JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

PAUL BACHMANN

Sur la théorie des substitutions, thèse dédiée à M. Édouard Kummer

Journal de mathématiques pures et appliquées 2^e série, tome 10 (1865), p. 209-233.
<http://www.numdam.org/item?id=JMPA_1865_2_10__209_0>

SUR

LA THÉORIE DES SUBSTITUTIONS,

THÈSE DÉDIÉE A M. ÉDOUARD KUMMER;

PAR M. PAUL BACHMANN [*].

Disquisitiones ad determinandum valorum numerum spectantes, quos functio n elementis composita elementorum permutatione induere potest, a generali quæstionis solutione longe adhuc absunt. Facile enim nonnulla theoremata generalia demonstrata sunt, ut illud, esse valorum numerum producti $\mathrm{N} = 1.2.3...n$ 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 quærenda, ut methodi, quas adhibitas esse novi, a generalitate absint et omnia, quorum solutio attacta sit, problemata singularibus considerationibus solvi debuerint, quæsivi, num modo directo tractatum problema ad methodum quandam generaliorem perducere possit. Quamvis difficillimum 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 quædam continentem;

Secundam, quæ de functionum m valorem formis generalibus theoremata nonnulla admonet;

Tertiam de substitutionum proprietatibus agentem.

---

[*] DE SUBSTITUTIONUM THEORIA MEDITATIONES QUÆDAM. — Dissertatio inauguralis, quam consensu et auctoritate amplissimi philosophorum ordinis in alma litterarum Uuiversitate Friderica Guilelma, ad summos in Philosophia honores rite capessendos, die XXIV. M. Martii A. MDCCCLXII. H. L. Q. S. publice defendet auctor *Paulus Bachmann*. — Berolini, typis Gustavi Schade.

I.

ART. 1. — Jam primum videamus, in quo problema generale consistat. Dato autem numero contento in serie 1, 2, 3,..., N, hæ quæstiones occurrunt :

Danturne functiones quarum numerus valorum æquet ipsum f? Quando vero exstant, quæ est forma earum generalis?

Quas igitur persequentes ad solas functiones algebraicas rationales integras respicimus, quippe quæ maximum in Algebra usum habeant atque emolumentum. Hæ omnes additione efficiuntur et multiplicatione; quibus operationibus evolutis, prodit aggregatum mononomiorum cum coefficientibus ab elementis non pendentibus; quare forma functionum generalis hæc erit $\Sigma c.\mathrm{M}$.

Quodcunque autem mononomium formam induit

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

ubi exponentium nonnulli cifræ æquales esse possunt. Habeant ipsorum m_1 valorem eundem, alii m_2 alium,..., denique m_k reliqui alium valorem, ut sit

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

quæ, si ipsis k, m_1, m_2,..., m_k omnes qui locum habere possunt valores tribuis, generalissima suppositio est, valorum numerus æquabit

$$\frac{1.2.3\dots n}{m_1!\, m_2! \dots m_k!}$$

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

ART. 2. — n elementa a_1, a_2,..., a_n modis N diversis permutari sive in ordinem redigi possunt. Si in cujusvis permutationis locum aliam permutationem substituis, substitutionem efficis, quas generaliter per θ, η,..., designabimus. Constituentibus autem elementis functionem, substitutiones plane ab eis independentes erunt neque

determinatæ, nisi permutatio quædam cui applicandæ sint datur [*]. Quoties substitutiones θ, η,..., successive adhibentur, operationem inde ortam per productum $\theta.\eta...$ repræsentabimus, 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 θ, quoniam pluries repetita certe identicam denique substitutionem generabit, ad exponentem quendam t pertinebit, sive erit t minimus exponens talis ut $\theta^t = 1$.

ART. 3. — Quærentem autem, quidnam methodi adhuc adhibitæ commune habeant, fugere non potest, earum quasi principium hoc esse : Datis substitutionibus θ_1, θ_2,..., et functione pro illis invariabili, inveniantur substitutiones et earum numerus, quæ functionis valorem non mutent.

Quæ nobis etiam quæstio fundamentalis erit. Quoniam vero, si substitutiones tales, quarum productum aliquod ex iisdem alicui æquale fiat, familiam (eine Gruppe) constituere dicimus, substitutiones quæsitæ aliæ non sunt nisi familia ex ipsis θ_1, θ_2,..., genita, quæstio illa in hanc recedit, ut datis quibusdam substitutionibus familia ex iis genita inveniatur.

ART. 4. — Valent autem de familiis nota hæc theoremata :

1° Quælibet familia substitutionem identicam et, si substitutionem θ, omnes etiam ejusdem potentias includit.

2° Data familia $\theta_1, \theta_2, \ldots, \theta_m$, designante θ quamvis familiæ substitutionem, producta

$$\theta_1\theta,\ \theta_2\theta,\ldots,\ \theta_m\theta,$$

sive etiam

$$\theta\theta_1,\ \theta\theta_2,\ldots,\ \theta\theta_m$$

---

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

totam familiam reproducunt. Sit vero η alia substitutio, producta

$$\eta\theta_1,\ \eta\theta_2,\ldots,\ \eta\theta_m$$

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 ipsæ familiam constituunt, earum numerus ipsarum g, g' divisor erit.

II.

DE FUNCTIONUM FORMIS.

ART. 5. — Elementa $a_1, a_2,\ldots, a_n$, quibus functiones componuntur, semper radices æquationis

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

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

Tum sint functiones quælibet 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, quæ æque 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 $\theta_1, \theta_2,\ldots, \theta_g$ familiam; data functione quadam sit f valorum numerus, quos per illas substitutiones induit, g_1 substitutionum, per quas immutata manet, numerus. Quæ 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 quæ per substitutionem θ non mutantur forma institui potest. Sit enim M (1) mononomium quodlibet functionis :

$$\Sigma c.\mathrm{M}(a_1, a_2, \ldots, a_n),$$

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

$$\text{cyc. M}(\theta^r) = \mathrm{M}(1) + \mathrm{M}(\theta) + \mathrm{M}(\theta^2) + \ldots + \mathrm{M}(\theta^{\tau-1})$$

$\mathrm{M}(\theta^i)$ valorem mononomii M (1) facta substitutione θ^i, facile intelligitur adæquatam functioni immutatæ conditionem esse, ut formam Σc. cyc. $\mathrm{M}(\theta^r)$ induat, ubi c coefficientem numericum, aut, si non omnia elementa permutantur, eorum quæ 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 $\sigma(a_1, a_2, .., a_n)$ designabimus. Quæ quum congruæ sint, primam classem constituunt aliasque omnes excludunt.

Art. 7. — Data functione F, f valoribus affecta, qui per $\mathrm{F}_1, \mathrm{F}_2, \ldots, \mathrm{F}_f$ repræsententur, functionem φ cogitemus hos valores quasi elementa continentem. Quorum elementorum permutationes quæ esse possunt $1.2.3 \ldots f$ generaliter non omnes permutando ipsa a produci possunt. Quare, si functio φ ipsorum F respectu symmetrica est, erit etiam ipsorum a respectu, de asymmetria autem quantitatum F illam quantitatum a concludere non licet. Sint vero m elementorum a functiones $\mathrm{F}_1, \mathrm{F}_2, \ldots, \mathrm{F}_m$, habente æquatione 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

$$\Pi(z - \mathrm{F}) = (z - \mathrm{F}_1)(z - \mathrm{F}_2) \ldots (z - \mathrm{F}_f),$$

æquationem illam hoc modo scribi posse

$$\Pi(z - \mathrm{F})^k = 0.$$

statim sequitur; uti etiam, si F_1, F_2,..., F_f quidam functionis valores diversi et æquationis, cujus radices sint, coefficientes symmetrici, illos omnes functionis valores esse, concludendum erit.

ART. 8. — Omnium functionum f formis affectarum indicium eo inveniri potest, ut æquationi irreductibili f^{ti} gradus sufficiant, sive ad æquationem f^{ti} gradus cum coefficientibus ipsorum a respectu symmetricis pertineant. Primo enim æquatio in duos factores disjungi nequit, quorum coefficientes symmetrici sint, quia tum alter factor, cui radices F_a, F_b,..., F_c inessent, omnes valores contineret contra hyp. Secundo functio pluribus ipso f valoribus affecta tali æquationi sufficere omnino non potest. Postremo functionis, quæ pauciores valores habet, quando æquationi sufficit, omnes valores totidem repetiti inveniri debent, quare læva pars expressionis coefficientibus symmetricis affectæ 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 familiæ 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

$$\psi(F) = 0$$

æquatio f ipsius F_1 valores quasi radices continens, quæ dum elementa a plane sunt indeterminata radices æquales habere non potest, erit

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

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

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

quod uno tantum modo perfici posse patet. Quia vice versa quævis

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 congruæ spêciem singularem constituunt.

Jam sit φ functio N valoribus affecta, quum quævis functio pauciorum valorum ipsi φ similis, functiones N valoribus affectæ ipsi φ congruæ sint, omnes functiones per unam illam exprimere et in formam

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

eruere possumus. Qua in forma quantitatibus σ rite et modo quam generalissimo determinatis, prodeunt formæ generales pro diversis functionum classibus incongruis.

Posito $G_1 = g(F_1)$, determinatis coefficientibus modo quam generalissimo, ut forma illa alias functiones non implicet nisi f valoribus affectas, si ipsius F valorem $f(\varphi)$ substituis, $G = gf(\varphi)$ functionum ipsi F congruarum ope functionis φ expressionem generalissimam esse obtinebis. Æquatio autem functionis G, quoniam, si G re vera f valores induit, irreductibilis, aliter expressionis irreductibilis potentia esse debet, coefficientes in $g(F)$ ita determinandi sunt, ut hoc evenire non possit.

Data igitur functione F, cui alius valor non exstat nisi — F, dato ex. gr. elementorum differentiarum producto, quævis duobus valoribus affecta functio formam $G = \sigma + \sigma_1 F$ induet, supposito σ_1 a cifra diverso. Quod etiam hinc concludendum, quod æquatio

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

cui G sufficit, quadratum esse non potest. Jam idem sequitur, designante F quamvis duobus valoribus affectam functionem.

ART. **10**. — Ad datam substitutionum familiam 1, θ_1, θ_2,..., θ_{g-1} functionem pertinere dicemus invariabilem pro omnibus in illa contentis substitutionibus, variabilem pro quavis alia; sin ultima conditio locum non habet, familiæ 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 φ_1, φ_2,..., φ_g functionis N valoribus affectæ, qui substitutionibus respondent, valores, horum quævis functio symmetrica familiæ sufficiet. Designante autem φ_1 mononomium $a_1^{\alpha_1} a_2^{\alpha_2} \ldots a_n^{\alpha_n}$, in quo omnes exponentes inter se diversi sunt, data functione

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

erit

$$F(\eta) = \varphi(\eta) + \varphi(\eta\theta_1) + \ldots + \varphi(\eta\theta_{g-1})$$

valor ipsi F(1) æqualis aut ab eo diversus, prout singula mononomia inter se consentiunt necne, sive, quod idem est, substitutiones. Quoties igitur substitutiones 1, θ_1, θ_2,..., θ_{g-1} familiam constituunt, functio F(1) inveniri potest ad eam pertinens; quare idem evadit numerus pro functionum incongruarum classibus, qui pro substitutionum familiis, illarumque investigatio in harum recedit.

III.

DE SUBSTITUTIONUM FAMILIIS.

ART. **11**. — Secundum quod art. **3**, **10** diximus, problema huic dissertationi propositum eo reducitur, ut omnis substitutionum familia et quot contineat substitutiones inveniatur, sive ut, datis substitutionibus θ_1, θ_2,..., θ_a, earum familia determinetur. Quod idem problema est atque hoc : data substitutionum familia θ_1, θ_2,..., θ_g, inveniatur, quomodo numerus terminorum augeatur, assumta nova substitutione θ. Cujus problematis generalis casus qui videntur simplicissimi hic proferentes, ab iis substitutionum familiis quæ 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 θ in alius potentiæ speciem exprimere licet. Namque sit ϑ quælibet ex omnium systemate, ejus potentiæ t substitutiones procreabunt, quando primum $\vartheta^t = 1$. Quod, si pro omnibus reliquis substitutionibus repetis, quævis substitutio θ aut ex ipsarum ϑ aut ex earum dignitatum erit serie. Substitutiones autem ϑ_1, ϑ_2,..., ϑ_ν ita

determinari possunt, ut binarum series non omnes habeant communes terminos, et pro quavis ϑ talem etiam potentiam ponere licet, cujus dignitates totam ipsius ϑ seriem reproducant. His propositis, illam substitutionum classificationem uno tantum modo perfici posse, facile demonstratur. Si duarum ϑ_1, ϑ_2 series terminos communes implicant, horum numerus communis exponentium, ad quos illæ pertinent, divisor esse debet. Substitutiones autem ϑ primitivas appellabimus.

ART. **13**. — Jam vero ill. Cauchy omnem substitutionem in plures cyclicas, quarum diversa quæque elementa permutat, dissolvi posse docuit. Quam paullo persequamur dissolutionem. Sit primum

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

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

$$\frac{1.2.3 \ldots n}{p \cdot q}$$

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

$$\frac{(n+1)(n+2)}{1.2}$$

formæ (p, q, r) simul formas (p, q) omnes involventes; quarum eas tantum retinebimus, quæ substitutiones ad aliarum diversas comparant. Generaliter n elementa, quum modis

$$\frac{(n+1)(n+2)\ldots(n+m-1)}{1.2.3\ldots(m-1)}$$

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

$$\frac{1.2.3\ldots(p+q+r+\ldots+s)}{p.q.r\ldots s}$$

calculatur, quæ per 1, 2, 3,..., μ etiam dividenda est, quoties μ quantitatum p, q, r,..., s æquales evadunt. Summa denique omnium pro $m = n$ hoc modo inventorum numerorum ipsum N æquare 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. — Hæc ill. Cauchy methodus ad inveniendum substitutionum primitivarum systema adhiberi potest. Cujus rei theoria hæc est : Sit $(a_1, a_2, a_3, \ldots, a_p)$ 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+1} in 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 divisorem 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 præcedentem cyclorum series institui potest

$$c_1(n)\, c_2(n) \ldots c_\nu(n) \qquad (n)$$

ubi

$$\nu = \frac{1.2.3\ldots(n-1)}{\varphi(n)},$$

quorum potentiæ omnes ordinis n cyclos continent. Quia neque binorum potentias inter se reducere licet, neque substitutionem concipere nisi ipsam n elementorum cyclum constituentem, cujus potentiæ cyclum ordinis n gignant, substitutiones (n) in primitivarum numero ducere possumus. Quarum potentiæ quum simul omnes substitutiones implicent, 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 $c(p)^r.\,c(q)^r$. Sit δ maximus ipsis p, q communis divisor, $p = p'\delta$, $q = q'\delta$, $\mu = p'q'\delta$, substitutio ad exponentem μ pertinebit. Sed, quia r^{ta} potentia tum solum ejusdem formæ substitutionem generabit, quum r et ad p et ad q primus, quod erit, quoties r ad ipsum μ primus et vice versa, inter μ dignitates $\varphi(\mu)$ tantum formam $c(p)\,c(q)$ retinebunt. Deinde $\frac{1.2.3\ldots n}{p!\,q!}$ series instituere licet, quarum $\frac{(p-1)!\,(q-1)!}{\varphi(\mu)}$ quæque substitutiones includit. Hæ denuo, quarum potentiæ omnes, in quibus cyclus n elementorum in duos p, q elementorum disjungitur, substitutiones implicant, inter primitivas quas diximus habendæ sunt. Jam satis quomodo pergendum sit, intelligitur.

ART. **16.** — Quæritur autem, quonam criterio substitutio primitiva ab aliis dignosci possit. Primum vero datam substitutionem θ et 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 θ_1 potentia x^{ta} ipsi θ æqualis 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 $x = i_2 k_2$, i_2 ad a primus. Deinde substitutionem consideremus θ 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

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

sit, statim concluditur. Quæ forma ab ipsius θ forma primitiva differet, quando non omnes quantitates k_i, l_i,..., unitati æquales. Jam sit illa potentia x^{ta}, conditiones exstant hæ:

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

quantitates i ad ipsum a, quantitates h ad ipsum b, etc., primæ. Quibus conditionibus si sufficere potes, data substitutio in alius potentiæ speciem exprimitur, neque primitiva est. Hæ autem illarum æquationum resolutionem non admittunt.

Designante $\mathfrak{s}$ quamvis substitutionem primitivam, $\mathrm{F}(\theta_1, \theta_2, \ldots, \theta_a)$ autem substitutionum $\theta_1, \theta_2, \ldots, \theta_a$ familiam, symbolum $\mathrm{F}(\mathfrak{s}^k)$ omnis primi ordinis familiæ locum obtinet. Exponentis t autem, ad quem $\mathfrak{s}$ pertinet, omnes divisores ad exprimendum substitutionum in primi ordinis familia contentarum numerum idonei sunt.

ART. **17**. — Ubi autem omnes qui esse possunt numeros diversis primi ordinis substitutionum familiis respondentes invenisse satis est, ut primitivæ substitutiones notæ sint, non poscitur. Namque si substitutio θ art. præc. ad exponentem μ pertinet, erit μ minimum ipsis a, b, $c, \ldots$, commune multiplum, atque exponentis μ', cui $\theta' = c(ka)c(lb)\ldots$ pertinet, divisor. Sed in posteriore substitutione binos cyclos diversum elementorum numerum includere supponi potest. Tum, quoniam familia $\mathrm{F}(\theta')$, quoties μ' divisorem quendam continet, familiam ei respondentem includet neque ullam aliam, ut omnes quæsiti numeri inveniantur, omnes quantitates μ, quæ ipsius n in summandos inæquales discerptionibus respondeant, inveniendas earumque divisores eruendos esse patet.

ART. **18**. — Transeuntes jam ad superiorum ordinum familias, notiones quasdam generales introducamus, quæ ad problematis reductionem servire possint. Substitutiones enim $\theta_1, \theta_2, \ldots, \theta_a$ quarum familiam inquirimus, generatrices appellabimus. Quarum familia, quoniam generaliter ex aliis etiam substitutionibus in ea contentis generatricibus produci poterit, eas quæ simplicissimam videntur præbere speciem, inquirere convenit. Primum igitur substitutiones $\theta_1, \theta_2, \ldots, \theta_a$ ita reducere licet, ut nulla tanquam ceterarum productum haberi possit. Deinde autem inter omnes familiam generandi modos eos eligamus, quorum numerus substitutionum generatricum quam minimus evadat, ita ut minor substitutionum numerus, in quarum producta substitutiones illæ generatrices exprimantur, in data familia inveniri non possit. Quæ in eam formam redacta $\mathrm{F}(\theta_1, \theta_2, \ldots, \theta_a)$ secundum substitu-

tionum generantium $\theta_1, \theta_2, \ldots, \theta_a$ numerum familia a^{ti} ordinis irreductibilis appellabitur.

ART. **19.** — Duo substitutionum complexus

$$\theta_1, \theta_2, \ldots, \theta_a, \quad \eta_1, \eta_2, \ldots, \eta_b$$

æquivalentes dicemus, quando eandem substitutionum familiam generant, sive, quoties illius complexus substitutiones in hujus familia sunt contentæ et vice versa. Jam, quando

$$\mathrm{F}(\theta_2, \theta_3, \ldots, \theta_a) = \mathrm{F}(\eta_2, \eta_3, \ldots, \eta_a) \qquad (1)$$

semper etiam erit

$$\mathrm{F}(\theta_1, \theta_2, \theta_3, \ldots, \theta_a) = \mathrm{F}(\theta_1, \eta_2, \eta_3, \ldots, \eta_a)$$

sed rem invertere generaliter non licebit. Videlicet, ut hæc æquatio locum habeat, supponere satis est, utramque familiam (1) eandem familiam et ejusdem familiæ substitutionum cum ipsa θ_1 combinationes quasdam, quæ pro utraque aliæ sint, continere. Generalius, quando familia F_1 ipsi F'_1, F_2 ipsi F'_2, etc., æquivalebit, æquivalebit etiam familia ex ipsarum $\mathrm{F}_1, \mathrm{F}_2, \ldots$, substitutionibus generatricibus genita illi familiæ, quam substitutiones ipsarum $\mathrm{F}'_1, \mathrm{F}'_2, \ldots$, generatrices producunt; quod convertere generaliter non licebit. Substitutioni autem θ ad exponentem t pertinenti alia η quoties $\eta = \theta^\tau$, τ vero ad ipsum t prima quantitas erit neque ullo alio casu æquivalet. Sit δ ipsius t divisor, æquivalebit etiam η^δ ipsi θ^δ. Quare, æquivalentibus

$$\theta_1, \theta_2, \ldots, \theta_a \quad \text{ipsis} \quad \eta_1, \eta_2, \ldots, \eta_a$$

resp., pro quovis exponentium valore erit

$$\mathrm{F}\left(\theta_1^{\alpha_1}, \theta_2^{\alpha_2}, \ldots, \theta_a^{\alpha_a}\right) = \mathrm{F}\left(\eta_1^{\alpha_1}, \eta_2^{\alpha_2}, \ldots, \eta_a^{\alpha_a}\right).$$

ART. **20.** — Data sit familia a^{ti} ordinis irreductibilis

$$\mathrm{F}(\theta_1, \theta_2, \ldots, \theta_a)$$

tum, exclusis k quibusvis substitutionum $\theta_1, \theta_2, \ldots, \theta_a$, familiam $(a-k)^{ti}$ ordinis irreductibilem evadere patet.

Substitutiones $\theta_1, \theta_2, \ldots, \theta_a$ quanquam familiam a^{ti} ordinis irreductibilem generantes tamen per substitutionum, quæ non omnes illi familiæ insint, numerum ipso a minorem exprimi posse concipere licet. Quare a substitutiones, quæ per minorem aliarum numerum omnino non exprimi possunt, independentes earumque familiam irreductibilem a substitutionibus independentibus affectam vocabimus. Qualem si $\theta_1^{\alpha_1}, \theta_2^{\alpha_2}, \ldots, \theta_a^{\alpha_a}$ generant, a fortiori id de substitutionibus $\theta_1, \theta_2, \ldots, \theta_a$ confirmare potes.

Data familia a substitutionibus independentibus $\theta_1, \theta_2, \ldots, \theta_a$ affecta, exclusis harum k, familia quæ restat, $a-k$ substitutionibus independentibus erit affecta. Aliter enim familia exstaret illas $a-k$ quæ restant substitutiones amplectens, numero autem ipso $a-k$ minore substitutionum independentium affecta; quo datam familiam in alia substitutiones generatrices ipso a pauciores includente contentam esse, contra hypothesin, statim fluit.

Porro secundum definitionem familia a independentium substitutionum aliam ipso a plures continentem amplecti non potest. Quare, si ad illam novam substitutionem aggregas, familia inde orta aut a^{ti} aut $(a+1)^{ti}$ ordinis erit, et quoties a^{ti} ordinis, substitutiones generatrices independentes esse debent.

ART. **21**. — Concipiantur jam binæ substitutiones et quas generant familiæ. Quarum si quamlibet sumis, hæc generaliter in alia, quæ denuo in alia, etc., continebitur, tandem ad familiam $F(\theta_1, \theta_2)$ pervenies neque ipsam in alia ab ea diversa familia duarum substitutionum generatricum contentam. His, quas familias secundi ordinis primitivas vocare convenit, omnibus inventis, si rursus ab aliis substitutionum familiis incipitur, ad systema ab illo re vera non discrepans revenitur. Substitutiones θ_1, θ_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 æqualis esse debet, quam igitur pro illa ponere permissum est.

Inde quid sub familiis tertii sive superiorum ordinum primitivis sit intelligendum videtur. Data igitur familia primitiva a^{ti} ordinis

$F(\theta_1, \theta_2, \ldots, \theta_a)$, 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

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

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

Quo etiam summum substitutionum independentium in familia quadam contentarum numerum ipsi ν æqualem esse concludimus.

ART. **22.** — Secundum hanc familiarum primitivarum définitionem proprietatem indicare licet, qua ab omnibus aliis differant. Data enim substitutione primitiva, quia in majore primi ordinis familia contenta esse non potest, quævis familia $F(\mathfrak{s}, \theta)$ secundi ordinis est. Vice versa autem, quoties familia quælibet $F(\mathfrak{s}, \theta)$ secundi ordinis, $\mathfrak{s}$ primitiva erit substitutio; si enim non esset, daretur familia primi ordinis ipsam $F(\mathfrak{s})$ amplectens, etiamsi hæc quavis cum substitutione conjuncta, secundi ordinis familiam procrearet, quam in alia primi ordinis contineri non posse facile intelligis. Generalius ad familiam a^{ti} 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 conjunctæ $(a+1)$ substitutiones independentes producunt, familiam a^{ti} ordinis primitivam constituunt; aliter enim in tali continerentur, quod cum suppositione modo facta convenire non potest.

ART. **23.** — Quæritur jam de familiis, quæ in alia, veluti a^{ti} ordinis contentæ sunt, et quomodo obtineantur, et quales quorumque ordinum esse possint; utrum fieri possit, ut familia a^{ti} ordinis alias majoris

contineat, necne. Quæ autem quæstio manifesto cum hac convenit, utrum $(a+1)$ substitutiones familiam $(a+1)^{ti}$ ordinis generantes independentes esse debeant, necne. Primum vero familiam, nullam $(a+1)^{ti}$ ordinis continentem, familias majorum etiam ordinum a fortiori amplecti non posse elucet. Supposito itaque, in a^{ti} ordinis familia aliam $(a+1)^{ti}$ contentam esse, obtineretur illa adjunctis huic quibusdam substitutionibus θ, θ',.... Adjuncta igitur primum ipsa θ, postquam familias a^{ti} ordinis in aliis minoris contentas esse non posse supposuimus, quæ nascitur familia aut a^{ti} aut majoris erit ordinis; quoties postremum evenit, adjuncta nova substitutione θ' denuo familia oritur aut a^{ti} aut majoris ordinis, etc., tandem familiam exstare oportet, ipso a majoris ordinis, quæ cum substitutione quadam θ conjuncta ad a^{tum} delabatur, sive etiam fieri debet, ut, substitutione quadam θ e familia a^{ti} ordinis exclusa, alia ordinis ipso a majoris familia obtineatur.

ART. **24**. — Data igitur sit familia ejusque substitutio θ; quam si ex illa excludis, aliud non agis nisi ut familiam ipsam θ non continentem inquiras, quæ cum hacce conjuncta datam familiam producat. Quam quoniam semper in formam

$$F(\theta_1, \theta_2, \ldots, \theta_a, \theta)$$

redigere licet plerumque quidem non irreductibilem attamen talem semper, ut ipsa $F(\theta_1, \theta_2, \ldots, \theta_a)$ irreductibilis sit, exclusa substitutione θ, hæcce familia eveniet. Quare nisi tales substitutiones θ_1, $\theta_2, \ldots, \theta_a$ eligi possunt, quarum ipsa θ non sit productum, hancce directe aufferre non potes, sed indirecto tantum modo, id est alias excludendo substitutiones, quibus sublatis ipsa etiam θ excipiatur. Substitutiones θ_1, $\theta_2, \ldots, \theta_a$ tales etiam supponere licet, quarum nulla sit productum e ceteris ipsaque θ conflatum, namque si veluti θ_1 inter tales esset, data familia ita etiam designari posset

$$F(\theta_2, \theta_3, \ldots, \theta_a, \theta)$$

et exclusa substitutione θ resultaret familia $F(\theta_2, \ldots, \theta_a)$. Denique vero semper familiam dari, cui nullam ipsius θ potentiam directe detrahere possis, quæ vero ipsi θ conjuncta datam familiam producat, facile perspicis.

Ex. gr. quibus sub conditionibus $F(\theta)$ ipsi $F(\theta^a, \theta^b)$ ita exæquari possit ut $F(\theta^b)$ substitutionem θ^a non contineat, inquiramus. Primum autem $\theta^{ax}.\theta^{by} = \theta^{ax+by} = \theta$, id est, si θ ad exponentem t pertinet, $ax + by \equiv 1 \pmod{t}$ esse debet, quare a, b inter se primi. Secundo necesse est, ut θ^{bx} ab ipsa θ^a, sive bx ab ipso $a \pmod{t}$ pro omni ipsius x valore differat, quod quoniam a, b ipsius t divisores esse supponere possumus, obtinemus posito $b > 1$. Id autem semper fieri potest, nisi a omnes numeros primos ipsum t metientes continet. Jam sit $t = p^\pi r^\rho \ldots q^k s^\sigma \ldots$, ubi p, r,... numeros primos qui ipsum a metiuntur, q, s,... eos qui non metiuntur, designant, quivis ipsius t divisor alios nisi q, s,... numeros primos non continens neque ullus alius ad ipsum a erit primus. Qui quum omnes excepta unitate pro ipso b sumi possint, dantur familiæ $(k+1)(\sigma+1)\ldots - 1$

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

ipsi $F(\theta)$ æquales. Porro, quoties θ^c ipsius θ^b potentia, manente c ad ipsum a primo, erit

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

ART. 25. — Quæstiones has generales, quum difficillimæ sint, si ad superiorum ordinum familias progredi vis, in posterum referentes, alias quæstiones particulares quæ illis tanquam præparandis utiles videntur, hic etiam paullo attingamus.

Datis igitur μ substitutionibus $\theta_1, \theta_2, \ldots, \theta_\mu$, quarum diversa quæque elementa permutat ab aliarum nulla permutata, harum familia, pertinente generaliter θ_i ad exponentem t_i, substitutionum numerum implicabit $t_1 . t_2, \ldots t_\mu$. Generalius autem, si τ minimum ipsis $t_1, t_2, \ldots, t_\mu$ commune multiplum designat, familiæ $F(\theta_1, \theta_2, \ldots, \theta_\mu)$ substitutionum numerus quasi ipsius τ multiplum evadit.

Jam sint θ_1, θ_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 θ_2 potentiæ æqualis evadat, neque minus $\theta_2^{k_2}$ ipsius θ_1 potentiæ; 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 $F(\theta_1, \theta_2)$

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 aliæ formæ $\theta_2^i \theta_1^k$ omnes convenient. Quæ ut familiam constituant, et poscitur et sufficiet, ut productum quodlibet in eandem formam reducere sive quamvis substitutionem $\theta_1^a \theta_2^b$ alii hujusmodi $\theta_2^i \theta_1^k$ æqualem reddere liceat.

Generalius duæ substitutionum familiæ quarum substitutiones quaslibet per θ, θ' designemus earum autem numerum per f, f'; quia familiam ex e substitutionibus η constitutam communem habebunt, substitutiones θ ita

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

sive breviter per $\mathfrak{s}\eta$ repræsentari possunt, omnes vero substitutiones $\theta\theta'$ cum his $\mathfrak{s}\theta'$ conveniunt. Quæ $\frac{ff'}{e}$ substitutiones diversæ familiam constituent, quando quævis $\theta'\mathfrak{s}$ harum $\mathfrak{s}\theta'$ alicui æquivalebit neque ullo alio modo. Semper vero substitutionum numerum ipso $\frac{ff'}{e}$ majorem esse affirmare licet.

Vice versa autem, data familia aliam continente, cujus membrum generale per θ designemus, quamvis substitutionem illius familiæ in formam $\theta'\theta$ sive etiam $\theta\theta'$ redigere licet. Designante igitur θ_1 quamvis familiæ F (θ') substitutionem, η autem omnes huic cum familia θ communes, illas omnes in formam $\theta'\eta$ redigere potes. Quoties itaque F (θ'), θ substitutiones communes nisi identicam non implicant, substitutiones θ' totam familiam F (θ') explent.

ART. **26**. — Jam semper familiam $\frac{\mathrm{N}}{2}$ substitutionibus affectam inveniri posse constat. Cujus termino generali per θ expresso omnes N substitutiones alteri serierum θ, $\eta\theta$ inesse debent, designante η 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, cujus substitutiones generatrices omnes p^{ti} ordinis cycli sunt, designante p numerum primum

imparem, in familia θ continentur. Quare si illorum cyclorum familias diversis ipsius p valoribus respondentes et æquivalentes 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, quæ omnibus p^{ti} ordinis cyclis generatur, æquivaleat necesse est, sive etiam omnes hæ diversis p respondentes familiæ æquivalebunt.

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 theorema, id est, continere illam familiam $\frac{1.2.3...(n+1)}{2}$ substitutiones, comprobemus. Jam exsistere semper numerum primum inter n et $\frac{n+1}{2}$ contentum, $n \geqq 6$, 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 $p.\frac{N}{2}$ substitutiones diversas

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

Jam, quoniam $p.\frac{N}{2} > \frac{(n+1)}{2}.\frac{N}{2}$, 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 con-

tento inter 2 et numerum primum p maximum infra n datum, statim sequitur. Quæ enim familia quum unum certe p^{ti} ordinis cyclum c non contineret, $p.\frac{\mathrm{N}}{a}$ substitutiones diversæ darentur, quod fieri non potest.

Art. **27**. — Jam utile esse potest scire, quot substitutiones ad alias omnes generandas necessariæ sint, sive cujus ordinis ν sit familia principalis omnes substitutiones implicans. Primum vero facile limitem indicere licet, quem numerus ν excedere non potest. Designentur enim per γ_n, γ_{n-1},..., γ_3, γ_2 substitutiones cyclicæ ordinum n, $n-1$,..., 3, 2, resp., ubi generaliter substitutio γ_i eorum, quibus γ_{i+1} adhibetur, elementorum i permutat, omnem substitutionem in formam sequentem redigi posse

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

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

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

Art. **28**. — Jam, quibus sud conditionibus duarum substitutionum ejusdem ordinis cyclicarum η, θ familiæ præter 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 η loco talis poni potest potentia η^r, ubi r ad ipsum n prima quantitas, ut ejus potentia k^{ta} ipsi θ^k æqualis evadat. Namque necesse est, quantitatem r ad n primam talem eligere, ut

$$rk \equiv ik\,(\mathrm{mod.}\ n) \quad \text{sive} \quad r \equiv i\left(\mathrm{mod.}\ \frac{n}{k}\right),$$

id est $r = i + z.\frac{k}{n}$; 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 æquationi $\eta^k = \theta^k$ satisfacere supponi potest. Quum autem θ^k in k cyclos disjungatur $c_1, c_2, \ldots, c_k$, η^k in eosdem disjungi debet alio ordine instructos, quæcunque autem horum permutatio substitutionem η conditionibus satisfacientem præbebit. Quarum numerus producto $1.2.3\ldots k$ major esse non potest.

Jam sit $n = 4$; quia neque k alii quantitati atque 2 æqualis esse potest, neque ipso 1.2.3 pauciores quarti ordinis cycli, eorum autem tres familiæ inveniuntur, duo cycli quorum familiæ nisi identicam substitutiones communes non habeant, eligi possunt. Qui profecto 4.4 substitutiones itaque omnes generabunt. Hic omnibus ipsius N divisoribus familiæ respondent, quarum ordinem vel primum vel secundum esse elucet.

ART. **29.** — Porro sit $n = 5$, simili modo ordinem familiæ $\frac{N}{2}$ substitutiones continentis invenire licet. Namque duorum quinti ordinis cyclorum θ_1, θ_2 familia, quia nullam præter identicam substitutionem communem generant, certe 25 continebit terminos. Quæ si ab illa differret, cyclum quendam quinti ordinis θ_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 æquaret, cyclum denuo quinti ordinis non contineret, quo adjuncto familia deinde orta certe 5.15 substitutiones implicans in illâ $\frac{N}{2} = 60$ substitutionibus constituta contineretur, quod absurdum est. Jam sit c_2 transpositio hac in familia non inventa, cyclus tertii ordinis c_3 elementa ab ea non permutata continens in eadem invenitur familia; designante igitur c_5 quinti ordinis cyclum, familia $F(c_2, c_3, c_5)$ principali æquivalet. Quum autem hæc: $F(c_2, c_3, c_5)$ substitutiones c_2, c_3, c_5 generet, illi æquivalebit, 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 familiæ $\frac{N}{2}$ substitutionibus constitutæ k^{tum} excedere non potest. Erit autem generaliter minor. Posito enim ex. gr. $n = p$; denotantibus θ_1, θ_2,..., p^{ti} ordinis cyclos, substitutionum numerus familiæ horum quosdam neque alias substitutiones quasi generatrices continentis ipsius p multiplum, divisor autem numeri $\frac{1}{2}.1.2.3...p$ esse debet. Sumtis vero numeris d_0, d_1, d_2,..., d_i, quorum generaliter d_r proximum ipso $d_{r-1}.p$ majorem numeri $\frac{1}{2}.1.2...(p-1)$ divisorem, d_0 unitatem designet; supposito esse i minimum valorem harum conditionum

$$d_{i-1}.p > \frac{1}{4}.1.2...p, \quad d_i.p > \frac{1}{2}.1.2...p$$

alteri satisfacientem, familiæ 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 afferamus. 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 alius ab alio pendebunt; quare, posito $r_i \equiv f(i) \pmod{n}$, substitutionem per symbolum $\theta = [i, f(i)]$ repræsentare 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 repræsentabit. Post ipsam θ 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 θ 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 adæquatum esse potest.

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

Ponamus igitur ex. gr. $\theta(i) \equiv ai + b \pmod{n}$, 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. Quæ (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 hæc methodus ad difficultates problematum quæ 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 summæ difficultati obnoxia esse mihi videtur. Generalissimum vero est supponere, $\theta(i)$ implicate ipsi i conjunctum esse congruentia

$$V[i, \theta(i)] \equiv 0 \pmod{n}$$

quam si algebraicam supponimus, in formam

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

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

$$\sum_{r=0}^{r=\varphi(n)} \left(a^{(r)}_{\varphi(n)} i^{\varphi(n)} + \ldots + a^{(r)}_1 i + a^{(r)}_0 \right) z^r \equiv 0,$$

in qua quantitates a tales eligendæ sunt, ut

1° Habente i valorem datum, unus ipsius z valor integer evadat neque plures; 2° percurrente i seriem quantitatum $1, 2, \ldots, n, z$, eandem quodam ordine seriem percurrat, sive etiam binæ congruentiæ 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 $n = 3$

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

quæ, 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 præter 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 lætor. Fidem autem evangelicam profiteor. Quum septem annos natus essem, a parentibus viro Cl. Ranke in disciplinam traditus, primum classes prævias dein gymnasium Friderico-Guilelmum usque ad mensem Martis MDCCCLV frequentavi. Tum maturitatis testimonio instructus, postquam ad confirmandam valetudinem tempus æstivum in Helvetia transegi, civibus academicis universitatis Fridericæ-Guilelmæ Berolinensis a Rectore ill. Mitscherlich adscriptus nomen Decano ill. Dove apud facultatem philosophicam professus sum. Anno sequente Gottingiam me contuli, ubi Rectore ill. Waitz philosophiæ studiosis adscriptus scholis interfui præ 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 præceptori carissimo ill. Schellbach, cujus institutione matheseos scientiæ adductum me esse profiteor.