Jahresbericht

über das

vereinigte alt- und neustädtsche

Gymnasium zu Brandenburg

von Michaelis 1842 — Ostern 1844,

womit zu der

öffentlichen

Prüfung und Redeübung

aller Klassen

Dienstag, den 2. April,

Vormittags von 8½ Uhr und Nachmittags von 2 Uhr an,

im Namen der Lehrer

ehrerbietig einladet

F. W. BRAUT,

Königl. Professor und Director, Ritter des R. A. O. 4. Cl.

Vorangeht eine Abhandlung:

„Grundzüge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist“,

vom Mathematicus Schönemann.

Brandenburg.

Gedruckt bei J. J. Wiesike.

1844.

GRUNDZÜGE
einer
allgemeinen Theorie
der
höhern
CONGRUENZEN,
deren Modul eine reelle Primzahl ist.

Vorwort.

Die Veranlassung zur folgenden Untersuchung fand ich schon vor längerer Zeit in dem Auffinden des Satzes: dass die Gleichung für die p^{ten} Potenzen der Wurzeln einer Gleichung, deren Coefficienten ganze Zahlen sind, mit der ursprünglichen Gleichung in ihren entsprechenden Coefficienten nach dem Modul p congruent sei, wenn p eine Primzahl ist. Obschon dieser Satz nach einer Seite hin eine bedeutende Verallgemeinerung des bekannten *Fermat*'schen Satzes ist, so erkannte ich dennoch bald, dass er in dieser Gestalt unvollendet sei. Er lässt sich nämlich nur als eine Verallgemeinerung des Satzes ansehen, dass $a^p \equiv a\,(mod.\,p)$ sei, wenn a irgend eine Zahl und p eine Primzahl bedeutet, nicht aber als eine Verallgemeinerung des Satzes, dass $a^{p-1} \equiv 1\,(mod.\,p)$ sei, wenn a eine Zahl bedeutet, die nicht $\equiv 0\,(mod.\,p)$ ist. Da der *Fermat*'sche Satz nun aber vorzüglich nur in der letzten Form fruchtbar wird, so bemühte ich mich jenen allgemeinen Satz auf eine ähnliche Form zurückzuführen. Dies erreichte ich zwar bald, aber blos von einigen Einzelnheiten geleitet. Der Beweis für die Allgemeinheit des Satzes schien mir bei dem Wenigen, welches wir über die Form der Wurzeln einer Gleichung kennen, mit sehr grossen Schwierigkeiten verbunden. Hierzu kam, dass Proberechnungen wegen zu grosser Weitläuftigkeit fast unmöglich wurden. Ich versuchte daher neuerdings, sobald es meine Zeit gestattete, auf rein speculativem Wege, wenn es möglich wäre, den Beweis zu finden. Dies ist mir nun auf eine für mich überraschend einfache Weise gelungen. Es haben sich aber hierbei so äusserst wichtige Sätze und Aufschlüsse über die Lehre der Congruenzen ergeben, dass ich in denselben die Grundzüge einer allgemeinen Theorie der Congruenzen höherer Grade, deren Modul eine reelle Primzahl ist, erblicke. Der Hauptsatz steht mit dem *Fermat*'schen Satz auf der einen Seite und mit der *Gaussi*'schen Methode der Kreistheilung auf der andern Seite in dem engsten Zusammenhange. Aus demselben geht zugleich hervor, dass sich alle Congruenzen gewissermassen auf reine reduciren lassen.

Der berühmte Verfasser der *Disquisitiones Arithmeticae* hatte für den achten Abschnitt seines Werkes eine allgemeine Theorie der höhern Congruenzen bestimmt. Da indessen dieser achte Abschnitt nicht erschien, und auch, so viel mir bewusst ist, über diesen Gegenstand sonst nichts von dem Verfasser bekannt gemacht oder nur bestimmt angedeutet worden ist, (denn die Untersuchungen über imaginäre Moduln gehören in ein anderes Gebiet) so wage ich nicht zu entscheiden, ob und wie weit die vorliegrnde Arbeit mit den Untersuchungen dieses berühmten Mannes in Berührung stehe. Sollte ich vielleicht zum Theil denselben Sätzen meine Forschung gewidmet haben, wie der tiefsinnige Begründer der Lehre von den Congruenzen, so würde mich über die Einbusse der ersten Entdeckung das Bewustsein schadlos halten, auf selbstständigem Wege mit dem Streben eines solchen Geistes zusammengetroffen zu sein.

Bei der Ausarbeitung habe ich nur das Gewöhnlichste aus der Algebra und Arithmetik vorausgesetzt. Die Sätze, von welchen ich später Gebrauch machen musste, habe ich daher fast alle in den Vortrag verflochten. Wenn dies nun auch grösstentheils unter eigenthümlichem Gesichts-Punkte geschehen ist, so werden Kundige in manchen Sätzen und noch mehreren Beweisen etwas ganz Bekanntes erblicken. Doch schien die für dieselbeu hieraus entspringende Unbequemlichkeit viel geringer als diejenige, welche minder Bewanderten aus einer entgegengesetzten Art der Auseinander-Setzung entstanden wäre. Die höhere Arithmetik, welche mit ihren Hilfsmitteln in das innerste Wesen der Mathematik eingreift, und vielen Principien ein Feld vollständiger Gestaltung gewährt, die ohne sie noch lange unfruchtbar darnieder lägen, ist bis jetzt das Eigenthum so Weniger, dass eine grössere Verbreitung derselben gewiss nur im Interesse der Wissenschaft liegen kann. Sollte es mir gelungen sein, bei Einigen der Leser das Interesse von rein algebraischen Untersuchungen auf zahlentheoretische zu ziehen, so werde ich mich für die Mühe der Ausarbeitung belohnt halten.

Benutzt sind für die folgende Abhandlung vorzüglich der dritte Abschnitt der *Disquisitiones Arithmeticae* von *Gauss* und eine Abhandlung über symmetrische Functionen etc., welche ich im 19. Bande des *Crelle*'schen Journals bekannt gemacht habe.

Brandenburg,
den 29. Januar 1844.

Schönemann.

Einleitung.

§. 1.

Lehrsatz. **B**ezeichnet a irgend eine ganze Zahl, und b_0, b_1, b_2, ... b_{a-1} die kleinsten Reste, welche die Zahlen $0b$, $1b$, $2b$, ... $(a-1)b$ durch a getheilt lassen, so werden diese alle von einander verschieden sein, wenn b keinen gemeinschaftlichen Theiler mit a hat; denn wären irgend zwei Zahlen, deren Indices ν und μ sein mögen, gleich, also $b_\nu = b_\mu$, so müsste $\nu b - \mu b = (\nu - \mu) b$ durch a aufgehen, welches offenbar nicht möglich ist, da b zu a relative Primzahl, und $\nu - \mu$ kleiner als a ist. Da also sämmtliche Reste b_0, b_1, b_2, ... b_{a-1} von einander verschieden sind, und es nur die a verschiedenen Reste $0, 1, 2, \ldots a-1$ giebt, so folgt, dass jene Zahlen mit diesen, wenn auch in anderer Ordnung, übereinstimmen werden. Hätte nun aber b mit a den grössten gemeinschaftlichen Theiler δ, so werden die Reste der Zahlen $0\frac{b}{\delta}$, $1 . \frac{b}{\delta}$, $2 . \frac{b}{\delta}$, ... $a - 1 . \frac{b}{\delta}$ wieder mit den Resten $0, 1, 2, \ldots . a - 1$ übereinstimmen. Denkt man sich diese Zahlen aber als Reste nach dem Divisor $\frac{a}{\delta}$, so ist klar, dass die Reste der Zahlen $0\frac{b}{\delta}, 1 . \frac{b}{\delta}, 2 . \frac{b}{\delta}, \ldots \left(\frac{a}{\delta} - 1\right)\frac{b}{\delta}$ mit den Zahlen $0, 1, 2, \ldots \frac{a}{\delta} - 1$ übereinstimmen, und dass diese Zahlen in den Resten der Zahlen $0\frac{b}{\delta}$, $1 . \frac{b}{\delta}$, $2\frac{b}{\delta}$, ... $a-1\frac{b}{\delta}$, δ mal enthalten sein werden.

§. 2.

Betrachtet man jetzt die Gleichung $x^a - 1 = 0$, und bezeichnet eine primitive Wurzel derselben durch α, so kann man bekanntlich die sämmtlichen Wurzeln jener Gleichung durch α^0, α^1, α^2, ... α^{a-1} darstellen. Die $b$ten Potenzen dieser Wurzeln werden folglich durch α^{0b}, $\alpha^{1 \cdot b}$, ... $\alpha^{a-1 \cdot b}$ dargestellt. Hat nun b mit a den grössten gemeinschaftlichen Theiler δ, so kann man jene Ausdrücke auch so schreiben:

$$\left(\alpha^{\delta}\right)^{0 . \frac{b}{\delta}}, \left(\alpha^{\delta}\right)^{1 . \frac{b}{\delta}}, \left(\alpha^{\delta}\right)^{2 . \frac{b}{\delta}}, \ldots . \left(\alpha^{\delta}\right)^{a-1 . \frac{b}{\delta}}.$$

Nun wird aber α^δ selbst eine primitive Wurzel der Gleichung $x^{\frac{a}{\delta}} - 1 = 0$ sein, und die Zahlen $0.\frac{b}{\delta}$, $1.\frac{b}{\delta}$, $2.\frac{b}{\delta}$, ... $a-1.\frac{b}{\delta}$ werden, durch $\frac{a}{\delta}$ getheilt, δmal die Reste $0, 1, 2, \ldots \frac{a}{\delta}-1$ erzeugen. Mithin werden die Ausdrücke $\left(\alpha^{\delta}\right)^{0\cdot\frac{b}{\delta}}$, $\left(\alpha^{\delta}\right)^{1\cdot\frac{b}{\delta}}$, $\left(\alpha^{\delta}\right)^{2\cdot\frac{b}{\delta}} \ldots\ldots$ $\left(\alpha^{\delta}\right)^{a-1\cdot\frac{b}{\delta}}$ δ mal die sämmtlichen Wurzeln der Gleichung $x^{\frac{a}{\delta}}-1=0$ enthalten. Die Gleichung für b^{ten} Potenzen der Wurzeln der Gleichung $x^a-1=0$, wird also unter der Form $\left(x^{\frac{a}{\delta}}-1\right)^{\delta}=0$ auftreten. Die Coefficienten dieser Gleichung werden folglich ganze positive Zahlen oder 0 sein. — Man hann nun behaupten, dass jede symmetrische Function der Ausdrücke $\alpha^0, \alpha^1, \alpha^2, \ldots\ldots \alpha^{a-1}$ sich als ganze in ganzen Zahlen ausgedrückte Function solcher Coefficienten, folglich auch als ganze positive oder negative Zahl oder auch als 0 werde darstellen lassen.

Um dies zu beweisen führe man folgende Bezeichnung ein: eine symmetrische Function von m Elementen, die aus lauter einzelnen Producten zusammengesetzt ist, in denen n verschiedene Elemente vorkommen, von denen das 1^{te} in die $c_1{}^{te}$, das zweite in die $c_2{}^{te}\ldots$, das n^{te} in die $c_n{}^{te}$ Potenz erhoben ist (und jede symmetrische ganze Function ist bekanntlich ein Aggregat solcher Functionen) bezeichne man durch $[c_1\ c_2\ c_3 \ldots c_n]$; so dass also z. B. für die Elemente α, β, γ, δ die symmetrische Function $\alpha\beta\gamma^2+\alpha\beta\delta^2+\alpha\gamma\delta^2+\alpha\delta\beta^2+\alpha\delta\gamma^2+\beta\gamma\alpha^2+\beta\gamma\delta^2+\beta\gamma\alpha^2+\beta\delta\gamma^2+\gamma\delta\alpha^2+\gamma\delta\beta^2$ durch $[1, 1, 2]$ dargestellt wird. Fallen nun diese m Elemente mit den Wurzeln der Gleichung $x^a-1=0$ zusammen, so wird sich der Coefficient von x^{a-n} in der Entwickelung von $\left(x^{\frac{a}{\delta}}-1\right)^{\delta}$ durch $(-1)^n\,[b_1\ b_2 \ldots\ldots b_n]$ darstellen lassen, wo $b=b_1=b_2=\ldots\ldots=b_n$ ist. Dies folgt unmittelbar aus der Identität der beiden Ausdrücke $\left(x^{\frac{a}{\delta}}-1\right)^{\delta}$ und $(x-\alpha^{0\cdot b})(x-\alpha^{1\cdot b})(x-\alpha^{2\cdot b}) \ldots\ldots (x-\alpha^{(a-1)b})$.

Es lässt sich nun leicht nachweisen, dass sich jede symmetrische Function $[c_1\ c_2 \ldots c_n]$ als ganze in ganzen Zahlen ausgedrückte Function anderer symmetrischen Functionen, die durch lauter gleiche, in Klammern eingeschlossene Zahlen angedeutet werden, ausdrücken lasse. Sind nämlich von den Zahlen $c_1, c_2, \ldots c_n$ eine Anzahl μ gleich α_1, eine zweite Anzahl ν gleich β_1, eine dritte Anzahl ρ gleich γ_1 etc., und setzt man $\alpha_1=\alpha_2=\ldots=\alpha_\mu$, $\beta_1=\beta_2\ldots\ldots=\beta_\nu$, $\gamma_1=\gamma_2\ldots\ldots=\gamma_\rho$ etc., so wird offenbar das Product $[\alpha_1\ \alpha_2\ldots\alpha_\mu]\ [\beta_1\ \beta_2\ldots\beta_\nu]\ [\gamma_1\ \gamma_2\ldots\gamma_\rho]$ etc. aus $[c_1\ c_2 \ldots\ldots c_n]$ und anderen symmetrischen Functionen bestehen, deren einzelne Summanden jedoch nur eine geringere Anzahl von Elementen enthalten kann, als n andeutet. Man erhält demnach $[\alpha_1\ \alpha_2\ldots\alpha_\mu]\ [\beta_1\ \beta_2\ldots\beta_\nu]\ [\gamma_1\ \gamma_2\ldots\gamma_\rho]$ etc. $=[c_1\ c_2\ldots c_n]+\Sigma$, wo Σ ein Aggregat einfacher symmetrischer Functionen bezeichnet, in deren einzelnen Summanden weniger als n verschiedene Elemente auftreten.

Demnach ist $[c_1 c_2 \dots c_n] = [\alpha_1 \alpha_2 \dots \alpha_\mu][\beta_1 \beta_2 \dots \beta_\nu][\gamma_1 \gamma_2 \dots \gamma_\varrho]$ etc. $- \Sigma$; und da man jede einzelne Function, die in Σ enthalten ist, wieder ähnlich transformiren kann, so ist klar, dass $[c_1 c_2 \dots c_n]$ zuletzt als ein Aggregat von Producten hervorgehen muss, deren jedes aus symmetrischen Functionen besteht, die durch gleiche eingeklammerte Zahlen angedeutet werden.

Beispiele.

1) $[8,5,3] = [8][5][3] - [13,3] - [11,5] - [8,8]$
Es ist aber $[13,3] = [13][3] - [16]$, und
$[11,5] = [11][5] - [16]$ folglich
$[8,5,3] = [8][5][3] - [8,8] - [13][3] - [11][5] + 2[16]$.

2) $[8,8,3] = [8,8][3] - [11,8]$; $[11,8] = [11][8] - [19]$, also
$[8,8,3] = [8,8][3] - [11][8] + [19]$.

3) $[8,8,3,3] = [8,8][3,3] - [11,8,3] - [11,11]$; $[11,8,3] = [11][8][3] - [19,3] - [14,8] - [11,11]$; $[19,3] = [19][3] - [22]$; $[14,8] = [14][8] - [22]$ folglich $[8,8,3,3] = [8,8][3,3] - [11][8][3] + [19][3] + [14][8] - 2[22]$.

Setzt man nun die Wurzeln der Gleichung $x^v - 1 = 0$ als Elemente der symmetrischen Functionen, so werden die durch lauter gleiche in Klammern eingeschlossene Zahlen angedeuteten Functionen mit den positiven oder negativen Coefficienten der Gleichungen für die ganzen Potenzen der Wurzeln der Gleichung $x^v - 1 = 0$ übereinstimmen, folglich nach dem Vorhergehenden ganze Zahlen sein; und da sich ferner jede ganze symmetrische Function jener Wurzeln als ganze Function dieser Zahlen entwickeln lässt, so folgt, dass diese Function selbst durch ganze Zahlen oder 0 werde darzustellen sein.

§. 3.

Aufgabe. Wenn eine Gleichung vom n^{ten} Grade $x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots a_n = 0$ vorliegt, eine andere Gleichung aufzustellen, welche die p^{ten} Potenzen der Wurzeln der vorliegenden Gleichung als Wurzeln enthält; vorausgesetzt p bedeute irgend eine ganze positive Zahl.

Auflösung. Gesetzt $b_1, b_2, b_3, \dots b_n$ wären die Wurzeln der vorliegenden Gleichung, und man hätte mithin $x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_n = (x - b_1)(x - b_2) \dots (x - b_n)$, so erhielte man die verlangte Gleichung, indem man das Product $(x^p - b_1^p)(x^p - b_2^p) \dots (x^p - b_n^p)$ entwickelte, dies gleich 0 setzte, und für x^p irgend eine andere Unbekannte z einführte. Bezeichnet nun α eine primitive Wurzel der Gleichung $x^p - 1 = 0$, so ist bekanntlich $x^p - b^p = (x - b)(x - b\alpha) \dots (x - b\alpha^{p-1})$. Werden auf diese Weise sämmtliche Factoren zerlegt, so geht das Product $(x^p - b_1^p)(x - b_2^p) \dots (x^p - b_n^p)$ in folgendes über:

$$
\begin{array}{l}
(x - b_1)(x - b_2)(x - b_5) \dots\dots\dots\dots (x - b_n)\,. \\
(x - b_1\alpha)(v - b_2\alpha)(x - b_3\alpha) \dots\dots\dots (x - b_n\alpha)\,. \\
(x - b_1\alpha^1)(x - b_2\alpha^2)(x - b_3\alpha^3) \dots\dots (x - b_n\alpha^2)\,. \\
\dots\dots\dots\dots\dots\dots\dots\dots\dots \\
(x - b_1\alpha^{p-1})(x - b_2\alpha^{p-1})(x - b_3\alpha^{p-1}) \dots (x - b_n\alpha^{p-1})\,.
\end{array}
$$

Jedes der Producte, die in einer Horizontal-Reihe enthalten sind, kann man leicht durch die ursprüngliche Gleichung und durch α darstellen. Man erhält dann das obige Product durch

$$
\begin{aligned}
&(x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots\ldots\ldots\ldots + a_n) \,.\\
&(x^n + a_1 \alpha x^{n-1} + a_2 \alpha^2 x^{n-2} + \ldots\ldots\ldots\ldots + a_n \alpha^n) \,.\\
&(x^n + a_1 \alpha^2 x^{n-1} + a_2 \alpha^4 x^{n-2} + \ldots\ldots\ldots\ldots + a_n \alpha^{2n}) \,.\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&(x^n + a_1 \alpha^{p-1} x^{n-1} + a_2 \alpha^{2(p-1)} x^{n-2} + \ldots\ldots + a_n \alpha^{(p-1)n})
\end{aligned}
$$

ausgedrückt.

Betrachtet man nun den Coefficienten irgend einer q^{ten} Potenz von x, so besteht dieser offenbar aus einer Summe von Gliedern, deren jedes einzelne ein Product aus den verschiedenen Coefficienten der ersten Gleichung ist, die der Bedingung unterworfen sind, dass die Summe ihrer Indices gleich $pn - q$ ist, und aus einer symmetrischen Function der Ausdrücke α^0, α^1, α^2, $\ldots \alpha^{p-1}$, welche nach §. 2. sich muss durch eine ganze Zahl darstellen lassen. Bezeichnet man nun die Coefficienten der Gleichung für die p^{ten} Potenzen der Wurzeln der ursprünglichen Gleichung durch a_{1_p}, a_{2_p}, $a_{3_p} \ldots\ldots a_{n_p}$, so folgt, dass dieselben ganze in ganzen Zahlen ausgedrückte Functionen der Coefficienten der ursprünglichen Gleichung seyn werden. Aus §. 2. folgt ferner, dass sich jede symmetrische Function der Wurzeln der ursprünglichen Gleichung als ganze Function der Grössen a_{1_p}, a_{2_p}, $\ldots\ldots a_{n_p}$ (wo p verschiedene ganze Zahlen bedeuten kann) ausdrücken lasse; daher folgt in Verbindung mit dem Vorhergehenden:

> dass sich jede symmetrische ganze Function der Wurzeln einer Gleichung als ganze in ganzen Zahlen ausgedrückte Function der Coefficienten dieser Gleichung ausdrücken lasse,

und ferner:

> dass sich jede symmetrische ganze Function der Wurzeln einer Gleichung, deren Coefficienten ganze Zahlen sind, selbst werde durch eine ganze Zahl ausdrücken lassen.

(Weitere Entwickelungen über diesen Gegenstand findet man in der erwähnten Abhandlung über symmetrische Functionen.)

§. 4.

Lehrsatz. Die symmetrischen Functionen sämmtlicher Wurzeln einer Gleichung ausser einer, lassen sich als ganze in ganzen Zahlen ausgedrückte Functionen jener einen und der Coefficienten der Gleichung darstellen.

Beweis. Es sei $x^n + a_1 x^{n-1} + \ldots + a^n = 0$ die Gleichung, und α_1, α_2, $\ldots \alpha_n$ die Wurzeln derselben, so ist nach der obigen Bezeichnung, wenn man diese Wurzeln selbst als Elemente von symmetrischen Functionen ansieht $[1] = -a_1$, $[11] = a_2$, $[111] = -a_3$ etc. Setzt man nun $\alpha_2, \alpha_3, \ldots \alpha_n$ als Elemente von symmetrischen Functionen, so mögen diese zum Unterschiede von jenen durch einen hinzugefügten Index bezeichnet werden, so dass also $[1]_1 = \alpha_2 + \alpha_3 + \ldots + \alpha_n$ $[11]_1 = \alpha_2\alpha_3 + \alpha_2\alpha_4 + \ldots + \alpha_{n-1}\alpha_n$ etc. ist. Offenbar ist nun $[1] = \alpha_1 + [1]_1$, $[11] = \alpha_1 [1]_1 + [11]_1$, $[111] = \alpha_1 [11]_1 + [111]_1$ $[1111] = \alpha_1 [111]_1 + [1111]_1$ etc. Hieraus folgt nun $-a_1 = \alpha_1 + [1]_1$, $+a_2 = \alpha_1 [1]_1 + [11]_1$, $-a_3 = \alpha_1 [11]_1 + [111]_1$, $a_4 = \alpha_1 [111]_1 + [1111]_1$ etc.

und hieraus $[1]_1 = -(a_1 + \alpha_1)$ $[11]_1 = a_2 + a_1\alpha_1 + \alpha_1^2$, $[111] = -(a_3 + a_2\alpha_1 + a_1\alpha_1^2 + \alpha_1^3)$ $[1111] = a_4 + a_3\alpha_1 + a_2\alpha_1^2 + a_1\alpha_1^3 + \alpha_1^4$ und im Allgemeinen die Summe der Combinationen zu m Elementen von $\alpha_2, \alpha_3, \ldots \alpha_n$ gleich $(-1)^m (a_m + a_{m-1}\alpha_1 + a_{m-2}\alpha_1^2 + \ldots a_1\alpha_1^{m-1} + \alpha_1^m)$. Da nun alle symmetrischen ganzen Functionen von $\alpha_2\,\alpha_3 \ldots\ldots \alpha_n$ sich nach §. 2. als ganze in ganzen Zahlen ausgedrückte Functionen von $[1]_1$, $[11]_1$, $[111]_1$, etc. darstellen lassen, und diese ähnliche Functionen von α_1 und den Coefficienten der Gleichung sind, so folgt, dass die symmetrischen Functionen von $\alpha_2, \alpha_3, \ldots \alpha_n$ sich ebenfalls als ganze in ganzen Zahlen ausgedrückte Functionen von α_1 und den Coefficienten der Gleichung darstellen lassen.

Es ist übrigens leicht zu sehen, dass man obige Entwickelungen auch aus der Division von $x^n + a_1 x^{n-1} + \ldots + a_n$ durch $x - \alpha_1$ hätte ableiten können.

Anmerkung. Die Gleichung für $\alpha_2, \alpha_3, \ldots \alpha_n$ wird offenbar nun folgende sein: $x^{n-1} + (a_1 + \alpha_1)x^{n-2} + (a_2 + a_1\alpha_1 + \alpha_1^2)x^{n-3} + \ldots\ldots$

$$+ (a_{n-1} + a_{n-2}\alpha_1 + a_{n-3}\alpha_1^2 + a_{n-4}\alpha_1^3 + \ldots\ldots a_1\alpha_1^{n-2} + \alpha_1^{n-1}) = 0.$$

Setzt man voraus, dass diese Gleichung für $x = \alpha_1$ realisirt wird, so findet man, wenn man statt x, α_1 setzt, und dieselbe nach α_1 ordnet

$$n\alpha_1^{n-1} + (n-1)a_1\alpha_1^{n-2} + (n-2)a_2\alpha_1^{n-3} + \ldots\ldots a_{n-1} = 0.$$

Hieraus folgert man leicht, dass, wenn die Gleichung $x^n + a_1 x^{n-1} + \ldots + a_n = 0$ zwei gleiche Wurzeln α_1 haben soll, sie eben diese Wurzel mit der Gleichung $nx^{n-1} + (n-1)a_1 x^{n-2} + (n-2)a_2 x^{n-3} + \ldots + a_{n-1} = 0$ gemeinschaftlich haben müsste. — Dieser Satz wird fast in allen Lehrbüchern aus der Differential-Rechnung abgeleitet, welches offenbar nicht naturgemäss ist.

§. 5.

Erklärung und Lehrsatz. Eine ganze rationale Function von x, deren Coefficienten rationale Zahlen sind, soll *irreductibel* heissen, wenn sie sich nicht in zwei Factoren zerfällen lässt, von denen jeder wieder eine ähnliche Function von x von einem niedrigeren Grade als die ursprüngliche ist.

Setzt man eine irreductible Function von x gleich 0, so soll diese Gleichung ebenfalls irreductibel heissen.

Eine irreductibele Gleichung kann mit einer andern, deren Coefficienten ebenfalls rationale Zahlen sind, keine Wurzel gemeinschaftlich haben, ohne alle Wurzeln mit ihr gemeinschaftlich zu haben.

Beweis. Gesetzt $fx = 0$ sei eine irreductibele Gleichung, so ist zunächst zu zeigen, dass, wenn $\phi x = 0$ eine Gleichung von einem niedrigeren Grade als $fx = 0$ bedeutet, deren Coefficienten ebenfalls rationale Zahlen sind, dass alsdann fx und ϕx keine Wurzel gemeinschaftlich haben können. Unter dieser Voraussetzung müsste sich nämlich ein gemeinschaftlicher algebraischer Theiler, dessen Coefficienten rationale Zahlen sind, nach der Methode den grössten algebraischen Theiler zweier Functionen zu finden, zwischen ϕx und fx aufstellen lassen. Da aber fx überhaupt keinen solchen Theiler zulassen kann, so ist die erste Voraussetzung nicht statthaft. Gesetzt nun ϕx sei von gleichem oder höherem Grade mit fx so bringe man ϕx durch algebraische Division mit fx auf die Form $fx \,.\, Qx + Rx$, wo Qx den algebraischen Quotienten und Rx den Rest angiebt, welchen ϕx bei der Division durch fx erzeugt. Hätte nun ϕx oder $fx \cdot Qx + Rx$ eine gemeinschaftliche Wurzel mit fx, so müsste auch Rx dieselbe haben. Da aber Rx von einem niedrigeren Grade als fx ist, so geht dies nicht an, nach dem eben Bewiesenen. Es kann mithin unter der gemachten Voraussetzung gar kein Rx existiren, oder es muss sich ϕx ohne Rest durch fx theilen lassen. Es enthält mithin die Gleichung $\phi x = 0$ sämmtliche Wurzeln der Gleichung $fx = 0$.

Zusatz. Aus der Anmerkung des §. 4. ergiebt sich nun leicht, dass die Gleichung $fx = 0$ nicht zwei gleiche Wurzeln haben könne.

Anmerkung. Die in diesem §. entwickelten Sätze gebühren dem berühmten Mathematiker *Abel.* Vergl. *Crelle's* Journal Tom. IV. Pg. 131.

§. 6.

Lehrsatz. Ist die Gleichung $fx = 0$ irreductibel, und sind $\alpha_1, \alpha_2, \ldots\ldots \alpha_n$ die Wurzeln dieser Gleichung, so sind die Werthe irgend einer rationalen Function von x, deren Coefficienten rationale Zahlen sind, wenn man in dieselbe nach der Reihe $\alpha_1, \alpha_2, \ldots \alpha_n$ statt x setzt, die Wurzeln einer irreductibeln Gleichung.

Beweis. Bezeichnet man die rationale Function von x durch ϕx, so werden $\phi\alpha_1, \phi\alpha_2, \ldots\ldots \phi\alpha_n$ von der Gleichung $(z - \phi\alpha_1)(z - \phi\alpha_2) \ldots\ldots (z - \phi\alpha_n) = 0$ abhängen. Offenbar werden die Coefficienten dieser Gleichung symmetrische Functionen von $\alpha_1, \alpha_2, \ldots \alpha_n$ sein, und sich mithin durch Coefficienten von fx rational darstellen lassen. Da diese Coefficienten selbst aber rationale Zahlen sind, so werden die Coefficienten von $(z - \phi\alpha_1)(z - \phi\alpha_2) \ldots\ldots (z - \phi\alpha_n)$ ebenfalls rationale Zahlen seyn. Setzt man nun $(z - \phi\alpha_1)(z - \phi\alpha_2) \ldots (z - \phi\alpha_n) = Fz$, so ist zu zeigen, dass Fz die Potenz eines irreductibeln Ausdruckes sei. Gesetzt nun Fz sei dem Product zweier in rationalen Zahlen ausgedrückten Functionen von niedrigerem Grade als dem n^{ten} gleich, so kann man die eine derselben, welche mit dz bezeichnet werden soll, als die Potenz einer irreductibelen Function von z ansehen, die mit dem anderen Factor $d_1 z$ keinen algebraischen Divisor mehr gemeinschaftlich hat. Da nun $Dz = dz\, d_1 z$ ist, so müssen die Wurzeln der Gleichung $dz = 0$ und $d_1 z = 0$ in $\phi\alpha_1, \phi\alpha_2, \ldots\ldots \phi\alpha_n$ enthalten sein. Setzt man nun in die beiden Gleichungen $dz = 0$ und $d_1 z = 0$ statt z seinen Ausdruck in x, nämlich ϕx, so müssen die Gleichungen $d\phi x = 0$ und $d_1\phi x = 0$ mit der Gleichung $fx = 0$ gewisse Wurzeln gemeinschaftlich haben. Deshalb muss aber fx sowohl ein Factor von $d\phi x$ wie von $d_1\phi x$ sein (§. 5.). Offenbar hätten also die Gleichungen $dz = 0$ und $d_1 z = 0$ die Wurzeln $\phi\alpha_1, \phi\alpha_2, \ldots\ldots \phi\alpha_n$ gemeinschaftlich. Nennt man nun δz den irreductibeln Ausdruck von z, von dem dz Potenz ist, so müssen auch die Gleichungen $dz = 0$ und $\delta z = 0$ die Wurzeln $\phi\alpha_1, \phi\alpha_2, \ldots\ldots \phi\alpha_n$ gemeinschaftlich haben. Mithin müssten auch δz und $d_1 z$ diese Wurzeln gemeinschaftlich haben. Dann würde aber folgen, dass δz ebenfalls ein Factor von $d_1 z$ sein müsse. Dies ist aber gegen die Voraussetzung. Es muss mithin Fz allein durch dz, welches eine Potenz des irreductibeln Factors δz ist, dargestellt werden, und mithin hängen die Werthe $\phi\alpha_1, \phi\alpha_2, \ldots\ldots \phi\alpha_n$ allein von der irreductibeln Gleichung $\delta z = 0$ ab.

§. 7.

Erklärung und Lehrsatz. Ist $fx=0$ eine Gleichung vom n^{ten} Grade, deren Wurzeln $\alpha_1, \alpha_2, \ldots \alpha_n$ sind, und $\phi x=0$ eine Gleichung vom m^{ten} Grade, deren Wurzeln $\beta_1, \beta_2, \ldots\ldots \beta_m$ sind, so soll das Product $f\beta_1 . f\beta_2 \ldots\ldots f\beta_m$ die Norm von f in Bezug auf ϕ heissen, und durch Nf_ϕ oder $N(f_\phi)$ bezeichnet werden. Da Nf_ϕ eine symmetrische Function der Wurzeln von $\phi x=0$ ist, so lässt es sich durch die Coefficienten dieser Gleichung und durch ganze Zahlen ausdrücken (§. 3.).

Sind die Coefficienten der höchsten Potenzen von fx und ϕx gleich 1, so ist die Norm von f in Bezug auf ϕ ist gleich der Norm von ϕ in Bezug auf f, positiv oder negativ genommen, jenachdem $n.m$ gerade oder ungerade ist, oder in allgemeinen Zeichen $Nf_\phi = N\phi_f(-1)^{mn}$.

Beweis. Da $\alpha_1, \alpha_2, \ldots \alpha_n$ die Wurzeln von $fx=0$ sind, und $\beta_1, \beta_2, \ldots \beta_m$ die Wurzeln von $\phi x=0$, so kann man $fx=(x-\alpha_1)(x-\alpha_2) \ldots (x-\alpha_n)$ und $\phi x = (x-\beta_1)(x-\beta_2) \ldots (x-\beta_m)$ setzen. Offenbar ist nun

$$\begin{aligned} Nf_\phi = f\beta_1\, f\beta_2 \ldots f\beta_m = {} & (\beta_1-\alpha_1)(\beta_1-\alpha_2)\ldots\ldots(\beta_1-\alpha_n) \,. \\ & (\beta_2-\alpha_1)(\beta_2-\alpha_2)\ldots\ldots(\beta_2-\alpha_n) \,. \\ & \ldots\ldots\ldots\ldots\ldots\ldots \\ & (\beta_m-\alpha_1)(\beta_m-\alpha_2)\ldots\ldots(\beta_m-\alpha_n) \end{aligned}$$

und

$$\begin{aligned} N\phi_f = \phi\alpha_1\, \phi\alpha_2 \ldots\ldots \phi\alpha_n = {} & (\alpha_1-\beta_1)(\alpha_1-\beta_2)\ldots\ldots(\alpha_1-\beta_m) \,. \\ & (\alpha_2-\beta_1)(\alpha_2-\beta_2)\ldots\ldots(\alpha_2-\beta_m) \,. \\ & \ldots\ldots\ldots\ldots\ldots\ldots \\ & (\alpha_n-\beta_m)(\alpha_n-\beta_m)\ldots\ldots(\alpha_n-\beta_m) \,. \end{aligned}$$

Vergleicht man nun die in einer Horizontal-Reihe stehenden Factoren des einen Products mit den in einer Vertikal-Reihe stehenden des andern, so findet man, dass die einen die negativen Werthe der andern bilden, und hieraus folgt der Satz unmittelbar.

§. 8.

Lehrsatz. Ist $fx=0$ eine irreductibele Gleichung und $\phi x=0$ eine Gleichung, deren Coefficienten rationale Zahlen sind, so ist fx ein algebraischer Divisor von ϕx, wenn $Nf_\phi=0$ ist.

Beweis. Offenbar kann Nf_ϕ nur dann gleich 0 werden, wenn die Gleichungen $fx=0$ und $\phi x=0$ eine gleiche Wurzel haben, alsdann ist aber $f\phi$ ein algebraischer Divisor von ϕx (§. 5.).

§. 9.

Erklärung und Lehrsatz. Zwei ganze Zahlen, welche durch eine Primzahl p getheilt gleiche Reste geben, heissen nach dieser Primzahl congruent, die Primzahl selbst wird alsdann der Modul genannt. Das Zeichen für die Congruenz ist $\equiv$, und $a \equiv b\ (mod.\, p)$ heisst, dass a und b durch p getheilt gleiche Reste geben.

Bedeuten a und b zwei ganze Zahlen, so lässt sich x stets so bestimmen, dass $ax \equiv b \,(mod. p)$ sei, vorausgesetzt a ist nicht $\equiv 0 \,(mod. p)$.

Beweis. Da a keinen gemeinschaftlichen Theiler mit p haben kann, so werden die Reste, welche $a \,.\, 0$, $a \,.\, 1$, $a \,.\, 2 \ldots a(p-1)$ durch p getheilt erzeugen, sämmtlich verschieden sein (§. 1.). Da es aber nur p verschiedene Reste nach dem Modul p giebt, so muss irgend eins dieser Producte denselben Rest wie b geben, und offenbar wird alsdann der Factor, in den a multiplicirt ist, das gesuchte x sein.

Grundzüge
einer
allgemeinen Theorie der höhern Congruenzen,
deren Modul eine reelle Primzahl ist.

---

§. 1.

Erklärungen. Eine rationale ganze Function von x in welcher diese Grösse bis zum n^{ten} Grade steigt und deren Coefficienten ganze Zahlen sind, wird in Folgendem schlechtweg ein Ausdruck vom n^{ten} Grade genannt werden. Zwei solche Ausdrücke werden ferner nach einer Primzahl p congruent heissen, wenn die Coefficienten der entsprechenden Potenzen von x in beiden nach dem Modul p congruent sind, und sollen fortan ebenfalls durch das Zeichen $\equiv$ verbunden werden, so dass also

$$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n \equiv b_0 x^n + b_1 x^{n-1} + b_2 x^{n-2} + \ldots + b_n \,(mod. p)$$

nichts weiter heisst, als dass $a_0 \equiv b_0$, $a_1 \equiv b_1$, $a_2 \equiv b_2 \ldots a_n \equiv b_n$ in Bezug auf den Modul p ist.

Ein solcher Ausdruck wird ein *einfacher* genannt, wenn der Coefficient der höchsten Potenz von x gleich 1, ein *vielfacher*, wenn derselbe weder 1 noch ein Vielfaches von p ist, dahingegen ein Ausdruck, in welchem der Coefficient der höchsten Potenz von x nebst mehreren der folgenden ein Vielfaches von p ist, nach der Natur des Gegenstandes der folgenden Untersuchung demjenigen niedrigeren Grade beigesellt wird, welcher die höchste Potenz von x angiebt, deren Coefficient nicht durch p aufgeht.

Setzt man einen Ausdruck gleich 0, so sollen die Wurzeln der hieraus hervorgehenden Gleichung auch Wurzeln des Ausdrucks heissen.

§. 2.

Lehrsatz. Jeder vielfache Ausdruck von x ist einem einfachen Ausdruck desselben Grades multiplicirt in den Coefficienten der höchsten Potenz von x nach irgend einem Modul p congruent.

Beweis. Sei der vielfache Ausdruck von x, $a_0x^n + a_1x^{n-1} + \ldots\ldots + a_n$, so ergiebt sich, wenn man α_1, α_2, $\ldots$ α_n durch die Congruenzen $a_0\alpha_1 \equiv a_1 (mod.\ p)$, $a_0\alpha_2 \equiv a_2 (mod.\ p)$ $\ldots\ldots$ $a_0\alpha_n \equiv (mod.\ p)$ bestimmt (§. 9. Einl.) dass $a_0x^n + a_1x^{n-1} + \ldots\ldots + a_n \equiv a_0 \{x^n + \alpha_1x^{n-1} + \ldots\ldots x_n\} (mod.\ p)$ sei. Hierdurch ist der Satz bewiesen.

Zusatz. Wenn mehrere der ersten Coefficienten a_0, a_1, a_2 etc. hinter einander $\equiv 0 (mod.\ p)$ nicht aber der ganze Ausdruck $\equiv 0 (mod.\ p)$ wird, so ist er wiederum congruent dem Product des Coefficienten der höchsten Potenz von x, der nicht $\equiv 0 (mod.\ p)$ wird, in einen einfachen Ausdruck desselben Grades.

§. 3.

Erklärungen. Ist es möglich ein Product zweier Ausdrücke aufzustellen (von denen aber keine einem niedrigeren Grade als dem ersten angehört) das einem gegebenen Ausdrucke nach dem Modul p congruent wird, so soll jeder der Factoren *ein Factor oder ein Divisor des gegebenen Ausdrucks in Bezug auf den Modul p*, oder wenn keine Zweideutigkeit zu befürchten ist, bloss ein Factor oder Divisor desselben heissen. Sind jene Factoren einfache Ausdrücke, so sollen sie *einfache Factoren oder Divisoren* des gegebenen Ausdruckes genannt werden.

Ein Ausdruck vom n^{ten} Grade, der keinen Divisor hat, soll ein *irreductibeler Ausdruck vom n^{ten} Grade* heissen.

Ist also $a_0x^n + a_1x^{n-1} + \ldots\ldots + a_n \equiv (b_0x^m + b_1x^{m-1} + \ldots + b_m)(c_0x^{n-m} + c_1x^{n-m-1} + \ldots\ldots + c_m) (mod.\ p)$ und $m < n$ und $m > 1$, so sollen $b_0x^m + b_1x^{m-1} + \ldots\ldots + b_m$ und $c_0x^{n-m} + c_1x^{n-m-1} + \ldots\ldots + c_{n-m}$ Factoren oder Divisoren von $a_0x^n + a_1x^{n-1} + \ldots + a_n$ heissen. Bsetimmt man ferner β_1, β_2, $\ldots\ldots \beta_m$ so, dass $b_0x^m + b_1x^{m-1} + \ldots + b_m \equiv b_0(x^m + \beta_1x^{m-1} + \beta_2x^{m-2} + \ldots + \beta_m) (mod.\ p)$ ist, so wird der einfache Ausdruck $x^m + \beta_1x^{m-1} + \ldots \beta_m$ ein einfacher Factor oder Divisor von $a_0x^n + a_1x^{n-1} + \ldots\ldots + a_n$ heissen.

Zusatz. Die obige Congruenz kann man nun offenbar als Gleichung auch so schreiben; $a_0x^n + a_1x^{n-1} + \ldots\ldots + a_n = b_0(x_m + \beta_1x^{m-1} + \ldots + \beta_m)(c_0x^{n-m} + c_1x^{n-m-1} + \ldots\ldots + c_{n-m}) + pFx$, wo Fx im Allgemeinen einen Ausdruck vom n^{ten} Grade bedeutet. Dividirt man diese Gleichung algebraisch durch den einfachen Ausdruck $x^m + \beta_1x^{m-1} + \ldots + \beta_m$, so muss offenbar der Rest, welchen $a_0x^n + a_1x^{n-1} + \ldots + a_n$ bei der Division giebt, gleich dem Reste sein, welchen pFx giebt. Die Coefficienten dieses Restes werden aber, wie leicht ersichtlich, sämmtlich durch p aufgehen, mithin müssen auch die Coefficienten vom Reste des gegebenen Ausdruckes durch p theilbar werden. Hat also der gegebene Ausdruck irgend einen Divisor, so muss er auch durch den einfachen Ausdruck dieses Divisors dividirt, einen Rest geben, der $\equiv 0 (mod.\ p)$ zu setzen ist.

Die Umkehrung dieses Satzes ist, wie leicht zu übersehen, ebenfalls richtig, und heisst: Giebt ein Ausdruck durch einen zweiten algebraisch dividirt einen Rest, dessen Coefficienten nach dem Modul p congruent 0 sind, so ist der zweite Ausdruck ein Divisor des ersten.

§. 4.

Lehrsatz. Das Product zweier einfachen Ausdrücke von x kann nicht $\equiv 0 (mod.\, p)$ sein.

Beweis. Ist der eine Ausdruck vom m^{ten}, der andere vom n^{ten} Grade, so ist offenbar das erste Glied der Entwickelung des Productes x^{n+m} und da der Coefficient dieses Gliedes gleich 1 und daher nicht $\equiv 0 (mod.\, p)$ ist, so darf offenbar der ganze Ausdruck nicht $\equiv 0 (mod.\, p)$ gesetzt werden.

Zusatz. Man leitet hieraus leicht den allgemeinen Satz ab: dass das Product zweier Ausdrücke nicht $\equiv 0 (mod.\, p)$ werden kann, wenn nicht einer von ihnen $\equiv 0 (mod.\, p)$ ist (§. 2.).

§. 5.

Lehrsatz. Ist das Product aus einem Ausdruck und einem irreductibeln einfachen Ausdrucke, dem Producte zweier andern Ausdrücke von x nach dem Modul p congruent, so hat einer derselben den irreductibeln Ausdruck nach dem Modul p zum Divisor.

Dieser Satz soll zunächst für $n = 1$ und $n = 2$ und dann durch den Schluss von n auf $n+1$ allgemein bewiesen werden.

Beweis. Ist also $n = 1$ und ist $x + a_1$ der irreductibele Factor vom ersten Grade, bedeuten ferner fx, Ax, und Bx Ausdrücke von x, so ist zu zeigen, dass, wenn $(x+a_1)fx \equiv Ax\, Bx (mod.\, p)$ ist, $x + a_1$ ein Factor von Ax oder von Bx sein müsse. Aus obiger Congruenz folgt aber, dass $Ax\, Bx$ für $x \equiv -a_1 (mod\, p)$ congruent 0, und hieraus, dass entweder $A(-a_1)$ oder $B(-a_1)$ congruent 0 werden müsse. Gesetzt nun $A(-a_1)$ wäre $\equiv 0 (mod.\, p)$, so hat man $Ax \equiv Ax - A(-a_1) (mod.\, p)$, aber $Ax - A(-a_1)$ hat offenbar die Wurzel $-a_1$ und daher der Factor $x + a_1$, woraus denn folgt, dass Ax in Bezug auf den Modul p den Factor $x + a_1$ habe.

Ist ferner $n = 2$, so sei der irreductibele einfache Ausdruck $x^2 + a_1 x + a_2$ und $(x^2 + a_1 x + a_2) fx \equiv Ax\, Bx (mod.\, p)$. Gesetzt nun Ax habe nicht den Factor $x^2 + a_1 x + a_2$, so muss ihn Bx haben. Um dies zu beweisen nenne man den algebraischen Quotienten, den man erhält, wenn man Bx durch $x^2 + a_1 x + a_2$ dividirt, Qx und den Rest $\alpha x + \beta$, so hat man $Bx = (x^2 + a_1 x + a_2) Qx + \alpha x + \beta$. Substituirt man diesen Ausdruck in obiger Congruenz, so erhält man $(x^2 + a_1 x + a_2)(fx - Qx\, Ax) \equiv (\alpha x + \beta) Ax (mod.\, p)$. Es ist nun zu zeigen, dass $\alpha x + \beta \equiv 0 (mod.\, p)$ oder dass $\alpha \equiv 0 (mod.\, p)$ und $\beta \equiv 0 (mod.\, p)$, und mithin $Bx \equiv (x^2 + a_1 x + a_2) Qx (mod\, p)$ sei. Wäre nun α nicht $\equiv 0 (mod.\, p)$ so bestimme man β_1 so, dass $\alpha(x + \beta_1) \equiv \alpha x + \beta (mod.\, p)$ und α_1 so, dass $\alpha\alpha_1 \equiv 1 (mod.\, p)$ sei, alsdann erhält man offenbar $\alpha\alpha_1 (x^2 + a_1 x + a_2) Mx \equiv \alpha (x + \beta_1) Ax (mod.\, p)$, wo $Mx = fx - Qx \,.\, Ax$ ist, und hieraus $\alpha_1 (x^2 + a_1 x + a_2) Mx \equiv (x + \beta_1) Ax (mod.\, p)$. Da nun $x + \beta_1$ ein Factor vom ersten Grade ist, so muss er nach Obigem (da $x^2 + a_1 x + a_2$ als irreductibeler Ausdruck ihn nicht enthalten kann) in Mx enthalten sein. Setzt man also $Mx \equiv (x + \beta_1) Q_1 x$, so erhält man $\{\alpha_1 (x_2 + a_1 x + a_2) Q_1 x - Ax\} (x + \beta_1) \equiv 0 (mod.\, p)$. Da nun $x + \beta_1$ nicht $\equiv 0 (mod.\, p)$ ist, so müsste $\alpha (x^2 + a_1 x + a_2) Q_1 x - Ax \equiv 0 (mod.\, p)$

oder $\alpha(x^2+a_1x+_2)Q_1x \equiv Ax\ (mod.\,p)$ und daher $x^2+a_1x+a_2$ gegen die Voraussetzung ein Factor von Ax sein. Wäre nun $\alpha \equiv 0\ (mod.\,p)$ aber nicht $\beta \equiv 0$, so bestimme man β_1 so, dass $\beta\beta_1 \equiv 1\ (mod.\,p)$ werde, alsdann leitet man leicht aus der obigen Congruenz $(x^2+a_1x+a_2)(fx-Qx.Ax) \equiv (\alpha x+\beta)$ $Ax\ (mod.\,p)$ die folgende ab $\beta_1(x^2+a_1x+a_2)(fx-Qx\,Ax) \equiv Ax\ (mod.\,p)$. Hiernach wäre aber wieder $x^2+a_1x+a_1$ ein Factor von Ax gegen die Voraussetzung. Es muss also $\alpha \equiv 0$ und $\beta \equiv 0\ (mod.\,p)$ sein.

Wir wollen nun voraussetzen, der Satz sei bis zu dem Grade n bewiesen, und zeigen er gelte auch für den Grad $n+1$. Es sei mithin ϕx ein irreductibeler Ausdruck vom Grade $n+1$ und $\phi x fx \equiv Ax Bx\ (mod.\,p)$. Ferner setze man voraus, Ax habe nicht den Divisor ϕx und bezeichne den algebraischen Quotienten, den man erhält, wenn man Bx durch ϕx dividirt, durch Qx und den Rest, welcher den n^{ten} Grad nicht überschreiten kann, durch Rx, so hat man $Bx = \phi x\,.\,Qx + Rx$, mithin $\phi x(fx - Ax\,Qx) \equiv Ax\,Rx\ (mod.\,p)$. Es ist nun zu zeigen, dass $Rx \equiv 0\ (mod.\,p)$ sei. Wäre Rx nicht $\equiv 0\ (mod.\,p)$, so könnte man, wenn α der Factor der höchsten Potenz von Rx ist, der nicht $\equiv 0\ (mod.\,p)$ wird, einen einfachen Ausdruck R_1x so bestimmen, dass $Rx \equiv \alpha R_1x\ (mod.\,p)$ ist. Bestimmt nun α_1 so, dass $\alpha\alpha_1 \equiv 1\ (mod.\,p)$, so zeigt man leicht, dass $\alpha_1\,\phi x\,(fx - Ax\,Qx) \equiv Ax\,R_1x\ (mod.\,p)$ sein müsse. Da der Grad von R_1x die Zahl n nicht überschreiten kann, und ϕx irreductibel ist, so muss R_1x ein Factor von $\alpha_1(fx - Ax\,Qx)$ sein. Setzt man also $\alpha_1(fx - Ax\,.\,Qx) \equiv Fx\,R_1x\ (mod.\,p)$, so leitet man sehr leicht $R_1x(\phi x\,Fx - Ax) \equiv 0\ (mod.\,p)$ ab. Wäre nun R_1x nicht $\equiv 0$, so müsste es $\phi x\,fx - Ax$ oder $\phi x\,.\,Fx \equiv Ax\ (mod.\,p)$ und daher ϕx gegen die Voraussetzung ein Factor von Ax sein. Es muss mithin $Rx \equiv 0\ (mod.\,p)$ und ϕx ein Factor von Bx sein.

§. 6.

Lehrsatz. Jeder Ausdruck kann nur auf eine Weise dem Product einfacher irreductibeler Ausdrücke und einer Zahl congruent gesetzt werden.

Beweis. Bedeutet α eine Zahl und Ax, Bx, Cx etc. einfache irreductibele Ausdrücke von x, ferner m, n, p etc. ganze positive Exponenten, so ist zu zeigen, dass $\alpha(Ax)^m(Bx)^n(Cx)^p$ etc. sich nicht congruent setzen lasse einem Producte, das in seinen einfachen irreductibelen Factoren anders als das vorliegende zusammengesetzt ist. Aus §. 5. folgt nun zunächst, dass jede vorausgesetzte andere Zerfällung ebenfalls nur die einfachen irreductibelen Factoren Ax, Bx, Cx etc. enthalten könne. Wollte man nun voraussetzen, irgend ein Factor z. B. Ax könne in einer andern Potenz als in der m^{ten} vorkommen, so setze man $\alpha(Ax)^m(Bx)^n(Cx)^p$ etc. $\equiv \alpha(Ax)^{m_1}(Bx)^{n_1}(Cx)^{p_1}$ etc. und $m > m_1$, so erhält man leicht $\alpha(Ax)^{m_1}((Ax)^{m-m_1}(Bx)^n(Cx)^p$ etc. $-$ $(Bx)^{n_1}$ $(Cx)^{p_1}$ etc.$) \equiv 0\ (mod.\,p)$. Da $\alpha(Ax)^{m-m_1}$ nicht $\equiv 0\ (mod.\,p)$ sein kann, so muss $(Ax)^{m-m_1}(Bx)^n(Cx)^p$ etc. $-$ $(Bx)^{n_1}(Cx)^{p_1}$ etc. $\equiv 0\ (mod.\,p)$ und mithin $(Ax)^{m-m_1}$ und daher auch Ax ein Factor von $(Bx)^{n_1}(Cx)^{p_1}$ etc. sein. Da dies sich aber durch §. 5. leicht als unmöglich nachweisen lässt, so muss $m = m_1$ sein.

§. 7.

Lehrsatz. Jeder Ausdruck, dessen Wurzeln in eine bestimmte Potenz eines irreductibeln Ausdrucks eingesetzt, dieselbe, wenn sie mit einer gewissen Zahl, die nicht $\equiv 0 (mod. p)$ ist, multiplicirt wird, einem bestimmten $p$fachen Ausdruck der jedesmaligen Wurzel gleich machen, ist selbst eine Potenz jenes irreductibeln Ausdruckes in Bezug auf den Modul p.

Beweis. Gesetzt fx sei die Potenz eines einfachen irreductibelen Ausdruckes, und Fx irgend ein einfacher Ausdruck, dessen Wurzeln α_1, α_2, ... α_n sind, ferner bezeichne Nx irgend einen Ausdruck von x und z eine eine ganze Zahl, so wäre obige Voraussetzung durch folgende Gleichungen ausgedrückt: $zf\alpha_1 = pN\alpha_1$, $zf\alpha_2 = pN\alpha_2$, ... $zf\alpha_n = pN\alpha_n$. Zu beweisen ist, dass Fx einer Potenz desjenigen Ausdrucks congruent sei, von dem fx Potenz ist. Da $zfx - pNx$ für jede Wurzel von Fx verschwindet, so kann man $zfx - pNx = (x-\alpha_1)\, Q(x, \alpha_1)$ setzen, wo $Q(x, \alpha_1)$ als Quotient von $zfx - pNx$ durch $x - \alpha_1$ eine Function vom $(n-1)^{ten}$ Grade ist, in deren Coefficienten α_1 eintritt. Ebenso erhält man $zfx - pNx = (x-\alpha_2)$ $Q(x, \alpha_2)$ etc. Setzt man nun diese Gleichungen unter einander, so erhält man

$$zfx - pNx = (x-\alpha_1)\,Q(x,\alpha_1)$$
$$zfx - pNx = (x-\alpha_2)\,Q(x,\alpha_2)$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$zfx - pNx = (x-\alpha_n)\,Q(x,\alpha_n)\ .$$

Multiplicirt man diese Gleichungen in einander und bedenkt, dass $(x-\alpha_1)$ $(x-\alpha_2) \ldots (x-\alpha_n) = Fx$ ist, so erhält man die Congruenz $(zfx)^n \equiv Fx$ $Q(x, \alpha_1)\, Q(x, \alpha_2) \ldots Q(x, \alpha_n)\ (mod.\ p)$. die Coefficienten von $Q(x, \alpha_1)$. $Q(x, \alpha_2) \ldots Q(x.\alpha_n)$ müssen offenbar symmetrische Functionen von α_1, α_2, ... α_n und mithin ganze Zahlen sein. Schreibt man daher für dies Product den Ausdruck Mx, so erhält man $(zfx)^n \equiv Fx\ .\ Mx\ (mod\ p)$ und hiernach ist offenbar Fx ein Factor von $(fx)^n$, und da $(fx)^n$ die n^{te} Potenz einer Potenz eines irreductibeln Ausdrucks, mithin selbst eine Potenz desselben irreductibeln Ausdrucks ist, so kann Fx als Divisor einer solchen selbst nur die Potenz jenes irreductibeln Ausdrucks sein.

§. 8.

Lehrsatz. Ist die Norm eines einfachen Ausdrucks in Bezug auf einen zweiten einfachen Ausdruck congruent $0 (mod.\ p)$, so ist auch die Norm des zweiten in Bezug auf den ersten congruent $0\ (mod.\ p)$.

Beweis. Nennt man die einfachen Ausdrücke, um die es sich handelt, fx und ϕx, so folgt zunächst (§. 7. Einl.), dass Nf_ϕ und $N\phi_f$ ganze Zahlen sein werden, weil nämlich die Coefficienten von fx und von ϕx ganze Zahlen sind. Da nun aber (§. 7. Einl.) $\pm N\phi_f = Nf_\phi$ ist, so folgt, dass $N\phi_f$ und Nf_ϕ stets zugleich $\equiv 0\ (mod.\ p)$ werden.

§. 9.

Lehrsatz. Die Norm eines Ausdruckes in Bezug auf einen zweiten Ausdruck, der dem Product mehrerer Ausdrücke congruent ist, ist dem Product der Normen des ersten Ausdruckes in Bezug auf sämmtliche Factoren des zweiten congruent. Oder wenn fx, ϕx, Ax, Bx, Cx etc. Ausdrücke von x bedeuten, und $\phi x \equiv Ax\ .\ Bx\ .\ Cx \ldots (mod.\ p)$ ist, so hat man Nf_ϕ $\equiv Nf_A\ .\ Nf_B\ .\ Nf_C$ etc. $(mod.\ p)$.

Beweis. Man kann annehmen, dass sämmtliche hier auftretende Ausdrücke einfache sind, denn die Verallgemeinerung ergiebt sich hieraus leicht. Zunächst ist nun zu bemerken, dass die symmetrischen Functionen der Wurzeln von ϕx und von $Ax \,.\, Bx \,.\, Cx \,..$ nach dem Modul p congruent sein werden. Da nämlich $\phi x \equiv Ax \,.\, Bx \,.\, Cx \,..\, (mod.\, p)$ ist, so muss $\phi x + pFx = Ax \,.\, Bx \,.\, Cx \,..$ sein, wo Fx irgend einen Ausdruck von x bedeutet. Offenbar werden aber die symmetrischen Functionen der Wurzeln von ϕx und von $\phi x + pFx$ nach dem Modul p congruent sein, weil sie als Ausdrücke congruenter Zahlen, nämlich der Coefficienten von ϕx und von $\phi x + pFx$ angesehen werden können (§. 3. Einl.); mithin wird die Norm von fx in Bezug auf $\phi x + pFx$ congruent der Norm von fx in Bezug auf ϕx sein. Da $\phi x + pFx = Ax \,.\, Bx \,.\, Cx \,..$ ist, so wird also auch die Norm von fx in Bezug auf ϕx congruent der Norm von fx in Bezug auf $Ax \,.\, Bx \,.\, Cx \,..$ sein. Löst man aber diese Norm (§. 7. Einl.) in ihre Factoren auf, so folgt, dass sie in Bezug auf $Ax\, Bx\, Cx \,..$ gleich $Nf_A \,.\, Bf_B \,.\, Nf_C \,..$ sein werde, und hieraus folgt $Nf_\phi \equiv Nf_A\, Nf_B\, Nf_C\, (mod.\, p)$, was zu beweisen war.

Zusatz. Nf_ϕ kann also nur $\equiv 0\, (mod.\, p)$ werden, wenn eine der Grössen Nf_A, Nf_B, $Bf_C \,...$ congruent $0\, (mod.\, p)$ wird.

§. 10.

Lehrsatz. Die Norm eines irreductibeln einfachen Ausdrucks kann in Bezug auf einen zweiten Ausdruck von geringerem Grade nicht congruent $0\, (mod.\, p)$ werden.

Ist also fx irreductibel und der Grad von ϕx kleiner als der von fx, so ist zu zeigen, dass Nf_ϕ nicht $\equiv 0\, (mod.\, p)$ werden kann. Zuerst soll nun der Grad von ϕx gleich 1, dann gleich zwei angenommen, und dann im Allgemeinen die Richtigkeit des Satzes durch den Schluss von m auf $m + 1$ gezeigt werden.

Beweis. Ist ϕx vom Grade 1, also gleich $x + a_1$, so ist $Nf_\phi = f(-a_1)$, wäre aber $f(-a_1) \equiv 0\, (mod.\, p)$, so hätte fx den Factor $x + a_1$ in Bezug auf den Modul p (Vergl. §. 5.) und wäre mithin nicht irreductibel. Es kann mithin für diesen Fall Nf_ϕ nicht $\equiv 0\, (mod.\, p)$ sein.

Setzt man nun voraus, ϕx sei vom zweiten Grade, so ist zu unterscheiden, ob es irreductibel ist oder nicht. Der zweite Fall ist leicht abzuthun, setzt man nämlich $\phi x \equiv \phi_1 x \,.\, \phi_2 x\, (mod.\, p)$, so kann Nf_ϕ nicht $\equiv 0$ $(mod.\, p)$ werden, wenn keiner von den Ausdrücken Nf_{ϕ_1} und Nf_{ϕ_2} congruent $0\, (mod.\, p)$ wird (§. 9.). Da aber $\phi_1 x$ und $\phi_2 x$ vom ersten Grade sind, so geht dies nicht an. Ist nun ϕx ein irreductibeler Ausdruck, so nenne man den algebraischen Quotienten, den fx durch ϕx dividirt, giebt, Qx und den Rest Rx. Offenbar muss nun, da $fx = Qx \,.\, \phi x + Rx$, $f\beta_1\, f\beta_2 = (Q\beta_1\, \phi\beta_1 + B\beta_1)(Q\beta_2\, \phi\beta_2 + R\beta_2)$ sein. Setzt man β_1 und β_2 als die beiden Wurzeln von $\phi x = 0$, so erhält man mithin $f\beta_1\, f\beta_2 = Nf_\phi = R\beta_1\, R\beta_2$. Da nun Rx im Allgemeinen vom 1ten Grade ist, so setze man $Rx \equiv \alpha(x + \alpha_1)\, (mod.\, p)$ und $(x + \alpha_1) = R_1 x$, so erhält man $Nf_\phi \equiv \alpha^2\, R_1\beta_1\, R_1\beta_2 \equiv \alpha^2\, NR_{1\phi}$. Sollte aber nun dieser Ausdruck $\equiv 0\, (mod.\, p)$ werden, so müsste $NR_{1\phi}$ und mithin auch $N\phi_{R_1}$ congruent 0 $(mod. p)$ werden (§. 8.). Da aber ϕx irreductibel und $R_1 x$ von einem geringeren Grade als ϕx, so geht dies wegen des vorher Bewiesenen nicht an.

Setzt man nun voraus es sei bewiesen, Nf_ϕ könne nicht $\equiv 0 \ (mod. p)$ werden, wenn fx irreductibel, und der Grad von ϕx gleich m ist, so ist jetzt zu zeigen, dass Nf_ϕ ebenfalls nicht $\equiv 0 \ (mod. p)$ werden könne, wenn der Grad von ϕx gleich $m + 1$ ist, so ferne nur der Grad von fx grösser als $m + 1$ ist.

Es sei also jetzt ϕx vom Grade $m + 1$, so ist wieder zu unterscheiden, ob ϕx irreductibel sei oder nicht. Ist ϕx nicht irreductibel, so setze man $\phi x \equiv Ax . Bx \ (mod. p)$. Da nun aber Nf_ϕ nicht $\equiv 0 \ (mod. p)$ werden kann, wenn nicht einer der Factoren Nf_A oder $Nf_B \equiv 0 \ (mod. p)$ wird (§. 10.), diese aber nicht $\equiv 0 \ (mod. p)$ werden können, weil ihr Grad die Zahl m nicht überschreiten kann (bis zu welcher Zahl der Satz ja als bewiesen angenommen wird), so kann Nf_ϕ nicht $\equiv 0 \ (mod. p)$ werden, wenn ϕx nicht irreductibel ist. Man setze jetzt voraus ϕx sei irreductibel, so bezeichne man den Quotienten, den fx durch ϕx dividirt giebt, durch Qx, und den Rest durch Rx, so erhält man $fx = \phi x . Qx + Rx$. Da nun für jede Wurzel von ϕx etwa für β_1, $f\beta_1 = R\beta_1$ ist (weil $\phi\beta_1 = 0$ ist), so hat man auch $Nf_\phi = NR_\phi$. Rx kann nicht $\equiv 0 \ (mod. p)$ sein, weil sonst fx nicht irreductibel wäre, wird aber im Allgemeinen kein einfacher Ausdruck sein: man setze es daher dem Producte einer Zahl a und eines einfachen Ausdruckes $R_1 x$ congruent (§. 2.), so erhält man $Rx \equiv aR_1 x \ (mod. p)$ und $NR_\phi \equiv a^{m+1} NR_1\phi \ (mod. p)$. Es kann mithin NR_ϕ nicht $\equiv 0 \ (mod\ p)$ werden, ohne dass es $NR_1\phi$ zugleich würde. $NR\,\phi$ kann aber nicht $\equiv 0 \ (mod. p)$ werden, wenn nicht zugleich $N\phi_{R_1}$ congruent 0 $(mod. p)$ wird (§. 8.). Dies geht aber nicht an, weil ϕx irreductibel ist und $R_1 x$ den Grad m nicht überschreiten kann. Es kann mithin auch nicht NR_ϕ und auch nicht Nf_ϕ congruent 0 $(mod. p)$ werden.

§. 11.

Lehrsatz. Ist fx ein irreductibeler Ausdruck und ϕx irgend ein einfacher Ausdruck, so ist fx ein Divisor von ϕx in Bezug auf den Modul p, wenn $Nf_\phi \equiv 0 \ (mod. p)$ ist, und umgekehrt.

Beweis. Ist $Nf_\phi \equiv 0 \ (mod. p)$, so kann nach §. 10. der Grad von ϕx nicht kleiner als der von fx sein. Nun setze man $fx \equiv kf_1 x \ (mod. p)$, wo k eine Zahl und $f_1 x$ einen einfachen Ausdruck bedeutet (§. 2.). Bezeichnet man nun den Grad von ϕx mit m, so erhält man $Nf_\phi = k^m Nf_{1_\phi}$. Sollte also $Nf_\phi \equiv 0 \ (mod. p)$ werden, so müsste auch $Nf_{1_\phi} \equiv 0 \ (mod. p)$ werden. Setzt man nun aber $\phi x = f_1 x . Qx + Rx$, wo Qx den Quotienten bezeichnet, den man erhält, wenn man ϕx durch $f_1 x$ dividirt, und Rx den Rest; so bemerke man, dass, wenn $Nf_{1_\phi} \equiv 0 \ (mod. p)$ wird, auch $N\phi_{f_1} \equiv 0$ (mod. p) ist (§. 8.). Aber $N\phi_{f_1}$ ist offenbar, weil $\phi x = f_1 x . Qx + Rx$ ist, gleich NR_{f_1}, und dieser Ausdruck kann nicht $\equiv 0 \ (mod. p)$ werden, wenn nicht zugleich

Nf_{1_R}

$Nf_{1R} \equiv 0$ (*mod. p.*) wird. Da aber $f_1 x$ irreductibel und Rx von einem niedrigeren Grade als fx ist, so geht dies nicht an (§. 10.). Da dieser Widerspruch nur fortfällt, wenn $Rx \equiv 0$ (*mod. p*), so muss fx in Bezug auf den Modul p ein Divisor von ϕx sein, wenn $Nf_\phi \equiv 0$ (*mod. p*) ist.

Die Umkehrung des Satzes ergiebt sich leicht.

§. 12.

Lehrsatz. Entwickelt man die Gleichung für einen Ausdruck der Wurzel eines in Bezug auf den Modul p einfachen irreductibeln Ausdrucks, und bezeichnet dieselbe durch $Fz = 0$, so ist Fz in Bezug auf den Modul p entweder irreductibel, oder die Potenz eines irreductibeln Ausdruckes.

Gesetzt also fx wäre ein einfacher irreductibeler Ausdruck, und seine Wurzeln $\alpha_1, \alpha_2, \ldots. \alpha_n$, bezeichnet ferner ϕx irgend einen Ausdruck von x, so hängen die Grössen $\phi\alpha_1, \phi\alpha_2, \ldots \phi\alpha_n$ von der Gleichung $(z - \phi\alpha_1)(z - \phi\alpha_2) \ldots. (z - \phi\alpha_n) = 0$ ab. Setzt man nun $(z - \phi\alpha_1)(z - \phi\alpha_2) \ldots. (z - \phi\alpha_n) = Fz$, so soll Fz irreductibel oder die Potenz eines irreductibeln Ausdruckes sein.

Beweis. Setzt man voraus, Fz habe in Bezug auf den Modul p, mehrere Divisoren $dz, d_1 z, d_2 z \ldots. d_m z$, von denen jeder die Potenz eines eigenen irreductibeln Ausdrucks in Bezug auf den Modul p ist, so muss zunächst $F\phi x$ algebraisch durch fx theilbar sein (§. 6. Einl.). Da aber $F\phi x \equiv d\phi x \,.\, d_1\phi x \ldots. d_m\phi x$ (*mod. p*), so muss einer der Factoren $d\phi x, d_1\phi x, \ldots d_m(\phi x)$ durch fx theilbar sein (§. 4.). Zunächst ist nun zu zeigen, dass unter den gemachten Voraussetzungen, nicht zwei jener, etwa $d\phi x$ und $d_1\phi x$ durch fx in Bezug auf den Modul p theilbar sein können. Zu dem Ende bezeichne man die irreductibelen Ausdrücke, von welchen $d\phi x$ und $d_1\phi x$ in Bezug auf den Modul p als Potenzen angesehen werden können, durch $m\phi x$ und $m_1\phi x$, so müssten auch $m\phi x$ und $m_1\phi x$ in Bezug auf den Modul p durch fx aufgehen. Man würde also stets Gleichungen folgender Art aufstellen können: $m\phi x = fx \,.\, Qx + pNx$, $m_1\phi x = fx \,.\, Q_1 x + pNx$, wo Qx, Nx, $Q_1 x$ und $N_1 x$ Ausdrücke von x bedeuten. Nimmt man nun an, der Grad von mz sei gleich oder höher wie der von $m_1 z$, so setze man $mz \equiv m_1 z \,.\, q_1 z + \alpha_2 m_2 z$ (*mod. p*), wo $q_1 z$ den algebraischen Quotienten bedeutet, den man erhält, wenn man mz durch $m_1 z$ dividirt, und $\alpha_2 m_2 z$ dem Ausdruck des Divisions-Restes in der Art congruent wird, dass α_2 eine Zahl und $m_2 z$ einen einfachen Ausdruck bedeutet. Auf ähnliche Weise setze man $m_1 z \equiv m_2 z q_2 z + \alpha_3 m_3 z$ (*mod. p*), und setze diese Operations-Weise fort bis man endlich $m_\nu z \equiv m_{\nu+1} z\, q_{\nu+1} z + \alpha_{\nu+2}\, m_{\nu+2} z$ (*mod. p*) erhält, wo $m_{\nu+2} z$ in Bezug auf z vom ersten Grade ist. Man muss auf jeden Fall die Operation bis dahin fortsetzen können, weil sie nur durarah unterbrochen werden könnte, dass irgend ein Rest etwa $m_\nu z \equiv 0$ (*mod. p*) würde. Dann würde man aber vermöge obiger Gleichungen leicht schliessen, dass $m_{\nu-2} z$ den Factor $m_{\nu-1} z$ haben müsse, und würde gleicherweise finden, dass alle Werthe, die dem $m_{\nu-1} z$ vorangehen, also auch $m_2 z$, $m_1 z$ und mz den Factor $m_{\nu-1} z$ haben müssten, was gegen die vorausgesetzte Irreductibilität der beiden Ausdrücke $m_1 z$ und mz streitet. Man kann mithin die Operation so lange fortsetzen, bis $m_{\nu-2} z$

vom Grade 1 ist. Es ist nun zu zeigen, dass sämmtliche Ausdiücke m_2z, m_3z, ... $m_{r+1}z$, wenn man in ihnen statt z, ϕx setzt, den Factor fx in Bezug auf den Modul p haben müssen. Dies nrgiebt sich zunächst für m_2z aus der Congruenz $mz \equiv m_1 z q_1 z + \alpha_2 m_2 z$ (mod. p). Da nämlich mz und m_1z, wenn man in ihnen statt z, ϕx setzt, den Factor fx enthalten, so muss, da $\alpha_2 m_2 z \equiv mz - m_1 z q_1 z$ (*mod.* p), m_2z oder vielmehr $m_2\phi x$ auch den Factor fx enthalten. In gleicher Weise schliesst man fort auf m_3z durch die Congruenz $m_1z \equiv m_2 z q_2 z + \alpha_3 m_3 z$ (*mod.* p) etc. bis auf $m_{r+2}z$. Da aber $m_{r+2}z$ vom ersten Grade ist, so ist es von der Form $z + A_1$, wo A_1 eine ganze Zahl bedeutet, und man erhält, da fx in Buzug auf den Modul p ein Factor von $z + A_1$ ist, $z + A_1 \equiv fx\, Ux$ (*mod.* p), wo Ux einen Ausdruck von x bedeutet. Setzt man für z seinen Ausdruck ϕx, so hat man $\phi x + A_1 \equiv fx \,.\, Ux$ (*mod.* p) und mithin $\phi x = -A_1 + fx \,.\, Ux + pSx$, wo Sx ebenfalls einen Ausdruck von x bedeutet. Ist nun α eine der Wurzeln von fx, so hat man offenbar $\phi\alpha = -A_1 + pS\alpha$, und hieraus leitet man leicht folgende Congruenz ab $(z - \phi\alpha_1)(z - \phi\alpha_2) \ldots (z - \phi\alpha_n) \equiv (z + A_1)^n$ (*mod.* p), wonach offenbar in Fz nicht zwei verschiedene irreductibele Ausdrücke von z als Factoren nach dem Modul p vorkommen können. Setzt man also unter obiger Voraussetzung $F\phi x \equiv d\phi x \,.\, d_1\phi x \,....\, d_m\phi x$ (*mod.* p), so kann, wenn $d\phi x$ den Divisor fx hat, keiner der übrigen Factoren diesen Ausdruck zum Divisor haben. Schreibt man nun obige Congruenz als Gleichung, so erhält man $Fz = dz\, d_1z \ldots d_mz + pRz$, wo Rz einen Ausdruck von z bedeutet. Setzt man irgend eine der Wurzeln von Fz gleich γ_1 und bezeichnet das Product $d_1z\, d_2z \ldots d_mz$ durch Dz, so erhält man $d\gamma_1 D\gamma_1 + pR\gamma_1 = 0$ und mithin

$$d\gamma_1 = -p\,\frac{R\gamma_1}{D\gamma_1} = -p\,\frac{R\gamma_1\, D\gamma_2\, D\gamma_3 \ldots D\gamma_n}{D\gamma_1\, D\gamma_2\, D\gamma_3 \ldots D\gamma_n} = -p\,\frac{R\gamma_1\, D\gamma_2\, D\gamma_3 \ldots D\gamma_n}{N(D_F)}\,.$$

Die Norm von Dz in Bezug auf Fz ist aber dieselbe wie die Norm von $D\phi x$ in Bezug auf fx. Es ist nämlich $N(D_F) = D\gamma_1\, D\gamma_2 \ldots D\gamma_n$ und die Norm von $D\phi x$ in Bezug auf fx ist $D\phi\alpha_1\, D\phi\alpha_2 \ldots D\phi\alpha_n$. Da aber die Werthe $\gamma_1, \gamma_2, \ldots \gamma_n$ mit den Werthen $\phi\alpha_1, \phi\alpha_2, \ldots \phi\alpha_n$ übereinstimmen, so hat man $D\gamma_1\, D\gamma_2 \ldots D\gamma_n = D\phi\alpha_1\, D\phi\alpha_2 \ldots D\phi\alpha_n$ und mithin $N(D_F) = N(D_f)$, wo man natürlich in letzterem Ausdruck D als einen Ausdruck von x ansieht. Da nun $D\phi x$ nicht den Factor fx in Bezug auf den Modul p haben kann, so kann auch $N(D_f)$ oder $N(D_F)$ nicht $\equiv 0$ (*mod.* p) sein (§. 11.). Bezeichnet man also die Zahl $N(D_F)$ durch z, so erhält man $zd\gamma_1 = -pR\gamma_1\, D\gamma_2\, D\gamma_3 \ldots D\gamma_n$. Da aber $D\gamma_2\, D\gamma_3 \ldots D\gamma_n$ ein symmetrischnr Ausdruck von $\gamma_2, \gamma_3, \ldots \gamma_n$ ist, so lässt es sich (§. 4. Einl.) als Ausdruck von γ_1 ansehen, wonach man auch $R\gamma_1\, D\gamma_2\, D\gamma_3 \ldots D\gamma_n$ als einen Ausdruck von γ_1 ansehen kann. Nennt man diesen $-Q\gamma_1$, so erhält man $zd\gamma_1 = pQ\gamma_1$

und auf gleiche Weise

$$zd\gamma_2 = pQ\gamma_2$$

$$zd\gamma_3 = pQ\gamma_3$$

$$\ldots\ldots\ldots$$

$$zd\gamma_n = pQ\gamma_n\,.$$

Da nun $\gamma_1, \gamma_2 \ldots \gamma_n$ die Wurzeln von $Fz = 0$ sind, so folgt (§. 7.), dass Fz einer Potenz desjenigen Ausdrucks nach dem Modul p congruent ist, von dem dz selbst in Bezug auf p als Potenz zu betrachten ist. Es kann mithin ausser dz keinen Factor von Fz in Bezug auf den Modul p geben, und Fz selbst ist der Potenz eines irreductibeln Ausdrucks nach dem Modul p congruent, was zu beweisen war.

Zusatz. Ist der Grad von fx gleich n, der von ϕx aber kleiner als n, so kann Fz nicht $\equiv (z-A_1)^n$ $(mod.\ p)$ werden, wenn A_1 eine ganze Zahl bedeutet.

Wäre nämlich $Fz \equiv (z-A_1)^n$ $(mod.\ p)$, so könnte man eine Gleichung von der Form $Fz = (z-A_1)^n - pRz$ aufstellen, wo Rz einen Ausdruck von z bedeutet. Da nun die Wurzeln von Fz, $\phi\alpha_1$, $\phi\alpha_2$, ... $\phi\alpha_n$ sind, so erhält man die Gleichungen

$$\begin{aligned}(\phi\alpha_1 - A_1)^n &= pR\alpha_1\\ (\phi\alpha_2 - A_1)^n &= pR\alpha_2\\ (\phi\alpha_3 - A_1)^n &= pR\alpha_3\\ &\ldots\ldots\\ (\phi\alpha_n - A_1)^n &= pR\alpha_n\,.\end{aligned}$$

Nun leitet man durch Multiplication dieser Gleichungen sehr leicht ab, dass $\{(\phi\alpha_1 - A_1)(\phi\alpha_2 - A_1) \ldots (\phi\alpha_n - A_1)\}^n = p^n R\alpha_1\, R\alpha_2 \ldots R\alpha_n$ sei. Da auf beiden Seiten der Gleichung symmetrische Functionen der Wurzeln von fx stehen, so sind diese ganze Zahlen, und mithin gewiss

$$\{(\phi\alpha_1 - A_1)(\phi\alpha_2 - A_1) \ldots (\phi\alpha_n - A_1)\}^n \equiv 0\ (mod.\ p)$$

und daher auch

$$(\phi\alpha_1 - A_1)(\phi\alpha_2 - A_1) \ldots (\phi\alpha_n - A_1) \equiv 0\ (mod.\ p)\,.$$

Setzt man nun $\phi x - A_1 = \psi x$, so ist auch ψx wie ϕx ven einem geringeren Grade als fx, mithin kann $N\psi_f$ oder $(\phi\alpha_1 - A_1)(\phi\alpha_2 - A_1)(\phi\alpha_3 - A_1) \ldots (\phi\alpha_n - A_1)$ nicht $\equiv 0$ $(mod.\ p)$ sein (§. 10.), welches doch stattfinden müsste, wenn $Fz \equiv (z-A_1)^n$ $(mod.\ p)$ wäre.

§. 13.

Lehrsatz. Zwei einfache Ausdrücke von x, von welchen die Wurzeln des einen die p^{ten} Potenzen der Wurzeln des andern sind, sind nach den Modul p congruent.

Zum Beweise bemerke man, dass

1) $(z-1)^p \equiv z^p - 1$ $(mod.\ p)$ ist, dies folgt unmittelbar aus der durch den binomischen Lehrsatz bestimmten Form der Coefficienten von $(z-1)^p$. Es werden mithin die symmetrischen Functionen der Wurzeln von $z^p - 1$ und von $(z-1)^p$ nach dem Modul p congruent sein. Da die Wurzeln von $(z-1)^p$ sämmtlich gleich 1 sind, so kann man statt jeder Wurzel von $z^p - 1$, so fern es sich um congruente Ausdrücke der symmetrischen Functionen der Wurzeln dieses Ausdrucks handelt, 1 setzen.

2) Ist $x^n + a_1 x^{n-1} + \ldots + a_n$ irgend ein einfacher Ausdruck von x, und bezeichnen α, α^2, ... α^{p-1} die Wurzeln von $z^p - 1$, so wird (§. 3. Einl.) der Ausdruck von x, dessen Wurzeln die p^{ten} Potenzen der Wurzeln des vorhergehenden sind, gefunden, wenn man das Product $(z^n + a_1 z^{n-1} + a_2 z^{n-2} + \ldots + a_n)(z^n + a_1\alpha z^{n-1} + a_2\alpha^2 z^{n-2} + \ldots .\, a_n\alpha^n)(z^n + a_1\alpha^2 z^{n-1} + a_1\alpha^4 z^{n-2} + \ldots + a_n\alpha^{2n}) \ldots\ldots (z^n + a_1\alpha^{p-1}z^{n-1} + a_1\alpha^{2(p-1)}z^{n-2} + \ldots\, a_n\alpha^{n(p-1)})$

entwickelt und statt z^n, x setzt. Setzt man nun hier nach (*No.* 1.) statt der Werthe $\alpha, \alpha^2, \ldots \alpha^{p-1}$ nur die Werthe 1, so geht jenes Product über in $(z^n + a_1 z^{n-1} + a_2 z^{n-2} + \ldots a_n)^p$. Es ist aber $(z^n + a_1 z^{n-1} + \ldots\ldots + a_n)^p \equiv z^{np} + a_1^p z^{n-1 \cdot p} + \ldots\ldots + a_n^p$ (*mod. p*). Dies folgt aus der durch den polynomischen Lehrsatz bestimmten Form der Coefficienten jener p^{ten} Potenz. Setzt man nun statt z^p, x, so wird der gesuchte Ausdruck von x, dessen Wurzeln die p^{ten} Potenzen der Wurzeln von $x^n + a_1 x^{n-1} + \ldots\ldots + a_n$ sind, dem Ausdruck $x^n + a_1^p x^{n-1} + a_2^p x^{n-2} + \ldots\ldots + a_n^p$ nach dem Modul p congruent werden. Oder der Ausdruck, welcher die p^{ten} Potenzen der Wurzeln eines gegebenen als Wurzeln enthält, ist nach dem Modul p einem Ausdruck congruent, dessen Coefficienten die p^{ten} Potenzen der entsprechenden Coefficienten des gegebenen sind.

3) Wendet man dies Resultat auf den Ausdruck $(x-1)^a$ an, in dem a eine ganze Zahl bedeutet, an, so findet man, da $(x-1)^a = x^a - ax^{a-1} +$ etc., dass der gesuchte Ausdruck $x^a - a^p x^{a-1} +$ etc. congruent sein werde. Da aber die Wurzeln von $(x-1)^a$ alle der Einheit gleich sind, so sind ihre p^{ten} Potenzen ebenfalls der Einheit gleich, und der gesuchte Ausdruck wird daher $(x-1)^a = x^a - ax^{a-1} +$ etc. sein. Man erhält mithin $x^a - a^p x^{a-1} =$ etc. $\equiv x^a - ax^{a-1} +$ etc. (*mod. p*) oder $a^p \equiv a$ (*mod. p*), und daher $a(a^{p-1} - 1) \equiv 0$ (*mod. p*) und mithinn, wenn a nicht $\equiv 0$ (*mod. p*) ist, $a^{p-1} \equiv 1$ (*mod. p*), d. h. also jede Zahl, die nicht $\equiv 0$ (*mod. p*) ist, giebt zur Potenz $p-1$, durch p dividirt den Rest 1. Da $x^{p-1} - 1$ für $x = a$ congruent 0 wird, so wird auch die Norm von $x^{p-1} - 1$ in Bezug auf $x - a$ congruent 0, und $x - a$ muss ein Factor von $x^{p-1} - 1$ sein (§. 11.). Setzt man für a nach der Reihe die Werthe $1, 2, \ldots\ldots p - 1$, so findet man, dass $x^{p-1} - 1$, die Factoren $x - 1, x - 2, \ldots\ldots x - (p-1)$ in Bezug auf den Modul p enthält. Da diese Factoren sämmtlich irreductibel sind, so schliesst man leicht, dass stets $x^{p-1} - 1 \equiv (x-1)(x-2) \ldots\ldots (x-(p-1))$ (*mod. p*) sei.*)

Durch Anwendung des in (*No.* 3.) enthaltenen Satzes auf das in (*No.* 2.) gewonnene Resultat geht nun der ausgesprochene Satz hervor. Der gesuchte Ausdruck war nämlich congruent $x^n + a_1^p x^{n-1} + \ldots\ldots + a_n^p$ und da nach (*No.* 2.) $a_1^p \equiv a_1$ (*mod. p*) etc. ist, so ist offenbar $x^n + a_1^p x^{n-1} + \ldots\ldots a_n^p \equiv x^n + a_1 x^{n-1} + \ldots\ldots + a_n$ (*mod. p*).

§. 14.

Erklärungen und Lehrsätze. 1) Zwei Ausdrücke derselben Wurzel α, eines irreductibelen einfachen Ausdrucks fx, sollen fortan nach dem Modul (p, α) congruent heissen, wenn sich der eine von ihnen als eine Summe des andern und eines $p$fachen Ausdrucks dieser Wurzel darstellen lässt.

Ist also $\phi\alpha = \psi\alpha + pR\alpha$, wo $\phi\alpha$, $\psi\alpha$ und $R\alpha$ Ausdrücke von α bedeuten, so ist $\phi\alpha$ congruent $\psi\alpha$ in Bezug auf den Modul (p, α), und es wird geschrieben werden $\phi\alpha \equiv \psi\alpha$ (*mod. p, α*).

2) Ist $\phi\alpha \equiv \psi\alpha$ (*mod. p, α*), so ist fx in Bezug auf den Modul p ein Divisor von $\phi x - \psi x$, und umgekehrt.

---

*) Anmerkung. Der Satz, dass $a^{p-1} \equiv 1$ (*mod. p*) gebührt *Fermat*, und trägt von ihm den Namen, der Satz, dass $x^{p-1} - 1 \equiv (x-1)(x-2) \ldots (x-(p-1))$ (*mod. p*) gebührt *Lagrange*.

Beweis. Da fx in Bezug auf den Modul p irreductibel ist, so ist es gewiss in algebraischer Beziehung irreductibel, und da $\phi\alpha \equiv \psi\alpha$ $(mod. p, \alpha)$ so muss $\phi\alpha - \psi\alpha - pR\alpha = 0$ sein. $\phi x - \psi x - pRx$ hat also mit fx die Wurzel α gemeinschaftlich, muss also durch fx algebraisch dividirbar sein (§. 5. Einl.). Man kann mithin $\phi x - \psi x - pRx = fx \,.\, Qx$ setzen, wo Qx einen Ausdruck von x bedeutet. Es ist mithin $\phi x - \psi x \equiv fx \,.\, Qx$ $(mod. p)$ und fx ein Divisor von $\phi x - \psi x$ in Bezug auf den Modul p. Die Umkehrung ergiebt sich leicht.

3) Bezeichnet α_1 eine andere Wurzel von fx als α, so hat man, wenn $\phi\alpha \equiv \psi\alpha$ $(mod. p, \alpha)$ ist, auch $\phi\alpha_1 \equiv \psi\alpha_1$ $(mod. p, \alpha_1)$.

Beweis. Wenn $\phi\alpha \equiv \psi\alpha$ $(mod. p, \alpha)$, so ist $\phi x - \psi x - pRx = fx \,.\, Qx$, und mithin da $f\alpha_1 = 0$ ist, $\phi\alpha_1 - \psi\alpha_1 - pR\alpha_1 = 0$ und daher $\phi\alpha_1 = \psi\alpha_1 + pR\alpha_1$ und $\phi\alpha_1 \equiv \psi\alpha_1$ $(mod. p, \alpha_1)$.

4) Man findet nun leicht folgende Sätze: die Summe, Differenz und das Product zweier Ausdrücke von α, die zweien anderen Ausdrücken nach dem Modul (p, α) einzeln verglichen congruent sind, ist congruent der Summe, Differenz oder dem Product der entsprechenden Ausdrücke nach dem Modul (p, α).

5. Wenn das Prodruct zweier Ausdrücke von α congruent 0 nach dem Modul (p, α) ist, so ist einer von jenen Ausdrücken selbst nach diesem Modul congruent 0.

Beweis. Gesetzt die beiden Ausdrücke wären $\phi\alpha$ und $\psi\alpha$, und also $\phi\alpha \,.\, \psi\alpha \equiv 0$ $(mod. p, \alpha)$, so muss (*№*. 3.) $\phi x \,.\, \psi x - pRx = fx \,.\, Qx$ sein, wo Rx und Qx wie oben Ausdrücke von x bedeuten. Man erhält mithin $\phi x \,.\, \psi x \equiv fx \,.\, Qx$ $(mod. p)$, und da fx ein irreductibeler Ausdruck ist, so muss er mithin (§. 5.) entweder ein Factor von ϕx oder von ψx in Bezug auf den Modul p sein. Für den ersten Fall findet man aber leicht $\phi\alpha \equiv 0$ $(mod. p, \alpha)$ und für den andern $\psi\alpha \equiv 0$ $(mod. p, \alpha)$.

6) Ist $\phi\alpha \,.\, \psi\alpha \equiv \phi_1\alpha \,.\, \psi_1\alpha$ $(mod. p, \alpha)$ und $\phi\alpha \equiv \phi_1\alpha$ $(mod. p, \alpha)$ aber nicht $\equiv 0$ $(mod. p, \alpha)$, so ist auch $\psi\alpha \equiv \psi_1\alpha$.

Beweis. Nach (*№*. 5.) ist $\phi\alpha \,.\, \psi\alpha \equiv \phi_1\alpha \,.\, \psi\alpha$ $(mod. p, \alpha)$. Man hat daher auch $\phi_1\alpha \,.\, \psi\alpha \equiv \phi_1\alpha \,.\, \phi_1\alpha$ $(mod. p, \alpha)$ oder $\phi_1\alpha\,(\psi\alpha - \psi_1\alpha) \equiv 0$ $(mod. p, \alpha)$. Da aber $\phi_1\alpha$ nicht $\equiv 0$ $(mod. p, \alpha)$ ist, so muss (*№*. 5.) $\psi\alpha - \psi_1\alpha \equiv 0$ $(mod\ p, \alpha)$ oder $\psi\alpha \equiv \psi_1\alpha$ $(mod. p, \alpha)$ sein.

7) Eine Function von x, deren Coefficienten Ausdrücke von α sind, wird als ein Ausdruck von x nach dem Modul (p, α) betrachtet werden. Zwei Ausdrücke von x werden nach dem Modul (p, α) congruent gesetzt werden, wenn die Coefficienten der gleichen Potenzen von x in beiden nach dem Modul (p, α) congruent sind.

8. Ein Ausdruck von α, der sich weder 0 noch einer ganzen Zahl nach dem Modul (p, α) congruent setzen lässt, soll noch insbesondere ein zum Modul (p, α) gehöriger Ausdruck genannt werden. Wohingegen diejenigen Ausdrücke von α, welche sich 0 oder einer ganzen Zahl nach dem Modul (p, α) congruent setzen lassen, zum Modul p gehörige Ausdrücke genannt werden sollen. Ebenso soll eine ganze Function von x, deren Coefficienten sämmtlich oder zum Theil Ausdrücke von α sind, die zum Modul (p, α) gehören, ein Aus-

druck von x, der zu dem Modul (p, α) gehört, heissen. Gehören aber die Coefficienten sämmtlich zum Modul p, so soll sie ein zu dem Modul p gehöriger Ausdruck von x heissen.

§. 15.

Lehrsatz. Die p^{te} Potenz irgend eines zum Modul (p, α) gehörigen Ausdrucks von x kann nicht dem Ausdruck selbst, nach dem Modul (p, α) congruent sein, oder wenn $\phi\alpha$ einen zum Modul p, α gehörigen Ausdruck darstellt, so kann nicht sein $(\phi\alpha)^p \equiv \phi\alpha \ (mod.\ p, \alpha)$.

Beweis. Wenn $(\phi\alpha)^p \equiv \phi\alpha \ (mod.\ p, \alpha)$ wäre, so wäre auch (§. 14. ℳo. 6.) $(\phi\alpha)^{p-1} \equiv 1$ oder $(\phi\alpha)^{p-1} - 1 \equiv 0 \ (mod.\ p.\ \alpha)$. Nach (§. 13. ℳo. 3.) ist aber $(\phi\alpha^{p-1} - 1) \equiv (\phi\alpha - 1)(\phi\alpha - 2) \ldots (\phi\alpha - (p-1)) \ (mod.\ p, \alpha)$, sollte also $(\phi\alpha^{p-1} - 1) \equiv 0 \ (mod.\ p.\ \alpha)$ werden, so müsste einer der Factoren $\phi\alpha - 1$, $\phi\alpha - 2 \ldots\ldots$, $\phi\alpha - (p-1) \equiv 0 \ (mod.\ p, \alpha)$ werden (§. 14. ℳo. 5.). Dies geht aber nicht an, weil $\phi\alpha$ ein zum Modul (p, α) gehöriger Ausdruck ist.

§. 16.

Lehrsatz. Der Ausdruck von x, welchen die p^{ten} Potenzen der Wurzeln eines Ausdrucks, dessen erster Coefficient 1 ist, und welcher zu dem Modul $(p.\ \alpha)$ gehört, als Wurzeln in sich schliesst, kann nicht mit jenem Ausdruck nach dem Modul (p, α) congruent sein.

Beweis. Bedeutet also Fx einen Ausdruck von x, dessen erster Coefficient 1 ist, und in welchem sonst Coefficienten vorkommen, die zum Modul (p, α) gehören, so soll der Ausdruck, dessen Wurzeln die p^{ten} Potenzen der Wurzeln von Fx sind, nicht mit Fx nach dem Modul (p, α) congruent sein können. Es folgt nämlich aus (§. 13. ℳo. 2.), dass dieser zweite Ausdruck aus Fx hervorgehen werde, wenn man statt der Coefficienten von Fx die p^{ten} Potenzen derselben einsetzt. Da aber die p^{ten} Potenzen von denjenigen Coefficienten, die zum Modul $(p.\ \alpha)$ gehören, sich nicht selbst nach diesem Modul congruent sind (§. 15.), so folgt der Satz.

§. 17.

Lehrsatz. $\alpha^{p^m} - \alpha$ kann nicht nach dem Modul $(p.\ \alpha)$ congruent 0 sein, wenn der Grad von fx, von welchem Ausdruck α eine Wurzel ist, die Zahl m überschreitet.

Beweis. Gesetzt $\alpha^{p^m} - \alpha \equiv 0 \ (mod.\ p, \alpha)$, so wäre auch $\alpha^{p^m} \equiv \alpha$ $(mod.\ p, \alpha)$ und daher auch

$$(x-\alpha)(x-\alpha^p)(x-\alpha^{p^2})\ldots\ldots(x-\alpha^{p^{m-1}}) \equiv (x-\alpha^p)(x-\alpha^{p^2})\ldots\ldots(x-\alpha^{p^{m-1}})$$
$$(x-\alpha^{p^m}) \ (mod.\ p, \alpha)\ .$$

Der Ausdruck rechts enthält aber offenbar die p^{ten} Potenzen der Wurzeln des ersten als Wurzeln, er kann ihm mithin nur dann congruent werden, wenn die Coefficienten von $(x-\alpha)(x-\alpha^p) \ldots (x-\alpha^{p^{m-1}})$ zum Modul p gehören (§. 16.), alsdann muss aber jeder Coefficient dieses Ausdrucks von der Form $z + pM\alpha$ sein, von $M\alpha$ einen Ausdruck von α bedeutet. Dies vorausgesetzt wird $(x-\alpha)(x-\alpha^p) \ldots\ldots (x-\alpha^{p^{m-1}})$ offenbar von der Form $x^m + A_1 x^{m-1} + A_2 x^{m-2} + \ldots\ldots + A^m + pF(x, \alpha)$ sein, wo $A_1, A_2, \ldots$

A_m ganze Zahlen und $F(x, \alpha)$ einen Ausdruck von x nach dem Modul (p, α) bedeutet. Bedenkt man aber, das die bisherigen Schlussfolgen, sich in derselben Weise auf jede der Wurzeln von fx anwenden lassen, so erhält man, indem man die sämmtlichen Wurzeln von fx mit $\alpha, \alpha_1, \alpha_2, \ldots. \alpha_{n-1}$ bezeichnet, folgende Gleichungen

$$(x-\alpha)(x-\alpha^p)(x-\alpha^{p^2})\ldots.(x-\alpha^{p^{m-1}}) = x^m + A_1x^{m-1} + A_2x^{m-2} + \ldots. + A_m + pF(x, \alpha)$$
$$(x-\alpha_1)(x-\alpha_1{}^p)(x-\alpha_1{}^{p^2})\ldots.(x-\alpha_1{}^{p^{m-1}}) = x^m + A_1x^{m-1} + A_2x^{m-2} + \ldots. + A_m + pF(x, \alpha_1)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$(x-\alpha_{n-1})(x-\alpha_{n-1}{}^p)(x-\alpha_{n-1}{}^{p^2})\ldots.(x-\alpha_{n-1}{}^{p^{m-1}}) = x^m + A_1x^{m-1} + A_2x^{m-2} + \ldots + A_m + pF(x, \alpha_{n-1}).$$

Multiplicirt man beide Seiten dieser Gleichungen in einander, so wird die rechte Seite offenbar $\equiv (x^m + A_1x^{m-1} + A_2x^{m-2} + \ldots + A_m)^n$ $(mod.\ p)$, die linke wird aber den Factor $(x-\alpha)(x-\alpha_1)(x-\alpha_2)\ldots.(x-\alpha_{n-1})$ oder fx haben, woraus zu schliessen, dass $(x^m + A_1x^{m-1} + \ldots. + A_m)^n$ ebenfalls den irreductibeln Ausdruck fx als Factor nach dem Modul p haben müsste. Dies geht aber nicht an, weil der Grad von fx der Voraussetzung nach grösser als m ist.

§. 18.

Hauptsatz. Wenn fx ein einfacher irreductibeler Ausdruck nach dem Modul p, und α eine Wurzel desselben ist, so ist $fx \equiv (x-\alpha)(x-\alpha^p)(x-\alpha^{p^2})\ldots.(x-\alpha^{p^{n-1}})$ $(mod.\ p, \alpha)$ und $\alpha^{p^n-1} \equiv 1$ $(mod.\ p, \alpha)$.

Beweis. Gesetzt $\alpha, \alpha_1, \ldots. \alpha_{n-1}$ seien die Wurzeln von fx, so folgt (§. 13.), dass jeder Ausdruck, dessen Wurzeln die (p^m)ten Potenzen jener sind (wenn m eine ganze positive Zahl bedeutet) mit fx nach dem Modul p congruent sein werde. Ein solcher Ausdruck wird daher von der Form sein $fx + pF_mx$, wo F_mx einen Ausdruck von x bedeutet. Setzt man daher in diesen Ausdruck statt x eine Wurzel desselben, also α^{p^m}, so erhält man $f\alpha^{p^m} + pF_m\alpha^{p^m} = 0$ oder $f\alpha^{p^m} \equiv 0$ $(mod.\ p, \alpha)$. Da α eine Wurzel von fx ist, so ist $x - \alpha$ ein algebraischer Divisor von fx und man kann daher $fx = (x-\alpha)(x^{n-1} + b_1x^{n-2} + b_2x^{n-3} + \ldots. + b_{n-1})$ setzen, wo $b_1, b_2, \ldots\ b_{n-1}$ Ausdrücke von α bedeuten. Setzt man nun in diese Gleichung statt x den Ausdruck α^p, so erhält man $f\alpha^p = (\alpha^p - \alpha)(\alpha^{p(n-1)} + b_1\alpha^{p(n-2)} + b_2\alpha^{p(n-3)} + \ldots. + b_{n-1})$. Da nun aber $f\alpha^p \equiv 0$ $(mod.\ p, \alpha)$ ist, und $\alpha^p - \alpha$ nicht $\equiv 0$ $(mod.\ p, \alpha)$ sein kann, wenn $n > 1$ ist, (§. 17.), so muss $\alpha^{p(n-1)} + b_1\alpha^{p(n-2)} + \ldots\ldots b_{n-1} \equiv 0$ $(mod.\ p, \alpha)$ sein (§. 14. №. 4.). Es ist mithin auch $x^{n-1} + b_1x^{n-2} + b_2x^{n-3} + \ldots. + b_{n-1} - (\alpha^{p(n-1)} + b_1\alpha^{p(n-2)} + b_2\alpha^{p(n-3)} + \ldots + b_{n-1})$ oder $x^{n-1} - \alpha^{p(n-1)} + b_1(x^{n-2} - \alpha^{p(n-2)}) + b_2(x^{n-3} - \alpha^{p(n-3)})\ldots\ldots. b_{n-2}(x - \alpha^p) \equiv x^{n-1} + b_1x^{n-2} + b_2x^{n-3} + \ldots. + b_{n-1}$ $(mod.\ p, \alpha)$. Offenbar hat aber die linke Seite der Congruenz den Factor $x - \alpha^p$ und man kann sie daher durch $(x-\alpha^p)(x^{n-2} + c_1x^{n-3} + c_2x^{n-4} + \ldots + c_{n-2})$ darstellen, wo $c_1, c_2, \ldots. c_{n-2}$ Ausdrücke von α bedeuten. Man erhält daher $fx \equiv (x-\alpha)(x-\alpha^p)(x^{n-2} + c_1x^{n-3} + c_2x^{n-4} + \ldots + c_{n-2})$ $(mod.\ p, \alpha)$ und daher auch $fx^{p^2} \equiv (\alpha^{p^2} - \alpha)(\alpha^{p^2} - \alpha^p)(\alpha^{p^2(n-2)} + c_1\alpha^{p^2(n-3)} + c_2\alpha^{p^2} + \ldots + c_{n-2})$ $(mod.\ p.\alpha)$. Offenbar ist aber $\alpha^{p^2} - \alpha^p \equiv (\alpha^p - \alpha)^p$ $(mod.\ p, \alpha)$*) und da (§. 17.) $\alpha^p - \alpha$ nicht $\equiv 0$ $(mod.\ p, \alpha)$ sein kann, so kann

*) Anmerkung. Entwickelt man nämlich $(\alpha^p - \alpha)^p$ nach dem binomischen Satze, so werden alle Glieder ausser dem ersten und letzten Coefficienten haben, die $\equiv 0$ $(mod.\ p)$ sind. Man erhält mithin $(\alpha^p - \alpha)^p \equiv \alpha^{p^2} - \alpha^p$ $(mod\ p, \alpha)$. Hieraus folgt nun $(\alpha^p - \alpha)^{p^2} \equiv (\alpha^{p^2} - \alpha^p)^p$ $(mod\ p, \alpha)$ und ferner durch den binomischen Satz $(\alpha^{p^2} - \alpha^p)^p \equiv \alpha^{p^3} - \alpha^{p^2}$ $(mod.\ p, \alpha)$ und daher $(\alpha^p - \alpha)^{p^2} \equiv \alpha^{p^3} - \alpha^{p^2}$ $(mod.\ p, \alpha)$ und allgemein $(\alpha^p - \alpha)^{p^{m-1}} \equiv \alpha^{p^m} - \alpha^{p^{m-1}}$ $(mod.\ p, \alpha)$.

auch nicht $(\alpha^p - \alpha)^p \equiv 0\,(mod.\ p, \alpha)$ sein (§. 14. *No.* 5.). Da nun $f\alpha^{p^2} \equiv 0$ und (so fern $n > 2$) $(\alpha^{p^2} - \alpha)\,(\alpha^{p^2} - \alpha^p)$ nicht $\equiv 0\ (mod.\ p, \alpha)$ sein kann (§. 14. *No.* 5. §. 17.), so muss $\alpha^{p^2(n-2)} + c_1 \alpha^{p^2(n-3)} + \ldots\ldots + c_{n-2} \equiv 0\ (mod.\ p, \alpha)$ sein. Hieraus schliesst man wie vorher, dass $x^{n-2} + c_1 x^{n-3} + \ldots + c_{n-2}$ den Factor $x - \alpha^{p^2}$ haben müsse, und erlangt $fx \equiv (x-\alpha)(x-\alpha^p)(x-\alpha^{p^2})$ $(x^{n-3} + d_1 x^{n-4} + d_2 x^{n-5} + \ldots\ldots + d_{n-3})\,(mod.\ p, \alpha)$. Durch fortgesetzte Anwendung der angeführten Sätze erlangt man nun natürlich zuletzt $fx \equiv (x-\alpha)$ $(x-\alpha^p)\,(x-\alpha^{p^2})\ldots\ldots(x-\alpha^{p^{n-1}})\,(mod.\ p, \alpha)$. Da nun $f\alpha^{p^n} \equiv 0\,(mod.\ p, \alpha)$ ist, so muss auch $(\alpha^{p^n} - \alpha)\,(\alpha^{p^n} - \alpha^p)(\alpha^{p^n} - \alpha p^2)\ldots\ldots(\alpha^{p^n} - \alpha^{p^{n-1}}) \equiv (mod.\ p, \alpha)$ sein. Da aber $(\alpha^{p^n} - \alpha^p)(\alpha^{p^n} - \alpha^{p^2})\ldots\ldots(\alpha^{p^n} - \alpha^{p^{n-1}}) \equiv (\alpha^{p^{n-1}} - \alpha)^p\,(\alpha^{p^{n-2}} - \alpha)^{p^2}\ldots\ldots$ $(\alpha^p - \alpha)^{p^{n-1}}\ (mod.\ p, \alpha)$ ist, (Vergl. die Anmerkung) und (§. 17.) keiner der Ausdrücke $\alpha^{p^{n-1}} - \alpha$, $\alpha^{p^{n-2}} - \alpha$, ... $\alpha^p - \alpha$ congruent 0 $(mod.\ p, \alpha)$ werden kann, so muss $\alpha^{p^n} - \alpha \equiv 0\,(mod.\ p, \alpha)$ werden. Da aber $\alpha^{p^n} - \alpha \equiv \alpha(\alpha^{p^n-1} - 1)$ $(mod.\ p, \alpha)$ ist, und α nicht $\equiv 0$ sein kann, wenn fx nicht x ist, so ist $\alpha^{p^n-1} \equiv 1\ (mod.\ p, \alpha)$.

Zusatz. Da $\alpha^{p^n-1} - 1 \equiv 0\ (mod.\ p, \alpha)$ ist, so folgt dass fx in Bezug auf den Modul p ein Divisor $x^{p^n} - 1$ ist (§. 14. *No.* 2.) Hieraus folgt, dass die Congruenz $x^k - 1 \equiv 0\ (mod. p)$ den allgemeinsten Character in Bezug auf ihre Wurzeln in sich trägt, wenn man dem k wie dem p alle hier möglichen Werthe beilegt.

§. 19.

Lehrsatz. Die $(p^n-1)^{te}$ Potenz jedes Ausdrucks von α ist congruent 1 nach dem Modul (p, α), wenn der Ausdruck nicht $\equiv 0\ (mod.\ p, \alpha)$ ist.

Beweis. Es sei $\phi\alpha$ der Ausdruck von α und $= a_0 \alpha^k + a_1 \alpha^{k-1} + \ldots\ldots + a_k$. Nun kann leicht, entweder durch den polymonischen Satz, oder durch fortgesetzte Anwendung des binomischen gezeigt werden, dass $(a_0 \alpha^k + a_1 \alpha^{k-1} + \ldots\ldots + a_k)^p \equiv a_0^p\ \alpha^{k \cdot p} + a_1 \alpha^{(k-1)\cdot p} + \ldots\ldots a_k^p\ (mod.\ p, \alpha)$ ist. Da aber $a_0, a_1, \ldots\ldots a_k$ ganze Zahlen sind, so ist $a_0^p \equiv a_0\ (mod.\ p)$, $a_1^p \equiv a_1\ (mod.\ p)$ etc. (§. 13. *No.* 3). Man erhält mithin $(a_0 \alpha^k + a_1 \alpha^{k-1} + \ldots\ldots a_k)^p \equiv a_0 \alpha^{k \cdot p} + a_1 \alpha^{k-1 \cdot p} + \ldots\ldots + a_k\ (mod.\ p, \alpha)$ und mithin $(a_0 \alpha^k + a_1 \alpha^{k-1} + \ldots\ldots a_k)^{p^2} \equiv (a_0 \alpha^{kp} + a_1 \alpha^{(k-1)p} + \ldots\ldots + a_k)^p\ (mod.\ p, \alpha)$ und den letzten Ausdruck durch ähnliche Schlussfolgen $\equiv a_0 \alpha^{k \cdot p^2} + a_1 \alpha^{(k-1)p^2} + \ldots\ldots + a_k$ $(mod.\ p, \alpha)$, mithin $(a_0 \alpha^k + a_1 \alpha^{k-1} + \ldots\ldots + a_k)^{p^2} \equiv a_0 \alpha^{k \cdot p^2} + a_1 \alpha^{(k-1)p^2} + \ldots$ $+ a_k\ (mod.\ p, \alpha)$. Durch eine fortgesetzte Schlussfolge derselben Art erhält man nun $(a_0 \alpha^k + a_1 \alpha^{k-1} + \ldots\ldots + a_k)^{p^n} \equiv a_0 \alpha^{k \cdot p^n} + a_1 \alpha^{(k-1)p^n} + \ldots\ldots + a_k$ $(mod.\ p, \alpha)$. Da nun aber $\alpha^{p^n} \equiv \alpha\ (mod.\ p, \alpha)$ ist (§. 18.), so erlangt man $(a_0 \alpha^k + a_1 \alpha^{k-1} + \ldots\ldots + a_k)^{p^n} \equiv a_0 \alpha^k + a_1 \alpha^{k-1} + \ldots\ldots + a_k\ (mod.\ p, \alpha)$ oder $(\phi\alpha)^{p^n} \equiv \phi\alpha\ (mod.\ p, \alpha)$, und daher durch Division, wenn $(\phi\alpha)$ nicht $\equiv 0$ $(mod.\ p, \alpha)$ ist, $(\phi\alpha)^{p^n-1} \equiv 1\ (mod.\ p, \alpha)$ was zu beweisen war.

Zusatz. Ist ϕx nicht $\equiv 0\ (mod.\ p, \alpha)$ und bedeutet $\psi\alpha$ irgend einen Ausdruck von α, so kann man stets einen andern Ausdruck von α, $\phi_1\alpha$ so bestimmen, dass $\phi\alpha \,.\, \phi_1\alpha \equiv \psi\alpha\ (mod.\ p, \alpha)$ wird. Man hat zu dem Ende $\phi_1\alpha$ nur

nur $\equiv (\phi\alpha)^{p^n-1} \cdot \psi\alpha$ (*mod. p. α*) zu setzen. Zwei verschiedene Ausdrücke von α, die beide jener Congruenz genügen, müssen nach dem Modul (p, α) congruent sein. Denn hätte man $\psi\alpha \equiv \phi\alpha \cdot \phi_1\alpha \equiv \phi\alpha \cdot \phi_2\alpha$ (*mod.* p, α), so folgt durch Division (§. 14. *No.* 6) $\phi_1\alpha \equiv \phi_2\alpha$ (*mod.* p, α).

§. 20.

Erklärungen und Lehrsätze. 1) Ein Ausdruck von α, dessen Grad geringer als der von fx ist, und dessen Coefficienten sämmtlich kleiner als p sind, soll ein kleinster Rest in Bezug auf den Modul (p, α) genannt werden.

2) Jeder Ausdruck von α ist einem kleinsten Reste nach dem Modul (p, α) congruent.

Beweis. Nennt man den Ausdruck $\phi\alpha$, so setze man $\phi x = fx \cdot Qx + Rx$, wo Qx den Quotienten angiebt, den man erhält, wenn man ϕx durch fx algebraisch dividirt, und Rx den Rest, so wird Rx offenbar von einem geringeren Grade als fx sein und man erhält zunächst $\phi\alpha \equiv R\alpha$ (*mod. p. α*). Nun setze man statt der Coefficienten von $R\alpha$ die Reste, welche man erhält, wenn man dieselben durch p dividirt, und nenne den hervorgehenden Ausdruck $R_1\alpha$, so wird $\phi\alpha \equiv R_1\alpha$ (*mod.* p, α) sein, und $R_1\alpha$ die verlangte Form haben.

3) Ist n der Grad von fx, so ist die Anzahl sämmtlicher verschiedenen kleinsten Reste nach dem Modul (p, α), wenn man 0 ausschliesst, durch $p^n - 1$ ausgedrückt.

Beweis. Die allgemeine Form eines kleinsten Restes ist $a_0\alpha^{n-1} + a_1\alpha^{n-2} + a_2\alpha^{n-3} + \ldots\ldots + a_{n-1}$. Dieselbe schliesst n Glieder in sich, und jeder der Coefficienten $a_0, a_1 \ldots a_{n-1}$ muss der Zahlenreihe 0, 1, 2, ... $p-1$ entnommen sein. Offenbar kann man nun nach bekannten Sätzen aus der Combinations-Lehre p^n solche Ausdrücke bilden. Da aber unter diesen einer ist, dessen sämmtliche Coefficienten 0 sind, und der mithin selbst 0 ist, so bleiben mit Ausschluss von diesem $p^n - 1$ verschiedene kleinste Reste.

4) Zwei Ausdrücke von α, welche verschiedenen kleinsten Resten nach dem Modul (p, α) congruent sind, sollen überhaupt verschiedene Ausdrücke nach dem Modul (p, α) oder schlechtweg verschiedene Ausdrücke heissen.

5) Ausdrücke von x nach dem Modul (p, α) sollen einfache heissen, wenn der Coefficient ihrer höchsten Potenz gleich 1 ist, vielfache hingegen, wenn er nicht 1 ist.

6) Jeder vielfache Ausdruck von x ist einem einfachen Ausdruck desselben Grades multiplicirt in den Coefficienten der höchsten Potenz von x, nach dem Modul (p, α) congruent.

Beweis wie im §. 2., mit Hinzuziehung des Zusatzes zu (§. 19.).

7) Ist es möglich ein Product zweier Ausdrücke von x aufzustellen (von denen aber keiner einem niedrigeren Grade als dem ersten angehört) das einem gegebenen Ausdrucke nach dem Modul (p, α) congruent wird, so soll jeder der Factoren ein Factor oder ein Divisor des gegebenen Ausdrucks, in

Bezug auf den Modul (p, α), oder wenn keine Zweideutigkeit zu befürchten, blos ein Factor oder Divisor desselben heissen.

Ein Ausdruck von x vom m^{ten} Grade, der keinen Divisor nach dem Modul (p, α) hat, soll ein irreductibeler Ausdruck vom m^{ten} Grade nach dem Modul (p, α) heissen.

8) Ein Rest nach dem Modul (p, α), der in einen Ausdruck von x, statt x eingesetzt den Ausdruck $\equiv 0$ $(mod.\ p, \alpha)$ macht, wird eine Wurzel des Ausdrucks nach dem Modul (p, α) heissen.

9) Ein Ausdruck von x, der vom m^{ten} Grade ist, kann höchstens m verschiedene Wurzeln nach dem Modul (p, α) haben.

Beweis. Man setze den Ausdruck congruent (*No.* 6.) $a_0(x^m + a_1 x^{m-1} + \ldots + a_m)$ $(mod.\ p, \alpha)$, wo $a_0, a_1, \ldots a_m$ Ausdrücke von α nach dem Modul (p, α) bedeuten. Gesetzt nun $\phi_1\alpha$ wäre eine Wurzel jenes Ausdrucks, so hätte man $a_0(\phi_1\alpha^m + a_1\phi_1\alpha^{m-1} + \ldots + a_m) \equiv 0$ $(mod.\ p, \alpha)$ und daher $a_0\{(x^m - \phi_1\alpha^m) + a_1(x^{m-1} - \phi_1\alpha^{m-1}) + \ldots\ a^{m-1}(x - \phi_1\alpha)\} \equiv a_0(x^m + a_1x^{m-1} + \ldots + a_m)$ $(mod.\ p, \alpha)$. Offenbar hat aber der Ausdruck auf der linken Seite den Factor $x - \phi_1\alpha$, man kann daher den Ausdruck auf die Form bringen $a_0(x - \phi_1\alpha)(x^{m-1} + b_1x^{m-2} + \ldots + \ldots b_{m-1})$, wo $b_1, b_2, \ldots b_{m-1}$ Ausdrücke von α bedeuten. Gesetzt nun $\phi_2\alpha$ wäre eine andere Wurzel des Ausdrucks, so müsste $a_0(\phi_2\alpha - \phi_1\alpha)(\phi_2\alpha^{m-1} + b_1\phi_2\alpha^{m-2} + \ldots + b_{m-1}) \equiv 0$ $(mod.\ p, \alpha)$ sein. Da aber $a_0(\phi_2\alpha - \phi_1\alpha)$ nicht $\equiv 0$ $(mod.\ p, \alpha)$ sein kann, so muss $\phi_2\alpha^{m-1} + b_1\phi_2\alpha^{m-2} + \ldots\ b_{m-1} \equiv 0$ $(mod.\ p, \alpha)$ und aus ähnlichem Grunde, wie vorher $x^{m-1} + b_1x^{m-2} + \ldots\ b_{m-1} \equiv (x - \phi_2\alpha)(x^{m-2} + c_1x^{m-3} + \ldots c_{m-2})$ $(mod.\ p, \alpha)$ sein, wo $c_1, c_2, \ldots c_{m-1}$ Reste nach dem Modul (p, α) bedeuten. Es wird mithin $a_0(x^m + a_1x^{m-1} + \ldots + a_m) \equiv a_0(x - \phi_1\alpha)(x - \phi_2\alpha)(x^{m-2} + c_1x^{m-3} + \ldots c_{m-2})$ $(mod.\ p, \alpha)$. Durch fortgesetzte Schlussfolgen derselben Art findet man, wenn $\phi_1\alpha, \phi_2\alpha, \ldots \phi_m\alpha$ sämmtlich Wurzeln des vorgelegten Ausdrucks sind $a_0(x^m + a_1x^{m-1} + \ldots + a_m) \equiv a_0(x - \phi_1\alpha)(x - \phi_2\alpha)(x - \phi_3\alpha) \ldots (x - \phi_m\alpha)$ $(mod.\ p, \alpha)$. Sollte der Ausdruck nun noch einen Rest $\psi\alpha$ zur Wurzel haben, so müsste $a_0(\psi\alpha - \phi_1\alpha)(\psi\alpha - \phi_2\alpha)(\psi\alpha - \phi_3\alpha) \ldots (\psi\alpha - \phi_m\alpha) \equiv 0$ $(mod.\ p, \alpha)$ sein. Dies kann aber nicht anders geschehen, als wenn einer der Factoren $\psi\alpha - \phi_1\alpha$, $\psi\alpha - \phi_2\alpha$, etc. $\equiv 0$ $(mod.\ p, \alpha)$ wird. Da aber dies nicht angeht, weil nach der Voraussetzung $\psi\alpha$, von sämmtlichen m Wurzeln $\phi_1\alpha, \phi_2\alpha, \ldots \phi_m\alpha$ verschieden ist, so kann auch der Ausdruck nicht mehr als m verschiedene Wurzeln haben.

Zusatz. Da sämmtliche kleinste Reste ausser 0 nach dem Modul (p, α) Wurzeln des Ausdruckes $x^{p^n-1} - 1$ sind, (§. 19.) so folgt, dass, wenn man dieselben mit $\phi_1\alpha, \phi_2\alpha, \ldots \phi_{p^n-1}\alpha$ bezeichnet, stets folgende Congruenz $x^{p^n-1} - 1 \equiv (x - \phi_1\alpha)(x - \phi_2\alpha) \ldots (x - \phi_{p^n-1}\alpha)$ $(mod.\ p, \alpha)$ statt finden werde.

10) Ist das Product aus einem Ausdruck von x nach dem Modul (p, α) und einem irreductibeln einfachen Ausdruck desselben Moduls, dem Product zweier andern Ausdrücke, nach dem Modul (p, α) congruent, so hat einer derselben den irreductibeln Ausdruck nach dem Modul (p, α) zum Divisor.

Beweis wie in §. 5.

11) Jeder Ausdruck kann nur auf eine Weise dem Producte einfacher irreductibeler Ausdrücke von x, und eines Restes nach dem Modul (p, α) congruent gesetzt werden.

Beweis wie in §. 6.

§. 21.

Erklärung und Lehrsatz. Ist q die kleinste Zahl, welche als Exponent zu dem Reste $\phi\alpha$ gesetzt die hervorgehende Potenz $\equiv 1$ $(mod.\ p, \alpha)$ macht, so soll gesagt werden $\phi\alpha$ gehöre zu q.

Gehört $\phi\alpha$ zu q, so muss q ein Theiler von $p^n - 1$ sein.

Beweis. Gesetzt q wäre kein Factor von $p^n - 1$, so setze man $p^n - 1 = q \,.\, d + r$, wo d der Quotient ist, den man bei der Division von $p^n - 1$ durch q erhält, und r der Rest. Es ist mithin $r < q$. Da nun $(\phi\alpha)^{qd+r} \equiv 1$ $(mod.\ p.\ \alpha)$ (§. 19.), und $(\phi\alpha)^{qd} \equiv 1$ $(mod.\ p, \alpha)$, weil $(\phi\alpha)^q \equiv 1$ $(mod\ p, \alpha)$ ist, so ist offenbar auch $(\phi\alpha)^r \equiv 1$ $(mod.\,p, \alpha)$, gegen die Voraussetzung, da $r < q$ ist.

Zusatz. Gehört nun $\phi\alpha$ zur Zahl q, so werden sämmtliche Ausdrücke $\phi\alpha$, $(\phi\alpha)^2, \ldots\ldots (\phi\alpha)^{q-1}$, $(\phi\alpha)^q$ deu Ausdruck $x^q - 1 \equiv 0$ $(mod.\ p, \alpha)$ machen, und sämmtlich von einander verschieden sein (denn wären etwa zwei congruent, deren Exponenten μ und ν sein mögen, so müsste, wenn $\nu > \mu$ ist, auch $\phi\alpha^{\nu-\mu} \equiv 1$ $(mod.\,p.\ \alpha)$ sein, was nicht möglich ist, da ν und μ und daher auch $\nu - \mu$ kleiner als q sein muss) es muss mithin (§. 10. No. 9.) $x^q - 1 \equiv (x - \phi\alpha)(x - \phi\alpha^2)(x - \phi\alpha^3) \ldots\ldots (x - \phi\alpha^q)$ $(mod.\,p, \alpha)$ sein.

§. 22.

Lehrsatz. Gehört $\phi\alpha$ zum Exponenten f und $\psi\alpha$ zum Exponenten q, so kann man stets einen Ausdruck bilden, der zu dem kleinsten gemeinschaftlichen Vielfachen von f und q gehört. Bildet man von diesem Ausdruck seine verschiedenen Potenzen, so werden unter diesen zwei Ausdrücke vorkommen, die mit $\phi\alpha$ und $\psi\alpha$ nach dem Modul $(p.\ \alpha)$ congruent sind.

Beweis. Sind f und q relative Primzahlen, so wird $\phi\alpha \,.\, \psi\alpha$ zu $f \,.\, q$ gehören. Zunächst wird nämlich

$$(\phi\alpha \,.\, \psi\alpha)^{fq} = (\phi\alpha^f)^q\,(\psi\alpha^q)^f \equiv 1 \;(mod.\,p, \alpha),$$

weil

$$(\phi\alpha)^f \equiv 1 \text{ und } (\psi\alpha)^q \equiv 1 \;(mod.\,p, \alpha)$$

ist. Hieraus folgt, dass der Exponent, zu dem $\phi\alpha \,.\, \psi\alpha$ gehört, ein Theiler von $p \,.\, q$ sein muss. Wäre er nun $\frac{q}{\mathfrak{q}} \cdot \frac{f}{\mathfrak{f}}$, wo $\mathfrak{q}$ und $\mathfrak{f}$, so wie $\frac{q}{\mathfrak{q}}$ und $\frac{f}{\mathfrak{f}}$ ganze Zahlen sind, so hätte man

$$(\phi\alpha \,.\, \psi\alpha)^{\frac{f}{\mathfrak{f}} \cdot \frac{q}{\mathfrak{q}}} \equiv 1 \;(mod.\,p.\ \alpha).$$

Erhebt man beide Seiten der Congruenz in die $\mathfrak{q}^{te}$ Potenz, und bedenkt, dass $(\psi\alpha)^{q \cdot \frac{f}{\mathfrak{f}}} \equiv 1$ $(mod.\ p, \alpha)$ sein muss, so erhält man $(\phi\alpha)^{\frac{f}{\mathfrak{f}} \cdot q} \equiv 1$ $(mod.\,p, \alpha)$. Da aber $\phi\alpha$ zu f gehört, so muss $\frac{f}{\mathfrak{f}} \,.\, q$ nothwendig ein Vielfaches von f, oder $\frac{q}{\mathfrak{f}}$ eine ganze Zahl sein. Da aber q zu f, mithin auch zu $\mathfrak{f}$ als einem Factor von f, relative Primzahl ist, so kann $\frac{q}{\mathfrak{f}}$ nur eine ganze Zahl sein, wenn $\mathfrak{f}$ gleich 1 ist. Es muss mithin f gleich 1, und ebenfalls nach ähnlichen Schlüssen $\mathfrak{q}$ gleich 1 sein. Da nun fq das kleinste Vielfache von f und q ist, wenn diese relative Primzahlen sind, und $\phi\alpha \,.\, \psi\alpha$ zu fq gehört, so ist unter der jetzt gemachten Annahme der erste Theil des Satzes bewiesen.

Sind nun f und q nicht relative Primzahlen, so setze man

$$f = a^{\alpha}\, b^{\beta}\, c^{\gamma} \ldots\ldots e^{\varepsilon}\, g^{\varkappa}\, l^{\lambda}$$
$$q = a^{\mathfrak{a}}\, b^{\mathfrak{b}}\, c^{\mathfrak{c}} \ldots\ldots e^{\mathfrak{e}}\, g^{\mathfrak{g}}\, l^{\mathfrak{l}},$$

wo $a, b, c, \ldots e, g, l \ldots$ Primzahlen, und $\alpha, \beta, \gamma, \ldots \varepsilon, \varkappa, \lambda$, so wie $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots \mathfrak{e}, \mathfrak{g}, \mathfrak{l}$, ganze positive Zahlen oder 0 in der Art bedeuten, dass die Werthe $\alpha, \beta, \gamma \ldots$ einzeln verglichen nicht kleiner sind als die ihnen entsprechenden in $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}, \ldots$ und dass die Werthe $\mathfrak{e}, \mathfrak{g}, \mathfrak{l} \ldots$ einzeln verglichen nicht kleiner sind, als die ihnen entsprechenden in $\varepsilon, \varkappa, \lambda \ldots$ Setzt man nun

$$a^{\alpha}\, b^{\beta}\, c^{\gamma} \ldots = M,\ e^{\varepsilon}\, g^{\varkappa}\, l^{\lambda} \ldots n \text{ und}$$
$$a^{\mathfrak{a}}\, b^{\mathfrak{b}}\, c^{\mathfrak{c}} \ldots = m,\ e^{\mathfrak{e}}\, g^{\mathfrak{g}}\, l^{\mathfrak{l}} \ldots N,$$

so wird offenbar MN das kleinste gemeinschaftliche Vielfache von $f \,.\, q$ sein. Da nun $\phi\alpha$ zu Mn gehört, so muss $(\phi\alpha)^n$ zu M, und da $\psi\alpha$ zu mN gehört, so muss $(\psi\alpha)^m$ zu N gehören. Offenbar sind aber M und N relative Primzahlen und daher muss $(\phi\alpha)^n\,(\psi\alpha)^m$ nach dem Obigen zu MN oder zu dem kleinsten gemeinschaftlichen Vielfachen von f und q gehören, und es ist somit der erste Theil des Satzes allgemein bewiesen.

Setzt man nun, $\mu\alpha$ gehöre zu einem Vielfachen von f z. B. zu kf, so werden sämmtliche Potenzen von diesem Ausdrucke, deren Exponenten kleiner als kf sind, von einander verschieden sein. Da mithin auch die Ausdrücke $(\mu\alpha)^k, (\mu\alpha)^{2k}, \ldots\ldots (\mu\alpha)^{fk}$ sämmtlich verschieden sein müssen, und da alle diese Ausdrücke der Congruenz $x^f - 1 \equiv 0\ (mod\ p, \alpha)$ genügen, so bilden sie die sämmtlichen f Wurzeln derselben. Jeder Ausdruck, der nun ebenfalls dieser Congruenz genügt, also auch $\phi\alpha$, welches zu f gehört, muss irgend einer Potenz von $\mu\alpha$ congruent werden. Setzt man statt $\mu\alpha$ den Ausdruck $(\phi\alpha)^n(\psi\alpha)^m$ so folgt, da derselbe zu NM gehört, also zu einem Vielfachen der Zahlen f und q, zu welchen $\phi\alpha$ und $\psi\alpha$ gehören, dass er einer der Potenzen von $(\phi\alpha)^n$ $(\psi\alpha)^m$ nach dem Modul (p, α) congruent werden müsse. Und hiermit ist der zweite Theil des Satzes bewiesen.

§. 23.

Erklärung und Lehrsatz. Ist α die Wurzel eines Ausdrucks vom n^{ten} Grade, so sollen die Ausdrücke von α, oder die Reste nach dem Modul (p, α), welche zu $p^n - 1$ gehören, primitive Wurzeln der Congruenz $x^{p^n-1} - 1 \equiv 0\ (mod.\ p, \alpha)$ heissen.

Es giebt so viele primitive Wurzeln der Congruenz $x^{p^n-1} - 1 \equiv 1\ (mod.\ p, \alpha)$ als es Zahlen giebt, die kleiner als $p^n - 1$, und zu dieser Zahl relative Primzahlen sind.

Beweis. Zunächst ist zu zeigen, dass überhaupt primitive Wurzeln von der Congruenz $x^{p^n-1} - 1 \equiv 0\ (mod.\ p, \alpha)$ existiren. Nach §. 22. kann man stets einen Ausdruck zu Grunde legen, der in seinen verschiedenen Potenzen irgend zwei gegebene Ausdrücke erzeugt. Sollte nun unter den Potenzen dieses Restes nach dem Modul $(p.\ \alpha)$ noch irgend ein Rest nach demselben Modul nicht enthalten sein, so bilde man wieder (§. 22.) einen Rest, der in seinen verschiedenen Potenzen sowohl diesen Rest, als auch denjenigen erzeugt, in dessen verschiedenen Potenzen die ersten beiden Reste vorkommen, und es folgt, dass in den Potenzen des zuletzt gebildeten Restes die gewählten drei Reste enthalten sein werden. Durch ein fortgesetztes Verfahren derselben Art muss man natürlich zuletzt einen Rest bilden, der in seinen verschiedenen Potenzen sämmtliche $p^n - 1$ Reste nach dem Modul $(p.\alpha)$ erzeugt. Gesetzt nun $\phi\alpha$ sei ein solcher Rest und m eine relative Primzahl zu $p^n - 1$, so muss auch $(\phi\alpha)^m$ eine primitive Wurzel der Congruenz $x^{p^n-1} - 1 \equiv 0$ $(mod\ p,\alpha)$ sein. Wollte man nämlich annehmen $\phi\alpha^m$ gehöre zu x, so müsste $\phi\alpha^{mx} \equiv 1$ $(mod.\ p.\alpha)$ sein, und es müsste mx ein Vielfaches von $p^n - 1$ sein, da aber m relative Primzahl zu $p^n - 1$, so muss x das kleinste Vielfache von $p^n - 1$ d. i. $p^n - 1$ selbst sein. — Es wird mithin so viele primitive Wurzeln der Congruenz $x^{p^n-1} - 1 \equiv 0\,(mod.\ p)$ geben, als es relative Primzahlen zu $p^n - 1$ giebt, die kleiner sind als diese Zahl, 1 mit eingerechnet. — Lässt man die Exponenten über $p^n - 1$ hinaus wachsen, so werden die hervorgehenden Potenzen von $\phi\alpha$ denjenigen Potenzen dieses Restes congruent sein, welche zu Exponenten gehören, die mit jenen nach dem Modul $p^n - 1$ congruent sind, oder $(\phi\alpha)^z$ wird $\equiv (\phi\alpha)^r$ $(mod.\ p.\ \alpha)$ sein, wenn r der kleinste Rest ist, den z durch $p^n - 1$ dividirt, lässt. Dies folgt leicht, wenn man für z eine Zahl von der Form $(p^n-1)\ q + r$ setzt, wo q den Quotienten angiebt, den x durch $p^n - 1$ dividirt, giebt, und r den Rest.

Zusatz. Bezeichnet $r\alpha$ eine primitive Wurzel der Congruenz $x^{p^n-1} - 1 \equiv 0$ $(mod.\ p)$, so folgt aus (§. 20. *No.* 9. *Zus.*), dass $x^{p^n-1} - 1 \equiv (x - r\alpha)(x - r\alpha^2)(x - r\alpha^3) \ldots\ldots (x - r\alpha^{p^n-1})$ $(mod.\ p)$ sei.

§. 24.

Lehrsatz. Ist die Norm eines einfachen Ausdrucks von x in Bezug auf einen zweiten einfachen Ausdruck congruent 0 $(mod.\ p,\alpha)$, so ist auch die Norm des zweiten in Bezug auf den ersten congruent 0 $(mod.\ p,\alpha)$.

Beweis. Nennt man die einfachen Ausdrücke, um die es sich handelt, Fx und ϕx, so folgt zunächst, dass NF_ϕ und $N\phi_F$ Ausdrücke der Coefficienten von Fx und von ϕx sein werden. Da diese Coefficienten selbst aber Ausdrücke von α sind, so folgt, dass NF_ϕ und $N\phi_F$ blos Ausdrücke von α sein werden. Da nun aber (§. 7. Einl.) $\pm NF_\phi = N\phi_F$ ist, so folgt, dass $N\phi_F$ und NF_ϕ stets zugleich $\equiv 0$ $(mod\ p,\alpha)$ werden.

§. 25.

Lehrsatz. Die Norm eines Ausdrucks von x in Bezug auf einen zweiten Ausdruck der dem Product mehrerer Ausdrücke congruent ist, ist dem Product der Normen des ersten Ausdruckes in Bezug auf sämmtliche Factoren des zweiten nach dem Modul p,α congruent.

Beweis wie in §. 9.

§. 26.

Lehrsatz. **Die Norm eines irreductibeln einfachen Ausdruckes von x nach dem Modul (p, α) kann in Bezug auf einen zweiten Ausdruck von x, von geringerem Grade nicht congruent 0 $(mod.\, p, \alpha)$ werden.**

Beweis wie in §. 10.

§. 27.

Lehrsatz. **Ist Fx ein irreductibeler Ausdruck und ϕx ein einfacher Ausdruck nach dem Modul (p, α), so ist Fx ein Divisor von ϕx in Bezug auf den Modul p, α, wenn $NF_\phi \equiv 0$ $(mod.\, p, \alpha)$ ist.**

Beweis wie in §. 11.

§. 28.

Lehrsatz. **Jeder zu dem Modul (p, α) gehörige Ausdruck von x, dessen Wurzeln in eine bestimmte Potenz eines irreductibeln Ausdrucks eingesetzt, dieselbe, wenn man sie mit einem gewissen Rest des Modul (p, α), der nicht $\equiv 0$ $(mod.\, p, \alpha)$ ist, multiplicirt, einem bestimmten p fachen Ausdruck der jedesmaligen Wurzel gleich machen, ist selbst eine Potenz jenes irreductibelen Ausdrucks nach dem Modul (p, α).**

Beweis wie in §. 7.

§. 29.

Lehrsatz. **Entwickelt man die Gleichung für einen Ausdruck der Wurzel eines in Bezug auf den Modul (p, α) einfachen irreductibelen Ausdruckes, und bezeichnet dieselbe durch $Gz = 0$, so ist Gz in Bezug auf den Modul (p, α) entweder irreductibel oder die Potenz eines irreductibelen Ausdruckes.**

Beweis wie in §. 12.

Zusatz. **Ist der Grad des einfachen irreductibeln Ausdrucks von x grösser als der Grad des Ausdrucks seiner Wurzel, so kann Gz nicht $\equiv (Z - B_1)^m$ $(mod.\, p, \alpha)$ werden, wenn B_1 einen Rest nach dem Modul (p, α) und m den Grad des irreductibeln Ausdrucks von x bedeutet.**

§. 30.

Lehrsatz. **Ist ϕx in Bezug auf den Modul (p, α) von einem höhern Grade als dem 0^{ten} und einem niedrigeren Grade als dem m^{ten}, so kann nicht $(\phi x)^{p^n} \equiv \phi x + Fx \,.\, Qx$ $(mod.\, p, \alpha)$ sein, wenn n den Grad des irreductibeln Ausdrucks anzeigt, von dem α eine Wurzel, und Fx nach dem Modul (p, α) irreductibel und vom m^{ten} Grade ist, ferner Qx irgend einen Ausdruck nach dem Modul (p, α) bedeutet.**

Beweis. Existirte obige Congruenz, so könnte man dieselbe auch so schreiben $\phi x \{ \phi x^{p^n - 1} - 1 \} \equiv Fx \,.\, Qx$ $(mod.\, p, \alpha)$, bedeutet aber $r\alpha$ eine pri-primitive Wurzel der Congruenz $x^{p^n-1} - 1 \equiv 0$ $(mod.\, p, \alpha)$, so hat man (§. 23. *Zus.*) $x^{p^n-1} - 1 \equiv (x - r\alpha)(x - (r\alpha)^2) \ldots\ldots (x - (r\alpha)^{p^n-1})$ $(mod.\, p, \alpha)$, und hieraus folgt $(\phi x)^{p^n-1} - 1 \equiv (\phi x - (r\alpha))(\phi x - (r\alpha)^2) \ldots\ldots (\phi x - (r\alpha)^{p^n-1})$ $(mod.\, p, \alpha)$. Sollte nun obige Congruenz bestehen, so müsste Fx in Bezug auf den Modul (p, α) ein Theiler einer der Ausdrücke ϕx, $\phi x - (r\alpha)$, ... $\phi x - (r\alpha)^{p^m-1}$ sein (§. 20. *No.* 10.). Da aber jeder dieser Ausdrücke von einem niedrigeren Grade als dem m^{ten} ist, so geht dies nicht an.

§. 31.

Erklärungen und Lehrsätze. Bedeutet $Fx \equiv 0$ *(mod. p. α)* eine einfache irreductibele Congruenz, und β eine Wurzel der Gleichung $Fx = 0$, so sollen zwei Ausdrücke von β, deren Coefficienten Ausdrücke von α sind, nach dem Modul (p, α, β) congruent heissen, wenn sich der eine von ihnen als Summe des andern und eines $p$fachen Ausdruckes von β, dessen Coefficienten ebenfalls Ausdrücke von α sind, darstellen lässt.

1) Hat man also $\phi\beta = \psi\beta + pR\beta$, wo $\phi\beta$, $\psi\beta$, $R\beta$ ganze rationale Functionen von β bedeuten, in welchen die Coefficienten Ausdrücke von α sind, so ist $\phi\beta$ congruent $\psi\beta$ in Bezug auf den Modul $(p, \alpha, \beta,)$ und es wird geschrieben werden $\phi\beta \equiv \psi\beta$ *(mod. p, α, β)*.

2) Ist $\phi\beta \equiv \psi\beta$ *(mod. p, α, β)*, so ist Fx in Bezug auf den Modul (p, α) ein Theiler von $\phi x - \psi x$.

Beweis. Da Fx nach dem Modul (p, α) irreductibel ist, so lässt es sich in algebraischer Beziehung gewiss nicht in zwei Factoren zerfällen, die ganze rationale Functionen von x und deren Coefficienten Ausdrücke von α sind. Hieraus folgt nun ähnlich wie (§. 5. Einl.), dass Fx mit einem Ausdrucke von x, dessen Coefficienten Ausdrücke von α sind, nur dann eine Wurzel gemeinschaftlich haben könne, wenn es algebraischer Divisor des Ausdruckes ist, da nun aber $Fx = 0$, und $\phi x - \psi x - pRx = 0$ die Wurzel β gemeinschaftlich haben, so muss Fx ein Factor von $\phi x - \psi x - pRx$ und mithin in Bezug auf den Modul (p, α) ein Factor von $\phi x - \psi x$ sein.

3) Wenn das Product zweier Ausdrücke von β congruent 0 nach dem Modul (p, α, β) ist, so ist einer von jenen Ausdrücken selbst nach diesem Modul congruent 0.

Beweis wie in §. 14. *No.* 5.

4) Eine Function von x, deren Coefficienten Ausdrücke von β nach dem Modul (p, α, β) sind, soll ein Ausdruck von x nach dem Modul (p, α, β) heissen. Zwei solche Ausdrücke werden einander congruent gesetzt nach dem Modul (p, α, β), wenn die Coefficienten der entsprechenden Potenzen von x in beiden nach diesem Modul congruent sind.

Zusatz. Nach dieser jetzt eingeführten Bezeichnung kann man den Inhalt des §. 30. folgendermassen aussprechen: Wenn β die Wurzel eines irreductibeln Ausdrucks vom m^{ten} Grade nach dem Modul (p, α) ist, und $\phi\beta$ bezeichnet irgend einen Ausdruck von β, dessen Coefficienten Ausdrücke von α sind, und dessen Grad in Bezug auf den Modul (p, α, β) kleiner als m und grösser als 0 ist, so kann nicht sein $(\phi\beta)^{p^n} \equiv \phi\beta$ *(mod. p, α, β)*.

§. 32.

Bedeutet Gx einen Ausdruck von x nach dem Modul (p, α, β), und denkt man sich die Coefficienten dieses Ausdrucks durch Division mit $F\beta$ auf ihre Reste reducirt, (weil die Vielfachen von $F\beta$ mit diesem Ausdrucke selbst verschwinden) mithin auf lauter Ausdrücke von geringerem Grade als Fx, und diese Ausdrücke reduciren sich nicht sämmtlich auf Ausdrücke von α, indem die verschiedenen Potenzen von β nur in solche Ausdrücke von α multiplicirt sind, die nach dem Modul (p, α) congruent 0 zu setzen sind, so kann auch der Ausdruck von x, dessen Wurzeln die $(p^n)^{ten}$ Potenzen der Wurzeln von Gx sind, nicht mit Gx nach dem Modul (p, α, β) übereinstimmen. Setzt man nämlich $Gz = \phi_0 \,.\, x^k + \phi_1 x^{k-1} + \ldots\ldots \phi_k$, wo $\phi_0, \phi_1, \ldots\ldots \phi_k$ Ausdrücke nach dem Modul (p, α, β) bezeichnen, so folgt (§. 13. *No.* 2.), dass der Ausdruck von x, dessen Wurzeln die $(p^n)^{ten}$ Potenzen der Wurzeln von Gx sind, nach dem Modul (p, α, β) congruent $\phi_0^{p^n} \,.\, x^k + \phi_1^{p^n} x^{k-1} + \ldots + \phi_k^{p^n}$ sein werde. Da nun aber diejenigen unter den Coefficienten von Gx, die sich nicht auf reine Ausdrücke von α reduciren, nicht mit ihren $(p^n)^{ten}$ Potenzen nach dem Modul (p, α, β) congruent sein können (§. 31.), so kann auch Gx nicht mit dem Ausdrucke congruent nach dem Modul (p, α, β) sein, dessen Wurzeln die $(p^n)^{ten}$ Potenzen seiner Wurzeln sind.

§. 33.

Lehrsatz. Es kann nicht sein $\beta^{p^{k \cdot n}} \equiv \beta \; (mod.\, p, \alpha, \beta)$, wenn k eine ganze Zahl bedeutet, die kleiner als der Grad des Ausdrucks Fx ist, von welchem β eine Wurzel ist.

Beweis. Wäre $\beta^{p^{k \cdot n}} \equiv \beta \; (mod.\, p, \alpha, \beta)$, so hätte man euch $(x-\beta)(x-\beta^{p^n})(x-\beta^{p^{2n}}) \ldots\ldots (x-\beta^{p^{k-1 \cdot n}}) \equiv (x-\beta^{p^n})(x-\beta^{p^{2n}}) \ldots\ldots (x-\beta^{p^{k-1 \cdot n}})(x-\beta^{p^{kn}}) \; (mod.\, p, \alpha, \beta)$. Da der zweite Ausdruck die $(p^n)^{ten}$ Potenzen des ersten enthält, so müsste (§. 32.) die Coefficienten von $(x-\beta)(x-\beta^{p^n}) \ldots\ldots (x-\beta^{p^{k-1 \cdot n}})$ sich auf reine Ausdrücke von α reduciren. Im Uebrigen folgt nun der Beweis wie im (§. 17.).

§. 34.

Lehrsatz. Ist $Fx \equiv 0 \; (mod.\, p, \alpha)$ eine einfache irreductibele Congruenz vom Grade m, deren Coefficienten im Allgemeinen zum Modul (p, α) gehören, und β eine Wurzel von Fx, so ist stets

$$Fx \equiv (x-\beta)(x-\beta^{p^n})(x-\beta^{p^{2 \cdot n}}) \ldots\ldots (x-\beta^{p^{m-1 \cdot n}}) \; (mod.\, p, \alpha, \beta)$$

und $\beta^{p^{m \cdot n}-1} \equiv 1 \; (mod.\, p, \alpha, \beta)$.

Beweis. Da die Coefficienten von Fx Ausdrücke von α sind, so sollen sie mit $\phi_1 \alpha, \phi_2 \alpha, \ldots \phi^m \alpha$ bezeichnet werden. Es is mithin $Fx = x^m + \phi_1 \alpha \,.\, x^{m-1} + \phi_2 \alpha \,.\, x^{m-2} + \ldots\ldots \phi^m \alpha$. Aus (§. 13. *No.*) folgt nun, dass derjenige Ausdruck, welcher die $p^{n \cdot k}$ Potenzen der Wurzeln von Fx enthält, wo k irgend eine ganze Zahl bedeutet, nach dem Modul $(p\ \alpha)$ congruent $x^m + (\phi_1 \alpha)^{p^{k \cdot n}} x^{m-1} + (\phi_2 \alpha)^{p^{k \cdot n}} x^{m-2} + \ldots\ldots + (\phi_m \alpha)^{p^{k \cdot n}}$ und daher aus (§. 19.), dass dieser Ausdruck nach demselben Modul congruent $x^m + \phi_1 \alpha \,.\, x^{m-1} + \phi_2 \alpha \,.\, x^{m-2} + \ldots\ldots + \phi^m \alpha$ sein werde. Hieraus folgt nun $F(\beta^{p^{kn}}) \equiv 1 \; (mod.\, p, \alpha, \beta)$. Im Uebrigen wird der Beweis mit Hinzuziehung der (§. 31. §. 33.) ganz ähnlich wie in §. 18. geführt.

Zusatz. Ist $fx \equiv 0 \; (mod.\, p, \alpha)$ eine einfache irreductibele Congruenz vom Grade n, in welcher aber die Coefficienten ebenfalls Ausdrücke von α sind, aber ganzen reellen Zahlen nach dem Modul (p, α) congruent gesetzt werden können, so ist

$fx \equiv (x-\alpha)(x-\alpha^p) \ldots\ldots (x-\alpha^{p^{n-1}}) (mod.\, p, \alpha)$ und $\alpha^{p^n-1} - 1 \equiv 0 \; (mod.\, p, \alpha)$.

Den

Der Beweis kann durchaus wie in §. 18. geführt werden, welches darauf beruht, dass die Sätze, welche sich auf reelle ganze Zahlen als Coefficienten nach dem Modul p beziehen, natürlich auch unmittelbar für den Modul (p, α) gelten.

§. 35.

Die Sätze über die Moduln von der Form Modul (p, α, β) hätten noch vollständiger aufgezählt und auch noch auf zusammengesetztere Moduln hinübergeführt werden können, doch scheint es, dass der Gang wie die Resultate solcher Untersuchung klar genug vorlägen, so dass man sich der weitern Ausführung überheben kann.

Wir wenden uns daher zu dem Theile der Untersuchung, welcher sich mit dem Beweise der Existenz irreductibeler Congruenzen jeden Grades nach dem Modul p, und mit der Anzahl solcher Congruenzen beschäftigt.

§. 36.

Lehrsatz. Ist $fx \equiv 0$ $(mod.\, p)$ eine irreductibele einfache Congruenz vom n^{ten} Grade, so wird der Ausdruck, welcher die $(p^n - 1)^{ten}$ Potenzen der Wurzeln von fx enthält nach dem Modul p congruent $(x-1)^n$. Setzt man ferner n_1 sei eine ganze Zahl und kleiner als n, und den Ausdruck, welcher die $(p^{n_1} - 1)^{ten}$ Potenzen der Wurzeln von fx enthält gleich dx, so kann nicht $d(1)$ congruent 0 nach dem Modul p sein.

Beweis. Bezeichnet α irgend eine Wurzel von fx, so folgt aus §. 18., dass man stets für jede dieser Wurzeln werde eine Gleichuug von der Form $\alpha^{p^n-1} = 1 + pR\alpha$, wo $R\alpha$ einen bestimmten Ausdruck von α bezeichnet, aufstellen können. Bezeichnet man nun die übrigen Wurzeln von fx mit α_1, α_2, $\ldots\, \alpha_{n-1}$, so folgt $(x - \alpha^{p^n-1})(x - \alpha_1^{p^n-1}) \ldots (x - \alpha_{n-1}^{p^n-1}) = (x - 1 - pR\alpha)$ $(x - 1 - pR\alpha_1) \ldots . (x - 1 - pR\alpha_{n-1})$. Dieser letzte Ausdruck ist aber offenbar $\equiv (x-1)^n$ $(mod.\, p, \alpha)$, wodurch der erste Theil des Satzes bewiesen ist.

Wollte man nun annehmen $d(1)$ wäre $\equiv 0$ $(mod.\, p)$, so müsste dx in Bezug auf den Modul p den Divisor $x - 1$ haben. Da nun (§. 12.) dx die Potenz eines irreductibelen Ausdruckes sein muss, so würde folgen $dx \equiv (x-1)^n$ $(mod.\, p)$. Es ist aber $dx = (x - \alpha^{p^{n_1}-1})\, D(x, \alpha)$, wo $D(x, \alpha)$ den Quotienten angiebt, den man erhält, wenn man dx durch $x - \alpha^{p^{n_1}-1}$ dividirt, und dessen Coefficienten mithin Ausdrücke von α sind. Man erhält mithin $(x-1)^n \equiv (x - \alpha^{p^{n_1}-1})\, D(x, \alpha)$ $(mod.\, p, \alpha)$. Hiernach müsste aber offenbar $x - 1 \equiv x - \alpha^{p^{n_1}-1}$ $(mod.\, p, \alpha)$ und $1 \equiv \alpha^{p^{n_1}-1}$ $(mod.\, p, \alpha)$ sein, welches aber (§. 17.) nicht angeht, weil $n_1 < n$ ist.

Zusatz. Enthält irgend ein Ausdruck in Bezug auf den Modul p, einen irreductibelen Divisor vom Grade m. und bezeichnet man den Ausdruck, welcher die $(p^m - 1)^{ten}$ Potenzen der Wurzeln jenes Ausdruckes zu seinen Wurzeln enthält mit dx, so wird dx offenbar den Factor $(x-1)^m$ in Bezug auf den Modul p enthalten, und demnach muss dann $d(1) \equiv 1$ $(mod.\, p)$ sein. Wird nun aber $d(1)$ nicht früher $\equiv 0$ $(mod.\, p)$ als indem $n_1 = n$ ist, so ist nothwendig der in Betracht gezogene Ausdruck irreductibel. Oder man erhält folgenden Lehrsatz:

§. 37.

Lehrsatz. Ist der Ausdruck fx von der Beschaffenheit, dass diejenigen Ausdrücke von x, deren Wurzeln die $(p^{n_1}-1)^{ten}$ Potenzen der Wurzeln von fx sind, nicht nach dem Modul p congruent 0 werden, wenn man in ihnen statt x, 1 setzt, so lange $n_1 < n$ ist, so ist fx in Bezug auf den Modul p irreductibel.

§. 38.

Lehrsatz. Ist Fx ein einfacher irreductibeler Ausdruck nach dem Modul (p, α) vom Grade m, und ist α die Wurzel eines irreductibelen Ausdrucks vom Grade n nach dem Modul p, so ist der Ausdruck, dessen Wurzeln die $(p^{mn}-1)^{ten}$ Potenzen der Wurzeln von Fx sind, congruent $(x-1)^m$ $(mod.\, p, \alpha)$.

Der Beweis folgt ähnlich wie im (§. 36.), doch hier mit Hinzuziehung des (§. 34.) statt des (§. 18.). Auf ähnlichem Wege wie vorher folgt nun auch der folgende Lehrsatz.

§. 39.

Lehrsatz. Ist der Ausdruck Fx von der Beschaffenheit, dass diejenigen Ausdrücke von x, die $(p^{m_1 n}-1)^{ten}$ Potenzen der Wurzeln von Fx sind, nicht nach dem Modul (p, α) congruent 0 werden, wenn man in ihnen statt x, 1 setzt, so lange $m_1 < m$ oder als der Grad von Fx ist, so muss Fx in Bezug auf den Modul (p, α) irreductibel sein.

§. 40.

Lehrsatz. Ist m ein Theiler von $p-1$ und g eine primitive Wurzel der Congruenz $x^{p-1}-1 \equiv 0$ $(mod.\, p)$, ferner k relative Primzahl zu m, so ist $x^m - g^k \equiv 0$ $(mod.\, p)$ eine irreductibele Congruenz.

Beweis. Da m ein Theiler von $p-1$ ist, so wird die Congruenz $x^m - 1 \equiv 0$ $(mod.\, p)$ m reelle Wurzeln haben, nennt man diese $\gamma_1, \gamma_2, \dots \gamma_m$, so wird der Ausdruck, dessen Wurzeln die $(p^q-1)^{ten}$ Potenzen der Wurzeln von $x^m - g^k$ sind, nach dem Modul p dem folgenden Ausdruck congruent sein:

$$\left(x-\left(\gamma_1 \sqrt[m]{g^k}\right)^{p^q-1}\right)\left(x-\left(\gamma_2 \sqrt[m]{g^k}\right)^{p^q-1}\right) \dots\dots \left(x-\left(\gamma_m \sqrt[m]{g^k}\right)^{p^q-1}\right).$$

Da aber offenbar jeder Werth von γ zur $(p^q-1)^{ten}$ Potenz erhoben $\equiv 1$ $(mod.\, p)$, so wird der Ausdruck die einfachere Gestalt annehmen $\left(x-g^{k\left(\frac{p^q-1}{m}\right)}\right)^m$, sollte dieser nun für $x=1$ congruent 0 $(mod.\, p)$ werden, so müsste $g^{k\left(\frac{p^q-1}{m}\right)} \equiv 1$ $(mod.\, p)$ sein. Es ist aber $k\left(\frac{p^q-1}{m}\right) = k.\left(\frac{p-1}{m}\right)\{p^{q-1}+p^{q-2}+\dots+1\}$ und da $p \equiv 1$ $(mod.\, p-1)$ ist, so ist $k\,\frac{p-1}{m}(p^{q-1}+p^{q-1}+\dots+1)$

$\equiv k\frac{p-1}{m} \cdot q$ (*mod.* $p-1$). Da aber k relative Primzahl zu m ist, so kann $k \cdot \frac{p-1}{m} \cdot q$ nur dann $\equiv 0$ (*mod.* $p-1$) werden, wenn q den Factor m enthält. So lange also q einen kleinern Werth als m hat, kann $g^{k\left(\frac{p^q-1}{m}\right)}$ nicht $\equiv 1$ (*mod.* p), und mithin der Ausdruck, dessen Wurzeln die $(p^q-1)^{ten}$ Potenzen der Wurzeln von $x^m - g^k$ sind, nicht, wenn man in ihm $x = 1$ setzt $\equiv 0$ (*mod.* p) werden. Demnach ist nun (§. 37.) $x^m - g^k$ nach dem Modul p irreductibel.

§. 41.

Lehrsatz. Ist $r\alpha$ eine primitive Wurzel der Congruenz $x^{p^n-1} - 1 \equiv 0$ (*mod.* p, α) und m ein Theiler von $p^n - 1$, ferner k relative Primzahl zu q, so ist $x^m - (r\alpha)^k$ ein irreductibeler Ausdruck nach dem Modul (p, α).

Beweis. Da m ein Theiler von $p^n - 1$ ist, so wird die Congruenz $x^m - 1$ (*mod.* p, α) m Reste nach dem Modul $(p. \alpha)$ zu Wurzeln haben. Nennt man diese $\gamma_1, \gamma_2, \ldots \gamma_m$, so wird der Ausdruck, welchen die $(p^{nq}-1)^{ten}$ Potenzen der Wurzeln von $x^m - (r\alpha)^k$ als Wurzeln enthält, nach dem Modul (p, α) congruent

$$\left(x-\left(\gamma_1 \sqrt[m]{r\alpha^k}\right)^{p^{nq}-1}\right)\left(x-\left(\gamma_2 \sqrt[m]{r\alpha^k}\right)^{p^{nq}-1}\right) \;\ldots\ldots\; \left(x-\left(\gamma_m \sqrt[m]{r\alpha^k}\right)^{p^{nq}-1}\right)$$

werden. Da aber $p^{nq} - 1$ den Factor $p^n - 1$ enthält, so wird jeder Werth von γ zur $(p^{nq}-1)^{ten}$ Potenz congruent 1 (*mod.* p, α) werden. Der Ausdruck geht also in den einfacheren $\left(x-(r\alpha)^{k \cdot \frac{p^{nq}-1}{m}}\right)^m$ über. Sollte dieser Ausdruck nach dem Modul (p, α) congruent 0 werden, wenn $x = 1$ ist, so müsste $(r\alpha)^{k \cdot \frac{p^{nq}-1}{m}} \equiv 1$ (*mod.* p, α) werden. Dies kann aber nur geschehen, wenn $k \cdot \frac{p^{nq}-1}{m}$ ein Vielfaches von $p^n - 1$ ist. Es ist aber $k \cdot \frac{p^{nq}-1}{m} = k\frac{p^n-1}{m}\{p^{n(q-1)} + p^{n(q-2)} + \ldots + 1\}$, nnd da $p^n \equiv 1$ (*mod.* p^n-1) ist, so ist

$$k\frac{p^n-1}{m}(p^{n(q-1)} + p^{n(q-2)} + \ldots + 1) \equiv k \cdot \frac{p^n-1}{m} \cdot q \;(mod.\, p^n-1).$$

Dieser Ausdruck kann aber, da k zu m relative Primzahl ist, nur dann congrueut 0 (*mod.* p^n-1) werden, wenn q den Factor m enthält. So lange also q einen kleinern Werth als m hat, kann der Ausdruck, dessen Wurzeln die $(p^{qn}-1)^{ten}$ Potenzen der Wurzeln von $x^m - (r\alpha)^k$ enthält, nicht für $x = 1$ nach dem Modul (p, α) congruent 0 werden, und mithin ist $x^m - (r\alpha)^k$ nach dem Modul (p, α) irreductibel (§. 39.).

§. 42.

Lehrsatz. Bedeutet $F(x, \alpha)$ irgend einen irreductibelen Ausdruck vom m^{ten} Grade nach dem Modul (p, α), in welchem der Coefficient irgend einer Potenz von x, der Congruenz $x^{p^{n_1}-1} - 1 \equiv 0$ (*mod.* p, α) nur genügt, wenn n_1 dem n oder einem Vielfachen dieser Zahl gleich wird, so ist $F(x, \alpha) \,.\, F(x, \alpha^{p}) \,.\, F(x, \alpha^{p^2})$ $\ldots\, F(x, \alpha^{p^{n-1}})$ ein Ausdruck, dessen Coefficienten nach dem Modul (p, α) ganzen reellen Zahlen congruent zu setzen ist, und der, wenn dies geschehen, nach dem Modul p ein irreductibeler Ausdruck vom $(m.n)^{ten}$ Grade ist.

Beweis. Ist α eine Wurzel von $fx = 0$ $(mod. p)$, so ist $fx \equiv (x-\alpha)$ $(x-\alpha^{p}) \ldots (x-\alpha^{p^{n-1}})$ $(mod.\ p, \alpha)$ (§. 18.). Nennt man nun die Wurzeln von fx, $\alpha, \alpha_1, \alpha_2, \ldots \alpha_{n-1}$, so folgt, dass $(x-\alpha)(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_{n-1})$ $\equiv (x-\alpha)(x-\alpha^{p})(x-\alpha^{p^{n-1}})$ $(mod.\ p, \alpha)$. Da sich aber jede symmetrische Function von $\alpha, \alpha^{p}, \alpha^{p^2}, \ldots \alpha^{p^{n-1}}$ als ganze in ganzen Zahlen ausgedrückte Function der Coefficienten von $(x-\alpha)(x-\alpha^{p})\ldots\ldots(x-\alpha^{p^{n-1}})$ ansehen lässt (§. 2 Einl.), und da diese Coefficienten selbst ganzen reellen Zahlen, nämlich den Coefficienten von fx nach dem Modul (p, α) congruent zu setzen sind, so folgt, dass überhaupt alle symmetrischen Functionen von $\alpha, \alpha^{p}, \alpha^{p^2}, \ldots \alpha^{p^{n-1}}$ nach dem Modul (p, α) reellen ganzen Zahlen congruent zu setzen sind. Offenbar sind aber die Coefficienten von $F(x, \alpha) F(x, \alpha^{p}) F(x, \alpha^{p^2}) \ldots F(x, \alpha^{p^{n-1}})$ symmetrische Functionen von $\alpha, \alpha^{p}, \alpha^{p^2}, \ldots \alpha^{p^{n-1}}$ und mithin nach dem Modul (p, α) ganzen reellen Zahlen congruent zu setzen.

Es soll nun zunächst gezeigt werden, dass sämmtliche Ausdrücke $F(x, \alpha)$, $F(x, \alpha^{p})$, $\ldots F(x, \alpha^{p^{n-1}})$ verschiedene irreductibele Ausdrücke nach dem Modul (p, α) sind. Verschieden sind aber zwei solche Ausdrücke schon, wenn in ihnen zwei entsprechende Coefficienten nach dem Modul (p, α) nicht congruent sind. Da $F(x, \alpha)$ mindestens einen Coefficienten enthalten soll, welcher der Congruenz $x^{p^{n_1}-2} - 1 \equiv 0$ $(mod.\ p, \alpha)$ nur genügt, wenn n_1 gleich n oder einem Vielfachen dieser Zahl gleich wird, so mag ein solcher durch $\phi\alpha$ bezeichnet werden. Nun werden aber die dem $\phi\alpha$ entsprechenden Coefficienten in $F(x, \alpha^{p})$, $F(x, \alpha^{p^2}) \ldots F(x, \alpha^{p^{n-1}})$ nach dem Modul (p, α) congruent $(\phi\alpha)^{p}$, $(\phi\alpha)^{p^2}, \ldots (\phi\alpha)^{p^{n-1}}$ sein. Da aber diese Ausdrücke (§. 17.) nach dem Modul (p, α) verschieden sind, so sind auch sämmmtliche Ausdrücke $F(x, \alpha)$, $F(x, \alpha^{p})$, $\ldots F(x, \alpha^{p^{n-1}})$ nach diesem Modul verschieden. Wäre nun einer dieser Ausdrücke $F(x, \alpha^{p^k})$, wo k eine der Zahlen $2, 3, \ldots n-1$ bedeutet, nicht nach dem Modul (p, α) irreductibel, se setze man $F(x, \alpha^{p^k}) \equiv \psi(x, \alpha)$ $\psi_1(x, \alpha)$ $(mod.\ p, \alpha)$, wo $\psi(x, \alpha)$ und $\psi_1(x, \alpha)$ Ausdrücke von x nach dem Modul (p, α) bedeuten. Setzt man nun in diese Congruenz statt α, den Ausdruck $\alpha^{p^{n-k}}$, so muss sie in eine andere aber in sich richtige Congruenz übergehen,*) man erhält mithin $F(x, \alpha^{p^n}) \equiv \psi(x, \alpha^{p^{n-k}}) \psi_1(x, \alpha^{p^{n-k}})$ $(mod.\ p, \alpha)$, und

---

*) Anmerkung. Hat man nämlich zwei Ausdrücke von α, die nach dem Modul (p, α) congruent sind, so bleiben sie congruent wenn man in ihnen statt α eine (p^m)te Potenz von α setzt, wo m irgend eine ganze Zahl bedeutet, oder wenn $\phi\alpha \equiv \psi\alpha$ $(mod.\ p, \alpha)$ ist, so ist auch $\phi(\alpha^{p^m}) \equiv \psi(\alpha^{p^m})$ $(mod.\ p, \alpha)$. Es ist nämlich im §. 19. erwiesen worden, dass $(\phi\alpha)^{p^m} \equiv \phi(\alpha^{p^m})$ $(mod.\ p, \alpha)$ ist, und da aus obiger Congruenz offenbar $(\phi\alpha)^{p^m} \equiv (\psi\alpha)^{p^m}$ $(mod.\ p, \alpha)$ folgt, so muss auch $\phi(\alpha^{p^m}) \equiv \psi(\alpha^{p^m})$ sein. Bedeuten nun $A(x, \alpha)$ und $B(x, \alpha)$ zwei nach dem Modul (p, α) congruente Ausdrücke von x, so muss auch $A(x, \alpha^{p^m}) \equiv B(x, \alpha^{p^m})$ $(mod.\ p, \alpha)$ sein, weil sich die Coefficienten beider Ausdrücke nur darin geändert haben, dass in ihnen

mithin da $\alpha^{p^n} \equiv \alpha$ (*mod.* p, α), und daher auch $F(x, \alpha^{p^n}) \equiv F(x, \alpha)$ (*mod.* p, α) ist, $F(x, \alpha) \equiv \psi(x, \alpha^{p^{n-k}}) \cdot \psi_1(x, \alpha^{p^{n-k}})$ (*mod.* p, α), welches gegen die vorausgesetzte Irreductibilität von $F(x, \alpha)$ streitet. Es ist mithin auch $F(x, \alpha^{p^k})$ irreductibel. Wollte man nun voraussetzen $F(x, \alpha)\, F(x, \alpha^p) \,\ldots\, F(x, \alpha^{p^{n-1}})$ wäre nach dem Modul p nicht irreductibel, so setze man

$$F(x, \alpha)\; F(x, \alpha^p) \;\ldots\; F(x, \alpha^{p^{n-1}}) \equiv \psi x\, \psi_1 x \ (mod.\, p, \alpha),$$

wo ψx und $\psi_1 x$ zwei Ausdrücke von x anzeigen, in deren Coefficienten α nicht eintritt. Da nun die linke Seite dieser Congruenz nur aus irreductibelen Ausdrücken besteht, so ist es nothwendig, dass das Product einer gewissen Anzahl dieser Ausdrücke dem ψx nach dem Modul (p, α) congruent werde. Es sei nun $\psi x = a_0 x^s + a_1 x^{s-1} + \ldots\ldots + a_s$, wo $a_0, a_1 \ldots a_s$ ganze Zahlen bedeuten, und jene Factoren seien $F(x, \alpha^{p^\mu})$, $F(x, \alpha^{p^{\mu+\nu}})$, $F(x, \alpha^{p^{\mu+\nu+\rho}})$, so hätte man $F(x, \alpha^{p^\mu})\, F(x, \alpha^{p^{\mu+\nu}})\, F(x, \alpha^{p^{\mu+\nu+\rho}}) \ldots \equiv a_0 x^s + a_1 x^{s-1} + \ldots a_s$ (*mod.* p, α). In der Entwickelung des Products kann man sämmtliche Coefficienten als Ausdrücke von α^{p^μ} ansehen, bezeichnet man sie nach der Reihe mit $\phi_0(\alpha^{p^\mu})\ \phi_1(\alpha^{p^\mu}), \ldots\ \phi_s(\alpha^{p^\mu})$, so hätte man folgende Congruenzen

$$a_0 - \phi_0(\alpha^{p^\mu}) \equiv 0\ (mod.\, p, \alpha)\quad a_1 - \phi_1(\alpha^{p^\mu}) \equiv 0\ (mod.\, p, \alpha), \ \ldots a_s - \phi_s(\alpha^{p^\mu}) \equiv 0$$

(*mod.* p, α). Es ist aber offenbar $a_0 - \phi_0(\alpha^{p^\mu}) \equiv (a_0 - \phi_0 \alpha)^{p^\mu}$ (*mod.* p, α) und daher auch $a_0 - \phi_0 \alpha \equiv 0$ (*mod.* p, α), und mithin $a_0 \equiv \phi_0 \alpha$ (*mod.* p, α), und auf gleiche Weise erhält man $a_1 \equiv \phi_1 \alpha$ (*mod.* p, α) . . . $a_s \equiv \phi_s \alpha$ (*mod.* p, α). Bedeutet nun k die kleinste Zahl, welche nicht in μ, $\mu + \nu$, $\mu + \nu + \rho$ etc. enthalten ist, so erhält man $(a_0)^{p^k} \equiv (\phi_0 \alpha)^{p^k}$ (*mod.* p, α) und daher $a_0 \equiv \phi_0(\alpha^{p^k})$ (*mod.* p, α) und auf gleiche Weise $a_1 \equiv \phi_1(\alpha^{p^k})$(*mod.* p, α) $\ldots a_s \equiv \phi_s(\alpha^{p^k})$ und daher auch aus der oben angenommenen Congruenz (Vergl. die Anmerkung) die folgende $F(x, \alpha^{p^k})\, F(x, \alpha^{p^{k+\nu}})\, F(x, \alpha^{p^{k+\nu+\rho}}) \ldots \equiv \phi_0(\alpha^{p^k})\, x^s + \phi_1(\alpha^{p^k})\, x^{s-1} + \ldots \phi_s \alpha^{p^k}$ (*mod.* p, α). Setzt man in den letzten Ausdruck die den Coefficienten congruenten Werthe $a_0, a_1, a_2, \ldots a_s$, so findet man die Congruenz

$$F(x, \alpha^{p^\mu})\; F(x, \alpha^{p^{\mu+\nu}})\; F(x, \alpha^{p^{\mu+\nu+\rho}}) \ldots \equiv F(x, \alpha^{p^k})\; F(x, \alpha^{p^{k+\nu}})\; F(x, \alpha^{p^{k+\nu+\rho}}) \ldots$$

(*mod.* p, α). Hiernach müsste aber $F(x, \alpha^{p^k})$ mit einem der Factoren $F(x, \alpha^{p^\mu})$

---

statt α, α^{p^m} geschrieben worden ist. Hierbei sind also die entsprechenden Coefficienten nach dem Modul (p, α) wieder congruent geworden, und es ist demnach eine neue richtige Congruenz oder $A(x, \alpha^{p^m}) \equiv B(x, \alpha^{p^m})$ (*mod.* p, α) hervorgegangen. Man kann auch umgekehrt schliessen, wenn $\phi(\alpha^{p^m}) \equiv \psi(\alpha^{p^m})$ (*mod* p, α) ist, so muss auch $\phi\alpha \equiv \psi\alpha$ (*mod.* p, α) sein. Da nämlich $\phi(\alpha^{p^m}) - \psi(\alpha^{p^m}) \equiv (\phi\alpha)^{p^m} - (\phi\alpha)^{p^m} \equiv (\phi\alpha - \psi\alpha)^{p^m}$ (*mod.* p, α) ist, und mithin $\phi\alpha - \psi\alpha$ mit $\phi(\alpha^{p^m}) - \psi(\alpha^{p^m})$ nach dem Modul (p, α) congruent 0 werden muss, so muss auch $\phi\alpha \equiv \psi\alpha$ (*mod* p, α) sein. Bedeutet nun m_1 irgend eine andere ganze Zahl, so muss daher auch nach dem Obigen $\phi(\alpha^{p^{m_1}}) \equiv \psi(\alpha^{p^{m_1}})$ (*mod.* p, α) sein, wenn $\phi(\alpha^{p^m}) \equiv \psi(\alpha^{p^m})$ (*mod.* p, α) ist. Auf ähnliche Weise wie oben folgt nun ferner, dass wenn $A(x, \alpha^{p^m}) \equiv B(x, \alpha^{p^m})$ (*mod.* p, α) ist, auch $A(x, \alpha^{p^{m_1}}) \equiv B(x, \alpha^{p^{m_1}})$ sein wird.

$F(x,\alpha^{p^{\mu+\nu}})$. $F(x,\alpha^{p^{\mu+\nu+\rho}})$ etc. congruent sein, da dies aber nach dem Vorhergehenden nicht möglich ist, so entsteht ein Widerspruch, der nur dadurch gehoben werden kann, dass der Ausdruck $F(x,\alpha)\ F(x,\alpha^p)\ F(x,\alpha^{p^2}) \ldots F(x,\alpha^{p^{n-1}})$ nach dem Modul p irreductibel wird.

§. 43.

Lehrsatz. Bedeutet $Gx \equiv 0$ (*mod. p*) eine irreductibele Congruenz vom $(m\,.\,n)^{ten}$ Grade, wo m und n ganze Zahlen bedeuten, und α eine Wurzel der Gleichung $Gx = 0$, ferner $r\alpha$ eine primitive Wurznl der Congruenz $x^{p^{mn}} - 1 \equiv 0$ (*mod. p, α*), und setzt man $(r\alpha)^{\frac{p^{mn}-1}{p^m-1}} = t\alpha$, so ist $(x - t\alpha)$ $(x-(t\alpha)^p) \ldots\ldots (x-(t\alpha)^{p^{m-n}})$ ein Ausdruck, dessen Coefficienten nach dem Modul (p, α) ganzen reellen Zahlen congruent werden, und der, wenn man diese Zahlen statt jener Coefficienten substituirt, nach dem Modul p irreductibel ist.

Beweis. Da $(t\alpha)^{p^m-1} \equiv (r\alpha)^{p^{mn}-1}$ (*mod. p, α*) ist, so folgt (§. 18.) $t\alpha^{p^m-1} \equiv 1$ (*mod. p, α*)$^{p^m} \equiv (t\alpha)$ (*mod. p, α*). Entwickelte man nun einen Ausdruck, dessen Wurzeln die p^{ten} Potenzen der Wurzeln von $(x-(t\alpha)^p) \ldots\ldots$ $(x-(t\alpha)^{p^{m-1}})$ sind, so folgt, dass derselbe mit $(x-t\alpha)(x-(t\alpha)^p)\ldots(x-(t\alpha)^{p^{m-n}})$ nach dem Modul (p, α) congruent sein werde. Andrerseits weiss man aber, dass die Coefficienten des Ausdruckes, dessen Wurzeln die p^{ten} Potenzen der Wurzeln jenes Ausdruckes sind, den p^{ten} Potenzen der entsprechenden Coefficienten desselben congruent sein werde (§. 13. *No.* 2.). Setzt man nun $(x-t\alpha)(x-(t\alpha)^p) \ldots\ldots (x-(t\alpha)^{p^{m-1}}) \equiv x^m + \phi_1\alpha\,.\,x^{m-1} + \phi_2\alpha\,.\,x^{m-2} + \ldots + \phi_m\alpha$, so folgt, dass $(\phi_1\alpha)^p \equiv \phi_1\alpha$ (*mod. p, α*) sei. Bezeichnei aber g eine primitive Wurzel von der Congruenz $x^{p-1} - 1 \equiv 0$ (*mod. p*), so folgt, da nach obiger Congruenz $\phi_1\alpha(\phi_1\alpha^{p-1}-1) \equiv 0$ (*mod. p, α*) ist, dass $\phi_1\alpha$ $(\phi_1\alpha-g)(\phi_1\alpha-g^2) \ldots\ldots (\phi_1\alpha-g^{p-1}) \equiv 0$ (*mod. p, α*) sein müsse. Es muss mithin $\phi_1\alpha$ einer der Zahlen $0, g, g^2, \ldots g^{p-1}$ nach dem Modul (p, α) congruent werden. Ebenso kann man zeigen, dass jeder der folgenden Coefficienten einer dieser Zahlen congruent werden müsse. Um nun den andern Theil des Satzes zu zeigen, bemerke man zuerst, dass $t\alpha, (t\alpha)^p, (t\alpha)^{p^2}, \ldots\ldots$ $(t\alpha)^{p^{m-1}}$ sämmtlich primitive Wurzeln der Congruenz $x^{p^m-1} - 1 \equiv 0$(*mod. p, α*) sein werden. Da nämlich $t\alpha$ gleich $(r\alpha)^{\frac{p^{mn}-1}{p^m-1}}$ ist, und $r\alpha$ primitive Wurzel von $x^{p^{mn}-1} - 1 \equiv 0$ (*mod. p, α*) ist, so muss $t\alpha$ offenbar primitive Wurzel der Congruenz $x^{p^m-1} - 1 \equiv 0$ (*mod. p, α*) sein. Die übrigen Ausdrücke $(t\alpha)^p, (t\alpha)^{p^2}, \ldots (t\alpha)^{p^{m-1}}$ müssen nun primitive Wurzeln derselben Congruenz sein, weil $p, p^2, \ldots p^{m-1}$ relative Primzahlen zu $p^m - 1$ sind. Wollte man nun annehmen $(x-t\alpha)(x-(t\alpha)^p)(x-(t\alpha)^{p^2}) \ldots\ldots (x-(t\alpha)^{p^{m-1}})$ hätte nach dem Modul p irgend einen irreductibeln Factor vom Grade m^1, wo $m^1 < m$ ist, so müsste der Ausdruck, dessen Wurzeln die $(p^{m^1}-1)^{ten}$ Potenzen der Wurzeln von $(x-t\alpha)(x-(t\alpha)^p) \ldots\ldots (x-(t\alpha)^{p^{m-1}})$ sind, für $x = 1$ congruent 0 (*mod. p*) werden (§. 36. *Zus.*). Setzt man also $p^{m^1} - 1 = q$, so müsste

$(1-(t\alpha)^q)(1-(t\alpha)^{qp}) \ldots (1-(t\alpha)^{q \cdot p^{m-1}}) \equiv 0$ (*mod.* p, α) sein. Es müsste mithin einer der Factoren auf der linken Seite $\equiv 0$ (*mod.* p, α) werden. Bezeichnet nun k einen der Werthe $0, 1, 2 \ldots m-1$, so müsste ein Ausdruck von der Form $1-(t\alpha)^{q \cdot p^k} \equiv 0$ (*mod.* p, α) werden. Da aber $(t\alpha)^{p^k}$ eine primitive Wurzel der Congruenz $x^{p^m-1}-1 \equiv 0$ (*mod.* p, α) ist, so kann, indem $q = p^{m_1}-1$, und $p^{m_1}-1$ kleiner als p^m-1 ist, diese Congruenz nicht Statt finden, und der obige Ausdruck muss daher irreductibel sein.

Zusatz. Wenn also in Bezug auf den Modul p eine irreductibele Congruenz vom Grade $m \cdot n$ existirt, so kann man in Bezug auf denselben Modul auch eine irreductibele Congruenz vom Grade m und eben so vom Grade n aufstellen.

§. 44.

Lehrsatz. Es giebt irreductibele Congruenzen jeden Grades nach dem Modul p, wenn p eine Primzahl ist.

Beweis. Es soll zuerst bewiesen werden, dass es irreductibele Congruenzen solcher Grade gebe, die Potenzen von p sind.

Um nun zu beweisen, dass es irreductibele Congruenzen vom Grede p gebe, setze man $p^\rho = p_1$, und es wird behauptet, dass $\frac{x^{p_1-1}-1}{x^{p-1}-1}$ in lauter irreductibele Factoren vom Grade p zerfällt werden könne. Setzt man nämlich voraus, der Ausdruck habe in Bezug auf den Modul p den Factor fx, so dass also $\frac{x^{p_1-1}-1}{x^{p-1}-1} = fx\,Qx + pRx$ ist, wo Qx und Rx Ausdrücke von x bedeuten, so folgt leicht aus dieser Gleichung, dass, wenn α eine Wurzel von fx ist, $\alpha^{p_1-1}-1 \equiv 0$ (*mod.* $p.\ \alpha$) sein werde. Hiernach kann also der Grad von fx nicht grösser als p_1 oder als p^ρ sein. (§. 17.). Wäre nun fx vom Grade n, so wäre auch $\alpha^{p^n-1}-1 \equiv 0$ (*mod.* $p.\ \alpha$) (§. 18.). Hieraus folgt nun leicht, dass, wenn k der grösste gemeinschaftliche Theiler von $p^\rho-1$ und p^n-1 ist, auch $\alpha^k \equiv 1$ (*mod.* $p.\ \alpha$) sein müsse. Da aber p und n nur den Factor p oder 1 gemeinschaftlich haben können, so muss der grösste gemeinschaftliche Theiler von $p^\rho-1$ und p^n-1 entweder $p^\rho-1$ oder $p-1$ sein (Vergl. die Anmerkung zum §. 48.). Kann der zweite Fall nicht Statt finden, so muss der erste in Erfüllung gehen, d. h. p^n-1 muss den Factor $p^\rho-1$ in sich schliessen, woraus dann folgt, dass $n = p$ sein muss. Fände nun aber der zweite Fall Statt, so hätte man $\alpha^{p-1}-1 \equiv 0$ (*mod.* p, α) und mithin $n = 1$, es müsste mithin der Ausdruck $\frac{x^{p_1-1}-1}{x^{p-1}-1}$ irgend einen Factor vom 1ten Grade haben, oder für irgend einen Zahlwerth von x congruent 0 (*mod.* p) werden. Es ist aber $p_1-1 = p^\rho-1 = (p-1)(p^{\rho-1}+p^{\rho-2}+\ldots+1)$ oder wenn man $p^{\rho-1}+p^{\rho-2}+\ldots+1 = s$ setzt so ist $p_1-1 = (p-1)s$ und mithin

$$\frac{x^{p_1-1}-1}{x^{p-1}-1} = \frac{x^{(p-1)s}-1}{x^{(p-1)}-1} = x^{(p-1)(s-1)} + x^{(p-1)(s-2)} + \ldots + x^{(p-1)\cdot 1} + 1 .$$

Setzt man hier für x irgend einen Zahlwerth, so wird der Ausdruck congruent s (*mod.* p), da jedes Glied in ihm congruent 1 wird. Es ist aber offenbar $s \equiv 1\ (mod.\ p)$, und $\frac{x^{p_1-1}-1}{x^{p-1}-1}$ kann mithin keinen Factor vom 1^{ten} Grade enthalten, und muss mithin in lauter Factoren vom Grade p zerfallen.

Auf ähnlichem Wege kann nun sogleich gezeigt werden, dass es irreductibele Congruenzen vom Grade p^2 und überhaupt von jedem Grade gebe, der einer Potenz von p gleich ist. Es wird genügen, dies noch einmal kurz für den Grad von p^2 durchzuführen. Man setze also $p^p = p_1$, $p^{p^2} = p_2$, so wird behauptet, dass der Ausdruck $\frac{x^{p_2-1}-1}{x^{p_1-1}-1}$ nur irreductibele Factoren vom Grade p^2 in sich schliessen könne. Setzt man nämlich voraus, fx wäre ein Factor dieses Ausdrucks, und α eine Wurzel von fx, so erhielte man wieder $\alpha^{p_2-1} - 1 \equiv 0\ (mod.\ p, \alpha)$. Da nun $p_2 = p^{p^2}$, so kann der Grad von fx diese Zahl nicht überschreiten. Ist nun fx vom Grade n, so hat man auch $\alpha^{p^n-1} - 1 \equiv 0\ (mod.\ p, \alpha)$. Bedeutet ferner k den grössten gemeinschaftlichen Theiler zwischen n und p^2, so ist auch $p^k - 1$ der grösste gemeinschaftliche Theiler zwischen $p^{p^2} - 1$ und $p^n - 1$ (Vergl. d. Anm. zum §. 48.) und mithin auch $\alpha^{p^k-1} - 1 \equiv 0\ (mod.\ p, \alpha)$, und hiernach muss k mit n zusammenfallen (§. 17.), d. h. es muss n ein Theiler von p^2 sein. Wenn mithin der Grad von fx nicht p^2 sein sollte, so müsste er 1 oder p sein. In beiden Fällen müsste α oder die Wurzel von fx der Congruenz genügen $\alpha^{p_1-1} - 1 \equiv 0\ (mod.\ p, \alpha)$. Wird also nachgewiesen, dass α dieser Congruenz nicht genügt, so ist fx vom Grade p^2. Es ist aber $p_2 - 1 = p_1^p - 1 = (p_1 - 1)(p_1^{p-1} + p_1^{p-2} + \ldots + 1)$. Setzt man wieder $p_1^{p-1} + p_1^{p-2} + \ldots + 1 = s$, so ist

$$\frac{x^{p_2-1}-1}{x^{p_1-1}-1} = \frac{x^{(p_1-1)s}-1}{x^{(p_1-1)}-1} = x^{(p_1-1)(s-1)} + x^{(p_1-1)(s-2)} + \ldots + 1.$$

Setzt man mithin in diesen Ausdruck statt x einen Werth α, welcher der Congruenz $\alpha^{p_1-1} - 1 \equiv 0\ (mod.\ p, \alpha)$ genügt, so wird derselbe offenbar nach dem Modul (p, α) congruent s, und da s congruent 1 ist, so wird er offenbar $\equiv 1\ (mod.\ p, \alpha)$. $\frac{x^{p_2-1}-1}{x^{p_1-1}-1}$ kann mithin keinen Factor vom Grade 1 oder vom Grade p haben, und muss mithin lauter irreductibele Factoten vom Grade p^2 in sich schliessen.

Setzt man $p^{p^n} = p_n$ und $p^{p^{n-1}} = p_{n-1}$, so kann man auf gleiche Weise zeigen, dass $\frac{x^{p_n-1}-1}{x^{p_{n-1}-1}-1}$ aus lauter irreductibelen Factoren vom Grade p^n zusammengesetzt sei.

Man setze nun voraus, der Satz sei für alle Grade bewiesen, die kleiner als lp^n sind, wo l eine Zahl andeutet, die nicht durch p aufgeht, und er solle auch für den Grad lp^n bewiesen werden, so setze man $l = a^\alpha\ b^\beta\ c^\gamma \ldots$, wo a, b, c, .. Primzahlen bedeuten, und $a^{\alpha-1}\ b^{\beta-1}\ c^{\gamma-1} \ldots (a-1)(b-1)(c-1) \ldots = A$, so ist offenbar $A < l$ und es wird daher irreductibele Congruenzen vom Grade $p^n A$ geben. Man setze nun, α sei eine Wurzel solcher Congruenz, mache $P = p^{p^n \cdot A}$, und bestimme $r\alpha$ als primitive Wurzel der Congruenz $x^{P-1} - 1 \equiv 0\ (mod.\ p, \alpha)$, so wird die Congruenz $x^l - r\alpha$, irre-

irreductibel sein, weil l ein Theiler von $P - 1$ oder von $p^{A\,p^n} - 1$ ist, wovon man sich leicht überzeugt, wenn man für A seinen Werth $a^{\alpha-1}\,b^{\beta-1}\,c^{\gamma-1}\ldots(a-1)(b-1)(c-1)\ldots$ setzt.*) (§. 41.). Bildet man nun das Product

$$(x'-r\alpha)\,(x'-(r\alpha)^p)\,(x'-(r\alpha)^{p^2})\ldots(x'-(r\alpha)^{p^{p^n A-1}}),$$

so ist dies ein irreductibeler Ausdruck vom Grade $l\,.\,A\,.\,p^n$ (§. 42.). Da nun lp^n ein Factor dieser Zahl ist, so muss es auch irreductibele Congruenzen vom Grade lp^n geben (§. 43.), wenn es irreductibele Congruenzen jeden Grades giebt, der kleiner als lp^n ist.

Da es nun nach jeder Primzahl irreductibele Congruenzen des 1^{ten} Grades giebt, so folgt jetzt leicht, dass es nach jeder Primzahl irreductibele Congruenzen jeden Grades gebe.

§. 45.

Bedeutet $\phi\alpha$ einen Ausdruck von α, und n_1 die kleinste Zahl, welche der Congruenz $x^{p^{n_1}-1} - 1 \equiv 0$ $(p.\alpha)$ genügt, so gehören die Coefficienten des Ausdrucks $(x-\phi\alpha)(x-\phi(\alpha^p))(x-\phi(\alpha^{p^2}))\ldots(x-\phi(\alpha^{p^{n_1-1}}))$ sämmtlich zum Modul p, sind also nach dem Modal (p,α) ganzen reellen Zahlen congruent zu setzen, und der Ausdruck $(x-\phi(\alpha))(x-\phi(\alpha^p))\ldots(x-\phi(\alpha^{p^{n_1-1}}))$ muss, wenn dies geschehen, nach dem Modul p irreductibel sein.

Die erste Aussage ergiebt sich aus §. 16., weil man leicht ableitet, dass der Ausdruck, dessen Wurzeln die p^{ten} Potenzen der Wurzeln von $(x-\phi\alpha)(x-\phi(\alpha^p))\ldots(x-\phi(\alpha^{p^{n_1-1}}))$ diesem Ausdruck nach dem Modul (p,α) congruent ist. Die zweite Aussage folgt aus der Annahme, dass n_1 die kleinste Zahl sei, welche der Congruenz $x^{p^{n_1}-1} - 1 \equiv 0$ (*mod.* p,α) genügt, dass mithin der Ausdruck für die $(p^m-1)^{ten}$ Potenzen der Wurzeln von $(x-\phi(\alpha))(x-\phi(\alpha^p))\ldots.(x-\phi(\alpha^{p^{n_1-1}}))$, wenn man statt x den Werth 1 setzt, nicht $\equiv 0$ (*mod.* p,α) werden kann, so lange $m < n_1$ ist (§. 37.). Aus §. 12. folgt übrigens, dass n_1 oder der Grad von $(x-\phi(\alpha))(x-\phi(\alpha^p))\ldots.(x-\phi(\alpha^{p^{n_1-1}}))$ ein Theiler von n oder von der Zahl sein müsse, welche den Grad des irreductibeln Ausdrucks von x angiebt, von dem α eine Wurzel ist. Bedeutet nun $\psi\alpha$ einen Ausdruck, der keinem der Ausdrücke $\phi(\alpha)$, $\phi(\alpha^p)$, $\ldots.\,\phi(\alpha^{p^{n_1-1}})$ congruent ist, und m_1 die kleinste Zahl, welche der Congruenz $(\psi\alpha)^{p^{m_1}-1} - 1 \equiv 0$ (*mod.* p,α) genügt, so wird auch $(x-\psi\alpha)(x-\psi(\alpha^p))\ldots(x-\psi(\alpha^{p^{m_1-1}-1}))$ ein zum Modul p gehöriger irreductibeler Ausdruck von x sein, der aber von $(x-\phi\alpha)(x-\phi(\alpha^p))\ldots.(x-\phi(\alpha^{p^{n_1-1}}))$ nach diesem Modul verschieden sein muss, weil offenbar beide Ausdrücke nach dem Modul (p,α) verschieden sind, da sie in Bezug auf diesen Modul aus verschiedenen Factoren zusammengesetzt sind. — Alle Ausdrücke von x, die auf ähnliche Weise wie $(x-\phi\alpha)$ $(x-\phi(\alpha^p))\ldots..(x-\phi(\alpha^{p^{n_1-1}}))$ gebildet sind, müssen nun in Bezug auf den

*) Siehe *Disquisitiones arithmeticae* §. 92. Pg. 90.

Wodul p Divisoren von $x^{p^n-1}-1$ sein. Da nämlich sämmtliche Wurzeln von $(x-\phi(\alpha))(x-\phi(\alpha^p))\ldots.(x-\phi(\alpha^{p^{n_1-1}}))$ unter einander verschieden sind, und zugleich der Congruenz $x^{p^n-1}-1\equiv 0$ (*mod.* p, α) genügen, so folgt, dass $x^{p^n-1}-1$ in Bezug auf den Modul (p, α) den Factor $(x-\phi(\alpha))(x-\phi(\alpha^p))\ldots(x-\phi(\alpha^{p^{n_1-1}}))$ haben werde (§. 20. *No.* 9.). Setzt man nun $(x-\phi\alpha)(x-\phi(\alpha^p))\ldots..(x-\phi(\alpha^{p^{n_1-1}}))=x^{n_1}+a_1x^{n_1-1}+a_2x^{n_1-2}+\ldots.a_n+pF(x,\alpha)$, wo $a_1, a_2, \ldots. a_n$ ganze Zahlen und $F(x,\alpha)$ einen zum Modul (p,α) gehörigen Ausdruck von x darstellt, so müssen die Normen von $x^{n_1}+a_1x^{n_1-1}+a_2x^{n_1-1}+\ldots.+a_n+pF(x,\alpha)$ und von $x^{n_1}+a_1x^{n_1-1}+a_2x^{n_1-2}+\ldots a_n$ in Bezug auf $x^{p^n-1}-1$ offenbar nach dem Modul (p,α) congruent sein; da der erste Ausdruck ein Divisor von $x^{p^n-1}-1$ ist, so müssen diese Normen in Bezug auf den Modul (p,α) congruent 0 werden. Offenbar ist aber die Norm von $x^{n_1}+a_1x^{n_1-1}+a_2x^{n_1-2}+\ldots+a_n$ in Bezug auf $x^{p^n-1}-1$ eine ganze Zahl, soll diese nach dem Modul $(p.\alpha)$ congruent 0 sein, so muss sie auch nach dem Modul p congruent 0 sein, wird aber diese Norm congruent 0, so ist auch (§. 11.) der irreductibele Ausdruck $x^{n_1}+a_1x^{n_1-1}+a_2x^{n_1-2}+\ldots a_{n_1}$ in Bnzug auf den Modul p ein Factor von $x^{p^n-1}-1$. Da nun die sämmtlichen p^n-1 Ausdrücke von α, die nicht congruent 0 (*mod.* p, α) zu setzen sind, die sämmtlichen Wurzeln von $x^{p^n-1}-1$ sind, so folgt, dass sich immer n_1 dieser Wurzeln, wo n_1 ein Factor von n ist, in einem zu dem Modul p gehörigen irreductibelen Ausdruck von x vereinigen. Es kann mithin $x^{p^n-1}-1$ nur solche irreductibele Ausdrücke von x zu Factoren nach dem Modul p haben, deren Grad in n aufgeht. Auf der andern Seite kann man behaupten, dass alle irreductibeln einfachen Ausdrücke von x, deren Grad in n aufgeht, Factoren von $x^{p^n-1}-1$ in Bezug auf den Wodul p sind. Setzt man nämlich $n=n_1n_2$ und n_1 und n_2 als ganze Zahlen voraus, ferner ϕx als einen einfachen irreductibeln Ausdruck vom Grade n_1, und β als eine Wurzel von ϕx, so erhält man (§. 18.) $\beta^{p^{n_1}-1}\equiv 1$ (*mod.* p, β) und mithin, da bekanntlich $p^{n_1}-1$ in $p^{n_1n_2}-1$ aufgeht auch $\beta^{p^{n_1n_2}-1}-1$ oder $\beta^{p^n-1}-1\equiv 0$ (*mod.* p. β) und daher (§. 14. *No.* 2) ϕx als Factor von $x^{p^n-1}-1$ in Bezug auf den Modul p. Hieraus folgt nun:

> dass jeder irreductibele Ausdruck, welcher nach dem Modul p ein Divisor von $x^{p^n-1}-1$ ist, einem Ausdruck von der Form $(x-\phi(\alpha))(x-\phi(\alpha^p))\ldots..(x-\phi(\alpha^{p^{n_1-1}}))$ in Bezug auf den Modul (p,α) congruent gesetzt werden könne.

§. 46.

Aufgabe. Die Anzahl der irreductibeln Congrueuzen vom Grade n nach dem Modul p zu bestimmen, wenn n eine Primzahl ist.

Auflösung. Da es irreductibele Congruenzen jeden Grades nach dem Modul p giebt, (§. 44.) so sei $fx\equiv 0$ (*mod.* p) eine solche vom n^{ten} Grade, und α eine Wurzel von fx. Nun giebt es im Ganzen p^n-1 verschiedene

Reste nach dem Modul (p, α), welche nicht $\equiv 0$ $(mod.\, p, \alpha)$ sind. Da nun n keinen Theiler ausser 1 hat, so ist jeder dieser Reste entweder als die Wurzel einer irreductibeln Congruenz des n^{ten} Grades oder des ersten Grades zu betrachten. Es können aber nur die $(p-1)$ Reste oder Ausdrücke von α auf Congruenzen des ersten Grades führen, in welchen die Coefficienten der Potenzen von α, welche den 0^{ten} Grad überschreiten, congruent 0 werden (§. 12. nebst Zus.). Dergleichen Ausdrücke giebt es aber offenbar nur $p - 1$, nämlich $1, 2, \ldots\, p - 1$. Mithin giebt es $p^n - 1 - (p-1) = p(p^{n-1} - 1)$ Ausdrücke von α, die zu irreductibeln Congruenzen vom Grade n nach dem Modul p führen. Da von diesen je n als Wurzeln zu einer Congruenz des n^{ten} Grades gehören, so giebt es offenbar $p\left(\frac{p^{n-1}-1}{n}\right)$ einfache irreductibele Congruenzen des n^{ten} Grades.

Anmerkung. Es folgt hieraus, dass $\frac{p^{n-1}-1}{n}$ eine ganze Zahl sein müsse, wenn p nicht gleich n ist. So erhält mithin der **Fermat**'sche Satz eine eigenthümliche Beleuchtung, indem $\frac{p^{n-1}-1}{n}$ einen Zahlenwerth andeutet, der seiner Natur nach sich nur auf eine ganze Zahl beziehen kann.

§. 47.

Aufgabe. Die Anzahl der irreductibelen Congruenzen vom Grade n^ν zu bestimmen, wenn n eine Primzahl und ν eine ganze Zahl bedeutet.

Auflösung. Es sei $fx \equiv 0$ $(mod.\, p)$ eine irreductibele Congruenz vom Grade n, α eine Wurzel von fx, $r\alpha$ eine primitive Wurzel der Congruenz $x^{p^{n^\nu}-1} - 1 \equiv 0$ $(mod.\, p, \alpha)$ und $\beta = \alpha^{\frac{p^{n^\nu}-1}{p^{n^{\nu-1}}-1}}$, so wird es Ausdrücke von α geben, die nicht $\equiv 0$ $(mod.\, p, \alpha)$ sind, $p^{n^\nu} - 1$, hingegen Ausdrücke von β (β hängt nur von einer Congruenz des $(n^{\nu-1})^{ten}$ Grades ab (§. 43.)), die nicht congruent 0 sind, wird es geben $p^{n^{\nu-1}} - 1$. Die sämmtlichen Ausdrücke von α realisiren die Congruenz $x^{p^{n^\nu}-1} - 1 \equiv 0$ $(mod.\, p, \alpha)$, diejenigen aber unter ihnen, welche sich als Wurzeln von irreductibeln Congruenzen eines niedrigeren Grades als des n^{ten} ansehen lassen, sind jedenfalls von einem Grade, der sich durch n^{ν_1} darstellen lässt, wo $\nu_1 < \nu$ ist, und genügen mithin der Congruenz $x^{p^{n^{\nu_1}}-1} - 1 \equiv 0$ $(mod.\, p, \alpha)$, und (da n^{ν_1} auf jeden Fall ein Factor von $n^{\nu-1}$ sein muss) daher auch der Congruenz $x^{p^{n^{\nu-1}}-1} - 1 \equiv 0$ $(mod.\, p, \alpha)$. Aber die sämmtlichen Ausdrücke von β stellen alle Ausdrücke von α dar, welche dieser Congruenz genügen; zieht man also von der Anzahl der Ausdrücke von α, die Anzahl der Ausdrücke von β ab, so behält man diejenigen Ausdrücke zurück, welche erst in der Potenz $p^{n^\nu} - 1$ congruent 1 nach dem Modul (p, α) werden, welche also die Wurzeln der irreductibeln Ausdrücke von x nach dem Modul p vom Grade n^ν darstellen. Ihre Anzahl beträgt mithin

$(p^{n^\gamma}-1)-(p^{n^{\gamma-1}}-1)$ oder $p^{n^{\gamma-1}}(p^{n^{\gamma-1}(n-1)}-1)$. Da aber je n' Ausdrücke von α in eine Congruenz des Grades n' eingehen, so ist die Anzahl der irreductibeln Congruenzen vom Grade n' nach dem Modul p stets ausgedrückt durch $p^{n^{\gamma-1}}\left(\frac{p^{n^{\gamma-1}(n-1)}-1}{n^\gamma}\right)$.

§. 48.

Aufgabe. Die Anzahl der irreductibeln Congruenzen vom Grade $A^a\ B^b\ C^c\ D^d$ zu bestimmen, wenn A, B, C, D Primzahlen und a, b, c, d ganze positive Zahlen bedeuten.

Die Schlüsse sollen an den vier Primzahlen A, B, C, D so geführt werden, dass ersichtlich wird: sie, so wie die durch sie abgeleiteten Formeln, gelten allgemein.

Auflösung. Man setze $A^a\ B^b\ C^c\ D^d = n$ ferner $p^{A^{a-1}B^{b-1}C^{c-1}D^{d-1}} = P$, so ist die Anzahl derjenigen Ausdrücke von α, welche der Congruenz $x^{p^{n_1}-1}-1 \equiv 0$ (*mod. p, α*) nicht genügen, wenn $n_1 < A^a\ B^b\ C^c\ D^d$ ist, durch die Formel $P^{ABCD}-P^{ABC}-P^{ABD}-P^{ACD}-P^{BCD}+P^{AB}+P^{AC}+P^{AD}+P^{BC}+P^{BD}+P^{CD}-P^A-P^B-P^C-P^D+P$ ausgedrückt. Das Bildungsgesetz ist leicht ersichtlich. Die Anzahl der gesuchten Congruenzen erhält man nun, wenn man diesen Ausdruch durch $A^a\ B^b\ C^c\ D^d$ dividirt, sie ist mithin gleich $\{P^{ABCD}-P^{ABC}-P^{ABD}-P^{ACD}-P^{BCD}+P^{AB}+P^{AC}+P^{AD}+P^{BC}+P^{BD}+P^{CD}-P^A-P^B-P^C-P^D+P\}\ \frac{1}{A^a\ B^b\ C^c\ D^d}$.

Beweis. Zunächst bemerke man, dass sich obiger Ausdruck nicht ändert, wenn man jedes Glied um 1 verringert. Er geht nämlich alsdann in $(P^{ABCD}-1)-(P^{ABC}-1)-(P^{ABD}-1)-(P^{ACD}-1)-(P^{BCD}-1)+(P^{AB}-1)+(P^{AC}-1)+(P^{AD}-1)+(P^{BC}-1)+(P^{BD}-1)+(P^{CD}-1)-(P^A-1)-(P^B-1)-(P^C-1)-(P^D-1)+(P-1)$ über, welcher Ausdruck ausser dem ersten offenbar noch $1-4+\frac{4\,.\,3}{1\,.\,2}-\frac{4\,.\,3\,.\,2}{1\,.\,2\,.\,3}+1$ enthält. Da aber dieser Zahlenausdruck gleich $(1-1)^4$ und mithin 0 ist, so kann man den ersten Ansdruck auch in der angeführten Gestalt schreiben. Nun giebt aber $P^{ABCD}-1$ die Anzahl der Wurzeln von $x^{p^{A^a B^b C^c D^d}-1}-1 \equiv 0$ (*mod. p, α*) an, ferner $P^{ABC}-1$ die Anzahl der Wurzeln von $x^{p^{A^a B^b C^c D^{d-1}}-1}-1 \equiv 0$ (*mod. p, α*) etc. bis endlich $P-1$ die Anzahl der Wurzeln von $x^{p^{A^{a-1} B^{b-1} C^{c-1} D^{d-1}}-1}-1$ angiebt. Jeder Ausdruck von α, der nicht congruent 0 (*mod. p, α*) wird, ist nun mitgerechnet in der Anzahl $(P^{ABCD}-1)$, durch die folgenden Ausdrücke $-(P^{ABC}-1)-(P^{ABD}-1)-$ etc. wird aher die Anzahl derjenigen Ausdrücke von α, welche der Congruenz $x^{p^{n_1}-1}-1 \equiv 0$ (*mod. p, α*) genügen, wenn $n_1 < A^a\ B^b\ C^c\ D^d$ ist auf 0 reducirt, indem die Anzahl derjenigen Ausdrücke von α, welche jener Congruenz nur genügen, wenn $n_1 \equiv A^a B^b C^c D^d$ wird, durch die folgenden Ausdrücke unverändert bleibt. Es muss nämlich jeder Ausdruck von α, welcher der Congruenz genügt, $x^{p^{n_1}-1} - 1 \equiv 0 \ (mod.\ p, \alpha)$, wenn $n_1 < A^a B^b C^c D^d$ ist, einer der Congruenzen genügen $x^{p^{A^{a-1} B^b C^c D^d}-1} - 1 \equiv 0 \ (mod.\ p, \alpha)$, $x^{p^{A^a B^{b-1} C^c D^d}-1} - 1 \equiv 0 \ (mod.\ p, \alpha)$ $x^{p^{A^a B^b C^{c-1} D^d}-1} - 1 \equiv 0 \ (mod.\ p, \alpha)$, $x^{p^{A^a B^b C^c D^{d-1}}-1} - 1 \equiv 0 \ (mod.\ p, \alpha)$. Hier ist nun zu unterscheiden, ob er einer, zweien, dreien oder allen vieren dieser Congruenzen zu gleicher Zeit genügt. 1) Gesetzt nun der Ausdruck genügte nur einer dieser Congruenzen z. B $x^{p^{A^a B^b C^c D^{d-1}}-1} - 1 \equiv 0 \ (mod.\ p, \alpha)$ oder $x^{p^{ABC}-1} - 1 \equiv 0 \ (mod.\ p, \alpha)$, so ist er nur mitgezählt, in jener obigen allgemeinen Formel, in den beiden Gliedern $(p^{ABAD}-1) - (p^{ABC}-1)$ und in übrigen nicht, und da er in beiden Gliedern mit entgegengesetzten Vorzeichen mitgezählt ist, so fällt er in der allgemeinen Formel ganz aus. 2) Gesetzt nun der Ausdruck genügte den beiden Congruenzen $x^{p^{ABC}-1} - 1 \equiv 0 \ (mod.\ p, \alpha)$ und $x^{p^{ABD}-1} - 1 \equiv 0 \ (mod.\ p, \alpha)$ so muss er auch der Congruenz genügen $x^{p^{AB}-1} - 1 \equiv 0 \ (mod.\ p, \alpha)$,*) weil $p^{AB} - 1$ der grösste gemeinschaftliche Theiler von $p^{ABC} - 1$ und von $p^{ABD} - 1$ ist. Es ist mithin der Ausdruck mitgezählt in der obigen allgemeinen Formel in den Gliedern $(p^{ABCD}-1) - (p^{ABC}-1) - (p^{ABD}-1) + (p^{AB}-1)$ mithin $1 - 2 + 1 = (1-1)^2$ oder 0 mal. Er fällt mithin aus der allgemeinen Formel ganz aus.

---

*) Anmerkung. Es wird hier von zweien Sätzen Gebrauch gemacht, welche folgendermassen lauten: 1) Genügt irgend ein Ausdruck $\phi\alpha$ zugleich den Congruenzen $x^a - 1 \equiv 0 \ (mod.\ p, \alpha)$, $x^b - 1 \equiv 0 \ (mod.\ p, \alpha)$, $x^c - 1 \equiv 0 \ (mod.\ p, \alpha)$ etc. und t ist der grösste gemeinschaftliche Theiler von a, b, c etc., so genügt $\phi\alpha$ auch der Congruenz $x^t - 1 \equiv 0 \ (mod.\ p, \alpha)$. 2) Ist t der grösste gemeinschsftliche Theiler zwischen a, b, c, etc., so ist $p^t - 1$ der grösste gemeinschaftliche Theiler zwischen $p^a - 1$, $p^b - 1$, $p^c - 1$ etc., wenn p irgend eine ganze Zahl bedeutet. *Beweis ad* 1) Gesetzt r sei der grösste gemeinschaftliche Theiler zwischen a und b, und a ist $= ra_1$, $b = rb_1$, so kann man x und y in ganzen Zahlen so bestimmen, dass $a_1 x - b_1 y = 1$ sei. Da nun $(\phi\alpha)^{ra_1} \equiv 1 \ (mod\ p, \alpha)$ und $(\phi\alpha)^{rb_1} \equiv 1 \ (mod.\ p, \alpha)$, so muss auch $(\phi\alpha)^{ra_1 x} \equiv 1 \ (mod,\ p, \alpha)$ und $(\phi\alpha)^{rb_1 y} \equiv 1 \ (mod.\ p, \alpha)$, und mithin auch $(\phi\alpha)^{ra_1 x - rb_1 y} \equiv 1 \ (mod.\ p, \alpha)$ und daher auch, weil $a_1 x - b_1 y = 1$ ist, $\phi\alpha^r \equiv 1 \ (mod.\ p, \alpha)$ sein. Der grösste gemeinschäftliche Theiler zwischen a, b, c etc. ist nun offenbar auch der grösste gemeinschaftliche Theiler zwischen r, c etc. und durch wiederholte Anwendung des bereits Bewiesenen auf r und c etc. geht der Satz leicht hervor. *ad* 2) Gesetzt r sei der grösste gemeinschaftliche Theiler zwischen a und b und a ist $= ra_1$, $b = rb_1$, so sei wieder $a_1 x - b_1 y = 1$, und x und y ganze Zahlen. Nun ist bekanntlich von $p^{ra_1 x} - 1$ und $p^{rb_1 y} - 1$ das erstere ein Vielfaches von $p^{ra_1} - 1$ und das zweite ein ein Vielfaches von $p^{rb_1} - 1$. Der grösste gemeinschaftliche Theiler beider Ausdrücke muss mithin auch ein Theiler der Differenz $(p^{ra_1 x}-1) - (p^{rb_1 y}-1)$ oder von $p^{ra_1 x} - p^{rb_1 y}$ oder von $p^{rb_1 y}(p^{ra_1 x - rb_1 y}-1)$ und mithin ein Theiler von $p^{rb_1 y}(p^r - 1)$ sein. Da nun $p^{rb_1 y}$ keinen Theiler mit $p^a - 1$ gemeinschaftlich haben kann, so muss dieser gemeinschaftliche Theiler in $p^r - 1$ liegen, und kann mithin nichts anderes als dieser Ausdruck selbst sein. Hieraus folgt nun, dass der grösste gemeinschaftliche Theiler zwischen $p^a - 1$, $p^b - 1$, $p^c - 1$ etc., zugleich der grösste gemeinschaftliche Theiler zwischen $p^r - 1$ und $p^c - 1$ etc. sei, und durch wiederholte Anwendung des nun schon Bewiesenen geht der Satz hervor.

3) Gesetzt nun der Ausdruck genügte den Conguenzen $x^{P^{ABC}-1}-1\equiv 0$ $(mod. p, \alpha)$, $x^{P^{ABD}-1}-1\equiv 0$ $(mod. d, \alpha)$, $x^{P^{ACD}-1}-1\equiv 0$ $(mod. p, \alpha)$, so müsste er auch der Congruenz $x^{P^{A}-1}-1\equiv 0$ $(mod. p, \alpha)$ genügen, da P^A-1 der grösste gemeinschaftliche Theiler von $P^{ABC}-1$, $P^{ABD}-1$, $P^{ACD}-1$ ist (Vergl. d. Anmerkung). Er müsste mithin auch den Congruenzen genügen $x^{P^{AB}-1}-1\equiv 0$ $(mod. p, \alpha)$, $x^{P^{AC}-1}-1\equiv 0$ $(mod. p, \alpha)$, $x^{P^{AD}-1}-1\equiv 0$ $(mod. p, \alpha)$. Demnach würde er in der allgemeinen Formel in folgenden Gliednrn mitgezählt sein: $(P^{ABCD}-1)-(P^{ABC}-1)-(P^{ABD}-1)-(P^{ACD}-1)+(P^{AB}-1)+(P^{AC}-1)+(P^{AD}-1)-(P^A-1)$. Da er nun in jedem Gliede einmal mitgezählt ist, so ist er im Ganzen gezählt $1-3+3-1=(1-1)^3$ oder 0 mal, fällt mithin aus der allgemeinen Formel aus.

4) Genügt der Ausdruck sämmtlichen oben angegebenen 4 Congruenzen, so genügt er auch der Congruenz $x^{P-1}-1\equiv 0$ $(mod. p, \alpha)$, weil $P-1$ der grösste gemeinschaftliche Theiler von $(P^{ABC}-1)$, $(P^{ABD}-1)$, $(P^{ACD}-1)$, und $(P^{BCD}-1)$ ist. Er genügt mithin auch den Congruenzen $x^{P^{A}-1}-1\equiv 0$ $(mod. p, \alpha)$, $(x^{P^{B}-1}-1)\equiv 0$ $(mod. p, \alpha)$ etc., $x^{P^{AB}-1}-1\equiv 0$ $(mod. p, \alpha)$, $x^{P^{AC}-1}-1\equiv 0$ $(mod. p, \alpha)$ etc. $x^{P^{ABC}-1}-1\equiv 0$ $(mod. p, \alpha)$ etc. und endlich auch $x^{P^{ABCD}-1}-1\equiv 0$ $(mod. p, \alpha)$. Er ist mithin in jedem Gliede der allgemeinen Formel mitgezählt, und kommt daher $1-4+6-4+1=(1-1)^4$ oder 0mal vor, fällt mithin aus der allgemeinen Formel aus. Es sind also in der allgemeinen Formel allein diejenigen Ausdrücke von α mitgezählt, die der Congruenz $x^{p^{n_1}-1}-1\equiv 0$ $(mod. p. \alpha)$ nur genügen, wenn $n_1=n$ ist. Denn diese liegen im ersten Gliede und bleiben von den folgenden unberührt. Da nun je n Ausdrücke von α in einen irreductibeln Ausdruck von x des n^{ten} Grades nach dem Modul p als Wurzeln eingehen, so ist die Anzahl sämmtlicher irreductibelen Ausdrücke von x, die zum n^{ten} Grade gehören, ausgedrückt durch die Formel $\{P^{ABCD}-P^{ABC}-P^{ABD}-P^{ACD}-P^{BCD}+P^{AB}+P^{AC}+P^{AD}+P^{BC}+P^{BD}+P^{CD}-P^A-P^B-P^C-P^D+P\}\frac{1}{A^a B^b C^c D^d}$, wo $P=p^{A^{a-1}B^{b-1}C^{c-1}D^{d-1}}$ ist, ferner A, B, C, D Primzahlen bedeuten, und der Grad $n=A^a B^b C^c D^d$ ist.

§. 49.

Einer aufmerksamen Betrachtung über die vorhergehenden Paragraphen wird es nicht entgehen, dass sich die erhaltenen Resultate auch auf die Modulu von der Form *Mod.* (p, α), *Mod.* (p, α, β) etc. hinüber führen lassen. Hier genüge es, Folgendes zu bemerken:

1) Es giebt in Bezug auf jeden Modul (p, α) irreductibele Congruenzen jedweden Grades.

2) Bedeutet $F(x) \equiv 0 \, (mod. \, p, \alpha)$ eine irreductibele Congruenz vom Grade m nach dem Modul (p, α) und hängt α selbst von einer irreductibeln Congruenz vom Grade n nach dem Modul p ab, so ist jeder irreductibele Ausdruck des $(m_1)^{ten}$ Grades von x, welcher nach dem Modul (p, α) ein Divisor von $x^{p^{mn}-1}-1$ ist, von der Form $(x-\phi(\beta))(x-\phi(\beta^{p^n}))(x-\phi(\beta^{p^{2n}}))\dots(x-\phi(\beta^{p^{(m_1-1)n}}))$ in Bezug auf den Modul (p, α).

3) Die Formeln für die Anzahl der irreductibeln Congruenzen nach dem Modul (p, α) gehen nun unter den gegebenen Voraussetzungen, aus den für den Modul p entwickelten hervor, wenn man statt p, p^n und statt n den Grad von Fx, also m setzt.

Ist also m eine Primzahl, so erhält man die Anzahl der irreductibeln Congruenzen vom Grade m, nach dem Modul (p, α) aus der Formel des §. 46. in der folgenden $p^n\left(\frac{p^{n(m-1)}-1}{m}\right)$ ausgedrückt. Die allgemeine Formel des §. 48. ändert sich nur in so fern, als P die Bedeutung $p^{nA^{a-1}B^{b-1}C^{c-1}D^{d-1}}$ annimmt.

§. 50.

Wenden wir zum Schluss noch einmal unsere Aufmerksamkeit auf den Ausdruck $x^n - 1$.

Im (§. 18.) wurde gefunden, dass jeder irreductibele Ausdruck sich nach dem Modul p als ein Divisor eines Ausdrucks von der Form $x^n - 1$ ansehen lasse. Es soll nun, unter der Voraussetzung, dass n eine Primzahl ist, a priori bestimmt werden, in wie viele irreductibele Ausdrücke des wie vielten Grades sich $\frac{x^n-1}{x-1}$ nach dem Modul p zerfällen lasse. — Zu dem Ende wird behauptet: dass, wenn n_1 die kleinste Zahl ist, welche der Congruenz $p^{n_1} - 1 \equiv 0 \, (mod. \, n)$ genügt, oder was gasselbe ist, wenn p in Bezug auf den Modul n zu n_1 gehört, so wird $\frac{x^n-1}{x-1}$ in Bezug auf den Modul p in $\frac{n-1}{n_1}$ irreductibele Ausdrücke vom Grade n_1 zerfällt werden können.

Beweis. Ist nämlich α eine Wurzel des Ausdrucks $\frac{x^n-1}{x-1}$, so ist bekanntlich, wenn n eine Primzahl ist, $\frac{x^n-1}{x-1} = (x-\alpha)(x-\alpha^2)\dots(x-\alpha^{n-1})$. Setzt man nun $p^{n_1} - 1 = N$, so wird der Ausdruck, welcher die N^{ten} Potenzen der Wurzeln von $\frac{x^n-1}{x-1}$ als Wurzeln in sich schliesst, $(x-\alpha^N)(x-\alpha^{2N})\dots(x-\alpha^{(n-1)N})$. Geht nun N nicht durch n auf, so werden die Reste von N, $2N$, ... $(n-1)N$ mit den Resten $1, 2, \dots n-1$ nach dem Modul n übereinstimmen, und der Ausdruck $(x-\alpha^N)(x-\alpha^{2N})\dots(x-\alpha^{(n-1)N})$ mit $(x-\alpha)(x-\alpha^2)\dots(x-\alpha^{n-1})$ oder mit $\frac{x^n-1}{x-1}$ zusammenfallen. Da dieser Ausdruck für $x = 1$ den Werth n annimmt, so schliesst man, wenn n nicht p

ist, dass $x^n - 1$ nach dem Modul p nur einen irreductibelen Factor von einem solchen Grade n_1 haben könne, welcher der Congruenz $p^{n_1} - 1 \equiv 0$ (*mod. n*) genügt (§. 37.). Es bleibt nun noch zu beweisen, dass, wenn n_1 die kleinste Zahl ist, welche die Congruenz $p^{n_1} - 1 \equiv 0$ (*mod. n*) realisirt, dass alsdann $\frac{x^n-1}{x-1}$ in $\frac{n-1}{n_1}$ irreductibele Factoren vom Grade n_1 zerfällt werden könne. Gesetzt nun es wäre $\frac{x^n-1}{x-1} = fx \,.\, Qx + pRx$, wo fx einen irreductibeln Factor nach dem Modul p andeutet, und Qx und Rx Ausdrücke von x sind, so übersieht man leicht, dass die beiden Ausdrücke, von welchen der eine die $(p^{n_1}-1)^{ten}$ Potenzen der Wurzeln von $fx \,.\, Qx + pRx$ und der andere dieselben Potenzen der Wurzeln von $fx \,.\, Qx$ als Wurzeln in sich schliesst, nach dem Modul p congruent sein werden (§. 2. §. 3. Einl.). Nennt man nun eine Wurzel von fx, α, so ist $fx \equiv (x-\alpha)(x-\alpha^p)\ldots\ldots(x-\alpha^{p^{m-1}})$ (*mod* p, α), wo m den Grad von fx umgiebt. Da nun, wenn $p^{n_1} - 1 \equiv 0$ (*mod. n*) ist, und der Ausdruck, welcher die $(p^{n_1}-1)^{ten}$ Potenzen der Wurzeln von $fx \,.\, Qx + pRx$ oder von $\frac{x^n-1}{x-1}$ als Wurzeln in sich schliesst, $(x-1)^n$ wird, so muss offenbar $(x-\alpha^N)(x-\alpha^{Np})\ldots(x-\alpha^{Np^{m-1}})$ in Bezug auf den Modul (p, α) ein Divisor von $(x-1)^n$ sein. Hiernach muss aber, wie leicht zu sehen, $\alpha^N \equiv 1$ (*mod. p. α*) rein. Da nun $N = p^{n_1} - 1$, so folgt, dass der Grad von fx die Zahl n_1 nicht überschreiten kann (§. 17.) Da er nun nach dem Vorhergehenden auch nicht weniger als n_1 betragen kann, so muss er n_1 selbst sein.

Zusatz 1. Ist $n = p$, so ist $x^p - 1 \equiv (x-1)^p$ (*mod. p*) und mithin $\frac{x^p-1}{x-1} \equiv (x-1)^{p-1}$ (*mod. p*).

Zusatz 2. Wenn p in Bezug auf den Modul n primitive Wurzel der Congruenz $x^{n-1} - 1 \equiv 0$ (*mod. n*) ist, so ist mithin der Ausdruck $\frac{x^n-1}{x-1}$ nach dem Modul p irreductibel. Da es nun stets primitive Wurzeln der Congruenz $x^{n-1} - 1 \equiv 0$ (*mod. n*) giebt, so sei g eine solche. Es giebt aber unendlich viele Primzahlen von der Form $g + yn$, wo y eine ganze Zahl bedeutet. (Vergl.: Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält, von *Lejeune-Dirichlet*, gelesen in der Academie der Wissenschaften 27. Juli 1837). Nach all diesen Primzahlen muss nun $\frac{x^n-1}{x-1}$ irreductibel sein, woraus denn unzweifelhaft folgt, dass es in algebraischer Beziehung gewiss irreductibel sein müsse.

Auf ganz anderem Wege hat *Gauss* den Satz (*Zus.* 2.) im §. 341. Pg. 599. der *Disquisitiones arithmeticae* bewiesen.

(Weitere Entwickelungen enthält die besonders erscheinende Abhandlung:

Grundzüge einer allgemeinen Theorie der höhern Congruenzen mit reellem Modul.)

Jahresbericht

von Michaelis 1842 bis Michaelis 1843.

I. Allgemeine Lehrverfassung.

1. Prima.

Classenordinarius: Professor Prorector Heffter.

A. Sprachen.

1) **Latein**, 8 St.: Horat. Od. libr. III. IV. und die Satiren mit Auswahl, wöchentl. 2 St., Dir.; Cic. de Oratore l. II. und III., 2 St., Tacit. Annal. l. I. vollständig und dann ausgewählte Stücke nach der Chrestomathie von Pabst, 2 St., Correctur der wöchentlichen Scripta und monatlichen freien Ausarbeitungen nebst Extemporalien, 2 St., Conrector Seyffert.

2) **Griechisch**, 5 St.: Sophoclis Antigone Hom. Ilias. libr. I—V., 2 St., Dir.: Platon. diall. min., 2 St., Prof. Heffter; Uebungen im Uebersetzen aus dem Deutschen, 1 St., Prof. Heffter.

3) **Deutsch**, 2 St.: Deutsche Literaturgeschichte, 1 St., Prof. Heffter; praktische Uebungen im deutschen Style, 1 St., Derselbe.

4) **Hebräisch**, 2 St.: Grammatik nach Gesenius und Lectüre der Psalmen (98—115.), Subrector Ramdohr.

5) **Französisch**, 2 St.: Kurzer Abriß der Gesch. der französ. Sprache; Lectüre der Phèdre par Racine und der Burgraves par Victor Hugo mit Bezug auf den Unterschied der class. und romant. Poesie; Uebungen in Uebers. aus Schillers pros. Schriften und freie Ausarbeitungen. Es wurde gewöhnlich französisch gesprochen. Collabor. II. Döhler.

B. Wissenschaften.

1) **Religionslehre**, 2 St.: Nach Marheineke's Lehrb. Artikel II. und Abriß der Kirchengeschichte. Dir.

2) **Philos Propädeutik**, 1 Nach Trendelenburg. 1 — 32. Ders.

3) **Geschichte und Geographie**, 3 St.: Geschichte des Mittelalters, nach Schmidt's Grundriß der allgem. Weltgeschichte. — Geographie von Italien, der pyren. Halbinsel, Frankreich, England und Deutschland. Subrector Ramdohr.

4) **Mathematik**, 3 St.: Die Lehre von den höhern arithm. Reihen, von den Combinationen und Kettenbrüchen nach dem 2. Theil des Müllerschen Lehrbuches. — Repetition der Lehre von den Potenzen, Logarithmen und Gleichungen des zweiten Grades &c.; der Stereometrie nach dem Lehrbuche von Mayer. — Wöchentlich 1 St. Vorträge der Primaner über verschiedene Aufgaben. Mathem. Schönemann.

5) **Physik**, 2 St.: Mechanik, Akustik und Optik nach dem Fischerschen Lehrbuche. Derselbe.

2. Secunda.

Classenordinarius: Conrector Prof. Dr. Seyffert.

A. Sprachen.

1) **Latein**, 10 St.: Virg. Aen. l. IV — V. 2 St.; Cicer. Oratt. Catilin. I — IV., von denen die 1ten im Sommersemester nach der Ruthardtschen Methode gelesen und memorirt worden, 3 St.; Correctur der wöchentlichen Scripta, 1 St.; metrische Uebungen und Extemporalien, 1 St.; Repetition des Gelesenen und Memorirten 1 St., Conrector; Livius l. II. im Sommersem. Prof. Heffter; l. III. 1 — 40., im Wintersem. Collab. Döhler, 2 St.

2) **Griechisch**, 6 St.: Hom. Odyss. I — VIII., Director, 2 St.; ausgewählte Gespräche Lucians und Xenoph. Memorabil. l. IV., 3 St.; die hauptsächlichsten Lehren der griech. Syntax nebst Extemporalien, 1 St., Conrector.

3) **Deutsch**, 2 St.: Anleitung zur Anfertigung deutscher Aufsätze, 1 St.; Correctur der deutschen Ausarbeitungen, 1 St., Pror. Prof. Heffter.

4) **Hebräisch**, 2 St.: Anfangsgründe der Sprache nach Gesenius, Pror. Prof. Heffter.

5) **Französisch**, 2 St.: im Sommer Bertrand et Raton von Scribe 2. Hälfte, im Winter La Calomnie von demselben Verf. 1. Hälfte gelesen, 1 St.; Uebungen im Uebersetzen aus deutschen Prosaikern, Grammatik nach Eugène Borel, freie Ausarbeitungen nach gegebenen Themen, 1 St., Collab. Döhler.

B. Wissenschaften.

1) **Religionslehre**, 2 St.: combinirt mit Prima, Director.

2) **Geschichte**, 2 St.: im Sommer griechische Geschichte bis zum Ende des polopones. Krieges, im Winter die griech. Geschichte beendet und Anfang der römischen bis zum Triumvirat, Conrector.

3) **Mathematik**, 4 St.: im Sommer Geometrie nach dem Lehrbuche von Steiner: Die geometrischen Constructionen &c., 3 St.; Uebungen in den algebraischen Gleichungen, 1 St.; im Winter Arithmetik: die leichtern Sätze aus der Lehre von den Congruenzen, Auflösung der unbestimmten Gleichungen des ersten Grades in Meyer Hirsch durch Congruenzen, 3 St.; Vorträge der Schüler über geometrische Aufgaben, 1 St., Mathem. Schönemann.

4) **Physik**, 2 St.: im Sommer Hydrostatik und Wellenlehre nach Fischer's Lehrbuche; im Winter die Lehre von den luftförmigen Körpern, Aërostatik und Pneumatik nach demselben Lehrbuche nebst Erklärung der gebräuchlichsten Maschinen, deren Theorie auf diesen Lehren beruht, nach dem 3. Hefte der Figurentafeln von Lautenschläger, Mathem. Schönemann.

C. Technische Fertigkeiten.

Zeichnen, 2 St.: S. Quarta.

3. Tertia.

Classenordinarius: Subrector Ramdohr.

A. Sprachen.

1) Latein, 9 St.: Ovid. Metam., im Sommer lib. V. mit Auswahl, Subr. Ramdohr, im Winter lib. VI. von 1 — 312. nebst metrischen Uebungen, 2 St.; Caesar de bello Gallico nach Dr. M. Seyffert's Ausgabe lib. IV. und V. bis c. 48. Daneben Cicero's erste Rede gegen Catilina, hauptsächlich zu Memorirübungen benutzt, 3 St.; Grammatik nach Zumpt, Repetition von Cap. 69 — 76. und Einübung von Cap. 76 — 83., mit Hülfe der Anleitung von August, Correctur der häuslichen Exercitien und Extemporalien, 4 St., Subrector Ramdohr.

2) Griechisch, 6 St.: Homeri Odyss. lib. VII. und VIII., 2 St., Conr. Dr. Seyffert; Grammatik nach Buttmann, Beendigung der Formenlehre mit Exercitien und Extemporalien, Jacobs' 2. Cursus pag. 61 — 93., 4 St., im Sommer Subr. Ramdohr, im Winter Dr. Tischer.

3) Deutsch, 2 St.: Lectüre, Erklärung und Erlernung von Gedichten aus Echtermeyer, und Aufsätze, im Sommer Dr. Wagler, im Winter Dr. Tischer.

4) Französisch, 2 St.: im Sommer Cours de leçons von Fränkel, von Michaelis an Télémaque; Exercitien nach Hirzel und Andern, Collab. Döhler.

Die vom Griechischen dispensirten Schüler wurden in besondern Lectionen unterrichtet, und zwar im Deutschen vom Director, 2 St.; im Französischen lasen sie unter Leitung des Collab. Döhler die Henriade von Voltaire, 2 St. Im Sommer ertheilte Collab. Döhler in 1 St. Unterricht im Englischen und las: The first reading von v. d. Berg.

B. Wissenschaften.

1) Religionslehre, 2 St.: Im Sommer: Marheineke's Lehrbuch: Dritter Artikel. Im Winter mit Quarta combinirt: Luther's Katechismus: drittes, viertes und fünftes Hauptstück, Director.

2) Geschichte und Geographie, 3 St.: Geschichte der alten Welt von Augustus an und Geschichte des Mittelalters nach Böttiger's Handbuch; Geographie der wichtigsten Länder der alten Welt nach dem Weimarschen Atlas der alten Welt und Geographie von Deutschland, Subr. Ramdohr.

3) Mathematik, 4 St.: im Sommer: Geometrie, 3 St: Congruenz der Dreiecke, Aehnlichkeits-Sätze; über das Ausmessen geradliniger Figuren, die einfachen Sätze vom Kreise. — 1 Stunde wöchentlich: Aufgaben über Gleichungen des ersten Grades. — Im Winter: Algebra, 3 St., die einfachen Operationen mit algebraischen Ausdrücken, Gleichungen des ersten Grades nach Meyer Hirsch; die verschiedenen Zahlsysteme nebst den Decimalbrüchen. — 1 St. wöchentlich geometrische Aufgaben, Mathem. Schönemann.

4) Physik, 2 St.: Im Sommer: Einige der einfachsten Gesetze der Statik, nebst Erklärung mehrer einfachen Maschinen. Im Winter: Repetition des vorhergehenden Cursus nebst Fortsetzung desselben, Mathem. Schönemann.

C. Technische Fertigkeiten.

Zeichnen, 2 St.: Freies Handzeichnen und architectonisch-geometrisches Zeichnen, im Sommer Mathem. Schönemann, im Winter Musikdirector Täglichsbeck.

4. Quarta.

Classenordinarien:

Im Sommer: Oberlehrer Klingenstein, nachher Candidat Wagler.

Im Winter: Collaborator Dr. Tischer.

A. Sprachen:

1) Latein, 9 St.: Corn. Nep. im Sommer Miltiad., Themist., Aristid., bei Collab. Döhler; Alcibiad. bei Oberl. Klingenstein (nachher Cand. Wagler), zusammen 4 Stunden. Im Winter Conon, Iphicr., Chabr., Timoth., Datames, 2 St., Dr. Tischer. Jacobs lat. Lesebuch VI., 3 St., Subr. Ramdohr. — Repetition der Verb. irreg., Syntax der Casus, Exercitien aus O. Schulz Aufgaben (nur im Sommer), Extemporalien und loci memoriales, im Sommer 5 St. beim Oberl. Klingenstein, nachher Cand. Wagler und Director Brautz; im Winter 4 St., Dr. Tischer.

2) Griechisch, 4 St.: Einübung der Formenlehre nach Buttmann bis zum regelmäß. Verbum incl. und Uebersetzung entsprechender Stücke aus Jacobs' Elementarbuch 1. Cursus, im Winter auch kleine Extemporalien. Im Sommer Oberl. Klingenstein, nachher Cand. Wagler; im Winter Dr. Tischer.

3) Deutsch, 2 St.: Grammatik nach Heyse's Leitfaden, orthographische Uebungen, Aufsätze, Declamiren; im Sommer Collab. Dehmel, im Winter Subr. Ramdohr.

4) Französisch, 2 St.: Müller's Lesebuch, Grammatik und Exercitien aus Fränkel's Stufenleiter, Collab. Döhler.

5) Englisch, im Sommer 1 St. Grammatik und Uebungen im Uebersetzen aus dem Deutschen ins Englische, Collab. Döhler.

B. Wissenschaften.

1) Religion, 2 St.: Im Sommer das Evangel. Matthäi, Oberl. Klingenstein, nachher Cand. Wagler; im Winter mit Tertia combinirt.

2) Geschichte und Geographie, 2 St.: Im Sommer: Geographie von Deutschland und Geschichte der Deutschen von Böttiger, Collab. Dehmel; im Winter: Geographie des preuß. Staats und preußisch-brandenburg. Geschichte nach Litzinger, Subr. Ramdohr.

3) Mathematik: Einleitung in die Geometrie, 2 St., Mathem. Schönemann; Bruchrechnung, Lehre von den Proportionen, zusammengesetzten Verhältnissen, Repartitions- und Gesellschaftsrechnung, 3 St., im Sommer Oberl. Klingenstein, nachher Cand. Wagler; im Winter Mathem. Schönemann.

4) Naturgeschichte, 1 St.: Im Sommer Botanik, besonders Anatomie der Pflanzen: im Winter Geologie, Collab. Döhler.

C. Technische Fertigkeiten.

1) Zeichnen, 2 St.: Im Sommer Mathem. Schönemann, im Winter Musikdir. Täglichsbeck.

2) Schreiben, 1 St.: Nach Vorlegeblättern von Mädler und Heinrigs, Collab. Döhler.

Die Nicht-Griechen hatten statt des griechischen Unterrichts 2 St. Französisch, Collab. Döhler, und 2 St. Deutsch, Collab. Dehmel.

5. Quinta.

Classenordinarius: Musikdirector Täglichsbeck.

A. Sprachen.

1) Latein, 9 St.: Uebersetzen aus Jacobs' Elementarbuch V. lib. I. II. III. 1 — 44., 3 St.; Einübung der regelmäßigen und unregelmäßigen Formenlehre nach D. Schulz Gramm. §. 1 — 64. und der nöthigsten Regeln der Syntax nach D. Schulz Aufgaben §. 1 — 20. nebst Anhang 1 — 15. schriftlich und mündlich, 3 St.; wöchentlich Extemporalien und Exercitien mit genauer Correctur und Besprechung derselben, 2 St.; Einübung der loci memoriales 1 — 45. nach Ruthardt, 1 St. — Musikdir. Täglichsbeck.

2) Deutsch, 4 St.: Sprachunterricht über die einfachen und zusammengesetzten Sätze nach Krause Theil 3 — 4., nebst orthographischen Uebungen, 3 St., Declamiren 1 St.; wöchentliche Correctur einer orthogr. Aufgabe und mitunter einer freieren Arbeit. — Musikdir. Täglichsbeck.

3) Französisch, 2 St.: Anfangsgründe nach Müller's franz. Lesebuche; Einübung der 4 regelmäßigen Conjugationen und des Passivs. — Prof. Heffter.

B. Wissenschaften.

1) Religionslehre, 2 St.: Lectüre des A. u. N. Testamentes; Auswendiglernen des Katechismus und biblischer Sprüche. — Prof. Heffter.

2) Geschichte, 1 St.: Alte und mittlere Geschichte nach Bredow's Tabellen. Prof. Heffter.

3) Geographie, 2 St.: Europa, Asien, Afrika, Amerika, Australien. — Prof. Heffter.

4) Rechnen, 4 St.: Rechnungen mit benannten Zahlen und die Brüche. — Im Sommersem. zuerst Oberl. Klingenstein, dann Cand. Wagler. — Im Wintersem. Dr. Tischer.

5) Naturgeschichte, 2 St.: nach v. Schubert's Lehrbuch. — Prof. Heffter.

C. Technische Fertigkeiten.

1) Freies Handzeichnen, 2 St.: Sommersem. Musikdir. Täglichsbeck. — Wintersem. Collab. Dehmel.

2) Schönschreiben, Sommersem. 3 St., Wintersem. 2 St.: nach Mädler's Vorlegeblättern. — Musikdir. Täglichsbeck.

6. Sexta a.

Classenordinarius: Collaborator III. Dehmel.

A. Sprachen.

1) Latein, 8 St.: Einübung der Formenlehre bis zu den regelmäßigen Conjugationen incl. nach D. Schulz Grammatik, Uebungen im Uebersetzen aus dem Deutschen in's Lateinische nach desselben Uebungsaufgaben I — IX. und aus dem Lateinischen in's Deutsche nach desselben Tirocinium 17 — 87; wöchentlich ein Exercitium und ein Extemporale zur Einübung der durchgenommenen Regeln. Collal. III. Dehmel.

2) Deutsch, 4 St.: Lehre vom einfachen Satz und Einiges über den zusammengesetzten Satz mit schriftlichen Uebungen nach Krause I. und II. Abth., 2 St.; Orthographie, 1 St.; Declamiren, 1 St. Collab. III. Dehmel.

3) Französisch, 2 St.: Uebungen im Lesen; die Declinationen; die Hülfszeitwörter nach Seidenstücker's Elementarbuch N. I. Collab. III. Dehmel.

B. Wissenschaften.

1) Religionslehre, 2 St.: combinirt mit Sexta b. Bibl. Gesch. d. A. u. N. Testaments nach Küster; Auswendiglernen von Liedern und Bibelversen. Professor Heffter.

2) Geschichte und Geographie, 3 St.: comb. mit Sexta b. Die wichtigsten Begebenheiten aus der allg. Weltgeschichte und das Wichtigste aus der allg. Geographie; Europa und Deutschland specieller. Collab. II. Döhler.

3) Rechnen, 4 St.: Numeriren, die 4 Species in unbenannten und benannten Zahlen, Multiplic. und Divis. Regeldetrie, Kopfrechnen. Collab. II. Döhler.

4) Naturgeschichte, 2 St.: comb. mit Sexta b. Zoologie nach Schubert's Lehrbuch. Collab. III. Dehmel.

C. Technische Fertigkeiten.

1) Schönschreiben, 3 St.: comb. mit Sexta b. Musikdir. Täglichsbeck.

2) Zeichnen, 2 St.: comb. mit Sexta b. Collab. III. Dehmel.

7. Sexta b.

A. Sprachen.

1) Latein, 5 St.: Formenlehre nach D. Schulz Tirocinium 1 — 42., 3 St., Cand. Dorscheimer; Uebung im Bilden kleiner Sätze, 2 St., Director Braut.

2) Deutsch, 7 St.: Uebungen im Lesen, Auswendiglernen kleiner Gedichte und Erzählungen, 3 St., Cand. Dorscheimer; Bildung leichter Sätze, 2 St., Director Braut; Orthographie, 2 St., Prof. Heffter.

B. Wissenschaften.

Rechnen, 2 St.: Numeriren; die 4 Species mit unbenannten Zahlen, verbunden mit Uebungen im Kopfrechnen, Collab. III. Dehmel.

Der Gesangunterricht wurde vom Musikdirector Täglichsbeck wöchentlich in 4 Stunden ertheilt:

3. Abtheilung: Einstimmiger Gesang.
2. Abtheilung: Zweistimmiger Gesang.
1. Abtheilung: Vierstimmiger Gesang.

Die erwachseneren Schüler der ersten Abtheilung, welche sich durch Lust und Liebe zum Gesang besonders hervorthaten, wurden außerdem noch zu den Uebungen des vom Musikdirector Täglichsbeck geleiteten Gesangvereins zugelassen.

II. Verordnungen der hohen Königl. Behörden.

Circular-Verfügung des Königl. Schul-Collegiums vom 2. Februar 1843.

Mit Bezug auf unsere Circular-Verfügung vom 15. September v. J. (S. 4766.) und in Folge einer ausdrücklichen Bestimmung des Herrn Geheimen Staats Ministers Eichhorn Excellenz, machen wir Ew. Wohlgeboren darauf aufmerksam, daß, wenn die Verhältnisse es nicht rathsam machen sollten, besondere von den öffentlichen Prüfungen getrennte Rede-Actus regelmäßig abzuhalten, es den Eifer der Jugend für Rede-Uebungen doch sehr anregen wird, wenn von Zeit zu Zeit und etwa halbjährlich einmal einer Auswahl der Schüler aus allen Klassen Gelegenheit gegeben würde, einzelne Reden und Declamationen, die in der Klasse schon eingeübt und vorgetragen sind, vor dem versammelten Lehrer-Collegium vorzutragen.

Sie wollen an der Ihrer Leitung anvertrauten Anstalt hierzu die erforderliche Einleitung treffen und über den Erfolg sich in dem nächsten Jahres-Berichte äußern.

Circular-Verfügung des Königl. Consistoriums und Schul-Collegiums vom 25. Februar 1843.

Des Königs Majestät haben in einer Allerhöchsten Cabinets-Ordre vom 12. Mai 1841 hinsichtlich des Schuldenmachens der Beamten zu erklären geruht, wie Allerhöchst Dieselben es nicht dulden können, daß Beamte den ihnen von ihren Gläubigern, insbesondere von Handwerkern gegebenen Credit mißbrauchen und sich bei der Execution durch das Privilegium der Abzugsfreiheit ihres Gehalts schützen; Allerhöchst Dieselben wollen vielmehr, daß gegen solche Beamte die Bestimmungen in §. 8. und folgende der Verordnung vom 28. Februar 1806 (Mylius Edictensammlung de 1806 pag. 59. seq.) mit aller Strenge zur Anwendung gebracht, und dieselben demgemäß Allerhöchst Ihnen angezeigt werden sollen, um nach Bewandtniß der Umstände ihre Entlassung zu verfügen. Diese Bestimmung soll nach Allerhöchstem Befehl den Beamten bekannt gemacht, und auf die Befolgung mit Nachdruck gehalten werdrn.

Nach Höherer Vorschrift findet dieselbe auch auf Lehrer Anwendung. Ew. Wohlgeboren veranlassen wir daher, die Allerhöchste Anordnung den Lehrern des dortigen Gymnasiums, welchen die Vorschrift des §. 160. des Anhangs zur allgemeinen Gerichtsordnung:

daß gegen diejenigen Beamten, welche nur 400 Rthlr. oder weniger Diensteinkünfte haben, kein Arrestschlag gestattet werden soll,

zu statten kommt, bekannt zu machen.

Circular-Verfügung des Königl. Schul-Collegiums vom 24. März 1843.

Des Königlichen Geheimen Staats-Ministers Herrn Eichhorn Excellenz haben, wenngleich ihm über die Erfolge der vorzugsweise in mehreren Gymnasien angewandten Ruthardtschen Methode erst die Berichte einiger Provinzial-Schul-Collegien vorlagen, und er der Ansicht ist, daß ein hinreichend begründetes Urtheil über diese Methode erst dann gewonnen werden kann, wenn dieselbe mit Schülern der Quinta bis zur Prima durchgeführt sein wird, sich durch die in wesentlichen Punkten auffallende Uebereinstimmung jener Berichte veranlaßt gesehen, auf den Grund der vorliegenden Resultate für die Fortsetzung oder Einführung der Memorir-Uebungen schon jetzt einige allgemeine Bestimmungen zu treffen.

Ist nämlich auch der Grundgedanke der Ruthardtschen Methode nicht neu, so gebührt dem Ruthardt doch das Verdienst, die den Gedächtniß-Uebungen auch bei dem Unterricht der alten Sprachen zu widmende Aufmerksamkeit von Neuem aufs lebhafteste angeregt, und das Nachdenken der Schulmänner auf eine zweck- und planmäßige Einrichtung derselben hingelenkt zu haben.

Ueberall, wo die Sache von den Lehrern mit Eifer und Liebe aufgefaßt worden, hat sich bei den Schülern auch lebhafte Theilnahme und eine große Vorliebe für diese Uebungen gezeigt; die Lebendigkeit und Selbstthätigkeit derselben ist in hohem Grade angeregt, ihre grammatische und stylistische Bildung eben sowohl, als geläufiges Verständniß der Klassiker gefördert worden. Dieser Gewinn ist so bedeutend, und wenn bei den Memorir-Uebungen das rechte Maaß gefunden und angewandt wird, mit so geringem Zeit- und Kraftaufwande zu erreichen, daß sich fast alle Gymnasial-Directoren für ein methodisch geordnetes Memoriren, wenn auch nur sehr wenige unbedingt für die Ruthardtschen Vorschläge, ausgesprochen, mehrere vielmehr die denselben eigenthümlichen Punkte in ihrer Anwendung, besonders in zahlreichen Klassen, als erfolglos und die meisten seine loci memoriales als nicht brauchbar bezeichnet haben.

Wenn nun der Unterricht in den alten Sprachen in der auf Einübung der Grammatik, auf Lectüre und Stylübungen ruhenden Lehrweise auch künftig, wie bisher, gegründet bleiben soll, so sind doch von jetzt an mit demselben, und zwar zunächst bei dem lateinischen Unterrichte, regelmäßige, methodisch geordnete Memorir-Uebungen in einer bestimmten, wöchentlich wiederkehrenden Zeit zu verbinden, und die erlernten Sätze und größeren Abschnitte mit Beachtung der Grundgedanken der Ruthardtschen Vorschläge unter den verschiedensten Gesichtspunkten zu wiederholen und alle Uebungen bei dem lateinischen Unterrichte auf dieselben zu beziehen. Hierdurch wird nicht allein für den lateinischen Unterricht eine concrete Grundlage gewonnen, sondern das in diesen Memorir-Uebungen liegende didactische Princip wird zugleich auf die bei der Einübung der Grammatik zu befolgende Methode wohlthätig zurückwirken, und für jüngere Lehrer die Weisung enthalten, bei dem grammatischen Unterrichte in den unteren und mittleren Classen nicht mit der abstracten Regel zu beginnen, sondern dieselbe erst in verschiedenartigen Beispielen anschaulich erkennen, dann für sie den passenden Ausdruck finden, und in einem schicklich gewählten Beispiel der Grammatik oder der loci memoriales festhalten zu lassen, dabei sich des frühern Philosophirens zu enthalten, vielmehr durch vielseitige Uebungen die unumgänglich nothwendige Sicherheit in ihren Schülern zu begründen. Die Grundgedanken der Ruthardtschen Methode sind in dem beigefügten Exemplare eines von Ruthardt selbst verfaßten Aufsatzes kurz und bestimmt ausgesprochen, welcher den Lehrer-Collegien zu wiederholter Erwägung und Berücksichtigung mitzutheilen ist. Es bleibt denselben anheim gestellt, bei den Memorir-Uebungen entweder die loci memoriales von Ruthardt, oder die von Meiring und Remacly herausgegebene Sammlung zum Grunde zu legen, oder in den untern Classen aus den in den eingeführten Grammatiken selbst enthaltenen Beispielen die passenden auszuwählen, in denjenigen Classen aber, in welchen einzelne Schriften classischer Autoren gelesen werden, größere Abschnitte von bedeutendem Inhalte einprägen zu lassen. Indem hiernach den einzelnen Gymnasien freigestellt bleibt, in der Weise zu verfahren, welche sie für die fruchtbringendste halten, ist denselben doch zur Pflicht zu machen, den ganzen Stoff zu Anfange des Schuljahrs nach gemeinsamer Berathung auszuwählen und innerhalb derselben Anstalt ein consequentes und bewußtes Verfahren zu Grunde zu legen. Da der volle Gewinn, welcher aus diesen Memorir-Uebungen hervorgehen kann, nur dann zu erreichen ist, wenn sämmtliche Lehrer denselben Lernstoff aller Classen beherrschen und zur Anwendung bringen, so wird nach Möglichkeit darauf zu halten sein, daß der Lehrer des Lateinischen seine Schüler wenigstens auf der unteren und eben so auf der mittleren Bildungsstufe behalte, also von Sexta zur Quinta, und von Quarta zur Tertia mit ihnen aufsteige.

Wo bereits Memorir-Uebungen genau nach den Ruthardtschen Vorschlägen eingeführt worden, da sind dieselben einstweilen fortzusetzen und bis in die obersten Classen durchzuführen, damit das Eigenthümliche derselben genau erkannt und sein Werth nach den in der Anwendung gewonnenen Resultaten beurtheilt werden könne.

Mit Beziehung auf die vorstehenden Bestimmungen verpflichten wir Ew. Wohlgeboren im Auftrage des Königlichen Geheimen Staats-Ministers Herrn Eichhorn Excellenz, diesen Uebungen, in welcher Weise sie auch angestellt werden mögen, Ihre fortgesetzte, sorgfältige Aufmerksamkeit zu widmen, sich von ihren Resultaten selbst zu überzeugen, und in den Jahresberichten sich sowohl über die Art der Ausführung, als auch über die wahrgenommenen Erfolge ausführlich auszusprechen. Was übrigens die bei den Memorir-Uebungen zu Grunde zu legende Stoffsammlung betrifft, so haben Sr. Excellenz angeordnet, daß die Aufstellung derselben Memorir-Abschnitte für sämmtliche Gymnasien und Progymnasien einer Provinz vorbereitet werde. Demgemäß und in Berücksichtigung, daß sich die loci memoriales des pp. Ruthardt bei den in seiner Methode angestellten Versuchen als nicht brauchbar erwiesen und die von Meiring und Remacly herausgegebene Sammlung sich zu einer allgemeinen Einführung ebenfalls nicht zu eignen scheint, ist es uns wünschenswerth, wenn der eine und andere Gymnasiallehrer von den Herren Directoren veranlaßt würde, eine eigene dem Zwecke entsprechende Stoffsammlung auszuarbeiten und demnächst uns zur weiteren Beschlußnahme einzureichen.

Cir-

Circular-Verfügung des Königl. Schul-Collegiums vom 9. März 1843.

Des Königlichen Geheimen Staats-Ministers Herrn Eichhorn Excellenz, dem wir in Betreff der körperlichen Züchtigungen bei den Gymnasien Vortrag gehalten haben, hat uns veranlaßt, in einer an die Gymnasial-Directoren und Rectoren zu erlassenden Verfügung die Grundsätze auszusprechen, welche bei Ausübung jenes Strafrechts zu beachten sind. Ew. Wohlgeboren eröffnen wir daher mit Bezugnahme auf den §. 12. der Instruction für die Directoren und Rectoren der gelehrten Schulen der Provinz Brandenburg vom 10. Juni 1824, daß es das Streben der Directoren und der Lehrer der Gymnasien sein muß, durch eine ernste Disciplin und eine zweckmäßige Benutzung der übrigen Strafmittel die körperlichen Züchtigungen in den Gymnasien möglichst entbehrlich zu machen, und es bei Anwendung dieses Strafmittels als Grundsatz gelten muß, daß bei körperlichen Züchtigungen der Schüler, mehr der moralische Eindruck der Strafe, als der körperliche Schmerz die Besserung des zu Bestrafenden bewirke.

Um dies zu bewirken wird den Herren Directoren und Rectoren empfohlen, daß sie nur denjenigen Lehrern, auf deren pädagogische Einsicht und Besonnenheit überhaupt und auf deren Mäßigung beim Strafen im Besonderen sie sich verlassen zu können glauben, jene Strafgewalt anvertrauen, und die mit derselben versehenen Lehrer anweisen, im Allgemeinen nur in den seltensten Fällen gleich nach dem Vergehen des Schülers, und auch nur dann an demselben eine korperliche Züchtigung zu vollziehen, wenn die Beschämung, welche er dadurch vor seinen Mitschülern erleidet, als nothig für seine Besserung erscheint oder überhaupt ein Aufschub der Strafe die wohlthätige Wirkung derselben vermindern würde, und die körperliche Züchtigung so auszuführen, daß in keiner Weise aus derselben irgend ein Nachtheil für die Gesundheit des Knaben erwachsen konne. In Rücksicht hierauf kann es nicht gestattet werden, daß bei solchen Bestrafungen andere Strafwerkzeuge als ein dünnes Rohrstöckchen oder eine Ruthe in Anwendung kommen. Auch werden die Lehrer auf die Verantwortlichkeit aufmerksam zu machen sein, welche sie in dem Falle haben, wenn eine solche Bestrafung der Gesundheit des Knaben nachtheilig wird, und ist event. von einem jeden Mißbrauch der Art uns sofort Anzeige zu erstatten. Was die Bestrafungen der Schüler durch Schuldiener betrifft, so sind sie, weil sie nur allzuleicht den Character einer polizeiartigen Züchtigung annehmen, im Allgemeinen unstatthaft, und wenn es sich vielleicht auch bei einzelnen gröberen Vergehen jüngerer Knaben rechtfertigen ließe, daß die Züchtigung auf den Beschluß der Conferenz oder des Directors in Gegenwart des Letzteren durch einen Schuldiener mit der Ruthe oder einem dünnen Rohrstöckchen vollzogen wird, so müßte dies doch stets als eine höchst seltene Ausnahme zu betrachten seyn, und würde in Rücksicht auf das Alter des Schülers und die Natur des Vergehens vor der Anwendung einer solchen Züchtigung zu erwägen sein, ob nicht, wenn von anderen Strafen ein Erfolg nicht zu erwarten ist, die Ausschließung aus der Schule in Anwendung zu bringen sei. In hohem Grade ist es in dieser Hinsicht zu mißbilligen, daß eine derartige Züchtigung, wie es an einigen Gymnasien geschehen ist, als Folge einer Anzahl von tadelnden Noten im Klassen-Tagebuche eintritt. Ueberhaupt wird es zweckmäßig sein, eine solche Bestrafung nur mit Vorwissen und Zustimmung der Eltern vollziehen zu lassen.

Nach Maaßgabe dieser Grundsätze wollen Sie sich über angemessene Ausübung des Rechts zu körperlichen Züchtigungen mit den Lehrern der Ihrer Leitung anvertrauten Anstalt einigen und dieselben stets sorgsam überwachen.

Circular-Verfügung des Königl. Schul-Collegiums vom 7. April 1843.

In Folge höherer Veranlassung ist unterm 12. August 1824 in Beziehung auf die Beaufsichtigung derjenigen Schüler der Gymnasien, deren Eltern, Vormünder oder Pfleger nicht an dem Orte des Gymnasii wohnen, Folgendes festgesetzt worden:

1) Jeder Schüler eines Gymnasii muß; wenn seine Eltern, Vormünder oder Pfleger nicht an dem Orte des Gymnasii wohnen, von diesen zur besondern Fürsorge einem tüchtigen Aufseher übergeben sein, der dem Director oder Rector des Gymnasii bei der Aufnahme des Schülers namhaft zu machen ist, und welcher über seinen Privatfleiß und sein sittliches Betragen außer der Schule, eine ernste und gewissenhafte Aufsicht zu führen hat;

2) ein jeder der gedachten Schüler hat dem Director oder Rector des Gymnasii die Wohnung, welche er in der Stadt zu beziehen gedenkt, bei seiner Aufnahme anzuzeigen;
3) in einem Wirthshause zu wohnen oder seine Kost an der Wirthstafel zu nehmen, ist keinem solchen Schüler verstattet;
4) er darf während seines Aufenthalts im Gymnasio nicht seinen Aufseher oder seine Wohnung wechseln, ohne vorherige Anzeige bei dem Director oder Rector des Gymnasii und ohne ausdrückliche Genehmigung desselben.

Mehrere wegen dieses Gegenstandes an uns ergangene Anfragen veranlaßten uns, diese Anordnung unter Zustimmung des Königlichen Ministeriums der geistlichen ꝛc. Angelegenheiten durch eine Circular-Verfügung vom 20. April 1833 auf folgende Weise näher zu bestimmen:

1) In Gymnasien und ähnliche höhere Lehranstalten können nur solche junge Leute aufgenommen werden, welche unter der Aufsicht ihrer Eltern oder Vormünder oder anderer zur Erziehung junger Leute geeigneter Personen stehen. Schüler, welche ohne geeignete Aufsicht sind, sollen auf Gymnasien und höheren Lehranstalten nicht geduldet werden.
2) Bei der Aufnahme junger Leute, deren Eltern oder Vormünder nicht am Orte wohnen, haben die Directoren der Gymnasien sich nachweisen zu lassen, auf welche Weise für die Beaufsichtigung derselben gesorgt ist. Halten sie die getroffenen Einrichtungen nicht für ausreichend, so haben sie dies den Eltern oder Vormündern zu eröffnen und darauf zu halten, daß eine anderweitige dem Zwecke entsprechende Einrichtung getroffen werde.
3) Ohne Vorwissen des Directors darf kein Schüler in eine anderweitige Aufsicht gegeben werden.
4) Der Director ist so berechtiget als verpflichtet, von dem häuslichen Leben auswärtiger Schüler entweder unmittelbar oder durch Lehrer der Anstalt Kenntniß zu nehmen, und wenn sich hierbei Uebelstände ergeben sollten, auf deren unverzügliche Abstellung zu dringen.
5) Findet der Director, daß die Aufsicht, unter welche auswärtige Schüler gestellt worden, unzureichend ist, oder daß die Verhältnisse, in welchen sie sich befinden, ihrer Sittlichkeit nachtheilig sind, so ist er berechtigt und verpflichtet, von den Eltern oder Vormündern eine Aenderung dieser Verhältnisse binnen einer nach den Umständen zu bestimmenden Frist zu verlangen.
6) Eltern und Vormünder, welche ihre Söhne oder Pflegebefohlenen Behufs ihrer Aufnahme in ein Gymnasium in Kost und Pflege geben, sind verpflichtet, diese Bestimmungen zu beachten und die Aufseher ihrer Söhne und Pflegebefohlenen von selbigen in Kenntniß zu setzen. Es bleibt auch lediglich ihnen überlassen, für den Fall, daß eine Aufhebung des Verhältnisses von der Anstalt verlangt werden möchte, mit den Aufsehern ihrer Kinder und Pflegebefohlenen die erforderlichen Verabredungen zu treffen.

Indem wir diese Bestimmungen den Herren Gymnasial-Directoren und Rectoren in Erinnerung bringen, veranlassen wir zugleich im Auftrage Seiner Excellenz des Königlichen Geheimen Staats-Ministers Herrn Eichhorn die Herren Directoren der hiesigen höheren Bürgerschulen die hier ausgesprochenen Bestimmungen auch hinsichts der auswärtigen Zöglinge der unter ihrer Leitung stehenden Anstalten zu befolgen.

Circular-Verfügung des Königl. Schul-Collegiums vom 6. Mai 1843.

Es ist die Erfahrung gemacht worden, daß der Unterricht in der Muttersprache in den untern und mittlern Klassen höherer Lehranstalten häufig in ganz zweckwidriger Weise ertheilt wird. Namentlich ist dem theoretisch-grammatischen Unterricht in derselben unter dem Namen „Sprachdenklehre" oder auch unter anderen Namen oft eine Gestalt gegeben, welche durch abstruse Terminologieen und durch dürre gehaltlose Uebungtn den jugendlichen Geist weit öfter abstumpft, als wahrhaft bildet, den Zweck lebendiger Anschauung der Muttersprache in gehaltvollen, Geist und Gemüth bildenden Musterstücken und sicherer Aneignung der Sprache zu geläufigem und correctem schriftlichen und mündlichen Gebrauch öfter hemmt als fördert, und somit einer inhaltsvollen, den Geist selbst mit gesunder frischer Nahrung für das ganze Leben erfüllenden Bildung der Jugend nicht nur die Zeit und Kraft des Lehrers wie der Schüler entzieht, sondern auch derselben durch ein todtes Formelwesen positiv nachtheilig wird.

Je weniger sich bis jetzt die verschiedenen Ansichten über die Ertheilung des deutschen Unterrichts in den höheren Lehranstalten geeinigt haben, desto nothwendiger ist es nach der Ansicht des Königlichen Geheimen Staats-Ministers Herrn Eichhorn Excellenz, diejenigen Versuche aus denselben fern zu halten, welche durch die Erfahrung sowohl als durch eine richtige Würdigung derselben als unfruchtbar oder gar nachtheilig erkannt werden. Dahin gehört nach der Ansicht Seiner Excellenz der in manchen Anstalten übliche theoretische grammatische Unterricht in der Muttersprache, welcher die deutsche Sprache den Schülern gegenüber gleichsam als eine fremde erst noch zu erlernende betrachtet, oder die natürlichen Aeußerungen der Sprachthätigkeit von dem Standpunkte eines philosophischen grammatischen Systems und zu einer bewußten zu erheben sucht und häufig schon in der Behandlung des Gegenstandes von Seiten des Lehrers, sowie in der sich kundgebenden Theilnamlosigkeit der Schüler seine Unzweckmäßigkeit zu erkennen giebt. Während der lateinische Unterricht am natürlichsten Gelegenheit darbietet, den Kindern an dieser ihnen fremden Sprache grammatische Formen und Verhältnisse anschauen und auffassen zu lassen und sie bei fortschreitender Entwickelung anzuleiten, die so erworbenen Kenntnisse allmählich und besonders, wenn ihnen das Verständniß der an Formen und feinen Unterscheidungen noch reicheren griechischen Sprache eröffnet wird, zu solchen zu erheben, welche auf dem sprachlichen Gebiete allgemeine Gültigkeit haben, billigt Seine Excellenz die Ansicht, daß der deutsche Unterricht überall die Aufgabe zu verfolgen habe, die Muttersprache in geeigneten, für das jedesmalige Alter der Schüler angemessenen Musterstücken zur lebendigen Anschauung zu bringen und dadurch die sichere Aneignung der Sprache zu fördern, und ist der Meinung, daß, wenn auf diese Weise die natürliche Sprachentwickelung unterstützt wird, es niemals an Veranlassung fehlen würde, beim Lesen das Fehlerhafte in der Aussprache zu entfernen, auf die richtige Formenbildung aufmerksam zu machen, die Orthographie zu befestigen, Natürlichkeit und Wahrheit des Ausdrucks zu befördern, überhaupt das Sprachgefühl ohne ein dürres Analysiren der einzelnen Wörter und Sätze immer mehr auszubilden und zu schärfen.

Indem wir Ew. Wohlgeboren hierdurch auf die bei der Ertheilung des deutschen Unterrichts zu vermeidenden Mißgriffe aufmerksam machen, empfehlen wir zugleich im Auftrage des Königlichen Geheimen Staats-Ministers Herrn Eichhorn Excellenz Ihnen und dem Lehrer-Collegium der Ihrer Leitung anvertrauten Anstalt, außer der Schrift von R. H. Hiecke, auf welche wir Sie bereits mittelst Verfügung vom 14. Februar v. J. aufmerksam gemacht, das in dem 4. Theile des von Ph. Wackernagel in Stuttgart herausgegebenen Lesebuches enthaltene Gespräch über den Unterricht in der Muttersprache und die in dem Programme des Gymnasiums zu Duisburg pro 1842 enthaltene Abhandlung des Gymnasial-Lehrers Hülsmann zur Erwägung und Beachtung.

Circular-Verfügung des Königl. Schul-Collegiums vom 8. Juni 1843.

Des Königs Majestät haben neuerdings anzuordnen geruhet, daß dem Schuldenmachen der Beamten fortwährend möglichst entgegengewirkt werde.

Nach einer demgemäß ergangenen Bestimmung des Königlichen Ministeriums der geistlichen ꝛc. Angelegenheiten soll auch in dessen Ressort dem Schuldenmachen überall durch Ermahnungen zu einer sparsamen, dem Einkommen entsprechenden Lebensweise und durch sonstige angemessene Vorhaltungen entgegengewirkt, und dergleichen Ermahnungen und Warnungen sollen vorzüglich den neu Angestellten bei Gelegenheit ihrer Diensteinführung ertheilt, und wenn sich ergeben möchte, daß solche nicht beherzigt werden, wiederholt, gegen unverbesserliche und leichtsinnige Schuldenmacher aber nach der Strenge der Gesetze eingeschritten werden.

Ew. Wohlgeboren setzen wir von diesen Bestimmungen mit dem Auftrage in Kenntniß, solche den Lehrern der Anstalt bekannt zu machen, dieselben vor leichtsinnigem Schuldenmachen zu verwarnen, und bei neuen Anstellungen von Lehrern demgemäß zu verfahren.

Circular-Verfügung des Herrn Ober-Präsidenten. In dessen Abwesenheit und Auftrag des Herrn Regierungs-Vice-Präsidenten. Vom 29. Juni 1843.

Junge Leute, welche zum einjährigen freiwilligen Militairdienste zugelassen zu werden wünschen, mußten, nach den seitherigen Bestimmungen, sich vor dem ersten August des Jahres, in welchem die Altersklasse, zu der sie gehörten, zum ersten Male zur Ersatzaushebung concurrirte, bei einer der Commissionen melden, welche zur Prüfung einjähriger Freiwilliger für die

Stadt Berlin und den hiesigen Regierungsbezirk in Berlin, für den Frankfurter Regierungsbezirk in Frankfurt niedergesetzt sind. Der Erlaß meines Herrn Amtsvorgängers vom 5. September 1826 (No. 1442. O. P.) hat Sie mit den dosfallsigen Vorschriften bekannt gemacht.

Durch Rescript der Königlichen Ministerien des Krieges und des Innern vom 15. April d. J. ist nun, im Zusammenhange mit Bestimmungen wegen alljährlicher Beendigung der Geschäfte der Kreis-Ersatz-Kommissionen, der vorbezeichnete Termin dahin abgeändert worden, daß sich die Eingangs gedachten jungen Leute künftighin schon vor dem ersten Mai des Jahres, in welchem sie zwanzig Jahre alt werden, bei der betreffenden Departements-Prüfungs-Commission zu melden haben.

Da die Unterlassung der rechtzeitigen Meldung den Verlust der Wohlthat des einjährigen freiwilligen Militairdienstes nach sich zieht, so gebietet es die Rücksicht auf das Wohl der Ihrer Leitung anvertrauten Schüler, dieselben auf ihre Militairpflicht überhaupt, sowie auf den vorbezeichneten abgeänderten Termin, die nachtheiligen Folgen dessen Nichtbeachtung und die Pflicht der rechtzeitigen Meldung insbesondere noch vor Erreichung ihres militairpflichtigen Alters eindringlichst aufmerksam zu machen.

Circular-Verfügung des Königl. Schul-Collegiums vom 30. Juni 1843.

Nach einem Erlasse des Königl. Geheimen Staats-Ministers Herrn Eichhorn Excellenz ist bemerkt worden, daß die Directoren der Gymnasien und anderer höherer Lehranstalten die Einführung neuer Lehrbücher oft ohne Weiteres veranlaßt haben. Wir machen daher die Herren Directoren und Rectoren der gedachten Anstalten auf die Bestimmungen der Dienst-Instruction für die Provinzial-Consistorien vom 23. October 1817 §. 7. No. 4. und 5. (cf. Gesetzsammlung pro 1817 pag. 240.) aufmerksam, und geben demzufolge und mit Beziehung auf unsere Verfügung vom 26. Januar 1833 denselben auf, zu jeder Einführung eines neuen Lehrbuchs unsere Bestimmung einzuholen.

Circular-Verfügung des Königl. Schul-Collegiums vom 27. December 1843.

Von Seiten eines der Königlichen Provinzial-Schul-Collegien ist in einer Circular-Verfügung an die Gymnasial-Directoren bestimmt worden, daß den Abiturienten, welche in der Zeit zwischen der Abiturienten-Prüfung und der förmlichen Entlassung erhebliche Vergehen gegen die Schul-Ordnung sich zu Schulden kommen lassen und durch ihr Verhalten Zweifel erregen, ob sie in sittlicher Beziehung für die selbstständigere Stellung auf der Universität hinreichend gereift sind, das Zeugniß der Reife vorenthalten und demnächst die Entscheidung des Provinzial-Schul-Collegii eingeholt werden solle, ob den Abiturienten das Zeugniß der Reife für's Erste abgesprochen werden müsse, und binnen welcher Frist gestattet werden könne, durch beigebrachte Beweise untadeligen Verhaltens und durch abermalige Prüfung das Zeugniß der Reife zu erwerben.

Des Königlichen Geheimen Staats-Ministers Herrn Eichhorn Excellenz hat, weil diese Bestimmung mit dem Abiturienten-Prüfungs-Reglement vom 4. Mai 1831 nicht in Uebereinstimmung steht, es für zureichend erachtet, daß das den Abiturienten nach der Prüfung zuerkannte Zeugniß rücksichtlich des Urtheils über Fleiß und Betragen abgeändert werde, wenn der Abiturient zwischen der Prüfung und der förmlichen Entlassung sich über die Schulordnung in strafbarer Weise hinweggesetzt hat, indem zur Beseitigung solcher immer nur selten vorkommenden Unordnungen die Autorität des Directors und der Lehrer, so wie ihr erziehender Einfluß auf die Schüler schon ausreichen werde.

Um indeß diese in ihren Bemühungen zu unterstützen, haben Se. Excellenz angeordnet, daß die Abiturienten-Prüfungen möglichst nahe vor dem Schluß des Schul-Semesters abgehalten und von den Königlichen Prüfungs-Commissarien den Abiturienten bei der Bekanntmachung noch besonders an's Herz gelegt werde, bis zu ihrer Entlassung den ihnen gegen die Schule obliegenden Verpflichtungen pünktlich nachzukommen und durch Vernachlässigung derselben eine ihrem Zeugnisse beizufügende Rüge nicht zu veranlassen; auch habe es in dieser Beziehung kein Bedenken, daß die Herren Directoren bei dem feierlichen Entlassungs-Acte nach Befinden der Umstände die Namen derer, welche nach der Abiturienten-Prüfung sich nicht ordnungsmäßig benommen haben, öffentlich nennen.

Indem wir von diesen Anordnungen hierdurch den Herren Directoren der Gymnasien der Provinz Brandenburg zur Nachachtung Kenntniß geben, veranlassen wir Ew. Wohlgeboren sorgfältig darüber zu wachen, daß die oft mit den nachtheiligsten und traurigsten Folgen verbundenen Trinkgelage, welche die Abiturienten, wie uns bekannt geworden, theils nach der schriftlichen, theils nach beendigter mündlicher Prüfung, sogar mit Zuziehung von Studirenden und Schülern der obern Classen zu veranstalten pflegen, abgestellt werden, und beauftragen Sie, uns anzuzeigen, ob dergleichen Gelage bei der unter Ihrer Leitung stehenden Anstalt in den letzten Jahren gehalten worden sind und event., welche Mittel Sie zu deren Abstellung angewandt haben, oder noch anzuwenden beabsichtigen.

Circular-Verfügung des Königl. Schul-Collegiums vom 29. Februar 1844.

Des Königlichen Geheimen Staats-Ministers Herrn Eichhorn Excellenz haben, nach näherer Kenntnißnahme von dem gegenwärtigen Zustande der verschiedenen bereits bestehenden Turnanstalten, sich veranlaßt gesehen, Behufs der weitern Ausführung der Allerhöchsten Ordre vom 6. Juni 1842, mittelst welcher Seine Majestät der König zu genehmigen geruht haben, daß die Leibesübungen als ein nothwendiger und unentbehrlicher Bestandtheil der männlichen Erziehung in den Königlichen Staaten förmlich anerkannt werden sollen, die Gesichtspunkte näher festzustellen, nach welchen den bereits vorhandenen Turnanstalten eine allgemeinere Verbreitung und bestimmtere Richtung zu geben und überhaupt diese wichtige Angelegenheit zu behandeln ist.

1) Um der landesväterlichen Absicht Seiner Majestät des Königs gemäß, durch eine harmonische Ausbildung der geistigen und körperlichen Kräfte dem Vaterlande tüchtige Söhne zu erziehen und alles möglichst entfernt zu halten, was nach den bis jetzt gemachten Erfahrungen physische und moralische Nachtheile bei der Behandlung des Turnwesens zur Folge haben könnte, ist die Gymnastik überall auf den einfachen Zweck zu beschränken, daß der menschliche Körper mit seinen Kräften durch eine angemessene, den verschiedenen Lebensaltern, Ständen und Lebenszwecken der Jugend entsprechende Reihenfolge von wohlberechneten Uebungen ausgebildet und befähigt werde, in jeglicher Beziehung des sittlichen Lebens der Diener und Träger des ihm einwohnenden Geistes zu seyn.

2) Aus diesem nicht nur auf die Entwickelung und Stärkung der körperlichen Kräfte, sondern auch auf Anstand, Ausdruck und gefällige Form der Bewegungen gerichteten und mit der Wehrpflichtigkeit jedes Preußischen Unterthans innig verbundenen Zwecke der Gymnastik folgt, daß, da die Ausbildung des Geistes und des zum Dienste desselben bestimmten Leibes nach den eigenthümlichen Anlagen jedes einzelnen Menschen die Aufgabe jeglicher Erziehung ist, die Gymnastik sich, wie der Körper dem Geiste, so auch dem die Ausbildung der geistigen Kräfte des Menschen bezweckenden Unterrichte überall unterordnen und sich den Verfügungen, durch welche dieser geleitet wird, unbedingt unterwerfen muß. Die Gymnastick, wenn sie in diesem natürlichen und richtigen Verhältnisse zu der geistigen Ausbildung und den dieselbe beabsichtigenden Mitteln erhalten wird, bildet in dem System des Unterrichts ein ebenso nothwendiges als nützliches Glied. Sie darf jetzt in demselben um so weniger fehlen, je mehr besonders in den höheren Ständen der bürgerlichen Gesellschaft die Forderungen, welche an die geistige Ausbildung gegenwärtig gemacht werden und nach dem Entwickelungsgange und jetzigen Standpunkte der Bildung gemacht werden müssen, im Vergleich mit früheren Zeilen gesteigert worden, je größere Anstrengungen der geistigen Kräfte zur Erfüllung dieser Forderungen unvermeidlich sind, und je dringender es daher ist, durch die Aufnahme der Gymnastik in den Kreis der öffentlichen Unterrichtsgegenstände ein Gleichgewicht aufzustellen, welches die körperliche Gesundheit erhalten und befördern und diese vor jeglicher bei der erhöhten geistigen Anstrengung möglichen Gefährdung schützen und schirmen könne.

3) Diese Maaßregel ist für jetzt auf die Jugend in den Städten zu beschränken und soll vorläufig mit jedem Gymnasium, jeder höheren Stadtschule und jedem Schullehrer-Seminar eine Turnanstalt verbunden werden, welche nicht als etwas für sich Bestehendes, sondern vielmehr als eine die Schule und ihr Geschäft ergänzende und fördernde Einrichtung zu betrachten und folglich mit der Schule, zu welcher sie gehört, in eine vollkommene Uebereinstimmung zu bringen und in solcher sorgfältig zu erhalten ist.

4) Ueberall und hauptsächlich in den größeren Städten ist darauf Bedacht zu nehmen, daß jedes Gymnasium und jede höhere Bürgerschule auch eine besondere nur für die Jugend der betreffenden Schule bestimmte Turnanstalt und somit jede derselben ihr gedecktes und geschlossenes Turnhaus für die Uebungen im Winter und bei sonst ungünstiger Witterung, und ihren eigenen Turnplatz im Freien erhalte. Wo dies wegen erheblicher Ursachen nicht wohl ausführbar ist, kann indeß auch eine und dieselbe Turnanstalt zugleich für ein Gymnasium und eine höhere Bürgerschule und nöthigenfalls selbst für mehrere Schulen dieser Art zur gemeinschaftlichen Benutzung bestimmt und eingerichtet werden. Die näheren Bedingungen, unter welchen eine solche gemeinschaftliche Benutzung einer Turnanstalt zulässig ist, werden zu seiner Zeit noch festgestellt werden.

5) Auch fernerhin soll, wie bisher, die Theilnahme der Jugend an den Leibesübungen lediglich von dem freien Ermessen der Eltern oder Stellvertreter abhängig bleiben. Hierbei ist von den Directoren, Vorstehern und Lehrern der Gymnasien, höheren Bürgerschulen und Schullehrer-Seminarien vertrauungsvoll zu erwarten, daß sie ihrerseits bereitwillig zur Beförderung des gymnastischen Unterrichts mitwirken, durch zweckmäßige Einrichtung desselben die Gleichgültigkeit und selbst die Abneigung, mit welcher viele die Gymnastik betrachten, allmählich beseitigen, und für dieselbe sowohl bei ihren Schülern, als auch bei deren Eltern die Theilnahme erwecken werden, ohne welche sie nicht zu einer gedeihlichen Entwickelung gelangen kann.

6) Die bisherige Erfahrung hat ergeben, daß die Gymnastik mit gutem Erfolge und mit erfreulicher Theilnahme auch von Seiten der bereits erwachsenen Schüler besonders in den Anstalten betrieben wird, wo der gymnastische Unterricht einem wissenschaftlich gebildeten Lehrer eines Gymnasiums oder einer höheren Bürgerschule, der zugleich als ordentlicher Classenlehrer fortwährend Gelegenheit hat, die Schüler näher kennen zu lernen und auf sie in allen wesentlichen Beziehungen einzuwirken, anvertraut worden. Auf Grund dieser Erfahrung und zur Verminderung der durch die Turnanstalten erwachsenden Kosten ist die Annahme von Lehrern, welche bloß zur Ertheilung des gymnastischen Unterrichts befähigt und nur mittelst desselben ihren Lebensunterhalt zu gewinnen genöthigt sind, möglichst zu vermeiden; vielmehr ist die unmittelbare Leitung der gymnastischen Uebungen in der Regel einem ordentlichen Lehrer und zwar der oberen Classe der betreffenden gelehrten oder höheren Bürgerschule zu übertragen. Zu dem Ende ist von jetzt an bei der Wiederbesetzung erledigter Lehrstellen an Gymnasien, höheren Bürgerschulen und Schullehrer-Seminarien auch die Rücksicht zu nehmen, daß für jede dieser Anstalten einige ordentliche Lehrer gewonnen werden, welche, außer den übrigen erforderlichen Eigenschaften, auch in den Leibesübungen sich die nöthige Durchbildung verschafft und sich, um dieselbe leiten zu können, mit den Gesetzen, nach welchen der Unterricht in der Gymnastik zweckmäßig zu ertheilen ist, genügend vertraut gemacht haben. Den bereits angestellten ordentlichen Lehrern der mehr gedachten Schulen, welche zwar geneigt sind, sich dem gymnastischen Unterrichte zu widmen, aber hierzu noch nicht die unentbehrliche Fertigkeit, Kenntniß und Erfahrung besitzen, ist der Besuch der gymnastischen Anstalt des hiesigen Universitäts-Fechtlehrers Eiselen anzurathen, wo sie sich nicht nur die eigene Fertigkeit in sämmtlichen Leibesübungen, sondern auch die Kunst, von denselben bei ihren künftigen Schülern einen weisen Gebrauch zu machen, in gründlich strenger Weise und innerhalb einer verhältnißmäßig kurzen Zeit werden erwerben können.

7. Dem Director der Schule, mit welcher eine Turnanstalt verbunden wird, und, wenn dieselbe mehreren Schulen gemeinschaftlich ist, den sämmtlichen Directoren derselben in einer für diesen Fall noch näher zu bestimmenden Weise liegt es ob, über die Leibesübungen die unmittelbare Aufsicht zu führen; ihnen sind die Lehrer der Gymnastik unterzuordnen, und sie sind für alles, was dem Zwecke der Jugendbildung im Abgemeinen und der Gymnastik im besondern widerstreitet, verantwortlich zu machen. Wie es einer Seits die Pflicht der Directoren ist, jeder falschen Richtung und möglichen Ausartung der Gymnastik von Anfang an vorzubeugen, ebenso ist andererseits von ihnen zu verlangen, daß sie in richtiger Würdigung des heilsamen Einflusses, den zweckmäßig betriebene Leibes-Uebungen nicht nur auf die körperliche, sondern auch auf die geistige Entwickelung, und auf die Bildung der Jugend zur Ordnung, Zucht und Sitte behaupten, sich ernstlich bestreben, die ihrer Leitung anvertraute Schule mit der ihr angehörigen Turn-Anstalt in den wirksamsten Zusammenhang zu bringen, und beide zu Einem lebensvollen Ganzen zu vereinigen.

8) Die Leibesübungen sind bei den Gymnasien und höheren Bürgerschulen, mit welchen kein Alumnat verbunden ist, in der Regel auf die schulfreien Nachmittage des Mittwochs und des

Sonnabends zu verlegen. Zu dem Ende ist auch der Lections-Plan dieser Anstalten von jetzt an so einzurichten, daß an diesen Nachmittagen der häusliche Fleiß für die Schule nicht in Anspruch genommen und den Schülern nicht zugemuthet werde, insbesondere vom Mittwoch zum Donnerstage größere schriftliche Arbeiten zu Hause anzufertigen. In Städten, wo die kleinere Schülerzahl und die übrigen örtlichen Verhältnisse es gestatten, kann zwar auch täglich nach Beendigung des nachmittäglichen Schulunterrichts eine Stunde zum Besuch der Turnanstalt verwandt werden. Da aber jener Vorschlag nicht überall und nicht in jeder Jahreszeit ausführbar, auch zur genügenden Lösung der dem gymnastischen Unterrichte zu stellenden Aufgabe ein mehrstündiger Betrieb der körperlichen Uebungen und der mit ihnen abwechselnden gemeinsamen gymnastischen Spiele erforderlich ist: so werden in der Regel die schulfreien Nachmittage des Mittwochs und des Sonnabends dem Unterrichte in der Gymnastik vorzubehalten sein.

9) Die Methode des gymnastischen Unterrichts kann nicht in einer Verfügung erörtert werden, und muß es daher bei der allgemeinen Andeutung sein Bewenden haben, daß der gymnastische Unterricht überall in gehöriger Vollständigkeit, aber mit der durch den Zweck bedingten Einfachheit und mit Entfernung alles Entbehrlichen und bloßen Schaugepränges wie jedes steifen und unlebendigen Mechanismus ertheilt und von Seiten des Lehrers vor allen Dingen das richtige Maaß einer wohlberechneten Abwechslung zwischen der ernsten Strenge der körperlichen Uebungen und der heitern Freiheit der gymnastischen Spiele inne gehalten werden muß.

10) Um der Schuljugend den wichtigen Zweck der Leibes-Uebungen stets gegenwärtig zu erhalten und bei ihr eine lebendige Theilnahme für dieselbe zu wecken, ist in den von den Prüfungs-Commissionen bei den Gymnasien und höheren Bürgerschulen reglementmäßig zu ertheilenden Zeugnissen der Reife von jetzt an ausdrücklich zu bemerken, ob und mit welchem Erfolge die zu Entlassenden den Unterricht in der Gymnastik benutzt haben.

11) Obwohl in der Regel nur die Schüler der Gymnasien und höheren Bürgerschulen zum Besuch der mit denselben in Verbindung stehenden Turnanstalten berechtigt sind, so kann doch unter Bedingungen, deren Feststellung vorbehalten bleibt, ausnahmsweise auch solchen jungen Leuten, welche ihren Unterricht und ihre Erziehung nur durch Privatlehrer und in Privatschulen erhalten, der Zutritt zu den öffentlichen gymnastischen Anstalten gestattet werden.

12) Die aus der Einrichtung und Unterhaltung der Turnanstalten und der für dieselben nöthigen Räumlichkeiten erwachsenden Kosten, so wie die den Lehrern der Gymnastik zu gewährenden Besoldungen oder Remunerationen sind den Allerhöchsten Bestimmungen gemäß zuvörderst aus den Fonds der Schulen, an welche sich die gymnastischen Anstalten anschließen, demnächst aus den mit Rücksicht auf die Verschiedenheit der örtlichen Verhältnisse festzustellenden Beiträgen der jene Anstalten besuchenden Jugend, und wo auch diese nicht ausreichen, mittelst eines angemessenen Zuschusses von Seiten der betreffenden städtischen Gemeinden zu decken. Die Beiträge der die Turnanstalten besuchenden Schüler sind, wie das gewöhnliche Schulgeld, an die betreffende Schul-Casse zu entrichten und in keinem Fall ist den Lehrern der Gymnastik die Einziehung jener Beiträge zuzumuthen; ebenso beziehen diese Lehrer die ihnen für ihren Unterricht in der Gymnastik billiger Weise zu gewährende Besoldung oder Remuneration nur aus der betreffenden Schul-Casse. Da endlich nach der bisherigen Erfahrung mit Grund zu erwarten ist, daß sich besonders in der gegenwärtigen Zeit die allgemeine Theilnahme auch dem öffentlichen Unterricht in der Gymnastik immer mehr zuwenden werde, so wird das gemeinnützige Bestreben derer, welche durch Beschaffung der zur Errichtung und Unterhaltung der gymnastischen Anstalten unentbehrlichen und etwa fehlenden Mittel dieser für die Erziehung der Jugend so wichtigen Angelegenheit ihre Theilnahme bethätigen und lediglich zu dem eben gedachten Zwecke einen Verein bilden wollen, nach Befinden der Umstände in angemessener Weise zu fördern sein; wobei es sich jedoch von selbst versteht, daß von solchen Vereinen ein Einfluß auf die Leitung der gymnastischen Anstalten nicht in Anspruch genommen werden kann.

Indem die weiteren und sonstigen Anordnungen, welche Behufs der Einreihung des gymnastischen Unterrichts in das Ganze des öffentlichen Erziehungswesens etwa noch zu treffen sein möchten, vorbehalten bleiben, beauftragen wir die Herren Directoren der Gymnasien und Seminarien der Provinz Brandenburg und die Herren Directoren der hiesigen höheren Bürgerschulen, und zwar bei den Anstalten Königlichen Patronats, uns baldigst anzuzeigen, wie bei den unter ihrer Leitung stehenden Anstalten sich die obigen von Sr. Excellenz in Betreff der Leibesübungen gegebenen Bestimmungen am zweckmäßigsten werden durchführen lassen, hinsichtlich der Anstalten städtischen Patronats aber wegen der für zweckmäßig oder nothwendig erachteten neuen Einrichtungen der betreffenden Patronatsbehörde ihre Anträge vorzulegen.

Circular-Verfügung des Königl. Schul-Collegiums vom 14. März 1844.

Des Königlichen Geheimen Staats-Ministers Herrn Eichhorn Excellenz hat auf unsern Antrag genehmigt, daß von der Bestimmung in unserer Circular-Verfügung vom 3. Januar 1838 — S. 5540., wonach die Directoren und Rectoren der höheren Lehranstalten gehalten sein sollen, das Manuscript des herauszugebenden Programms der vorgesetzten Provinzialbehörde oder dem von dieser zu bestellenden Commissarius vor dem Abdrucke zur Prüfung vorzulegen, bei den Gymnasien der Provinz Brandenburg und den hiesigen höheren Bürgerschulen im Allgemeinen abgesehen, und diese Bestimmung nur bei denjenigen Anstalten in Anwendung gebracht werde, wo besondere Umstände solches erfordern sollten.

Unter diesen Umständen wollen wir Euer Wohlgeboren von der Einreichung der Manuscripte der herauszugebenden Programme an unsern hierzu ernannten Commissarius entbinden, erwarten aber desto zuversichtlicher, daß Sie alles Ungeeignete aus den Manuscripten der herauszugebenden Programme nach Maaßgabe unserer Circular-Verfügungen vom 3. Januar 1838 und 23. December 1842 zu entfernen wissen werden. Hiernach bleibt Ihnen die unmittelbare Beförderung der Programme zur Censur überlassen.

III. Chronik des Gymnasiums.

Der Winter-Cursus von 1842 — 43 begann mit der Feier des Geburtstages Sr. Majestät des Königs durch einen öffentlichen Rede-Act im großen Hörsaale des Gymnasiums. So wohl die Festrede, gehalten vom Conrector des Gymnasiums Herrn Professor Dr. Seyffert, als die sämmtlichen Vorträge und Gesänge der Schüler bezogen sich, wie im vorigen Jahre, auf vaterländische Geschichte und Interessen. Auch diesmal fand diese speciellere Richtung und Bedeutung des herkömmlichen Herbst-Rede-Actus am Gymnasium lebhafte Theilnahme von Seiten des Publikums.

Im Anfange des Sommerhalbjahres, am 12. Juni 1843, erlitt das Gymnasium einen schmerzlichen Verlust durch den Tod des ersten Collaborators und Oberlehrers Joh. Traugott Klingenstein. Geb. zu Gollme bei Halle im Jahre 1798, erhielt er seine gelehrte Bildung auf der lateinischen Schule des Waisenhauses zu Halle und seit 1817 auf der Universität daselbst, wo er sich der Theologie und Pädagogik vorzugsweise widmete. Von der Universität ging er 1821 als Hauslehrer nach Schönebeck und von da 1823 nach Ziesar. Zu Michaelis 1827 kam er als Lehrer an die hiesige Ritter-Akademie und 1829 an das Gymnasium als dritter Collaborator. Seitdem unserer Anstalt angehörend, hat er mit entschiedener Neigung und wahrhaftem Berufe für das Lehr- und Erziehungsfach bis an seinen Tod treu, gewissenhaft und segensreich gearbeitet. Des treuen Freundes und Lehrers werden seine Mitlehrer, seine Schüler und deren Eltern stets mit dankbarer Liebe gedenken.

Da die Stelle des verstorbenen Klingenstein nicht sofort besetzt werden konnte, die übrigen Lehrer der Anstalt aber, selbst schon übermäßig mit Lehrstunden und Arbeiten überhäuft, die zahlreichen Lectionen und das Ordinariat Klingensteins in Quarta zu übernehmen außer Stand waren, so wurde anfänglich die Unterstützung des Cand. Färber und dann die von Seiten der verehrl. Direction der hiesigen Ritter-Akademie dargebotene Aushilfe dankbar angenommen, und es trat der an dieser Anstalt fungirende Schulamts-Cand. Herr Wagler während des Sommersemesters für den Verstorbenen ein, der mit Gewissenhaftigkeit und anerkennungswerther Leichtigkeit die ihm anvertrauten Klassen geleitet hat.

Mit

Mit dem Anfang des Wintersemesters trat der von Einem Wohllöbl. Patronate zum ersten Collaborator erwählte Nachfolger Klingensteins, Herr **Dr.** Tischer ein, nachdem derselbe seit 8 Jahren an dem Joachimsthalischen Gymnasium zu Berlin, erst als Hülfslehrer, in den letzten 5 Jahren als Adjunctus und ordentlicher Lehrer in den mittlern Klassen bis **Secunda** mit anerkannter Tüchtigkeit, Treue und sichtbarem Erfolge gearbeitet hatte. Ihm wurde vornehmlich das Ordinariat der **Quarta** und die **Tertia Graeca** als seine wesentl. Functionen übertragen, und Herr **Dr.** Tischer hat diese Verpflichtungen bisher in einer Weise erfüllt, daß sich mit Zuversicht das Beste für die Zukunft erwarten läßt.

Am 22. November, an welchem Tage vor 25 Jahren der Director des Gymnasiums zum ersten Male als Lehrer an einer öffentlichen Anstalt und zwar an hiesiger Ritter-Academie fungirte, hat des Königl. Geheimen Staats-Ministers Herrn Eichhorn Excellenz den Conrector am hiesigen Gymnasium, Herrn **Dr.** Seyffert, in Anerkennung seiner ausgezeichneten Leistungen als Gelehrter und seiner Verdienste um das hiesige Gymnasium, zum Professor ernannt, wodurch der von den Collegen, Freunden und Schülern des Directors privatim gefeierte Tag auch eine für das Gymnasium öffentliche ehrenvolle und erfreuliche Bedeutung erhalten hat.

Auch hat im Laufe des Wintersemesters des Königl. Geheimen Staats-Ministers Herrn Eichhorn Excellenz dem **Cand. Theol.** Dorfscheimer für die Unterstützung, welche er dem Gymnasium im Schuljahre gewährt, 50 Rthlr., dem Herrn Professor Seyffert als außerordentliche Unterstützung 50 Rthlr. zweimal für 1842 und 1843 und eben so viel dem Director zu seiner Bade-Cur im Sommer huldreichst bewilligt.

IV. Statistik des Gymnasiums.

Die Schülerzahl beträgt für das laufende Vierteljahr 194; in **Prima** 28, in **Secunda** 16, in **Tertia** 44, in **Quarta** 31, in **Quinta** 30, in **Sexta a.** und **b.** 45.

Aufgenommen wurden im Laufe des Schuljahrs 45.

Abgegangen sind:

A. Zur Universität:

a. Zu Ostern 1843:

1. Siegmund Ernst Steudener aus Hage bei Friesack, 19 Jahr alt, evangel. Conf., Sohn des evangel. Predigers Hrn. Steudener zu Hage, 4 Jahr lang Schüler des Gymn., 2 Jahr in **Prima**, studirt Philologie in Halle.
2. Oskar Richard Lange aus Burg, 19 Jahr alt, evangel. Conf., Sohn des Hrn. Oberpredigers **Dr.** Lange in Burg, 6 Jahr Schüler des Gymnasiums, 2 Jahr in **Prima**, studirt Theologie und Philologie in Halle.
3. Julius Wilhelm Ferdinand Dieckmann aus Sandau, 21 Jahr alt, evangel. Conf., Sohn des Kaufmanns Hrn. Dieckmann in Sandau, 7 Jahr lang Schüler des Gymn., 2 Jahr in **Prima**, studirt Jurisprudenz in Berlin.

b. Zu Michaelis 1843:

1. Reinhold Hugo Wilhelm Seckt, geb. zu Storkow, 21 Jahr alt, evangel. Conf., Sohn des Königl. Land- und Stadtgerichtsrathes Hrn. Seckt zu Brandenburg, 6½ Jahr am Gymn., 2½ Jahr in **Prima**, studirt Theologie in Breslau.
2. Gustav Friedrich Keßler aus Kriele bei Friesack, 19 Jahr alt, evangel. Conf., Sohn des evangel. Predigers Hrn. Keßler zu Kriele, 6½ Jahr am Gymn., 2½ in **Prima**, studirt Theologie in Halle.

3. Adolph Julius Ziem aus Tremmen bei Nauen, 19 Jahr alt, evangel. Conf., Sohn des evangel. Predigers Hrn. Ziem in Tremmen, 5½ Jahr am Gymn., 2 Jahr in **Prima**, studirt Theologie in Halle.

4. Friedrich Wilhelm Ernst Sachse, aus Fraustadt im Großherzogthum Posen, evangel. Conf., Sohn des Königl. Land- und Stadtgerichtsraths Hrn. Sachse zu Krotoschin, 4 Jahr Schüler des Gymn., 2 Jahr in **Prima**, studirt Mathematik in Königsberg.

c. Zu Ostern 1844:

1. Ludwig Wilhelm Maximilian Braut, geb. zu Brandenburg, 19 Jahr alt, evangel. Conf., Sohn des Directors dieser Anstalt, 11 Jahr lang Schüler des Gymn., 2 Jahr in **Prima**, will Jurisprudenz in Berlin studiren.

2. Hermann Deutsch, geb. zu Brandenburg, 19 Jahr alt, evangel. Conf., Sohn des zweiten Lehrers der hiesigen höheren Töchterschule, 11 Jahr am Gymn., 2 Jahr in **Prima**, will Theologie in Berlin studiren.

3. Karl Wolff Stielow, geb. zu Mäthlow, 19 Jahr alt, evangel. Conf., Sohn des Rittergutsbesitzers Hrn. Stielow zu Mäthlow bei Brandenburg, 10 Jahr Schüler des Gymn., 2 Jahr in **Prima**, will Jurisprudenz in Berlin studiren.

4. Johann Emil August Duchstein, geb. zu Etzin bei Nauen, 19 Jahr alt, evangel. Conf., Sohn des Königl. Superintendenten Hrn. Duchstein zu Etzin, 5½ Jahr Schüler des Gymn., 2 Jahr in **Prima**, will Theologie in Berlin studiren.

5. Karl Friedrich Gustav Haußmann, aus Sandau, 20 Jahr alt, evangel. Conf., Sohn des Königl. Rentmeisters Hrn. Haußmann zu Sandau, 8 Jahr lang Schüler des Gymn., 2 Jahr in **Prima**, will Theologie in Berlin studiren.

6. Xaver Gustav Friedrich Philipp Hoyer Uebel, geb. zu Helfta im Mansfeldischen, evangel. Conf., 19 Jahr alt, Sohn des verstorbenen Amtsrathes Hrn. Uebel zu Helfta, 2½ Jahr lang am Gymn., 2 Jahr in **Prima**, will Jurisprudenz in Berlin studiren.

7. Johann Martin Bernhardi, aus Potsdam, 20 Jahr alt, evangel. Conf., Sohn des Königl. Hof- und Garnisonpredigers Hrn. Bernhardi zu Potsdam, seit 1½ Jahren Schüler des Gymn. und Mitglied der **Prima**, will Theologie in Berlin studiren.

B. Zu anderweitiger Bestimmung:

1) aus **Prima**: Otto, Eckolt, Kurth, Fromm, Graf v. Bredow **II.**; 2) aus **Secunda**: Jouanne **I.** und **II.**, Münnich, v. Schulz, Spiegel, Stampe, Maß, Hülsen; 3) aus **Tertia**: Curtius, Regendanck, Grützmacher, Krümling, Borchard, Hampke, Spitta, Gumpert, Leykum, Weigel, Blume, Müller, Brandt, Sehlmacher **I.**; 4) aus **Quarta**: Döhler, Ewald, Giese, Hechel, Kannberg, Mezner, Reiche, Schelle, Schnee, Spitta, Wolff, Brunzlow, Steindorff, Kiesel; 5) aus **Quinta**: Ahlert, Götter, George **I.**, Otto, Schlunck, Stavenow, Liebau, Lindemann; 6) aus **Sexta**: Gems, Dames, Meinicke, Maschmann, Blume, Brunzlow.

Verzeichniss der Schüler

im letzten Vierteljahr in alphabetischer Ordnung.

Prima.

Martin Bernhardi.	Otto Gr. v. Bredow.	Emil Duchstein.
Albrecht Böttiger.	Oscar Gr. v. Bredow.	Adolph Eichmann.
Maximilian Braut.	Hermann Deutsch.	August Freund.

Theodor Fromm.
Carl Geißler.
Gustav Haußmann.
Hermann Hintze.
Carl Hirschberg.
Bernhard Hülsen.
August Kurth.
Hermann Meinshausen.
Louis Müller.
Robert Otto.
Julius Rüthenick.
Eberhard Sachse.
Carl Schmidt.
Bernhard Schulze I.
Eduard Schulze II.
Carl Stielow I.
Hans Stielow II.
Xaver Uebel.
Adolph Waßmannsdorff.

Secunda.

Carl Becker.
Moritz Bournót.
August Brandt.
Julius Giebe.
Albert Hirschberg.
Otto v. Kleist.
Adolph Leidemit.
Albrecht Lucas.
Theodor Märcker.
Udo Möbes.
Louis Pätsch.
Robert Schiebler.
Reinhold Schnee.
Wilhelm Wiesike.
Max Ziem.

Tertia a.

Konstantin Arens.
Ferdinand Böttcher.
August Buchholz.
August Busse.
Eduard Brunow.
Werner Duncker.
Richard Gebhard.
Rudolph Hammer.
Rudolph Hertel.
Hermann Keßler.
Gustav Klingenstein.
Julius Meißner.
Julius Ossent.
Otto Sehlmacher.
Johannes Seltmann.
Louis Sens.
Felix Steinbeck.
August Uhlmann.
Albert Wiesike.

Tertia b.

Adolph Burkhardt.
Georg Deegener.
Louis Guttmann.
Julius Gläslein.
Hermann Klingenstein.
Karl Koch.
Hermann Krumpholz.
Heinrich Löbener.
Julius Lork.
Heinrich Meier.
Oscar Mylius.
Rudulph v. Puttkammer.
Hugo Rüdinger.
Hermann Schiebler.
Adolph Schultze.
Berthold v. Bersen.
Julius Voigt.
Rudolph Westphal.
Robert Wilke.
Karl Wolf.

Quarta.

Alex. Braune I.
Albert Braune II.
Theodor Buchholtz.
Julius Bumke.
Franz Daubert.
Wilhelm Dähne.
Rudolph Drewien.
Hermann Ernst.
Richard Franz.
Wilhelm Hampke.
Otto Haselhorst.
Robert Hartwig.
Wilhelm Helmsdorff.
Albert Hintze.
Albert Hollberg.
Karl Keferstein.
Louis Kiesel.
Emil König.
Reinhold Möbes.
Isidor Pintus.
Bernhard Rupprecht.
Rudolph Schucke.
Julius Schütze.
Wilhelm Siegmund.
Wilhelm Spiecke.
Karl Spitta.
Wolff Stielow.
Hermann Techow.
Julius Wiggert.
Otto Winterfeldt.
Theodor Zeysing.

Quinta.

Julius Buchholtz.
Reinhold Busse.
August Chemnitz.
Otto Duncker.
Johannes Engel.
Arthur Ewald.
Emil Friese.
Henri George.
Karl Heyne.
Emil Keferstein.
Julius Krüger.
Richard Meinhard.

Friedrich Meyer.
Hermann Ramdohr.
Rudolf Rietz.
Theodor Runge.
Gustav Schaff.
Wilhelm Schelle.
Adolf Schröder.
Gustav Schwartze.
Adolf Schwarz.
Wilhelm Seckt.
Gustav Simon.
Hermann Spiescke.
Eduard Spitta.
Otto Steinbeck.
Gustav Tegener.
Richard Bocke.
Richard Wölcker.
Wilhelm Zeysing.

Sexta a.

Eugen Augustin.
Heinrich Berger.
Louis v. Bohlen.
Adolph Gerlach.
Hermann Giese.
Richard Görke.
Hermann Hartwig.
Eduard Hechel.
Karl Herchner.
Julius Kaul.
Leopold Kiesel I.
Otto Klingenstein.
Theodor Krabath.
Hermann Leue.
Adolph Metzenthin.
Rudolph Neumann.
Reinhold Pouet.
Hermann Preckwinckel.
Julius Reetsch.
Emil Regener.
Gottfried Salomon.
Gustav Schonert.
Hermann Seyring.
Albert Steinbeck I.
Fritz Steinbeck II.
Johannes Streich.
Robert Techow.
Franz Waßmannsdorff.
Ernst Zeysing I.
Karl Zeysing II.

Sexta b.

Richard Braut.
Theodor Bumke.
Julius Ewald.
Otto Gläslein.
Gustav Hintze.
Bernhard Kiesel II.
Karl Kreckow.
Max Kuschke.
Wilhelm Löbner.
Karl Lelms.
Otto Negendank.
Gustav v. Podewils.
Hermann Raab.
Gustav Schmidt.
Friedrich Schwarze.
Eduard Steinbeck III.

Zuwachs der Bibliothek.

A. Durch Geschenke: vom hohen Ministerio der Geistl., Unterrichts- und Medicinal-Angelegenheiten: Riedels Cod. diplom. Brandeb. II. B. 3. Liefer. III. B. 1 — 3. Liefer.; desselben Werkes 2. Hauptheil I. B. 1 — 4. Liefer.; Lehmann Gesangbuch für Schulen; Rose: Reise nach dem Ural 2. B ; Danneil: Gesch. der Reform. in der Stadt Salzwedel; v. Spruner: Atlas 5. und 6. Liefer.; die Scriptores Byzantini, so weit sie die Bibliothek bisher noch nicht hatte; Dietrichs Flora Borussica 10. B.; Bürde und Wiegmann: Beschreibung und Abbildungen merkwürdiger Säugethiere; Gerhard's auserles. griechisch. Vasengemälde 2. B.; Kosegarten: Codex Pomeran. diplom. I. B. 1. Heft; Meiring: latein. Schulgrammatik; Panofka: Bilder antiken Lebens; Biese: Philosophie des Aristoteles 2 BB.; Suidae lex. ed. Bernhardy T. I. fasc. 7.; Ptolemaei geogr. ed. Wilberg fasc. IV.

B. Durch Ankauf: Hegel's Werke 7. B.; de Wette's exeg. Handbuch zum N. T. II. B. 3. Liefer.; Hitzig's exeget. Handbuch zum A. T. 3. u. 4. Liefer.; Neander's Gesch. des apostol. Zeitalters 3. Aufl.; Drumann's Gesch. Rom's 5. Th.; Peter: Epochen der röm. Geschichte; Schlegel's Gesch. der Literatur, herausg. von Mundt; Leo's Lehrb. der Universalgeschichte 4. B.; Uckert und Heeren: Geschichte der europ. Staaten 18. und 19. Liefer.; San Marte: Eschenbach's Leben rc. 1. B.; Graff's althochd. Sprachschatz 23. und 24. Liefer.; Curtius Rufus, ed. Mützell; Stephani thesaur. linguae graec. fasc. 27 — 30; Voigt's Gesch. Preußens 2. und 3. B.; Kurz: Commentar zur deutschen Literatur; Schöll: Leben des Sophocles; Schaffarik: slaw. Alterthümer; Becker's Demosthenes; Palacky: Gesch. Böhmens II. B.; Sextus Empir. ed. Bekker; Stephan. Byz. ed. Westermann etc.

Die frühere Schüler-Bibliothek bestand aus 178 Theilen. Dazu kamen aus der Bibliothek der früheren literar. Gesellschaft 572 Thle.

Durch Schenkungen erhielt die Schülerbibl. 1) von Hrn. Buchhändler Müller: Rochow's Gesch. v. Brandenb., herausg. v. Heffter; 2) von dem Primaner Braut: a, Petiscus, Denkmäler menschl. Tugend und Größe, b, Blumenhagen, der Mann und sein Schutzengel; 3) Von dem Quartaner W. Dähne: a, Pichler: Ferdinand II., König von Ungarn und Böhmen, b, Schilling: Häusl. Bilder 2. und 3. Thl.; 4) von dem Quintaner Keferstein: Schoppe: Kleine Mährchen-Bibliothek 1. Thl.

Durch Ankauf: 1) Grote, Erzählungen und Mährchen; 2) Münchhausen's wunderbare Reisen und Abenteuer; 3) Schoppe: Kleine Mährchen-Bibliothek 2. Thl.; 4) Schubart: Bibliothek der Unterrichts-Lectüre 4 Bdchn.; 5) Stiller: Wunderbuch; 6) Ziehnert: Deutsche Sagen und Mährchen; 7) Tausend und eine Nacht 24 Bdchen.; 8) Genlis: Auswahl moral. Erzählungen, übers. von Lochmann, 2 Thle.; 9) Soave: Moral. Erzählungen, übers. von Zehner, 4 Bdchn.; 10) Liebmann: Die Auswanderer nach America; 11) Marezoll: v. Reinstein's lehrreiche und unterhaltende Reisen durch die Rheinlande nach Holland und Belgien; 12) v. Biederfeld: Theater des Lebens; 13) Held: Klaudine, eine schweiz. Geschichte; 14) Ziehnert: Unterhaltende und belehrende Erzählungen für die Jugend; 15) Rockstroh: Erzählungen aus der ältern und mittlern Geschichte zum ersten gründlichen Unterricht in der Weltgesch. 3 Thl. 1. und 2. Abtheil.; 16) Le Petit: Sittengallerie der Nationen; 17) Eylert, Leben Friedrich Wilhelm III.

V. Folge der Prüfung und Redeübung.

Dienstag, den 2. April, Vormittags 8½ Uhr.

Choral.

Quarta und Tertia combin.: Religionslehre. Director.

Tertia: Latein. Hr. Subrector Ramdohr.
Mechanik: Hr. Mathematicus Schönemann.

Secunda: Geschichte. Hr. Professor Dr. Seyffert.
Hebräisch. Hr. Professor Heffter.

Prima: Latein. Hr. Professor Dr. Seyffert.
Französisch. Hr. Collaborator Döhler.

Lateinischer Vortrag des Sekundaners Leidemit: Laudatio M. Porcii Catonis Censorii.

Lateinischer Vortrag des Abiturienten Stielow: Qualis fuerit heroicis Graecorum temporibus religio et civitatis forma.

Gesang No. II.

Nachmittags von 2 Uhr an.

Gesang No. III.

Quarta: Griechisch. Hr. Collaborator Dr. Tischer.
Latein. Derselbe.

Quinta: Latein. Hr. Musik=Director Täglichsbeck.
Geographie. Hr. Professor Heffter.

Sexta a: Latein und Deutsch. Hr. Collaborator Dehmel.

Sexta b: Latein und Deutsch. Hr. Cand. Dorscheimer.

Zwischen den Lectionen declamiren:

1. Aus Quarta:

Braune II.: Die beiden Feigen, von Castelli.
Haselhorst: Schlechter Gewinn, von J. P. Hebel.
Hollberg: Die Beförderung, von Langbein.
Kiesel: Das Compliment nach einer Anekdote, von D. Horn.
Siegmund: Das Gewissen, von Neuendorf.

2. Aus Quinta:

Ramdohr — Krüger — Runge — Busse — Schröder tragen vor: Tobias Witt, von Engel.
Keferstein: Des kleinen Peters Beruf, von Castelli.
Seckt — Buchholtz — George — Meinhard tragen vor: Der Wolf und der Mensch, von Grimm.

3. Aus Sexta a:

Berger: Die kleinen Leute, von Weiße.
Görke: Die beiden Hunde, von Pfeffel.
Reetsch: Der kleine Gerngroß, von Langbein.
Leue: Das Männlein in der Gans, von Fr. Rückert.

4. Aus Sexta b:

Ewald: Der Riese Goliath, von Claudius.
Bumke: Die vier Brüder.
Braut: Der Fischer, von Besselt.
Steinbeck: Reim, Verstand und Dichtkunst.

Französischer Vortrag des Primaners Schmidt: La lutte de l'homme contre la nature.

Lateinischer Vortrag des Abiturienten Deutsch: Arminii adhortatio ad Germanos de armis Segesti et Caesari Germanico inferendis. (Lat. Gedicht.)

Vortrag des Abiturienten Braut, der zugleich Abschied nimmt: Warum denkt der Mensch so gern der Vergangenheit?

Ihm antwortet im Namen der Schule der Primaner Waßmannsdorff.

Entlassung der Abiturienten durch den Director

Choral.

Zur geneigten Theilnahme an dieser Schulfeier, beehre ich mich, im Namen des Gymnasiallehrer=Collegiums, Einen Wohllöblichen Magistrat und die hochzuverehrenden Herren Stadtverordneten, den Königl. Compatronats=Commissarius und Superintendenten Herrn Bauer, Hochwürden, und den Herrn Oberbürgermeister Ziegler als städtischen Patronats Commissarius, Hochwohlgeboren, so wie alle hiesigen Gönner und Freunde des Schulwesens, gehorsamst und ergebenst einzuladen.

Text zu den Gesängen beim Schulexamen Ostern 1844.

Vormittags.

No. I. Choral.

1. Gott, du Licht, das ewig bleibet,
Das ohn' allen Wechsel ist,
Das die Finsterniß vertreibet,
Der du bleibest, wie du bist:
Ich verlasse meine Ruh,
Rufe: werde Licht! mir zu,
Daß ich, der ich Nacht und Erde,
Durch dein Licht verkläret werde.

2. Segne meiner Hände Werke,
Und befördre meine Pflicht.
Bleibe meiner Schwachheit Stärke,
Meines Lebens Kraft und Licht:
Laß mein Lebensziel allein
Deines Namens Ehre sein;
Hilf, daß ich stets wahre Liebe,
Gegen meinen Nächsten übe.

No. II. Chor aus dem Tod Jesu v. Graun.

Freuet euch alle, ihr Frommen. Denn des Herren Wort ist wahrhaftig, und was er zusaget, das hält er gewiß.

Nachmittags.

No. III. Der treue Kamerad, Lied v. Uhland und Silcher.

1. Ich hatt' einen Kameraden,
Einen bessern find'st du nit;
Die Trommel schlug zum Streite,
Er ging an meiner Seite
In gleichem Schritt und Tritt.

2. Eine Kugel kam geflogen,
Gilt sie mir oder gilt sie dir?
Ihn hat sie weggerissen,
Er liegt vor meinen Füßen,
Als wär's ein Stück von mir!

3. Will mir die Hand noch geben,
Dieweil ich eben lad';
Kann dir die Hand nicht geben.
Bleib du im ew'gen Leben
Mein guter Kamerad.

No. IV. Choral.

Wie herrlich ist die neue Welt
Die Gott den Frommen hat bestellt!
Kein Mensch kann sie erwerben.
O Jesu, Herr der Herrlichkeit,
Du hast die Stätt' auch mir bereit,
Hilf sie mir auch ererben.
Einen kleinen Blick in jene Freudenscene gieb mir Schwachen,
Mir den Abschied leicht zu machen.

Nachricht.

Der neue Lehr-Cursus beginnt Montag, den 15. April, Vormittags 9 Uhr. — Zur Prüfung der neu aufzunehmenden Scholaren bin ich vom 10 — 14. April täglich von früh 9 — 12 Uhr in meiner Wohnung bereit, und bemerke dabei zugleich, daß für diejenigen Scholaren, welche nicht studiren und von Quarta an von den Griechischen Lectionen dispensirt sein sollen, die Extra-Lectionen im Französischen, Englischen, Deutschen 2c. in Quarta und Tertia auch im nächsten Cursus ertheilt werden.

Braut.