G. Frobenius

Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe

ISBN 978-3-662-40537-6 ISBN 978-3-662-41014-1 (eBook)
DOI 10.1007/978-3-662-41014-1

Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe

Von G. Frobenius

In seiner Arbeit *Über die Irreductibilität von Gleichungen* (Sitzungsber. 1880, S. 155) hat Kronecker folgenden Satz entwickelt:

Ist $\Phi(x)$ eine ganze ganzzahlige Function von x, durchläuft p alle positiven rationalen Primzahlen, und ist ν_p die Anzahl der reellen Wurzeln der Congruenz $\Phi(x) \equiv 0 \pmod{p}$, so ist

$$\sum \nu_p p^{-1-w} = m \log\left(\frac{1}{w}\right) + \mathfrak{P}(w), \tag{1.}$$

wo m die Anzahl der irreductibeln Factoren von $\Phi(x)$ und $\mathfrak{P}(w)$ eine nach ganzen positiven Potenzen von w fortschreitende, für hinreichend kleine Werthe von w convergente Reihe bezeichnet.

Er beweist mittelst dieses Satzes nicht nur die Irreductibilität einiger Zahlengleichungen, sondern er macht auch noch auf mehrere andere arithmetische und algebraische Fragen aufmerksam, die sich mit seiner Hülfe erledigen lassen, namentlich auf die Frage nach der Dichtigkeit der Primzahlen, für welche eine gegebene Congruenz eine bestimmte Anzahl von reellen Wurzeln hat. Diese Untersuchung soll hier nach den von ihm gegebenen Andeutungen weiter ausgeführt werden.

Ich habe die folgende Arbeit im November 1880 verfasst und die darin entwickelten Resultate meinen Freunden Stickelberger und Dedekind mitgetheilt. Ihre Grundlagen stehen in engster Beziehung zu den Gesetzen, nach denen die rationalen Primzahlen in einem algebraischen und speciell in einem normalen Körper in ideale Primfactoren zerlegt werden. Nach einigen Bemerkungen in Dedekind's Schriften musste ich annehmen, dass dieser sich mit der Erforschung jener Gesetze seit langer Zeit beschäftigt hatte, und in der That sandte er mir auf meine Anfrage am 8. Juni 1882 das Skelett dieser Theorie, das er unter dem Titel *Zur Theorie der Ideale* am 10. September 1894

in den Göttinger Nachrichten publicirt hat. Ich hatte immer gewünscht, dass dieser Abriss vor meiner eigenen Arbeit veröffentlicht würde, und dies war mit der Grund, weshalb ich mich erst jetzt zu ihrer Herausgabe entschlossen habe. Indessen habe ich den gruppentheoretischen Theil der Untersuchung schon 1887 in der Arbeit *Über die Congruenz nach einem aus zwei endlichen Gruppen gebildeten Doppelmodul*, CRELLE's Journal Bd. 101 publicirt.

Wenn man die in DEDEKIND's Arbeit dargelegten Beziehungen als bekannt voraussetzt, lässt sich die vorliegende Untersuchung wesentlich abkürzen. Auf diesem Wege hat HURWITZ den in § 5 dieser Arbeit entwickelten Satz gefunden, wie er mir in einem Briefe vom 2. Januar 1896 mitgetheilt hat. Dies Schreiben hat mich bewogen, meine ursprüngliche Absicht, die vorliegende Untersuchung ganz umzuarbeiten, aufzugeben, und sie, von einigen Kürzungen abgesehen, genau in der Form zu veröffentlichen, wie ich sie 1880 abgefasst habe.

§ 1.

Sei $\mathfrak{S}$ die Gruppe aller $n! = s$ Substitutionen von n Symbolen. Sind A, B, S Substitutionen von $\mathfrak{S}$, und ist $S^{-1}AS = B$, so heissen A und B *ähnliche* Substitutionen, und S heisst die Transformation, die A in B überführt. Die Gesammtheit der Substitutionen von $\mathfrak{S}$, die einer bestimmten und folglich auch unter einander ähnlich sind, nenne ich eine *Classe* von Substitutionen. Besteht eine Substitution einer Classe aus e Cyklen von $f_1, f_2, \cdots f_e$ Elementen, so nenne ich die Zahlen $f_1, f_2, \cdots f_e$, welche der Bedingung

$$f_1 + f_2 + \cdots + f_e = n \tag{2.}$$

genügen, die *Invarianten* der Classe, weil ihre Übereinstimmung die nothwendige und hinreichende Bedingung für die Ähnlichkeit zweier Substitutionen ist (CAUCHY, *Exercices d'analyse et de physique math.* tom. 3, p. 165). Diese Classen, deren Anzahl l sei, mögen so angeordnet werden, dass eine spätere Classe nicht eine grössere Anzahl von Invarianten besitzt als eine frühere. Die erste Classe besteht also aus der identischen Substitution E und hat n Invarianten, deren jede gleich 1 ist; die zweite Classe hat $n-1$ Invarianten, von denen eine gleich 2, die anderen gleich 1 sind, u. s. w., die l^{te} Classe hat nur eine Invariante n. Dabei ist die Anordnung der Classen, welche gleich viele Invarianten haben, ganz willkürlich gelassen. Ist λ eine der Zahlen von 1 bis l, F irgend eine Substitution der λ^{ten} Classe, und sind $S_1, S_2, \cdots S_s$ die s Substitutionen der Gruppe $\mathfrak{S}$ in irgend einer Reihenfolge, so sind

$$S_1^{-1}FS_1,\ S_2^{-1}FS_2,\ \cdots\ S_s^{-1}FS_s$$

alle Substitutionen der λ^{ten} Classe. Sind v_λ derselben gleich F, giebt es also v_λ mit F vertauschbare Substitutionen, so sind je v_λ jener s Substitutionen einander gleich. Ist daher s_λ die Anzahl der verschiedenen Substitutionen der λ^{ten} Classe, so ist $s = s_\lambda v_\lambda$.

Sei $\varphi(x)$ eine ganze ganzzahlige Function n^{ten} Grades von x ohne quadratischen Theiler, in welcher ich der Einfachheit halber den Coefficienten von x^n gleich 1 voraussetze. Sei p eine positive rationale Primzahl, die nicht in der Discriminante d von $\varphi(x)$ aufgeht, und sei

$$\varphi(t) \equiv P_1(t)\ P_2(t)\ \cdots\ P_e(t) \pmod{p},$$

wo $P_1, P_2, \cdots P_e$ Primfunctionen (mod. p), bez. von den Graden $f_1, f_2, \cdots f_e$ seien. Ist f ein gemeinschaftliches Vielfaches von $f_1, f_2, \cdots f_e$ und $P(t)$ eine Primfunction f^{ten} Grades, so giebt es f_1 verschiedene ganze Functionen x von t, die der Congruenz $P_1(x) \equiv 0$ (modd. p, P) genügen. Ist x_1 eine derselben, so sind $x_1^p \equiv x_2$, $x_2^p \equiv x_3$, $\cdots$ $x_{f_1-1}^p \equiv x_{f_1}$ die übrigen, und es ist $x_{f_1}^p \equiv x_1$. Sind daher $x_1, x_2, \cdots x_n$ die n verschiedenen Functionen von t, die der Congruenz $\varphi(x) \equiv 0$ (modd. p, P) genügen, und ist $x_1^p \equiv x_\alpha$, $x_2^p \equiv x_\beta, \cdots x_n^p \equiv x_\gamma$, so stimmen $x_\alpha, x_\beta, \cdots x_\gamma$, abgesehen von der Reihenfolge, mit $x_1, x_2, \cdots x_n$ überein, und die Substitution

$$F = \begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_\alpha & x_\beta & \cdots & x_\gamma \end{pmatrix}$$

besteht aus e Cyklen von je $f_1, f_2, \cdots f_e$ Elementen. Ist $\varphi(x)$ gegeben, so hängen die Zahlen $f_1, f_2, \cdots f_e$ allein von der Primzahl p ab, die Substitution F aber ausser von p auch noch von der Wahl der Primfunction P. Wie man dieselbe aber auch wählen mag, so ist doch die Classe von Substitutionen, der F angehört, immer dieselbe, und mithin ist diese durch p allein vollständig bestimmt. Wir wollen daher sagen, diese Classe von Substitutionen und die Primzahl p entsprechen einander.

Ist $\psi(x_1, x_2, \cdots x_n)$ eine Function von $x_1, x_2, \cdots x_n$, so bezeichne ich die Function $\psi(x_\alpha, x_\beta, \cdots x_\gamma)$ auch mit $\psi(x_1, x_2, \cdots x_n)_F$.

Sind $\xi_1, \xi_2, \cdots \xi_n$ die n Wurzeln der Gleichung $\varphi(x) = 0$, so ist jede ganze ganzzahlige symmetrische Function von $\xi_1, \xi_2, \cdots \xi_n$ eine ganze ganzzahlige Function der Coefficienten von $\varphi(x)$ und daher der analogen Function von $x_1, x_2, \cdots x_n$ (modd. p, P) congruent.

§ 2.

Sei $\mathfrak{G}$ eine beliebige Gruppe von Substitutionen, g ihre Ordnung, und sei $\psi(t_1, t_2, \cdots t_n)$ eine ganze ganzzahlige Function der n unabhängigen Variabeln $t_1, t_2, \cdots t_n$, welche durch die Substitutionen von

$\mathfrak{G}$ und nur durch diese ungeändert bleibt. Ausserdem sei sie so gewählt, dass die $\frac{s}{g}$ verschiedenen Functionen, in welche ψ durch die Substitutionen von $\mathfrak{S}$ übergeht, auch verschiedene Werthe haben, wenn man $t_1 = \xi_1, \cdots t_n = \xi_n$ setzt. Nach Abel genügt man diesen Forderungen, indem man

$$\psi(t_1, t_2, \cdots t_n) = \Pi(u + t_\alpha u_1 + t_\beta u_2 + \cdots + t_\gamma u_n)$$

setzt, wo

$$\begin{pmatrix} t_1 & t_2 & \cdots & t_n \\ t_\alpha & t_\beta & \cdots & t_\gamma \end{pmatrix}$$

die Substitutionen von $\mathfrak{G}$ durchläuft, und $u, u_1, \cdots u_n$ ganze Zahlen sind, für die nur gewisse Werthe auszuschliessen sind. Von einer solchen Function ψ will ich sagen, sie gehöre zu der Gruppe $\mathfrak{G}$.

Durchläuft dann S alle s Substitutionen von $\mathfrak{S}$, so ist

$$\prod_S (x - \psi(\xi_1, \xi_2, \cdots \xi_n)s) = \Phi(x)$$

eine ganze ganzzahlige Function s^{ten} Grades von x, auf die ich nun die Formel (1.) anwenden will.

Da sich in dieser p^{-1-w} nach Potenzen von w in eine beständig convergirende Reihe entwickeln lässt, so kann man auf der linken Seite der Gleichung (1.) eine endliche Anzahl von Primzahlen weglassen oder allgemeiner in einer endlichen Anzahl von Gliedern die Zahlen ν_p durch beliebige andere constante Coefficienten ersetzen, ohne dass diese Gleichung ihre Form, also die ganze Zahl m ihre Bedeutung ändert.

Macht man in $\psi(\xi_1, \xi_2, \cdots \xi_n)$ nur die $\frac{s}{g}$ in Bezug auf $\mathfrak{G}$ verschiedenen Substitutionen der Gruppe $\mathfrak{S}$, so ist das Quadrat des Differenzenproductes der erhaltenen Werthe

$$d' = \Pi(\psi(\xi_\alpha, \xi_\beta, \cdots \xi_\gamma) - \psi(\xi_\varkappa, \xi_\lambda, \cdots \xi_\mu))^2$$

eine von Null verschiedene ganze Zahl. Ich schliesse von der folgenden Betrachtung nicht nur die in der Discriminante d von $\varphi(x)$, sondern auch die in d' aufgehenden Primzahlen aus. Sind dann A und B zwei Substitutionen von $\mathfrak{S}$, so kann die Congruenz $\psi(x_1, x_2, \cdots x_n)_A \equiv \psi(x_1, x_2, \cdots x_n)_B$ (modd. p, P) nicht anders bestehen, als wenn $A \infty B$ in Bezug auf $\mathfrak{G}$ ist, d. h. wenn AB^{-1} in $\mathfrak{G}$ enthalten ist. Denn da d' eine symmetrische Function von $\xi_1, \xi_2, \cdots \xi_n$ ist, so ist

$$d' \equiv \Pi(\psi(x_\alpha, x_\beta, \cdots x_\gamma) - \psi(x_\varkappa, x_\lambda, \cdots x_\mu))^2 \text{ (modd. } p, P).$$

Wären also A und B nicht in Bezug auf $\mathfrak{G}$ aequivalent, so wäre einer der Factoren dieses Productes congruent 0 (modd. p, P), und daher wäre d' durch p theilbar.

Zunächst ist die Anzahl ν_p der reellen Wurzeln der Congruenz $\Phi(x) \equiv 0 \pmod{p}$ zu bestimmen. Nennt man zwei Functionen einer Variabeln x congruent, falls ihre entsprechenden Coefficienten der Reihe nach congruent sind, so ist

$$\Phi(x) \equiv \prod_S \left(x - \psi(x_1, x_2, \cdots x_n)_S\right) \text{ (modd. } p, P),$$

weil die Coefficienten von $\Phi(x)$ symmetrische Functionen von $\xi_1, \xi_2, \cdots \xi_n$ sind. Mithin sind die s Ausdrücke $\psi(x_1, x_2, \cdots x_n)_S$ die Wurzeln der Congruenz $\Phi(x) \equiv 0$ (modd. p, P). Damit eine dieser Wurzeln $\psi(x_\varrho, x_\sigma, \cdots x_\tau)$ einer rationalen Zahl congruent sei, ist nach dem FERMAT'schen Satze nothwendig und hinreichend, dass

$$\psi(x_\varrho, x_\sigma, \cdots x_\tau) \equiv \left(\psi(x_\varrho, x_\sigma, \cdots x_\tau)\right)^p \equiv \psi(x_\varrho^p, x_\sigma^p, \cdots x_\tau^p) \qquad \text{(modd. } p. P)$$

ist. Sei

$$S = \begin{pmatrix} x_1 & x_2 \cdots x_n \\ x_\varrho & x_\sigma \cdots x_\tau \end{pmatrix} \text{ und } F = \begin{pmatrix} x_1 & x_2 \cdots x_n \\ x_\alpha & x_\beta \cdots x_\gamma \end{pmatrix},$$

falls $x_1^p \equiv x_\alpha$, $x_2^p \equiv x_\beta$, $\cdots x_n^p \equiv x_\gamma$ ist. Dann lautet die obige Bedingung

$$\psi(x_1, x_2, \cdots x_n)_S \equiv \psi(x_1, x_2, \cdots x_n)_{SF}.$$

Mithin müssen die Substitutionen S und SF in Bezug auf die Gruppe $\mathfrak{G}$ einander gleich sein, oder es muss SFS^{-1} in $\mathfrak{G}$ enthalten sein. Daher giebt die Zahl ν_p an, wie viele der s Substitutionen

$$S_1 F S_1^{-1}, S_2 F S_2^{-1}, \cdots S_s F S_s^{-1}$$

der Gruppe $\mathfrak{G}$ angehören. Sei F eine Substitution der λ^{ten} Classe und g_λ die Anzahl der in $\mathfrak{G}$ enthaltenen Substitutionen dieser Classe. Unter jenen s Substitutionen befindet sich jede Substitution der λ^{ten} Classe und jede $v_\lambda = \frac{s}{s_\lambda}$mal. Folglich sind $g_\lambda \frac{s}{s_\lambda}$ dieser Substitutionen in $\mathfrak{G}$ enthalten, und mithin ist

$$\nu_p = \frac{g_\lambda s}{s_\lambda}. \tag{3.}$$

Nunmehr ist die Anzahl m der irreductibeln Factoren von $\Phi(x)$ zu ermitteln. Zu dem Zwecke benutze ich den folgenden Satz (CAMILLE JORDAN, *Traité des substitutions*, § 366):

Ist $\mathfrak{G}$ eine Gruppe von Substitutionen, zu der die Function $\psi(\xi_1, \xi_2, \cdots \xi_n)$ gehört, ist $\mathfrak{H}$ die Gruppe der Gleichung $\varphi(x) = 0$, $\mathfrak{D}$ der grösste gemeinsame Divisor von $\mathfrak{G}$ und $\mathfrak{H}$, und sind d und h die Ordnungen der Gruppen $\mathfrak{D}$ und $\mathfrak{H}$, so genügt ψ einer irreductibeln Gleichung vom Grade $\frac{h}{d}$ mit rationalen Coefficienten. Sind $A, B, \cdots$ die $\frac{h}{d}$ in Bezug auf $\mathfrak{G}$ verschiedenen Substitutionen von $\mathfrak{H}$, so sind $\psi_A, \psi_B, \cdots$ die Wurzeln dieser Gleichung.

Ist S_σ eine der s Substitutionen von $\mathfrak{S}$, und durchläuft G alle Substitutionen von $\mathfrak{G}$, so bilden die Substitutionen $S_\sigma^{-1} G S_\sigma$ eine Gruppe g^{ter} Ordnung, die ich mit $S_\sigma^{-1}\mathfrak{G}S_\sigma = \mathfrak{G}_\sigma$ bezeichnen werde. Die Function $\psi(\xi_1, \xi_2, \cdots \xi_n)_{S_\sigma}$ gehört dann zu der Gruppe $\mathfrak{G}_\sigma$. Seien nun

$$\psi_{S_\alpha}, \psi_{S_\beta}, \cdots \psi_{S_\gamma}$$

die c verschiedenen Wurzeln eines irreductibeln Divisors c^{ten} Grades der Gleichung $\Phi(x) = 0$. Der Grad der irreductibeln Gleichung, der ψ_{S_α} genügt, ist nach dem obigen Satze $c = \frac{h}{d^{(\alpha)}}$, wenn $d^{(\alpha)}$ die Ordnung des grössten gemeinsamen Divisors $\mathfrak{D}_\alpha$ der Gruppen $\mathfrak{H}$ und $\mathfrak{G}_\alpha$ ist. Ebenso ist aber auch $c = \frac{h}{d^{(\beta)}}, \cdots c = \frac{h}{d^{(\gamma)}}$, und mithin ist

$$d^{(\alpha)} + d^{(\beta)} + \cdots + d^{(\gamma)} = cd^{(\alpha)} = h.$$

Diese Summe hat also für alle irreductibeln Factoren von $\Phi(x)$ einen und denselben Werth h. Daraus folgt, dass

$$d^{(1)} + d^{(2)} + \cdots + d^{(s)} = mh \tag{4.}$$

ist, wo m die Anzahl der irreductibeln Factoren von $\Phi(x)$ bezeichnet.

Ist $d_\lambda^{(\sigma)}$ die Anzahl der Substitutionen der λ^{ten} Classe in $\mathfrak{D}_\sigma$, so ist $d^{(\sigma)} = \sum_\lambda^l{}_1 d_\lambda^{(\sigma)}$ und mithin

$$mh = \sum_\sigma^s{}_1 d^{(\sigma)} = \sum_\sigma (\sum_\lambda d_\lambda^{(\sigma)}) = \sum_\lambda (\sum_\sigma d_\lambda^{(\sigma)}).$$

Sind $G_1, G_2, \cdots G_{g_\lambda}$ die Substitutionen der λ^{ten} Classe in $\mathfrak{G}$, so sind $S_\sigma^{-1} G_1 S_\sigma$, $S_\sigma^{-1} G_2 S_\sigma$, $\cdots S_\sigma^{-1} G_{g_\lambda} S_\sigma$ die Substitutionen der λ^{ten} Classe in $\mathfrak{G}_\sigma$. Mithin ist $\sum_\sigma d_\lambda^{(\sigma)}$ die Anzahl der Substitutionen

$$\begin{array}{llll} S_1^{-1} G_1 S_1, & S_2^{-1} G_1 S_2, & \cdots & S_s^{-1} G_1 S_s, \\ S_1^{-1} G_2 S_1, & S_2^{-1} G_2 S_2, & \cdots & S_s^{-1} G_2 S_s, \\ \cdot & \cdot & \cdots & \cdot \\ S_1^{-1} G_{g_\lambda} S_1, & S_2^{-1} G_{g_\lambda} S_2, \cdots & & S_s^{-1} G_{g_\lambda} S_s, \end{array}$$

welche in $\mathfrak{H}$ enthalten sind. In der ersten Zeile stehen sämmtliche Substitutionen der λ^{ten} Classe, und jede $\frac{s}{s_\lambda}$ Mal. Ist daher h_λ die Anzahl der Substitutionen der λ^{ten} Classe in der Gruppe $\mathfrak{H}$, so sind von den Substitutionen dieser Zeile $h_\lambda \frac{s}{s_\lambda}$ in $\mathfrak{H}$ enthalten, und folglich, da diese Zahl von G_1 unabhängig ist, unter den sämmtlichen aufgeführten Substitutionen $g_\lambda h_\lambda \frac{s}{s_\lambda}$. Mithin ist $\sum_\sigma d_\lambda^{(\sigma)} = g_\lambda h_\lambda \frac{s}{s_\lambda}$ und daher

$$m = \frac{s}{h} \sum_\lambda^l{}_1 \frac{g_\lambda h_\lambda}{s_\lambda}. \tag{5.}$$

Durchläuft p_λ alle Primzahlen, die der λ^{ten} Classe von Substitutionen entsprechen, so ergiebt sich jetzt aus den Formeln (1.), (3.) und (5.)

$$\sum_{\lambda}^{1\cdots l} \frac{g_\lambda s}{s_\lambda} (\Sigma p_\lambda^{-1-w}) = \frac{s}{h} \left(\sum_{\lambda}^{1\cdots l} \frac{g_\lambda h_\lambda}{s_\lambda} \right) \log\left(\frac{1}{w}\right) + \mathfrak{P}(w).$$

Nach einer früheren Bemerkung ist es dabei gleichgültig, ob die in den Discriminanten d und d' aufgehenden Primzahlen ausgeschlossen werden oder nicht. Setzt man

$$\Sigma p_\lambda^{-1-w} = \frac{h_\lambda}{h} \log\left(\frac{1}{w}\right) + \mathfrak{P}_\lambda(w), \tag{6.}$$

wo sich die Summe auf alle der λ^{ten} Classe von Substitutionen entsprechenden Primzahlen bezieht, so ist also

$$\sum_{\lambda}^{1\cdots l} \frac{g_\lambda}{s_\lambda} \mathfrak{P}_\lambda = \mathfrak{P}(w). \tag{7.}$$

Indem man in dieser Gleichung für $\mathfrak{G}$ andere und andere Gruppen wählt, erhält man so viele Gleichungen, als es Gruppen giebt. Ich behaupte, dass dieselben zur Bestimmung der (von $\mathfrak{G}$ unabhängigen) l Unbekannten $\mathfrak{P}_\lambda$ vollständig ausreichen (vergl. CRELLE's Journal Bd. 101, S. 280). Man wähle aus jeder Classe von Substitutionen eine aus, und nehme für $\mathfrak{G}$ die Gruppe der Potenzen derselben. So erhält man l Gleichungen, aus denen man die l Unbekannten $\mathfrak{P}_\lambda$ successive ermitteln kann, falls man die Classen von Substitutionen in der Weise anordnet, wie es in §1 festgesetzt worden ist. Denn in der ersten dieser Gleichungen besteht $\mathfrak{G}$ allein aus der identischen Substitution E. Es kommt darin also nur die Unbekannte $\mathfrak{P}_1$ mit einem von Null verschiedenen Coefficienten vor. In der λ^{ten} Gleichung besteht $\mathfrak{G}$ aus den Potenzen einer Substitution F der λ^{ten} Classe. Sind $f_1, f_2, \cdots f_e$ die Invarianten dieser Classe, so hat eine Potenz von F entweder die nämlichen e Invarianten, oder sie hat mehr als e Invarianten. In der betreffenden Gleichung hat daher $\mathfrak{P}_\lambda$ einen von Null verschiedenen Coefficienten, und es kommen ausser $\mathfrak{P}_\lambda$ nur solche Unbekannte $\mathfrak{P}_\mu, \mathfrak{P}_\nu \cdots$ vor, deren Indices kleiner als λ sind. Damit ist die Behauptung dargethan, und es folgt aus dem System der Gleichungen (7.), dass $\mathfrak{P}_\lambda(w)$ eine lineare Verbindung mehrerer Potenzreihen $\mathfrak{P}(w)$ ist, also ebenfalls in eine nach ganzen positiven Potenzen von w fortschreitende convergente Reihe entwickelt werden kann. Nennt man also den durch die Gleichung

$$\Sigma p_\lambda^{-1-w} = D_\lambda \log\left(\frac{1}{w}\right) + \mathfrak{P}(w) \tag{8.}$$

bestimmten Coefficienten D_λ die Dichtigkeit der Primzahlen p_λ, so ist

(9.) $$D_\lambda = \frac{h_\lambda}{h}.$$

I. *Ist* $\varphi(x)$ *eine ganze ganzzahlige Function* n^{ten} *Grades, und sind* $f_1, f_2, \cdots f_e$ *beliebige positive ganze Zahlen, deren Summe gleich n ist, so ist die Dichtigkeit der Primzahlmoduln, für welche* $\varphi(x)$ *in ein Product von e Primfunctionen von den Graden* $f_1, f_2, \cdots f_e$ *zerfällt, gleich der Anzahl derjenigen Substitutionen der Gruppe von* $\varphi(x)$*, welche aus e Cyklen von* $f_1, f_2, \cdots f_e$ *Elementen bestehen, dividirt durch die Ordnung dieser Gruppe.*

Wenn also in der Gruppe von $\varphi(x)$ solche Substitutionen existiren, so giebt es unzählig viele Primzahlen, die dieser Classe von Substitutionen entsprechen. Wenn es aber in der Gruppe von $\varphi(x)$ keine Substitution giebt, die aus e Cyklen von $f_1, f_2, \cdots f_e$ Elementen besteht, so lässt sich zeigen, dass es nur eine endliche Anzahl von Primzahlmoduln geben kann, in Bezug auf welche $\varphi(x)$ einem Producte von e Primfunctionen von den Graden $f_1, f_2, \cdots f_e$ congruent ist. Indessen ist es im Hinblick auf diese Ergänzung des obigen Satzes vortheilhafter, ihn so auszusprechen (vergl. Dedekind, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen; Göttinger Abh. Bd. 23):

II. *Ist ein Körper* n^{ten} *Grades gegeben und e positive ganze Zahlen* $f_1, f_2, \cdots f_e$*, deren Summe gleich n ist, so ist die Dichtigkeit der rationalen Primzahlen, welche in e ideale Primfactoren von den Graden* $f_1, f_2, \cdots f_e$ *zerfallen, gemessen an der Dichtigkeit aller Primzahlen, gleich der Anzahl derjenigen Substitutionen der Gruppe des Körpers, die aus e Cyklen von* $f_1, f_2, \cdots f_e$ *Symbolen bestehen, dividirt durch die Ordnung der ganzen Gruppe.*

Die Dichtigkeit der Primzahlen, welche der λ^{ten} oder μ^{ten} Classe von Substitutionen entsprechen, ist offenbar $D_\lambda + D_\mu = \frac{h_\lambda + h_\mu}{h}$. Sei ν eine der Zahlen von 0 bis n. Betrachtet man dann alle diejenigen Classen, von deren Invarianten ν und nicht mehr als ν gleich 1 sind, so erhält man den Satz:

III. *Die Dichtigkeit der Primzahlmoduln, für welche eine Congruenz* $\varphi(x) \equiv 0$ *genau* ν *reelle Wurzeln hat, ist gleich der Anzahl der Substitutionen der Gruppe von* $\varphi(x)$*, welche genau* ν *Symbole ungeändert lassen, dividirt durch die Ordnung dieser Gruppe.*

§ 3.

Ich hatte Dedekind gegenüber die Vermuthung geäussert, dass umgekehrt, wenn in einem Körper eine rationale Primzahl in e ideale Primfactoren von den Graden $f_1, f_2, \cdots f_e$ zerfällt, auch seine Gruppe eine

Substitution enthalten müsse, die aus e Cyklen von $f_1, f_2, \cdots f_e$ Symbolen besteht. Enthält die Gruppe des Körpers keine solche Substitution, so folgt aus dem Satze II nur, dass die Dichtigkeit der entsprechenden Primzahlen 0 ist. Damit wäre aber nicht ausgeschlossen, dass solche Primzahlen in endlicher und sogar in unendlicher Anzahl existirten. Für die Primzahlen, die nicht in der Discriminante des Körpers aufgehen, ergiebt sich, wie mir DEDEKIND antwortete, der von mir vermuthete Satz in der That aus seiner Theorie. Die bezügliche Stelle seines Briefes vom 8. Juni 1882, worin dieselben Bezeichnungen benutzt sind, wie in dem Abriss von 1894, lautet so:

Ist eine rationale Primzahl $\mathfrak{o}'p = \mathfrak{p}_1' \mathfrak{p}_2' \cdots \mathfrak{p}_{e'}'$, *wo* $\mathfrak{p}_1', \mathfrak{p}_2' \cdots \mathfrak{p}_{e'}'$ *verschiedene Primideale in* $\mathfrak{o}'$ *von den Graden* $f_1', f_2', \cdots f_{e'}'$ *sind, so giebt es in der Gruppe* Φ *des Körpers* Ω' *eine Substitution* ψ_0, *die aus* e' *Cyklen von* $f_1', f_2', \cdots f_{e'}'$ *Elementen besteht.*

Denn, wenn alle $a_r = 1$, mithin alle $g_r = g$ sind, so ist X gemeinschaftlicher Theiler aller $\varphi_r \Phi' \varphi_r^{-1}$ und überhaupt aller mit Φ' conjugirten Gruppen $\varphi \Phi' \varphi^{-1}$; da diese aber, wenn wirklich Φ die Gruppe von Ω', d. h. Ω die Norm von Ω' ist, keinen gemeinsamen Theiler haben[1], so muss $X = 1$, $g = 1$ sein, d. h. p ist durch kein Primidealquadrat in Ω theilbar. Dann ist

$$\Psi_r' = 1 + \psi_r^{f_r'} + \psi_r^{2f_r'} + \cdots + \psi_r^{(f_r-1)f_r'},$$

wo $\psi_r = \varphi_r^{-1} \psi_0 \varphi_r$, und

$$\Phi' \varphi_r^{-1} \Psi = \Phi' \varphi_r^{-1} + \Phi' \varphi_r^{-1} \psi_0 + \Phi' \varphi_r^{-1} \psi_0^2 + \cdots + \Phi' \varphi_r^{-1} \psi_0^{f_r'-1};$$

ersetzt man in der Zerlegung

$$\Phi = \Phi' \varphi_1^{-1} \Psi + \cdots + \Phi' \varphi_{e'}^{-1} \Psi$$

jeden einzelnen Complex $\Phi' \varphi_r^{-1} \Psi$ durch das vorstehende System der f_r' Complexe, so wird Φ überhaupt in

$$n' = f_1' + f_2' + \cdots + f_{e'}'$$

Complexe $\Phi' \varphi$ zerlegt, deren jedem bekanntlich[2] eine Permutation von Ω' (eine Wurzel der irreductibeln Gleichung vom Grade n') entspricht; die Permutation ψ_0 verwandelt dieselben in die Complexe $\Phi' \varphi \psi_0$, bringt also eine Permutation dieser n' Complexe (Elemente) $\Phi' \varphi$ hervor, bei welcher die in $\Phi' \varphi_r^{-1} \Psi$ enthaltenen f_r' Complexe (Elemente, Wurzeln) cyklisch in einander übergehen.

---

[1] Vergl. C. JORDAN, *Traité des substitutions*, Nr. 382, und meine Arbeit *Über endliche Gruppen*, *Sitzungsber.* 1895, S. 179.

[2] Über endliche Gruppen § 4.

§ 4.

Ich will jetzt den Begriff einer *Classe* von Substitutionen enger fassen, als in § 1, dadurch dass ich durchgängig an Stelle der alle Substitutionen umfassenden Gruppe $\mathfrak{S}$ eine bestimmte Gruppe $\mathfrak{H}$ nehme. Zwei Substitutionen A und B der Gruppe $\mathfrak{H}$ sollen conjugirt heissen, wenn es in $\mathfrak{H}$ eine Substitution H giebt, die der Gleichung $H^{-1}AH = B$ genügt. Die Gesammtheit der Substitutionen von $\mathfrak{H}$, die einer gegebenen conjugirt sind, nenne ich eine *Classe* von Substitutionen der Gruppe $\mathfrak{H}$. Je zwei conjugirte Substitutionen sind auch ähnlich, aber nicht je zwei ähnliche Substitutionen von $\mathfrak{H}$ sind conjugirt. Besteht eine Substitution einer Classe aus e Cyklen von $f_1, f_2, \cdots f_e$ Elementen, so sind diese Zahlen zwar Invarianten der Classe, aber es sind nicht ihre sämmtlichen Invarianten.

Ist l die Anzahl der Classen und F eine Substitution der λ^{ten} Classe, und sind $H_1, H_2, \cdots H_h$ die h Substitutionen von $\mathfrak{H}$, so sind

$$(10.) \qquad H_1^{-1}FH_1, \quad H_2^{-1}FH_2, \cdots \quad H_h^{-1}FH_h$$

die sämmtlichen Substitutionen der λ^{ten} Classe. Sind v_λ derselben gleich F, giebt es also in $\mathfrak{H}$ v_λ mit F vertauschbare Substitutionen, so sind je v_λ dieser h Substitutionen einander gleich. Ist h_λ die Anzahl der verschiedenen Substitutionen der λ^{ten} Classe, so ist daher $h = v_\lambda h_\lambda$. Da v_λ die Anzahl der Transformationen irgend einer Substitution der λ^{ten} Classe in sich selbst bezeichnet, so ist $\frac{1}{v_\lambda}$ von Eisenstein (Crelle's Journal Bd. 35, S. 120) die *Dichtigkeit* der λ^{ten} Classe genannt worden.

Sei nun Ω ein normaler Körper h^{ten} Grades, d. h. ein solcher, dessen conjugirte Körper mit ihm identisch sind, und sei $\mathfrak{o}$ die Art aller ganzen Zahlen in Ω. Ist $\mathfrak{p}$ ein Primideal in $\mathfrak{o}$, so nenne ich eine ganze Function mehrerer unabhängigen Variabeln $u_1, u_2, u_3, \cdots$, deren Coefficienten ganze Zahlen in $\mathfrak{o}$ sind, durch $\mathfrak{p}$ theilbar, wenn alle ihre Coefficienten durch $\mathfrak{p}$ theilbar sind. Man ordne die Glieder einer solchen ganzen Function so, dass $\omega u_1^a u_2^b u_3^c \cdots$ vor $\omega' u_1^{a'} u_2^{b'} u_3^{c'} \cdots$ steht, falls von den Differenzen $a-a'$, $b-b'$, $c-c'$, $\cdots$ die erste, die nicht verschwindet, positiv ist (vergl. Gauss' Werke, Bd. 3, S. 36). Dann ist das Anfangsglied des Productes mehrerer ganzen Functionen gleich dem Producte der Anfangsglieder der einzelnen Factoren. Lässt man in jedem Factor die durch $\mathfrak{p}$ theilbaren Glieder weg, so ist also das Anfangsglied des Productes nicht durch $\mathfrak{p}$ theilbar, falls in keinem der Factoren alle Coefficienten durch $\mathfrak{p}$ theilbar sind. Daher kann ein Product mehrerer ganzen Functionen nicht durch $\mathfrak{p}$ theilbar sein, ohne dass einer der Factoren durch $\mathfrak{p}$ theilbar ist.

Sei $\mathfrak{H}$ die Gruppe der h Substitutionen, die den Körper Ω in die h conjugirten Körper überführen. Wenn eine Zahl ω durch die Substitution H der Gruppe $\mathfrak{H}$ in ω' übergeht, so will ich $\omega' = \omega_H$ setzen. Sind $H_1, H_2, \cdots H_h$ die Substitutionen von $\mathfrak{H}$, bilden $\omega_1, \omega_2, \cdots \omega_h$ eine Basis der Art $\mathfrak{o}$, und ist $\omega_{\mathfrak{o}}^{(\alpha)} = (\omega_{\mathfrak{o}})_{H_\alpha}$, so sind die Coefficienten der ganzen Function

$$\prod_{\alpha}^{h}{}_1 (u - u_1\omega_1^{(\alpha)} - u_2\omega_2^{(\alpha)} - \cdots - u_h\omega_h^{(\alpha)}) = \varphi(u, u_1, u_2, \cdots u_h)$$

rationale ganze Zahlen. In der Entwicklung von

$$\varphi(u_1\omega_1 + u_2\omega_2 + \cdots + u_h\omega_h, u_1, u_2, \cdots u_h)$$

nach Potenzen von $u_1, u_2, \cdots u_h$ sind ferner alle Coefficienten gleich Null. Man kann daher jeden einzelnen Coefficienten durch seine p^{te} Potenz ersetzen, und findet so, falls p die durch $\mathfrak{p}$ theilbare rationale Primzahl ist,

$$\varphi(u_1\omega_1^p + \cdots + u_h\omega_h^p, u_1, u_2, \cdots u_h) \equiv 0 \pmod{p},$$

also

$$\Pi\left(u_1(\omega_1^p - \omega_1^{(\alpha)}) + \cdots + u_h(\omega_h^p - \omega_h^{(\alpha)})\right) \equiv 0 \pmod{\mathfrak{p}}.$$

Folglich muss einer der Factoren dieses Productes durch $\mathfrak{p}$ theilbar sein, es muss also in der Gruppe $\mathfrak{H}$ eine Substitution F geben, für welche

$$\omega_1^p \equiv (\omega_1)_F, \quad \omega_2^p \equiv (\omega_2)_F, \cdots \quad \omega_h^p \equiv (\omega_h)_F,$$

mithin auch, wenn $x_1, x_2, \cdots x_h$ rationale ganze Zahlen sind,

$$(x_1\omega_1 + \cdots + x_h\omega_h)^p \equiv (x_1\omega_1 + \cdots + x_h\omega_h)_F$$

ist. Auch sieht man leicht, dass es nicht mehr als eine derartige Substitution geben kann, wenn p nicht in der Grundzahl des Körpers aufgeht. Da nun jede ganze Zahl ω der Art $\mathfrak{o}$ auf die Form

$$x_1\omega_1 + \cdots + x_h\omega_h$$

gebracht werden kann, so giebt es in der Gruppe $\mathfrak{H}$ eine Substitution F der Art, dass jede Zahl ω in $\mathfrak{o}$ die Congruenz

$$\omega^p \equiv \omega_F \pmod{\mathfrak{p}} \tag{11.}$$

befriedigt. Die Substitution F und das Primideal $\mathfrak{p}$ will ich einander entsprechend nennen.

Dieser Satz bildet die Grundlage der Eingangs erwähnten Arbeit von DEDEKIND, *Zur Theorie der Ideale.* Er selbst hat ihn, wie er mir am 14. Juni 1882 schrieb, aus der leicht zu beweisenden Existenz einer ganzen Zahl θ abgeleitet, welche, falls f der Grad von $\mathfrak{p}$ ist, (mod. $\mathfrak{p}$) einer irreductibeln Congruenz f^{ten} Grades mit rationalen Coefficienten genügt, und welche man zugleich so wählen kann, dass sie

nicht durch $\mathfrak{p}$, wohl aber durch jedes andere in p aufgehende Primideal theilbar ist.

Den obigen Beweis habe ich im November 1880 STICKELBERGER mitgetheilt. Das Princip, auf dem er beruht, die Benutzung von ganzen Functionen mehrerer Variabeln, hat KRONECKER in der im Jahre 1882 erschienenen Festschrift *Grundzüge einer arithmetischen Theorie der algebraischen Grössen* zum Fundament der Idealtheorie gewählt.

Ist $\mathfrak{p}_{H\alpha} = \mathfrak{p}_\alpha$, so ist das Product der h mit $\mathfrak{p}$ conjugirten Primideale

$$\mathfrak{p}_1\,\mathfrak{p}_2 \cdots \mathfrak{p}_h = N(\mathfrak{p}_\alpha) = p^f.$$

Ist $h = ef$, und geht p nicht in der Discriminante d des Körpers Ω auf, so sind von diesen h Idealen je f einander gleich, und wenn etwa $\mathfrak{p}_1, \mathfrak{p}_2, \cdots \mathfrak{p}_e$ verschieden sind, so ist

$$\mathfrak{o}p = \mathfrak{p}_1\,\mathfrak{p}_2 \cdots \mathfrak{p}_e. \tag{12.}$$

Entspricht dem Primideal $\mathfrak{p}$ die Substitution F, so entspricht dem Primideal $\mathfrak{p}_\alpha$ die Substitution $H_\alpha^{-1} F H_\alpha$. Den in p aufgehenden Primidealen entsprechen daher die Substitutionen (10.), d. h. die sämmtlichen Substitutionen der Classe, welcher F angehört. Ich sage daher, diese Classe von Substitutionen der Gruppe $\mathfrak{H}$ entspreche der rationalen Primzahl p. Es handelt sich jetzt umgekehrt darum, wenn eine Classe von Substitutionen gegeben ist, die Dichtigkeit der entsprechenden Primzahlen zu bestimmen.

§ 5.

Sei $\mathfrak{G}$ eine Gruppe g^{ter} Ordnung, ein Divisor von $\mathfrak{H}$, und ξ eine Zahl in $\mathfrak{o}$, welche durch die Substitutionen von $\mathfrak{G}$ und nur durch diese ungeändert bleibt. Geht ξ durch die $\frac{h}{g} = n$ in Bezug auf $\mathfrak{G}$ verschiedenen Substitutionen von $\mathfrak{H}$ in $\xi_1, \xi_2, \cdots \xi_n$ über, so ist

$$\Pi(x - \xi_\nu) = \Psi(x)$$

die irreductible Function mit rationalen Coefficienten, die für $x = \xi$ verschwindet.

Sei p eine Primzahl, die weder in der Discriminante d' dieser Function noch in d aufgeht, und $\mathfrak{p}$ ein in p enthaltenes Primideal. Ist $\Psi(a) \equiv 0 \pmod{p}$ für eine rationale ganze Zahl a, so ist $\Pi(a - \xi_\nu) \equiv 0 \pmod{\mathfrak{p}}$, und folglich muss einer der Factoren dieses Productes durch $\mathfrak{p}$ theilbar sein, und nur einer, weil d', also auch $\xi_\mu - \xi_\nu$ durch $\mathfrak{p}$ nicht theilbar ist. Ist $\xi_\nu \equiv a \pmod{\mathfrak{p}}$, so ist $\xi_\nu^p \equiv \xi_\nu \pmod{\mathfrak{p}}$. Umgekehrt folgt aus dieser Congruenz oder $\xi_\nu(\xi_\nu - 1)(\xi_\nu - 2) \cdots (\xi_\nu - p + 1) \equiv 0$, dass ξ_ν einer rationalen Zahl $a \pmod{\mathfrak{p}}$ congruent ist, und dass diese die Con-

gruenz $\Psi(a) \equiv 0 \pmod{p}$ befriedigt. Die Anzahl der reellen Wurzeln dieser Congruenz ist also gleich der Anzahl der Zahlen $\xi_1, \xi_2, \cdots \xi_n$, die der Congruenz $\xi_\nu^p \equiv \xi_\nu \pmod{\mathfrak{p}}$ genügen. Ist $\xi_{H_\alpha} = \xi_\alpha$ und

$$\Pi_1^h (x - \xi_\alpha) = \Phi(x),$$

so ist

$$\Phi(x) = \big(\Psi(x)\big)^g, \tag{13.}$$

und daher ist die Anzahl ν_p der reellen Wurzeln der Congruenz $\Phi(x) \equiv 0 \pmod{p}$ gleich der Anzahl der Zahlen $\xi_1, \xi_2, \cdots \xi_h$, welche die Congruenz $\xi_\alpha^p \equiv \xi_\alpha \pmod{\mathfrak{p}}$ befriedigen. Ist F die dem Primideal $\mathfrak{p}$ entsprechende Substitution von $\mathfrak{H}$, so ist $\xi_{H_\alpha}^p \equiv \xi_{H_\alpha F} \pmod{\mathfrak{p}}$. Damit also $\xi_{H_\alpha}^p \equiv \xi_{H_\alpha}$ sei, muss $\xi_{H_\alpha F} = \xi_{H_\alpha}$ sein, und folglich müssen $H_\alpha F$ und H_α in Bezug auf $\mathfrak{G}$ einander gleich sein. Die Zahl ν_p giebt daher an, wie viele der h Substitutionen

$$H_1 F\, H_1^{-1},\ H_2 F\, H_2^{-1}, \cdots H_h F\, H_h^{-1}$$

der Gruppe $\mathfrak{G}$ angehören. Ist F eine Substitution der λ^{ten} Classe, so stellt diese Reihe die sämmtlichen Substitutionen der λ^{ten} Classe und jede $\frac{h}{h_\lambda}$ Mal dar. Giebt es also g_λ Substitutionen der λ^{ten} Classe in $\mathfrak{G}$, so sind $g_\lambda \frac{h}{h_\lambda}$ jener h Substitutionen in $\mathfrak{G}$ enthalten, und folglich ist

$$\nu_p = g_\lambda \frac{h}{h_\lambda}. \tag{14.}$$

Die Anzahl der irreductibeln Factoren von $\Phi(x)$ ist ferner nach Formel (13.) gleich

$$m = g = \sum_1^l{}_\lambda g_\lambda. \tag{15.}$$

Durchläuft p_λ alle rationalen Primzahlen, die der λ^{ten} Classe von Substitutionen entsprechen, so ergiebt sich daher aus den Formeln (1.), (14.) und (15.)

$$\sum_1^l{}_\lambda \frac{h}{h_\lambda} g_\lambda (\Sigma p_\lambda^{-1-w}) = \Big(\sum_1^l{}_\lambda g_\lambda\Big) \log\left(\frac{1}{w}\right) + \mathfrak{P}(w).$$

Indem man hier für $\mathfrak{G}$ der Reihe nach alle cyklischen Untergruppen von $\mathfrak{H}$ setzt, erhält man eine Reihe von Gleichungen, die aber nicht ausreichen, um schliessen zu können, dass

$$\Sigma\, p_\lambda^{-1-w} = \frac{h_\lambda}{h} \log\left(\frac{1}{w}\right) + \mathfrak{P}_\lambda(w) \tag{16.}$$

ist. Zu den Theilgleichungen, in welche jene Relation zerfällt, führt folgende Überlegung: Ist r relativ prim zu f, so sind die Substitutionen F und F^r ähnlich im Sinne des § 1, aber nicht nothwendig conjugirt in Bezug auf $\mathfrak{H}$. Sind sie nicht conjugirt, so gehören sie zwei ver-

schiedenen Classen an, etwa der λ^{ten} und der μ^{ten} Classe. Da auch F eine Potenz von F^r ist, so ist jede Substitution von $\mathfrak{H}$, die mit der einen dieser beiden Substitutionen vertauschbar ist, auch mit der andern vertauschbar. Folglich ist $v_\lambda = v_\mu$, also auch $h_\lambda = h_\mu$. Ferner enthält die Gruppe $\mathfrak{G}$ entweder keine der beiden Substitutionen $H_\alpha F H_\alpha^{-1}$ und $H_\alpha F^r H_\alpha^{-1} = (H_\alpha F H_\alpha^{-1})^r$ oder beide, und mithin ist auch $g_\lambda = g_\mu$. Durchläuft r die $\varphi(f)$ Zahlen, die zu f theilerfremd sind, so vereinige ich die Classen, denen die Potenzen F^r angehören, zu einer Abtheilung. Eine solche Abtheilung kann man auch so erhalten: Man nehme eine cyklische Untergruppe von $\mathfrak{H}$ und die mit ihr conjugirten Gruppen. Ist f ihre Ordnung, so nehme man in dem System dieser Gruppen die Elemente, deren Ordnung gleich f ist.

Wenn nun die l Classen in m Abtheilungen zerfallen, so denke ich die Bezeichnung so gewählt, dass die Classen 1, 2, $\cdots m$ alle verschiedenen Abtheilungen angehören, diese m Classen aber seien in derselben Weise wie in § 1 angeordnet. Enthält die μ^{te} Abtheilung ausser der Classe μ noch die Classen $\alpha, \beta, \gamma, \cdots$, so ist $g_\mu = g_\alpha = g_\beta = g_\gamma \cdots$.

Ist also k_μ die Anzahl der in der μ^{ten} Abtheilung vereinigten Classen, so ist $g_\mu + g_\alpha + g_\beta + g_\gamma \cdots = k_\mu g_\mu$. Durchläuft nun p_μ die Primzahlen, die den sämmtlichen in der μ^{ten} Abtheilung vereinigten Classen entsprechen, so ist

$$\sum_1^m \frac{h}{h_\mu} g_\mu \left(\sum p_\mu^{-1-w}\right) = \left(\sum_1^m g_\mu k_\mu\right) \log\left(\frac{1}{w}\right) + \mathfrak{P}(w),$$

und daraus folgt, wie in § 2

$$\sum p_\mu^{-1-w} = \frac{h_\mu}{h} k_\mu \log\left(\frac{1}{w}\right) + \mathfrak{P}_\mu(w). \tag{17.}$$

Es ergiebt sich also das Resultat:

IV. *Hat in der Gruppe $\mathfrak{H}$ die Substitution F die Ordnung f, und durchläuft r die $\varphi(f)$ zu f theilerfremden Zahlen, so ist die Anzahl der verschiedenen Substitutionen von $\mathfrak{H}$, die den $\varphi(f)$ Potenzen F^r conjugirt sind, der Dichtigkeit der rationalen Primzahlen proportional, die diesen Classen von Substitutionen entsprechen.*

Wenn es gelänge die Formel (16.) zu beweisen, so würde sich für die Dichtigkeit der Primzahlen p_λ, die der λ^{ten} Classe von Substitutionen entsprechen, der einfache Ausdruck

$$D_\lambda = \frac{h_\lambda}{h} = \frac{1}{v_\lambda} \tag{18.}$$

ergeben, es würde also der Satz gelten:

V. *Jeder Classe von Substitutionen der Gruppe $\mathfrak{H}$ entsprechen unzählig viele rationale Primzahlen. Ihre Dichtigkeit ist der Anzahl der verschiedenen Substitutionen der Classe proportional.*

Oder:

Die Dichtigkeit der Primzahlen, die einer Classe von Substitutionen der Gruppe $\mathfrak{H}$ entsprechen, ist der Dichtigkeit der Classe gleich.

Den Primidealen $\mathfrak{p}_1, \mathfrak{p}_2, \cdots \mathfrak{p}_h$ entsprechen der Reihe nach die Substitutionen (10.), von denen v_λ gleich F sind. Unter den verschiedenen Primfactoren $\mathfrak{p}_1, \mathfrak{p}_2, \cdots \mathfrak{p}_e$ von p befinden sich folglich $\frac{v_\lambda}{f}$, die der Substitution F entsprechen. Nimmt man daher in die Reihe Σp_λ^{-1-w} jede Primzahl p nicht ein Mal, sondern so viele Male auf, als es der Substitution F entsprechende in p aufgehende Primideale giebt, so ist

$$\sum \frac{v_\lambda}{f} p_\lambda^{-1-w} = \frac{1}{f} \log\left(\frac{1}{w}\right) + \mathfrak{P}(w).$$

VI. *Jeder Substitution der Gruppe $\mathfrak{H}$ entsprechen unzählig viele Primideale. Ihre Dichtigkeit ist dem reciproken Werthe der Ordnung der Substitution gleich.*

Ausgegeben am 2. Juli.

Berlin, gedruckt in der Reichsdruckerei.