

DE

UNITATIBUS COMPLEXIS.

DISSERTATIO

INAUGURALIS ARITHMETICA

QUAM

CONSENSU ET AUCTORITATE

AMPLISSIMI PHILOSOPHORUM ORDINIS

IN

ALMA LITERARUM UNIVERSITATE FRIDERICA GUILLEM

PRO

SUMMIS IN PHILOSOPHIA HONORIBUS

RITE CAPESSENDIS

DIE X. M. SEPTEMBRIS A. MDCCCXLV.

B. L. Q. S.

PUBLICE DEFENDET

LEOPOLDUS KRONECKER

LIGNICIENSIS.

ADVERSARI ERUNT:

G. EISENSTEIN, PHIL. DR.

E. CAUER, PHIL. CAND.

H. RUEHLE, MED. CAND.

BEROLINI,

TYPIS GUSTAVI SCHADE.

PRAECEPTORI DILECTISSIMO
ERNESTO EDUARDO KUMMER,

PHILOSOPHIAE DOCTORI A. L. MAGISTRO, MATHEMATICORUM IN UNIVERSITATE LITERARIA
VRATISLAVIENSI PROFESSORI PUBLICO ORDINARIO, ACADEMIAE SCIENT.
REG. BORUSSICAE SOCIO EPISTOL.

HANC DISSERTATIONEM

PIO GRATIQUE ANIMO

D. D. D.

AUCTOR.

In principia doctrinae numerorum incrementa introductionem numerorum complexorum, ipsi summo hujus scientiae creatori debitam, referendam esse inter omnes constat. Qui numeri quam vim ad promovendam scientiam habeant inde eluet, quod arcte et cum residuis potestatum et cum theoria formarum altiorum graduum et cum circuli sectione cohaerent. Summus Gauss primus disquisitiones de numeris complexis formae $a+b\sqrt{-1}$ in publicum edidit, quarum theorematum postea Cl. Lejeune-Dirichlet uberior tractavit¹). Generalioris numerorum complexorum speciei mentionem fecit Cl. Jacobi, qui circuli sectionem pertractans in hanc quaestionem incidit²). Praeterea ad hanc doctrinae numerorum spectant observatio Cli. Jacobi³) et recentiore tempore disputatio Cli. Kummer „de numeris complexis qui unitatis radicibus et numeris integris realibus constant,” denique commentatio Illi. Eisenstein „de formis cubicis trium variabilium etc.” (in diario Crelliano tom. 28). — Ex quo prospectu, quam pauca de numeris complexis hue usque in publicum edita sint, jam eluet ideoque in sequentibus praecipue tantum ad illam Cli. Kummer disputationem lectorem rejicere potero. Quum vero nonnulla theorematata in illa commentatione jam tradita elegantius demonstrare mihi contigerit, etiamque alia quaedam nondum tradita ad perscrutandas unitates complexas adhibenda sint, quumque denique, quoad nunc possim, totum aliquod confidere velim, disquisitionem fere ab initio repetere paeferam. Quem ad finem prior hujus dissertationis unitatibus complexis deditae pars illas disquisitiones numerorum complexorum quasi fundamentales continebit.

¹) Crelle's Journal Bd. 24.

²) v. etiam commentationem Illi. Eisenstein in diario Crell. tom. 27. „Beiträge zur Kreisteilung.”

³) Crelle's Journal Bd. 19. pag. 314.

Denique adnotandum recentissimo tempore Clum. Lejeune-Dirichlet, dum in Italia versabatur, quaestiones de unitatibus principales ratione maxime generali latissimeque patente mira quidem simplicitate tractavisse, quarum rerum prospectum nunc in publicum editurus est. Quod quidem quum acciperem his meis disquisitionibus jam finitis, eas elaborare tamen non plane inutile videbatur et quia hae quae proferentur methodi ab illis methodis generalibus omnino differunt et quia in pertractandis unitatibus ex unitatis radicibus compositis quaestiones quaedam se offerunt, quas ipsas tanquam speciales alicujus momenti esse arbitror.

PARS PRIOR.

§. 1.

Ne postea investigationum ordinem interrumpere oporteat, hoc quod sequitur lemma, cuius frequens erit usus et quo nonnullae demonstrationes praecedentur, antea praemittimus.

Sint aequationis algebraicae n^n gradus coefficientibus integris (coefficientis ipsius x^n sit unitas) n radices: α, β, γ etc. atque ejusdem aequationis, si tanquam congruentiam modulo p (ubi p numerus primus) consideres, n radices: a, b, c etc. sit porro $f(\alpha, \beta, \gamma \dots)$ functio radicum algebraica integra symmetrica, congruentiam $f(\alpha, \beta, \gamma \dots) \equiv f(a, b, c \dots) \text{ mod. } p$ locum habere dico.

Dem. Etenim quamque functionem radicum algebraicam integrum symmetricam *identice* tanquam functionem integrum expressionum: $\alpha + \beta + \gamma + \dots, \alpha\beta + \alpha\gamma + \dots$ etc. repraesentari posse constat. Ergo $f(a, b, c \dots)$ eadem functio integra expressionum: $a + b + \dots, ab + ac + \dots$ etc. quae $f(\alpha, \beta, \gamma \dots)$ ipsarum $\alpha + \beta + \gamma + \dots, \alpha\beta + \alpha\gamma + \dots$ etc. sit oportet. Quum vero $a + b + c + \dots$ coefficienti ipsius x^{n-1} i. e. quantitati $\alpha + \beta + \gamma + \dots$ pariterque $ab + ac + \dots$ ipsi $\alpha\beta + \alpha\gamma + \dots$ etc. secundum modulum p congrua esse notum est, id quod contendimus facile concludi potest.

Nunc sit ν numerus primus, ω radix aequationis $\omega^\nu = 1$ primitiva, sint porro $\varepsilon, \varepsilon_1, \dots, \varepsilon_{\lambda-1}$ λ periodi radicum ω quarum quaeque μ terminos contineat, ita ut habeamus $\lambda\mu = \nu - 1$ et:

$$\begin{aligned} \varepsilon &= \omega + \omega^{g^{\lambda}} + \omega^{g^{2\lambda}} + \dots + \omega^{g^{(\mu-1)\lambda}} \\ \varepsilon_1 &= \omega^g + \omega^{g^{\lambda+1}} + \omega^{g^{2\lambda+1}} + \dots + \omega^{g^{(\mu-1)\lambda+1}} \\ \vdots &\quad \vdots \quad \vdots \\ \varepsilon_{\lambda-1} &= \omega^{g^{\lambda-1}} + \omega^{g^{2\lambda-1}} + \omega^{g^{3\lambda-1}} + \dots + \omega^{g^{\mu\lambda-1}} \end{aligned}$$

ubi g est radix primitiva ipsius ν .

Ex quibus aequationibus statim colligitur:

$$\varepsilon_{\lambda+r} = \varepsilon_r \text{ et } 1 + \varepsilon + \varepsilon_1 + \dots + \varepsilon_{\lambda-1} = 0.$$

Jam posito $a\varepsilon + a_1\varepsilon_1 + a_2\varepsilon_2 + \dots + a_{\lambda-1}\varepsilon_{\lambda-1} = f(\varepsilon)$ ¹⁾ ubi literis: $a, a_1, \dots, a_{\lambda-1}$ numeri reales integri designantur, talem expressionem $f(\varepsilon)$ numerum complexum voco. Jam quia omnis periodorum functio rationalis tanquam omnium periodorum functio linearis repraesentari potest, productum numerorum complexorum rursum in formam ipsius $f(\varepsilon)$ redigi posse patet. Deinde eadem, qua Cl. Kummer in disputatione illa jam laudata §. 1. usus est ratione, ex aequatione:

$$a\varepsilon + a_1\varepsilon_1 + \dots + a_{\lambda-1}\varepsilon_{\lambda-1} = b\varepsilon + b_1\varepsilon_1 + \dots + b_{\lambda-1}\varepsilon_{\lambda-1}$$

sequitur ut sint $a = b, a_1 = b_1, \dots, a_{\lambda-1} = b_{\lambda-1}$.

Numeri $f(\varepsilon_1), f(\varepsilon_2), \dots, f(\varepsilon_{\lambda-1})$ numero $f(\varepsilon)$ conjuncti dicuntur et facile, brevitatis causa $f(\varepsilon) = f, f(\varepsilon_1) = f_1$ etc. positis, aequationes sequentes locum habere eluet:

$$\begin{aligned} a\varepsilon + a_1\varepsilon_1 + \dots + a_{\lambda-1}\varepsilon_{\lambda-1} &= f \\ a\varepsilon_1 + a_1\varepsilon_2 + \dots + a_{\lambda-1}\varepsilon &= f_1 \\ \vdots &\quad \vdots \quad \vdots \\ a\varepsilon_{\lambda-1} + a_1\varepsilon + \dots + a_{\lambda-1}\varepsilon_{\lambda-2} &= f_{\lambda-1} \end{aligned}$$

Quod aequationum systema ut secundum quantitates a, a_1, \dots solvamus, litera α aliquam aequationis $\alpha^\lambda = 1$ radicem designamus. Tum aequatione prima in 1, secunda in α , tertia in α^2 etc. postrema in $\alpha^{\lambda-1}$ ductis iisque additis aequationem:

¹⁾ Quum illa periodorum functio linearis eadem tanquam functio ipsius ε rationalis integra repraesentari possit.

$$\text{III. } (\varepsilon + \varepsilon_1 \alpha + \varepsilon_2 \alpha^2 + \dots + \varepsilon_{\lambda-1} \alpha^{\lambda-1}) (a + a_1 \alpha^{-1} + a_2 \alpha^{-2} + \dots + a_{\lambda-1} \alpha^{-(\lambda-1)}) \\ = f + f_1 \alpha + f_2 \alpha^2 + \dots + f_{\lambda-1} \alpha^{\lambda-1}$$

pro quaque unitatis radice λ^{μ} α obtinemus.

Quum vero expressio $\varepsilon + \varepsilon_1 \alpha + \dots + \varepsilon_{\lambda-1} \alpha^{\lambda-1}$ nihil aliud sit, nisi id quod Cl. Jacobi signo (α, ω) denotat¹⁾, formulam loco laudato traditam in auxilium vocamus:

$(\varepsilon + \varepsilon_1 \alpha + \dots + \varepsilon_{\lambda-1} \alpha^{\lambda-1}) (\varepsilon + \varepsilon_1 \alpha^{-1} + \dots + \varepsilon_{\lambda-1} \alpha^{-(\lambda-1)}) = \nu \cdot \alpha^{\frac{1}{2}(\nu-1)} = \nu \cdot \alpha^{\frac{1}{2}\mu\lambda}$
quae pro quoque ipsius α valore excepto illo $\alpha = 1$ locum habet. Qua adhibita atque aequatione III. per ipsum $\varepsilon + \varepsilon_1 \alpha^{-1} + \varepsilon_2 \alpha^{-2} + \dots + \varepsilon_{\lambda-1} \alpha^{-(\lambda-1)}$ multiplicata aequatio:

$$\text{IV. } \nu(a + a_1 \alpha^{-1} + a_2 \alpha^{-2} + \dots + a_{\lambda-1} \alpha^{-(\lambda-1)}) = (f + f_1 \alpha + \dots + f_{\lambda-1} \alpha^{\lambda-1}). \\ (\varepsilon + \varepsilon_1 \alpha^{-1} + \dots + \varepsilon_{\lambda-1} \alpha^{-(\lambda-1)})$$

(posito μ numerum esse parem) oritur, atque pro quoque ipsius α valore unitate excepta valet. Unde concludi licet:

$$\begin{array}{rcl} \nu a &= f\varepsilon + f_1\varepsilon_1 + f_2\varepsilon_2 + \dots + f_{\lambda-1}\varepsilon_{\lambda-1} + m \\ \nu a_1 &= f\varepsilon_1 + f_1\varepsilon_2 + f_2\varepsilon_3 + \dots + f_{\lambda-1}\varepsilon + m \\ \vdots &\vdots &\vdots \\ \nu a_{\lambda-1} &= f\varepsilon_{\lambda-1} + f_1\varepsilon + f_2\varepsilon_1 + \dots + f_{\lambda-1}\varepsilon_{\lambda-2} + m. \end{array}$$

Quando enim pro quibusvis quantitatibus b et c systema aequationum habemus:

$$\begin{aligned} b + b_1 \alpha + \dots + b_r \alpha^r + \dots + b_{\lambda-1} \alpha^{\lambda-1} &= c + c_1 \alpha + \dots + c_r \alpha^r + \dots + c_{\lambda-1} \alpha^{\lambda-1} \\ b + b_1 \alpha^1 + \dots + b_r \alpha^{2r} + \dots + b_{\lambda-1} \alpha^{2(\lambda-1)} &= c + c_1 \alpha^2 + \dots + c_r \alpha^{2r} + \dots + c_{\lambda-1} \alpha^{2(\lambda-1)} \\ &\vdots &\vdots &\vdots \\ b + b_1 \alpha^{\lambda-1} + \dots + b_r \alpha^{(\lambda-1)r} + \dots + b_{\lambda-1} \alpha &= c + c_1 \alpha^{\lambda-1} + \dots + c_r \alpha^{(\lambda-1)r} + \dots + c_{\lambda-1} \alpha \end{aligned}$$

facile prima aequatione in α^{-r} , secunda in α^{-2r} etc. ducta iisque additis aequatio colligitur:

$$\lambda b_r - (b + b_1 + \dots + b_{\lambda-1}) = \lambda c_r - (c + c_1 + \dots + c_{\lambda-1}) \text{ seu } b_r = c_r + m$$

ubi m respectu r constans est.

¹⁾ Monatsberichte der Berliner Akademie 1837.

Ut quantitas m definiatur, adnotamus istis aequationibus ν additis fieri:

VI. $\nu(a + a_1 + \dots + a_{\lambda-1}) = (f + f_1 + \dots + f_{\lambda-1})(\varepsilon + \varepsilon_1 + \dots + \varepsilon_{\lambda-1}) + \lambda m.$
 Quum vero $\varepsilon + \varepsilon_1 + \dots + \varepsilon_{\lambda-1} = -1$ sit et $a + a_1 + \dots + a_{\lambda-1} = -(f + f_1 + \dots + f_{\lambda-1})$ esse ex aequatione III. ibi ponendo $\alpha = 1$ colligatur, aequatio VI. mutatur in:

$$-(\nu - 1)(f + f_1 + \dots + f_{\lambda-1}) = \lambda m \text{ seu } -\mu(f + f_1 + \dots + f_{\lambda-1}) = m.$$

Quo valore ipsius m substituto has consequimur aequationes systemata II. et V. repraesentantes:

$$\text{VII. } fr = a\varepsilon_r + a_1\varepsilon_{r+1} + \dots + a_{\lambda-1}\varepsilon_{r-1}$$

$$-\nu a_r = f(\mu - \varepsilon_r) + f_1(\mu - \varepsilon_{r+1}) + \dots + f_{\lambda-1}(\mu - \varepsilon_{r-1})$$

pro valoribus ipsius $r : 0, 1, 2, \dots, \lambda - 1$.

Jam vero respecta analogia numerorum complexorum qui radicibus unitatis ad numeros compositos (ν) pertinentibus constant, numeros complexos $f(\varepsilon)$ sub hac forma accipere convenit, scilicet:

$$f(\varepsilon) = a + a_1\varepsilon + a_2\varepsilon^2 + \dots + a_{\lambda-1}\varepsilon^{\lambda-1}$$

quamquam *unitates* complexas in posterum illius formae supra exhibitae ponemus. — Productum talium numerorum $f(\varepsilon)$ rursus in eandem formam redigi posse inde eluet, quod quaevis periodus tanquam functio rationalis integra unius repraesentari potest, quodque quaevis functio integra periodi ε per aequationem illam gradus λ^n , quarum radices $\varepsilon, \varepsilon_1, \dots, \varepsilon_{\lambda-1}$ sunt, ad gradum $\lambda - 1$ redigi potest. Denique ex aequalitate duorum numerorum complexorum aequalitatem singulorum coefficientium colligi posse inde patet, quod functio periodi integra gradus $\lambda - 1$ evanescere nequit, nisi omnes ejus coefficientes evanescunt.

Productum omnium numerorum conjunctorum, tanquam functio periodorum invariabilis integra, numerus realis integer est atque norma appellatur. Est igitur:

$$f(\varepsilon) f(\varepsilon_1) \dots f(\varepsilon_{\lambda-1}) = Nf(\varepsilon)$$

et quidem respectu ε . Quodsi enim $f(\varepsilon)$ tanquam functio alias periodi e. g. ipsius ω consideratur, ita ut sit: $f(\varepsilon) = \varphi(\omega)$ appareat esse $N\varphi(\omega) = \varphi(\omega)\varphi(\omega_1)\dots\varphi(\omega_{\nu-2})$ sive $N\varphi(\omega) = (Nf(\varepsilon))^{\mu}$. Neque unquam, ne ex aequalitate signorum ambiguitas oriatur, verendum est.

Caeterum ex ipsa definitione colliguntur aequationes:

$$Nf(\varepsilon) = Nf(\varepsilon_r) \text{ et } N(f(\varepsilon), \varphi(\varepsilon)) = Nf(\varepsilon) \cdot N\varphi(\varepsilon).$$

Quum sit $(Nf(\varepsilon))^{\mu} = N\varphi(\omega) \equiv 1 \text{ mod. } \nu$, posito numerum $Nf(\varepsilon)$ ad ipsum ν primum esse (Disput. Cl. Kummer §. 2), sequitur, ut quaevis norma respectu ε residuum sit λ^{μ} potestatis modulo ν .

§. 2.

Ponatur p numerus primus ejusmodi, ut sit $p^{\mu} \equiv 1 \text{ mod. } \nu$, atque sit:
$$p = p(\varepsilon) p(\varepsilon_1) \dots p(\varepsilon_{\lambda-1}) = Np(\varepsilon)$$

istos factores ulterius in factores complexos ex his ipsis periodis ε compositos discripi non posse atque inter se diversos esse, eadem qua Cl. Kummer in disputatione sua §. 5 usus est ratione probatur.

Deinde quum a Clo. Kummer¹⁾ demonstratum sit, congruentiam λ^{μ} gradus: $(x - \varepsilon)(x - \varepsilon_1) \dots (x - \varepsilon_{\lambda-1}) \equiv 0 \text{ mod. } p$ semper habere λ radices, si p condicioni sufficit $p^{\mu} \equiv 1 \text{ mod. } \nu$, has ipsas designemus literis: $e, e_1, \dots, e_{\lambda-1}$ ²⁾. Jam hae duae habentur theorematum:

1. Si $f(\varepsilon)$ numerus est complexus cujus norma per numerum primum p divisibilis est, unus numerorum $f(e), f(e_1), \dots$ secundum modulum p nihilo congruus erit; et quando unum numerorum $f(e)$ ipsum p metitur, etiam $Nf(\varepsilon)$ factorem p impiebat.

Dem. Quum productum $f(\varepsilon) f(\varepsilon_1) \dots f(\varepsilon_{\lambda-1})$ functio sit algebraica integra symmetrica radicum aequationis $(x - \varepsilon)(x - \varepsilon_1) \dots (x - \varepsilon_{\lambda-1}) = 0$ secundum primum nostrum lemma erit:

$$\begin{aligned} f(\varepsilon) f(\varepsilon_1) \dots f(\varepsilon_{\lambda-1}) &\equiv f(e) f(e_1) \dots f(e_{\lambda-1}) \text{ mod. } p \\ \text{sive } Nf(\varepsilon) &\equiv f(e) f(e_1) \dots f(e_{\lambda-1}) \text{ mod. } p \end{aligned}$$

unde theorematum illa sponte manant.

2. *Theorema.* Sint $p(\varepsilon), p(\varepsilon_1), \dots$ factores complexi primi numeri primi p sitque $p(e)$ ille factor, qui condicionem explet $p(e) \equiv 0 \text{ mod. } p$ congruentia haec locum habebit:

$$e \equiv \varepsilon \text{ mod. } p(\varepsilon)$$

Dem. Ponatur expressio $(e - \varepsilon) p(\varepsilon_1) p(\varepsilon_2) \dots p(\varepsilon_{\lambda-1}) = \varphi(\varepsilon)$ unde
$$(e - \varepsilon_i) p(\varepsilon) p(\varepsilon_2) \dots p(\varepsilon_{\lambda-1}) = \varphi(\varepsilon_i) \text{ etc.}$$

¹⁾ in commentatione „de divisoribus formarum quarundam etc.” quae proximo tempore in Diario Crelliano edetur; vel etiam in commentatione Cli. Schoenemann Diar. Crell. tom. 19. pag. 306.

²⁾ Adnotamus quodvis e_r eandem ipsius e functionem integrum esse quam ε_r ipsius ε .

tum erit $\varphi(e) = 0$ et $\varphi(e_1) \equiv \varphi(e_2) \equiv \dots \varphi(e_{\lambda-1}) \equiv 0 \text{ mod. } p$ quia omnes hi numeri factorem $p(e)$ implicant, quem nihilo congruum supposuimus. Jam erit secundum illud lemma:

$\varphi(\varepsilon) + \varphi(\varepsilon_1) + \dots + \varphi(\varepsilon_{\lambda-1}) \equiv \varphi(e) + \varphi(e_1) + \dots + \varphi(e_{\lambda-1}) \equiv 0 \text{ mod. } p$. Deinde erit $\varphi(\varepsilon)^2 + \varphi(\varepsilon)\varphi(\varepsilon_1) + \dots + \varphi(\varepsilon)\varphi(\varepsilon_{\lambda-1}) \equiv \varphi(e)^2$ quum reliqua producta omnes factores $p(\varepsilon)$ ideoque ipsum p contineant. Ergo habemus: $\varphi(\varepsilon)^2 \equiv 0 \text{ mod. } p$. Jam si p ad ν primum supponitur erit $p^{\nu-1} \equiv 1 \text{ mod. } \nu$ atque $\varphi(\varepsilon)^{p^{\nu-1}} \equiv \varphi(\varepsilon)^{p^{\nu-1}} \equiv \varphi(\varepsilon)^1 \equiv \varphi(\varepsilon) \text{ mod. } p$.

Erit autem $\varphi(\varepsilon)^{p^{\nu-1}} = \varphi(\varepsilon)^{p^{\nu-1}-2} \cdot \varphi(\varepsilon)^2 \equiv 0$ unde denique:

$\varphi(\varepsilon) \equiv 0 \text{ mod. } p$ i. e. $(e - \varepsilon)p(\varepsilon_1)p(\varepsilon_2)\dots p(\varepsilon_{\lambda-1}) \equiv 0 \text{ mod. } p(\varepsilon)p(\varepsilon_1)\dots p(\varepsilon_{\lambda-1})$ ergo: $e - \varepsilon \equiv 0 \text{ mod. } p(\varepsilon)$.

Casu $p = \nu$ habemus $Np(\varepsilon) = \nu$ et posito $p(\varepsilon) = f(\omega)$ erit $Nf(\omega) = (Np(\varepsilon))^{\mu}$ ergo $Nf(\omega) \equiv 0 \text{ mod. } \nu^{\mu}$. Eaque de re $f(1) \equiv 0 \text{ mod. } \nu$ (disputatio Cli. Kummer §. 2) ergo quum sit $(1 - \omega)(1 - \omega^2)\dots = \nu$ erit quoque $f(1) \equiv 0 \text{ mod. } (1 - \omega)$. Deinde propter congruentiam $1 \equiv \omega \text{ mod. } (1 - \omega)$, $f(\omega) \equiv 0 \text{ mod. } (1 - \omega)$. Jam posito $f(\omega) = (1 - \omega)f'(\omega)$ erit $Nf'(\omega) \equiv 0 \text{ mod. } \nu^{\mu-1}$, ergo sicut supra $f'(\omega) = (1 - \omega)f''(\omega)$. Qua ratione denique obtainemus $f(\omega) = (1 - \omega)^{\mu}\varphi(\omega)$. Est vero $Nf(\omega) = \nu^{\mu} = \nu^{\mu}N\varphi(\omega)$ unde $\varphi(\omega)$ unitatem complexam esse patet. Ergo erit quoque:

$$(1 - \omega)^{\mu} \equiv 0 \text{ mod. } f(\omega) \text{ seu mod. } p(\varepsilon).$$

Deinde quum simili modo e congruentia $N(e - \varepsilon) \equiv 0 \text{ mod. } \nu$ colligatur $(e - \varepsilon) = (1 - \omega)^{\mu}\psi(\omega)$ sive $(e - \varepsilon) \equiv 0 \text{ mod. } (1 - \omega)^{\mu}$ denique habebitur: $e - \varepsilon \equiv 0 \text{ mod. } p(\varepsilon)$ respecta congruentia illa: $(1 - \omega)^{\mu} \equiv 0 \text{ mod. } p(\varepsilon)$.

3. *Theorema.* Si duo habentur factores primi complexi non conjuncti ejusdem numeri primi p e. g. $p(\varepsilon)$ et $p^1(\varepsilon)$ singuli factores $p^1(\varepsilon)$ e singulis $p(\varepsilon)$ multiplicando per unitates complexas deducuntur¹⁾.

Dem. Sint $p(e)$ et $p^1(e)$ factores per ipsum p divisibles, erit:

$$p^1(e) \equiv 0 \text{ mod. } p \text{ ideoque etiam mod. } p(\varepsilon)$$

¹⁾ v. §. 3, 1.

²⁾ Quod theorema casus tantum specialis theorematis 2 in §. 3 est.

Est vero $e \equiv s \pmod{p(\epsilon)}$ unde $p^1(\epsilon) \equiv 0 \pmod{p(\epsilon)}$ i. e. $p^1(\epsilon) = p(\epsilon) \cdot \varphi(\epsilon)$ ubi $\varphi(\epsilon)$ unitas complexa est, quia $Np^1(\epsilon) = p = Np(\epsilon) \cdot N\varphi(\epsilon) = p \cdot N\varphi(\epsilon)$ ergo $N\varphi(\epsilon) = 1$.

4. Theorema. Quando norma numeri complexi $p(\epsilon)$ numerus primus p est ab ipso ν diversus, unum tantum numerorum $p(\epsilon)$ numerus p metiri potest.

Dem. Sit $p(\epsilon) \equiv p(e_r) \equiv 0 \pmod{p}$ ergo $p(e_r) \equiv 0 \pmod{p(\epsilon)}$. Deinde quum habeamus $e \equiv \epsilon$ et $e_r \equiv \epsilon_r \pmod{p(\epsilon)}$ ¹⁾ sequitur, ut sit: $p(\epsilon_r) \equiv 0 \pmod{p(\epsilon)}$ sive $p(\epsilon_r) = p(\epsilon) \cdot \varphi(\epsilon)$. Ergo quum sit: $p(\epsilon) \cdot p(\epsilon_1) \dots p(\epsilon_{\lambda-1}) \equiv 0 \pmod{p}$, etiam erit:

$p(\epsilon) \cdot p(\epsilon) \cdot p(\epsilon_1) \dots p(\epsilon_{\lambda-1}) = p(\epsilon_r) \cdot p(\epsilon_1) \dots p(\epsilon_{r-1}) p(\epsilon_{r+1}) \dots \equiv 0$
 etiamque $p(\epsilon_r)^{p^\mu} \cdot p(\epsilon_1) \dots p(\epsilon_{r-1}) p(\epsilon_{r+1}) \dots \equiv p(\epsilon_r) \cdot p(\epsilon_1) \dots \equiv 0$ ²⁾
 i. e. $\frac{Np(\epsilon)}{p(\epsilon)} = \frac{p}{p(\epsilon)} \equiv 0 \pmod{p}$, sive $\frac{p}{p(\epsilon)} = p \cdot f(\epsilon)$ sive denique $1 = f(\epsilon) \cdot p(\epsilon)$ id quod fieri non posse facile patet, si in utraque aequationis parte normam formes. Tum enim esset $1 = p \cdot Nf(\epsilon)$.

• §. 3.

Quum omnes numeri complexi, qui periodis constant, etiam tanquam functiones ipsarum radicum considerari possint, quumque iis quae sequuntur haec forma simplicior magis accommodata sit, hanc ipsam accipiemus, ubicunque salva quaestionum generalitate fieri poterit.

1. Theorema. Quando norma aliqua $Nf(\omega)$ numerum primum p continet, qui ad exponentem μ modulo ν pertineat, illam ipsam normam μ ipsius p potestas metiri debet.

Dem. Quum sit $\mu \cdot \lambda = \nu - 1$ quumque p ad numerum μ pertineat, ponatur $p \equiv g^\lambda$. Jam erit secundum rationem saepe usitatam: $f(\omega) \equiv f(\omega), f(\omega)^p \equiv f(\omega^p)$ $f(\omega)^{p^2} \equiv f(\omega^{p^2}), \dots f(\omega)^{p^{\mu-1}} \equiv f(\omega^{p^{\mu-1}}) \pmod{p}$. Quibus aequationibus inter se multiplicatis obtainemus:

$$f(\omega)^1 + p + p^2 + \dots + p^{\mu-1} \equiv f(\omega) \cdot f(\omega^p) \dots f(\omega^{p^{\mu-1}}) \pmod{p}.$$

In qua aequatione si deinceps loco ipsius ω substituuntur valores: $\omega^g, \omega^{g^2}, \dots \omega^{g^{\lambda-1}}$, atque aequationes, quae hoc modo prodeunt, inter se multiplicantur, fit: $\{f(\omega) \cdot f(\omega^g) \dots f(\omega^{g^{\lambda-1}})\}^{1+p+\dots+p^{\mu-1}} \equiv Nf(\omega) \equiv 0 \pmod{p}$

¹⁾ v. adnotationem ad §. 2. — ²⁾ v. §. 3, 1.

sive posito $f(\omega) \cdot f(\omega^g) \cdots f(\omega^{g^{\lambda-1}}) = \varphi(\omega)$:

$$\varphi(\omega)^1 + p + \cdots + p^{\mu-1} \equiv 0 \pmod{p}$$

Jam quum sit $1 + p + \cdots + p^{\mu-1} < p^\mu$ certo etiam erit $\varphi(\omega)^{p^\mu} \equiv 0$.

Est vero $\varphi(\omega)^{p^\mu} \equiv \varphi(\omega^{p^\mu}) \equiv \varphi(\omega) \pmod{p}$. ergo $\varphi(\omega) \equiv 0 \pmod{p}$ unde mutatis radicibus ω oriuntur relationes:

$$\varphi(\omega) \equiv \varphi(\omega^{g^\lambda}) \equiv \varphi(\omega^{g^{2\lambda}}) \equiv \cdots \equiv \varphi(\omega^{g^{(\mu-1)\lambda}}) \equiv 0 \pmod{p}$$

unde respecta ipsius $\varphi(\omega)$ definitione:

$$Nf(\omega) = \varphi(\omega) \cdot \varphi(\omega^{g^\lambda}) \cdots \varphi(\omega^{g^{(\mu-1)\lambda}}) \equiv 0 \pmod{p^\mu}$$

2. *Theorema.* Normam aliquam $Nf(\omega)$ si numerus primus p metitur, qui ad exponentem μ modulo r pertinet quique in λ factores primos complexos e periodis ε compositos dissolvi potest, quotiens illius normae et summae quae ea continetur numeri primi potestatis ipse tanquam norma repraesentari potest.

Dem. Primum adnotamus potestatem ipsius p summam numero $Nf(\omega)$ contentam secundum supra dicta multiplum ipsius μ esse debere. Jam sit $p = Np(\varepsilon)$, deinde ponatur $f(\omega) \cdot f(\omega^{g^\lambda}) \cdot f(\omega^{g^{2\lambda}}) \cdots f(\omega^{g^{(\mu-1)\lambda}}) = \varphi(\varepsilon)$ ¹⁾. Tum habemus secundum suppositionem nostram:

$$Nf(\omega) = N\varphi(\varepsilon) \equiv 0 \pmod{p}$$

unde secundum §. 2, 1: $\varphi(\varepsilon_r) \equiv 0 \pmod{p}$ ideoque mod. $p(\varepsilon)$. Quumque habeamus secundum §. 2, 2: $e \equiv \varepsilon \pmod{p(\varepsilon)}$ erit:

$$\varphi(\varepsilon_r) \equiv 0 \pmod{p(\varepsilon)} \text{ sive mutatis periodis } \varphi(\varepsilon) \equiv 0 \pmod{p(\varepsilon_{-r})}$$

i. e. $f(\omega) \cdot f(\omega^{g^\lambda}) \cdots f(\omega^{g^{(\mu-1)\lambda}}) \equiv 0 \pmod{p(\varepsilon_{-r})}$ sive si congruentiam $p \equiv g^\lambda$

mod. r respicimus: $f(\omega) \cdot f(\omega^p) \cdots f(\omega^{p^{\mu-1}}) \equiv 0 \pmod{p(\varepsilon_{-r})}$. Est vero:

$$f(\omega) \cdot f(\omega^p) \cdots f(\omega^{p^{\mu-1}}) \equiv f(\omega)^1 + p + \cdots + p^{\mu-1} \pmod{p^2} \text{ ideoque mod. } p(\varepsilon_{-r}),$$

unde ratione supra exhibita colligimus esse:

$$f(\omega) \equiv 0 \pmod{p(\varepsilon_{-r})} \text{ sive } f(\omega) = \psi(\omega) \cdot p(\varepsilon_{-r})$$

Ad normam transeuntes obtinemus aequationem:

$$Nf(\omega) = p^\mu \cdot N\psi(\omega) \text{ sive } \frac{Nf(\omega)}{p^\mu} = N\psi(\omega) \text{ q. e. d.}$$

¹⁾ Gauss disq. arithm. 345.

²⁾ v. paragraphum antecedentem.

Jam hac methodo iterum atque iterum adhibita facile patet e suppositione
 $Nf(\omega) \equiv 0 \pmod{q^{n+\mu}}$ congruentiam colligi hujus modi:

$$f(\omega) \equiv 0 \pmod{p(\varepsilon_x)^m \cdot p(\varepsilon_{x'})^{m'} \dots}$$

ubi $m + m' + \dots = n$; denique habebitur theorema hocce: quando norma aliqua divisibilis est per numerum cuius factores primi reales in factores complexos quam plurimos discripi possunt¹⁾, quotiens illius normae et summae quae ea continetur denominatoris potestatis ipse tanquam norma repraesentari potest.

Adnotatio. Si $Nf(\omega) \equiv 0 \pmod{\nu}$, habemus $f(\omega) \equiv 0 \pmod{(1-\omega)^2}$ pariterque e congruentia $Nf(\omega) \equiv 0 \pmod{\nu^m}$ congruentiam colligimus $f(\omega) \equiv 0 \pmod{(1-\omega)^m}$.

§. 4.

Sit $f(\omega)$ numerus aliquis complexus, N numerus realis ejusmodi, ut factores ejus primi reales in factores complexos quam plurimos discripi possint, sitque factor numerorum $f(\omega)$ et N communis maximus $\varphi(\omega)$ ²⁾, numerus $\psi(\omega)$ inveniri potest talis ut sit: $\psi(\omega) \cdot f(\omega) \equiv \varphi(\omega) \pmod{N}$ ³⁾.

Dem. Sit primum numerus N potestas numeri primi ergo: $N = p^\pi$; sit deinde $p = Np(\varepsilon)$ et $p \equiv g^\lambda \pmod{\nu}$.

Jam erit secundum §. 3, 2: $f(\omega) = F(\omega) \cdot p(\varepsilon_x)^m \cdot p(\varepsilon_{x'})^{m'} \dots$ ubi $p^{m+m'+\dots}$ summa ipsius p potestas numero $Nf(\omega)$ contenta. Est igitur $NF(\omega)$ numerus ad ipsum p primus, quare exstat numerus x talis ut sit: $x \cdot NF(\omega) \equiv 1 \pmod{p^\pi}$. Hinc habemus:

$$\begin{aligned} I. \quad & x \cdot F(\omega^3) F(\omega^5) \dots F(\omega^{\nu-1}) \cdot f(\omega) = x \cdot NF(\omega) \cdot p(\varepsilon_x)^m \cdot p(\varepsilon_{x'})^{m'} \dots \\ & \equiv p(\varepsilon_x)^m \cdot p(\varepsilon_{x'})^{m'} \dots \pmod{p^\pi}. \end{aligned}$$

Designemus complexum omnium factorum ipsis $p(\varepsilon_x)^m \cdot p(\varepsilon_{x'})^{m'} \dots$ et $p^\pi = p(\varepsilon)^\pi \cdot p(\varepsilon_1)^\pi \dots$ communium signo $P(\varepsilon)$ ita ut sint:

¹⁾ Numerum aliquem primum p ad divisorem μ ipsius $\nu - 1$ pertinentem in factores complexos quam plurimos discripi posse dicimus, si in $\frac{\nu-1}{\mu}$ factores complexos e periodis ε compositos eosque conjunctos dissolvi potest.

²⁾ v. §. 2, 2.

³⁾ De factore communi maximo sermonem esse posse inde elucet, quod factores ipsius N primi in factores complexos dissolvi queunt, igitur ad eos omnes theorema §. 3, 2. adhiberi potest. Caeterum hoc in ipsa demonstratione probabitur.

⁴⁾ Modulum realem accipimus, quia si complexus est multiplicando per factores conjunctos realis reddi potest.

$$P(\varepsilon) \cdot p(\varepsilon_a)^{\alpha} \cdot p(\varepsilon_{a'})^{\alpha'} \dots = P(\varepsilon) \cdot A(\varepsilon) = p(\varepsilon_x)^m \cdot p(\varepsilon_{x'})^{m'} \dots$$

$$P(\varepsilon) \cdot p(\varepsilon_b)^{\beta} \cdot p(\varepsilon_{b'})^{\beta'} \dots = P(\varepsilon) \cdot B(\varepsilon) = p^{\pi}$$

Jam nullum indicem a nulli indice b aequalem esse patet. Sint indices $c, c' \dots$ i , qui conjuncti cum indicibus a et b seriem $0, 1, 2, \dots, \lambda - 1$ efficiunt atque posito $C(\varepsilon) = p(\varepsilon_c) \cdot p(\varepsilon_c') \dots$ formetur expressio:

$$V(\varepsilon) = A(\varepsilon) + B(\varepsilon) \cdot C(\varepsilon)$$

normam hujus expressionis numerus p metiri nequit; tum enim pro uno valore e congruentiae $N(e - \varepsilon) \equiv 0 \pmod{p}$ esse deberet $V(e) \equiv 0 \pmod{p}$ ¹⁾ i. e.

$$A(e) + B(e) \cdot C(e) \equiv 0.$$

Quum vero pro quovis e unus tantum factorum $p(e)$ nihilo congruus esse possit²⁾ aut $A(e)$ aut $B(e)$ aut $C(e)$ minime igitur $A(e) + B(e) \cdot C(e)$ nihilo congruum erit. Quare jam existet numerus y talis ut sit: $y \cdot NV(\varepsilon) \equiv 1 \pmod{p^{\pi}}$ sive substituto ipsius $V(\varepsilon)$ valore:

$$y \cdot V(\varepsilon_1) \dots V(\varepsilon_{\lambda-1}) A(\varepsilon) + y \cdot V(\varepsilon_1) \dots V(\varepsilon_{\lambda-1}) B(\varepsilon) \cdot C(\varepsilon) \equiv 1 \pmod{p^{\pi}}.$$

Qua congruentia in numerum $P(\varepsilon)$ ducta, atque respectu habito aequationis $B(\varepsilon) \cdot P(\varepsilon) = p^{\pi}$, obtinemus:

$$\text{II. } y \cdot V(\varepsilon_1) \dots V(\varepsilon_{\lambda-1}) A(\varepsilon) \cdot P(\varepsilon) \equiv P(\varepsilon) \pmod{p^{\pi}}$$

Unde si illam congruentiam I:

$$x \cdot F(\omega^0) \dots F(\omega^{\nu-1}) \cdot f(\omega) \equiv A(\varepsilon) \cdot P(\varepsilon) \pmod{p^{\pi}}$$

respicimus atque $x \cdot F(\omega^0) \dots F(\omega^{\nu-1}) \cdot y \cdot V(\varepsilon_1) \dots V(\varepsilon_{\lambda-1}) = \psi(\omega)$ ponimus denique prodit congruentia:

$$\psi(\omega) \cdot f(\omega) \equiv P(\varepsilon) \pmod{p^{\pi}}$$

ubi numerum $P(\varepsilon)$ factorem esse numerorum $f(\omega)$ et p^{π} communem maximum ex ipsa expressionis $P(\varepsilon)$ definitione elucet. Istam congruentiam si tanquam aequationem scribimus designante $G(\omega)$ numerum integrum complexum, obtinemus:

$$\psi(\omega) \cdot f(\omega) = P(\varepsilon) + G(\omega) \cdot p^{\pi} \text{ sive } \psi(\omega) \cdot \frac{f(\omega)}{p^{\pi}} = \frac{1}{B(\varepsilon)} + G(\omega)$$

Casu $p = \nu$ habemus $f(\omega) = (1 - \omega)^{\pi} F(\omega)$ ubi numerus $NF(\omega)$ ad ipsum ν primus est³⁾. Jam posito $x \cdot NF(\omega) \equiv 1 \pmod{\nu^{\pi}}$ atque: $x \cdot F(\omega^0) \cdot F(\omega^1) \dots F(\omega^{\nu-1}) = \psi(\omega)$ obtinemus: $\psi(\omega) f(\omega) \equiv (1 - \omega)^{\pi} \pmod{\nu^{\pi}}$.

Jam posito $N = p^a \cdot q^b \dots$ ubi p, q, \dots sunt numeri primi inter se diversi, inveniri possunt numeri $\psi_1(\omega), \psi_2(\omega), \dots$ tales ut sint:

$$\psi_1(\omega) \cdot f(\omega) \equiv P(\varepsilon) \pmod{p^a}, \quad \psi_2(\omega) \cdot f(\omega) \equiv Q(\varepsilon') \pmod{q^b}, \dots$$

¹⁾ v. §. 2, 1. —

²⁾ v. §. 2, 4. —

³⁾ v. adnotationem §. 3, 2.

ubi $P(\varepsilon)$ $Q(\varepsilon')$, ... factores sunt communes maximi numerorum $f(\omega)$ et $p^a f(\omega)$ et q^b cet. Itaque habemus:

$$Q(\varepsilon') \cdot R(\varepsilon'') \dots \psi_1(\omega) \cdot f(\omega) = \chi_1(\omega) f(\omega) \equiv P(\varepsilon) Q(\varepsilon') \dots \text{mod. } p^a$$

$$P(\varepsilon) \cdot R(\varepsilon'') \dots \psi_2(\omega) \cdot f(\omega) = \chi_2(\omega) f(\omega) \equiv P(\varepsilon) Q(\varepsilon') \dots \text{mod. } q^b$$

$$\begin{matrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{matrix}$$

Deinde numerus inveniri potest complexus $\psi(\omega)$ talis ut sit:

$$\psi(\omega) \equiv \chi_1(\omega) \text{ mod. } p^a, \quad \psi(\omega) \equiv \chi_2(\omega) \text{ mod. } q^b, \dots$$

quia pro singulis coefficientibus potestatum radicum ω in ipsis $\chi(\omega)$ hae ipsae congruentiae expleri possunt. Unde denique habemus:

$$\psi(\omega) \cdot f(\omega) \equiv P(\varepsilon) \cdot Q(\varepsilon') \cdot R(\varepsilon'') \dots \text{mod. } N$$

ubi dextra congruentiae pars factorem numerorum $f(\omega)$ et N communem maximum continet.

§. 5.

Dato aliquo numero primo p , qui condicionem implet $p^a \equiv 1 \text{ mod. } p$ semper exstare numerum π talem, ut sit $\pi p = N(e - \varepsilon)$ jam supra diximus (v. §. 2.). Quem numerum π generaliter ita eligere possumus, ut sit ad p primus. Quodsi enim π numerum p ideoque $N(e - \varepsilon)$ numerum p^2 implicat, habemus:

$$N(p + e - \varepsilon) = \pi' p = N(e - \varepsilon) + p \left\{ (e - \varepsilon_1)(e - \varepsilon_2) \dots + (e - \varepsilon)(e - \varepsilon_s) + \dots \right\} + p^2 \left\{ \dots \right\}$$

Jam si et ipsum π' factorem p contineret etiam illa expressio per ipsum p multiplicata nihilo congrua foret modulo p . Quae expressio tanquam functio ipsorum ε symmetrica etiam mutatis quantitatibus ε cum numeris e nihilo congrua esse deberet. Tum autem omnes termini primo excepto evanescunt, qua de causa obtainemus:

$$(e - e_1)(e - e_2) \dots \equiv 0 \text{ mod. } p$$

sive igitur $e \equiv e_r \text{ mod. } p$ id quod fieri non potest, nisi pro certis quibusdam numeris p qui et ipsi divisores numeri $N(e - \varepsilon_r)$ sunt. Quodsi $e \equiv e_r \text{ mod. } p$ est quoque:

$$(e - e_r)(e_1 - e_{r+1}) \dots (e_{\lambda-1} - e_{r+\lambda-1}) \equiv 0 \equiv (e - e_r)(e_1 - e_{r+1}) \dots \equiv N(e - \varepsilon_r) \text{ mod. } p$$

Theorema. Si normam numeri complexi $Nf(\omega)$ numerus primus p metitur ad exponentem μ modulo ν pertinens atque $\pi p = N(e - \varepsilon)$ est, numerum $\pi \cdot f(\omega)$ aliquis factor $e - \varepsilon_x$ metiri debet.

Dem. Ponatur $f'(\omega) \cdot f'(\omega^{g^1}) \cdots f'(\omega^{g^{(u-1)\lambda}}) = \varphi(\varepsilon)$ ¹⁾. Tum habemus:
 $Nf'(\omega) = N\varphi(\varepsilon) \equiv 0 \pmod{p}$ ergo secundum §. 2, 1: $\varphi(e_r) \equiv 0 \pmod{p}$ et $\pi \cdot \varphi(e_r) \equiv 0 \pmod{\pi \cdot p}$ ideoque mod. $(e - \varepsilon)$. Deinde quum appareat esse $e \equiv \varepsilon$ et $e_r \equiv \varepsilon_r$ mod. $(e - \varepsilon)$ obtinemus congruentias: $\pi \varphi(e_r) \equiv \pi \cdot \varphi(\varepsilon_r) \equiv 0 \pmod{(e - \varepsilon)}$ sive $\pi \cdot \varphi(\varepsilon) \equiv 0 \pmod{(e - \varepsilon - r)}$ i. e.

$$\pi \cdot f'(\omega) \cdot f'(\omega^{g^1}) \cdots f'(\omega^{g^{(u-1)\lambda}}) \equiv 0 \pmod{(e - \varepsilon - r)}$$

sive si congruentiam $p \equiv g^\lambda$ respicimus:

$$\pi \cdot f'(\omega) \cdot f'(\omega^p) \cdots f'(\omega^{p^{u-1}}) \equiv 0 \pmod{(e - \varepsilon - r)}$$

Est vero $\pi \cdot f'(\omega) \cdot f'(\omega^p) \cdots f'(\omega^{p^{u-1}}) \equiv \pi \cdot f'(\omega)^{1+p+\dots+p^{u-1}}$ mod. πp ideoque mod. $(e - \varepsilon - r)$ ergo ratione supra adhibita:

$$\pi \cdot f'(\omega) \equiv 0 \pmod{(e - \varepsilon - r)} \text{ q. e. d.}$$

Qua ratione iterata facile supposita congruentia $Nf'(\omega) \equiv 0 \pmod{p^{n+u}}$ colligimus congruentiam locum habere hujusmodi:

$$\pi^{n+u} f'(\omega) \equiv 0 \pmod{(e - \varepsilon_x)^m \cdot (e - \varepsilon_{x'})^{m'} \cdots}$$

ubi $m + m' + \dots = n$ est.

§. 6.

Sit p numerus primus ut sit $p^u \equiv 1 \pmod{p}$ atque $\pi p = N(e - \varepsilon)$ sitque π numerus ad ipsum p primus. Deinde ponatur $(e - \varepsilon_1)(e - \varepsilon_2) \cdots (e - \varepsilon_{\lambda-1}) = \varphi(\varepsilon)$ ubi $\varphi(\varepsilon)$ ipsum p metiri non posse patet, quia positio $\varphi(\varepsilon) = p \cdot \psi(\varepsilon)$ esset $(e - \varepsilon) \cdot \varphi(\varepsilon) = N(e - \varepsilon) = \pi p = p \cdot \psi(\varepsilon) (e - \varepsilon)$ ergo $\pi = \psi(\varepsilon) (e - \varepsilon)$ et $\pi^\lambda = N\psi(\varepsilon) \cdot \pi p$ unde sequeretur, ut ipsum π per numerum p divisibile esset. — Jam numero complexo fracto $\frac{p}{\varphi(\varepsilon)}$ tanquam modulo ad hanc quae sequitur disquisitionem utamur; id quod facile fieri potest, si statuamus congruentiam $a \equiv b \pmod{\frac{m}{n}}$ locum tenere hujuscce $an \equiv bn \pmod{m}$.

Jam patet esse $e \equiv \varepsilon \pmod{\frac{p}{\varphi(\varepsilon)}}$; est enim re vera $(e - \varepsilon) \varphi(\varepsilon) \equiv 0 \pmod{p}$ quia $(e - \varepsilon) \varphi(\varepsilon) = N(e - \varepsilon) = \pi p$. Deinde si numerus complexus $f(\varepsilon)$ congruentiae sufficit $f(\varepsilon) \equiv 0 \pmod{\frac{p}{\varphi(\varepsilon)}}$ numerus p ejus normam metiatur oportet. Ex ista enim congruentia concluditur $f(\varepsilon) \cdot \varphi(\varepsilon) \equiv 0 \pmod{p}$ sive $Nf(\varepsilon) \cdot N\varphi(\varepsilon) \equiv 0$

¹⁾ v. Gauss disq. arithm. 345.

mod. p^{λ} et quum habeamus $Nq(\varepsilon) = p^{\lambda-1} \pi^{\lambda-1}$ obtinemus $\pi^{\lambda-1} Nf(\varepsilon) \equiv 0$ mod. p et quia π ad ipsum p primus est $Nf(\varepsilon) \equiv 0$ mod. p . — Ex illa congruentia $e \equiv \varepsilon$ sequitur, ut quivis numerus complexus numero reali congruus sit scilicet $f(\varepsilon) \equiv f(e)$ mod. $\frac{p}{q(\varepsilon)}$, unde p residua hoc modulo incongrua exstare eluet eaque numeri 0, 1, 2, ..., $p-1$. Etenim plures non existere inde patet quod quivis numerus complexus numero reali, quivis autem numerus realis unius illorum numerorum modulo p etiamque igitur modulo $\frac{p}{q(\varepsilon)}$ congruus est. Sin vero duo illorum numerorum inter se congrui essent, earum differentia nihilo congrua fieret. Quam si litera d designamus, esset $d q(\varepsilon) \equiv 0$ mod. p ergo $d^{\lambda} \cdot Nq(\varepsilon) = d^{\lambda} \cdot \pi^{\lambda-1} \cdot p^{\lambda-1} \equiv 0$ mod. p^{λ} ergo: $d^{\lambda} \cdot \pi^{\lambda-1} \equiv 0$ mod p id quod esse nequit quia π ad ipsum p primus atque $d < p$ est.

Jam accepto numero x ejusmodi, ut sit $x^{\lambda} \leq p < (x+1)^{\lambda}$ statuamus cunctos numeros complexos formae $c + c_1 \varepsilon + \dots + c_{\lambda-1} \varepsilon^{\lambda-1}$ in quibus coefficientes isti c valores 0, 1, 2, ..., x induunt. Horum multitudo erit $(x+1)^{\lambda} > p$ inter quos igitur certe duo inter se congrui erunt secundum modulum $\frac{p}{q(\varepsilon)}$. Quorum altero ab altero subtracto obtinemus numerum complexum $f(\varepsilon)$ cuius coefficientes omnes inter $-x$ et $+x$ sunt, et cuius norma numerum p continet, quum ipse nihilo congruus sit modulo $\frac{p}{q(\varepsilon)}$. Quare sit norma ejus $Nf(\varepsilon) = np$. Jam si litera M_{λ} maximum valorem expressionis $N(x + x_1 \varepsilon + \dots + x_{\lambda-1} \varepsilon^{\lambda-1})$ designamus, ea condicione ut quantitates x cunctae inter -1 et $+1$ sint, obtinemus:

$$\frac{np}{x^{\lambda}} = N \frac{f(\varepsilon)}{x} \text{ ideoque } \frac{np}{x^{\lambda}} < M_{\lambda} \text{ sive} \\ np < M_{\lambda} x^{\lambda} < M_{\lambda} p \text{ unde denique } n < M_{\lambda}$$

Hinc habemus hoc theorema magni momenti. Dato aliquo numero p qui conditionem implet $p^{\mu} \equiv 1$ mod. ν semper invenire licet numerum n minorem finita quadam quantitate ab ipso p independente eumque talem, ut productum np in λ factores complexos conjunctos dissolvi possit. Quod theorema respondeat illi in theoria formarum quadraticarum, quod numerus formarum reductarum finitus est. Etiam adnotandum illam rationem agendi adhiberi non posse ad eos numeros primos p qui divisores sunt numerorum $N(\varepsilon - \varepsilon_r)$ quarum igitur multitudo finita est. — Deinde ope hujus theorematis, quantitate M determinata, numerus quam

minimus inveniri potest numerorum n , quibus opus est, ut pro quolibet numero primo p proprietate supra dicta praedito unum productorum $n p$ norma numeri complexi sit.

Ut pro certis quibusdam numeris ν pro quovis ipsius $\nu - 1$ divisore λ omnes numeri primi, residua $\lambda^{\nu-1}$ potestatum ipsius ν , in λ factores complexos dissolvi possint¹⁾, tantummodo necesse est, numeros primos qui sint residua $\lambda^{\nu-1}$ potestatis modulo ν quantitatibus illis M_λ minores in λ factores complexos conjunctos discerpi posse²⁾. — Sit enim λ divisor ipsius $\nu - 1$, designetur deinde signo d quilibet ipsius λ divisor excepto ipso λ , probandum est, quemvis numerum primum, residuum $\lambda^{\nu-1}$ potestatis, in λ factores complexos dissolvi posse, si modo hoc pro numeris primis p ipso M_λ minoribus eveniat praetereaque omnes numeri primi residua $d^{\nu-1}$ potestatum in d factores complexos discerpi possint. Quum enim $n p$ tanquam norma repraesentari liceat, quumque factores ipsius n primi aut residua $d^{\nu-1}$ potestatum aut residua $\lambda^{\nu-1}$ potestatis iique $\leq n < M_\lambda$ sint, ideoque in factores complexos discerpi possint, respectu habitu theorematis §. 3, 2 sententiam illam probari eluet. Jam primum pro ipso λ factores ipsius $\nu - 1$ primos accipientes, illa quae ad divisores numeri λ spectat condicione sublata, ea tantum restat, ut numeri primi residua $\lambda^{\nu-1}$ potestatis quantitate M_λ minores in λ factores complexos discerpi possint. Deinde transeundo ad eos ipsius λ divisores, qui duabus tantum numeris primis constant, similem condicionem adjicieudam tantum esse patet: eaque ipsa ratione ad divisores ipsius $\nu - 1$ e pluribus factoribus primis compositos progredientes denique illam condicionem supra indicatam obtineri liquet. — Ita ut unum tantum exemplum afferamus posito $\nu = 5$ pro ipso numero $\nu - 1 = 4$ simplicissimis jam adjumentis $M_4 = 49$ invenitur. Jam vero tres numeri primi formae $5n + 1$ ipso M minores scilicet 11, 31, 41 in quatuor factores complexos conjunctos e radicibus unitatis quintis compositos discerpi possunt²⁾. Deinde pro divitore $\lambda = 2$ omnes numeri primi residua ipsius 5 quadraticia in duos factores complexos $(a + a_1 \varepsilon) \cdot (a + a_1 \varepsilon_1)$.

¹⁾ Ad notamus illud etiam ita exhiberi posse, ut pro his numeris ν omnes numeros primos formarum $x\nu + g^\lambda$ in λ factores complexos conjunctos dissolvi posse dicamus. Id quod illi sententiae equivalere e facili consideratione eluet.

²⁾ Addendum est praeterea eos numeros primos, qui numeros $N(\varepsilon - \varepsilon_r)$ metiantur pro se quoque disquirendos esse.

³⁾ v. Cli. Kummer disput. pag. 21.

dissolvi possunt. Id quod vel illa ipsa ratione erui vel e theoria formarum secundi gradus probari potest. Est enim $(a + a_1 \varepsilon)(a + a_1 \varepsilon_1) = (a + a_1 \omega + a_1 \omega^{-1}) \times (a + a_1 \omega^2 + a_1 \omega^{-2}) = a^2 - a a_1 - a_1^2$.

Hinc igitur quemvis numerum primum formae $5n+1$ in quatuor, quemvis numerum primum formae $5n-1$ in duos factores complexos conjunctos e radicibus unitatis quintis compositos discripi posse colligimus.

§. 7.

Jam transeuntes ad numeros ν compositos adnotamus, nos plerumque ut iteratione supersedere possimus ad methodos pro numeris primis exhibitas lectorem delegaturos esse, quippe quae in his quae sequantur paucis exceptis prorsus adhiberi possint.

Ponatur numerus compositus $\nu = a^\alpha \cdot b^\beta \cdot c^\gamma \dots$ designantibus a, b, c, \dots numeros primos inter se diversos sitque ω radix primitiva aequationis $x^\nu = 1$, hanc ipsam radicem esse aequationis:

$$f(x) = \frac{(x^\nu - 1)(x^{\frac{\nu}{ab}} - 1)(x^{\frac{\nu}{ac}} - 1) \dots}{(x^{\frac{\nu}{a}} - 1)(x^{\frac{\nu}{b}} - 1)(x^{\frac{\nu}{c}} - 1) \dots} = 0$$

notis methodis probatur, quae quidem aequatio $\varphi(\nu)$ ¹⁾ gradus¹⁾ omnes ν^{th} radices unitatis primitivas amplectitur. Hanc vero aequationem reduci non posse sive radices quasdam ω aequatione inferioris gradus atque coefficientium integrorum contineri non posse, hic probare omittimus²⁾ quum limites hujus libelli demonstrationem hic tradere non patientur. Ex ea vero aequationis illius proprietate sequitur, ut quaecunque functio ipsius ω integra pro quibusdam ipsius ω valoribus evanescat, eadem pro omnibus quoque reliquis valoribus nihilo aequalis fiat. Quod nisi fieret, factor communis maximus istius functionis et functionis $f(x)$, quum et idem functio sit integra, tamen illas certas tantum radices ω haberet atque factor functionis $f(x)$ foret, id quod fieri nequit. — Jam designentur radices primitivae numerorum a^α, b^β, \dots resp. literis g, h, \dots deinde ponatur $\frac{\nu}{a^\alpha} = a', \frac{\nu}{b^\beta} = b', \dots$ tum forma $a'g^m + b'h^n + \dots$ sistema numerorum ad numerum ν primorum atque inter se incongruorum contineri constat, si numeris m, n, \dots sensim sensim resp. valores

¹⁾ $\varphi(\nu)$ numerus ille est numerorum ad ipsum ν primorum eoque minorum.

²⁾ Demonstrationem illam, de qua sermo est, proximo tempore in Diario Crelliano in publicum editurus sum.

$1, 2, \dots a^{\alpha-1}(a-1); 1, 2, \dots b^{\beta-1}(b-1)$, etc. tribuuntur. — Nunc sit λ divisor aliquis ipsius $a^{\alpha-1}(a-1)$ talis ut multiplum sit ipsius $a^{\alpha-1}$, λ' divisor ipsius $b^{\beta-1}(b-1)$ multiplum ipsius $b^{\beta-1}$ etc. ita ut habeamus $\lambda\mu = a^{\alpha-1}(a-1)$, $\lambda'\mu' = b^{\beta-1}(b-1) \dots$ et ponatur:

$$\varepsilon_{x, x'} \dots = \sum_{m=0}^{m=\mu-1} \sum_{n=0}^{n=\mu'-1} \dots \omega^{a'g^{m\lambda+x} + b'h^{n\lambda'+x'}} + \dots$$

sive $\varepsilon_{x, x'} \dots = \sum_m \omega^{a'g^{m\lambda+x}} \cdot \sum_n \omega^{b'h^{n\lambda'+x'}} \dots$

quae expressiones partes periodorum in numeris primis ν agunt. — Numerus terminorum expressionis talis erit: $\mu \cdot \mu' \cdot \mu'' \dots$, numerus periodorum ε inter se diversarum: $\lambda \cdot \lambda' \cdot \lambda'' \dots$ quum quantitates x, x', \dots resp. valores $0, 1, 2 \dots \lambda-1; 0, 1, 2, \dots \lambda'-1$, etc. induere possint.

Productum $\Pi(x-\varepsilon)$, ubi signum Π in omnes ipsius ε valores extendi debet, functionem radicum ω symmetricam ideoque integris potestatum x coefficientibus gaudere appetet. — Per aequationem $\Pi(x-\varepsilon) = 0$, quippe quae sit gradus $\lambda \cdot \lambda' \cdot \lambda'' \dots$, quaevis ipsius ε potestas $\geq \lambda \lambda' \lambda'' \dots$ potestatibus inferioribus exprimi potest.

Duae periodi ε diversorum indicum aequales esse non possunt.

Primum enim ex aequatione $\varepsilon_{o, o, \dots} = \varepsilon_{x, x', x'', \dots}$ sequeretur aequatio ejusmodi $\varepsilon_{o, o, \dots} = \varepsilon_{x, m x', n x'', \dots}$ ¹⁾ designantibus m, n, \dots numeros quoscunque integrlos. Jam ponendo $m = b^{\beta-1}(b-1), n = c^{\gamma-1}(c-1)$ etc. obtinemus $\varepsilon_{o, o, o, \dots} = \varepsilon_{x, o, o, \dots}$ sive respecta illa altera ipsorum ε definitione atque sublatis factoribus utriusque partis communibus:

$$\sum \omega^{a'g^{m\lambda}} = \sum \omega^{a'g^{m\lambda+x}}$$

quumque $\omega^{a'}$ sit radix aequationis $x^{a^\alpha} = 1$ primitiva, pro iis unitatis radicibus, quae ad numerorum primorum potestates pertinent, illud theorema demonstrare sufficit. Quem ad finem designamus brevitatis causa signo ε_x expressionem $\sum \omega^{a'g^{m\lambda+x}}$ et ipsam radicem unitatis $a^{\alpha m}$ primitivam litera ω , ponatur denique $a^{\alpha-1}(a-1) = a$ ita ut habeamus $\varepsilon_x = \sum \omega^{g^{m\lambda+x}}$. Jam colliguntur ex aequatione $\varepsilon_o = \varepsilon_x$ haece: $\varepsilon_1 = \varepsilon_x + 1, \varepsilon_2 = \varepsilon_x + 2$ etc. unde igitur:

¹⁾ nempe mutando ipsum ω , id quod secundum supra dicta facere licet.

I. $\varepsilon + \varrho \varepsilon_1 + \varrho^2 \varepsilon_2 + \dots + \varrho^{\lambda-1} \varepsilon_{\lambda-1} = \varepsilon_x + \varrho \varepsilon_{x+1} + \varrho^2 \varepsilon_{x+2} + \dots + \varrho^{\lambda-1} \varepsilon_{x+\lambda-1}$
 ubi ϱ radix quaecunque sit aequationis $x^a = 1$. Posito:

$$\varrho + \varrho \omega^y + \varrho^2 \omega^{y^2} + \dots + \varrho^{a-1} \omega^{y^{a-1}} = (\varrho, \omega)$$

obtinemus secundum I. pro quovis ipsius ϱ valore, qui radix est aequationis $x^\lambda = 1$:

$$(\varrho, \omega) = (\varrho, \omega^{y^x}) = (\varrho, \omega) \cdot \varrho^{-x} \text{ unde } (\varrho, \omega) (1 - \varrho^{-x}) = 0$$

id quod certe fieri non posse pro radicibus ϱ aequationis $x^\lambda = 1$ primitivis jam probemus. Pro his enim $1 - \varrho^{-x}$ evanescere nequit, quia $x < \lambda$ est. Deinde (ϱ, ω) non evanescit, quod demonstrari potest¹) productum $(\varrho, \omega) (\varrho^{-1}, \omega) = \pm a^c$ evadere nisi $\varrho^{a^{c-2}(a-1)} = 1$; quumque λ multiplum ipsius a^{c-1} atque ϱ radicem aequationis $x^\lambda = 1$ primitivam supposuerimus, radicem ϱ aequationi $\varrho^{a^{c-2}(a-1)} = 1$ sufficere non posse ideoque quantitatem (ϱ, ω) non evanescere facile perspicitur.

Posito A, A_1, \dots numeros reales integros esse, expressio formae:

$$A + A_1 \varepsilon + A_2 \varepsilon^2 + \dots + A_{L-1} \varepsilon^{L-1} = f(\varepsilon)$$

numerus complexus dicetur.

Ex aequatione $f(\varepsilon) = 0$ colligitur $f(\varepsilon_x) = 0$, quia $f(\varepsilon)$ radicum ω functio est integra. — Deinde e relatione $f(\varepsilon) = 0$ colligimus esse $A = A_1 = A_2 = \dots = 0$. Quum enim $f(x)$ pro omnibus periodis ε i. e. pro L valoribus ipsius x (quos inter se diversos esse supra probavimus) evanescat, tamenque gradus tantum $L-1$ ² sit, coefficientes evanescere necesse est. Unde hae theorematum patent: duabus numeris complexis inter se aequalibus et singuli numeri conjuncti et coefficientes resp. aequales sunt.

Quaevis periodus $\varepsilon_x, \varepsilon'_x, \varepsilon''_x, \dots$ tanquam functio integra coefficientium rationalium unius periodi repraesentari potest. Ad quod probandum prium numerus ν potestas numeri primi ($\nu = a^c$) ponendus est. Jam designante litera ω radicem primitivam aequationis $x^a = 1$ ponatur:

$$\omega^{y^x} + \omega^{y^{1+x}} + \dots + \omega^{y^{(a-1)\lambda+x}} = \varepsilon_x = \varepsilon (\omega^{y^x})$$

denique $\lambda = a^{c-1} \cdot d$ et $d \cdot \mu = a - 1$.

Radix ω quum aequationi sufficiat:

$$1 + \omega^{a^{c-1}} + \omega^{2a^{c-1}} + \dots + \omega^{(a-1)a^{c-1}} = 0$$

ideoque $\omega^r + \omega^{r+a^{c-1}} + \omega^{r+2a^{c-1}} + \dots + \omega^{r+(a-1)a^{c-1}} = 0$ habemus

¹) Id quod fusius exponere omittimus.

²) Posuimus $L = \lambda \cdot \lambda' \cdot \lambda'' \dots$

aequationes: $\varepsilon(\omega^r) + \varepsilon(\omega^{a^{n-1}+r}) + \dots + \varepsilon(\omega^{(a-1)a^{n-1}+r}) = 0$ in quibus numerus r valores 1, 2, … $a^{n-1}-1$ induere potest. Inter quas vero quaeque μ inter se congruant, unde numerus aequationum inter se diversarum est $\frac{a^{n-1}-1}{\mu} + 1$ addita illa aequatione pro $r=0$ scilicet:

$$\mu + \varepsilon(\omega^{a^{n-1}}) + \dots + \varepsilon(\omega^{(a-1)a^{n-1}}) = 0.$$

Numerus expressionum omnium $\varepsilon(\omega^n)$ inter se diversarum est $\frac{a^{n-1}-1}{\mu}$, quarum autem $\frac{a^{n-1}-1}{\mu} + 1$ reliquis per illas aequationes lineariter exprimere licet; qua de causa tantum $\frac{a^{n-1}-a^{n-1}}{\mu} - 1$ sive $\lambda-1$ restant.

Jam quamvis ipsius $\varepsilon(\omega^y)$ potestatem tanquam functionem linearem omnium expressionum $\varepsilon(\omega^n)$ ideoque tanquam functionem linearem aliquarum ($\lambda-1$) quantitatum $\varepsilon(\omega^n)$ repraesentari posse nullo negotio perspicitur. Qua de causa ponamus potestates $\varepsilon_x^2, \varepsilon_x^3, \dots, \varepsilon_x^{\lambda-1}$ repraesentatas $\lambda-1$ expressionibus $\varepsilon(\omega^n)$ inter quas sint ε_x et $\varepsilon(\omega^n)$. Ex quibus $\lambda-2$ aequationibus reliquis $\lambda-3$ quantitatibus $\varepsilon(\omega^n)$ eliminatis restabit aequatio hujus formae:

$$A + A_1 \varepsilon_x + A_2 \varepsilon_x^2 + \dots + A_{\lambda-1} \varepsilon_x^{\lambda-1} = B \varepsilon(\omega^n)$$

ubi certe non omnes coefficientes A evanescere possunt. Coefficientem B evanescere non posse, solutionem igitur non illusoriam esse, inde eluet, quod functio periodi ε_x gradus $\lambda-1^n$ integra evanescere nequit, nisi ipsi coefficientes nihil aequales sunt¹).

Quodsi jam ν numerum aliquem compositum ponimus, atque

$$\Sigma \omega^{a^i g^{m\lambda+z}} = \varepsilon_x, \quad \Sigma \omega^{b^i h^{n\lambda+z'}} = \varepsilon'_{x'}, \text{ etc.}$$

igitur secundum illam definitionem: $\varepsilon_{x, x'} \dots = \varepsilon_x \cdot \varepsilon'_{x'} \dots$ scimus hoc productum exprimi posse producto functionum rationalium ipsorum $\varepsilon, \varepsilon', \varepsilon'', \dots$. Restat igitur, ut probemus quodvis productum $\varepsilon^i \cdot \varepsilon'^{i'} \dots$ repraesentari posse potestatis $(\varepsilon \cdot \varepsilon' \cdot \varepsilon'' \dots), (\varepsilon \cdot \varepsilon' \cdot \varepsilon'' \dots)^2, \dots, (\varepsilon \cdot \varepsilon' \cdot \varepsilon'' \dots)^{L-1}$. Quum vero quaeque i^a ipsius ε potestas potestate prima, secunda, etc., $(\lambda-1)^a$ exprimi possit, illae $L-1$ potestates quantitatis $(\varepsilon \cdot \varepsilon' \cdot \varepsilon'' \dots)$ repraesentari possunt variis productis $\varepsilon^i \cdot \varepsilon'^{i'} \dots$, in quibus $i < \lambda, i' < \lambda', \dots$ quorum igitur numerus est $\lambda \cdot \lambda' \cdot \lambda'' \dots = L$, vel excepto producto $\varepsilon^0 \cdot \varepsilon'^0 \dots = 1$ restant $L-1$ producta, quibus potestates $(\varepsilon \cdot \varepsilon' \dots)^2, (\varepsilon \cdot \varepsilon' \dots)^3, \dots$ expressae sunt. Ex quibus aequationibus $L-2$ si

¹) Id quod ratione supra (pag. 18) exhibita probatur.

omnia eliminamus producta exceptis $\varepsilon \cdot \varepsilon' \cdot \varepsilon'' \dots$ et certo quodam $\varepsilon^i \cdot \varepsilon^{i'} \dots$ quorum igitur multitudo $L - 3$, obtainemus aequationem formae:

$A + A_1(\varepsilon \cdot \varepsilon' \dots) + A_2(\varepsilon \cdot \varepsilon' \dots)^2 + \dots + A_{L-1}(\varepsilon \cdot \varepsilon' \dots)^{L-1} = B\varepsilon^i \cdot \varepsilon^{i'} \dots$
in qua certe non omnes coefficientes A evanescere possunt. Ideoque coefficien-
tem B non evanescere inde patet, quod functio periodi ε gradus $L - 1$ evanescere
nequit, nisi omnes ejus coefficientes evanescunt. (v. supra pag. 18.)

Ex quibus dictis satis elucet, quodque numerorum complexorum pro-
ductum rursus in formam:

$$A + A_1 \varepsilon + A_2 \varepsilon^2 + \dots + A_{L-1} \varepsilon^{L-1}$$

redigi posse ideoque et ipsum numerum complexum esse.

Productum numerorum conjunctorum omnium norma appellatur et sicut
supra signo $N(\varepsilon)$ denotatur.

Jam eadem ratione, qua Cl. Kummer in numeris primis ν demonstravit,
congruentiam λ'' gradus $N(x - \varepsilon) \equiv 0$ mod. p habere λ radices numero primo p
sufficiente condicione $p^\mu \equiv 1$ mod. ν et casu $p = \nu$ (v. §. 2); id quod huic rei
respondet positio ν numerum esse compositum probari potest: scilicet congruen-
tiam gradus $\lambda\lambda' \dots$ hanc $N(x - \varepsilon) \equiv 0$ mod. p habere totidem radices reales, si p
supponitur numerus talis, ut sit $p^\mu \equiv 1$ mod. $a^\alpha, p^{\mu'} \equiv 1$ mod. b^β, \dots vel etiam
pro aliquo ipso ipsius ν factori primo e. g. $p = a$ dummodo $a^{\mu'} \equiv 1$ mod. b^β
etc. sit¹⁾.

Pro talibus numeris primis p quales tantum congruentias sufficient

$$p^{a^\alpha \cdot \delta} \equiv 1 \text{ mod. } a^\alpha, p^{b^{\alpha'} \cdot \delta'} \equiv 1 \text{ mod. } b^\beta, \dots$$

(ubi $\delta, \delta' \dots$ divisores numerorum $a - 1, b - 1, \dots$ numeri autem α, α', \dots vel
omnes vel partim > 0 sunt) erit $N(x - \varepsilon) \equiv 0$ mod. p designante ε periodum
compositam e radicibus primitivis aequationis $z^{a^{\alpha-z} \cdot b^{\beta-z'}} \dots = 1$ atque habe-
buntur $\frac{q(\nu)}{a^\alpha \cdot \delta \cdot b^{\alpha'} \cdot \delta'} \dots$ istius congruentiae radices x .

Quibus jam praeparatis theorematibus, quae in paragraphis 2 — 6 pro
numeris primis ν tradita sunt, respondentia nullo fere negotio pro numeris com-
positis ν probari possunt.

¹⁾ Id quod etiam e theoremate quodam generali a Clo. Schoenemann in Diar. Crel-
liano tom. 19. pag. 293 tradito colligi potest.

PARS ALTERA.

§. 8.

Posito literas: $\nu, \mu, \lambda, \omega, \varepsilon$ eandem habere vim quam in §. 1 etiamque acceptis numeris complexis formae illius:

$$a\varepsilon + a_1\varepsilon_1 + \dots + a_{\lambda-1}\varepsilon_{\lambda-1} = f(\varepsilon)$$

numerum talem complexum, cuius norma sit ± 1 , unitatem complexam vocamus.

Disquisitio igitur unitatum complexarum eadem est, quae disquisitio formarum quarundam altiorum graduum $F = 1$. Normam enim numeri $a\varepsilon + a_1\varepsilon_1 + \dots + a_{\lambda-1}\varepsilon_{\lambda-1}$ formam esse λ^{ii} gradus atque λ indeterminatarum $a, a_1, \dots, a_{\lambda-1}$ et quidem determinantis, ut ita dicam, numeri primi ν sponte patet¹⁾. Quas formas fere partes aequationis Pellianaee agere imprimis ex eo eluet, quod casu $\lambda = 2$ atque $\nu \equiv 1 \pmod{4}$ sit $\varepsilon = -\frac{1}{2} + \frac{1}{2}\sqrt{\nu}, \varepsilon_1 = -\frac{1}{2} - \frac{1}{2}\sqrt{\nu}$

$$\text{unde: } Nf(\varepsilon) = \frac{1}{4} \left\{ (a + a_1)^2 - \nu(a - a_1)^2 \right\}$$

Nunc primum adnotamus ipsas unitatis radices ω unitates simplices appellari atque quilibet unitatem complexam unitate simplici multiplicatam realem reddi posse demonstrabimus, in qua demonstratione Cli. Kummer vestigia fere omnino sequemur²⁾.

Quum omnis periodorum functio etiam tanquam ipsarum radicum functio considerari possit, ponimus $f(\varepsilon) = \varphi(\omega)$ sitque $Nf(\varepsilon) = 1$ ergo etiam $N\varphi(\omega) = 1$.

Sit porro quotiens $\frac{\varphi(\omega)}{\varphi(\omega - 1)} = \psi(\omega)$ quem numerum integrum esse aper-
tum est, scilicet $\psi(\omega) = \varphi(\omega)^{\nu} \varphi(\omega^2) \dots \varphi(\omega^{\nu-2})$. Jam positio

$$\psi(\omega) = c + c_1\omega + c_2\omega^2 + \dots + c_{\nu-1}\omega^{\nu-1} \text{ additis aequationibus:}$$

$$\psi(\omega) \cdot \psi(\omega^{-1}) = 1, \psi(\omega^2) \cdot \psi(\omega^{-2}) = 1, \dots \psi(\omega^{\nu-1}) \cdot \psi(\omega^{-(\nu-1)}) = 1$$

$$\text{obtinemus: } \nu(c^2 + c_1^2 + \dots + c_{\nu-1}^2) - (c + c_1 + \dots + c_{\nu-1})^2 = \nu - 1^2$$

¹⁾ Cf. Eisenstein „de formis cubicis etc.” Diar. Crel. tom. 28.

²⁾ Disputatio Cli. Kummer §. 4.

³⁾ cf. id pag. 4 exposuimus.

unde $c + c_1 + \dots + c_{\nu-1} \equiv \pm 1 \text{ mod. } \nu$ quocirca haec coefficientium summa etiam aequalis ± 1 accipi potest. Itaque habemus:

$$c^2 + c_1^2 + \dots + c_{\nu-1}^2 = 1$$

unde sequitur, ut esse debeat $c_n = 1$ omnes reliqui vero numeri c nihilo aequales.

Invenimus igitur $\psi(\omega) = \frac{\varphi(\omega)}{\varphi(\omega^{-1})} = \omega^n$ esse unde: $\varphi(\omega) = \omega^n \cdot \varphi(\omega^{-1})$

atque posito $-n \equiv 2m \text{ mod. } \nu$ denique:

$$\omega^m \varphi(\omega) = \omega^{-m} \varphi(\omega^{-1})$$

ex qua aequatione apparet, quamlibet unitatem $\varphi(\omega)$, multiplicando per unitatem quandam simplicem, talem fieri posse, ut mutato ω in ω^{-1} immutata maneat i.e. ut functio ipsorum $\omega + \omega^{-1}$, $\omega^2 + \omega^{-2}$, ... ergo realis evadat. Sive si ad unitates formae $f(\epsilon)$ revertimur, unitates complexae tanquam functiones periodorum paris terminorum numeri accipi possunt.

Jam ostendemus pro quibusvis numeris ν et λ unitates existere infinite multas easque inter se diversas. Posito enim:

$$\varphi(\omega) = \frac{(1 - \omega^g)(1 - \omega^{g\lambda+1}) \dots (1 - \omega^{g(\mu-1)\lambda+1})}{(1 - \omega)(1 - \omega^{g\lambda}) \dots (1 - \omega^{g(\mu-1)\lambda})} = \psi(\epsilon)$$

normam hujus expressionis unitati aequalem facile patet, quum norma et numeratori et denominatoris sit ν^μ . Deinde illam expressionem numerum complexum integrum esse patet, quum pro se quisque factor numeratoris $(1 - \omega^{g\lambda+1})$ factore quodam denominatoris $(1 - \omega^{g\lambda})$ dividi possit quia $\frac{1 - \omega^{g\lambda+1}}{1 - \omega^{g\lambda}} = \frac{1 - x^g}{1 - x}$ posito $\omega^{g\lambda} = x$. Denique illa expressio functio periodorum ϵ est, quia mutata radice ω in $\omega^{g\lambda}$ immutata manet. Hinc igitur patet $\psi(\epsilon)$ unitatem esse integrum complexam. — Etiamque producta:

$$\psi(\epsilon)^n \cdot \psi(\epsilon_1)^{n_1} \dots \psi(\epsilon_{\lambda-1})^{n_{\lambda-1}}$$

designantibus $n_1, n_2, \dots, n_{\lambda-1}$ quoscunque numeros integros unitates integras complexas esse appareat, quas quidem omnes inter se diversas infra probabimus.

Adnotamus quamvis quantitatatem $\psi(\epsilon_x)$ positivam realem esse. Etenim quum numerus μ par suppositus sit, cuique factori

$$1 - \omega^{g^{n\lambda+x+1}} \text{ factor } 1 - \omega^{-g^{n\lambda+x+1}}$$

respondet. Quibus multiplicatis obtinemus $2 - 2 \cos v = 4 \sin^2 \frac{1}{2}v$ ubi $v = \frac{2}{\nu} \cdot g^{n\lambda+x+1} \cdot \pi$. Unde jam et numeratorem et denominatorem ipsius $\psi(\epsilon_x)$ positivum esse eluet.

§. 9.

Sit unitas illa $\psi(\varepsilon) = c\varepsilon + c_1\varepsilon_1 + \dots + c_{\lambda-1}\varepsilon_{\lambda-1}$, quam positivam realem esse modo demonstravimus, atque ponatur:

$$c\varepsilon + c_1\varepsilon_1 + \dots + c_{\lambda-1}\varepsilon_{\lambda-1} = r_1$$

$$c\varepsilon_1 + c_1\varepsilon_2 + \dots + c_{\lambda-1}\varepsilon = r_2$$

I.

$$\begin{matrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{matrix}$$

$$c\varepsilon_{\lambda-1} + c_1\varepsilon + \dots + c_{\lambda-2}\varepsilon_{\lambda-2} = r_{\lambda}$$

Deinde sit data aliqua unitas $a\varepsilon + a_1\varepsilon_1 + \dots + a_{\lambda-1}\varepsilon_{\lambda-1}$ atque designentur similiter valores absoluti factorum conjunctorum resp. literis $f_1, f_2, \dots, f_{\lambda}$. Jam

ponantur:

$$f_1 = r_1^{n_1} \cdot r_2^{n_2} \cdots r_{\lambda-1}^{n_{\lambda-1}}$$

$$f_2 = r_2^{n_1} \cdot r_3^{n_2} \cdots r_{\lambda}^{n_{\lambda-1}}$$

$$f_3 = r_3^{n_1} \cdot r_4^{n_2} \cdots r_1^{n_{\lambda-1}}$$

II.

$$\begin{matrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{matrix}$$

$$f_{\lambda-1} = r_{\lambda-1}^{n_1} \cdot r_{\lambda}^{n_2} \cdots r_{\lambda-3}^{n_{\lambda-1}}$$

$$f_{\lambda} = r_{\lambda}^{n_1} \cdot r_1^{n_2} \cdots r_{\lambda-2}^{n_{\lambda-1}}$$

Quod sistema $\lambda-1$ aequationum atque $\lambda-1$ indeterminatarum n est, nam aequationibus omnibus multiplicatis per condicionem $f_1 f_2 \cdots f_{\lambda} = r_1 r_2 \cdots r_{\lambda} = 1$ aequationem identicam $1=1$ obtinemus, unde sequitur ut quaevis istarum aequationum $\epsilon \lambda-1$ reliquis deduci possit. Quodsi in systemate II. logarithmos pro numeris adhibemus atque signis log. $f_x = \varphi_x$, log. $r_x = \varrho_x$ valores logarithmorum naturalium denotamus, obtinetur:

$$\varphi_1 = n_1 \varrho_1 + n_2 \varrho_2 + \dots + n_{\lambda-1} \varrho_{\lambda-1}$$

$$\varphi_2 = n_1 \varrho_2 + n_2 \varrho_3 + \dots + n_{\lambda-1} \varrho_{\lambda}$$

III.

$$\begin{matrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{matrix}$$

$$\varphi_{\lambda} = n_1 \varrho_{\lambda} + n_2 \varrho_1 + \dots + n_{\lambda-2} \varrho_{\lambda-2}$$

Quibus aequationibus deinceps per $1, \alpha, \alpha^2, \dots, \alpha^{\lambda-1}$ multiplicatis (ubi α radix aliqua unitatis λ^n est) iisque additis eadem qua in §. I usi sumus ratione obtinemus:

$$\text{IV. } q_1 + q_2 \alpha + \dots + q_{\lambda} \alpha^{\lambda-1} = (n_1 + n_2 \alpha^{-1} + \dots + n_{\lambda-1} \alpha^{-(\lambda-2)}) \\ \times (\varrho_1 + \varrho_2 \alpha + \dots + \varrho_{\lambda} \alpha^{\lambda-1})$$

$$\text{Jam positis: } q_1 + q_2 \alpha + q_3 \alpha^2 + \dots + q_{\lambda} \alpha^{\lambda-1} = \varphi(\alpha) \\ \varrho_1 + \varrho_2 \alpha + \varrho_3 \alpha^2 + \dots + \varrho_{\lambda} \alpha^{\lambda-1} = \varrho(\alpha)$$

erit $\varphi(\alpha) = \varrho(\alpha)(n_1 + n_2 \alpha^{-1} + \dots + n_{\lambda-1} \alpha^{-(\lambda-2)})$ ergo:

$$\text{V. } \frac{\varphi(\alpha) \cdot \varrho(\alpha^2) \cdot \varrho(\alpha^3) \dots \varrho(\alpha^{\lambda-1})}{\varrho(\alpha) \cdot \varrho(\alpha^2) \cdot \varrho(\alpha^3) \dots \varrho(\alpha^{\lambda-1})} = n_1 + n_2 \alpha^{-1} + \dots + n_{\lambda-1} \alpha^{-(\lambda-2)}$$

quae aequatio systematis III. solutionem repraesentat. Etenim posito brevitatis causa:

$$\frac{\varphi(\alpha) \cdot \varrho(\alpha^2) \dots \varrho(\alpha^{\lambda-1})}{\varrho(\alpha) \cdot \varrho(\alpha^2) \dots \varrho(\alpha^{\lambda-1})} = \psi(\alpha)$$

atque designante α radicem unitatis λ^{am} primitivam aequatio V. locum tenet aequationum:

$$\psi(\alpha^x) = n_1 + n_2 \alpha^{-x} + \dots + n_{\lambda-1} \alpha^{-x(\lambda-2)}$$

pro valoribus ipsius $x : 1, 2, \dots, \lambda-1$. Unde (sicut pag. 4) colligimus esse:

$$\alpha^x \cdot \psi(\alpha) + \alpha^{2x} \psi(\alpha^2) + \dots + \alpha^{(\lambda-1)x} \cdot \psi(\alpha^{\lambda-1}) = \lambda n_x - (n_1 + n_2 + \dots + n_{\lambda-1})$$

et $\alpha^{\lambda-1} \psi(\alpha) + \alpha^{2(\lambda-1)} \psi(\alpha^2) + \dots + \alpha^{(\lambda-1)^2} \cdot \psi(\alpha^{\lambda-1}) = -(n_1 + n_2 + \dots + n_{\lambda-1})$
ergo denique:

$$\text{VI. } \lambda n_x = (\alpha^x - \alpha^{-1}) \psi(\alpha) + (\alpha^{2x} - \alpha^{-2}) \psi(\alpha^2) + \dots + (\alpha^{(\lambda-1)x} - \alpha) \psi(\alpha^{\lambda-1})$$

qua aequatione re vera quodvis n quantitatibus ϱ et φ expressum est.

Sed etiam determinantem systematis III. non evanescere, demonstrandum est. Qui determinans denominator sinistrae partis aequationis V. scilicet productum $\varrho(\alpha) \cdot \varrho(\alpha^2) \dots \varrho(\alpha^{\lambda-1})$ est, designante α radicem primitivam. Ergo probandum est, nullum istius producti factorem evanescere seu quantitatem:

$$\varrho_1 + \varrho_2 \alpha + \varrho_3 \alpha^2 + \dots + \varrho_{\lambda} \alpha^{\lambda-1} = \sum_{x=0}^{\lambda-1} \varrho_{x+1} \alpha^x$$

pro quavis unitatis radice λ^{a} unitate excepta a nihilo diversam esse. — Jam substituto ipsius ϱ_{x+1} valore scilicet:

$$\varrho_{x+1} = \log. r_{x+1} = \log. \frac{(1-\omega^{g^x+1}) (1-\omega^{g^x+1+\lambda}) \dots (1-\omega^{g^x+1+(\mu-1)\lambda})}{(1-\omega^{g^x}) (1-\omega^{g^x+\lambda}) \dots (1-\omega^{g^x+(\mu-1)\lambda})}$$

sive: $\varrho_{x+1} = \log. (1-\omega^{g^x+1}) + \log. (1-\omega^{g^x+1+\lambda}) + \dots + \log. (1-\omega^{g^x+1+(\mu-1)\lambda})$
 $- \log. (1-\omega^{g^x}) - \log. (1-\omega^{g^x+\lambda}) - \dots - \log. (1-\omega^{g^x+(\mu-1)\lambda})$

$\varrho(\alpha) = \sum \varrho_{x+1} \alpha^x$ abit in:

$$\begin{aligned} & \sum_{o}^{\lambda-1} \left\{ \log. (1 - \omega^{g^x+1}) + \log. (1 - \omega^{g^x+1+\lambda}) + \dots + \log. (1 - \omega^{g^x+1+(\mu-1)\lambda}) \right\} \alpha^x \\ & - \sum_{o}^{\lambda-1} \left\{ \log. (1 - \omega^{g^x}) + \log. (1 - \omega^{g^x+\lambda}) + \dots + \log. (1 - \omega^{g^x+(\mu-1)\lambda}) \right\} \alpha^x \\ & \text{sive } = \sum_{x=0}^{\lambda-1} \alpha^x \cdot \log. (1 - \omega^{g^x+1}) - \sum_{x=0}^{\lambda-1} \alpha^x \log. (1 - \omega^{g^x}) \end{aligned}$$

ratione scilicet habita aequationis $\alpha^{x+s\lambda} = \alpha^x$.

Jam quum sit:

$$\begin{aligned} & - \log. (1 - \omega^{g^x}) = \frac{\omega^{g^x}}{1} + \frac{\omega^{2g^x}}{2} + \frac{\omega^{3g^x}}{3} + \dots \text{ fit:} \\ & - \sum_{o}^{\lambda-1} \alpha^x \log. (1 - \omega^{g^x}) = \sum_n \sum_{x=0}^{\lambda-1} \alpha^x \cdot \frac{\omega^{ng^x}}{n} \end{aligned}$$

in qua summatione n omnes numeros integros positivos ad numerum ν primos designat. Nam pro valoribus $n=r\nu$ fit:

$$\omega^{ng^x} = 1 \text{ et } \sum_{o}^{\lambda-1} \frac{\alpha^x}{n} = \frac{1}{n} (1 + \alpha + \alpha^2 + \dots + \alpha^{\lambda-1}) = 0$$

Quodsi Cli. Jacobi signis utimur¹⁾ expressio

$$\sum_n \sum_{o}^{\lambda-1} \alpha^x \cdot \frac{\omega^{ng^x}}{n} \text{ abit in } \sum_n \frac{1}{n} (\alpha, \omega^n)$$

et adhibita relatione $(\alpha, \omega^n) = \alpha^{-Ind. n} (\alpha, \omega)$ obtinemus:

$$- \sum \alpha^x \cdot \log. (1 - \omega^{g^x}) = (\alpha, \omega) \sum \frac{\alpha^{-Ind. n}}{n}$$

et mutato ω in ω^g :

$$\sum \alpha^x \cdot \log. (1 - \omega^{g^x+1}) = -(\alpha, \omega^g) \sum \frac{\alpha^{-Ind. n}}{n}$$

$$\text{i. e. } \sum \alpha^x \cdot \log. (1 - \omega^{g^x+1}) = -\alpha^{-1} (\alpha, \omega) \cdot \sum \frac{\alpha^{-Ind. n}}{n}$$

Ergo habemus denique:

$$\varrho(\alpha) = (1 - \alpha^{-1}) (\alpha, \omega) \sum_n \frac{\alpha^{-Ind. n}}{n}$$

Jam neque factor (α, ω) neque $(1 - \alpha^{-1})$ evanescere potest. Prior enim sententia ex aequatione $(\alpha, \omega) (\alpha^{-1}, \omega) = \pm \nu$ secunda ex eo, quod α ab unitate diversum positum est, elucet. Restat igitur, ut factorem $\sum_n \frac{\alpha^{-Ind. n}}{n}$ non evanescere probetur. Tum etiam $\sum_n \frac{\alpha^{-Ind. n}}{n}$ evanescere deberet, id quod pro

¹⁾ Monatsberichte d. Berliner Akademie, Jahrg. 1837.

nullo α quod sit radix aequationis $x^{\nu-1} = 1$ ideoque etiam pro nulla radice unitatis $\lambda^\nu \alpha$ (excepta unitate) fieri posse Cl. Lejeune-Dirichlet in illustri illa commentatione „de progressionem arithmetica infinita” etc. §. 4 et 5 singularibus illis methodis demonstravit.

§. 10.

Si in valoribus quantitatum n aequatione IV §. 9 determinatis, numeros integros quam maximos secernimus, ita ut sint: $n_1 = E_1 + \delta_1$, $n_2 = E_2 + \delta_2$, ... quantitatibus δ inter 0 et 1 acceptis, aequationes II §. 9 mutantur in:

$$\text{I. } f_i = r_1^{-E_1} \cdot r_2^{-E_2} \cdots r_{\lambda-1}^{-E_{\lambda-1}} \cdot r_1^{\delta_1} r_2^{\delta_2} \cdots r_{\lambda-1}^{\delta_{\lambda-1}}$$

etc.

Ex quibus aequationibus quum et f_i et $r_1^{-E_1} \cdot r_2^{-E_2} \cdots r_{\lambda-1}^{-E_{\lambda-1}}$ unitates integrae complexae sint, alterum quoque dextrae partis factorem: $r_1^{\delta_1} \cdot r_2^{\delta_2} \cdots r_{\lambda-1}^{\delta_{\lambda-1}}$ unitas integra complexa sit oportet. Ponatur igitur:

$$r_1^{\delta_1} r_2^{\delta_2} \cdots r_{\lambda-1}^{\delta_{\lambda-1}} = F_i = A \varepsilon + A_1 \varepsilon_1 + \cdots + A_{\lambda-1} \varepsilon_{\lambda-1}$$

$$r_2^{\delta_1} r_3^{\delta_2} \cdots r_\lambda^{\delta_{\lambda-1}} = F_2 = A \varepsilon_1 + A_1 \varepsilon_2 + \cdots + A_{\lambda-1} \varepsilon$$

II.

$$\begin{array}{ccc} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{array}$$

$$r_\lambda^{\delta_1} r_1^{\delta_2} \cdots r_{\lambda-2}^{\delta_{\lambda-1}} = F_\lambda = A \varepsilon_{\lambda-1} + A_1 \varepsilon + \cdots + A_{\lambda-1} \varepsilon_{\lambda-2}$$

designantibus A , A_1 , ... numeros integros. Quo facto secundum aequationes illas VII. §. 1 has quae sequuntur aequationes tanquam istius systematis aequationum II. solutionem nanciscimur:

$$-\nu \cdot A = F_1(\mu - \varepsilon) + F_2(\mu - \varepsilon_1) + \cdots + F_\lambda(\mu - \varepsilon_{\lambda-1})$$

$$-\nu \cdot A_1 = F_1(\mu - \varepsilon_1) + F_2(\mu - \varepsilon_2) + \cdots + F_\lambda(\mu - \varepsilon)$$

III.

$$\begin{array}{ccc} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{array}$$

$$-\nu \cdot A_{\lambda-1} = F_1(\mu - \varepsilon_{\lambda-1}) + F_2(\mu - \varepsilon) + \cdots + F_\lambda(\mu - \varepsilon_{\lambda-2})$$

Periodos ε minores esse numero μ , quo numerum terminorum periodi designavimus, facile perspicitur. Nam quaevis periodus ε (posito $\frac{1}{2}\mu = m$) formae est:

$$\omega^{x_1} + \omega^{-x_1} + \omega^{x_2} + \omega^{-x_2} + \cdots + \omega^{xm} + \omega^{-xm}$$

sive igitur formae

$$2 \left\{ \cos \frac{2x_1 \pi}{\nu} + \cos \frac{2x_2 \pi}{\nu} + \cdots + \cos \frac{2\pi}{\nu} x_m \right\}$$

quod aggregatum cosinuum ipsorum numero $\binom{\mu}{2}$ minus esse in promtu est.

Deinde absolutos ipsorum F valores limites quosdam $\mathfrak{F}_1, \mathfrak{F}_2, \dots$ superare non posse ex aequationibus II. et condicionibus, quibus ibidem quantitates δ sunt circumscriptae, colligi potest. Unde sequitur, ut quantitates quoque $-v A, -v A_1, \dots$ limitibus quibusdam contineantur, scilicet quum quantitates $\mu - \varepsilon$ sint positivae:

$$\begin{aligned} \mathfrak{F}_1(\mu - \varepsilon_x) + \mathfrak{F}_2(\mu - \varepsilon_{x+1}) + \dots + \mathfrak{F}_\lambda(\mu - \varepsilon_{x-1}) &> -v A_x \\ -\mathfrak{F}_1(\mu - \varepsilon_x) - \mathfrak{F}_2(\mu - \varepsilon_{x+1}) - \dots - \mathfrak{F}_\lambda(\mu - \varepsilon_{x-1}) &< -v A_x \end{aligned}$$

sive

$$\frac{1}{v} \left\{ \mathfrak{F}_1(\mu - \varepsilon_x) + \dots + \mathfrak{F}_\lambda(\mu - \varepsilon_{x-1}) \right\} > A_x > -\frac{1}{v} \left\{ \mathfrak{F}_1(\mu - \varepsilon_x) + \dots + \mathfrak{F}_\lambda(\mu - \varepsilon_{x-1}) \right\}$$

Quum vero A_x numerus integer esse debeat, multitudinem tantum finitam numerorum A, A_1, \dots etiamque igitur numerum finitum unitatum F , quae forma in II. accepta gaudeant, existere posse patet.

Quae quum conferamus cum aequatione I. sequitur, ut quaelibet unitas f potestatis integris unitatum conjunctarum $r_1, r_2, \dots, r_{\lambda-1}$ et unitatibus quibusdam numeri finiti exprimi possint; i. e. ut cunctae unitates forma

$$F \cdot r_1^{x_1} \cdot r_2^{x_2} \cdots r_{\lambda-1}^{x_{\lambda-1}}$$

contineantur, designantibus x_1, x_2, \dots numeros integros et F unitatem quandam e numero unitatum finito electam sive denique ut numerus unitatum fundamentium quarum potestatis integris omnis unitas repraesentari queat, finitus sit.

§. 11.

Jam accuratius, quibus limitibus numeri integri A, A_1, \dots sint circumscripti, consideratur sumus, quo labor inveniendi unitates fundamentales aliquanto diminuatur. Ad quem finem disquisitionem instituamus de illis expressionibus:

$$\text{I. } -v A_x = F_1(\mu - \varepsilon_x) + F_2(\mu - \varepsilon_{x+1}) + \dots + F_\lambda(\mu - \varepsilon_{x-1})$$

$$\text{ubi } F_n = r_n^{\delta_1} \cdot r_{n+1}^{\delta_2} \cdots r_{n-2}^{\delta_{\lambda-1}}$$

eamque consideremus tanquam functionem quantitatum δ . Quotientes differentiales istius functionis I. respectu quantitatum $\delta_1, \delta_2, \dots$ sunt:

$$F_1(\mu - \varepsilon_x) \varrho_1 + F_2(\mu - \varepsilon_{x+1}) \varrho_2 + \dots + F_\lambda(\mu - \varepsilon_{x-1}) \varrho_\lambda$$

$$F_1(\mu - \varepsilon_x) \varrho_1 + F_2(\mu - \varepsilon_{x+1}) \varrho_2 + \dots + F_\lambda(\mu - \varepsilon_{x-1}) \varrho_\lambda$$

II.

$$\begin{array}{ccc} \cdot & \cdot & \cdot \\ \vdots & \vdots & \vdots \\ \cdot & \cdot & \cdot \end{array}$$

in quibus formulis notatione jam supra adhibita $\log. r_x = \varrho_x$ usi sumus.

Quotientes differentiales secundi et quidem ii, quos expressionum II. prima respectu δ_1 , secunda respectu δ_2 , etc. differentiatis obtinemus, erunt:

$$\begin{aligned} F_1(\mu - \varepsilon_x) \varepsilon_1^2 + F_2(\mu - \varepsilon_{x+1}) \varepsilon_2^2 + \dots + F_k(\mu - \varepsilon_{x-1}) \varepsilon_k^2 \\ F_1(\mu - \varepsilon_x) \varepsilon_1^2 + F_2(\mu - \varepsilon_{x+1}) \varepsilon_2^2 + \dots + F_k(\mu - \varepsilon_{x-1}) \varepsilon_k^2 \\ \vdots \quad \vdots \quad \vdots \\ \vdots \quad \vdots \quad \vdots \end{aligned}$$

quas expressiones pro quibusvis quantitatibus δ valoribus positivas manere elucet. Unde facili consideratione colligi potest functionem illam I. dum variabiles δ intervallum inter 0 et 1 percurrunt, valorem haud majorem obtinere posse eo, qui inter valores functionis extremis ipsorum δ valoribus respondentes maximus sit. Quare quaestio de valore ipsius νA_x absolute maximo ad disquisitionem valorum, qui ad valores quantitatum δ hos: 0 et 1 pertinent, restringitur. Valoribus igitur quantitatum r computatis, quantitates F combinationibus quibusvis valorum 0 et 1 pro ipsis δ (multitudinis igitur 2^{k-1}) respondentes computentur, ut valor earum maximus M inveniatur. Sit numerus integer ipso $\frac{M}{\nu}$ minor eique proximus = n ; jam unitates omnes complexae cuius coefficientes inter $-n$ et $+n$ sunt statuendae atque inter eas, quae ad alias reduci possunt rejiciendae ut tandem numerus unitatum fundamentalium quam minimus restet.

Sic e. g. posito $\nu = 7$, $k = 3$ atque $r_1 = \omega + \omega^{-1}$ etc. iste numerus $n = 1$ sine magno labore invenitur, ita ut valores coefficientium sint: $-1, 0, +1$. Numeri igitur complexi 24 disquirendi ¹⁾ inter quos vero terni factores sunt conjuncti. Inter octo illos, qui supersunt, rursus bini numeros aequales sed signo tantum oppositos praebent, ita ut denique hi quatuor restent:

$$\begin{aligned} \varepsilon_1 &= \omega + \omega^{-1} \\ \varepsilon_1 + \varepsilon_2 &= \omega + \omega^{-1} + \omega^2 + \omega^{-2} = \varepsilon_2 \cdot \varepsilon_3 \\ \varepsilon_1 + \varepsilon_2 - \varepsilon_3 &= \omega + \omega^{-1} + \omega^2 + \omega^{-2} - \omega^3 - \omega^{-3} = -\varepsilon_2 \cdot \varepsilon_3 \\ \varepsilon_1 - \varepsilon_2 &\text{ unitas complexa non est.} \end{aligned}$$

Quumque tres illas unitates unitatibus ipsis ε exprimere liceat, has ipsas tanquam fundamentales accipere possumus i. e. quarum potentatibus integris omnes unitates complexae ad $\nu = 7$, $k = 3$ pertinentes repraesentari possint.

Haud inutile videtur hoc ipsum exemplum paulo uberior exponere, ut id de quo agitur magis in promtu sit. Quum enim sit:

$$N(x\varepsilon + y\varepsilon_1 + z\varepsilon_2) = (x + y + z)^3 - 7(xy^2 + yz^2 + zx^2 + xyz) = \varphi(x, y, z)$$

¹⁾ nempe omissis his: 0, $\varepsilon_1 + \varepsilon_2 + \varepsilon_3$, $-\varepsilon_1 - \varepsilon_2 - \varepsilon_3$.

solutionem formae $\varphi(x, y, z) = \pm 1$ numeris integris ita invenimus, ut numeri x, y, z integri determinantur aequationibus¹⁾:

$$\begin{aligned} -7x &= (\omega + \omega^{-1})^m \cdot (\omega^2 + \omega^{-2})^n \cdot (2 - \omega - \omega^{-1}) + (\omega^2 + \omega^{-2})^m \cdot (\omega^3 + \omega^{-3})^n \cdot (2 - \omega^2 - \omega^{-2}) \\ &\quad + (\omega^3 + \omega^{-3})^m \cdot (\omega + \omega^{-1})^n \cdot (2 - \omega^3 - \omega^{-3}) \\ -7y &= (\omega + \omega^{-1})^m \cdot (\omega^2 + \omega^{-2})^n \cdot (2 - \omega^2 - \omega^{-2}) + (\omega^2 + \omega^{-2})^m \cdot (\omega^3 + \omega^{-3})^n \cdot (2 - \omega^3 - \omega^{-3}) \\ &\quad + (\omega^3 + \omega^{-3})^m \cdot (\omega + \omega^{-1})^n \cdot (2 - \omega - \omega^{-1}) \\ -7z &= (\omega + \omega^{-1})^m \cdot (\omega^2 + \omega^{-2})^n \cdot (2 - \omega^3 - \omega^{-3}) + (\omega^2 + \omega^{-2})^m \cdot (\omega^3 + \omega^{-3})^n \cdot (2 - \omega - \omega^{-1}) \\ &\quad + (\omega^3 + \omega^{-3})^m \cdot (\omega + \omega^{-1})^n \cdot (2 - \omega^2 - \omega^{-2}) \end{aligned}$$

designantibus m, n quoslibet numeros integros. Quod exemplum analogiam aequationis Pellianae prae se ferre appetet.

§. 12.

Postquam demonstravimus numerum unitatum fundamentalium finitum esse, de hoc ipso numero disquisitiones instituamus ac primum quidem illum numerum ipso $\lambda - 1$ minorem esse non posse sumus probaturi.

Sint igitur unitates fundamentales: f, f', f'', \dots quarum logarithmi resp. literis $\varphi, \varphi', \varphi'', \dots$ designentur. Quodsi literis $r_1, r_2, \dots; \varrho_1, \varrho_2, \dots$ eadem quam in paragraphis antecedentibus tribuimus vim, hae ipsae unitates potestatis integris ipsorum f exprimi possint, oportet. Quare sit:

$$r_1 = f^{a_1} \cdot f'^{b_1} \cdot f''^{c_1} \dots \qquad \varrho_1 = a_1\varphi + b_1\varphi' + c_1\varphi'' + \dots$$

$$r_2 = f^{a_2} \cdot f'^{b_2} \cdot f''^{c_2} \dots \qquad \varrho_2 = a_2\varphi + b_2\varphi' + c_2\varphi'' + \dots$$

.

.

$$r_{\lambda-1} = f^{a_{\lambda-1}} \cdot f'^{b_{\lambda-1}} \cdot f''^{c_{\lambda-1}} \dots \varrho_{\lambda-1} = a_{\lambda-1}\varphi + b_{\lambda-1}\varphi' + c_{\lambda-1}\varphi'' + \dots$$

Quum vero numerus quantitatum φ sit $\leq \lambda - 2$, his ipsis eliminatis certe una restabit aequatio formae:

$$\text{I. } n_1\varrho_1 + n_2\varrho_2 + \dots + n_{\lambda-1}\varrho_{\lambda-1} = 0$$

in qua aequatione n_1, n_2, \dots non omnes nihilo aequales atque numeri integri esse deberent, quum et ipsa a, b, c, \dots numeri sint integri. Id quod esse non posse sequentibus probatur.

Ex aequatione enim I. colligimus aequationem: $r_1^{n_1} \cdot r_2^{n_2} \dots r_{\lambda-1}^{n_{\lambda-1}} = 1$ unde rursus mutatis periodis quae expressionibus r continentur hoc oritur aequationum sistema:

¹⁾ v. III. §. 10.

$$\begin{aligned} r_1^{n_1} r_2^{n_2} \cdots r_{\lambda-1}^{n_{\lambda-1}} &= 1 \\ r_2^{n_1} r_3^{n_2} \cdots r_\lambda^{n_{\lambda-1}} &= 1 \\ &\vdots \\ r_\lambda^{n_1} r_1^{n_2} \cdots r_{\lambda-2}^{n_{\lambda-1}} &= 1. \end{aligned}$$

Unde per aequationem IV. §. 9. obtinemus:

$$(n_1 + n_2 \alpha^{-1} + \cdots + n_{\lambda-1} \alpha^{-(\lambda-2)}) (\varrho_1 + \varrho_2 \alpha + \cdots + \varrho_{\lambda} \alpha^{\lambda-1}) = 0$$

pro quoque ipsius α valore. Quum autem factorem secundum non evanescere jam supra (§. 9.) demonstratum sit, factor prior pro quoque ipsius α valore unitate excepta evanescere deberet id quod fieri nequit nisi $n_1 = n_2 = \cdots = 0$.

§. 13.

Antequam vero ad ulteriorem disquisitionem accedamus minime a re abhorrere videtur notationem quandam indicare qua formulae magnopere contrahantur.

Designantibus enim $r_1, r_2 \dots r_{\lambda-1}, r_\lambda$ unitates aliquas conjunctas, denotamus productum $r_1^{n_1} \cdot r_2^{n_2} \cdots r_{\lambda-1}^{n_{\lambda-1}}$ signo:

$$r_1^{n_1} + n_2 \alpha + \cdots + n_{\lambda-1} \alpha^{\lambda-2} = r_1^{n(\alpha)}$$

Id quod ita quoque exhiberi potest, ut dicamus positio:

$$r_1^{n_1} \cdot r_2^{n_2} \cdots r_{\lambda-1}^{n_{\lambda-1}} = f_1$$

pro aequationibus illis (IV. §. 9.):

$$\varphi(\alpha^x) = (n_1 + n_2 \alpha^{-x} + \cdots + n_{\lambda-1} \alpha^{-(\lambda-2)}) \varrho(\alpha^x)$$

substitui aequationem:

$$f_1 = r_1^{n_1} + n_2 \alpha + \cdots + n_{\lambda-1} \alpha^{\lambda-2}.$$

Jam primum adnotandum est, productum $r_1^{n_1} \cdot r_2^{n_2} \cdots r_\lambda^{n_\lambda}$ aequatione $r_1 \cdot r_2 \cdots r_\lambda = 1$ ad productum $\lambda-1$ terminorum pariterque numerum complexum $n(\alpha)$ ope aequationis $1 + \alpha + \alpha^2 + \cdots + \alpha^{\lambda-1}$ ad expressionem $\lambda-1$ terminorum redigi posse.

E definitione statim sequuntur aequationes:

$$\begin{aligned} r_1^{n(\alpha)} &= r_1^{\alpha-1 n(\alpha)} = r_2^{\alpha-2 n(\alpha)} = \cdots = r_\lambda^{\alpha-(\lambda-1) n(\alpha)} \\ r_1^{m(\alpha)} + n(\alpha) &= r_1^{m(\alpha)} \cdot r_1^{n(\alpha)} \end{aligned}$$

Etiamque altera potestatum verarum virtute hoc nostrum symbolum gaudet, scilicet:

$$[r_1^{n(\alpha)}]^{m(\alpha)} = r_1^{n(\alpha) \cdot m(\alpha)}$$

Posito enim $r_1^{n(\alpha)} = s_1$ et $[r_1^{n(\alpha)}]^{m(\alpha)} = s_1^{m(\alpha)} = t_1$ habemus aequationes: $r_1^{n_1} \cdot r_2^{n_2} \cdots = s_1$, $r_2^{n_1} \cdot r_3^{n_2} \cdots = s_2$, ... quae posito $\log s_x = \sigma_x$ secundum §. 9, II.—IV. eandem habent vim quam aequatio:

$$n(\alpha^{-1})\varrho(\alpha) = \sigma(\alpha)$$

quae ipsa ut supra aequationum $\lambda - 1$ locum tenet. Eodem modo est:

$$m(\alpha^{-1}) \cdot \sigma(\alpha) = \tau(\alpha) \text{ ergo } n(\alpha^{-1}) \cdot m(\alpha^{-1}) \varrho(\alpha) = \tau(\alpha)$$

pro qua igitur aequatione, quod ad definitionem nostram, substituere possumus hanc: $t_1 = r_1^{n(\alpha)} \cdot m(\alpha)$ q. e. d.

Jam patet posito λ numerum primum esse istos exponentes symbolicos sicuti numeros complexos tractari posse, quum omnes eorum reductiones eo tantum niterentur, ut sit: $1 + \alpha + \alpha^2 + \cdots + \alpha^{\lambda-1} = 0$ id quod cum nostra definitione consentit scilicet $r_1^{-1} + \alpha + \cdots + \alpha^{\lambda-1} = r_1 \cdot r_2 \cdots r_\lambda = 1 = r_1^0$.

Deinde praemittendum est, literis r illa priore vi gaudentibus quum nullum factorem $\varrho(\alpha)$ evanescere demonstratum sit, unitates $r_1^{n(\alpha)}$ et $r_1^{m(\alpha)}$ aequales esse non posse nisi $n_1 = m_1$, $n_2 = m_2$, ..., $n_{\lambda-1} = m_{\lambda-1}$ i. e. nisi $n(\alpha) = m(\alpha)$ pro omnibus λ'' unitatis radicibus excepta unitate.

Demonstravimus in §. 9. quamvis unitatem complexam formam $r_1^{n_1} \cdot r_2^{n_2} \cdots r_{\lambda-1}^{n_{\lambda-1}}$ contineri, quae quantitates n etiam loco citato determinatae sunt. Jam vero istas quantitates rationales esse probabimus. — Etenim initio §. 10, posita unitate integra complexa $f_1 = r_1^{n_1} \cdot r_2^{n_2} \cdots r_{\lambda-1}^{n_{\lambda-1}}$ etiam productum $r_1^{\delta_1} \cdot r_2^{\delta_2} \cdots r_{\lambda-1}^{\delta_{\lambda-1}}$ unitatem integrum esse ostendimus, si quantitates δ residua sunt ipsorum n numero integro quam maximo subtracto. Quum vero quis numerus irrationalis variis numeris integris multiplicatus innumera praebat residua unitate minora eaque inter se diversa, quumque unitas f ad potestatem aliquam integrum evecta rursus unitas integra sit, variis potestatibus integris unitatis f innumeritas unitates inter se diversas formae $r_1^{\delta_1} \cdot r_2^{\delta_2} \cdots r_{\lambda-1}^{\delta_{\lambda-1}}$ (ubi $\delta_1, \delta_2, \dots < 1$) obtineri posse elucet. Illo autem §. 10 finitum tantummodo numerum unitatum complexarum hujus formae existere demonstravimus; id quod itaque a propositione nostra, quantitates n irrationales esse, abhorret. — Quod quum conferamus cum forma §. 10 (sub finem) omnes unitates formae esse patet:

$$r_1^{\frac{m(\alpha)}{n}} \cdot r_1^{\tau(\alpha)}$$

designantibus $m(\alpha)$, $\tau(\alpha)$ numeros integros complexos, n numerum realem, in qua quidem numerus fractionum diversarum $\frac{m(\alpha)}{n}$ finitus est.

§. 14.

Jam primum ad casum simpliciorem accedamus in quo scilicet λ numerus primus ponitur. Quem quoque talem supponimus, ut quivis numerus formae $x\lambda + g^d$ (designante d divisorem numeri $\lambda - 1$) in d factores complexos dissolvi queat (v. §. 6).

Quum secundum supra dicta numerus unitatum formae $r^{\frac{m(\alpha)}{n}}$ (quibus praeter ipsas r ad repraesentandas omnes opus sit) finitus sit, hae ipsae sint:

$$\text{I. } r^{\frac{m(\alpha)}{n}}, r^{\frac{m'(\alpha)}{n'}}, \dots .$$

Jam sit factor numerorum $m(\alpha)$ et n communis maximus $v(\alpha)$ ¹⁾ ita ut $m(\alpha) = a(\alpha) \cdot v(\alpha)$, $n = c(\alpha) \cdot v(\alpha)$, loco illius exponentis $\frac{m(\alpha)}{n}$ scribere licet hunc: $\frac{a(\alpha)}{c(\alpha)}$. Quumque $a(\alpha)$ et $c(\alpha)$ nullum amplius factorem communem habeant, numerus inveniri potest $b(\alpha)$ talis, ut sit $b(\alpha) \cdot a(\alpha) \equiv 1 \pmod{c(\alpha)}$ (v. §. 4) sive $b(\alpha) \cdot a(\alpha) = 1 + F(\alpha) \cdot c(\alpha)$. Quum vero $r^{\frac{m(\alpha)}{n}} = r^{\frac{a(\alpha)}{c(\alpha)}}$ unitas integra sit, eadem proprietate unitatem $r^{\frac{a(\alpha) \cdot b(\alpha)}{c(\alpha)}} = r^{\frac{1}{c(\alpha)}} \cdot r^{F(\alpha)}$ ideoque etiam unitatem $r^{\frac{1}{c(\alpha)}}$ gaudere patet. De qua unitate quum illa unitas data deduci possit, scilicet evehendo eam ad potestatem integrum $a(\alpha)$, hanc ipsam loco illius accipere convenit. Hinc elucet, pro illis unitatibus I. accipi posse unitates hujus formae:

$$\text{II. } r^{\frac{1}{n(\alpha)}}, r^{\frac{1}{n'(\alpha)}}, \dots .$$

Ut harum unitatum binae in unam conflentur, sit factor numerorum $n(\alpha)$ et $n'(\alpha)$ communis maximus $c(\alpha)$ ita ut sit $n(\alpha) = c(\alpha) \cdot m(\alpha)$, $n'(\alpha) = c(\alpha) \cdot m'(\alpha)$. Jam quum numeri $m(\alpha)$ et $m'(\alpha)$ nullum amplius habeant factorem communem, numerus inveniri potest $a(\alpha)$ talis, ut sit $a(\alpha) \cdot m(\alpha) \equiv 1 \pmod{m'(\alpha)}$ (v. §. 4) sive $a(\alpha) \cdot m(\alpha) + b(\alpha) \cdot m'(\alpha) = 1$. Quum vero unitates $r^{\frac{b(\alpha)}{n(\alpha)}}$ et $r^{\frac{b(\alpha)}{n'(\alpha)}}$ integrae sint, unitates quoque $r^{\frac{a(\alpha)}{n(\alpha)}}$ et $r^{\frac{a(\alpha)}{n'(\alpha)}}$, etiamque $r^{\frac{b(\alpha)}{n(\alpha)}} \cdot r^{\frac{a(\alpha)}{n'(\alpha)}} = r^{\frac{b(\alpha)}{n(\alpha)}} + \frac{a(\alpha)}{n'(\alpha)}$ integras esse in promtu est. Est vero:

$$\frac{b(\alpha)}{n(\alpha)} + \frac{a(\alpha)}{n'(\alpha)} = \frac{1}{c(\alpha)} \left\{ \frac{b(\alpha)}{m(\alpha)} + \frac{a(\alpha)}{m'(\alpha)} \right\} = \frac{1}{c(\alpha) \cdot m(\alpha) \cdot m'(\alpha)}$$

unde igitur unitatem $r^{\frac{1}{c(\alpha) \cdot m(\alpha) \cdot m'(\alpha)}}$ integrum esse liquet.

¹⁾ De factore communi maximo sermonem esse posse e suppositione illa de natura ipsius λ facta elucet. (Cf. adnotatio ad. §. 4.)

$\frac{1}{1}$

De qua quum illae unitates $r^{\frac{1}{n(\alpha)}}$ et $r^{\frac{1}{m(\alpha)}}$ evehendo eam resp. ad potestates integras $m'(\alpha)$ et $n(\alpha)$ deduci possint, hanc ipsam loco illarum accipere licet. Qua ratione agendi iterata denique loco unitatum I. vel II. una restabit formae $r^{\frac{1}{v(\alpha)}}$, qua praeter unitates r ad repraesentandas omnes unitates opus erit. Quodsi $r^{\frac{1}{v(\alpha)}} = u$ ponimus, est $r = u^{v(\alpha)}$ ex qua aequatione, ut ipsae unitates r integris ipsorum u potestatibus exprimi possint, sequitur; ergo forma:

$$u_1^{\frac{n(\alpha)}{1}} = u_1^{n_1} \cdot u_2^{n_2} \cdots u_{\lambda-1}^{n_{\lambda-1}}$$

designantibus $n_1, n_2, \dots, n_{\lambda-1}$ quoscunque numeros integros reales, omnes unitates integrae complexae eaeque solae continentur.

Postquam hanc methodum quasi geneticam exposuimus, aliam allaturi sumus rationem, quae hujus paragraphi summam a posteriori probet.

§. 15.

Unitas r nisi ipsa fundamentalis est, praeter eas unitates, quae potestatis ipsius r integris complexis repraesentari possunt, numerus finitus existet unitatum formae: $r^{\frac{1}{n}}$. Inter quas erit una quaedam (vel plures) in qua norma exponentis i. e. $N^{\frac{m(\alpha)}{n}}$ reliquis minor est. Qualem unitatem litera u designemus. Quae unitas eam habet proprietatem, ut si quae exstet unitas integra formae: $u^{\frac{h(\alpha)}{x}}$ norma exponentis i. e. $N^{\frac{h(\alpha)}{x}}$ unitate major sit oporteat. Etenim quum $r^{\frac{1}{n}} = u$ ideoque $r^{\frac{m(\alpha)}{n}} \cdot r^{\frac{h(\alpha)}{x}} = u^{\frac{m(\alpha)}{n}} \cdot u^{\frac{h(\alpha)}{x}}$ praetereaque $N^{\frac{m(\alpha)}{n}} \cdot \frac{h(\alpha)}{x} > N^{\frac{m(\alpha)}{n}}$ secundum suppositionem de unitate u factam esse debeat, illa condicio $N^{\frac{h(\alpha)}{x}} > 1$ sponte manat. — Jam demonstrabimus unitatem u illa ratione electam fundamentalem esse, sive nullam existere unitatem integrum, nisi quae ejus potestate integra complexa repraesentari possit. Quodsi enim unitas exstet formae $u^{\frac{h(\alpha)}{x}}$ sive formae $u^{\frac{m(\alpha)}{n}}$ ubi numeros $m(\alpha)$ et $n(\alpha)$ omni factori communi carere supponere licet, numerus $a(\alpha)$ inveniri potest talis, ut sit $a(\alpha) m(\alpha) \equiv 1 \pmod{n(\alpha)}$ (v. §. 4). Quum vero unitas $u^{\frac{m(\alpha)}{n}}$ ideoque $u^{\frac{a(\alpha)m(\alpha)}{n(\alpha)}}$ integra sit, ratione supra (§. 14) adhibita unitatem quoque $u^{\frac{1}{n(\alpha)}}$ integrum esse colligimus. Ergo secundum supra exhibita $N^{\frac{1}{n(\alpha)}} \geq 1$ esse debet i. e. $Nn(\alpha) \leq 1$. Quum vero $Nn(\alpha)$ tanquam numerus integer unitate minor esse nequeat, tantum restat ut sit $Nn(\alpha) = 1$ i. e. ut numerus $n(\alpha)$

unitas complexa sit. Unde ut fractio $\frac{m(\alpha)}{n(\alpha)}$ tanquam numerus complexus integer scribi possit atque igitur ut omnes unitates integrae potestatibus ipsius n integris complexis repraesentari possint sequitur.

§. 16.

Postquam ostendimus existere unitates quasdam fundamentales numeri $\lambda - 1$ easque conjunctas in numeris λ illa virtute initio §. 14. memorata praeditis, de his ipsis quaedam adnotamus. Designentur unitates aliquae fundamentales ut supra literis: $u_1, u_2 \dots u_{\lambda-1}$ has ipsas tales esse ostendimus, ut: $u_i^{n(\alpha)}$ cunctas repraesentet unitates, posito $n(\alpha)$ numerum aliquem integrum complexum. Quaeque unitates n ea ipsa proprietate gaudent, fundamentales sunt. Nunc designante $x(\alpha)$ unitatem aliquam complexam integrum atque posito: $u_i^{x(\alpha)} = v_i$ aperte est:

$$u_1^{x(\alpha) x(\alpha^2) \dots x(\alpha^{\lambda-1})} = u_i = v_i^{x(\alpha^2) \dots x(\alpha^{\lambda-1})} = v_i^{K(\alpha)}$$

quae aequatio ipsam unitatem n potestate integra complexa ipsius v reprezentat, unde hanc ipsam quoque unitatem v fundamentalem esse eluet. Sive posita aliqua unitate fundamentali n omnes unitates fundamentales eaeque solae forma continentur: $u^{x(\alpha)}$ designante $x(\alpha)$ unitatem complexam. Hinc colligimus existere tot unitates fundamentales quot unitates diversae ex numeris integris et radicibus unitatis λ^n compositae ergo pro $\lambda = 2$ duae, pro $\lambda = 3$ sex, pro $\lambda \geq 5$ numerus infinitus exstat unitatum fundamentalium conjunctarum. — Etiamque unitates $\lambda - 1$ non conjunctae statui possunt, quarum potestatibus integris cunctae repraesentari possunt unitates. Posito enim:

$$u_1^{a_1} \cdot u_2^{a_2} \cdots u_{\lambda-1}^{a_{\lambda-1}} = A$$

$$u_1^{b_1} \cdot u_2^{b_2} \cdots u_{\lambda-1}^{b_{\lambda-1}} = B$$

⋮ ⋮ ⋮

designantibus a, b, \dots numeros integros obtinebimus aequationes $\lambda - 1$:

$$a_1 \log. u_1 + a_2 \log. u_2 + \cdots + a_{\lambda-1} \log. u_{\lambda-1} = \log. A$$

$$b_1 \log. u_1 + b_2 \log. u_2 + \cdots + b_{\lambda-1} \log. u_{\lambda-1} = \log. B$$

⋮ ⋮ ⋮

ex quo systemate quantitates $\log. u_1, \log. u_2, \dots$ determinari possunt, idque hac ratione:

$$A \cdot \log. u_1 = m_1 \cdot \log. A + m_2 \cdot \log. B + \dots$$

designante A determinantem illius systematis; $m_1, m_2 \dots$ numeros quosdam integros. Hinc jam patet, si sistema istud ea gaudet proprietate ut sit $A = \pm 1$, unitates u ideoque omnes unitates potestatibus integris unitatum A, B, \dots exprimi posse. Unde etiam tales unitates A, B, \dots infinitis modis (dummodo $\lambda \geq 3$) eligi posse, plane in promtu est.

Quae ut ad unum tantum exemplum adhibeamus, ponamus uti in §. 11 $\nu = 7, \lambda = 3$. Loco citato ostendimus unitates: $u_1 = \omega + \omega^{-1}, u_2 = \omega^2 + \omega^{-2}$ sive $u_1 = \varepsilon_1, u_2 = \varepsilon_2$ fundamentales esse. Jam quum sint unitates pro $\lambda = 3$ sex scilicet:

$$1, \alpha, \alpha^2, -1, -\alpha, -\alpha^2$$

habemus sexies binas unitates conjunctas fundamentales:

$$\begin{array}{ll} u_1^{-1} \text{ ergo } \varepsilon_1, \varepsilon_2 & u_1^{-1} \dots \varepsilon_1 + \varepsilon_2, \varepsilon_2 + \varepsilon_3 \\ u_1^{-\alpha} \dots \varepsilon_2, \varepsilon_3 & u_1^{-\alpha} \dots \varepsilon_2 + \varepsilon_3, \varepsilon_3 + \varepsilon_1 \\ u_1^{-\alpha^2} \dots \varepsilon_3, \varepsilon_1 & u_1^{-\alpha^2} \dots \varepsilon_3 + \varepsilon_1, \varepsilon_1 + \varepsilon_2 \end{array}$$

deinde positis $u_1^{a_1} \cdot u_2^{a_2} = A, u_1^{b_1} \cdot u_2^{b_2} = B$ erit:

$$a_1 \log. u_1 + a_2 \log. u_2 = \log. A$$

$$b_1 \log. u_1 + b_2 \log. u_2 = \log. B$$

ideoque $A = a_1 b_2 - a_2 b_1 = \pm 1$ condicio illa, ut unitates A et B partes unitatum fundamentalium agant. Cui aequationi innumeris modis satisfieri potest. E. g. positis:

$$a_1 = 3, a_2 = 2, b_1 = 4, b_2 = 3$$

habemus ut unitates fundamentales:

$$A = u_1^3 \cdot u_2^2 = 5\varepsilon_1 + \varepsilon_2 + 3\varepsilon_3, B = u_1^4 \cdot u_2^3 = 11\varepsilon_1 + 2\varepsilon_2 + 7\varepsilon_3.$$

Jam relictis iis, quae in dissertatione de unitatibus ad formas graduum (λ) ceterorum praesertim compositorum pertinentibus conscripsi, impressionem hujus libelli hic praecido; brevi autem in diario Crelliano accuratiorem earum disquisitionum expositionem in publicum editurus sum.



V I T A.

Natus sum ego Leopoldus Kronecker Lignicii d. VII m. Decembris anni h. s. XXIII patre Isidoro matre Johanna e gente Prausnitzeriana. Quos mihi Deus o. m. ad summam senectutem conservet. Religioni addictus sum mosaicae. Literarum elementis imbutus gymnasium Ligniciense adii, quod tunc beato Pinzger deinde Kochler, viro doctissimo, florebat. Ex praecceptorum numero, quorum ibi usus sum disciplina optime de excolendo ingenio merchantur Proreector Dr. Werner, quem jam defunctum lugeo, et Dr. Kummer v. cl. h. t. professor p. o. in universitate literaria Vratislaviensi, qui alter me jam dum in gymnasio ipso versabar sublimioribus matheseos partibus imbuebat. Quorum etiam consuetudine me usum esse gaudeo, debitamque pro utilitate quam inde percepi gratiam nullo tempore me abjecturum esse promitto. Maturitatis testimonio instructus vere anni XLI ab rectore magnifico Illo. Lichtenstein ab Illo. Zumpt decano maxime spectabili philosophorum ordini adscriptus sum universitatis lit. Berolinensis. Postquam vere anni XLIII universitatem almam Fridericianam Bonensem, autumno universitatem Vratislavensem adii, denique autumno anni XLIV ad universitatem Berolinensem reverti. Scientiis mathematicis operam dedi. Duces mihi studiorum fuere: viri III. doct. Lejeune-Dirichlet, Encke, Jacobi, Ohm, Steiner; Dove, Mitscherlich; Argelander; Kummer; — in philosophia et philologia: Schelling, Heydemann, Werder; Ritschl, Dahlmann; Haase. — Quibus viris gratias maximas et ago et semper agam.

T H E S E S.

- I. Rempublicam summam societatis humanae formam esse nego.
 - II. In natura nihil supervacaneum est.
 - III. Mathesis et ars et scientia dicenda.
 - IV. Fermatius theorema suum inlytum non demonstravit.
-