

## MEMÓRIA SOBRE UMA CLASSE PARTICULAR DE EQUAÇÕES RESOLÚVEIS ALGEBRICAMENTE

*Niels Henrik Abel*

(1802–1829)

Tradução do artigo: *Mémoire sur une classe particulière d'équations résolubles algébriquement*, N.H. Abel, *Journal für die reine und angewandte Mathematik*, **4**, 131-156(1829).

Jason Gallas, <http://www.if.ufrgs.br/~jgallas> Instituto de Física, Universidade Federal do Rio Grande do Sul, 91501-970 Porto Alegre, Brasil.

Embora a resolução algébrica das equações não seja possível em geral, existem porém equações particulares de todos os graus que admitem uma tal solução<sup>1</sup>. Tais são, por exemplo as equações da forma  $x^n - 1 = 0$ . A resolução de tais equações fundamenta-se em certas relações que existem entre as raízes. Eu procurei generalizar essa observação supondo que duas raízes de uma dada equação estejam ligadas de tal modo entre si, que se possa exprimir racionalmente uma delas pela outra, e encontrei, que uma tal equação pode sempre ser resolvida com o auxílio de um certo número de equações *menos elevadas*. Existem mesmo casos onde se pode resolver *algebricamente* a própria equação dada. Isto ocorre, por exemplo, todas as vezes em que, sendo a equação dada irredutível, seu grau for um número primo. O mesmo acontece ainda se todas as raízes de uma equação puderem

---

<sup>1</sup>NT(*Nota do tradutor*): Esta primeira frase foi tirada da versão publicada na página 478 das *Oeuvres Complètes de Abel*, Tomo I, editada por L. Sylow e S. Lie, 1881. Tal frase difere daquela que aparece no *Journal für die reine und angewandte Mathematik*, **4**, 131-156(1829). Como mencionado por Sylow e Lie no prefácio do Tomo I, na versão publicada em seu *Journal*, Crelle "...fez várias correções do estilo em parte inúteis; existem mesmo algumas que modificaram o sentido [original]. Assim, as traduções alemãs de Crelle não podendo ser consideradas como versões absolutamente exatas do texto original, nós [Sylow e Lie] cremos, como Holmboe, dever apresentar estas *Memórias* em francês a fim de conservar a unidade linguística da nossa edição [das *Oeuvres Complètes*]. Tais *Oeuvres Complètes* foram re-impressas em 1992 e são comercializadas pelas *Éditions Jacques Gabay*, Sceaux, ISBN 2-87647-073-X.

ser expressas por<sup>2</sup>

$$x, \theta(x), \theta^2(x), \theta^3(x), \dots, \theta^{n-1}(x) \quad \text{onde [tem-se]} \quad \theta^n(x) = x,$$

sendo  $\theta(x)$  uma função racional de  $x$  e  $\theta^2(x), \theta^3(x), \dots$  funções da mesma forma de  $\theta(x)$ , tomadas duas vezes, três vezes, etc.

A equação  $(x^n - 1)/(x - 1) = 0$ , onde  $n$  é um número primo, está neste caso; pois designando-se por  $\alpha$  uma raiz primitiva para o módulo  $n$ , pode-se, como se sabe, exprimir as  $n - 1$  raízes por:

$$x, x^\alpha, x^{\alpha^2}, x^{\alpha^3}, \dots, x^{\alpha^{n-2}}, \quad \text{onde} \quad x^{\alpha^{n-1}} = x,$$

ou seja, fazendo-se  $x^\alpha = \theta(x)$ , por:

$$x, \theta(x), \theta^2(x), \theta^3(x), \dots, \theta^{n-2}(x), \quad \text{onde} \quad \theta^{n-1}(x) = x.$$

A mesma propriedade é satisfeita por uma certa classe de equações que nos oferece a teoria das funções elípticas.

Em geral, consegui demonstrar o teorema seguinte:

Se as raízes de uma equação de um grau qualquer estiverem ligadas entre si de sorte que *todas* as suas raízes possam ser expressas racionalmente através de uma delas, que designaremos por  $x$ , se mais ainda, [132] designando-se por  $\theta(x), \theta_1(x)$  duas outras quaisquer das raízes em questão, se tiver

$$\theta(\theta_1(x)) = \theta_1(\theta(x)),$$

então a equação em questão será sempre resolúvel algebricamente. Além disto, se supusermos a equação como irredutível e com seu grau expresso por

$$\alpha_1^{\nu_1} \alpha_2^{\nu_2} \dots \alpha_\omega^{\nu_\omega},$$

onde  $\alpha_1, \alpha_2, \dots, \alpha_\omega$  são números primos diferentes, poder-se-á reduzir a resolução desta equação à resolução de  $\nu_1$  equações do grau  $\alpha_1$ , de  $\nu_2$  equações de grau  $\alpha_2$ , de  $\nu_3$  equações de grau  $\alpha_3$ , etc.

---

<sup>2</sup>NT: Conforme era usual na época, Abel escreveu

$$x, \theta x, \theta^2 x, \theta^3 x, \dots, \theta^{n-1} x \quad \text{onde} \quad \theta^n x = x.$$

para indicar o que modernamente escreve-se assim:

$$x, \theta(x), \theta^2(x), \theta^3(x), \dots, \theta^{n-1}(x) \quad \text{onde} \quad \theta^n(x) = x.$$

Para facilitar a leitura, iremos usar sempre a notação moderna  $\theta(x)$  em vez de  $\theta x$ , etc.

Após haver apresentado esta teoria em geral, eu aplicá-la-ei às funções circulares e elípticas.

## §1.

Começaremos por considerar o caso no qual supõe-se que duas raízes duma equação irredutível<sup>3</sup> estejam ligadas de tal modo entre si, que uma possa ser expressa racionalmente pela outra.

Seja

$$\varphi(x) = 0 \quad (1)$$

uma equação do grau  $\mu$ , e  $x'$  e  $x_1$  as duas raízes que estão ligadas entre si pela equação

$$x' = \theta(x_1), \quad (2)$$

onde  $\theta(x)$  designa uma função racional de  $x$  e de quantidades conhecidas. A quantidade  $x'$  sendo uma das raízes da equação, ter-se-á  $\varphi(x') = 0$  e, em virtude da (2),

$$\varphi(\theta(x_1)) = 0. \quad (3)$$

Eu afirmo agora que esta equação será também satisfeita se, em vez de  $x_1$ , colocarmos uma outra raiz qualquer da equação proposta. Ter-se-á efetivamente o teorema seguinte<sup>4</sup>

---

<sup>3</sup>Uma equação  $\varphi(x) = 0$ , cujos coeficientes são funções racionais de um certo número de quantidades conhecidas  $a, b, c, \dots$  chama-se *irredutível*, quando for impossível se expressar suas raízes por uma equação de grau menor, cujos coeficientes sejam igualmente funções racionais de  $a, b, c, \dots$ .

<sup>4</sup>Este teorema demonstra-se facilmente como segue:

Qualquer que seja a função racional  $f(x)$ , pode-se sempre fazer  $f(x) = M/N$ , onde  $M$  e  $N$  são funções inteiras de  $x$ , que não possuem fator comum; porém uma função de  $x$  pode sempre ser colocada sob a forma  $P + Q\varphi(x)$ , onde  $P$  e  $Q$  são funções inteiras, tais, que o grau de  $P$  seja menor que o grau da função  $\varphi(x)$ . Portanto, fazendo-se  $M = P + Q\varphi(x)$ , ter-se-á  $f(x) = (P + Q\varphi(x))/N$ . Isto posto, seja  $x$  a raiz de  $\varphi(x) = 0$  que satisfaz simultaneamente a  $f(x) = 0$ ;  $x_1$  será igualmente uma raiz da equação  $P = 0$ . Mas, se  $P$  não for zero para um valor qualquer de  $x$ , esta equação fornecerá  $x$  como raiz de uma equação de um grau menor que o de  $\varphi(x) = 0$ ; o que contradiz a hipótese; portanto  $P = 0$  e por conseqüência  $f(x) = \varphi(x) Q/N$ , donde se vê que  $f(x)$  será igual a zero quando  $\varphi(x)$  o for, q.e.d.

[133] **Teorema I.** Se uma das raízes de uma equação irredutível  $\varphi(x) = 0$  satisfaz a uma outra equação  $f(x) = 0$ , onde  $f(x)$  designa uma função racional de  $x$  e de quantidades conhecidas que se supõe contidas em  $\varphi(x)$ , esta última equação irá ser também satisfeita ao nela substituir-se  $x$  por uma raiz qualquer da equação  $\varphi(x) = 0$ ; mas o termo  $\varphi(\theta(x_1))$  na equação (3) é uma função racional da variável, portanto ter-se-á

$$\varphi(\theta(x)) = 0, \quad \text{se} \quad \varphi(x) = 0, \quad (4)$$

ou seja, se  $x$  é uma raiz da equação  $\varphi(x) = 0$ , a quantidade  $\theta(x)$  também o será.

Agora, em virtude do que precede,  $\theta(x_1)$  é uma raiz da equação  $\varphi(x) = 0$ , portanto  $\theta(\theta(x_1))$  o será também; igualmente  $\theta(\theta(\theta(x_1)))$ , etc ... o serão, ao repetir-se a operação denotada por  $\theta$  um número qualquer de vezes.

Seja, para abreviar,

$$\theta(\theta(x_1)) = \theta^2(x_1), \quad \theta(\theta^2(x_1)) = \theta^3(x_1), \quad \theta(\theta^3(x_1)) = \theta^4(x_1), \quad \text{etc,}$$

ter-se-á a série

$$x_1, \quad \theta(x_1), \quad \theta^2(x_1), \quad \theta^3(x_1), \quad \theta^4(x_1), \quad \dots \quad (5)$$

sendo todas estas quantidades raízes da equação  $\varphi(x) = 0$ . A série (5) terá uma infinidade de termos, mas a equação  $\varphi(x) = 0$  não tendo mais do que um número finito de raízes diferentes, faz-se necessário que várias quantidades da série (5) sejam iguais entre si.

Suponhamos pois, por exemplo,

$$\theta^m(x_1) = \theta^{m+n}(x_1),$$

ou ainda

$$\theta^n(\theta^m(x_1)) - \theta^m(x_1) = 0, \quad (6)$$

observando-se que  $\theta^{n+m}(x_1) = \theta^n(\theta^m(x_1))$ .

O membro à direita da equação (6) é uma função racional de  $\theta^m(x_1)$ ; mas esta quantidade é uma raiz da equação  $\varphi(x) = 0$ , portanto em virtude do teorema enunciado mais ao alto, poder-se-á colocar  $x_1$  no lugar de  $\theta^m(x_1)$ .

[134] Isto dá

$$\theta^n(x_1) = x_1, \quad (7)$$

onde se pode supor que  $n$  tenha o menor valor possível, de sorte que todas as quantidades

$$x_1, \theta(x_1), \theta^2(x_1), \dots, \theta^{n-1}(x_1) \quad (8)$$

sejam diferentes entre si.

A equação (7) fornecerá

$$\theta^k(\theta^n(x_1)) = \theta^k(x_1), \quad \text{ou seja} \quad \theta^{n+k}(x_1) = \theta^k(x_1).$$

Esta fórmula faz ver que a partir do termo  $\theta^{n-1}(x_1)$ , os termos da série (8) se reproduzirão na mesma ordem. As  $n$  quantidades (8) serão portanto as únicas da série (5) diferentes entre si.

Isto posto, se  $\mu > n$ , seja  $x_2$  uma outra raiz da equação proposta, que não esteja contida na série (8); segue do teorema I que todas as quantidades

$$x_2, \theta(x_2), \theta^2(x_2), \dots, \theta^{n-1}(x_2), \dots \quad (9)$$

serão igualmente raízes da equação proposta. Eu afirmo agora que esta série não conterà mais que  $n$  quantidades diferentes entre si e das quantidades (8). De fato, tendo-se  $\theta^n(x_1) - x_1 = 0$ , ter-se-á, em virtude do teorema I,  $\theta^n(x_2) = x_2$  e, conseqüentemente,

$$\theta^{n+k}(x_2) = \theta^k(x_2).$$

Portanto as únicas quantidades da série (9) que poderão ser diferentes entre si serão as  $n$  primeiras

$$x_2, \theta(x_2), \theta^2(x_2), \dots, \theta^{n-1}(x_2). \quad (10)$$

Estas aqui serão necessariamente diferentes entre si e entre as quantidades (8). De fato, se se tiver

$$\theta^m(x_2) = \theta^\nu(x_2),$$

onde  $m$  e  $\nu$  são menores que  $n$ , resultará  $\theta^m(x_1) = \theta^\nu(x_1)$ , o que é impossível, pois todas as quantidades (8) são diferentes entre si. Se, ao contrário, tivéssemos

$$\theta^m(x_2) = \theta^\nu(x_1),$$

resultaria

$$\theta^{n-m}(\theta^\nu(x_1)) = \theta^{n-m}(\theta^m(x_2)) = \theta^{n-m+m}(x_2) = \theta^n(x_2) = x_2,$$



## §2.

Consideremos um qualquer dos grupos em (12), por exemplo o primeiro, e façamos

$$\begin{aligned} (x - x_1)(x - \theta(x_1))(x - \theta^2(x_1)) \cdots (x - \theta^{n-1}(x_1)) = \\ = x^n + A_1' x^{n-1} + A_1'' x^{n-2} + \cdots + A_1^{(n-1)} x + A_1^{(n)}; \end{aligned} \quad (14)$$

as raízes desta equação serão

$$x_1, \theta(x_1), \theta^2(x_1), \dots, \theta^{n-1}(x_1),$$

e os coeficientes  $A_1', A_1'', \dots, A_1^{(n)}$  serão funções racionais e [136] simétricas destas quantidades. Veremos que se pode fazer tais coeficientes dependerem da resolução duma única equação do grau  $m$ .

Para mostrá-lo, consideremos em geral uma função racional e simétrica qualquer de  $x_1, \theta(x_1), \theta^2(x_1), \dots, \theta^{n-1}(x_1)$ , e seja

$$y_1 = f(x_1, \theta(x_1), \theta^2(x_1), \dots, \theta^{n-1}(x_1)) \quad (15)$$

tal função.

Colocando-se no lugar de  $x_1$  sucessivamente  $x_2, x_3, \dots, x_m$ , a função  $y_1$  assumirá diferentes valores, que designaremos por  $y_1, y_2, y_3, \dots, y_m$ . Isto posto, se se forma uma equação do grau  $m$ :

$$y^m + p_1 y^{m-1} + p_2 y^{m-2} + \cdots + p_{m-1} y + p_m = 0, \quad (16)$$

cujas raízes são  $y_1, y_2, y_3, \dots, y_m$ , eu afirmo que os coeficientes dessa equação poderão ser expressos racionalmente pelas quantidades conhecidas, que se supõe dados pela equação proposta.

Como as quantidades  $x_1, \theta(x_1), \theta^2(x_1), \dots, \theta^{n-1}(x_1)$  são funções racionais de  $x_1$ , a função  $y_1$  também o será. Seja

$$\begin{cases} y_1 = F(x_1), \\ \text{então teremos também} \\ y_2 = F(x_2); \quad y_3 = F(x_3); \quad \cdots; \quad y_m = F(x_m). \end{cases} \quad (17)$$

Colocando na (15) sucessivamente  $\theta(x_1), \theta^2(x_1), \theta^3(x_1), \dots, \theta^{n-1}(x_1)$  no lugar de  $x_1$  e observando que  $\theta^n(x_1) = x_1$ ;  $\theta^{n+1}(x_1) = \theta(x_1)$ ;  $\theta^{n+2}(x_1) = \theta^2(x_1)$ ; etc., fica claro que a função  $y_1$  não mudará de valor; ter-se-á portanto

$$y_1 = F(x_1) = F(\theta(x_1)) = F(\theta^2(x_1)) = \cdots = F(\theta^{n-1}(x_1))$$

e, igualmente,

$$\begin{aligned} y_2 &= F(x_2) = F(\theta(x_2)) = F(\theta^2(x_2)) = \cdots = F(\theta^{n-1}(x_2)), \\ &\vdots \\ y_m &= F(x_m) = F(\theta(x_m)) = F(\theta^2(x_m)) = \cdots = F(\theta^{n-1}(x_m)). \end{aligned}$$

Elevando cada membro destas equações à  $\nu$ -ésima potência, obtém-se<sup>5</sup>

$$\begin{cases} y_1^\nu = \frac{1}{n} \left\{ (F(x_1))^\nu + (F(\theta(x_1)))^\nu + \cdots + (F(\theta^{n-1}(x_1)))^\nu \right\}, \\ y_2^\nu = \frac{1}{n} \left\{ (F(x_2))^\nu + (F(\theta(x_2)))^\nu + \cdots + (F(\theta^{n-1}(x_2)))^\nu \right\}, \\ \vdots \\ y_m^\nu = \frac{1}{n} \left\{ (F(x_m))^\nu + (F(\theta(x_m)))^\nu + \cdots + (F(\theta^{n-1}(x_m)))^\nu \right\}. \end{cases} \quad (18)$$

Adicionando-se estas últimas equações tem-se o valor de

$$y_1^\nu + y_2^\nu + y_3^\nu + \cdots + y_m^\nu$$

[137] expresso como função *racional* e *simétrica* de todas as raízes da equação  $\varphi(x) = 0$ , a saber

$$y_1^\nu + y_2^\nu + y_3^\nu + \cdots + y_m^\nu = \frac{1}{n} \sum (F(x))^\nu. \quad (19)$$

O termo à direita desta equação pode ser expresso racionalmente através dos coeficientes de  $\varphi(x)$  e  $\theta(x)$ , i.e., através de quantidades conhecidas. Portanto, definindo-se

$$r_\nu = y_1^\nu + y_2^\nu + y_3^\nu + \cdots + y_m^\nu, \quad (20)$$

ter-se-á o valor de  $r_\nu$  para um valor qualquer inteiro de  $\nu$ . Conhecendo-se  $r_1, r_2, \dots, r_m$ , poder-se-á obter racionalmente o valor de qualquer função simétrica das quantidades  $y_1, y_2, \dots, y_m$ . Poder-se-á, portanto, encontrar desta maneira todos os coeficientes da equação (16) e, em consequência, determinar toda função racional e simétrica de  $x_1, \theta(x_1), \theta^2(x_1), \dots, \theta^{n-1}(x_1)$ , com o auxílio duma equação do grau  $m$ -ésimo. Deste modo ter-se-á, portanto, os coeficientes da equação (14), cuja resolução fornecerá o valor de  $x_1$ , etc.

---

<sup>5</sup>NT: Não existe nenhuma equação com número "18" no artigo que foi publicado no *Journal für die reine und angewandte Mathematik*, 4, 131-156(1829). A equação (18) aparece, entretanto, na versão publicada nos *Oeuvres Complètes de Abel*, Tomo I, página 484.



Vê-se, deste modo, que se pode reduzir a resolução da equação  $\varphi(x) = 0$ , de grau  $\mu = m \cdot n$ , à resolução duma certa quantidade de equações de grau  $m$  e  $n$ . É suficiente mesmo, como iremos ver, resolver-se uma única equação de grau  $m$  e  $m$  equações de grau  $n$ .

Seja  $\psi(x_1)$  um qualquer dos coeficientes  $A'_1, A''_1, \dots, A_1^{(n)}$  e façamos

$$t_\nu = y_1^\nu \psi(x_1) + y_2^\nu \psi(x_2) + y_3^\nu \psi(x_3) + \dots + y_m^\nu \psi(x_m). \quad (21)$$

Como  $y_1^\nu \psi(x_1)$  é uma função simétrica das quantidades  $x_1, \theta(x_1), \dots, \theta^{n-1}(x_1)$ , ter-se-á, observando-se que  $\theta^n(x_1) = x_1, \theta^{n+1}(x_1) = \theta(x_1)$ , etc.

$$\begin{aligned} y_1^\nu \psi(x_1) &= \left(F(x_1)\right)^\nu \psi(x_1) = \left(F(\theta(x_1))\right)^\nu \psi(\theta(x_1)) = \dots \\ &= \left(F(\theta^{n-1}(x_1))\right)^\nu \psi(\theta^{n-1}(x_1)), \end{aligned}$$

ou seja,

$$\begin{aligned} y_1^\nu \psi(x_1) &= \frac{1}{n} \left\{ \left(F(x_1)\right)^\nu \psi(x_1) + \left(F(\theta(x_1))\right)^\nu \psi(\theta(x_1)) + \dots \right. \\ &\quad \left. + \left(F(\theta^{n-1}(x_1))\right)^\nu \psi(\theta^{n-1}(x_1)) \right\}. \end{aligned}$$

Expressões semelhantes para  $y_2^\nu \psi(x_2), y_3^\nu \psi(x_3), \dots, y_m^\nu \psi(x_m)$  serão encontradas ao colocar-se  $x_2, x_3, \dots, x_m$  no lugar de  $x_1$ . Em substituindo-se estes valores, vê-se que  $t_\nu$  tornar-se-á uma função *racional* e *simétrica* de todas as raízes da equação  $\varphi(x) = 0$ . De fato, ter-se-á

$$t_\nu = \frac{1}{n} \sum \left(F(x)\right)^\nu \psi(x). \quad (22)$$

Portanto, pode-se exprimir  $t_\nu$  racionalmente através de quantidades conhecidas.

Isto posto, fazendo-se  $\nu = 0, 1, 2, 3, \dots, m-1$ , a fórmula (21) dará [138]

$$\begin{aligned} \psi(x_1) + \psi(x_2) + \dots + \psi(x_m) &= t_0, \\ y_1 \psi(x_1) + y_2 \psi(x_2) + \dots + y_m \psi(x_m) &= t_1, \\ y_1^2 \psi(x_1) + y_2^2 \psi(x_2) + \dots + y_m^2 \psi(x_m) &= t_2, \\ &\vdots \\ y_1^{m-1} \psi(x_1) + y_2^{m-1} \psi(x_2) + \dots + y_m^{m-1} \psi(x_m) &= t_{m-1}. \end{aligned}$$

Destas equações, lineares em relação a  $\psi(x_1), \psi(x_2), \dots, \psi(x_m)$ , tira-se facilmente os valores destas quantidades como funções racionais de  $y_1, y_2, y_3, \dots, y_m$ .

De fato, fazendo-se

$$(y - y_2)(y - y_3) \dots (y - y_m) = y^{m-1} + R_{m-2}y^{m-2} + R_{m-3}y^{m-3} + \dots + R_1 y + R_0, \quad (23)$$

ter-se-á

$$\psi(x_1) = \frac{t_0 R_0 + t_1 R_1 + t_2 R_2 + \dots + t_{m-2} R_{m-2} + t_{m-1}}{R_0 + R_1 y_1 + R_2 y_1^2 + \dots + R_{m-2} y_1^{m-2} + y_1^{m-1}}. \quad (24)$$

As quantidades  $R_0, R_1, \dots, R_{m-2}$  são funções racionais de  $y_2, y_3, y_4 \dots, y_m$ , mas se pode exprimi-las em função de  $y_1$  somente. De fato, multiplicando-se (23) por  $y - y_1$ , ter-se-á:

$$\begin{aligned} (y - y_1)(y - y_2) \dots (y - y_m) &= \\ &= y^m + p_1 y^{m-1} + p_2 y^{m-2} \dots + p_{m-1} y + p_m \\ &= y^m + (R_{m-2} - y_1) y^{m-1} + (R_{m-3} - y_1 R_{m-2}) y^{m-2} + \dots \end{aligned}$$

donde se tirará, ao comparar-se as potências iguais de  $y$ :

$$\begin{cases} R_{m-2} = y_1 + p_1, \\ R_{m-3} = y_1 R_{m-2} + p_2 = y_1^2 + p_1 y_1 + p_2, \\ R_{m-4} = y_1 R_{m-3} + p_3 = y_1^3 + p_1 y_1^2 + p_2 y_1 + p_3 \\ \vdots \\ R_0 = y_1^{m-1} + p_1 y_1^{m-2} + p_2 y_1^{m-3} + \dots + p_{m-1}. \end{cases} \quad (25)$$

Substituindo-se estes valores, a expressão de  $\psi(x_1)$  tornar-se-á uma função racional de  $y_1$  e de quantidades conhecidas, e vê-se que é sempre possível encontrar  $\psi(x_1)$  desta maneira, sob a condição que o denominador

$$R_0 + R_1 y_1 + R_2 y_1^2 + \dots + R_{m-2} y_1^{m-2} + y_1^{m-1}$$

não seja zero. Se pode dar à função  $y_1$  uma infinidade de formas que tornarão impossível esta equação, por exemplo, em se fazendo

$$y_1 = (\alpha - x_1)(\alpha - \theta(x_1))(\alpha - \theta^2(x_1)) \dots (\alpha - \theta^{n-1}(x_1)), \quad (26)$$

onde  $\alpha$  é indeterminado, o denominador em questão não pode anular-se. De fato, sendo este denominador a mesma coisa que

$$(y_1 - y_2)(y_1 - y_3) \dots (y_1 - y_m),$$

[139] teríamos

$$y_1 = y_k$$

se ele fosse nulo, ou seja,

$$(\alpha - x_1)(\alpha - \theta(x_1)) \dots (\alpha - \theta^{n-1}(x_1)) = (\alpha - x_k)(\alpha - \theta(x_k)) \dots (\alpha - \theta^{n-1}(x_k)),$$

o que é impossível, pois todas as raízes  $x_1, \theta(x_1), \theta^2(x_1), \dots, \theta^{n-1}(x_1)$ , são diferentes das raízes  $x_k, \theta(x_k), \theta^2(x_k), \dots, \theta^{n-1}(x_k)$ .

Os coeficientes  $A'_1, A''_1, \dots, A_1^{(n)}$  podem portanto ser expressos racionalmente por uma mesma função  $y_1$ , cuja expressão depende duma equação de grau  $m$ .

As raízes da equação (14) são

$$x_1, \theta(x_1), \theta^2(x_1), \dots, \theta^{n-1}(x_1).$$

Substituindo-se  $y_1$  nos coeficientes  $A'_1, A''_1$ , etc. por  $y_2, y_3, \dots, y_m$ , se obtém outras  $m - 1$  equações, cujas raízes serão respectivamente:

$$\begin{array}{cccc} x_2, & \theta(x_2), & \dots, & \theta^{n-1}(x_2), \\ x_3, & \theta(x_3), & \dots, & \theta^{n-1}(x_3), \\ & & \vdots & \\ x_m, & \theta(x_m), & \dots, & \theta^{n-1}(x_m). \end{array}$$

**Teorema II.** A equação proposta  $\varphi(x) = 0$  pode portanto ser decomposta numa quantidade  $m$  de equações do grau  $n$ ; portanto os coeficientes destas equações são funções racionais duma mesma raiz de uma única equação do grau  $m$ .

Em geral, esta última equação não é resolúvel algebricamente quando seu grau é maior do que quatro, mas a equação (14) e as outras semelhantes o são sempre, supondo-se conhecidos os coeficientes  $A'_1, A''_1$ , etc., como veremos no parágrafo seguinte.

### §3.

No parágrafo precedente consideramos o caso no qual  $m$  é maior que a unidade. Agora iremos nos ocupar do caso  $m = 1$ .

Neste caso temos  $\mu = n$ , e as raízes da equação  $\varphi(x) = 0$  serão

$$x_1, \quad \theta(x_1), \quad \theta^2(x_1), \quad \dots, \quad \theta^{n-1}(x_1); \quad (27)$$

eu afirmo agora que toda equação cujas raízes possam ser expressas deste modo é resolúvel algebricamente.

[140] Seja  $\alpha$  uma raiz qualquer da equação  $\alpha^\mu - 1 = 0$ , e façamos

$$\psi(x) = (x + \alpha\theta(x) + \alpha^2\theta^2(x) + \alpha^3\theta^3(x) + \dots + \alpha^{\mu-1}\theta^{\mu-1}(x))^\mu; \quad (28)$$

então  $\psi(x)$  será uma função racional de  $x$ . Essa função pode ser expressa racionalmente através dos coeficientes de  $\varphi(x)$  e  $\theta(x)$ .

Substituindo-se  $\theta^m(x)$  no lugar de  $x$ , tem-se

$$\begin{aligned} \psi(\theta^m(x)) = & (\theta^m(x) + \alpha\theta^{m+1}(x) + \alpha^2\theta^{m+2}(x) + \dots \\ & + \alpha^{\mu-m}\theta^\mu(x) + \alpha^{\mu-m+1}\theta^{\mu+1}(x) + \dots + \alpha^{\mu-1}\theta^{\mu+m-1}(x))^\mu; \end{aligned}$$

entretanto, tem-se,

$$\theta^\mu(x) = x, \quad \theta^{\mu+1}(x) = \theta(x), \quad \dots, \quad \theta^{\mu+m-1}(x) = \theta^{m-1}(x),$$

donde:

$$\begin{aligned} \psi(\theta^m(x)) = & (\alpha^{\mu-m}(x) + \alpha^{\mu-m+1}(x) + \dots + \alpha^{\mu-1}\theta^{m-1}(x) + \theta^m(x) + \\ & + \alpha\theta^{m+1}(x) + \dots + \alpha^{\mu-m-1}\theta^{m-1}(x))^\mu. \end{aligned}$$

Porém, como  $\alpha^\mu = 1$ , temos

$$\begin{aligned} \psi(\theta^m(x)) = & [\alpha^{\mu-m}(x + \alpha\theta(x) + \alpha^2\theta^2(x) + \dots + \alpha^{\mu-1}\theta^{\mu-1}(x))]^\mu \\ = & \alpha^{\mu(\mu-m)}(x + \alpha\theta(x) + \dots + \alpha^{\mu-1}\theta^{\mu-1}(x))^\mu, \end{aligned}$$

e, como

$$\alpha^{\mu(\mu-m)} = 1,$$

vê-se que

$$\psi(\theta^m(x)) = \psi(x).$$

Fazendo-se  $m = 1, 2, 3, \dots, \mu - 1$ , e somando-se as expressões assim obtidas, encontrar-se-á:

$$\psi(x) = \frac{1}{n} \left\{ \psi(x) + \psi(\theta(x)) + \psi(\theta^2(x)) + \dots + \psi(\theta^{\mu-1}(x)) \right\}. \quad (29)$$

$\psi(x)$  é portanto uma função racional e simétrica de todas as raízes da equação  $\varphi(x) = 0$  e, por conseqüência, se poderá exprimi-la racionalmente através de quantidades conhecidas.

Sendo  $\psi(x) = \nu$ , tira-se da equação (28):

$$\sqrt[\mu]{\nu} = x + \alpha\theta(x) + \alpha^2\theta^2(x) + \dots + \alpha^{\mu-1}\theta^{\mu-1}(x). \quad (30)$$

Isto posto, designemos as  $\mu$  raízes da equação

$$\alpha^\mu - 1 = 0$$

por

$$1, \quad \alpha_1, \quad \alpha_2, \quad \alpha_3, \quad \dots, \quad \alpha_{\mu-1}, \quad (31)$$

e os valores correspondentes de  $\nu$  através de

$$\nu_0, \quad \nu_1, \quad \nu_2, \quad \nu_3, \quad \dots, \quad \nu_{\mu-1}; \quad (32)$$

a equação (30) dará, colocando-se no lugar de  $\alpha$  sucessivamente  $1, \alpha_1, \alpha_2, \dots, \alpha_{\mu-1}$ :

[141]

$$\left\{ \begin{array}{l} \sqrt[\mu]{\nu_0} = x + \theta(x) + \theta^2(x) + \dots + \theta^{\mu-1}(x), \\ \sqrt[\mu]{\nu_1} = x + \alpha_1\theta(x) + \alpha_1^2\theta^2(x) + \dots + \alpha_1^{\mu-1}\theta^{\mu-1}(x), \\ \sqrt[\mu]{\nu_2} = x + \alpha_2\theta(x) + \alpha_2^2\theta^2(x) + \dots + \alpha_2^{\mu-1}\theta^{\mu-1}(x), \\ \vdots \\ \sqrt[\mu]{\nu_{\mu-1}} = x + \alpha_{\mu-1}\theta(x) + \alpha_{\mu-1}^2\theta^2(x) + \dots + \alpha_{\mu-1}^{\mu-1}\theta^{\mu-1}(x). \end{array} \right. \quad (33)$$

Somando-se estas equações ter-se-á:

$$x = \frac{1}{\mu} \left\{ -A + \sqrt[\mu]{\nu_1} + \sqrt[\mu]{\nu_2} + \sqrt[\mu]{\nu_3} + \dots + \sqrt[\mu]{\nu_{\mu-1}} \right\}, \quad (34)$$

onde  $A$  expressa a quantidade racional  $\sqrt[\mu]{\nu_0}$ .

Deste modo, conhece-se a raiz  $x$ . Em geral, encontra-se a raiz  $\theta^m(x)$  multiplicando-se a primeira das equações (33) por  $1$ , a segunda por  $\alpha_1^{-m}$ , a terceira por  $\alpha_2^{-m}$ , etc., e somando-se; isso resulta em

$$\theta^m(x) = \frac{1}{\mu} \left\{ -A + \alpha_1^{-m} \sqrt[\mu]{\nu_1} + \alpha_2^{-m} \sqrt[\mu]{\nu_2} + \dots + \alpha_{\mu-1}^{-m} \sqrt[\mu]{\nu_{\mu-1}} \right\}. \quad (35)$$

Dando-se a  $m$  os valores  $0, 1, 2, \dots, \mu - 1$ , obtém-se os valores de todas as raízes da equação.

A expressão precedente das raízes contém, geralmente, uma quantidade  $\mu - 1$  de radicais diferentes, da forma  $\sqrt[\mu]{v}$ . Ela terá, portanto, uma quantidade  $\mu^{\mu-1}$  de valores, enquanto que a equação  $\varphi(x) = 0$  não possui mais que  $\mu$  raízes. Mas se pode dar à expressão das raízes uma outra forma, não exposta a esta dificuldade. De fato, quando o valor de  $\sqrt[\mu]{v_1}$  é fixado, o valor dos outros radicais o será também, como iremos ver agora.

Qualquer que seja o número  $\mu$ , primo ou não, se pode sempre encontrar uma raiz  $\alpha$  da equação  $\alpha^\mu - 1 = 0$ , tal que as raízes

$$\alpha_1, \quad \alpha_2, \quad \alpha_3, \quad \dots, \quad \alpha_{\mu-1}$$

possam ser representadas por

$$\alpha, \quad \alpha^2, \quad \alpha^3, \quad \dots, \quad \alpha^\mu. \quad (36)$$

Isto posto, tem-se

$$\begin{cases} \sqrt[\mu]{v_k} = x + \alpha^k \theta(x) + \alpha^{2k} \theta^2(x) + \dots + \alpha^{(\mu-1)k} \theta^{\mu-1}(x), \\ \sqrt[\mu]{v_1} = x + \alpha \theta(x) + \alpha^2 \theta^2(x) + \dots + \alpha^{\mu-1} \theta^{\mu-1}(x), \end{cases} \quad (37)$$

donde se tira

$$\begin{cases} \sqrt[\mu]{v_k} \sqrt[\mu-k]{v_1} = \left( x + \alpha^k \theta(x) + \alpha^{2k} \theta^2(x) + \dots + \alpha^{(\mu-1)k} \theta^{\mu-1}(x) \right) \times \\ \left( x + \alpha \theta(x) + \alpha^2 \theta^2(x) + \dots + \alpha^{\mu-1} \theta^{\mu-1}(x) \right)^{\mu-k}. \end{cases} \quad (38)$$

[142] O lado direito desta equação é uma função racional de  $x$ , que não mudará de valor ao colocar-se no lugar de  $x$  uma outra raiz qualquer  $\theta^m(x)$ , como se verá facilmente, fazendo-se esta substituição e levando em conta a equação  $\theta^{\mu+\nu}(x) = \theta^\nu(x)$ . Designando-se portanto a função em questão por  $\psi(x)$ , ter-se-á:

$$\sqrt[\mu]{v_k} \sqrt[\mu-k]{v_1} = \psi(x) = \psi(\theta(x)) = \psi(\theta^2(x)) = \dots = \psi(\theta^{\mu-1}(x)),$$

e dela:

$$\sqrt[\mu]{v_k} \left( \sqrt[\mu]{v_1} \right)^{\mu-k} = \frac{1}{\mu} \left\{ \psi(x) + \psi(\theta(x)) + \psi(\theta^2(x)) + \dots + \psi(\theta^{\mu-k}(x)) \right\}. \quad (39)$$

A expressão à direita nesta equação é uma função racional e simétrica das raízes, que podemos expressar através de grandezas conhecidas. Designando-a por  $a_k$ , temos:

$$\sqrt[\mu]{\nu_k} \sqrt[\mu-k]{\nu_1} = a_k \quad (40)$$

e dela:

$$\sqrt[\mu]{\nu_k} = \frac{a_k}{\nu_1} (\sqrt[\mu]{\nu_1})^k. \quad (41)$$

Com auxílio desta fórmula a expressão da raiz  $x$  tornar-se-á:

$$x = \frac{1}{\mu} \left\{ -A + \sqrt[\mu]{\nu_1} + \frac{a_2}{\nu_1} (\sqrt[\mu]{\nu_1})^2 + \frac{a_3}{\nu_1} (\sqrt[\mu]{\nu_1})^3 + \dots + \frac{a_{\mu-1}}{\nu_1} (\sqrt[\mu]{\nu_1})^{\mu-1} \right\}. \quad (42)$$

Esta expressão de  $x$  não possui mais que  $\mu$  valores distintos, que serão obtidos ao colocar-se no lugar de  $\sqrt[\mu]{\nu_1}$  os  $\mu$  valores

$$\sqrt[\mu]{\nu_1}, \quad \alpha \sqrt[\mu]{\nu_1}, \quad \alpha^2 \sqrt[\mu]{\nu_1}, \quad \dots, \quad \alpha^{\mu-1} \sqrt[\mu]{\nu_1}.$$

O método que seguimos acima para a resolução da equação  $\varphi(x) = 0$  é, no fundo, o mesmo que o senhor Gauss usou no seu “*Disquisitiones arithmeticae*, pag. 645 e seguintes” para resolver uma certa classe de equações, às quais ele foi conduzido nas suas pesquisas sobre a equação  $x^n - 1 = 0$ . Estas equações têm a mesma propriedade que nossa equação  $\varphi(x) = 0$ , a saber, que todas as suas raízes podem ser representadas sob a forma:

$$x, \quad \theta(x), \quad \theta^2(x), \quad \dots, \quad \theta^{\mu-1}(x),$$

$\theta(x)$  sendo uma função racional.

Em virtude daquilo que precede, podemos enunciar o teorema seguinte:

**Teorema III.** Se as raízes duma equação algébrica puderem ser representadas por

$$x, \quad \theta(x), \quad \theta^2(x), \quad \dots, \quad \theta^{\mu-1}(x),$$

[143] onde  $\theta^\mu(x) = x$  e  $\theta(x)$  designa uma função racional de  $x$  e de quantidades conhecidas, tal equação será sempre resolúvel algebricamente.

Tira-se o seguinte, como corolário:

**Teorema IV.** Se duas raízes duma equação *irredutível*, cujo grau é um número *primo*, estiverem relacionadas de um modo tal, que se possa expressar uma *racionalmente* pela outra, essa equação será resolúvel algebricamente.

De fato, tal segue imediatamente da equação (11)

$$\mu = m \cdot n,$$

onde se deve ter  $m = 1$ , se  $\mu$  é um número primo, e por conseqüência as raízes se exprimem através de  $x, \theta(x), \theta^2(x), \dots, \theta^{\mu-1}(x)$ .

No caso em que todas as quantidades conhecidas de  $\varphi(x)$  e  $\theta(x)$  são *reais*, as raízes da equação  $\varphi(x)$  gozam de uma propriedade notável, que iremos demonstrar.

Pelo que precede vê-se que  $a_{\mu-1}$  pode ser expresso racionalmente através dos coeficientes de  $\varphi(x)$  e  $\theta(x)$ , e por  $\alpha$ . Se portanto estes coeficientes são reais,  $a_{\mu-1}$  deve ter a forma

$$a_{\mu-1} = a + b\sqrt{-1},$$

onde  $\sqrt{-1}$  entra apenas através da quantidade  $\alpha$ , que em geral é imaginária<sup>6</sup>, e que geralmente pode ter o valor

$$\alpha = \cos \frac{2\pi}{\mu} + \sqrt{-1} \operatorname{sen} \frac{2\pi}{\mu}.$$

Mudando-se portanto em  $\alpha$  o sinal de  $\sqrt{-1}$  e designando por  $a'_{\mu-1}$  o valor correspondente de  $a_{\mu-1}$ , ter-se-á

$$a'_{\mu-1} = a - b\sqrt{-1}.$$

Conforme a (40), é evidente que  $a'_{\mu-1} = a_{\mu-1}$  e, portanto, que  $b = 0$  e

$$a_{\mu-1} = a. \tag{43}$$

Portanto  $a_{\mu-1}$  tem sempre um valor real. Mostra-se da mesma maneira que

$$\nu_1 = c + d\sqrt{-1} \quad \text{e} \quad \nu_{\mu-1} = c - d\sqrt{-1},$$

onde  $c$  e  $d$  são reais.

Portanto

$$\begin{aligned} \nu_1 + \nu_{\mu-1} &= 2c, \\ \nu_1 \nu_{\mu-1} &= a^\mu. \end{aligned}$$

---

<sup>6</sup>NT: seguindo o uso de então, Abel escreve 'imaginário' para aquilo que se chama hodiernamente de 'complexo'.



Disto tira-se

$$\nu_1 = c + \sqrt{-1} \sqrt{a^\mu - c^2}, \quad (44)$$

[144] e, por conseqüência,  $\sqrt{a^\mu - c^2} = d$ ; donde se ve que  $\sqrt{a^\mu - c^2}$  tem sempre um valor real.

Isto posto, se pode fazer

$$c = (\sqrt{\rho})^\mu \cos \delta, \quad \sqrt{a^\mu - c^2} = (\sqrt{\rho})^\mu \text{sen } \delta, \quad (45)$$

onde  $\rho$  é uma quantidade positiva.

Disto segue que

$$c^2 + \left[ \sqrt{a^\mu - c^2} \right]^2 = (\sqrt{\rho})^{2\mu},$$

ou seja,

$$a^\mu = \rho^\mu; \quad (46)$$

em conseqüência,  $\rho$  será igual ao valor numérico de  $a$ . Além disto vê-se que  $a$  é sempre positivo se  $\mu$  for um número ímpar.

Conhecendo-se  $\rho$  e  $\delta$  teremos

$$\nu_1 = (\sqrt{\rho})^\mu \left( \cos \delta + \sqrt{-1} \text{sen } \delta \right)$$

e, por conseqüência,

$$\sqrt[\mu]{\nu_1} = (\sqrt{\rho}) \left( \cos \frac{\delta + 2m\pi}{\mu} + \sqrt{-1} \text{sen } \frac{\delta + 2m\pi}{\mu} \right).$$

Substituindo-se este valor de  $\sqrt[\mu]{\nu_1}$  na expressão (42) para  $x$ , esta toma a forma:

$$\begin{aligned} x = \frac{1}{\mu} \left\{ -A + \sqrt{\rho} \left( \cos \frac{\delta + 2m\pi}{\mu} + \sqrt{-1} \text{sen } \frac{\delta + 2m\pi}{\mu} \right) \right. \\ + (f + g \sqrt{-1}) \left( \cos \frac{2(\delta + 2m\pi)}{\mu} + \sqrt{-1} \text{sen } \frac{2(\delta + 2m\pi)}{\mu} \right) \\ + (F + G \sqrt{-1}) \sqrt{\rho} \left( \cos \frac{3(\delta + 2m\pi)}{\mu} + \sqrt{-1} \text{sen } \frac{3(\delta + 2m\pi)}{\mu} \right) \\ \left. + (f_1 + g_1 \sqrt{-1}) \left( \cos \frac{4(\delta + 2m\pi)}{\mu} + \sqrt{-1} \text{sen } \frac{4(\delta + 2m\pi)}{\mu} \right) + \text{etc.} \right\} \end{aligned} \quad (47)$$

onde  $\rho, A, f, g, F, G$ , etc., são funções racionais de  $\cos(2\pi/\mu)$  e  $\sin(2\pi/\mu)$  e dos coeficientes de  $\varphi(x)$  e  $\theta(x)$ . Encontrar-se-á todas as raízes dando-se a  $m$  os valores  $0, 1, 2, 3, \dots, \mu - 1$ .

A expressão precedente de  $x$  faz ver:

**Teorema V.** Para resolver a equação  $\varphi(x) = 0$ , é suficiente:

1. dividir a circunferência inteira do círculo em  $\mu$  partes iguais,
2. dividir um ângulo  $\delta$ , que se pode construir a seguir, em  $\mu$  partes iguais,
3. e extrair a raiz quadrada duma única quantidade  $\rho$ .

Este teorema não é mais que uma extensão de um teorema semelhante, que o senhor Gauss fornece sem demonstração na obra citada mais acima, pág. 651.

[145] Deve-se ainda observar que as raízes da equação  $\varphi(x) = 0$  são ou todas reais ou todas imaginárias. De fato, se uma raiz  $x$  é real, as outras o são igualmente, como o fazem ver as expressões

$$\theta(x), \quad \theta^2(x), \quad \dots, \quad \theta^{\mu-1}(x),$$

que não contém mais que quantidades reais. Se, pelo contrário,  $x$  é imaginário<sup>7</sup> as outras raízes o serão também pois se, por exemplo,  $\theta^m(x)$  fosse real,  $\theta^{\mu-m}(\theta^m(x)) = \theta^\mu(x) = x$ , se-lo-ia igualmente, contra a hipótese. No primeiro caso  $a$  será positivo e no segundo negativo.

Se  $\mu$  é um número ímpar, todas as raízes serão reais.

O método que fornecemos neste parágrafo, para resolver a equação  $\varphi(x) = 0$ , é aplicável em todos os casos, seja o número  $\mu$  primo ou não; mas se  $\mu$  é um número composto, existe ainda um outro método que oferece algumas simplificações e que iremos expor agora em poucas palavras.

Se tivermos  $\mu = m \cdot n$ , as raízes

$$x, \quad \theta(x), \quad \theta^2(x), \quad \dots, \quad \theta^{\mu-1}(x)$$

---

<sup>7</sup>NT: como já observado anteriormente, seguindo o uso de então, Abel escreve ‘imaginário’ para aquilo que chamaríamos modernamente de ‘complexo’.

poderão ser agrupadas da maneira seguinte:

$$\begin{array}{ccccccc}
 x, & \theta^m(x), & \theta^{2m}(x), & \dots, & \theta^{(n-1)m}(x), \\
 \theta(x), & \theta^{m+1}(x), & \theta^{2m+1}(x), & \dots, & \theta^{(n-1)m+1}(x), \\
 \theta^2(x), & \theta^{m+2}(x), & \theta^{2m+2}(x), & \dots, & \theta^{(n-1)m+2}(x), \\
 & & & & \vdots \\
 \theta^{m-1}(x), & \theta^{2m-1}(x), & \theta^{3m-1}(x), & \dots, & \theta^{mn-1}(x).
 \end{array}$$

Em fazendo-se, para abreviar,

$$\theta^m(x) = \theta_1(x), \quad (48)$$

$$x = x_1, \quad \theta(x) = x_2, \quad \theta^2(x) = x_3, \quad \dots, \quad \theta^{m-1}(x) = x_m, \quad (49)$$

se pode escrever as raízes como segue:

$$\left\{ \begin{array}{l}
 1' \ x_1, \quad \theta_1(x_1), \quad \theta_1^2(x_1), \quad \dots, \quad \theta_1^{n-1}(x_1), \\
 2' \ x_2, \quad \theta_1(x_2), \quad \theta_1^2(x_2), \quad \dots, \quad \theta_1^{n-1}(x_2), \\
 \vdots \\
 m' \ x_m, \quad \theta_1(x_m), \quad \theta_1^2(x_m), \quad \dots, \quad \theta_1^{n-1}(x_m).
 \end{array} \right. \quad (50)$$

Portanto, em virtude do que se viu no §2, se pode decompor a equação  $\varphi(x) = 0$ , que é do grau  $m \cdot n$ , em  $m$  equações do grau  $n$ , cujos coeficientes dependerão de uma equação do grau  $m$ . As raízes destas  $m$  equações serão, respectivamente, as raízes  $1', 2', \dots, m'$ .

Se  $n$  for um outro número composto,  $m_1 \cdot n_1$ , se pode decompor da mesma maneira cada uma das equações de grau  $n$ , em  $m_1$  equações [146] do grau  $n_1$ , cujos coeficientes dependerão duma equação do grau  $m_1$ . Se  $n_1$  for ainda um número composto, se pode continuar a decomposição da mesma maneira.

**Teorema VI.** Em geral, se supusermos

$$\mu = m_1 \cdot m_2 \cdot m_3 \dots m_n, \quad (51)$$

a resolução da equação proposta  $\varphi(x) = 0$  se reduzirá àquela de  $n$  equações dos graus:

$$m_1, \quad m_2, \quad m_3, \quad \dots, \quad m_n.$$

É mesmo suficiente conhecer-se apenas uma raiz destas equações, pois se se conhece uma raiz da equação proposta, se terá todas as outras raízes, expressas como funções racionais da raiz conhecida.

O método precedente é no fundo o mesmo que o senhor Gauss dá para a redução da equação a dois termos  $x^\mu - 1 = 0$ .

Para fazer ver mais claramente a decomposição precedente da equação  $\varphi(x) = 0$  em outras de graus menos elevados suponhamos, por exemplo,  $\mu = 30 = 5 \cdot 3 \cdot 2$ .

Neste caso as raízes serão

$$x, \quad \theta(x), \quad \theta^2(x), \quad \dots, \quad \theta^{29}(x).$$

Para começar, formemos uma equação do sexto grau, cujas raízes serão

$$x, \quad \theta^5(x), \quad \theta^{10}(x), \quad \theta^{15}(x), \quad \theta^{20}(x), \quad \theta^{25}(x).$$

Sendo  $R = 0$  tal equação, se pode determinar seus coeficientes, racionalmente, através duma mesma quantidade  $y$ , que será raiz duma outra equação do quinto grau:  $P = 0$ .

O grau da equação  $R = 0$  sendo ele próprio um número composto, formaremos uma equação do terceiro grau:  $R_1 = 0$ , cujas raízes serão

$$x, \quad \theta^{10}(x), \quad \theta^{20}(x),$$

e cujos coeficientes são funções racionais de  $y$ , e de uma mesma quantidade  $z$ , que é raiz duma equação do segundo grau  $P_1 = 0$ , na qual os coeficientes são expressos racionalmente por  $y$ .

Eis aqui um quadro das operações

$$\begin{aligned} x^3 + f(y, z) x^2 + f_1(y, z) x + f_2(y, z) &= 0, \\ z^2 + f(y) z + f_1(y) &= 0, \\ y^5 + A_1 y^4 + A_2 y^3 + A_3 y^2 + A_4 y + A_5 &= 0. \end{aligned}$$

Pode-se começar por uma equação do segundo grau em  $x$  ou mesmo com uma equação do quinto grau.

[147]

Retomemos a equação geral  $\varphi(x) = 0$ .

Em supondo-se  $\mu = m \cdot n$ , se pode fazer

$$x^n + f(y) x^{n-1} + f_1(y) x^{n-2} + \dots = 0, \quad (52)$$

onde  $y$  é determinado por uma equação do  $m$ -ésimo grau:

$$y^m + A y^{m-1} + \dots = 0, \quad (53)$$

na qual todos os coeficientes são expressos racionalmente através de quantidades conhecidas.

Isto posto, sejam

$$\begin{cases} \mu = m_1 \cdot m_2 \cdot m_3 \cdot \dots \cdot m_\omega & \text{e} \\ \mu = m_1 \cdot n_1, \mu = m_2 \cdot n_2; \dots & \text{e } \mu = m_\omega \cdot n_\omega, \end{cases} \quad (54)$$

diferentes maneiras de se decompor o número  $\mu$  em dois fatores, poder-se-á decompor a equação proposta  $\varphi(x) = 0$  em duas outras das  $\omega$  maneiras seguintes:

1.  $F_1(x_1, y_1) = 0$ , cujas raízes serão  $x, \theta^{m_1}(x), \theta^{2m_1}(x), \dots, \theta^{(n_1-1)m_1}(x)$  e cujos coeficientes são funções racionais duma quantidade  $y_1$ , raiz duma equação  $f_1(y_1) = 0$ , do grau  $m_1$ .
2.  $F_2(x_1, y_2) = 0$ , cujas raízes serão  $x, \theta^{m_2}(x), \theta^{2m_2}(x), \dots, \theta^{(n_2-1)m_2}(x)$  e cujos coeficientes são funções racionais duma mesma quantidade  $y_2$ , raiz duma equação  $f_2(y_2) = 0$ , do grau  $m_2$ .
3.  $\vdots$
4.  $F_\omega(x_1, y_\omega) = 0$ , cujas raízes serão  $x, \theta^{m_\omega}(x), \theta^{2m_\omega}(x), \dots, \theta^{(n_\omega-1)m_\omega}(x)$  e cujos coeficientes são funções racionais duma mesma quantidade  $y_\omega$ , raiz duma equação  $f_\omega(y_\omega) = 0$ , do grau  $m_\omega$ .

Suponhamos agora que  $m_1, m_2, \dots, m_\omega$ , tomados dois a dois, sejam primos entre si. Eu afirmo que se poderá exprimir o valor de  $x$  racionalmente através das quantidades  $y_1, y_2, y_3, \dots, y_n$ . De fato, se  $m_1, m_2, \dots, m_\omega$  são primos entre si, é claro que não existe mais do que uma única raiz, que satisfará por sua vez a todas as equações

$$F_1(x, y_1) = 0, \quad F_2(x, y_2) = 0, \quad \dots, \quad F_\omega(x, y_\omega) = 0, \quad (55)$$

a saber, a raiz  $x$ . Portanto, segundo um teorema conhecido, se pode exprimir  $x$  racionalmente através dos coeficientes destas equações e, conseqüentemente, através das quantidades  $y_1, y_2, \dots, y_\omega$ .

Eis aqui, portanto, a redução da resolução da equação proposta à solução de  $\omega$  equações,  $f_1(y_1) = 0, f_2(y_2) = 0, \dots, f_\omega(y_\omega) = 0$ , que são respectivamente dos graus  $m_1, m_2, \dots, m_\omega$ , e cujos coeficientes são funções racionais dos coeficientes de  $\varphi(x)$  e  $\theta(x)$ .

[148] Se desejarmos que as equações

$$f_1(y_1) = 0; \quad f_2(y_2) = 0; \quad \dots; \quad f_\omega(y_\omega) = 0 \quad (56)$$

sejam [de grau] o menos elevado possível, é preciso escolher  $m_1, m_2, \dots, m_\omega$  tais que estes números sejam potências de números primos. Por exemplo, se a equação proposta  $\varphi(x) = 0$  for do grau

$$\mu = \varepsilon_1^{\nu_1} \cdot \varepsilon_2^{\nu_2} \cdot \dots \cdot \varepsilon_\omega^{\nu_\omega}, \quad (57)$$

onde  $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_\omega$  são números primos diferentes, se terá

$$m_1 = \varepsilon_1^{\nu_1}, \quad m_2 = \varepsilon_2^{\nu_2}, \quad \dots, \quad m_\omega = \varepsilon_\omega^{\nu_\omega}. \quad (58)$$

Sendo a equação proposta resolúvel algebricamente, as equações (56) também o serão; pois as raízes destas equações são funções racionais de  $x$ . Pode-se resolve-las facilmente da seguinte maneira:

A quantidade  $y$  é uma função racional e simétrica das raízes da equação (53), ou seja, de

$$x, \quad \theta^m(x), \quad \theta^{2m}(x), \quad \dots, \quad \theta^{(n-1)m}(x). \quad (59)$$

Sejam

$$y = F(x) = f\left(x, \theta^m(x), \theta^{2m}(x), \dots, \theta^{(n-1)m}(x)\right), \quad (60)$$

então as raízes da equação (53) serão

$$F(x); \quad F(\theta(x)), \quad F(\theta^2(x)), \quad \dots, \quad F(\theta^{m-1}(x)); \quad (61)$$

eu afirmo que se pode exprimir estas raízes da maneira seguinte:

$$y, \quad \lambda(y), \quad \lambda^2(y), \quad \dots, \quad \lambda^{m-1}(y), \quad (62)$$

onde  $\lambda(y)$  é uma função racional de  $y$  e de quantidades conhecidas.

Se terá

$$F(\theta(x)) = f\left\{\theta(x), \theta(\theta^m(x)), \theta(\theta^{2m}(x)), \dots, \theta(\theta^{(n-1)m}(x))\right\}, \quad (63)$$

portanto  $F(\theta(x))$  será, bem como  $F(x)$ , uma função racional e simétrica das raízes  $x, \theta^m(x), \dots, \theta^{(n-1)m}(x)$ , donde se pode, pelo processo encontrado em (24), expressar  $\psi(\theta(x))$  racionalmente através de  $\psi(x)$ . Seja portanto

$$\psi(\theta(x)) = \lambda(\psi(x)) = \lambda(y),$$

ter-se-á (em virtude do primeiro teorema), ao substituir-se  $x$  por  $\theta(x), \theta^2(x), \dots, \theta^{m-1}(x)$ :

$$\psi(\theta^2(x)) = \lambda(\psi(\theta(x))) = \lambda^2(y),$$

$$\begin{aligned} \psi(\theta^3(x)) &= \lambda(\psi(\theta^2(x))) = \lambda^3(y), \\ &\vdots \\ \psi(\theta^{m-1}(x)) &= \lambda(\psi(\theta^{m-2}(x))) = \lambda^{m-1}(y), \end{aligned}$$

o que queríamos demonstrar.

Como agora as raízes da equação (53) poderiam ser representadas por:

$$y, \quad \lambda(y), \quad \lambda^2(y), \quad \dots, \quad \lambda^{m-1}(y),$$

se pode resolver algebricamente esta equação da mesma maneira que [149] a equação  $\varphi(x) = 0$  (Veja o teorema III.)

Se  $m$  é uma potência dum número primo,  $m = \varepsilon^\nu$ , se pode ainda determinar  $y$  com o auxílio de  $\nu$  equações do grau  $\varepsilon$ . (Veja o teorema VI.)

Se no teorema III se supuser que  $\mu$  seja uma potência de 2, ter-se-á, como corolário, o teorema seguinte:

**Teorema VII.** Se as raízes duma equação de grau  $2^\omega$  puderem ser representadas através de

$$x, \quad \theta(x), \quad \theta^2(x), \quad \dots, \quad \theta^{2^\omega-1}(x) \quad \text{onde} \quad \theta^{2^\omega}(x) = x,$$

esta equação poderá ser resolvida com o auxílio da extração de  $\omega$  raízes quadradas.

Este teorema, aplicado à equação

$$\frac{x^{1+2^\omega} - 1}{x - 1} = 0,$$

onde  $1 + 2^\omega$  é um número primo, dá o teorema do senhor Gauss para o círculo.

#### §4.

*Das equações para as quais todas as raízes podem ser expressas racionalmente por uma dentre elas.*

Vimos anteriormente (teorema III) que uma equação de grau qualquer, cujas raízes podem ser expressas por

$$x, \quad \theta(x), \quad \theta^2(x), \quad \dots, \quad \theta^{\mu-1}(x)$$

é sempre resolúvel algebricamente.

Neste caso todas as raízes são expressáveis racionalmente por uma dentre elas; mas uma equação cujas raízes possuam esta propriedade não é sempre resolúvel algebricamente; apesar disto, excetuando o caso considerado, existe ainda um outro, no qual isto ocorre. Tem-se o teorema seguinte:

**Teorema VIII.** Seja  $\chi(x) = 0$  uma equação algébrica qualquer, cujas raízes possam todas ser expressas racionalmente por uma entre elas, que designaremos por  $x$ . Sendo  $\theta(x)$  e  $\theta_1(x)$  duas outras raízes quaisquer, a equação proposta será resolúvel algebricamente se tivermos  $\theta(\theta_1(x)) = \theta_1(\theta(x))$ .

A demonstração deste teorema pode ser reduzida imediatamente à teoria exposta no §2, como iremos ver agora.

Se se conhece a raiz  $x$ , ter-se-á também simultaneamente todas as outras; é suficiente, portanto, procurar o valor de  $x$ .

Se a equação

$$\chi(x) = 0 \tag{64}$$

não for irredutível, seja

$$\varphi(x) = 0 \tag{65}$$

[150] a equação menos elevada, a qual possa a raiz  $x$  satisfazer, os coeficientes desta equação não contendo mais que quantidades conhecidas. Neste caso as raízes da equação  $\varphi(x) = 0$  se encontrarão entre as raízes da equação  $\chi(x) = 0$  (veja o primeiro teorema) e, por conseqüência, poderão ser expressas racionalmente por uma dentre elas.

Isto posto, seja  $\theta(x)$  uma raiz diferente de  $x$ . Em virtude daquilo que foi visto no primeiro parágrafo, as raízes da equação  $\varphi(x) = 0$  poderão ser expressas como se segue:

$$\begin{array}{ccccccc} x, & \theta(x), & \theta^2(x), & \dots, & \theta^{n-1}(x), \\ x_1, & \theta(x_1), & \theta^2(x_1), & \dots, & \theta^{n-1}(x_1), \\ & & \dots & & \\ x_{m-1}, & \theta(x_{m-1}), & \theta^2(x_{m-1}), & \dots, & \theta^{n-1}(x_{m-1}), \end{array}$$

e, em se formando a equação

$$x^n + A' x^{n-1} + A'' x^{n-2} + A''' x^{n-3} + \dots + A^{(n-1)} x + A^{(n)} = 0, \tag{66}$$

cujas raízes são  $x, \theta(x), \theta^2(x), \dots, \theta^{n-1}(x)$ , os coeficientes  $A', A'', \dots, A^{(n)}$  poderão ser expressos racionalmente por uma mesma quantidade  $y$ , que será



raiz duma equação irredutível<sup>8</sup>:

$$y^m = p_1 y^{m-1} + p_2 y^{m-2} + \cdots + p_{m-1} y + p_m = 0, \quad (67)$$

cujos coeficientes são quantidades conhecidas (veja §2).

A determinação de  $x$  pode efetuar-se com o auxílio das duas equações (66) e (67). A primeira destas equações é resolúvel algebricamente, em se supondo conhecidos os coeficientes, o que equivale dizer, supondo-se  $y$  conhecido (veja o teorema III). Quanto à equação em  $y$ , iremos demonstrar que suas raízes gozam da mesma propriedade que aquelas da equação proposta  $\varphi(x) = 0$ , a saber de serem expressáveis racionalmente por uma dentre elas.

A quantidade  $y$  é [veja (15)] uma certa função racional e simétrica das raízes  $x, \theta(x), \theta^2(x), \dots, \theta^{n-1}(x)$ . Em fazendo-se

$$\left\{ \begin{array}{l} y = f(x, \theta(x), \theta^2(x), \dots, \theta^{n-1}(x)), \\ \text{as outras raízes da equação (67) serão:} \\ y_1 = f(x_1, \theta(x_1), \theta^2(x_1), \dots, \theta^{n-1}(x_1)), \\ \vdots \\ y_{m-1} = f(x_{m-1}, \theta(x_{m-1}), \theta^2(x_{m-1}), \dots, \theta^{n-1}(x_{m-1})). \end{array} \right. \quad (68)$$

[151] Agora, no caso em questão  $x_1, \dots, x_{m-1}$  serão funções racionais da raiz  $x$ . Façamos, em consequência,

$$x_1 = \theta(x_1), \quad x_2 = \theta(x_2), \quad \dots, \quad x_{m-1} = \theta_{m-1}(x),$$

então as raízes da equação (67) terão a forma:

$$y_1 = f\left(\theta_1(x), \theta(\theta_1(x)), \theta^2(\theta_1(x)), \dots, \theta^{n-1}(\theta_1(x))\right).$$

Conforme a hipótese, as funções  $\theta(x)$  e  $\theta_1(x)$  têm a propriedade

$$\theta(\theta_1(x)) = \theta_1(\theta(x)),$$

equação que, em virtude do teorema I, terá lugar substituindo-se no lugar de  $x$  uma outra raiz qualquer da equação  $\varphi(x) = 0$ . Disto obtém-se sucessivamente

$$\theta^2(\theta_1(x)) = \theta(\theta_1(\theta(x))) = \theta_1(\theta^2(x)),$$

---

<sup>8</sup>Demonstrar-se-á facilmente que esta equação não pode ser redutível. Seja  $R = 0$  a equação irredutível em  $y$ , e  $\nu$  seu grau. Em eliminando-se  $y$ , se terá uma equação em  $x$  do grau  $n\nu$ ; portanto  $n\nu \geq \mu$ . Mas se tem  $\mu = n \cdot m$  e, portanto,  $\nu \geq m$ , o que é impossível, pois  $\nu$  é menor que  $m$ . Logo, etc.

$$\begin{aligned}\theta^3(\theta_1(x)) &= \theta(\theta_1(\theta^2(x))) = \theta_1(\theta^3(x)), \\ &\vdots \\ \theta^{n-1}(\theta_1(x)) &= \theta(\theta_1(\theta^{n-2}(x))) = \theta_1(\theta^{n-1}(x)).\end{aligned}$$

Com isto, a expressão de  $y_1$  tornar-se-á

$$y_1 = f\left(\theta_1(x), \theta_1(\theta(x)), \theta_1(\theta^2(x)), \dots, \theta_1(\theta^{n-1}(x))\right),$$

e vê-se que  $y_1$ , como  $y$ , é uma função *racional* e *simétrica* das raízes

$$x, \quad \theta(x), \quad \theta^2(x), \quad \dots, \quad \theta^{n-1}(x).$$

Logo, em virtude do §2, se pode exprimir  $y_1$  racionalmente através de  $y$  e de quantidades conhecidas. O mesmo arazoado aplicar-se-á a toda raiz da equação (67). Sejam agora  $\lambda(y)$  e  $\lambda_1(y)$  duas raízes quaisquer, eu afirmo que se terá

$$\lambda(\lambda_1(y)) = \lambda_1(\lambda(y)).$$

De fato, tendo-se, por exemplo,

$$\lambda(y) = f\left(\theta_1(x), \theta(\theta_1(x)), \dots, \theta^{n-1}(\theta_1(x))\right),$$

se

$$y = f\left(x, \theta(x), \dots, \theta^{n-1}(x)\right),$$

se terá, colocando  $\theta_2(x)$  no lugar de  $x$ :

$$\lambda(y_2) = f\left(\theta_1(\theta_2(x)), \theta(\theta_1(\theta_2(x))), \dots, \theta^{n-1}(\theta_1(\theta_2(x)))\right),$$

onde

$$y_2 = f\left(\theta_2(x), \theta(\theta_2(x)), \dots, \theta^{n-1}(\theta_2(x))\right) = \lambda_1(y),$$

portanto

$$\lambda(\lambda_1(y)) = f\left(\theta_1(\theta_2(x)), \theta(\theta_1(\theta_2(x))), \dots, \theta^{n-1}(\theta_1(\theta_2(x)))\right)$$

e, igualmente,

$$\lambda_1(\lambda(y)) = f\left(\theta_2(\theta_1(x)), \theta(\theta_2(\theta_1(x))), \dots, \theta^{n-1}(\theta_2(\theta_1(x)))\right),$$

donde, uma vez que  $\theta_1(\theta_2(x)) = \theta_2(\theta_1(x))$ ,

$$\lambda(\lambda_1(y)) = \lambda_1(\lambda(y)).$$

As raízes da equação (67) terão, portanto, precisamente a mesma propriedade que aquelas da equação  $\varphi(x) = 0$ .

[152] Isto posto, se pode aplicar à equação (67) o mesmo procedimento que à equação  $\varphi(x) = 0$ ; isto significa dizer, a determinação de  $y$  pode se efetuar com o auxílio de duas equações, das quais uma será resolúvel algebricamente e a outra terá a propriedade da equação  $\varphi(x) = 0$ .

Portanto, o mesmo procedimento pode ainda ser aplicado a esta última equação. Em se continuando, fica claro que a determinação de  $x$  poderá se efetuar com o auxílio de um certo número de equações que serão todas resolúveis algebricamente. Portanto, finalmente, a equação  $\varphi(x) = 0$  será resolúvel com o auxílio de operações algébricas, em supondo-se conhecidas as quantidades que com  $x$  compõem as funções:

$$\varphi(x), \quad \theta(x), \quad \theta_1(x), \quad \theta_2(x), \quad \dots, \quad \theta_{m-1}(x).$$

É claro que o grau de cada uma das equações às quais se reduz a determinação de  $x$ , será um fator de  $\mu$  que marca o grau da equação  $\varphi(x) = 0$ . Disto segue:

**Teorema IX.** Se se designa os graus destas equações respectivamente por

$$n, \quad n_1, \quad n_2, \quad \dots, \quad n_\omega,$$

se terá

$$\mu = n \cdot n_1 \cdot n_2 \dots n_\omega.$$

Unindo o que precede com aquilo que foi exposto no §3 ter-se-á o seguinte teorema:

**Teorema X.** Supondo-se o grau  $\mu$  da equação  $\varphi(x) = 0$  decomposto como se segue:

$$\mu = \varepsilon_1^{\nu_1} \cdot \varepsilon_2^{\nu_2} \cdot \varepsilon_3^{\nu_3} \dots \varepsilon_\alpha^{\nu_\alpha}, \quad (69)$$

onde  $\varepsilon_1, \varepsilon_2, \varepsilon_3, \dots, \varepsilon_\alpha$  são números primos, a determinação de  $x$  poderá se efetuar com o auxílio da resolução de  $\nu_1$  equações do grau  $\varepsilon_1$ , de  $\nu_2$  equações do grau  $\varepsilon_2$ , etc., e todas estas equações serão resolúveis algebricamente.

No caso em que  $\mu = 2^\nu$ , se pode encontrar o valor de  $x$  com o auxílio da extração de  $\nu$  raízes quadradas.

§5.

*Aplicações às funções circulares.*

Designando-se por  $\alpha$  a quantidade  $2\pi/\mu$ , sabe-se que se pode encontrar uma equação algébrica do grau  $\mu$ , cujas raízes serão as  $\mu$  quantidades:

$$\cos a, \quad \cos 2a, \quad \cos 3a, \quad \dots, \quad \cos \mu a,$$

[153] e cujos coeficientes serão números racionais. Esta equação será

$$x^\mu - \frac{1}{4}\mu \cdot x^{\mu-2} + \frac{1}{16} \cdot \frac{\mu(\mu-3)}{1 \cdot 3} \cdot x^{\mu-4} \dots = 0. \quad (70)$$

Vamos ver que esta equação tem a mesma forma que a equação  $\chi(x) = 0$ , considerada no parágrafo precedente.

Seja  $\cos a = x$ , ter-se-á segundo uma fórmula conhecida, qualquer que seja  $a$ :

$$\cos ma = \theta(\cos a), \quad (71)$$

onde  $\theta$  designa uma função inteira. Portanto  $\cos ma$ , que exprime uma raiz qualquer da equação (70), será uma função racional da raiz  $x$ . Seja  $\theta_1(x)$  uma outra raiz, eu afirmo que se terá

$$\theta(\theta_1(x)) = \theta_1(\theta(x)).$$

De fato, seja  $\theta_1(x) = \cos m'a$ , a fórmula (71) dará, colocando-se  $m'a$  no lugar de  $a$ :

$$\cos(mm'a) = \theta(\cos m'a) = \theta(\theta_1(x)).$$

Da mesma maneira se terá

$$\cos(m'ma) = \theta_1(\cos ma) = \theta_1(\theta(x)),$$

portanto:

$$\theta(\theta_1(x)) = \theta_1(\theta(x)).$$

Portanto, de acordo com o que se viu no parágrafo precedente,

$$x \quad \text{ou} \quad \cos a = \cos \frac{\pi}{\mu}$$

poderá ser determinado algebricamente. Isto é conhecido.

Suponhamos agora que  $\mu$  seja um número primo igual a  $2n + 1$ ; as raízes da equação (70) serão:

$$\cos \frac{2\pi}{2n+1}, \quad \cos \frac{4\pi}{2n+1}, \quad \dots, \quad \cos \frac{4n\pi}{2n+1}, \quad \cos 2\pi.$$

A última raiz,  $\cos 2\pi$ , é igual à unidade, portanto, a equação (70) é divisível por  $x - 1$ . As outras raízes serão sempre iguais entre si aos pares, pois tem-se  $\cos \frac{2m\pi}{2n+1} = \cos \frac{(2n+1-m)2\pi}{2n+1}$ , portanto pode-se encontrar uma equação cujas raízes serão

$$\cos \frac{2\pi}{2n+1}, \quad \cos \frac{4\pi}{2n+1}, \quad \dots, \quad \cos \frac{2n\pi}{2n+1}. \quad (72)$$

Esta equação será:

$$\begin{aligned} x^n + \frac{1}{2}x^{n-1} - \frac{1}{4}(n-1)x^{n-2} - \frac{1}{8}(n-2)x^{n-3} + \\ + \frac{1}{16} \frac{(n-2)(n-3)}{1 \cdot 2} x^{n-4} + \frac{1}{32} \frac{(n-2)(n-3)}{1 \cdot 2} x^{n-5} - \text{etc} = 0. \end{aligned} \quad (73)$$

Isto posto, seja [154]

$$\cos \frac{2\pi}{2n+1} = x = \cos a,$$

se terá, após o que precede:

$$\cos \frac{2m\pi}{2n+1} = \theta(x) = \cos ma.$$

A equação (73) será portanto satisfeita pelas raízes

$$x, \quad \theta(x), \quad \theta^2(x), \quad \theta^3(x), \quad \dots \quad (74)$$

Tem-se, qualquer que seja o valor de  $a$ :

$$\theta(\cos a) = \cos ma.$$

Daí se tira, sucessivamente:

$$\begin{aligned} \theta^2(\cos a) &= \theta(\cos ma) = \cos m^2 a, \\ \theta^3(\cos a) &= \theta(\cos m^2 a) = \cos m^3 a, \\ &\vdots \\ \theta^\mu(\cos a) &= \theta(\cos m^{\mu-1} a) = \cos m^\mu a. \end{aligned}$$

As raízes (74) ficarão, portanto,

$$\cos a, \quad \cos ma, \quad \cos m^2a, \quad \cos m^3a, \quad \dots, \quad \cos m^\mu a, \quad \dots \quad (75)$$

Isto posto, se  $m$  é uma raiz primitiva para o módulo  $2n + 1$  (veja Gauss, *Disquisitiones arithmeticae*, pág. 53), eu afirmo que todas as raízes

$$\cos a, \quad \cos ma, \quad \cos m^2a, \quad \dots, \quad \cos m^{n-1}a, \quad \dots \quad (76)$$

serão diferentes entre si. De fato, se se tivesse

$$\cos m^\mu a = \cos m^\nu a,$$

onde  $\mu$  e  $\nu$  são menores que  $n$ , se obteria:

$$m^\mu a = \pm m^\nu a + 2k\pi,$$

onde  $k$  é inteiro. Isto fornece, ao substituir-se  $a$  pelo seu valor  $2\pi/(2n + 1)$ ,

$$m^\mu = \pm m^\nu + k(2n + 1),$$

donde

$$m^\mu \mp m^\nu = m^\nu(m^{\mu-\nu} \mp 1) \quad \left[ \equiv k(an + 1) \right],$$

e, em consequência,

$$m^{2(\mu-\nu)} - 1$$

seria divisível por  $2n + 1$ , o que é impossível, pois  $2(\mu - \nu)$  é menor do que  $2n$ , e foi suposto que  $m$  é uma raiz primitiva.

Se terá ainda

$$\cos m^n a = \cos a,$$

pois  $m^{2n} - 1 = (m^n - 1)(m^n + 1)$  é divisível por  $2n + 1$ ; portanto:

$$m^n = -1 + k(2n + 1),$$

e, em consequência,

$$\cos m^n a = \cos(-a + k2\pi) = \cos a.$$

[155]

Disto se vê que as  $n$  raízes da equação (73) poderão se expressar através da (76); o que significa dizer, por:

$$x, \theta(x), \theta^2(x), \theta^3(x), \dots, \theta^{n-1}(x), \quad \text{onde} \quad \theta^n(x) = x.$$

Portanto, em virtude do teorema III, esta equação será resolúvel algebricamente.

Em fazendo-se  $n = m_1 \cdot m_2 \dots m_\omega$ , se pode dividir a circunferência inteira do círculo em  $2n + 1$  partes iguais, com auxílio de  $\omega$  equações dos graus  $m_1, m_2, m_3, \dots, m_\omega$ . Se os números  $m_1, m_2, m_3, \dots, m_\omega$  são primos entre si, os coeficientes destas equações serão números racionais.

Em se supondo  $n = 2^\omega$ , ter-se-á o teorema conhecido sobre polígonos regulares, que podem ser construídos geometricamente.

Em virtude do teorema V se vê que para dividir a circunferência inteira do círculo em  $2n + 1$  partes iguais, é suficiente

1. dividir a circunferência inteira do círculo em  $2n$  partes iguais,
2. dividir um arco, que se pode construir a seguir, em  $2n$  partes iguais,
3. e extrair a raiz quadrada duma única quantidade  $\rho$ .

O senhor Gauss enunciou este teorema no seu *Disquisitiones*, tendo acrescentado que a quantidade da qual se deve extrair a raiz será igual a  $2n + 1$ . É isto que se pode demonstrar facilmente como se segue.

Vimos [(40), (38), (46)] que  $\rho$  é o valor numérico da quantidade

$$\left( x + \alpha\theta(x) + \alpha^2\theta^2(x) + \dots + \alpha^{n-1}\theta^{n-1}(x) \right) \\ \left( x + \alpha^{n-1}\theta(x) + \alpha^{n-2}\theta^2(x) + \dots + \alpha\theta^{n-1}(x) \right)$$

onde  $\alpha = \cos 2\pi/n + \sqrt{-1} \operatorname{sen} 2\pi/n$ . Substituindo-se  $x, \theta(x), \dots$  pelos seus valores  $\cos \alpha, \cos m\alpha, \cos m^2\alpha, \dots$  se terá

$$\pm\rho = \left\{ \cos a + \alpha \cos ma + \alpha^2 \cos m^2a + \dots + \alpha^{n-1} \cos m^{n-1}a \right\} \times \\ \left\{ \cos a + \alpha^{n-1} \cos ma + \alpha^{n-2} \cos m^2a + \dots + \alpha \cos m^{n-1}a \right\}.$$

Desenvolvendo-se e colocando  $\pm\rho$  sob a forma

$$\pm\rho = t_0 + t_1 \alpha + t_2 \alpha^2 + \dots + t_{n-1} \cdot \alpha^{n-1},$$

encontrar-se-á facilmente:

$$t_\mu = \cos a \cdot \cos m^\mu a + \cos ma \cdot \cos m^{\mu+1} a + \cdots + \cos m^{n-1-\mu} a \cdot \cos m^{n-1} a + \\ \cos m^{m-\mu} a \cdot \cos a + \cos m^{n-\mu+1} a \cdot \cos ma + \cdots + \cos m^{n-1} a \cdot \cos m^{\mu-1} a.$$

Agora, se tem

$$\cos m^\nu a \cdot \cos m^{\mu+\nu} a = \frac{1}{2} \cos(m^{\mu+\nu} a + m^\nu a) + \frac{1}{2} \cos(m^{\mu+\nu} a - m^\nu a),$$

portanto

$$t_\mu = \frac{1}{2} \left\{ \cos(m^\mu + 1)a + \cos(m^\mu + 1)ma + \right. \\ \left. + \cos(m^\mu + 1)m^2 a + \cdots + \cos(m^\mu + 1)m^{n-1} a \right\} \\ + \frac{1}{2} \left\{ \cos(m^\mu - 1)a + \cos(m^\mu - 1)ma + \right. \\ \left. + \cos(m^\mu - 1)m^2 a + \cdots + \cos(m^\mu - 1)m^{n-1} a \right\}.$$

[156]

Se se faz  $(m^\mu + 1)a = a'$ ,  $(m^\mu - 1)a = a''$ , ter-se-á:

$$t_\mu = \frac{1}{2} \left\{ \cos a' + \theta(\cos a') + \theta^2(\cos a') + \cdots + \theta^{n-1}(\cos a') \right\} \\ + \frac{1}{2} \left\{ \cos a'' + \theta(\cos a'') + \theta^2(\cos a'') + \cdots + \theta^{n-1}(\cos a'') \right\}.$$

Isto posto, existem dois casos, a saber:  $\mu$  é diferente de zero ou não.

No primeiro caso é claro que  $\cos a'$  e  $\cos a''$  são raízes da equação (73), portanto  $\cos a' = \theta^\delta(x)$ ,  $\cos a'' = \theta^\varepsilon(x)$ . Substituindo-se, virá, observando-se que  $\theta^n(x) = x$ :

$$t_\mu = \frac{1}{2} \left\{ \theta^\delta(x) + \theta^{\delta+1}(x) + \cdots + \theta^{n-1}(x) + x + \theta(x) + \cdots + \theta^{\delta-1}(x) \right\} \\ + \frac{1}{2} \left\{ \theta^\varepsilon(x) + \theta^{\varepsilon+1}(x) + \cdots + \theta^{n-1}(x) + x + \theta(x) + \cdots + \theta^{\varepsilon-1}(x) \right\},$$

portanto

$$t_\mu = x + \theta(x) + \theta^2(x) + \cdots + \theta^{n-1}(x),$$

o que significa dizer que  $t_\mu$  é igual à soma das raízes; por conseqüência, em virtude da equação (73):

$$t_\mu = -\frac{1}{2}.$$



No caso em que  $\mu = 0$ , o valor de  $t_\mu$  tornar-se-á:

$$t_0 = \frac{1}{2} \left\{ \cos 2a + \cos 2ma + \cdots + \cos 2m^{n-1}a \right\} + \frac{1}{2} n;$$

agora  $\cos 2a$  é uma raiz da equação (73), portanto, fazendo-se  $\cos 2a = \theta^\delta(x)$ , se terá:

$$\begin{aligned} \cos 2a + \cos 2ma + \cdots + \cos 2m^{n-1}a &= \theta^\delta(x) + \theta^{\delta+1}(x) + \\ &+ \cdots + \theta^{n-1}(x) + x + \theta(x) + \cdots + \theta^{\delta-1}(x) = -\frac{1}{2}, \end{aligned}$$

e, em consequência:

$$t_0 = \frac{1}{2}n - \frac{1}{4}.$$

Em virtude destes valores de  $t_0$  e  $t_\mu$ , o valor de  $\pm\rho$  será

$$\pm\rho = \frac{1}{2}n - \frac{1}{4} - \frac{1}{2} \left\{ \alpha + \alpha^2 + \alpha^3 + \cdots + \alpha^{n-1} \right\},$$

mas  $\alpha + \alpha^2 + \alpha^3 + \cdots + \alpha^{n-1} = -1$ , portanto

$$\pm\rho = \frac{1}{2}n + \frac{1}{4},$$

e como  $\rho$  é essencialmente positivo,  $\rho = (2n + 1)/4$ . Esse valor de  $\rho$  dá

$$\sqrt{\rho} = \frac{1}{2}\sqrt{2n + 1},$$

portanto a raiz quadrada que se tem a extrair é aquela do número  $2n + 1$ , como diz o senhor Gauss<sup>9</sup>.

Christiania<sup>10</sup>, 29 de março de 1828.

---

<sup>9</sup>Nota do redator (Crelle): O autor desta memória dará em outra ocasião aplicações às funções elípticas. NT: Abel morreu sem fazê-lo.

<sup>10</sup>NT: Christiania é o nome antigo de Oslo.