KØBENHAVNS UNIVERSITETS MATEMATISKE INSTITUT

BØRGE JESSEN

ELEMENTÆR ALGEBRA

1965

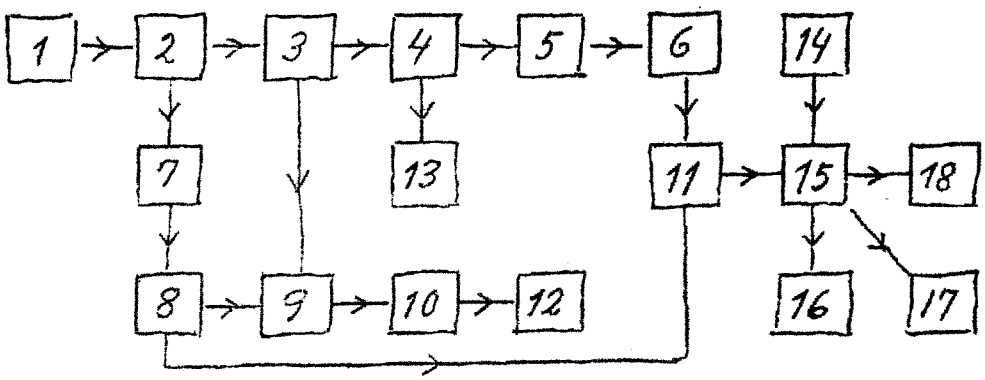
Omfatter 112 sider

mærket Elem. alg. O-111

Selbst zu erfinden ist schön, doch glücklich von anderen Gefundenes, fröhlich erkannt und geschätzt, nennst du das weniger dein?

GOETHE

Indhold.



§1. Indledning.

Ordet algebra kommer af al jebr (arabisk) = forening af adskilte dele, anvendt i betydningen flytning af led fra den ene side af lighedstegnet til den anden. Specielt kom ordet til at betegne løsning af ligninger, ved hvis opstilling der kun gøres brug af de fire elementære regningsarter.

Allerede Babylonerne kendte løsningen af andengradsligningen. I geometrisk form genfindes denne hos grækerne. I det 16. årh. fandt man løsningen af tredjegradsligningen og fjerdegradsligningen, begyndte at opstavregningen udvikledes, og man begyndte at operere med komplekse tal.

Den senere udvikling skete i nøjeste forbindelse med udviklingen af analysen og den analytiske geometri. Vi nævner:

Cramer (1704–1752). Systemer af lineære ligninger 1750.

Lagrange (1736–1813). Begyndelsen til en teori for ligninger af højere grad.

Gauss (1777–1855). Konstruktion af den regulære 17-kant 1796. Bevis for algebraens fundamentalsætning 1799. Disquisitiones arithmeticae 1801. Heri bl.a. diskussion af, hvilke regulære polygoner, der kan konstrueres med passer og lineal.

Abel (1802–1829). Umuligheden af at løse femtegradsligningen ved rodtegn.

Galois (1811–1832). Almen teori for ligninger af højere grad.

Hermed var grunden lagt til den moderne udvikling, som i vore dage har ført til den abstrakte algebra.

I nærværende fremstilling, der er baseret på gentagne forelæsninger gennem en række år, gives en behandling af de simpleste dele af teorien for ligninger af højere grad i det komplekse tallegeme, herunder læren om algebraiske tal. Som hovedpunkter behandles Gauss' sætning om konstruerbare regulære polygoner og Lindemanns sætning om transcendensen af π, der indeholder umuligheden af cirklens kvadratur ved konstruktion med passer og lineal.

§ 2. Polynomier i en variabel.

I det $\mathbb{C}$ er det komplekse tallegeme, betegner vi med $\mathbb{C}[x]$ mængden af polynomier

$$F = F(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

hvor koefficienterne $a_0, a_1, \cdots, a_n$ tilhører $\mathbb{C}$, medens x er en kompleks variabel. Et polynomium er åbenbart en kontinuert funktion på $\mathbb{C}$ med værdier i $\mathbb{C}$.

Identitetssætningen. To polynomier i $\mathbb{C}[x]$, der stemmer overens i værdi for alle x, er identiske, d.v.s. hvis de to polynomier skrives på formen

$F(x) = a_0 + a_1 x + \cdots + a_n x^n$ og $G(x) = b_0 + b_1 x + \cdots + b_n x^n$

med samme n [hvad der er muligt ved evt. tilføjelse af nuller], gælder

$$a_0 = b_0,\ a_1 = b_1,\ \cdots,\ a_n = b_n.$$

Bevis. For $x = 0$ fås $F(0) = a_0$, $G(0) = b_0$. Altså er $a_0 = b_0$. Følgelig gælder for alle x

$$a_1 x + a_2 x^2 + \cdots + a_n x^n = b_1 x + b_2 x^2 + \cdots + b_n x^n.$$

For alle $x \neq 0$ gælder derfor

$$a_1 + a_2 x + \cdots + a_n x^{n-1} = b_1 + b_2 x + \cdots + b_n x^{n-1}.$$

På grund af kontinuiteten må dette også gælde for $x = 0$. Altså er $a_1 = b_1$. Ved fortsættelse af ræsonnementet ses, at $a_2 = b_2, \cdots, a_n = b_n$.

Hvis i et polynomium

$$F = F(x) = a_0 + a_1 x + \cdots + a_n x^n$$

alle koefficienterne er 0, kaldes F <u>nulpolynomiet</u> og skrives 0, ellers kaldes F et <u>egentligt polynomium</u>. Ved <u>graden</u> af et egentligt polynomium forstås den største index i, for hvilken $a_i \neq 0$. Graden er altså et helt tal $\geqslant 0$. Polynomierne af grad 0 er konstanter $a \neq 0$. Nulpolynomiet tillægges ingen grad. Dog vil vi, når vi taler om mængden af polynomier af grad $\leqslant n$, af bekvemmelighedsgrunde medregne nulpolynomiet.

Idet

$$F(x) = a_0 + a_1 x + \cdots + a_n x^n \text{ og } G(x) = b_0 + b_1 x + \cdots + b_m x^m,$$

er $F(x) + G(x)$ og $F(x)\,G(x)$ også polynomier. Altså er addition og multiplikation kompositionsregler i $C[x]$. Med disse kompositionsregler er $C[x]$ en <u>integritetsring</u>, d. v. s. en kommutativ ring med et element (polynomiet 1) og uden nuldivisorer. Den sidste egenskab, at der ikke er nuldivisorer, fremgår af udtrykket for produktet

$$F(x)\,G(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \cdots + a_n b_m x^{n+m},$$

som viser, at når F og G er egentlige polynomier af grader n og m, er FG et egentligt polynomium af grad $n + m$.

<u>Sætning.</u> For givne indbyrdes forskellige tal $x_0, x_1, \cdots, x_n \in C$ og givne tal $y_0, y_1, \cdots, y_n \in C$ findes et og kun et polynomium

$$F(x) = a_0 + a_1 x + \cdots + a_n x^n$$

[altså et og kun et polynomium af grad $\leqslant n$], for hvilket

$$F(x_0) = y_0,\ F(x_1) = y_1,\ \cdots,\ F(x_n) = y_n.$$

Bevis. Lad $F(x) = a_0 + a_1 x + \cdots + a_n x^n$ være et vilkårligt polynomium af grad $\leqslant n$. Vi sætter $c_n = a_n$. Det ved subtraktion af $c_n(x-x_0)(x-x_1)\cdots(x-x_{n-1})$ fremkomne polynomium vil være af grad $\leqslant n-1$, altså af formen $\cdots + c_{n-1}x^{n-1}$. Subtraheres $c_{n-1}(x-x_0)(x-x_1)\cdots(x-x_{n-2})$ fås et polynomium af grad $\leqslant n-2$. Ved gentagelse af processen når man efter n subtraktioner til et polynomium af grad $\leqslant 0$, altså en konstant c_0. Hermed er F skrevet på formen

$$F(x) = c_0 + c_1(x-x_0) + c_2(x-x_0)(x-x_1) + \cdots + c_n(x-x_0)(x-x_1)\cdots(x-x_{n-1}).$$

Man ser nu ved successiv indsættelse af $x_0, x_1, \cdots, x_n$, at betingelserne $F(x_0) = y_0, F(x_1) = y_1, \cdots, F(x_n) = y_n$ opfyldes for et og kun et sæt af koefficienter $c_0, c_1, \cdots, c_n$.

Den således fundne formel for F er Newtons interpolationsformel. Undertiden er det bekvemmere at bestemme F ved Lagranges interpolationsformel

$$F(x) = y_0\frac{(x-x_1)(x-x_2)\cdots(x-x_n)}{(x_0-x_1)(x_0-x_2)\cdots(x_0-x_n)} + y_1\frac{(x-x_0)(x-x_2)\cdots(x-x_n)}{(x_1-x_0)(x_1-x_2)\cdots(x_1-x_n)}$$
$$+ \cdots + y_n\frac{(x-x_0)(x-x_1)\cdots(x-x_{n-1})}{(x_n-x_0)(x_n-x_1)\cdots(x_n-x_{n-1})}.$$

Af sætningen uddrager vi en skærpelse af identitetssætningen: Hvis to polynomier af grad $\leqslant n$ stemmer overens i værdi for $n+1$ værdier af x, er de identiske.

Taylors formel. Et polynomium

$$F(x) = a_0 + a_1 x + \cdots + a_n x^n$$

er en differentiabel funktion på $\mathbb{C}$, og dets afledede $F'(x)$ er polynomiet

$$F'(x) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}.$$

Thi man finder (for $h \neq 0$) ved brug af binomialformlen

$$\frac{F(x+h)-F(x)}{h} = \sum_{\nu=1}^{n} a_\nu \frac{(x+h)^\nu - x^\nu}{h}$$

$$= \sum_{\nu=1}^{n} a_\nu \frac{\binom{\nu}{1}x^{\nu-1}h + \binom{\nu}{2}x^{\nu-2}h^2 + \cdots + \binom{\nu}{\nu}h^\nu}{h},$$

hvoraf $\lim_{h\to 0} \frac{F(x+h)-F(x)}{h} = \sum_{\nu=1}^{n} a_\nu \nu x^{\nu-1}$.

Følgelig er $F(x)$ vekårligt ofte differentiabel, og man har

$$F''(x) = 2a_2 + \cdots + n(n-1)a_n x^{n-2},$$

$$\cdots\cdots$$

$$F^{(n)}(x) = n!\,a_n,$$

$$F^{(n+1)}(x) = 0, \quad F^{(n+2)}(x) = 0, \text{ etc.}$$

Heraf fås Taylors formel for et polynomium $F(x)$ af grad $\leqslant n$ svarende til punktet 0

$$F(x) = F(0) + \frac{F'(0)}{1!}x + \frac{F''(0)}{2!}x^2 + \cdots + \frac{F^{(n)}(0)}{n!}x^n.$$

For fast x_0 er $F(x_0+t) = G(t)$ et polynomium i t af grad $\leqslant n$, og vi har

$$G'(t) = \lim_{h\to 0} \frac{G(t+h)-G(t)}{h} = \lim_{h\to 0} \frac{F(x_0+t+h)-F(x_0+t)}{h} = F'(x_0+t),$$

$$G''(t) = F''(x_0+t), \text{ etc.}$$

Anvendelse af Taylors formel svarende til punktet 0 på $G(t)$ giver derfor Taylors formel for polynomiet $F(x)$ svarende til punktet x_0

$$F(x_0+t) = F(x_0) + \frac{F'(x_0)}{1!}t + \frac{F''(x_0)}{2!}t^2 + \cdots + \frac{F^{(n)}(x_0)}{n!}t^n$$

eller

$$F(x) = F(x_0) + \frac{F'(x_0)}{1!}(x-x_0) + \frac{F''(x_0)}{2!}(x-x_0)^2 + \cdots + \frac{F^{(n)}(x_0)}{n!}(x-x_0)^n.$$

§ 3. Algebraens fundamentalsætning.

Ved en rod i et egentligt polynomium $F(x)$ forstås et tal x_0, for hvilket $F(x_0)=0$. Et polynomium af grad 0 har naturligvis ingen rod. Et polynomium af grad $n \geqslant 1$ har højst n rødder. Thi havde det flere, vilde det for $n+1$ værdier af x have samme værdi som nulpolynomiet, og måtte altså ifølge den skærpede identitetssætning være nulpolynomiet.

Algebraens fundamentalsætning. Ethvert polynomium $F(x)$ af grad $\geqslant 1$ har en rod.

Det første bevisforsøg skyldes d'Alembert 1746, og sætningen kaldes også d'Alemberts sætning. Den blev først bevist af Gauss 1799. Følgende bevis skyldes Argand 1815. Det kaldes ofte Cauchys bevis.

Bevis. Lad

$$F(x) = a_0 + a_1 x + \cdots + a_n x^n, \quad n \geqslant 1, \ a_n \neq 0.$$

Da er $F(0) = a_0$. For $|x| = R > 0$ gælder

$$|F(x)| \geqslant |a_n| R^n - |a_0| - |a_1| R - \cdots - |a_{n-1}| R^{n-1}$$

$$= R^n \left(|a_n| - \frac{|a_0|}{R^n} - \frac{|a_1|}{R^{n-1}} - \cdots - \frac{|a_{n-1}|}{R} \right).$$

For $R \to +\infty$ konvergerer højre side mod $+\infty$. Vi vælger R, så at højre side er $> |a_0|$. Restriktionen af $|F(x)|$ til cirkelskiven $\{x \mid |x| \leqslant R\}$ er en kontinuert reel funktion på en kompakt mængde. Der findes altså et punkt x_0 i skiven, så at $|F(x_0)| \leqslant |F(x)|$ for ethvert x i skiven. Specielt gælder $|F(x_0)| \leqslant |F(0)| = |a_0|$, hvoraf, da $|F(x)| > |a_0|$ for $|x| = R$, følger, at $|x_0| < R$. Vi vil vise, at $F(x_0) = 0$. Beviset er indirekte. Vi antager altså,

at $F(x_0) \neq 0$.

Vi sætter $x = x_0 + h$ og finder

$$F(x_0+h) = A_0 + A_1 h + \cdots + A_n h^n, \quad A_0 = F(x_0) \neq 0, \; A_n = a_n \neq 0.$$

Lad A_j være det første af tallene $A_1, \cdots, A_n$, som er $\neq 0$. Da er

$$F(x_0+h) = F(x_0) + A_j h^j + \cdots + A_n h^n, \quad A_j \neq 0.$$

Vi betragter nu et tal r, om hvilket vi foreløbig blot forudsætter, at $0 < r \leqslant R - |x_0|$, og sætter $h = re^{i\theta}$. Endvidere skrives

$$F(x_0) = |F(x_0)| e^{i\varphi}, \quad A_j = |A_j| e^{i\psi}.$$

Da er

$$F(x_0+h) = |F(x_0)| e^{i\varphi} + |A_j| r^j e^{i(\psi+j\theta)} + A_{j+1} h^{j+1} + \cdots + A_n h^n.$$

Vi vælger nu θ således, at $\psi + j\theta = \varphi + \pi$. Da er

$$F(x_0+h) = \left(|F(x_0)| - |A_j| r^j\right) e^{i\varphi} + A_{j+1} h^{j+1} + \cdots + A_n h^n.$$

Nu pålægger vi r den yderligere betingelse, at $|A_j| r^j \leqslant |F(x_0)|$. Da fås

$$\begin{aligned} |F(x_0+h)| &\leqslant |F(x_0)| - |A_j| r^j + |A_{j+1}| r^{j+1} + \cdots + |A_n| r^n \\ &= |F(x_0)| - r^j \left(|A_j| - |A_{j+1}| r - \cdots - |A_n| r^{n-j}\right). \end{aligned}$$

Størrelsen i parenteren konvergerer mod $|A_j| > 0$ for $r \to 0$. Vi kan derfor vælge r i overensstemmelse med de betingelser, der foran er pålagt r, således at størrelsen i parentesen er > 0. Da er $|F(x_0+h)| < |F(x_0)|$, og da $|x_0+h| \leqslant |x_0| + r \leqslant R$, er vi nået til en modstrid.

<u>Ethvert polynomium</u> $F(x)$ <u>af grad</u> $\geqslant 1$ <u>kan på en og, bortset fra førstegradsfaktorernes rækkefølge, kun på en måde skrives på formen</u>

$$(*) \qquad F(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n), \quad a \neq 0.$$

Denne sætning indeholder naturligvis algebraens

fundamentalsætning. På den anden side følger den, som vi skal se, meget let af den.

Bevis. (1) Fremstillingens mulighed. Lad $F(x)$ have graden n, og lad α_1 være en rod i $F(x)$. Taylors formel giver da

$$F(x) = \frac{F'(\alpha_1)}{1!}(x-\alpha_1) + \frac{F''(\alpha_1)}{2!}(x-\alpha_1)^2 + \cdots + \frac{F^{(n)}(\alpha_1)}{n!}(x-\alpha_1)^n$$
$$= (x-\alpha_1)\,F_1(x),$$

hvor $F_1(x)$ er et polynomium af grad $n-1$. Nu fortsættes med $F_1(x)$, og i n skridt er vi færdige.

(2) Fremstillingens entydighed. Lad

$$a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) = b(x-\beta_1)(x-\beta_2)\cdots(x-\beta_m), \quad a\neq 0, b\neq 0.$$

Da de to polynomier har henholdsvis ax^n og bx^m som højeste led, er $n=m$ og $a=b$. Da α_1 er rod på venstre side, og altså også på højre side, er α_1 et af tallene β_j, f. eks. β_1. Ellers ændres rækkefølgen af tallene β_j. Ved division med $x-\alpha_1$ fås for $x\neq\alpha_1$

$$a(x-\alpha_2)\cdots(x-\alpha_n) = b(x-\beta_2)\cdots(x-\beta_m).$$

Af kontinuitetsgrunde må dette også gælde for $x=\alpha_1$. Efter n skridt er vi færdige.

De n ikke nødvendigvis indbyrdes forskellige tal $\alpha_1, \alpha_2, \ldots, \alpha_n$ er åbenbart samtlige rødder i $F(x)$. Idet en rod regnes med <u>multiplicitet</u> bestemt ved antallet af gange, den forekommer i udtrykket $a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$, kan vi sige, at et polynomium af grad $n \geqslant 1$ har <u>netop</u> n <u>rødder</u>. Er $\alpha_1, \ldots, \alpha_r$ de <u>indbyrdes forskellige</u> rødder i $F(x)$ og $\nu_1, \ldots, \nu_r$ deres multipliciteter, har vi $\nu_1 + \cdots + \nu_r = n$, og fremstillingen lyder

$$(5) \qquad F(x) = a(x-\alpha_1)^{\nu_1}\cdots(x-\alpha_r)^{\nu_r}.$$

I stedet for at sige, at α er rod i $F(x)$ med multipliciteten ν kan man sige, at α er ν gange rod i $F(x)$. Hvis $\nu = 1$ kaldes α en <u>simpel</u> eller <u>enkelt rod</u>, hvis $\nu > 1$ en <u>multipel rod</u>, specielt hvis $\nu = 2$ en <u>dobbelt rod</u>.

Fremstillingen (※) eller (§) kan naturligvis også benyttes for polynomier af grad 0, idet så blot førstegradsfaktorerne mangler.

<u>Divisorer</u>. I overensstemmelse med den sædvanlige sprogbrug for ringe kaldes et egentligt polynomium G divisor i polynomiet F, hvis der findes et polynomium Q, således at $F = GQ$. Da $\mathbb{C}[x]$ ikke har nuldivisorer, vil polynomiet Q være entydig bestemt; det kaldes <u>kvotienten</u> af F og G og betegnes $Q = \frac{F}{G}$.

For givne polynomier F og G, $G \neq 0$, afgør man, om G er divisor i F, ved hjælp af den velkendte divisionsmetode, som giver en fremstilling

$$F = GQ + R,$$

hvor R enten er nulpolynomiet eller et egentligt polynomium af lavere grad end G. Der er kun en sådan fremstilling, thi hvis $F = GQ + R = GQ_1 + R_1$, hvor R og R_1 hver for sig enten er nulpolynomiet eller et polynomium af lavere grad end G, får vi $G(Q - Q_1) = R_1 - R$. Var nu $Q \neq Q_1$, var $G(Q - Q_1)$ et egentligt polynomium af grad $\geq$ graden af G, medens $R_1 - R$ er nulpolynomiet eller et egentligt polynomium af grad $<$ graden af G. Altså er $Q = Q_1$ og følgelig $R = R_1$. Den anførte ligning kaldes <u>divisionsligningen</u> og R den <u>principale rest</u> af F ved division med G. Man ser nu, at G er divisor i F, hvis og kun hvis R er nulpolynomiet.

Nulpolynomiet har som divisorer samtlige egentlige polynomier. Et egentligt polynomium F af grad n har kun divisorer af grad $\leqslant n$. Som trivielle divisorer har vi alle polynomier af grad 0, altså alle konstanter $a \neq 0$, og alle polynomier aF, hvor $a \neq 0$. Disse kaldes de med F <u>associerede</u> polynomier. Blandt disse findes et og kun et <u>normeret</u>, d.v.s. med 1 som koefficient til leddet af højest grad. Andre divisorer kaldes <u>ægte</u>. For $n=0$ og $n=1$ findes naturligvis kun de trivielle divisorer. Associerede polynomier har naturligvis de samme divisorer. Hvis F har G som divisor, da også de med G associerede.

<u>Bestemmelse af samtlige divisorer i et egentligt polynomium</u> $F(x)$. Ud fra fremstillingen (S) bestemmes divisorerne i F ved

$$G(x) = b(x-\alpha_1)^{\sigma_1} \dots (x-\alpha_r)^{\sigma_r}, \quad b \neq 0, \qquad \begin{matrix} 0 \leqslant \sigma_1 \leqslant \nu_1 \\ \dots \\ 0 \leqslant \sigma_r \leqslant \nu_r. \end{matrix}$$

[Her skal en faktor $(x-\alpha_j)^{\sigma_j}$ med $\sigma_j = 0$ læses som 1.] Thi disse polynomier er åbenbart divisorer i F, og der kan ikke være andre. Hvis nemlig $F = GQ$, skal vi ved indsætning af fremstillingerne af G og Q få fremstillingen af F.

<u>Bestemmelse af samtlige fælles divisorer i to egentlige polynomier</u> F_1 <u>og</u> F_2. Lad de fælles rødder være $\alpha_1, \dots, \alpha_t$ med multiplicæteter henholdsvis $\nu_1, \dots, \nu_t$ og $\mu_1, \dots, \mu_t$, og lad desuden F_1 have rødderne $\beta_1, \dots, \beta_u$ med multiplicæteter $\lambda_1, \dots, \lambda_u$ og F_2 rødderne $\gamma_1, \dots, \gamma_v$ med multiplicæteter $\varkappa_1, \dots, \varkappa_v$. Vi har da

$$F_1 = a_1(x-\alpha_1)^{\nu_1} \dots (x-\alpha_t)^{\nu_t}(x-\beta_1)^{\lambda_1} \dots (x-\beta_u)^{\lambda_u}$$

$$F_2 = a_2(x-\alpha_1)^{\mu_1} \dots (x-\alpha_t)^{\mu_t}(x-\gamma_1)^{\varkappa_1} \dots (x-\gamma_v)^{\varkappa_v},$$

og ser, at samtlige fælles divisorer i F_1 og F_2 bestemmes ved

$$G = b(x-\alpha_1)^{\rho_1}\cdots(x-\alpha_t)^{\rho_t},\ b\neq 0,\qquad 0\leqslant \rho_1\leqslant \sigma_1 = \min\{\nu_1,\mu_1\}\ \cdots\ 0\leqslant \rho_t\leqslant \sigma_t = \min\{\nu_t,\mu_t\}.$$

Heraf aflæses: Der findes et og kun et normeret polynomium D med den egenskab, at samtlige fælles divisorer i F_1 og F_2 netop er samtlige divisorer i D, nemlig polynomiet

$$D = (x-\alpha_1)^{\tau_1}\cdots(x-\alpha_t)^{\tau_t}.$$

Dette polynomium kaldes største fælles divisor for F_1 og F_2 og betegnes $D = (F_1, F_2)$.

Dette vigtige resultat kan også vises på en anden måde, og vi får herved samtidig en metode til bestemmelse af D, uden at nulpunkterne for F_1 og F_2 behøver at være kendt. Herfil benyttes

Euklids algoritme. Vi opskriver divisionsligningerne

$$\begin{aligned}
F_1 &= F_2Q_1 + F_3 && \text{grad } F_3 < \text{grad } F_2\\
F_2 &= F_3Q_2 + F_4 && \text{grad } F_4 < \text{grad } F_3\\
&\cdots\\
F_{m-2} &= F_{m-1}Q_{m-2} + F_m && \text{grad } F_m < \text{grad } F_{m-1}\\
F_{m-1} &= F_mQ_{m-1}, &&
\end{aligned}$$

idet processen fortsættes, indtil man når en ligning, hvori resten er nulpolynomiet, hvilket må indtræffe engang. Nu ser man: Enhver fælles divisor i F_1 og F_2 er også divisor i F_3, den er altså fælles divisor i F_2 og F_3 og følgelig også divisor i F_4, etc. Den er altså divisor i F_m. Omvendt: Enhver divisor i F_m er også divisor i F_{m-1}, den er altså fælles divisor i F_{m-1} og F_m og følgelig også divisor i F_{m-2}, etc. Den er altså fælles divisor i F_1 og F_2. Det med F_m

associerede normerede polynomium D har altså den egenskab, at de fælles divisorer i F_1 og F_2 netop er samtlige divisorer i D. Hvis D_1 ligeledes er et normeret polynomium, hvis divisorer netop er de fælles divisorer i F_1 og F_2, må D være divisor i D_1 og D_1 divisor i D, hvilket (da polynomierne er normerede) medfører, at $D = D_1$.

Er $(F_1, F_2) = D$, og er H et vilkårligt normeret polynomium, gælder $(F_1 H, F_2 H) = DH$.

Dette ses f. eks. af, at Euklids algoritme for $F_1 H$ og $F_2 H$ fremgår af Euklids algoritme for F_1 og F_2 ved at multiplicere alle divisionsligningerne med H.

[For k egentlige polynomier $F_1, \ldots, F_k$ gælder ligeledes, at der findes et og kun et normeret polynomium D med den egenskab, at samtlige fælles divisorer i $F_1, \ldots, F_k$ netop er samtlige divisorer i D. Det kaldes største fælles divisor for $F_1, \ldots, F_k$ og betegnes $D = (F_1, \ldots, F_k)$. Det samme gælder naturligvis, hvis nogle af polynomierne (men ikke alle) er nulpolynomiet, og betegnelsen benyttes også i dette tilfælde.]

Et tal α er rod i det egentlige polynomium $F(x)$ med multiplicitet ν, hvis og kun hvis

$$F(\alpha) = 0,\ F'(\alpha) = 0,\ \ldots,\ F^{(\nu-1)}(\alpha) = 0,\ F^{(\nu)}(\alpha) \neq 0.$$

Bevis. (1) Hvis $F(\alpha) = 0, F'(\alpha) = 0, \ldots, F^{(\nu-1)}(\alpha) = 0$, $F^{(\nu)}(\alpha) \neq 0$, viser Taylors formel, at

$$F(x) = \frac{F^{(\nu)}(\alpha)}{\nu!}(x-\alpha)^\nu + \ldots$$

$$= (x-\alpha)^\nu G(x),$$

hvor $G(x)$ er et polynomium med $G(\alpha) \neq 0$. Hvis F har grad n, vil G have grad $n-\nu$, og vil altså have en fremstilling $a(x-\beta_1)\cdots(x-\beta_{n-\nu})$, hvor tallene β_j

er $\neq \alpha$. Følgelig er α rod i $F(x)$ med multiplicitet ν.

(2) Hvis α er rod i $F(x)$ med multiplicitet ν, kan $F(x)$ en fremstilling $(x-\alpha)^\nu G(x)$, hvor $G(x)$ er et polynomium med $G(\alpha) \neq 0$. Hvis F har grad n, vil G have grad $n-\nu$. Anvendes Taylors formel på G, fås for F en fremstilling

$$F(x) = c_\nu (x-\alpha)^\nu + c_{\nu+1}(x-\alpha)^{\nu+1} + \cdots + c_n (x-\alpha)^n, \quad c_\nu \neq 0,$$

hvoraf ses, at $F(\alpha)=0$, $F'(\alpha)=0, \ldots, F^{(\nu-1)}(\alpha)=0$, $F^{(\nu)}(\alpha)\neq 0$.

Af sætningen fremgår, at <u>hvis α er ν gange rod i $F(x)$</u>, <u>vil α være $\nu-1$ gange rod i $F'(x)$</u>, hvormed naturligvis for $\nu=1$ menes, at α ikke er rod i $F'(x)$. Hvis vi derfor i fremstillingen (§) først tænker os skrevet de rødder $\alpha_1, \ldots, \alpha_t$, hvis multipliciteter er ≥ 2, og derefter de simple rødder $\alpha_{t+1}, \ldots, \alpha_r$, således at fremstillingen lyder

$$F(x) = a(x-\alpha_1)^{\nu_1} \cdots (x-\alpha_t)^{\nu_t}(x-\alpha_{t+1}) \cdots (x-\alpha_r),$$

vil $F'(x)$ have $\alpha_1, \ldots, \alpha_t$ som rødder med multipliciteter $\nu_1-1, \ldots, \nu_t-1$, men vil ikke have noget af tallene $\alpha_{t+1}, \ldots, \alpha_r$ som rod. Fremstillingen af $F'(x)$ bliver derfor

$$F'(x) = na(x-\alpha_1)^{\nu_1-1} \cdots (x-\alpha_t)^{\nu_t-1}(x-\beta_1)^{\mu_1} \cdots (x-\beta_s)^{\mu_s},$$

hvor $\beta_1, \ldots, \beta_s$ er de øvrige rødder i $F'(x)$ og $\mu_1, \ldots, \mu_s$ disses multipliciteter. Heraf aflæses, at

$$D = (F, F') = (x-\alpha_1)^{\nu_1-1} \cdots (x-\alpha_t)^{\nu_t-1}.$$

<u>Rødderne i $D=(F,F')$ er altså netop de multiple rødder i F, men hver af disse er rod i D med en multiplicitet, der er 1 lavere end dens multiplicitet i F.</u>

Dette kan benyttes til en opløsning af et polynomium F i faktorer, der hver for sig kun har simple rødder. For simpelheds skyld antages F normeret. Lad de indbyrdes forskellige rødder være $\alpha_1, \ldots, \alpha_r$.

ordnet således, at vi først tager rødderne med multiplicitet 1, så dem af multiplicitet 2, etc. Herved fås

$$F = G_1 G_2^2 \cdots G_m^m,$$

hvor G_q er produktet af de faktorer $x-\alpha_i$, der svarer til rødderne af multiplicitet q, og m er den højeste forekommende multiplicitet. [Hvis der ikke er rødder af multiplicitet q, sættes naturligvis $G_q = 1$.] Vi har da

$$\begin{aligned} D_1 &= (F, F') = G_2 G_3^2 \cdots G_m^{m-1} \\ D_2 &= (D_1, D_1') = G_3 \cdots G_m^{m-2} \\ &\cdots \\ D_{m-1} &= (D_{m-2}, D_{m-2}') = G_m \\ D_m &= (D_{m-1}, D_{m-1}') = 1. \end{aligned}$$

Man når altså til polynomiet 1 efter netop m skridt. Herved er m bestemt, idet regningerne udføres under anvendelse af Euklids algoritme, indtil polynomiet 1 er nået. Ved division fås herefter

$$\frac{F}{D_1} = G_1 G_2 \cdots G_m, \quad \frac{D_1}{D_2} = G_2 \cdots G_m, \quad \cdots, \quad \frac{D_{m-1}}{1} = G_m$$

og følgelig

$$G_1 = \frac{F D_2}{D_1^2}, \quad G_2 = \frac{D_1 D_3}{D_2^2}, \quad \cdots, \quad G_{m-1} = \frac{D_{m-2} \cdot 1}{D_{m-1}^2}, \quad G_m = D_{m-1}.$$

§4. Polynomier med koefficienter fra et tallegeme.

Idet $\mathcal{L}$ er et vilkårligt tallegeme (et dellegeme af $\mathbb{C}$) betegner vi med $\mathcal{L}[x]$ mængden af polynomier med koefficienter fra $\mathcal{L}$. Et polynomium F i $\mathcal{L}[x]$ kaldes også et polynomium over $\mathcal{L}$. Man ser umiddelbart, at $\mathcal{L}[x]$ <u>er en delintegritetsring</u> af $\mathbb{C}[x]$. Hvis et egentligt polynomium F tilhører $\mathcal{L}[x]$, vil også det med F associerede normerede polynomium tilhøre $\mathcal{L}[x]$. Når F tilhører $\mathcal{L}[x]$, vil

også F' tilhøre $\mathcal{L}[x]$.

Hvis F og G er polynomier tilhørende $\mathcal{L}[x]$, og G er egentligt, vil de to polynomier Q og R i divisionsligningen

$$F = GQ + R$$

også tilhøre $\mathcal{L}[x]$. Ved betragtning af divisionsmetoden ser man nemlig, at alle de polynomier, der fremkommer under divisionen, må få koefficienter i $\mathcal{L}$. Specielt ses, at <u>hvis G er divisor i F i $C[x]$, er G også divisor i F i $\mathcal{L}[x]$</u>. Divisorerne i F i integritetsringen $\mathcal{L}[x]$ er altså simpelthen de divisorer i F i $C[x]$, der tilhører $\mathcal{L}[x]$.

<u>For to egentlige polynomier F og G i $\mathcal{L}[x]$ vil $D = (F, G)$ ligeledes tilhøre $\mathcal{L}[x]$</u>.

Dette ses af, at der i Euklids algoritme anvendt på F og G kun vil optræde polynomier i $\mathcal{L}[x]$.

Nulpolynomiet har som divisorer i $\mathcal{L}[x]$ samtlige egentlige polynomier i $\mathcal{L}[x]$. For et egentligt polynomium F i $\mathcal{L}[x]$ har vi som trivielle divisorer i $\mathcal{L}[x]$ alle polynomier af grad 0 i $\mathcal{L}[x]$, altså alle konstanter $a \neq 0$, $a \in \mathcal{L}$, og alle med F associerede polynomier i $\mathcal{L}[x]$, altså alle polynomier aF, hvor $a \neq 0$, $a \in \mathcal{L}$. Andre divisorer i F i $\mathcal{L}[x]$ kaldes ægte.

Idet F antages af grad $\geqslant 1$ og tilhørende $\mathcal{L}[x]$, kaldes F <u>reduktibelt</u> i $\mathcal{L}[x]$ (eller over $\mathcal{L}$), hvis F har ægte divisorer i $\mathcal{L}[x]$, altså hvis $F = GQ$, hvor G og Q er polynomier i $\mathcal{L}[x]$, der begge er af grad $\geqslant 1$. Ellers kaldes F <u>irreduktibelt</u> i $\mathcal{L}[x]$ (eller over $\mathcal{L}$). To associerede polynomier i $\mathcal{L}[x]$ er enten begge reduktible eller begge irreduktible.

Ethvert polynomium i $\mathcal{L}[x]$ af grad 1 er naturligvis irreduktibelt.

For $\mathcal{L} = \mathbb{C}$ har vi ifølge algebraens fundamentalsætning:

Et polynomium i $\mathbb{C}[x]$ er da og kun da irreduktibelt i $\mathbb{C}[x]$, når dets grad er 1.

Sætningen om fremstilling af egentlige polynomier på formen $a(x-\alpha_1)\cdots(x-\alpha_n)$ kan derfor også formuleres således:

Ethvert egentligt polynomium i $\mathbb{C}[x]$ kan på en og, bortset fra de irreduktible faktorers rækkefølge, kun på en måde skrives som produkt af et tal $a \neq 0$ og normerede irreduktible polynomier i $\mathbb{C}[x]$.

Af grundlæggende betydning er nu, at en tilsvarende sætning gælder for ethvert talegeme $\mathcal{L}$.

Hovedsætning. For ethvert talegeme $\mathcal{L}$ kan ethvert egentligt polynomium F i $\mathcal{L}[x]$ på en og, bortset fra de irreduktible faktorers rækkefølge, kun på en måde skrives på formen

$$F = a P_1 \cdots P_s,$$

hvor $a \neq 0$ er et tal i $\mathcal{L}$, og $P_1, \cdots, P_s$ er normerede irreduktible polynomier i $\mathcal{L}[x]$.

Bemærk analogien med hovedsætningen om de hele tals integritetsring $\mathbb{Z}$ (den elementære talteoris hovedsætning), hvorefter ethvert tal $n \in \mathbb{Z}$, $n \neq 0$, på en og, bortset fra primfaktorernes rækkefølge, kun på en måde kan skrives på formen

$$n = a p_1 \cdots p_s,$$

hvor a er enten $+1$ eller -1, og $p_1, \cdots, p_s$ er primtal.

Bevis. (1) Fremstillingens mulighed. Hvis

det egentlige polynomium F i $\mathfrak{L}[x]$ er af grad 0 eller er ireduktibelt, er sagen klar. Hvis F er reduktibelt af grad n, er $F = F_1 F_2$, hvor F_1 og F_2 er polynomier i $\mathfrak{L}[x]$ af grader $< n$. Hvis de er ireduktible, er sagen klar. Ellers fortsættes. Efter højst n skridt er F skrevet som produkt af ireduktible faktorer, og sagen er klar.

(2) Vanskeligheden er at bevise fremstillingens entydighed. Vi går frem i skridt.

(a) Hvis F og G er egentlige polynomier i $\mathfrak{L}[x]$, og P er et ireduktibelt polynomium i $\mathfrak{L}[x]$, som er divisor i FG men ikke i F, da er P divisor i G.

Vi kan antage, at alle polynomierne er normerede. Vi danner $D = (F, P)$. Dette er ligeledes et polynomium i $\mathfrak{L}[x]$. Det er divisor i P, som er ireduktibelt. Altså er $D = 1$ eller $D = P$. Men D er divisor i F. Da P ikke er divisor i F, må vi have $D = 1$.

Af ligningen $(F, P) = 1$ fås ifølge §3 ligningen $(FG, PG) = G$. Nu er P divisor i både FG og PG. Altså er P divisor i G.

(b) Hvis et ireduktibelt polynomium i $\mathfrak{L}[x]$ er divisor i et produkt af polynomier i $\mathfrak{L}[x]$, er det divisor i mindst et af disse polynomier.

Dette følger straks af (a) ved induktion.

(c) Lad nu

$$a P_1 \cdots P_s = b Q_1 \cdots Q_t,$$

hvor $a \neq 0$ og $b \neq 0$ er tal i $\mathfrak{L}$, og $P_1, \ldots, P_s$ og $Q_1, \ldots, Q_t$ er normerede ireduktible polynomier i $\mathfrak{L}[x]$. Da er åbenbart $a = b$. Hvis $s = 0$, er også $t = 0$, og vi er færdige. Hvis $s > 0$, er også $t > 0$. Da nu P_1 er divisor i venstre side, er P_1 også divisor i højre side, altså ifølge (b) divisor i mindst en af faktorerne Q_j, f. eks. i Q_1.

Ellers ændres rækkefølgen af faktorerne Q_j. Men Q_1 er irreduktibelt. Altså er $P_1 = Q_1$, og vi kan forkorte. Efter s skridt er vi færdige, idet faktorerne på de to sider må slippe op samtidig.

Hvis $\mathcal{L}$ og $\mathcal{L}_1$ er to tallegemer, og $\mathcal{L} \subset \mathcal{L}_1$, gælder åbenbart $\mathcal{L}[x] \subset \mathcal{L}_1[x]$, og man ser, at hvis $F \in \mathcal{L}[x]$ er reduktibelt i $\mathcal{L}[x]$, er F også reduktibelt i $\mathcal{L}_1[x]$, eller (hvad der kommer ud på det samme), hvis $F \in \mathcal{L}[x]$ er irreduktibelt i $\mathcal{L}_1[x]$, er F også irreduktibelt i $\mathcal{L}[x]$.

For et polynomium $F \in \mathcal{L}[x]$ finder man ud fra fremstillingen $F = a P_1 \cdots P_s$

ved hjælp af normerede irreduktible polynomier $P_1, \ldots, P_s$ i $\mathcal{L}[x]$ fremstillingen af F ved hjælp af normerede irreduktible polynomier i $\mathcal{L}_1[x]$, idet man for hvert af polynomierne $P_1, \ldots, P_s$ indsætter dets fremstilling ved hjælp af normerede irreduktible polynomier i $\mathcal{L}_1[x]$.

Som følge af hovedsætningen er det nu en væsentlig opgave for ethvert legeme $\mathcal{L}$ at bestemme eller i hvert fald undersøge de irreduktible polynomier i $\mathcal{L}[x]$. Det er allerede nævnt, at polynomierne i $\mathcal{L}[x]$ af grad 1 altid er irreduktible, og at disse i tilfældet $\mathcal{L} = \mathbb{C}$ er de eneste irreduktible polynomier.

Et tallegeme $\mathcal{L}$ med den egenskab, at polynomierne af grad 1 er de eneste irreduktible polynomier i $\mathcal{L}[x]$, kaldes <u>algebraisk afsluttet</u>. Man ser, at et tallegeme $\mathcal{L}$ er algebraisk afsluttet, hvis og kun hvis det for ethvert egentligt polynomium F i $\mathcal{L}[x]$ gælder, at samtlige rødder i F hilhører $\mathcal{L}$. På det nuværende trin kan vi ikke nævne noget andet eksempel på

et algebraisk afsluttet tallegeme end $\mathbb{C}$ selv. I § 11 skal vi møde endnu et eksempel.

For ethvert tallegeme $\mathcal{L}$ gælder, at et polynomium i $\mathcal{L}[x]$ af grad 2 er ireduktibelt, hvis og kun hvis ingen af rødderne tilhører $\mathcal{L}$.

Thi hvis en rod α tilhører $\mathcal{L}$, har polynomiet jo den ægte divisor $x-\alpha$ i $\mathcal{L}[x]$ og er altså reduktibelt i $\mathcal{L}[x]$, og hvis omvendt polynomiet er reduktibelt i $\mathcal{L}[x]$, altså har en ægte divisor i $\mathcal{L}[x]$, må det, da en sådan divisor må have grad 1, have en rod i $\mathcal{L}$.

Vi vil specielt betragte det tilfælde, hvor $\mathcal{L}$ er de reelle tals legeme $\mathbb{R}$. Som ireducible polynomier i $\mathbb{R}[x]$ har vi efter det foranstående dels polynomierne $ax+b$ af grad 1, dels polynomierne ax^2+bx+c af grad 2 med imaginære rødder, d. v. s. med $b^2-4ac<0$. Disse er de eneste ireducible polynomier i $\mathbb{R}[x]$. Thi hvis et polynomium $F = a_n x^n + \cdots + a_1 x + a_0$ i $\mathbb{R}[x]$ af grad n har rødderne $\alpha_1, \ldots, \alpha_n$, og altså fremstillingen

$$F = a_n x^n + \cdots + a_1 x + a_0 = a_n (x-\alpha_1)\cdots(x-\alpha_n),$$

fås ved konjugering

$$a_n \overline{x}^n + \cdots + a_1 \overline{x} + a_0 = a_n (\overline{x}-\overline{\alpha_1})\cdots(\overline{x}-\overline{\alpha_n}).$$

Følgelig gælder

$$F = a_n x^n + \cdots + a_1 x + a_0 = a_n (x-\overline{\alpha_1})\cdots(x-\overline{\alpha_n}).$$

De to talsæt $\alpha_1, \ldots, \alpha_n$ og $\overline{\alpha_1}, \ldots, \overline{\alpha_n}$ er altså bortset fra rækkefølgen det samme. Idet vi først skriver de reelle og derefter de imaginære rødder, kan talsættet altså skrives

$$\alpha_1, \ldots, \alpha_r, \xi_1+i\eta_1, \xi_1-i\eta_1, \ldots, \xi_s+i\eta_s, \xi_s-i\eta_s,$$

og fremstillingen bliver da

$$F = a_n (x-\alpha_1)\cdots(x-\alpha_r)(x^2-2\xi_1 x+\xi_1^2+\eta_1^2)\cdots(x^2-2\xi_s x+\xi_s^2+\eta_s^2).$$

Hermed er ikke blot vist, at der ikke er andre ireducible polynomier i $\mathbb{R}[x]$ end de nævnte, men vi kan

tillige ud fra rødderne fundet fremstillingen af et polynomium F i $R[x]$ ved hjælp af normerede irreduktible faktorer i $R[x]$.

For et vilkårligt tallegeme L gælder følgende simple sætninger:

(1) Hvis et irreduktibelt polynomium P i $L[x]$ har en rod fælles med et polynomium F i $L[x]$, er P divisor i F. (Det omvendte gælder naturligvis også.)

Thi $D = (F, P)$ er da af grad ≥ 1, og D tilhører $L[x]$. Da D er divisor i P, som er irreduktibelt, må P være associeret med D. Men D er divisor i F. Altså er P divisor i F.

(2) To forskellige normerede irreduktible polynomier i $L[x]$ har ingen fælles rod.

Thi hvis de havde en fælles rod, var hvert af dem divisor i det andet, og de var altså det samme polynomium.

(3) Ethvert irreduktibelt polynomium i $L[x]$ har lutter simple rødder.

Thi hvis et irreduktibelt polynomium P i $L[x]$ havde en multipel rod, var denne også rod i P', som ligeledes tilhører $L[x]$. Følgelig måtte P være divisor i P', hvilket er umuligt, da P' er af lavere grad.

§5. Polynomier med rationale koefficienter.

Af særlig interesse er studiet af integritetsringen $Q[x]$, hvor Q er de rationale tals legeme. For ethvert polynomium i $Q[x]$ findes associerede polynomier

med hele koefficienter (man multiplicerer blot med en fælles nævner for koefficienterne). Mange betragtninger over polynomier med rationale koefficienter henføres derfor til betragtninger over polynomier med hele koefficienter.

Hvis et egentligt polynomium $F = a_0 + a_1 x + \cdots + a_n x^n$ med hele koefficienter har en rational rod, og denne skrives som en uforkortelig brøk $\frac{a}{b}$, må a gå op i a_0 og b gå op i a_n.

Ved hjælp af denne sætning kan man finde alle rationale rødder i et polynomium med hele koefficienter, idet der kun bliver et endeligt antal mulighed at prøve.

Bevis. Ved indsætning og multiplikation med b^n fås $a_0 b^n + a_1 b^{n-1} a + \cdots + a_{n-1} b a^{n-1} + a_n a^n = 0$. Heraf ses, at a må gå op i $a_0 b^n$; da a og b er uden fælles primfaktor, gælder det samme om a og b^n; altså må a gå op i a_0. På samme måde ses, at b må gå op i a_n.

Et egentligt polynomium med hele koefficienter kaldes primitivt, hvis koefficienterne ikke har nogen fælles divisor > 1. Ethvert egentligt polynomium F i $Q[x]$ er associeret med et primitivt polynomium $F^* = a_0 + a_1 x + \cdots + a_n x^n$ med positiv øverste koefficient, nemlig det polynomium F^*, der fås af det med F associerede normerede polynomium ved at multiplicere med den mindste fælles nævner for dettes koefficienter. Et vilkårligt med F associeret polynomium i $Q[x]$ fås ved at multiplicere F^* med et rationalt tal $\neq 0$. Lad dette være skrevet som en uforkortelig

brøk $\frac{a}{b}$, $b \geq 1$. Man ser da, at $\frac{a}{b} F^*$ kun kan blive et polynomium med hele koefficienter, når $b=1$. Thi hvis b skal gå op i tallene $aa_0, aa_1, \ldots, aa_n$, må b gå op i tallene $a_0, a_1, \ldots, a_n$. Specielt gælder, at F^* og $-F^*$ er de eneste med F associerede primitive polynomier.

Gauss' sætning. Produktet af to primitive polynomier er igen et primitivt polynomium.

Bevis. Lad

$$F = a_0 + a_1 x + \cdots + a_n x^n \quad \text{og} \quad G = b_0 + b_1 x + \cdots + b_m x^m$$

være primitive polynomier. Produktet

$$FG = c_0 + c_1 x + \cdots + c_{n+m} x^{n+m}$$

har hele koefficienter. For at vise, at det er primitivt, er det nok at vise, at disse ikke har nogen fælles primfaktor p. Lad altså p være et vilkårligt primtal. Da F er primitivt, går p ikke op i alle koefficienterne $a_0, a_1, \ldots, a_n$. Lad a_k være den første, hvori p ikke går op. Da G er primitivt, går p ikke op i alle koefficienterne $b_0, b_1, \ldots, b_m$. Lad b_l være den første, hvori p ikke går op. Vi betragter nu c_{k+l}, der bestemmes som

$$c_{k+l} = a_k b_l + \left\{ \begin{array}{l} a_{k-1} b_{l+1} + a_{k-2} b_{l+2} + \cdots \\ a_{k+1} b_{l-1} + a_{k+2} b_{l-2} + \cdots \end{array} \right.$$

(hvor leddenes antal beror på nummeret). Nu går p op i alle produkterne til højre for klammen, men ikke i $a_k b_l$. Følgelig går p ikke op i c_{k+l}. Koefficienterne $c_0, c_1, \ldots, c_{n+m}$ har altså ingen fælles primfaktor.

Corollar. Idet vi for et vilkårligt egentligt ra-

lynomium F i $Q[x]$ med F^* betegner det med F associerede primitive polynomium med positiv øverste koefficient, gælder for vilkårlige polynomier F og G i $Q[x]$, at

$$H = FG \quad \text{medfører} \quad H^* = F^*G^*.$$

Thi F^*G^* er jo associeret med FG, altså med H og ifølge Gauss' sætning er F^*G^* primitivt. Da end videre øverste koefficient i F^*G^* er positiv, må F^*G^* være H^*.

Af særlig interesse er følgende specialtilfælde:

Hvis et normeret polynomium H med hele koefficienter er produkt af to normerede polynomier F og G med rationale koefficienter, må F og G have hele koefficienter.

Thi nu er $H^* = H$, altså $FG = F^*G^*$. Men F^* og G^* fremgår af F og G ved multiplikation med hele tal ≥ 1. Disse tal må da begge være 1.

Anderledes udtrykt:

Hvis et normeret polynomium F med rationale koefficienter er divisor i et normeret polynomium H med hele koefficienter, må F have hele koefficienter, og kvotienten G må ligeledes være et normeret polynomium med hele koefficienter.

Metode til at afgøre, om et polynomium i $Q[x]$ er reduktibelt, og til i bekræftende fald at bestemme dets opløsning i irreduktible faktorer i $Q[x]$.

I følge corollaret til Gauss' sætning er det tilstrækkeligt for et primitivt polynomium at undersøge, om det kan skrives som produkt af pri-

mitive polynomier af lavere grad. Vi illustrere metoden ved eksemplet

$$F = 2x^7 - 3x^5 + 2x^4 - 3x^3 - x^2 + x + 4.$$

Hvis F var reduktibelt, kunde det skrives $F = GH$, hvor G og H var primitive polynomier af lavere grad. Et af dem, f. eks. G, måtte da være af grad ≤ 3. Nu beregnes F for fire heltallige værdier af x, f. eks. $x = 0, 1, -1, 2$. For hver af disse fås $F(x) = G(x)H(x)$, hvor tallene alle er hele. Vi finder

$F(0) = 4 = 2 \cdot 2$
$F(1) = 2$
$F(-1) = 8 = 2 \cdot 2 \cdot 2$
$F(2) = 170 = 2 \cdot 5 \cdot 17$

hvoraf mu-
lighederne

$G(0) = -4, -2, -1, 1, 2, 4$
$G(1) = -2, -1, 1, 2$
$G(-1) = -8, -4, -2, -1, 1, 2, 4, 8$
$G(2) = 1, 2, 5, 10, 17, 34, 85, 170,$

idet vi kan disponere således, at $G(2) > 0$. Det giver ialt $6 \cdot 4 \cdot 3 \cdot 8 = 1536$ kombinationer. For hver af disse bestemmes (lettest ved brug af Lagranges interpolationsformel) det polynomium af grad ≤ 3, som i $0, 1, -1, 2$ har de omhandlede værdier. Af de fundne polynomier beholdes kun de, der er primitive og af grad ≥ 1. For disse prøves, om de er divisorer i F. Hvis man ikke finder nogen divisor, er F irreduktibelt; ellers er F reduktibelt, og det er let at finde dets opløsning i irreduktible faktorer, idet man nu kender alle dets primitive divisorer. — Tør man tage fat, lønner det sig prøve med andre hele værdier af x, idet arbejdet bliver mindre, jo mindre sammensatte værdier af $F(x)$ man finder.

Denne metode kan naturligvis kun benyttes for bestemte polynomier, ikke for typer af polynomier. Et vigtigt alment kriterium er følgende:

Schönemann - Eisensteins irreducibilitetskriterium (1846, 1850). Hvis der for et polynomium

$$F = a_0 + a_1 x + \cdots + a_n x^n$$

med hele koefficienter findes et primtal p, som går op i $a_0, a_1, \ldots, a_{n-1}$, men ikke i a_n, og hvis kvadrat p^2 ikke går op i a_0, da er F irreduktibelt i $\mathbb{Q}[x]$.

Bevis. Hvis F var reduktibelt, var ifølge corollaret til Gauss' sætning F^* produkt af to primitive polynomier af grad $< n$, og da $F = a F^*$, hvor a et tal, var F altså produkt af to polynomier af grad $< n$ med hele koefficienter, lad os sige $F = GH$, hvor

$$G = b_0 + b_1 x + \cdots + b_l x^l \quad \text{og} \quad H = c_0 + c_1 x + \cdots + c_m x^m,$$

hvor hele koefficienter, $l + m = n$ og $l < n$, $m < n$.

Vi har da følgende formler, i hvilke et b_j med $j > l$ og et c_k med $k > m$ skal betegne 0:

$$a_0 = b_0 c_0$$
$$a_1 = b_0 c_1 + b_1 c_0$$
$$\cdots$$
$$a_i = b_0 c_i + b_1 c_{i-1} + \cdots + b_{i-1} c_1 + b_i c_0$$
$$\cdots$$
$$a_n = b_0 c_n + b_1 c_{n-1} + \cdots + b_{n-1} c_1 + b_n c_0.$$

Vi ser først på a_0. Da p går op i a_0, medens p^2 ikke går op i a_0, må p gå op i et af tallene b_0 og c_0, men ikke i begge. Lad os sige, at p går op i b_0, men ikke i c_0. Vi ser så på a_1. Da p går op i a_1 og b_0, men ikke i c_0, må p gå op i b_1. Dette ræsonnement kan fortsættes frem til a_{n-1} og viser, at p går op i alle tallene $b_0, b_1, \ldots, b_{n-1}$. Men b_n betegner 0. Af udtrykket for a_n ser da, at p går op i a_n, i strid med antagelsen.

Eksempel. $x^n - 2$ er ireduktibelt for ethvert $n \geq 1$. Thi kriteriets betingelser er opfyldt for $p = 2$.

Der findes altså irreduktible polynomier i $\mathbb{Q}[x]$ af enhver grad ≥ 1.

Cirkeldelingspolynomiet svarende til et primtal.

Som et særlig vigtigt tilfælde betragtes for $p \geq 2$ polynomiet

$$F(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \frac{x^p - 1}{x - 1} = (x - \varepsilon_1) \cdots (x - \varepsilon_{p-1}),$$

hvor $\varepsilon_1, \ldots, \varepsilon_{p-1}$ betegner de fra 1 forskellige p^{te} enhedsrødder $\varepsilon_\nu = \cos \frac{2\pi}{p}\nu + i \sin \frac{2\pi}{p}\nu$.

Hvis p er sammensat, lad os sige $p = kl$, hvor $k > 1$, $l > 1$, er F reduktibelt i $\mathbb{Q}[x]$, idet

$$F = \frac{x^{kl} - 1}{x - 1} = \frac{(x^k)^l - 1}{x - 1} = \frac{(x^k - 1)(x^{k(l-1)} + x^{k(l-2)} + \cdots + x^k + 1)}{x - 1}$$

$$= (x^{k-1} + x^{k-2} + \cdots + x + 1)(x^{k(l-1)} + x^{k(l-2)} + \cdots + x^k + 1).$$

Derimod gælder: Hvis p er et primtal, er F irreduktibelt i $\mathbb{Q}[x]$. Dette ses ikke direkte ved betragtning af $F(x)$. Vi bemærker imidlertid, at hvis $G(x)$ er et polynomium i $\mathbb{Q}[x]$, vil også $H(x) = G(x + r)$ for ethvert $r \in \mathbb{Q}$ være et polynomium i $\mathbb{Q}[x]$, og de to polynomier vil samtidig være reduktible, resp. irreduktible. Thi af $G(x) = G_1(x)\, G_2(x)$, fås jo $H(x) = G_1(x + r)\, G_2(x + r)$, og af $H(x) = H_1(x)\, H_2(x)$ fås $G(x) = H_1(x - r)\, H_2(x - r)$. I stedet for at betragte $F(x)$, kan vi derfor betragte

$$F(x+1) = \frac{(x+1)^p - 1}{x + 1 - 1} = \frac{x^p + \binom{p}{1} x^{p-1} + \cdots + \binom{p}{p-1} x + 1 - 1}{x}$$

$$= x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + \binom{p}{p-2} x + \binom{p}{p-1} = a_{p-1} x^{p-1} + \cdots + a_0.$$

Dette polynomium har hele koefficienter og opfylder svarende til primtallet p betingelserne i Eisensteins kriterium. Thi $a_0 = \binom{p}{p-1} = p$. Altså går p op i a_0, men p^2 går ikke op i a_0.

Endvidere er $a_p \neq 1$. Altså går p ikke op i a_{p-1}. Og for $1 \leqslant r \leqslant p-2$ er

$$a_r = \binom{p}{p-r-1} = \frac{p(p-1)\cdots(p-r)}{1\cdot 2\cdots(r+1)}.$$

Dette er et helt tal; nævneren må altså kunne bortforkortes, men da nævneren ikke indeholder primfaktoren p, må faktoren p i tælleren forblive urørt ved forkortningen, hvilket viser, at p går op i a_r.

§6. Algebraiske og transcendente tal.

I slutningen af §4 viste vi for et vilkårligt tallegeme L tre sætninger om irreduktible polynomier i $L[x]$. Vi vil nu anvende disse sætninger i tilfældet $L = Q$ og eiterer dem udtrykkeligt i dette tilfælde.

(1) Hvis et irreduktibelt polynomium P i $Q[x]$ har en rod fælles med et polynomium F i $Q[x]$, er P divisor i F.

(2) To forskellige irreduktible polynomier i $Q[x]$ har ingen fælles rod.

(3) Ethvert irreduktibelt polynomium i $Q[x]$ har lutter simple rødder.

F normeret

Et tal kaldes <u>algebraisk</u>, hvis det er rod i et egentligt polynomium F i $Q[x]$.

<u>Ethvert algebraisk tal α er rod i netop et normeret irreduktibelt polynomium P i $Q[x]$.</u>

<u>Bevis.</u> Ifølge forudsætning er α rod i et egentligt polynomium $F \in Q[x]$. Dette kan skrives på formen $F = aP_1 \cdots P_s$, hvor $a \in Q$, $a \neq 0$, og $P_1, \ldots, P_s$ er normerede irreduktible polynomier i $Q[x]$. Man ser, at

α må være rod i et af disse polynomier. På den anden side kan α ifølge (2) ikke være rod i to forskellige normerede irreduktible polynomier i $\mathbb{Q}[x]$.

Det entydigt bestemte normerede irreduktible polynomium P i $\mathbb{Q}[x]$, der har et givet algebraisk tal α som rod, kaldes det <u>karakteristiske polynomium for</u> α, og dets grad kaldes <u>graden af</u> α.

Hvis α har graden n, har dets karakteristiske polynomium P ifølge (3) n indbyrdes forskellige rødder $\alpha_1, \ldots, \alpha_n$ (hvoriblandt α); disse er åbenbart alle algebraiske og har P som karakteristisk polynomium. Tallene $\alpha_1, \ldots, \alpha_n$ kaldes <u>indbyrdes konjugerede</u> algebraiske tal. (Denne brug af ordet konjugeret må naturligvis ikke sammenblandes med brugen af ordet i betydningen komplekst konjugeret.)

Ifølge (1) gælder: Hvis et algebraisk tal er rod i et polynomium i $\mathbb{Q}[x]$, er også alle dets konjugerede rødder i polynomiet.

De algebraiske tal af grad 1 er netop de rationale tal.

Et algebraisk tal kaldes <u>helt algebraisk</u>, hvis dets karakteristiske polynomium har <u>hele</u> koefficienter. Dets konjugerede tal er da også helt algebraiske.

Et rationalt tal er helt algebraisk, hvis og kun hvis det er et helt tal.

(I teorien for algebraiske tal benytter man ofte udtrykket „helt tal" i betydningen „helt algebraisk tal". Et helt tal i sædvanlig betydning kaldes da et „helt rationalt tal".)

Hvis et tal overhovedet er rod i et normeret polynomium med hele koefficienter, er det et helt alge-

brudt tal. Thi da har dets karakteristiske polynomium ifølge Gauss' sætning (specialtilfældet) også hele koefficienter.

Et vilkårligt algebraisk tal α har formen $\alpha = \frac{\beta}{h}$ hvor β er et helt algebraisk tal og h et helt tal $\neq 0$. Thi α er rod i et polynomium $a_n x^n + \dots + a_0$ med hele koefficienter og $a_n \neq 0$. Følgelig er $a_n\alpha$ rod i det normerede polynomium $x^n + a_{n-1}x^{n-1} + a_n a_{n-2} x^{n-2} + \dots + a_n^{n-2} a_1 x + a_n^{n-1} a_0$. Som β kan de for benyttes tallet $a_n\alpha$ og som h tallet a_n.

Et tal, der ikke er algebraisk, kaldes <u>transcendent</u>. At der findes transcendente tal er ikke på forhånd klart.

<u>Liouvilles eksempel på transcendente tal</u> (1844).

Som udgangspunkt for angivelsen af transcendente tal benyttes vi følgende sætning, der udtrykker at et algebraisk tal ikke kan approksimeres særlig godt med rationale tal.

<u>Hvis α er et reelt algebraisk tal af grad n, gælder det for enhver følge af rationale tal</u> $\frac{p_i}{q_i} \neq \alpha$ (p_i og q_i hele, $q_i > 0$), <u>som konvergerer mod α, at</u>

$$\left|\alpha - \frac{p_i}{q_i}\right| > \frac{1}{q_i^{n+1}} \quad \text{<u>for alle i fra et vist trin</u>.}$$

<u>Bevis</u>. Vi bemærker først, at det af sætningens antagelser følger, at $q_i \to +\infty$. Thi for ethvert helt tal $A > 0$ findes i mængden af brøken $\frac{p}{q} > \alpha$ med $0 < q \leq A$ en mindste og i mængden af brøken $\frac{p}{q} < \alpha$ med $0 < q \leq A$ en største. Der findes altså et $\delta > 0$ således, at det for enhver brøk $\frac{p}{q} \neq \alpha$ (med $q > 0$), for hvilken $\left|\alpha - \frac{p}{q}\right| < \delta$, gælder, at $q > A$. Følgelig gælder $q_i > A$ for alle i fra et vist trin.

Lad α være rod i polynomiet

$$F = a_0 + a_1 x + \cdots + a_n x^n$$

med hele koefficienter ($a_n \neq 0$). Vi vælger et interval $[\alpha - d, \alpha + d]$ på den reelle akse, hvori F ikke har nogen anden rod end α, og sætter

$$M = \max_{x \in [\alpha-d, \alpha+d]} |F'(x)|.$$

For enhver brøk $\frac{p}{q} \neq \alpha$ i $[\alpha - d, \alpha + d]$ fås da ved brug af middelværdisætningen

$$|F(\tfrac{p}{q})| = |F(\alpha) - F(\tfrac{p}{q})| \leqslant M |\alpha - \tfrac{p}{q}|.$$

Nu kan $F(\frac{p}{q}) = a_0 + a_1 \frac{p}{q} + \cdots + a_n \left(\frac{p}{q}\right)^n$ skrives som en brøk med nævner q^n. Da $F(\frac{p}{q}) \neq 0$ følger heraf, at $|F(\frac{p}{q})| \geqslant \frac{1}{q^n}$. Uligheden giver derfor

$$|\alpha - \tfrac{p}{q}| \geqslant \frac{1}{M q^n}$$

og følgelig $|\alpha - \frac{p}{q}| > \frac{1}{q^{n+1}}$ for $q > M$,

hvormed sætningen er bevist.

Ved hjælp heraf kan vi nu vise:

<u>Ethvert tal</u> α <u>bestemt ved en uendelig decimalbrø</u>

$$\alpha = 0, a_1 a_2 000 a_6 0 \cdots 0 a_{24} 0 \cdots 0 a_{120} 0 \cdots,$$

<u>i hvilken alle decimaler, som ikke hører til numrene</u> $i!$ ($i = 1, 2, \ldots$) <u>er</u> 0, <u>medens de øvrige er</u> > 0 (altså hver er et af tallene $1, 2, \cdots, 9$) <u>må være transcendent</u>.

Thi sættes

$$p_i = a_1 a_2 000 a_6 0 \cdots 0 a_{24} 0 \cdots 0 a_{i!}, \quad q_i = 10^{i!},$$

gælder $\frac{p_i}{q_i} \neq \alpha$ for alle i, og $\frac{p_i}{q_i} \to \alpha$. Hvis α var algebraisk af grad n, måtte altså for alle i fra et vist trin gælde

$$|\alpha - \frac{p_i}{q_i}| > \frac{1}{(10^{i!})^{n+1}}.$$

Men $\alpha - \frac{p_i}{q_i}$ fremstilles ved en uendelig decimalbrøk i hvilken den første fra 0 forskellige decimal har nummeret $(i+1)!$. Følgelig gælder

$$\left|\alpha - \frac{p_i}{q_i}\right| \leqslant \frac{1}{10^{(i+1)!-1}}.$$

Hvis α var algebraisk af grad n, måtte altså for alle i fra et vist trin gælde

$$\frac{1}{10^{i!(n+1)}} < \frac{1}{10^{(i+1)!-1}} \quad \text{d.v.s.} \quad i!(n+1) > (i+1)! - 1,$$

hvilket ikke kan være tilfældet, da $\frac{(i+1)!-1}{i!} \to +\infty$ for $i \to +\infty$.

Et helt andet bevis for eksistensen af transcendente tal skyldes Cantor 1874, der viste, at mængden af alle algebraiske tal er numererbar, medens mængden af alle tal ikke er numererbar.

§7. Polynomier af flere variable.

Med $\mathbb{C}[x_1, x_2, \cdots, x_n]$ betegner vi mængden af polynomier

$$F = F(x_1, x_2, \cdots, x_n) = \sum a_{p_1, p_2 \cdots p_n} x_1^{p_1} x_2^{p_2} \cdots x_n^{p_n},$$

hvor summen skal udstrækkes over et endeligt antal af indbyrdes forskellige sæt $(p_1, p_2, \cdots, p_n)$ af hele tal $\geqslant 0$, og koefficienterne $a_{p_1, p_2 \cdots p_n}$ er komplekse tal, medens $x_1, x_2, \cdots, x_n$ er komplekse variable. Et polynomium er åbenbart en kontinuert funktion på $\mathbb{C}^n$ med værdier i $\mathbb{C}$.

Identitetssætningen. To polynomier i $\mathbb{C}[x_1, x_2, \cdots, x_n]$, der stemmer overens i værdi for alle talsæt $(x_1, x_2, \cdots, x_n) \in \mathbb{C}^n$, er identiske, d.v.s.

hvis de to polynomier skrives på formen

$$F(x_1, x_2, \cdots, x_n) = \sum_{\substack{0 \leq p_1 \leq m_1 \\ 0 \leq p_2 \leq m_2 \\ \cdots \\ 0 \leq p_n \leq m_n}} a_{p_1 p_2 \cdots p_n} x_1^{p_1} x_2^{p_2} \cdots x_n^{p_n}$$

og

$$G(x_1, x_2, \cdots, x_n) = \sum_{\substack{0 \leq p_1 \leq m_1 \\ 0 \leq p_2 \leq m_2 \\ \cdots \\ 0 \leq p_n \leq m_n}} b_{p_1 p_2 \cdots p_n} x_1^{p_1} x_2^{p_2} \cdots x_n^{p_n}$$

med samme $m_1, m_2, \cdots, m_n$ [hvad der er muligt ved evt. tilføjelse af nulled], gælder

$$a_{p_1 p_2 \cdots p_n} = b_{p_1 p_2 \cdots p_n} \text{ for alle } (p_1, p_2, \cdots, p_n)$$

med $0 \leq p_1 \leq m_1, 0 \leq p_2 \leq m_2, \cdots, 0 \leq p_n \leq m_n$.

Bevis. Vi fører beviset for $n = 2$. For vilkårligt n indføres sætningen ved samme slutningsmåde under brug af induktion. Vi har

$$F(x_1, x_2) = \sum_{p_2=0}^{m_2} f_{p_2}(x_1) x_2^{p_2}, \text{ hvor } f_{p_2}(x_1) = \sum_{p_1=0}^{m_1} a_{p_1 p_2} x_1^{p_1}$$

$$G(x_1, x_2) = \sum_{p_2=0}^{m_2} g_{p_2}(x_1) x_2^{p_2}, \text{ hvor } g_{p_2}(x_1) = \sum_{p_1=0}^{m_1} b_{p_1 p_2} x_1^{p_1}.$$

For fastholdt x_1 viser identitetssætningen for polynomier af en variabel, at $f_{p_2}(x_1) = g_{p_2}(x_1)$ for alle p_2 med $0 \leq p_2 \leq m_2$. Samme sætning viser derefter, at der for hvert p_2 gælder $a_{p_1 p_2} = b_{p_1 p_2}$ for alle p_1 med $0 \leq p_1 \leq m_1$.

Hvis for et polynomium $F \in \mathbb{C}[x_1, x_2, \cdots, x_n]$ alle koefficienterne er 0, kaldes F nulpolynomiet og skrives 0. Ellers kaldes F et egentligt polyno-

minum. Ved graden af et led $a x_1^{p_1} x_2^{p_2} \dots x_n^{p_n}$ med $a \neq 0$ forstås $p_1 + p_2 + \dots + p_n$, medens p_i kaldes leddets grad efter x_i. Ved graden af et egentligt polynomium F forstås den højeste forekommende grad af leddene med koefficient $\neq 0$; ved graden efter x_i forstås den højeste forekommende grad efter x_i af leddene med koefficient $\neq 0$. Man ser let, at der gælder

$$\text{grad efter hvert } x_i \leqslant \text{grad} \leqslant \sum_{i=1}^{n} \text{grad efter } x_i .$$

Graden af leddene er ikke nok til at bestemme en ordning af leddene. Derfor indføres begrebet signatur. Ved signaturen af et led $a x_1^{p_1} x_2^{p_2} \dots x_n^{p_n}$ med $a \neq 0$ forstås talsættet $(p_i) = (p_1, p_2, \dots, p_n)$. Mængden af signaturer ordnes nu ved, at man først ordner efter grad og derefter inden for hver grad ordner teksikografisk, d. v. s. for to forskellige signaturer $(p_1, p_2, \dots, p_n)$ og $(q_1, q_2, \dots, q_n)$ skriver vi

$$(p_1, p_2, \dots, p_n) \prec (q_1, q_2, \dots, q_n),$$

hvis enten $p_1 + p_2 + \dots + p_n < q_1 + q_2 + \dots + q_n$ eller $p_1 + p_2 + \dots + p_n = q_1 + q_2 + \dots + q_n$ og $p_i < q_i$ for det første (d. v. s. det mindste) i, for hvilket $p_i \neq q_i$. Man viser let, at dette virkelig er en ordning af mængden af alle signaturer. Ved signaturen af et egentligt polynomium forstås nu den højeste forekommende signatur.

Eksempel. For $n = 2$ er ordningen følgende:
$(0,0), (0,1), (1,0), (0,2), (1,1), (2,0), (0,3), (1,2), (2,1), (3,0)$, o. s. v.

Ligesom for polynomier af en variabel gælder

det, at addition og multiplikation er kompositionsregler i $\mathbb{C}[x_1, x_2, \cdots, x_n]$. Med disse kompositionsregler er $\mathbb{C}[x_1, x_2, \cdots, x_n]$ en integritetsring. Gyldigheden af nulreglen er indeholdt i følgende

Sætning. Produktet af to egentlige polynomier i $\mathbb{C}[x_1, x_2, \cdots, x_n]$ er egentligt, og leddet af højest signatur i produktet er produktet af leddene af højest signatur i de to polynomier.

Bevis. Herfra må vises:

$(p_i) < (q_i)$ og $(r_i) < (s_i)$ medfører $(p_i + r_i) < (q_i + s_i)$

$(p_i) = (q_i)$ og $(r_i) < (s_i)$ medfører $(p_i + r_i) < (q_i + s_i)$

$(p_i) < (q_i)$ og $(r_i) = (s_i)$ medfører $(p_i + r_i) < (q_i + s_i)$.

Hvis enten $\sum p_i < \sum q_i$ eller $\sum r_i < \sum s_i$, er sagen klar, idet $(p_i + r_i)$ så har lavere grad end $(q_i + s_i)$. Hvis $\sum p_i = \sum q_i$ og $\sum r_i = \sum s_i$, har $(p_i + r_i)$ og $(q_i + s_i)$ samme grad. Vi betragter da det første i, for hvilket $p_i \neq q_i$ eller $r_i \neq s_i$. Da er $p_i \leqslant q_i$ og $r_i \leqslant s_i$; og i mindst en af disse relationer gælder tegnet $<$. Følgelig er i den første index, for hvilken $p_i + r_i \neq q_i + s_i$, og der gælder $p_i + r_i < q_i + s_i$.

Indsættes i et polynomium $F(x_1, x_2, \cdots, x_n) \in \mathbb{C}[x_1, x_2, \cdots, x_n]$ for $x_1, x_2, \cdots, x_n$ polynomier $\mathcal{G}_1(y_1, \cdots y_m)$, $\mathcal{G}_2(y_1, \cdots, y_m), \cdots, \mathcal{G}_n(y_1, \cdots y_m) \in \mathbb{C}[y_1, \cdots, y_m]$, fås et polynomium $F(\mathcal{G}_1, \mathcal{G}_2, \cdots, \mathcal{G}_n) \in \mathbb{C}[y_1, \cdots, y_m]$.

[Et polynomium, i hvilket alle led har samme grad, kaldes homogent, eller en form.]

I det $\mathbb{L}$ er et tallegeme, betegner $\mathbb{L}[x_1, x_2, \cdots, x_n]$ mængden af polynomier $F(x_1, x_2, \cdots, x_n)$ med koefficienter fra $\mathbb{L}$. Det er en delintegritetsring af $\mathbb{C}[x_1, x_2, \cdots, x_n]$.

§8. Symmetriske polynomier.

Et polynomium $S = S(\alpha_1, \dots, \alpha_n)$ i $\mathbb{C}[\alpha_1, \dots, \alpha_n]$ — af grunde, som senere vil træde frem, betegner vi de variable med $\alpha_1, \dots, \alpha_n$ i stedet for $x_1, \dots, x_n$ — kaldes <u>symmetrisk</u>, hvis det for ethvert talsæt $\alpha_1, \dots, \alpha_n$ og enhver permutation $\nu_1, \dots, \nu_n$ af $1, \dots, n$ gælder, at

$$S(\alpha_{\nu_1}, \dots, \alpha_{\nu_n}) = S(\alpha_1, \dots, \alpha_n).$$

Ifølge identitetssætningen er dette ensbetydende med, at det polynomium, der fremgår af S ved at erstatte $\alpha_1, \dots, \alpha_n$ med $\alpha_{\nu_1}, \dots, \alpha_{\nu_n}$ for enhver permutation $\nu_1, \dots, \nu_n$ af $1, \dots, n$ er identisk med S.

Hvis vi i et vilkårligt polynomium $T = T(y_1, \dots, y_p)$ i $\mathbb{C}[y_1, \dots, y_p]$ for $y_1, \dots, y_p$ indsætter symmetriske polynomier $S_1(\alpha_1, \dots, \alpha_n), \dots, S_p(\alpha_1, \dots, \alpha_n)$, fremkommer åbenbart et symmetrisk polynomium $T(S_1, \dots, S_p)$ i $\mathbb{C}[\alpha_1, \dots, \alpha_n]$.

Et polynomium $S(x_1, \dots, x_s; \alpha_1, \dots, \alpha_n)$ i $\mathbb{C}[x_1, \dots, x_s; \alpha_1, \dots, \alpha_n]$ kan være symmetrisk <u>i de variable</u> $\alpha_1, \dots, \alpha_n$ <u>for sig</u>. Skriver vi polynomiet som et polynomium $\sum c_{\rho_1, \dots, \rho_s}(\alpha_1, \dots, \alpha_n) x_1^{\rho_1} \dots x_s^{\rho_s}$ i de variable $x_1, \dots, x_s$ med koefficienter fra $\mathbb{C}[\alpha_1, \dots, \alpha_n]$, er symmetrien i $\alpha_1, \dots, \alpha_n$ ensbetydende med, at alle polynomierne $c_{\rho_1, \dots, \rho_s}(\alpha_1, \dots, \alpha_n)$ er symmetriske.

Et eksempel herpå er polynomiet

$$S(x; \alpha_1, \dots, \alpha_n) = (x - \alpha_1) \dots (x - \alpha_n)$$
$$= x^n + a_1(\alpha_1, \dots, \alpha_n) x^{n-1} + \dots + a_n(\alpha_1, \dots, \alpha_n).$$

De her optrædende koefficientpolynomier

$$a_1 = -(\alpha_1 + \cdots + \alpha_n)$$
$$a_2 = +(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_{n-1}\alpha_n)$$
$$\cdots$$
$$a_n = (-1)^n \alpha_1 \cdots \alpha_n$$

kaldes de <u>elementarsymmetriske polynomier</u> i de variable $\alpha_1, \ldots, \alpha_n$. Det p^{te} elementarsymmetriske polynomium $a_p = a_p(\alpha_1, \ldots, \alpha_n)$ er bestemt som

$$a_p = (-1)^p \sum \alpha_{i_1} \cdots \alpha_{i_p},$$

hvor summationen skal udstrækkes over de $\binom{n}{p}$ sæt af indices $i_1, \ldots, i_p$, $1 \leqslant i_1 < \cdots < i_p \leqslant n$.

<u>Hovedsætning.</u> <u>For ethvert symmetrisk polynomium</u> $S = S(\alpha_1, \ldots, \alpha_n)$ <u>i</u> $\mathbb{C}[\alpha_1, \ldots, \alpha_n]$ <u>findes et og kun et polynomium</u> $T = T(a_1, \ldots, a_n)$ i $\mathbb{C}[a_1, \ldots, a_n]$ <u>således, at når vi i</u> T <u>for</u> $a_1, \ldots, a_n$ <u>indsætter de elementarsymmetriske polynomier i</u> $\alpha_1, \ldots, \alpha_n$ <u>får</u> S. <u>Vi skriver kort</u>

$$S(\alpha_1, \ldots, \alpha_n) = T(a_1, \ldots, a_n).$$

<u>Bevis.</u> (1) Vi beviser først <u>eksistensen</u> af et sådant polynomium T, idet vi simpelthen angiver en fremgangsmåde til at finde det.

Hvis S er nulpolynomiet, er sagen klar, idet vi for T kan benytte nulpolynomiet. Hvis S ikke er nulpolynomiet, betragter vi det led $c\alpha_1^{p_1} \cdots \alpha_n^{p_n}$ i S, der har den højeste signatur $(p_1, \ldots, p_n)$. Signaturen $(p_1, \ldots, p_n)$ er altså det, vi kalder polynomiets signatur. Da S er symmetrisk, vil S for enhver permutation $\nu_1, \ldots, \nu_n$ af $1, \ldots, n$ også indeholde leddet $c\alpha_{\nu_1}^{p_1} \cdots \alpha_{\nu_n}^{p_n}$. Specielt må S for to vilkårlige indices i og j, $1 \leqslant i < j \leqslant n$, indeholde leddet $c\alpha_1^{p_1} \cdots \alpha_j^{p_i} \cdots \alpha_i^{p_j} \cdots \alpha_n^{p_n} =$

$c\alpha_1^{p_1}\cdots\alpha_i^{p_1}\cdots\alpha_j^{p_i}\cdots\alpha_n^{p_n}$, hvis signatur $(p_1,\cdots,p_j,\cdots,p_i,\cdots,p_n)$ fremgår af den højeste signatur $(p_1,\cdots,p_i,\cdots,p_j,\cdots,p_n)$ ved ombytning af p_i og p_j. De to led har samme grad. Vi slutter altså, at $p_i \not\geq p_j$. For den højeste signatur gælder altså $p_1 \geq \cdots \geq p_n$.

Betragtes specielt polynomierne $a_1, a_2, \cdots, a_n$, ser vi, at disse som led af højest signatur har henholdsvis $-\alpha_1, +\alpha_1\alpha_2, \cdots, (-1)^n\alpha_1\cdots\alpha_n$. Signaturerne af disse er $(1,0,\cdots,0), (1,1,0,\cdots,0), \cdots, (1,1,\cdots,1)$. Da leddet af højest signatur i et produkt af to — og følgelig også i et produkt af et vilkårligt antal — polynomier er produktet af leddene af højest signatur, vil polynomiet $a_1^{q_1}a_2^{q_2}\cdots a_n^{q_n}$ for vilkårlige hele $q_i \geq 0$ som led af højest signatur have

$$(-\alpha_1)^{q_1}(+\alpha_1\alpha_2)^{q_2}\cdots((-1)^n\alpha_1\cdots\alpha_n)^{q_n},$$

hvis signatur er

$$(q_1+q_2+\cdots+q_n, q_2+\cdots+q_n, \cdots, q_n).$$

Vælger vi $q_1 = p_1-p_2$, $q_2 = p_2-p_3, \cdots, q_{n-1} = p_{n-1}-p_n, q_n = p_n$, bliver dette netop signaturen $(p_1,\cdots,p_n)$. For også at få den rigtige koefficient c skal vi betragte $c(-a_1)^{q_1}(+a_2)^{q_2}\cdots((-1)^n a_n)^{q_n}$.

Differensen

$$S - c(-a_1)^{q_1}(+a_2)^{q_2}\cdots((-1)^n a_n)^{q_n}$$

vil derfor enten være nulpolynomiet eller et symmetrisk polynomium $S_1 = S_1(\alpha_1,\cdots,\alpha_n)$ af lavere signatur end S. Fortsættes med dette må vi efter et antal skridt nå til nulpolynomiet. De efterhånden subtraherede udtryk udgør tilsammen et

polynomium $T = T(a_1, \ldots, a_n)$ af den ønskede art.

(2) Vi beviser dernæst entydigheden af polynomiet T. Lad altså T_1 og T_2 være to polynomier af den ønskede art. Vi skal vise, at så er $T_1 - T_2$ nulpolynomiet.

Lad i modsat fald $d\, a_1^{r_1} \ldots a_n^{r_n}$ med $d \neq 0$ være et led i $T_1 - T_2$. Indsættes heri for $a_1, \ldots, a_n$ de elementarsymmetriske polynomier, fås ifølge det foranstående et polynomium i $x_1, \ldots, x_n$, i hvilket leddet af højest signatur er

$$d(-x_1)^{r_1}(+x_1x_2)^{r_2} \ldots ((-1)^n x_1 \ldots x_n)^{r_n}.$$

Signaturen af dette led er

$$(r_1 + r_2 + \cdots + r_n,\ r_2 + \cdots + r_n,\ \ldots,\ r_n).$$

Betragter vi nu først de led i $T_1 - T_2$, for hvilke $r_1 + \cdots + r_n$ er størst, derefter blandt disse de led, for hvilke $r_2 + \cdots + r_n$ er størst, u. s. v., får vi i $T_1 - T_2$ udskilt et bestemt led $d\, a_1^{r_1} \ldots a_n^{r_n}$ med den egenskab, at det og kun det ved indsætning af de elementarsymmetriske polynomier fører til et led med den omhandlede signatur $(r_1 + r_2 + \cdots + r_n,\ r_2 + \cdots + r_n,\ \ldots,\ r_n)$. Dette er imidlertid i strid med, at det ved indsætningen fremkomne polynomium skal være nulpolynomiet.

Tilføjelse til hovedsætningen. Hvis det symmetriske polynomium $S = S(x_1, \ldots, x_n)$ har lutter rationale, resp. lutter hele koefficienter, får det tilsvarende polynomium $T = T(a_1, \ldots, a_n)$ lutter rationale, resp. lutter hele koefficienter.

Dette fremgår umiddelbart af den i beviset for hovedsætningen givne fremgangsmåde til at finde T.

En umiddelbar generalisation af hovedsætningen og tilføjelsen til den er følgende:

For ethvert polynomium $S = S(x_1, \dots, x_s; a_1, \dots, a_n)$, der er symmetrisk i de variable $x_1, \dots, x_n$ for sig, findes et og kun et polynomium $T = T(x_1, \dots, x_s; a_1, \dots, a_n)$, af hvilket det fremgår, når man for $a_1, \dots, a_n$ indsætter de elementarsymmetriske polynomier i $x_1, \dots, x_n$.

Hvis S har brøker rationale, resp. brøker hele koefficienter, får T brøker rationale, resp. brøker hele koefficienter.

Eksistensen ses, ved at man skriver S på formen $\sum c_{p_1, \dots, p_s}(x_1, \dots, x_n) x_1^{p_1} \dots x_s^{p_s}$, hvor koefficienterne $c_{p_1, \dots, p_s}(x_1, \dots, x_n)$ er symmetriske polynomier i $x_1, \dots, x_n$. Entydigheden følger af, at hvis et polynomium T af den ønskede art skrives på formen $\sum d_{p_1, \dots, p_s}(a_1, \dots, a_n) x_1^{p_1} \dots x_s^{p_s}$, må $c_{p_1, \dots, p_s}(x_1, \dots, x_n)$ fremgå af polynomiet $d_{p_1, \dots, p_s}(a_1, \dots, a_n)$, ved at man for $a_1, \dots, a_n$ indsætter de elementarsymmetriske polynomier i $x_1, \dots, x_n$.

Vi kan også betragte polynomier $S = S(x_1, \dots, x_s; \alpha_1, \dots, \alpha_n; \beta_1, \dots, \beta_m)$, der er symmetriske i de variable $\alpha_1, \dots, \alpha_n$ for sig og i de variable $\beta_1, \dots, \beta_m$ for sig. Forsåvidt de elementarsymmetriske polynomier $a_1, \dots, a_n$ i $\alpha_1, \dots, \alpha_n$ får vi da brug for de elementarsymmetriske polynomier

$$b_1 = -(\beta_1 + \dots + \beta_m)$$
$$b_2 = +(\beta_1\beta_2 + \beta_1\beta_3 + \dots + \beta_{m-1}\beta_m)$$
$$\dots$$
$$b_m = (-1)^m \beta_1 \dots \beta_m$$

i $\beta_1, \dots, \beta_m$. Ved at anvende foranstående sætning

to gange finder vi:

For ethvert polynomium $S = S(x_1,\dots,x_s;\alpha_1,\dots,\alpha_n;\beta_1,\dots,\beta_m)$, der er symmetrisk i de variable $\alpha_1,\dots,\alpha_n$ for sig og i de variable $\beta_1,\dots,\beta_m$ for sig, findes et og kun et polynomium $T = T(x_1,\dots,x_s;a_1,\dots,a_n;b_1,\dots,b_m)$, af hvilket det frengår, når man for $a_1,\dots,a_n$ indsætter de elementarsymmetriske polynomier i $\alpha_1,\dots,\alpha_n$ og for $b_1,\dots,b_m$ de elementarsymmetriske polynomier i $\beta_1,\dots,\beta_m$.

Hvis S har hutter rationale, resp. hutter hele koefficienter, får T hutter rationale, resp. hutter hele koefficienter.

Som nemt sluttes i to skridt: Først ses, at der til S findes et og kun et polynomium $U = U(x_1,\dots,x_s;\alpha_1,\dots,\alpha_n;b_1,\dots,b_m)$, af hvilket S frengår ved at man for $b_1,\dots,b_m$ indsætter de elementarsymmetriske polynomier i $\beta_1,\dots,\beta_m$. Da S ikke forandres, ved at man for en vilkårlig permutation $\nu_1,\dots,\nu_n$ af $1,\dots,n$ erstatter $\alpha_1,\dots,\alpha_n$ med $\alpha_{\nu_1},\dots,\alpha_{\nu_n}$, må det samme gælde om U; altså er også U symmetrisk i de variable $\alpha_1,\dots,\alpha_n$ for sig. Der eksisterer derfor et og kun et polynomium $T = T(x_1,\dots,x_s;a_1,\dots,a_n;b_1,\dots,b_m)$, hvoraf U frengår, ved at man for $a_1,\dots,a_n$ indsætter de elementarsymmetriske polynomier i $\alpha_1,\dots,\alpha_n$. Af dette T og kun af dette frengår S, ved at man foretager begge indsætninger.

Ved induktion udvides sætningen til polynomier, i hvilke der foruden vilkårlige variable $x_1,\dots,x_s$ optræder et antal variabelsæt, og som er symmetriske i hvert af disse sæt af variable for sig.

§ 9. Potenssummer.

Hvis $a_1, \cdots, a_n$ er givne tal, og polynomiet $F(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ har rødderne $\alpha_1, \cdots, \alpha_n$, altså

$$F(x) = x^n + a_1 x^{n-1} + \cdots + a_n = (x-\alpha_1)\cdots(x-\alpha_n),$$

er $a_1, \cdots, a_n$ naturligvis værdierne for talsættet $\alpha_1, \cdots, \alpha_n$ af de elementarsymmetriske polynomier. Værdien af et vilkårligt symmetrisk polynomium $f(\alpha_1, \cdots, \alpha_n)$ for talsættet $\alpha_1, \cdots, \alpha_n$ er derfor lig med værdien for talsættet $a_1, \cdots, a_n$ af det ifølge hovedsætningen om symmetriske polynomier til $f(\alpha_1, \cdots, \alpha_n)$ svarende polynomium $F(a_1, \cdots, a_n)$.

Tallet $f(\alpha_1, \cdots, \alpha_n)$ kan altså beregnes alene ud fra kendskabet til koefficienterne $a_1, \cdots, a_n$, uden at man behøver at bestemme rødderne $\alpha_1, \cdots, \alpha_n$.

Som et eksempel vil vi bestemme røddernes potenssummer

$$s_m = \alpha_1^m + \cdots + \alpha_n^m, \quad m = 1, 2, \cdots.$$

Ved at differentiere de to udtryk for $F(x)$ får vi, idet vi benytter den let beviste regel, at den afledede af et produkt $g_1(x)\cdots g_n(x)$ er summen af de n polynomier $g_1(x)\cdots g_{i-1}(x)\, g_i'(x)\, g_{i+1}(x)\cdots g_n(x)$, $i = 1, \cdots, n$, at

$$F'(x) = n x^{n-1} + (n-1) a_1 x^{n-2} + \cdots + a_{n-1}$$

$$= \frac{F(x)}{x-\alpha_1} + \cdots + \frac{F(x)}{x-\alpha_n}.$$

Nu er

$$\frac{F(x)}{x-\alpha_i} = \frac{F(x) - F(\alpha_i)}{x-\alpha_i}$$

$$= \frac{x^n - \alpha_i^n}{x-\alpha_i} + a_1 \frac{x^{n-1} - \alpha_i^{n-1}}{x-\alpha_i} + \cdots + a_{n-1} \frac{x-\alpha_i}{x-\alpha_i}$$

$$= x^{n-1} + \alpha_i x^{n-2} + \alpha_i^2 x^{n-3} + \cdots + \alpha_i^{n-1}$$
$$+ a_1 (x^{n-2} + \alpha_i x^{n-3} + \cdots + \alpha_i^{n-2})$$
$$+ \cdots$$
$$+ a_{n-1}.$$

Ved addition fås et udtryk for $F(x)$, som sammenholdt med det første udtryk for $F'(x)$ giver

$$\begin{aligned} &s_1 + n a_1 &&= (n-1) a_1 \\ &s_2 + a_1 s_1 + n a_2 &&= (n-2) a_2 \\ &\cdots \\ &s_{n-1} + a_1 s_{n-2} + \cdots + a_{n-2} s_1 + n a_{n-1} &&= 1 \cdot a_{n-1}. \end{aligned}$$

Nu er

$$\alpha_i^n + a_1 \alpha_i^{n-1} + \cdots + a_{n-1} \alpha_i + a_n = 0.$$

Ved addition fås

$$s_n + a_1 s_{n-1} + \cdots + a_{n-1} s_1 + n a_n = 0.$$

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

$$\alpha_i^{n+k} + a_1 \alpha_i^{n+k-1} + \cdots + a_{n-1} \alpha_i^{k+1} + a_n \alpha_i^k = 0.$$

Ved addition fås

$$s_{n+k} + a_1 s_{n+k-1} + \cdots + a_{n-1} s_{k+1} + a_n s_k = 0.$$

De udledte formler, der kaldes <u>Newtons formler</u>, kan for alle n skrives på formen

$$\begin{aligned} &s_1 + a_1 = 0 \\ &s_2 + a_1 s_1 + 2a_2 = 0 \\ (*) \qquad &s_3 + a_1 s_2 + a_2 s_1 + 3a_3 = 0 \\ &\cdots \\ &s_q + a_1 s_{q-1} + a_2 s_{q-2} + \cdots + a_{q-1} s_1 + q a_q = 0 \\ &\cdots, \end{aligned}$$

idet formelsystemet for et bestemt n fremkommer, ved at man erstatter alle a_l, for hvilke $l > n$, med 0.

Af disse formler kan man successivt beregne $s_1, s_2, \ldots$. Man finder

$$s_1 = -a_1$$
$$s_2 = a_1^2 - 2a_2$$
$$s_3 = -a_1^3 + 3a_1a_2 - 3a_3$$
$$s_4 = a_1^4 - 4a_1^2a_2 + 4a_1a_3 + 2a_2^2 - 4a_4$$
$$\ldots.$$

Et eksplicit udtryk for s_q fås, idet man skriver de q første af ligningerne (*) på formen

$$\begin{aligned} s_1 &= -a_1 \\ a_1s_1 + s_2 &= -2a_2 \\ a_2s_1 + a_1s_2 + s_3 &= -3a_3 \\ &\ldots \\ a_{q-1}s_1 + a_{q-2}s_2 + \cdots + a_1s_{q-1} + s_q &= -qa_q. \end{aligned}$$

Dette er et lineært ligningssystem i $s_1, \ldots, s_q$ med determinant 1. Vi får altså

$$s_q = \det \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & -a_1 \\ a_1 & 1 & 0 & \cdots & 0 & -2a_2 \\ a_2 & a_1 & 1 & \cdots & 0 & -3a_3 \\ \cdots & & & & & \\ a_{q-1} & a_{q-2} & a_{q-3} & \cdots & a_1 & -qa_q \end{pmatrix}.$$

§10. Resultant og diskriminant.

Lad $F(x)$ og $G(x)$ være to vilkårlige normerede polynomier:

$$F(x) = x^n + a_1x^{n-1} + \cdots + a_n = (x-\alpha_1)\cdots(x-\alpha_n)$$

og

$$G(x) = x^m + b_1x^{m-1} + \cdots + b_m = (x-\beta_1)\cdots(x-\beta_m).$$

Ved <u>resultanten</u> $R(F,G)$ af de to polynomier F og G, nævnt i denne orden, forstås tallet

$$R(F,G) = \prod_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}} (\alpha_i - \beta_j).$$

For givne gradtal n og m vil vi nu opfatte $\alpha_1, \ldots, \alpha_n$ og $\beta_1, \ldots, \beta_m$ som variable. Det anførte produkt er da et polynomium $S(\alpha_1, \ldots, \alpha_n; \beta_1, \ldots, \beta_m)$, som er symmetrisk i de variable $\alpha_1, \ldots, \alpha_n$ for sig og i de variable $\beta_1, \ldots, \beta_m$ for sig. Der findes altså et og kun et polynomium $T(a_1, \ldots, a_n; b_1, \ldots, b_m)$, hvor af S fremgår, når man for $a_1, \ldots, a_n$ indsætter de elementarsymmetriske polynomier i $\alpha_1, \ldots, \alpha_n$ og for $b_1, \ldots, b_m$ de elementarsymmetriske polynomier i $\beta_1, \ldots, \beta_m$. Resultanten $R(F, G)$ af de to givne polynomier F og G er altså simpelthen værdien af polynomiet T for det ved koefficienterne $a_1, \ldots, a_n$ og $b_1, \ldots, b_m$ bestemte talsæt:

$$R(F, G) = T(a_1, \ldots, a_n; b_1, \ldots, b_m).$$

Af definitionen fås umiddelbart

$$R(G, F) = (-1)^{nm} R(F, G).$$

Resultantens betydning ligger i følgende sætning, hvis rigtighed umiddelbart fremgår af definitionen:

<u>En nødvendig og tilstrækkelig betingelse for, at de to polynomier F og G kan en fælles rod, er at</u>

$$R(F, G) = 0.$$

For givet n og m er $T(a_1, \ldots, a_n; b_1, \ldots, b_m)$ et ganske bestemt polynomium i de $n+m$ variable $a_1, \ldots, a_n; b_1, \ldots, b_m$. Man kan opskrive dette eksplicit ved hjælp af determinanten. Dette vil vi dog ikke udføre. Alment gælder

$$R(F, G) = \prod_{i=1}^{n} \prod_{j=1}^{m} (\alpha_i - \beta_j) = \prod_{i=1}^{n} G(\alpha_i) = \prod_{i=1}^{n} (\alpha_i^m + b_1 \alpha_i^{m-1} + \ldots + b_m).$$

Anvendes dette for eksempel for $n=2$, $m=2$, hvor
$F(x)=x^2+a_1x+a_2=(x-\alpha_1)(x-\alpha_2)$, $G(x)=x^2+b_1x+b_2=(x-\beta_1)(x-\beta_2)$,
fås

$$\begin{aligned}R(F,G)&=(\alpha_1^2+b_1\alpha_1+b_2)(\alpha_2^2+b_1\alpha_2+b_2)\\&=\alpha_1^2\alpha_2^2+b_1(\alpha_1^2\alpha_2+\alpha_1\alpha_2^2)+b_2(\alpha_1^2+\alpha_2^2)+b_1^2\alpha_1\alpha_2\\&\quad+b_1b_2(\alpha_1+\alpha_2)+b_2^2\\&=a_2^2+b_1(-a_1a_2)+b_2(a_1^2-2a_2)+b_1^2a_2\\&\quad+b_1b_2(-a_1)+b_2^2,\end{aligned}$$

altså

$$R(F,G)=a_2^2-a_1a_2b_1+a_1^2b_2-2a_2b_2+a_2b_1^2-a_1b_1b_2+b_2^2.$$

Sammen med et vilkårligt normeret polynomium

$$F(x)=x^n+a_1x^{n-1}+\cdots+a_n=(x-\alpha_1)\cdots(x-\alpha_n)$$

betragter vi

$$F'(x)=nx^{n-1}+(n-1)a_1x^{n-2}+\cdots+a_{n-1}.$$

Resultanten $R(F,\frac{F'}{n})$ er da et polynomium i koefficienterne $a_1,\dots,a_n$, som har værdien 0, hvis og kun hvis F og F' har en fælles rod, d.v.s. hvis og kun hvis F har en multipel rod. Idet

$$\begin{aligned}F'(x)=&\quad 1\cdot(x-\alpha_2)(x-\alpha_3)\cdots\quad(x-\alpha_n)\\&+(x-\alpha_1)\cdot 1\cdot(x-\alpha_3)\cdots\quad(x-\alpha_n)\\&+\cdots\\&+(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{n-1})\cdot 1,\end{aligned}$$

fås

$$\begin{aligned}n^nR(F,\tfrac{F'}{n})&=n^n\prod_{i=1}^n\frac{F'(\alpha_i)}{n}=\prod_{i=1}^nF'(\alpha_i)\\&=\quad 1\cdot(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\cdots\quad(\alpha_1-\alpha_n)\\&\quad(\alpha_2-\alpha_1)\cdot 1\cdot(\alpha_2-\alpha_3)\cdots\quad(\alpha_2-\alpha_n)\\&\quad\cdots\\&\quad(\alpha_n-\alpha_1)(\alpha_n-\alpha_2)\cdots(\alpha_n-\alpha_{n-1})\cdot 1\\&=(-1)^{\frac{n(n-1)}{2}}\prod_{1\le j<i\le n}(\alpha_i-\alpha_j)^2.\end{aligned}$$

Ved <u>diskriminanten</u> $\mathcal{D}(F)$ af polynomiet F forstås tallet

$$\mathcal{D}(F) = \prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n(n-1)}{2}} n^n R(F, \frac{F'}{n}).$$

Man ser, at der findes et og kun et polynomium $U(a_1, \ldots, a_n)$, således at F for givet n

$$\mathcal{D}(F) = U(a_1, \ldots, a_n)$$

Af definitionen ses:

<u>En nødvendig og tilstrækkelig betingelse for, at polynomiet F har en multipel rod, er at</u>

$$\mathcal{D}(F) = 0.$$

Idet som bekendt

$$\det \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \cdots & & & \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{pmatrix} = \prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j),$$

får vi, idet determinantens kvadrat udregnes ved 'søjle-søjle multiplikation'

$$\mathcal{D}(F) = \det \begin{pmatrix} n & s_1 & s_2 & \cdots & s_{n-1} \\ s_1 & s_2 & s_3 & \cdots & s_n \\ s_2 & s_3 & s_4 & \cdots & s_{n+1} \\ \cdots & & & & \\ s_{n-1} & s_n & s_{n+1} & \cdots & s_{2n-2} \end{pmatrix},$$

som kan tjene til eksplicit bestemmelse af polynomiet $U(a_1, \ldots, a_n)$, idet man for potenssummerne $s_1, s_2, \ldots$ indsætter de ud fra Newtons formler fundne udtryk.

For $n = 2$ er $F(x) = x^2 + a_1 x + a_2 = (x - \alpha_1)(x - \alpha_2)$, og vi får

$$\mathcal{D} = (\alpha_2 - \alpha_1)^2 = \det \begin{pmatrix} 2 & s_1 \\ s_1 & s_2 \end{pmatrix} = \det \begin{pmatrix} 2 & -a_1 \\ -a_1 & a_1^2 - 2a_2 \end{pmatrix} = a_1^2 - 4a_2.$$

Antages specielt, at koefficienterne a_1 og a_2 er reelle, må polynomiet have enten to forskellige reelle

rødder, en dobbelt reel rod, eller to imaginære komplekst konjugerede rødder. Af udtrykket $D=(\alpha_2-\alpha_1)$ aflæses, at man i de tre tilfælde har henholdsvis $D>0$, $D=0$, $D<0$. Altså gælder også det omvendte. Dette velkendte resultat er således her fundet uden brug af udtrykket for rødderne.

For $n=3$ og $a_1=0$, $a_2=p$, $a_3=q$ er $F(x)=x^3+px+q=(x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$, og vi får

$$D=(\alpha_3-\alpha_1)^2(\alpha_3-\alpha_1)^2(\alpha_3-\alpha_2)^2=\det\begin{pmatrix}3 & s_1 & s_2\\ s_1 & s_2 & s_3\\ s_2 & s_3 & s_4\end{pmatrix}$$

$$=\det\begin{pmatrix}3 & 0 & -2p\\ 0 & -2p & -3q\\ -2p & -3q & 2p^2\end{pmatrix}=-4p^3-27q^2.$$

Antages specielt, at koefficienterne p og q er reelle, må polynomiet have enten tre forskellige reelle rødder eller tre ikke indbyrdes forskellige reelle rødder (d.v.s. enten en reel dobbeltrod og en reel enkeltrod eller en reel tripelrod) eller en reel rod og to imaginære komplekst konjugerede rødder. Af udtrykket $D=(\alpha_2-\alpha_1)^2(\alpha_3-\alpha_1)^2(\alpha_3-\alpha_2)^2$ aflæses let, at man i de tre tilfælde har henholdsvis $D>0$, $D=0$, $D<0$. Altså gælder også det omvendte.

§11. De algebraiske tals legeme.

Ved hjælp af hovedsætningen om symmetriske polynomier vil vi nu bevise:

Mængden $\bar{A}$ af algebraiske tal er et tallegeme.

Bevis. Vi skal vise, at hvis α og β er algebraiske tal, er også $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$, og (såfremt $\beta\neq 0$) $\frac{\alpha}{\beta}$ algebraiske tal.

Lad α være rod i det normerede polynomium

$$F = F(x) = x^n + a_1 x^{n-1} + \cdots + a_n = (x-\alpha_1)\cdots(x-\alpha_n) \in \dot{Q}[x],$$

og lad β være rod i det normerede polynomium

$$G = G(x) = x^m + b_1 x^{m-1} + \cdots + b_m = (x-\beta_1)\cdots(x-\beta_m) \in \dot{Q}[x];$$

α er således et af tallene $\alpha_1, \cdots, \alpha_n$, og β er et af tallene $\beta_1, \cdots, \beta_m$. Da er $\alpha+\beta$ rod i polynomiet

$$H = H(x) = \prod_{\substack{i=1,\cdots,n \\ j=1,\cdots,m}} (x-(\alpha_i+\beta_j)) = x^{nm} + c_1 x^{nm-1} + \cdots + c_{nm}.$$

Opfatter vi $\alpha_1, \cdots, \alpha_n$ og $\beta_1, \cdots, \beta_m$ som variable, er produktet et polynomium $\Phi = \Phi(x; \alpha_1, \cdots, \alpha_n; \beta_1, \cdots, \beta_m)$, som er symmetrisk i de variable $\alpha_1, \cdots, \alpha_n$ for sig og i de variable $\beta_1, \cdots, \beta_m$ for sig. Der findes altså et og kun ét polynomium $T = T(x; a_1, \cdots, a_n; b_1, \cdots, b_m)$, hvoraf det fremgår, når man for $a_1, \cdots, a_n$ indsætter de elementarsymmetriske polynomier i $\alpha_1, \cdots, \alpha_n$ og for $b_1, \cdots, b_m$ de elementarsymmetriske polynomier i $\beta_1, \cdots, \beta_m$. Da endvidere Φ har lutter hele koefficienter, får T lutter hele koefficienter. Polynomiet H fremgår af T, ved at man for $a_1, \cdots, a_n$ og $b_1, \cdots, b_m$ indsætter koefficienterne i polynomierne F og G. Da disse er rationale, ses at koefficienterne $c_1, \cdots, c_{nm}$ i H alle er rationale. Følgelig er $\alpha+\beta$ et algebraisk tal.

På ganske samme måde indses, at $\alpha-\beta$ og $\alpha\beta$ er algebraiske tal, idet man blot vælger henholdsvis

$$H = \prod_{\substack{i=1,\cdots,n \\ j=1,\cdots,m}} (x-(\alpha_i-\beta_j)) \quad \text{og} \quad H = \prod_{\substack{i=1,\cdots,n \\ j=1,\cdots,m}} (x-\alpha_i\beta_j).$$

Endelig indses (under antagelsen $\beta \neq 0$), at $\frac{\alpha}{\beta}$ er algebraisk, idet man bemærker, at vi da kan antage $b_m \neq 0$, således at alle rødderne $\beta_1, \cdots, \beta_m$ i G er $\neq 0$ (ellers bortdividerer i G potensen x^k, hvor

b_{n-k} er den koefficient i G med højest nummer, der er $\neq 0$); beviset er da som før, idet man vælger

$$H = \prod_{\substack{i=1,\dots,n \\ j=1,\dots,m}} (\beta_j X - \alpha_i) = c_0 X^{nm} + c_1 X^{nm-1} + \cdots + c_{nm}.$$

Da får H rationale koefficienter. [I dette tilfælde er H ikke nødvendigvis normeret; koefficienten c_0 bliver $= (\beta_1 \cdots \beta_m)^n = ((-1)^m b_m)^n$.]

Antages, at α og β er <u>hele algebraiske</u> tal, kan vi for F og G benytte polynomier med hele koefficienter. Man ser da, at $\alpha+\beta$ bliver helt algebraisk, idet koefficienterne i H nu bliver hele tal. På samme måde ses, at $\alpha-\beta$ og $\alpha\beta$ bliver hele algebraiske tal. Vi har altså:

<u>Mængden $\mathfrak{H}$ af hele algebraiske tal er en integritetsring.</u>

Som vist i § 6 kan ethvert algebraisk tal α skrives på formen $\frac{\beta}{b}$, hvor β er helt algebraisk og b er et sædvanligt helt tal $\neq 0$. Ethvert algebraisk tal er altså kvotient af to hele algebraiske tal. De algebraiske tals legeme $\mathfrak{A}$ er således kvotientlegeme for integritetsringen $\mathfrak{H}$ af hele algebraiske tal.

<u>For reelle tal a og b er tallet $a+ib$ algebraisk, hvis og kun hvis a og b er algebraiske.</u>

<u>Bevis</u>. Tallet i er algebraisk (endda helt algebraisk), da det er rod i polynomiet x^2+1. Hvis a og b er algebraiske, er derfor også $a+ib$ algebraisk. Hvis omvendt $a+ib$ er algebraisk, er også $a-ib$ algebraisk (idet et polynomium i $\mathbb{Q}[x]$, der har $a+ib$ til rod, også har $a-ib$ til rod). Følgelig er også

$a = \frac{1}{2}[(a+ib)+(a-ib)]$ og $b = \frac{1}{2i}[(a+ib)-(a-ib)]$ algebraisk.

De algebraiske tals legeme $\bar{A}$ er algebraisk afsluttet.

Bevis. Vi skal vise, at rødderne i et vilkårligt egentligt polynomium med algebraiske koefficienter er algebraiske tal. Ifølge det foregående er det nok at se på normerede polynomier med algebraiske koefficienter.

Lad altså

$$P = P(x) = x^n + \gamma_1 x^{n-1} + \cdots + \gamma_n \in \bar{A}[x]$$

være et sådant polynomium. Hver koefficient γ_i er som algebraisk tal rod i et normeret polynomium

$$F_i = F_i(x) = x^{m_i} + a_{i1}x^{m_i-1} + \cdots + a_{im_i} = (x-\gamma_{i1})\cdots(x-\gamma_{im_i}) \in \bar{Q}[x]$$

γ_i er således et af tallene $\gamma_{i1}, \cdots, \gamma_{im_i}$. Svarende til $i = 1, \cdots, n$ får vi de n talsæt $\gamma_{11}, \cdots, \gamma_{1m_1}; \cdots;$ $\gamma_{n1}, \cdots, \gamma_{nm_n}$. Nu danner vi polynomiet

$$H = H(x) = \prod_{\substack{j_1=1,\cdots,m_1 \\ \cdots \\ j_n=1,\cdots,m_n}} (x^n + \gamma_{1j_1}x^{n-1} + \cdots + \gamma_{nj_n}) = x^N + c_1x^{N-1} + \cdots + c_N,$$

hvor $N = nm_1 \cdots m_n$. Blandt faktorerne findes polynomiet P, hvis rødder derfor alle er rødder i H. Opfatter vi $\gamma_{11}, \cdots, \gamma_{1m_1}; \cdots; \gamma_{n1}, \cdots, \gamma_{nm_n}$ som variable, er produktet et polynomium $S = S(x; \gamma_{11}, \cdots, \gamma_{1m_1}; \cdots; \gamma_{n1}, \cdots, \gamma_{nm_n})$, som for hvert $i = 1, \cdots, n$ er symmetrisk i de variable $\gamma_{i1}, \cdots, \gamma_{im_i}$ for sig. Der findes derfor et og kun et polynomium $T = T(x; a_{11}, \cdots, a_{1m_1}; \cdots; a_{n1}, \cdots, a_{nm_n})$, hvoraf det fremgår, når man for hvert $i = 1, \cdots, n$ for $a_{i1}, \cdots, a_{im_i}$ indsætter de elementarsymmetriske polynomier i $\gamma_{i1}, \cdots, \gamma_{im_i}$. Da endvidere S har lutter hele koefficienter, får T lutter hele koefficienter. Polynomiet H fremgår af T

ved at man for hvert i for $a_{i1}, \ldots, a_{im_i}$ indsætter koefficienterne i polynomiet F_i. Da disse alle er rationale, ses, at koefficienterne $c_1, \ldots, c_N$ i H alle er rationale. Altså er rødderne i H, og specielt rødderne i P, algebraiske tal.

Da ethvert tallegeme L indeholder de rationale tals legeme Q, må ethvert algebraisk afsluttet tallegeme L indeholde A (idet det skal indeholde rødderne i ethvert polynomium i $L[x]$ og altså specielt rødderne i ethvert polynomium i $Q[x]$). Ligesom Q kaldes det mindste tallegeme, kaldes derfor A det mindste algebraisk afsluttede tallegeme.

§ 12. Ligninger af grad $\leqslant 4$.

En rod i det egentlige polynomium $F(x)$ kaldes også en rod i ligningen $F(x) = 0$. Hvis graden af F er n, taler vi om en n^{te} gradsligning.

Forbemærkninger. Ligningen $x^n - 1 = 0$ har rødderne $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$, hvor $\varepsilon = \exp i\frac{2\pi}{n} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$. Tallene $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$ kaldes de n^{te} enheds rødder. Bemærk, at der for $n \geqslant 2$ gælder $1 + \varepsilon + \varepsilon^2 + \ldots + \varepsilon^{n-1} = 0$.

For et vilkårligt a vil vi med $\sqrt[n]{a}$ betegne en vilkårlig n^{te} rod af a, altså en vilkårlig af rødderne i ligningen $x^n - a = 0$. Symbolet $\sqrt[n]{a}$ kan altså betegne enhver af de n rødder, men vi vil altså betegne enhver af de n rødder, men vi vil altid, når talen er om en sådan ligning, tænke os truffet et valg, således at $\sqrt[n]{a}$ er en bestemt af rødderne. Ligningens n rødder er da $\sqrt[n]{a}, \varepsilon\sqrt[n]{a}, \varepsilon^2\sqrt[n]{a}, \ldots, \varepsilon^{n-1}\sqrt[n]{a}$. For n lige og a reel og $\geqslant 0$ vel-

ger man i reglen at lade $\sqrt[n]{a}$ betegne den ikke negative reelle rod, og for n ulige og a reel vælger man i reglen at lade $\sqrt[n]{a}$ betegne den reelle rod.

Bortskaffning af leddet af næsthøjest grad i en n^{te} gradsligning. Hvis vi i polynomiet

$$F(x) = x^n + a_1 x^{n-1} + \cdots + a_n = (x-\alpha_1)\cdots(x-\alpha_n)$$

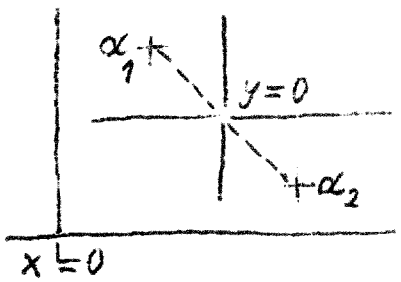
sætter $x = y + c$, fås

$$G(y) = F(y+c) = y^n + \left[\binom{n}{1}c + a_1\right]y^{n-1} + \cdots = (y-(\alpha_1-c))\cdots(y-(\alpha_n-c))$$

Polynomiet $G(y)$ har altså rødderne $\alpha_1 - c, \cdots, \alpha_n - c$. Vælges specielt $c = -\frac{a_1}{n}$, bliver koefficienten til y^{n-1} lig med 0. Dette er ensbetydende med, at rødderne i $G(y)$ har summen 0. Substitutionen $x = y - \frac{a_1}{n}$ er ensbetydende med en parallelforskydning af koordinatsystemet, hvorved det nye begyndelsespunkt $y=0$ bliver punktet $x = -\frac{a_1}{n} = \frac{\alpha_1 + \cdots + \alpha_n}{n}$, altså rødderes tyngdepunkt.

Andengradsligningen. For ligningen

$$x^2 + a_1 x + a_2 = 0$$



giver substitutionen $x = y - \frac{a_1}{2}$ ligningen $y^2 - \left(\frac{a_1^2}{4} - a_2\right) = 0$ med rødderne $\sqrt{\frac{a_1^2}{4} - a_2}$ og $-\sqrt{\frac{a_1^2}{4} - a_2}$, hvor efter den ovenfor angivne vedtægt $\sqrt{\frac{a_1^2}{4} - a_2}$ står for en bestemt af rødderne og $-\sqrt{\frac{a_1^2}{4} - a_2}$ altså for den anden. Andengradsligningens rødder er derfor

$$\left.\begin{matrix}\alpha_1 \\ \alpha_2\end{matrix}\right\} = -\frac{a_1}{2} \pm \sqrt{\frac{a_1^2}{4} - a_2}.$$

Man konstaterer, at diskriminanten $D = (\alpha_2 - \alpha_1)^2$, i overensstemmelse med, hvad vi fandt i § 10, er $= a_1^2 - 4a_2$. Rødderne kan derfor skrives $-\frac{a_1}{2} \pm \sqrt{\frac{D}{4}}$.

Tredjegradsligningen. Løsningen skyldes del Ferro 1515 og Tartaglia 1535 og blev offentliggjort af Cardano i Ars magna 1545.

For ligningen

$$x^3 + a_1 x^2 + a_2 x + a_3 = 0$$

giver substitutionen $x = y - \frac{a_1}{3}$ ligningen

$$y^3 + py + q = 0,$$

hvor $p = -\frac{a_1^2}{3} + a_2$, $q = \frac{2a_1^3}{27} - \frac{a_1 a_2}{3} + a_3$. Vi kan derfor i det følgende nøjes med at betragte sidstnævnte ligning. Betegnes dennes rødder $\beta_1, \beta_2, \beta_3$, er rødderne i den oprindelige ligning $\alpha_1 = -\frac{a_1}{3} + \beta_1$, $\alpha_2 = -\frac{a_1}{3} + \beta_2$, $\alpha_3 = -\frac{a_1}{3} + \beta_3$. Vi har $\beta_1 + \beta_2 + \beta_3 = 0$.

Sættes $y = u + v$, fås

$$u^3 + v^3 + (3uv + p)(u + v) + q = 0.$$

Nu kan vi for ethvert y vælge u og v således, at

$$y = u + v$$
$$-\frac{p}{3} = uv.$$

Disse ligninger betyder blot, at u og v er rødderne i andengradsligningen $z^2 - yz - \frac{p}{3} = 0$. Når $uv = -\frac{p}{3}$, antager den fundne ligning formen $u^3 + v^3 = -q$. Heraf ses, at <u>et tal y er rod i tredjegradsligningen, hvis og kun hvis det har formen $y = u + v$, hvor u og v tilfredsstiller ligningerne</u>

$$u^3 + v^3 = -q$$
$$uv = -\frac{p}{3}.$$

To tal u og v, der tilfredsstiller disse ligninger, vil også tilfredsstille ligningerne

$$u^3 + v^3 = -q$$
$$u^3 v^3 = -\frac{p^3}{27},$$

d.v.s. u^3 og v^3 må være rødderne i andengrads-

ligningen $z^2+qz-\frac{p^3}{27}=0$. Vi må altså have

$$\left.\begin{matrix}u^3\\ v^3\end{matrix}\right\} = -\frac{q}{2} \pm \sqrt{\frac{q^2}{4}+\frac{p^3}{27}}, \text{ d.v.s. } \begin{matrix} u=\sqrt[3]{-\frac{q}{2}+\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}} \\ v=\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}. \end{matrix}$$

Her skal efter vor vedtægt $\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$ stå for en bestemt af symbolets to værdier og $-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$ altså for den anden. På grund af symmetrien i u og v ligger der ingen indskrænkning i at knytte u^3 til $\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$ og v^3 til $-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}$.

For u fås altså tre (eventuelt sammenfaldende) værdier, nemlig, idet u_0 er en af værdierne, tallene $u_0, \varepsilon u_0, \varepsilon^2 u_0$, hvor $\varepsilon = -\frac{1}{2}+i\frac{\sqrt{3}}{2}$ og $\varepsilon^2 = -\frac{1}{2}-i\frac{\sqrt{3}}{2}$ er de to fra 1 forskellige tredje enhedsrødder. Tilsvarende fås for v tre (eventuelt sammenfaldende) værdier, nemlig, idet v_0 er en af værdierne, tallene $v_0, \varepsilon v_0, \varepsilon^2 v_0$. At kombinationerne kan vi benytte de og kun de, for hvilke $uv=-\frac{p}{3}$. For hver af kombinationerne er $u^3v^3=-\frac{p^3}{27}$, og altså uv et af tallene $-\frac{p}{3}, \varepsilon(-\frac{p}{3}), \varepsilon^2(-\frac{p}{3})$. Vi skelner nu mellem to tilfælde:

1) Hvis $p\neq 0$, er alle de omhandlede værdier $\neq 0$. Hvis u_0 og v_0 er valgt således, at $u_0v_0=-\frac{p}{3}$, vil de andre brugbare kombinationer være $\varepsilon u_0, \varepsilon^2 v_0$ og $\varepsilon^2 u_0, \varepsilon v_0$. Hvis u_0 og v_0 er valgt således, at u_0v_0 er $\varepsilon(-\frac{p}{3})$, omdøber vi $\varepsilon^2 u_0$ til u_0 og har da atter $u_0v_0=-\frac{p}{3}$, og hvis u_0v_0 er $\varepsilon^2(-\frac{p}{3})$, omdøber vi εu_0 til u_0 og har da atter $u_0v_0=-\frac{p}{3}$. Der bliver altså tre brugbare kombinationer.

2) Hvis $p=0$, bliver enten de tre u-værdier $=0$ eller de tre v-værdier $=0$ (evt. begge dele). Alle kombinationer er da brugbare. Hvis u_0, v_0 er

en vilkårlig kombination, vil denne sammen med $\varepsilon u_0, \varepsilon^2 v_0$ og $\varepsilon^2 u_0, \varepsilon v_0$ dække alle.

Hermed er vist: Et tal y er rod i tredjegradsligningen, hvis og kun hvis det har formen

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

hvor de to kubikrødder er valgt således, at deres produkt er $-\frac{p}{3}$. Betegner u_0, v_0 en brugbar kombination, bestemmes samtlige brugbare kombinationer ved

$$u_0, v_0; \qquad \varepsilon u_0, \varepsilon^2 v_0; \qquad \varepsilon^2 u_0, \varepsilon v_0.$$

Løsningsformlen kaldes Cardanos formel.

De tre tal

$$u_0 + v_0, \qquad \varepsilon u_0 + \varepsilon^2 v_0, \qquad \varepsilon^2 u_0 + \varepsilon v_0$$

er hver for sig rod i ligningen, og enhver rod i ligningen er et af disse tal. Heraf følger:

1) Hvis de tre tal er indbyrdes forskellige, har ligningen tre forskellige rødder, nemlig de tre tal.

2) Hvis de tre tal er ligestore, $= \beta$, har ligningen en tripelrod, nemlig β (som må være 0, da summen af ligningens rødder er 0).

3) Hvis to af tallene er ligestore, $= \beta$, men det tredje forskelligt derfra, $= \gamma$, har ligningen kun rødderne β og γ. Dette giver anledning til to muligheder: Enten må ligningen have β som dobbeltrod og γ som enkeltrod, eller den må have β som enkeltrod og γ som dobbeltrod. Den sidste mulighed kan imidlertid ikke indtræffe. Thi de tre tal har summen 0 (idet $1 + \varepsilon + \varepsilon^2 = 0$). Vi har altså $2\beta + \gamma = 0$. Hvis ligningen havde β som enkeltrod og γ som dobbeltrod, skulde vi have $\beta + 2\gamma = 0$ (idet summen af ligningens

rødder er 0). Ved subtraktion fås $\beta - \gamma = 0$, i strid med at $\beta \neq \gamma$.

Vi har altså: <u>De tre tal</u>

$$\beta_1 = u_0 + v_0, \quad \beta_2 = \varepsilon u_0 + \varepsilon^2 v_0, \quad \beta_3 = \varepsilon^2 u_0 + \varepsilon v_0,$$

<u>den findes ved Cardanos formel, er ligningen tre rødder.</u>

Man konstaterer ved udregning, at diskriminanten $D = (\beta_2 - \beta_1)^2 (\beta_3 - \beta_1)^2 (\beta_3 - \beta_2)^2$, i overensstemmelse med hvad vi fandt i § 10, er $= -4p^3 - 27q^2$. Cardanos formel kan således også skrives

$$y = \sqrt[3]{-\frac{q}{2} + \sqrt{-\frac{D}{108}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{-\frac{D}{108}}}.$$

<u>Diskussion i tilfælde af reelle p og q.</u>

1) $\frac{q^2}{4} + \frac{p^3}{27} = 0$, d. v. s. $D = 0$. I følge diskussionen i § 10 skal da findes enten en reel enkeltrod og en reel dobbeltrod eller en reel tripelrod.

Hvis $q = 0$, er $p = 0$, og ligningen har tripelroden 0.

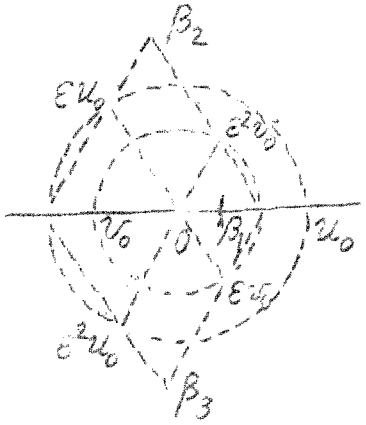
Hvis $q \neq 0$, er $p < 0$. Som u_0 og v_0 kan da benyttes den reelle værdi af $\sqrt[3]{-\frac{q}{2}}$, og vi finder enkeltroden $u_0 + v_0 = 2\sqrt[3]{-\frac{q}{2}}$ og dobbeltroden $\varepsilon u_0 + \varepsilon^2 v_0 = \varepsilon^2 u_0 + \varepsilon v_0 = -\sqrt[3]{-\frac{q}{2}}$.

2) $\frac{q^2}{4} + \frac{p^3}{27} > 0$, d. v. s. $D < 0$. I følge diskussionen i § 10 skal da findes en reel rod og to imaginære konjugerede rødder.

Tallene $-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ er her reelle, og som u_0 og v_0 kan benyttes de reelle kubikrødder. Vi får $u_0 > v_0$.

Hvis $p = 0$, $q > 0$, bliver $u_0 = 0$, $v_0 = \sqrt[3]{-q}$, og hvis $p = 0$, $q < 0$, bliver $u_0 = \sqrt[3]{-q}$, $v_0 = 0$. I begge tilfælde bliver rødderne $\sqrt[3]{-q}$, $\varepsilon\sqrt[3]{-q}$, $\varepsilon^2\sqrt[3]{-q}$.

Af $u_0 v_0 = -\frac{p}{3}$ ses, at hvis $p>0$, har u_0 og v_0 modsat fortegn, og hvis $p<0$ (og følgelig $q \neq 0$), har u_0 og v_0 samme fortegn (nemlig det modsatte fortegn af q). Vi finder den reelle rod $\beta_1 = u_0 + v_0$ og de to komplekst konjugerede rødder $\beta_2 = \varepsilon u_0 + \varepsilon^2 v_0$ og $\beta_3 = \varepsilon^2 u_0 + \varepsilon v_0$. Figuren illustrerer røddernes konstruktion i tilfældet $p>0$. Tilfældene $p<0, q>0$ og $p<0, q<0$ giver analoge figurer.



3) $\frac{q^2}{4} + \frac{p^3}{27} < 0$, d. v. s. $D>0$. I følge diskussionen i §10 skal da findes tre forskellige reelle rødder.

I dette tilfælde må gælde $p<0$. Vi finder, jfr. figuren,

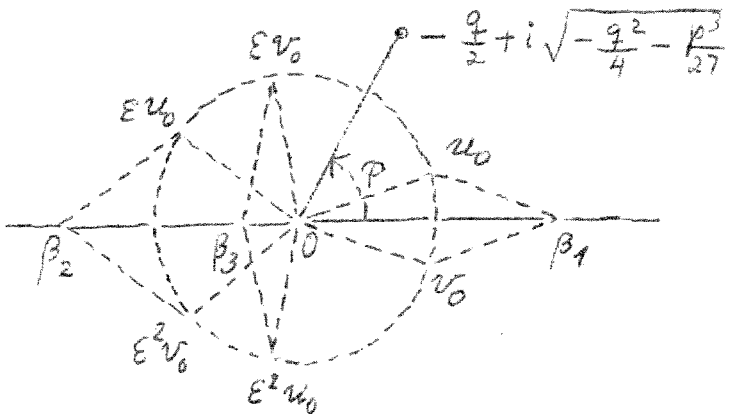
$$-\frac{q}{2} \pm \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} = -\frac{q}{2} \pm i\sqrt{-\frac{q^2}{4} - \frac{p^3}{27}} = \sqrt{-\frac{p^3}{27}}\,(\cos\varphi \pm i\sin\varphi),$$

hvor $\cos\varphi = \dfrac{-\frac{q}{2}}{\sqrt{-\frac{p^3}{27}}}$. En brugbar kombination u_0, v_0 er

$$\left.\begin{matrix} u_0 \\ v_0 \end{matrix}\right\} = \sqrt{-\frac{p}{3}}\left(\cos\frac{\varphi}{3} \pm i\sin\frac{\varphi}{3}\right),$$

og vi finder de tre reelle rødder

$$\beta_1 = 2\sqrt{-\frac{p}{3}}\cos\frac{\varphi}{3},\quad \beta_2 = 2\sqrt{-\frac{p}{3}}\cos\frac{\varphi+2\pi}{3},\quad \beta_3 = 2\sqrt{-\frac{p}{3}}\cos\frac{\varphi+4\pi}{3}.$$



Man ser, at Cardanos formel giver rødderne på kompleks form, hvad man i 16. årh. ikke beherskede; derfor betegnelsen casus irreducibilis i dette tilfælde. Den trigonometriske form af løsningen blev fundet af Viète 1591 ud fra formlen $\cos 3v = 4\cos^3 v - 3\cos v$.

Fjerdegradsligningen. Løsningen skyldes Ferrari og blev offentliggjort af Cardano i Ars magna 1545.

På ligningen

$$x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0$$

anvendes substitutionen $x = y - \frac{a_1}{4}$. Herved fås en ligning

$$y^4 + py^2 + qy + r = 0.$$

Tilfældet $q = 0$ er trivielt. Vi antager derfor $q \neq 0$. Ligningen skrives

$$(y^2 + z)^2 - \{(2z - p)y^2 - qy + z^2 - r\} = 0.$$

Nu kan z vælges således, at $\{\dots\}$ får formen $(ay + b)^2$. Hertil kræves, at

$$R(z) = 4(2z - p)(z^2 - r) - q^2 = 0.$$

For enhver rod z i denne tredjegradsligning har vi $2z - p \neq 0$ (da $q \neq 0$), og vi får

$$\{\dots\} = (ay + b)^2 \quad \text{med} \quad a = \sqrt{2z - p}, \; b = -\frac{q}{2a}.$$

Den oprindelige ligning kan da skrives

$$(y^2 + ay + z + b)(y^2 - ay + z - b) = 0,$$

og rødderne findes som rødderne i de to andengradspolynomier.

Bemærkning. Hvis fjerdegradsligningen har reelle koefficienter, kan man benytte en reel værdi $z > \frac{p}{2}$. Thi $R(z)$ har da reelle koefficienter, og da $R(\frac{p}{2}) = -q^2 < 0$, medens $R(z) \to +\infty$ for $z \to +\infty$, må der findes en reel rod $z > \frac{p}{2}$ i $R(z)$. Følgelig bliver $a = \sqrt{2z - p}$ reel og dermed også $b = -\frac{q}{2a}$ reel. De to andengradspolynomier får således reelle koefficienter.

§13. Reelle rødder i polynomier med reelle koefficienter.

Vi vil undersøge de reelle rødders antal og beliggenhed for et polynomium

$$F = F(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

med reelle koefficienter.

De eventuelle reelle rødder i F tilhører intervallet $[-1-K, 1+H]$, hvor

$-H = \min\{a_1, \cdots, a_n, 0\}$ og $-K = \min\{-a_1, +a_2, \cdots (-1)^n a_n, 0\}$.

Bevis. For $x > 1+H$ gælder

$$F(x) \geqslant x^n - H(x^{n-1} + x^{n-2} + \cdots + 1) = x^n - H\frac{x^n - 1}{x-1}$$

$$= \frac{(x-1)x^n - Hx^n + H}{x-1} > \frac{Hx^n - Hx^n + H}{x-1} \geqslant 0.$$

Der er altså ingen rod $> 1+H$. Følgelig har polynomiet

$$(-1)^n F(-x) = x^n - a_1 x^{n-1} + a_2 x^{n-2} - \cdots + (-1)^n a_n$$

ingen rod $> 1+K$, d.v.s. $F(x)$ har ingen rod $< -1-K$.

Eksempel. $F(x) = x^{19} - 4x^3 + 6x^{10} + 20x^5 - 2x^3 - 2x^2 - 4$. Man finder $H = 4$, $K = 6$. Alle reelle rødder ligger således i intervallet $[-7, 5]$.

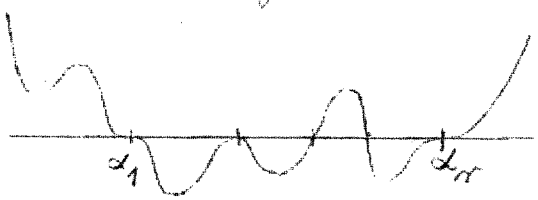
Hvis F er af lige grad, har F et lige antal reelle rødder. Hvis F er af ulige grad, har F et ulige antal reelle rødder. Hver rod skal regnes med sin multiplicitet.

Bevis. Dette fremgår umiddelbart af, at F har et lige antal imaginære rødder (regnet med multiplicitet).

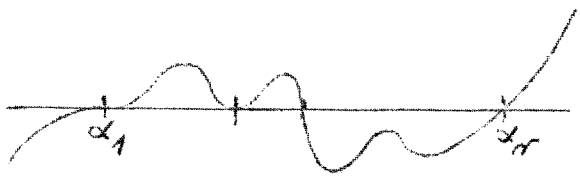
Sætningen fremgår også let af Taylors formel. Hvis $\alpha_1, \cdots, \alpha_r$ betegner de indbyrdes forskellige reelle rødder ordnet voksende, har $F(x)$ åbenbart kon-

stant fortegn i hvert af intervallerne $]-\infty,\alpha_1[$, $]\alpha_1,\alpha_2[$, ..., $]\alpha_{r-1},\alpha_r[$, $]\alpha_r,+\infty[$. Da $F(x)\to+\infty$ for $x\to+\infty$, er $F(x)$ positiv i $]\alpha_r,+\infty[$, og da $F(x)\to+\infty$ eller $F(x)\to-\infty$ for $x\to-\infty$, eftersom n er lige eller ulige, er $F(x)$ positiv eller negativ i $]-\infty,\alpha_1[$, eftersom n er lige eller ulige. Hvis α_i er rod af multiplicitet ν_i, har vi $F(x)=\frac{F^{(\nu_i)}(\alpha_i)}{\nu_i!}(x-\alpha_i)^{\nu_i}+\dots$, altså $\frac{F(x)}{(x-\alpha_i)^{\nu_i}}\to\frac{F^{(\nu_i)}(\alpha_i)}{\nu_i!}$ for $x\to\alpha_i$, hvor $F^{(\nu_i)}(\alpha_i)\neq 0$. Følgelig har $F(x)$ samme fortegn i intervallet lige venstre for α_i og i intervallet lige højre for α_i, hvis ν_i er lige, og forskelligt fortegn i de to intervaller, hvis ν_i er ulige. Antallet $\nu_1+\dots+\nu_r$ af reelle rødder (regnet med multiplicitet) er altså lig med antallet af fortegnsskifter for $F(x)$, idet x gennemløber $]-\infty,+\infty[$, plus et lige tal ≥ 0, og er følgelig lige eller ulige, eftersom n er lige eller ulige.

n lige



n ulige



<u>Descartes' sætning.</u> <u>Antallet af positive rødder i F regnet med multiplicitet er højst lig med antallet af fortegnsskifter i følgen $1, a_1, \dots, a_n$, og forskellen mellem de to antal er et lige tal.</u>

Sætningen står i Descartes' *La géométrie* 1637.

Ved optællingen af antallet af fortegnsskifter tages kun de fra 0 forskellige koefficienter i betragtning.

Eksempler. $F(x) = x - 1$. Der er et fortegnsskifte, altså en positiv rod. $F(x) = x^2 - x + 1$. Der er to fortegnsskifter, altså ingen eller to positive rødder (der er ingen). $F(x) = x^2 - 3x + 1$. Der er to fortegnsskifter, altså ingen eller to positive rødder (der er to).

For det ovenfor betragtede polynomium $F(x) = x^{19} - 4x^{13} + 6x^{10} + 20x^5 - 3x^3 - 2x^2 - 4$ ses, at der må være en eller tre positive rødder. Betragtes $-F(-x) = x^{19} - 4x^{13} - 6x^{10} + 20x^5 - 3x^3 + 2x^2 + 4$ ses, at $F(x)$ må have ingen, to eller fire negative rødder.

Bevis. Vi kan antage, at $a_n = F(0) \neq 0$. Ellers, altså hvis $F(0) = 0$, bortdivideres x^k, hvor k er multiplicieteten af roden 0.

Vi skal vise: Hvis der er r positive rødder, er der $r + 2p$ fortegnsskifter (p hel og ≥ 0). Beviset føres ved induktion efter r.

1) Hvis $r = 0$, må $F(x)$ have konstant fortegn for $x \geq 0$, og da $F(x) \to +\infty$ for $x \to +\infty$, må vi have $F(x) > 0$ for $x \geq 0$, altså specielt $a_n = F(0) > 0$. Dette medfører, at antallet af fortegnsskifter i følgen $1, a_1, \ldots, a_n$ er lige.

2) Udsagnet antages rigtigt for $r = r_0$ og skal så vises for $r = r_0 + 1$. Vi antager altså, at F har $r_0 + 1$ positive rødder. Lad α være en af dem. Da er

$$F(x) = x^n + a_1 x^{n-1} + \cdots + a_n = (x - \alpha) F_0(x),$$

hvor

$$F_0(x) = x^{n-1} + b_1 x^{n-2} + \cdots + b_{n-1}$$

har r_0 positive rødder og følgelig $r_0 + 2p_0$ fortegnsskifter (p_0 hel og ≥ 0). I følgen $1, b_1, \ldots, b_{n-1}$ betegner vi med b_{λ_1} det første negative tal, med b_{λ_2} det første positive tal efter b_{λ_1}, $\ldots$, med

$b_{\lambda_{r_0+2p_0}}$, eftersom r_0+2p_0 er $\left\{\begin{matrix}\text{lige}\\ \text{ulige}\end{matrix}\right\}$, det første $\left\{\begin{matrix}\text{positive}\\ \text{negative}\end{matrix}\right\}$ tal efter $b_{\lambda_{r_0+2p_0-1}}$. Herefter indtræffer ingen fortegnskifter. Skematisk har vi altså:

$$\underbrace{1,\dots,}_{>0}\ \underbrace{b_{\lambda_1},\dots,}_{\geqslant 0}\ \underbrace{b_{\lambda_2},\dots,}_{<0}\ \underbrace{\dots,\dots,}_{\leqslant 0}\ \underbrace{b_{\lambda_{r_0+2p_0}},\dots}_{>0\ \text{hvis}\ r_0+2p_0\ \left\{\begin{matrix}\text{lige:}\\ \text{ulige}\end{matrix}\right.}\ \begin{matrix}\leqslant 0 & >0 & \geqslant 0\\ \geqslant 0 & <0 & \leqslant 0\end{matrix}$$

Nu er koefficienterne $a_0=1, a_1, a_2, \dots, a_n$ i $F(x)$ bestemt udfra koefficienterne $b_0=1, b_1, \dots, b_{n-1}$ i $F_0(x)$ ved

$$a_0=1,\ a_1=b_1-\alpha b_0,\ a_2=b_2-\alpha b_1,\ \dots,\ a_{n-1}=b_{n-1}-\alpha b_{n-2},\ a_n=-\alpha b_{n-1}.$$

Specielt fås:

$$\begin{aligned}
a_0 &= 1 && >0\\
a_{\lambda_1} &= b_{\lambda_1}-\alpha b_{\lambda_1-1} && <0\\
a_{\lambda_2} &= b_{\lambda_2}-\alpha b_{\lambda_2-1} && >0\\
&\dots\\
a_{\lambda_{r_0+2p_0}} &= b_{\lambda_{r_0+2p_0}}-\alpha b_{\lambda_{r_0+2p_0}-1} && \left\{\begin{matrix}>0\\ <0\end{matrix}\right. \text{eftersom } r_0+2p_0 \text{ er} \left\{\begin{matrix}\text{lige}\\ \text{ulige}\end{matrix}\right.\\
a_n &= -\alpha b_{n-1} && \left\{\begin{matrix}<0\\ >0\end{matrix}\right. \quad \text{--- " ---}
\end{aligned}$$

Vedrørende sidste linie bemærkes, at b_{n-1}, som jo er $\neq 0$, må have samme fortegn som $b_{\lambda_{r_0+2p_0}}$ (hvis $\lambda_{r_0+2p_0}=n-1$, er b_{n-1} naturligvis $b_{\lambda_{r_0+2p_0}}$). I følgen $1, a_1, \dots, a_n$ findes der således fra 1 til a_{λ_1} et ulige antal fortegnsskifter, fra a_{λ_1} til a_{λ_2} et ulige antal fortegnsskifter, …, fra $a_{\lambda_{r_0+2p_0}}$ til a_n et ulige antal fortegnsskifter. Antallet af fortegnsskifter er således r_0+2p_0+1 plus et lige tal $\geqslant 0$, altså lig med r_0+1+2p (p hel $\geqslant 0$).

Anvendes Descartes' sætning for et vilkårligt reelt x_0 på

$$F(x_0+t)=F(x_0)+\frac{F'(x_0)}{1!}t+\dots+\frac{F^{(n)}(x_0)}{n!}t^n,$$

(hvor naturligvis $F^{(n)}(x_0) = n!$) ses, at antallet af rødder for F i $]x_0, +\infty[$ (regnet med multiplicitet) højst er lig med antallet $V(x_0)$ af fortegnsskifter i følgen $F(x_0), F'(x_0), \ldots, F^{(n)}(x_0)$, og at forskellen mellem de to antal er et lige tal. For et vilkårligt til venstre åbent og til højre afsluttet interval $]\alpha, \beta]$ er antallet af rødder for F i $]\alpha, \beta]$ (regnet med multiplicitet) altså lig med $(V(\alpha) - 2A) - (V(\beta) - 2B)$, hvor A og B er ikke negative hele tal, altså lig med $V(\alpha) - V(\beta) - 2(A-B)$. Antallet er altså lig med $V(\alpha) - V(\beta)$ påner et lige tal. Vi vil vise, at man altid har $A \geq B$. Dette, og lidt mere, er indholdet af

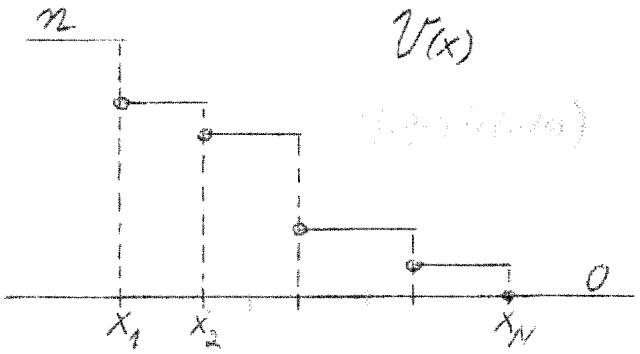
Fouriers sætning. Antallet $V(x)$ af fortegnskifter i følgen $F(x), F'(x), \ldots, F^{(n)}(x)$ er en monotont aftagende og fra højre kontinuert funktion. For ethvert interval $]\alpha, \beta]$ er antallet af rødder for F i $]\alpha, \beta]$ højst lig med $V(\alpha) - V(\beta)$, og forskellen mellem de to tal er lige. For store negative x er $V(x) = n$, og for store positive x er $V(x) = 0$.

Sætningen er meddelt af Fourier i forelæsninger 1797 og senere; først offentliggjort 1820. Den kaldes også Budans sætning eller Fourier–Budans sætning.

Bevis. Lad $x_1, \ldots, x_N$ være samtlige reelle tal, der er rod i mindst et af polynomierne $F(x), F'(x), \ldots, F^{(n-1)}(x)$, ordnet voksende. I hvert af intervallerne $]-\infty, x_1[,]x_1, x_2[, \ldots,]x_{N-1}, x_N[,]x_N, +\infty[$ har hvert af polynomierne $F(x), F'(x), \ldots, F^{(n-1)}(x)$ konstant fortegn. Desuden er $F^{(n)}(x) = n! > 0$ for alle x. Følgelig er $V(x)$ konstant i hvert af de nævnte intervaller. Idet $F(x) \to +\infty, F'(x) \to +\infty, \ldots, F^{(n-1)}(x) \to +\infty$ for $x \to +\infty$, er $F(x), F'(x), \ldots, F^{(n)}(x)$ alle > 0 i $]x_N, +\infty[$. Følgelig er

$V(x) = 0$ i $]x_N, +\infty[$. Da endvidere $(-1)^n F(x) \to +\infty$, $(-1)^{n-1} F'(x) \to +\infty, \ldots, -F^{(n-1)}(x) \to +\infty$ for $x \to -\infty$, er $F(x), F'(x), \ldots, F^{(n)}(x)$ skiftevis >0 og <0 i $]-\infty, x_1[$ (fortegnsfølgen er $+,-,+,\ldots,+$, hvis n er lige, og $-,+,-,\ldots,+$, hvis n er ulige). Følgelig er $V(x) = n$ i $]-\infty, x_1[$. Sætningen vil derfor være bevist, når vi viser:

For ethvert $i = 1, \ldots, N$ gælder: Værdien $V(x_i)$ er lig med værdien af $V(x)$ i intervallet til højre for x_i og $\leqslant$ værdien $V(x_i - 0)$ af $V(x)$ i intervallet til venstre for x_i, og differensen $V(x_i - 0) - V(x_i)$ er et lige tal, hvis x_i ikke er rod i $F(x)$, ellers lig med multipliciteten af x_i som rod i $F(x)$ plus et lige tal $\geqslant 0$.



Vi ser på $F(x), F'(x), \ldots, F^{(n)}(x)$ i punktet x_i og i de tilstødende intervaller. Hvis x_i er rod i $F(x)$ med multiplicitet m, begynder følgen $F(x_i), F'(x_i), \ldots, F^{(m)}(x_i)$ med m nuller, hvorefter følger et tal $F^{(m)}(x_i)$, som er $\neq 0$. Dettes fortegn kan være $+$ som angivet i tabellen eller $-$ som angivet i alternativet. Hvis x_i ikke er rod i $F(x)$ begynder følgen med et tal $F(x_i) \neq 0$. Det kan indtræffe, at der senere en eller flere gange kommer et eller flere på hinanden følgende nuller i følgen $F(x_i), F'(x_i), \ldots, F^{(n)}(x_i)$. I tabellen er angivet en sådan følge gående fra $F^{(k+1)}(x_i)$ til $F^{(l-1)}(x_i)$, og for hvilken $F^{(k)}(x_i)$ og $F^{(l)}(x_i)$ har fortegnskombinationen $+,+$, medens fortegnskombinationerne $-,-$; $+,-$; og $-,+$ er angivet som alternativer.

For ethvert nummer j, for hvilket $F^{(j)}(x_i) \neq 0$, har $F^{(j)}(x)$ samme fortegn i intervallerne til højre og til venstre for x_i som i x_i. For et j, for hvilket både $F^{(j)}(x_i)$ og $F^{(j+1)}(x_i)$ er $\neq 0$, vil der derfor fra parret $F^{(j)}(x)$, $F^{(j+1)}(x)$ komme samme bidrag til $V(x)$ [enten 0 eller 1] i intervallerne til højre og til venstre for x_i som i punktet x_i selv.

	til venstre for x_i	x_i	til højre for x_i
$F(x)$	$\pm$	0	+
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$F^{(m)}(x)$	−	0	+
$\vdots$	+	+	+
$F^{(k)}(x)$	+	+	+
$F^{(k+1)}(x)$	$\pm$	0	+
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$F^{(l-1)}(x)$	−	0	+
$F^{(l)}(x)$	+	+	+
$\vdots$			
$F^{(n)}(x)$	+	+	+

skiftende / skiftende

Alternativ

$\pm$	0	−
$\vdots$	$\vdots$	$\vdots$
+	0	−
−	−	−

Alternativer

−	−	−
$\pm$	0	−
$\vdots$	$\vdots$	$\vdots$
+	0	−
−	−	−

+	+	+
$\pm$	0	−
$\vdots$	$\vdots$	$\vdots$
+	0	−
−	−	−

−	−	−
$\pm$	0	+
$\vdots$	$\vdots$	$\vdots$
−	0	+
+	+	+

Hvis x_i er rod i $F(x)$, slutter vi vedrørende delfølgen $F(x), \ldots, F^{(m)}(x)$ således: Ifølge Taylors formel er

$$F(x) = \frac{F^{(m)}(x_i)}{m!}(x-x_i)^m + \cdots, \text{ altså } \frac{F(x)}{(x-x_i)^m} \to \frac{F^{(m)}(x_i)}{m!}$$

$$\cdots$$

$$F^{(m-2)}(x) = \frac{F^{(m)}(x_i)}{2!}(x-x_i)^2 + \cdots, \text{ altså } \frac{F^{(m-2)}(x)}{(x-x_i)^2} \to \frac{F^{(m)}(x_i)}{2!}$$

$$F^{(m-1)}(x) = \frac{F^{(m)}(x_i)}{1!}(x-x_i) + \cdots, \text{ altså } \frac{F^{(m-1)}(x)}{x-x_i} \to \frac{F^{(m)}(x_i)}{1!}$$

for $x \to x_i$.

Heraf ses, at $F(x), \ldots, F^{(m-1)}(x)$ i intervallet til højre for x_i har samme fortegn som $F^{(m)}(x_i)$, medens det i intervallet til venstre for x_i gælder, at $F^{(m-1)}(x)$ har modsat fortegn af $F^{(m)}(x_i)$, $F^{(m-2)}(x)$ har samme fortegn som $F^{(m)}(x_i)$, o.s.v. I delfølgen $F(x), \ldots, F^{(m)}(x)$ er der altså 0 fortegnsskifter såvel i x_i som i intervallet til højre for x_i og m fortegnsskifter i intervallet til venstre for x_i.

Vedrørende en delfølge $F^{(k)}(x), \ldots, F^{(l)}(x)$ viser samme slutningsmåde, at $F^{(k+1)}(x), \ldots, F^{(l-1)}(x)$ i intervallet til højre for x_i har samme fortegn som $F^{(l)}(x_i)$, medens det i intervallet til venstre for x_i gælder, at $F^{(l-1)}(x)$ har modsat fortegn af $F^{(l)}(x_i)$, $F^{(l-2)}(x)$ har samme fortegn som $F^{(l)}(x_i)$, o.s.v. I delfølgen $F^{(k)}(x), \ldots, F^{(l)}(x)$ er der derfor lige så mange fortegnsskifter i intervallet til højre for x_i som i x_i, nemlig 0, hvis fortegnskombinationen for $F^{(k)}(x_i)$ og $F^{(l)}(x_i)$ er $+,+$ eller $-,-$, og 1, hvis fortegnskombinationen er $+,-$ eller $-,+$. I intervallet til venstre for x_i er antallet af fortegnsskifter åbenbart lige, hvis fortegnskombinationen er $+,+$ eller $-,-$ [nemlig = det største lige tal $\leq l-k$], og ulige, hvis fortegnskombinationen er $+,-$ eller $-,+$ [nemlig = det største ulige tal $\leq l-k$].

Af denne diskussion fremgår påstanden, idet vi har fundet samme antal fortegnsskifter til højre for x_i som i x_i og ved passagen af x_i har konstateret et tab på m fortegnsskifter, såfremt x_i er rod i $F(x)$ af multiplicitet m, samt af et lige antal fortegnsskifter for hver delfølge $F^{(k)}(x), \ldots, F^{(l)}(x)$.

Eksempel. For polynomiet $F(x) = x^5 - x^4 - 3x^3 + 2x + 5$ fås følgende tabel over fortegnene for $F(x), F'(x), \ldots, F^{(5)}(x)$ og dermed værdien af $V(x)$ for forskellige værdier af x.

x	$-\infty$	-2	-1	0	1	2	$+\infty$
$F(x) = x^5 - x^4 - 3x^3 + 2x + 5$	$-$	$-$	$+$	$+$	$+$	$+$	$+$
$F'(x) = 5x^4 - 4x^3 - 9x^2 + 2$	$+$	$+$	$+$	$+$	$-$	$+$	$+$
$F''(x) = 20x^3 - 12x^2 - 18x$	$-$	$-$	$-$	0	$-$	$+$	$+$
$F'''(x) = 60x^2 - 24x - 18$	$+$	$+$	$+$	$-$	$+$	$+$	$+$
$F^{(4)}(x) = 120x - 24$	$-$	$-$	$-$	$-$	$+$	$+$	$+$
$F^{(5)}(x) = 120$	$+$	$+$	$+$	$+$	$+$	$+$	$+$
$V(x)$	5	5	4	2	2	0	0

Kolonnerne $-\infty$ og $+\infty$ svarer til så store negative og positive x, at fortegnene er dem, der bestemmes af leddene af højest grad. Man ser, at alle de reelle rødder i $F(x)$ må ligge i intervallet $]-2,2[$, og at der er en rod i $]-2,-1[$, ingen eller to rødder i $]-1,0[$, ingen rod i $]0,1[$, og ingen eller to rødder i $]1,2[$.

Problemet om bestemmelse af antallet af reelle rødder i et interval blev løst i 1829 af Sturm ved en metode, som endda for enhver multiplicitet giver antallet af rødder i intervallet med denne multiplicitet.

Vi anvender Euklids algoritme på F og F', idet divisionsligningerne skrives

$$\begin{aligned} F &= F' Q_1 - F_2 \\ F' &= F_2 Q_2 - F_3 \\ F_2 &= F_3 Q_3 - F_4 \\ &\circ\ \circ\ \circ \\ F_{m-2} &= F_{m-1} Q_{m-1} - F_m \\ F_{m-1} &= F_m Q_m . \end{aligned}$$

Skrevet på den sædvanlige form bliver divisionsalg-

ningerne

$$\begin{aligned} F &= F' Q_1 + (-F_2) \\ F' &= (-F_2)(-Q_2) + (-F_3) \\ -F_2 &= (-F_3) Q_3 + F_4 \\ -F_3 &= F_4 (-Q_4) + F_5 \\ F_4 &= F_5 Q_5 + (-F_6) \quad \text{o. s. v.} \end{aligned}$$

Den sidste af de opskrevne ligninger har samme fortegnskombination som den første, og fortegnskombinationerne vil derfor gentage sig med perioden 4. Den ændrede form betyder altså blot, at kvotienterne i divisionsligningerne er blevet betegnet $Q_1, -Q_2, Q_3, -Q_4, \ldots$ og resterne $-F_2, -F_3, F_4, F_5, \ldots$. Altså er (F, F') det med F_m associerede normerede polynomium.

Polynomiet F_m er divisor i alle polynomierne $F, F', F_2, \ldots, F_m$. Nu dannes <u>Sturms kæde</u>

$$\frac{F}{F_m} = \mathcal{H}, \quad \frac{F'}{F_m} = \mathcal{H}_1, \quad \frac{F_2}{F_m} = \mathcal{H}_2, \quad \ldots, \quad \frac{F_{m-1}}{F_m} = \mathcal{H}_{m-1}, \quad \frac{F_m}{F_m} = \mathcal{H}_m = 1.$$

For polynomierne $\mathcal{H}, \mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_m$ gælder de

(*)
$$\begin{aligned} \mathcal{H} &= \mathcal{H}_1 Q_1 - \mathcal{H}_2 \\ \mathcal{H}_1 &= \mathcal{H}_2 Q_2 - \mathcal{H}_3 \\ \mathcal{H}_2 &= \mathcal{H}_3 Q_3 - \mathcal{H}_4 \\ &\ldots \\ \mathcal{H}_{m-2} &= \mathcal{H}_{m-1} Q_{m-1} - \mathcal{H}_m \\ \mathcal{H}_{m-1} &= \mathcal{H}_m Q_m, \qquad \mathcal{H}_m = 1. \end{aligned}$$

Samtlige optrædende polynomier har reelle koefficienter. Hvis

$$F = (x-\alpha_1)^{\nu_1} \ldots (x-\alpha_s)^{\nu_s},$$

hvor $\alpha_1, \ldots, \alpha_s$ er de indbyrdes forskellige (reelle og imaginære) rødder i F og $\nu_1, \ldots, \nu_s$ deres multipliciteter, har vi (§ 3)

$$(F, F') = (x-\alpha_1)^{\nu_1 - 1} \cdots (x-\alpha_s)^{\nu_s - 1},$$

(hvor en faktor $(x-\alpha_i)^{\nu_i-1}$ med $\nu_i = 1$ skal læses som 1). Da F_m er associeret med (F, F'), har vi altså

$$H = a(x-\alpha_1)\cdots(x-\alpha_s), \qquad a \neq 0.$$

Polynomiet H har altså de samme rødder som F, men rødderne i H er alle simple.

Sturms sætning. Antallet $W(x)$ af fortegnsskifter i følgen $H(x), H_1(x), \cdots, H_m(x)$ er en monotont aftagende og fra højre kontinuert funktion. For ethvert interval $]\alpha, \beta]$ er antallet af indbyrdes forskellige rødder for F i $]\alpha, \beta]$ lig med $W(\alpha) - W(\beta)$.

Bevis. Lad $x_1, \cdots, x_N$ være samtlige reelle tal, der er rod i mindst et af polynomierne $H, H_1, \cdots, H_{m-1}$. I hvert af de åbne intervaller $]-\infty, x_1[$, $]x_1, x_2[$, $\cdots$, $]x_{N-1}, x_N[$, $]x_N, +\infty[$ har hvert af polynomierne H, $H_1, \cdots, H_{m-1}$ konstant fortegn. Desuden er $H_m(x) = 1 > 0$ for alle x. Følgelig er $W(x)$ konstant i hvert af de nævnte intervaller. Sætningen vil derfor være bevist, når vi viser:

For ethvert $i = 1, \cdots, N$ gælder: Værdien $W(x_i)$ er lig med værdien af $W(x)$ i intervallet til højre for x_i. I intervallet til venstre for x_i er $W(x) = W(x_i)$, hvis x_i ikke er rod i F, og $= W(x_i) + 1$, hvis x_i er rod i F.

Vi ser på $H(x), H_1(x), \cdots, H_m(x)$ i punktet x_i og i de tilstødende intervaller. Da $H_m(x_i) = 1 \neq 0$, ses af ligningerne $(*)$, at to på hinanden følgende tal i følgen $H(x_i), H_1(x_i), \cdots, H_m(x_i)$ ikke begge kan være 0. Hvis x_i er rod i F, og altså også i H, begynder følgen med 0. Da er det næste tal $H_1(x_i) \neq 0$, og dets fortegn kan være + som angivet i tabellen

eller – som angivet i alternativet. Hvis x_i ikke er rod i F, og altså heller ikke i H, begynder følgen med et tal $H(x_i) \neq 0$. Det kan indtræffe, at der senere en eller flere gange i følgen kommer et $H_k(x_i) = 0$. Da er $H_{k-1}(x_i)$ og $H_{k+1}(x_i)$ begge $\neq 0$. Af formlen

$$H_{k-1}(x_i) = H_k(x_i)\, Q_k(x_i) - H_{k+1}(x_i)$$

ses, at $H_{k-1}(x_i)$ og $H_{k+1}(x_i)$ må have hver sit fortegn. I tabellen er angivet et tilfælde, hvor fortegnskombinationen $-\,+$ er angivet som alternativ.

For ethvert nummer j, for hvilket $H_j(x_i) \neq 0$, har $H_j(x)$ samme fortegn i intervallerne til højre og til venstre for x_i som i x_i. For et j, for hvilket både $H_j(x_i)$ og $H_{j+1}(x_i)$ er $\neq 0$, vil der altså fra parret $H_j(x), H_{j+1}(x)$ indkomme samme bidrag til $W(x)$ [enten 0 eller 1] i intervallerne til højre og til venstre for x_i som i punktet x_i selv.

	til venstre for x_i	x_i	til højre for x_i
$H(x)$	$-$	0	$+$
$H_1(x)$	$+$	$+$	$+$
$\vdots$			
$H_{k-1}(x)$	$+$	$+$	$+$
$H_k(x)$		0	
$H_{k+1}(x)$	$-$	$-$	$-$
$\vdots$			
$H_m(x)$	$+$	$+$	$+$

Alternativ

$+$	0	$-$
$-$	$-$	$-$

Alternativ

$-$	$-$	$-$
	0	
$+$	$+$	$+$

Hvis x_i er rod i F af multiplicitet m, har vi ifølge Taylors formel

$$F(x) = \frac{F^{(m)}(x_i)}{m!}(x-x_i)^m + \cdots, \quad F'(x) = \frac{F^{(m)}(x_i)}{(m-1)!}(x-x_i)^{m-1} + \cdots,$$

hvoraf ses, at $F(x)$ og $F'(x)$ i et vist interval $]x_i, x_i+\varepsilon[$ har samme fortegn [nemlig samme fortegn som $F^{(m)}(c_i)$]. Følgelig har $H(x)$ og $H_1(x)$ også samme fortegn i $]x_i, x_i+\varepsilon[$ og følgelig i hele intervallet til højre for x_i. Da x_i er simpelt nulpunkt for H, er fortegnet for $H(x)$ i intervallet til venstre for x_i det modsatte af fortegnet i intervallet til højre for x_i. Heraf ses, at parret $H(x)$, $H_1(x)$ giver 0 fortegnsskifte i x_i og i intervallet til højre for x_i, men 1 fortegnsskifte i intervallet til venstre for x_i.

Når $H_k(x_i)=0$, ses, at der, ligegyldigt hvilke fortegn $H_k(x)$ har i intervallerne til højre og til venstre for x_i, i delfølgen $H_{k-1}(x), H_k(x), H_{k+1}(x)$ vil være 1 fortegnsskifte såvel i x_i som i intervallerne til højre og til venstre for x_i.

Af denne diskussion fremgår påstanden, idet vi har fundet samme antal fortegnsskifter til højre for x_i som i x_i og ved passagen af x_i har konstateret et tab på 1 fortegnsskifte, såfremt x_i er rod i F, og ingen forandring i antallet af fortegnsskifter, såfremt x_i ikke er rod i F.

F multipel

Bemærk, at når x ikke er rod i F, d.v.s. ikke er rod i F_m, kan antallet $W(x)$ bestemmes som antallet af fortegnsskifter i følgen $F(x), F'(x), F_2(x), \dots, F_m(x)$. Divisionen med $F_m(x)$ kan derfor spares, hvis man er tilfreds med at kunne finde antallet af rødder i intervaller, hvis endepunkter ikke er multiple rødder.

I slutningen af §3 har vi vist, at man for et vilkårligt polynomium F og ethvert g ved gentagen anvendelse af Euklids algoritme kan bestemme det polynomium G_g, der er produkt af de faktorer $x-\alpha_i$,

der svarer til rødderne af multiplicitet q i F. Ved at anvende Sturms sætning på disse polynomier G_q finder vi for ethvert q og ethvert interval $]\alpha,\beta]$ antallet af rødder af multiplicitet q for F i $]\alpha,\beta]$.

Bemærkning. Bestemmelsen af polynomierne $F_2,\dots,F_m$ besværliggøres ofte af de ved divisionerne frembragte nævnere i koefficienterne. Da det imidlertid for beregningen af $W(x)$ kun kommer an på fortegnene, gør det ingen forskel, om vi multiplicerer hvert polynomium med en positiv konstant. I det følgende eksempel betegner $\approx$, at det anførte polynomium er det pågældende F_q multipliceret med en positiv konstant.

Eksempel. Vi betragter samme polynomium som under Fouriers sætning, altså $F(x) = x^5 - x^4 - 3x^3 + 2x + 5$, og får følgende tabel.

x	$-\infty$	-2	-1	0	1	2	$+\infty$
$F(x) = x^5 - x^4 - 3x^3 + 2x + 5$	$-$	$-$	$+$	$+$	$+$	$+$	$+$
$F'(x) = 5x^4 - 4x^3 - 9x^2 + 2$	$+$	$+$	$+$	$+$	$-$	$+$	$+$
$F_2(x) \approx 34x^3 + 9x^2 - 40x - 127$	$-$	$-$	$-$	$-$	$-$	$+$	$+$
$F_3(x) \approx 79x^2 - 574x + 827$	$+$	$+$	$+$	$+$	$+$	$-$	$+$
$F_4(x) \approx -3953x + 7578$	$+$	$+$	$+$	$+$	$+$	$-$	$-$
$F_5(x) =$ negativ konstant	$-$	$-$	$-$	$-$	$-$	$-$	$-$
$W(x)$	4	4	3	3	3	1	1

Da $F_5(x)$ er konstant, har F kun simple rødder. Kolonnerne $-\infty$ og $+\infty$ svarer til så store negative og positive x, at fortegnene er dem, der bestemmes af leddene af højest grad. Man ser, at der er ialt 3 reelle rødder, nemlig 1 i intervallet $]-2,-1[$ og 2 i intervallet $]1,2[$. Ved beregning af $F(x)$ for værdier af x i disse intervaller finder man, at de tre rødder er $\alpha_1 = -1{,}17$, $\alpha_2 = 1{,}56$, $\alpha_3 = 1{,}90$.

§14. Konstruktion med passer og lineal. Gauss' sætning om regulære polygoner.

Konstruktion med passer og lineal er det ældste konstruktionsbegreb, der benyttes i Euklids elementer, deraf den rolle, det har spillet i matematikkens historie.

Vi præcisérer begrebet på følgende måde:

Der må være givet et antal punkter $O, A, B, \ldots, K$.

De tilladte operationer er:

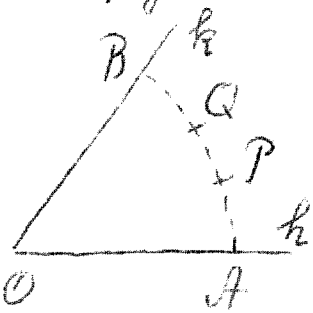
(1) at tegne den rette linie gennem to givne eller allerede fundne punkter;

(2) at tegne cirklen med et givet eller allerede fundet punkt som centrum og afstanden mellem to givne eller allerede fundne punkter som radius;

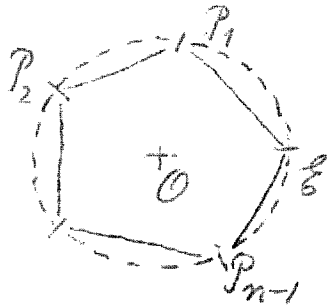
(3) at opsøge skæringspunkter mellem tegnede linier og cirkler.

Punkter, der kan findes ud fra de givne ved gentagen anvendelse af disse operationer, kaldes konstruerbare med passer og lineal ud fra punkterne $O, A, B, \ldots, K$.

Indfasningen af gængse konstruktionsopgaver under denne definition kan nødvendiggøre en omformulering. Dreje det sig for eksempel om tredeling (i lige store dele) af en vinkel hk, kan vi som givne punkter tage toppunktet O og skæringspunkterne A og B mellem benene h og k og en cirkel med centrum O. Opgaven går da ud på ud fra O, A, B at konstruere tredelingspunkterne P og Q for cirkelbuen AB.



Opgaven at konstruere en regulær n-kant ($n \geq 3$) skal forstås således: Der er givet to Punkter O og E. Det gælder om ud fra O og E at konstruere de øvrige vinkelspidser $P_1, \ldots, P_{n-1}$ i den i cirklen med centrum O og radius OE indskrevne regulære n-kant, hvis ene vinkelspids er E.



I Euklids elementer findes konstruktionen af den regulære n-kant for $n = 3, 4, 5, 15$ og dermed (ved hjælp af vinkelhalvering) for ethvert n, der fås af disse ved multiplikation med en potens af 2. Det var vel almindeligt antaget, at konstruktionen i andre tilfælde ikke var mulig, og det vakte derfor opsigt, da Gauss i 1796 viste, at man kan konstruere den regulære 17-kant. I Disquisitiones arithmeticae 1801 udviklede han sin metode.

Gauss' sætning. Den regulære n-kant kan konstrueres med passer og lineal, hvis og kun hvis primfaktoropløsningen for n har formen

$$n = 2^r p_1 p_2 \cdots p_s,$$

hvor $p_1, p_2, \ldots, p_s$ er indbyrdes forskellige ulige primtal af formen $2^{2^h}+1$.

Gauss bevistе tilstrækkeligheden af betingelsen og angav uden bevis, at den også er nødvendig.

Tallene $F_h = 2^{2^h}+1$, $h \geq 0$, kaldes Fermat tal. For $h = 0, 1, 2, 3, 4$ finder man $F_h = 3, 5, 17, 257, 65537$, der alle er primtal. Fermat formodede, at F_h er et primtal for ethvert h, men Euler viste, at $F_5 = 4294967297$ er sammensat, idet det er deleligt med 641. [Det ses næsten uden regning som følger: Man har $641 =$

$5 \cdot 2^7 + 1 = 5^4 + 2^4$. Altså er $5 \cdot 2^7 \equiv -1 \bmod 641$ og $5^4 \equiv -2^4 \bmod 641$. Heraf fås $5^4 \cdot 2^{28} \equiv 1 \bmod 641$ og følgelig $-2^4 \cdot 2^{28} \equiv 1 \bmod 641$, d.v.s. $F_5 = 2^{32} + 1 \equiv 0 \bmod 641$.] Man kender ikke andre Fermat primtal end de anførte. Derimod vides F_n at være sammensat for $5 \leqslant n \leqslant 16$ og for $n = 18, 19, 23, 36, 38, 39, 55, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 260, 267, 268, 284, 316, 452, 1945$. [Således har F_{1945} som mindste divisor tallet $5 \cdot 2^{1947} + 1$, der altså er et primtal.]

På grundlag af Fermat primtallene 3, 5, 17, 257, 65537 finder vi ud fra Gauss' sætning 31 ulige værdier af n, for hvilke den regulære n-kant kan konstrueres, nemlig de nævnte 5 primtal, de 10 produkter af 2 forskellige, af disse (heriblandt Euklids $15 = 3 \cdot 5$), de 10 produkter af 3 forskellige af disse, de 5 produkter af 4 forskellige af disse, og endelig produktet af alle 5 (som er 4294967295). Hvis der findes flere, er de i hvert fald $\geqslant F_{17}$ (som har 39457 cifre).

Specielt følger af Gauss' sætning, at den regulære 9-kant ikke kan konstrueres, hvoraf følger, at <u>vinklens tredeling med passer og lineal ikke er mulig</u> (idet man i så fald ud fra den regulære 3-kant kunde konstruere den regulære 9-kant).

§15. <u>Konstruerbare tal.</u>

Vi lader planen være den komplekse plan, så at et punkt bliver ensbetydende med et komplekst tal $x = \xi + i\eta$. Som givne punkter vælger vi 0 og 1. Mængden K af punkter x, der kan konstrueres med passer og lineal ud fra 0 og 1 kaldes <u>mængden af konstruerbare tal</u>. Undersøgelsen af K kræver nogle forberedelser.

Lad $\mathcal{L}$ være et tallegeme, der indeholder et tal q, men ikke $\sqrt{q}$ [hvor $\sqrt{q}$ i overensstemmelse med vor vedtagt skal betegne en bestemt af symbolets to værdier; når den ene værdi ikke tilhører $\mathcal{L}$, gælder det samme naturligvis om den anden]. Vi vil betragte mængden $\mathcal{L}^*$ af alle tal af formen $a_1+a_2\sqrt{q}$, hvor $a_1, a_2 \in \mathcal{L}$.

$\mathcal{L}^*$ indeholder $\mathcal{L}$, idet ethvert $a \in \mathcal{L}$ kan skrives på formen $a = a + 0\sqrt{q}$. Endvidere indeholder $\mathcal{L}^*$ tallet $\sqrt{q}$, idet $\sqrt{q}$ kan skrives på formen $\sqrt{q} = 0 + 1\sqrt{q}$.

Lad $a = a_1 + a_2\sqrt{q}$ og $b = b_1 + b_2\sqrt{q}$ (hvor $a_1, a_2, b_1, b_2 \in \mathcal{L}$) være to tal i $\mathcal{L}^*$. Da gælder, at hvis $a = b$, er $a_1 = b_1$ og $a_2 = b_2$. Thi af $a = b$ fås $a_1 - b_1 = (b_2 - a_2)\sqrt{q}$. Heraf følger $a_2 = b_2$. Thi ellers var $\sqrt{q} = \frac{a_1 - b_1}{b_2 - a_2}$, og altså $\sqrt{q}$ et tal i $\mathcal{L}$. Af $a_2 = b_2$ følger $a_1 = b_1$. Ethvert tal a i $\mathcal{L}^*$ har således netop en fremstilling af formen $a = a_1 + a_2\sqrt{q}$, hvor $a_1, a_2 \in \mathcal{L}$. Specielt gælder $a = 0$, hvis og kun hvis a_1 og a_2 begge er 0.

Vi vil nu vise, at $\mathcal{L}^*$ er et tallegeme.

Lad $a = a_1 + a_2\sqrt{q}$ og $b = b_1 + b_2\sqrt{q}$ (hvor $a_1, a_2, b_1, b_2 \in \mathcal{L}$) være to tal i $\mathcal{L}^*$. Vi finder da

$$a + b = (a_1 + b_1) + (a_2 + b_2)\sqrt{q}$$
$$a - b = (a_1 - b_1) + (a_2 - b_2)\sqrt{q}$$
$$ab = (a_1 b_1 + a_2 b_2 q) + (a_1 b_2 + a_2 b_1)\sqrt{q},$$

hvoraf ses, at $a+b, a-b, ab \in \mathcal{L}^*$. Antages $b \neq 0$, har vi $(b_1, b_2) \neq (0,0)$ og altså også $b_1 - b_2\sqrt{q} \neq 0$, og vi finder

$$\frac{a}{b} = \frac{(a_1 + a_2\sqrt{q})(b_1 - b_2\sqrt{q})}{(b_1 + b_2\sqrt{q})(b_1 - b_2\sqrt{q})} = \frac{a_1 b_1 - a_2 b_2 q}{b_1^2 - b_2^2 q} + \frac{-a_1 b_2 + a_2 b_1}{b_1^2 - b_2^2 q}\sqrt{q},$$

hvoraf ses, at $\frac{a}{b} \in \mathcal{L}^*$. Da $\mathcal{L}^*$ ikke består af 0 alene, er hermed bevist, at $\mathcal{L}^*$ er et tallegeme.

Tallegemet $\mathcal{L}^*$ betegnes $\mathcal{L}(\sqrt{q})$, og vi siger, at $\mathcal{L}^* = \mathcal{L}(\sqrt{q})$ er frembragt af $\mathcal{L}$ ved adjunktion af kvadratroden $\sqrt{q}$.

For et vilkårligt $a = a_1 + a_2\sqrt{q} \in \mathcal{L}^*$ (hvor $a_1, a_2 \in \mathcal{L}$) er tallet $\tilde{a} = a_1 - a_2\sqrt{q}$ også et tal i $\mathcal{L}^*$. Vi kalder $\tilde{a}$ det til a konjugerede tal i $\mathcal{L}^*$. Det til $\tilde{a}$ konjugerede tal er åbenbart a. De to tal a og $\tilde{a}$ kan derfor også kaldes indbyrdes konjugerede. Hvis $a_2 = 0$, d. v. s. hvis $a \in \mathcal{L}$, har vi $a = \tilde{a}$. Hvis $a_2 \neq 0$, d. v. s. hvis $a \in \mathcal{L}^* \setminus \mathcal{L}$, har vi $a \neq \tilde{a}$. Tallene i $\mathcal{L}$ er altså de eneste selvkonjugerede tal i $\mathcal{L}^* = \mathcal{L}(\sqrt{q})$.

Hvis vi i ovenstående formler erstatter de to tal $a = a_1 + a_2\sqrt{q}$ og $b = b_1 + b_2\sqrt{q}$ med deres konjugerede $\tilde{a} = a_1 - a_2\sqrt{q}$ og $\tilde{b} = b_1 - b_2\sqrt{q}$, finder vi

$$\begin{aligned}
\tilde{a} + \tilde{b} &= (a_1 + b_1) - (a_2 + b_2)\sqrt{q} \\
\tilde{a} - \tilde{b} &= (a_1 - b_1) - (a_2 - b_2)\sqrt{q} \\
\tilde{a}\tilde{b} &= (a_1 b_1 + a_2 b_2 q) - (a_1 b_2 + a_2 b_1)\sqrt{q} \\
\frac{\tilde{a}}{\tilde{b}} &= \frac{a_1 b_1 - a_2 b_2 q}{b_1^2 - b_2^2 q} - \frac{-a_1 b_2 + a_2 b_1}{b_1^2 - b_2^2 q}\sqrt{q}.
\end{aligned}$$

Altså er $\tilde{a} + \tilde{b}$, $\tilde{a} - \tilde{b}$, $\tilde{a}\tilde{b}$, $\frac{\tilde{a}}{\tilde{b}}$ simpelthen de konjugerede tal til $a + b$, $a - b$, ab, $\frac{a}{b}$.

Eksempel. I tilfældet $\mathcal{L} = \mathbb{R}$, $q = -1$, $\sqrt{q} = i$ er $\mathcal{L}^* = \mathbb{R}(i) = \mathbb{C}$, og det konjugerede tal til et tal $a = a_1 + ia_2$ (hvor $a_1, a_2 \in \mathbb{R}$) er det komplekst konjugerede tal $\bar{a} = a_1 - ia_2$.

Af det ovenstående følger, at hvis $P(x_1, \ldots, x_n)$ er et vilkårligt polynomium i $\mathcal{L}[x_1, \ldots, x_n]$, så vil for vilkårlige tal $a_1 = a_{11} + a_{12}\sqrt{q}, \ldots, a_n = a_{n1} + a_{n2}\sqrt{q}$ i $\mathcal{L}^*$ tallet $P(\tilde{a}_1, \ldots, \tilde{a}_n)$ være det konjugerede tal til tallet $P(a_1, \ldots, a_n)$.

Heraf fremgår, at hvis

$$x^n + a_1 x^{n-1} + \cdots + a_n = (x^m + b_1 x^{m-1} + \cdots + b_m)(x^{n-m} + c_1 x^{n-m-1} + \cdots + c_{n-m})$$

hvor koefficienterne $a_1, \cdots, a_n, b_1, \cdots, b_m, c_1, \cdots, c_{n-m}$ tilhører $\mathcal{L}^*$, da er også

$$x^n + \tilde{a}_1 x^{n-1} + \cdots + \tilde{a}_n = (x^m + \tilde{b}_1 x^{m-1} + \cdots + \tilde{b}_m)(x^{n-m} + \tilde{c}_1 x^{n-m-1} + \cdots + \tilde{c}_{n-m})$$

Thi de to formler betyder henholdsvis, at

$$\begin{aligned} a_1 &= b_1 + c_1 \\ a_2 &= b_2 + b_1 c_1 + c_2 \\ &\cdots \\ a_n &= b_m c_{n-m} \end{aligned} \qquad \text{og} \qquad \begin{aligned} \tilde{a}_1 &= \tilde{b}_1 + \tilde{c}_1 \\ \tilde{a}_2 &= \tilde{b}_2 + \tilde{b}_1 \tilde{c}_1 + \tilde{c}_2 \\ &\cdots \\ \tilde{a}_n &= \tilde{b}_m \tilde{c}_{n-m}. \end{aligned}$$

Specielt gælder altså:

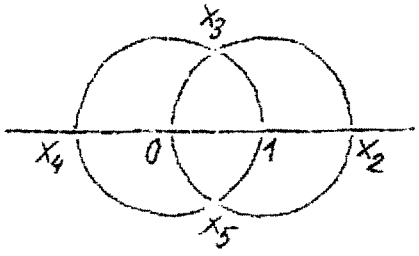
Hvis et polynomium $x^n + a_1 x^{n-1} + \cdots + a_n \in \mathcal{L}^*[x]$ er irreduktibelt i $\mathcal{L}^*[x]$, da er polynomiet $x^n + \tilde{a}_1 x^{n-1} + \cdots + \tilde{a}_n$ det også.

Endvidere finder vi:

For ethvert polynomium $x^n + a_1 x^{n-1} + \cdots + a_n \in \mathcal{L}^*[x]$ gælder $(x^n + a_1 x^{n-1} + \cdots + a_n)(x^n + \tilde{a}_1 x^{n-1} + \cdots + \tilde{a}_n) \in \mathcal{L}[x]$.

Thi koefficienterne i det angivne produkt er jo $a_1 + \tilde{a}_1$, $a_2 + a_1 \tilde{a}_1 + \tilde{a}_2$, $\cdots$, $a_n \tilde{a}_n$ og er altså selvkonjugerede.

Vi går nu over til at betragte mængden K af konstruerbare tal. De givne tal 0 og 1 betegnes x_0 og x_1. På x_0 og x_1 anvender vi de tilladte operationer (1)–(3), idet vi tegner alle de mulige rette linier og cirkler (det bliver 1 linie og 2 cirkler) og opsøger alle disses skæringspunkter ud over 0 og 1 (det bliver 4 punkter); disse betegnes i en eller anden rækkefølge $x_2, \cdots, x_{n_1}$ (hvor altså $n_1 = 5$). Dernæst anvender vi på $x_0, x_1, \cdots, x_{n_1}$ de tilladte operationer (1)–(3), idet



vi atter tegner alle de mulige linier og cirkler, som ikke allerede er tegnet, (det bliver 9 linier og 22 cirkler), og opsøger alle disses skæringspunkter, som ikke allerede er markeret; disse betegnes i en eller anden rækkefølge $x_{n_1+1}, \dots, x_{n_2}$. Således fortsættes. Herved fås samtlige punkter i $\dot{K}$ skrevet som en punktfølge

$$x_0 = 0, x_1 = 1, x_2, x_3, \dots, x_n, \dots,$$

hvor hvert x_n med $n > 1$ er skæringspunkt enten for to linier, der hver går gennem to af de foregående punkter, eller for en sådan linie og en cirkel med et af de foregående punkter som centrum og afstanden mellem to af de foregående punkter som radius, eller mellem to sådanne cirkler.

For at udnytte dette sætter vi $x_n = \xi_n + i\eta_n$ og vil vise:

Der findes en følge af reelle tallegemer $\mathfrak{L}_1 = \dot{Q}, \mathfrak{L}_2, \mathfrak{L}_3, \dots$, således at koordinaterne $\xi_0, \eta_0, \xi_1, \eta_1, \dots, \xi_n, \eta_n$ til punkterne x_p, $p \leqq n$, for ethvert $n \geqq 1$ tilhører $\mathfrak{L}_n$, og således at hvert $\mathfrak{L}_{n+1}$, $n \geqq 1$, enten er $= \mathfrak{L}_n$, eller er $= \mathfrak{L}_n(\sqrt{q_n})$, hvor q_n er et positivt tal i $\mathfrak{L}_n$, for hvilket $\sqrt{q_n}$ ikke tilhører $\mathfrak{L}_n$.

Bevis. Vi anvender induktion. Koordinaterne til 0 og 1 tilhører åbenbart $\mathfrak{L}_1 = \dot{Q}$. Lad os antage, at vi er nået til et reelt tallegeme $\mathfrak{L}_n$, der indeholder koordinaterne til punkterne x_p, $p \leqq n$, og lad os betragte punktet x_{n+1}.

Linien gennem to af punkterne $x_0, x_1, \dots, x_n$, f. eks. x_p og x_q, har ligningen $(\xi - \xi_p)(\eta_q - \eta_p) - (\eta - \eta_p)(\xi_q - \xi_p) = 0$, altså en ligning af formen $a\xi + b\eta + c = 0$, hvor $a, b, c \in \mathfrak{L}_n$ og $(a, b) \neq (0, 0)$. Cirklen med centrum i et af punkterne $x_0, x_1, \dots, x_n$, f. eks. x_r, og afstanden mellem to af disse, f. eks. x_s og x_t, som radius har ligningen $(\xi - \xi_r)^2 + (\eta - \eta_r)^2 = (\xi_s - \xi_t)^2 + (\eta_s - \eta_t)^2$, altså en ligning af formen

$\xi^2+\eta^2+d\xi+e\eta+f=0$, hvor $d,e,f\in\mathcal{L}_n$. Der er nu tre muligheder:

(1) x_{n+1} er skæringspunkt mellem to linier. Da er (ξ_{n+1},η_{n+1}) løsningen til to ligninger

$$a\xi+b\eta+c=0, \qquad a_1\xi+b_1\eta+c_1=0$$

med koefficienter fra $\mathcal{L}_n$, som vides at fremstille skærende linier, altså at have determinant $\neq 0$. Følgelig er

$$(\xi_{n+1},\eta_{n+1})=\left(\frac{-cb_1+c_1b}{ab_1-a_1b},\ \frac{ca_1-c_1a}{ab_1-a_1b}\right),$$

hvoraf ses, at $\xi_{n+1},\eta_{n+1}\in\mathcal{L}_n$. Vi kan da vælge $\mathcal{L}_{n+1}=\mathcal{L}_n$.

(2) x_{n+1} er skæringspunkt mellem en linie og en cirkel. Da er (ξ_{n+1},η_{n+1}) løsning til to ligninger

$$a\xi+b\eta+c=0, \qquad \xi^2+\eta^2+d\xi+e\eta+f=0$$

med koefficienter fra $\mathcal{L}_n$, som vides at have to løsninger. Antages f.eks. $b\neq 0$, finder vi ved elimination af η ligningen

$$\xi^2+\left(-\frac{a}{b}\xi-\frac{c}{b}\right)^2+d\xi+e\left(-\frac{a}{b}\xi-\frac{c}{b}\right)+f=0,$$

d.v.s. en ligning $A\xi^2+B\xi+C=0$, hvor $A,B,C\in\mathcal{L}_n$ og $A\neq 0$, som må have to løsninger, nemlig abscisserne til de to skæringspunkter. Altså er $B^2-4AC>0$, og vi har

$$\xi_{n+1}=-\frac{B}{2A}\pm\frac{1}{2A}\sqrt{B^2-4AC}, \qquad \eta_{n+1}=-\frac{a}{b}\xi_{n+1}-\frac{c}{b}.$$

Der er nu to muligheder: (α) Hvis $\sqrt{B^2-4AC}\in\mathcal{L}_n$, gælder $\xi_{n+1},\eta_{n+1}\in\mathcal{L}_n$, og vi kan vælge $\mathcal{L}_{n+1}=\mathcal{L}_n$. ($\beta$) Hvis $\sqrt{B^2-4AC}\notin\mathcal{L}_n$, sætter vi $q_n=B^2-4AC$ og har da $\xi_{n+1},\eta_{n+1}\in\mathcal{L}_{n+1}=\mathcal{L}_n(\sqrt{q_n})$.

(3) x_{n+1} er skæringspunkt mellem to cirkler. Da er (ξ_{n+1},η_{n+1}) løsning til to ligninger

$$\xi^2+\eta^2+d\xi+e\eta+f=0, \qquad \xi^2+\eta^2+d_1\xi+e_1\eta+f_1=0$$

med koefficienter fra $\mathcal{L}_n$, som vides at fremstille skærende cirkler, hvilket medfører, at $(d,e)\neq(d_1,e_1)$. I stedet for de to ligninger kan da benyttes ligningerne

$\xi^2+\eta^2+d\xi+e\eta+f=0$, $(d-d_1)\xi+(e-e_1)\eta+(f-f_1)=0$,
hvorved diskussionen bliver som i det foregående tilfælde.

For i stedet for tallegemerne $\mathcal{L}_n$, der indeholder koordinaterne til de konstruerbare punkter, at få tallegemer, der indeholder punkterne selv, danner vi nu følgen af tallegemer $R_n = \mathcal{L}_n(i)$. Er $\mathcal{L}$ et reelt tallegeme og $q>0$ et tal i $\mathcal{L}$, for hvilket $\sqrt{q}$ ikke tilhører $\mathcal{L}$, gælder åbenbart, at $\mathcal{L}(\sqrt{q})(i) = \mathcal{L}(i)(\sqrt{q})$ [thi det første tallegeme består af alle tal $(a_1+a_2\sqrt{q})+i(b_1+b_2\sqrt{q})$, hvor $a_1, a_2, b_1, b_2 \in \mathcal{L}$, og det andet af alle tal $(a_1+ib_1)+(a_2+ib_2)\sqrt{q}$, hvor $a_1, a_2, b_1, b_2 \in \mathcal{L}$]. Legemerne R_n fås derfor ud fra $R_1 = \dot{Q}(i)$ ved successiv adjunktion af kvadratrødder, idet vi for ethvert $n \geq 0$ enten har $R_{n+1} = R_n$ eller $R_{n+1} = R_n(\sqrt{q_n})$.

Et tallegeme $\mathcal{L}$ kaldes <u>afsluttet over for kvadratrodsuddragning</u>, hvis det for ethvert $a \in \mathcal{L}$ gælder, at også $\sqrt{a} \in \mathcal{L}$ [når dette gælder for den ene af værdierne af $\sqrt{a}$, gælder det naturligvis også for den anden]. Vi kan nu vise:

<u>Mængden $\dot{K}$ af konstruerbare tal er et over for kvadratrodsuddragning afsluttet tallegeme. Ethvert over for kvadratrodsuddragning afsluttet tallegeme indeholder $\dot{K}$.</u>

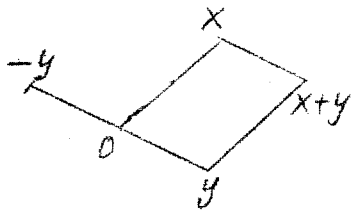
<u>Der findes en følge af tallegemer $K_0, K_1, K_2, \ldots$, hvor $K_0 = \dot{Q}$ og hvert K_{n+1}, $n \geq 0$, er af formen $K_{n+1} = K_n(\sqrt{k_n})$, hvor $k_n \in K_n$, $\sqrt{k_n} \notin K_n$, således at</u>

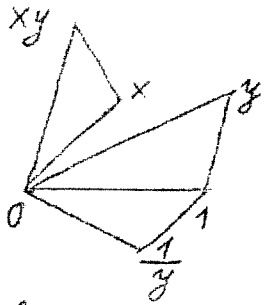
$$\dot{K} = \bigcup_{n=1}^{\infty} K_n .$$

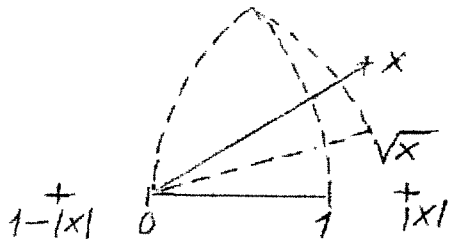
Vi udtrykker dette ved at sige, at $\dot{K}$ er <u>det mindste over for kvadratrodsuddragning afsluttede tallegeme,</u>

og at $\grave{K}$ kan dannes ud fra Q ved sukcessiv adjunktion af kvadratrødder.

Bevis. For vilkårlige $x, y \in \grave{K}$ $(x \neq 0, y \neq 0)$ kan $x+y$, $x-y$, xy, $\frac{x}{y}$ konstrueres som følger: Når x og y ikke ligger på samme linie gennem 0, fås $x+y$ ved skæring af cirklen med centrum x og radius $|y|$ og cirklen med centrum y og radius $|x|$, og $x-y$ på samme måde ud fra x og $-y$, idet $-y$ umiddelbart findes. Ligger x og y på samme linie gennem 0, er konstruktionen af $x+y$ og $x-y$ triviel.







Når y ikke er reel, fås xy ved hjælp af de ensvinklede trekanter $0,1,y$ og $0,x,xy$ og $\frac{x}{y}$ på samme måde ud fra x og $\frac{1}{y}$, idet $\frac{1}{y}$ fås ved hjælp af de ensvinklede trekanter $0,1,y$ og $0,\frac{1}{y},1$ (de nødvendige afsætninger af vinkler kan udføres ved hjælp af cirkelbuer med radius 1). Når y er reel, kan man først konstruere et imaginært z, hvorefter xy og $\frac{x}{y}$ fås som $\frac{x}{z}yz$ og $\frac{xz}{yz}$. For et vilkårligt $x \in \grave{K}$ $(x \neq 0)$ kan $\sqrt{x}$ konstrueres, idet $\sqrt{x}$ skal ligge på vinkelhalveringslinien for vinklen $1,0,x$ i afstand $\sqrt{|x|}$ fra 0. Denne afstand fås, når $|x| > 1$, som afstanden fra 0 til et af skæringspunkterne for cirklerne med centrer $|x|$ og $1-|x|$ (som let findes) og radius $|x|$. Når $|x| < 1$, benyttes cirklerne med centrer 1 og $|x|-1$ og radius 1.

$\grave{K}$ er altså et over for kvadratrodsuddragning afsluttet tallegeme. Ethvert over for kvadratrodsuddragning afsluttet tallegeme L må imidlertid indeholde samtlige ovenfor konstruerede tallegemer R_n (thi det må indeholde Q, altså også tallet $i = \sqrt{-1}$ og følgelig $R_1 = Q(i)$, o.s.v.). Følgelig gælder både $\grave{K} \subseteq \bigcup R_n$

og $\dot{K} \supseteq \bigcup R_n$; altså er $\dot{K} = \bigcup R_n$, og for ethvert over for kvadratrodsuddragning afsluttet tallegeme L må gælde $L \supseteq \dot{K}$.

Sidste del af sætningen fås nu, idet vi vælger $K_0 = \dot{Q}$, $K_1 = R_1 = \dot{Q}(i)$, K_2 = det første R_n, der er $\supset K_1$, K_3 = det første R_n, der er $\supset K_2$, o.s.v. Processen må fortsætte ubegrænset. Thi ellers måtte $\dot{K}$ være et af tallegemerne R_n, og sikkert ikke $R_1 = \dot{Q}(i)$, idet $\dot{Q}(i)$ åbenbart ikke er afsluttet over for kvadratrodsuddragning. $\dot{K}$ måtte altså være af formen $L(\sqrt{q})$, hvor $i \in L$. Et sådant tallegeme kan imidlertid ikke være afsluttet overfor kvadratrodsuddragning. Thi i så fald måtte det specielt indeholde $\sqrt[4]{q}$. Vi måtte altså have $\sqrt[4]{q} = a_1 + a_2\sqrt{q}$, hvor $a_1, a_2 \in L$. Dette vilde medføre, at $\sqrt{q} = a_1^2 + a_2^2 q + 2a_1 a_2 \sqrt{q}$, altså $a_1^2 + a_2^2 q = 0$ og $2a_1 a_2 = 1$, hvoraf $\sqrt{q} = \pm i 2a_1^2$, hvilket er umuligt, da $\pm i 2a_1^2 \in L$.

Som konsekvens af den fundne fremstilling af $\dot{K}$ vil vi udlede følgende sætning, der rummer alt, hvad vi senere får brug for:

<u>Ethvert konstruerbart tal er algebraisk, og dets grad er en potens af 2.</u>

<u>Bevis.</u> Lad a være et konstruerbart tal.

Hvis a tilhører $K_0 = \dot{Q}$, er a algebraisk af grad $1 = 2^0$.

Hvis a ikke tilhører K_0, betragter vi det mindste n, for hvilket a tilhører K_{n+1}. Da er $a = a_1 + a_2\sqrt{k_n}$, hvor $a_1, a_2 \in K_n$ og $a_2 \neq 0$. Vi betragter også dets konjugerede tal $\tilde{a} = a_1 - a_2\sqrt{k_n}$ i K_{n+1}, og danner polynomiet

$$F(x) = (x-a)(x-\tilde{a}) = x^2 + bx + c.$$

Dette er da et ireduktibelt polynomium i $K_n[x]$.

Hvis b og c begge tilhører $\dot{Q}$, er F også ireduktibelt i $\dot{Q}[x]$, og a følgelig algebraisk af grad 2.

I modsat fald betragter vi det mindste m, for hvilket både b og c tilhører K_{m+1}. Da er $m<n$, og F er også irreduktibelt i $K_{m+1}[x]$. Vi har $b=b_1+b_2\sqrt{k_m}$, $c=c_1+c_2\sqrt{k_m}$, hvor $b_1,b_2,c_1,c_2\in K_m$, og mindst et af tallene b_2 og c_2 er $\neq 0$. Vi betragter også de til b og c konjugerede tal $\tilde{b}=b_1-b_2\sqrt{k_m}$ og $\tilde{c}=c_1-c_2\sqrt{k_m}$ i K_{m+1}. Polynomiet $F_1(x)=x^2+\tilde{b}x+\tilde{c}$ er også irreduktibelt i $K_{m+1}[x]$, og da F og F_1 ikke tilhører $K_m[x]$, er polynomiet

$$G(x)=F(x)F_1(x)=(x^2+bx+c)(x^2+\tilde{b}x+\tilde{c})=x^4+dx^3+ex^2+fx+g$$

et irreduktibelt polynomium i $K_m[x]$.

Hvis d,e,f,g alle tilhører Q, er G også irreduktibelt i $Q[x]$, og a følgelig algebraisk af grad $4=2^2$.

I modsat fald betragter vi det mindste p, for hvilket alle tallene d,e,f,g tilhører K_{p+1}. Da er $p<m$, og G er også irreduktibelt i $K_{p+1}[x]$. Vi har $d=d_1+d_2\sqrt{k_p}$, $e=e_1+e_2\sqrt{k_p}$, $f=f_1+f_2\sqrt{k_p}$, $g=g_1+g_2\sqrt{k_p}$, hvor $d_1,d_2,e_1,e_2,f_1,f_2,g_1,g_2\in K_p$, og mindst et af tallene d_2,e_2,f_2,g_2 er $\neq 0$. Vi betragter også de til d,e,f,g konjugere tal $\tilde{d}=d_1-d_2\sqrt{k_p}$, $\tilde{e}=e_1-e_2\sqrt{k_p}$, $\tilde{f}=f_1-f_2\sqrt{k_p}$, $\tilde{g}=g_1-g_2\sqrt{k_p}$ i K_{p+1}. Polynomiet $G_1(x)=x^4+\tilde{d}x^3+\tilde{e}x^2+\tilde{f}x+\tilde{g}$ er også irreduktibelt i $K_{p+1}[x]$, og da G og G_1 ikke tilhører $K_p[x]$, er polynomiet

$$H(x)=G(x)G_1(x)=(x^4+dx^3+ex^2+fx+g)(x^4+\tilde{d}x^3+\tilde{e}x^2+\tilde{f}x+\tilde{g})$$
$$=x^8+hx^7+\cdots$$

et irreduktibelt polynomium i $K_p[x]$.

Hvis dets koefficienter $h,\ldots$ alle tilhører Q, er H også irreduktibelt i $Q[x]$, og a følgelig algebraisk af grad $8=2^3$.

Ellers fortsætter vi processen, som må ende engang. Hvis den ender efter k skridt, må a være algebraisk af grad 2^k.

Bemærk, at vi i bevisføreisen har benyttet tegnet $\sim$ for konjugering i forskellig betydning på de forskellige trin, først for konjugering i K_{n+1}, så for konjugering i K_{m+1}, o.s.v.

§16. Nødvendigheden af Gauss' betingelse.

I den komplekse plan er vinkelspidserne i den i cirklen med centrum 0 og radius 1 indskrevne regulære n-kant, hvis ene vinkelspids er 1, bestemt som rødderne i polynomiet $x^n - 1$. For at godtgøre nødvendigheden af Gauss' betingelse skal vi altså vise:

Hvis rødderne i polynomiet $x^n - 1$ er konstruerbare, og primfaktoropløsningen for n er

$$n = 2^r p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s},$$

er hvert p_j af formen $2^{2^k}+1$ og hvert $\alpha_j = 1$.

Vi bemærker, at hvis den regulære n-kant kan konstrueres, og $m \geqslant 3$ er divisor i n, kan den regulære m-kant også konstrueres (idet dens vinkelspidser findes blandt n-kantens vinkelspidser).

1) Hvert p_j har formen $2^{2^k}+1$. Vi sætter $p_j = p$. Da p er divisor i n, kan den regulære p-kant konstrueres. De fra 1 forskellige vinkelspidser i denne er rødderne i polynomiet

$$F(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1.$$

Om polynomiet $F(x)$ har vi i §5 vist, at det er irreduktibelt i $Q[x]$ for ethvert primtal p. Dets rødder er altså algebraiske tal af grad $p-1$. Da de for det her betragtede p er konstruerbare, må deres grad være en potens af 2. Vi har altså $p - 1 = 2^k$ eller $p = 2^k + 1$.

Et tal af formen 2^k+1 kan imidlertid kun være et primtal, når k er en potens af 2. Thi hvis k ikke er en potens af 2, har k en ulige divisor $u > 1$. Vi har altså $k = uv$ (u ulige og $\geqslant 3$, v hel $\geqslant 1$). Da har 2^k+1 den ægte divisor $2^v + 1$, idet

$$2^k + 1 = (2^v)^u + 1 = (2^v + 1)(2^{v(u-1)} - 2^{v(u-2)} + 2^{v(u-3)} - \dots + 1).$$

2) Hvert α_j er $=1$. I modsat fald fandtes et $p_j = p$ med $\alpha_j \geqslant 2$. Da var p^2 divisor i n, og følgelig kunde den regulære p^2-kant konstrueres. De fra vinkelspidserne i den regulære p-kant forskellige vinkelspidser i denne er rødderne i polynomiet

$$G(x) = \frac{x^{p^2}-1}{x^p-1} = x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1.$$

Dettes rødder måtte altså være konstruerbare. Vi viser, at dette ikke kan være tilfældet, idet vi viser, at polynomiet $G(x)$ er irreduktibelt i $Q[x]$ for ethvert primtal p. Dets rødder er altså algebraiske af grad $p(p-1)$ og kan følgelig ikke være konstruerbare, når p er ulige.

Irreducibiliteten af polynomiet $G(x)$ vises, idet vi viser ireducibiliteten af polynomiet

$$G(x+1) = \frac{(x+1)^{p^2}-1}{(x+1)^p-1} = \frac{x^{p^2} + a_1 x^{p^2-1} + \cdots + a_{p^2-1}x}{x^p + b_1 x^{p-1} + \cdots + b_{p-1}x}.$$

Her er (jfr. § 5) koefficienterne $b_1, \cdots, b_{p-1}$ alle delelige med p, og $b_{p-1} = p$. For koefficienterne $a_1, \cdots, a_{p^2-1}$ har vi

$$a_q = \binom{p^2}{q} = \frac{p^2(p^2-1)\cdots(p^2-q+1)}{1\cdot 2 \cdots q} \qquad (q \leqslant p^2-1).$$

Da tallet er helt, kan nævneren bortforkortes. I tælleren har vi p som primfaktor 2 gange, hvis $q \leqslant p$, 3 gange, hvis $p+1 \leqslant q \leqslant 2p$, o.s.v. I nævneren har vi p som primfaktor 0 gange, hvis $q \leqslant p-1$, 1 gange, hvis $p \leqslant q \leqslant 2p-1$, o.s.v. Det ses, at p altid forekommer oftere som primfaktor i tælleren end i nævneren. Følgelig er tallene $a_1, \cdots, a_{p^2-1}$ alle delelige med p. Man bemærker endvidere, at $a_{p^2-1} = p^2$. Udtrykket for $G(x+1)$ antager derfor (efter forkortning med x) formen

$$G(x+1) = \frac{x^k + a_1 x^{k-1} + \cdots + a_{k-1}x + p^2}{x^l + b_1 x^{l-1} + \cdots + b_{l-1}x + p},$$

hvor $a_1, \cdots, a_{k-1}, b_1, \cdots, b_{l-1}$ er hele tal delelige med p.

Nu tænkes divisionen (som vi ved går op) udført efter

den kendte metode. Regneskemaet får da udseendet

$$x^l + \cdots + p \;)\; x^k + \cdots + p^2\left(x^{k-l} + c_1 x^{k-l-1} + \cdots + c_{k-l}\right)$$

$$x^k + \cdots$$

$$\cdots + p^2$$

$$\cdots + p^2$$

$$\text{o.s.v.}$$

De med ~ forsynede led i første linie har koefficienter delelige med p. Det samme gælder derfor de med ~ forsynede led i anden linie, og altså også i tredje linie. Dette viser, at koefficienten c_1 bliver delelig med p. Følgelig har alle led i fjerde linie en koefficient delelig med p. Det samme gælder da om femte linie, hvoraf ses, at den næste koefficient i kvotienten bliver delelig med p, o.s.v. Vi ser altså, at $G(x+1)$ får formen

$$G(x+1) = x^{k-l} + c_1 x^{k-l-1} + \cdots + c_{k-l},$$

hvor alle $c_1, \cdots, c_{k-l}$ er delelige med p. Ved indsætning af $x=0$ ses, at $c_{k-l} = p$. Af Schönemann-Eisensteins irreducibilitetskriterium fremgår derfor, at $G(x+1)$ er irreducibelt i $Q[x]$.

§17. Tilstrækkeligheden af Gauss' betingelse.

Hvis den regulære n_1-kant og den regulære n_2-kant, hvor n_1 og n_2 er to indbyrdes primiske tal, begge kan konstrueres, kan den regulære $n = n_1 n_2$-kant også konstrueres. For at indse dette benytter vi følgende sætning fra talteorien:

Når de positive hele tal n_1 og n_2 er indbyrdes primiske, findes der hele tal x_1 og x_2, således at $x_1 n_1 + x_2 n_2 = 1$.

Bevis. Vi opskriver Euklids algoritme for tallene

n_1 og n_2:

$$n_1 = n_2 q_1 + n_3 \qquad 0 < n_3 < n_2$$
$$n_2 = n_3 q_2 + n_4 \qquad 0 < n_4 < n_3$$
$$\cdots$$
$$n_{s-2} = n_{s-1} q_{s-2} + n_s \qquad 0 < n_s < n_{s-1}$$
$$n_{s-1} = n_s q_{s-1}.$$

Da er n_s største fælles divisor for n_1 og n_2, altså i det foreliggende tilfælde $= 1$. Den første ligning viser, at n_3 er en linearkombination af n_1 og n_2 med hele koefficienter (nemlig $1 \cdot n_1 + (-q_1) n_2$). Indsættes n_3 i den anden ligning, ses at n_4 ligeledes er en linearkombination af n_1 og n_2 med hele koefficienter. Fortsættes således, finder vi, at n_s er en linearkombination af n_1 og n_2 med hele koefficienter.

Af ligningen $x_1 n_1 + x_2 n_2 = 1$ følger for et vilkårligt helt tal d, idet $n = n_1 n_2$, at

$$d\frac{2\pi}{n} = x_1 d \frac{2\pi}{n_2} + x_2 d \frac{2\pi}{n_1}, \text{ altså } e^{id\frac{2\pi}{n}} = e^{ix_1 d\frac{2\pi}{n_2}} e^{ix_2 d\frac{2\pi}{n_1}}.$$

Nu er $e^{ix_1 d\frac{2\pi}{n_2}}$ en vinkelspids i den regulære n_2-kant og $e^{ix_2 d\frac{2\pi}{n_1}}$ en vinkelspids i den regulære n_1-kant. Ifølge forudsætning kan disse konstrueres. Altså kan $e^{id\frac{2\pi}{n}}$ konstrueres for ethvert helt d, d. v. s. den regulære n-kant kan konstrueres.

For at godtgøre tilstrækkeligheden af Gauss' betingelse er det derfor nok at vise, at den regulære p-kant kan konstrueres for ethvert ulige primtal af formen $p = 2^{2^k} + 1$ eller, hvad der (§ 16) kommer ud på det samme, for ethvert ulige primtal af formen $p = 2^k + 1$. Thi hvis dette er vist, og $n = 2^r p_1 p_2 \cdots p_s$, hvor $p_1, p_2, \ldots, p_s$ er indbyrdes forskellige ulige primtal af denne form, slutter vi først, at den regulære $p_1 p_2$-kant kan kon-

struere, dernæst at den regulære $(p_1p_2)p_3$-kant kan konstrueres, o.s.v., altså at den regulære $p_1p_2\cdots p_s$-kant kan konstrueres, hvoraf følger, at den regulære n-kant kan konstrueres.

Restklasseringen modulo et primtal. For et vilkårligt primtal p betragter vi mængden Z_p af restklasser af Z mod p. Idet vi for et vilkårligt $x \in Z$ betegner den restklasse mod p, der indeholder x, med (x), består Z_p af de p restklasser $(0), (1), \cdots, (p-1)$. Gennem fastsættelserne

$$(x) + (y) = (x+y), \qquad (x)(y) = (xy)$$

er Z_p organiseret som en kommutativ ring, hvis nulelement er (0). Den har et et element, nemlig (1).

Denne ring er et legeme. Thi for et vilkårligt element $(a) \neq (0)$ af Z_p er produkterne $(a)(0), (a)(1), \cdots, (a)(p-1)$ indbyrdes forskellige. [Hvis nemlig $(a)(x_1) = (a)(x_2)$, altså $(ax_1) = (ax_2)$, må p gå op i $a(x_1 - x_2)$; da p ikke går op i a, må p gå op i $x_1 - x_2$, d.v.s. $(x_1) = (x_2)$.] Ligningen $(a)(x) = (b)$ har derfor for ethvert (b) i Z_p en og kun en løsning (x).

Da $(a)(0) = (0)$, slutter vi af det foregående, at når $(a) \neq (0)$, er $(a)(1), (a)(2), \cdots, (a)(p-1)$ en permutation af $(1), (2), \cdots, (p-1)$. Følgelig er

$$(a)(1)(a)(2)\cdots(a)(p-1) = (1)(2)\cdots(p-1).$$

Idet $(1)(2)\cdots(p-1) \neq (0)$, følger heraf Fermats sætning

$$(a)^{p-1} = (1).$$

For en vilkårlig restklasse $(a) \neq (0)$ betegner vi det mindste hele positive tal g, for hvilket $(a)^g = (1)$, som graden af (a). I følgen

$$(a), (a)^2, \cdots, (a)^g, (a)^{g+1}, \cdots$$

er $\textcircled{a}^g$ altså den første restklasse, som er $=\textcircled{1}$. Idet $\textcircled{a}^{g+1}=\textcircled{a}$, $\textcircled{a}^{g+2}=\textcircled{a}^2$, ..., ser vi, at den næste restklasse i følgen, der er $=\textcircled{1}$, må være $\textcircled{a}^{2g}$, den næste igen $\textcircled{a}^{3g}$, o.s.v. Da $\textcircled{a}^{p-1}=\textcircled{1}$, slutter vi, at g <u>må være divisor i</u> $p-1$. Hvis graden af $\textcircled{a}$ netop er $p-1$ kaldes $\textcircled{a}$ <u>primitiv</u>. I såfald er $\textcircled{a}, \textcircled{a}^2, \ldots, \textcircled{a}^{p-1}$ en permutation af $\textcircled{1}, \textcircled{2}, \ldots, \textcircled{p-1}$. Thi $\textcircled{a}, \textcircled{a}^2, \ldots, \textcircled{a}^{p-1}$ er alle $\neq\textcircled{0}$ og må være indbyrdes forskellige, idet af $\textcircled{a}^r=\textcircled{a}^s$, $1\leqslant r<s\leqslant p-1$, vilde følge $\textcircled{a}^{s-r}=\textcircled{1}$.

En klassisk sætning i talteorien udsiger, at <u>der findes primitive restklasser for ethvert primtal</u> p. Vi vil her nøjes med at eftervise dette for ulige primtal p af formen $p=2^k+1$.

I dette tilfælde må graden g af enhver restklasse $\textcircled{a}\neq\textcircled{0}$ som divisor i $p-1=2^k$ være et af tallene $1, 2, 2^2, \ldots, 2^k$. For de $\textcircled{a}$, for hvilke $g<2^k$, gælder altså $\textcircled{a}^{2^{k-1}}=\textcircled{1}$. Vi skal vise, at dette ikke kan gælde for alle $\textcircled{a}$. Hertil bemærkes, at hvis $\textcircled{x}^2=\textcircled{y}^2$, altså $(\textcircled{x}-\textcircled{y})(\textcircled{x}+\textcircled{y})=\textcircled{0}$, er enten $\textcircled{x}=\textcircled{y}$ eller $\textcircled{x}=-\textcircled{y}$. En ligning $\textcircled{x}^2=\textcircled{b}$ har altså højst to løsninger. Heraf følger, at en ligning $\textcircled{x}^4=\textcircled{b}$ har højst 4 løsninger [idet man først må søge de højst to $\textcircled{z}$, for hvilke $\textcircled{z}^2=\textcircled{b}$, og derefter for hvert af dem de højst to $\textcircled{x}$, for hvilke $\textcircled{x}^2=\textcircled{z}$]. Fortsættes således, ses, at en ligning $\textcircled{x}^{2^g}=\textcircled{b}$ har højst 2^g løsninger. Følgelig kan $\textcircled{a}^{2^{k-1}}=\textcircled{1}$ ikke gælde for alle $\textcircled{a}\neq\textcircled{0}$.

Vi er nu i stand til at vise, at <u>den regulære p-kant kan konstrueres, når</u> p <u>er et ulige primtal af formen</u> $p=2^k+1$. For simpelheds skyld knytter vi betragtningerne til tilfældet $p=17$, men fremstillingen formes således, at man kan se, at den er

gyldig i alle tilfælde.

I tilfældet $p=17$ er ③ en primitiv restklasse, som det ses af følgende tabel:

q	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$③^q$	③	⑨	⑩	⑬	⑤	⑮	⑪	⑯	⑭	⑧	⑦	④	⑫	②	⑥	①

Heraf ses, at hvis vi ordner rødderne $\varepsilon_j = e^{ij\frac{2\pi}{17}}$, $j = 1, 2, \dots, 16$ i polynomiet

$$\frac{x^{17}-1}{x-1} = x^{16} + x^{15} + \dots + x + 1$$

i rækkefølgen

$$\varepsilon_3\ \varepsilon_9\ \varepsilon_{10}\ \varepsilon_{13}\ \varepsilon_5\ \varepsilon_{15}\ \varepsilon_{11}\ \varepsilon_{16}\ \varepsilon_{14}\ \varepsilon_8\ \varepsilon_7\ \varepsilon_4\ \varepsilon_{12}\ \varepsilon_2\ \varepsilon_6\ \varepsilon_1$$

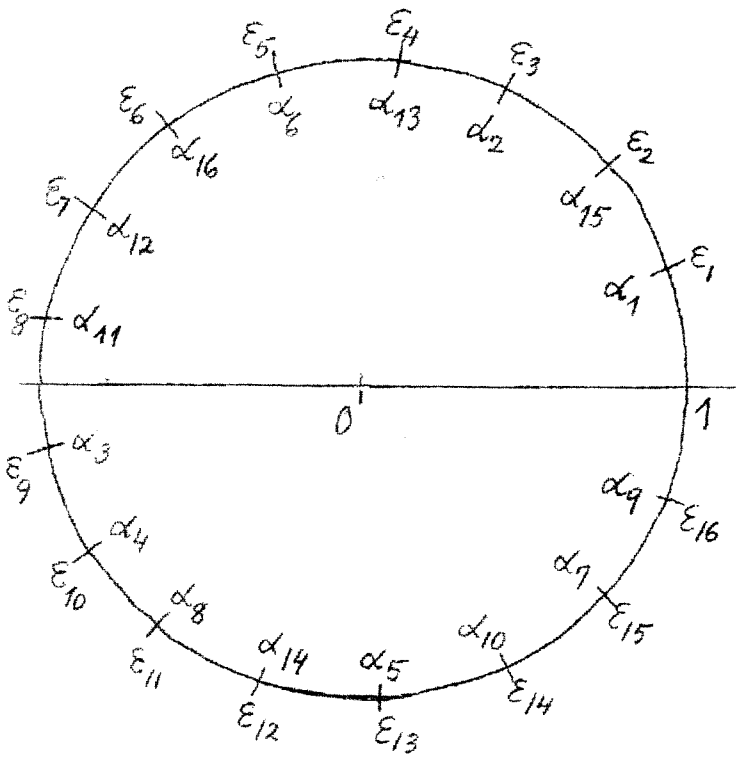
og svarende til denne rækkefølge benævner dem

$$\alpha_2\ \alpha_3\ \alpha_4\ \alpha_5\ \alpha_6\ \alpha_7\ \alpha_8\ \alpha_9\ \alpha_{10}\ \alpha_{11}\ \alpha_{12}\ \alpha_{13}\ \alpha_{14}\ \alpha_{15}\ \alpha_{16}\ \alpha_1,$$

gælder

$$\alpha_1^3 = \alpha_2,\ \alpha_2^3 = \alpha_3,\ \dots,\ \alpha_{14}^3 = \alpha_{15},\ \alpha_{15}^3 = \alpha_{16},\ \alpha_{16}^3 = \alpha_1.$$

I den <u>cykliske orden</u>, hvor α_2 er efterfølger for α_1, α_3 efterfølger for α_2, $\dots$, α_{16} efterfølger for α_{15}, og α_1 er efterfølger for α_{16}, gælder altså, at hver rod er tredje potens af sin forgænger. Vi bemærker, at α_1 og α_9 er konjugerede, ligeså α_2 og α_{10}, $\dots$, α_8 og α_{16}. Sættes $\frac{2\pi}{17} = u$, ser man, at



$$\alpha_1+\alpha_9 = 2\cos u \quad \alpha_2+\alpha_{10} = 2\cos 3u \quad \alpha_3+\alpha_{11} = 2\cos 8u \quad \alpha_4+\alpha_{12} = 2\cos 7u$$

$$\alpha_5+\alpha_{13} = 2\cos 4u \quad \alpha_6+\alpha_{14} = 2\cos 5u \quad \alpha_7+\alpha_{15} = 2\cos 2u \quad \alpha_8+\alpha_{16} = 2\cos 6u.$$

Vi bemærker endelig, at

$$\alpha_1+\alpha_2+\cdots+\alpha_{16}=-1$$

(nemlig lig med (-1) gange koefficienten til x^{15} i polynomiet $x^{16}+x^{15}+\cdots+x+1$).

Vi spalter nu summen $\alpha_1+\alpha_2+\cdots+\alpha_{16}$ i de to summer

$$\beta_1=\alpha_1+\alpha_3+\alpha_5+\alpha_7+\alpha_9+\alpha_{11}+\alpha_{13}+\alpha_{15}=2\cos u+2\cos 8u+2\cos 4u+2\cos 2u$$

$$\beta_2=\alpha_2+\alpha_4+\alpha_6+\alpha_8+\alpha_{10}+\alpha_{12}+\alpha_{14}+\alpha_{16}=2\cos 3u+2\cos 7u+2\cos 5u+2\cos 6u.$$

En grov vurdering viser, at $\beta_1>\beta_2$. Vi har

$$\beta_1+\beta_2=-1$$

og vil nu også beregne $\beta_1\beta_2$. Det gør vi ved at beregne

$$\begin{aligned}2\beta_1\beta_2=\ &\alpha_1\alpha_2+\alpha_2\alpha_3+\alpha_3\alpha_4+\cdots+\alpha_{15}\alpha_{16}+\alpha_{16}\alpha_1\\ &+\alpha_1\alpha_4+\alpha_2\alpha_5+\alpha_3\alpha_6+\cdots+\alpha_{15}\alpha_2+\alpha_{16}\alpha_3\\ &+\alpha_1\alpha_6+\alpha_2\alpha_7+\alpha_3\alpha_8+\cdots+\alpha_{15}\alpha_4+\alpha_{16}\alpha_5\\ &+\cdots\\ &+\alpha_1\alpha_{16}+\alpha_2\alpha_1+\alpha_3\alpha_2+\cdots+\alpha_{15}\alpha_{14}+\alpha_{16}\alpha_{15}.\end{aligned}$$

Vi har fundet $2\beta_1\beta_2$ ved at multiplicere hvert led i β_1 med alle led i β_2 og hvert led i β_2 med alle led i β_1. Dette giver 128 produkter, der er opstillet således: I første søjle har vi skrevet produkterne af α_1 og leddene i β_2 begyndende med α_2 og følgende ordenen af leddene i β_2. I anden søjle har vi skrevet produkterne af α_2 og leddene i β_1 begyndende med α_3 og følgende ordenen af leddene i β_1, så at vi efter α_{15} ender med α_1. I tredje søjle har vi skrevet produkterne af α_3 og leddene i β_2 begyndende med α_4 og følgende ordenen af leddene i β_2, så at vi efter α_{16} ender med α_2, o.s.v. På denne måde er opnået, at leddene i anden søjle er tredje potenserne af leddene i første søjle, idet i hver række de to faktorer i anden søjle er efterfølgerne i den cykliske orden for de to faktorer i første søjle. På tilsvarende måde er leddene i tredje søjle tredje potenserne af leddene i anden søjle, o.s.v. Dette

medfører, at vi kan beregne summen af de 128 led uden faktisk at udregne leddene. Thi hvert produkt $\alpha_i\alpha_j$, der optræder i $2\beta_1\beta_2$, er selv et α_k [idet jo de eneste produkter $\alpha_i\alpha_j$, for hvilke dette ikke gælder, er dem, for hvilke de to indices har differens 8, og sådanne produkter forekommer ikke i $2\beta_1\beta_2$]. Hvis nu en række begynder f. ek. med α_{13} [dette er tilfældet for første række], må andet led i rækken være α_{14}, o.s.v., så at leddene i rækken er $\alpha_{13}, \alpha_{14}, \alpha_{15}, \alpha_{16}, \alpha_1, \alpha_2, \ldots, \alpha_{12}$. I hver række er summen af leddene derfor -1. Vi har derfor $2\beta_1\beta_2 = -8$ og følgelig

$$\beta_1\beta_2 = -4.$$

Tallene β_1 og β_2 er derfor rødderne i polynomiet x^2+x-4, og da $\beta_1 > \beta_2$ finder vi

$$\left.\begin{matrix}\beta_1\\ \beta_2\end{matrix}\right\} = -\frac{1}{2} \pm \sqrt{\left(\frac{1}{2}\right)^2+4}.$$

Vi spalter nu β_1 i

$$\gamma_1 = \alpha_1+\alpha_5+\alpha_9+\alpha_{13} = 2\cos u + 2\cos 4u$$

$$\gamma_3 = \alpha_3+\alpha_7+\alpha_{11}+\alpha_{15} = 2\cos 8u + 2\cos 2u.$$

Da er $\gamma_1 > \gamma_3$ og $\gamma_1+\gamma_3 = \beta_1$. Vi ønsker at beregne $\gamma_1\gamma_3$. Idet vi går frem som foran, finder vi

$$\begin{aligned} 2\gamma_1\gamma_3 = {} & \alpha_1\alpha_3+\alpha_3\alpha_5+\cdots+\alpha_{15}\alpha_1 \\ & +\alpha_1\alpha_7+\alpha_3\alpha_9+\cdots+\alpha_{15}\alpha_5 \\ & +\alpha_1\alpha_{11}+\alpha_3\alpha_{13}+\cdots+\alpha_{15}\alpha_9 \\ & +\alpha_1\alpha_{15}+\alpha_3\alpha_1+\cdots+\alpha_{15}\alpha_{13}. \end{aligned}$$

Her er i hver række hvert led niende potens af sin forgænger og hvert af de optrædende produkter $\alpha_i\alpha_j$ er selv et α_k. Hvis nu en række begynder f. eks. med α_4 [dette er tilfældet for første række], må rækken bestå af $\alpha_4, \alpha_6, \alpha_8, \alpha_{10}, \alpha_{12}, \alpha_{14}, \alpha_{16}, \alpha_2$, og dens sum må være β_2. Man ser, at for hver række er leddenes sum enten β_1 eller β_2. Følgelig kan $\gamma_1\gamma_3$ udtrykkes ved hjælp af de allerede be-

regnede tal β_1 og β_2. Ved at udregne de første led i de fire rækker finder man, at første og fjerde række giver summen β_2 og anden og tredje række summen β_1. Vi finder derfor $2\gamma_1\gamma_3 = 2\beta_1 + 2\beta_2 = -2$. Altså er $\gamma_1\gamma_3 = -1$. Tallene γ_1 og γ_3 er derfor rødderne i polynomiet $x^2 - \beta_1 x - 1$, og da $\gamma_1 > \gamma_3$, har vi

$$\left.\begin{matrix}\gamma_1\\ \gamma_3\end{matrix}\right\} = \frac{\beta_1}{2} \pm \sqrt{\left(\frac{\beta_1}{2}\right)^2 + 1}.$$

På tilsvarende måde spalter vi β_2 i

$$\gamma_2 = \alpha_2 + \alpha_6 + \alpha_{10} + \alpha_{14} = 2\cos 3u + 2\cos 5u$$
$$\gamma_4 = \alpha_4 + \alpha_8 + \alpha_{12} + \alpha_{16} = 2\cos 7u + 2\cos 6u.$$

Da er $\gamma_2 > \gamma_4$ og $\gamma_2 + \gamma_4 = \beta_2$. Vi finder

$$\begin{aligned} 2\gamma_2\gamma_4 = {} & \alpha_2\alpha_4 + \alpha_4\alpha_6 + \cdots + \alpha_{16}\alpha_2 \\ & + \alpha_2\alpha_8 + \alpha_4\alpha_{10} + \cdots + \alpha_{16}\alpha_6 \\ & + \alpha_2\alpha_{12} + \alpha_4\alpha_{14} + \cdots + \alpha_{16}\alpha_{10} \\ & + \alpha_2\alpha_{16} + \alpha_4\alpha_2 + \cdots + \alpha_{16}\alpha_{14}, \end{aligned}$$

og ved at udregne de første led i de fire rækker finder man, at første og fjerde række giver summen β_1 og anden og tredje række summen β_2. Altså er $2\gamma_2\gamma_4 = 2\beta_1 + 2\beta_2 = -2$ og $\gamma_2\gamma_4 = -1$, så at γ_2 og γ_4 er rødderne i polynomiet $x^2 - \beta_2 x - 1$. Da $\gamma_2 > \gamma_4$ fås

$$\left.\begin{matrix}\gamma_2\\ \gamma_4\end{matrix}\right\} = \frac{\beta_2}{2} \pm \sqrt{\left(\frac{\beta_2}{2}\right)^2 + 1}.$$

Således kan vi fortsætte, og vi ser, at processen må ende med, at vi finder udtryk for alle rødderne $\alpha_1, \alpha_2, \ldots, \alpha_{16}$. Da regningerne stadig fører til konstruerbare tal, må 17-kanten være konstruerbar.

For at nå til en konstruktion er det dog ikke nødvendigt at gennemføre beregningen af alle rødderne. Det er tilstrækkeligt, at vi nu spalter γ_1 i

$$\delta_1 = \alpha_1 + \alpha_9 = 2\cos u$$
$$\delta_5 = \alpha_5 + \alpha_{13} = 2\cos 4u.$$

Da er $\delta_1 + \delta_5 = \gamma_1$, og vi finder

$$\delta_1\delta_5 = \alpha_1\alpha_5 + \alpha_5\alpha_4 + \alpha_4\alpha_{13} + \alpha_{13}\alpha_1 = \alpha_{10} + \alpha_{14} + \alpha_2 + \alpha_{16} = \gamma_2 .$$

Altså er δ_1 og δ_5 rødderne i polynomiet $x^2 - \gamma_1 x + \gamma_2$, og da $\delta_1 > \delta_5$, finder vi

$$\left.\begin{matrix}\delta_1\\ \delta_5\end{matrix}\right\} = \frac{\gamma_1}{2} \pm \sqrt{\left(\frac{\gamma_1}{2}\right)^2 - \gamma_2} .$$

På grundlag af værdien for $\delta_1 = 2\cos u = 2\cos\frac{2\pi}{17}$ kan man konstruere $\alpha_1 = \varepsilon_1$ og dermed 17-kanten. Til selve konstruktionen benytter vi følgende formler, der blot er en let omskrivning af de ovenfor fundne:

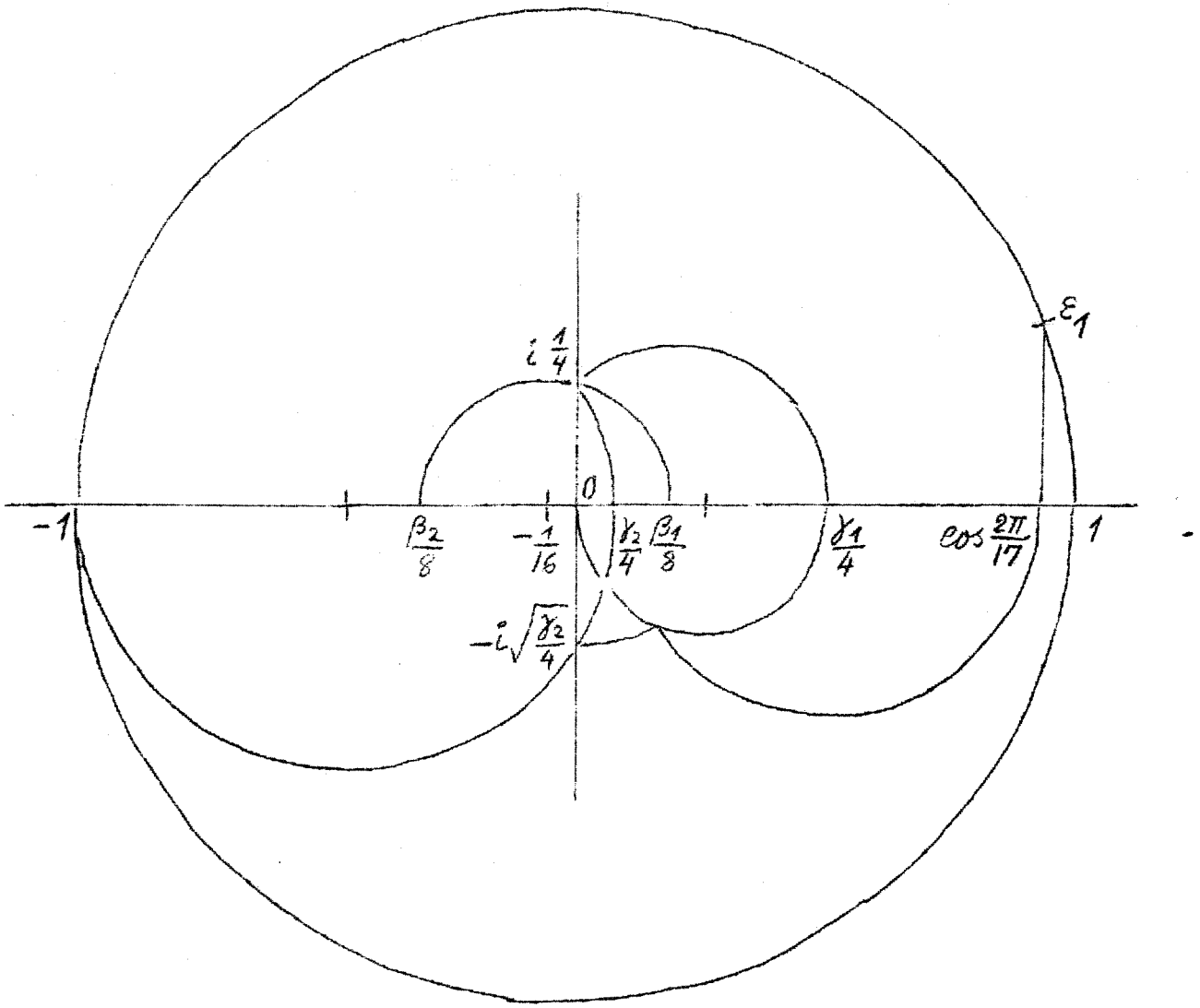
$$\cos\frac{2\pi}{17} = \frac{\gamma_1}{4} + \sqrt{\left(\frac{\gamma_1}{4}\right)^2 - \frac{\gamma_2}{4}},$$

hvor

$$\frac{\gamma_1}{4} = \frac{\beta_1}{8} + \sqrt{\left(\frac{\beta_1}{8}\right)^2 + \left(\frac{1}{4}\right)^2}, \qquad \frac{\gamma_2}{4} = \frac{\beta_2}{8} + \sqrt{\left(\frac{\beta_2}{8}\right)^2 + \left(\frac{1}{4}\right)^2},$$

hvor

$$\frac{\beta_1}{8} = -\frac{1}{16} + \sqrt{\left(\frac{1}{16}\right)^2 + \left(\frac{1}{4}\right)^2}, \qquad \frac{\beta_2}{8} = -\frac{1}{16} - \sqrt{\left(\frac{1}{16}\right)^2 + \left(\frac{1}{4}\right)^2}.$$



§18. Transcendens af e og π.

Det klassiske problem om cirklens kvadratur går ud på ud fra to givne punkter O og E ved hjælp af passer og lineal at konstruere et kvadrat med samme areal som cirklen med centrum O og radius OE. Man ser, at det kommer ud på ud fra punkterne 0 og 1 i den komplekse plan at konstruere punktet $\sqrt{\pi}$. At dette ikke er muligt blev vist af Lindemann 1882, idet han endda viste, at π (og følgelig også $\sqrt{\pi}$) er et transcendent tal. En forudsætning for dette bevis var det af Hermite 1873 givne bevis for, at e er et transcendent tal. Begge beviser er senere blevet simplificeret på forskellig vis.

Vi skal benytte, at eksponentialfunktionen e^x er en differentiabel funktion på $\mathbb{C}$ med den afledede e^x.

For et vilkårligt polynomium $F(x) \in \mathbb{C}[x]$ skriver vi $F(0)e^x$ på formen

$$F(0)e^x = F(x) + g(x)e^x.$$

Da er funktionen $g(x) = F(0) - F(x)e^{-x}$ differentiabel med den afledede

$$g'(x) = (F(x) - F'(x))e^{-x} = f(x)e^{-x},$$

hvor $f(x)$ er polynomiet $F(x) - F'(x)$. Heraf fås $f'(x) = F'(x) - F''(x)$, $f''(x) = F''(x) - F'''(x)$, o.s.v., altså

$$F(x) = f(x) + f'(x) + f''(x) + \cdots,$$

hvor leddene i den uendelige række naturligvis er 0 fra et vist trin. I stedet for at gå ud fra $F(x)$ kan vi gå ud fra et vilkårligt polynomium $f(x) \in \mathbb{C}[x]$ og definere $F(x)$ ved det anførte udtryk. Da bliver åbenbart $F(x) - F'(x) = f(x)$, og vi finder altså (idet $g(0) = 0$)

$$F(0)e^x = F(x) + R(x), \qquad R(x) = \left(\int_0^x f(t)e^{-t}\,dt\right)e^x,$$

hvor integrationen f.eks. er langs liniestykket fra 0 til x. Heraf fås for $|x| \leqslant s$ vurderingen

$$|R(x)| = \left| \int_0^x f(t)\, e^{x-t}\, dt \right| \leqslant \varrho \sup_{|t| \leqslant \varrho} |f(t)|\, e^{\varrho}.$$

[Valges specielt $f(x) = \frac{x^n}{n!}$, bliver $F(x)$ afsnittet $1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$ i potensrækken for e^x. Idet $F(0) = 1$, fås $e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!} + R(x)$, med $|R(x)| \leqslant \frac{\varrho^{n+1}}{n!} e^{\varrho}$ for $|x| \leqslant \varrho$. For det følgende er dette valg af $f(x)$ uden værdi.]

Transcendens af e. Vi skal vise, at et egentligt polynomium

$$P(x) = a_0 + a_1 x + \cdots + a_n x^n$$

med hele koefficienter ikke kan have roden e. Vi kan åbenbart antage $a_0 \neq 0$. Vi skal altså vise, at

$$P(e) = a_0 + a_1 e + \cdots + a_n e^n \neq 0.$$

For at finde udtryk for $e, \cdots, e^n$, hvoraf dette kan fremgå, benytter vi det foranstående, idet vi vælger

$$f(x) = \frac{x^{p-1}(x-1)^p \cdots (x-n)^p}{(p-1)!},$$

hvor p er et primtal, over hvilket der senere skal disponeres. Vi går nu frem i skridt.

(1) Undersøgelse af $F(0)$. Man ser, at

$$f(x) = \frac{x^{p-1}}{(p-1)!}\left([(-1)^n n!]^p + c_1 x + c_2 x^2 + \cdots \right),$$

hvor $c_1, c_2, \cdots$ er hele tal. Sammenholdes dette med Taylors formel, ses, at $f(0), f'(0), \cdots, f^{(p-2)}(0)$ alle er 0, medens $f^{(p-1)}(0) = [(-1)^n n!]^p$, og $f^{(p)}(0), f^{(p+1)}(0), \cdots$ alle er hele tal deleligе med p. Følgelig er $F(0) = f(0) + f'(0) + f''(0) + \cdots$ et helt tal, som sikkert ikke er deleligt med p, hvis blot $p > n$. Da er specielt $F(0) \neq 0$. I det følgende antages $p > n$.

(2) Undersøgelse af $F(1), \cdots, F(n)$. For et vilkårligt $k = 1, \cdots, n$ finder vi

$$f(k+y) = \frac{y^p}{(p-1)!}\,(d_0 + d_1 y + d_2 y^2 + \cdots),$$

hvor $d_0, d_1, d_2, \cdots$ er hele tal. Sammenholdes dette med

Taylors formel, ses, at $f(k), f'(k), \cdots, f^{(p-1)}(k)$ alle er 0, medens $f^{(p)}(k), f^{(p+1)}(k), \ldots$ alle er hele tal delelige med p. Følgelig er $F(k)$ et helt tal deleligt med p.

(3) Vurdering af $R(1), \cdots, R(n)$. For $|x| \leqslant n$, og specielt altså for $x = 1, \ldots, n$, finder vi

$$|R(x)| \leqslant n \frac{n^{p-1}(n+1)^p \cdots (2n)^p}{(p-1)!} e^n = A \frac{B^p}{(p-1)!},$$

hvor A og B er positive tal, der ikke afhænger af p.

(4) I $P(e)$ indsættes nu $e^k = \frac{F(k)+R(k)}{F(0)}$, hvorved fås

$$P(e) = \frac{a_0 F(0) + a_1 F(1) + \cdots + a_n F(n) + a_1 R(1) + \cdots + a_n R(n)}{F(0)} = \frac{Q+\varepsilon}{F(0)}.$$

Her er $Q = a_0 F(0) + a_1 F(1) + \cdots + a_n F(n)$ et helt tal. Da $F(0)$ ikke er deleligt med p, medens $F(1), \ldots, F(n)$ er delelige med p, ses, at Q ikke er deleligt med p, hvis blot $p > |a_0|$. Da gælder naturligvis $Q \neq 0$ og følgelig $|Q| \geqslant 1$.

På den anden side gælder om $\varepsilon = a_1 R(1) + \cdots + a_n R(n)$, at $|\varepsilon| \leqslant (|a_1| + \cdots + |a_n|) A \frac{B^p}{(p-1)!}$. Da højre side går mod 0, når $p \to \infty$, findes et N, så at $|\varepsilon| < 1$, når blot $p > N$.

Ved at vælge $p > \max\{n, |a_0|, N\}$ ser vi, at $P(e) \neq 0$.

<u>Transcendens af π.</u> Som udgangspunkt tager vi Eulers ligning

$$e^{i\pi} = -1 \quad \text{eller} \quad 1 + e^{i\pi} = 0.$$

Hvis π var algebraisk, var $i\pi$ også algebraisk. Beviset for, at π er transcendent, kan derfor føres ved at vi viser, at der for ethvert algebraisk tal α gælder

$$1 + e^{\alpha} \neq 0.$$

Dette er ensbetydende med at vise, at hvis $\alpha_1, \ldots, \alpha_n$ er rødderne i et polynomium $x^n + a_1 x^{n-1} + \cdots + a_n$ med rationale koefficienter, er

$$K = (1 + e^{\alpha_1}) \cdots (1 + e^{\alpha_n}) \neq 0.$$

Ved at multiplicere ud får vi

$$K = 1 + e^{\alpha_1} + \cdots + e^{\alpha_n} + e^{\alpha_1+\alpha_2} + \cdots + e^{\alpha_{n-1}+\alpha_n} + \cdots + e^{\alpha_1+\cdots+\alpha_n}.$$

De $\binom{n}{1}+\binom{n}{2}+\cdots+\binom{n}{n}$ tal, der optræder som eksponenter i dette udtryk, er rødderne i polynomiet

$$(x-\alpha_1)\cdots(x-\alpha_n)(x-(\alpha_1+\alpha_2))\cdots(x-(\alpha_{n-1}+\alpha_n))\cdots(x-(\alpha_1+\cdots+\alpha_n)).$$

Betragtes et øjeblik $\alpha_1, \cdots, \alpha_n$ som variable, er dette et polynomium $S(x;\alpha_1,\cdots,\alpha_n)$, der er symmetrisk i $\alpha_1,\cdots,\alpha_n$ og har lutter hele koefficienter. Det fremkommer altså af et polynomium $T(x;a_1,\cdots,a_n)$ med hele koefficienter, ved at man for $a_1,\cdots,a_n$ indsætter de elementarsymmetriske polynomier i $\alpha_1,\cdots,\alpha_n$. Indsættes talværdierne $\alpha_1,\cdots,\alpha_n$, bliver værdierne af de elementarsymmetriske polynomier koefficienterne i polynomiet $x^n+a_1x^{n-1}+\cdots+a_n$. Eksponenterne i K er derfor rødderne i et polynomium med rationale koefficienter.

Lad $\beta_1,\cdots,\beta_m$ være de af disse rødder, der er $\neq 0$. Da er

$$K = b_0 + e^{\beta_1} + \cdots + e^{\beta_m},$$

hvor b_0 $(= 2^n - m)$ er et helt tal >0, og hvor $\beta_1,\cdots,\beta_m$ er rødderne i et polynomium med rationale koefficienter og fra 0 forskelligt konstantled. Altså er $\beta_1,\cdots,\beta_m$ også rødderne i et polynomium

$$\varphi(x) = hx^m + h_1x^{m-1} + \cdots + h_m = h(x-\beta_1)\cdots(x-\beta_m)$$

med hele koefficienter, hvor $h>0$, $h_m\neq 0$. Følgelig er $h\beta_1,\cdots,h\beta_m$ rødderne i polynomiet

$$h^{m-1}\varphi\left(\frac{x}{h}\right) = x^m + h_1x^{m-1} + hh_2x^{m-2} + \cdots + h^{m-1}h_m = (x-h\beta_1)\cdots(x-h\beta_m).$$

Tallene $h\beta_1,\cdots,h\beta_m$ er således hele algebraiske tal.

For at finde udtryk for $e^{\beta_1},\cdots,e^{\beta_m}$, hvoraf det kan fremgå, at $K\neq 0$, vælger vi nu

$$f(x) = \frac{(hx)^{p-1}(hx-h\beta_1)^p\cdots(hx-h\beta_m)^p}{(p-1)!},$$

hvor ligesom før p er et primtal, hvorover der senere

skal disponeres, og går atter frem i skridt.

(1) Undersøgelse af $F(0)$. Vi bemærker, at produktet $(hx-h\beta_1)\cdots(hx-h\beta_m)$ simpelthen er polynomiet $h^{m-1}\varphi(x)$; det har altså hele koefficienter og konstantleddet $h^{m-1}h_m$. Følgelig er

$$f(x)=\frac{x^{p-1}}{(p-1)!}\left(h^{p-1}[h^{m-1}h_m]^p+c_1x+c_2x^2+\cdots\right),$$

hvor $c_1, c_2, \ldots$ er hele tal. Sammenholdes dette med Taylors formel, ses, at $f(0), f'(0), \ldots, f^{(p-2)}(0)$ alle er 0, medens $f^{(p-1)}(0)=h^{p-1}[h^{m-1}h_m]^p$, og $f^{(p)}(0), f^{(p+1)}(0), \ldots$ alle er hele tal deleligе med p. Følgelig er $F(0)=f(0)+f'(0)+f''(0)+\cdots$ et helt tal, som sikkert ikke er deleligt med p, hvis blot $p>\max\{h,|h_m|\}$. Da er specielt $F(0)\neq 0$. I det følgende antages $p>\max\{h,|h_m|\}$.

(2) Undersøgelse af $F(\beta_1),\ldots,F(\beta_m)$. For et vilkårligt $k=1,\ldots,m$ finder vi

$$f(\beta_k+y)=\frac{y^p}{(p-1)!}(d_0+d_1y+d_2y^2+\cdots),$$

hvor koefficienterne $d_0, d_1, d_2, \ldots$ er hele algebraiske tal. Sammenholdes dette med Taylors formel, ses, at $f(\beta_k)$, $f'(\beta_k),\ldots,f^{(p-1)}(\beta_k)$ alle er 0, medens $f^{(p)}(\beta_k), f^{(p+1)}(\beta_k),\ldots$ alle er af formen p gange et helt algebraisk tal. Følgelig er også $F(\beta_k)=f(\beta_k)+f'(\beta_k)+f''(\beta_k)+\cdots$ af formen p gange et helt algebraisk tal.

(3) Vurdering af $R(\beta_1),\ldots,R(\beta_m)$. Sættes $\varrho=\max\{|\beta_1|,\ldots,|\beta_m|\}$, gælder for $|x|\leqslant\varrho$, og specielt altså for $x=\beta_1,\ldots,\beta_m$, at

$$|R(x)|\leqslant\varrho\frac{(h\varrho)^{p-1}(h2\varrho)^p\cdots(h2\varrho)^p}{(p-1)!}e^{\varrho}=A\frac{B^p}{(p-1)!},$$

hvor A og B betegner positive tal, der ikke afhænger af p.

(4) I K indsættes nu $e^{\beta_k}=\dfrac{F(\beta_k)+R(\beta_k)}{F(0)}$, hvorved fås

$$K = \frac{b_0 F(0) + F(\beta_1) + \cdots + F(\beta_m) + R(\beta_1) + \cdots + R(\beta_m)}{F(0)} = \frac{Q+\varepsilon}{F(0)}.$$

Idet $F(x)$ har rationale koefficienter (da $f(x)$ har det) er $F(\beta_1) + \cdots + F(\beta_m)$ som værdi for talsættet $\beta_1, \cdots, \beta_m$ af det symmetriske polynomium $U(x_1, \cdots, x_m) = F(x_1) + \cdots + F(x$ med rationale koefficienter et rationalt tal. Endvidere er ifølge det ovenstående $F(\beta_1) + \cdots + F(\beta_m)$ af formen p gange et helt algebraisk tal. Det pågældende hele algebraiske tal må altså være rationalt og er følgelig et sædvanligt helt tal. Altså er tallet $F(0) + F(\beta_1) + \cdots + F(\beta_m)$ et helt tal deleligt med p. Tallet $F(0)$ er ligeledes helt, men er ikke deleligt med p. Følgelig er tallet $Q = b_0 F(0) + F(\beta_1) + \cdots + F(\beta_m)$ et helt tal, der ikke er deleligt med p, hvis blot $p > b_0$. Da gælder naturligvis $Q \neq 0$ og følgelig $|Q| \geqslant 1$.

På den anden side gælder om $\varepsilon = R(\beta_1) + \cdots + R(\beta_m)$, at $|\varepsilon| \leqslant m A \frac{B^p}{(p-1)!}$. Da højre side går mod 0, når $p \to \infty$, findes et N, så at $|\varepsilon| < 1$, når blot $p > N$.

Ved at vælge $p > \max\{k, |h_m|, b_0, N\}$ ser vi, at $K \neq 0$.

Opgaver.

1. Find såvel ved Newtons som ved Lagranges interpolationsformel det polynomium af grad $\leqslant 3$, som for $x = -1, 0, 1, 3$ antager værdierne $y = 2, -1, 3, 1$.

2. Et polynomium $F(x) = a_0 + a_1 x + \cdots + a_n x^n$ vides at antage hele værdier for alle hele værdier af x. Vis, at polynomiets koefficienter er rationale, men ikke nødvendig vis hele tal. Vis, at tallene $n!a_0, n!a_1, \ldots, n!a_n$ er hele tal.

3. Vis, at for et vilkårligt polynomium $F(x) \in \dot{C}[x]$ af grad $n \geqslant 2$ ligger samtlige rødder for $F'(x)$ i den mindste konvekse mængde, der indeholder rødderne for $F(x)$. (Gauss.)

Vink. Hvis $\alpha_1, \ldots, \alpha_n$ er rødderne for $F(x)$, er

$$\frac{F'(x)}{F(x)} = \frac{1}{x-\alpha_1} + \cdots + \frac{1}{x-\alpha_n}.$$

Vis, at dette ikke kan være 0, når x er uden for den nævnte mængde.

4. Rødderne i polynomiet $F(x) = x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$ vides at være vinkelspidser i et parallelogram. Vis, at rødderne i polynomiet $F'(x)$ må ligge på en ret linie.

5. Bestem a og b således, at $x^2 + x + 1$ går op i $x^4 + 3x^3 + 5x^2 + ax + b$.

6. Find største fælles divisor for $x^4 - 3x^3 + 5x^2 + x - 4$ og $x^5 + 7x^4 - 8x^3 + 5x^2 - 4x - 1$.

7. Find største fælles divisor for $x^4 - 1$ og $x^6 - 1$.

8. Bestem a således, at polynomierne
$$x^3 - x^2 - 17x - 15 \quad \text{og} \quad x^3 - 7x - a$$
har en fælles rod.

9. Find de positive hele tal n, for hvilke polynomiet $(x+1)^{n+1} + x^{n+1} + 1$ har multiple rødder, og angiv disse samt deres multiplicitet.

10. Bestem for polynomiet
$$F(x) = x^6 - 3x^5 + 7x^4 - 9x^3 + 9x^2 - 5x + 2$$
faktoropløsningen $F = G_1 G_2^2 \dots G_m^m$, hvor G_q er produktet af de faktorer $x - \alpha_i$, der svarer til rødderne af multiplicitet q, og m er den højeste forekommende multiplicitet.

11. Vis, at hvis et polynomium med rationale koefficienter har en rod α med multiplicitet ν, medens alle andre rødder har en fra ν forskellig multiplicitet, er α rational.

12. Find rødderne i polynomiet
$$F(x) = \det \begin{pmatrix} a-x & c & b \\ c & b-x & a \\ b & a & c-x \end{pmatrix}.$$

13. Tallene $u_0 = 2$, $u_1 = 2\cos\theta$, $u_2, u_3, \dots$ tilfredsstiller relationen
$$u_n = u_1 u_{n-1} - u_{n-2}$$
for alle $n \geq 2$. Vis, at $u_n = 2\cos n\theta$.

Udtryk ved hjælp af den givne relation u_5 som et polynomium i u_1, og vis herved, at polynomiet
$$u_1^4 + u_1^3 - 4u_1^2 - 4u_1 + 1$$
har roden $2\cos\frac{\pi}{15}$. Find også polynomiets øvrige rødder.

14. Vis, at det for ethvert tallegeme $\mathcal{L}$ gælder, at et polynomium i $\mathcal{L}[x]$ af grad 3 er irreduktibelt i $\mathcal{L}[x]$, hvis og kun hvis ingen af dets rødder tilhører $\mathcal{L}$.

15. Opløs polynomiet $x^{2n} - (2\cos n\varphi)x^n + 1$, hvor $-1 < \cos n\varphi < 1$, i irreduktible polynomier i $\dot{R}[x]$. Samme opgave for $x^{2n} + 2x^n + 1$ og $x^{2n} - 2x^n + 1$.

16. Idet F er et polynomium i $\dot{R}[x]$, skal man vise, at $F(x) \geqslant 0$ for alle reelle x, hvis og kun hvis der findes to polynomier G og H i $\dot{R}[x]$, således at

$$F(x) = G(x)^2 + H(x)^2.$$

Vink. For reelle a og b er $a^2 + b^2 = (a+ib)(a-ib)$.

17. Idet F er et polynomium i $\dot{R}[x]$, skal man vise, at $F(x) \geqslant 0$ for alle reelle $x > 0$, hvis og kun hvis der findes polynomier G_1, H_1, G_2, H_2 i $\dot{R}[x]$, således at

$$F(x) = [G_1(x)^2 + H_1(x)^2] + x\,[G_2(x)^2 + H_2(x)^2].$$

18. Et polynomium $x^3 + a_1x^2 + a_2x + a_3$ med rationale koefficienter vides at have en rod $a+ib$, hvor a er reel og b er rational og $\neq 0$. Vis, at polynomiet har en rational rod.

19. Bestem de rationale rødder i polynomiet

$$x^5 + 2x^4 - 2x^3 + 2x^2 - 3x.$$

Find dernæst alle polynomiets rødder.

20. Vis, at hvis u er et reelt tal med den egenskab, at både $\cos u$ og $\frac{u}{\pi}$ er rationale, er $\cos u$ et af tallene $-1, -\frac{1}{2}, 0, \frac{1}{2}, 1$.

21. Afgør, om polynomiet

$$F(x) = 2x^7 - 3x^5 + 2x^4 - 3x^3 - x^2 + x + 4$$

er reduktibelt eller irreduktibelt i $\dot{Q}[x]$.

22. Afgør, om polynomiet $x^6 + x^3 + 1$ er reduktibelt eller irreduktibelt i $\dot{Q}[x]$.

23. Afgør, om polynomiet

$$7x^5 - 9x^4 + 8x^3 + 3x^2 - x + 2$$

er reduktibelt eller irreduktibelt i $\dot{Q}[x]$.

24. Afgør, om polynomiet $x^4 - x^3 - x^2 + 2x - 2$ er reduktibelt eller irreduktibelt i $\dot{Q}[x]$.

25. Bestem et sæt af rationale tal a, b, c, for hvilke polynomierne

$$x^5 + 3x^4 + 4x^3 + ax^2 + bx + c \quad \text{og} \quad x^3 + x + 1$$

har en fælles rod.

26. Vis, at et polynomium $F(x)$ af grad $\geqslant 2$ med hele koefficienter er irreduktibelt i $\dot{Q}[x]$, hvis der findes uendelig mange hele værdier af x, for hvilke $F(x)$ er et primtal.

27. Vis, at ethvert polynomium

$$(x - h_1) \cdots (x - h_n) - 1,$$

hvor $h_1, \ldots, h_n$ er indbyrdes forskellige hele tal, er irreduktibelt i $\dot{Q}[x]$.

28. Vis, at ethvert polynomium

$$(x - h_1)^2 \cdots (x - h_n)^2 + 1,$$

hvor $h_1, \ldots, h_n$ er indbyrdes forskellige hele tal, er irreduktibelt i $\dot{Q}[x]$.

29. Vis, at polynomiet $x^n - 105x + 12$ er irreduktibelt i $\mathbb{Q}[x]$ for ethvert $n \geq 2$.

30. Vis, at ethvert tal af formen $x = \xi + i\eta$, hvor ξ og η er rationale tal og $\eta \neq 0$, er algebraisk af grad 2. Vis, at et sådant tal er algebraisk helt, hvis og kun hvis ξ og η er hele tal.

31. Vis, at tallet $\sqrt{2} + \sqrt{3}$ er algebraisk af grad 4. Find dets karakteristiske polynomium og dets konjugerede tal.

32. Udtryk det symmetriske polynomium af fem variable
$$S(\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5) = \sum \alpha_{\nu_1}^2 \alpha_{\nu_2}^2 \alpha_{\nu_3}^2,$$
hvor der skal summeres over de $\binom{5}{3} = 10$ mulige kombinationer ν_1, ν_2, ν_3, ved hjælp af de elementarsymmetriske polynomier a_1, a_2, a_3, a_4, a_5 af $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5$.

33. Idet α, β, γ betegner rødderne i polynomiet $x^3 + ax^2 + bx + c$, skal man udtrykke
$$\alpha^3\beta^2 + \alpha^3\gamma^2 + \alpha^2\beta^3 + \alpha^2\gamma^3 + \beta^3\gamma^2 + \beta^2\gamma^3$$
ved hjælp af a, b, c.

34. Vis, at der for et givet n og et givet $R > 0$ kun findes et endeligt antal hele algebraiske tal af grad $\leq n$, som tillige med deres konjugerede tilhører cirkelskiven $\{x \mid |x| \leq R\}$.

35. Vis, at når tallene $\alpha_1, \ldots, \alpha_n$ er rødderne i et normeret polynomium med rationale, respektive hele, koefficienter, gælder det samme om tallene $\alpha_1^k, \ldots, \alpha_n^k$ for ethvert helt $k > 1$.

36. Vis, at hvis et helt algebraisk tal $\alpha \neq 0$ og alle dets konjugerede tilhører cirkelskiven $\{x \mid |x| \leqslant 1\}$, da er $|\alpha| = 1$, og α er endda en enheds-rod, d.v.s. rod i et polynomium $x^n - 1$, n hel $\geqslant 1$.

37. Lad $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ være rødderne i polynomiet $x^4 + px + q$. Opskriv det normerede polynomium af grad 4, hvis rødder er $\alpha_1^5, \alpha_2^5, \alpha_3^5, \alpha_4^5$.

38. Find diskriminanten for polynomiet $x^4 + ax + b$.

39. Bevis formlen

$$\det \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-1} \\ \cdots & & & \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{pmatrix} = \prod_{1 \leqslant j < i \leqslant n} (\alpha_i - \alpha_j).$$

40. Vis, at ethvert tal, der er rod i et normeret polynomium $x^n + \gamma_1 x^{n-1} + \cdots + \gamma_n$ med hele algebraiske koefficienter, er et helt algebraisk tal.

41. Et reelt algebraisk tal kaldes totalreelt, såfremt dets konjugerede også er reelle. 1) Nævn nogle totalreelle algebraiske tal og nogle reelle algebraiske tal, der ikke er totalreelle. 2) Vis, at de totalreelle algebraiske tal udgør et tallegeme. 3) Vis, at dette tallegeme indeholder $\sqrt{a^2 + b^2}$, når det indeholder a og b. 4) Nævn et totalreelt tal $q > 0$, for hvilket $\sqrt{q}$ ikke er totalreelt. — Mængden af punkter (x, y) og linier $ax + by + c = 0$ i den sædvanlige aritmetiske geometri med totalreelle koordinater x, y og koefficienter a, b, c bestemmer ifølge 2) og 3) en geometri, der opfylder Hilberts aksiomer I–V_1. I denne gælder ifølge 4) ikke, at enhver linie gennem et indre punkt af en cirkel skærer cirklen.

42. Vis, at ligningen $x^2+y^2+z^2 = xy+yz+zx$, hvor x,y,z er komplekse tal, udtrykker, at punkterne x,y,z er vinkelspidser i en ligesidet trekant (eller sammenfaldende).

43. Find rødderne i ligningen $y^3+3y-4=0$ ved Cardanos formel og på anden måde.

44. Find rødderne i ligningen $y^3-2y+1=0$ ved Cardanos formel og på anden måde.

45. Ligningen $x^3+ax^2+bx+c=0$ antages at have reelle koefficienter og kun en reel rod. Find en ligning mellem a,b,c, der udtrykker, at ligningens rødder ligger på en ret linie.

46. Vis, at det normerede tredjegradspolynomium, hvis rødder er kvadraterne på differenserne mellem rødderne i polynomiet x^3+px+q, er

$$x(x+3p)^2+4p^3+27q^2.$$

47. Find rødderne i ligningen

$$y^4-27y^2-14y+120=0.$$

48. En n^{te}-grads ligning $a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n=0$ antages at opfylde betingelserne $a_k=a_{n-k}$ for $k=0,\cdots,n$. Vis, at hvis $\alpha_1,\cdots,\alpha_n$ [som åbenbart alle er $\neq 0$] er ligningens rødder, er $\frac{1}{\alpha_1},\cdots,\frac{1}{\alpha_n}$ en permutation af $\alpha_1,\cdots,\alpha_n$.

49. Find rødderne i polynomiet

$$x(x+a)(x+b)(x+a+b)+c.$$

50. Vis, at et polynomium $x^n+a_1x^{n-1}+\cdots+a_n$ med $a_n\neq 0$, i hvilket to på hinanden følgende koefficienter a_i og a_{i+1} er 0, ikke kan have lutter reelle rødder.

51. Anvend Descartes', Fouriers og Sturms sætninger på polynomiet $F(x) = x^4 - 7x^2 + 6x - 1$.

52. Idet $V(x)$ for et polynomium $F(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ er antallet af fortegnsskifter i følgen $F(x), F'(x), \cdots, F^{(n)}(x)$ og $V^*(x)$ antallet af fortegnsskifter i følgen $F(x), -F'(x), F''(x), -F'''(x), \cdots, (-1)^n F^{(n)}(x)$, skal man vise, at $V(x-0) = n - V^*(x)$ for alle x. Vis herved, at antallet af rødder for F i et åbent interval $]\alpha, \beta[$ er højst lig med $n - V^*(\beta) - V(\alpha)$, og at forskellen er et lige tal.

53. Find antallet af reelle rødder i polynomiet $F(x) = x^3 + px + q$ for vilkårlige reelle p og q ved at diskutere monotoniintervallerne for $F(x)$.

54. Find antallet af reelle rødder i polynomiet $F(x) = x^3 + px + q$ for vilkårlige reelle p og q ved hjælp af Sturms sætning.

55. Idet Legendre-, Laguerre- og Hermite polynomierne af grad n defineres ved

$$P_n(x) = \frac{1}{2^n n!} \frac{d^n}{dx^n}(x^2-1)^n,$$

$$L_n(x) = \frac{1}{n!} e^x \frac{d^n}{dx^n}(e^{-x}x^n),$$

$$H_n(x) = \frac{1}{n!} e^{\frac{1}{2}x^2} \frac{d^n}{dx^n}(e^{-\frac{1}{2}x^2}),$$

skal man vise, at disse polynomier hver har n indbyrdes forskellige rødder, og at disse er beliggende henholdsvis i $]-1,1[$, $]0,+\infty[$ og $]-\infty,+\infty[$.

56. Vis, at hvis en tredjegradsligning med rationale koefficienter har en konstruerbar rod, er alle dens rødder konstruerbare, og mindst en af dem er rational.

57. Vis, at terningens fordobling, d.v.s. konstruktionen af $\sqrt[3]{2}$, ikke er mulig med passer og lineal.

58. Vis, at hvis en femtegradsligning med rationale koefficienter har tre konstruerbare rødder, er alle dens rødder konstruerbare, og mindst en af dem er rational.

59. Tilbagefør løsningen af ligningen $x^4+4x-2=0$ til løsningen af en tredjegradsligning. Vis herved, at der findes algebraiske tal, hvis grad er en potens af 2, og som ikke er konstruerbare. Find endelig ligningens rødder.

60. Vis, at to vilkårlige Fermat tal $F_h = 2^{2^h}+1$ og $F_k = 2^{2^k}+1$, $h \neq k$, er indbyrdes primiske.

61. Vis, at der for et ulige primtal af formen $p = 2^k+1$ findes 2^{k-1} primitive restklasser i $\dot{Z}_p$.

62. Find en konstruktion af den regulære 5-kant ved at følge den for 17-kanten anvendte metode.

63. Udtryk $x^3+\frac{1}{x^3}$ og $x^2+\frac{1}{x^2}$ ved hjælp af $z = x+\frac{1}{x}$. Find herved ud fra ligningen $\frac{x^7-1}{x-1} = x^6+x^5+x^4+x^3+x^2+x+1 = 0$ ved division med x^3 den ligning $z^3+a_1z^2+a_2z+a_3 = 0$, hvis rødder er $2\cos\frac{2\pi}{7}$, $2\cos\frac{4\pi}{7}$, $2\cos\frac{6\pi}{7}$, og bestem rødderne ved hjælp af Cardanos formel. Vis herved, at konstruktionen af den regulære 7-kant kan udføres ved passer og lineal i forbindelse med en vinkeltredeling.

Litteratur

O. Perron. Algebra I-II. 2. Aufl. Walter de Gruyter & Co, Berlin und Leipzig 1932-33.

F. Enriques. Fragen der Elementargeometrie II. 2. Aufl. B. G. Teubner, Leipzig · Berlin 1923.

F. Rudio. Archimedes, Huygens, Lambert, Legendre. Vier Abhandlungen über die Kreismessung. Deutsch herausgegeben und mit einer Übersicht über die Geschichte des Problemes von der Quadratur des Zirkels, von den ältesten Zeiten bis auf unsere Tage. B. G. Teubner, Leipzig 1892.

Rettelser

Side

10 l. 5 f.o. Disse : skal vere : Disse sidste

23 l. 14 f.o. hele : skal vere: hele

27 l. 6 f.n. Ethvert : skal vere: Ethvert

37 l. 5 f.o. $p_i \leqslant p_j$: skal vere: $p_i \geqslant p_j$

57 l. 14 f.n. $\cos\frac{\varphi}{3} + i\sin\frac{\varphi}{3}$: skal vere: $\cos\frac{\varphi}{3} \pm i\sin\frac{\varphi}{3}$

61 l. 7 og 9 f.o. $-3x^3$: skal vere: $-2x^3$

62 l. 5 f.o. hvis : skal vere: eftersom

64 Figuren. Bemærk, at punkterne $x_1, x_2, \ldots, x_N$ ikke nødvendig vis alle er diskontinuitetspunkter for $V(x)$.

95 l. 2 f.o. α_{16} : skal vere: α_6