af cyklerne i σ's kanoniske cykelfremstilling er $\ell_1, \ldots, \ell_t$.

Lemma 2.2. *To permutationer σ og τ i S_n er konjugerede $\iff$ σ og τ har samme cykeltype.*

Bevis. Betragt permutationen $\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$. For ethvert $\sigma \in S_n$ er

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} \sigma \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}^{-1} = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_{\sigma(1)} & a_{\sigma(2)} & \cdots & a_{\sigma(n)} \end{pmatrix}.$$

Dvs. overgang til en konjugeret permutation svarer til "navneskift" af de permuterede objekter. Dette giver umiddelbart lemmaet. □

Lemma 2.3. *Lad $\sigma \in S_n$ have cykeltypen $(\ell_1, \ldots, \ell_t)$. Da er σ's orden lig mindste fælles multiplum af $\ell_1, \ldots, \ell_t$.*

Bevis. Umiddelbart. □

Sætning 2.4. *For $n \neq 2$, $n \neq 6$ er S_n fuldkommen; dvs. $Z(S_n) = 1$ og $\mathrm{Aut}(S_n) = \mathrm{Aut}_i(S_n) \simeq S_n$.*

Bevis. Nok at godtgøre $\mathrm{Aut}(S_n) \simeq S_n$.

Det sker i to etaper:

1° Lad $\varphi \in \mathrm{Aut}(S_n)$, og antag φ (transposition) = transposition. Da er φ en indre automorfi for S_n.

Bevis for 1° Da enhver permutation i S_n er produkt af transpositioner af formen $(1; k)$, $k = 2, 3, \ldots, n$, er det nok at se på billederne af $(1\ 2) \ldots (1\ n)$.

Antag $\varphi(1\ 2) = (a\ b)$.

Da $(1\ 2)$ og $(1\ 3)$ ej er ombyttelige, er $\varphi(1\ 2)$ og $\varphi(1\ 3)$ ej ombyttelige. Hvis $\varphi(1\ 3) = (x\ y)$, må $\{x, y\}$ og $\{a, b\}$ have et fælles element, f.eks. a. Dvs., vi kan antage

$$\varphi(1\ 3) = (a\ c), \quad a, b, c \text{ indbyrdes forskellige}.$$

Hvis $\varphi(1\ 4) = (u\ v)$ må $\{u, v\}$ have netop ét fælles element med $\{a, b\}$, og netop ét fælles element med $\{a, c\}$, dvs. $(u\ v)$ må enten være $(b\ c)$ eller $(a\ d)$ for passende d, $(\neq a, \neq b, \neq c)$. Hvis $\varphi(1\ 4) = (b\ c)$, skulle $\varphi((1\ 2)(1\ 3)(1\ 4)) = \varphi(1\ 4\ 3\ 2)$ være lig $(a\ b)(a\ c)(b\ c) = (a\ c)$, hvilket er umuligt, da $(1\ 4\ 3\ 2)$ har orden 4 og $(a\ c)$ har orden 2. Altså *må* $(1\ 4) = (a\ d)$ for passende d.

Videre ses, at $\varphi(1\ 5) = (a\ e)$ for passende e osv. Dvs. der findes indbyrdes forskellige elementer $a_1 = a, a_2 = b, a_3 = c, a_4 = d, \ldots$ så $\varphi(1\ k) = (a_1\ a_k)$ for $2 \leq k \leq n$. Idet $(a_1\ a_2 \ldots a_n)$ er en permutation af $1, 2, \ldots, n$, gælder

$$\varphi(1\ k) = (a_1\ a_k) = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix} \begin{pmatrix} 1 & k \\ k & 1 \end{pmatrix} \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ 1 & 2 & \cdots & n \end{pmatrix}$$
$$= \begin{pmatrix} a_1 & a_k \\ a_k & a_1 \end{pmatrix},$$

dvs. φ og den ved $\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$ bestemte indre automorfi for S_n stemmer overens på transpositionerne $(1\ k)$, $1 \leq k \leq n$. Ifølge tidligere bemærkning er φ derfor den ved $\begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$ bestemte indre automorfi.

$\underline{2}^\circ$ Hvis $n \neq 2$, $n \neq 6$, vil enhver automorfi for S_n føre transpositioner over i transpositioner.

Bevis for 2° Lad $\varphi \in \mathrm{Aut}(S_n)$, og lad $(a\ b)$ være en transposition. Da $(a\ b)$ har orden 2, har $\varphi(a\ b)$ orden 2, dvs. ifølge Lemma 2.3 er $\varphi(a\ b)$ et produkt af k indbyrdes disjunkte transpositioner, $1 \leq k \leq \frac{n}{2}$. Da vil φ føre konjugationsklassen bestemt ved $(a\ b)$, dvs. mængden af alle transpositioner, over i konjugationsklassen C_k af alle permutationer, der er produkt af k indbyrdes disjunkte transpositioner. Antallet af transpositioner er $\frac{n(n-1)}{2}$. Et kombinatorisk argument viser, at C_k består af

$$\frac{1}{k!}\left(\frac{n(n-1)}{2}\frac{(n-2)(n-3)}{2}\cdots\frac{(n-2k+2)(2-2k+1)}{2}\right)$$

permutationer (hvorfor?)

Vi viser 2° ved at godtgøre, at $|C_k| = \frac{n(n-1)}{2}$ for $n \neq 2$, $n \neq 6$ medfører $k = 1$. Denne ligning kan omskrives til

$$(n-2)(n-3)\ldots(n-2k+1) = k!2^{k-1}\,. \tag{3}$$

Da venstre side er positiv, må $n \geq 2k$. For fast n fås

$$\text{venstre side} \quad \geq (2k-2)(2k-3)\ldots(2k-2k-1) = (2k-2)!$$

Ved induktion ses let, at

$$(2k-2)! > k!2^{k-1}\,, \quad \text{for } k \geq 4$$

så (3) kan kun gælde for $k < 4$ uafhængigt af n.

$k = 2$ kan ikke forekomme, da $(n-2)(n-3) = 2!2 = 4$ ikke har heltalsløsninger i n. Hvis $k = 3$ må $n \geq 6$. Hvis $n > 6$ er venstre side i (3), $(n-2)(n-3)(n-4)(n-5)$ mindst $5 \cdot 4 \cdot 3 \cdot 2 = 120$, hvilket er $> 3!2^{3-1} = 24$.

Altså er der kun muligheden $n = 6$.

Dette godtgør 2°. □

Bemærkning 2.5. For $n = 6$, $k = 3$ gælder (3), og vi skal senere vise, at S_6 ej er fuldkommen.

Vi har faktisk bevist, at hvis en automorfi φ for S_6 ikke er en indre automorfi, må $\varphi(C_1) = C_3$ og $\varphi(C_3) = C_1$.

3 Homomorfien ρ

Lad H være undergruppe i gruppen G med $[G : H] = n$, hvor $n \in \mathbb{N}$. Lad $G = \bigcup_{i=1}^{n} g_i H$ være inddelingen af G i disjunkte højreklasser med hensyn til H. Vi kan f.eks. antage $g_1 = e$. For ethvert $g \in G$ vil $G = \bigcup_{i=1}^{n} g g_i H$ igen være en inddeling af G i højresideklasser, hvorfor $\begin{pmatrix} g_1H & g_2H & \cdots & g_nH \\ gg_1H & gg_2H & \cdots & gg_nH \end{pmatrix}$ vil være en permutation af sideklasserne g_iH, $1 \leq i \leq n$. $\begin{pmatrix} g_1H & g_2H & \cdots & g_nH \\ gg_1H & gg_2H & \cdots & gg_nH \end{pmatrix}$ kan opfattes som element i S_n, og vi definerer $\rho : G \to S_n$ ved $\rho g = \begin{pmatrix} g_1H & g_2H & \cdots & g_nH \\ gg_1H & gg_2H & \cdots & gg_nH \end{pmatrix}$.

Vi skriver $gg_iH = g_{\rho(g)[i]}H$, $1 \leq i \leq n$.

Det ses let, at ρ er en homomorfi. Endvidere vil ρG være en transitiv undergruppe i S_n, hvorfor $n \mid |\rho G|$.

$\operatorname{Ker}\rho = \bigcap_{i=1}^{n} g_i H g_i^{-1} \subseteq H$ og $\operatorname{Ker}\rho \triangleleft G$, så $G/\operatorname{Ker}\rho \simeq \rho G$.

Eksempel 3.1. Lad G være en simpel ikke-abelsk gruppe. Hvis $G \supsetneq H$, H undergruppe i G og $[G : H] = n$, da må $|G|$ gå op i $n!$

Opgave 3.1. Vis ved hjælp af Sylows sætninger og ovenstående, at enhver gruppe af orden < 60 er opløselig.

Definition 3.2. For $1 \leq i \leq n$ sættes $S_n^{(i)} = \{\sigma \in S_n | \sigma(i) = i\}$.

Bemærkning 3.3. $[S_n : S_n^{(i)}] = n$.

Sætning 3.4. *$S_n^{(i)}$ er en maksimal undergruppe i S_n, dvs. H undergruppe i S_n og $S_n^{(i)} \subseteq H \subseteq S_n \implies S_n^{(i)} = H \vee S_n = H$.*

Bevis. For $n = 2, 3, 4$ verificeres direkte.

For $5 \geq n$ føres beviset indirekte. Antag der fandtes undergruppe H for hvilken $S_n^{(i)} \subsetneq H \subsetneq S_n$, og dermed $[S_n : H] = t$, $1 < t < n$.

Betragt homomorfien $\rho : S_n \to S_t$ defineret ovenfor.

Da vil $\operatorname{Ker} \triangleleft S_n$ og $\operatorname{Ker}\rho \subseteq H$. Ifølge Galois' sætning om S_n, må $\operatorname{Ker}\rho = e, A_n, S_n$ (da $n \geq 5$). Her kan $\operatorname{Ker}\rho = A_n$ eller $\operatorname{Ker}\rho = S_n$ ikke forekomme, dvs. $\operatorname{Ker}\rho = e$, så ρ er injektiv, og dermed S_n isomorf med en undergruppe i S_t.

Dette giver den ønskede modstrid da $t! < n!$ □

Sætning 3.5. *Antag $n \geq 5$ og $\operatorname{Aut}(S_n) = \operatorname{Aut}_i(S_n)$. Lad H være en undergruppe i S_n for hvilken $[S_n : H] = n$. Da er $H = S_n^{(i)}$ for passende i, $1 \leq i \leq n$.*

Bevis. Vi betragter homomorfien $\rho : S_n \to S_n$ med hensyn til H.

Hvis $S_n = \bigcup_{i=1}^{n} \sigma_i H$ gælder altså $\sigma\sigma_i = \sigma_{\rho(\sigma)[i]}H$. (Vi antager $\sigma_1 = e$).

Som ovenfor ses, at ρ er injektiv og dermed bijektiv, dvs. $\rho : S_n \to S_n$, hvor $\rho(\sigma)$ er den ved $\sigma\sigma_i = \sigma_{\rho(\sigma)[i]}H$ bestemte permutation i S_n, er en automorfi for S_n. Ifølge forudsætningen er ρ en indre automorfi, dvs. $\exists \tau \in S_n$ så $\rho(\sigma) = \tau\sigma\tau^{-1} \forall \sigma \in S_n$.

Lad nu $\sigma \in H$, da er $\sigma H = H$, dvs. $\sigma\sigma_1 H = \sigma_1 H$ og dermed $\rho(\sigma)[1] = 1$; følgelig er $\rho(\sigma) \in S_n^{(1)}$, og derfor $\tau\sigma\tau^{-1} \in S_n^{(1)}$ eller $\tau H \tau^{-1} \subseteq S_n^{(1)}$; da $|H| = |\tau H \tau^{-1}| = |S_n^{(1)}|$ $(= (n-1)!)$ er $\tau H \tau^{-1} = S_n^{(1)}$, hvorfor $H = \tau^{-1} S_n^{(1)} \tau$. Da gælder $H = S_n^{(j)}$, hvor $\tau(j) = 1$. □

Vi er nu i stand til at vise

Sætning 3.6. *S_6 har ikke-indre automorfier.*

Bevis. Ifølge Sætning 3.5 er det nok at finde en undergruppe H i S_6 af indeks 6 i S_6, så $H \neq S_6^{(i)}$ for ethvert i, $1 \leq i \leq 6$.

S_5 har netop 6 5-Sylowundergrupper $P_1, P_2, \ldots, P_6$, der hver især har orden 5. Ifølge Sylows 2. Sætning er $P_1, P_2, \ldots, P_6$ indbyrdes konjugerede.

Vi definerer nu en afbildning $\varphi : S_5 \to S_6$, hvor S_6 opfattes som permutationer af $P_1, P_2, \ldots, P_6$:

$$x \in S_5\,, \quad \varphi(x) = \begin{pmatrix} P_1 & P_2 & P_3 & P_4 & P_5 & P_6 \\ xP_1x^{-1} & xP_2x^{-1} & xP_3x^{-1} & xP_4x^{-1} & xP_5x^{-1} & xP_6x^{-1} \end{pmatrix}$$

φ er en gruppehomomorfi, og φS_5 er (p.g.a. Sylows 2. Sætning), en transitiv undergruppe i S_6. Følgelig vil $6 \mid |\varphi S_5| = [S_5 : \operatorname{Ker}\varphi]$. Da $\operatorname{Ker}\varphi \triangleleft S_5$, må $\ker\varphi = \{e\}$. Altså $\varphi(S_5)$ har indeks 6 i S_6. Da φS_5 er transitiv, kan φS_5 ikke have formen $S_6^{(i)}$ for noget i. □

Af det ovenstående fås, at $[\operatorname{Aut}(S_6) : \operatorname{Aut}_i(S_6)] \geq 2$.

Lad $\alpha \in \operatorname{Aut}(S_6) \setminus \operatorname{Aut}_i(S_6)$. Hvis C_1 er konjugationsklassen i S_6 bestående af alle transpositioner, og C_3 konjugationsklassen i S_6 bestående af alle permutationer der er produkt af 3 disjunkte transpositioner, da fremgår det af beviset for Sætning 2.4, at $\alpha(C_1) = C_3$ og $\alpha(C_3) = C_1$. Derfor er $[\operatorname{Aut}(S_6) : \operatorname{Aut}_i(S_6)] = 2$.

4 Orbit

Lad S_n operere på en mængde M, f.eks. mængden af polynomier i n variable over et legeme.

For $m \in M$ definerer vi $\operatorname{Stab}(m) = \{\sigma \in S_n | \sigma m = m\}$, samt *banen* eller *orbit* for m som mængden $\{\sigma m | \sigma \in S_n\}$. Da gælder

Sætning 4.1. *Antallet af elementer i m's bane ($|\operatorname{Orbit}(m)|$) er lig indekset $[S_n : \operatorname{Stab}(m)]$.*

Bevis. $\sigma_1 m = \sigma_2 m \iff \sigma_1^{-1}\sigma_2 m = m \iff \sigma_1^{-1}\sigma_2 \in \operatorname{Stab}(m) \iff \sigma_1 \sim_{\operatorname{Stab(m)}} \sigma_2$. □

Derfor er det af interesse at bestemme undergrupper i S_n af givet indeks.

Sætning 4.2. *Lad H være en undergruppe i S_n, $H \neq S_n$, $H \neq A_n$. Da er $[S_n : H] \geq n$, bortset fra tilfældet $n = 4$, hvor S_4 indeholder undergrupper af indeks 3.*

Bevis. Lad $[S_n : H] = t$: Vi skal vise $t \geq n$ (når $n \neq 4$). For $n = 1, 2$ eller 3 er alt klart. For $n = 4$ vil en 2-Sylowgruppe i S_4 have indeks 3. For $n \geq 5$ betragtes homomorfien ρ:

$$S_n \underset{\rho}{\mapsto} S_t$$

$\operatorname{Ker}\rho \subseteq H$ og $\operatorname{Ker}\rho \triangleleft S_n$, hvorfor $\operatorname{Ker}\rho = \{e\}$. Altså er ρ injektiv, og $t \geq n$. □

Eksempel 4.3. Lad S_4 operere på $K[X_1, X_2, X_3, X_4]$. Stabilisatoren for $f(X_1, X_2, X_3, X_4) = X_1X_3 + X_2X_4$ er $\simeq D_4$. Altså er $|\operatorname{Orbit}(f)| = 3$; der gælder:

$$\operatorname{Orbit}(f) = \{X_1X_3 + X_2X_4, X_1X_4 + X_2X_3, X_1X_2 + X_3X_4\}\,.$$

Fra sætningen om undergrupper i S_n af indeks n fås

Sætning 4.4. *Lad $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$, $n \neq 6$. Da gælder $|\operatorname{Orbit}(f)| = n$ (i.e. ved permutationer af de n variable $X_1, \ldots, X_n$ i $f(X_1, \ldots, X_n)$ fås netop n forskellige polynomier) $\iff$ $f(X_1, \ldots, X_n)$ er ikke-symmetrisk i $X_1, \ldots, X_n$, men der findes et i $(1 \leq i \leq n)$, så f er symmetrisk i de $(n-1)$ variable $X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n$.*

Bevis. "$\Leftarrow$": $\operatorname{Stab}(f) = S_n^{(i)}$ (benyt at $S_n^{(i)}$ er en maksimal undergruppe i S_n).

"$\Rightarrow$": $\operatorname{Stab}(f)$ er en undergruppe i S_n af indeks n, hvorfor der findes et i $(1 \leq i \leq n)$, så $\operatorname{Stab}(f) = S_n^{(i)}$. □

5 Warings formel

Med notationerne fra Newtons formler for potenssummer, kan man vise følgende:

$$P_m = \sum_{\nu_1,\ldots,\nu_n} (-1)^{\nu_1+\cdots+\nu_n} \frac{m(\nu_1 + \cdots + \nu_n - 1)!}{\nu_1!\nu_2! \ldots \nu_n!} a_1^{\nu_1} a_2^{\nu_2} \ldots a_n^{\nu_n}\,.$$

$\nu_1, \ldots, \nu_n$ gennemløber alle ikke-negative hele tal for hvilke $\nu_1 + 2\nu_2 + \cdots + n\nu_n = m$ og $a_i = (-1)^i s_i$ for $i = 1, 2, \ldots n$.

6 Trediegradspolynomier

Lad $f(X) = X^3 + a_1X^2 + a_2X + a_3$ være et polynomium i $\mathbb{Q}[X]$. Diskriminanten er

$$\operatorname{Disk}(f) = a_1^2a_2^2 - 4a_2^3 - 4a_1^3a_3 - 27a_3^2 + 18a_1a_2a_3\,.$$

Ved hjælp af 12A i kapitel III [Alg3, Theorem 3.41] fås:

Sætning 6.1. *Lad M være spaltningslegeme for $f(X)$ over $\mathbb{Q}$. Antag $f(X)$ har lutter simple rødder. Da gælder* $\operatorname{Gr}(M/\mathbb{Q})$*:*

$f(x)$	$\operatorname{Disk}(f) \in \mathbb{Q}^2$	$\operatorname{Disk}(f) \notin \mathbb{Q}^2$
$f(x)$ irred.	$\operatorname{Gr}(M/\mathbb{Q}) \simeq A_3$	$\operatorname{Gr}(M/\mathbb{Q}) \simeq S_3$
$f(x)$ reducib.	$\operatorname{Gr}(M/\mathbb{Q}) \simeq \{1\}$	$\operatorname{Gr}(M/\mathbb{Q}) \simeq S_2$

7 Fjerdegradspolynomier

Lad $f(X) = X^4 + aX^3 + bX^2 + cX + d$ være et polynomium i $\mathbb{Q}[X]$ med rødderne $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, der antages at være indbyrdes forskellige. Den *kubiske resolvent* for $f(X)$ defineres som

$$g(y) = (y - \alpha_1\alpha_2 - \alpha_3\alpha_4)(y - \alpha_1\alpha_3 - \alpha_2\alpha_4)(y - \alpha_1\alpha_4 - \alpha_2\alpha_3)$$

og man udregner

$$g(y) = y^3 - by^2 + (ac - 4d)y - a^2d + 4bd - c^2\,,$$

som altså får koefficienter i $\mathbb{Q}$. Diskriminanten af g er

$$[(\alpha_1\alpha_2 + \alpha_3\alpha_4 - \alpha_1\alpha_3 - \alpha_2\alpha_4)(\alpha_1\alpha_2 + \alpha_3\alpha_4 - \alpha_1\alpha_4 - \alpha_2\alpha_3)(\alpha_1\alpha_3 + \alpha_2\alpha_4 - \alpha_1\alpha_4 - \alpha_2\alpha_3)]^2\,,$$

der netop er lig diskriminanten for f (udregning!). Specielt er rødderne i $g(y)$ indbyrdes forskellige, da rødderne i $f(X)$ er forudsat indbyrdes forskellige.

Antag nu $f(X)$ er irreducibel i $\mathbb{Q}[X]$, og lad M være spaltningslegeme for $f(X)$ over $\mathbb{Q}$. Da er $\mathrm{Gr}(M/\mathbb{Q})$ en transitiv undergruppe i S_4, og der er de fem muligheder for $\mathrm{Gr}(M/\mathbb{Q})$: $S_4, A_4, D_4, \mathbb{Z}/4\mathbb{Z}$, og V_4.

Lad $\mathcal{V}$ være undergruppen i S_4 bestående af

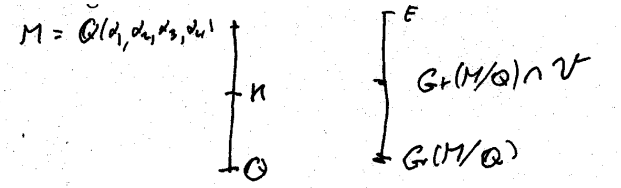
$$(1), (12)(34), (13)(24) \text{ og } (14)(23)\,.$$

$\mathcal{V}$ er isomorf med Kleins Vierergruppe V_4, og $\mathcal{V}$ er den eneste *transitive* undergruppe i S_4, der er isomorf med V_4.

Lad nu $K = \mathbb{Q}(\alpha_1\alpha_2 + \alpha_3\alpha_4, \alpha_1\alpha_3 + \alpha_2\alpha_4, \alpha_1\alpha_4 + \alpha_2\alpha_3)$ være spaltningslegemet (*resolventlegemet*) over $\mathbb{Q}$ for den kubiske resolvent $g(y)$). Ved direkte verifikation fås

$$TK = \{\sigma \in \mathrm{Gr}(M/\mathbb{Q}) | \forall k \in K : \sigma(k) = k\} = \mathrm{Gr}(M/\mathbb{Q}) \cap \mathcal{V}\,.$$

Vi har altså diagrammet

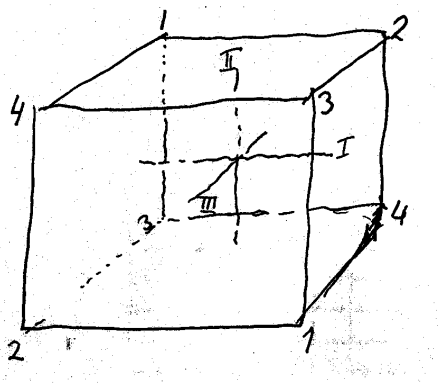


Lad $m = [K : \mathbb{Q}]$ som må være $6, 3, 2$ eller 1. Endvidere er $[M : K]$ divisor i 4, altså $1, 2$ eller 4. Ved bl.a. diskriminantovervejelser fås

Sætning 7.1.

$$\begin{aligned}
m = 6 &\implies \mathrm{Gr}(M/\mathbb{Q}) \simeq S_4\,.\\
m = 3 &\implies \mathrm{Gr}(M/\mathbb{Q}) \simeq A_4\,.\\
m = 2 &\implies \mathrm{Gr}(M/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}\,, \text{ eller } D_4\,.\\
m = 1 &\implies \mathrm{Gr}(M/\mathbb{Q}) \simeq V_4\,.
\end{aligned}$$

Vi tænker på S_4 som hexaedergruppen, bestående af alle drejninger i rummet, der fører et hexaeder (en terning) over i sig selv.



- Til I svarer to sideflader, hvortil vi knytter polynomiet $X_1X_2 + X_3X_4$.
- Til II svarer to sideflader, hvortil vi knytter polynomiet $X_1X_3 + X_2X_4$.
- Til III svarer to sideflader, hvortil vi knytter polynomiet $X_1X_4 + X_2X_3$.

Til hver drejning i hexaedergruppen ($\simeq S_4$) svarer en permutation af I, II og III, og vi får derved en surjektiv homomorfi $\varphi : S_4 \to S_3$; $\ker(\varphi) = \mathcal{V}$. S_4 opererer på polynomierne i X_1, X_2, X_3 og X_4. En permutation i $\mathcal{V}$ fixer $X_1X_2 + X_3X_4, X_1X_3 + X_2X_4$ og $X_1X_4 + X_2X_3$, mens en permutation, der ikke ligger i $\mathcal{V}$ effektivt flytter mindst et af ovenstående tre polynomier.

Hvert af de tre polynomier $X_1X_2 + X_3X_4, X_1X_3 + X_2X_4$ og $X_1X_4 + X_2X_3$ har en med D_4 isomorf stabilitetsgruppe. Disse tre stabilitetsgrupper er netop de tre 2-Sylowgrupper i S_4.

Vedrørende tilfældet $m = 2$. Her er $g(y) = (y-\gamma)(y^2+\beta y+\delta)$ for passende $\gamma, \beta, \delta \in \mathbb{Q}$, og $y^2 + \beta y + \delta$ er irreducibelt i $\mathbb{Q}[X]$. Det kubiske resolventlegeme K er $\mathbb{Q}(\sqrt{\beta^2 - 4\delta})$. Da gælder

Sætning 7.2. $\mathrm{Gr}(M/\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z} \iff x^2 - \gamma x + d$ *og* $x^2 + ax + (b - \gamma)$ *har rødder i* K.

Bevis. Vi kan antage $\gamma = \alpha_1\alpha_2 + \alpha_3\alpha_4$. Da finder vi

$$\left.\begin{aligned} x^2 - \gamma x + d &= (x - \alpha_1\alpha_2)(x - \alpha_3\alpha_4) \\ x^2 + ax + b - \gamma &= [x - (\alpha_1 + \alpha_2)][x - (\alpha_3 + \alpha_4)] \end{aligned}\right\} \qquad (\star)$$

Hvis $\mathrm{Gr}(M/\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$ er K det eneste kvadratiske dellegeme af M; følgelig vil rødderne til ovenstående to andengradspolynomier ($\star$) som tilhører M, allerede ligge i K.

Antag omvendt, at de to andengradspolynomier ($\star$) har rødder i K. For at vise $\mathrm{Gr}(M/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ er det, (jf. Sætning 7.1), nok at godtgøre $[M : \mathbb{Q}] = 4$. Hertil bemærkes først, at $M = K(\alpha_1, \alpha_2)$; thi

$$K(\alpha_1, \alpha_2) = \mathbb{Q}(\alpha_1\alpha_2 + \alpha_3\alpha_4, \alpha_1\alpha_3 + \alpha_2\alpha_4, \alpha_1\alpha_4 + \alpha_2\alpha_3, \alpha_1, \alpha_2)\,,$$

og åbenbart gælder

$$\begin{aligned} \alpha_1, \alpha_2 &\in K(\alpha_1, \alpha_2) \\ \alpha_1\alpha_3 + \alpha_2\alpha_4 &\in K(\alpha_1, \alpha_2) \\ \alpha_3 + \alpha_4 = -a - \alpha_1 - \alpha_2 &\in K(\alpha_1, \alpha_2)\,. \end{aligned}$$

Da $\alpha_1 \neq \alpha_2$ viser løsning af de to sidste ligninger (lineære i α_3 og α_4), at α_3 og α_4 ligger i $K(\alpha_1, \alpha_2)$. Altså:

$$M = K(\alpha_1, \alpha_2, \alpha_3, \alpha_4) \subseteq K(\alpha_1, \alpha_2)\,.$$

Da den modsatte inklusion er triviel, fås således $M = K(\alpha_1, \alpha_2)$. Da rødderne til $(\star)$ ligger i K, gælder specielt:

$$\alpha_1 + \alpha_2 \in K \quad \text{og} \quad \alpha_1\alpha_2 \in K\,.$$

Da $(x - \alpha_1)(x - \alpha_2)$ således har koefficienter i K, fås

$$[M : K] = [K(\alpha_1, \alpha_2) : K] \leq 2\,.$$

Nu er $m = [K : \mathbb{Q}] = 2$ og $[M : K] \leq 2$, hvorfor $[M : \mathbb{Q}] \leq 4$, hvilket som tidligere nævnt medfører, at $\mathrm{Gr}(M/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$, □

Vi har altså nu en systematisk metode til at bestemme Galoisgruppen for et fjerdegradspolynomium. Undertiden kan følgende være nyttig:

Opgave 7.1. Lad $f(X)$ være et fjerdegradspolynomium i $\mathbb{Q}[X]$. Vis, at $f(X)$ er irreducibelt i $\mathbb{Q}[X]$, hvis hverken $f(X)$ eller den kubiske resolvent har rationale rødder.

Lad os nu betragte det "bikvadratiske" tilfælde:

$$f(X) = X^4 + bX^2 + d\,.$$

Hertil først et kriterium for, at $f(X)$ er irreducibelt.

Sætning 7.3. *Lad $f(X) = X^4 + bX^2 + d \in \mathbb{Q}[X]$ have rødderne $\pm\alpha$, $\pm\beta$. Da er følgende betingelser ækvivalente:*

(i) *$f(X)$ er irreducibelt i $\mathbb{Q}[X]$.*
(ii) *$\alpha^2 \notin \mathbb{Q}$ og ingen af tallene $\alpha \pm \beta$ ligger i $\mathbb{Q}$.*
(iii) *$b^2 - 4d \notin \mathbb{Q}^2$ og $-b \pm 2\sqrt{d} \notin \mathbb{Q}^2$.*

Bevis. Vi bemærker først, at $f(X) = X^4 + bX^2 + d$ kan skrives

$$f(X) = (X - \alpha)(X + \alpha)(X - \beta)(X + \beta) = (X^2 - \alpha^2)(X^2 - \beta^2) = X^4 - (\alpha^2 + \beta^2)X^2 + \alpha^2\beta^2\,,$$

dvs. $\alpha^2 + \beta^2 = -b \in \mathbb{Q}$, og $(\alpha\beta)^2 = d$.

Vi viser sætningen i kontraponeret form. *Antag $f(X)$ er reducibelt i $\mathbb{Q}[X]$.* Da må $f(X)$ enten have en førstegradsfaktor i $\mathbb{Q}[X]$ eller en andengradsfaktor i $\mathbb{Q}[X]$. I det første tilfælde må α eller β ligge i $\mathbb{Q}$. Dermed må α^2 eller β^2 ligge i $\mathbb{Q}$. Da $\alpha^2 + \beta^2 = -b \in \mathbb{Q}$, må specielt $\alpha^2 \in \mathbb{Q}$. I det andet tilfælde må et af polynomierne

$$(1) \quad (X - \alpha)(X + \alpha) \qquad (2) \quad (X - \alpha)(X - \beta) \qquad (3) \quad (X - \alpha)(X + \beta)$$

have koefficienter i $\mathbb{Q}$.

- I tilfældet (1) vil $\alpha^2 \in \mathbb{Q}$.
- I tilfældet (2) vil $\alpha + \beta \in \mathbb{Q}$.
- I tilfældet (3) vil $\alpha - \beta \in \mathbb{Q}$.

Antag nu at $\alpha^2, \alpha+\beta$ eller $\alpha-\beta$ ligger i $\mathbb{Q}$. Da er $f(X)$ reducibelt i $\mathbb{Q}[X]$. Thi:

- $\alpha^2 \in \mathbb{Q} \implies X^2-\alpha^2$ er en faktor i $\mathbb{Q}[X]$ til $f(X)$.
- $\alpha+\beta \in \mathbb{Q} \implies \alpha\beta = \frac{(\alpha+\beta)^2-(\alpha^2+\beta^2)}{2} = \frac{(\alpha+\beta)^2+b}{2} \in \mathbb{Q} \implies (X-\alpha)(X-\beta)$ er en faktor i $\mathbb{Q}[X]$ til $f(X)$.
- $\alpha-\beta \in \mathbb{Q} \implies \alpha\beta = \frac{(\alpha-\beta)^2-(\alpha^2+\beta^2)}{-2} = \frac{(\alpha-\beta)^2+b}{-2} \in \mathbb{Q} \implies (X-\alpha)(X+\beta)$ er en faktor i $\mathbb{Q}[X]$ til $f(X)$.

Beviset for sætningen afsluttes nu ved at bemærke:

- $\alpha^2 \in \mathbb{Q} \iff \alpha^2 = \frac{-b\pm\sqrt{b^2-4d}}{2} \in \mathbb{Q} \iff b^2-4d \in \mathbb{Q}^2$.
- $\alpha\pm\beta \in \mathbb{Q} \iff (\alpha\pm\beta)^2 \in \mathbb{Q}^2 \iff \alpha^2+\beta^2 \pm 2\alpha\beta \in \mathbb{Q}^2 \iff -b \pm 2\sqrt{d} \in \mathbb{Q}^2$.

□

Sætning 7.4. *Lad $f(X) = X^4+bX^2+d$ være irreducibelt i $\mathbb{Q}[X]$. Da gælder for $\mathrm{Gr}(M/\mathbb{Q})$, hvor M er spaltningslegemet for $f(X)$ over $\mathbb{Q}$.*

1. $d \in \mathbb{Q}^2 \implies \mathrm{Gr}(M/\mathbb{Q}) \simeq V_4$.
2. $d \notin \mathbb{Q}^2$, *men* $d(b^2-4d) \in \mathbb{Q}^2 \implies \mathrm{Gr}(M/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$.
3. $d \notin \mathbb{Q}^2$, *og* $d(b^2-4d) \notin \mathbb{Q}^2 \implies \mathrm{Gr}(M/\mathbb{Q}) \simeq D_4$.

Bevis. Den kubiske resolvent bliver

$$g(y) = y^3-by^2-4dy+4bd = (y-b)(y^2-4d)\,.$$

Hvis $d \in \mathbb{Q}^2$, er $g(y)$ et produkt af førstegradsfaktorer i $\mathbb{Q}[X]$ hvorfor $m=1$, og dermed (Sætning 7.1) $\mathrm{Gr}(M/\mathbb{Q}) \simeq V_4$.

Hvis $d \notin \mathbb{Q}^2$ er $m=2$, og vi får brug for Sætning 7.2. Vi skal betragte polynomierne

$$X^2-bX+d \quad \text{og} \quad X^2+0\cdot X+0 = X^2\,.$$

Det sidste polynomium har naturligvis rødder i K. Det første polynomium har rødder i K netop når

$$\sqrt{b^2-4d} \in K\,.$$

Nu er $K = \mathbb{Q}(\sqrt{\beta^2-4\delta}) = \mathbb{Q}(\sqrt{16d}) = \mathbb{Q}(\sqrt{d})$. Da $f(X)$ er irreducibelt, er $b^2-4d \notin \mathbb{Q}^2$ ifølge Sætning 7.3. Ifølge Sætning 7.2 er $\mathrm{Gr}(M/\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$ eller D_4 alt efter om enten $\sqrt{b^2-4d} \in \mathbb{Q}(\sqrt{d})$ eller ikke. Ifølge en opgave i 3AL, er $\mathbb{Q}(\sqrt{b^2-4d}) = \mathbb{Q}(\sqrt{d}) \iff d(b^2-4d) \in \mathbb{Q}^2$. Altså er $\mathrm{Gr}(M/\mathbb{Q}) = \mathbb{Z}/4\mathbb{Z}$ netop når $d(b^2-4d) \in \mathbb{Q}^2$.

Vi giver nu en anvendelse.

Sætning 7.5. *Lad $q \in \mathbb{Q}$, $q \notin \mathbb{Q}^2$. Da er $\mathbb{Q}(\sqrt{q})$ indeholdt i en normal udvidelse $N/\mathbb{Q}$ med $\mathbb{Z}/4\mathbb{Z}$ som Galoisgruppe, netop når q er en sum af to kvadrater.*

Bevis. Antag først $\mathbb{Q}(\sqrt{q}) \subset N$, $\mathrm{Gr}(N/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$. Det eneste (ægte) mellemlegeme mellem $\mathbb{Q}$ og N er $\mathbb{Q}(\sqrt{q})$. Da $[N:\mathbb{Q}(\sqrt{q})] = 2$ findes rationale tal q_1 og q_2, så

$$N = \mathbb{Q}(\sqrt{q}, \sqrt{q_1+q_2\sqrt{q}})\,.$$

Da $\mathbb{Q}(\sqrt{q})$ er eneste ægte dellegeme af N, må $N = \mathbb{Q}(\sqrt{q_1 + q_2\sqrt{q}})$, og N er da spaltningslegeme over $\mathbb{Q}$ for $\mathrm{Irr}(\sqrt{q_1 + q_2\sqrt{q}}, \mathbb{Q})$, der må have grad 4. Nu er $\sqrt{q_1 + q_2\sqrt{q}}$ rod i

$$X^4 - 2q_1X^2 + (q_1^2 - q_2^2 q)\,,$$

der altså må være irreducibelt i $\mathbb{Q}[X]$.

Da $\mathrm{Gr}(N/\mathbb{Q})$ *ikke* er V_4. er (ifølge Sætning 7.4) $q_1^2 - q_2^2 q \notin \mathbb{Q}^2$, hvorfor $q_2 \neq 0$. Da $\mathrm{Gr}(N/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ er (ifølge Sætning 7.4)

$$(q_1^2 - q_2^2 q)(4q_1^2 - 4(q_1^2 - q_2^2 q)) \in \mathbb{Q}^2\,,$$

dvs.

$$(q_1^2 - q_2^2 q)4q_2^2 q \in \mathbb{Q}^2\,.$$

Da må $q_1 \neq 0$.

Lad os nu skrive $(q_1^2 - q_2^2 q)4q_2^2 q = r^2$ for passende $r \in \mathbb{Q}$. Følgelig er $q = \frac{(2qq_2^2)^2 + r^2}{(2q_1q_2)^2}$, der er sum af to kvadrater i $\mathbb{Q}$.

Antag omvendt, at q er en sum af to kvadrater i $\mathbb{Q}$:

$$q = q_1^2 + q_2^2\,.$$

Da er polynomiet $f(X) = X^4 - 2qX^2 + q_1^2 q$ irreducibelt i $\mathbb{Q}[X]$. Dette vises ved hjælp af Sætning 7.3:

$$4q^2 - 4q_1^2 q = 4q(q - q_1^2) = 4qq_2^2 \notin \mathbb{Q}^2\,,$$

da $q \notin \mathbb{Q}^2$, og endvidere er

$$2q \pm 2\sqrt{q_1^2 q} = 2q \pm 2q_1\sqrt{q} \notin \mathbb{Q}^2 \ \ (\text{endda} \notin \mathbb{Q})\,.$$

Rødderne til $f(X)$ kan skrives $\pm\alpha$, $\pm\beta$, så

$$f(X) = (X - \alpha)(X + \alpha)(X - \beta)(X + \beta)\,.$$

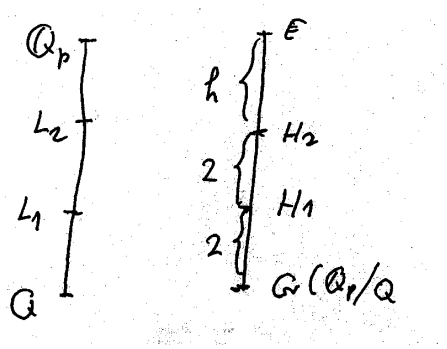
Konstantleddet er $\alpha^2\beta^2 = q_1^2 q$, dvs. $\frac{\alpha\beta}{q_1} = \pm\sqrt{q}$, hvorfor $\sqrt{q}$ ligger i spaltningslegemet $M = \mathbb{Q}(\alpha, \beta)$ for $f(X)$ over $\mathbb{Q}$. For at bestemme $\mathrm{Gr}(M/\mathbb{Q})$, benyttes Sætning 7.4. Konstantleddet $q_1^2 q \notin \mathbb{Q}^2$, hvor $\mathrm{Gr}(M/\mathbb{Q})$ *ikke* er $\simeq V_4$. Endvidere er

$$q_1^2 q(4q^2 - 4q_1^2 q) = 4q_1^2 q^2(q - q_1^2) = 4q_1^2 q^2 q_2^2 \in \mathbb{Q}^2\,,$$

hvorfor $\mathrm{Gr}(M/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$.

Eksempel 7.6. 3 er ikke sum af to kvadrater i $\mathbb{Q}$, hvorfor $\mathbb{Q}(\sqrt{3})$ *ikke* er indeholdt i en normal udvidelse af $\mathbb{Q}$ med $\mathbb{Z}/4\mathbb{Z}$ som Galoisgruppe. Derimod er $\sqrt{5} = \sqrt{1^2 + 2^2}$ indeholdt i en sådan udvidelse (f.eks. $\mathbb{Q}_5 = \mathbb{Q}(e^{\frac{2\pi i}{5}})$).

Eksempel 7.7. Lad p være en primtal $\equiv 1(4)$. Da er $\mathbb{Q}_p/\mathbb{Q}$ normal, og $\mathrm{Gr}(\mathbb{Q}_p/\mathbb{Q}) \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. Vi kan skrive $p = 1+4h$, $h \in \mathbb{Z}$. Til enhver divisor d i $4h$ findes netop én undergruppe i $\mathbb{Z}/(p-1)\mathbb{Z} = \mathbb{Z}/4h\mathbb{Z}$ af indeks d. Specielt findes netop én undergruppe H_1 af indeks 2 og netop én undergruppe H_2 af indeks 4. Vi har følgende diagram:



Altså findes netop ét dellegeme L_1 (nemlig $F(H_1)$) af dimension 2 over $\mathbb{Q}$, og netop ét dellegeme L_2 (nemlig $F(H_2)$), der har dimension 2 over L_1 og $\mathrm{Gr}(L_2/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$. Ifølge et eksempel i Mat 3AL p.4.7 (2000-udgave), er $L_1 = \mathbb{Q}(\sqrt{p})$. Altså kan $\mathbb{Q}(\sqrt{p})$ indlejres i en $(\mathbb{Z}/4\mathbb{Z})$-udvidelse. Ifølge Sætning 7.5 er p altså sum af to kvadrater af rationale tal. (En rent talteoretisk sætning!)

8 Generiske/parametriske $\mathbb{Z}/3\mathbb{Z}$–polynomier

Polynomiet $f_a(X) = X^3 - aX^2 + (a-3)X + 1$ er "parametrisk" for $\mathbb{Z}/3\mathbb{Z}$-udvidelse over $\mathbb{Q}$. Dvs.:

Sætning 8.1. *Lad M være spaltningslegeme for $f_a(X)$ over $\mathbb{Q}$, hvor a er et rationalt tal.*

1. *For ethvert $a \in \mathbb{Q}$ er $\mathrm{Gr}(M/\mathbb{Q})$ enten triviel eller $\mathbb{Z}/3\mathbb{Z}$.*
2. *Enhver $\mathbb{Z}/3\mathbb{Z}$-udvidelse af $\mathbb{Q}$ er spaltningslegeme over $\mathbb{Q}$ for $f_a(X)$ for passende $a \in \mathbb{Q}$.*

Bevis. (1) følger af, at $\mathrm{Disk}(f_a(X)) = (a^2 - 3a + 9)^2$ (jf. Sætning 12A i kap. III Mat 3AL).

(2): Lad $M/\mathbb{Q}$ være normal med $\mathrm{Gr}(M/\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$. Lad $\alpha \in M \setminus \mathbb{Q}$ og $\mathrm{Gr}(M/\mathbb{Q}) = \{e, \sigma, \sigma^2\}$. Da er α, $\sigma\alpha$ og $\sigma\alpha^2$ indbyrdes forskellige. Sæt $\beta = \frac{\alpha - \sigma^2\alpha}{\alpha - \sigma\alpha}$; da er $\sigma\beta = \frac{\sigma\alpha - \alpha}{\sigma\alpha - \sigma^2\alpha} = \frac{1}{1-\beta}$; $\sigma^2\beta = \frac{1}{1-\sigma\beta} = \frac{1}{1-\frac{1}{1-\beta}} = 1 - \frac{1}{\beta}$. $f(X) = (X-\beta)(X-\sigma\beta)(X-\sigma^2\beta)$ får rationale koefficienter, idet

$$f(X) = X^3 - (\beta + \sigma\beta + \sigma^2\beta)X^2 + (\beta\sigma\beta + \beta\sigma^2\beta + (\sigma\beta)(\sigma^2\beta))X - \beta(\sigma\beta)(\sigma^2\beta)\,.$$

Sæt $a = \beta + \sigma\beta + \sigma^2\beta$. Da viser udregning, at $\beta\sigma\beta + \beta\sigma^2\beta + (\sigma\beta)(\sigma^2\beta) = a - 3$, og $\beta(\sigma\beta)(\sigma^2\beta) = -1$. Her må $\sigma\beta$ være forskellig fra β, da β ellers var rational, og dermed ville $\sigma\beta = \frac{1}{1-\beta} = \beta$; men $X^2 - X + 1$ har ingen rationale rødder.

Altså er $M = \mathbb{Q}(\beta)$ og $\mathrm{Irr}(\beta, \mathbb{Q})$ bliver

$$X^3 - (\beta + \sigma\beta + \sigma^2\beta)X^2 + (\beta\sigma\beta + \beta\sigma^2\beta + (\sigma\beta)(\sigma^2\beta))X + 1 = f_a(X)\,,$$

for $a = \beta + \sigma\beta + \sigma^2\beta$. Altså er M spaltningslegeme for $f_a(X)$ over $\mathbb{Q}$. □

9 Lineære grupper

Lad K være et legeme. For vilkårlige elementer a og $b \in K$, $a \neq 0$, vil afbildningen fra K til K defineret ved

$$\sigma(x) = ax + b$$

være bijektiv. Når a og b gennemløber alle elementer i $K\backslash\{0\}$ og K, vil disse afbildninger udgøre en gruppe kaldet $\mathrm{Aff}(K,1)$, "den affine gruppe af dimension 1 over K".

Mængden $T = \{x \to x + c | c \in K\}$ af "translationer" udgør en (med $(K,+)$ isomorf) abelsk undergruppe i $\mathrm{Aff}(K,1)$. Der gælder $T \triangleleft \mathrm{Aff}(K,1)$; thi hvis $\sigma \in \mathrm{Aff}(K,1)$, $\sigma(x) = ax + b$, $a \neq 0$, da er $\sigma^{-1}(x) = \frac{x}{a} - \frac{b}{a}$ og $\sigma\tau\sigma^{-1} \in T$, idet $\sigma\tau\sigma^{-1}(x) = x + ac$ for $\tau = (x \to x + c)$. Endvidere er $\mathrm{Aff}(K,1)$ en opløselig gruppe, da T er en abelsk normaldeler i $\mathrm{Aff}(K,1)$ og faktorgruppen er isomorf med den multiplikative gruppe af de fra 0 forskellige elementer i K og dermed abelsk.

Lad os nu betragte tilfældet hvor K er det endelige legeme $\mathbb{F}_p$, p et primtal. Da er $\mathrm{Aff}(\mathbb{F}_p,1)$, som vi for kortheds skyld betegner L_p, en opløselig gruppe af orden $p(p-1)$. L_p bliver undergruppe i S_p, idet vi opfatter S_p som gruppen af permutationer af de p restklasser $\bar{0}, \bar{1}, \ldots, \overline{p-1}$ i $\mathbb{F}_p$.

Det ses let, at L_p er en transitiv undergruppe i S_p.

Lemma 9.1. *Lad G være en transitiv undergruppe i S_p, og $N \triangleleft G$. Hvis $N \neq E$, da er N transitiv.*

Bevis. S_p er mængden af permutationer af $\bar{0}, \bar{1}, \ldots, \overline{p-1}$. Vi definerer $a \sim b$, $a, b \in \mathbb{F}_p$, hvis $\exists \nu \in N : \nu a = b$. Relationen $\sim$ er en ækvivalensrelation, da N er en undergruppe i S_p. Endvidere gælder $a \sim b \implies \sigma a \sim \sigma b$; thi $a \sim b \implies \exists \nu \in N : \nu a = b$; da $N \triangleleft G$, vil $\sigma\nu\sigma^{-1} \in N$. Nu er $\sigma\nu\sigma^{-1}(\sigma a) = \sigma\nu a = \sigma b$.

Heraf sluttes, at alle ækvivalensklasser har samme elementantal. (Jf. bevis Mat 3AL, Lemma kap.5 p.11-12, [Alg3, Chap.5. Lemma 5.23]). Altså

$p =$ (antallet af ækvivalensklasser)·(det fælles elementantal i ækvivalensklasserne).

Da $N \neq E$ er sidste faktor > 1. Idet p er et primtal, bliver sidste faktor $= p$, dvs. alle elementer i $\mathbb{F}_p$ er ækvivalente, dvs. N er transitiv. □

Vi er nu i stand til at vise:

Sætning 9.2. *Lad G være en transitiv undergruppe i S_p. Da er G opløselig $\iff \exists \mu \in S_p : \mu G \mu^{-1} \subseteq L_p$ (dvs. G er konjugeret med en undergruppe i L_p).*

Bevis. "$\Leftarrow$" klar.

"$\Rightarrow$". Lad $G \triangleright \cdots \triangleright G_{s-1} \triangleright G_s = \{e\}$ være en kompositionsrække. Da er $|G_{s-1}|$ et primtal. På grund af ovenstående lemma er G_{s-1} transitiv, hvorfor $p \mid |G_{s-1}|$. Dette indebærer, at $|G_{s-1}| = p$.

G_{s-1} er derfor cyklisk og frembragt af en p-cykel, f.eks. $\rho = \left(\begin{smallmatrix} a_0 & a_1 & \cdots & a_{p-1} \\ a_1 & a_2 & \cdots & a_0 \end{smallmatrix}\right)$.

Lad μ være permutationen $\begin{pmatrix} a_0 & a_1 & \cdots & a_{p-1} \\ \bar{0} & \bar{1} & \cdots & \overline{p-1} \end{pmatrix}$. Da gælder

$$\mu G_{s-1}\mu^{-1} \text{ er frembragt af } p\text{-cyklen } \begin{pmatrix} \bar{0} & \bar{1} & \cdots & \overline{p-1} \\ \bar{1} & \bar{2} & \cdots & \bar{0} \end{pmatrix}.$$

Sidstnævnte kan betragtes som translationen $x \to x+\bar{1}$. Sætningen fås da ved successive anvendelser af nedenstående lemma. □

Lemma 9.3. *Lad $G \subseteq S_p$, $N \lhd G$, $N \subseteq L_p$, og antag N indeholder translationen $\tau(x) = x + 1$, $x \in \mathbb{F}_p$. Da vil $G \subseteq L_p$.*

Bevis. Lad σ være et vilkårligt element i G. Da N er normaldeler i G , ligger $\sigma\tau\sigma^{-1}$ i N, og da τ har orden p vil også $\sigma\tau\sigma^{-1}$ have orden p. Da $|L_p| = p(p-1)$ findes der ifølge Sylows 3. sætning, netop én p-Sylowgruppe i L_p, og derfor også kun én p-Sylowgruppe i N. Dvs. elementerne $\tau, \tau^2, \ldots, \tau^{p-1}$ er de eneste elementer i N som har orden p. Altså må $\sigma\tau\sigma^{-1} = \tau^a$, $1 \leq a \leq p-1$.

Nu er $\sigma\tau = \tau^a\sigma$.

$$\begin{aligned} \sigma(y+1) &= \sigma\tau(y) = \tau^a\sigma(y) = \sigma(y) + a \ \forall y \in \mathbb{F}_p \\ \sigma(y+2) &= \sigma(y+1) + a = \sigma(y) + 2a \\ \sigma(y+3) &= \sigma(y) + 3a \\ \sigma(y+x) &= \sigma(y) + xa \ \forall y \in \mathbb{F}_p \\ \sigma(x) &= \sigma(0) + ax \text{ i.e. } \sigma \in L_p\,. \end{aligned}$$

□

Lemma 9.4. *Lad A være den af en p-cykel frembragte undergruppe i S_p. Da er A sin egen centralisator i S_p (centralisatoren er defineret i Mat 3AL side 1.39 [Alg3, Chap1, Def.1.88]).*

Bevis. Da A er abelsk, må $C_A \supseteq A$. Åbenbart er $|A| = p$. Vi betragter nu følgende undergruppe $C_A^{(1)}$ i C_A defineret ved $C_A^{(1)} = \{\sigma \in C_A | \sigma(1) = 1\}$; vi påstår, at denne undergruppe har orden 1. Lad nemlig σ være et element i $C_A^{(1)}$. Da må for alle $\rho \in A$ gælde, at $\rho\sigma = \sigma\rho$ og dermed $\rho\sigma(1) = \sigma\rho(1)$. Da $\sigma(1) = 1$, er $\rho(1) = \sigma\rho(1)$ for alle $\rho \in A$. Da A er frembragt af en p-cykel, er A transitiv, hvorfor σ er identiteten. $C_A^{(1)}$ får derfor orden 1. Nu er C_A transitiv, da den indeholder A og derfor er $[C_A : C_A^{(1)}] = p$.

Altså har C_A orden p, hvorfor $C_A = A$. □

Hovedsætning 9.1. *Lad G være en transitiv undergruppe i S_p, p primtal. Da er følgende betingelser ækvivalente:*

1. *G har netop én p-Sylowgruppe.*
2. *G er opløselig.*
3. *G er konjugeret med en undergruppe i L_p.*
4. *Enhver permutation ($\neq E$) i G har højst ét fixpunkt.*
5. *$|G| = p \cdot l$, hvor $l \mid (p-1)$.*

Bevis. $1 \implies 2 \implies 3 \implies 4 \implies 1$, dernæst $3 \implies 5$ og $5 \implies 1$.

$\underline{1 \implies 2}$ Da G er transitiv, må $p \mid |G|$. Da $|G| \mid p(p-1)(p-2)\ldots 2\cdot 1$ og $p^2 \nmid p!$, fås $p^2 \nmid |G|$. Den entydigt bestemte p-Sylowgruppe A i G er derfor cyklisk af orden p.

Da A er den eneste p-Sylowgruppe, er normalisatoren $N_A = G$. Ifølge ovenstående lemma er $C_A = A$. Derfor er G/A isomorf med en undergruppe i $\mathrm{Aut}(A)$, (jf. Mat 3AL s.1.38). $\mathrm{Aut}(A)$ er cyklisk af orden $p-1$, hvorfor G/A er cyklisk, og $E \triangleleft A \triangleleft G$ er en normalrække med abelske (endda cykliske) faktorer. Altså er G opløselig.

$\underline{2 \implies 3}$ Dette fås af sætning 9.2.

$\underline{3 \implies 4}$ Direkte verifikation.

$\underline{4 \implies 1}$ Vi antager altså, at enhver fra identiteten forskellig permutation i G højst har ét fixpunkt. Vi betragter stabilitetsgruppen $G^{(0)}$ i 0, dvs. $G^{(0)} = \{\sigma \in G \mid \sigma(0) = 0\}$. Da G er transitiv, er $[G : G^{(0)}] = p$. På grund af antagelsen 4 har de fra identiteten forskellige permutationer i $G^{(0)}$ ingen fixpunkter bortset fra 0. Følgelig vil forskellige permutationer i $G^{(0)}$ føre 1 over i forskellige elementer, hvorfor $|G^{(0)}| \leq p-1$. Altså er $|G| \leq p(p-1)$.

Da $p \mid |G|$ må $|G| = p \cdot l$, hvor $l \leq p-1$. Ifølge Sylows 3. sætning, bliver antallet af p-Sylowgrupper netop én.

$\underline{3 \implies 5}$ Når G er konjugeret med en undergruppe i L_p, må ordenen af G gå op i $|L_p| = p(p-1)$. Da p er divisor i ordenen af G, kan vi for et passende hele tal k og l skrive: $p(p-1) = |G| \cdot k = p \cdot l \cdot k$. Altså er $|G| = p \cdot l$, hvor l er en divisor i $p-1$.

$\underline{5 \implies 1}$ Følger af Sylows 3. sætning.

Hovedsætningen er hermed bevist. □

9.1 Eksempler og opgaver

Opgave 9.1. Vis, at L_p er dobbelt transitiv.

Opgave 9.2. Vis (ved brug af Lemma 9.3), at L_p er sin egen normalisator i S_p.

Opgave 9.3. Vis, at en dobbelt transitiv undergruppe i S_p har en orden, der er delelig med $p(p-1)$.

Opgave 9.4. Vis (vha. hovedsætningen), at en opløselig dobbelt-transitiv undergruppe i S_p (p primtal), er konjugeret med L_p.

I forbindelse med Opgave 9.4 kan nævnes en berømt (og dybtliggende) sætning af Burnside: *Enhver transitiv undergruppe i S_p (p primtal), der <u>ikke</u> er opløselig, er dobbelt transitiv,*

Ved brug af Galoisteoriens hovedsætning og Sætning 12 Kapitel III i 3AL[Alg3 Theorem 3.40] fås:

Sætning 9.5. *Lad $f(X)$ være et irreducibelt polynomium i $\mathbb{Q}[X]$ af primtalsgrad p. Lad $\alpha_1, \alpha_2, \ldots, \alpha_p$ være rødderne i $f(X)$, og lad M være spaltningslegeme for $f(X)$ over $\mathbb{Q}$. Da er følgende betingelser ækvivalente:*

1. *$f(X)$ er opløselig ved rodtegn.*
2. *$\mathrm{Gr}(M/\mathbb{Q})$ er opløselig.*
3. *$\forall (i,j)$, $i \neq j$, $1 \leq i,j \leq p$ er $M = \mathbb{Q}(\alpha_i, \alpha_j)$.*
4. *$\exists (i,j)$, $i \neq j$, $1 \leq i,j \leq p$ så $M = \mathbb{Q}(\alpha_i, \alpha_j)$.*

Bevis. $\underline{1 \iff 2}$ er hovedsætningen i 3AL Kapitel V s.5.6.[Alg3. Theorem 5.16]

$\underline{2 \implies 3}$ $\mathrm{Gr}(M/\mathbb{Q})$ opfattes som en permutation

$$\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_p \\ \sigma\alpha_1 & \sigma\alpha_2 & \cdots & \sigma\alpha_p \end{pmatrix}.$$

Ifølge Hovedsætningen (udsagn 4) på side 21 i dette afsnit, vil $\sigma \in \mathrm{Gr}(M/\mathbb{Q})$, $\sigma \neq e$ højst holde ét af α'erne fast, dvs. hvis $\alpha_i \neq \alpha_j$ og $\sigma(\alpha_i) = \alpha_i$, $\sigma(\alpha_j) = \alpha_j$, da er $\sigma = \mathrm{Id}$, eller ifølge Galoisteoriens hovedsætning, $T(\mathbb{Q}(\alpha_i, \alpha_j)) = E$, hvorfor $\mathbb{Q}(\alpha_i, \alpha_j) = M$.

$\underline{3 \implies 4}$ er triviel.

$\underline{4 \implies 1}$ Antag der findes to rødder α_i, α_j så $M = \mathbb{Q}(\alpha_i, \alpha_j)$,

$$[\mathbb{Q}(\alpha_i) : \mathbb{Q}] = \mathrm{Grad}(\mathrm{Irr}(\alpha_i, \mathbb{Q})) = \mathrm{Grad}(f(X)) = p\,,$$

så

$$[\mathbb{Q}(\alpha_i, \alpha_j) : \mathbb{Q}] = [\mathbb{Q}(\alpha_i, \alpha_j) : \mathbb{Q}(\alpha_i)] \cdot [\mathbb{Q}(\alpha_i) : \mathbb{Q}] = \mathrm{Grad}(\mathrm{Irr}(\alpha_j, \mathbb{Q}(\alpha_i))) \cdot p\,.$$

Da $\mathrm{Grad}(\mathrm{Irr}(\alpha_j, \mathbb{Q}(\alpha_i))) \leq p-1$, og $|\mathrm{Gr}(M/\mathbb{Q})|$ er delelig med p, er $|\mathrm{Gr}(M/\mathbb{Q})| = p \cdot l$, hvor $l \leq p-1$.

ALtså har $\mathrm{Gr}(M/\mathbb{Q})$ ifølge Sylows 3. sætning netop én p-Sylowgruppe. Da $\mathrm{Gr}(M/\mathbb{Q})$ desuden er en transitiv undergruppe i S_p (ifølge Sætning 12 Kapitel III i 3AL[Alg3. Theorem 3.40]), medfører hovedsætningen (udsagn 1) på side 21 i dette afsnit, at $\mathrm{Gr}(M/\mathbb{Q})$ er opløselig. □

Korollar 9.6. *Lad $f(X)$ være et irreducibelt polynomium i $\mathbb{Q}[X]$ af primtalsgrad p. Lad t være antallet af reelle rødder til $f(X)$. Hvis $1 < t < p$, er $f(X)$ ikke opløselig ved rodtegn.*

Eksempel 9.7. $f(X) = X^7 - 7X + 3$ er irreducibelt i $\mathbb{Q}[X]$ (Eisenstein på $f(X+4)$). $f(X)$ har netop 3 reelle rødder, og er derfor ikke opløselig ved rodtegn.

Tilføjelse til Hovedsætning side 21 i dette afsnit:

Til enhver divisor l i $(p-1)$, hvor p er et primtal, findes én – og pånær konjugering – kun én transitiv undergruppe i S_p af orden $p \cdot l$.

Bevis. På grund af Hovedsætningen er det nok at vise, at L_p har netop én undergruppe af orden $p \cdot l$. Undergruppen $T = \{(x \to x+a) | a \in \mathbb{F}_p\}$ er en normal-deler i L_p af orden p, og $L_p/T \simeq (\mathbb{F}_p \setminus \{0\}, \cdot)$, der er cyklisk af orden $p-1$. Til enhver divisor l i $(p-1)$ findes derfor netop én undergruppe i $(\mathbb{F}_p \setminus \{0\}, \cdot)$ af orden l.

Ved Noethers 2. isomorfisætning anvendt på

$$\begin{array}{ccccc} L_p & & \bullet & \longrightarrow & \bullet & & (\mathbb{F}_p \setminus \{0\}, \cdot) \\ \\ T & & \bullet & \longrightarrow & \bullet & & \{e\} \end{array}$$

ses derfor, at der findes én undergruppe i L_p, der indeholder T og har orden $p \cdot l$.

Beviset afsluttes nu ved at bemærke, at T er den eneste undergruppe i L_p af orden p. □

Definition 9.8. Den ovenfor indførte – pånær konjugering entydigt bestemte – undergruppe i S_p af orden $p \cdot l$, kaldes *Frobeniusgruppen*, og betegnes F_{pl}. Bemærk, at $F_{2p} = D_p$ (diedergruppen af orden $2p$).

Angående antallet af undergrupper, der er konjugerede med F_{pl} viser vi

Sætning 9.9. *Lad $F_{pl} \subseteq L_p \subseteq S_p$. Da er L_p normalisatoren af F_{pl} i S_p. Specielt findes netop $(p-2)!$ med F_{pl} konjugerede undergrupper i S_p.*

Bevis. Åbenbart er $F_{pl} \lhd L_p$, dvs. normalisatoren indeholder L_p. Ved anvendelse af Lemma 9.3 med $G =$ normalisatoren af F_{pl} i S_p og $N = F_{pl}$ ses, at normalisatoren er indeholdt i L_p, og dermed eksakt $= L_p$.

Som nævnt i 3AL Kapitel I s.32[Alg3, Theorem 1.91], er antallet af med F_{pl} konjugerede undergrupper i S_p lig $[S_p : L_p] = \frac{p!}{p(p-1)} = (p-2)!$ □

Eksempel 9.10. Lad p være et ulige primtal, og lad M være spaltningslegeme for $X^p - 2$ over $\mathbb{Q}$. Da er $[M : \mathbb{Q}] = p(p-1)$.

$\mathrm{Gr}(M/\mathbb{Q})$ er da en transitiv opløselig undergruppe i S_p (jf. Hovedsætning i 3AL vedrørende opløselighed ved rodtegn). Den må være isomorf med L_p, eller med ovenstående notation Frobeniusgruppen $F_{p(p-1)}$.

9.2 En gruppeteoretisk anvendelse

I Mat 3AL, Kapitel I [Alg3.Chap. 1]) blev vist, at en gruppe af orden pq er opløselig, hvis p og q er primtal. Hvis p og q

er forskellige primtal så $p \not\equiv 1 \pmod{q}$ og $q \not\equiv 1 \pmod{p}$, blev det vist, at F endda må være cyklisk.

Vi viser nu

Sætning 9.11. *Lad p og q være primtal så $p \equiv 1 \pmod{q}$. Da findes netop to grupper af orden pq: den cykliske $\mathbb{Z}/pq\mathbb{Z}$, og en ikke-abelsk, Frobeniusgruppen F_{pq}.*

Bevis. Eksistensen af de to grupper er klar (jf. tilføjelse til Hovedsætning s.2). Vi skal derfor blot vise, at der højst findes én ikke-abelsk gruppe af orden pq.

Da $|G| = pq$, hvor $q \mid p-1$, findes ifølge Sylows 3. sætning, netop én p-Sylowgruppe i G. Hvis G også kun havde én q-Sylowgruppe, måtte både p-Sylowgruppen og q-Sylowgruppen være normaldelere i G. G ville da være det direkte produkt af en cyklisk gruppe af orden p og en cyklisk gruppe af orden q, og dermed selv cyklisk. Altså findes en undergruppe Q i G, så $|Q| = q$ og Q *ikke* er normaldeler i G.

Vi betragter nu afbildningen $\rho : G \to S_p$ (som angivet i 3AL s.18 Kapitel I eller i afsnittet angående $\mathrm{Aut}(S_n)$ etc.), svarende til $H = Q$, dvs.

$$G = g_1Q \cup g_2Q \cup \cdots \cup g_pQ\,,$$

og for $g \in G$, er

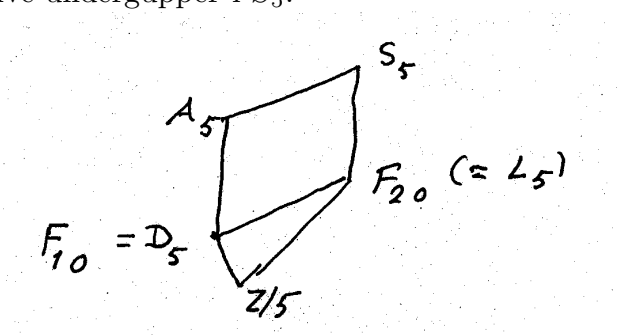
$$\rho(g) = \begin{pmatrix} g_1Q & g_2Q & \cdots & g_pQ \\ gg_1Q & gg_2Q & \cdots & gg_pQ \end{pmatrix}.$$

Billedet ρG er en transitiv undergruppe i S_p og $\ker(\rho) \lhd G$, $\ker(\rho) \subseteq Q$; da $|Q|$ er et primtal og $Q \not\lhd G$, må $\ker(\rho) = \{e\}$. ρ er altså injektiv, og G derfor isomorf med en

transitiv, opløselig undergruppe i S_p. Derfor er G isomorf med Frobeniusgruppen F_{pq}. □

Vi afslutter dette afsnit med en oversigt over *samtlige* transitive (ikke blot opløselige) undergrupper i S_p for $p = 5, 7, 11$ (angivet pånær isomorfi).

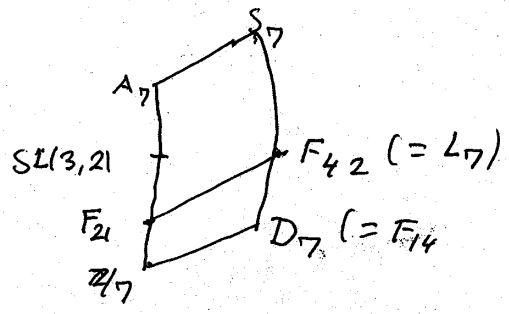
$\underline{p = 5}$ Hvis en transitiv undergruppe i S_5 ikke er opløselig, må den have orden mindst 60. Men de eneste undergupper i S_5 af orden ≤ 60, er A_5 og S_5. Altså er konjugeretklasserne af de transitive undergupper i S_5:



(Bemærk, at F_{20} indeholder en ulige permutation, mens alle permutationer i $F_{10} = D_5$ er lige).

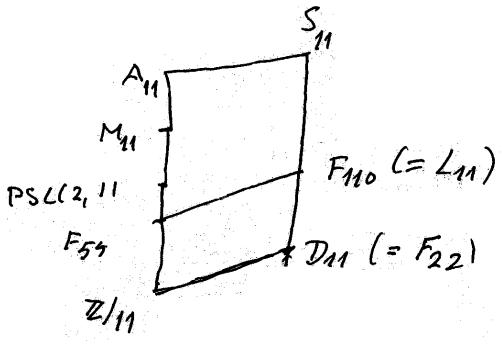
Mens A_5 er "selvkonjugeret", er der (jf. Sætning 9.9 i dette afsnit) $(5-2)! = 6$ med F_{20} konjugerede undergrupper, 6 med D_5 konjugerede undergrupper, og 6 med $\mathbb{Z}/5\mathbb{Z}$ konjugerede undergrupper indenfor S_5.

$\underline{p = 7}$ Konjugeretklasserne af de transitive undergrupper i S_7 er:



Her er $SL(3, 2)$ gruppen af alle (3×3)-matricer med elementer i legemet $\mathbb{F}_2$ (med 2 elementer), og determinant 1. Denne gruppe er simpel, og har orden 168.

$\underline{p = 11}$



M_{11} betegner den skarpt 4-transitive permutationsgruppe i S_{11}, *Mathieugruppen* M_{11}, (der er simpel). $SL(2,11)$ er gruppen af alle (2×2)-matricer over $\mathbb{F}_{11}$ med determinant 1. $PSL(2,11) = SL(2,11)/\text{centret}$. $PSL(2,11)$ er også simpel. $|M_{11}| = 7920$, $|PSL(2,11)| = 660$.

10 Supplement til lineære grupper
(Arbejdstitel)

Sætning 10.1. *Lad G være en transitiv undergruppe i S_p. Da er følgende betingelser ækvivalente:*

1. *G er opløselig.*
2. *G er konjugeret med en undergruppe i* $\mathrm{Aff}(1,\mathbb{F}_p)$.
3. *Alle ikke-trivielle permutationer i G har højst ét fixpunkt.*
4. *$|G| = p\cdot l$, $l|p-1$.*

Definition 10.2. G som ovenfor, kaldes Frobeniusgruppen $F_{p,l}$.

Definition 10.3. Lad $f(X)$ være irreducibel i $\mathbb{Q}[X]$ af primtalsgrad $p \geq 5$. Lad $\alpha_1,\ldots,\alpha_p$ være rødderne til $f(X)$. Da er

$$P_{\binom{p}{k}}(X) := \prod_{i_1<\cdots<i_k} [X - (\alpha_{i_1}+\cdots+\alpha_{i_k})] \in \mathbb{Q}[X]\,, \quad 2\leq k\leq p-1\,.$$

Sætning 10.4. $\mathrm{Gr}(f) = D_p$ *eller* $\mathbb{Z}/p$ *hvis og kun hvis* $P_{\binom{p}{2}}$ *er et produkt af* $\frac{p-1}{2}$ *irreducible* p^{te}*gradspolynomier i* $\mathbb{Q}[X]$.

Sætning 10.5. *Lad $f(X)$ være et irreducibelt polynomium i $\mathbb{Q}[X]$ af grad 7. Da gælder:*

1. $\mathrm{Gr}(f) = S_7$ *eller* $A_7 \iff P_{35}$ *er irreducibelt i* $\mathbb{Q}[X]$.
2. $\mathrm{Gr}(f) = PSL(2,7) \iff P_{35}$ *er et produkt af 2 irreducible polynomier af grad hhv.* 7 *og* 28.
3. $\mathrm{Gr}(f) = F_{42} \iff P_{35}$ *er produkt af 2 irreducible polynomier af grad hhv.* 14 *og* 21.
4. $\mathrm{Gr}(f) = F_{21} \iff P_{35}$ *er produkt af 3 irreducible polynomier af grad hhv.* 7, 7 *og* 21.
5. $\mathrm{Gr}(f) = D_7 \iff P_{35}$ *er produkt af 4 irreducible polynomier af grad hhv.* 14, 7, 7 *og* 7.
6. $\mathrm{Gr}(f) = \mathbb{Z}/7 \iff P_{35}$ *er produkt af 5 irreducible 7.gradspolynomier.*

Eksempel 10.6. For $f(X) = X^5 + aX + b$ er

$$P_{10}(X) = X^{10} - 3aX^6 - 11bX^5 - 4a^2X^2 + 4abX - b^2\,.$$

For $a=-5$, $b=12$ bliver

$$P_{10}(X) = (X^5 - 5X^3 - 10X^2 + 30X - 36)(X^5 + 5X^3 + 10X^2 + 10X + 4)\,.$$

Lad p være et primtal, og $f(X)$ irreducibel i $\mathbb{Q}[X]$ med rødderne $\alpha_1, \ldots, \alpha_p$. Da har

$$P_{\frac{p(p-1)}{2}} = \prod_{i<j} [X - (\alpha_i + \alpha_j)], \quad \text{og}$$
$$P_{\frac{p(p-1)(p-2)}{6}} = \prod_{i<j<k} [X - (\alpha_i + \alpha_j + \alpha_k)]$$

simple rødder.

Sætning 10.7. *For $f(X) = X^5 + aX + b$ er*

$$P_{10}(X) = X^{10} - 3aX^6 - 11bX^5 - 4a^2X^2 + 4abX - b^2 .$$

For $f(X) = X^7 + aX + b$ er

$$\begin{aligned} P_{21}(X) =& X^{21} - 25aX^{15} - 57bX^{14} - 53a^2X^9 - 30abX^8 \\ & - 289b^2X^7 - 27a^3X^3 + 27a^2X^2 - 9ab^2X + b^3 , \end{aligned}$$

og

$$\begin{aligned} P_{35}(X) =& X^{35} + 40aX^{29} + 302bX^{28} - 1614a^2X^{23} + 2706abX^{22} \\ & + 3828b^2X^{21} - 5072a^3X^{17} + 2778a^2X^{16} - 1808ab^2X^{15} \\ & + 3625b^3X^{14} - 5147a^4X^{11} - 1354a^3X^{10} - 21192a^2b^2X^9 \\ & - 2632ab^3X^8 - 7309b^4X^7 - 1728a^5X^5 - 1728a^4bX^4 \\ & + 720a^3X^3 + 928a^2b^2X^2 - 64ab^4X - 128b^5 . \end{aligned}$$

Sætning 10.8. *Lad $f(X)$ være et irreducibelt polynomium i $\mathbb{Q}[X]$ af primtalsgrad p. Da er $\mathrm{Gr}(f) = D_p$ eller $\mathbb{Z}/p$ hvis og kun hvis $P_{\frac{p(p-1}{2}}$ er produkt af $\frac{p-1}{2}$ irreducible p^{te}gradspolynomier i $\mathbb{Q}[X]$.*

Bemærkning 10.9. Et polynomium med Mathieugruppen M_{11} som Galoisgruppe over $\mathbb{Q}$ er ifølge Matzat:

$$\begin{aligned} & X^{11} + 21X^{10} + 183X^9 + 4263 \cdot 5^{-1}X^8 + 56874 \cdot 5^{-2}X^7 + 86034 \cdot 5^{-2}X^6 \\ & + 345606 \cdot 5^{-3}X^5 + 870726 \cdot 5^{-4}X^4 + 5160633 \cdot 5^{-5}X^3 + 6971469 \cdot 5^{-5}X^2 \\ & - 11160261 \cdot 5^{-8}X - 531441 \cdot 5^{-8} . \end{aligned}$$

Sætning 10.10. *Lad $f(X)$ være et irreducibelt plynomium i $\mathbb{Q}[X]$ af primtalsgrad $p > 11$. Da er $\mathrm{Gr}(f)$ opløselig hvis og kun hvis enten $P_{\frac{p(p-1)}{2}}$ er reducibel i $\mathbb{Q}[X]$, eller $P_{\frac{p(p-1)(p-2)}{6}}$ er produkt af mindst 3 irreducible polynomier i $\mathbb{Q}[X]$.*

Beviset er ikke trivielt.

11 Resolventer for 5$^{\text{te}}$gradspolynomier

Lad S_5 være den symmetriske gruppe af grad 5 bestående af alle permutationer af 0 1 2 3 4. Den lineære undergruppe L_5 er frembragt af $\sigma : \left(\begin{smallmatrix} 0&1&2&3&4\\ 1&2&3&4&0 \end{smallmatrix}\right)$ og $\tau : \left(\begin{smallmatrix} 0&1&2&3&4\\ 0&2&4&1&3 \end{smallmatrix}\right)$. (Dvs. skrevet i $\mathbb{Z}/5\mathbb{Z}$ er $\sigma(x) = x + \bar{1}$ og $\tau(x) = \bar{2}x$). L_5 har orden 20, og der findes 6 med L_5 konjugerede undergrupper indenfor S_5 (idet L_5 som vist i en opgave, er lig sin egen normalisator i S_5). L_5 indeholder netop én undergruppe af orden 10, nemlig diedergruppen D_5. D_5 er frembragt af σ og τ^2; D_5 består af de drejninger og spejlinger, der fører en regulær femkant over i sig selv. Som tidligere vist gælder:

> *Enhver transitiv opløselig undergruppe S_5 er indeholdt i en med L_5 konjugeret undergruppe i S_5.*

Åbenbart er $[S_5 : L_5] = [A_5 : D_5] = 6$, og der findes et fælles repræsentantsystem for de respektive højresideklasser:

$$\begin{aligned} A_5 &= D_5 \cup (012)D_5 \cup (021)D_5 \cup (014)D_5 \cup (041)D_5 \cup (023)D_5 \\ S_5 &= L_5 \cup (012)L_5 \cup (021)L_5 \cup (014)L_5 \cup (041)L_5 \cup (023)L_5 \,. \end{aligned}$$

Vi betragter nu det generelle 5^{te}gradspolynomium

$$\begin{aligned} f(T) &= (T - X_0)(T - X_1)(T - X_2)(T - X_3)(T - X_4) \\ &= T^5 + a_1T^4 + a_2T^3 + a_3T^2 + a_4T + a_5 \,. \end{aligned}$$

Lad

$$u = \underbrace{\underbrace{X_0X_1 + X_1X_2 + X_2X_3 + X_3X_4 + X_4X_0}_{v} \underbrace{- X_0X_2 - X_2X_4 - X_1X_4 - X_1X_3 - X_0X_3}_{-\tau v}}_{\text{invariant overfor } D_5} \underbrace{\qquad\qquad}_{\text{invariant overfor } D_5} .$$

Altså er $u_0 = u$ invariant overfor D_5. A_5 opererer på $\mathbb{Q}[X_0, X_1, X_2, X_3, X_4]$. Mængden $\{A_5u\}$ omfatter følgende 6 polynomier: $u_0 = u$; $u_1 = (012)u$; $u_2 = (021)u$; $u_3 = (014)u$; $u_4 = (041)u$; $u_5 = (023)u$. En udregning viser:

$$\begin{aligned} u_0 &= X_0X_1 + X_1X_2 + X_2X_3 + X_3X_4 + X_4X_0 - X_0X_2 - X_2X_4 - X_1X_4 - X_1X_3 - X_0X_3 \\ u_1 &= X_1X_2 + X_0X_2 + X_0X_3 + X_3X_4 + X_1X_4 - X_0X_1 - X_0X_4 - X_4X_2 - X_2X_3 - X_1X_3 \\ u_2 &= X_0X_2 + X_0X_1 + X_1X_3 + X_3X_4 + X_2X_4 - X_1X_2 - X_1X_4 - X_0X_4 - X_0X_3 - X_2X_3 \\ u_3 &= X_1X_4 + X_2X_4 + X_2X_3 + X_0X_3 + X_0X_1 - X_1X_2 - X_0X_2 - X_0X_4 - X_3X_4 - X_1X_3 \\ u_4 &= X_0X_4 + X_0X_2 + X_2X_3 + X_1X_3 + X_1X_4 - X_2X_4 - X_1X_2 - X_0X_1 - X_0X_3 - X_3X_4 \\ u_5 &= X_1X_2 + X_1X_3 + X_0X_3 + X_0X_4 + X_2X_4 - X_2X_3 - X_3X_4 - X_1X_4 - X_0X_1 - X_0X_2 \end{aligned}$$

Endvidere gælder:

(i)

$$\begin{aligned} \tau u_0 &= -u_0 \\ \tau u_1 &= -u_1 \\ \tau u_2 &= -u_3 \\ \tau u_3 &= -u_5 \\ \tau u_4 &= -u_2 \\ \tau u_5 &= -u_4 \end{aligned}$$

(ii) Til enhver lige permutation af $X_0, \ldots, X_4$ svarer en permutation af $u_0, \ldots, u_5$.
(iii) A_5 opererer transitivt på $u_0, \ldots, u_5$.
(iv) S_5 opererer transitivt på $u_0^2, \ldots, u_5^2$.
(v) u_0^2 er invariant overfor L_5. (Der gælder mere præcist $\mathrm{Stab}_{S_5}(u_0^2) = L_5$).

Nu er L_5 sin egen normalisator i S_5 (hvorfor?); følgelig er $\rho L_5 \rho^{-1}$ ($\rho = E$, (012), (021), (014), (041) eller (023)) de 6 med L_5 konjugerede undergrupper i S_5. For enhver transitiv opløselig undergruppe H i S_5 findes derfor et u_i ($0 \leq i \leq 5$), så u_i^2 er invariant overfor H.

Vi betragter nu polynomiet

$$\begin{aligned} F(Y) &= (Y-u_0)(Y-u_1)(Y-u_2)(Y-u_3)(Y-u_4)(Y-u_5) \\ &\in \mathbb{Q}[X_0, X_1, X_2, X_3, X_4][Y]\,. \end{aligned}$$

$F(Y)$ er invariant overfor alle lige permutationer af $X_0, \ldots, X_4$. Derfor er koefficienterne $B_1, \ldots, B_6$ i

$$F(Y) = Y^6 + B_1 Y^5 + B_2 Y^4 + B_3 Y^3 + B_4 Y^2 + B_5 Y + B_6$$

invariante overfor A_5. Endvidere gælder for $\tau = \left(\begin{smallmatrix} 0&1&2&3&4 \\ 0&2&4&1&3 \end{smallmatrix}\right)$, at

$$\begin{aligned} \tau F(Y) &= (Y+u_0)(Y+u_1)(Y+u_2)(Y+u_3)(Y+u_4)(Y+u_5) \\ &= Y^6 - B_1 Y^5 + B_2 Y^4 - B_3 Y^3 + B_4 Y^2 - B_5 Y + B_6\,. \end{aligned}$$

Heraf sluttes, at

$$B_2, B_4 \text{ og } B_6 \text{ er symmetriske i } X_0, \ldots, X_4\,,$$

og

$$B_1, B_3 \text{ og } B_5 \text{ er skævsymmetriske i } X_0, \ldots, X_4\,.$$

Ifølge Sætning 1.6 i afsnittet om symmetriske polynomier, er B_1, B_3 og B_5 derfor multipla af

$$\Delta = \prod_{0 \leq j < i \leq 4} (X_i - X_j)$$

indenfor $\mathbb{Q}[X_0, \ldots, X_4]$. Da B_1, B_3 og Δ er homogene polynomier i $X_0, \ldots, X_4$ af grad hhv. 2, 6 og 10 ($= \binom{5}{2}$)), er $B_1 = B_3 = 0$.

Da B_5 er homogent i $X_0, \ldots, X_4$ af grad 10, må $B_5 = k \cdot \Delta$, $k \in K$. k kan bestemmes ved for $X_0, \ldots, X_4$ at indsætte komplekse tal $\alpha_0, \ldots, \alpha_4$, for hvilke $\prod_{0 \leq j < i \leq 4}(\alpha_i - \alpha_j) \neq 0$, f.eks. rødderne i polynomiet $X^5 - X$. Man finder da $B_5 = -32 \cdot \Delta$. Da B_2, B_4 og B_6 er homogene i $X_0, \ldots, X_4$ af grad hhv. 4, 8 og 12, findes konstanter l, m og $n \in K$, så

$$\begin{aligned} B_2 &= l \cdot a_4 \ \ + \text{polynomium, hvori } a_1, a_2 \text{ eller } a_3 \text{ indgår} \\ B_4 &= m \cdot a_4^2 + \text{polynomium, hvori } a_1, a_2 \text{ eller } a_3 \text{ indgår} \\ B_6 &= n \cdot a_4^3 \ + \text{polynomium, hvori } \alpha_1, \alpha_2 \text{ eller } \alpha_3 \text{ indgår}\,. \end{aligned}$$

Ved indsættelse af talværdier som ovenfor fås:

$$l = -20, \quad m = 240 \text{ og } n = 320\,.$$

Polynomiet $F(Y)\cdot F(-Y)=\prod_{i=0}^{5}(Y^2-u_i^2)$ er invariant overfor S_5, dvs. koefficienterne er symmetriske polynomier i $X_0,\ldots,X_4$, hvorfor $F(Y)\cdot F(-Y)\in\mathbb{Q}[a_0,\ldots,a_4][Y]$. Mere eksplicit fås:

$$\begin{aligned}F(Y)\cdot F(-Y)&=(Y^6+B_2Y^4+B_4Y^2+B_6)^2-32^2\Delta^2Y^2\\&=(Y^6+B_2Y^4+B_4Y^2+B_6)^2-32^2dY^2\,,\end{aligned}$$

hvor $d=\Delta^2$ er diskriminanten for det (generelle) 5^{te}gradspolynomium. Det kan være praktisk at betragte polynomiet $G(Z)=(Z^3+B_2Z^2+B_4Z+B_6)^2-32^2dZ$, der har rødderne $u_0^2,u_1^2,\ldots,u_5^2$.

B_2, B_4 og B_6 er visse heltalspolynomier i $a_1,\ldots,a_5$, som kan bestemmes eksplicit. (Vi vil senere foretage en sådan bestemmelse i et specialtilfælde).

Lad nu $b_1,\ldots,b_5$ være rationale tal, og $\beta_0,\beta_1,\beta_2,\beta_3,\beta_4$ rødderne (indenfor $\mathbb{C}$) til polynomiet $X^5+b_1X^4+b_2X^3+b_3X^2+b_4X+b_5$. Hvis vi lader B_2, B_4 og B_6 være de rationale tal som fås ved for a_i at indsætte b_i, $1\le i\le 5$, vil

$$(Z^3+B_2Z^2+B_4Z+B_6)^2-1024dZ=(Z-(\beta_0\beta_1+\cdots+\beta_4\beta_0-\beta_0\beta_2-\cdots-\beta_0\beta_3)^2(\ldots)\ldots,$$

hvor faktorerne på højre side fås ved i udtrykkene for $u_0^2,\ldots,u_5^2$ at indsætte $X_0=\beta_0,\ldots,X_4=\beta_4$, og d er diskriminanten for $X^5+b_1X^4+b_2X^3+b_3X^2+b_4X+b_5$.

Vi er nu i stand til at formulere og bevise

Sætning 11.1. *Lad $f(X)=X^5+b_1X^4+b_2X^3+b_3X^2+b_4X+b_5$ være et irreducibelt polynomium i $\mathbb{Q}[X]$ med spaltningslegeme $M=\mathbb{Q}(\beta_0,\beta_1,\beta_3,\beta_3,\beta_4)$. Da gælder $f(X)$ opløselig ved rodtegn (dvs. $\mathrm{Gr}(M/\mathbb{Q})$ er opløselig) hvis og kun hvis $G(Z)=(Z^3+B_2Z^2+B_4Z+B_6)^2-1024dZ$ har en rational rod. (Her betegner B_2,B_4 og B_6 de tal man får ved for a_1 at indsætte b_1, for a_2 at indsætte b_2 , etc.)*

Bevis. "kun hvis": Lad $f(X)$ være opløselig ved rodtegn. $\mathrm{Gr}(M/\mathbb{Q})$ er da en transitiv opløselig undergruppe i S_5. Ifølge tidligere bemærkning, findes et i, $0\le i\le 5$, så $u_i^2(\beta_0,\ldots,\beta_4)$ er invariant overfor $\mathrm{Gr}(M/\mathbb{Q})$. Det betyder, at $u_i^2(\beta_0,\ldots,\beta_4)$ som er rod i $G(Z)$, er rational.

"hvis": Lad $\mathrm{Gr}(M/\mathbb{Q})$ være ikke-opløselig. Da må $\mathrm{Gr}(M/\mathbb{Q})$ være isomorf med A_5 eller S_5 (hvorfor?) Som tidligere nævnt opererer såvel A_5 som S_5 transitivt på $u_0^2,\ldots,u_5^2$. Dette indebærer, at en eventuel rational rod α til $G(Z)$ måtte have multiplicitet 6, dvs.

$$(Z^3+B_2Z^2+B_4Z+B_6)^2-1024dZ=(Z-\alpha)^6\,,$$

eller

$$((Z^3+B_2Z^2+B_4Z+B_6)+(Z-\alpha)^3)((Z^3+B_2Z^2+B_4Z+B_6)-(Z-\alpha)^3)=1024dZ\,,$$

hvilket er umuligt, da diskriminanten d for f er et fra 0 forskelligt rationalt tal. ($f(X)$ har ingen multiple rødder). Hermed er sætningen bevist. □

Vi udregner nu $G(Z)$ eksplicit i det tilfælde, hvor $b_1=b_2=b_3=0$, i.e. $f(X)$ har formen $X^5+aX+b\in\mathbb{Q}[X]$. Med henblik på udregninger af konstanterne l, m og n fås let:

$$G(Z)=(Z^3-20aZ^2+240a^2Z+320a^3)^2-1024dZ\,,$$

hvor $d=4^4a^5+5^5b^4$ (jf. tidligere udregning). $G(Z)$ kan omskrives:

$$\widetilde{G}(Z)=\frac{G(4Z)}{4^6}=(Z^2-6aZ+25a^2)(Z-a)^4-5^5b^4Z\,.$$

Vi får herved:

Sætning 11.2. *Lad a og b være rationale tal så $f(X) = X^5 + aX + b$ er et irreducibelt polynomium i $\mathbb{Q}[X]$. Da er $f(X)$ opløselig ved rodtegn hvis og kun hvis $\widetilde{G}(Z) = (Z^2 - 6aZ + 25a^2)(Z-a)^4 - 5^5 b^4 Z$ har en rational rod.*

Idet polynomiet $f(X) = X^5 + aX + b$ højst kan have 3 reelle rødder (hvorfor?), kan Galoisgruppen for $f(X)$'s spaltningslegeme over $\mathbb{Q}$ ikke være cyklisk. Dette medfører følgende eksplicitte kriterium:

Sætning 11.3. *Lad a og b være rationale tal så $f(X) = X^5 + aX + b$ er et irreducibelt polynomium i $\mathbb{Q}[X]$. Lad $d = 4^4 a^5 + 5^5 b^4$ være diskriminanten. Da gælder for spaltningslegemet M for $f(X)$ over $\mathbb{Q}$:*

$\widetilde{G}(Z)$ har rat.rod.	$d \in \mathbb{Q}^2$	$\mathrm{Gr}(M/\mathbb{Q})$
$+$	$+$	D_5
$+$	$-$	L_5
$-$	$+$	A_5
$-$	$-$	S_5

Eksempel 11.4. $f(X) = x^5 - 5X + 12$. $\widetilde{G}(Z) = (Z^2 + 30Z + 625)(Z+5)^4 - 5^5 12^4 Z$ har den rationale rod 25, og $d = (2^6 5^3)^2$, i.e. $\mathrm{Gr}(M/\mathbb{Q}) \simeq D_5$.

Eksempel 11.5. $f(X) = X^5 + 15X + 12$, $\mathrm{Gr}(M/\mathbb{Q}) \simeq L_5$.

Eksempel 11.6. $f(X) = X^5 + 20X + 16$, $\mathrm{Gr}(M/\mathbb{Q}) \simeq A_5$. (Disk $= 2^{16}5^6$).

Eksempel 11.7. $f(X) = X^5 - X + 1$, $\mathrm{Gr}(M/\mathbb{Q}) \simeq S_5$.

Vi giver nu sluttelig en parametrisering af de irreducible 5^{te}gradspolynomier $X^5 + aX + b$, der er opløselige ved rodtegn. Vi antager $a \neq 0$. Hvis w er en rational rod til $\widetilde{G}(Z)$, kan vi bestemme to rationale tal λ, μ således, at

$$w = a\lambda\,, \quad b = a\mu\,.$$

Dette giver følgende betingelse for a:

$$(a\lambda - a)^4(a^2\lambda^2 - 6a^2\lambda + 25a^2) - 3125a^5\lambda\mu^4 = 0\,,$$

hvoraf:

Sætning 11.8. *Lad $f(X) = X^5 + aX + b$ være et irreducibelt polynomium i $\mathbb{Q}[X]$. Da er (for $a \neq 0$), $f(X)$ opløselig ved rodtegn hvis og kun hvis*

$$a = \frac{3125\lambda\mu^4}{(\lambda-1)^4(\lambda^2 - 6\lambda + 25)} \quad \text{og} \quad b = \frac{3125\lambda\mu^5}{(\lambda-1)(\lambda^2 - 6\lambda + 25)}\,,$$

hvor λ og μ er rationale tal forskellige fra 0.

Eksempel 11.9. $\lambda = -5$ og $\mu = -\frac{12}{5}$ giver $X^5 - 5X + 12$.

12 Mathieugrupperne

Vi betragter undergrupper i S_{11}, S_{12}, S_{22}, S_{23} og S_{24}. Lad

$$A = (1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11)$$
$$B = (5\,6\,4\,10)(11\,8\,3\,7)$$
$$C = (1\,12)(2\,11)(3\,6)(4\,8)(5\,9)(7\,10)$$

Mathieugruppen M_{12} er defineret som undergruppen i S_{12} frembragt af A, B og C, dvs. $M = \langle A, B, C\rangle$. M_{12} har orden $12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 = 95040$, den er simpel, og er 5-dobbelt transitiv i S_{12}.

M_{11} er defineret som undergruppen i S_{11} frembragt af A og B, dvs. $M_{11} = \langle A, B\rangle$. Den har orden $11 \cdot 10 \cdot 9 \cdot 8 = 7920$, den er simpel, og er 4-dobbelt transitiv i S_{11}.

Lad

$$D = (1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11\,12\,13\,14\,15\,16\,17\,18\,19\,20\,21\,22\,23)$$
$$E = (3\,17\,10\,7\,9)(5\,4\,13\,14\,19)(11\,12\,23\,8\,18)(21\,16\,15\,20\,22)$$
$$F = (1\,24)(2\,23)(3\,12)(4\,16)(5\,18)(6\,10)(7\,20)(8\,14)(9\,21)(11\,17)(13\,22)(19\,15)$$

Da er $M_{23} := \langle D, E, F\rangle$ og $M_{23} := \langle D, E\rangle$. $|M_{24}| = 24 \cdot 23 \cdot 22 \cdot 20 \cdot 16 \cdot 3$, og $|M_{23}| = 23 \cdot 22 \cdot 21 \cdot 20 \cdot 16 \cdot 3$. M_{24} er 5-dobbelt transitiv i S_{24}, og M_{23} er 4-dobbelt transitiv i S_{23}. M_{24} og M_{23} er simple.

Lad

$$G = (1\,2\,2\,4\,5\,6\,7\,8\,9\,10\,11\,12\,13\,14\,15\,16\,17\,18\,19\,20\,21\,22)$$
$$H = (1\,4\,5\,9\,3)(2\,8\,10\,7\,6)(12\,15\,16\,20\,14)(13\,14\,21\,18\,17)$$
$$I = (11\,22)(1\,21)(2\,10\,8\,6)(12\,14\,16\,20)(4\,7\,3\,13)(5\,19\,9\,18)$$

Da er $M_{22} := \langle G, H, I\rangle$ (indenfor S_{22}). M_{22} har orden $22 \cdot 21 \cdot 20 \cdot 16 \cdot 3$, den er 3-dobbelt transitiv og simpel.

Bortset fra de symmetriske og alternerende grupper, er M_{12} og M_{24} de eneste 5-dobbelt transitive permutationsgrupper. Bortset fra de symmetriske og alternerende grupper og M_{12} og M_{24} er M_{11} og M_{23} de eneste 4-dobbelt transitive permutationsgrupper. (Beviset herfor beror på klassifikationen af de endelige simple grupper!)

13 Kroneckers metode til eksplicit bestemmelse af Galoisgrupper og anvendelser heraf

Først et par hjælpesætninger:

Lemma 13.1. *For et ethvert legeme K er K algebraisk afsluttet i $K(X_1, \ldots, X_n)$, dvs.*

$$\xi \in K(X_1, \ldots, X_n)\,,\ \xi \text{ algebraisk over } K \implies \xi \in K\,.$$

Bevis. Polynomiumsringen $K[X_1,\ldots,X_n]$ er UFD (jf. Mat 3AL '99 Sætning 6, p.2.4 [Alg3 Theorem 2.34]). Et element $\xi \in K(X_1,\ldots,X_n)$ kan skrives $\xi = \frac{p}{q}$, hvor p og q er indbyrdes primiske polynomier i $K[X_1,\ldots,X_n]$. Hvis ξ er algebraisk over K, findes elementer $a_1,\ldots,a_m \in K$, så

$$\left(\frac{p}{q}\right)^m + a_1\left(\frac{p}{q}\right)^{m-1} + \cdots + a_m = 0\,,$$

og dermed

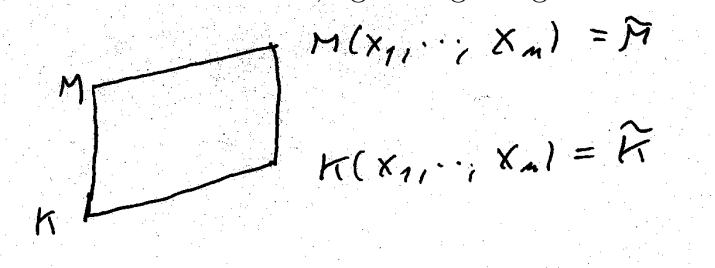
$$p^m + a_1 p^{m-1}q + \cdots + a_m q^m = 0\,.$$

Altså vil $q|p^m$. Da $K[X_1,\ldots,X_n]$ er UFD, og p og q er indbyrdes primiske, må q være invertibel i $K[X_1,\ldots,X_n]$, dvs. $q \in K$.

Analogt fås, at $p|q^m a_m$. Da q^m og a_m tilhører K, må også p tilhøre K, hvorfor $\xi = \frac{p}{q} \in K$. □

Lad nu $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$ være et polynomium i $K[X]$, og antag at $f(X)$ har lutter simple rødder $\alpha_1,\ldots,\alpha_n$ i sit spaltningslegeme $M = K(\alpha_1,\ldots,\alpha_n)$.

Lad $X_1,\ldots,X_n$ være variable over K, og betragt diagrammet



Ifølge Lemma 13.1 er $M \cap \widetilde{K} = K$, hvorfor translationssætningen (jf. Mat 3AL '99 p.3.12 [Alg3. Theorem 3.46]) indebærer, at $\mathrm{Gr}(M/K) \simeq \mathrm{Gr}(\widetilde{M}/\widetilde{K})$.

Endvidere gælder $\widetilde{M} = \widetilde{K}(\alpha_1X_1 + \cdots + \alpha_nX_n)$. (Øvelsesopgave 69 i Mat 3AL).

Vi betragter nu polynomiet

$$W(f;X,X_1,\ldots,X_n) = \prod_{\sigma\in S_n}\Big[X - \sum_{i=1}^{n}\alpha_i X_{\sigma(i)}\Big]\,.$$

På grund af Hovedsætningen om symmetriske polynomier (Sætning 1.3), er

$$W(f;X,X_1,\ldots,X_n) = X^{n!} + \sum_{i,i_1,\ldots,i_n} h_{i,i_1,\ldots,i_n}(a_1,\ldots,a_n)X^iX_1^{i_1}\ldots X_n^{i_n}\,,$$

hvor $h_{i,i_1,\ldots,i_n}$ er et (universelt) heltalspolynomium i $a_1,\ldots,a_n$.

S_n opererer på naturlig vis på ringen $K(\alpha_1,\ldots,\alpha_n)[X,X_1,\ldots,X_n]$ ved permutation af de variable $X_1,\ldots,X_n$.

Åbenbart er $W(f;X,X_1,\ldots,X_n) \in K[X,X_1,\ldots,X_n]$, og W er normeret mht. X.

Vi skriver Wf som produkt af irreducible polynomier i $K[X,X_1,\ldots,X_n]$

$$Wf = g_1\ldots g_s\,,$$

hvor hvert g_i kan antages normeret mht. X.

Ved Sætning 4 i Mat 3AL p.2.2 [Alg3. Theorem 2.31] generaliseret til polynomier over UFD ses, at hvert g_i er irreducibelt i $\widetilde{K}[X] = K(X_1, \ldots, X_n)[X]$.

S_n opererer transitivt på $g_1, \ldots, g_s$, derfor er stabilitetsgrupperne

$$\mathrm{Stab}(g_i) = \{\rho \in S_n | \rho g_i = g_i\}$$

indbyrdes konjugerede i S_n.

$\mathrm{Gr}(M/K) = \mathrm{Gr}(\widetilde{M}/\widetilde{K})$ kan opfattes som en undergruppe i S_n. Her gælder

Sætning 13.2. $\mathrm{Gr}(M/K)$ *opfattet på sædvanlig vis som undergruppe i* S_n*, er isomorf med de indbyrdes konjugerede grupper* $\mathrm{Stab}(g_i)$*.*

Bevis. Lad g_1 være den irreducible faktor i Wf, der indeholder den lineære faktor $(X - \alpha_1 X_1 - \alpha_2 X_2 - \cdots - \alpha_n X_n)$.

Da g_1 også er irreducibelt i $K(X_1, \ldots, X_n)[X]$, bliver

$$g_1 = \mathrm{Irr}(\alpha_1 X_1 + \cdots + \alpha_n X_n, K(X_1, \ldots, X_n)) \,.$$

Ifølge Mat 3AL '99 p.3.6 Sætning 7 (Vigtigt Lemma [Alg3. Lemma 3.4]), er derfor

$$g_1 = \prod_{\varphi \in \mathrm{Gr}(M/K)} [X - \varphi(\alpha_1 X_1 + \cdots + \alpha_n X_n)] \,.$$

Lad nu $\varphi(\alpha_i) = \alpha_{\overline{\varphi}(i)}$ for $1 \leq i \leq n$, hvor $\overline{\varphi} \in S_n$, og $\varphi \mapsto \overline{\varphi}$ er afbildningen $\mathrm{Gr}(M/K) \to S_n$. Åbenbart kan g_1 skrives

$$\begin{aligned} \prod_{\varphi \in \mathrm{Gr}(M/K)} \Big[X - \sum_{i=1}^{n} X_i \alpha_{\overline{\varphi}(i)}\Big] &= \prod_{\varphi \in \mathrm{Gr}(M/K)} \Big[X - \sum_{i=1}^{n} X_{\overline{\varphi}^{-1}(i)} \alpha_i\Big] \\ &= \prod_{\varphi \in \mathrm{Gr}(M/K)} \Big[X - \sum_{i=1}^{n} X_{\overline{\varphi}(i)} \alpha_i\Big] \,. \end{aligned}$$

Antag nu $\psi \in \mathrm{Gr}(M/K)$, og dermed $\overline{\psi} \in \mathrm{Im}(\mathrm{Gr}(M/K) \to S_n)$. Da er

$$\overline{\psi} g_1 = \prod_{\varphi \in \mathrm{Gr}(M/K)} \Big[X - \sum_{i=1}^{n} X_{\overline{\psi}\overline{\varphi}(i)} \alpha_i\Big] = \prod_{\varphi \in \mathrm{Gr}(M/K)} \Big[X - \sum_{i=1}^{n} X_{\overline{\varphi}(i)} \alpha_i\Big] = g_1 \,,$$

dvs. $\overline{\psi} \in \mathrm{Stab}(g_1)$.

Lad nu omvendt $\rho \in S_n$, $\rho \in \mathrm{Stab}(g_1)$. Da vi indenfor $M[X_1, \ldots, X_n, X]$ har $(X - \alpha_1 X_1 - \cdots - \alpha_n X_n) | g_1$ og $\rho g_1 = g_1$, vil der findes $\varphi \in \mathrm{Gr}(M/K)$, så $X - \sum_{i=1}^{n} X_{\overline{\varphi}(i)} \alpha_i = X - \sum_{i=1}^{n} X_{\rho(i)} \alpha_i$, dvs. $\overline{\varphi}(i) = \rho(i)$, $\forall i$, $i \leq i \leq n$, og dermed $\rho = \overline{\varphi} \in \mathrm{Im}(\mathrm{Gr}(M/K) \to S_n)$.

Altså er $\mathrm{Stab}(g_1) = \mathrm{Im}(\mathrm{Gr}(M/K) \to S_n)$. □

Vi skal senere bevise

Sætning 13.3. Hilberts Irreducibilitetssætning. *Lad*

$$f_i(X_1,\ldots,X_n;T_1,\ldots,T_m)\,,\quad 1\le i\le s\,,$$

være s irreducible polynomier i $\mathbb{Q}[X_1,\ldots,X_n;T_1,\ldots,T_m]$. Da findes uendeligt mange rationale talsæt $(\alpha_1,\ldots,\alpha_m)\in\mathbb{Q}^m$, for hvilket polynomierne $f_i(X_1,\ldots,X_n;\alpha_1,\ldots,\alpha_m)$ er irreducible (evt. konstanter) i $\mathbb{Q}[X_1,\ldots,X_n]$.

Modulo HIS (Hilberts Irreducibilitetssætning (13.3)), kan nu vises

Sætning 13.4. *Antag at en endelig gruppe G kan realiseres som Galoisgruppe for en endelig normal udvidelse af $\mathbb{Q}(T_1,\ldots,T_m)$; da kan G også realiseres som Galoisgruppe for en endelig normal udvidelse af $\mathbb{Q}$.*

Bevis. På grund af antagelsen, findes et irreducibelt polynomium f i

$$\mathbb{Q}(T_1,\ldots,T_m)[X]\,,$$

for hvilket Galoisgruppen for spaltningslegemet over $\mathbb{Q}(T_1,\ldots,T_m)$ er $\simeq G$. Vi kan antage, at $f=f(X;T_1,\ldots,T_m)\in\mathbb{Q}[X;T_1,\ldots,T_m]$, og at f er normeret mht. X (hvorfor?)

Da er $W(f)=Wf(X;X_1,\ldots,X_n;T_1,\ldots,T_m)\in\mathbb{Q}[X;X_1,\ldots,X_n;T_1,\ldots,T_m]$.

Lad $Wf(X;X_1,\ldots,X_n;T_1,\ldots,T_m)=\prod g_i(X;X_1,\ldots,X_n;T_1,\ldots,T_m)$ være produktfremstillingen af irreducible faktorer i $\mathbb{Q}[X;X_1,\ldots,X_n;T_1,\ldots,T_m]$.

Lad os betragte én af faktorerne $g_j(X;X_1,\ldots,X_n;T_1,\ldots,T_m)$.

Lad $(\alpha_1,\ldots,\alpha_m)\in\mathbb{Q}^m$, så $g_j(X;X_1,\ldots,X_n;\alpha_1,\ldots,\alpha_m)$ og $f(X;\alpha_1,\ldots,\alpha_m)$ er irreducible i $\mathbb{Q}[X;X_1,\ldots,X_n]$. Ifølge HIS (13.3) findes uendeligt mange sådanne talsæt. Da vil

$$\begin{aligned}&[Wf(X;X_1,\ldots,X_n;T_1,\ldots,T_m)]_{t_1\to\alpha_1,\ldots,t_m\to\alpha_m}\\&=Wf(X;X_1,\ldots,X_n;\alpha_1,\ldots,\alpha_m)\,,\end{aligned}$$

og $\mathrm{Stab}(g_j(X;X_1,\ldots,X_n;\alpha_1,\ldots,\alpha_m))=\mathrm{Stab}(g_j(X;X_1,\ldots,X_n;T_1,\ldots,T_m))$ taget under hensyn til S_n opererende via permutationer af $X_1,\ldots,X_n$.

Under hensyn til den tidligere viste Sætning 13.2 fås herved, at Galoisgruppen for spaltningslegemet over $\mathbb{Q}$ for $f(X;\alpha_1,\ldots,\alpha_m)$, er $\simeq G$. □

Korollar 13.4. *(Under forudsætning af* HIS *(13.3).) S_n, $n\ge 1$, er realiseret som Galoisgruppe for en endelig normal udvidelse af $\mathbb{Q}$.*

13.1 Bestemmelse af Galoisgrupper via reduktion mod p.

Lad $f(X) = X^n + a_1X^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ have lutter simple rødder $\alpha_1, \ldots, a_n$. Da er $Wf(X; X_1, \ldots, X_n) \in \mathbb{Z}[X; X_1, \ldots, X_n]$, og koefficienterne er heltalspolynomier i $a_1, \ldots, a_m$.

Lad $Wf = g_1 \ldots g_s$ være produktfremstillingen i irreducible polynomier i $\mathbb{Z}[X; X_1, \ldots, X_n]$. Da er $g_1, \ldots, g_s$ (if. Gauss' Lemma etc.) også irreducible i $\mathbb{Q}[X; X_1, \ldots, X_n]$.

Lad for $1 \leq j \leq s$, $G_j = \mathrm{Stab}(g_j) = \{\rho \in S_n | \rho g_j = g_j\}$. Da er G_j, $1 \leq j \leq s$, konjugerede undergrupper i S_n og isomorfe med Galoisgruppen for spaltningslegemet af f over $\mathbb{Q}$, idet denne Galoisgruppe opfattes som permutationsgruppe af rødderne $\alpha_1, \ldots, \alpha_n$.

Betragt nu $\bar{f}(X) = X^n + \bar{a}_1X^{n-1} + \cdots + \bar{a}_n \in \mathbb{Z}_p$, hvor p er et primtal der ikke går op i $\mathrm{Disk}(f)$. Der gælder, at $\overline{\mathrm{Disk}(f)} = \mathrm{Disk}(\overline{f})$ (hvorfor?) Derfor får $\bar{f}$ lutter simple rødder i spaltningslegemet over $\mathbb{Z}_p$. Lad disse være $\beta_1, \ldots, \beta_n$,

$$W\bar{f} = \prod_{\sigma \in S_n} \left[X - \sum_{i=1}^{n} \beta_i X_{\sigma(i)}\right] = \overline{Wf}\,.$$

Ud fra fremstillingen $Wf = g_1 \ldots g_s$ irreducible i $\mathbb{Z}[X; X_1, \ldots, X_n]$ fås da

$$W\bar{f} = \bar{g}_1 \ldots \bar{g}_s \ \text{ i } \ \mathbb{Z}_p[X; X_1, \ldots, X_n]\,,$$

med $\bar{g}_1, \ldots, \bar{g}_s$ ikke nødvendigvis irreducible i $\mathbb{Z}_p[X; X_1, \ldots, X_n]$.

Hertil gælder

$$G_1 = \{\rho \in S_n | \rho g_1 = g_1\} = \{\rho \in S_n | \rho \bar{g}_1 = \bar{g}_1\}\,.$$

("$\subseteq$" triviel; "$\supseteq$" kræver en lille overvejelse).

Lad $\bar{g}_1 = \bar{g}_{11}, \ldots, \bar{g}_{1\nu}$ være spaltning af $\bar{g}_1$ i irreducible faktorer i $\mathbb{Z}_p[X; X_1, \ldots, X_n]$.

Lad $\mathcal{G}_{11} = \{\rho \in S_n | \rho \bar{g}_{11} = \bar{g}_{11}\}$.

Da er $\mathcal{G}_{11} \subseteq G_1$; thi antag $\rho \in \mathcal{G}_{11}$, $\rho \notin G_1$, da ville $\rho g_1 = g_j$, $(j \geq 2)$.

Idet $\bar{g}_{11} \,|\, \bar{g}_1$ indenfor $\mathbb{Z}_p[X; X_1, \ldots, X_n]$, ville hermed

$$g_{11} = \rho\bar{g}_{11} \,|\, \rho\bar{g}_1 = \bar{g}_j\,,$$

men $\bar{g}_1$ og $\bar{g}_j$ er indbyrdes primiske.

Altså er $\mathcal{G}_{11} \subseteq G_1$.

Hvis L er spaltningslegemet for $\bar{f}$ over $\mathbb{Z}_p$, er $\mathcal{G}_{11} \simeq \mathrm{Gr}(L/\mathbb{Z}_p)$ opfattet som permutationsgruppe i rødderne $\beta_1, \ldots, \beta_n$.

Antag $\bar{f} = \bar{f}_1 \ldots \bar{f}_m$, hvor $\bar{f}_1, \ldots, \bar{f}_m$ er irreducible i $\mathbb{Z}_p[X]$.

Lad grad $\bar{f}_i = \ell_1$, og rødderne i $\bar{f}_i$ være $\beta_{i1}, \ldots, \beta_{i\ell_i}$. Så er $\sum_{i=1}^{m} \ell_i = n$.

L er kompositet af spaltningslegemerne for $\bar{f}_i$ over $\mathbb{Z}_p$, $(i \leq p \leq m)$.

Spaltningslegemet for $\bar{f}_i$ over $\mathbb{Z}_p$ er $\simeq \mathrm{GF}(p^{\ell_i})$.

$[L : \mathbb{Z}_p]$ = mindste fælles multiplum af $\ell_1, \ldots, \ell_m$.

Hver af Galoisgrupperne $\mathrm{Gr}(\mathrm{GF}(p^{\ell_i})/\mathbb{Z}_p)$ er cykliske af orden ℓ_i, og hver af disse frembringes af automorfien σ (Frobeniusautomorfien), der er potensering med p.

Den til σ svarende permutation bliver således

$$\underset{(\text{ cykel af længde } \ell_1)}{\begin{pmatrix} \beta_{11} & \cdots & \beta_{1\ell_1} \\ \sigma(\beta_{11}) & \cdots & \sigma(\beta_{1\ell_1}) \end{pmatrix}} \underset{(\text{ cykel af længde } \ell_2)}{\begin{pmatrix} \beta_{21} & \cdots & \beta_{2\ell_2} \\ \sigma(\beta_{21}) & \cdots & \sigma(\beta_{2\ell_2}) \end{pmatrix}} \cdots \underset{(\text{ cykel af længde } \ell_m)}{\begin{pmatrix} \beta_{m1} & \cdots & \beta_{m\ell_m} \\ \sigma(\beta_{m1} & \cdots & \sigma(\beta_{m\ell_m}) \end{pmatrix}}$$

Derfor findes i $\mathrm{Gr}(\mathrm{Spl}\, f(X)/\mathbb{Q})$, opfattet som permutationsgruppe af rødderne $\alpha_1, \ldots, \alpha_m$, en permutation af formen

$$(\text{ cykel af længde } \ell_1)\ (\text{ cykel af længde } \ell_2) \cdots (\text{ cykel af længde } \ell_m)$$

(disjunkte cykler), hvor $\ell_1 + \ell_2 + \cdots + \ell_m = n$.

Hermed er bevist den ene halvdel af

Sætning 13.6. (Frobenius-Dedekind). *Lad $f(X) = X^n + a_1 Z^{n-1} + \cdots + a_n \in \mathbb{Z}[X]$ være et polynomium med lutter simple rødder. Lad M være spaltningslegemet over $\mathbb{Q}$, og $G = \mathrm{Gr}(M/\mathbb{Q})$, Galoisgruppen opfattet som undergruppe i S_n.*

Lad p være et primtal, og $p \nmid \mathrm{Disk}(f)$. Antag $f(X)$ modulo p er

$$(\text{irr . pol . i } \mathbb{Z}_p[X] \text{ af grad } \ell_1)\,(\text{irr . pol . i } \mathbb{Z}_p[X] \text{ af grad } \ell_2) \cdots (\text{irr . pol . i } \mathbb{Z}_p[X] \text{ af grad } \ell_m) \qquad (4)$$

hvor $\ell_1 + \ell_2 + \cdots + \ell_m = n$.

Da findes permutation i G, der er

$$(\text{ cykel af længde } \ell_1)\ (\text{ cykel af længde } \ell_2) \cdots (\text{ cykel af længde } \ell_m)$$

(indbyrdes disjunkte.

Omvendt, antag G indeholder en permutation, der er

$$(\text{ cykel af længde } \ell_1)\ (\text{ cykel af længde } \ell_2) \cdots (\text{ cykel af længde } \ell_m) \qquad (5)$$

hvor $\ell_1 + \ell_2 + \cdots + \ell_m = n$. Da findes uendelig mange primtal p, ($p \nmid \mathrm{Disk}(f)$), for hvilke $f(X)$ modulo p har en spaltning i irreducible faktorer af formen (4).

"Tætheden" af sådanne primtal er = den forventede, dvs.:

$$\frac{\#(\text{Elementer i } G \text{ der har fremstilling (5)})}{|G|}$$

Vi beviser ikke 2. halvdel af sætningen.

Den 1. (og af os beviste) halvdel, er i praksis den vigtigste.

Vi illustrerer dette ved at vise *direkte*

Sætning 13.7. *For ethvert n er S_n Galoisgruppe for en normal udvidelse af $\mathbb{Q}$.*

Vi får brug for

Lemma 13.8. *Lad G være en transitiv undergruppe i S_n, der indeholder en 2-cykel og en $(n-1)$-cykel. Da er $G = S_n$.*

Bevis. Antag $\tau = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n-1 \\ 2 & 3 & \cdots & n-1 & 1 \end{pmatrix} \in G$. Lad $(i,j) \in G$. Da G er transitiv findes $\sigma \in G$, så $\sigma(i) = n$, $\sigma(i,j)\sigma^{-1} = (n,k)$ med $k = \sigma(j)$.

Transpositionerne $\tau^a(n,k)\tau^{-a}$, $a = 1, 2, \ldots$ er i passende rækkefølge

$$(1,n), (2,n), \ldots, (n-1,n)\,,$$

hvorfor $G = S_n$. □

Bevis for Sætning 13.7.

For $n \leq 3$ er resultatet velkendt. Så antag, at $n > 3$.

Lad f_1 være et normeret polynomium i $\mathbb{Z}[X]$ der har grad n, og er irreducibelt modulo 2. Lad f_2 være et normeret polynomium i $\mathbb{Z}[X]$ der har grad n og modulo 3 er

$$\text{(et 1.grads pol.) (et irr. } (n-1) \text{ grads pol.)}\,.$$

Lad f_3 være et normeret polynomium i $\mathbb{Z}[X]$ der har grad n og modulo 5 er

$$\text{(et irr. 2.grads pol.) (et irr. } (n-2) \text{ grads pol.) når } n \text{ er ulige}\,,$$

og

$$\text{(et irr. 2.grads pol.) (et 1.grads pol.) (et irr. } (n-3) \text{ grads pol.) når } n \text{ er lige}\,.$$

Hvis $f = -15f_1 + 10f_2 + 6f_3$, er

$$\begin{aligned} f &\equiv f_1 \mod 2 \\ f &\equiv f_2 \mod 3 \\ f &\equiv f_3 \mod 5 \end{aligned}$$

Da $f \equiv f_1 \mod 2$ er f irreducibelt i $\mathbb{Z}[X]$, og dermed i $\mathbb{Q}[X]$; dvs. Galoisgruppen G for spaltningslegemet af f over $\mathbb{Q}$, er en transitiv undergruppe i S_n.

Da $f \equiv f_2 \mod 3$, indeholder G en $(n-1)$-cykel.

Da $f \equiv f_2 \mod 5$, indeholder G for ulige n et produkt af to disjunkte cykler af længde hhv. $(n-2)$ og 2. Den $(n-2)$-te potens af dette produkt er en 2-cykel. For lige n indeholder G et produkt af to disjunkte cykler af længde hhv. $(n$-3) og 2. Den $(n$-3)-te potens af dette produkt er en 2-cykel. I begge tilfælde vil G derfor indeholde en 2-cykel.

Ovenstående lemma (13.8) giver nu resultatet. □

14 Realisering af visse lineære grupper som Galoisgrupper

Vi begynder med et "teknisk lemma".

Lemma 14.1. *Lad K være et legeme af karakteristik 0 der indeholder de p'te enhedsrødder, hvor p er et primtal. Lad α, β være elementer i K. Da gælder:*

$$K(\sqrt[p]{\alpha}) = K(\sqrt[p]{\beta}) \iff \exists t\,,\ 1 \le t \le p-1\,, \exists \gamma \in K : \beta = \alpha^t \gamma^p\,.$$

Bevis. Vi kan antage $\alpha \notin K^p$, og dermed $\beta \notin K^p$.

"$\Leftarrow$" er klar.

"$\Rightarrow$": Antag $\sqrt[p]{\beta} \in K(\sqrt[p]{\alpha})$. Da findes $k_0, k_1, \ldots, k_{p-1} \in K$, så

$$\sqrt[p]{\beta} = k_0 + k_1 \sqrt[p]{\alpha} + k_2 \sqrt[p]{\alpha}^2 + \cdots + k_{p-1} \sqrt[p]{\alpha}^{p-1}\,.$$

Fra Mat 3AL (kapitel 5[Alg3. Theorem 5.6]) ved vi, at $\mathrm{Gr}(K(\sqrt[p]{\alpha})/K)$ er cyklisk af orden p, og en frembringer σ er defineret ved $\sigma(\sqrt[p]{\alpha}) = \sqrt[p]{\alpha}\varepsilon$, hvor ε betegner en (vilkårlig, men fast) primitiv p'te enhedsrod. Da må $\sigma(\sqrt[p]{\beta}) = \sqrt[p]{\beta}\varepsilon^t$ for et passende t, $1 \le t \le p-1$. På den anden side har vi

$$\sigma(\sqrt[p]{\beta}) = k_0 + k_1 \sqrt[p]{\alpha}\varepsilon + k_2 \sqrt[p]{\alpha}^2\varepsilon^2 + \cdots + k_{p-1} \sqrt[p]{\alpha}^{p-1}\varepsilon^{p-1}\,,$$

og

$$\sqrt[p]{\beta}\varepsilon^t = k_0\varepsilon^t + k_1 \sqrt[p]{\alpha}\varepsilon^t + k_2 \sqrt[p]{\alpha}^2\varepsilon^t + \cdots + k_{p-1} \sqrt[p]{\alpha}^{p-1}\varepsilon^t\,.$$

Heraf sluttes, at $k_i = 0$ for alle i, $0 \le i \le p-1$ undtagen $i = t$, dvs. $\sqrt[p]{\beta} = k_t(\sqrt[p]{\alpha}^t)$, hvilket giver den ønskede relation. □

Lad $\mathbb{Q}_p = \mathbb{Q}(\varepsilon)$, ε er primitiv p'te enhedsrod, være det p'te cirkeldelingslegeme. Fra Mat 3AL vides, at $\mathrm{Gr}(\mathbb{Q}_p/\mathbb{Q})$ er cyklisk af orden $p-1$, og at en frembringer ρ for $\mathrm{Gr}(\mathbb{Q}_p/\mathbb{Q})$ er defineret ved $\rho(\varepsilon) = \varepsilon^g$, hvor g er en "primitiv" rod modulo p, dvs. $\bar{g}$ er frembringer for den multiplikative gruppe $((\mathbb{Z}/p\mathbb{Z}) \setminus 0)^\times$.

Sætning 14.2. *Lad $\alpha \in \mathbb{Q}_p$, og antag $\alpha \notin \mathbb{Q}_p^p$ (i.e. $x^p - \alpha$ har ingen rødder i $\mathbb{Q}_p$). Da gælder: $N = \mathbb{Q}_p(\sqrt[p]{\alpha})$ er normal udvidelse af $\mathbb{Q}$ $\iff$ $\exists \beta \in \mathbb{Q}_p\ \exists t$, $1 \le t \le p-1$: $\rho(\alpha) = \alpha^t \beta^p$.*

Bevis. "$\Rightarrow$": Antag $N/\mathbb{Q}$ normal. Automorfien $\rho \in \mathrm{Gr}(\mathbb{Q}_p/\mathbb{Q})$ kan ifølge Galoisteoriens hovedsætning (punkt 5) fortsættes til automorfi $\rho' \in \mathrm{Gr}(N/\mathbb{Q})$. Da $\alpha = \sqrt[p]{\alpha}^p$, fås $\rho'(\alpha) = \rho(\alpha) = (\rho'(\sqrt[p]{\alpha}))^p$, i.e. $\sqrt[p]{\rho'(\alpha)} \in N$; endvidere er $\rho'(\alpha) = \rho(\alpha) \notin \mathbb{Q}_p^p$. Altså er $\mathbb{Q}_p(\sqrt[p]{\alpha}) = \mathbb{Q}_p(\sqrt[p]{\rho(\alpha)})$, og ovenstående lemma giver det ønskede β og t.

"$\Leftarrow$": Spaltningslegemerne over $\mathbb{Q}_p$ for hvert af polynomierne

$$x^p - \alpha\,,\ \ x^p - \rho(\alpha)\,,\ \ x^p - \rho^2(\alpha), \ldots, x^p - \rho^{p-2}(\alpha)$$

er N. Følgelig er N spaltningslegemet over $\mathbb{Q}$ for polynomiet

$$(x^p - \alpha)(x^p - \rho(\alpha))(x^p - \rho^2(\alpha)) \ldots (x^p - \rho^{p-2}(\alpha))\,,$$

der har koefficienter i $\mathbb{Q}$. □

Sætning 14.3. *Lad $\alpha \in \mathbb{Q}_p$, $\alpha \notin \mathbb{Q}_p^p$, og antag $N = \mathbb{Q}_p(\sqrt[p]{\alpha})$ er normal over $\mathbb{Q}$. Ifl. Sætning 14.2 er altså $\rho(\alpha) = \alpha^t \beta^p$ for et passende β i $\mathbb{Q}_p$ og et passende $t, 1 \leqq t \leqq p-1$. Da er $\mathrm{Gr}(N/\mathbb{Q})$ af orden $p(p-1)$, og frembragt af følgende to automorfier*

$$\sigma \in \mathrm{Gr}(N/\mathbb{Q}_p)\,, \quad \sigma(\sqrt[p]{\alpha}) = \sqrt[p]{\alpha}\varepsilon \quad (\varepsilon \text{ primitiv } p\text{'te enhedsrod})\,,$$

og ρ', hvor $\rho'|_{\mathbb{Q}_p} = \rho$.

Der gælder følgende relationer for σ og ρ':

1. *ρ' har orden $p-1$.*
2. *σ har orden p.*
3. *$\rho'\sigma(\rho')^{-1} = \sigma^c$, hvor c er bestemt ved $tc \equiv g(p)$, hvor t er det i Sætning 14.2 definerede tal.*

Endvidere gælder: $\mathrm{Gr}(N/\mathbb{Q})$ *abelsk* $\iff t \equiv g(p)$.

Bevis. Fra Galoisteoriens hovedsætning fås en eksakt følge

$$(1) \longrightarrow \mathrm{Gr}(N/\mathbb{Q}_p) \xrightarrow[\text{inj.}]{} \mathrm{Gr}(N/\mathbb{Q}) \xrightarrow[\mathrm{Res},\,\mathbb{Q}_p]{} \mathrm{Gr}(\mathbb{Q}_p/\mathbb{Q}) \longrightarrow (1)$$

(dvs. $\mathrm{Res}, \mathbb{Q}_p$ er surjektiv, $\ker(\mathrm{Res}, \mathbb{Q}_p) = \mathrm{im}(\mathrm{Gr}(N/\mathbb{Q}_p) \to \mathrm{Gr}(N/\mathbb{Q}))$. Da $|\,\mathrm{Gr}(N/\mathbb{Q}_p)| = p$ og $|\,\mathrm{Gr}(\mathbb{Q}_p/\mathbb{Q})| = p-1$, må der findes $\rho' \in \mathrm{Gr}(N/\mathbb{Q})$, så ρ' har orden $p-1$ og $\rho'|_{\mathbb{Q}_p} = \rho$. (Hvorfor ?)

Nu gælder

$$\rho'(\sqrt[p]{\alpha}) = \sqrt[p]{\alpha}^t \beta' \;\text{ for }\; 1 \leq t \leq p-1\,,\; \beta' \in \mathbb{Q}_p\,,$$

og

$$\rho'\sigma(\sqrt[p]{\alpha}) = \sqrt[p]{\alpha}^t \beta' \varepsilon^g$$
$$\sigma^c\rho'(\sqrt[p]{\alpha}) = \sqrt[p]{\alpha}^t \beta' \varepsilon^{ct}\,.$$

Heraf ses, at for $ct \equiv g(p)$ fås

$$\rho'\sigma = \sigma^c\rho' \quad \text{eller} \quad \rho'\sigma(\rho')^{-1} = \sigma^c\,.$$

Da ρ' har orden $p-1$, og σ har orden p, kan ethvert element i $\mathrm{Gr}(N/\mathbb{Q})$ entydigt skrives $(\rho')^i\sigma^j$, $1 \leq i \leq p-1$, $1 \leq j \leq p$. □

I det følgende skriver vi for simpelheds skyld ρ i stedet for ρ'.

Sætning 14.4. *Med benævnelserne fra Sætning 14.3, antag $t \not\equiv g(p)$, så $\mathrm{Gr}(N/\mathbb{Q})$ ikke er abelsk. Da er centret $Z(\mathrm{Gr}(N/\mathbb{Q}))$ frembragt af ρ^ℓ, hvor ℓ er ordenen af restklassen $\bar{c}$ af c i $(\mathbb{Z}/p\mathbb{Z})^\times$. Specielt er $Z(\mathrm{Gr}(N/\mathbb{Q}))$ cyklisk af orden $\frac{p-1}{\ell}$.*

Bevis. Antag $\rho^i\sigma^j \in Z(\mathrm{Gr}(N/\mathbb{Q}))$. Da må

$$\rho^i\sigma^j\rho = \rho\rho^i\sigma^j\,, \qquad (*)$$

og dermed

$$\sigma^j\rho = \rho\sigma^j\,.$$

Da $\rho\sigma\rho^{-1} = \sigma^c$ (ifølge Sætning 14.3), må $\rho\sigma^j\rho^{-1} = \sigma^{cj}$, der sammenholdt med $(*)$ medfører

$$\rho\sigma^j = \sigma^{cj}\rho = \sigma^j\rho\,,$$

og dermed $cj \equiv j(p)$; da $t \not\equiv g(p)$ indebærer $c \not\equiv 1(p)$, vil kongruensen $cj \equiv j(p)$, (der kan skrives $(c-1)j \equiv 0(p)$), medføre

$$j \equiv 0(p)\,.$$

$Z(\mathrm{Gr}(N/\mathbb{Q}))$ kan altså kun bestå af potenser af ρ.

Lad $\rho^i \in Z(\mathrm{Gr}(N/\mathbb{Q}))$. Af relationen

$$\rho\sigma\rho^{-1} = \sigma^c$$

fås

$$\rho^i\sigma\rho^{-i} = \sigma^{c^i}\,,$$

hvorfor $\rho^i\sigma = \sigma\rho^i \iff c^i \equiv 1(p) \iff \ell|i$, hvor ℓ er det mindste naturlige tal for hvilket $c^\ell \equiv 1(p)$. Følgelig fås

$$Z(\mathrm{Gr}(N/\mathbb{Q})) = \{\rho^\ell, \rho^{2\ell}, \ldots, \rho^{p-1} = e\}\,.$$

□

Antag med ovennævnte benævnelser, at $N/\mathbb{Q}$ er normal med ikke-abelsk $\mathrm{Gr}(N/\mathbb{Q})$. Hvad bliver $\widehat{G} = \mathrm{Gr}(N/\mathbb{Q})/Z(\mathrm{Gr}(N/\mathbb{Q}))$? Denne faktorgruppe bliver frembragt af de homomorfe billeder $\bar\sigma$ og $\bar\rho$ af σ og ρ. Relationerne mellem $\bar\sigma$ og $\bar\rho$, bliver

$$(\bar\sigma)^p = \bar e = (\bar\rho)^\ell \quad \bar\rho\bar\sigma(\bar\rho)^{-1} = (\bar\sigma)^c\,.$$

Frobeniusgruppen $F_{p\ell}$, $\ell|p-1$ er gruppen af alle permutationer af det endelige legeme $\mathbb{F}_p$ givet ved

$$x \mapsto (\bar c)^i x + \bar a\,, \quad i \text{ modulo } \ell\,,\ \bar a \in \mathbb{F}_p\,.$$

Ved afbildningen

$$\{x \mapsto \bar c^i x + \bar a\} \mapsto (\bar\sigma)^a(\bar\rho)^i$$

fås en bijektion $F_{p\ell} \to \widehat{G}$, der er en homomorfi, idet

$$(\bar c^i x + \bar a) \circ (\bar c^j x + \bar b) = \bar c^{i+j} x + \bar c^i \bar b + \bar a\,,$$

og der gælder

$$(\bar\sigma)^a(\bar\rho)^i(\bar\sigma)^b(\bar\rho)^j = (\bar\sigma)^{c^i b + a}(\bar\rho)^{i+j}\,,$$

da

$$\bar\rho\bar\sigma(\bar\rho)^{-1} = (\bar\sigma)^c$$
$$(\bar\rho)^i\bar\sigma(\bar\rho)^{-i} = (\bar\sigma)^{c^i}$$
$$(\bar\rho)^i(\bar\sigma)^b(\bar\rho)^{-i} = (\bar\sigma)^{bc^i}\,.$$

Konklusion: Frobeniusgruppen $F_{p\ell}$ kan realiseres som Galoisgruppe for en normal udvidelse af $\mathbb{Q}$, hvis der findes et $\alpha \in \mathbb{Q}_p$, så $\alpha \notin \mathbb{Q}_p^p$, $\rho(\alpha) = \alpha^t \beta^p$, ($\beta \in \mathbb{Q}_p$), hvor $tc \equiv g(p)$, g er en primitiv rod modulo p, så $\rho(\varepsilon) = \varepsilon^g$ og $\bar{c}$ er en restklasse i $\mathbb{F}_p^\times$ af (multiplikativ) orden ℓ.

Eksistensen af et sådant α er ikke-triviel. En ansats hertil er følgende: Lad $\gamma \in \mathbb{Q}_p$, og definer for $a_0, a_1, \ldots, a_{p-2} \in \mathbb{Z}$ den "symbolske potens"

$$\gamma^{a_0+a_1\rho+a_2\rho^2+\cdots+a_{p-2}\rho^{p-2}} := \gamma^{a_0}(\rho(\gamma))^{a_1}(\rho^2(\gamma))^{a_2}\ldots(\rho^{p-2}(\gamma))^{a_{p-2}}\,.$$

Lad nu t være et helt tal, så $1 \le t \le p-1$. Vi søger $\beta \in \mathbb{Q}_p$, så

$$\rho\left(\gamma^{a_0+a_1\rho+a_2\rho^2+\cdots+a_{p-2}\rho^{p-2}}\right) = \left(\gamma^{a_0+a_1\rho+a_2\rho^2+\cdots+a_{p-2}\rho^{p-2}}\right)^t \cdot \beta^p\,.$$

Dette giver anledning til en ligning i "grupperingen" $(Z/p\mathbb{Z})[G]$, hvor G betegner den af ρ frembragte cykliske gruppe af orden $p-1$:

$$\rho(\bar{a}_0 + \bar{a}_1\rho + \bar{a}_2\rho^2 + \cdots + \bar{a}_{p-2}\rho^{p-2}) = t(\bar{a}_0 + \bar{a}_1\rho + \bar{a}_2\rho^2 + \cdots + \bar{a}_{p-2}\rho^{p-2})\,.$$

Dette giver følgende system af lineære ligninger

$$\begin{aligned}
\bar{a}_{p-2} &= t\bar{a}_0\\
\bar{a}_0 &= t\bar{a}_1\\
\bar{a}_1 &= t\bar{a}_2\\
&\vdots\\
\bar{a}_{p-4} &= t\bar{a}_{p-3}\\
\bar{a}_{p-3} &= t\bar{a}_{p-2}\,.
\end{aligned}$$

En løsning hertil er

$$\begin{aligned}
\bar{a}_{p-2} &= \bar{1}\\
\bar{a}_{p-3} &= \bar{t}\\
\bar{a}_{p-4} &= \bar{t}^2\\
&\vdots\\
\bar{a}_2 &= \bar{t}^{p-4}\\
\bar{a}_1 &= \bar{t}^{p-3}\\
\bar{a}_0 &= \bar{t}^{p-2}\,,
\end{aligned}$$

idet vi bemærker, at $\bar{t}^{p-1} = 1$. Derfor tilfredsstiller elementet

$$\alpha = \gamma^{t^{p-2}+t^{p-3}\rho+\cdots+t\rho^{p-3}+\rho^{p-2}}$$

ligningen $\rho(\alpha) = \alpha^t\beta^p$ for passende $\beta \in \mathbb{Q}_p$.

Ved hjælp af algebraisk talteori *kan* man finde $\gamma \in \mathbb{Q}_p$, så ovenstående $\alpha \notin \mathbb{Q}_p^p$.

Vi benytter her i stedet Hilberts Irreducibilitetssætning (HIS) til at finde et $\gamma \in \mathbb{Q}_p$, så $\alpha \notin \mathbb{Q}_p^p$. Hertil bemærkes først, at for legemerne $\mathbb{Q}(T)$ og $\mathbb{Q}_p(T)$ af brudne rationale funktioner i T, vil $\mathbb{Q}_p(T)/\mathbb{Q}(T)$ være en normal udvidelse, og $\mathrm{Gr}(\mathbb{Q}_p(T)/\mathbb{Q}(T)) = \mathrm{Gr}(\mathbb{Q}_p/\mathbb{Q})$, idet enhver automorfi i $\mathrm{Gr}(\mathbb{Q}_p/\mathbb{Q})$ på entydig vis kan fortsættes til en automorfi i $\mathrm{Gr}(\mathbb{Q}_p(T)/\mathbb{Q}(T))$, nemlig koefficientvis. (Jf. kapitlet om Kroneckers metode til bestemmelse af Galoisgrupper).

Da $\mathbb{Q}_p[T]$ er UFD ses det let, at $(T+\varepsilon)^{t^{p-2}+t^{p-3}\rho+\cdots+t\rho^{p-3}+\rho^{p-2}}$ ikke er p'te potens af et element i $\mathbb{Q}_p(T)$. Derfor er

$$h(X,T) = X^p - (T+\varepsilon)^{t^{p-2}+t^{p-3}\rho+\cdots+t\rho^{p-3}+\rho^{p-2}}$$

et irreducibelt polynomium i $\mathbb{Q}_p[X,T]$ (jf. Sætning 3 i Mat 3AL p.5.4 [Alg3. Theorem 5.7]). Produktpolynomiet

$$H(X,T) = \prod_{\nu=0}^{p-2} \rho^\nu h(X,T) = \prod_{\nu=0}^{p-2} \left(X^p - (T+\rho^\nu\varepsilon)^{t^{p-2}+t^{p-3}\rho+\cdots+t\rho^{p-3}+\rho^{p-2}} \right),$$

har rationale koefficienter, idet de er invariante under automorfien ρ. Nu er $H(X,T)$ irreducibelt i $\mathbb{Q}[X,T]$. Thi antag der fandtes en ikke-triviel faktorisering

$$H(X,T) = H_1(X,T)H_2(X,T) \qquad (*)$$

indenfor $\mathbb{Q}[X,T]$. Da $h(X,T)$ er en divisor i $H(X,T)$ indenfor $\mathbb{Q}_p[X,T]$, og $h(X,T)$ er irreducibel i $\mathbb{Q}_p[X,T]$, måtte $h(X,T)$ (indenfor $\mathbb{Q}_p[X,T]$), gå op i enten $H_1(X,T)$ eller $H_2(X,T)$. Antag f.Eks., at $h(X,T)$ går op i $H_1(X,T)$. Ved anvendelse af automorfien ρ fås da

$$\begin{aligned}
\rho h(X,T) \;&|\; \rho H_1(X,T) \quad &= H_1(X,T)\\
\rho^2 h(X,T) \;&|\; \rho^2 H_1(X,T) \quad &= H_1(X,T)\\
&\vdots\\
\rho^{p-2} h(X,T) \;&|\; \rho^{p-2} H_1(X,T) = H_1(X,T)
\end{aligned}$$

Da $h(X,T)$, $\rho h(X,T), \ldots, \rho^{p-2}h(X,T)$ er indbyrdes primiske, får vi for produktet, at

$$\prod_{\nu=0}^{p-2} \rho^\nu h(X,T) = H(X,T) | H_1(X,T)\,,$$

hvor "gå op" relationen a priori gælder indenfor $\mathbb{Q}_p[X,T]$, og da $H(X,T)$ og $H_1(X,T)$ har rationale koefficienter, må "gå op" relationen også gælde i $\mathbb{Q}[X,T]$. Men $H(X,T)|H_1(X,T)$ og $H_1(X,T)|H(X,T)$ strider imod at $(*)$ var en ikke-triviel faktorisering.

Ifølge HIS findes rationale tal q, så $H(X,q)$ er irreducibel i $\mathbb{Q}[X]$. Men da må $h(X,q)$ være irreducibel i $\mathbb{Q}_p[X]$. (Hvorfor?) Dermed er

$$(q+\varepsilon)^{t^{p-2}+t^{p-3}\rho+\cdots+t\rho^{p-3}+\rho^{p-2}}$$

ikke p'te potens af et tal i $\mathbb{Q}_p$ og dermed et brugbart α.

Konklusion: *For ethvert primtal p og enhver divisor ℓ i $p-1$, findes en normal udvidelse af $\mathbb{Q}$ med Frobeniusgruppen $F_{p\ell}$ som Galoisgruppe.*

ANVENDELSER AF ALGEBRAISK TALTEORI

Nogle Grundbegreber i algebraisk Talteori.

Vi minder om nogle grundlæggende begreber og sætninger i algebraisk talteori. For udførlige beviser henvises til f.eks. A.L.Schmidt's Noter i Algebraisk Talteori.

Definition. *Et komplekst tal kaldes algebraisk, hvis det er rod i et egentligt polynomium i* $\mathbb{Q}[x]$.

Definition. *Et komplekst tal kaldes "helt algebraisk", hvis det er rod i et normeret polynomium i* $\mathbb{Z}[x]$.

Bemærkning 14.5. *Lad* α *være et komplekst tal og* h *et naturligt tal. Hvis* α^h *er et helt algebraisk tal, da er også* α *et helt algebraisk tal.*

Det følgende er en simpel konsekvens af Gauss' s sætning ang. primitive polynomier:

Sætning 14.6. *Lad* α *være et algebraisk tal. Da gælder:*
α *er et helt algebraisk tal* $\Leftrightarrow Irr(\alpha, \mathbb{Q}) \in \mathbb{Z}[x]$.

Korollar. *Et rationalt tal er helt algebraisk hvis og kun det er et (sædvanligt) helt rationalt tal.*

De efterfølgende sætninger er ikke svære at eftervise. Udførlige beviser kan f.eks. ses i Asmus L. Schmidt's Noter i algebraisk talteori.

Sætning 14.7. *Sum, differens og produkt af hele algebraiske tal er selv hele algebraiske tal. Med andre ord: de hele algebraiske tal udgør en ring med sædvanlig addition og multiplikation.*

Sætning 14.8. *Lad* D *være et kvadratfrit helt rationalt tal, der er* $\equiv 1$ *(mod 4). De hele algebraiske tal i* $\mathbb{Q}(\sqrt{D})$ *er netop tallene af formem* $(a+b\sqrt{D})/2$ *, hvor* a *og* b *ligger i* $\mathbb{Z}$ *og* $a \equiv b$ *(mod 2).*

Vi får endvidere brug for følgende sætning kendt fra 3AL:

Sætning 14.9. *For et ulige primtal* p *gælder:*
$\mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}_p \Leftrightarrow p \equiv 1$ *(mod 4)*
$\mathbb{Q}(\sqrt{-p}) \subseteq \mathbb{Q}_p \Leftrightarrow p \equiv 3$ *(mod 4).*

Eksplicit Realisering af $F_{p(p-1)/2}$ som Galoisgruppe over $\mathbb{Q}$ for Primtal $p \equiv 3$ mod 4.

For et ulige primtal p der er $\equiv 3 \pmod 4$ vil vi eksplicit realisere Frobeniusgruppen $F_{p(p-1)/2}$ som Galoisgruppe over $\mathbb{Q}$. [$F_{p(p-1)/2}$ er undergruppen i $L_p = F_{p(p-1)}$ af orden $p(p-1)/2$ bestående af alle permutationer $\{x \mapsto ax+b \mid a \in (\mathbb{Z}/\mathbb{Z}p)^2 \setminus 0, b \in (\mathbb{Z}/\mathbb{Z}p)\}$.]

Specielt får vi eksplicit realiseret de ikke-abelske grupper af orden 21 og 55 som Galoisgrupper.

Vi benytter overvejelserne fra 14.1-14.3. Hvis g er en primitiv rod modulo p og $p \equiv 3 \pmod 4$ vil den ved $-g$ bestemte rstklasse modulo p have orden $(p-1)/2$ i $(\mathbb{Z}/\mathbb{Z}p \setminus 0, \cdot)$. Vi søger derfor et α i $\mathbb{Q}_p \setminus \mathbb{Q}_p^p$, men $\alpha\rho(\alpha) \in \mathbb{Q}_p^p$, hvor ρ som sædvanlig er den automorfi i $Gr(\mathbb{Q}_p/\mathbb{Q})$, der sender en primitiv p-te enhedsrod ε over i ε^g.

Sætning 14.10. *Lad a og b være tal i $\mathbb{Z}$ så $a \equiv b$ (mod 2) og ab ikke er deleligt med p, hvor p er et primtal der er $\equiv 3$ (mod 4). Da er $\left(\frac{a^2+b^2p}{4}\right)^{\frac{p-1}{2}} \cdot \left(\frac{a+b\sqrt{-p}}{2}\right)$ et brugbart α.*

Inden beviset bringer vi et alment lemma, der er interessant i sig selv og er meget nyttigt.

Abel's Lemma. *Lad K være et legeme af karakteristik 0 og p et primtal. For ethvert a i K gælder:*

$x^p - a$ er reducibelt i $K[x] \Leftrightarrow x^p - a$ har en rod i K.

Bevis for Abel's Lemma. $\Leftarrow$: klart.

$\Rightarrow$: Antag $x^p - a$ er reducibelt. Inden for spaltningslegemet for $x^p - a$ over K gælder

$$x^p - a = \prod_{i=0}^{p-1}(x - \beta\varepsilon^i),$$

hvor β er et element i spaltningslegemet, hvis p-te potens er lig a og ε er en primitiv p-te enhedsrod.

Når $x^p - a$ er reducibelt i $K[x]$, må der findes et t, hvor $1 \le t \le p-1$, så $\beta^t \cdot (p$-te enhedsrod) ligger i K. Følgelig må β^{pt} ligge i K^p. (Her betegner K^p den multiplikative gruppe af fra 0 forskellige p-te potenser i K.) Da $\beta^p = a$ slutter vi at $a^t \in K^p$. Da endvidere a^p tilhører K^p og $(t,p) = 1$, fås, at a ligger i K^p, dvs. $x^p - a$ har en rod i K. □

Bevis for Sætning 14.10. Vi bemærker først, at p.gr. af Sætning 14.8 vil $\left(\frac{a^2+b^2p}{4}\right)^{\frac{p-1}{2}} \cdot \left(\frac{a+b\sqrt{-p}}{2}\right)$ virkelig ligge i det p-te cirkeldelingslgeme $\mathbb{Q}_p$. Med de hidtige betegnelser vil restriktionen af ρ til $\mathbb{Q}(\sqrt{-p}$ være kompleks konjugering, hvorfor

$$\alpha\rho(\alpha) = \left(\frac{a^2+b^2p}{4}\right)^{\frac{p-1}{2}} \cdot \left(\frac{a+b\sqrt{-p}}{2}\right) \cdot \left(\frac{a^2+b^2p}{4}\right)^{\frac{p-1}{2}} \cdot \left(\frac{a-b\sqrt{-p}}{2}\right) = \left(\frac{a^2+pb^2}{4}\right)^p$$

der ligger i $\mathbb{Q}_p^p$.

Vi skal godtgøre, at α ikke ligger i $\mathbb{Q}_p^p$. Vi viser først, at α ikke er p-te potens af et tal i $\mathbb{Q}(\sqrt{-p})$.

Antag $\alpha = \gamma^p$ for et γ i $\mathbb{Q}(\sqrt{-p})$.

Ifl. Bemærkning 14.5 måtte γ være et helt algebraisk tal i $\mathbb{Q}(\sqrt{-p})$ og kunne derfor ifl. sætning 14.8 skrives på formen $(c+d\sqrt{-p})/2$, hvor c og d ligger i $\mathbb{Z}$ og $c \equiv d \pmod 2$. Vi måtte da have:

$$\left(\frac{a^2+b^2p}{4}\right)^{\frac{p-1}{2}} \cdot \left(\frac{a+b\sqrt{-p}}{2}\right) = \left(\frac{c+d\sqrt{-p}}{2}\right)^p$$

$$= \frac{\left(c^p + \binom{p}{1}c^{p-1}d\sqrt{-p} + \binom{p}{2}c^{p-2}d^2(-p) + \cdots + d^p(-p)^{\frac{p-1}{2}}\sqrt{-p}\right)}{2^p}$$

Ved at identificere imaginærdelene på højre og venstre side og at udnytte $\binom{p}{1}$, $\binom{p}{3}$, $\ldots$, $\binom{p}{p-1}$ er delelige med p fås da:

$$\left(a^2+b^2p\right)^{\frac{p-1}{2}} b \equiv 0 \pmod p,$$

hvilket er umuligt, da p hverken går op i a eller b.

Altså er α ikke p-te potens af et tal i $\mathbb{Q}(\sqrt{-p})$.

P.gr.af Abel's lemma er $x^p - \alpha$ derfor irreducibelt i $\mathbb{Q}(\sqrt{-p})[x]$.

Antag der fandtes et γ i $\mathbb{Q}_p$, så $\gamma^p = \alpha$. Da ville $x^p - \alpha$ være lig $Irr(\gamma, \mathbb{Q}(\sqrt{-p})$ og dermed ville graden af γ over $\mathbb{Q}(\sqrt{-p})$ være p. Men dimensionen $[\mathbb{Q}_p : \mathbb{Q}(\sqrt{-p})]$ er $(p-1)/2$. Modstrid! $\square$.

Sætning 14.11. *Lad p være et primtal $\equiv 3$ (mod 4) og a og b tal i $\mathbb{Z}$ for hvilke $p \nmid ab$ og $a \equiv b$ (mod 2). Da er*

$$M = \mathbb{R} \cap \mathbb{Q}_p\left(\sqrt[p]{\left(\frac{a^2+b^2p}{4}\right)^{\frac{p-1}{2}} \cdot \left(\frac{a+b\sqrt{-p}}{2}\right)}\right)$$

en normal udvidelse af $\mathbb{Q}$ med Frobeniusgruppen $F_{p(p-1)/2}$ som Galoisgruppe.

Bemærkning. Den ovenstående p-te rod er kun bestemt på nær en faktor, der er en p-te enhedsrod. Men da den ovenstående p-te rod skal adjungeres til et legeme der indeholder alle p-te enhedsrødder, fås samme legeme M uanset hvilken af de p værdier man vælger.

Bevis for Sætning 14.11. Hvis N betegner legemet $\mathbb{Q}_p\left(\sqrt[p]{\left(\frac{a^2+b^2p}{4}\right)^{\frac{p-1}{2}} \cdot \left(\frac{a+b\sqrt{-p}}{2}\right)}\right)$ viser konstruktionen, at $Gr(N/\mathbb{Q})$ er den i sætning 14.3 bestemte gruppe af orden $p(p-1)$, hvor $c = -g$ og $\ell = (p-1)/2$. Centret for denne gruppe er (jfr. sætning 14.4) er cyklisk af orden 2. Da $p(p-1) = 2\cdot($ ulige tal), er centret den eneste undergruppe i $Gr/N/\mathbb{Q})$ af orden 2. Fixpunktslegemet for centret giver en normal udvidelse af $\mathbb{Q}$ med $F_{p(p-1)/2}$ som Galoisgruppe. Kompleks konjugering er en automorfi af orden 2, så centret består af identiteten og kompleks konjugering. Det omhandlede fixpunktslegeme er derfor $\mathbb{R} \cap N$. $\square$

Vi vil nu angive eksplicitte irreducible p-te gradspolynomier i $\mathbb{Q}[x]$, hvis spaltningslegemer over $\mathbb{Q}$ har $F_{p(p-1)/2}$ som Galoisgruppe.

Vi skriver

$$\left(\frac{a^2+b^2p}{4}\right)^{\frac{p-1}{2}} \cdot \left(\frac{a+b\sqrt{-p}}{2}\right) = \sqrt{\left(\frac{a^2+b^2p}{4}\right)^p} \cdot (\cos\theta + i\sin\theta),$$

hvor $\cos\theta = \frac{a}{\sqrt{a^2+b^2p}}$.

Realdelene af de p rødder $\sqrt[p]{\left(\frac{a^2+b^2p}{4}\right)^{\frac{p-1}{2}} \cdot \left(\frac{a+b\sqrt{-p}}{2}\right)}$ er tallene

$$\sqrt{\frac{a^2+b^2p}{4}} \cdot \cos\left(\frac{\theta+2\pi k}{p}\right), \quad k = 0, 1, 2, \ldots, p-1.$$

Vi får nu brug for de såkaldte Tschebycheff polynomier.

Sætning 14.12. *For ethvert naturligt tal n findes et n-te gradspolynomium $T_n(x) \in \mathbb{Z}[x]$, så cos $nx = T_n(\cos x)$.*

Bevis. Ifl. "de Moivres formel" er

$$\cos nx + i\sin nx = (\cos x + i\sin x)^n.$$

Ved anvendelse af binomialformlen på højre side fås:

$$(\cos x + i\sin x)^n = \cos^n x + \binom{n}{1}\cos^{n-1}x(i\sin x) + \binom{n}{2}\cos^{n-2}x(-\sin^2 x) + \cdots$$

Da realdelen af højre side er cos nx, fås:

$$\cos nx = \cos^n x + \binom{n}{2}\cos^{n-2}x(-\sin^2 x) + \binom{n}{4}\cos^{n-4}x(\sin^4 x) - \cdots.$$

Da $\sin^2 x = 1 - \cos^2 x$, ser vi at cos nx bliver et heltalspolynomium i cos x. □

Definition. *$T_n(x)$ kaldes det n-te Tschebucheff polynomium (af 1-ste art).*

Eksempler. $T_1(x) = x$; $T_2(x) = 2x^2 - 1$; $T_3(x) = 4x^3 - 3x$; $T_4(x) = 8x^4 - 8x^2 + 1$; $T_5(x) = 16x^5 - 20x^3 + 5x$; ; $T_6(x) = 32x^6 - 48x^4 + 18x^2 - 1$; $T_7(x) = 64x^7 - 112x^5 + 56x^3 - 7x$.

Et alment eksplicit udtryk er følgende:

$$T_n(x) = 2^{n-1}x^n - \frac{n}{n-1}\binom{n-1}{1}2^{n-3}x^{n-2} + \frac{n}{n-2}\binom{n-2}{2}2^{n-5}x^{n-4} + \cdots.$$

Der gælder rekursionsformlen

$$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x).$$

For ulige (resp.lige) n er $T_n(x)$ en ulige (resp. lige) funktion i x (dvs. kun ulige (resp. lige) potenser af x optræder i $T_n(x)$).

Nu tilbage til Galoisgruppen for $M/\mathbb{Q}$.

Realdelene af de p værdier for $\sqrt[p]{\left(\frac{a^2+b^2p}{4}\right)^{\frac{p-1}{2}} \cdot \left(\frac{a+b\sqrt{-p}}{2}\right)}$ er rødderne i polynomiet

$$\sqrt{a^2+b^2p} \cdot T_p\left(\frac{2x}{\sqrt{a^2+b^2p}}\right) - a,$$

der er et polynomium i $\mathbb{Q}[x]$, da $T_p(x)$ er en ulige funktion.

Ovennævnte polynomium kaldes $G_p(a,b,x)$.

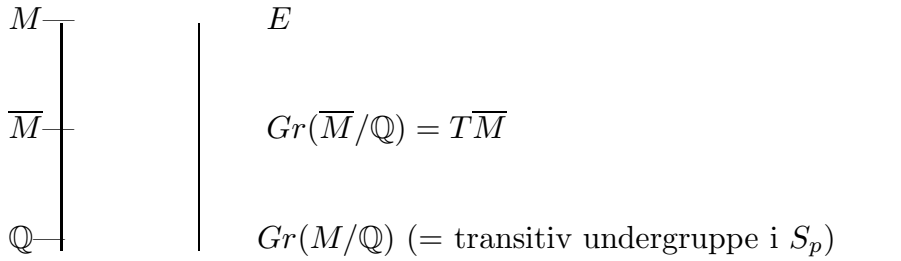
Det er klart, at spaltningslegemet $\overline{M}$ for $G_p(a,b,x)$ over $\mathbb{Q}$ er indeholdt i M.

Med notationerne fra sætningerne 14.3 og 14.4 vil σ give en cyklisk forskydning af de p værdier for $\sqrt[p]{\left(\frac{a^2+b^2p}{4}\right)^{\frac{p-1}{2}} \cdot \left(\frac{a+b\sqrt{-p}}{2}\right)}$.

M er $\mathbb{R} \cap N$ og består derfor af de tal i N der er invariante under kompleks konjugering. Som tidligere nævnt ligger kompleks konjugering i centret for $Gr(N/\mathbb{Q})$. Derfor vil σ(realdelen af et tal γ i N) være lig realdelen af $\sigma(\gamma)$. Det medfører, at σ giver en cyklisk forskydning af realdelene for de p værdier for $\sqrt[p]{\left(\frac{a^2+b^2p}{4}\right)^{\frac{p-1}{2}} \cdot \left(\frac{a+b\sqrt{-p}}{2}\right)}$.

$G_p(a,b,x)$ er derfor irreducibelt i $\mathbb{Q}[x]$, hvorfor specielt p går op i dimensionen $[\overline{M} : \mathbb{Q}]$.

Vi har nu diagrammet



Da $Gr(M/\mathbb{Q})$ er en transitiv undergruppe i S_p og $T\overline{M}$ er normaldeler i $Gr(M/\mathbb{Q})$ vil ifl. lemma 9.1 $T\overline{M}$ enten være E eller en transitiv undergruppe i S_p. Hvis sidstnævnte var tilfældet, måtte p gå op i $T\overline{M} = [M : \overline{M}]$. Men da p også er en divisor i $[\overline{M} : \mathbb{Q}]$, måtte p^2 gå op i $[M : \mathbb{Q}] = p(p-1)/2$, hvilket er umuligt.

Altså er $T\overline{M} = E$ og dermed er $\overline{M} = M$. □

Korollar. *Lad p være et primtal $\equiv 3$ (mod 4) og a og b tal i $\mathbb{Z}$ for hvilke $a \equiv b$ (mod 2) og $p \nmid ab$. Da er $G_p(a,b,x)$ et irreducibelt p-te gradspolynomium i $\mathbb{Q}[x]$, hvis spaltningslegeme over $\mathbb{Q}$ har Frobeniusgruppen $F_{p(p-1)/2}$ som Galoisgruppe.*

Eksempler. For $p = 7$ og $a = b = 1$ vil man efter en simpel transformation [benyt, at et n-te gradspolynomium $f(x)$ vil have samme spaltningslegeme som $x^n f(\frac{1}{x})$] få, at

$$x^7 + 14x^6 - 56x^4 + 56x^2 - 16$$

har Frobeniusgruppen F_{21} som Galoisgruppe over $\mathbb{Q}$.

For $p = 11$ og $a = b = 1$ vil man på lignende vis få, at

$$x^{11} - 33x^9 + 396x^7 - 2079x^5 + 4455x^3 - 2673x - 243$$

har Frobeniusgruppen F_{55} som Galoisgruppe over $\mathbb{Q}$.