
桑木文庫
洋書

LEOPOLD KRONECKER'S WERKE.

L. Kronecker

Verlag v. B. G. Teubner in Leipzig. Messenbach Riffarth & Co. Berlin grav.

LEOPOLD KRONECKER'S WERKE.

HERAUSGEGEBEN AUF VERANLASSUNG DER KÖNIGLICH PREUSSISCHEN AKADEMIE DER WISSENSCHAFTEN

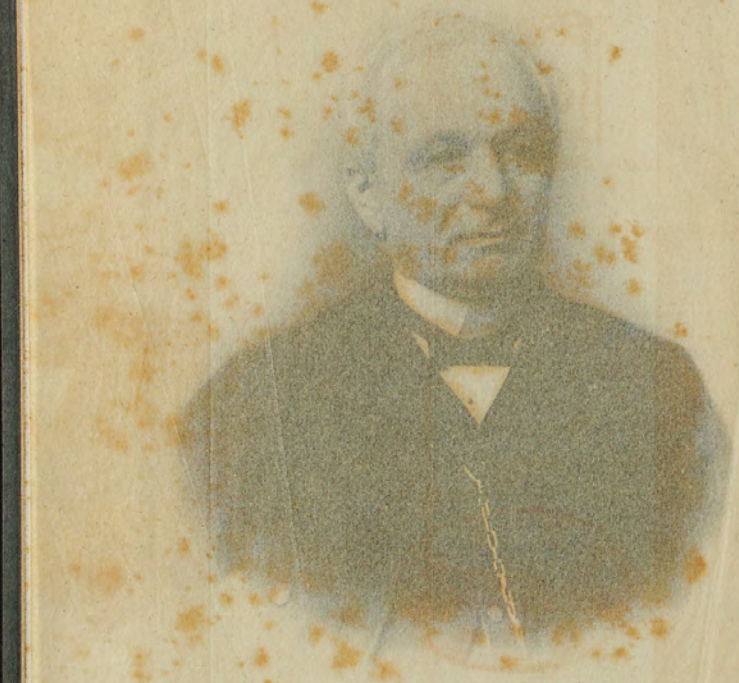
VON

K. HENSEL.

ERSTER BAND.

MIT L. KRONECKER'S BILDNISS.

LEIPZIG,
DRUCK UND VERLAG VON B. G. TEUBNER.
1895.



LEOPOLD KRONECKER'S WERKE.

HERAUSGEGEBEN AUF VERANLASSUNG
DER
KÖNIGLICH PREUSSISCHEN AKADEMIE DER WISSENSCHAFTEN
VON

K. HENSEL.

ERSTER BAND.

MIT L. KRONECKER'S BILDNISS.

LEIPZIG,
DRUCK UND VERLAG VON B. G. TEUBNER.
1895.

VORREDE.

Bald nach dem Tode Leopold Kronecker's beschloss die Akademie der Wissenschaften zu Berlin, seine Abhandlungen in derselben Weise sammeln und herausgeben zu lassen, wie früher die Werke von Jacobi, Dirichlet, Steiner und Borchardt, und auf ihre Veranlassung habe ich diese Aufgabe übernommen.

Die Gesammtausgabe der Werke Kronecker's, deren ersten Band ich hiermit der Oeffentlichkeit übergebe, wird alle von ihm selbst veröffentlichten wissenschaftlichen Arbeiten, sowie eine Reihe von Abhandlungen enthalten, welche sich ganz oder theilweise ausgearbeitet in dem Nachlasse vorgefunden haben. Hieran soll sich eine Darstellung der weiteren Ergebnisse anschliessen, welche eine genaue Durchforschung des reichen, mit grosser Sorgfalt aufbewahrten wissenschaftlichen Nachlasses geliefert hat.

Bei der grossen Anzahl und dem verschiedenartigen Inhalt der Abhandlungen wäre bei rein chronologischer Aufeinanderfolge derselben ihr innerer Zusammenhang nicht genügend hervorgetreten. Daher habe ich sie nach ihrem Inhalte in drei grosse Abtheilungen geordnet, welche vollständig und naturgemäss gegen einander abgegrenzt werden konnten.

Für diese Eintheilung sind die folgenden Gesichtspunkte massgebend gewesen: Einen grossen Theil seiner Lebensarbeit hat Kronecker der Begründung und dem Ausbau der Disciplin gewidmet, welcher er selbst in

seinen späteren Jahren den Namen der „allgemeinen Arithmetik“ beigelegt hat. Er versteht darunter die Anwendung der Begriffe und Methoden der Zahlentheorie auf die Untersuchung der rationalen Functionen beliebig vieler Variabeln. Dieses sehr ausgedehnte Untersuchungsgebiet umfasst also zunächst die Betrachtung der Systeme ganzer Zahlen, also die gesammte reine Zahlentheorie, ferner die Untersuchung der linearen Systeme, also die Lehre von den Determinanten, den bilinearen und den quadratischen Formen, und endlich die allgemeine Theorie der Systeme algebraischer Zahlen und Functionen von einer und von mehreren Veränderlichen, deren Grundzüge Kronecker in seiner „Festschrift zu Kummer's Doctorjubiläum“ in grosser Allgemeinheit entwickelt und seitdem in einer Reihe von Abhandlungen weiter ausgestaltet hat.

Alle Arbeiten über Fragen der allgemeinen Arithmetik werden nun in den ersten Bänden dieser Ausgabe vereinigt werden.

Die hieran sich anschliessende zweite Abtheilung zerfällt in zwei getrennte Abschnitte, deren Inhalt zwar mit den Aufgaben der allgemeinen Arithmetik in sehr nahem Zusammenhange steht, aber doch nur in einem übertragenen Sinne zu ihr gerechnet werden könnte. Der erste Abschnitt umfasst alle die algebraischen Untersuchungen, welche sich auf die Auflösung der Gleichungen und die hieran sich anschliessenden Fragen beziehen, insbesondere auf die Eintheilung der Gleichungen in Classen nach ihrem „Affecte“; bei ihnen tritt zu den oben erwähnten rein arithmetischen Begriffen noch der der Wurzel einer algebraischen Gleichung hinzu. Der zweite Abschnitt enthält alle Arbeiten über die Anwendung der Analysis auf Probleme der Zahlentheorie; hier ist es der wichtige Begriff der Grenze oder des Limes, durch dessen Hinzutreten diese von Lejeune-Dirichlet in die Wissenschaft eingeführten Untersuchungsmethoden scharf von denen der allgemeinen Arithmetik geschieden werden.

Den Inhalt der letzten Abtheilung bilden die analytischen Arbeiten Kronecker's, ferner die Untersuchungen über Potentialtheorie und über Gegenstände der mathematischen Physik, sowie einige kleinere Abhandlungen vermischten Inhalts.

Innerhalb dieser grossen Abschnitte folgen die Abhandlungen im Wesentlichen in chronologischer Ordnung auf einander; die nachgelassenen Arbeiten werden am Ende derjenigen Abtheilungen ihre Stelle finden, zu denen sie ihrem Inhalte nach gehören; ein vollständiges Verzeichniss aller Abhandlungen Kronecker's am Ende des letzten Bandes, welches nach der Zeit ihrer Veröffentlichung geordnet ist, soll die Uebersicht erleichtern.

In dem vorliegenden Bande sind die 22 ersten Abhandlungen über allgemeine Arithmetik vereinigt, deren Abfassung in die Zeit von 1845—1874 fällt. Er beginnt mit dem Irreductibilitätsbeweise der Kreistheilungsgleichungen vom Primzahlgrade, welchen Kronecker noch als Student gefunden hat, und mit seiner Doctordissertation, und schliesst ab mit den Untersuchungen über bilineare und quadratische Formen, welche Kronecker erst in seinen letzten Lebensjahren in weiterem Umfange wieder aufgenommen hat.

Ich habe es als meine Aufgabe angesehen, jede Abhandlung dieses Bandes vor ihrem Abdrucke selbst einer sorgfältigen Revision zu unterwerfen, und ich habe sie so von einer grösseren Anzahl von Druck- und Schreibfehlern, sowie von solchen Unrichtigkeiten gereinigt, welche offenbar bloss durch ein Versehen entstanden waren. Dagegen habe ich an einigen wenigen Stellen die Hinzufügung einer Bemerkung für nöthig gehalten; ich werde solche Zusätze bei dieser ganzen Ausgabe in einem Anhange vereinigen, welcher jedesmal an das Ende der betreffenden Abtheilung gestellt werden wird; dieselben konnten nicht jedem einzelnen Bande angefügt werden, da sie viele Verweisungen auf spätere Arbeiten der nämlichen Abtheilung enthalten.

Die zum Theil schwere Aufgabe der genauen Nachprüfung aller Abhandlungen dieses Bandes ist mir durch die gütige Hülfe der Herren G. Landsberg und K. Th. Vahlen erleichtert worden; die von diesen Herren beigefügten Bemerkungen sind im Anhange als von ihnen herrührend gekennzeichnet worden; es ist mir aber ein Bedürfniss ihnen an dieser Stelle meinen verbindlichsten Dank auszusprechen. Ferner hat Herr Ch. Hermite das Andenken seines dahingegangenen Freundes dadurch in der schönsten und pietätvollsten Weise geehrt, dass er die in französischer Sprache geschriebenen Abhandlungen Kronecker's vor der Drucklegung ebenso durchgesehen hat, wie er diess früher bei den von Kronecker herausgegebenen Arbeiten Lejeune-Dirichlet's gethan hatte.

Endlich möchte ich mit Dank aussprechen, dass die Verlagsbuchhandlung von B. G. Teubner keine Mühe und keine Opfer gescheut hat, um dieses Werk auch äusserlich zu einem würdigen Denkmal für den Verewigten zu machen.

Berlin, den 20. Mai 1895.

K. Hensel.

INHALTSVERZEICHNISS.

BEWEIS
DASS FÜR JEDE PRIMZAHL p DIE GLEICHUNG
$1+x+x^2+\cdots+x^{p-1}=0$ IRREDUCTIBEL IST.

VON

HERRN L. KRONECKER,
STUD. PHIL. ZU BERLIN.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 29. p. 280.

BEWEIS, DASS FÜR JEDE PRIMZAHL p DIE GLEICHUNG $1 + x + x^2 + \cdots + x^{p-1} = 0$ IRREDUCTIBEL IST.

Bei der Wichtigkeit des Gegenstandes dürfte es nicht ohne Interesse sein, dem von *Gauss* in den Disq. arithm. gegebenen Beweise einen zweiten sehr einfachen hinzuzufügen. Ich schicke dabei, um den Gang nachher nicht zu stören, folgenden Satz voraus:

„Wenn p eine Primzahl, α eine von 1 verschiedene $p$te Wurzel der Einheit und $a, a_1, \ldots a_{p-1}$ ganze Zahlen bedeuten, und man

$$a + a_1\alpha + a_2\alpha^2 + \cdots + a_{p-1}\alpha^{p-1} = f(\alpha)$$

setzt, so findet die Congruenz

$$f(\alpha)\, f(\alpha^2) \cdots f(\alpha^{p-1}) \equiv f(1)^{p-1} \pmod{p}$$

statt, wobei sogleich bemerkt werden kann, dafs jenes Product als ganze symmetrische Function aller Wurzeln eine ganze reelle Zahl sein mufs."

Beweis. Man setze

$$a + a_1 x + a_2 x^2 + \cdots + a_{p-1} x^{p-1} = f(x)$$

und denke sich die Entwickelung des Products $f(x)\, f(x^2) \ldots f(x^{p-1})$ nach Potenzen von x, so dafs das allgemeine Glied darin $A_n x^n$ wird. Setzt man nun in der so entstandenen identischen Gleichung für x nach einander die Werthe $1, \alpha, \alpha^2, \ldots \alpha^{p-1}$ und summirt alle diese p Gleichungen, so erhält man auf der einen Seite:

$$f(1)^{p-1} + (p-1)\, f(\alpha)\, f(\alpha^2) \cdots f(\alpha^{p-1}).$$

Denn für jedes r aus der Reihe der Zahlen $1, 2, \ldots (p-1)$ fallen die Gröfsen

$\alpha^r, \alpha^{2r}, \ldots \alpha^{(p-1)r}$ mit den ursprünglichen $\alpha, \alpha^2, \ldots \alpha^{p-1}$ nur in anderer Ordnung zusammen, woraus folgt, dafs

$$f(\alpha^r) f(\alpha^{2r}) \cdots f(\alpha^{(p-1)r}) = f(\alpha) f(\alpha^2) \cdots f(\alpha^{p-1})$$

ist. Auf der andern Seite erhält man für das allgemeine Glied

$$A_n (1 + \alpha^n + \alpha^{2n} + \cdots + \alpha^{(p-1)n}),$$

welche Summe für jedes durch p theilbare n den Werth p erhält, für jedes andere n aber verschwindet. Man hat also die Gleichung

$$f(1)^{p-1} + (p-1) f(\alpha) f(\alpha^2) \cdots f(\alpha^{p-1}) = p(A_0 + A_p + A_{2p} + \cdots),$$

oder

$$f(\alpha) f(\alpha^2) \cdots f(\alpha^{p-1}) \equiv f(1)^{p-1} \pmod{p},$$

was zu beweisen war.

Es sei nun $1 + x + x^2 + \cdots + x^{p-1} = X$ das Product zweier ganzen rationalen Functionen von x mit ganzen Coëfficienten, also $X = f(x) \cdot \varphi(x)$, so wird aus dieser Gleichung für $x = 1$ offenbar $p = f(1) \cdot \varphi(1)$, wo $f(1)$ und $\varphi(1)$ ganze Zahlen sind, was also nur möglich ist, wenn die eine gleich 1, die andere gleich p ist. Es sei $f(1) = 1$. Nun mufs aber andererseits $f(x)$ für so viele von 1 verschiedene $p$te Wurzeln der Einheit, als der Grad dieser Function andeutet, also doch wenigstens für eine verschwinden. Es wird daher jedenfalls

$$f(\alpha) f(\alpha^2) \cdots f(\alpha^{p-1}) = 0.$$

Andererseits hat man nach obigem Satze

$$f(\alpha) f(\alpha^2) \cdots f(\alpha^{p-1}) \equiv f(1)^{p-1} \equiv 1 \pmod{p},$$

welches den Widerspruch giebt.

Anmerkung: Ich will noch bemerken, dafs ich in Bezug auf den obigen Hülfssatz nicht auf *Kummer's* „Disputatio de numeris complexis etc. § 2." verwiesen habe, weil bei dem Beweise desselben dort schon die Irreductibilität der Gleichung $X = 0$ vorausgesetzt wird.

DE

UNITATIBUS COMPLEXIS.

DISSERTATIO INAUGURALIS ARITHMETICA

QUAM

CONSENSU ET AUCTORITATE

AMPLISSIMI PHILOSOPHORUM ORDINIS

IN

ALMA LITERARUM UNIVERSITATE FRIDERICA GUILELMA

PRO

SUMMIS IN PHILOSOPHIA HONORIBUS

RITE CAPESSENDIS

DIE X M. SEPTEMBRIS A. MDCCCXLV

H. L. Q. S.

PUBLICE DEFENDET

LEOPOLDUS KRONECKER

LIGNICIENSIS.

ADVERSARII ERUNT:

G. EISENSTEIN PHIL. DR.
E. CAUER PHIL. CAND.
H. RUEHLE MED. CAND.

BEROLINI

MDCCCXLV.

PRAECEPTORI DILECTISSIMO

ERNESTO EDUARDO KUMMER

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

HANC DISSERTATIONEM

PIO GRATOQUE ANIMO

D. D. D.

AUCTOR

DE UNITATIBUS COMPLEXIS.

Dissertatio inauguralis arithmetica *).

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“ [2]), et

*) 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 [1]).

**) *Crelles* Journal Bd. 24 [S. 291—371. *Lejeune-Dirichlets* Werke Bd. I S. 533—618.]

***) Monatsberichte der Berliner Akademie, 1837 [S. 127—139. *C. G. J. Jacobis* Werke Bd. VI S. 254—274]; v. etiam commentationem Illi. *Eisenstein*. „Beiträge zur Kreistheilung“ (*Crelles* Journal Bd. 27 [S. 269—278]).

†) *Crelles* Journal Bd. 19 S. 314—318.

[1]) Zusatz L. Kroneckers zu dem vollständigen Abdruck dieser Arbeit im Journal für Mathematik Bd. 93 S. 1—52. H.

[2]) *E. E. Kummer:* Disputatio de numeris complexis, qui unitatis radicibus et numeris integris realibus constant. Gratulationsschrift der Breslauer Universität zum dreihundertjährigen Jubiläum der Universität Königsberg. Breslau 1844. H.

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, 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[1]). 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: $\alpha, \beta, \gamma \ldots$ atque eiusdem aequationis, si tanquam congruentiam modulo p (ubi p numerus primus) consideres, n

*) *Crelles* Journal Bd. 28 [S. 289—374].

[1]) Zur Theorie der complexen Einheiten. Berl. Akad. Ber. v. J. 1846. S. 103—107. *Lejeune-Dirichlets* Werke Bd. I S. 639—644. H.

radices: $a, b, c \ldots$; 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 $\varepsilon, \varepsilon_1, \ldots \varepsilon_{\lambda-1}$ periodi radicum ω, quarum quaeque μ terminos contineat, ita ut habeamus $\lambda\mu = \nu - 1$ et:

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

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

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

Iam posito

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

ubi literis: $a, a_1, \ldots a_{\lambda-1}$ 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:

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

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

sequitur, ut sint

$$a = b, \quad a_1 = b_1, \quad \ldots \quad a_{\lambda-1} = b_{\lambda-1}.$$

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

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

Quod aequationum systema ut secundum quantitates a, $a_1, \ldots$ 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:

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

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:

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

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

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

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

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

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

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

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

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

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

seu

$$b_r = c_r + m,$$

ubi m respectu r constans est.

Ut quantitas m definiatur, adnotamus istis aequationibus (V) additis fieri:

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

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:

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

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

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

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

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 $\varepsilon, \varepsilon_1, \ldots \varepsilon_{\lambda-1}$ 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:

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

et quidem respectu ε. Quodsi enim $f(\varepsilon)$ tanquam functio alius periodi exempli gratia ipsius ω consideratur, ita ut sit: $f(\varepsilon) = \varphi(\omega)$, apparet esse $\mathrm{Nm}\, \varphi(\omega) = \varphi(\omega)\varphi(\omega_1)\cdots\varphi(\omega_{\mu-2})$ sive

$$\mathrm{Nm}\, \varphi(\omega) = \big(\mathrm{Nm}\, f(\varepsilon)\big)^{\kappa}.$$

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

$$\mathrm{Nm}\, f(\varepsilon) = \mathrm{Nm}\, f(\varepsilon_r)$$

et

$$\mathrm{Nm}\, \big(f(\varepsilon)\cdot\varphi(\varepsilon)\big) = \mathrm{Nm}\, f(\varepsilon)\cdot \mathrm{Nm}\, \varphi(\varepsilon).$$

Cum sit

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

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:

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

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:

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

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

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

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

$$f(\varepsilon)\, f(\varepsilon_1)\cdots f(\varepsilon_{\lambda-1}) \equiv f(e)\, f(e_1)\cdots f(e_{\lambda-1}) \pmod{p}$$

sive

$$\mathrm{Nm}\, f(\varepsilon) \equiv f(e)\, f(e_1)\cdots f(e_{\lambda-1}) \pmod{p},$$

unde theoremata illa sponte manant.

2. *Theorema.* Sint $p(\varepsilon), p(\varepsilon_1), \ldots$ 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

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

unde

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

tum erit $\varphi(e) = 0$ et

*) In commentatione „de divisoribus formarum quarundam etc.“ quae proximo tempore edetur[1]); vel etiam in commentatione Cli. *Schoenemann* (Diar. *Crell.* tom. 19 pag. 306).

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

[1]) Ueber die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung entstehen. *Crelles* Journal Bd. 30, S. 107—116. H.

$$\varphi(\varepsilon_1) \equiv \varphi(\varepsilon_2) \equiv \cdots \equiv \varphi(\varepsilon_{\lambda-1}) \equiv 0 \pmod{p},$$

quia omnes hi numeri factorem $p(e)$ implicant, quem nihilo congruum supposuimus. Iam erit secundum illud lemma:

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

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:

$$\varphi(\varepsilon)^2 \equiv 0 \pmod{p}.$$

Iam si p ad ν primum supponitur, erit $p^{\nu-1} \equiv 1 \pmod{\nu}$ atque (cf. § 3, 1)

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

Erit autem

$$\varphi(\varepsilon)^{p^{\nu-1}} = \varphi(\varepsilon)^{p^{\nu-1}-2} \cdot \varphi(\varepsilon)^2 \equiv 0 \pmod{p},$$

unde denique $\varphi(\varepsilon) \equiv 0 \pmod{p}$, i. e.:

$$(e-\varepsilon)\, p(\varepsilon_1)\, p(\varepsilon_2) \cdots p(\varepsilon_{\lambda-1}) \equiv 0 \pmod{p(\varepsilon)\, p(\varepsilon_1) \cdots p(\varepsilon_{\lambda-1})},$$

ergo:

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

Casu $p = \nu$ habemus $\operatorname{Nm} p(\varepsilon) = \nu$, et posito $p(\varepsilon) = f(\omega)$ erit $\operatorname{Nm} f(\omega) = \big(\operatorname{Nm} p(\varepsilon)\big)^\mu$, ergo $\operatorname{Nm} f(\omega) \equiv 0 \pmod{\nu^\mu}$. Eaque de re

$$f(1) \equiv 0 \pmod{\nu}$$

(disputatio Cli. *Kummer* § 2); ergo cum sit $(1-\omega)\,(1-\omega^2)\cdots = \nu$, erit quoque $f(1) \equiv 0 \pmod{(1-\omega)}$. Deinde propter congruentiam $1 \equiv \omega \pmod{(1-\omega)}$ habemus $f(\omega) \equiv 0 \pmod{(1-\omega)}$. Iam posito

$$f(\omega) = (1-\omega)\, f'(\omega)$$

erit

$$\operatorname{Nm} f'(\omega) \equiv 0 \pmod{\nu^{\mu-1}},$$

ergo sicut supra

$$f'(\omega) = (1-\omega)\, f''(\omega).$$

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

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

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

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

Deinde cum simili modo e congruentia $\operatorname{Nm}(e-\varepsilon) \equiv 0 \pmod{\nu}$ colligatur

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

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

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

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

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

$$p'(e) \equiv 0 \pmod{p} \quad \text{ideoque etiam} \quad \pmod{p(\varepsilon)}.$$

Est vero $e \equiv \varepsilon \pmod{p(\varepsilon)}$, unde $p'(\varepsilon) \equiv 0 \pmod{p(\varepsilon)}$ i. e.

$$p'(\varepsilon) = p(\varepsilon) \cdot \varphi(\varepsilon),$$

ubi $\varphi(\varepsilon)$ unitas complexa est, quia

$$\operatorname{Nm} p'(\varepsilon) = p = \operatorname{Nm} p(\varepsilon) \cdot \operatorname{Nm} \varphi(\varepsilon) = p \cdot \operatorname{Nm} \varphi(\varepsilon),$$

ergo $\operatorname{Nm} \varphi(\varepsilon) = 1$.

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:

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

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

*) Quod theorema casus tantum specialis theorematis 2 in § 3 est.
**) v. adnotationem secundam ad § 2.

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

etiamque

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

id est

$$\frac{\mathrm{Nm}\, p(\varepsilon)}{p(\varepsilon)} = \frac{p}{p(\varepsilon)} \equiv 0 \pmod{p}, \quad \text{sive} \quad \frac{p}{p(\varepsilon)} = p\cdot f(\varepsilon),$$

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

§ 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 $\mu\cdot\lambda = \nu - 1$ cumque p ad numerum μ pertineat, ponatur $p \equiv g^\lambda \pmod{\nu}$. Iam erit secundum rationem saepe usitatam:

$$f(\omega) \equiv f(\omega),\ f(\omega)^p \equiv f(\omega^p),\ f(\omega)^{p^2} \equiv f(\omega^{p^2}),\ \ldots\ f(\omega)^{p^{\mu-1}} \equiv f(\omega^{p^{\mu-1}}) \pmod{p}.$$

Quibus congruentiis inter se multiplicatis obtinemus:

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

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

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

sive posito:

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

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

*) v. § 3, 1.

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

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

Est vero $\varphi(\omega)^{p^\mu} \equiv \varphi(\omega^{p^\mu}) \equiv \varphi(\omega) \pmod{p}$, ergo

$$\varphi(\omega) \equiv 0 \pmod{p},$$

unde mutatis radicibus ω oriuntur relationes:

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

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

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

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

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

Tum habemus secundum suppositionem nostram:

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

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

$$f(\omega)\cdot f(\omega^{g^\lambda})\cdots f(\omega^{g^{(\mu-1)\lambda}}) \equiv 0 \left(\mathrm{mod.}\, p(\varepsilon_{-r})\right),$$

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

$$f(\omega)\cdot f(\omega^p)\cdots f(\omega^{p^{\mu-1}}) \equiv 0 \left(\mathrm{mod.}\, p(\varepsilon_{-r})\right).$$

Est vero:

*) *Gauss* disquisitiones arithmeticae. art. 347.

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

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

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

Ad normam transeuntes obtinemus aequationem:

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

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

$$f(\omega)\equiv 0 \quad \left(\text{mod. } p(\varepsilon_k)^m\cdot p(\varepsilon_{k'})^{m'}\cdots\right),$$

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 $\text{Nm } f(\omega)\equiv 0 \pmod{\nu}$, habemus $f(\omega)\equiv 0 \left(\text{mod.}(1-\omega)\right)$***), pariterque e congruentia $\text{Nm } f(\omega)\equiv 0 \pmod{\nu^m}$ congruentiam colligimus

$$f(\omega)\equiv 0 \quad \left(\text{mod. } (1-\omega)^m\right).$$

§ 4.

Sit $f(\omega)$ numerus aliquis complexus, N numerus realis eiusmodi, ut factores eius primi reales in factores complexos quam plurimos discerpi possint,

*) v. § 3, 1.

**) 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.

sitque factor numerorum $f(\omega)$ et N communis maximus $\varphi(\omega)$*), numerus $\psi(\omega)$ inveniri potest talis, ut sit:

$$\psi(\omega)\cdot f(\omega)\equiv \varphi(\omega) \quad \pmod{N}\ **).$$

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

Iam erit secundum § 3, 2:

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

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

$$x\cdot \text{Nm } F(\omega)\equiv 1 \quad \pmod{p^{\pi}}.$$

Hinc habemus:

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

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

$$P(\varepsilon)\cdot p(\varepsilon_a)^{\alpha}\cdot p(\varepsilon_{a'})^{\alpha'}\cdots = P(\varepsilon)\cdot A(\varepsilon) = p(\varepsilon_k)^m\cdot p(\varepsilon_{k'})^{m'}\cdots,$$

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

Iam nullum indicem a nulli indici b aequalem esse patet. Sint $c, c', \ldots$ indices ii, qui coniuncti cum indicibus a et b seriem $0, 1, 2, \ldots \lambda-1$ efficiunt, atque posito

$$C(\varepsilon) = p(\varepsilon_c)\cdot p(\varepsilon_{c'})\cdots$$

formetur expressio:

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

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

$$A(e) + B(e)\cdot C(e)\equiv 0 \quad \pmod{p}.$$

*) 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 ultiplicando per fact ores coniunctos realis reddi potest.

***) v. § 2, 1.

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 $A(e)+B(e)\cdot C(e)$, nihilo congruum erit. Quare iam existet numerus y talis, ut sit:

$$y\cdot \mathrm{Nm}\, V(\varepsilon) \equiv 1 \pmod{p^\pi},$$

sive substituto ipsius $V(\varepsilon)$ valore:

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

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

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

Unde si illam congruentiam (I):

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

respicimus atque

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

ponimus, denique prodit congruentia:

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

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

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

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

$$x\cdot \mathrm{Nm}\, F(\omega)\equiv 1 \pmod{\nu^\pi}$$

atque:

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

obtinemus:

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

*) v. § 2, 4.

**) v. adnotationem in fine paragraphi 3.

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

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

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:

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

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

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

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

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

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

§ 5.

Dato aliquo numero primo p, qui condicionem implet $p^\mu\equiv 1 \pmod{\nu}$, 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 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:

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

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 $\pi \cdot f(\omega)$ aliquis factor $e - \varepsilon_k$ metiri debet.

Dem. Ponatur

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

Tum habemus:

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

ergo secundum § 2, 1:

$$\varphi(\varepsilon_r) \equiv 0 \pmod{p} \quad \text{et} \quad \pi\cdot\varphi(\varepsilon_r) \equiv 0 \pmod{\pi\cdot p} \quad \text{ideoque} \quad \left(\mathrm{mod.}\,(e-\varepsilon)\right).$$

Deinde cum appareat esse $e \equiv \varepsilon$ et $\varepsilon_r \equiv \varepsilon_r \left(\mathrm{mod.}\,(e-\varepsilon)\right)$, obtinemus congruentias:

$$\pi\cdot\varphi(\varepsilon_r) \equiv \pi\cdot\varphi(\varepsilon_r) \equiv 0 \left(\mathrm{mod.}\,(e-\varepsilon)\right) \text{ sive } \pi\cdot\varphi(\varepsilon) \equiv 0 \left(\mathrm{mod.}\,(e-\varepsilon_{-r})\right)$$

id est

$$\pi\cdot f(\omega)\cdot f(\omega^{g^2})\cdots f(\omega^{g^{(\mu-1)\lambda}}) \equiv 0 \left(\mathrm{mod.}\,(e-\varepsilon_{-r})\right),$$

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

$$\pi\cdot f(\omega)\cdot f(\omega^{p})\cdots f(\omega^{p^{\mu-1}}) \equiv 0 \left(\mathrm{mod.}\,(e-\varepsilon_{-r})\right).$$

Est vero

$$\pi\cdot f(\omega)\cdot f(\omega^{p})\cdots f(\omega^{p^{\mu-1}}) \equiv \pi\cdot f(\omega)^{1+p+\cdots+p^{\mu-1}} \pmod{\pi p} \quad \text{ideoque} \quad \left(\mathrm{mod.}\,(e-\varepsilon_{-r})\right),$$

ergo ratione supra adhibita:

$$\pi\cdot f(\omega) \equiv 0 \left(\mathrm{mod.}\,(e-\varepsilon_{-r})\right) \quad \text{q. e. d.}$$

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

$$\pi^n\cdot f(\omega) \equiv 0 \left(\mathrm{mod.}\,(e-\varepsilon_k)^m\cdot(e-\varepsilon_k)^{m'}\cdots\right),$$

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

*) v. *Gauss* disquisitiones arithmeticae. art. 347.

§ 6.

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

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

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

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

ergo

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

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 $(e-\varepsilon)\cdot\varphi(\varepsilon) \equiv 0 \pmod{p}$, quia

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

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 congruentia concluditur $f(\varepsilon)\cdot\varphi(\varepsilon) \equiv 0 \pmod{p}$ sive

$$\mathrm{Nm} f(\varepsilon)\cdot\mathrm{Nm}\,\varphi(\varepsilon) \equiv 0 \pmod{p^\lambda},$$

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

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

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 $d \cdot \varphi(\varepsilon) \equiv 0 \pmod{p}$, ergo $d^\lambda \cdot \mathrm{Nm}\, \varphi(\varepsilon) = d^\lambda \cdot \pi^{\lambda-1} \cdot p^{\lambda-1} \equiv 0 \pmod{p^\lambda}$, ergo: $d^\lambda \cdot \pi^{\lambda-1} \equiv 0 \pmod{p}$, id quod esse nequit, quia π ad ipsum p primus atque $d < p$ est.

Iam accepto numero k eiusmodi, ut sit

$$k^\lambda \leq p < (k+1)^\lambda,$$

statuamus cunctos numeros complexos formae $c + c_1\varepsilon + \cdots + c_{\lambda-1}\varepsilon^{\lambda-1}$, in quibus coefficientes isti c valores $0, 1, 2, \ldots k$ 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:

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

sive

$$np \leq M_\lambda k^\lambda \leq M_\lambda p,$$

unde denique

$$n \leq M_\lambda.$$

Hinc habemus hoc theorema magni momenti:

> Dato aliquo numero p, qui condicionem implet $p^\mu \equiv 1 \pmod{\nu}$, semper invenire licet numerum n non maiorem 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 complexos dissolvi possint*), tantummodo necesse est, numeros primos, qui sint residua λ^{tae} potestatis modulo ν quantitatibus illis M_λ non maiores, 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 non maioribus 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 $\leq n \leq M_\lambda$ 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 non maiores, in λ factores complexos discerpi possint. Deinde transeundo ad eos ipsius λ divisores, qui duabus

*) Adnotamus illud etiam ita exhiberi posse, ut pro his numeris ν omnes numeros primos formarum $k\nu + y^\lambda$ 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.

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_4 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 $(a + a_1\varepsilon)\cdot(a + a_1\varepsilon_1)$ dissolvi possunt. Id quod vel illa ipsa ratione erui vel e theoria formarum secundi gradus probari potest. Est enim

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

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.

§ 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

$$\nu = a^\alpha \cdot b^\beta \cdot c^\gamma \cdots,$$

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

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

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

notis methodis probatur, quae quidem aequatio $\varphi(\nu)^{ti}$ 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^α, b^β, ... resp. literis $g, h, \ldots$, deinde ponatur

$$\frac{\nu}{a^\alpha} = a', \quad \frac{\nu}{b^\beta} = b', \quad \ldots;$$

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 $1, 2, \ldots a^{\alpha-1}(a-1)$; $1, 2, \ldots b^{\beta-1}(b-1)$; $\cdots$ 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

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

et ponatur

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

sive

$$\varepsilon_{k,k',\ldots} = \sum_{m} \omega^{a'g^{m\lambda+k}} \cdot \sum_{n} \omega^{b'h^{n\lambda'+k'}} \cdots;$$

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

**) Demonstrationem illam, de qua sermo est, proximo tempore in publicum editurus sum[1]).

[1]) *L. Kronecker*, Mémoire sur les facteurs irréductibles de l'expression $x^n - 1$. *Liouville* Journal sér. I tome 19 pag. 177—192. No. 3 des I. Bandes dieser Ausgabe von *L. Kronecker's* Werken.

quae expressiones partes periodorum in numeris primis ν agunt. — Numerus terminorum expressionis talis erit: $\mu\cdot\mu'\cdot\mu''\cdots$, numerus periodorum ε inter se diversarum: $\lambda\cdot\lambda'\cdot\lambda''\cdots$, 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 $\lambda\cdot\lambda'\cdot\lambda''\cdots$, quaevis ipsius ε potestas $\geqq\lambda\cdot\lambda'\cdot\lambda''\cdots$ potestatibus inferioribus exprimi potest.

Duae periodi ε diversorum indicum aequales esse non possunt.

Primum enim ex aequatione $\varepsilon_{0,0,0,\ldots}=\varepsilon_{k,k',k'',\ldots}$ sequeretur aequatio eiusmodi $\varepsilon_{0,0,0,\ldots}=\varepsilon_{k,mk',nk'',\ldots}$ *) 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:

$$\sum\omega^{\alpha'g^{m\lambda}}=\sum\omega^{\alpha'g^{m\lambda+k}};$$

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

$$\varepsilon_k=\sum'\omega^{g^{m\lambda+k}}.$$

Iam colliguntur ex aequatione $\varepsilon_0=\varepsilon_k$ haece:

$$\varepsilon_1=\varepsilon_{k+1},\quad \varepsilon_2=\varepsilon_{k+2},\ \cdots$$

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:

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

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

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

$$(\varrho,\omega)=(\varrho,\omega^{g^k})=(\varrho,\omega)\cdot\varrho^{-k},$$

unde

$$(\varrho,\omega)\cdot(1-\varrho^{-k})=0,$$

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 $(\varrho,\omega)\cdot(\varrho^{-1},\omega)=\pm a^\alpha$ 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 $A, A_1, \ldots$ numeros reales integros esse, expressio formae:

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

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

*) Id quod fusius exponere omittimus.
**) Posuimus $L=\lambda\cdot\lambda'\cdot\lambda''\cdots$.

$$\lambda = a^{\alpha-1}\cdot d \quad \text{et} \quad d\cdot\mu = a-1.$$

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 $1, 2, \ldots a^{\alpha-1}-1$ induere potest. Inter quas vero quaeque μ inter se congruunt, unde numerus aequationum inter se diversarum 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 $\varepsilon(\omega^{p^{\lambda}})$ 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 $\varepsilon_k^2, \varepsilon_k^3, \ldots \varepsilon_k^{\lambda-1}$ 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:

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

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

$$\Sigma\omega^{a^{\alpha}g^{m\lambda+k}}=\varepsilon_k, \quad \Sigma\omega^{b^{\beta}a^{\alpha}g^{n\lambda'+k'}}=\varepsilon_{k'}, \ldots,$$

*) Id quod ratione supra (pag. 31) exhibita probatur.

igitur secundum illam definitionem:

$$\varepsilon_{k,k',\ldots}=\varepsilon_k\cdot\varepsilon_{k'}\cdot\cdots,$$

scimus hoc productum exprimi posse producto functionum rationalium ipsorum $\varepsilon, \varepsilon', \varepsilon'', \ldots$. Restat igitur, ut probemus quodvis productum $\varepsilon^{i}\varepsilon'^{i'}\cdots$ repraesentari posse potestatibus

$$(\varepsilon\cdot\varepsilon'\cdot\varepsilon''\cdots), \quad (\varepsilon\cdot\varepsilon'\cdot\varepsilon''\cdots)^2, \quad \ldots \quad (\varepsilon\cdot\varepsilon'\cdot\varepsilon''\cdots)^{L-1}.$$

Cum vero quaeque i^{ta} ipsius ε potestas potestate prima, secunda, etc., $(\lambda-1)^{\text{ta}}$ exprimi possit, illae $L-1$ potestates quantitatis $(\varepsilon\cdot\varepsilon'\cdot\varepsilon''\cdots)$ repraesentari possunt variis productis $\varepsilon^{i}\varepsilon'^{i'}\cdots$, in quibus $i<\lambda$, $i'<\lambda', \ldots$, quorum igitur numerus est $\lambda\cdot\lambda'\cdot\lambda''\cdots=L$, vel excepto producto $\varepsilon^0\cdot\varepsilon'^0\cdots=1$ restant $L-1$ producta, quibus potestates $(\varepsilon\cdot\varepsilon'\cdots)^2, (\varepsilon\cdot\varepsilon'\cdots)^3, \ldots$ expressae sunt. Ex quibus aequationibus $L-2$ si omnia eliminamus producta exceptis $\varepsilon\cdot\varepsilon'\cdot\varepsilon''\cdots$ et certo quodam $\varepsilon^{i}\cdot\varepsilon'^{i'}\cdots$, quorum igitur multitudo $L-3$, obtinemus aequationem formae:

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

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. 31).

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 $p^{n}\equiv 1 \pmod{\nu}$, et casu $p=\nu$ (v. § 2), id quod huic rei respondet, posito ν numerum esse compositum, probari potest: scilicet congruentiam gradus $\lambda\cdot\lambda'\cdot\lambda''\cdots$ hanc:

$$\mathrm{Nm}\,(x-\varepsilon)\equiv 0 \pmod{p}$$

habere totidem radices reales, si p supponitur numerus talis, ut sit

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

vel etiam pro aliquo ipsius ν factore primo e. g. $p = a$, dummodo

$$a^{\mu'} \equiv 1 \pmod{b^{\beta}}, \quad a^{\mu''} \equiv 1 \pmod{c^{\gamma}}, \cdots$$

sit*).

Pro talibus numeris primis p, quales tantum congruentiis sufficiunt

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

ubi δ, $\delta' \ldots$ divisores numerorum $a-1$, $b-1$, $\ldots$, numeri autem k, $k', \ldots$ vel omnes vel partim >0 sunt, erit $\mathrm{Nm}(x-\varepsilon) \equiv 0 \pmod{p}$ designante ε periodum compositam e radicibus primitivis aequationis

$$z^{a^{\alpha-k} \cdot b^{\beta-k'} \cdots} = 1,$$

atque habebuntur $\frac{\varphi(\nu)}{a^k \delta \cdot b^{k'} \delta' \cdots}$ 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 (*Crelle's* 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^{μ} gradus atque λ indeterminatarum a, a_1, $\ldots$ $a_{\lambda-1}$ 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

*) Cf. *Eisenstein* „de formis cubicis etc." (*Crelles* Journal, Bd. 28 [S. 289—374]).
**) Disputatio Cli. *Kummer* § 4.

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

quem numerum integrum esse apertum est, scilicet

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

Iam posito

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

additis aequationibus:

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

obtinemus:

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

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):

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

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:

*) Cf. id quod pag. 13 exposuimus.

$$\varphi(\omega) = \frac{(1-\omega^{\rho})\cdot(1-\omega^{\rho\lambda+1})\cdots(1-\omega^{\rho(\mu-1)\lambda+1})}{(1-\omega)\cdot(1-\omega^{\rho\lambda})\cdots(1-\omega^{\rho(\mu-1)\lambda})} = \psi(\varepsilon),$$

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 $(1-\omega^{\rho\lambda\lambda+1})$ factore quodam denominatoris $(1-\omega^{\rho k\lambda})$ dividi possit, quia $\frac{1-\omega^{\rho\lambda\lambda+1}}{1-\omega^{\rho k\lambda}} = \frac{1-x^{\rho}}{1-x}$ posito $\omega^{\rho\lambda} = x$. Denique illa expressio functio periodorum ε est, quia mutata radice ω in $\omega^{\rho\lambda}$ immutata manet. Hinc igitur patet $\psi(\varepsilon)$ unitatem esse integram complexam. — Etiamque producta:

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

designantibus $n_1, n_2, \ldots n_{\lambda-1}$ 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

$$1 - \omega^{\rho^{\mu\lambda+k}+k+1} \quad \text{factor} \quad 1 - \omega^{\rho^{\mu\lambda+k}+1}$$

respondet. Quibus multiplicatis obtinemus

$$2 - 2\cos v = 4\sin^2\tfrac{1}{2}v,$$

ubi

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

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

§ 9.

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

$$\begin{array}{rl} & c\varepsilon \quad + c_1\varepsilon_1 + \cdots + c_{\lambda-1}\varepsilon_{\lambda-1} = r_1, \\ (1.) & c\varepsilon_1 \quad + c_1\varepsilon_2 + \cdots + c_{\lambda-1}\varepsilon \quad = r_2, \\ & \quad\vdots \qquad\quad \vdots \qquad\quad \vdots \\ & c\varepsilon_{\lambda-1} + c_1\varepsilon \quad + \cdots + c_{\lambda-1}\varepsilon_{\lambda-2} = r_{\lambda}. \end{array}$$

Deinde sit data aliqua unitas $a\varepsilon + a_1\varepsilon_1 + \cdots + a_{\lambda-1}\varepsilon_{\lambda-1}$ atque designentur

similiter valores absoluti factorum coniunctorum resp. literis f_1, f_2, ... f_λ. Iam ponantur:

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

Quod systema $\lambda - 1$ aequationum atque $\lambda - 1$ indeterminatarum n est, nam aequationibus omnibus multiplicatis per condicionem

$$f_1 \cdot f_2 \cdots f_\lambda = r_1 \cdot r_2 \cdots r_\lambda = 1$$

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

$$\log f_k = \varphi_k, \qquad \log r_k = \varrho_k$$

valores logarithmorum naturalium denotamus, obtinetur:

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

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

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

Iam positis:

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

erit

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

ergo:

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

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

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

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. 13) 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:

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

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

$$\varrho(\alpha) \cdot \varrho(\alpha^2) \cdots \varrho(\alpha^{\lambda-1})$$

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:

$$\varrho_{k+1} = \log r_{k+1} = \log \frac{(1-\omega^{\rho^{k+1}}) \cdot (1-\omega^{\rho^{k+1+\lambda}}) \cdots (1-\omega^{\rho^{k+1+(\mu-1)\lambda}})}{(1-\omega^{\rho^k}) \cdot (1-\omega^{\rho^{k+\lambda}}) \cdots (1-\omega^{\rho^{k+(\mu-1)\lambda}})},$$

sive:

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

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

$$\left\{\begin{array}{l}\sum_0^{\lambda-1}\{\log(1-\omega^{\varrho^k+1})+\log(1-\omega^{\varrho^{k+1}+\lambda})+\cdots+\log(1-\omega^{\varrho^{k+1}+(\mu-1)\lambda})\}\alpha^k \\ -\sum_0^{\lambda-1}\{\log(1-\omega^{\varrho^k})\quad+\log(1-\omega^{\varrho^k+\lambda})\quad+\cdots+\log(1-\omega^{\varrho^k+(\mu-1)\lambda})\}\alpha^k\end{array}\right.$$

sive

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

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

Iam cum sit:

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

fit:

$$-\sum_0^{\mu\lambda-1}\alpha^k\cdot\log(1-\omega^{\varrho^k})=\sum_n\sum_{k=0}^{k=\mu\lambda-1}\alpha^k\cdot\frac{\omega^{n\varrho^k}}{n},$$

in qua summatione n omnes numeros integros positivos ad numerum ν primos designat. Nam pro valoribus $n=r\nu$ fit $\omega^{n\varrho^k}=1$ 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

$$\sum_n\sum_0^{\mu\lambda-1}\alpha^k\cdot\frac{\omega^{n\varrho^k}}{n}\qquad\text{abit in}\qquad\sum_n\frac{1}{n}(\alpha,\omega^n),$$

ubi

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

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

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

et mutato ω in ω^ϱ:

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

id est

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

Ergo habemus denique:

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

Iam neque factor (α,ω) neque $(1-\alpha^{-1})$ evanescere potest. Prior enim sententia ex aequatione

$$(\alpha,\omega)\cdot(\alpha^{-1},\omega)=\pm\nu,$$

secunda ex eo, quod α ab unitate diversum positum est, elucet. Restat igitur, ut factorem $\sum\frac{\alpha^{-\mathrm{Ind.}\,n}}{n}$ non evanescere probetur. Tum etiam $\sum\frac{\alpha^{+\mathrm{Ind.}\,n}}{n}$ evanescere deberet, id quod pro nullo α, quod sit radix aequationis $x^{\nu-1}=1$, ideoque etiam pro nulla radice unitatis λ^{tm} α fieri posse Cl. *Lejeune-Dirichlet* in illustri illa commentatione „de progressione arithmetica infinita“[1] 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

$$n_1=E_1+\delta_1,\quad n_2=E_2+\delta_2,\ \ldots,$$

quantitatibus δ inter 0 et 1 acceptis, aequationes II § 9 mutantur in:

(I.)
$$f_1=r_1^{E_1}\cdot r_2^{E_2}\cdots r_{\lambda-1}^{E_{\lambda-1}}\cdot r_1^{\delta_1}\cdot r_2^{\delta_2}\cdots r_{\lambda-1}^{\delta_{\lambda-1}}$$
$$\cdots\cdots\cdots\cdots$$

Ex quibus aequationibus, cum et f_1 et $r_1^{E_1}\cdot r_2^{E_2}\cdots r_{\lambda-1}^{E_{\lambda-1}}$ unitates integrae complexae sint, alter quoque dextrae partis factor:

$$r_1^{\delta_1}\cdot r_2^{\delta_2}\cdots r_{\lambda-1}^{\delta_{\lambda-1}}$$

unitas integra complexa sit oportet. Ponatur igitur:

[1]) *G. Lejeune-Dirichlet*, Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. Abh. d. Preuss. Akad. d. Wissensch. v. J. 1837. S. 45—81. *Lejeune-Dirichlet's* Werke. Bd. I S. 313—342. H.

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

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

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

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 $\mathfrak{F}_1, \mathfrak{F}_2, \ldots$ superare non posse ex aequationibus (II) et condicionibus, quibus ibidem quantitates ϑ sunt circumscriptae, colligi potest. Unde sequitur, ut quantitates quoque $-\nu A$, $-\nu A_1, \ldots$ limitibus quibusdam contineantur, scilicet cum quantitates $\mu - \varepsilon$ sint positivae:

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

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 $A, A_1, \ldots$ 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 $r_1, r_2, \ldots r_{\lambda-1}$ et unitatibus quibusdam numeri finiti exprimi possit; i. e. ut cunctae unitates forma

$$F\cdot r_1^{k_1}\cdot r_2^{k_2}\cdots r_{\lambda-1}^{k_{\lambda-1}}$$

contineantur, designantibus $k_1, k_2, \ldots$ 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):

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

ubi

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

eamque consideremus tanquam functionem quantitatum ϑ. Quotientes differentiales istius functionis (I) respectu quantitatum $\vartheta_1, \vartheta_2, \ldots$ sunt:

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

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 ϑ_1, secunda respectu ϑ_2 etc. differentiatis obtinemus, erunt:

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

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 $\nu\Delta_\lambda$ 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 valorem 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 exempli gratia posito

$$\nu = 7, \quad \lambda = 3$$

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:

$$\varepsilon_1 = \omega + \omega^{-1},$$

$$\varepsilon_1 + \varepsilon_2 = \omega + \omega^{-1} + \omega^2 + \omega^{-2} = \varepsilon_2 \cdot \varepsilon_3,$$

$$\varepsilon_1 + \varepsilon_2 - \varepsilon_3 = \omega + \omega^{-1} + \omega^2 + \omega^{-2} - \omega^3 - \omega^{-3} = \varepsilon_2 \cdot \varepsilon_3^3,$$

$\varepsilon_1 - \varepsilon_2$ 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:

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

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

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*):

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

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

§ 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

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

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

*) v. III. § 10.

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

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

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

in qua aequatione n_1, n_2, ... non omnes nihilo aequales atque numeri integri esse deberent, cum et ipsa a, b, c, ... 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:

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

Unde per aequationem (IV) § 9 obtinemus:

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

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

$$r_1, r_2, \cdots r_{\lambda-1}, r_\lambda$$

unitates aliquas coniunctas, denotamus productum

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

signo:

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

Id quod ita quoque exhiberi potest, ut dicamus, posito

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

pro aequationibus illis (IV § 9):

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

substitui aequationem:

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

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

$$r_1\cdot r_2\cdots r_\lambda = 1$$

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

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

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

E definitione statim sequuntur aequationes:

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

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

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

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

Posito enim

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

habemus aequationes:

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

quae posito

$$\log s_k = \sigma_k$$

secundum § 9, (II), (III), (IV) eandem habent vim quam aequatio:

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

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

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

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

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

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

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

$$n_1 = m_1, \quad n_2 = m_2, \quad \ldots \quad n_{\lambda-1} = m_{\lambda-1} \quad \text{i. e. nisi} \quad n(\alpha) = m(\alpha)$$

pro omnibus λ^{tis} unitatis radicibus excepta unitate.

Demonstravimus in § 9, quamvis unitatem complexam forma

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

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

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

etiam productum

$$r_1^{\delta_1} \cdot r_2^{\delta_2} \cdots r_{\lambda-1}^{\delta_{\lambda-1}}$$

unitatem 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

$$r_1^{\delta_1} \cdot r_2^{\delta_2} \cdots r_{\lambda-1}^{\delta_{\lambda-1}}$$

(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:

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

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:

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

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

$$m(\alpha) = a(\alpha) \cdot v(\alpha), \qquad n = c(\alpha) \cdot v(\alpha),$$

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

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)

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

sive

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

Cum vero $r^{\frac{m(\alpha)}{n}}$ sive $r^{\frac{a(\alpha)}{c(\alpha)}}$ unitas integra sit, eadem proprietate unitatem $r^{\frac{a(\alpha)\cdot b(\alpha)}{c(\alpha)}}$ sive $r^{\frac{1}{c(\alpha)}}\cdot r^{F(\alpha)}$ 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:

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

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

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

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

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

sive

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

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 $r^{\frac{b(\alpha)}{n(\alpha)}}\cdot r^{\frac{a(\alpha)}{n'(\alpha)}}$ sive $r^{\frac{b(\alpha)}{n(\alpha)}+\frac{a(\alpha)}{n'(\alpha)}}$ integras esse in promptu est. Est vero:

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

unde igitur unitatem $r^{\frac{1}{c(\alpha)\cdot m(\alpha)\cdot m'(\alpha)}}$ 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 $r^{\frac{1}{\pi(\alpha)}}$, qua praeter unitates r ad repraesentandas omnes unitates opus erit. Quodsi $r^{\frac{1}{\pi(\alpha)}} = u$ ponimus, est $r = u^{\pi(\alpha)}$, ex qua aequatione, ut ipsae unitates r integris ipsorum u potestatibus exprimi possint, sequitur; ergo forma:

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

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. $\mathrm{Nm}\frac{h(\alpha)}{k} \geqq 1$ 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 $\mathrm{Nm}\frac{m(\alpha)}{n}\cdot\frac{h(\alpha)}{k} \geqq \mathrm{Nm}\frac{m(\alpha)}{n}$ secundum suppositionem de unitate u factam esse debeat, illa condicio $\mathrm{Nm}\frac{h(\alpha)}{k} \geqq 1$ 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)

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

Cum vero unitas $u^{\frac{m(\alpha)}{n(\alpha)}}$ ideoque $u^{a(\alpha)\cdot\frac{m(\alpha)}{n(\alpha)}}$ 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:

$$u_1,\ u_2,\ \cdots\ u_{\lambda-1},$$

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:

$$u_1^{k(\alpha)\cdot k(\alpha')\cdots k(\alpha^{\lambda-1})} = u_1 = v_1^{k(\alpha')\cdots k(\alpha^{\lambda-1})} = v_1^{K(\alpha)},$$

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:

$$\begin{aligned} u_1^{a_1}\cdot u_2^{a_1}\cdots u_{\lambda-1}^{a_{\lambda-1}} &= A,\\ u_1^{b_1}\cdot u_2^{b_2}\cdots u_{\lambda-1}^{b_{\lambda-1}} &= B,\\ \vdots\quad &\quad\vdots\quad\ \vdots, \end{aligned}$$

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

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

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

$$\begin{aligned} \Delta\cdot\log u_1 &= m_1\cdot\log A + m_2\cdot\log B + \cdots,\\ &\cdots\cdots\cdots\cdots\cdots, \end{aligned}$$

designante Δ determinantem illius systematis, $m_1,\ m_2,\ \ldots$ 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 $A,\ B,\ \ldots$ exprimi posse. Unde etiam tales unitates $A,\ B,\ \ldots$ infinitis modis (dummodo $\lambda \geqq 3$) eligi posse, plane in promptu est.

Quae ut ad unum tantum exemplum adhibeamus, ponamus uti in § 11

$$p = 7, \quad \lambda = 3.$$

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:

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

habemus sexies binas unitates coniunctas fundamentales:

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

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

$$a_1 \log u_1 + a_2 \log u_2 = \log A,$$
$$b_1 \log u_1 + b_2 \log u_2 = \log B,$$

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

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

habemus ut unitates fundamentales:

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

§ 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

$$r_1, \quad r_2, \quad \cdots \quad r_{\lambda-1}$$

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:

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

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

$$hk + gl = 1,$$

ergo

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

*) 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).

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

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

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

(II.) $$r^{\frac{k(\alpha)}{p^\alpha}}, \quad r^{\frac{k'(\alpha)}{p^\beta}}, \quad \cdots ,$$

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 (mod. λ) 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:

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

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

$$x \cdot \mathrm{Nm}\, f(\alpha) \equiv 1 \pmod{p^\alpha}.$$

Unde cum unitas $r^{\frac{\pi^n k(\alpha)}{p^\alpha}}$ integra sit, unitatem quoque hanc:

$$r^{\frac{p(\varepsilon)^m \cdot p(\varepsilon_1)^{m_1} \cdots}{p^\alpha}} = s$$

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

*) 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.

$$y \cdot f(\alpha) \cdot p(\varepsilon)^{m} \cdot p(\varepsilon_1)^{m_1} \cdots \equiv k(\alpha) \pmod{p^a}$$

sive aequatio:

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

unde

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

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

$$\text{(IV.)} \qquad r^{\frac{p(\varepsilon)^{m} \cdot p(\varepsilon_1)^{m_1} \cdots}{p^a}}, \quad r^{\frac{q(\varepsilon)^{n} \cdot q(\varepsilon_1)^{n_1} \cdots}{q^b}}, \quad \ldots .$$

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

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

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

$$p(\varepsilon)^{m} \cdot p(\varepsilon_1)^{m_1} \cdots = f(\varepsilon) \cdot p(\varepsilon_k)^{r} \cdot p(\varepsilon_{k'})^{r'} \cdots = f(\varepsilon) \cdot \varphi(\varepsilon),$$

$$p(\varepsilon)^{n} \cdot p(\varepsilon_1)^{n_1} \cdots = f(\varepsilon) \cdot p(\varepsilon_k)^{w} \cdot p(\varepsilon_{k'})^{w'} \cdots = f(\varepsilon) \cdot \psi(\varepsilon),$$

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:

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

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: $x \cdot \mathrm{Nm}\,\chi(\varepsilon) \equiv 1 \pmod{p^a}$. Deinde cum unitates:

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

integrae sint, ope illius congruentiae $x \cdot \mathrm{Nm}\,\chi(\varepsilon) \equiv 1 \pmod{p^a}$ 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 $b \leqq a$. Fractionis $\frac{\psi(\varepsilon)}{p^b}$ et numeratore et denominatore numero $(\pi p)^{a-b}$ 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

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

erit:

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

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

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

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:

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

Quam enim unitatem integram esse elucet, atque unitates illas (V) ope unitatum r_1, r_2, ... $r_{\lambda-1}$ ex unitate s deduci posse hoc modo probatur. Cum

productum $q^b \cdot \cdots$ ad ipsum p primum sit, numerus inveniri potest x talis, ut sit:

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

quare erit

$$s_1^{x \cdot q^b \cdot t^c \cdots} = r_1^{\frac{k(\omega)}{p^a}} \cdot r_1^{\eta k(\omega) + \varkappa t^c \cdots k'(\omega) + \cdots},$$

unde unitatem $r_1^{\frac{k(\omega)}{p^a}}$ re vera potestatibus integris unitatum r et s exprimi posse manifestum est. Cuius explicationis summam hoc modo exhibere possumus:

Acceptis quibuslibet unitatibus coniunctis

$$r_1, \ r_2, \ \cdots \ r_{\lambda-1},$$

semper inveniri potest systema unitatum coniunctarum

$$s_1, \ s_2, \ \cdots \ s_{\lambda-1}$$

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 $p, q, \ldots$ contineat, atque „r“ unitas illa in § 9 memorata; ostendamus exstare unitates $s_1, s_2, \ldots$ eiusmodi, ut his aequationibus satisfaciant:

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

praetereaque his:

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

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

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

atque his:

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

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:

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

ubi

$$a_1 + a_2\alpha + \cdots + a_{\lambda-1}\alpha^{\lambda-2}$$

$$= (1 + \alpha^d + \cdots + \alpha^{(\delta-1)d}) \cdot (1 + \alpha + \alpha^2 + \cdots + \alpha^{\frac{d}{p}-1}) \cdot (1 + \alpha + \alpha^2 + \cdots + \alpha^{\frac{d}{q}-1}) \cdots .$$

Ex qua aequatione numeri $a_1, a_2, \ldots$ ita sunt determinandi, ut explicato producto dextrae partis eoque solius aequationis $\alpha^\lambda = 1$ ope reducto singularum ipsius α potestatum coefficientes quantitatibus $a_1, a_2, \ldots$ 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 § 9 tradito, ut sit:

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

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:

$$f_1, \quad f_2, \quad \cdots \quad f_d;$$

designentur deinde valores absoluti logarithmorum harum quantitatum signis:

$$\varphi_1, \quad \varphi_2, \quad \cdots \quad \varphi_d;$$

hoc aequationum systema semper solvi potest:

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

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:

$$\text{(VII.)} \quad \varphi_1 + \varphi_2 w + \cdots + \varphi_d w^{d-1} = (n_1 + n_2 w^{-1} + \cdots + n_k w^{-(k-1)})\cdot(\sigma_1 + \sigma_2 w + \cdots + \sigma_d w^{d-1}).$$

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 illius non evanescere probandum est. Determinans autem cum sit:

$$\sigma(w)\cdot\sigma(w^h)\cdot\sigma(w^{h'})\cdots,$$

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:

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

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

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

esse deberet:

$$\varrho(\alpha^\delta)\cdot(a_1 + a_2\alpha^{-\delta} + \cdots) = 0,$$

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

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

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

---

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

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:

$$s_1^{\frac{m_1}{n}} \cdot s_2^{\frac{m_2}{n}} \cdots s_k^{\frac{m_k}{n}}$$

sive:

$$s_1^{\frac{1}{n}(m_1 + m_2 w + \cdots + m_k w^{k-1})},$$

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:

$$1 + w^{\frac{d}{p}} + w^{2\frac{d}{p}} + \cdots + w^{(p-1)\frac{d}{p}} = 0,$$

$$1 + w^{\frac{d}{q}} + w^{2\frac{d}{q}} + \cdots + w^{(q-1)\frac{d}{q}} = 0,$$

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

et

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

cumque vera sit:

$$s_1^{1 + w^{\frac{d}{p}} + \cdots + w^{(p-1)\frac{d}{p}}} = s_1 \cdot s_{\frac{d}{p}+1} \cdots s_{(p-1)\frac{d}{p}+1} = 1 = s_1^0$$

. . . . . .

nec non:

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

§ 19.

Respectu habito eorum, quae in § 7 cum explicata tum indicata sint, atque posito „λ“ numerum esse eiusmodi, ut quivis numerus primus formae

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

$k\lambda + r$ in n factores complexos, compositos e radicibus unitatis λ^{tis}, discerpi possit, si statuamus g, g', g'', ... resp. numerorum p^a, q^b, t^c, ... radices primitivas,

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

$$n = h \cdot h' \cdot h'' \cdots *),$$

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 $\mathrm{Nm}\, m(w) = 1$. Etiamque unitates non coniunctae statui possunt fundamentales multitudinis $\varphi(d)$, et quidem numerus unitatum diversarum, quae statui possunt, fundamentalium coniunctarum erit 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.

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

**) v. § 7.

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

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:

$$f,\ f',\ f'',\ \cdots,\qquad .$$

itaque illas quoque unitates „s“ potestatibus harum f integris repraesentari posse oportet. Quare sit posito $\log f = \varphi$, $\log f' = \varphi'$, ... et $k = \varphi(d)$:

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

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

$$\begin{aligned}
s_1^{n_1}\cdot s_2^{n_2}\cdots s_k^{n_k} &= 1,\\
s_2^{n_1}\cdot s_3^{n_2}\cdots s_{k+1}^{n_k} &= 1,\\
\vdots \qquad\quad &\vdots \qquad\quad \vdots\ ,
\end{aligned}$$

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

$$(n_1 + n_2w^{-1} + \cdots + n_kw^{-(k-1)})\cdot(\sigma_1 + \sigma_2w + \cdots + \sigma_dw^{d-1}) = 0$$

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

$$u_{d,1},\quad u_{d,2},\quad \cdots,$$

earumque logarithmi sint

$$v_{d,1},\quad v_{d,2},\quad \cdots\ .$$

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:

$$r_1^{\alpha_1}\cdot r_2^{\alpha_2}\cdots r_{\lambda-1}^{\alpha_{\lambda-1}} = r_1^{\alpha(\alpha)} = s_1.$$

Sed esse debet

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

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

$$\text{(I.)}\quad \sigma_1 + \sigma_2w + \cdots + \sigma_dw^{d-1} = (n_1 + n_2w^{-1} + \cdots + n_kw^{-(k-1)})\cdot(v_{d,1} + v_{d,2}w + \cdots + v_{d,d}w^{d-1})$$

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

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

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

$$a(w^{-1})\cdot(\varrho_1 + \varrho_2w + \cdots + \varrho_\lambda w^{\lambda-1}) = \sigma_1 + \sigma_2w + \cdots + \sigma_\lambda w^{\lambda-1},$$

atque per aequationem (I) aliquanto mutatam:

$$\text{(III.)}\qquad \left\{\begin{aligned}
&a(w^{-1})\cdot(\varrho_1 + \varrho_2w + \cdots + \varrho_\lambda w^{\lambda-1})\\
&= (n_1 + n_2w^{-1} + \cdots + n_kw^{-(k-1)})\cdot(v_{d,1} + v_{d,2}w + \cdots + v_{d,\lambda}w^{\lambda-1}).
\end{aligned}\right.$$

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

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

sit (designante w radicem primitivam), habemus aequationem:

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

atque si ponimus unitatem:

$$r_1 \cdot u_{d_i 1}^{-m_1} \cdot u_{d_i 2}^{-m_2} \cdots u_{d_i k}^{-m_k} = t_1$$

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

$$a(\alpha^{-1}) \cdot (\tau_1 + \tau_2 \alpha + \cdots + \tau_\lambda \alpha^{\lambda-1}) = c(\alpha^{-1}) \cdot (v_{d_i 1} + v_{d_i 2} \alpha + \cdots + v_{d_i \lambda} \alpha^{\lambda-1})$$

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

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

cum pro his ipsius α valoribus sit $v_{d_i 1} + v_{d_i 2} \alpha + \cdots = 0$.

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:

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

secundum notum illud theorema.

Statutis certis quibusdam residuorum systematis modulis

$$a(w), \quad a'(w'), \quad \ldots$$

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

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:

$$d_1, \quad d_2, \quad \ldots \quad d_i;$$

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

$$r, s, t, \ldots$$

omnes illas, quae supra ipso „r“ denotatae sunt, inveniri apertum est. Deinde adnotamus, pro divisore 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

$$\xi_1 + \xi_2 \alpha + \cdots + \xi_\lambda \alpha^{\lambda-1} = 0$$

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:

$$a(w^{-1}) \cdot (\xi_1 + \xi_2 w + \cdots + \xi_\lambda w^{\lambda-1}) = (n_1 + n_2 w^{-1} + \cdots) \cdot (v_{d_i 1} + v_{d_i 2} w + \cdots),$$

ubi w est radix d_i^{ta} primitiva, numerus $n(w)$ ipso $a(w)$ dividi posse deberet, propterea que 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 $t, \ldots$) 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 $s, t, \ldots$ 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

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

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

$$m(w) \cdot \psi(w) \equiv 1 \qquad \big(\text{mod. } a(w)\big)\ ^*),$$

ergo

$$n(w) \cdot \psi(w) \equiv \varphi(w) \qquad \big(\text{mod. } a(w)\big).$$

Itaque cum unitas $r_1^{\psi(\omega)}$ quoque integra sit, unitas existit, cuius residuum respectu d_1 ipse numerus $\varphi(w)$ est. Quae si litera r' designatur, erit $r'^{m(\omega)}$ 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.

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

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

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

$$m(w) \cdot \varphi(w) + n(w) \cdot \psi(w) \equiv \chi(w) \qquad \big(\text{mod. } a(w)\big),$$

ubi $\chi(w)$ factor est communis maximus ipsorum $\varphi(w)$ et $\psi(w)$, illa sententia elucet. Cumque etiam $r^{m(\omega)} \cdot r'^{n(\omega)}$ unitas sit integra eaque talis, ut residuum respectu d_1 sit $\chi(w)$, hanc ipsam unitatem, ex qua ope unitatum $s, t, \ldots$ 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 resi-

*) Cf. § 4 et § 7.

duorum 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 $s, t, \ldots$ 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:

$$u_{d_1}, \quad u_{d_2}, \quad u_{d_3}, \quad \ldots \quad u_{d_{i-1}}, \quad u_{d_i},$$
$$r, \quad s, \quad t, \quad \ldots \quad z.$$

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

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

vel

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

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

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

ideoque posito $\log x_i = \xi_i$:

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

Cum vero $c(\alpha^{-1})$, eaque de re $\xi(\alpha)$, pro illo ipsius α valore $\alpha = w$ evanescat,

unitas x_1 unitatibus $u_{d_1} \ldots$ atque unitatibus $s, t, \ldots$ repraesentari potest. Ergo r_{k+1} unitatibus $r_1, r_2, \ldots r_k$ et unitatibus utriusque illius seriei reliquis exprimi potest; pariterque r_{k+2} unitatibus $r_2, r_3, \ldots r_{k+1}$ ideoque unitatibus $r_1, r_2, \ldots r_k$ et reliquis etc. etc. Itaque pro illis unitatibus „u_{d_i}“ et „r“ tantum accipiendae sunt unitates:

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

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 $s_1, s_2, \ldots s_{\varphi(d_2)}$ adiunctis illis $u_{d_2}, \ldots t, \ldots z$, 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 $x, x_1, \ldots x_{\lambda-1}$ 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 $u_1^{\pi(a)}$ sive

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

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 $r_1, r_2, \ldots r_{\lambda-1}$ semper inveniri posse alterum systema $s_1, s_2, \ldots s_{\lambda-1}$ tale, ut omnes unitates integris istarum unitatum r et s potestatibus exprimi liceat, sequitur, ut accepto quolibet systemate $x^0, x_1^0, \ldots x_{\lambda-1}^0$ alterum systema $x', x_1', \ldots x_{\lambda-1}'$ 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.

VITA.

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

THESES.

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

MÉMOIRE
SUR LES FACTEURS IRRÉDUCTIBLES DE L'EXPRESSION $x^n - 1$;

PAR

M. LÉOPOLD KRONECKER.

Liouville, Journal de mathématiques pures et appliquées Sér. I Tome 19 p. 177—192.

MÉMOIRE SUR LES FACTEURS IRRÉDUCTIBLES DE L'EXPRESSION $x^n - 1$.

On sait que l'expression $(x^n - 1)$, n désignant un nombre entier quelconque, peut se décomposer en facteurs rationnels dont le nombre est égal à celui des diviseurs de n. En effet, en dénotant par

$$F_m(x) = 0$$

l'équation qui ne contient que les racines primitives de l'équation $x^m = 1$, on aura

$$x^n - 1 = F_d(x) F_{d'}(x) F_{d''}(x) \cdots,$$

où d, d', d'', ..., désignent tous les divers diviseurs du nombre n. On peut dire que cette manière de décomposer l'expression $x^n - 1$ correspond à la décomposition d'un nombre entier en facteurs premiers; car tous les facteurs $F_d(x)$, $F_{d'}(x)$, ..., sont irréductibles, et c'est cette propriété des fonctions $F_d(x)$, $F_{d'}(x)$, ..., bien importante pour la théorie des nombres, qui sera l'objet du présent Mémoire.

Décomposons le nombre n en ses facteurs premiers, et soit

$$n = p^a q^b r^c \cdots t^g,$$

p, q, r, ..., t désignant des nombres premiers quelconques inégaux. Alors on peut représenter l'équation $F_n(x) = 0$, qui ne contient que les racines primitives de l'équation $x^n = 1$, de la manière suivante

$$F_n(x) = \frac{(x^n - 1)\cdot(x^{\frac{n}{p\cdot q}} - 1)\cdot(x^{\frac{n}{p\cdot r}} - 1)\cdots}{(x^{\frac{n}{p}} - 1)\cdot(x^{\frac{n}{q}} - 1)\cdot(x^{\frac{n}{r}} - 1)\cdots} = 0.$$

En effectuant la division, la fonction $F_n(x)$ se présentera comme fonction rationnelle entière de x à coefficients entiers du degré

$$p^{a-1}(p-1)\cdot q^{b-1}(q-1)\cdots t^{g-1}(t-1),$$

dans laquelle le coefficient du premier terme sera égal à 1.

En se proposant de prouver l'irréductibilité de cette équation et en essayant de profiter des méthodes par lesquelles on a réussi dans le cas spécial où n est un nombre premier, on trouve que ces méthodes ne suffisent, à moins que le nombre n ne soit une puissance d'un seul nombre premier (*voir* un article de M. Serret, tome XV, page 296). Car si le nombre n contient des nombres premiers inégaux, la fonction $F_n(x)$ prend un caractère tout à fait différent; et il fallait des modifications essentielles si l'on voulait adapter à ce cas les méthodes, qui ont servi pour démontrer l'irréductibilité de l'expression

$$F_p(x) = 1 + x + x^2 + \cdots + x^{p-1},$$

p étant un nombre premier. On verra, en effet, que l'irréductibilité de $F_n(x)$ revient, au fond, à une propriété de $F_m(x)$, m désignant une des puissances p^a, q^b, ..., t^g, qu'on peut énoncer brièvement en disant: *Que la fonction $F_m(x)$ ne cesse pas d'être irréductible, même en adjoignant de certains nombres complexes.* C'est cette propriété de l'expression $F_m(x)$ qui fait voir distinctement la nature des difficultés qui s'offrent en passant du cas spécial où n ne contient qu'un seul nombre premier, au cas général où n est un nombre quelconque, et c'est cette même propriété qui sera l'objet d'un théorème auxiliaire que nous allons établir.

§ I.

Théorème. — En désignant par p un nombre premier et par a un nombre entier quelconque, je dis que l'expression

$$1 + x^{p^{a-1}} + x^{2p^{a-1}} + \cdots + x^{(p-1)p^{a-1}}$$

ne peut se décomposer en facteurs d'un moindre degré, dont les coefficients soient des fonctions rationnelles d'une racine primitive de l'unité, à moins que l'exposant de cette racine ne soit divisible par p.

Démonstration. — Désignons par $f(x)$ l'expression

$$1 + x^{p^{a-1}} + x^{2p^{a-1}} + \cdots + x^{(p-1)p^{a-1}}$$

et par ω une racine primitive quelconque de l'équation $x^{p^a} = 1$, on a, comme on sait,

$$f(x) = (x-\omega^k)\cdot(x-\omega^{k'})\cdot(x-\omega^{k''})\cdots,$$

où k, k', k'', ..., sont tous les nombres entiers positifs non-divisibles par p au-dessous de p^a. Donc, si le théorème énoncé n'avait pas lieu, on aurait une équation

$$f(x) = \varphi(x)\,\psi(x), \tag{1}$$

$\varphi(x)$ et $\psi(x)$ désignant des fonctions rationnelles entières de x dont les coefficients seraient des fonctions rationnelles (entières ou fractionnaires) d'une racine primitive de l'équation

$$\varrho^{\varpi} = 1,$$

ϖ étant un nombre entier quelconque non-divisible par p. La fonction $f(x)$ ayant pour coefficient de la plus haute puissance de x l'unité, on peut supposer que les fonctions $\varphi(x)$ et $\psi(x)$ jouissent de la même propriété. Cela posé, on aura, en vertu de l'équation (1), deux équations de la forme

$$\begin{aligned} \varphi(x) &= (x-\omega^h)\cdot(x-\omega^{h'})\cdot(x-\omega^{h''})\cdots, \\ \psi(x) &= (x-\omega^i)\cdot(x-\omega^{i'})\cdot(x-\omega^{i''})\cdots, \end{aligned} \tag{2}$$

où h, h', h'', ..., i, i', i'', ... sont de certains nombres non-divisibles par p. Ensuite, il est clair qu'en faisant $x = 1$ les fonctions $\varphi(x)$ et $\psi(x)$ se réduiront à des fonctions rationnelles de la racine ϱ. On peut donc poser

$$\begin{aligned} \varphi(1) &= \frac{A + A_1\varrho + A_2\varrho^2 + \cdots + A_{r-1}\varrho^{r-1}}{M}, \\ \psi(1) &= \frac{B + B_1\varrho + B_2\varrho^2 + \cdots + B_{r-1}\varrho^{r-1}}{N}, \end{aligned} \tag{3}$$

où r désigne le degré de l'équation rationnelle *irréductible*, à laquelle satisfait la racine ϱ, et où M, N, A, A_1, A_2, ..., A_{r-1}, B, B_1, B_2, ..., B_{r-1} dé-

signent des nombres entiers, tels que M n'ait aucun diviseur commun avec *tous* les nombres $A, A_1, A_2, \ldots, A_{r-1}$ et que N n'ait aucun diviseur commun avec *tous* les nombres $B, B_1, B_2, \ldots, B_{r-1}$.

En observant que $f(1) = p$, on obtient, par l'équation (1),

$$\varphi(1)\,\psi(1) = p.$$

Donc, en remplaçant $\varphi(1)$ et $\psi(1)$ par leurs valeurs tirées de l'équation (3), et en posant, pour abréger,

$$A + A_1\varrho + A_2\varrho^2 + \cdots + A_{r-1}\varrho^{r-1} = A(\varrho),$$
$$B + B_1\varrho + B_2\varrho^2 + \cdots + B_{r-1}\varrho^{r-1} = B(\varrho),$$

on aura

$$A(\varrho)\cdot B(\varrho) = p\cdot MN. \tag{4}$$

Or, en faisant $x = 1$ dans l'une des équations (2), on obtient

$$\varphi(1) = (1-\omega^h)\cdot(1-\omega^{h'})\cdot(1-\omega^{h''})\cdots.$$

Cette égalité, élevée à la puissance p^α, peut s'écrire

$$\varphi(1)^{p^\alpha} = p\cdot X(\omega),$$

$X(\omega)$ désignant une fonction entière de ω à coefficients entiers. En effet, en ne développant que le premier facteur $(1-\omega^h)^{p^\alpha}$ suivant les puissances de ω^h, on voit aisément que le premier et le dernier terme se détruisent, p étant impair, et que la somme de ces deux termes est égale à 2, p étant lui-même égal à 2; tandis que les coefficients de tous les autres termes sont toujours divisibles par p. Donc, en faisant, pour abréger, $p^\alpha = m$, l'équation

$$\big(Z - pX(\omega)\big)\cdot\big(Z - pX(\omega^2)\big)\cdot\big(Z - pX(\omega^3)\big)\cdots\big(Z - pX(\omega^m)\big) = 0 \tag{5}$$

sera évidemment satisfaite en posant $Z = \varphi(1)^m$. Développons le premier membre de cette équation suivant les puissances de Z, le coefficient du premier terme sera égal à 1, tandis que les coefficients des autres termes contiennent des fonctions symétriques entières des quantités $\omega, \omega^2, \omega^3 \ldots, \omega^m$, c'est-à-dire de toutes les racines de l'équation $x^m = 1$, multipliées par les

diverses puissances du nombre p. Donc, comme les dites fonctions symétriques se réduisent à de simples nombres entiers, l'équation (5) prendra la forme

$$Z^m + pu_1Z^{m-1} + p^2u_2Z^{m-2} + \cdots + p^mu_m = 0,$$

$u_1, u_2, \ldots, u_m$ désignant des nombres entiers. En substituant dans cette équation la valeur

$$Z = \varphi(1)^m = \frac{A(\varrho)^m}{M^m},$$

par laquelle elle est satisfaite, on obtient une égalité de la forme suivante:

$$A(\varrho)^{m'} = p\cdot C(\varrho),$$

où $C(\varrho)$ désigne une fonction entière de ϱ à coefficients entiers; et il est évident qu'une équation de la même forme aura lieu pour toute puissance de $A(\varrho)$ dont l'exposant est plus grand que m^2. Soit donc k un nombre tel qu'on ait $p^k > m^2$ avec la condition $p^k \equiv 1 \pmod{\varpi}$, ce qui est évidemment possible, ϖ étant premier à p; alors on obtiendra une équation de la forme

$$A(\varrho)^{p^k} = p\cdot D(\varrho).$$

Or, en développant l'expression du premier membre de cette équation, il vient

$$A(\varrho)^{p^k} = A^{p^k} + A_1^{p^k}\varrho^{p^k} + A_2^{p^k}\varrho^{2p^k} + \cdots + A_{r-1}^{p^k}\varrho^{(r-1)p^k} + p\cdot E(\varrho),$$

où $D(\varrho)$ et $E(\varrho)$ désignent des fonctions entières de ϱ à coefficients entiers. Donc, en observant que $p^k \equiv 1 \pmod{\varpi}$, et que, par conséquent, $\varrho^{p^k} = \varrho$, on aura enfin

$$A^{p^k} + A_1^{p^k}\varrho + A_2^{p^k}\varrho^2 + \cdots + A_{r-1}^{p^k}\varrho^{r-1} = p\cdot D(\varrho) - p\cdot E(\varrho) = p\cdot G(\varrho), \tag{6}$$

$G(\varrho)$ désignant une fonction entière de ϱ à coefficients entiers *d'un degré quelconque*. Mais l'équation irréductible du degré r à laquelle satisfait la racine ϱ doit être un facteur de l'équation $x^\varpi - 1 = 0$; donc, en vertu d'un théorème connu (*voir Gauss, Disquisitiones arithmeticae*, sect. II, art. 42), le coefficient du premier terme x^r étant égal à 1, tous les autres coefficients sont des

nombres entiers. C'est pourquoi toute fonction rationnelle entière de ϱ à coefficients entiers peut se réduire à une fonction dont le degré est inférieur à r et dont les coefficients sont encore des nombres entiers. D'où il suit qu'on peut poser

$$G(\varrho) = G + G_1\varrho + G_2\varrho^2 + \cdots + G_{r-1}\varrho^{r-1},$$

$G, G_1, G_2, \ldots, G_{r-1}$ désignant des nombres entiers. On a donc par l'équation (6), en observant que la racine ϱ ne peut satisfaire à une équation rationnelle d'un degré inférieur à r, les égalités suivantes:

$$A^{p^k} = p \cdot G, \quad A_1^{p^k} = p \cdot G_1, \quad A_2^{p^k} = p \cdot G_2, \quad \ldots, \quad A_{r-1}^{p^k} = p \cdot G_{r-1}.$$

Il faut donc que les nombres $A, A_1, A_2, \ldots, A_{r-1}$ aient le nombre p comme diviseur commun, et, par suite, que le quotient $\frac{A(\varrho)}{p}$ soit une fonction entière de ϱ à coefficients entiers.

Par le même procédé, en partant de la seconde des équations (3), on obtiendra un résultat analogue; c'est-à-dire on trouve que les nombres $B, B_1, B_2, \ldots, B_{r-1}$ ont le diviseur commun p, et que le quotient $\frac{B(\varrho)}{p}$ est, par suite, une fonction entière de ϱ à coefficients entiers. Le produit $\frac{A(\varrho)}{p} \cdot \frac{B(\varrho)}{p}$ sera donc lui-même une fonction entière de ϱ à coefficients entiers; et en désignant cette fonction par $H(\varrho)$, l'équation (4) devient

$$p \cdot H(\varrho) = MN.$$

Or, en vertu de ce que nous avons exposé plus haut, la fonction $H(\varrho)$ peut se réduire à un degré inférieur à r, sans que les coefficients cessent d'être des nombres entiers. On aura donc, en posant

$$H(\varrho) = H + H_1\varrho + H_2\varrho^2 + \cdots + H_{r-1}\varrho^{r-1},$$

où $H, H_1, H_2, \ldots, H_{r-1}$ sont des nombres entiers,

$$p \cdot (H + H_1\varrho + H_2\varrho^2 + \cdots + H_{r-1}\varrho^{r-1}) = MN,$$

d'où l'on conclura, comme plus haut,

$$H_1 = H_2 = \cdots = H_{r-1} = 0$$

et

$$MN = p \cdot H.$$

Il faut donc qu'un des nombres M ou N soit divisible par p; mais tous les nombres $A, A_1, \ldots, A_{r-1}, B, B_1, \ldots, B_{r-1}$ sont eux-mêmes divisibles par p: un des nombres M ou N aurait donc le facteur p commun avec les nombres $A, A_1, \ldots, A_{r-1}, B, B_1, \ldots, B_{r-1}$, ce qui est contre l'hypothèse; car nous avons supposé chacune des fractions (3) tellement réduite, que le dénominateur et les nombres entiers contenus comme coefficients dans le numérateur soient dégagés de tout diviseur commun.

§ II.

Maintenant, pour démontrer l'irréductibilité de l'équation qui ne contient que les racines primitives de l'équation $x^n = 1$, n étant un nombre entier quelconque, conservons les notations employées plus haut, et soit

$$n = p^a q^b r^c \cdots t^g.$$

Puis, en désignant par ϖ le nombre $q^b r^c \cdots t^g$, supposons que l'irréductibilité de l'équation qui ne contient que les racines primitives de l'équation $x^\varpi = 1$ soit démontrée. Enfin, représentons par

$$\omega, \quad \omega_1, \quad \omega_2, \quad \ldots, \quad \omega_{\mu-1}$$

les racines primitives de l'équation $x^{p^a} = 1$, et par

$$\varrho, \quad \varrho_1, \quad \varrho_2, \quad \ldots, \quad \varrho_{r-1}$$

celles de l'équation $x^\varpi = 1$. Cela posé, l'équation dont nous allons démontrer l'irréductibilité peut s'écrire de la manière suivante

$$(1) \qquad \Pi(x - \varrho\,\omega_k) \cdot \Pi(x - \varrho_1\,\omega_k) \cdot \Pi(x - \varrho_2\,\omega_k) \cdots \Pi(x - \varrho_{r-1}\,\omega_k) = 0,$$

où tous les signes Π s'étendent à tous les indices de $k = 0$ jusqu'à $k = \mu - 1$. En observant que le produit $\Pi(x - \omega_s)$ est égal à

$$1 + x^{p^{a-1}} + x^{2p^{a-1}} + \cdots + x^{(p-1)p^{a-1}},$$

et, en désignant cette expression comme plus haut par $f(x)$, l'équation (1) prendra la forme

$$f\left(\frac{x}{\varrho}\right) \cdot f\left(\frac{x}{\varrho_1}\right) \cdot f\left(\frac{x}{\varrho_2}\right) \cdots f\left(\frac{x}{\varrho_{r-1}}\right) = 0 .$$

Le degré de cette équation est égal à μr, et pour en démontrer l'irréductibilité il suffit de prouver que tout facteur rationnel de cette équation devrait être du même degré. Soit donc $\varphi(x)$ un facteur rationnel quelconque de l'équation précédente qu'on peut évidemment supposer tel qu'il évanouit en faisant $x = \varrho\omega$. Cela posé, les équations

$$\varphi(x) = 0 \quad \text{et} \quad f\left(\frac{x}{\varrho}\right) = 0$$

auront la racine commune $x = \varrho\omega$; donc, en cherchant le plus grand commun diviseur des fonctions $\varphi(x)$ et $f\left(\frac{x}{\varrho}\right)$, on trouvera une fonction d'un degré ≥ 1 dont les coefficients ne sauraient contenir que l'irrationalité ϱ. En désignant cette fonction par $\varphi(\varrho, x)$, on aura une équation de la forme suivante:

$$f\left(\frac{x}{\varrho}\right) = \varphi(\varrho, x) \cdot \psi(\varrho, x) ;$$

ou, en faisant $x = \varrho Z$,

$$f(Z) = \varphi(\varrho, \varrho Z) \cdot \psi(\varrho, \varrho Z) .$$

Mais, en vertu du paragraphe précédent, cette équation ne peut subsister, à moins que le degré de $\varphi(\varrho, \varrho Z)$ par rapport à Z ne soit égal à celui de $f(Z)$. On voit par là que le plus grand commun diviseur des fonctions $\varphi(x)$ et $f\left(\frac{x}{\varrho}\right)$ doit être la fonction $f\left(\frac{x}{\varrho}\right)$ elle-même, et l'on aura, par suite, une équation

$$\varphi(x) = f\left(\frac{x}{\varrho}\right) \cdot \chi(\varrho, x), \tag{2}$$

où $\chi(\varrho, x)$ désigne une fonction rationnelle entière de x, dont les coefficients sont des fonctions rationnelles de ϱ. Comme nous avons supposé l'irréductibilité de l'équation dont les racines sont $\varrho, \varrho_1, \varrho_2, \ldots, \varrho_{r-1}$, on peut évidemment changer dans l'équation (2) successivement ϱ en $\varrho_1, \varrho_2, \ldots \varrho_{r-1}$; c'est dire que la fonction $\varphi(x)$ n'est pas seulement divisible par $f\left(\frac{x}{\varrho}\right)$, mais

aussi par $f\left(\frac{x}{\varrho_1}\right), f\left(\frac{x}{\varrho_2}\right), \ldots, f\left(\frac{x}{\varrho_{r-1}}\right)$. Il n'y a pas de facteur commun à deux de ces fonctions, car le produit de toutes ces quantités étant diviseur de l'expression $x^n - 1$, l'équation $x^n = 1$ aurait des racines égales, ce qui n'a pas lieu. Par conséquent, la fonction $\varphi(x)$ doit être divisible par le produit

$$f\left(\frac{x}{\varrho}\right) \cdot f\left(\frac{x}{\varrho_1}\right) \cdot f\left(\frac{x}{\varrho_2}\right) \cdots f\left(\frac{x}{\varrho_{r-1}}\right),$$

qui est du degré μr; elle ne saurait donc être d'un degré inférieur: ce qu'il fallait démontrer.

Mais toute cette démonstration est fondée sur la supposition de l'irréductibilité de l'équation qui ne contient que les racines primitives de $x^\varpi = 1$; donc, en conservant les notations employées plus haut, nous n'avons que ramené l'irréductibilité de $F_n(x)$ à celle de $F_\varpi(x)$. Cependant, par le même procédé, l'irréductibilité de $F_\varpi(x)$ se ramène à celle de $F_{\varpi'}(x)$, où $\varpi' = r^\alpha s^\beta \cdots t^\vartheta$; et en continuant ainsi l'on voit que, pour compléter la démonstration qui est l'objet de ce paragraphe, il ne s'agit, enfin, que de prouver l'irréductibilité de $F_\tau(x)$ où $\tau = t^\vartheta$. Or c'est déjà fait dans le paragraphe précédent, comme on peut s'en assurer en y faisant $p^\alpha = t^\vartheta$, $\varpi = 1$, et, par suite, $\varrho = 1$.

§ III.

La méthode que je viens d'exposer suffit encore pour démontrer le théorème plus général que voici:

Théorème. — En désignant par n un nombre entier quelconque et par α une racine d'une équation irréductible à coefficients entiers dont le premier soit égal à 1; en supposant, enfin, que le déterminant de cette équation soit premier à n; je dis que l'équation qui ne contient que les racines primitives de l'équation $x^n = 1$ reste irréductible, même en adjoignant la quantité α; c'est-à-dire, qu'elle ne peut se décomposer en facteurs dont le degré soit inférieur à celui de l'équation et dont les coefficients soient des fonctions rationnelles de la quantité α.

En effet, en conservant toujours les notations employées précédemment et en supposant que l'équation qui ne contient que les racines primitives de l'équation $\varrho^\varpi = 1$ reste irréductible en adjoignant la quantité α, on peut se

servir de la méthode exposée pour démontrer le théorème énoncé, si l'on peut prouver que:

L'expression $1 + x^{p^{a-1}} + x^{2p^{a-1}} + \cdots + x^{(p-1)p^{a-1}}$ *n'est pas décomposable en facteurs d'un moindre degré dont les coefficients soient des fonctions rationnelles des deux quantités* ϱ *et* α.

C'est donc à l'aide de ce second théorème qu'on pourra employer les conclusions du paragraphe précédent pour ramener finalement le théorème énoncé plus haut à un cas spécial du même théorème, savoir à celui où n est une puissance d'un nombre premier. Or il est visible que pour une telle valeur de n le premier théorème est en même temps un cas spécial du second théorème, savoir en y faisant $\varpi = 1$, et, par suite, $\varrho = 1$. Il ne s'agit donc que de prouver généralement ce second théorème, en supposant que l'équation $F_\varpi(x) = 0$ reste irréductible en adjoignant la quantité α. Ce qu'on peut faire comme il suit.

Supposons que le théorème en question n'ait pas lieu et conservons les notations employées dans le § I. Alors on aura, comme plus haut, les équations

$$f(x) = \varphi(x) \cdot \psi(x), \tag{1}$$

$$\begin{aligned} \varphi(x) &= (x - \omega^h)\cdot(x - \omega^k)\cdot(x - \omega^{h'})\cdots, \\ \psi(x) &= (x - \omega^i)\cdot(x - \omega^{i'})\cdot(x - \omega^{i''})\cdots, \end{aligned} \tag{2}$$

où $\varphi(x)$ et $\psi(x)$ désignent des fonctions entières de x dont les coefficients sont des fonctions rationnelles des deux quantités α et ϱ. Donc, en faisant $x = 1$, les fonctions $\varphi(x)$ et $\psi(x)$ sont réductibles à la forme suivante

$$\begin{aligned} \varphi(1) &= \frac{A(\alpha) + A_1(\alpha)\varrho + A_2(\alpha)\varrho^2 + \cdots + A_{r-1}(\alpha)\varrho^{r-1}}{M}, \\ \psi(1) &= \frac{B(\alpha) + B_1(\alpha)\varrho + B_2(\alpha)\varrho^2 + \cdots + B_{r-1}(\alpha)\varrho^{r-1}}{N}, \end{aligned} \tag{3}$$

où M et N désignent des nombres entiers, tandis que

$$A(\alpha),\ A_1(\alpha),\ A_2(\alpha),\ \ldots,\ A_{r-1}(\alpha), \qquad B(\alpha),\ B_1(\alpha),\ B_2(\alpha),\ \ldots,\ B_{r-1}(\alpha)$$

désignent des fonctions entières de α à coefficients entiers d'un degré inférieur à celui de l'équation irréductible, à laquelle satisfait la racine α.

La lettre r représente le degré de l'équation irréductible $F_\varpi(x) = 0$. En outre, on peut supposer que chacune des deux fractions (3) soit tellement réduite que le dénominateur n'ait aucun diviseur qui soit en même temps un facteur commun de tous les nombres entiers contenus comme coefficients dans le numérateur.

Or, en dénotant, pour abréger, par $A(\alpha, \varrho)$ et $B(\alpha, \varrho)$ respectivement les numérateurs des deux fractions (3), on aura, comme plus haut,

$$A(\alpha, \varrho) \cdot B(\alpha, \varrho) = p \cdot MN, \tag{4}$$

et, en suivant tout à fait la marche expliquée dans le § 1, on arrive à l'équation correspondante à celle du § I, (6),

$$A(\alpha)^{p^k} + A_1(\alpha)^{p^k}\varrho + A_2(\alpha)^{p^k}\varrho^2 + \cdots + A_{r-1}(\alpha)^{p^k}\varrho^{r-1} = p \cdot G(\alpha, \varrho), \tag{5}$$

$G(\alpha, \varrho)$ désignant une fonction rationnelle entière de α et ϱ à coefficients entiers.

En vertu de ce que nous avons dit plus haut on sait que l'équation irréductible $F_\varpi(x) = 0$, à laquelle satisfait la racine ϱ, jouit de la propriété d'avoir pour coefficients des nombres entiers et celui du premier terme égal à 1. Donc le degré de $F_\varpi(x)$ étant égal à r, la fonction $G(\alpha, \varrho)$, quel que soit son degré par rapport à ϱ, peut se réduire à la forme

$$G(\alpha, \varrho) = G(\alpha) + G_1(\alpha)\varrho + G_2(\alpha)\varrho^2 + \cdots + G_{r-1}(\alpha)\varrho^{r-1},$$

$G(\alpha)$, $G_1(\alpha)$, $G_2(\alpha)$, ..., $G_{r-1}(\alpha)$ désignant des fonctions entières de α à coefficients entiers. Donc l'équation (5) peut s'écrire

$$\begin{aligned} &A(\alpha)^{p^k} + A_1(\alpha)^{p^k}\varrho + A_2(\alpha)^{p^k}\varrho^2 + \cdots + A_{r-1}(\alpha)^{p^k}\varrho^{r-1} \\ &= pG(\alpha) + pG_1(\alpha)\varrho + pG_2(\alpha)\varrho^2 + \cdots + pG_{r-1}(\alpha)\varrho^{r-1}, \end{aligned}$$

ce qui entraîne les égalités

$$\begin{aligned} A(\alpha)^{p^k} &= pG(\alpha), \\ A_1(\alpha)^{p^k} &= pG_1(\alpha), \\ A_2(\alpha)^{p^k} &= pG_2(\alpha), \\ &\vdots \\ A_{r-1}(\alpha)^{p^k} &= pG_{r-1}(\alpha). \end{aligned} \tag{6}$$

Car nous avons supposé que l'équation $F_\varrho(x) = 0$, à laquelle satisfait la racine ϱ, reste irréductible en adjoignant la quantité α; la racine ϱ ne peut donc satisfaire à une équation d'un degré inférieur à celui de $F_\varrho(x)$ dont les coefficients soient des fonctions rationnelles de α.

Désignons maintenant par

$$\Phi(x) = 0$$

l'équation irréductible à laquelle satisfait la racine α, et par $\beta, \gamma, \ldots, \theta$ ses autres racines. Puis considérons une quelconque des égalités (6), par exemple la première, et posons, en dénotant par λ le degré de $\Phi(x)$,

$$A(\alpha) = a + b\alpha + c\alpha^2 + \cdots + l\alpha^{\lambda-1},$$

$a, b, c, \ldots, l$ désignant des nombres entiers. Alors on a, par une formule connue,

$$(7) \qquad A(Z) = \frac{A(\alpha)}{\Phi'(\alpha)} \cdot \frac{\Phi(Z)}{Z-\alpha} + \frac{A(\beta)}{\Phi'(\beta)} \cdot \frac{\Phi(Z)}{Z-\beta} + \cdots + \frac{A(\theta)}{\Phi'(\theta)} \cdot \frac{\Phi(Z)}{Z-\theta},$$

où $\Phi'(Z)$ est la fonction dérivée de $\Phi(Z)$. Désignons par Δ le déterminant de l'équation $\Phi(Z) = 0$, de sorte qu'on ait

$$\Delta = \Phi'(\alpha) \cdot \Phi'(\beta) \cdot \Phi'(\gamma) \cdots \Phi'(\theta),$$

et faisons

$$\frac{\Delta}{\Phi'(\alpha)} \cdot \frac{\Phi(Z)}{Z-\alpha} = \Psi(\alpha, Z),$$

où $\Psi(\alpha, Z)$ est évidemment une fonction rationnelle entière de α et Z à coefficients entiers. Cela posé, l'équation (7) peut s'écrire

$$\Delta \cdot a + \Delta \cdot bZ + \Delta \cdot cZ^2 + \cdots + \Delta \cdot lZ^{\lambda-1} = A(\alpha) \cdot \Psi(\alpha, Z) + A(\beta) \cdot \Psi(\beta, Z) + \cdots + A(\theta) \cdot \Psi(\theta, Z).$$

En comparant les coefficients des diverses puissances de la variable Z, on obtient, pour chacun des coefficients $a, b, c, \ldots, l$, par exemple pour le coefficient h, une équation de la forme

$$\Delta \cdot h = A(\alpha) \cdot V(\alpha) + A(\beta) \cdot V(\beta) + \cdots + A(\theta) \cdot V(\theta),$$

$V(\alpha)$ désignant une fonction entière de α à coefficients entiers. Elevons

cette égalité à la puissance p^k et réunissons ceux des termes du second membre, dont les coefficients sont divisibles par p, il en résulte une équation de la forme suivante

$$(8) \qquad \Delta^{p^k} \cdot h^{p^k} = A(\alpha)^{p^k} \cdot V(\alpha)^{p^k} + A(\beta)^{p^k} \cdot V(\beta)^{p^k} + \cdots + A(\theta)^{p^k} \cdot V(\theta)^{p^k} + p \cdot W(\alpha, \beta, \ldots, \theta),$$

où $W(\alpha, \beta, \ldots, \theta)$ désigne une fonction rationnelle entière des racines $\alpha, \beta, \ldots, \theta$ à coefficients entiers. Or il est visible que cette fonction est symétrique; elle se réduit donc à un simple nombre entier. Désignons ce nombre par P et observons que $\Phi(x) = 0$ étant irréductible, l'équation (6)

$$A(\alpha)^{p^k} = p\,G(\alpha)$$

entraîne

$$A(\beta)^{p^k} = p\,G(\beta), \quad A(\gamma)^{p^k} = p\,G(\gamma), \quad \ldots, \quad A(\theta)^{p^k} = p\,G(\theta).$$

Donc, en faisant usage de ces égalités, l'équation (8) se change en celle-ci:

$$(9) \qquad \Delta^{p^k} \cdot h^{p^k} = p \cdot (G(\alpha) \cdot V(\alpha)^{p^k} + G(\beta) \cdot V(\beta)^{p^k} + \cdots + G(\theta) \cdot V(\theta)^{p^k}) + p \cdot P.$$

L'expression contenue entre les parenthèses est une fonction entière symétrique des racines $\alpha, \beta, \ldots, \theta$ et à coefficients entiers; elle se réduit donc à un simple nombre entier; car dans l'équation $\Phi(x) = 0$ (qui a pour racines $\alpha, \beta, \ldots, \theta$), tous les coefficients sont supposés être des nombres entiers et celui du premier terme égal à 1. Par suite, l'équation (9) entraîne la congruence

$$\Delta^{p^k} h^{p^k} \equiv 0 \pmod{p},$$

et, enfin, Δ étant supposé premier au nombre n qui est divisible par p, on a

$$h \equiv 0 \pmod{p},$$

c'est-à-dire: *Il faut que tous les coefficients de $A(\alpha)$ soient divisibles par p.*

On peut conclure de la même manière que tous les coefficients contenus dans $A_1(\alpha), A_2(\alpha), \ldots, A_{r-1}(\alpha)$, de même que les coefficients contenus dans $B(\alpha), B_1(\alpha), B_2(\alpha), \ldots, B_{r-1}(\alpha)$ doivent être divisibles par p. Les

quotients $\frac{A(\alpha, \varrho)}{p}$ et $\frac{B(\alpha, \varrho)}{p}$ seront, par suite, des fonctions entières de α et ϱ à coefficients entiers. Donc, en posant

$$\frac{A(\alpha, \varrho)}{p} \cdot \frac{B(\alpha, \varrho)}{p} = H(\alpha, \varrho),$$

l'expression $H(\alpha, \varrho)$ sera elle-même une fonction entière de α et ϱ à coefficients entiers; et, à l'aide de cette égalité, l'équation (4) peut s'écrire

$$p \cdot H(\alpha, \varrho) = MN.$$

Or, en vertu de ce que nous avons dit plus haut, la fonction $H(\alpha, \varrho)$ est réductible à la forme

$$H(\alpha, \varrho) = H(\alpha) + H_1(\alpha)\varrho + H_2(\alpha)\varrho^2 + \cdots + H_{r-1}(\alpha)\varrho^{r-1},$$

$H(\alpha)$, $H_1(\alpha)$, $H_2(\alpha)$, ..., $H_{r-1}(\alpha)$ désignant des fonctions entières de α et ϱ à coefficients entiers. On a donc

$$pH(\alpha) + pH_1(\alpha)\varrho + pH_2(\alpha)\varrho^2 + \cdots + pH_{r-1}(\alpha)\varrho^{r-1} = MN;$$

en ayant égard à ce que nous avons supposé, que l'équation irréductible du degré r, dont ϱ est une racine, reste irréductible en adjoignant la quantité α, on en conclut

$$p \cdot H(\alpha) = MN. \tag{10}$$

Rappelons encore que, dans l'équation irréductible à laquelle satisfait la racine α, tous les coefficients sont supposés être des nombres entiers et celui du premier terme égal à 1. Donc, en dénotant comme plus haut par λ le degré de cette équation, l'expression $H(\alpha)$ est réductible à la forme

$$H(\alpha) = h + h_1\alpha + h_2\alpha^2 + \cdots + h_{\lambda-1}\alpha^{\lambda-1},$$

h, h_1, h_2, ..., $h_{\lambda-1}$ désignant des nombres entiers; en substituant cette valeur de $H(\alpha)$ dans l'équation (10) et en observant que la racine α ne peut satisfaire à une équation rationnelle d'un degré inférieur à λ, on arrive à l'égalité suivante

$$ph = MN.$$

Il faut donc qu'un des nombres M ou N soit divisible par p; mais nous

avons prouvé que tous les nombres contenus comme coefficients dans $A(\alpha, \varrho)$ et $B(\alpha, \varrho)$ sont divisibles par p; un des nombres M ou N aurait donc le facteur p commun avec tous les coefficients de $A(\alpha, \varrho)$ et $B(\alpha, \varrho)$, ce qui est contre l'hypothèse: car nous avons supposé chacune des fractions (3) tellement réduite que le dénominateur et les nombres entiers contenus comme coefficients dans le numérateur soient débarrassés de tout diviseur commun.

§ IV.

Nous avons assujetti dans le paragraphe précédent la quantité α à la condition d'être la racine d'une équation irréductible dont le déterminant soit premier au nombre n. Cependant on peut encore simplifier cette condition en supprimant le mot *irréductible*. Car nous allons voir que l'équation *irréductible* $\Phi(x) = 0$, dont α est une racine, remplit la condition proposée, si le déterminant d'une équation *quelconque*

$$F(x) = 0,$$

à laquelle satisfait la racine α est premier à n.

En effet, soit

$$F(x) = \Phi(x) \cdot \Psi(x),$$

$\Psi(x)$ désignant (de même que $F(x)$ et $\Phi(x)$) une fonction entière de x à coefficients entiers, dont le premier soit égal à 1. Puis dénotons, comme plus haut, par α, β, γ, ..., θ toutes les racines de l'équation $\Phi(x) = 0$, et par a, b, c, ..., k celles de l'équation $\Psi(x) = 0$. Alors, en désignant par D, Δ, Δ_1 respectivement les déterminants des équations $F(x) = 0$, $\Phi(x) = 0$, $\Psi(x) = 0$, et, en employant les notations ordinaires des dérivées de $F(x)$, $\Phi(x)$ et $\Psi(x)$, on aura l'égalité

$$D = F'(\alpha)F'(\beta)\cdots F'(\theta) \cdot F'(a)F'(b)\cdots F'(k). \tag{1}$$

Remplaçons les facteurs du second membre par leurs valeurs tirées de l'équation

$$F'(x) = \Phi'(x)\Psi(x) + \Psi'(x)\Phi(x),$$

et observons que

$$\Phi(\alpha) = \Phi(\beta) = \cdots = \Phi(\theta) = 0,$$

et semblablement

$$\Psi(a) = \Psi(b) = \cdots = \Psi(k) = 0.$$

Alors l'égalité (1) se change en celle-ci:

$$D = \Phi'(\alpha)\Psi(\alpha) \cdot \Phi'(\beta)\Psi(\beta) \cdots \Phi'(\theta)\Psi(\theta) \\ \times \Psi'(a)\Phi(a) \cdot \Psi'(b)\Phi(b) \cdots \Psi'(k)\Phi(k),$$

équation qui peut s'écrire comme il suit:

$$D = \Delta\Delta_1 \cdot \Psi(\alpha)\Psi(\beta) \cdots \Psi(\theta) \cdot \Phi(a)\Phi(b) \cdots \Phi(k).$$

Les produits dans le second membre se réduisent évidemment à de simples nombres entiers, d'où il suit que

$$D \text{ divisible par } \Delta\Delta_1.$$

Donc si D est premier à un nombre quelconque n, le déterminant Δ jouit de la même propriété; ce qu'il fallait démontrer.

D'après ce que nous venons d'exposer, on peut énoncer le théorème général du paragraphe précédent de la manière suivante:

Tous les facteurs irréductibles de l'expression $x^n - 1$ restent irréductibles même si l'on adjoint une quantité α qui satisfait à une équation à coefficients entiers dont le premier est l'unité, pourvu que le déterminant de cette équation soit un nombre premier à n.

Pour donner une seule application de ce théorème, supposons que α soit une racine primitive de l'équation $x^m = 1$. Donc, le déterminant de cette équation étant égal à m^m, les conditions du théorème seront remplies si l'on suppose que m soit premier à n. D'où l'on voit que: *tous les facteurs irréductibles de l'expression $x^n - 1$ restent irréductibles en adjoignant une racine primitive de l'unité dont l'exposant est premier à n.* Or il est visible que celui des facteurs de la fonction $x^n - 1$, que nous avons désigné par $F_n(x)$, cesse d'être irréductible si l'on adjoint une racine primitive de l'unité telle que son exposant ait un diviseur commun avec le nombre n. On a donc, enfin, ce résultat qui comprend comme cas spécial le théorème énoncé dans le § I:

Afin que l'équation qui ne contient que les racines primitives de l'équation $x^n - 1$ devienne réductible en adjoignant une racine primitive de l'unité, il faut et il suffit que l'exposant de cette racine ait un diviseur commun avec le nombre n.

DÉMONSTRATION D'UN THÉORÈME DE M. KUMMER;

PAR

M. Léopold KRONECKER.

Liouville, Journal de mathématiques pures et appliquées, Sér. II, Tome 1 p. 396—398.

DÉMONSTRATION D'UN THÉORÈME DE M. KUMMER.

Dans son Mémoire sur la Théorie des nombres complexes composés de racines $\lambda^{ièmes}$ de l'unité et de nombres entiers, *M. Kummer* a donné le théorème important que voici*):

La condition nécessaire et suffisante pour que le premier facteur du nombre des classes H soit divisible par λ, consiste en ce qu'un quelconque des $\frac{\lambda-3}{2}$ premiers nombres bernoulliens soit divisible par λ.

On peut démontrer ce théorème d'une manière très-simple. En effet, si l'on conserve les notations de *M. Kummer***), tout se réduit à examiner si la congruence

$$\psi(\gamma^{2n-1}) = b_0 + b_1\gamma^{2n-1} + \cdots + b_{\lambda-2}\cdot\gamma^{(\lambda-2)\cdot(2n-1)} \equiv 0 \pmod{\lambda},$$

est ou n'est pas satisfaite pour une quelconque des valeurs de

$$n = 1, 2, 3, \ldots, \mu.$$

Donc, puisqu'on a***)

$$\lambda b_k = \gamma\gamma_{k-1} - \gamma_k,$$

il s'agit d'examiner la congruence

---

*) *Voir* ce Journal, tome XVI, page 479.
**) *Voir* ce Journal, tome XVI, page 475.
***) *Voir* ce Journal, tome XVI, page 474.

(I) $$\lambda \cdot \psi(\gamma^{2n-1}) = \Sigma(\gamma\gamma_{k-1} - \gamma_k)\cdot\gamma^{(2n-1)k} \equiv 0 \pmod{\lambda^2},$$

où le signe de sommation s'étend à toutes les valeurs de

$$k = 0, 1, 2, 3, \ldots, (\lambda - 2).$$

Partons de l'égalité identique

$$\gamma^k - (\gamma^k - \gamma_k) = \gamma_k.$$

En élevant les deux membres à la puissance $2n$ et en observant que le nombre entier $(\gamma^k - \gamma_k)$ est un multiple de λ, on obtient la congruence

$$\gamma^{2nk} - 2n\gamma^{(2n-1)k}(\gamma^k - \gamma_k) \equiv \gamma_k^{2n}, \pmod{\lambda^2},$$

ou

$$(1-2n)\gamma^{2nk} + 2n\gamma_k\gamma^{(2n-1)k} \equiv \gamma_k^{2n} \pmod{\lambda^2}.$$

Remplaçons k par $(k-1)$ et multiplions par γ^{2n}, il vient

$$(1-2n)\gamma^{2nk} + 2n\gamma_{k-1}\gamma^{(2n-1)k+1} \equiv \gamma^{2n}\gamma_{k-1}^{2n} \pmod{\lambda^2}.$$

En retranchant de cette congruence celle qui précède, on obtient

$$2n(\gamma\gamma_{k-1} - \gamma_k)\gamma^{(2n-1)k} \equiv \gamma^{2n}\gamma_{k-1}^{2n} - \gamma_k^{2n} \pmod{\lambda^2}.$$

Donc on aura de même

$$2n\,\Sigma(\gamma\gamma_{k-1} - \gamma_k)\gamma^{(2n-1)k} \equiv \gamma^{2n}\Sigma\gamma_{k-1}^{2n} - \Sigma\gamma_k^{2n} \pmod{\lambda^2}.$$

Or, comme les nombres $\gamma_0, \gamma_1, \gamma_2, \ldots, \gamma_{\lambda-2}$ et $1, 2, 3, \ldots, (\lambda-1)$ sont les mêmes à l'ordre près, on a enfin

(II) $$2n\,\Sigma(\gamma\gamma_{k-1} - \gamma_k)\gamma^{(2n-1)k} \equiv (\gamma^{2n}-1)\cdot(1^{2n} + 2^{2n} + \cdots + (\lambda-1)^{2n}) \pmod{\lambda^2}.$$

Le nombre $2n$ est moindre que λ. On voit donc que la discussion de la congruence (I) se réduit à la question si le second membre de la congruence (II) est divisible par λ^2. Cela n'a pas lieu pour la valeur

$$2n = 2\mu = \lambda - 1.$$

Car, suivant l'hypothèse (faite par *M. Kummer*) que $\gamma^\mu + 1$ ne soit pas divisible par λ^2, le nombre $(\gamma^{2\mu} - 1)$ ne contiendra qu'*une* fois le facteur λ, et, en vertu du théorème de Fermat, la somme

$$1^{\lambda-1} + 2^{\lambda-1} + \cdots + (\lambda-1)^{\lambda-1}$$

sera congrue à -1 suivant le module λ. Ensuite, pour décider si le produit

$$(\gamma^{2n} - 1)\cdot(1^{2n} + 2^{2n} + \cdots + (\lambda-1)^{2n})$$

est divisible par λ^2 pour une des valeurs de $n = 1, 2, \ldots, (\mu-1)$, observons que, dans ces cas, le nombre $(\gamma^{2n} - 1)$ n'est pas divisible par λ, et que l'expression connue de la somme

$$1^{2n} + 2^{2n} + \cdots + (x-1)^{2n}$$

en fonction rationnelle entière de x, fournit la congruence

$$1^{2n} + 2^{2n} + \cdots + (\lambda-1)^{2n} \equiv \pm B_n\cdot\lambda \pmod{\lambda^2},$$

B_n désignant le nombre bernoullien $n^{ième}$. Donc, pour que la congruence (I) ait lieu pour une quelconque des valeurs de

$$n = 1, 2, 3, \ldots, \mu,$$

il faut et il suffit que la congruence

$$B_n \equiv 0 \pmod{\lambda}$$

soit satisfaite pour une quelconque des valeurs de $n = 1, 2, \ldots, (\mu-1)$; ce qu'il fallait démontrer.

DÉMONSTRATION DE L'IRRÉDUCTIBILITÉ DE L'ÉQUATION $x^{n-1}+x^{n-2}+\cdots+1=0$, OU n DÉSIGNE UN NOMBRE PREMIER;

PAR

M. LÉOPOLD KRONECKER.

Liouville, Journal de mathématiques pures et appliquées, Sér. II, Tome 1 p. 399—400.

DÉMONSTRATION DE L'IRRÉDUCTIBILITÉ DE L'ÉQUATION $x^{n-1}+x^{n-2}+\cdots+1=0$, OU n DÉSIGNE UN NOMBRE PREMIER.

Si l'expression $x^{n-1}+x^{n-2}+\cdots+1$ était le produit de deux polynômes à coefficients entiers $\varphi(x)$ et $\psi(x)$, on obtiendrait, en faisant $x=1$, l'équation

$$n=\varphi(1)\cdot\psi(1).$$

Il résulte de là que l'un des nombres entiers $\varphi(1)$ et $\psi(1)$ doit être égal à ± 1 et l'autre à $\pm n$. Supposons que l'on ait

$$\varphi(1)=\pm 1.$$

Puis désignons par m_k un nombre entier positif tel que la congruence

$$k\cdot m_k \equiv 1 \pmod{n}$$

soit satisfaite, k étant un quelconque des nombres $1, 2, 3, \ldots, n-1$. Enfin soit ω une des racines de l'équation

$$x^{n-1}+x^{n-2}+\cdots+1=0,$$

qui font évanouir le facteur $\varphi(x)$. Cela posé, on aura l'égalité

$$\varphi(\omega^{k\cdot m_k})=\varphi(\omega)=0.$$

D'où l'on voit que l'expression $\varphi(x^{m_k})$ s'annule pour $x=\omega^k$, c'est-à-dire qu'elle contient le facteur $x-\omega^k$. Donc le produit

(I) $$\varphi(x^{m_1})\cdot\varphi(x^{m_2})\cdots\varphi(x^{m_{n-1}})$$

sera divisible par

$$(x-\omega)\cdot(x-\omega^2)\cdots(x-\omega^{n-1}),$$

c'est-à-dire

$$x^{n-1}+x^{n-2}+\cdots+1.$$

Ce produit est une fonction entière de x à coefficients entiers. Par suite, en désignant cette fonction par $P(x)$, le quotient qu'on obtient en divisant $P(x)$ par $x^{n-1}+x^{n-2}+\cdots+1$ sera lui-même une fonction entière de x à coefficients entiers. Or, si l'on fait $x=1$, il en résulte que le quotient $\frac{P(1)}{n}$ devrait être égal à un nombre entier; ce qui est impossible, car nous avons supposé que l'on a

$$\varphi(1)=\pm 1,$$

et par suite

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

On voit aisément qu'on peut appliquer le même raisonnement à l'équation qui ne contient que les racines primitives de l'équation x^n-1, si n est une puissance d'un nombre premier.

ZWEI SÄTZE ÜBER GLEICHUNGEN MIT GANZZAHLIGEN COEFFICIENTEN.

VON

L. KRONECKER

ZU BERLIN.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 53, S. 173—175.

ZWEI SÄTZE ÜBER GLEICHUNGEN MIT GANZZAHLIGEN COEFFICIENTEN.

I. Wenn die Wurzeln einer ganzzahligen Gleichung, in welcher der erste Coefficient *Eins* ist, alle imaginär und ihre analytischen Moduln sämmtlich gleich *Eins* sind, so müssen dieselben stets Wurzeln der Einheit sein.

Beweis. Es seien

$$a,\ b,\ c,\ \ldots$$

die Wurzeln der Gleichung:

$$F(x) = x^n - Ax^{n-1} + Bx^{n-2} - Cx^{n-3} + \cdots \pm N = 0\,,$$

in welcher $A,\ B,\ C,\ \ldots N$ ganze Zahlen bedeuten. Da nun die Wurzeln $a,\ b,\ c,\ \ldots$ lauter imaginäre Grössen mit dem Modul *Eins* sein sollen, so setze man, indem man $\sqrt{-1}$ mit i bezeichnet:

$$a = \cos\alpha + i\sin\alpha,\quad b = \cos\beta + i\sin\beta,\quad c = \cos\gamma + i\sin\gamma,\ \ldots\ .$$

Alsdann erhält man, wenn die Coefficienten $A,\ B,\ C,\ \ldots$ durch die Wurzeln ausgedrückt werden:

$$\begin{aligned} A &= \cos\alpha + \cos\beta + \cos\gamma + \cdots,\\ B &= \cos(\alpha+\beta) + \cos(\alpha+\gamma) + \cos(\alpha+\delta) + \cdots,\\ C &= \cos(\alpha+\beta+\gamma) + \cos(\alpha+\beta+\delta) + \cdots,\\ &\ \ \vdots \qquad\qquad\qquad \vdots\ . \end{aligned}$$

Also muss A gleich einer Summe von n Grössen sein, deren jede nicht kleiner als -1 und nicht grösser als $+1$ ist. Ebenso muss B gleich einer Summe von $\frac{n(n-1)}{1\cdot 2}$ solchen Grössen sein, C gleich einer Summe von $\frac{n(n-1)(n-2)}{1\cdot 2\cdot 3}$ solchen Grössen u. s. w. Da aber A, B, C, ... ganze Zahlen sein sollen, so sieht man, dass jeder Coefficient der Gleichung $F(x)=0$ nur eine begrenzte Anzahl von Werthen haben kann; und das Product aller dieser Anzahlen giebt offenbar die Anzahl aller derjenigen Werth*systeme* an, welche den Coefficienten A, B, C, ... überhaupt zukommen können. Hieraus geht hervor, *dass es für jeden bestimmten Grad n nur eine endliche Anzahl von Gleichungen geben kann, welche die im obigen Satze angegebenen Bedingungen erfüllen.*

Die Anzahl aller dieser Gleichungen n^{ten} Grades sei r, und es sei ferner für irgend eine ganze Zahl k:

$$F_k(x) = (x-a^k)\cdot(x-b^k)\cdot(x-c^k)\cdots .$$

Dann genügt auch die Gleichung $F_k(x)=0$ allen in dem obigen Satze gemachten Voraussetzungen. Denn erstens sind die Coefficienten dieser Gleichung als symmetrische Functionen von a, b, c, ... offenbar ganze Zahlen, und zweitens sind die analytischen Moduln ihrer Wurzeln:

$$a^k = \cos k\alpha + i\sin k\alpha,\quad b^k = \cos k\beta + i\sin k\beta,\quad c^k = \cos k\gamma + i\sin k\gamma,\quad \ldots$$

sämmtlich gleich *Eins*. Folglich müssen mindestens zwei unter den Gleichungen:

$$F(x)=0,\quad F_2(x)=0,\quad F_3(x)=0,\quad \ldots,\quad F_{r+1}(x)=0$$

identisch sein, d. h. es muss zwei von einander verschiedene Zahlen h und k geben, für welche $F_h(x)=F_k(x)$ ist. Die Wurzeln der Gleichung $F_h(x)=0$, nämlich:

$$a^h,\ b^h,\ c^h,\ \ldots$$

müssen daher mit den Wurzeln der Gleichung $F_k(x)=0$, nämlich mit:

$$a^k,\ b^k,\ c^k,\ \ldots,$$

abgesehen von der Ordnung, übereinstimmen.

Für irgend eine Grösse der ersten Reihe z. B. a^h sei nun b^k diejenige aus der zweiten Reihe, welche derselben gleich wird, so dass $a^h=b^k$ ist. Ebenso sei c^k diejenige unter den $(n-1)$ noch übrig bleibenden Grössen a^k, c^k, d^k, ... der zweiten Reihe, die gleich b^h, d^k diejenige von den $(n-2)$ Grössen a^k, d^k, ..., welche gleich c^h ist u. s. w. Wenn man so fortfährt, muss man offenbar auch zu einer Gleichung kommen, in welcher a^k auf der rechten Seite steht. Man erhält also ein System von Gleichungen von folgender Form:

$$a^h = b^k,\quad b^h = c^k,\quad c^h = d^k,\quad \ldots,\quad m^h = a^k.$$

Wird die Anzahl dieser Gleichungen mit μ bezeichnet, und eliminirt man aus denselben die $(\mu-1)$ Grössen: b, c, d, ... m, so erhält man, wie leicht zu sehen:

$$a^{h^\mu - k^\mu} = 1.$$

Da nun, wie oben bemerkt, h und k von einander verschiedene ganze Zahlen sind, so zeigt diese Gleichung, dass a in der That eine Wurzel der Einheit ist; und dieses Resultat gilt offenbar für *alle* Wurzeln der Gleichung $F(x)=0$, da a ganz beliebig unter denselben gewählt worden ist.

II. Wenn eine Gleichung mit ganzzahligen Coefficienten, von denen der erste gleich *Eins* ist, lauter reelle Wurzeln hat, die in den Grenzen -2 und $+2$ liegen, die also durch

$$2\cos\alpha,\quad 2\cos\beta,\quad 2\cos\gamma,\quad \ldots$$

dargestellt werden können, so stehen die Winkel α, β, γ ... sämmtlich in commensurablem Verhältniss zu einem Rechten.

Beweis. Es sei

$$\Phi(y)=0$$

eine Gleichung von den angegebenen Eigenschaften, und

$$2\cos\alpha,\quad 2\cos\beta,\quad 2\cos\gamma,\quad \ldots$$

die Wurzeln derselben. Wenn man nun den Grad von $\Phi(y)$ mit ν bezeichnet, und man setzt:

$$x^{\nu} \cdot \Phi\left(x + \frac{1}{x}\right) = F(x),$$

so ist $F(x) = 0$ offenbar eine Gleichung, in welcher alle Coefficienten ganze Zahlen sind und der erste derselben gleich *Eins*. Ferner sieht man leicht, dass die Wurzeln dieser Gleichung:

$$\cos\alpha \pm i\sin\alpha, \quad \cos\beta \pm i\sin\beta, \quad \cos\gamma \pm i\sin\gamma, \quad \ldots$$

sind, also lauter imaginäre Grössen mit dem Modul *Eins*. Somit genügt die Gleichung $F(x) = 0$ allen in dem obigen ersten Satze aufgestellten Bedingungen, und durch Anwendung desselben ergiebt sich, dass die Wurzeln:

$$\cos\alpha \pm i\sin\alpha, \quad \cos\beta \pm i\sin\beta, \quad \ldots$$

sämmtlich Wurzeln der Einheit sein müssen; ein Resultat, aus welchem die zu beweisende Eigenschaft der Winkelgrössen $\alpha, \beta, \gamma, \ldots$ unmittelbar hervorgeht.

ÜBER COMPLEXE EINHEITEN.

VON

L. KRONECKER.

Crelle, Journal für die reine und angewandte Mathematik, Bd. 53, S. 176—181.

ÜBER COMPLEXE EINHEITEN.

Es ist von Herrn *Kummer* zuerst gezeigt worden, dass, wenn λ eine ungrade Primzahl ist, jede complexe Zahl, welche aus Wurzeln der Gleichung: $x^\lambda = 1$ gebildet, und deren Norm gleich *Eins* ist, durch Multiplication mit einer dieser Wurzeln reell gemacht werden kann. Die dabei von Herrn *Kummer* gegebene Beweismethode dürfte indess kaum zu einer Anwendung auf den Fall geeignet sein, in welchem λ eine beliebige zusammengesetzte Zahl ist. Ich werde nun im Folgenden mit Hülfe ganz andrer Principien die analoge Eigenschaft der complexen Einheiten für diesen allgemeineren Fall herleiten; eine Eigenschaft, die noch dadurch ein besonderes Interesse erhält, dass die Kenntniss derselben bei der Anwendung der Theorie der complexen Zahlen auf algebraische Untersuchungen als unumgänglich nöthig erscheint.

Bezeichnet man mit n eine ganze Zahl, welche entweder ungrade oder durch 4 theilbar ist, und mit $a, b, c, \ldots$ alle diejenigen unter den Zahlen $2, 3, 4, \ldots n-1$, welche relative Primzahlen zu n sind, so sind bekanntlich:

$$\omega,\ \omega^a,\ \omega^b,\ \omega^c,\ \ldots$$

die *sämmtlichen* primitiven Wurzeln der Gleichung: $x^n = 1$, wenn ω irgend eine derselben bedeutet*). Ferner sind in der Gleichung:

*) Der Fall, wo $n = 2m$ und m ungrade ist, wird deshalb ausgeschlossen, weil für solche Werthe von n eine primitive n^{te} Wurzel der Einheit sich auf eine primitive m^{te} Wurzel der Einheit, mit negativem Vorzeichen genommen, reducirt; so dass also in diesem Falle die aus Wurzeln der Gleichung: $x^n = 1$ gebildeten complexen Zahlen stets als solche betrachtet werden können, welche aus Wurzeln der Gleichung: $x^m = 1$ zusammengesetzt sind.

(I.) $$(x-\omega)\cdot(x-\omega^a)\cdot(x-\omega^b)\cdot(x-\omega^c)\cdots = 0$$

die Coefficienten der verschiedenen Potenzen von x sämmtlich ganze Zahlen, und es folgt hieraus, dass jede ganze symmetrische Function der Grössen $\omega, \omega^a, \omega^b, \ldots$, mit ganzzahligen Coefficienten, einer ganzen Zahl gleich ist. Endlich erinnere ich noch daran, dass die Gleichung (I) (wie ich in einem im 19ten Bande des *Liouville*'schen Journals abgedruckten Aufsatze[1]) bewiesen habe) irreductibel ist, und dass daher jede Gleichung, welche ausser ω nur ganze Zahlen enthält, noch gültig bleiben muss, wenn für die Grösse ω irgend eine Potenz derselben substituirt wird, deren Exponent relative Primzahl zu n ist.

Dies vorausgeschickt, können nunmehr die üblichen Benennungen und Zeichen ohne Weiteres auf die aus n^{ten} Wurzeln der Einheit gebildeten complexen Zahlen übertragen werden. Wenn nämlich $f(\omega)$ irgend eine solche complexe Zahl d. h. eine ganze ganzzahlige Function von ω ist, so sollen:

$$f(\omega),\ f(\omega)^a,\ f(\omega)^b\cdots,$$

„die einander conjugirten complexen Zahlen" heissen, und das Product derselben soll *„die Norm"* von $f(\omega)$ genannt und mit: $Nf(\omega)$ bezeichnet werden. Diese Norm ist, weil sie die Wurzeln $\omega, \omega^a, \omega^b, \ldots$ symmetrisch enthält, eine ganze Zahl. Ferner sollen diejenigen ganzen complexen Zahlen, deren Norm gleich *Eins* ist, *„complexe Einheiten"*, und die einfachsten unter denselben, nämlich:

$$\pm 1,\ \pm\omega,\ \pm\omega^2,\ \pm\omega^3,\ \ldots,\ \pm\omega^{n-1}$$

„einfache Einheiten" heissen.

Wenn nun $E(\omega)$ irgend eine complexe Einheit bedeutet, so wird das in Bezug auf $\omega, \omega^a, \omega^b, \ldots$ symmetrische Product:

(II.) $$\left(x\cdot E(\omega)-E(\omega^{-1})\right)\cdot\left(x\cdot E(\omega^a)-E(\omega^{-a})\right)\cdot\left(x\cdot E(\omega^b)-E(\omega^{-b})\right)\cdots$$

[1]) *Liouville*, Journal de mathématiques I, tome 19, pag. 177—192. S. 75—92 dieser Ausgabe von *L. Kronecker's* Werken. H.

nach Potenzen von x entwickelt, offenbar eine ganze ganzzahlige Function von x ergeben, in welcher der Coefficient der höchsten Potenz von x die Norm von $E(\omega)$ also *Eins* ist. Bezeichnet man diese Function, oder, was dasselbe ist, das Product (II.) mit $F(x)$, so sind:

$$\frac{E(\omega^{-1})}{E(\omega)},\ \frac{E(\omega^{-a})}{E(\omega^a)},\ \frac{E(\omega^{-b})}{E(\omega^b)},\ \ldots$$

die sämmtlichen Wurzeln der Gleichung: $F(x)=0$; und da die analytischen Moduln aller dieser Wurzeln gleich *Eins* sind, so erfüllt, wie man sieht, die Gleichung: $F(x)=0$ alle Bedingungen des ersten der beiden Sätze, welche ich in der vorstehenden Abhandlung[1]) bewiesen habe. Es muss daher eine ganze Zahl m geben, für welche

$$\left(\frac{E(\omega^{-1})}{E(\omega)}\right)^m = 1$$

ist. — Wenn man nun mit ϱ irgend eine primitive Wurzel der Gleichung:

$$x^{m\cdot n}=1$$

bezeichnet, so lässt sich bekanntlich jede m^{te} und jede n^{te} Wurzel der Einheit als Potenz von ϱ darstellen. Es sei demnach ϱ^r diejenige m^{te} Wurzel der Einheit, welcher $\frac{E(\omega^{-1})}{E(\omega)}$ gleich wird, so dass:

(III.) $$E(\omega^{-1}) = \varrho^r\cdot E(\omega),$$

und es sei ferner $\omega=\varrho^\lambda$, also:

$$E(\varrho^{-\lambda}) = \varrho^r\cdot E(\varrho^\lambda).$$

In dieser Gleichung kann — wenn das, was ich oben über die Eigenschaften der Gleichung der primitiven n^{ten} Wurzeln der Einheit gesagt habe, auf die primitiven Wurzeln der Gleichung: $x^{m\cdot n}=1$ angewendet wird — für ϱ auch ϱ^r gesetzt werden, sobald r relative Primzahl zu $m\cdot n$ ist. Wenn dies geschieht, und alsdann für ϱ^λ wieder ω eingesetzt wird, so erhält man:

[1]) S. 103—108 dieser Ausgabe von *L. Kronecker's* Werken. H.

$$E(\omega^{-r}) = \varrho^{r \cdot \nu} \cdot E(\omega^r).$$

Die Gleichung (III.), zur r^{ten} Potenz erhoben, giebt aber:

$$E(\omega^{-1})^r = \varrho^{r \cdot \nu} \cdot E(\omega)^r,$$

und die Combination der beiden vorstehenden Gleichungen:

(IV.) $$E(\omega^r) \cdot E(\omega^{-1})^r = E(\omega^{-r}) \cdot E(\omega)^r,$$

welche Gleichung, wie ich nochmals erwähne, für *jede* Zahl r gültig sein muss, die relative Primzahl zu $m \cdot n$ ist.

Bezeichnet man nun mit μ den grössten aller derjenigen Divisoren von m, welche relative Primzahlen zu n sind (so dass also auch $\mu = 1$ sein kann), so ist leicht zu sehen, dass die Zahlen $\mu - n$, $\mu + n$ und, wenn n grade ist, auch $\mu + 2n$ relative Primzahlen zu m und n sind. Man kann also in der Gleichung (IV.) für r diese drei Zahlen nach einander einsetzen und erhält dann, wenn man berücksichtigt, dass $\omega^{\mu-n}$, $\omega^{\mu+n}$, $\omega^{\mu+2n}$ sämmtlich gleich ω^{μ}, und $\omega^{-\mu+n}$, $\omega^{-\mu-n}$, $\omega^{-\mu-2n}$ sämmtlich gleich $\omega^{-\mu}$ sind:

$$E(\omega^{\mu}) \cdot E(\omega^{-1})^{\mu-n} = E(\omega^{-\mu}) \cdot E(\omega)^{\mu-n},$$
$$E(\omega^{\mu}) \cdot E(\omega^{-1})^{\mu+n} = E(\omega^{-\mu}) \cdot E(\omega)^{\mu+n},$$
$$E(\omega^{\mu}) \cdot E(\omega^{-1})^{\mu+2n} = E(\omega^{-\mu}) \cdot E(\omega)^{\mu+2n}.$$

Die letzte dieser drei Gleichungen gilt aber nur, wenn n grade ist. Dividirt man dieselbe durch die zweite, so erhält man für diesen Fall:

$$E(\omega^{-1})^n = E(\omega)^n,$$

und wenn man die Wurzel auszieht:

(V.) $$E(\omega^{-1}) = \omega^k \cdot E(\omega),$$

wo k eine ganze Zahl bedeutet. Ferner erhält man für den Fall, wo n ungrade ist, indem man die zweite jener drei Gleichungen durch die erste dividirt:

$$E(\omega^{-1})^{2n} = E(\omega)^{2n},$$

und wenn man die Wurzel auszieht:

(VI.) $$E(\omega^{-1}) = \pm \omega^h \cdot E(\omega),$$

wo h eine ganze Zahl ist. Man sieht also, *dass, sowohl wenn n grade als wenn es ungrade ist, jede aus n^{ten} Wurzeln der Einheit gebildete complexe Einheit, durch die reciproke dividirt, als Quotient eine einfache Einheit ergiebt.*

Mit Hülfe dieses Resultats lässt sich nunmehr folgender Satz beweisen:

„Jede complexe, aus Wurzeln der Gleichung $x^n = 1$ gebildete Einheit kann durch „Multiplication mit einer Wurzel der Einheit reell gemacht werden. In dem „Falle, wo n die Potenz einer einfachen Primzahl ist, sind die n^{ten} Wurzeln „der Einheit selbst hierzu im Allgemeinen erforderlich und stets ausreichend. „Enthält aber die Zahl n verschiedene Primfactoren, so bedarf man, wenn n „grade ist, noch der $2n^{ten}$, und, wenn n ungrade ist, noch der $4n^{ten}$ Wurzeln „der Einheit.“

Ich werde *zuerst* darthun, dass in den drei unterschiedenen Fällen die erwähnten Arten von Wurzeln der Einheit im Allgemeinen *erforderlich* sind. Zu diesem Behufe werde ich für jeden der drei Fälle eine specielle Einheit $e(\omega)$ angeben und in Bezug auf diese zeigen, dass eine Wurzel der Einheit v, für welche $v \cdot e(\omega)$ reell wird, nicht zu einem kleineren Exponenten als resp. zu n, $2n$ und $4n$ gehören kann.

Im ersten Falle, wo n eine Primzahlpotenz ist, nehme man für $e(\omega)$ die complexe Einheit:

$$1 + \omega + \omega^2 + \cdots + \omega^{n-2}.$$

Wenn nun $v \cdot e(\omega)$ reell sein soll, so muss offenbar:

$$v \cdot e(\omega) = v^{-1} \cdot e(\omega^{-1})$$

sein, also:

$$v^2 = \frac{e(\omega^{-1})}{e(\omega)}.$$

Setzt man hierin für $e(\omega)$ und $e(\omega^{-1})$ ihre Werthe, so erhält man:

$$v^2 = \omega^2,$$

woraus unmittelbar hervorgeht, dass keine niedrigere Potenz von v als die n^{te} gleich *Eins* werden kann.

In den andern beiden Fällen, wo n verschiedene Primzahlen enthält, ist, wie leicht zu sehen, $(1-\omega)$ eine Einheit. Soll diese nun durch Multiplication mit einer Wurzel der Einheit v reell werden, so muss

$$v\cdot(1-\omega) = v^{-1}\cdot(1-\omega^{-1})$$

sein, also:

$$v^2 = -\omega^{-1}.$$

Für ein *grades* n wird: $(-\omega^{-1})^n = 1$, also $v^{2n} = 1$, und es ist dies auch offenbar die *niedrigste* Potenz von v, welche gleich *Eins* wird, weil sonst auch eine niedrigere Potenz von $(-\omega^{-1})$ als die n^{te} gleich *Eins* werden müsste. Wenn aber n ungrade ist, so ist klar, dass erst die $2n^{te}$ Potenz von $(-\omega^{-1})$ gleich *Eins* wird, dass also, da $v^2 = -\omega^{-1}$ ist, erst die $4n^{te}$ Potenz von v gleich *Eins* werden kann.

Ich werde nunmehr *zweitens* zeigen, dass die in dem obigen Satze angegebenen Arten von Wurzeln der Einheit stets *ausreichend* sind, um durch Multiplication mit denselben jede complexe Einheit reell zu machen. Zu diesem Zwecke werde ich der Reihe nach beweisen, dass

1) wenn n grade ist, stets Wurzeln der Gleichung: $x^{2n} = 1$, aber, wenn es eine Potenz von 2 ist, schon Wurzeln der Gleichung: $x^n = 1$ ausreichen, und dass

2) wenn n ungrade ist, stets Wurzeln der Gleichung $x^{4n} = 1$, aber, wenn es Primzahlpotenz ist, schon Wurzeln der Gleichung: $x^n = 1$ ausreichen.

Es erschöpft dies offenbar alle in dem Texte des zu beweisenden Satzes angegebenen Resultate, die ich aber dort um der bessern Uebersichtlichkeit willen theils zusammengefasst, theils anders angeordnet habe.

1. Die Gleichung (V.), welche sich für jede Einheit $E(\omega)$ als nothwendig ergeben hatte, wenn n grade angenommen wurde, lässt sich offenbar in folgender Form darstellen:

$$\omega^{-\frac{k}{2}}\cdot E(\omega^{-1}) = \omega^{\frac{k}{2}}\cdot E(\omega). \tag{VII.}$$

Hieraus ersieht man sofort, dass in dem vorliegenden Falle, wo n grade ist, stets eine Wurzel der Einheit: $\omega^{\frac{k}{2}}$ d. h. also eine gewisse Wurzel der Gleichung: $x^{2n} = 1$ ausreicht, um durch Multiplication mit derselben eine Einheit $E(\omega)$ reell zu machen. Die Gleichung (VII.) zeigt aber ferner, dass schon eine n^{te} Wurzel der Einheit ausreicht, wenn der Exponent $\frac{k}{2}$ eine ganze Zahl, also wenn k *grade* ist. Dies muss nun stets der Fall sein, wenn n eine Potenz von 2 ist. Wäre nämlich in diesem Falle $k = 2h-1$, so hätte man die Gleichung (VII.) in folgender Form:

$$\omega\cdot\omega^{-h}\cdot E(\omega^{-1}) = \omega^h\cdot E(\omega)$$

also:

$$\omega^{-h}\cdot E(\omega^{-1}) - \omega^h\cdot E(\omega) = (1-\omega)\cdot\omega^{-h}\cdot E(\omega^{-1}).$$

Diese Gleichung kann aber nicht stattfinden; denn wenn man auf beiden Seiten die Norm nimmt, so erhält man, da die linke Seite offenbar durch $(\omega^{-1}-\omega)$ theilbar ist, als Norm derselben ein ganzes Vielfaches von: $N(\omega^{-1}-\omega)$ d. h. von 4, während die Norm der rechten Seite nur $N(1-\omega)$ d. h. gleich 2 wird.

2. Die Gleichung (VI.), welche sich für jede Einheit $E(\omega)$ als nothwendig ergeben hatte, wenn n ungrade angenommen wurde, lautete:

$$E(\omega^{-1}) = \pm\,\omega^h\cdot E(\omega).$$

Diese Gleichung verwandelt sich, wenn man eine Zahl k durch die Congruenz $h \equiv 2k \pmod{n}$ bestimmt, in folgende:

$$\omega^{-k}\cdot E(\omega^{-1}) = \pm\,\omega^k\cdot E(\omega). \tag{VIII.}$$

Hieraus ergiebt sich, dass $E(\omega)$ entweder mit ω^k oder mit $\omega^k\cdot\sqrt{-1}$ multi-

plicirt reell wird, also, dass für ein ungrades n allemal eine Wurzel der Gleichung: $x^{4n}=1$ ausreicht, um durch Multiplication mit derselben eine complexe Einheit $E(\omega)$ reell zu machen. Die Gleichung (VIII.) zeigt ferner, dass, wenn auf der rechten Seite das *obere* Zeichen gilt, schon eine Potenz von ω d. h. eine n^{te} Wurzel der Einheit ausreichend ist. Dies ist stets der Fall, wenn n eine Primzahlpotenz: p^r ist. Denn wäre alsdann:

$$\omega^{-k}\cdot E(\omega^{-1}) = -\omega^{k}\cdot E(\omega),$$

so würde die Gleichung

$$\omega^{k}\cdot E(\omega) - \omega^{-k}\cdot E(\omega^{-1}) = 2\omega^{k}\cdot E(\omega)$$

unmittelbar daraus folgen. Diese Gleichung kann aber nicht stattfinden; denn, wenn man auf beiden Seiten die Norm nimmt, so erhält man, da die linke Seite offenbar durch $(\omega-\omega^{-1})$ theilbar ist, als Norm derselben ein ganzes Vielfaches von $N(\omega-\omega^{-1})$ d. h. von p, während die Norm der rechten Seite nur einer Potenz von 2 gleich wird. Da aber p eine ungrade Primzahl bedeutet, so ist dies unmöglich.

Hiermit ist der über die Realität der complexen Einheiten aufgestellte Satz in allen seinen Theilen bewiesen.

ÜBER CUBISCHE GLEICHUNGEN MIT RATIONALEN COEFFICIENTEN.

VON

L. KRONECKER.

Crelle, Journal für die reine und angewandte Mathematik Bd. 56 S. 188.

ÜBER CUBISCHE GLEICHUNGEN MIT RATIONALEN COEFFICIENTEN.

Das letzte *Fermat*'sche Theorem enthält bekanntlich in dem einfachsten schon von *Euler* behandelten Falle den Satz, dass die Gleichung:

$$r^3 + s^3 - 1 = 0$$

nicht anders durch rationale Werthe von r und s erfüllt werden kann, als wenn r oder s gleich Null ist. Durch die Substitution:

$$r = \frac{2a}{3b-1}, \quad s = \frac{3b+1}{3b-1}$$

erhält man:

$$(3b-1)^3 \cdot (r^3 + s^3 - 1) = 2(4a^3 + 27b^2 + 1),$$

woraus der Satz hervorgeht, dass die Gleichung:

$$4a^3 + 27b^2 + 1 = 0$$

nicht anders durch rationale Werthe von a und b erfüllt werden kann, als wenn

$$a = -1, \quad b = \pm\frac{1}{3}$$

gesetzt wird; und es ist auch umgekehrt der oben erwähnte Satz über die Gleichung: $r^3 + s^3 = 1$ eine *Folge* dieses letzteren. Da nun der Ausdruck $4a^3 + 27b^2$ den negativen Werth der Discriminante der Gleichung:

$$x^3 + ax + b = 0$$

angiebt, so ist

$$x^3 - x \pm \frac{1}{3} = 0$$

die einzige cubische Gleichung mit rationalen Coefficienten, für welche die Summe der Wurzeln gleich Null und das Quadrat des Products der drei Wurzeldifferenzen gleich Eins wird. — Die Wurzeln dieser besondern Gleichung dritten Grades sind:

$$\pm\frac{2}{\sqrt{3}}\cdot\sin\frac{\pi}{9}, \quad \pm\frac{2}{\sqrt{3}}\cdot\sin\frac{2\pi}{9}, \quad \mp\frac{2}{\sqrt{3}}\cdot\sin\frac{4\pi}{9}.$$

Der *Fermat*'sche Satz über die Gleichung $x^3 + y^3 = z^3$ lässt sich daher, wie leicht zu sehen, in folgender bemerkenswerther Fassung aussprechen:

Es kann die Discriminante einer cubischen Gleichung mit rationalen Coefficienten nicht die sechste Potenz einer rationalen Zahl werden, ausser wenn ihre drei Wurzeln

$$m + n\sqrt{3}\cdot\sin\frac{\pi}{9}, \quad m + n\sqrt{3}\cdot\sin\frac{2\pi}{9}, \quad m - n\sqrt{3}\cdot\sin\frac{4\pi}{9}$$

und m, n rational sind.

ÜBER DIE KLASSENANZAHL DER AUS WURZELN DER EINHEIT GEBILDETEN COMPLEXEN ZAHLEN.

VON

L. KRONECKER.

Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin vom Jahre 1863. S. 340—345.

ÜBER DIE KLASSENANZAHL DER AUS WURZELN DER EINHEIT GEBILDETEN COMPLEXEN ZAHLEN.

[Gelesen in der Akademie der Wissenschaften am 23. Juli 1863.]

In den beiden denselben Gegenstand betreffenden Mittheilungen des Hrn. *Kummer*, welche in den Monatsberichten vom December 1861 und Januar d. J. veröffentlicht sind[1]), ist auf den merkwürdigen Umstand aufmerksam gemacht, dass der erste der beiden Factoren, in welche sich der Ausdruck für jene Klassenanzahl scheidet, nicht immer ganzzahlig ist. Hr. *Kummer* hat bereits in seiner Notiz vom 9. December 1861 erwähnt, dass die vorkommenden Nenner nur Potenzen der Zahl Zwei seien, ohne jedoch deren Höhe zu bestimmen. Das Interesse, welches mir die hiernach noch offen gebliebene Frage zu haben schien, veranlasste mich zu einer Beschäftigung mit diesem Gegenstande, und ich habe dabei das Resultat erlangt, dass *nur die Zahl Zwei selbst* und niemals eine höhere Potenz derselben in den erwähnten Nennern auftreten kann. Dieses Resultat, welches ich hier in aller Kürze begründen will, kann folgendermassen ausgesprochen werden:

„Wenn man unter Beibehaltung der von Hrn. *Kummer* im Monatsberichte vom Januar d. J. eingeführten Bezeichnungen die Klassenanzahl H durch das Product: $P_1 \cdot \frac{\theta}{\Delta}$ darstellt, sobald n die Potenz

[1]) *E. E. Kummer*, Über die Klassenanzahl der aus n^{ten} Einheitswurzeln gebildeten complexen Zahlen. Monatsberichte der Kgl. Preuss. Akademie der Wissenschaften zu Berlin v. J. 1861. S. 1051—1053. H.

E. E. Kummer, Über die Klassenanzahl der aus zusammengesetzten Einheitswurzeln gebildeten idealen complexen Zahlen. Monatsberichte der Kgl. Preuss. Akademie der Wissenschaften v. J. 1863. S. 21—28. H.

einer einzigen Primzahl ist, hingegen durch: $P_1 \cdot \frac{\theta}{2\Delta}$, sobald n verschiedene Primfactoren enthält, so ist sowohl der erste als der zweite Factor der Klassenanzahl stets ganzzahlig, und der letztere repräsentirt für sich selbst die Klassenanzahl der aus den Perioden:

$$\omega + \omega^{-1}, \quad \omega^2 + \omega^{-2}, \quad \ldots$$

gebildeten complexen Zahlen."

Die Beziehung der hier als erster Factor bezeichneten Zahl P_1 zu der Grösse P', welche Hr. *Kummer* (a. a. O. pag. 26) den ersten Factor der Klassenanzahl genannt hat, ist einfach die, dass

$$P_1 = P' \quad \text{oder} \quad P_1 = 2P'$$

wird, je nachdem n zu der ersten oder zu der zweiten der beiden unterschiedenen Arten von Zahlen gehört. Ebenso tritt natürlich in Betreff des zweiten Factors nur für solche Zahlen n, die mehrere verschiedene Primfactoren enthalten, ein Unterschied zwischen der obigen und der von Hrn. *Kummer* gebrauchten Ausdrucksweise auf.

Um nun zuvörderst die oben gemachte Angabe zu erläutern, dass je nach den beiden für die Zahl n unterschiedenen Fällen der Ausdruck $\frac{\theta}{\Delta}$ oder $\frac{\theta}{2\Delta}$ die Klassenanzahl für die Zahlen in $\omega + \omega^{-1}$ repräsentire, während Hr. *Kummer* sie für *jedes* n durch $\frac{\theta}{\Delta}$ ausgedrückt findet, bemerke ich, dass derselbe bei Berechnung der erwähnten Klassenanzahl von vorn herein von den vorhandenen wirklichen complexen Zahlen diejenigen ausschliesst resp. als nicht vorhanden betrachtet, deren Norm negativ ist. Hiernach wird der Begriff des Wirklichen in einem engeren Sinne genommen, und es muss in Folge dessen ein Product idealer Primfactoren auch dann als ideal d. h. als nicht wirklich angesehen werden, wenn es wirkliche Zahlen giebt, die in Bezug auf alle ihre Primfactoren mit jenem Product übereinstimmen, aber keine solche, deren Norm positiv ist. Bei dieser Anschauung verdoppelt sich, wie leicht zu sehen, die Klassenanzahl, sobald keine complexen Einheiten existiren, deren Norm -1 ist. Giebt es aber dergleichen Einheiten,

so bleibt die Klassenanzahl ungeändert. Das Letztere findet nur dann statt, wenn n eine einfache Primzahlpotenz ist. Denn alsdann stellt in der That:

$$\frac{\omega^g - \omega^{-g}}{\omega - \omega^{-1}}$$

eine complexe Zahl in $\omega + \omega^{-1}$ dar, deren Norm gleich -1 ist, vorausgesetzt dass man unter n die Potenz einer ungraden Primzahl und unter g eine primitive Wurzel derselben versteht; und es wird ferner

$$N(1 + \omega + \omega^{-1} + \omega^2 + \omega^{-2}) = -1,$$

wenn der Exponent der Einheitswurzel ω eine Potenz von Zwei ist. Enthält aber die Zahl n verschiedene Primfactoren und bedeutet p einen derselben, so ist

$$Nf(\omega + \omega^{-1})$$

stets von der Form $kp + 1$, und es kann daher keine complexen Einheiten geben, deren Norm gleich -1 wäre. Hierdurch erklärt sich also der Umstand, dass die Klassenanzahl der complexen Zahlen in $\omega + \omega^{-1}$, wenn n eine Zahl der ersten Art ist, bei beiden Zählungsweisen übereinstimmt, während dieselbe für Zahlen der zweiten Art durch $\frac{\theta}{2\Delta}$ oder durch $\frac{\theta}{\Delta}$ repräsentirt wird, je nachdem man *alle* complexen Zahlen:

$$a + a_1(\omega + \omega^{-1}) + a_2(\omega^2 + \omega^{-2}) + \cdots$$

als wirklich betrachtet oder nur diejenigen, deren Norm positiv ist.

Nach den gegebenen Erläuterungen bedarf es zur Rechtfertigung der oben ausgesprochenen Behauptung nur noch des Nachweises, dass P_1 stets eine ganze Zahl ist, oder mit andern Worten

> „dass die Klassenanzahl der complexen Zahlen in $\omega + \omega^{-1}$, wenn der Begriff des Wirklichen im gewöhnlichen (weiteren) Sinne genommen wird, stets ein aliquoter Theil der Klassenanzahl für die complexen Zahlen in ω ist".

Man kann sich behufs dessen genau der Schlussweise bedienen, welche Hr. *Kummer* im 40^sten^ Bande des Journals für Mathematik pag. 115 angewendet hat[1]), und es ist dabei nur nöthig, die dort gemachte — wenn auch nicht ausdrücklich erwähnte — Voraussetzung zu begründen, dass je zwei zu verschiedenen Klassen gehörige Zahlen in $\omega + \omega^{-1}$ auch in der Theorie der complexen Zahlen in ω nicht einander äquivalent sein können.

Man sieht leicht, dass, wenn zwei nicht äquivalente Zahlen in $\omega + \omega^{-1}$, als Zahlen in ω betrachtet, einander äquivalent wären, nothwendig gewisse ideale (nicht wirkliche) Zahlen in $\omega + \omega^{-1}$ zu wirklichen Zahlen in ω werden müssten. Es ist also nur zu zeigen, dass eine ideale d. h. nicht wirkliche complexe Zahl $\varphi(\omega + \omega^{-1})$ niemals durch eine wirkliche Zahl $f(\omega)$ repräsentirt werden kann. Wäre dies der Fall, so müssten innerhalb der Theorie der complexen Zahlen in ω die idealen Primfactoren von $\varphi(\omega + \omega^{-1})$ mit denen von $f(\omega)$, also auch mit denen von $f(\omega^{-1})$ übereinstimmen; die beiden conjugirten wirklichen Zahlen $f(\omega)$ und $f(\omega^{-1})$ könnten sich also nur durch eine Einheit $e(\omega)$ von einander unterscheiden. Es müsste also:

$$f(\omega^{-1}) = e(\omega) \cdot f(\omega)$$

und deshalb auch:

$$e(\omega) \cdot e(\omega^{-1}) = 1$$

sein. Hieraus folgt vermöge des Satzes, welchen ich im 53^sten^ Bande des Journals für Mathematik pag. 173 bewiesen habe[2]), dass $e(\omega)$ nur eine einfache Wurzel der Einheit sein kann, und zwar, je nachdem n grade oder ungrade ist, eine n^{te} oder $2n^{te}$ Wurzel der Einheit, da keine andre sich rational durch ω darstellen lässt. Für ein grades n müsste also entweder die Gleichung:

$$f(\omega^{-1}) = \omega^{2r} \cdot f(\omega),$$

oder die Relation:

[1]) *E. E. Kummer*, Bestimmung der Anzahl nicht äquivalenter Klassen für die aus λ^{ten} Wurzeln der Einheit gebildeten complexen Zahlen und die idealen Factoren derselben. Journal für Mathematik. Bd. 40. S. 93—116. H.

[2]) Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten. Bd. I. S. 103—108 dieser Ausgabe von *L. Kronecker's* Werken. H.

$$f(\omega^{-1}) = \omega^{2r+1} \cdot f(\omega)$$

bestehen, in welcher r eine ganze Zahl bedeutet. Für ein ungrades n aber müsste $f(\omega^{-1}) = \pm \omega^{k} \cdot f(\omega)$, also, da in diesem Falle $k \equiv 2r \pmod{n}$ gesetzt werden kann, entweder wiederum:

$$f(\omega^{-1}) = \omega^{2r} \cdot f(\omega)$$

oder:

$$f(\omega^{-1}) = -\omega^{2r} \cdot f(\omega)$$

sein. Es sind demnach im Ganzen nur drei verschiedene Relationen zwischen $f(\omega)$ und $f(\omega^{-1})$ zulässig.

Fande nun *erstens* die Gleichung $f(\omega^{-1}) = \omega^{2r} \cdot f(\omega)$ statt, so würde $\omega^{r} \cdot f(\omega)$ bei der Verwandlung von ω in ω^{-1} ungeändert bleiben d. h. es wäre eine aus den zweigliedrigen Perioden: $\omega + \omega^{-1}$, $\omega^2 + \omega^{-2}$, ... zusammengesetzte ganze complexe Zahl. Bezeichnet man eine solche mit $F(\omega + \omega^{-1})$, so hätte man also die Gleichung:

(I.) $$f(\omega) = \omega^{-r} \cdot F(\omega + \omega^{-1}).$$

Legt man *zweitens* für den Fall, dass n grade ist, die Gleichung $f(\omega^{-1}) = \omega^{2r+1} \cdot f(\omega)$ zu Grunde, so folgt daraus, wenn man

$$\frac{\omega^{r} \cdot f(\omega) - \omega^{-r} \cdot f(\omega^{-1})}{\omega - \omega^{-1}} = F(\omega + \omega^{-1})$$

setzt, die Relation:

(II.) $$f(\omega) = -\omega^{-r-1} \cdot (1 + \omega) \cdot F(\omega + \omega^{-1}),$$

in welcher $F(\omega + \omega^{-1})$ wiederum, wie oben, eine aus den zweigliedrigen Perioden zusammengesetzte ganze complexe Zahl bedeutet.

Wenn endlich *drittens* für ein ungrades n die Gleichung:

$$f(\omega^{-1}) = -\omega^{2r} \cdot f(\omega)$$

erfüllt wäre, so könnte

(III.) $$f(\omega) = \frac{\omega^{-r}}{\omega - \omega^{-1}} \cdot F(\omega + \omega^{-1})$$

gesetzt werden, insofern alsdann $(\omega - \omega^{-1}) \cdot \omega^r \cdot f(\omega)$ bei der Verwandlung von ω in ω^{-1} ungeändert bleiben, also eine aus den zweigliedrigen Perioden zusammengesetzte ganze complexe Zahl sein würde.

Bei der offenbar zulässigen Voraussetzung, dass die ideale Zahl $\varphi(\omega+\omega^{-1})$ von allen *wirklichen* Primfactoren befreit sei, darf dieselbe und also auch $f(\omega)$ keinen Primfactor von p enthalten, wenn n die Potenz einer einfachen Primzahl p ist. Deshalb sind für solche Zahlen n die letzten beiden von den obigen drei Fällen auszuschliessen. Wäre nämlich $n = 2^\lambda$ und alsdann $f(\omega^{-1}) = \omega^{2r+1} \cdot f(\omega)$, so müsste $f(\omega)$ den Factor $(1 + \omega)$, welcher ein Primfactor von 2 ist, enthalten; und ebenso müsste, wenn n die Potenz einer ungraden Primzahl p und $f(\omega^{-1}) = -\omega^{2r} \cdot f(\omega)$ wäre, $f(\omega)$ durch den Primfactor von p, nämlich durch $(1 - \omega)$ theilbar sein. Es braucht daher, wenn n Primzahlpotenz ist, nur die Annahme berücksichtigt zu werden, aus welcher sich die Gleichung (I.) ergeben hat, während, wenn n aus verschiedenen Primfactoren besteht, noch die Gleichungen (II.) und (III.) stattfinden könnten. Da aber für solche Zahlen n die in diesen Gleichungen als Factoren von $F(\omega + \omega^{-1})$ auftretenden Grössen stets complexe Einheiten sind, so sieht man, dass die gemachten Voraussetzungen *in allen Fällen* auf eine Relation:

$$f(\omega) = \varepsilon(\omega) \cdot F(\omega + \omega^{-1})$$

führen, in welcher $\varepsilon(\omega)$ eine complexe Einheit und $F(\omega + \omega^{-1})$ eine wirkliche complexe aus zweigliedrigen Perioden zusammengesetzte Zahl bedeutet. Diese Relation zeigt jedoch, dass die complexe Zahl $F(\omega + \omega^{-1})$ mit $f(\omega)$ und also auch mit $\varphi(\omega + \omega^{-1})$ in allen ihren Primfactoren übereinstimmt; die Zahl $\varphi(\omega + \omega^{-1})$ wäre in Folge dessen durch die wirkliche Zahl

$$F(\omega + \omega^{-1})$$

zu ersetzen und könnte keiner andern Klasse idealer d. h. nicht wirklicher Zahlen in $\omega + \omega^{-1}$ angehören.

Ich bemerke schliesslich, um jede Unklarheit zu beseitigen, dass die zuletzt angewendeten Schlüsse ihre Geltung verlieren, sobald man in der Theorie der complexen Zahlen in $\omega + \omega^{-1}$ den Begriff des Wirklichen in dem oben angedeuteten engeren Sinne auffasst. Alsdann würde nämlich die Zahl $F(\omega + \omega^{-1})$ nicht stets als wirklich anzusehen sein, sondern nur in dem Falle, dass ihre Norm positiv ist.

ÜBER EINIGE INTERPOLATIONSFORMELN FÜR GANZE FUNCTIONEN MEHRER VARIABELN.

VON

L. KRONECKER.

Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin vom Jahre 1865. S. 686—691.

ÜBER EINIGE INTERPOLATIONSFORMELN FÜR GANZE FUNCTIONEN MEHRER VARIABELN.

[Gelesen in der Akademie der Wissenschaften am 21. December 1865.]

Indem ich versuchte meine Resultate über die Zerlegung der Discriminante von Eliminationsgleichungen auf die *Lagrange*'sche Interpolationsformel anzuwenden, bin ich zu allgemeineren Formeln gelangt, welche ungeachtet ihrer grossen Einfachheit, so viel ich weiss, bisher noch nicht aufgestellt worden sind.

Es seien

$$F_1, F_2, \ldots F_n$$

ganze, nicht homogene Functionen der Variabeln $x_1, x_2, \ldots x_n$ resp. von den Dimensionen

$$\nu_1, \nu_2, \ldots \nu_n.$$

Es seien ferner

$$x_1 = \xi_{1k}, \quad x_2 = \xi_{2k}, \quad \ldots\ldots \quad x_n = \xi_{nk},$$

für $k = 1, 2, \ldots m$ die m verschiedenen Systeme endlicher Werthe, für welche die n Functionen F gleichzeitig verschwinden. Alsdann besteht für jede dieser Functionen F eine Gleichung:

$$F_i = (x_1 - \xi_{1k}) F_{1i}^{(k)} + (x_2 - \xi_{2k}) F_{2i}^{(k)} + \cdots\cdots + (x_n - \xi_{nk}) F_{ni}^{(k)},$$

in welcher $F_{1i}^{(k)}, F_{2i}^{(k)}, \ldots$ ganze Functionen von $x_1, x_2, \ldots x_n$, $\xi_{1k}, \xi_{2k}, \ldots \xi_{nk}$ bedeuten. Die aus den n^2 Functionen

$$F_{hi}^{(k)}$$

gebildete Determinante, welche also ebenfalls eine ganze Function der Variabeln x und deren durch den zweiten Index k bezeichneten Werthe ist, verschwindet stets, wenn darin für die Variabeln x eines der übrigen $(m-1)$ Werthsysteme gesetzt wird. Diese einfache Bemerkung ist von fundamentaler Bedeutung für die Eliminationstheorie und kann bei Entwickelung derselben füglich zum Ausgangspunkt genommen werden. Ich behalte die Darstellung des hiernach einzuschlagenden Weges einer künftigen Mittheilung vor und erwähne hier nur, dass die Betrachtung jener Determinante ganz unmittelbar auf eine Verallgemeinerung der *Lagrange*'schen Interpolationsformel führt. Bezeichnet man nämlich die aus den Functionen $F_{hi}^{(k)}$ gebildete Determinante mit

$$D_k(x_1, x_2, \ldots x_n)$$

und setzt

$$D_k(\xi_{1k}, \xi_{2k}, \ldots \xi_{nk}) = \Delta_k,$$

so stellt der Ausdruck:

$$(A) \qquad \sum_1^m \mathfrak{F}_k \cdot \frac{D_k}{\Delta_k}$$

eine ganze Function von $x_1, x_2, \ldots x_n$ dar, welche für jedes der m Werthsysteme:

$$x_1 = \xi_{1k}, \quad x_2 = \xi_{2k}, \quad \ldots\ldots \quad x_n = \xi_{nk}$$

resp. den Werth $\mathfrak{F}_k$ annimmt. Die hierbei zu machende Voraussetzung, dass keine der m Grössen Δ_k gleich Null werde, kommt damit überein, dass das System der n Gleichungen:

$$F = 0$$

keines der m Werthsysteme mehrfach enthalte; denn der Werth von Δ_k ist gleich dem Werthe, welchen die Functionaldeterminante von $F_1, F_2, \ldots F_n$ für:

$$x_1 = \xi_{1k}, \quad x_2 = \xi_{2k}, \quad \ldots\ldots \quad x_n = \xi_{nk}$$

erhält. Ist $\mathfrak{F}(x_1, x_2, \ldots x_n)$ eine beliebige ganze Function, und

$$\mathfrak{F}(\xi_{1k}, \xi_{2k}, \ldots \xi_{nk}) = \mathfrak{F}_k,$$

so ist die Differenz:

$$\mathfrak{F}(x_1, x_2, \ldots x_n) - \sum_1^m \mathfrak{F}_k \cdot \frac{D_k}{\Delta_k}$$

als homogene lineare Function der n Functionen F darstellbar. Auch die verschiedenen Determinanten D_k, welche man erhält, wenn man die oben eingeführten, aber nicht vollkommen bestimmten Functionen $F_{hi}^{(k)}$ anders und anders wählt, unterscheiden sich nur durch einen homogenen linearen Ausdruck von $F_1, F_2, \ldots F_n$.

Die Functionen $F_{hi}^{(k)}$ können so gewählt werden, dass sie in den Gliedern der höchsten Dimension mit denen von

$$\frac{1}{\nu_i} \cdot \frac{\partial F_i}{\partial x_h}$$

oder, was dasselbe ist, mit dem Ausdrucke:

$$\frac{1}{\nu_i} \cdot \frac{\partial f_i}{\partial x_h}$$

übereinstimmen, wenn f_i den Complex der Glieder höchster Dimension in F_i bedeutet. Alsdann sind auch die Glieder der höchsten Dimensionen von $\nu_1 \cdot \nu_2 \cdots \nu_n \cdot D_k$ für jeden Werth von k mit der Functionaldeterminante von $f_1, f_2, \ldots f_n$ identisch. Bezeichnet man nun diese Functionaldeterminante mit

$$R(x_1, x_2, \ldots x_n),$$

so muss für jede Function $\mathfrak{F}(x_1, \ldots x_n)$, deren Dimension kleiner als die von R d. h. kleiner als $\nu_1 + \nu_2 + \cdots + \nu_n - n$ ist,

$$R(x_1, x_2, \ldots x_n) \cdot \sum \frac{1}{\Delta_k} \cdot \mathfrak{F}(\xi_{1k}, \xi_{2k}, \ldots \xi_{nk})$$

durch Hinzufügung einer linearen homogenen Function von $F_1, F_2, \ldots F_n$ auf eine niedrigere Dimension gebracht werden können. Hiernach muss entweder

$$(B) \qquad \sum \frac{1}{\Delta_k} \cdot \mathfrak{F}(\xi_{1k}, \xi_{2k}, \ldots \xi_{nk}) = 0$$

oder

$$(C) \qquad R(x_1, x_2, \ldots x_n) = \varphi_1 f_1 + \varphi_2 f_2 + \cdots + \varphi_n f_n$$

sein, wo unter $\varphi_1, \varphi_2, \ldots \varphi_n$ ganze homogene Functionen von $x_1, x_2, \ldots x_n$ zu verstehen sind. Die letztere dieser beiden Gleichungen enthält die nothwendige und hinreichende Bedingung dafür, dass die n homogenen Gleichungen: $f = 0$ gleichzeitig zu befriedigen sind und dass mithin die n Gleichungen: $F = 0$ weniger als $\nu_1 \cdot \nu_2 \cdots \nu_n$ endliche Werthsysteme für die Variabeln $x_1, x_2, \ldots x_n$ ergeben. Die Gleichung (C) besteht demnach nur, wenn $m \leqq \nu_1 \cdot \nu_2 \cdots \nu_n$ ist, und es muss also für $m = \nu_1 \cdot \nu_2 \cdots \nu_n$ die Gleichung (B) stattfinden. Diese enthält die bekannten *Jacobi*'schen Relationen für die den n Gleichungen: $F = 0$ genügenden simultanen Werthsysteme von $x_1, x_2, \ldots x_n$, Relationen, welche demnach auf die hier angedeutete Weise ganz ebenso unmittelbar aus den Eigenschaften der Formel (A) folgen wie die *Euler*'schen Gleichungen aus der *Lagrange*'schen Interpolationsformel, in welche der Ausdruck (A) für den Fall $n = 1$ übergeht.

Die einschränkende Bedingung, an welche im Vorstehenden die Giltigkeit der Gleichung (B) geknüpft erscheint, wird von *Jacobi*, welcher den Fall $n = 2$ im XIV. Bande des Journals für Mathematik ausführlich behandelt hat[1]), nicht erwähnt. Die daselbst angewendete Bezeichnungsweise lässt im

[1]) *C. G. J. Jacobi*, Theoremata nova algebraica circa systema duarum aequationum inter duas variabiles propositarum. Journal für Mathematik Bd. 14, S. 281—288. Jacobi's Werke Bd. III S. 285—294. H.

Gegentheil auf die Annahme einer unbeschränkten Giltigkeit der hergeleiteten Formeln schliessen. Indessen überzeugt man sich leicht davon, dass die Gleichung (B) nicht mehr allgemein giltig bleiben kann, wenn $m < \nu_1 \cdot \nu_2 \cdots \nu_n$ ist, da alsdann eine Function $\mathfrak{F}(x_1, x_2, \ldots x_n)$ existirt, deren Dimension kleiner als $\nu_1 + \nu_2 + \cdots + \nu_n - n$ ist, und welche dennoch für alle m Werthsysteme:

$$x_1 = \xi_{1k}, \quad x_2 = \xi_{2k}, \quad \ldots\ldots \quad x_n = \xi_{nk}$$

mit der Functionaldeterminante von $F_1, F_2, \ldots F_n$ übereinstimmt. Bei genauerer Betrachtung der *Jacobi*'schen Methode zeigt sich auch die Stelle, an welcher die obige einschränkende Bedingung auftritt. Wenn diese Bedingung nicht erfüllt ist, wird nämlich *Jacobi*'s Bestimmung des Grades der von ihm benutzten Multiplicatoren unrichtig. Eben dieselbe Bemerkung gilt in Bezug auf die Ausführungen des Herrn *Betti*, mittels deren derselbe im I. Bande der Tortolinischen Annalen die *Jacobi*'sche Methode ohne wesentliche Modification auf eine beliebige Anzahl von Gleichungen übertragen hat[1]). Die *erste* Herleitung der *Jacobi*'schen Relationen für eine beliebige Anzahl von Gleichungen hat Hr. *Liouville* im VI. Bande seines Journals gegeben[2]) und sich dabei ausdrücklich auf den sogenannten allgemeinen Fall, in welchem $m = \nu_1 \cdot \nu_2 \cdots \nu_n$ und also die oben angegebene Bedingung wirklich erfüllt ist, beschränkt. Die Formeln, auf welche Hr. *Liouville* a. a. O. durch die Theorie der Elimination zuvörderst geführt wird, erscheinen allgemeiner als die *Jacobi*'schen Formeln; sie sind aber, wie ich bei dieser Gelegenheit erwähnen will, von gleicher Allgemeinheit, da sie aus den *Jacobi*'schen Formeln hervorgehen, wenn für eine der Functionen F ein Product zweier ganzer Functionen von n Variabeln genommen wird.

Wiewohl für den Fall, wo $m < \nu_1 \cdot \nu_2 \cdots \nu_n$ ist, entweder mit Hilfe gebrochener linearer Substitutionen oder direct aus dem interpolatorischen Ausdrucke (A) ebenfalls gewisse, den *Jacobi*'schen Relationen entsprechende Beziehungen abgeleitet werden können, so übergehe ich doch denselben, um

[1]) *E. Betti*, Sopra l'equazioni algebriche con più incognite. Annali di matematica, tomo I, p. 1—8. H.

[2]) *J. Liouville*, Mémoire sur quelques propositions générales de géométrie et sur la théorie de l'élimination dans les équations algébriques. Journal de mathématiques. T. VI p. 345—411. H.

noch eine Bemerkung an den sogenannten allgemeinen Fall zu knüpfen. Alsdann kann nämlich jede ganze Function von $x_1, x_2, \dots x_n$ durch Hinzufügung einer linearen homogenen Function von $F_1, F_2, \dots F_n$ auf eine solche reducirt werden, deren Grad in Beziehung auf x_k kleiner als ν_k ist. Es lassen sich also auch die Functionen D_k auf solche reduciren, und wenn man dies als geschehen annimmt, so stellt die Summe:

$$\sum_1^m \mathfrak{F}_k \cdot \frac{D_k}{\Delta_k}$$

diejenige vollkommen bestimmte ganze Function von $x_1, x_2, \dots x_n$ dar, welche in Bezug auf jede der Variabeln x den entsprechenden Grad $(\nu - 1)$ nicht übersteigt und für jedes der m verschiedenen Werthsysteme ξ den vorgeschriebenen Werth $\mathfrak{F}_k$ erhält.

Schliesslich will ich hier noch eine andere Verallgemeinerung der *Lagrange*'schen Interpolationsformel mittheilen, welche mit der oben angegebenen in einem leicht ersichtlichen Zusammenhange steht. Es sei nämlich $F(x)$ eine ganze Function m^{ten} Grades von x und der Coefficient von x^m darin gleich Eins. Ferner denke man sich $F(x)$ auf alle möglichen Weisen als Product zweier Factoren $\varphi(x)$ und $\psi(x)$ dargestellt, von denen der erstere vom Grade n, der andere vom Grade $(m-n)$ ist. Die Anzahl dieser Darstellungen d. h. $\frac{m(m-1)\cdots(m-n+1)}{1\cdot 2 \cdot \dots \cdot n}$ sei ν, so dass

$$F(x) = \varphi_k(x) \cdot \psi_k(x)$$

wird, für $k = 1, 2, \dots \nu$. Bezeichnet man nun das Eliminationsresultat von $\varphi_k(x) = 0$ und $\psi_k(x) = 0$ durch R_k, so erhält das Product:

$$\psi_k(x_1) \cdot \psi_k(x_2) \cdot \dots \cdot \psi_k(x_n)$$

eben diesen Werth R_k, wenn man die Variabeln $x_1, x_2, \dots x_n$ durch die n Wurzeln der Gleichung: $\varphi_k(x) = 0$ ersetzt, während dasselbe verschwindet, wenn für $x_1, x_2, \dots x_n$ die n Wurzeln irgend einer andern Gleichung: $\varphi(x) = 0$ genommen werden. Hieraus ergiebt sich die identische Gleichung:

$$(D) \qquad f(x_1, x_2, \dots x_n) = \sum_{k=1}^{k=\nu} \frac{f_k}{R_k} \cdot \psi_k(x_1)\psi_k(x_2)\cdots\psi_k(x_n),$$

wenn $f(x_1, x_2, \dots x_n)$ eine symmetrische Function der Variabeln x bedeutet, welche in Bezug auf jede derselben vom Grade $(m-n)$ ist und also ν Constanten enthält, und wenn f_k den Werth bedeutet, welchen $f(x_1, x_2, \dots x_n)$ für die n Wurzeln der Gleichung: $\varphi_k(x) = 0$ annimmt. Ist der Coefficient von $(x_1 \cdot x_2 \cdots x_n)^{m-n}$ in f gleich Null, so folgt:

$$\sum \frac{f_k}{R_k} = 0.$$

Die Gleichung (D) enthält die Darstellung einer symmetrischen Function von n Variabeln durch die Werthe, welche sie annimmt, wenn man die Variabeln durch je n Wurzeln einer gegebenen Gleichung ersetzt. In dieser Interpolationsformel ist u. A. die *Rosenhain*'sche Darstellung der Eliminationsresultante zweier Gleichungen[1]) und namentlich auch die von Hrn. *Borchardt* in den Abhandlungen der Akademie vom Jahre 1860 aufgestellte Formel[2]) als specieller Fall inbegriffen, und mit Hilfe jener allgemeineren Formel (D) lassen sich die a. a. O. von Hrn. *Borchardt* gegebenen Ausführungen zum Theil vereinfachen.

---

[1]) *G. Rosenhain*, Neue Darstellung der Resultante der Elimination von z aus zwei algebraischen Gleichungen, etc. Journal f. Math. Bd. 30, S. 157—165. H.

[2]) Über eine Interpolationsformel für eine Art symmetrischer Functionen und über deren Anwendung. Abh. d. Akad. d. Wiss. a. d. J. 1860. S. 1—20. *C. W. Borchardt's* Werke S. 151—172. H.