

DE  
SUBSTITUTIONUM THEORIA  
MEDITATIONES QUAEDAM.

---

DISSE<sup>T</sup>RAT<sup>I</sup>O INAUGURALIS  
QUAM  
CONSENSU ET AUCTORITATE  
AMPLISSIMI PHILOSOPHORUM ORDINIS  
IN  
ALMA LITTERARUM UNIVERSITATE  
FRIDERICA GUILELMA  
AD SUMMOS  
IN PHILOSOPHIA HONORES  
RITE CAPESSENDOS  
DIE XXIV. M. MARTII A. MDCCCLXII.  
H. L. Q. S.  
PUBLICKE DEFENDET  
AUCTOR  
PAULUS BACHMANN  
BEROLINENSIS.

---

ADVERSARIORUM PARTES SUSCIPIENT:  
E. FISCHER, DR. PHIL.  
F. BACHMANN, DR. PHIL.  
J. TEICHERT, CAND. PHIL.

---

BEROLINI  
TYPIS GUSTAVI SCHADE.



VIRO

ILLUSTRISSIMO CELEBERRIMO AMPLISSIMO

ERNESTO EDUARDO KUMMER

PHILOSOPHIAE DOCTORI, PROFESSORI PUBLICO ORDINARIO IN UNIVERSITATE  
FRIDERICO - GUIELMA BEROLINENSI

PRAECEPTORI REVERENDO CARISSIMO

HASCE

S T U D I O R U M P R I M I T I A S

GRATO ANIMO

OFFERT

A U C T O R.

Disquisitiones ad determinandum valorum numerum spectantes, quos functio  $n$  elementis composita elementorum permutatione induere potest, a generali quaestionis solutione longe adhuc absunt. Facile enim nonnulla theorematata generalia demonstrata sunt, ut illud, esse valorum numerum producti  $N = 1 \cdot 2 \cdot 3 \dots n$  divisorem. Quum autem inventum esset, non omnes hos divisores ad exprimendum illum numerum aptos esse, eorum qui essent indagatio paucos adhuc amplexa est. Hujus rei causa quum in eo mihi videatur quaerenda, ut methodi, quas adhibitas esse novi, a generalitate absint et omnia, quorum solutio attacta sit, problemata singularibus considerationibus solvi debuerint, quaesivi, num modo directo tractatum problema ad methodum quandam generaliorem perducere possit. Quamvis difficultum hoc problema ut longe alia via ad solutionem sit provehendum fieri possit, eam tamen quam persecutus sim, hac dissertatione designare mihi liceat. Quam in tres partes dividamus

primam principia quaedam continentem,  
secundam, quae de functionum  $m$  valorum formis generalibus theoremata nonnulla admonet,  
tertiam de substitutionum proprietatibus agentem.

## I.

ART. 1. Jam primum videamus, in quo problema generale consistat. Dato autem numero contento in serie 1, 2, 3 . . .  $N$ , hae quaestiones occurunt:

Danturne functiones quarum numerus valorum aequet ipsum  $f$ ? Quando vero exstant, quae est forma earum generalis?

Quas igitur persequentes ad solas functiones algebraicas rationales integras respicimus, quippe quae maximum in Algebra usum habeant atque emolumentum. Hae omnes additione efficiuntur et multiplicatione; quibus operationibus evolutis, prodit aggregatum mononomiorum cum coefficientibus ab elementis non pendentibus; quare forma functionum generalis haec erit  $\Sigma c_i M_i$ .

Quocunque autem mononomium formam induit

$$a_1^{\alpha_1} a_2^{\alpha_2} \cdots \cdots a_n^{\alpha_n}$$

ubi exponentium nonnulli cifrae aequales esse possunt. Habeant ipsorum  $m_1$  valorem eundem, alii  $m_2$ , aliud, . . . denique  $m_k$  reliqui aliud valorem, ut sit

$$m_1 + m_2 + \cdots + m_k = n,$$

quae, si ipsis  $k, m_1, m_2, \dots, m_k$  omnes qui locum habere possunt valores tribuis, generalissima suppositio est, valorum numerus aequabit

$$\frac{1. 2. 3. \cdots n}{m_1! m_2! \cdots m_k!}$$

Qua in formula generalis pro hocce casu simplici problematis solutio continetur.

ART. 2.  $n$  elementa  $a_1, a_2, \dots, a_n$  modis  $N$  diversis permutari sive in ordinem redigi possunt. Si in cujusvis permutationis locum aliam permutationem substituis, substitutionem efficis, quas generaliter per  $\theta, \eta, \dots$  designabimus. Constituentibus autem elementis functionem, substitutiones plane ab

eis independentes erunt neque determinatae, nisi permutatio quaedam cui applicandae sint datur \*). Quoties substitutiones  $\theta$ ,  $\eta$ , ... successive adhibentur, operationem inde ortam per productum  $\theta \cdot \eta \cdot \dots$  reprezentabimus, in quo generaliter ordinem factorum immutare non licet. Quo statim quid sub potentia seu dignitate substitutionis sit intelligendum elucet. Designata deinde substitutione identica per unitatem, substitutio  $\theta$ , quoniam plures repetita certe identicam denique substitutionem generabit, ad exponentem quendam  $t$  pertinebit, sive erit  $t$  minimus exponentis talis ut  $\theta^t = 1$ .

ART. 3. Quaerentem autem, quidnam methodi adhuc adhibitae commune habeant, fugere non potest, earum quasi principium hoc esse: Datis substitutionibus  $\theta_1, \theta_2, \dots$  et functione pro illis invariabili, inveniantur substitutiones et earum numerus, quae functionis valorem non mutent.

Quae nobis etiam quaestio fundamentalis erit. Quoniam vero, si substitutiones tales, quarum productum aliquod ex iisdem alicui aequale fiat, familiam (eine Gruppe) constituere dicimus, substitutiones quae sitae aliae non sunt nisi familia ex ipsis  $\theta_1, \theta_2, \dots$  genita, quaestio illa in hanc recedit, ut datis quibusdam substitutionibus familia ex iis genita inveniatur.

ART. 4. Valent autem de familiis nota haec theorematum:

1. Quaelibet familia substitutionem identicam et, si substitutionem  $\theta$ , omnes etiam ejusdem potentias includit.

\*) Dato enim functionis valore quodam, designatis locis, quos elementa occupant, indicibus 1, 2, 3 ...  $n$ , haec locorum determinatio eadem manet, quomodo elementa permutentur. Substitutionem  $\theta$  autem, ex. gr. (1, 2, 3, ...  $n$ ) id indicere volumus, ut elementis, quae in quovis functionis valore commodum dato locos 1, 2, ...  $n$  obtinent, ea quae locis 2, 3, ... 1 respondent, substituantur. Alia igitur substitutio post  $\theta$  adhibenda iis denuo elementis adhibetur, quae in valore jam obtento locos 1, 2, 3, ...  $n$  occupant.

2. Data familia  $\theta_1, \theta_2, \dots, \theta_m$ , designante  $\theta$  quamvis familiae substitutionem, producta

$$\theta_1\theta, \theta_2\theta, \dots, \theta_m\theta, \text{ sive etiam}$$

$$\theta\theta_1, \theta\theta_2, \dots, \theta\theta_m.$$

totam familiam reproducunt. Sit vero  $\eta$  alia substitutio, producta

$$\eta\theta_1, \eta\theta_2, \dots, \eta\theta_m$$

et inter se et a familia diversa erunt.

3. Habeat deinde familia  $F$  numerum  $g$  substitutionum et familia  $F'$  in ea contenta  $g'$  substitutiones, erit  $g'$  ipsius  $g$  divisor.

4. Quare, quia substitutiones duabus familiis  $F, F'$  e  $g, g'$  terminis constitutis communes ipsae familiam constituunt, earum numerus ipsarum  $g, g'$  divisor erit.

## II. DE FUNCTIONUM FORMIS.

ART. 5. Elementa  $a_1, a_2, \dots, a_n$ , quibus functiones componuntur, semper radices aequationis

$$x^n + p_1 x^{n-1} + \dots + p_{n-1} x + p_n = 0$$

esse supponuntur, praeterea plane arbitraria, indeterminata neque ullam inter se relationem habentia.

Tum sint functiones quaelibet  $F, F'$ . Jam vero quia satis non est, ut has functiones eodem valorum numero gaudere scias, sed fieri potest, ut adhibita substitutione altera mutetur, altera valorem servet, eas functiones amplectentes, quae aequae se habeant et quas functiones congruas dicemus, totam functionum  $n$  elementis compositarum multitudinem in classes disjungimus tales, ut e singulis classibus una qualibet functione sumta, omnes qui locum habere possunt casus diversos obtineamus. Similium vero functionum nomen iis reservabimus, quarum altera pro omnibus quidem substitutionibus, quibus altera non mutetur, immutata maneat neque vero vice versa.

ART. 6. Constituant substitutiones  $\theta_1, \theta_2, \dots, \theta_g$  familiam; data functione quadam sit  $f$  valorum numerus, quos per illas substitutiones induit,  $g_1$  substitutionum, per quas immutata manet, numerus. Quae quoniam familiam constituunt,  $g_1$  ipsius  $g$  divisor esse debet, unde esse  $f = \frac{g}{g_1}$  et valorum quos functio induere potest, numerum ipsius  $N$  divisorem facile intelligitur.

Hinc generalis functionum quae per substitutionem  $\theta$  non mutantur forma institui potest. Sit enim  $M(1)$  mononomium quodlibet functionis:

$$\Sigma c. M(a_1, a_2, \dots, a_n),$$

$\theta^t = 1$ ;  $M(1)$  per substitutionem  $\theta$  aut mutatur aut non mutatur, profecto autem substitutione  $t^{ies}$  repetita numerus  $\tau$  valorum resultat, ubi  $\tau$  ipsum  $t$  metitur. Quare designante

Cyc.  $M(\theta^r) = M(1) + M(\theta) + M(\theta^2) + \dots + M(\theta^{r-1})$   $M(\theta^i)$  valorem mononomii  $M(1)$  facta substitutione  $\theta^i$ , facile intelligitur adaequatam functioni immutatae conditionem esse, ut formam  $\Sigma c.$  Cyc.  $M(\theta^r)$  induat, ubi  $c$  coefficientem numericum, aut, si non omnia elementa permutantur, eorum quae non mutantur functionem designat. Quo statim fluit, omnem functionem symmetricam eadem forma gaudere, in qua vero singulus cyclus omnes mononomii valores continere debet. Functiones symmetricas per signum  $\sigma$  ( $a_1, a_2, \dots, a_n$ ) designabimus. Quae quum congruae sint, primam classem constituunt aliasque omnes excludunt.

ART. 7. Data functione  $F f$  valoribus affecta, qui per  $F_1, F_2, \dots, F_f$  reprezententur, functionem  $\varphi$  cogitemur hos valores quasi elementa continentem. Quorum elementorum permutationes quae esse possunt 1. 2. 3.  $\dots, f$  generaliter non omnes permutando ipsa  $\alpha$  produci possunt. Quare, si functio  $\varphi$  ipsorum  $F$  respectu symmetrica est, erit etiam ipsorum  $\alpha$  respectu, de asymmetria autem quantitatum  $F$  illam quantitatum  $\alpha$  con-

cludere non licet. Sint vero  $m$  elementorum  $a$  functiones  $F_1, F_2, \dots, F_m$ , habente aequatione  $m^{ti}$  gradus illas radices continente coefficientes symmetricos, valores diversi, quos veluti  $F_1$  induere potest, inter illas functiones reperiuntur. Quas si pro diversis ipsius  $F_1$  valoribus habemus, designante

$$\Pi(z - F) = (z - F_1)(z - F_2) \dots (z - F_f),$$

aequationem illam hoc modo scribi posse

$$\Pi(z - F)^k = 0$$

statim sequitur; uti etiam, si  $F_1, F_2, \dots, F_f$  quidam functionis valores diversi et aequationis, cuius radices sint, coefficientes symmetrici, illos omnes functionis valores esse, concludendum erit.

ART. 8. Omnium functionum  $f$  formis affectarum indicium eo inveniri potest, ut aequationi irreductibili  $f^{ti}$  gradus sufficiant, sive ad aequationem  $f^{ti}$  gradus cum coefficientibus ipsorum  $a$  respectu symmetricis pertineant. Primo enim aequatio in duos factores disjungi nequit, quorum coefficientes symmetrici sint, quia tum alter factor, cui radices  $F_a, F_b, \dots, F_c$  insent, omnes valores contineret contra hyp. Secundo functio pluribus ipso  $f$  valoribus affecta tali aequationi sufficere omnino non potest. Postremo functionis, quae pauciores valores habet, quando aequationi sufficit, omnes valores totidem repetiti inveniri debent, quare laeva pars expressionis coefficientibus symmetricis affectae potentia erit neque irreductibilis.

ART. 9. Sit  $F_1$  functio  $f$  valoribus affecta,  $G_1$  alia functio per nullam substitutionem ipsam  $F_1$  non mutantem valorem mutans, familiam substitutionum ad functionem  $G_1$  pertinentem multiplum familiae ad ipsam  $F_1$  pertinentis ideoque numerum valorum functionis  $G_1$  divisorem ipsius  $f$  esse, facile perspicitur. Constat, functiones  $G_1$  per functionem  $F_1$  rationaliter exprimi posse. Sit enim

$$\psi(F) = 0$$

aequatio  $f$  ipsius  $F_1$  valores quasi radices continens, quae dum elementa  $a$  plane sunt indeterminata radices aequales habere non potest, erit

$$G_1 = \frac{\varphi(F_1)}{\psi'(F_1)} = \frac{\varphi(F_1) \psi'(F_2) \dots \psi'(F_f)}{N(\psi'[F_1])}.$$

Quoniam autem hujus fractionis denominator symmetrica elementorum functio, numerator integra ipsius  $F_1$  et quantitatum  $p_1, p_2, \dots, p_n$  functio est, illam expressionem in hanc redigere licet formam

$$G_1 = \sigma + \sigma_1 F_1 + \sigma_2 F_1^2 + \dots + \sigma_{f-1} \cdot F_1^{f-1}.(g)$$

quod uno tantum modo perfici posse patet. Quia vice versa quaevis functio  $G_1$ , quam in formam illam redigere licet, per nullam substitutionem ipsam  $F_1$  non mutantem valorem mutat, has tantum, quas ipsi  $F_1$  similes vocavimus, ea proprietate affectas esse sequitur. Quarum functiones congruae speciem singularem constituunt.

Jam sit  $\varphi$  functio  $N$  valoribus affecta, quum quaevis functio pauciorum valorum ipsi  $\varphi$  similis, functiones  $N$  valoribus affectae ipsi  $\varphi$  congruae sint, omnes functiones per unam illam exprimere et in formam

$$F_1 = \sigma + \sigma_1 \varphi_1 + \sigma_2 \varphi_1^2 + \dots + \sigma_{N-1} \varphi_1^{N-1}(f)$$

eruere possumus. Qua in forma quantitatibus  $\sigma$  rite et modis quam generalissimo determinatis, prodeunt formae generales pro diversis functionum classibus incongruis.

Posito  $G_1 = g(F_1)$ , determinatis coefficientibus modis quam generalissimo, ut forma illa alias functiones non impliceat nisi  $f$  valoribus affectas, si ipsius  $F$  valorem  $f(\varphi)$  substituis  $G = gf(\varphi)$  functionum ipsi  $F$  congruarum ope functionis  $g$  expressionem generalissimam esse obtinebis. Aequatio autem functionis  $G$ , quoniam, si  $G$  re vera  $f$  valores induit, irreductibilis, aliter expressionis irreductibilis potentia esse debet, coef-

ficientes in  $\mathbf{g}(\mathbf{F})$  ita determinandi sunt, ut hoc evenire non possit.

Data igitur functione  $\mathbf{F}$ , cui aliis valor non exstat nisi  $-\mathbf{F}$ , dato ex. gr. elementorum differentiarum producto, quaevis duobus valoribus affecta functio formam  $\mathbf{G} = \sigma + \sigma_1 \mathbf{F}$  induet, supposito  $\sigma_1$  a cifra diverso. Quod etiam hinc concludendum, quod aequatio

$$y^2 - 2\sigma y + (\sigma^2 - \sigma_1^2 F^2) = 0$$

cui  $\mathbf{G}$  sufficit, quadratum esse non potest. Jam idem sequitur, designante  $\mathbf{F}$  quamvis duobus valoribus affectam functionem.

ART. 10. Ad datam substitutionum familiam  $1, \theta_1, \theta_2, \dots, \theta_{g-1}$  functionem pertinere dicemus invariabilem pro omnibus in illa contentis substitutionibus, variabilem pro quavis alia; sin ultima conditio locum non habet, familiae eam sufficere dicemus. Ad quamvis functionem substitutionum familia inveniri potest, ea scilicet ad quam functio pertinet; vice versa autem semper invenire licet functionem ad datam substitutionum familiam pertinentem. Sint enim  $\varphi_1, \varphi_2, \dots, \varphi_g$  functionis  $N$  valoribus affectae, qui substitutionibus respondent, valores, horum quaevis functio symmetrica familiae sufficiet. Designante autem  $p_1$  mononomium  $a_1^{\alpha_1} a_2^{\alpha_2} \dots a_n^{\alpha_n}$ , in quo omnes exponentes inter se diversi sunt, data functione

$$\mathbf{F}(1) = \varphi(1) + \varphi(\theta_1) + \dots + \varphi(\theta_{g-1})$$

$$\text{erit } \mathbf{F}(\eta) = \varphi(\eta) + \varphi(\eta\theta_1) + \dots + \varphi(\eta\theta_{g-1})$$

valor ipsi  $\mathbf{F}(1)$  aequalis aut ab eo diversus, prout singula monomia inter se consentiunt necne, sive, quod idem est, substitutiones. Quoties igitur substitutiones  $1, \theta_1, \theta_2, \dots, \theta_{g-1}$  familiam constituunt, functio  $\mathbf{F}(1)$  inveniri potest ad eam pertinens; quare idem evadit numerus pro functionum incongruarum classibus, qui pro substitutionum familiis, illarumque investigatione harum recedit.

### III. DE SUBSTITUTIONUM FAMILIIS.

ART. 11. Secundum quod artt. 3, 10 diximus, problema huic dissertationi propositum eo reducitur, ut omnis substitutionum familia et quot contineat substitutiones inveniatur, sive ut, datis substitutionibus  $\theta_1, \theta_2, \dots, \theta_a$ , earum familia determinetur. Quod idem problema est atque hoc: data substitutionum familia  $\theta_1, \theta_2, \dots, \theta_g$ , inveniatur, quomodo numerus terminorum augeatur, assumta nova substitutione  $\theta$ . Cujus problematis generalis casus qui videntur simplicissimi hic proferentes, ab iis substitutionum familiis quae ex una tantum generantur, quas primi ordinis appellabimus, initium faciamus.

ART. 12. Si vero in substitutionum naturam inquiris, quomodo alia ab alia pendeat, hanc primam invenies methodum. Quamvis enim substitutionem  $\theta$  in alias potentiae speciem exprimere licet. Namque sit  $\vartheta$  quaelibet ex omnium systemate, ejus potentiae  $t$  substitutiones procreabunt, quando primum  $\vartheta^t = 1$ . Quod, si pro omnibus reliquis substitutionibus repetis, quaevis substitutio  $\theta$  aut ex ipsarum  $\vartheta$  aut ex earum dignatum erit serie. Substitutiones autem  $\vartheta_1, \vartheta_2, \dots, \vartheta_s$ , ita determinari possunt, ut binarum series non omnes habeant communes terminos, et pro quavis  $\vartheta$  talem etiam potentiam ponere licet, cujus dignitates totam ipsius  $\vartheta$  seriem reproducant. His propositis, illam substitutionum classificationem uno tantum modo perfici posse, facile demonstratur. Si duarum  $\vartheta_1, \vartheta_2$ , series terminos communes implicant, horum numerus communis exponentium, ad quos illae pertinent, divisor esse debet. Substitutiones autem  $\vartheta$  primitivas appellabimus.

ART. 13. Jam vero ill. Cauchy omnem substitutionem in plures cyclicas, quarum diversa quaeque elementa permuat,

dissolvi posse docuit. Quam paullo persequamur dissolutionem.  
Sit primum

$$\theta = (a_1 \ a_2 \ \dots \ a_p) \ (a_{p+1} \ a_{p+2} \ \dots \ a_{p+q}) \ (p, q).$$

Qua in forma si omnes qui esse possunt, cyclos sumis,  
 $p + q = n$  elementis omnimodis in  $p, q$  divisis,

$$\frac{1. 2. 3 \dots n}{p \cdot q}$$

substitutiones continentur. Ipsi autem  $p, q$  modis  $(n + 1)$  valores tribuendo quorum summa =  $n$ , substitutiones contentae in formis  $(p, q), (p', q')$  diversae inter se erunt, nisi  $p' = q$ ,  $q' = p$ . Eodem modo,  $n$  elementa in tres classes dividendo prodeunt

$$\frac{(n + 1) (n + 2)}{1. 2}$$

formae  $(p, q, r)$  simul formas  $(p, q)$  omnes involventes; quarum eas tantum retinebimus, quae substitutiones ab aliarum diversas comparant. Generaliter  $n$  elementa, quum modis

$$\frac{(n + 1) (n + 2) \dots (n + m - 1)}{1. 2. 3 \dots (m - 1)}$$

diversis in  $m$  classes dirimi possint, totidem formae  $(p, q, r, \dots s)$  resultant, et postquam abundantes sublatae sunt, pro quavis restante numerus substitutionum, quas continet, formula

$$\frac{1. 2. 3 \dots (p + q + r + \dots + s)}{p \cdot q \cdot r \dots s}$$

calculatur, quae per  $1. 2. 3 \dots \mu$  etiam dividenda est, quoties  $\mu$  quantitatum  $p, q, r, \dots s$  aequales evadunt. Summa denique omnium pro  $m = n$  hoc modo inventorum numerorum ipsum  $N$  aequare debet, ex. gr. pro  $n = 4$

$$1. 2. 3. 4 = 1. 2. 3. 4 \left( \frac{1}{4} + \frac{1}{1. 3} + \frac{1}{2} \cdot \frac{1}{1. 2. 1. 2} + \frac{1}{2} \cdot \frac{1}{1. 1. 2} + \frac{1}{24} \cdot \frac{1}{1. 1. 1. 1} \right).$$

ART. 14. Haec ill. Cauchy methodus ad inveniendum substitutionum primitivarum systema adhiberi potest. Cujus rei theoria haec est: Sit  $(a_1, a_2, a_3, \dots, a_p)$  cyclus ordinis  $p$ , repetita substitutione cyclica  $r^{ies}$ , novus cyclus secundum illam methodum instructus in plures cyclos distingui potest. Namque  $a_1$  in  $a_{r+1}, a_{r+2}, \dots, a_{2r+1}$  etc. abeunt. Itaque, si  $r$  ad ipsum  $p$  primus est, ad  $a_1$  non prius revertimur, quam omnia elementa obviam venissent; sin habent maximum quendam divisorum  $s$ , quum minimum ipsis commune multiplum sit  $\frac{p}{s} \cdot r$ , unus ille cyclus in  $s$  minores  $\frac{p}{s}$  elementis compositos disjungitur. Quare inter cycli ordinis  $p$  repetitiones sunt  $\varphi(p)$  tantum ejusdem ordinis, ubi  $\varphi(p)$  significatione in numerorum theoria usitata gaudet. Sumto aliorum qui ex iisdem elementis componi possunt cyclorum quodam, alii  $\varphi(p)$  cycli ordinis  $p$  obtinentur a prioribus plane diversi.

ART. 15. Jam primum cyclum  $n$  elementorum consideremus. Secundum articulum praecedentem cyclorum series institui potest

$$c_1(n) \ c_2(n) \ \dots \ c_n(n) \quad (n)$$

ubi

$$\nu = \frac{1 \cdot 2 \cdot 3 \ \dots \ (n-1)}{\varphi(n)},$$

quorum potentiae omnes ordinis  $n$  cyclos continent. Quia neque binorum potentias inter se reducere licet, neque substitutionem concipere nisi ipsam  $n$  elementorum cyclum constituentem, cuius potentiae cyclus ordinis  $n$  gignant, substitutiones  $(n)$  in primitivarum numero ducere possumus. Quarum potentiae quum simul omnes substitutiones implicant, in quibus  $n$  elementorum cyclus in nonnullos totidem elementis compositos disjungitur, (neque ullam aliam) ad illas in sequentibus respiciendum non erit. Dividamus igitur cyclum  $n$  elementorum in duos  $p, q$  elementa continentes; qua substitutione per  $c(p) \ c(q)$  designata  $r^{ies}$  repetita, prodit  $c(p)^r \cdot c(q)^r$ . Sit  $\delta$  maximus ipsis  $p, q$

communis divisor,  $p = p' \delta$ ,  $q = q' \delta$ ,  $\mu = p' q' \delta$ , substitutio ad exponentem  $\mu$  pertinebit. Sed, quia  $r^{\alpha}$  potentia tum solum ejusdem formae substitutionem generabit, quum  $r$  et ad  $p$  et ad  $q$  primus, quod erit, quoties  $r$  ad ipsum  $\mu$  primus et vice versa, inter  $\mu$  dignitates  $\varphi(\mu)$  tantum formam  $c(p)c(q)$  retinebunt.

Deinde  $\frac{1 \cdot 2 \cdot 3 \dots n}{p! q!}$  series instituere licet, quarum  $\frac{(p-1)! (q-1)!}{\varphi(\mu)}$

quaeque substitutiones includit. Hae denuo, quarum potentiae omnes, in quibus cyclus  $n$  elementorum in duos  $p, q$  elementorum disjungitur, substitutiones implicant, inter primitivas quas diximus habendae sunt. Jam satis quomodo pergendum sit, intelligitur.

ART. 16. Quaeritur autem, quoniam criterio substitutio primitiva ab aliis dignosci possit. Primum vero datam substitutionem  $\theta$  ex  $k$  cyclis  $a$  elementorum compositam talis tantum substitutionis potentiam evadere posse, cujus cyclis singulis multiplum  $a$  elementorum insit, facile perspicitur. Posito igitur  $k_1 + k_2 = k$ ,  $\theta_1 = c(k_1 a) c(k_2 a)$ , quoniam ipsius  $\theta_1$  potentia  $x^{\alpha}$  ipsi  $\theta$  aequalis evadere debet,  $c(k_1 a)^x$  in  $k_1$  cyclos  $a$  elementis constantes dirimitur, eritque  $x$  ipsius  $k_1$  multiplum, scilicet  $i_1 k_1$ , ubi  $i_1$  ad  $a$  prima quantitas. Eodem modo  $x = i_1 k_1, i_2, \dots, i_n$  ad  $a$  primus. Deinde substitutionem consideremus  $\theta$  constantem ex  $k$  cyclis  $a$  elementorum, ex  $l$  cyclis  $b$  elementorum, ex  $m$  cyclis  $c$  elementorum etc.; quam talis tantum substitutionis quasi potentiam haberi, cujus forma:

$$c(k_1 a) \dots c(k_\alpha a) c(l_1 b) \dots c(l_\beta b) c(m_1 c) \dots$$

sit, statim concluditur. Quae forma ab ipsius  $\theta$  forma primitiva differet, quando non omnes quantitates  $k_i, l_i, \dots$  unitati aequales. Jam sit illa potentia  $x^{\alpha}$ , conditiones exstant hae:

$$x = i_1 k_1 = i_2 k_2 = \dots = h_1 l_1 = h_2 l_2 = \dots \text{ etc.}$$

quantitates  $i$  ad ipsum  $a$ , quantitates  $h$  ad ipsum  $b$  etc. primae. Quibus conditionibus si sufficere potes, data substitutio in alias

$\theta_1, \theta_2$ , autem independentes esse nec non tanquam primitivas supponi posse, inde patet, quod, posito  $\theta_1 = \vartheta_1^{a_1}, \theta_2 = \vartheta_2^{a_2}$ ,  $F(\theta_1, \theta_2)$  in ipsa  $F(\vartheta_1, \vartheta_2)$  contenta, et quoties primitiva, eidem aequalis esse debet, quam igitur pro illa ponere permisum est.

Inde quid sub familiis tertii sive superiorum ordinum primitivis sit intelligendum videtur. Data igitur familia primitiva  $a^{ti}$  ordinis  $F(\theta_1, \theta_2, \dots, \theta_a)$ , erit  $a^{ti}$  ordinis irreductibilis, quod, quamvis ad oculos sit, ita demonstretur. Supposito enim, usque ad  $(a-1)^{tum}$  ordinem familiam primitivam non dari omnes substitutiones implicantem, sit

$$F(\theta_1, \theta_2, \dots, \theta_a) = F(\eta_1, \eta_2, \dots, \eta_{a-1}),$$

$\theta$  alia in familia non contenta substitutio, illa familia hujus  $F(\eta_1, \eta_2, \dots, \eta_{a-1}, \theta)$ , quae ipso  $a$  majoris ordinis esse non potest, pars erit neque primitiva. Quando autem nulla exstat substitutio  $\theta$ , quum familia data omnes substitutiones contineat, secundum suppositionem nostram ipso  $a$  minoris ordinis primitiva esse non potest. Jam sit  $v^{tus}$  ordo primus omnes substitutiones implicans, ejusdem ordinis unam tantum existere familiam primitivam neque ullam majoris ordinis facile perspicitur.

Quo etiam summum substitutionum independentium in familia quadam contentarum numerum ipsi  $v$  aequalem esse concludimus.

ART. 22. Secundum hanc familiarum primitivarum definitionem proprietatem indicare licet, qua ab omnibus aliis different. Data enim substitutione primitiva, quia in majore primi ordinis familia contenta esse non potest, quaevis familia  $F(\vartheta, \theta)$  secundi ordinis est. Vice versa autem, quoties familia quaelibet  $F(\vartheta, \theta)$  secundi ordinis,  $\vartheta$  primitiva erit substitutio; si enim non esset, daretur familia primi ordinis ipsam  $F(\vartheta)$  amplectens, etiamsi haec quavis cum substitutione conjuncta, se-

cundi ordinis familiam procrearet, quam in alia primi ordinis contineri non posse facile intelligis. Generalius ad familiam  $a^t_i$  ordinis primitivam qualibet assumta substitutione, quoniam familia illa in alia ejusdem ordinis contineri non potest, familia irreductibilis ( $a+1$ ) substitutionibus independentibus affecta oritur. Vice versa autem, quando  $a$  substitutiones generatrices cum qualibet alia substitutione conjunctae ( $a+1$ ) substitutiones independentes producunt, familiam  $a^t_i$  ordinis primitivam constituunt; aliter enim in tali continerentur, quod cum suppositione modo facta convenire non potest.

ART. 23. Quaeritur jam de familiis, quae in alia, veluti  $a^t_i$  ordinis contentae sunt, et quomodo obtineantur, et quales quorumque ordinum esse possint; utrum fieri possit, ut familia  $a^t_i$  ordinis alias majoris contineat, necne. Quae autem quaestio manifesto cum hac convenit, utrum ( $a+1$ ) substitutiones familiam ( $a+1)^t_i$  ordinis generantes independentes esse debeant, necne. Primum vero familiam, nullam ( $a+1)^t_i$  ordinis continentem, familias majorum etiam ordinum a fortiori amplecti non posse elucet. Supposito itaque, in  $a^t_i$  ordinis familia aliam ( $a+1)^t_i$  contentam esse, obtineretur illa adjunctis huic quibusdam substitutionibus  $\theta, \theta', \dots$ . Adjuncta igitur primum ipsa  $\theta$ , postquam familias  $a^t_i$  ordinis in aliis minoris contentas esse non posse supposuimus, quae nascitur familia aut  $a^t_i$  aut majoris erit ordinis; quoties postremum evenit, adjuncta nova substitutione  $\theta'$  denuo familia oritur aut  $a^t_i$  aut majoris ordinis etc., tandem familiam exstare oportet, ipso  $a$  majoris ordinis, quae cum substitutione quadam  $\theta$  conjuncta ad  $a^{tum}$  delabatur, sive etiam fieri debet, ut, substitutione quadam  $\theta$  e familia  $a^t_i$  ordinis exclusa, alia ordinis ipso  $a$  majoris familia obtineatur.

ART. 24. Data igitur sit familia ejusque substitutio  $\theta$ ; quam si ex illa excludis, aliud non agis nisi ut familiam ipsam  $\theta$  non

continentem inquiras, quae cum hacce conjuncta datam familiam producat. Quam quoniam semper in formam

$$\mathbf{F}(\theta_1, \theta_2, \dots, \theta_a, \theta)$$

redigere licet plerumque quidem non irreductibilem attamen talem semper, ut ipsa  $\mathbf{F}(\theta_1, \theta_2, \dots, \theta_a)$  irreductibilis sit, exclusa substitutione  $\theta$ , haecce familia eveniet. Quare nisi tales substitutiones  $\theta_1, \theta_2, \dots, \theta_a$  eligi possunt, quarum ipsa  $\theta$  non sit productum, hancce directe auferre non potes, sed indirecto tantum modo, id est alias excludendo substitutiones, quibus sublatis ipsa etiam  $\theta$  excipiatur. Substitutiones  $\theta_1, \theta_2, \dots, \theta_a$  tales etiam supponere licet, quarum nulla sit productum e ceteris ipsaque  $\theta$  conflatum, namque si veluti  $\theta_1$  inter tales esset, data familia ita etiam designari posset

$$\mathbf{F}(\theta_2, \theta_3, \dots, \theta_a, \theta)$$

et exclusa substitutione  $\theta$  resultaret familia  $\mathbf{F}(\theta_2, \dots, \theta_a)$ . Denique vero semper familiam dari, cui nullam ipsius  $\theta$  potentiam directe detrahere possis, quae vero ipsi  $\theta$  conjuncta datam familiam producat, facile perspicis.

Ex. gr. quibus sub conditionibus  $\mathbf{F}(\theta)$  ipsi  $\mathbf{F}(\theta^a, \theta^b)$  ita exaequari possit ut  $\mathbf{F}(\theta^b)$  substitutionem  $\theta^a$  non contineat, inquiramus. Primum autem  $\theta^{ax} \cdot \theta^{by} = \theta^{ax+by} = \theta$ , id est, si  $\theta$  ad exponentem  $t$  pertinet,  $ax+by \equiv 1 \pmod{t}$  esse debet, quare  $a, b$  inter se primi. Secundo necesse est, ut  $\theta^{bx}$  ab ipsa  $\theta^a$ , sive  $bx$  ab ipso  $a \pmod{t}$  pro omni ipsius  $x$  valore differat, quod quoniam  $a, b$  ipsius  $t$  divisores esse supponere possumus, obtainemus posito  $b > 1$ . Id autem semper fieri potest, nisi  $a$  omnes numeros primos ipsum  $t$  metientes continet. Jam sit  $t = p^\alpha r^\beta \dots q^\kappa s^\sigma \dots$ , ubi  $p, r, \dots$  numeros primos qui ipsum  $a$  metiuntur,  $q, s, \dots$  eos qui non metiuntur, designant, quivis ipsius  $t$  divisor alios nisi  $q, s, \dots$  numeros primos non continens neque ullus aliis ad ipsum  $a$  erit primus.

Qui quum omnes excepta unitate pro ipso  $b$  sumi possint, dantur familiae  $(k+1)(\sigma+1) \dots -1$

$$\mathbf{F}(\theta^a, \theta^b), \mathbf{F}(\theta^a, \theta^{b'}), \dots$$

ipsi  $\mathbf{F}(\theta)$  aequales. Porro, quoties  $\theta^c$  ipsius  $\theta^b$  potentia, manente  $c$  ad ipsum  $a$  primo, erit

$$\mathbf{F}(\theta^a, \theta^c) = \mathbf{F}(\theta^a, \theta^b).$$

ART. 25. Quaestiones has generales, quum difficillimae sint, si ad superiorum ordinum familias progredi vis, in postrem referentes, alias quaestiones particulares quae illis tanquam praeparandis utiles videntur, hic etiam paullo attingamus.

Datis igitur  $\mu$  substitutionibus  $\theta_1, \theta_2, \dots, \theta_\mu$ , quarum diversa quaeque elementa permuat ab aliarum nulla permutata, harum familia, pertinente generaliter  $\theta_i$  ad exponentem  $t_i$ , substitutionum numerum implicabit  $t_1 \cdot t_2 \dots t_\mu$ . Generalius autem, si  $\tau$  minimum ipsis  $t_1, t_2, \dots, t_\mu$  commune multiplum designat, familiae  $\mathbf{F}(\theta_1, \theta_2, \dots, \theta_\mu)$  substitutionum numerus quasi ipsius  $\tau$  multiplum evadit.

Jam sint  $\theta_1, \theta_2$  substitutiones ad exponentes  $t_1, t_2$  resp. pertinentes. Quia semper fieri debet, ut  $\theta_1^{k_1}$  pro ipsius  $k_1$  valore apte electo ipsius  $\theta_2$  potentiae aequalis evadat, neque minus  $\theta_2^{k_2}$  ipsius  $\theta_1$  potentiae; si  $k_1, k_2$  exponentes minimos his conditionibus convenientes designant, semper esse debet  $\frac{t_1}{k_1} = \frac{t_2}{k_2}$ .

Quotiente hoc per  $t$  expresso, familia  $\mathbf{F}(\theta_1, \theta_2)$  omnes  $\frac{t_1 t_2}{t}$  substitutiones diversas continebit hac in forma contentas

$$\theta_2^i \theta_1^k, \quad i < k_2, \quad k < t_1$$

quibuscum aliae formae  $\theta_2^i \theta_1^k$  omnes convenient. Quae ut familiam constituant, et poscitur et sufficiet, ut productum quolibet in eandem formam reducere sive quamvis substitutionem  $\theta_1^a \theta_2^b$  alii hujusmodi  $\theta_2^i \theta_1^k$  aequalem reddere liceat.

Generalius duae substitutionum familiae quarum substitu-

tiones quaslibet per  $\theta, \theta'$  designemus earum autem numerum per  $f, f'$ ; quia familiam ex  $e$  substitutionibus  $\eta$  constitutam communem habebunt, substitutiones  $\theta$  ita

$$\eta, \theta_1\eta, \theta_2\eta, \dots, \theta_{\frac{f}{e}-1}\cdot\eta$$

sive breviter per  $\vartheta\eta$  repraesentari possunt, omnes vero substitutiones  $\theta\theta'$  cum his  $\vartheta\theta'$  conveniunt. Quae  $\frac{ff'}{e}$  substitutiones diversae familiam constituent, quando quaevis  $\theta'\vartheta$  harum  $\vartheta\theta'$  alicui aequivalebit neque ullo alio modo. Semper vero substitutionum numerum ipso  $\frac{ff'}{e}$  majorem esse affirmare licet.

Vice versa autem, data familia aliam continente, cuius membrum generale per  $\theta$  designemus, quamvis substitutionem illius familiae in formam  $\theta'\theta$  sive etiam  $\theta\theta'$  redigere licet. Designante igitur  $\theta_1$  quamvis familiae  $F(\theta')$  substitutionem,  $\eta$  autem omnes huic cum familia  $\theta$  communes, illas omnes in formam  $\theta'\eta$  redigere potes. Quoties itaque  $F(\theta')$ ,  $\theta$  substitutiones communes nisi identicam non implicant, substitutiones  $\theta'$  totam familiam  $F(\theta')$  explent.

ART. 26. Jam semper familiam  $\frac{N}{2}$  substitutionibus affectam inveniri posse constat. Cujus termino generali per  $\theta$  expresso omnes  $N$  substitutiones alteri serierum  $\theta, \eta\theta$  inesse debent, designante  $\eta$  substitutionem quandam ad exponentem parem pertinentem. Idem quoniam de quavis substitutione  $\eta\theta$  affirmare potes, ii omnes, qui ad imparem pertinent exponentem itaque tota familia, cuius substitutiones generatrices omnes  $p^{ti}$  ordinis cycli sunt, designante  $p$  numerum primum imparem, in familia  $\theta$  continentur. Quare si illorum cyclorum familias diversis ipsis  $p$  valoribus respondentes et aequivalentes et  $\frac{N}{2}$  substitutionibus affectas esse demonstraveris, unam tantum exsistere  $\frac{N}{2}$  substitutionum familiam simul probatum erit.

Primum vero, quum omnis tertii ordinis cyclus adhibitis duobus  $p^{ti}$  ordinis cyclis, neque minus quivis  $p^{ti}$  ordinis cyclus

per  $\frac{p-1}{2}$  tertii obtineatur, horum cyclorum familia ut illi, quae omnibus  $p^{ti}$  ordinis cyclis generatur, aequivaleat necesse est, sive etiam omnes hae diversis  $p$  respondentes familiae aequivalebunt.

Secundo autem postquam usque ad certum ipsius  $n$  valorem probatum esse supposuimus, omnium  $p^{ti}$  ordinis cyclorum familiam  $\frac{N}{2}$  substitutionibus affectam esse, pro sequente etiam valore idem valere theorema, id est, continere illam familiam  $\frac{1 \cdot 2 \cdot 3 \dots (n+1)}{2}$  substitutiones, comprobemus. Jam exsistere semper numerum primum inter  $n$  et  $\frac{n+1}{2}$  contentum,  $n \geq 6$ , inde patet, quod Tchebicheff, quoties  $a > 7$ , talem inter  $a$  et  $\frac{a}{2}$  semper inveniri demonstravit. Dato igitur hujusmodi numero  $p$ , cycli  $p^{ti}$  ordinis  $n$  tantum  $(n+1)$  elementorum certis adhibiti  $\frac{N}{2}$  substitutiones familiam constituentes generabunt. Omnium vero cyclorum  $p^{ti}$  ordinis ut familiam obtineas, unam certe substitutionem talem, quam  $c$  appellabimus, adjungere debes; obtinebis igitur profecto  $p \cdot \frac{N}{2}$  substitutiones diversas

$$\theta, c\theta, c^2\theta, \dots, c^{p-1}\theta.$$

Jam, quoniam  $p \cdot \frac{N}{2} > \frac{(n+1)}{2} \cdot \frac{N}{2}$ , illaque familia in alia  $(n+1)\frac{N}{2}$  substitutionibus affecta contineri debet, cum illa identicam eam esse concluditur. Quod theorema, quum pro ipsius  $n$  valoribus 3, 4, 5 facile verificetur, jam generaliter probatum est.

Nullam dari familiam  $\frac{N}{a}$  substitutionibus constitutam, ipso  $a$  contento inter 2 et numerum primum  $p$  maximum infra  $n$  datum, statim sequitur. Quae enim familia quum unum certe  $p^{ti}$  ordinis cyclum  $c$  non contineret,  $p \cdot \frac{N}{a}$  substitutiones diverse darentur, quod fieri non potest.

ART. 27. Jam utile esse potest scire, quot substitutiones ad alias omnes generandas necessariae sint, sive cuius ordinis  $\nu$  sit familia principalis omnes substitutiones implicans. Primum vero facile limitem indicere licet, quem numerus  $\nu$  excedere non

potest. Designentur enim per  $\gamma_n, \gamma_{n-1}, \dots, \gamma_3, \gamma_2$  substitutiones cycliae ordinum  $n, n-1, \dots, 3, 2$ , resp., ubi generaliter substitutio  $\gamma_i$  eorum, quibus  $\gamma_{i+1}$  adhibetur, elementorum  $i$  permuat, omnem substitutionem in formam sequentem redigi posse

$$\gamma_n^\alpha \gamma_{n-1}^\beta \dots \gamma_3^\rho \gamma_2^\sigma,$$

et his expressionibus, si exponentibus omnes qui locum habere possunt valores tribuuntur, totam substitutionum multitudinem implicari haud difficile perspicitur. Quo numerum  $\nu$  ipso  $n-1$  majorem esse non posse concludimus. Idem inde sequitur, quod omnes  $N$  substitutiones obtinentur datis omnibus transpositionibus, hae autem per  $n-1$  sequentes

$$(1, 2) \ (1, 3) \ \dots \ (1, n).$$

ART. 28. Jam, quibus sub conditionibus duarum substitutionum ejusdem ordinis cyclicarum  $\eta, \theta$  familiae praeter identicam alias etiam substitutiones communes habeant inquiramus. Quod quum fieri nequeat, quoties  $n$  numerus primus, contrarium casum locum habere supponimus. Posito igitur  $\eta^l = \theta^k$ , quia ex. gr.  $k$  semper ipsius  $n$  divisor haberi potest,  $l = ik$  esse debere facile invenitur,  $i$  quantitate ad  $\frac{n}{k}$  prima. Tum substitutionis  $\eta$  loco talis poni potest potentia  $\eta^r$ , ubi  $r$  ad ipsum  $n$  prima quantitas, ut ejus potentia  $k^{ta}$  ipsi  $\theta^k$  aequalis evadat. Namque necesse est, quantitatem  $r$  ad  $n$  primam talem eligere, ut

$$rk \equiv ik \pmod{n} \text{ sive } r \equiv i \pmod{\frac{n}{k}}$$

id est  $r = i + z \cdot \frac{k}{n}$ ;  $z$  autem semper ita determinare licet, ut expressio illa jam ad ipsum  $\frac{n}{k}$  prima divisorem cum ipso  $k$  communem non habeat. Quare ab initio substitutionem aequationi  $\eta^k = \theta^k$  satisfacere supponi potest. Quum autem  $\theta^k$  in  $k$  cyclos disjungatur  $c_1, c_2, \dots, c_k$ ,  $\eta^k$  in eosdem disjungi debet alio ordine instructos, quaecunque autem horum permutatio substitutionem  $\eta$  conditionibus satisfacentem praebebit. Quarum numerus producto  $1. 2. 3. \dots. k$  major esse non potest.

Jam sit  $n = 4$ ; quia neque  $k$  alii quantitati atque 2 aequalis esse potest, neque ipso 1. 2. 3 pauciores quarti ordinis cycli, eorum autem tres familiae inveniuntur, duo cycli quorum familiae nisi identicam substitutiones communes non habeant, eligi possunt. Qui profecto 4. 4 substitutiones itaque omnes generabunt. Hic omnibus ipsius  $N$  divisoribus familiae respondent, quarum ordinem vel primum vel secundum esse elucet.

ART. 29. Porro sit  $n = 5$ , simili modo ordinem familiae  $\frac{N}{2}$  substitutiones continentis invenire licet. Namque duorum quinti ordinis cyclorum  $\theta_1, \theta_2$  familia, quia nullam praeter identicam substitutionem communem generant, certe 25 continebit terminos. Quae si ab illa differret, cyclum quendam quinti ordinis  $\theta_3$  non implicaret, familia igitur  $F(\theta_1, \theta_2, \theta_3)$  125 minimum substitutionibus constaret, id quod fieri nequit. Quare  $\frac{N}{2}$  substitutionum familia secundi erit ordinis. Obtinemus eam etiam, sumtis cyclo tertii ordinis, alioque quinti; horum enim familia, nisi illam aequaret, cyclum denuo quinti ordinis non contineret, quo adjuncto familia deinde orta certe 5. 15 substitutiones implicans in illa  $\frac{N}{2} = 60$  substitutionibus constituta contineretur, quod absurdum est. Jam sit  $c_s$  transpositio hac in familia non inventa, cyclus tertii ordinis  $c_s$  elementa ab ea non permutata continens in eadem invenitur familia; designante igitur  $c_s$  quinti ordinis cyclum, familia  $F(c_s, c_s, c_s)$  principali aequivalet. Quum autem haec:  $F(c_s, c_s, c_s)$  substitutiones  $c_s, c_s, c_s$  generet, illi aequivalebit, sive etiam familia principalis secundi erit ordinis.

ART. 30. Designante  $p$  numerum primum maximum infra  $n$  datum,  $k$  autem minimum numerum talem ut  $p^k > \frac{N}{4}$ , ordo familiae  $\frac{N}{2}$  substitutionibus constitutae  $k^{tum}$  excedere non potest. Erit autem generaliter minor. Posito enim ex. gr.  $n = p$ ; denotantibus  $\theta_1, \theta_2, \dots, p^{ti}$  ordinis cyclos, substitutionum numerus

familiae horum quosdam neque alias substitutiones quasi generatrices continentis ipsius  $p$  multiplum, divisor autem numeri  $\frac{1}{2} \cdot 1 \cdot 2 \cdot 3 \dots p$  esse debet. Sumtis vero numeris  $d_0, d_1, d_2, \dots d_i$ , quorum generaliter  $d_r$  proximum ipso  $d_{r-1} \cdot p$  majorem numeri  $\frac{1}{2} \cdot 1 \cdot 2 \dots (p-1)$  divisorem,  $d_0$  unitatem designet; supposito esse  $i$  minimum valorem harum conditionum

$$d_{i-1} \cdot p > \frac{1}{4} \cdot 1 \cdot 2 \dots p, \quad d_i \cdot p > \frac{1}{2} \cdot 1 \cdot 2 \dots p$$

alteri satisfacientem, familiae de qua agimus ordo  $i^{tum}$  certe superare non potest,  $i$  generaliter ipso  $k$  minore; ex. gr. pro  $n = 7$  inveniuntur  $k = 4, i = 3$ .

ART. 31. Antequam hanc dissertationem finimus, de methodo etiam, qua substitutiones functionibus exprimuntur, ab ill. Galois, ni fallor, primo in analysin introducta, nostro autem tempore cl. Mathieu aliisque usitata quasdam observationes afferramus. Data enim substitutione

$$\theta = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ r_1 & r_2 & r_3 & \dots & r_n \end{pmatrix},$$

si binos indices  $r, s$  secundum modulum  $n$  congruos identicos haberi convenimus, indices quilibet  $i, r_i$  in substitutione respondentes certo modo aliis ab alio pendebunt; quare, posito  $r_i \equiv f(i)$  (mod.  $n$ ), substitutionem per symbolum  $\theta = (i, f[i])$  reprezentare possumus. Quod, ut re vera substitutionem exprimat, valores  $f(1), f(2), \dots, f(n)$  numeri integri secundum  $n$  incongrui esse debent; vice versa, hac conditione soluta, symbolum  $(i, f[i])$  certe substitutionem quandam repreäsentabit. Post ipsam  $\theta$  si aliam adhibes substitutionem

$$\eta = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ s_1 & s_2 & s_3 & \dots & s_n \end{pmatrix},$$

obtinebis  $\theta\eta = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ r_{s_1} & r_{s_2} & r_{s_3} & \dots & r_{s_n} \end{pmatrix}$

quod, posito  $s_i \equiv f'(i)$  itaque  $r_{s_i} \equiv f(s_i) \equiv ff'(i)$ , per  $\theta\eta =$

$(i, ff'[i])$  exprimere potes. Quare  $\theta^k = (i, f^k[i])$ ; pertinente autem  $\theta$  ad exponentem  $t$ , pro quovis ipsius  $i$  valore integro erit  $f^t(i) \equiv i$ . Designante  $f, f', \dots$  quasvis substitutionibus convenientes functiones,  $ff' \dots$  quoque tali conveniet, et vice versa; contra harum functionum quadam nulli substitutioni conveniente, neque productum ulli adaequatum esse potest.

Secundum has observationes omnia, quae de ipsarum  $\theta$  familiis diximus, sine ambagibus ipsis  $f$  applicare, sive posito  $\theta = (i, \theta[i])$ , supra ubique sub signo  $\theta$  functionem intelligere licet.

Ponamus igitur ex. gr.  $\theta(i) \equiv ai + b$  (mod.  $n$ ), designante jam  $n$  numerum primum; quoniam  $a$  valorem a cifra diversum habere debet,  $n$  residua incongruis ipsius  $i$  valoribus respondentia inter se differunt. Quare omnes hujusmodi functiones  $n(n-1)$ , quia residua pro diversis quidem functionibus, eodem autem ipsius  $i$  valore diversa sunt, eidem substitutionum diversarum numero adtinebunt. Quae (sec. art. 25) familiam constituentes ex. gr. generatricibus  $\theta'(i) \equiv ai$ , designante  $a$  radicem primitivam, et  $\theta''(i) \equiv i + 1$  obtinentur; familia autem, quia

$$\theta^k(i) \equiv a^k i + \frac{a^k - 1}{a - 1} b$$

itaque, nisi  $a \equiv 1$ , profecto  $\theta^{n-1}(i) \equiv i$  erit, una ejus substitutionum generari non potest, itaque secundi erit ordinis.

ART. 32. Attamen nescio, an haec methodus ad difficultates problematum quae in theoria nostra occurrunt, vincendas commoda sit. Namque et functionem mathematicam cuicunque substitutioni respondentem inveniri posse demonstratione egere, et ipsa functionum determinatio tam substitutionibus quam maxime familiis convenientium summae difficultati obnoxia esse mihi videtur. Generalissimum vero est supponere,  $\theta(i)$  impli- cate ipsi  $i$  conjunctum esse congruentia

$$V(i, \theta[i]) \equiv 0 \text{ (mod. } n\text{)}$$

quam si algebraicam supponimus, in formam

$$U_0 z^\alpha + U_1 z^{\alpha-1} + \dots + U_{\alpha-1} z + U_\alpha \equiv 0$$

ubi  $z$  pro  $\theta(i)$  positum, coefficientes  $U$  autem functiones ipsius  $i$  integrae sunt, redigere licet. Haec congruentia generalis, quoniam et  $\alpha$  et ipsius  $i$  exponentem maximum in quovis coefficiente  $U$  ipso  $\varphi(n)$  majorem non esse supponere licet, hanc alteram induit formam:

$$\sum_{r=0}^{\varphi(n)} \left( a_{\varphi(n)}^{(r)} i^{\varphi(n)} + \dots + a_1^{(r)} i + a_0^{(r)} \right) z^r \equiv 0,$$

in qua quantitates  $a$  tales eligendae sunt, ut

1) habente  $i$  valorem datum, unus ipsius  $z$  valor integer evadat neque plures, 2) percurrente  $i$  seriem quantitatum 1, 2, ...,  $n$ ,  $z$  eandem quodam ordine seriem percurrat, sive etiam binae congruentiae diversis ipsius  $i$  valoribus respondentes et ipsi  $z$  diversos suppeditent valores. His solutis conditionibus exstat substitutio  $(i, z)$ . Inveniri autem debent tot ipsorum  $a$  valorum systemata, quot substitutiones habentur.

Quod ut exemplo etiam explicetur, simplicissimum casum  $n = 3$  consideremus. Quum autem congruentia

$$c_2 z^2 + c_1 z + c \equiv 0$$

modulo numero primo  $n$ , vel duas vel omnino nullam habeat radicem, congruentia in simpliciorem hanc recedit pro  $n = 3$

$$(a_2 i^2 + a_1 i + a) z \equiv a'_2 i^2 + a'_1 i + a'$$

quae, quoniam duobus ipsius  $i$  valoribus diversi ipsius  $z$  valores respondere debent, et ipsius  $i$  respectu linearis supponenda est, sive erit

$$(a_1 i + a) z \equiv a'_1 i + a'.$$

Deinde propter conditionem 1)  $a_1 i + a$  pro quovis ipsius  $i$  valore a cifra differre, sive etiam  $a_1 \equiv 0$ ,  $a$  vero a zero diversum esse debet. Quare posito  $a \equiv 1$ , congruentia in hanc recedit

$$z \equiv a_1 i + a \pmod{3}$$

qua, positis pro  $a_1$ ,  $a$  omnibus praeter hunc  $a_1 \equiv 0$  valoribus, omnes substitutiones pro hocce casu continentur.

## VITA.

---

Natus sum Paulus Gustavus Henricus Bachmann Berolinensis die XXII. mensis Junii anno MDCCCXXXVII, patre Friderico Joanne e regiis consiliariis ecclesiasticis, matre autem Julia e gente Lieder, quibus adhuc viventibus laetor. Fidem autem evangelicam profiteor. Quum septem annos natus essem, a parentibus viro Cl. Ranke in disciplinam traditus, primum classes praevias dein gymnasium Friderico-Guilelmum usque ad mensem Martis MDCCCLV frequentavi. Tum maturitatis testimonio instructus, postquam ad confirmandam valetudinem tempus aestivum in Helvetia transeggi, civibus academicis universitatis Fridericae Guilelmae Berolinensis a Rectore ill. Mitscherlich adscriptus nomen Decano ill. Dove apud facultatem philosophicam professus sum. Anno sequente Gottingiam me contuli, ubi rectore ill. Waitz philosophiae studiosis adscriptus scholis interfui pre omnibus Maximi Dirichlet, tum ill. ill. Weber, Woehler, Lotze, Riemann, Dedekind. Berolinum reversus, Rectore ill. Rudorff Decano ill. Kummer in civium academicorum numerum receptus sum. Scholas autem frequentavi Berolini Cel. Cel. Kummer, Encke, Magnus, Dove, Rose, Trendelenburg, Weierstrass, Poggendorff, Borchardt, Arndt.

Quibus omnibus viris optime de me meritis gratias semper quam maximas agam, neque minores praceptor carissimo ill. Schellbach, cuius institutione matheseos scientiae adductum me esse profiteor.

---

# THESES.

---

1. Qui quantitates infinitas in numerorum theoriam introduxerit,  
magnum quid fecisse.
  2. Simplices proportiones arithmeticas solam consonantiarum  
causam esse affirmatur.
  3. Jure nondum poscitur, ut vibrationes longitudinales in opticen  
admittantur.
  4. In tradenda mechanica ab aequilibritatis scientia initium  
faciendum esse.
-