Werk

Titel: Journal für die reine und angewandte Mathematik

Verlag: de Gruyter

Jahr: 1882

Kollektion: Mathematica

Werk Id: PPN243919689_0093

PURL: http://resolver.sub.uni-goettingen.de/purl?PID=PPN243919689_0093|LOG_0004

Contact

Niedersächsische Staats- und Universitätsbibliothek Göttingen
Georg-August-Universität Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen
Germany
Email: gdz@sub.uni-goettingen.de

De unitatibus complexis.

Dissertatio inauguralis arithmetica *).

(Auctore *L. Kronecker.*)

In principalia doctrinae numerorum incrementa introductionem numerorum complexorum, ipsi summo huius scientiae creatori debitam, referendam esse inter omnes constat. Qui numeri quam vim ad promovendam scientiam habeant, inde elucet, 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 theoriam postea Cl. *Lejeune-Dirichlet* uberius tractavit**). Generalioris numerorum complexorum speciei mentionem fecit Cl. *Jacobi,* qui circuli sectionem pertractans in hanc quaestionem incidit***). Praeterea ad hanc partem doctrinae numerorum spectant et observatio Cli. *Jacobi* †) et recentiore tempore disputatio Cli. *Kummer* „de numeris complexis qui unitatis radicibus et numeris integris realibus constant," et commentatio Illi. *Eisenstein* „de formis cubicis trium variabilium etc." ††). — Ex quo prospectu, quam pauca de numeris complexis huc usque in publicum edita sint, iam elucet, ideoque in sequentibus praecipue tantum ad illam Cli. *Kummer* disputationem lectorem reiicere potero. Cum vero nonnulla theoremata in illa commentatione iam tradita elegantius demonstrare mihi contigerit, etiamque alia quaedam nondum tradita ad perscrutandas unitates complexas adhibenda sint, cumque denique, quoad nunc possim,

*) Haec dissertatio aestate anni MDCCCXLV ordini philosophorum universitatis Berolinensis proposita eique ex auctoritate summi viri *Lejeune-Dirichlet* probata est. Typis autem tum non excusa est nisi pars aliqua, scilicet paragraphi 1—16, quae publice prodiit d. X. m. Septembris a. MDCCCXLV; quae sequuntur paragraphi 17—20 ineditae adhuc nunc primum evulgantur.

**) *Crelles* Journal Bd. 24.

***) Monatsberichte der Berliner Akademie, 1837 (S. 127 sqq.); v. etiam commentationem Illi. *Eisenstein.* „Beiträge zur Kreistheilung" (*Crelles* Journal Bd. 27).

†) *Crelles* Journal Bd. 19 S. 314. ††) *Crelles* Journal Bd. 28.

totum aliquod conficere velim, disquisitionem fere ab initio repetere praeferam. Quem ad finem pars prior huius dissertationis, unitatibus complexis deditae, illas disquisitiones numerorum complexorum quasi fundamentales continebit.

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 cum acciperem his meis disquisitionibus iam 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 alicuius momenti esse arbitror.

PARS PRIOR.

§ 1.

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

Sint aequationis algebraicae n^{ti} gradus coefficientibus integris (coefficiens ipsius x^n sit unitas) n radices: α, β, γ etc. atque eiusdem aequationis, si tanquam congruentiam modulo p (ubi p numerus primus) consideres, n radices: a, b, c etc.; sit porro $f(\alpha, \beta, \gamma, \ldots)$ functio radicum algebraica integra symmetrica, congruentiam

$$f(\alpha, \beta, \gamma, \ldots) \equiv f(a, b, c, \ldots) \pmod{p}$$

locum habere dico.

Dem. Etenim quamque functionem radicum algebraicam integram symmetricam *identice* tanquam functionem integram expressionum: $\alpha+\beta+\gamma+\cdots$, $\alpha\beta+\alpha\gamma+\cdots$ etc. repraesentari posse constat. Ergo $f(a, b, c, \ldots)$ eadem functio integra expressionum: $a+b+\cdots$, $ab+ac+\cdots$ etc., quae $f(\alpha, \beta, \gamma, \ldots)$ ipsarum $\alpha+\beta+\gamma+\cdots$, $\alpha\beta+\alpha\gamma+\cdots$ etc. sit oportet. Cum vero $a+b+c+\cdots$ coefficienti ipsius x^{n-1} i. e. quantitati $\alpha+\beta+\gamma+\cdots$ pariterque $ab+ac+\cdots$

ipsi $\alpha\beta+\alpha\gamma+\cdots$ 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 ε, ε_1, ... $\varepsilon_{\lambda-1}$ periodi radicum ω, quarum quaeque μ terminos contineat, ita ut habeamus $\lambda\mu = \nu - 1$ et:

$$\text{(I.)} \quad \begin{cases} \varepsilon &= \omega + \omega^{g^\lambda} + \omega^{g^{2\lambda}} + \cdots + \omega^{g^{(\mu-1)\lambda}}, \\ \varepsilon_1 &= \omega^g + \omega^{g^{\lambda+1}} + \omega^{g^{2\lambda+1}} + \cdots + \omega^{g^{(\mu-1)\lambda+1}}, \\ & \vdots \quad\quad \vdots \quad\quad \vdots \\ \varepsilon_{\lambda-1} &= \omega^{g^{\lambda-1}} + \omega^{g^{2\lambda-1}} + \omega^{g^{3\lambda-1}} + \cdots + \omega^{g^{\mu\lambda-1}}, \end{cases}$$

ubi g est radix primitiva ipsius ν. Ex quibus aequationibus statim colligitur:

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

Iam posito

$$a\varepsilon + a_1\varepsilon_1 + a_2\varepsilon_2 + \cdots + a_{\lambda-1}\varepsilon_{\lambda-1} = f(\varepsilon)^*),$$

ubi literis: a, a_1, ... $a_{\lambda-1}$ numeri reales integri designantur, talem expressionem $f(\varepsilon)$ numerum complexum voco. Iam 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 iam laudata (§ 1) usus est ratione, ex aequatione:

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

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

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

$$\text{(II.)} \quad \begin{cases} a\varepsilon + a_1\varepsilon_1 + \cdots + a_{\lambda-1}\varepsilon_{\lambda-1} &= f, \\ a\varepsilon_1 + a_1\varepsilon_2 + \cdots + a_{\lambda-1}\varepsilon &= f_1, \\ \quad\vdots \quad\quad \vdots \quad\quad \vdots & \\ a\varepsilon_{\lambda-1} + a_1\varepsilon + \cdots + a_{\lambda-1}\varepsilon_{\lambda-2} &= f_{\lambda-1}. \end{cases}$$

Quod aequationum systema ut secundum quantitates a, a_1, ... 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:

---

*) Cum illa periodorum functio linearis eadem tanquam functio ipsius ε rationalis integra repraesentari possit.

$$\text{(III.)}\quad \begin{aligned}&(\varepsilon+\varepsilon_1\alpha+\varepsilon_2\alpha^2+\cdots+\varepsilon_{\lambda-1}\alpha^{\lambda-1})(a+a_1\alpha^{-1}+a_2\alpha^{-2}+\cdots+a_{\lambda-1}\alpha^{-(\lambda-1)})\\&\qquad=f+f_1\alpha+f_2\alpha^2+\cdots+f_{\lambda-1}\alpha^{\lambda-1}\end{aligned}$$

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

Cum vero expressio $\varepsilon+\varepsilon_1\alpha+\cdots+\varepsilon_{\lambda-1}\alpha^{\lambda-1}$ nihil aliud sit, nisi id quod Cl. *Jacobi* in commentatione illa iam supra laudata*) signo $F(\alpha)$ denotat, formulam l. c. traditam in auxilium vocamus:

$$(\varepsilon+\varepsilon_1\alpha+\cdots+\varepsilon_{\lambda-1}\alpha^{\lambda-1})(\varepsilon+\varepsilon_1\alpha^{-1}+\cdots+\varepsilon_{\lambda-1}\alpha^{-(\lambda-1)})=\nu.\alpha^{\frac{1}{2}\mu(\nu-1)}=\nu.\alpha^{\frac{1}{2}\mu\lambda},$$

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

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

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

$$\text{(V.)}\quad \begin{cases}\nu a &= f\varepsilon &+f_1\varepsilon_1+f_2\varepsilon_2+\cdots+f_{\lambda-1}\varepsilon_{\lambda-1}+m,\\ \nu a_1 &= f\varepsilon_1 &+f_1\varepsilon_2+f_2\varepsilon_3+\cdots+f_{\lambda-1}\varepsilon \quad +m,\\ &\quad\vdots &\quad\vdots\qquad\quad\vdots\\ \nu a_{\lambda-1} &= f\varepsilon_{\lambda-1} &+f_1\varepsilon+f_2\varepsilon_1+\cdots+f_{\lambda-1}\varepsilon_{\lambda-2}+m.\end{cases}$$

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

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

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

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

ubi m respectu r constans est.

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

$$\text{(VI.)}\quad \nu(a+a_1+\cdots+a_{\lambda-1})=(f+f_1+\cdots+f_{\lambda-1})(\varepsilon+\varepsilon_1+\cdots+\varepsilon_{\lambda-1})+\lambda m.$$

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

*) Monatsberichte der Berliner Akademie 1837 (S. 128).

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

Quo valore ipsius m substituto has consequimur aequationes, systemata (II) et (V) repraesentantes:

$$\text{(VII.)} \quad \begin{cases} f_r = a\varepsilon_r + a_1\varepsilon_{r+1} + \cdots + a_{\lambda-1}\varepsilon_{r-1}, \\ -\nu a_r = f(\mu-\varepsilon_r) + f_1(\mu-\varepsilon_{r+1}) + \cdots + f_{\lambda-1}(\mu-\varepsilon_{r-1}) \end{cases}$$

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

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

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

quamquam ***unitates*** complexas in posterum illius formae supra exhibitae ponemus. — Productum talium numerorum $f(\varepsilon)$ rursus in eandem formam redigi posse inde elucet, quod quaevis periodus tanquam functio rationalis integra unius repraesentari potest, quodque quaevis functio integra periodi ε per aequationem illam gradus λ^{ti}, quarum radices ε, ε_1, ... $\varepsilon_{\lambda-1}$ sunt, ad gradum $(\lambda-1)^{\text{tum}}$ redigi potest. Denique ex aequalitate duorum numerorum complexorum aequalitatem singulorum coefficientium colligi posse inde patet, quod functio periodi integra gradus $(\lambda-1)^{\text{ti}}$ evanescere nequit, nisi omnes eius coefficientes evanescunt.

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

$$f(\varepsilon)f(\varepsilon_1)\ldots f(\varepsilon_{\lambda-1}) = \mathrm{Nm}\, f(\varepsilon)$$

et quidem respectu ε. Quodsi enim $f(\varepsilon)$ tanquam functio alius periodi e. g. ipsius ω consideratur, ita ut sit: $f(\varepsilon) = \varphi(\omega)$, apparet esse

$$\mathrm{Nm}\,\varphi(\omega) = \varphi(\omega)\varphi(\omega_1)\ldots\varphi(\omega_{\nu-2}) \quad \text{sive} \quad \mathrm{Nm}\,\varphi(\omega) = (\mathrm{Nm}\, f(\varepsilon))^{\mu}.$$

Neque unquam, ne ex aequalitate signorum ambiguitas oriatur, verendum est. Caeterum ex ipsa definitione colliguntur aequationes:

$$\mathrm{Nm}\, f(\varepsilon) = \mathrm{Nm}\, f(\varepsilon_r) \quad \text{et} \quad \mathrm{Nm}\,(f(\varepsilon).\varphi(\varepsilon)) = \mathrm{Nm}\, f(\varepsilon).\mathrm{Nm}\,\varphi(\varepsilon).$$

Cum sit

$$(\mathrm{Nm}\, f(\varepsilon))^{\mu} = \mathrm{Nm}\,\varphi(\omega) \equiv 1 \pmod{\nu},$$

posito numerum $\mathrm{Nm}\, f(\varepsilon)$ ad ipsum ν primum esse (Disput. Cli. ***Kummer*** § 2), sequitur, ut quaevis norma respectu ε residuum sit λ^{tae} potestatis modulo ν.

§ 2.

Ponatur p numerus primus eiusmodi, ut sit $p^\mu \equiv 1 \pmod{\nu}$, atque sit:

$$p = p(\varepsilon)p(\varepsilon_1)\dots p(\varepsilon_{\lambda-1}) = \mathrm{Nm}\,p(\varepsilon),$$

istos factores ulterius in factores complexos ex his ipsis periodis ε compositos discerpi non posse atque inter se diversos esse, eadem qua Cl. ***Kummer*** in disputatione sua (§ 5) usus est ratione probatur. Deinde cum nuper a Clo. ***Kummer*** demonstratum sit, congruentiam λ^{ti} gradus:

$$(x-\varepsilon)(x-\varepsilon_1)\dots(x-\varepsilon_{\lambda-1}) \equiv 0 \pmod{p}$$

semper habere λ radices, si p condicioni sufficit $p^\mu \equiv 1 \pmod{\nu}$*), has ipsas designemus literis: e, e_1, $\dots$ $e_{\lambda-1}$**). Iam haec duo habentur theoremata:

1. Si $f(\varepsilon)$ numerus est complexus, cuius norma per numerum primum p divisibilis est, unus numerorum $f(e)$, $f(e_1)$, $\dots$ secundum modulum p nihilo congruus erit; et quando unus numerorum $f(e)$ ipsum p metitur, etiam $\mathrm{Nm}\,f(\varepsilon)$ factorem p implicat.

Dem. Cum 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:

$$f(\varepsilon)f(\varepsilon_1)\dots f(\varepsilon_{\lambda-1}) \equiv f(e)f(e_1)\dots f(e_{\lambda-1}) \pmod{p}$$
$$\text{sive } \mathrm{Nm}\,f(\varepsilon) \equiv f(e)f(e_1)\dots f(e_{\lambda-1}) \pmod{p},$$

unde theoremata illa sponte manant.

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

$$e \equiv \varepsilon \pmod{p(\varepsilon)}.$$

Dem. Ponatur

$$(e-\varepsilon)p(\varepsilon_1)p(\varepsilon_2)\dots p(\varepsilon_{\lambda-1}) = \varphi(\varepsilon),$$

unde

$$(e-\varepsilon_1)p(\varepsilon)p(\varepsilon_2)\dots p(\varepsilon_{\lambda-1}) = \varphi(\varepsilon_1) \text{ etc.};$$

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

$$\varphi(\varepsilon)+\varphi(\varepsilon_1)+\dots+\varphi(\varepsilon_{\lambda-1}) \equiv \varphi(e)+\varphi(e_1)+\dots+\varphi(e_{\lambda-1}) \equiv 0 \pmod{p}.$$

---

*) In commentatione „de divisoribus formarum quarundam etc.“ quae proximo tempore edetur; vel etiam in commentatione Cli. *Schoenemann* (*Crelles* Journal, Bd. 19, S. 306).

**) Adnotamus quodvis e_r eandem ipsius e functionem integram esse quam ε_r ipsius ε.

Deinde erit $\varphi(\varepsilon)^2+\varphi(\varepsilon)\varphi(\varepsilon_1)+\cdots+\varphi(\varepsilon)\varphi(\varepsilon_{\lambda-1})\equiv\varphi(\varepsilon)^2$, cum reliqua producta omnes factores $p(\varepsilon)$ ideoque ipsum p contineant. Ergo habemus: $\varphi(\varepsilon)^2\equiv 0\ (\mathrm{mod}.p)$. Iam si p ad ν primum supponitur, erit $p^{\nu-1}\equiv 1\ (\mathrm{mod}.\nu)$ atque (cf. § 3, 1)

$$\varphi(\varepsilon)^{p^{\nu-1}}\equiv\varphi(\varepsilon^{p^{\nu-1}})\equiv\varphi(\varepsilon)\ (\mathrm{mod}.p).$$

Erit autem

$$\varphi(\varepsilon)^{p^{\nu-1}}=\varphi(\varepsilon)^{p^{\nu-1-2}}.\varphi(\varepsilon)^2\equiv 0\ (\mathrm{mod}.p),$$

unde denique:

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

$$e-\varepsilon\equiv 0\ (\mathrm{mod}.p(\varepsilon)).$$

Casu $p=\nu$ habemus $\mathrm{Nm}\,p(\varepsilon)=\nu$ et posito $p(\varepsilon)=f(\omega)$ erit $\mathrm{Nm}f(\omega)=(\mathrm{Nm}\,p(\varepsilon))^\mu$, ergo $\mathrm{Nm}f(\omega)\equiv 0\,(\mathrm{mod}.\nu^\mu)$. Eaque de re $f(1)\equiv 0\,(\mathrm{mod}.\nu)$ (disputatio Cli. ***Kummer*** § 2); ergo cum sit $(1-\omega)(1-\omega^2)\cdots=\nu$, erit quoque $f(1)\equiv 0\ (\mathrm{mod}.(1-\omega))$. Deinde propter congruentiam $1\equiv\omega\,(\mathrm{mod}.(1-\omega))$ habemus $f(\omega)\equiv 0\,(\mathrm{mod}.(1-\omega))$.

Iam posito $\quad f(\omega)=(1-\omega)f'(\omega)$ erit $\mathrm{Nm}f'(\omega)\equiv 0\,(\mathrm{mod}.\nu^{\mu-1})$,

ergo sicut supra $\quad f'(\omega)=(1-\omega)f''(\omega)$.

Qua ratione denique obtinemus $f(\omega)=(1-\omega)^\mu\varphi(\omega)$. Est vero

$$\mathrm{Nm}f(\omega)=\nu^\mu=\nu^\mu\,\mathrm{Nm}\,\varphi(\omega),$$

unde $\varphi(\omega)$ unitatem complexam esse patet. Ergo erit quoque:

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

Deinde cum simili modo e congruentia $\mathrm{Nm}(e-\varepsilon)\equiv 0\ (\mathrm{mod}.\nu)$ colligatur

$$(e-\varepsilon)=(1-\omega)^\mu\psi(\omega)\quad\text{sive}\quad(e-\varepsilon)\equiv 0\ (\mathrm{mod}.(1-\omega)^\mu),$$

denique respecta congruentia illa: $(1-\omega)^\mu\equiv 0\ (\mathrm{mod}.p(\varepsilon))$ habebitur:

$$e-\varepsilon\equiv 0\ (\mathrm{mod}.p(\varepsilon)).$$

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

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

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

Est vero $e\equiv\varepsilon\,(\mathrm{mod}.p(\varepsilon))$, unde $p^1(\varepsilon)\equiv 0\,(\mathrm{mod}.p(\varepsilon))$ i. e. $p^1(\varepsilon)=p(\varepsilon).\varphi(\varepsilon)$, ubi $\varphi(\varepsilon)$ unitas complexa est, quia $\mathrm{Nm}p^1(\varepsilon)=p=\mathrm{Nm}p(\varepsilon).\mathrm{Nm}\varphi(\varepsilon)=p.\mathrm{Nm}\varphi(\varepsilon)$, ergo $\mathrm{Nm}\,\varphi(\varepsilon)=1$.

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

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

Dem. Sit $p(e) \equiv p(e_r) \equiv 0 \pmod{p}$ ergo $p(e_r) \equiv 0 \pmod{p(\varepsilon)}$. Deinde cum habeamus $e \equiv \varepsilon$ et $e_r \equiv \varepsilon_r \pmod{p(\varepsilon)}$*), sequitur, ut sit:

$$p(\varepsilon_r) \equiv 0 \pmod{p(\varepsilon)} \text{ sive } p(\varepsilon_r) = p(\varepsilon).\varphi(\varepsilon).$$

Ergo cum sit: $p(\varepsilon).p(\varepsilon_1)\dots p(\varepsilon_{\lambda-1}) \equiv 0 \pmod{p}$, etiam erit:

$$\varphi(\varepsilon).p(\varepsilon).p(\varepsilon_1)\dots p(\varepsilon_{\lambda-1}) = p(\varepsilon_r)^2.p(\varepsilon_1)\dots p(\varepsilon_{r-1})p(\varepsilon_{r+1})\cdots \equiv 0 \pmod{p}$$

etiamque

$$p(\varepsilon_r)^{p^\mu}.p(\varepsilon_1)\dots p(\varepsilon_{r-1})p(\varepsilon_{r+1})\cdots \equiv p(\varepsilon_r).p(\varepsilon_1)\cdots \equiv 0^{**}) \pmod{p}$$

i. e. $$\frac{\mathrm{Nm}\,p(\varepsilon)}{p(\varepsilon)} = \frac{p}{p(\varepsilon)} \equiv 0 \pmod{p}, \text{ sive } \frac{p}{p(\varepsilon)} = p.f(\varepsilon)$$

sive denique $1 = f(\varepsilon).p(\varepsilon)$, id quod fieri non posse facile patet, si in utraque aequationis parte normam formes. Tum enim esset $1 = p.\mathrm{Nm}\,f(\varepsilon)$.

§ 3.

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

1. *Theorema.* Quando norma aliqua $\mathrm{Nm}\,f(\omega)$ numerum primum p continet, qui ad exponentem μ modulo ν pertineat, illam ipsam normam μ^{ta} ipsius p potestas metiri debet.

Dem. Cum sit $\mu.\lambda = \nu - 1$ cumque p ad numerum μ pertineat, ponatur $p \equiv g^\lambda$. Iam 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 congruentiis inter se multiplicatis obtinemus:

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

Qua in congruentia si deinceps valores: ω^g, ω^{g^2}, $\dots$ $\omega^{g^{\lambda-1}}$ loco ipsius ω substituuntur, atque congruentiae, quae hoc modo prodeunt, inter se multiplicantur, fit:

$$\{f(\omega).f(\omega^g)\dots f(\omega^{g^{\lambda-1}})\}^{1+p+\cdots+p^{\mu-1}} \equiv \mathrm{Nm}\,f(\omega) \equiv 0 \pmod{p}$$

---

*) v. adnotationem secundam ad § 2.

**) v. § 3, 1.

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

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

Iam cum sit $1+p+\dots+p^{\mu-1} < p^\mu$, certo etiam erit

$$\varphi(\omega)^{p^\mu} \equiv 0 \pmod{p}.$$

Est vero

$$\varphi(\omega)^{p^\mu} \equiv \varphi(\omega^{p^\mu}) \equiv \varphi(\omega) \pmod{p}, \quad \text{ergo} \quad \varphi(\omega) \equiv 0 \pmod{p},$$

unde mutatis radicibus ω oriuntur relationes:

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

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

$$\mathrm{Nm} f(\omega) = \varphi(\omega).\varphi(\omega^{g^\lambda})\dots\varphi(\omega^{g^{(\mu-1)\lambda}}) \equiv 0 \pmod{p^\mu}.$$

2. *Theorema.* Normam aliquam $\mathrm{Nm} f(\omega)$ si numerus primus p metitur, qui ad exponentem μ modulo ν 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 summam ipsius p potestatem numero $\mathrm{Nm} f(\omega)$ contentam secundum supra dicta multiplum ipsius μ esse debere. Iam sit $p = \mathrm{Nm} p(\varepsilon)$, deinde ponatur

$$f(\omega).f(\omega^{g^\lambda}).f(\omega^{g^{2\lambda}})\dots f(\omega^{g^{(\mu-1)\lambda}}) = \varphi(\varepsilon)\ ^*).$$

Tum habemus secundum suppositionem nostram:

$$\mathrm{Nm} f(\omega) = \mathrm{Nm}\,\varphi(\varepsilon) \equiv 0 \pmod{p},$$

unde secundum § 2, 1: $\varphi(e_r) \equiv 0 \pmod{p}$ ideoque $(\mathrm{mod.}\, p(\varepsilon))$. Cumque habeamus secundum § 2, 2: $e \equiv \varepsilon \pmod{p(\varepsilon)}$, erit: $\varphi(\varepsilon_r) \equiv 0 \pmod{p(\varepsilon)}$, sive mutatis periodis $\varphi(\varepsilon) \equiv 0 \pmod{p(\varepsilon_{-r})}$ i. e.

$$f(\omega).f(\omega^{g^\lambda})\dots f(\omega^{g^{(\mu-1)\lambda}}) \equiv 0 \pmod{p(\varepsilon_{-r})},$$

sive si congruentiam $p \equiv g^\lambda \pmod{\nu}$ respicimus:

$$f(\omega).f(\omega^p)\dots f(\omega^{p^{\mu-1}}) \equiv 0 \pmod{p(\varepsilon_{-r})}.$$

Est vero:

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

ideoque $(\mathrm{mod.}\, p(\varepsilon_{-r}))$, unde ratione supra exhibita colligimus esse:

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

---

*) *Gauss* disq. arithm. 345.

**) v. paragraphum antecedentem.

Ad normam transeuntes obtinemus aequationem:

$$\mathrm{Nm} f(\omega) = p^{\mu}.\mathrm{Nm}\,\psi(\omega) \quad \text{sive} \quad \mathrm{Nm}\frac{f(\omega)}{p^{\mu}} = \mathrm{Nm}\,\psi(\omega) \quad \text{q. e. d.}$$

Iam hac methodo iterum atque iterum adhibita facile patet e suppositione $\mathrm{Nm} f(\omega) \equiv 0 \pmod{p^{n.\mu}}$ congruentiam colligi huiusmodi:

$$f(\omega) \equiv 0 \pmod{p(\varepsilon_k)^m.p(\varepsilon_{k'})^{m'}\ldots},$$

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

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

$$f(\omega) \equiv 0 \pmod{(1-\omega)^m}.$$

§ 4.

Sit $f(\omega)$ numerus aliquis complexus, N numerus realis eiusmodi, ut factores eius primi reales in factores complexos quam plurimos discerpi possint, sitque factor numerorum $f(\omega)$ et N communis maximus $\varphi(\omega)$***), numerus $\psi(\omega)$ inveniri potest talis, ut sit: $\psi(\omega).f(\omega) \equiv \varphi(\omega) \pmod{N}$†).

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

Iam erit secundum §. 3, 2:

$$f(\omega) = F(\omega).p(\varepsilon_k)^m.p(\varepsilon_{k'})^{m'}\ldots,$$

ubi $p^{m+m'+\cdots}$ summa ipsius p potestas numero $\mathrm{Nm} f(\omega)$ contenta. Est igitur $\mathrm{Nm} F(\omega)$ numerus ad ipsum p primus, quare exstat numerus x talis, ut sit: $x.\mathrm{Nm} F(\omega) \equiv 1 \pmod{p^{\pi}}$. Hinc habemus:

---

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

**) v. § 2, 2.

***) 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.

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

$$(\text{I.}) \qquad \begin{aligned} x.F(\omega^2)F(\omega^3)\dots F(\omega^{\nu-1}).f(\omega) &= x.\mathrm{Nm}F(\omega).p(\varepsilon_k)^m.p(\varepsilon_{k'})^{m'}\dots \\ &\equiv p(\varepsilon_k)^m.p(\varepsilon_{k'})^{m'}\dots \pmod{p^\pi}. \end{aligned}$$

Designemus complexum factorum omnium et producto $p(\varepsilon_k)^m.p(\varepsilon_{k'})^{m'}\dots$ et numero p^π i. e. producto $p(\varepsilon)^\pi.p(\varepsilon_1)^\pi\dots$ communium signo $P(\varepsilon)$, ita ut sint:

$$P(\varepsilon).p(\varepsilon_a)^\alpha.p(\varepsilon_{a'})^{\alpha'}\cdots = P(\varepsilon).A(\varepsilon) = p(\varepsilon_k)^m.p(\varepsilon_{k'})^{m'}\dots,$$
$$P(\varepsilon).p(\varepsilon_b)^\beta.p(\varepsilon_{b'})^{\beta'}\cdots = P(\varepsilon).B(\varepsilon) = p^\pi.$$

Iam nullum indicem a nulli indici b aequalem esse patet. Sint c, c', ... indices ii, qui coniuncti cum indicibus a et b seriem 0, 1, 2, ... $\lambda-1$ efficiunt, atque posito $C(\varepsilon) = p(\varepsilon_c).p(\varepsilon_{c'})\dots$ formetur expressio:

$$V(\varepsilon) = A(\varepsilon)+B(\varepsilon).C(\varepsilon),$$

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

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

Cum vero pro quovis e unus tantum factorum $p(e)$ nihilo congruus esse possit**), aut $A(e)$ aut $B(e)$ aut $C(e)$, minime igitur $A(e)+B(e).C(e)$, nihilo congruum erit. Quare iam existet numerus y talis, ut sit: $y.\mathrm{Nm}V(\varepsilon) \equiv 1 \pmod{p^\pi}$ sive substituto ipsius $V(\varepsilon)$ valore:

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

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

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

Unde si illam congruentiam (I):

$$x.F(\omega^2)\dots F(\omega^{\nu-1}).f(\omega) \equiv A(\varepsilon).P(\varepsilon) \pmod{p^\pi}$$

respicimus atque

$$x.F(\omega^2)\dots F(\omega^{\nu-1}).y.V(\varepsilon_1)\dots V(\varepsilon_{\lambda-1}) = \psi(\omega)$$

ponimus, denique prodit congruentia:

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

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,

*) v. § 2, 1.
**) v. § 2, 4.

obtinemus:

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

Casu $p=\nu$ habemus $f(\omega)=(1-\omega)^{\pi}F(\omega)$, ubi numerus $\mathrm{Nm}F(\omega)$ ad ipsum ν primus est*). Iam posito $x.\mathrm{Nm}F(\omega)\equiv 1 \pmod{\nu^{\pi}}$ atque:

$$x.F(\omega^2).F(\omega^3)\ldots F(\omega^{\nu-1}) = \psi(\omega)$$

obtinemus:

$$\psi(\omega)f(\omega)\equiv(1-\omega)^{\pi} \pmod{\nu^{\pi}}.$$

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

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

ubi $P(\varepsilon)$ factor est communis maximus numerorum $f(\omega)$ et p^a, $Q(\varepsilon')$ factor communis maximus numerorum $f(\omega)$ et q^b etc. Itaque habemus:

$$\begin{aligned} Q(\varepsilon').R(\varepsilon'')\ldots\psi_1(\omega).f(\omega) &= \chi_1(\omega)f(\omega)\equiv P(\varepsilon)\,Q(\varepsilon')\ldots \pmod{p^a},\\ P(\varepsilon).R(\varepsilon'')\ldots\psi_2(\omega).f(\omega) &= \chi_2(\omega)f(\omega)\equiv P(\varepsilon)\,Q(\varepsilon')\ldots \pmod{q^b}.\\ &\vdots \qquad\quad \vdots \qquad\quad \vdots \end{aligned}$$

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

$$\psi(\omega)\equiv\chi_1(\omega) \pmod{p^a},\quad \psi(\omega)\equiv\chi_2(\omega) \pmod{q^b},\ \ldots,$$

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

$$\psi(\omega).f(\omega)\equiv P(\varepsilon).Q(\varepsilon').R(\varepsilon'')\ldots \pmod{N},$$

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

§ 5.

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

$$\mathrm{Nm}(p+e-\varepsilon)=\pi' p=\mathrm{Nm}(e-\varepsilon)+p\{(e-\varepsilon_1)(e-\varepsilon_2)\cdots+(e-\varepsilon)(e-\varepsilon_2)\cdots+\cdots\}+p^2\{\cdots\}.$$

Iam si et ipsum π' factorem p contineret, etiam illa expressio per ipsum p

*) v. adnotationem in fine paragraphi 3.

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 obtinemus:

$$(e-e_1)(e-e_2)\cdots \equiv 0 \pmod{p}$$

sive igitur

$$e \equiv e_r \pmod{p},$$

id quod fieri non potest, nisi pro certis quibusdam numeris p, qui et ipsi divisores numeri $\mathrm{Nm}(\varepsilon-\varepsilon_r)$ sunt. Quodsi enim $e\equiv e_r \pmod{p}$, est quoque:

$$(e-e_r)(e_1-e_{r+1})\ldots(e_{\lambda-1}-e_{r+\lambda-1}) \equiv 0 \equiv (\varepsilon-\varepsilon_r)(\varepsilon_1-\varepsilon_{r+1})\cdots \equiv \mathrm{Nm}(\varepsilon-\varepsilon_r) \pmod{p}.$$

Theorema. Si normam numeri complexi $\mathrm{Nm}f(\omega)$ numerus primus p metitur ad exponentem μ modulo ν pertinens atque $\pi p = \mathrm{Nm}(e-\varepsilon)$ est, numerum $\pi.f(\omega)$ aliquis factor $e-\varepsilon_k$ metiri debet.

Dem. Ponatur

$$f(\omega).f(\omega^{g^\lambda})\ldots f(\omega^{g^{(\mu-1)\lambda}}) = \varphi(\varepsilon)^*).$$

Tum habemus: $\mathrm{Nm}f(\omega) = \mathrm{Nm}\varphi(\varepsilon) \equiv 0 \pmod{p}$, ergo secundum § 2, 1:

$$\varphi(e_r) \equiv 0 \pmod{p} \quad \text{et} \quad \pi.\varphi(e_r) \equiv 0 \pmod{\pi.p} \quad \text{ideoque} \quad \pmod{(e-\varepsilon)}.$$

Deinde cum appareat esse $e \equiv \varepsilon$ et $e_r \equiv \varepsilon_r \pmod{(e-\varepsilon)}$, obtinemus congruentias:

$$\pi\varphi(e_r) \equiv \pi.\varphi(\varepsilon_r) \equiv 0 \pmod{(e-\varepsilon)} \quad \text{sive} \quad \pi.\varphi(\varepsilon) \equiv 0 \pmod{(e-\varepsilon_{-r})}$$

i. e.

$$\pi.f(\omega).f(\omega^{g^\lambda})\ldots f(\omega^{g^{(\mu-1)\lambda}}) \equiv 0 \pmod{(e-\varepsilon_{-r})}$$

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

$$\pi.f(\omega).f(\omega^p)\ldots f(\omega^{p^{\mu-1}}) \equiv 0 \pmod{(e-\varepsilon_{-r})}.$$

Est vero

$$\pi.f(\omega).f(\omega^p)\ldots f(\omega^{p^{\mu-1}}) \equiv \pi.f(\omega)^{1+p+\ldots+p^{\mu-1}} \pmod{\pi p} \text{ ideoque } \pmod{(e-\varepsilon_{-r})}$$

ergo ratione supra adhibita:

$$\pi.f(\omega) \equiv 0 \pmod{(e-\varepsilon_{-r})} \quad \text{q. e. d.}$$

Qua ratione iterata facile supposita congruentia $\mathrm{Nm}f(\omega) \equiv 0 \pmod{p^{n\cdot\mu}}$ colligimus congruentiam locum habere huiusmodi:

$$\pi^n.f(\omega) \equiv 0 \pmod{(e-\varepsilon_k)^m.(e-\varepsilon_{k'})^{m'}\ldots},$$

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

---

*) v. *Gauss* disq. arithm. 345.

§ 6.

Sit p numerus primus talis, ut sit $p^{\nu} \equiv 1 \pmod{\nu}$ atque $\pi p = \mathrm{Nm}(e-\varepsilon)$, sitque π numerus ad ipsum p primus. Deinde ponatur

$$(e-\varepsilon_1)(e-\varepsilon_2)\ldots(e-\varepsilon_{\lambda-1}) = \varphi(\varepsilon),$$

ubi $\varphi(\varepsilon)$ ipsum p metiri non posse patet, quia posito $\varphi(\varepsilon) = p.\psi(\varepsilon)$ esset

$$(e-\varepsilon).\varphi(\varepsilon) = \mathrm{Nm}(e-\varepsilon) = \pi p = p.(e-\varepsilon)\psi(\varepsilon),$$

ergo

$$\pi = (e-\varepsilon)\psi(\varepsilon) \text{ et } \pi^{\lambda} = \pi p.\mathrm{Nm}\,\psi(\varepsilon),$$

unde sequeretur, ut ipsum π per numerum p divisibile esset. — Iam numero complexo fracto $\frac{p}{\varphi(\varepsilon)}$ tanquam modulo ad hanc quae sequitur disquisitionem utamur; id quod facile fieri potest, si statuamus

congruentiam $a \equiv b \left(\mathrm{mod.}\ \frac{m}{n}\right)$ locum tenere huiusce $an \equiv bn \pmod{m}$.

Iam patet esse

$$e \equiv \varepsilon \left(\mathrm{mod.}\ \frac{p}{\varphi(\varepsilon)}\right);$$

est enim re vera

$$(e-\varepsilon)\varphi(\varepsilon) \equiv 0 \pmod{p}, \quad \text{quia} \quad (e-\varepsilon)\varphi(\varepsilon) = \mathrm{Nm}(e-\varepsilon) = \pi p.$$

Deinde si numerus complexus $f(\varepsilon)$ congruentiae sufficit

$$f(\varepsilon) \equiv 0 \left(\mathrm{mod.}\ \frac{p}{\varphi(\varepsilon)}\right),$$

numerus p eius normam metiatur oportet. Ex ista enim congruentia concluditur $f(\varepsilon).\varphi(\varepsilon) \equiv 0 \pmod{p}$ sive $\mathrm{Nm}f(\varepsilon).\mathrm{Nm}\,\varphi(\varepsilon) \equiv 0 \pmod{p^{\lambda}}$, et cum habeamus $\mathrm{Nm}\varphi(\varepsilon) = p^{\lambda-1}\pi^{\lambda-1}$, obtinemus $\pi^{\lambda-1}\mathrm{Nm}f(\varepsilon) \equiv 0 \pmod{p}$, et quia π ad ipsum p primus est,

$$\mathrm{Nm}f(\varepsilon) \equiv 0 \pmod{p}.$$

Ex illa congruentia

$$e \equiv \varepsilon \left(\mathrm{mod.}\ \frac{p}{\varphi(\varepsilon)}\right)$$

sequitur, ut quivis numerus complexus numero reali congruus sit, scilicet

$$f(\varepsilon) \equiv f(e) \left(\mathrm{mod.}\ \frac{p}{\varphi(\varepsilon)}\right),$$

unde p residua hoc modulo incongrua exstare elucet eaque numeri $0, 1, 2, \ldots p-1$. Etenim plures non existere inde patet, quod quivis numerus complexus numero

reali quivis autem numerus realis uni illorum numerorum modulo p, etiamque igitur modulo $\frac{p}{\varphi(\varepsilon)}$, congruus est. Sin vero duo illorum numerorum inter se congrui essent, earum differentia nihilo congrua fieret. Quam si litera d designamus, esset $d.\varphi(\varepsilon) \equiv 0 \pmod{p}$, ergo $d^\lambda.\mathrm{Nm}\,\varphi(\varepsilon) = d^\lambda.\pi^{\lambda-1}.p^{\lambda-1} \equiv 0 \pmod{p^\lambda}$, ergo: $d^\lambda.\pi^{\lambda-1} \equiv 0 \pmod{p}$, id quod esse nequit, quia π ad ipsum p primus atque $d < p$ est.

Iam accepto numero k eiusmodi, ut sit $k^\lambda \leqq p < (k+1)^\lambda$, statuamus cunctos numeros complexos formae $c + c_1\varepsilon + \cdots + c_{\lambda-1}\varepsilon^{\lambda-1}$, in quibus coefficientes isti c valores 0, 1, 2, ... k induunt. Horum multitudo erit $(k+1)^\lambda > p$, inter quos igitur certe duo inter se congrui erunt secundum modulum $\frac{p}{\varphi(\varepsilon)}$. Quorum altero ab altero subtracto obtinemus numerum complexum $f(\varepsilon)$, cuius coefficientes omnes inter $-k$ et $+k$ sunt, et cuius norma numerum p continet, cum ipse nihilo congruus sit modulo $\frac{p}{\varphi(\varepsilon)}$. Quare sit $\mathrm{Nm}\,f(\varepsilon) = np$. Iam si litera M_λ maximum valorem expressionis

$$\mathrm{Nm}(x + x_1\varepsilon + \cdots + x_{\lambda-1}\varepsilon^{\lambda-1})$$

designamus, ea condicione ut quantitates x cunctae inter -1 et $+1$ sint, obtinemus:

$$\frac{np}{k^\lambda} = \mathrm{Nm}\frac{f(\varepsilon)}{k}, \quad \text{ideoque} \quad \frac{np}{k^\lambda} < M_\lambda$$

sive

$$np < M_\lambda k^\lambda < M_\lambda p, \quad \text{unde denique} \quad n < M_\lambda.$$

Hinc habemus hoc theorema magni momenti. Dato aliquo numero p, qui condicionem implet $p^\mu \equiv 1 \pmod{\nu}$, semper invenire licet numerum n minorem finita quadam quantitate ab ipso p independente eumque talem, ut productum np in λ factores complexos coniunctos dissolvi possit. Quod theorema respondet illi in theoria formarum quadraticarum theoremati fundamentali, secundum quod numerus formarum reductarum finitus est. Etiam adnotandum illam rationem agendi adhiberi non posse ad eos numeros primos p, qui divisores sunt numerorum $\mathrm{Nm}(\varepsilon - \varepsilon_r)$, quarum igitur multitudo finita est. — Deinde ope huius 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 np norma numeri complexi sit.

Ut pro certis quibusdam numeris ν pro quovis ipsius $\nu - 1$ divisore λ omnes numeri primi, residua λ^{tarum} potestatum ipsius ν, in λ factores com-

plexos dissolvi possint *), tantummodo necesse est, numeros primos, qui sint residua λ^{tae} potestatis modulo ν quantitatibus illis M_λ minores, in λ factores complexos coniunctos discerpi posse **). — Sit enim λ divisor ipsius $\nu-1$, designetur deinde signo d quilibet ipsius λ divisor excepto ipso λ; probandum est, quemvis numerum primum, residuum λ^{tae} potestatis, in λ factores complexos dissolvi posse, simodo hoc pro numeris primis p ipso M_λ minoribus eveniat praetereaque omnes numeri primi, residua d^{tarum} potestatum, in d factores complexos discerpi possint. Cum enim np tanquam norma repraesentari liceat, cumque factores ipsius n primi aut residua d^{tarum} potestatum aut residua λ^{tae} potestatis iique $\leqq n < M_\lambda$ sint ideoque in factores complexos discerpi possint, respectu habito theorematis § 3, 2 sententiam illam probari elucet. Iam 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 λ^{tae} 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 adiiciendam 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 iam adiumentis $M_4 = 49$ invenitur. Iam vero tres numeri primi formae $5n+1$ ipso M minores, scilicet 11, 31, 41, in quatuor factores complexos coniunctos, e radicibus unitatis quintis compositos, discerpi possunt ***). Deinde pro divisore $\lambda = 2$ omnes numeri primi, residua ipsius 5 quadratica, in duos factores complexos $(a+a_1\varepsilon).(a+a_1\varepsilon_1)$ dissolvi possunt. Id quod vel illa ipsa ratione erui vel e theoria formarum secundi gradus probari potest. Est enim

$$(a+a_1\varepsilon)(a+a_1\varepsilon_1) = (a+a_1\omega+a_1\omega^{-1}).(a+a_1\omega^2+a_1\omega^{-2}) = a^2-aa_1-a_1^2.$$

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

---

*) Adnotamus illud etiam ita exhiberi posse, ut pro his numeris ν omnes numeros primos formarum $k\nu+g^\lambda$ in λ factores complexos coniunctos dissolvi posse dicamus. Id quod illi sententiae aequivalere e facili consideratione elucet.

**) Addendum est praeterea eos numeros primos, qui numeros $\mathrm{Nm}(\varepsilon-\varepsilon_r)$ metiantur, pro se quosque disquirendos esse.

***) v. Cli. *Kummer* disput. pag. 21.

§ 7.

Iam 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 $\nu = a^\alpha . b^\beta . c^\gamma \ldots$ designantibus $a, b, c, \ldots$ numeros primos inter se diversos, sitque ω radix primitiva aequationis $x^\nu = 1$; hanc ipsam radicem esse aequationis:

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

notis methodis probatur, quae quidem aequatio $\varphi(\nu)^{\text{ti}}$ gradus*) omnes ν^{tas} 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 omittimus**), cum limites huius libelli demonstrationem hic tradere non patiantur. 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 $f(x)$, cum et idem functio sit integra, tamen illas certas tantum radices ω haberet atque factor functionis $f(x)$ foret, id quod fieri nequit. — Iam designentur radices primitivae numerorum $a^\alpha, b^\beta, \ldots$ resp. literis $g, h, \ldots$, deinde ponatur $\frac{\nu}{a^\alpha} = a'$, $\frac{\nu}{b^\beta} = b'$, $\ldots$; tum forma

$$a' g^m + b' h^n + \cdots$$

systema numerorum ad numerum ν primorum atque inter se incongruorum contineri constat, si numeris $m, n, \ldots$ sensim sensimque resp. valores $1, 2, \ldots a^{\alpha-1}(a-1)$; $1, 2, \ldots b^{\beta-1}(b-1)$; 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

$$\lambda\mu = a^{\alpha-1}(a-1), \quad \lambda'\mu' = b^{\beta-1}(b-1), \quad \ldots,$$

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

**) Demonstrationem illam, de qua sermo est, proximo tempore in publicum editurus sum.

et ponatur:

$$\varepsilon_{k,k',\ldots} = \sum_{m=0}^{m=\mu-1} \sum_{n=0}^{n=\mu'-1} \ldots \omega^{\alpha' g^{m\lambda+k} + b' h^{n\lambda'+k'} + \ldots}$$

sive

$$\varepsilon_{k,k',\ldots} = \sum_{m} \omega^{\alpha' g^{m\lambda+k}} . \sum_{n} \omega^{b' h^{n\lambda'+k'}} \ldots,$$

quae expressiones partes periodorum in numeris primis ν agunt. — Numerus terminorum expressionis talis erit: $\mu.\mu'.\mu''\ldots$, numerus periodorum ε inter se diversarum: $\lambda.\lambda'.\lambda''\ldots$, cum quantitates $k, k', \ldots$ resp. valores 0, 1, 2, $\ldots \lambda - 1$; 0, 1, 2, $\ldots \lambda'-1$; 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 apparet. — Per aequationem $\Pi(x-\varepsilon) = 0$, quippe quae sit gradus $\lambda.\lambda'.\lambda''\ldots$, quaevis ipsius ε potestas $\geqq \lambda\lambda'\lambda''\ldots$ potestatibus inferioribus exprimi potest.

Duae periodi ε diversorum indicum aequales esse non possunt.

Primum enim ex aequatione $\varepsilon_{0,0,\ldots} = \varepsilon_{k,k',k'',\ldots}$ sequeretur aequatio eiusmodi $\varepsilon_{0,0\ldots} = \varepsilon_{k,mk',nk'',\ldots}$*) designantibus $m, n, \ldots$ numeros quoscunque integros. Iam ponendo $m = b^{\beta-1}(b-1)$, $n = c^{\gamma-1}(c-1)$, etc. obtinemus $\varepsilon_{0,0,0,\ldots} = \varepsilon_{k,0,0,\ldots}$ sive respecta illa altera ipsorum ε definitione atque sublatis factoribus utriusque partis communibus:

$$\Sigma\omega^{\alpha' g^{m\lambda}} = \Sigma\omega^{\alpha' g^{m\lambda+k}},$$

cumque $\omega^{\alpha'}$ sit radix aequationis $x^{\alpha} = 1$ primitiva, pro iis unitatis radicibus, quae ad numerorum primorum potestates pertinent, illud theorema demonstrare sufficit. Quem ad finem designamus brevitatis causa signo ε_k expressionem $\Sigma\omega^{\alpha' g^{m\lambda+k}}$ et ipsam radicem unitatis $a^{\alpha\text{tam}}$ primitivam litera ω, ponatur denique $a^{\alpha-1}(a-1) = \mathfrak{a}$, ita ut habeamus $\varepsilon_k = \Sigma\omega^{g^{m\lambda+k}}$. Iam colliguntur ex aequatione $\varepsilon_0 = \varepsilon_k$ haece: $\varepsilon_1 = \varepsilon_k + 1$, $\varepsilon_2 = \varepsilon_k + 2$, etc., unde igitur:

I. $$\varepsilon + \varrho\varepsilon_1 + \varrho^2\varepsilon_2 + \cdots + \varrho^{\lambda-1}\varepsilon_{\lambda-1} = \varepsilon_k + \varrho\varepsilon_{k+1} + \varrho^2\varepsilon_{k+2} + \cdots + \varrho^{\lambda-1}\varepsilon_{k+\lambda-1},$$

ubi ϱ radix quaecunque sit aequationis $x^{\mathfrak{a}} = 1$. Posito:

$$\omega + \varrho\omega^g + \varrho^2\omega^{g^2} + \cdots + \varrho^{\mathfrak{a}-1}\omega^{g^{\mathfrak{a}-1}} = (\varrho, \omega)$$

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

$$(\varrho, \omega) = (\varrho, \omega^{g^k}) = (\varrho, \omega).\varrho^{-k}, \text{ unde } (\varrho, \omega)(1-\varrho^{-k}) = 0,$$

---

*) Nempe mutando ipsum ω, id quod secundum supra dicta facere licet.

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

Posito A, A_1, ... numeros reales integros esse, expressio formae:

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

numerus complexus dicetur.

Ex aequatione $f(\varepsilon) = 0$ colligitur $f(\varepsilon_k) = 0$, quia $f(\varepsilon)$ radicum ω functio est integra. — Deinde e relatione $f(\varepsilon) = 0$ colligimus esse $A = A_1 = A_2 = \cdots = 0$. Cum 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 $L-1^{\text{ti}}$ sit, coefficientes evanescere necesse est. Unde haec theoremata patent: duabus numeris complexis inter se aequalibus et singuli numeri coniuncti et coefficientes resp. aequales sunt.

Quaevis periodus $\varepsilon_{k,k',k'',\ldots}$ tanquam functio integra coefficientium rationalium unius periodi repraesentari potest. Ad quod probandum primum numerus ν potestas numeri primi ($\nu = a^{\alpha}$) ponendus est. Iam designante litera ω radicem primitivam aequationis $x^{a^{\alpha}} = 1$ ponatur:

$$\omega^{g^k} + \omega^{g^{\lambda}+k} + \cdots + \omega^{g^{(\mu-1)\lambda}+k} = \varepsilon_k = \varepsilon(\omega^{g^k}),$$

denique $\lambda = a^{\alpha-1}.d$ et $d.\mu = a-1$. — Radix ω cum aequationi sufficiat:

$$1 + \omega^{a^{\alpha-1}} + \omega^{2a^{\alpha-1}} + \cdots + \omega^{(a-1)a^{\alpha-1}} = 0$$

ideoque

$$\omega^r + \omega^{r+a^{\alpha-1}} + \omega^{r+2a^{\alpha-1}} + \cdots + \omega^{r+(a-1)a^{\alpha-1}} = 0,$$

habemus aequationes:

$$\varepsilon(\omega^r) + \varepsilon(\omega^{a^{\alpha-1}+r}) + \cdots + \varepsilon(\omega^{(a-1)a^{\alpha-1}+r}) = 0,$$

in quibus numerus r valores 1, 2, ... $a^{\alpha-1}-1$ induere potest. Inter quas vero quaeque μ inter se congruunt, unde numerus aequationum inter se di-

*) Id quod fusius exponere omittimus.

**) Posuimus $L = \lambda.\lambda'.\lambda''\ldots$

versarum est $\frac{a^{\alpha-1}-1}{\mu}+1$, addita illa aequatione pro $r=0$ scilicet:

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

Numerus expressionum omnium $\varepsilon(\omega^r)$ inter se diversarum est $\frac{a^\alpha-1}{\mu}$, quarum autem $\frac{a^{\alpha-1}-1}{\mu}+1$ reliquis per illas aequationes lineariter exprimere licet; qua de causa tantum $\frac{a^\alpha-a^{\alpha-1}}{\mu}-1$ sive $\lambda-1$ restant. Iam quamvis ipsius $\varepsilon(\omega^{g^k})$ potestatem tanquam functionem linearem *omnium* expressionum $\varepsilon(\omega^r)$ ideoque tanquam functionem linearem aliquarum $(\lambda-1)$ quantitatum $\varepsilon(\omega^r)$ repraesentari posse nullo negotio perspicitur. Qua de causa ponamus potestates ε_k^2, ε_k^3, ... $\varepsilon_k^{\lambda-1}$ repraesentatas $\lambda-1$ expressionibus $\varepsilon(\omega^r)$, inter quas sint ε_k et $\varepsilon(\omega^n)$. Ex quibus $\lambda-2$ aequationibus, reliquis $\lambda-3$ quantitatibus $\varepsilon(\omega^r)$ eliminatis, restabit aequatio huius formae:

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

ubi certe non omnes coefficientes A evanescere possunt. Coefficientem B evanescere non posse, solutionem igitur non illusoriam esse, inde elucet, quod functio periodi ε_k gradus $(\lambda-1)^{\text{ti}}$ integra evanescere nequit, nisi ipsi coefficientes nihilo aequales sunt*).

Quodsi iam ν numerum aliquem compositum ponimus, atque

$$\Sigma\omega^{a^\alpha g^{m\lambda+k}}=\varepsilon_k,\quad \Sigma\omega^{b^\beta h^{n\lambda+k'}}=\varepsilon'_{k'},\ \text{etc.}$$

igitur secundum illam definitionem: $\varepsilon_{k,k',\ldots}=\varepsilon_k.\varepsilon'_{k'}\ldots$ scimus hoc productum exprimi posse producto functionum rationalium ipsorum ε, ε', ε'', ... Restat igitur, ut probemus quodvis productum $\varepsilon^i.\varepsilon'^{i'}\ldots$ repraesentari posse potestatibus $(\varepsilon.\varepsilon'.\varepsilon''\ldots)$, $(\varepsilon.\varepsilon'.\varepsilon''\ldots)^2$, ... $(\varepsilon.\varepsilon'.\varepsilon''\ldots)^{L-1}$. Cum vero quaeque i^{ta} ipsius ε potestas potestate prima, secunda, etc., $(\lambda-1)^{\text{ta}}$ exprimi possit, illae $L-1$ potestates quantitatis $(\varepsilon.\varepsilon'.\varepsilon''\ldots)$ repraesentari possunt variis productis $\varepsilon^i.\varepsilon'^{i'}\ldots$, in quibus $i<\lambda$, $i'<\lambda'$, ..., quorum igitur numerus est $\lambda.\lambda'.\lambda''\ldots=L$, vel excepto producto $\varepsilon^0.\varepsilon'^0\cdots=1$ restant $L-1$ producta, quibus potestates $(\varepsilon.\varepsilon'\ldots)^2$, $(\varepsilon.\varepsilon'\ldots)^3$, ... expressae sunt. Ex quibus aequationibus $L-2$ si omnia eliminamus producta exceptis $\varepsilon.\varepsilon'.\varepsilon''\ldots$ et certo quodam $\varepsilon^i.\varepsilon'^{i'}\ldots$, quorum igitur multitudo $L-3$, obtinemus aequationem formae:

$$A+A_1(\varepsilon.\varepsilon'\ldots)+A_2(\varepsilon.\varepsilon'\ldots)^2+\cdots+A_{L-1}(\varepsilon.\varepsilon'\ldots)^{L-1}=B\varepsilon^i.\varepsilon'^{i'}\ldots,$$

*) Id quod ratione supra (pag. 19) exhibita probatur.

in qua certe non omnes coefficientes A evanescere possunt. Ideoque coefficientem B non evanescere inde patet, quod functio periodi ε gradus $L-1^{\text{ti}}$ evanescere nequit, nisi omnes eius coefficientes evanescunt (v. supra pag. 19).

Ex quibus dictis satis elucet, quodque numerorum complexorum productum rursus in formam:

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

redigi posse ideoque et ipsum numerum complexum esse.

Productum numerorum coniunctorum omnium norma appellatur et sicut supra signo $\mathrm{Nm}f(\varepsilon)$ denotatur.

Iam eadem ratione, qua Cl. *Kummer* in numeris primis ν demonstravit congruentiam λ^{ti} gradus $\mathrm{Nm}(x-\varepsilon)\equiv 0 \pmod{p}$ habere λ radices, et numero primo p sufficiente condicioni $p^\mu\equiv 1 \pmod{\nu}$ et casu $p=\nu$ (v. § 2), id quod huic rei respondet, posito ν numerum esse compositum, probari potest: scilicet congruentiam gradus $\lambda\lambda'\lambda''\ldots$ hanc $\mathrm{Nm}(x-\varepsilon)\equiv 0 \pmod{p}$ habere totidem radices reales, si p supponitur numerus talis, ut sit $p^\mu\equiv 1 \pmod{a^\alpha}$, $p^{\mu'}\equiv 1 \pmod{b^\beta}$, ..., vel etiam pro aliquo ipso ipsius ν factore primo e. g. $p=a$, dummodo $a^{\mu'}\equiv 1 \pmod{b^\beta}$ etc. sit*).

Pro talibus numeris primis p, quales tantum congruentiis sufficiunt

$$p^{a^k\delta}\equiv 1 \pmod{a^\alpha},\quad p^{b^{k'}\delta'}\equiv 1 \pmod{b^\beta},\quad \ldots,$$

ubi δ, $\delta'\ldots$ divisores numerorum $a-1$, $b-1$, ..., numeri autem k, k', ... vel omnes vel partim >0 sunt, erit $\mathrm{Nm}(x-\varepsilon)\equiv 0 \pmod{p}$ designante ε periodum compositam e radicibus primitivis aequationis $z^{a^{\alpha-k}b^{\beta-k'}\ldots}=1$ atque habebuntur $\frac{\varphi(\nu)}{a^k.\delta.b^{k'}.\delta'\ldots}$ istius congruentiae radices x.

Quibus iam praeparatis theoremata iis, quae in paragraphis 2–6 pro numeris primis ν tradita sunt, respondentia nullo fere negotio pro numeris compositis ν probari possunt.

---

*) Id quod etiam e theoremate quodam generali a Clo. *Schoenemann* tradito colligi potest (*Crelles* Journal Bd. 19, S. 293).

PARS ALTERA.

§ 8.

Posito literas ν, μ, λ, ω, ε eandem habere vim quam in § 1 etiamque acceptis numeris complexis formae illius:

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

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

$$a\varepsilon + a_1\varepsilon_1 + \cdots + a_{\lambda-1}\varepsilon_{\lambda-1}$$

formam esse λ^{ti} gradus atque λ indeterminatarum a, a_1, ... $a_{\lambda-1}$ et quidem determinantis, ut ita dicam, numeri primi ν sponte patet*). Quas aequationes $F = 1$ fere partes aequationis Pellianae agere imprimis ex eo elucet, quod casu $\lambda = 2$ atque $\nu \equiv 1 \pmod 4$ fit

$$\varepsilon = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{\nu}, \quad \varepsilon_1 = -\tfrac{1}{2} - \tfrac{1}{2}\sqrt{\nu},$$

unde:

$$\mathrm{Nm} f(\varepsilon) = \tfrac{1}{4}\{(a+a_1)^2 - \nu(a-a_1)^2\}.$$

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

Cum omnis periodorum functio etiam tanquam ipsarum radicum functio considerari possit, ponimus $f(\varepsilon) = \varphi(\omega)$, sitque $\mathrm{Nm} f(\varepsilon) = 1$, ergo etiam $\mathrm{Nm}\,\varphi(\omega) = 1$. Sit porro

$$\frac{\varphi(\omega)}{\varphi(\omega^{-1})} = \psi(\omega),$$

quem numerum integrum esse apertum est, scilicet

$$\psi(\omega) = \varphi(\omega)^2 \varphi(\omega^2) \ldots \varphi(\omega^{\nu-2}).$$

Iam posito

$$\psi(\omega) = c + c_1\omega + c_2\omega^2 + \cdots + c_{\nu-1}\omega^{\nu-1}$$

*) Cf. *Eisenstein* „de formis cubicis etc.“ (*Crelles* Journal, Bd. 28).

**) Disputatio Cli. *Kummer* § 4.

additis aequationibus:

$$\psi(\omega).\psi(\omega^{-1}) = 1, \quad \psi(\omega^2).\psi(\omega^{-2}) = 1, \quad \ldots \quad \psi(\omega^{\nu-1}).\psi(\omega^{-(\nu-1)}) = 1$$

obtinemus:

$$\nu(c^2+c_1{}^2+\cdots+c_{\nu-1}^2)-(c+c_1+\cdots+c_{\nu-1})^2 = \nu-1\ ^*),$$

unde

$$c+c_1+\cdots+c_{\nu-1} \equiv \pm 1 \pmod{\nu},$$

quocirca haec coefficientium summa etiam aequalis ± 1 accipi potest. Itaque habemus:

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

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

$$\psi(\omega) = \frac{\varphi(\omega)}{\varphi(\omega^{-1})} = \pm\omega^n$$

esse, unde (cum signum + valere ex congruentia $\varphi(\omega) \equiv \omega^n\varphi(\omega^{-1}) \pmod{(1-\omega)}$ colligere possimus):

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

atque posito $-n \equiv 2m \pmod{\nu}$ 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. Igitur si ad unitates formae $f(\varepsilon)$ revertimur, unitates complexae tanquam functiones periodorum *paris* terminorum numeri accipi possunt.

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

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

normam huius expressionis unitati aequalem facile patet, cum norma et numeratoris et denominatoris sit ν^{μ}. Deinde illam expressionem numerum complexum integrum esse patet, cum pro se quisque factor numeratoris $(1-\omega^{g^{k\lambda+1}})$ factore quodam denominatoris $(1-\omega^{g^{k\lambda}})$ dividi possit, quia $\frac{1-\omega^{g^{k\lambda+1}}}{1-\omega^{g^{k\lambda}}} = \frac{1-x^g}{1-x}$ posito $\omega^{g^{k\lambda}} = x$. Denique illa expressio functio periodorum ε est, quia mu-

*) Cf. id quod pag. 4 exposuimus.

tata radice ω in $\omega^{g^{k\lambda}}$ immutata manet. Hinc igitur patet $\psi(\varepsilon)$ unitatem esse integram complexam. — Etiamque producta:

$$\psi(\varepsilon)^n . \psi(\varepsilon_1)^{n_1} \dots \psi(\varepsilon_{\lambda-1})^{n_{\lambda-1}},$$

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

Adnotamus quamvis quantitatem $\psi(\varepsilon_k)$ positivam realem esse. Etenim cum numerus μ par suppositus sit, cuique factori

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

respondet. Quibus multiplicatis obtinemus $2-2\cos v = 4\sin^2 \frac{1}{2} v$, ubi

$$v = \frac{2}{\nu} \cdot g^{n\lambda+k+1} . \pi.$$

Unde iam et numeratorem et denominatorem ipsius $\psi(\varepsilon_k)$ positivum esse elucet.

§ 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:

$$\text{(I.)} \quad \begin{cases} c\varepsilon & + c_1\varepsilon_1 + \dots + c_{\lambda-1}\varepsilon_{\lambda-1} = r_1, \\ c\varepsilon_1 & + c_1\varepsilon_2 + \dots + c_{\lambda-1}\varepsilon \quad = r_2, \\ \quad \vdots & \quad \vdots \quad \vdots \\ c\varepsilon_{\lambda-1} & + c_1\varepsilon + \dots + c_{\lambda-1}\varepsilon_{\lambda-2} = r_\lambda. \end{cases}$$

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

$$\text{(II.)} \quad \begin{cases} f_1 = r_1^{n_1} . r_2^{n_2} \dots r_{\lambda-1}^{n_{\lambda-1}}, \\ f_2 = r_2^{n_1} . r_3^{n_2} \dots r_\lambda^{n_{\lambda-1}}, \\ f_3 = r_3^{n_1} . r_4^{n_2} \dots r_1^{n_{\lambda-1}}, \\ \quad \vdots \quad \vdots \quad \vdots \\ f_{\lambda-1} = r_{\lambda-1}^{n_1} . r_\lambda^{n_2} \dots r_{\lambda-3}^{n_{\lambda-1}}, \\ f_\lambda = r_\lambda^{n_1} . r_1^{n_2} \dots r_{\lambda-2}^{n_{\lambda-1}}. \end{cases}$$

Quod systema $\lambda-1$ aequationum atque $\lambda-1$ indeterminatarum n est, nam aequationibus omnibus multiplicatis per condicionem $f_1 f_2 \dots f_\lambda = r_1 r_2 \dots r_\lambda = 1$ aequationem identicam $1 = 1$ obtinemus, unde sequitur, ut quaevis istarum

aequationum e $\lambda-1$ reliquis deduci possit. Quodsi in systemate (II) logarithmos pro numeris adhibemus atque signis $\log f_k = \varphi_k$, $\log r_k = \varrho_k$ valores logarithmorum naturalium denotamus, obtinetur:

$$\text{(III.)} \quad \begin{cases} \varphi_1 = n_1\varrho_1 + n_2\varrho_2 + \cdots + n_{\lambda-1}\varrho_{\lambda-1}, \\ \varphi_2 = n_1\varrho_2 + n_2\varrho_3 + \cdots + n_{\lambda-1}\varrho_\lambda, \\ \vdots \qquad\quad \vdots \quad\; \vdots \quad\; \vdots \\ \varphi_\lambda = n_1\varrho_\lambda + n_2\varrho_1 + \cdots + n_{\lambda-1}\varrho_{\lambda-2}. \end{cases}$$

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

$$\text{(IV.)} \quad \varphi_1+\varphi_2\alpha+\cdots+\varphi_\lambda\alpha^{\lambda-1} = (n_1+n_2\alpha^{-1}+\cdots+n_{\lambda-1}\alpha^{-(\lambda-2)}).(\varrho_1+\varrho_2\alpha+\cdots+\varrho_\lambda\alpha^{\lambda-1}).$$

Iam positis:

$$\varphi_1+\varphi_2\alpha+\varphi_3\alpha^2+\cdots+\varphi_\lambda\alpha^{\lambda-1} = \varphi(\alpha),$$
$$\varrho_1+\varrho_2\alpha+\varrho_3\alpha^2+\cdots+\varrho_\lambda\alpha^{\lambda-1} = \varrho(\alpha)$$

erit

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

ergo:

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

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

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

atque designante α radicem unitatis λ^{tam} ***primitivam*** aequatio (V) locum tenet aequationum:

$$\psi(\alpha^k) = n_1+n_2\alpha^{-k}+\cdots+n_{\lambda-1}\alpha^{-k(\lambda-2)} \qquad (k=1, 2, \ldots \lambda-1).$$

Unde (sicut pag. 4) colligimus esse:

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

pro valoribus $k=0, 1, \ldots \lambda-2$ et

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

ergo denique:

$$\text{(VI.)} \quad \lambda n_{k+1} = (\alpha^k-\alpha^{-1})\psi(\alpha)+(\alpha^{2k}-\alpha^{-2})\psi(\alpha^2)+\cdots+(\alpha^{(\lambda-1)k}-\alpha)\psi(\alpha^{\lambda-1}),$$

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

$$\varrho(\alpha).\varrho(\alpha^2)\ldots\varrho(\alpha^{\lambda-1})$$

est, designante α radicem primitivam. Ergo probandum est, nullum istius producti factorem evanescere, seu quantitatem

$$\varrho_1+\varrho_2\alpha+\varrho_3\alpha^2+\cdots+\varrho_\lambda\alpha^{\lambda-1} \quad \text{i. e.} \quad \sum_{k=0}^{k=\lambda-1}\varrho_{k+1}\alpha^k$$

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

$$\varrho_{k+1}=\log r_{k+1}=\log\frac{(1-\omega^{g^{k+1}})(1-\omega^{g^{k+1+\lambda}})\ldots(1-\omega^{g^{k+1+(\mu-1)\lambda}})}{(1-\omega^{g^k})\quad(1-\omega^{g^{k+\lambda}})\quad\ldots(1-\omega^{g^{k+(\mu-1)\lambda}})}$$

sive:

$$\begin{aligned}\varrho_{k+1} \;=\; &\log(1-\omega^{g^{k+1}})+\log(1-\omega^{g^{k+1+\lambda}})+\cdots+\log(1-\omega^{g^{k+1+(\mu-1)\lambda}})\\ &-\log(1-\omega^{g^k})\quad-\log(1-\omega^{g^{k+\lambda}})\quad-\cdots-\log(1-\omega^{g^{k+(\mu-1)\lambda}})\end{aligned}$$

$\varrho(\alpha)$ sive $\Sigma\varrho_{k+1}\alpha^k$ abit in:

$$\begin{cases}\sum_0^{\lambda-1}\{\log(1-\omega^{g^{k+1}})+\log(1-\omega^{g^{k+1+\lambda}})+\cdots+\log(1-\omega^{g^{k+1+(\mu-1)\lambda}})\}\alpha^k\\ -\sum_0^{\lambda-1}\{\log(1-\omega^{g^k})\quad+\log(1-\omega^{g^{k+\lambda}})\quad+\cdots+\log(1-\omega^{g^{k+(\mu-1)\lambda}})\}\alpha^k\end{cases}$$

sive

$$\sum_{k=0}^{k=\mu\lambda-1}\alpha^k.\log(1-\omega^{g^{k+1}})-\sum_{k=0}^{k=\mu\lambda-1}\alpha^k.\log(1-\omega^{g^k}),$$

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

Iam cum sit:

$$-\log(1-\omega^{g^k}) \;=\; \frac{\omega^{g^k}}{1}+\frac{\omega^{2g^k}}{2}+\frac{\omega^{3g^k}}{3}+\cdots,$$

fit:

$$-\sum_0^{\mu\lambda-1}\alpha^k\log(1-\omega^{g^k}) \;=\; \sum_n\sum_{k=0}^{k=\mu\lambda-1}\alpha^k.\frac{\omega^{ng^k}}{n},$$

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

$$\omega^{ng^k}=1 \text{ et } \sum_0^{\mu\lambda-1}\frac{\alpha^k}{n}=\frac{1}{n}(1+\alpha+\alpha^2+\cdots+\alpha^{\mu\lambda-1})=0.$$

Quodsi Cli. *Jacobi* signis utimur, expressio

$$\sum_n\sum_0^{\mu\lambda-1}\alpha^k.\frac{\omega^{ng^k}}{n} \quad \text{abit in} \quad \sum_n\frac{1}{n}(\alpha,\omega^n),$$

ubi

$$(\alpha,\omega) \;=\; \omega+\alpha\omega^g+\alpha^2\omega^{g^2}+\cdots+\alpha^{\nu-2}\omega^{g^{\nu-2}},$$

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

$$-\Sigma\alpha^k.\log(1-\omega^{gk}) = (\alpha, \omega)\Sigma\frac{\alpha^{-\mathrm{Ind}.n}}{n}$$

et mutato ω in ω^g:

$$\Sigma\alpha^k.\log(1-\omega^{gk+1}) = -(\alpha, \omega^g)\Sigma\frac{\alpha^{-\mathrm{Ind}.n}}{n}$$

i. e.

$$\Sigma\alpha^k.\log(1-\omega^{gk+1}) = -\alpha^{-1}(\alpha, \omega).\Sigma\frac{\alpha^{-\mathrm{Ind}.n}}{n}.$$

Ergo habemus denique:

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

Iam 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 $\Sigma\frac{\alpha^{-\mathrm{Ind}.n}}{n}$ non evanescere probetur. Tum etiam $\Sigma\frac{\alpha^{+\mathrm{Ind}.n}}{n}$ evanescere deberet, id quod pro nullo α, quod sit radix aequationis $x^{\nu-1} = 1$, ideoque etiam pro nulla radice unitatis λ^{ta} α fieri posse Cl. *Lejeune-Dirichlet* in illustri illa commentatione „de progressione 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:

$$\text{(I.)} \quad f_1 = r_1^{E_1}.r_2^{E_2}\ldots r_{\lambda-1}^{E_{\lambda-1}}.r_1^{\delta_1}r_2^{\delta_2}\ldots r_{\lambda-1}^{\delta_{\lambda-1}} \quad \text{etc.}$$

Ex quibus aequationibus, cum et f_1 et $r_1^{E_1}.r_2^{E_2}\ldots r_{\lambda-1}^{E_{\lambda-1}}$ unitates integrae complexae sint, alter quoque dextrae partis factor: $r_1^{\delta_1}.r_2^{\delta_2}\ldots r_{\lambda-1}^{\delta_{\lambda-1}}$ unitas integra complexa sit oportet. Ponatur igitur:

$$\text{(II.)} \quad \begin{cases} r_1^{\delta_1}r_2^{\delta_2}\ldots r_{\lambda-1}^{\delta_{\lambda-1}} = F_1 = A\varepsilon & + A_1\varepsilon_1 + \cdots + A_{\lambda-1}\varepsilon_{\lambda-1}, \\ r_2^{\delta_1}r_3^{\delta_2}\ldots r_{\lambda}^{\delta_{\lambda-1}} = F_2 = A\varepsilon_1 & + A_1\varepsilon_2 + \cdots + A_{\lambda-1}\varepsilon, \\ \quad\vdots \qquad\qquad \vdots & \qquad\vdots \\ r_{\lambda}^{\delta_1}r_1^{\delta_2}\ldots r_{\lambda-2}^{\delta_{\lambda-1}} = F_\lambda = A\varepsilon_{\lambda-1} + A_1\varepsilon & + \cdots + A_{\lambda-1}\varepsilon_{\lambda-2} \end{cases}$$

designantibus A, A_1, ... numeros integros. Quo facto secundum aequationes

illas VII § 1 has quae sequuntur aequationes tanquam istius systematis aequationum II solutionem nanciscimur:

$$\text{(III.)}\quad \begin{cases} -\nu.A &= F_1(\mu-\varepsilon) &+F_2(\mu-\varepsilon_1)+\cdots+F_\lambda(\mu-\varepsilon_{\lambda-1}),\\ -\nu.A_1 &= F_1(\mu-\varepsilon_1) &+F_2(\mu-\varepsilon_2)+\cdots+F_\lambda(\mu-\varepsilon),\\ &\vdots &\vdots\quad\vdots\\ -\nu.A_{\lambda-1} &= F_1(\mu-\varepsilon_{\lambda-1})+F_2(\mu-\varepsilon) &+\cdots+F_\lambda(\mu-\varepsilon_{\lambda-2}). \end{cases}$$

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

$$\omega^{k_1}+\omega^{-k_1}+\omega^{k_2}+\omega^{-k_2}+\cdots+\omega^{k_\mathfrak{m}}+\omega^{-k_\mathfrak{m}}$$

sive igitur formae

$$2\cdot\left\{\cos\frac{2k_1\pi}{\nu}+\cos\frac{2k_2\pi}{\nu}+\cdots+\cos\frac{2k_\mathfrak{m}\pi}{\nu}\right\},$$

quod aggregatum cosinuum ipsorum numero $\frac{1}{2}\mu$ minus esse in promptu est.

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

$$\mathfrak{F}_1(\mu-\varepsilon_k)+\mathfrak{F}_2(\mu-\varepsilon_{k+1})+\cdots+\mathfrak{F}_\lambda(\mu-\varepsilon_{k-1})>-\nu A_k,$$
$$-\mathfrak{F}_1(\mu-\varepsilon_k)-\mathfrak{F}_2(\mu-\varepsilon_{k+1})-\cdots-\mathfrak{F}_\lambda(\mu-\varepsilon_{k-1})<-\nu A_k,$$

sive

$$\frac{1}{\nu}\{\mathfrak{F}_1(\mu-\varepsilon_k)+\cdots+\mathfrak{F}_\lambda(\mu-\varepsilon_{k-1})\}>A_k>-\frac{1}{\nu}|\mathfrak{F}_1(\mu-\varepsilon_k)+\cdots+\mathfrak{F}_\lambda(\mu-\varepsilon_{k-1})|.$$

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

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

$$F.r_1^{k_1}.r_2^{k_2}\ldots r_{\lambda-1}^{k_{\lambda-1}}$$

contineantur, designantibus k_1, k_2, ... numeros integros et F unitatem quandam e numero unitatum finito electam, sive denique ut numerus unitatum fundamentalium, quarum potestatibus integris omnis unitas repraesentari queat, finitus sit.

§ 11.

Iam accuratius, quibus limitibus numeri integri $A, A_1, \ldots$ sint circumscripti, consideraturi sumus, quo labor inveniendi unitates fundamentales aliquanto diminuatur. Ad quem finem disquisitionem instituamus de illa expressione ipsius $-\nu A_k$ (§ 10, III):

$$\text{(I.)} \qquad F_1(\mu-\varepsilon_k)+F_2(\mu-\varepsilon_{k+1})+\cdots+F_\lambda(\mu-\varepsilon_{k-1}),$$

ubi

$$F_n = r_n^{\delta_1}.r_{n+1}^{\delta_2}\ldots r_{n-2}^{\delta_{\lambda-1}},$$

eamque consideremus tanquam functionem quantitatum δ. Quotientes differentiales istius functionis 1 respectu quantitatum δ_1, δ_2, ... sunt:

$$\text{(II.)} \quad \begin{cases} F_1(\mu-\varepsilon_k)\varrho_1 & +F_2(\mu-\varepsilon_{k+1})\varrho_2+\cdots+F_\lambda(\mu-\varepsilon_{k-1})\varrho_\lambda, \\ F_1(\mu-\varepsilon_k)\varrho_2 & +F_2(\mu-\varepsilon_{k+1})\varrho_3+\cdots+F_\lambda(\mu-\varepsilon_{k-1})\varrho_1, \\ \qquad\vdots & \qquad\vdots \qquad\qquad\vdots \\ F_1(\mu-\varepsilon_k)\varrho_{\lambda-1}+F_2(\mu-\varepsilon_{k+1})\varrho_\lambda+\cdots+F_\lambda(\mu-\varepsilon_{k-1})\varrho_{\lambda-2}, \end{cases}$$

in quibus formulis notatione iam supra adhibita, $\log r_k = \varrho_k$, usi sumus.

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

$$\begin{cases} F_1(\mu-\varepsilon_k)\varrho_1^2 & +F_2(\mu-\varepsilon_{k+1})\varrho_2^2+\cdots+F_\lambda(\mu-\varepsilon_{k-1})\varrho_\lambda^2, \\ F_1(\mu-\varepsilon_k)\varrho_2^2 & +F_2(\mu-\varepsilon_{k+1})\varrho_3^2+\cdots+F_\lambda(\mu-\varepsilon_{k-1})\varrho_1^2, \\ \qquad\vdots & \qquad\vdots \qquad\qquad\vdots \\ F_1(\mu-\varepsilon_k)\varrho_{\lambda-1}^2+F_2(\mu-\varepsilon_{k+1})\varrho_\lambda^2+\cdots+F_\lambda(\mu-\varepsilon_{k-1})\varrho_{\lambda-2}^2, \end{cases}$$

quas expressiones pro quibusvis quantitatum δ valoribus positivas manere elucet. Unde facili consideratione colligi potest, functionem illam (I), dum variabiles δ intervallum inter 0 et 1 percurrunt, valorem haud maiorem obtinere posse eo, qui inter valores functionis extremis ipsorum δ valoribus respondentes maximus sit. Quare quaestio de valore ipsius νA_k 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 $2^{\lambda-1}$) respondentes computentur, ut valor earum maximus M inveniatur. Sit numerus integer ipso $\frac{M}{\nu}$ minor eique proximus $= n$; iam unitates omnes complexae, quarum coefficientes inter $-n$ et $+n$ sunt, statuendae atque inter eas, quae ad alias reduci possunt, reiiciendae, ut tandem numerus unitatum fundamentalium quam minimus restet.

Sic e. g. posito $\nu = 7$, $\lambda = 3$ atque

$$r_1 = \omega + \omega^{-1}, \quad r_2 = \omega^2 + \omega^{-2}, \quad r_3 = \omega^3 + \omega^{-3}$$

iste numerus $n = 1$ sine magno labore invenitur, ita ut valores coefficientium sint -1, 0, $+1$. Numeri igitur complexi 24 disquirendi *), inter quos vero terni factores sunt coniuncti. Inter octo illos, qui supersunt, rursus bini numeros aequales sed signo tantum oppositos praebent, ita ut denique hi quatuor restent:

$$\varepsilon_1 = \omega + \omega^{-1},$$
$$\varepsilon_1 + \varepsilon_2 = \omega + \omega^{-1} + \omega^2 + \omega^{-2} = \varepsilon_2 . \varepsilon_3,$$
$$\varepsilon_1 + \varepsilon_2 - \varepsilon_3 = \omega + \omega^{-1} + \omega^2 + \omega^{-2} - \omega^3 - \omega^{-3} = -\varepsilon_2 . \varepsilon_3^3,$$
$$\varepsilon_1 - \varepsilon_2 \text{ unitas complexa non est.}$$

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

Haud inutile videtur hoc ipsum exemplum paulo uberius exponere, ut id de quo agitur magis in promptu sit. Cum enim sit:

$$\mathrm{Nm}(x\varepsilon + y\varepsilon_1 + z\varepsilon_2) = (x+y+z)^3 - 7(xy^2 + yz^2 + zx^2 + xyz),$$

solutionem aequationis

$$(x+y+z)^3 - 7(xy^2 + yz^2 + zx^2 + xyz) = \pm 1$$

numeris integris ita invenimus, ut numeri x, y, z integri determinentur aequationibus **):

$$\begin{cases} -7x = (\omega+\omega^{-1})^m(\omega^2+\omega^{-2})^n(2-\omega-\omega^{-1}) + (\omega^2+\omega^{-2})^m(\omega^3+\omega^{-3})^n(2-\omega^2-\omega^{-2}) \\ \qquad\qquad + (\omega^3+\omega^{-3})^m(\omega+\omega^{-1})^n(2-\omega^3-\omega^{-3}), \\ -7y = (\omega+\omega^{-1})^m(\omega^2+\omega^{-2})^n(2-\omega^2-\omega^{-2}) + (\omega^2+\omega^{-2})^m(\omega^3+\omega^{-3})^n(2-\omega^3-\omega^{-3}) \\ \qquad\qquad + (\omega^3+\omega^{-3})^m(\omega+\omega^{-1})^n(2-\omega-\omega^{-1}), \\ -7z = (\omega+\omega^{-1})^m(\omega^2+\omega^{-2})^n(2-\omega^3-\omega^{-3}) + (\omega^2+\omega^{-2})^m(\omega^3+\omega^{-3})^n(2-\omega-\omega^{-1}) \\ \qquad\qquad + (\omega^3+\omega^{-3})^m(\omega+\omega^{-1})^n(2-\omega^2-\omega^{-2}), \end{cases}$$

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

---

*) Nempe omissis his: 0, $\varepsilon_1 + \varepsilon_2 + \varepsilon_3$, $-\varepsilon_1 - \varepsilon_2 - \varepsilon_3$.

**) v. III. § 10.

§ 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: $f, f', f'', \ldots$, quarum logarithmi resp. literis $\varphi, \varphi', \varphi'', \ldots$ designentur. Quodsi literis

$$r_1, \quad r_2, \quad \ldots \quad r_\lambda; \quad \varrho_1, \quad \varrho_2, \quad \ldots \quad \varrho_\lambda$$

eandem quam in paragraphis antecedentibus tribuimus vim, hae ipsae unitates potestatibus integris ipsorum f exprimi possint oportet. Quare sit:

$$\begin{aligned}
r_1 &= f^{a_1} \cdot f'^{b_1} \cdot f''^{c_1} \cdots, & \varrho_1 &= a_1\varphi + b_1\varphi' + c_1\varphi'' + \cdots,\\
r_2 &= f^{a_2} \cdot f'^{b_2} \cdot f''^{c_2} \cdots, & \varrho_2 &= a_2\varphi + b_2\varphi' + c_2\varphi'' + \cdots,\\
&\vdots & &\vdots\\
r_{\lambda-1} &= f^{a_{\lambda-1}} \cdot f'^{b_{\lambda-1}} \cdot f''^{c_{\lambda-1}} \cdots, & \varrho_{\lambda-1} &= a_{\lambda-1}\varphi + b_{\lambda-1}\varphi' + c_{\lambda-1}\varphi'' + \cdots.
\end{aligned}$$

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

$$\text{(I.)} \qquad n_1\varrho_1 + n_2\varrho_2 + \cdots + n_{\lambda-1}\varrho_{\lambda-1} = 0,$$

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

Ex aequatione enim (I) colligimus aequationem:

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

unde rursus mutatis periodis, quae expressionibus r continentur, hoc oritur aequationum systema:

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

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. Cum autem factorem secundum non evanescere iam 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 $r_1, r_2, \ldots r_{\lambda-1}, r_\lambda$ unitates aliquas coniunctas, denotamus productum:

$$r_1^{n_1} . r_2^{n_2} \ldots r_{\lambda-1}^{n_{\lambda-1}}$$

signo:

$$r_1^{n_1+n_2\alpha+\cdots+n_{\lambda-1}\alpha^{\lambda-2}} \quad \text{sive} \quad r_1^{n(\alpha)}.$$

Id quod ita quoque exhiberi potest, ut dicamus, posito

$$r_1^{n_1} . r_2^{n_2} \ldots r_{\lambda-1}^{n_{\lambda-1}} = f_1,$$

pro aequationibus illis (IV § 9):

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

substitui aequationem:

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

Iam primum adnotandum est, productum $r_1^{n_1} . r_2^{n_2} \ldots r_\lambda^{n_\lambda}$ aequatione

$$r_1 . r_2 \ldots r_\lambda = 1$$

ad productum $\lambda-1$ terminorum pariterque numerum complexum $n(\alpha)$ ope aequationis

$$1+\alpha+\alpha^2+\cdots+\alpha^{\lambda-1} = 0$$

ad expressionem $\lambda-1$ terminorum redigi posse.

E definitione statim sequuntur aequationes:

$$r_1^{n(\alpha)} = r_2^{\alpha^{-1}n(\alpha)} = r_3^{\alpha^{-2}n(\alpha)} = \cdots = r_\lambda^{\alpha^{-(\lambda-1)}n(\alpha)},$$

$$r_1^{m(\alpha)+n(\alpha)} = r_1^{m(\alpha)} . r_1^{n(\alpha)}.$$

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

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

Posito enim

$$r_1^{n(\alpha)} = s_1 \quad \text{et} \quad [r_1^{n(\alpha)}]^{m(\alpha)} = s_1^{m(\alpha)} = t_1$$

habemus aequationes:

$$r_1^{n_1} . r_2^{n_2} \cdots = s_1, \quad r_2^{n_1} . r_3^{n_2} \cdots = s_2, \quad \ldots,$$

quae posito $\log s_k = \sigma_k$ secundum § 9, (II), (III), (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:

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

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

Iam patet, posito λ numerum primum esse, istos exponentes symbolicos sicuti numeros complexos tractari posse, cum omnes eorum reductiones eo tantum nitantur, ut sit:

$$1+\alpha+\alpha^2+\cdots+\alpha^{\lambda-1} = 0,$$

id quod cum nostra definitione consentit, scilicet

$$r_1^{1+\alpha+\cdots+\alpha^{\lambda-1}} = r_1.r_2\ldots r_\lambda = 1 = r_1^0.$$

Deinde praemittendum est, literis r illa priore vi gaudentibus, cum 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^{tis} unitatis radicibus excepta unitate.

Demonstravimus in § 9 quamvis unitatem complexam forma

$$r_1^{n_1}.r_2^{n_2}\ldots r_{\lambda-1}^{n_{\lambda-1}}$$

contineri, quae quantitates n etiam loco citato determinatae sunt. Iam vero istas quantitates rationales esse probabimus. — Etenim initio § 10, posita unitate integra complexa

$$f_1 = r_1^{n_1}.r_2^{n_2}\ldots r_{\lambda-1}^{n_{\lambda-1}},$$

etiam productum

$$r_1^{\delta_1}.r_2^{\delta_2}\ldots r_{\lambda-1}^{\delta_{\lambda-1}}$$

unitatem integram esse ostendimus, si quantitates δ residua sunt ipsorum n numero integro quam maximo subtracto. Cum vero quivis numerus irrationalis, variis numeris integris multiplicatus, innumera praebeat residua unitate minora eaque inter se diversa, cumque unitas f ad potestatem aliquam integram evecta rursus unitas integra sit, variis potestatibus integris unitatis f innumeras unitates inter se diversas formae

$$r_1^{\delta_1}.r_2^{\delta_2}\ldots r_{\lambda-1}^{\delta_{\lambda-1}}$$

(ubi $\delta_1, \delta_2, \ldots < 1$) obtineri posse elucet. Illo autem § 10 finitum tantummodo numerum unitatum complexarum huius formae existere demonstravimus;

id quod itaque a propositione nostra, quantitates n irrationales esse, abhorret. — Quod cum conferamus cum forma § 10 (sub finem) omnes unitates formae esse patet:

$$r_1^{\frac{m(\alpha)}{n}} . r_1^{k(\alpha)},$$

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

§ 14.

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

Cum 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:

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

Iam sit factor numerorum $m(\alpha)$ et n communis maximus $v(\alpha)$*), ita ut

$$m(\alpha) = a(\alpha).v(\alpha), \quad n = c(\alpha).v(\alpha),$$

loco illius exponentis $\frac{m(\alpha)}{n}$ scribere licet hunc: $\frac{a(\alpha)}{c(\alpha)}$. Cumque $a(\alpha)$ et $c(\alpha)$ nullum amplius factorem communem habeant, numerus inveniri potest $b(\alpha)$ talis, ut sit (v. § 4)

$$b(\alpha).a(\alpha) \equiv 1 \pmod{c(\alpha)}$$

sive

$$b(\alpha).a(\alpha) = 1 + F(\alpha).c(\alpha).$$

Cum vero $r^{\frac{m(\alpha)}{n}}$ sive $r^{\frac{a(\alpha)}{c(\alpha)}}$ unitas integra sit, eadem proprietate unitatem $r^{\frac{a(\alpha).b(\alpha)}{c(\alpha)}}$ sive $r^{\frac{1}{c(\alpha)}}.r^{F(\alpha)}$ ideoque etiam unitatem $r^{\frac{1}{c(\alpha)}}$ gaudere patet. De qua unitate cum illa unitas data deduci possit, scilicet evehendo eam ad potestatem integram $a(\alpha)$, hanc ipsam loco illius accipere convenit. Hinc elucet, pro illis unitatibus (I) accipi posse unitates huius formae:

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

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

Ut harum unitatum binae in unam conflentur, sit factor numerorum $n(\alpha)$ et $n'(\alpha)$ communis maximus $c(\alpha)$, ita ut sit

$$n(\alpha) = c(\alpha).m(\alpha), \quad n'(\alpha) = c(\alpha).m'(\alpha).$$

Iam cum numeri $m(\alpha)$ et $m'(\alpha)$ nullum amplius habeant factorem communem, numerus inveniri potest $a(\alpha)$ talis, ut sit (v. § 4)

$$a(\alpha).m(\alpha) \equiv 1 \pmod{m'(\alpha)}$$

sive

$$a(\alpha).m(\alpha)+b(\alpha).m'(\alpha) = 1.$$

Cum vero unitates $r^{\frac{1}{n(\alpha)}}$ et $r^{\frac{1}{n'(\alpha)}}$ integrae sint, unitates quoque $r^{\frac{b(\alpha)}{n(\alpha)}}$ et $r^{\frac{a(\alpha)}{n'(\alpha)}}$ etiamque $r^{\frac{b(\alpha)}{n(\alpha)}}.r^{\frac{a(\alpha)}{n'(\alpha)}}$ sive $r^{\frac{b(\alpha)}{n(\alpha)}+\frac{a(\alpha)}{n'(\alpha)}}$ integras esse in promptu est. Est vero:

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

unde igitur unitatem $r^{\frac{1}{c(\alpha).m(\alpha).m'(\alpha)}}$ integram esse liquet. De qua cum illae unitates $r^{\frac{1}{n(\alpha)}}$ et $r^{\frac{1}{n'(\alpha)}}$ evehendo eam resp. ad potestates integras $m'(\alpha)$ et $m(\alpha)$ 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:

$$u_1^{n(\alpha)} = u_1^{n_1}.u_2^{n_2}\ldots u_{\lambda-1}^{n_{\lambda-1}},$$

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

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

§ 15.

Unitas r nisi ipsa fundamentalis est, praeter eas unitates, quae potestatibus ipsius r integris complexis repraesentari possunt, numerus finitus existet unitatum formae: $r^{\frac{m(\alpha)}{n}}$. Inter quas erit una quaedam (vel plures), in qua norma exponentis i. e. $\mathrm{Nm}\frac{m(\alpha)}{n}$ reliquis minor est. Qualem unitatem

litera u designemus. Quae unitas eam habet proprietatem, ut si quae exstet unitas integra formae: $u^{\frac{h(\alpha)}{k}}$, norma exponentis i. e. $\mathrm{Nm}\frac{h(\alpha)}{k}$ unitate maior sit oporteat. Etenim cum

$$r^{\frac{m(\alpha)}{n}} = u$$

ideoque

$$r^{\frac{m(\alpha)}{n}\cdot\frac{h(\alpha)}{k}} = u^{\frac{h(\alpha)}{k}}$$

praetereaque $\mathrm{Nm}\frac{m(\alpha)}{n}\cdot\frac{h(\alpha)}{k} > \mathrm{Nm}\frac{m(\alpha)}{n}$ secundum suppositionem de unitate u factam esse debeat, illa condicio $\mathrm{Nm}\frac{h(\alpha)}{k} > 1$ sponte manat. — Iam demonstrabimus, unitatem u illa ratione electam fundamentalem esse, sive nullam existere unitatem integram, nisi quae eius potestate integra complexa repraesentari possit. Quodsi enim unitas exstet formae $u^{\frac{h(\alpha)}{k}}$ sive formae $u^{\frac{m(\alpha)}{n(\alpha)}}$, ubi numeros $m(\alpha)$ et $n(\alpha)$ omni factore communi carere supponere licet, numerus $a(\alpha)$ inveniri potest talis, ut sit (v. § 4)

$$a(\alpha)m(\alpha) \equiv 1 \pmod{n(\alpha)}.$$

Cum vero unitas $u^{\frac{m(\alpha)}{n(\alpha)}}$ ideoque $u^{a(\alpha)\frac{m(\alpha)}{n(\alpha)}}$ integra sit, ratione supra (§ 14) adhibita unitatem quoque $u^{\frac{1}{n(\alpha)}}$ integram esse colligimus. Ergo secundum supra exhibita $\mathrm{Nm}\frac{1}{n(\alpha)} \geqq 1$ esse debet i. e. $\mathrm{Nm}\,n(\alpha) \leqq 1$. Cum vero $\mathrm{Nm}\,n(\alpha)$ tanquam numerus integer unitate minor esse nequeat, tantum restat, ut sit $\mathrm{Nm}\,n(\alpha) = 1$, 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 u integris complexis repraesentari possint sequitur.

§ 16.

Postquam ostendimus, existere unitates quasdam fundamentales numeri $\lambda-1$ easque coniunctas in numeris λ illa virtute initio § 14 memorata praeditis, de his ipsis quaedam adnotamus. Designentur unitates aliquae fundamentales ut supra literis: $u_1, u_2, \ldots u_{\lambda-1}$, has ipsas tales esse ostendimus, ut $u_1^{n(\alpha)}$ cunctas repraesentet unitates, posito $n(\alpha)$ numerum aliquem integrum complexum. Quaeque unitates u ea ipsa proprietate gaudent, fundamentales

sunt. Nunc designante $k(\alpha)$ unitatem aliquam complexam integram atque posito: $u_1^{k(\alpha)} = v_1$, aperte est:

$$u_1^{k(\alpha)k(\alpha^2)\dots k(\alpha^{\lambda-1})} = u_1 = v_1^{k(\alpha^2)\dots k(\alpha^{\lambda-1})} = v_1^{K(\alpha)},$$

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

$$\begin{cases} u_1^{a_1} . u_2^{a_2} \dots u_{\lambda-1}^{a_{\lambda-1}} = A, \\ u_1^{b_1} . u_2^{b_2} \dots u_{\lambda-1}^{b_{\lambda-1}} = B, \\ \quad \vdots \qquad \vdots \qquad \vdots, \end{cases}$$

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

$$\begin{cases} a_1 \log u_1 + a_2 \log u_2 + \dots + a_{\lambda-1} \log u_{\lambda-1} = \log A, \\ b_1 \log u_1 + b_2 \log u_2 + \dots + b_{\lambda-1} \log u_{\lambda-1} = \log B, \\ \quad \vdots \qquad \vdots \qquad \vdots \qquad \vdots, \end{cases}$$

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

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

designante Δ determinantem illius systematis, m_1, m_2, ... numeros quosdam integros. Hinc iam patet, si systema istud ea gaudet proprietate, ut sit $\Delta = \pm 1$, unitates u ideoque omnes unitates potestatibus integris unitatum $A, B, \dots$ exprimi posse. Unde etiam tales unitates $A, B, \dots$ infinitis modis (dummodo $\lambda \geqq 3$) eligi posse, plane in promptu 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. Iam cum sint unitates pro $\lambda = 3$ sex scilicet:

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

habemus sexies binas unitates coniunctas fundamentales:

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

deinde positis $u_1^{a_1}.u_2^{a_2} = A$, $u_1^{b_1}.u_2^{b_2} = B$, 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 $\Delta = a_1 b_2 - a_2 b_1 = \pm 1$ condicio illa, ut unitates A et B partes unitatum fundamentalium agant. Cui aequationi innumeris modis satisfieri potest. E. g. positis:

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

habemus ut unitates fundamentales:

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

§ 17.

Nunc omissa suppositione illa, qua statuitur, omnem numerum primum formae $k\lambda + g^h$ in h factores complexos discerpi posse, servata vero ea, qua λ numerum esse primum continetur, unitates investigemus.

Quodsi literis $r_1, r_2, \ldots r_{\lambda-1}$ aliquas unitates coniunctas *) designamus, quaevis unitas integris istius unitatis datae potestatibus repraesentari potest, adiuncto numero finito certarum quarundam fractarum ipsorum r potestatum. Quare sint cunctae unitates, quibus praeter ipsas r ad exprimendas omnes unitates opus sit:

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

Iam si $n = kl$ et numerus k ad numerum l primus est, existunt numeri g et h tales, ut sit

$$hk + gl = 1,$$

ergo

$$\frac{hk^2}{n} + g = \frac{1}{l}, \quad \frac{gl^2}{n} + h = \frac{1}{k};$$

quare loco unitatis $r^{\frac{m(\alpha)}{n}}$ accipi possunt unitates

$$r^{\frac{m(\alpha)}{k}}, \quad r^{\frac{m(\alpha)}{l}},$$

cum illa unitas $r^{\frac{m(\alpha)}{n}}$ tanquam productum

$$r^{g.\frac{m(\alpha)}{k}}.r^{h.\frac{m(\alpha)}{l}}$$

*) Quae vero tales esse debent, ut expressio illa $\mathrm{Nm}(\varrho_1 + \varrho_2\alpha + \cdots + \varrho_\lambda\alpha^{\lambda-1})$ non evanescat (cf. § 9).

repraesentari potest. Eadem ratione probari potest, pro istis unitatibus (I) accipi posse unitates huius formae

$$\text{(II.)} \quad r^{\frac{k(\alpha)}{p^a}}, \quad r^{\frac{k'(\alpha)}{q^b}}, \quad \ldots,$$

quorum exponentium numeratores et denominatores factores reales communes non habere supponimus. Sit vero summa ipsius p potestas, qua numerus $\mathrm{Nm}\, k(\alpha)$ dividi possit: $p^{n\delta}$, ubi δ divisor ipsius $\lambda-1$ est is, ad quem $p \pmod{\lambda}$ pertinet. Iam in § 5 probavimus ista statuta condicione eaque addita, ut productum πp *) discerpi possit in δ factores complexos coniunctos, ita ut $\mathrm{Nm}\, p(\varepsilon) = \pi p$ sit, aequationem locum habere:

$$\text{(III.)} \quad \pi^n k(\alpha) = f(\alpha).p(\varepsilon)^m.p(\varepsilon_1)^{m_1}\ldots,$$

ubi $m+m_1+\cdots = n$ esse debet. Iam numero $\mathrm{Nm}\, f(\alpha)$ nullum amplius factorem p contineri patet, ideoque exstare numerum x talem, ut sit $x.\mathrm{Nm}\, f(\alpha) \equiv 1 \pmod{p^a}$. Unde cum unitas $r^{\frac{\pi^n k(\alpha)}{p^a}}$ integra sit, unitatem quoque hanc:

$$r^{\frac{p(\varepsilon)^m.p(\varepsilon_1)^{m_1}\ldots}{p^a}} = s$$

integram esse colligimus, atque ex hac ipsa illam unitatem datam $r^{\frac{k(\alpha)}{p^a}}$ deduci posse facile intelligitur. Posito enim y numero tali, ut sit $y\pi^n \equiv 1 \pmod{p^a}$, ex aequatione (III) sequitur congruentia:

$$yf(\alpha).p(\varepsilon)^m.p(\varepsilon_1)^{m_1}\cdots \equiv k(\alpha) \pmod{p^a}$$

sive aequatio:

$$yf(\alpha).p(\varepsilon)^m.p(\varepsilon_1)^{m_1}\cdots = k(\alpha)+p^a.\varphi(\alpha),$$

$$\text{unde} \quad s^{yf(\alpha)} = r^{\frac{k(\alpha)}{p^a}}.r^{\varphi(\alpha)} \quad \text{sive} \quad r^{\frac{k(\alpha)}{p^a}} = s^{yf(\alpha)}.r^{-\varphi(\alpha)}.$$

Quod si ad omnes illas unitates (II) adhibemus, sequitur, ut pro illis hae accipi possint unitates:

$$\text{(IV.)} \quad r^{\frac{p(\varepsilon)^m.p(\varepsilon_1)^{m_1}\ldots}{p^a}}, \quad r^{\frac{q(\varepsilon)^m.q(\varepsilon_1)^{m_1}\ldots}{q^a}}, \quad \ldots.$$

Qua in serie unitatum, si quae iisdem gaudent denominatoribus, eas hac ratione in unam conflare possumus. Sint datae:

$$r^{\frac{p(\varepsilon)^m.p(\varepsilon_1)^{m_1}\ldots}{p^a}}, \quad r^{\frac{p(\varepsilon)^n.p(\varepsilon_1)^{n_1}\ldots}{p^a}}$$

*) Numerus π talis eligendus, ut sit ad p primus, id quod tantum pro certis numerorum $\mathrm{Nm}(\varepsilon-\varepsilon_r)$ factoribus fieri nequit (v. § 5). His numeris vero methodus supra exhibita facili negotio adaptatur.

sitque complexus factorum $p(\varepsilon)$ utrique numeratori communium $f(\varepsilon)$, ita ut existant aequationes:

$$p(\varepsilon)^m . p(\varepsilon_1)^{m_1} \cdots = f(\varepsilon) . p(\varepsilon_h)^v . p(\varepsilon_{h'})^{v'} \cdots = f(\varepsilon) . \varphi(\varepsilon),$$
$$p(\varepsilon)^n . p(\varepsilon_1)^{n_1} \cdots = f(\varepsilon) . p(\varepsilon_k)^w . p(\varepsilon_{k'})^{w'} \cdots = f(\varepsilon) . \psi(\varepsilon),$$

ubi nullum k nulli h aequivalere potest. Quodsi numeri i, i'... tales sunt, ut coniuncti cum ipsis k et h seriem indicum 1, 2, ... $\frac{\lambda-1}{\delta}$ expleant, atque ponitur:

$$\varphi(\varepsilon) + \psi(\varepsilon) . p(\varepsilon_i) p(\varepsilon_{i'}) \cdots = \chi(\varepsilon),$$

in numero $\mathrm{Nm}\chi(\varepsilon)$ factor p inesse nequit, id quod ratione supra (§ 4) exhibita probari potest. Quare numerus exstat x, qui congruentiae satisfaciat: $x . \mathrm{Nm}\chi(\varepsilon) \equiv 1 \pmod{p^a}$. Deinde cum unitates:

$$r^{\frac{f(\varepsilon)\varphi(\varepsilon)}{p^a}} \quad \text{et} \quad r^{\frac{f(\varepsilon).\psi(\varepsilon)}{p^a}} \quad \text{ideoque} \quad r^{\frac{f(\varepsilon)\chi(\varepsilon)}{p^a}}$$

integrae sint, ope illius congruentiae $x . \mathrm{Nm} f(\varepsilon) \equiv 1 \pmod{p^a}$ etiam unitatem $r^{\frac{f(\varepsilon)}{p^a}}$ integram esse colligimus, ex qua quidem illas duas superiores deduci posse plane in promptu est.

Iam si quae exstant unitates seriei IV, quarum exponentium denominatores diversae potestates eiusdem numeri primi sunt, eas quoque in unam conflari posse hoc modo probamus. Sint datae unitates integrae:

$$r^{\frac{\varphi(\varepsilon)}{p^a}}, \quad r^{\frac{\psi(\varepsilon)}{p^b}},$$

ubi $b < a$. Fractionis $\frac{\psi(\varepsilon)}{p^b}$ et numeratore et denominatore numero πp^{a-b} multiplicatis obtinemus:

$$\frac{\psi(\varepsilon)}{p^b} = \frac{p(\varepsilon_1)^{a-b} p(\varepsilon_2)^{a-b} \ldots \psi(\varepsilon)}{\pi^{a-b} p^a} = \frac{\chi(\varepsilon)}{\pi^{a-b} p^a}.$$

Iam unitates $r^{\frac{\varphi(\varepsilon)}{p^a}}$ et $r^{\frac{\chi(\varepsilon)}{p^a}}$ methodo modo exhibita in unam possunt conflari, ex qua illas duas derivare licet. Ab hac vero unitate $r^{\frac{\chi(\varepsilon)}{p^a}}$ illa data $r^{\frac{\psi(\varepsilon)}{p^b}}$ facile deducitur. Est enim

$$r^{\frac{\chi(\varepsilon)}{p^a}} = r^{\pi^{a-b}\frac{\psi(\varepsilon)}{p^b}},$$

unde si x est numerus talis, ut sit

$$x.\pi^{a-b} \equiv 1 \pmod{p^b} \quad \text{sive} \quad x\pi^{a-b} = 1 + kp^b,$$

erit:

$$r^{x.\frac{\chi(\varepsilon)}{p^a}}.r^{-k\psi(\varepsilon)} = r^{\frac{\psi(\varepsilon)}{p^b}}.$$

Ex quibus dictis patet, loco illarum unitatum (I), vel (II), vel (IV) accipi posse unitates quasdam:

$$\text{(V.)} \quad r^{\frac{k(\alpha)}{p^a}}, \quad r^{\frac{k'(\alpha)}{q^b}}, \quad \ldots,$$

in quibus p, q, ... numeri sint primi inter se diversi, quaeque coniunctae cum ipsis r ad repraesentandas omnes unitates sufficiant. Iam probaturi sumus has ipsas unitates conflari posse in hanc:

$$r_1^{\frac{k(\alpha)}{p^a}+\frac{k'(\alpha)}{q^b}+\frac{k''(\alpha)}{t^c}+\ldots} = s_1.$$

Quam enim unitatem integram esse elucet, atque unitates illas (V) ope unitatum $r_1, r_2, \ldots r_{\lambda-1}$ ex unitate s deduci posse hoc modo probatur. Cum productum $q^b.t^c\ldots$ ad ipsum p primum sit, numerus inveniri potest x talis, ut sit:

$$x.q^b.t^c\ldots \equiv 1 \pmod{p^a} \quad \text{sive} \quad x.q^b.t^c\ldots = 1 + np^a,$$

quare erit

$$s^{x.q^b.t^c\ldots} = r_1^{\frac{k(\alpha)}{p^a}}.r_1^{nk(\alpha)+t^c\ldots k'(\alpha)+\ldots},$$

unde unitatem $r_1^{\frac{k(\alpha)}{p^a}}$ re vera potestatibus integris unitatum r et s exprimi posse manifestum est. Cuius explicationis summam hoc modo exhibere possumus: Acceptis quibuslibet unitatibus coniunctis $r_1, r_2, \ldots r_{\lambda-1}$, semper inveniri potest systema unitatum coniunctarum $s_1, s_2, \ldots s_{\lambda-1}$ tale, ut omnes unitates integris istarum unitatum r et s potestatibus exprimi liceat.

Iam cum summam tam determinatam neque de numero neque de natura unitatum fundamentalium casu generali huc usque consequi potuerimus, quam paragraphis 14 et 15 suppositione illa speciali explicavimus, relictis iis, quae insuper his methodis derivari possunt, si unitates „r“ certa quadam ratione eliguntur, ad casum eum transeamus, in quo λ numerus est compositus.

§ 18.

Nostra methodus cum eo nitatur, quod istas symbolicas exponentium expressiones ratione numerorum re vera complexorum tractavimus, etiam casu quo λ numerus est compositus, tales instituamus unitates, ut his adiumentis

uti possimus. Quem ad finem sit „d“ aliquis ipsius λ divisor, qui factores primos p q, ... contineat, atque „r“ unitas illa in § 9 memorata; ostendamus exstare unitates s_1, s_2, ... eiusmodi, ut his aequationibus satisfaciant:

$$\text{(I.)} \qquad s_k = s_{d+k} = s_{2d+k} = \cdots = s_{(\delta-1)d+k} \quad \text{posito} \quad \delta d = \lambda,$$

praetereaque his:

$$\text{(II.)} \qquad \begin{cases} s_k \cdot s_{\frac{d}{p}+k} \cdot s_{2\frac{d}{p}+k} \cdots s_{(p-1)\frac{d}{p}+k} = 1, \\ s_k \cdot s_{\frac{d}{q}+k} \cdot s_{2\frac{d}{q}+k} \cdots s_{(q-1)\frac{d}{q}+k} = 1, \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots \end{cases},$$

sive his quae illis aequivalent, si $\log s_k = \sigma_k$ et α radix quaevis aequationis $x^\lambda = 1$ ponitur:

(III.) $\sigma_1+\sigma_2\alpha+\cdots+\sigma_\lambda\alpha^{\lambda-1} = \sigma_{d+1}+\sigma_{d+2}\alpha+\cdots+\sigma_d\alpha^{\lambda-1}$, ergo $= \alpha^{-d}(\sigma_1+\sigma_2\alpha+\cdots+\sigma_\lambda\alpha^{\lambda-1})$

atque his:

$$\text{(IV.)} \qquad \begin{cases} (\sigma_1+\sigma_2\alpha+\cdots+\sigma_\lambda\alpha^{\lambda-1})(1+\alpha^{-\frac{d}{p}}+\alpha^{-2\frac{d}{p}}+\cdots+\alpha^{-(p-1)\frac{d}{p}}) = 0, \\ (\sigma_1+\sigma_2\alpha+\cdots+\sigma_\lambda\alpha^{\lambda-1})(1+\alpha^{-\frac{d}{q}}+\alpha^{-2\frac{d}{q}}+\cdots+\alpha^{-(q-1)\frac{d}{q}}) = 0, \\ \vdots \qquad\qquad\qquad\qquad \vdots \qquad\qquad\qquad\qquad \vdots \end{cases}.$$

Quae ipsae condiciones explentur, si expressio $\sigma(\alpha)$ pro quovis ipsius α valore exceptis iis, qui radices unitatis d^{tae} primitivae sunt, evanescit. Quod si fit, aequatio (III), quae pro valoribus ipsius α aequationi $\alpha^d = 1$ sufficientibus re ipsa expletur, etiam pro reliquis ipsius α valoribus locum tenet. Deinde aequationes (IV), quae pro iis tantum ipsius α valoribus, qui radices primitivae d^{tae} sunt, re ipsa explentur, etiam pro reliquis ipsius α valoribus valent. Iam ponamus:

$$\text{(V.)} \qquad s_1 = r_1^{a_1+a_2\alpha+\cdots+a_{\lambda-1}\alpha^{\lambda-2}} = r_1^{a_1} r_2^{a_2} \ldots r_{\lambda-1}^{a_{\lambda-1}},$$

ubi

$$a_1+a_2\alpha+\cdots+a_{\lambda-1}\alpha^{\lambda-2}$$
$$= (1+\alpha^d+\cdots+\alpha^{(\delta-1)d})(1+\alpha+\alpha^2+\cdots+\alpha^{\frac{d}{p}-1})(1+\alpha+\alpha^2+\cdots+\alpha^{\frac{d}{q}-1})\ldots .$$

Ex qua aequatione numeri a_1, a_2, ... ita sunt determinandi, ut explicato producto dextrae partis eoque solius aequationis $\alpha^\lambda = 1$ ope reducto singularum ipsius α potestatum coefficientes quantitatibus a_1, a_2... aequales ponantur, sive hoc modo, ut positis in aequatione (V) singulis ipsius α valoribus ex his $(\lambda-1)$ aequationibus illae $(\lambda-1)$ quantitates „a“ determinentur. — Unitates „s“ sic definitas illis aequationibus (I), (II), (III), (IV) satisfacere

iam probaturi sumus. — Ex illa enim aequatione (V) sequitur modo in § 10 tradito, ut sit:

$$\sigma_1+\sigma_2\alpha+\cdots+\sigma_\lambda\alpha^{\lambda-1} = a(\alpha^{-1})(\varrho_1+\varrho_2\alpha+\cdots+\varrho_\lambda\alpha^{\lambda-1})$$

pro quavis radice α. Cum vero expressio:

$$a(\alpha^{-1}) = \frac{1-\alpha^{-\lambda}}{1-\alpha^{-d}}\cdot\frac{1-\alpha^{-\frac{d}{p}}}{1-\alpha^{-1}}\cdot\frac{1-\alpha^{-\frac{d}{q}}}{1-\alpha^{-1}}\cdots$$

pro omnibus ipsius α valoribus exceptis radicibus d^{tis} primitivis evanescat, etiam expressionem $\sigma(\alpha)$ hanc ipsam habere proprietatem ideoque unitates „s" illis condicionibus sufficere patet.

Quaecunque unitates illis aequationibus (I), (II), (III), (IV) satisfaciunt classem efficiunt unitatum eam, quam ad divisorem „d" pertinere dicimus. Iam primum unitates eiusdem classis inter se comparabimus, et quidem omnes potestatibus vel integris vel fractis unius systematis unitatum coniunctarum exprimi posse probabimus. Etenim sint unitates aliquae ad divisorem d pertinentes hae: $f_1, f_2, \ldots f_d$; designentur deinde valores absoluti logarithmorum harum quantitatum signis: $\varphi_1, \varphi_2, \ldots \varphi_d$; hoc aequationum systema semper solvi potest:

$$\text{(VI.)}\quad \begin{cases} \varphi_1 = n_1\sigma_1+n_2\sigma_2+\cdots+n_k\sigma_k, \\ \varphi_2 = n_1\sigma_2+n_2\sigma_3+\cdots+n_k\sigma_{k+1}, \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ \varphi_d = n_1\sigma_d+n_2\sigma_1+\cdots+n_k\sigma_{k-1}, \end{cases}$$

ubi indeterminatae sunt quantitates $n_1, n_2, \ldots n_k$ atque numerus harum quantitatum, litera k designatus, numerus ille est, quem *Gauss* signo $\varphi(d)$ denotat, i. e. numerus numerorum ad ipsum „d" primorum eoque minorum. Designante w radicem aequationis $w^d = 1$ pro qualibet hac radice w, ratione in § 9 exhibita prodit aequatio:

$$\text{(VII.)}\quad \varphi_1+\varphi_2 w+\cdots+\varphi_d w^{d-1} = (n_1+n_2w^{-1}+\cdots+n_kw^{k-1})(\sigma_1+\sigma_2 w+\cdots+\sigma_d w^{d-1}).$$

Quam aequationem pro omnibus radicibus w non primitivis re ipsa expleri ex eo elucet, quod his casibus et $\varphi(w)$ et $\sigma(w)$ evanescunt, cum et unitates f et unitates s in classe ad divisorem d pertinente insint*). — Singuli ipsius w valores primitivi totidem aequationes praebent formae (VII), quarum igitur numerus k numero indeterminatarum aequalis est. Ut igitur indeterminatas ex iis determinari posse ostendamus, tantummodo determinantem systematis

*) v. quae supra indicata sit unitatum ad classem pertinentium proprietas.

illius non evanescere probandum est. Determinans autem cum sit:

$$\sigma(w).\sigma(w^h).\sigma(w^{h'})\ldots,$$

designantibus h, h', ... systema numerorum inter se incongruorum ad ipsum d primorum, aliquis factor $\sigma(w^h)$ evanescere deberet, ideoque foret:

$$\sigma_1+\sigma_2 w+\sigma_3 w^2+\cdots+\sigma_d w^{d-1} = 0$$

pro aliqua radice primitiva w, sive ratione habita aequationum (I) nec non aequationis huius: $\alpha^\delta = w$ esse deberet:

$$\sigma_1+\sigma_2\alpha^\delta+\sigma_3\alpha^{2\delta}+\cdots+\sigma_\lambda\alpha^{\delta(\lambda-1)} = 0$$

pro aliqua radice primitiva α. — Iam cum sit secundum aequationem (V):

$$\sigma_1+\sigma_2\alpha^\delta+\cdots+\sigma_\lambda\alpha^{\delta(\lambda-1)} = (\varrho_1+\varrho_2\alpha^\delta+\cdots+\varrho_\lambda\alpha^{\delta(\lambda-1)})(a_1+a_2\alpha^\delta+\cdots),$$

esse deberet:

$$\varrho(\alpha^\delta)(a_1+a_2\alpha^\delta+\cdots) = 0,$$

sive substituto ipsius $a(\alpha^\delta)$ valore et posito $\alpha^\delta = w$:

$$\ldots\ \varrho(\alpha^\delta).\delta.\frac{1-w^{\frac{d}{p}}}{1-w}.\frac{1-w^{\frac{d}{q}}}{1-w}\cdots = 0,$$

id quod fieri nequit, cum nullum factorem $(1-w^{\frac{d}{p}})$, ..., designante w radicem *primitivam* d^{tam}, evanescere pateat, neque factorem $\varrho(\alpha^\delta)$ nihilo aequivalere posse supra in § 9 demonstratum sit.

Iam cum probaverimus, quamvis unitatem ad ipsum „d“ pertinentem potestatibus ipsorum s repraesentari posse*), exponentes harum potestatum non irrationales esse ex eo elucet, quod, cum unitates s potestatibus integris unitatum r expressae sint, etiam unitates quaedam potestatibus ipsorum „r“ irrationalibus repraesentari possent, id quod fieri non posse in § 13 demonstravimus. Quare forma generalis unitatum ad divisorem „d“ pertinentium erit:

$$s_1^{\frac{m_1}{n}}.s_2^{\frac{m_2}{n}}\ldots s_k^{\frac{m_k}{n}}$$

sive:

$$s_1^{\frac{1}{n}(m_1+m_2w+\cdots+m_kw^{k-1})}$$

designantibus n, m_1, m_2, ... numeros integros reales.

In quibus unitatibus exponentes symbolicos tanquam veros numeros complexos tractare possumus, quia omnes eorum reductiones aequationibus nituntur:

*) Nempe si in aequationibus (VI) a logarithmis ad numeros transeas.

$$\begin{cases} 1+w^{\frac{d}{p}}+w^{2\frac{d}{p}}+\cdots+w^{(p-1)\frac{d}{p}} = 0, \\ 1+w^{\frac{d}{q}}+w^{2\frac{d}{q}}+\cdots+w^{(q-1)\frac{d}{q}} = 0, \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots \end{cases}$$

et

$$1+w+w^2+\cdots+w^{d-1} = 0,$$

cumque re vera sit:

$$s^{1+w^{\frac{d}{p}}+\cdots+w^{(p-1)\frac{d}{p}}} = s_1 . s_{\frac{d}{p}+1} \ldots s_{(p-1)\frac{d}{p}+1} = 1 = s_1^0 \quad \text{etc.}$$

nec non:

$$s_1^{1+w+\cdots+w^{d-1}} = s_1 . s_2 \ldots s_d = 1 = s_1^0.$$

§ 19.

Respectu habito eorum, quae in § 7 cum explicata tum indicata sint, atque posito „λ“ numerum esse eiusmodi, ut quivis numerus primus formae $k\lambda+r$ in n factores complexos, compositos e radicibus unitatis λ^{tis}, discerpi possit, si statuamus $g, g', g'', \ldots$ resp. numerorum $p^a, q^b, t^c, \ldots$ radices primitivas,

$$\lambda = p^a . q^b . t^c \ldots, \quad r \equiv \frac{\lambda}{p^a} \cdot g^h + \frac{\lambda}{q^b} \cdot g'^{h'} + \frac{\lambda}{t^c} g''^{h''} + \cdots \pmod{\lambda},$$

$$n = h . h' . h'' \ldots *),$$

omnino eadem qua in § 15 usi sumus ratione probatur, exstare in quavis classe unitatem u, cuius potestatibus integris complexis omnes unitates ad eandem classem pertinentes repraesentari possint. Cumque quivis numerus complexus integer ex unitatis radicibus d^{tis} compositus ad expressionem $\varphi(d)$ terminorum integram redigi possit**), $\varphi(d)$ unitates coniunctas exstare patet, quarum potestatibus integris omnes unitates ad divisorem d pertinentes exprimi possint.

Iam eadem qua in § 16 usi sumus ratione probari potest, designante „u“ unitatem fundamentalem classis ad ipsum d pertinentis, omnes reliquas eiusdem classis unitates fundamentales easque solas forma contineri: $u^{m(w)}$, si $m(w)$ numerus est talis, ut $\text{Nm}\, m(w) = 1$. Etiamque unitates non coniunctae statui possunt fundamentales multitudinis $\varphi(d)$, et quidem numerus unitatum diversarum, quae statui possunt, fundamentalium coniunctarum erit

*) Numeri $h, h', \ldots$ resp. multipla numerorum $p^{a-1}, q^{b-1}, \ldots$ esse debent.

**) v. § 7.

infinitus, dummodo $\varphi(d) > 2$, ergo $d \geqq 8$, numerus vero unitatum fundamentalium non coniunctarum erit infinitus, quando $\varphi(d) \geqq 2$, ergo $d > 2$.

Denique omissa illa suppositione, qua statuitur, omnem numerum primum formae $k\lambda + r$ in n factores complexos discerpi posse, ratione illa in § 17 exhibita demonstrari potest: dato quocunque systemate unitatum coniunctarum ad classem aliquam pertinentium*), semper existere aliud systema, quo alteri adiuncto cunctae eiusdem classis unitates repraesentari possint. Et quidem secundum supra adnotata utrarumque unitatum tantummodo $\varphi(d)^{\text{nis}}$ opus erit.

Iam etiam probemus numerum unitatum fundamentalium ipso $\varphi(d)$ minorem non sufficere ad repraesentandas omnes unitates eiusdem classis. Quem ad finem sint unitates quaedam fundamentales: $f, f', f'', \ldots$, itaque illas quoque unitates „s“ potestatibus harum f integris repraesentari posse oportet. Quare sit posito $\log f = \varphi$, $\log f' = \varphi'$, ... et $k = \varphi(d)$:

$$\begin{cases} \sigma_1 = a_1\varphi + b_1\varphi' + c_1\varphi'' + \cdots, \\ \sigma_2 = a_2\varphi + b_2\varphi' + c_2\varphi'' + \cdots, \\ \vdots \qquad\quad \vdots \qquad\quad \vdots \\ \sigma_k = a_k\varphi + b_k\varphi' + c_k\varphi'' + \cdots. \end{cases}$$

Cum vero numerus ipsorum f itaque ipsorum φ sit $\leqq k-1$, his ipsis eliminatis certe una restabit aequatio formae huiusce:

$$\text{(I.)} \qquad n_1\sigma_1 + n_2\sigma_2 + \cdots + n_k\sigma_k = 0,$$

in qua aequatione $n_1, n_2, \ldots$ numeri esse debent integri atque non omnes nihilo aequales. Id quod fieri non posse sequentibus probatur. Ex aequatione enim (I) sequitur: $s_1^{n_1} s_2^{n_2} \ldots s_k^{n_k} = 1$, unde mutatis periodis iis, quae unitatibus „s“ continentur, oritur systema aequationum:

$$\begin{cases} s_1^{n_1} s_2^{n_2} \ldots s_k^{n_k} = 1, \\ s_2^{n_1} s_3^{n_2} \ldots s_{k+1}^{n_k} = 1, \\ \vdots \qquad\quad \vdots \qquad\quad \vdots, \end{cases}$$

ex quo ope formulae (IV) § 9 deducimus aequationem:

$$(n_1 + n_2 w^{-1} + \cdots + n_k w^{-k+1})(\sigma_1 + \sigma_2 w + \cdots + \sigma_d w^{d-1}) = 0$$

pro qualibet d^{ta} radice unitatis w. Cum autem factorem alterum pro nulla

*) Ea tantum condicione, ut expressio illa $\sigma(w)$ pro nullo valore ipsius w primitivo evanescat. v. § 18.

radice w primitiva evanescere supra (§ 18) demonstratum sit, factor prior pro his omnibus k valoribus ipsius w evanescere deberet; id quod (nisi $n_1 = n_2 = \cdots = 0$) fieri non posse ex § 7 colligitur.

§ 20.

Iam quid ex hac singularum classium disquisitione pro universis unitatibus colligi possit, inquiramus. Quodsi supponimus numerum λ illa virtute, initio § 19 memorata, gaudere, ea ipsa proprietate divisores quoque ipsius λ praeditos esse patet. Hoc igitur casu pro quolibet divisore „d" exstant quaedam unitates fundamentales coniunctae, quarum $\varphi(d)$ ad repraesentandas omnes huius classis unitates sufficiunt; quae designentur notis $u_{d,1}$, $u_{d,2}$, ..., earumque logarithmi sint $v_{d,1}$, $v_{d,2}$, ...

Sit „r" unitas aliqua, atque formetur ex ea unitas classis ad divisorem „d" pertinentis illa ipsa ratione, qua initio § 18 usi sumus. Sitque haec unitas „s", ita ut habeamus servata designatione illic adhibita:

$$r_1^{a_1} r_2^{a_2} \ldots r_{\lambda-1}^{a_\lambda - 1} = r_1^{a(a)} = s_1.$$

Sed esse debet

$$s_1 = u_{d,1}^{n_1} . u_{d,2}^{n_2} \ldots u_{d,k}^{n_k}$$

designantibus n_1, n_2... numeros quosdam integros. Itaque habemus aequationem:

$$\text{(I.)} \quad \sigma_1 + \sigma_2 w + \cdots + \sigma_d w^{d-1} = (n_1 + n_2 w^{-1} + \cdots + n_k w^{-(k-1)})(v_{d,1} + v_{d,2} w + \cdots + v_{d,d} w^{d-1})$$

ratione saepe usitata pro qualibet radice w aequationis $w^d = 1$. Deinde est:

$$\text{(II.)} \quad \sigma_1 + \sigma_2 \alpha \cdots + \sigma_\lambda \alpha^{\lambda-1} = a(\alpha^{-1})(\varrho_1 + \varrho_2 \alpha + \cdots + \varrho_\lambda \alpha^{\lambda-1})$$

pro quaque radice unitatis λ^{ta}. Substituta igitur pro α radice w obtinemus:

$$a(w^{-1})(\varrho_1 + \varrho_2 w + \cdots + \varrho_\lambda w^{\lambda-1}) = \sigma_1 + \sigma_2 w + \cdots + \sigma_\lambda w^{\lambda-1},$$

atque per aequationem (I) aliquanto mutatam:

$$\text{(III.)} \quad \begin{cases} a(w^{-1})(\varrho_1 + \varrho_2 w + \cdots + \varrho_\lambda w^{\lambda-1}) \\ = (n_1 + n_2 w^{-1} + \cdots + n_k w^{-(k-1)})(v_{d,1} + v_{d,2} w + \cdots + v_{d,\lambda} w^{\lambda-1}). \end{cases}$$

Quotiescunque igitur $n(w^{-1})$, numero $a(w^{-1})$ divisus, residuum habet $c(w^{-1})$, ita ut

$$n(w^{-1}) = m(w^{-1}) a(w^{-1}) + c(w^{-1})$$

sit (designante w radicem primitivam), habemus aequationem:

$$a(w^{-1})(\varrho_1 + \varrho_2 w + \cdots) = a(w^{-1}) m(w^{-1})(v_{d,1} + v_{d,2} w + \cdots) + c(w^{-1})(v_{d,1} + v_{d,2} w + \cdots),$$

atque si ponimus unitatem:

$$r_1 . u_{d,1}^{-m_1} . u_{d,2}^{-m_2} \dots u_{d,k}^{-m_k} = t_1$$

et $\log . t_1 = \tau_1$, erit:

$$a(\alpha^{-1})(\tau_1 + \tau_2 \alpha + \dots + \tau_\lambda \alpha^{\lambda-1}) = c(\alpha^{-1})(v_{d,1} + v_{d,2} \alpha + \dots + v_{d,\lambda} \alpha^{\lambda-1})$$

pro quoque ipsius α valore, qui radicem d^{tam} primitivam praebet. Pro omnibus reliquis ipsius α valoribus erit:

$$\tau_1 + \tau_2 \alpha + \dots + \tau_\lambda \alpha^{\lambda-1} = \varrho_1 + \varrho_2 \alpha + \dots + \varrho_\lambda \alpha^{\lambda-1},$$

cum pro his ipsius α valoribus sit $v_{d,1} + v_{d,2} \alpha + \dots = 0$.

Unde elucet, quamvis unitatem „r“ ope unitatum „u“ ad unitatem „t“ reduci posse talem, ut si unitas classis ad „d“ pertinentis ratione supra indicata ex ea formetur atque potestate ipsius „u“ complexa repraesentetur, exponens certo quodam residuorum systemate modulo $a(w)$ contineatur*). Hinc tanquam corollarium sequitur, ut si tales tantum unitates existant, quarum exponentes illi cuncti residua nihilo aequalia habeant, quascunque unitates integris ipsorum „u“ potestatibus exprimere liceat, itaque numerus unitatum fundamentalium sit:

$$\varphi(\lambda) + \dots + \varphi(d) + \dots = \lambda - 1$$

secundum notum illud theorema.

Statutis certis quibusdam residuorum systematis modulis $a(w)$, $a'(w')$, ... pro singulis ipsius λ divisoribus, sit unitas „r“ eiusmodi, ut exponentes, ad quos pertinent unitates classium ex illa „r“ formatae, pro singulis $a(w)$ residuis quibusdam ex istis systematis aequales sint; tum brevitatis causa seriem quandam residuorum ad unitatem „r“ pertinere dicemus. Iam primum ex illis supra dictis concludimus, cunctas unitates unitatibus „u“ et unitatibus „r“ repraesentari posse.

Deinde supponamus divisores ipsius λ certo aliquo ordine dispositos:

$$d_1, d_2, \dots d_i;$$

sint porro unitates „r“ tales, ut residua, quae ad eas respectu divisoris d_1 pertineant, non evanescant; sint unitates „s“ tales, ut residuis respectu d_1 evanescentibus residua, quae ad eas respectu divisoris d_2 pertineant, non evanescant etc. Inter has unitates r, s, t, ... omnes illas, quae supra ipso „r“ denotatae sunt, inveniri apertum est. Deinde adnotamus, pro divisore

*) Sic supra pro unitate „r“, ad quam exponens $k(w)$ pertinebat, ad unitatem „t“ reducta est, ad quam exponens $c(w)$, qui est residuum ipsius $n(w)$ modulo $a(w)$, pertinet.

ultimo tales unitates existere non posse. Tum enim residua respectu omnium divisorum, excepto ipso d_i, evanescere deberent ideoque, posito illam unitatem z eiusque logarithmum ζ esse, aequatio

$$\zeta_1 + \zeta_2 \alpha + \cdots + \zeta_\lambda \alpha^{\lambda-1} = 0$$

pro omnibus ipsius α valoribus exceptis radicibus d_i^{tis} primitivis locum habere deberet. Itaque unitas z in ipsa classe ad divisorem d_i pertinente inest (v. § 18) atque in aequatione:

$$a(w^{-1})(\zeta_1 + \zeta_2 w + \cdots + \zeta_\lambda w^{\lambda-1}) = (n_1 + n_2 w^{-1} + \cdots)(v_{d_i,1} + v_{d_i,2} w + \cdots),$$

ubi w est radix d_i^{ta} primitiva, numerus $n(w)$ ipso $a(w)$ dividi posse deberet, proptereaque residuum respectu divisoris d_i quoque evanesceret.

Iam unitates „r“ inter se reducendae sunt. Primum, si quae existant, ad quas idem residuum respectu ipsius d_1 pertineat, e. g. r et r', pro his accipi possunt unitates r et $\frac{r}{r'}$, quarum alteram ad genus unitatum „s“ (vel inter ipsas t, ...) referendam esse patet, quippe quae eius residuum respectu d_1 evanescat. Unde concludimus, quaecunque unitates r eodem residuo respectu d_1 gaudeant, ex eis unam tantum eligendam esse, cum ceterae ope huius et unitatum s, t, ... repraesentari possint. — Deinde sit $n(w)$ residuum alicuius „r“ respectu d_1 (ubi w radix primitiva d_1^{ta}), sitque $\varphi(w)$ factor communis maximus numerorum $n(w)$ et illius $a(w)$, ita ut sit

$$n(w) = \varphi(w) . m(w),$$

numerum invenire licet $\psi(w)$ talem, ut sit

$$m(w)\psi(w) \equiv 1 \pmod{a(w)} \text{ *)},$$

ergo

$$n(w)\psi(w) \equiv \varphi(w) \pmod{a(w)}.$$

Itaque cum unitas $r_1^{\psi(\alpha)}$ quoque integra sit, unitas existit, cuius residuum respectu d_1 ipse numerus $\varphi(w)$ est. Quae si litera r' designatur, erit $r'^{m(\alpha)}$ unitas, cuius residuum respectu d_1 numerus $n(w)$, quae igitur secundum supra dicta pro illa unitate r accipi potest. Hinc sequitur, ut loco omnium earum unitatum, quarum residua eundem factorem communem maximum $\varphi(w)$ cum numero $a(w)$ habeant, unam tantum, cuius residuum ipse hic numerus $\varphi(w)$ sit, accipere liceat.

---

*) Cf. § 4 et § 7.

Sint unitatum r et r' residua respectu d_1 numeri $\varphi(w)$ et $\psi(w)$, qui uterque numerum illum $a(w)$ metiens supponi potest. Tum erit factor communis maximus numerorum

$$m(w)\varphi(w)+n(w)\psi(w), \quad a(w)$$

ipse factor communis numerorum $\varphi(w)$ et $\psi(w)$. Positis enim $m(w)$, $n(w)$ numeros esse tales, ut sit

$$m(w)\varphi(w)+n(w)\psi(w) \equiv \chi(w) \pmod{a(w)},$$

ubi $\chi(w)$ factor est communis maximus ipsorum $\varphi(w)$ et $\psi(w)$, illa sententia elucet. Cumque etiam $r^{m(w)}.r'^{n(w)}$ unitas sit integra eaque talis, ut residuum respectu d_1 sit $\chi(w)$, hanc ipsam unitatem, ex qua ope unitatum s, t, ... unitates illae (r, r') derivari possunt, loco duarum unitatum r, r' accipere licet. Quaecunque igitur unitates variorum respectu d_1 residuorum existunt, semper una talis pro iis accipi potest, cuius residuum respectu d_1 factor omnium residuorum communis maximus sit. Et, si respicimus supra dicta, pro hac ipsa talis statui potest unitas, ut residuum respectu d_1 sit factor ipsius $a(w)$.

Quae cum de unitatibus r exposuerimus, ad unitates s, t, ... adhibere liceat, concludimus, praeter unitates „u“ ad repraesentandas omnes unitates his tantum opus esse: unitate quadam „r“ (cum eius coniunctis), cuius residuum respectu d_1 est factor ipsius $a(w)$; unitate quadam „s“, cuius residuum respectu d_2 est factor ipsius $b(w')$ etc. Itaque hanc obtinemus seriem unitatum fundamentalium:

$$\begin{array}{cccccc} u_{d_1}, & u_{d_2}, & u_{d_3}, & \ldots & u_{d_{i-1}}, & u_{d_i}, \\ r, & s, & t, & \ldots & z. & \end{array}$$

Iam si residuum, quod ad unitatem r respectu d_1 pertinet, $\varphi(w)$ ponitur, ita ut sit $a(w) = \varphi(w).\psi(w)$, habemus aequationem:

$$a(w^{-1})(\varrho_1+\varrho_2 w+\cdots) = \varphi(w^{-1})(v_{d_1,1}+v_{d_1,2}w+\cdots)$$

vel

$$\psi(w^{-1})(\varrho_1+\varrho_2 w+\cdots) = v_{d_1,1}+v_{d_1,2}w+\cdots,$$

pro qualibet radice d_1^{ta} primitiva w. Unde patet unitatem $r^{\psi(\alpha)}.u_{d_1,1}^{-1}$ esse talem, ut eius residuum respectu d_1 sit nihilo aequale, eamque igitur unitatibus u_{d_2}, u_{d_3}, ... et s, t, ... repraesentari posse. Ergo ipsae unitates coniunctae u_{d_1} unitatibus „r“ et reliquis utriusque seriei unitatibus expri-

muntur. Inter has vero unitates „r“ eae, quarum index numero $\varphi(d_1)$ maior est, ad priores reducuntur. Sit enim (posito $\varphi(d_1) = k$)

$$x^k + c_{k-1}x^{k-1} + \cdots + c_1 x + c = 0$$

illa aequatio, quarum radices sunt radices unitatis d_1^{tae} primitivae, in qua coefficientem ipsius x^k unitatem esse e forma illius aequationis in § 7 exhibita manifestum est, et fingamus unitatem integram:

$$r_1^c . r_2^{c_1} \ldots r_{k-1}^{c_{k-2}} . r_k^{c_{k-1}} . r_{k+1} = x_1,$$

ideoque posito $\log x_i = \xi_i$:

$$(c + c_1\alpha + \cdots + c_{k-1}\alpha^{k-1} + \alpha^k)(\varrho_1 + \varrho_2\alpha + \cdots) = \xi_1 + \xi_2\alpha + \cdots.$$

Cum vero $c(\alpha)$, eaque de re $\xi(\alpha)$, pro illo ipsius α valore $\alpha = w$ evanescat, unitas x_1 unitatibus $u_{d_2} \ldots$ atque unitatibus s, t, ... repraesentari potest. Ergo r_{k+1} unitatibus r_1, r_2, ... r_k et unitatibus utriusque illius seriei reliquis exprimi potest; pariterque r_{k+2} unitatibus r_2, r_3, ... r_{k+1} ideoque unitatibus r_1, r_2, ... r_k et reliquis etc. etc. Itaque pro illis unitatibus „u_{d_1}“ et „r“ tantum accipiendae sunt unitates:

$$r_1, \quad r_2, \quad \ldots \quad r_{\varphi(d_1)}.$$

Simili modo pro unitatibus u_{d_2} et s tantum accipiendae sunt unitates

$$s_1, \quad s_2, \quad \ldots \quad s_{\varphi(d_2)},$$

quia sicuti supra et unitates ceterae cum s_1 coniunctae et unitates „u_{d_2}“ per unitates s_1, s_2, ... $s_{\varphi(d_2)}$ adiunctis illis u_{d_2}, ... t, ... z, exprimi possunt. Denique pro unitatibus $u_{d_{i-1}}$ et z accipiendae sunt unitates

$$z_1, \quad z_2, \quad \ldots \quad z_{\varphi(d_{i-1})},$$

quia his ipsis ope unitatum u_{d_i} illae repraesentari possunt. Habemus igitur tanquam unitates fundamentales, ad repraesentandas omnes unitates sufficientes, has:

$$\begin{array}{llll} r_1, & r_2, & \ldots & r_{\varphi(d_1)}, \\ s_1, & s_2, & \ldots & s_{\varphi(d_2)}, \\ \vdots & \vdots & & \vdots \\ z_1, & z_2, & \ldots & z_{\varphi(d_{i-1})}, \\ u_{d_i,1}, & u_{d_i,2}, & \ldots & u_{d_i,\varphi(d_i)}, \end{array}$$

quia ceteras cum ipsis u_{d_i} coniunctas unitates „u“ illis exprimi posse iam supra adnotavimus. Numerus igitur unitatum fundamentalium erit:

$$\varphi(d_1)+\varphi(d_2)+\cdots+\varphi(d_i) = \lambda-1,$$

eumque numerum ipso $\lambda-1$ minorem esse non posse in § 12 demonstravimus.

Numerus igitur unitatum fundamentalium hic idem est, qui erat casu quo λ numerus primus, sed cum casu generali, tanquam unitates fundamentales semper unitates accipi posse *coniunctas*, non probaverimus, num re vera unitates fundamentales *coniunctae* pro quovis λ existant, in dubio remanet. Haec autem quaestio quanti sit momenti ex eo elucet, quod problema illud Diophanteum (v. § 11) inveniendorum numerorum x, x_1, ... $x_{\lambda-1}$ aequationi

$$\mathrm{Nm}(x\varepsilon+x_1\varepsilon_1+\cdots+x_{\lambda-1}\varepsilon_{\lambda-1}) = \pm 1$$

satisfacientium systematis unitatum fundamentalium *coniunctarum* perfecte solvitur. Nam si omnes unitates forma $u_1^{n(\alpha)}$ sive

$$(\xi\varepsilon+\xi_1\varepsilon_1+\cdots+\xi_{\lambda-1}\varepsilon_{\lambda-1})^{n(\alpha)}$$

continentur, cuncta ipsorum x systemata *functionibus rationalibus integris* illius unius systematis (ξ) repraesentari possunt. Sin vero duorum systematum unitatum coniunctarum opus est, omnia systemata ipsorum x nonnisi duobus systematis (ξ), (ξ') modo rationali exprimi possunt. Quoniam autem in § 17 demonstratum est, acceptis quibuslibet unitatibus coniunctis r_1, r_2, ... $r_{\lambda-1}$ semper inveniri posse alterum systema s_1, s_2, ... $s_{\lambda-1}$ tale, ut omnes unitates integris istarum unitatum r et s potestatibus exprimi liceat, sequitur, ut accepto quolibet systemate x^0, x_1^0, ... $x_{\lambda-1}^0$ alterum systema x', x_1', ... $x_{\lambda-1}'$ inveniri possit tale, ut omnia systemata ipsorum x tanquam functiones rationales integrae illarum 2λ quantitatum x^0, x' repraesentari possint. Sed cum e disquisitionibus illis generalibus Cli. *Lejeune-Dirichlet*, quas supra pagina huius dissertationis secunda commemoravimus, tantummodo concludi possit, $\lambda-1$ quantitatum x systemata sive $\lambda(\lambda-1)$ quantitates x ad repraesentanda cuncta ipsorum x systemata sufficere, casu quem in hac dissertatione tractavimus speciali problema Diophanteum, quaestione unitatum complexarum exhibitum, peculiarem ac simpliciorem solutionem admittere bene animadvertendum est.