ist $S\mathfrak{L}$ von $\mathfrak{L}$ verschieden, und daher sind auch alle l Primideale $\mathfrak{L}$, $S\mathfrak{L}, \ldots, S^{l-1}\mathfrak{L}$ unter einander verschieden.

Umgekehrt, wenn $\mathfrak{l}$ eine Zerlegung dieser Art im Kummer'schen Körper $k(M, \zeta)$ gestattet, so stimmen nach einer oben gemachten und, wie dort erwähnt, auch für $\mathfrak{p} = \mathfrak{l}$ zutreffenden Bemerkung die Normen von $\mathfrak{L}$ in $k(M, \zeta)$ und von $\mathfrak{l}$ in $k(\zeta)$ überein, und es muss daher jede ganze Zahl des Körpers $k(M, \zeta)$ einer ganzen Zahl des Körpers $k(\zeta)$ nach $\mathfrak{L}$ congruent sein. Da $\mathfrak{l}$ alsdann nach Satz 93 gewiss nicht in der Relativdiscriminante des Körpers $k(M, \zeta)$ in Bezug auf $k(\zeta)$ enthalten ist, so können wir nach Satz 148 $\mu^* \equiv \alpha^l$ nach $\mathfrak{l}^l$ setzen, und demgemäss ist $\frac{\alpha - M^*}{\lambda}$ eine ganze Zahl. Da $\mathfrak{L}$ ein Primideal ersten Grades in $k(M, \zeta)$ wird, so können wir diese ganze Zahl congruent a nach $\mathfrak{L}$ setzen, so dass a eine ganze rationale Zahl bedeutet; dann folgt, wenn N_k als Bezeichnung der Relativnorm in Bezug auf $k(\zeta)$ dient, die Congruenz

$$N_k\left(\frac{\alpha - M^*}{\lambda} - a\right) \equiv 0, \quad (\mathfrak{l}),$$

d. h.

$$(\alpha - a\lambda)^l - \mu^* \equiv 0, \quad (\mathfrak{l}^{l+1});$$

es ist mithin $\left\{\frac{\mu^*}{\mathfrak{l}}\right\} = \left\{\frac{\mu}{\mathfrak{l}}\right\} = 1$. Diese Thatsachen beweisen auch für das Primideal $\mathfrak{l}$ den letzten Teil des Satzes 149.

Durch den Satz 149 haben wir ein einfaches Mittel erlangt, um die im Beweise des Satzes 93 aufgezählten drei Arten von Primidealen eines Körpers in Hinsicht auf einen relativ-cyklischen Oberkörper von einem Primzahlrelativgrade für den vorliegenden Fall der Körper $k(M, \zeta)$ und $k(\zeta)$ zu unterscheiden.

Capitel XXIX.

Die Normenreste und Normennichtreste des Kummer'schen Körpers.

§ 129.

Die Definition der Normenreste und Normennichtreste.

Es sei, wie in § 125, μ eine Zahl des Kreiskörpers $k(\zeta)$, für welche $M = \sqrt[l]{\mu}$ nicht in $k(\zeta)$ liegt, und es bedeute $k(M, \zeta)$ den durch M

und ζ bestimmten Kummer'schen Körper; für eine Zahl A in $k(M, \zeta)$ werde die Relativnorm in Bezug auf $k(\zeta)$ mit $N_k(A)$ bezeichnet. Es sei $\mathfrak{w}$ ein beliebiges Primideal des Kreiskörpers $k(\zeta)$ und ν eine beliebige ganze Zahl in $k(\zeta)$. Wenn dann ν nach $\mathfrak{w}$ der Relativnorm einer ganzen Zahl des Körpers $k(M, \zeta)$ congruent ist, und wenn ausserdem auch für jede höhere Potenz von $\mathfrak{w}$ stets eine solche ganze Zahl A im Körper $k(M, \zeta)$ gefunden werden kann, dass $\nu \equiv N_k(A)$ nach jener Potenz von $\mathfrak{w}$ ausfällt, so nenne ich ν einen **Normenrest des Kummer'schen Körpers** $k(M, \zeta)$ **nach** $\mathfrak{w}$. In jedem anderen Falle nenne ich ν einen **Normennichtrest des Kummer'schen Körpers** $k(M, \zeta)$ **nach** $\mathfrak{w}$.

§ 130.

Der Satz von der Anzahl der Normenreste. Die Verzweigungsideale.

Es gilt der folgende wichtige Satz:

Satz 150. *Wenn $\mathfrak{w}$ ein Primideal des Kreiskörpers $k(\zeta)$ ist, das nicht in der Relativdiscriminante des Kummer'schen Körpers $k(M, \zeta)$ aufgeht, so ist jede zu $\mathfrak{w}$ prime Zahl in $k(\zeta)$ Normenrest des Kummer'schen Körpers $k(M, \zeta)$ nach $\mathfrak{w}$.*

Wenn dagegen $\mathfrak{w}$ ein Primideal des Kreiskörpers $k(\zeta)$ ist, das in der Relativdiscriminante des Kummer'schen Körpers $k(M, \zeta)$ aufgeht, und e im Falle $\mathfrak{w} \neq \mathfrak{l}$ ein beliebiger positiver Exponent, im Falle $\mathfrak{w} = \mathfrak{l}$ ein beliebiger Exponent $> l$ bedeutet, so sind von allen vorhandenen, zu $\mathfrak{w}$ primen und nach $\mathfrak{w}^e$ einander incongruenten Zahlen in $k(\zeta)$ genau der $l$te Teil Normenreste nach $\mathfrak{w}$.

Beweis. Es sei zunächst $\mathfrak{w}$ ein in der Relativdiscriminante des Körpers $k(M, \zeta)$ nicht aufgehendes und von $\mathfrak{l}$ verschiedenes Primideal des Kreiskörpers $k(\zeta)$; dann sind zwei Fälle zu unterscheiden, je nachdem $\mathfrak{w}$ in $k(M, \zeta)$ zerlegbar ist oder nicht. Im ersteren Falle sei $\mathfrak{W}$ ein in $\mathfrak{w}$ aufgehendes Primideal des Kummer'schen Körpers $k(M, \zeta)$. Im Hinblick auf den Beweis zu Satz 148 können wir, ohne dadurch eine Beschränkung einzuführen, annehmen, es sei μ und mithin auch die Relativdiscriminante der Zahl $M = \sqrt[l]{\mu}$ in Bezug auf $k(\zeta)$ nicht durch $\mathfrak{W}$ teilbar; es giebt dann gewiss im Körper $k(M, \zeta)$ ein System von l ganzen Zahlen $A_1, \ldots, A_l$, für welche die l Congruenzen

$$\left.\begin{array}{lll}
A_1+A_2 M & +\cdots+A_l M^{l-1} & \equiv \nu, \\
A_1+A_2 \zeta M & +\cdots+A_l(\zeta M)^{l-1} & \equiv 1, \\
A_1+A_2 \zeta^2 M & +\cdots+A_l(\zeta^2 M)^{l-1} & \equiv 1, \\
\cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot\ \cdot \\
A_1+A_2 \zeta^{l-1} M & +\cdots+A_l(\zeta^{l-1} M)^{l-1} & \equiv 1,
\end{array}\right\} (\mathfrak{W})$$

erfüllt sind. Nun ist offenbar jede ganze Zahl des Körpers $k(M, \zeta)$ nach $\mathfrak{W}$ einer ganzen Zahl in $k(\zeta)$ congruent; setzen wir

$$A_1 \equiv \alpha_1, \quad A_2 \equiv \alpha_2, \quad \ldots, \quad A_l \equiv \alpha_l, \quad (\mathfrak{W}),$$

so dass $\alpha_1, \alpha_2, \ldots, \alpha_l$ ganze Zahlen in $k(\zeta)$ sind, und

$$A = \alpha_1+\alpha_2 M+\cdots+\alpha_l M^{l-1},$$

so ergiebt sich daher

$$\nu \equiv A, \quad 1 \equiv SA, \quad \ldots, \quad 1 \equiv S^{l-1} A, \quad (\mathfrak{W}),$$

und durch Multiplication folgt $\nu \equiv N_k(A)$ nach $\mathfrak{W}$ und daher auch nach $\mathfrak{w}$. Damit ist unter der gegenwärtigen Annahme über das Primideal $\mathfrak{w}$ der erste Teil des Satzes für den Fall $e=1$ bewiesen. Um zu den Fällen $e>1$ überzugehen, nehmen wir an, es sei $\nu \not\equiv N_k(A)$ nach $\mathfrak{w}^2$, und setzen dann

$$\frac{\nu}{N_k(A)} \equiv 1+\omega, \quad (\mathfrak{w}^2),$$

so dass dabei ω eine ganze, durch $\mathfrak{w}$, aber nicht durch $\mathfrak{w}^2$ teilbare Zahl in $k(\zeta)$ bedeutet. Die ganze Zahl $B=A(1+l^*\omega)$, wobei l^* eine ganze rationale, der Congruenz $ll^* \equiv 1$ nach $\mathfrak{w}$ genügende Zahl sein soll, erfüllt dann die Bedingung $\nu \equiv N_k(B)$ nach $\mathfrak{w}^2$. Durch die gehörige Fortsetzung des hier eingeschlagenen Verfahrens gelangen wir schliesslich zu einer ganzen Zahl in $k(M, \zeta)$, deren Relativnorm in Bezug auf $k(\zeta)$ der Zahl ν nach einer beliebig hohen Potenz $\mathfrak{w}^e$ congruent ist.

Es sei andererseits $\mathfrak{w}$ im Körper $k(M, \zeta)$ nicht weiter zerlegbar; wir können es wiederum einrichten, dass μ nicht durch $\mathfrak{w}$ teilbar sei, und es ist dann nach Satz 149 μ jedenfalls kein $l$ter Potenzrest nach $\mathfrak{w}$. Nach den Folgerungen aus Satz 139 giebt es in $k(\zeta)$ genau $r=\frac{n(\mathfrak{w})-1}{l}$ zu $\mathfrak{w}$ prime $l$te Potenzreste nach $\mathfrak{w}$; sind diese nach $\mathfrak{w}$ durch $\varrho_1, \ldots, \varrho_r$

) kö Primid 1 Grades

vertreten, so fallen die $n(\mathfrak{w})-1$ Zahlen

$$\varrho_i\mu^g \qquad \begin{pmatrix} i = 1, 2, \ldots, r, \\ g = 0, 1, 2, \ldots, l-1 \end{pmatrix}$$

sämtlich nach $\mathfrak{w}$ unter einander incongruent aus, da μ nicht $l$ter Potenzrest nach $\mathfrak{w}$ ist, und es ist also jede zu $\mathfrak{w}$ prime Zahl in $k(\zeta)$ einer dieser Zahlen nach $\mathfrak{w}$ congruent. Setzen wir $\varrho_1 \equiv \alpha_1^l, \ldots, \varrho_r \equiv \alpha_r^l$ nach $\mathfrak{w}$, so dass $\alpha_1, \ldots, \alpha_r$ ebenfalls Zahlen in $k(\zeta)$ sind, so folgt

$$\varrho_i\mu^g \equiv N_k(\alpha_i M^g), \quad (\mathfrak{w})$$

und es ist also jede zu $\mathfrak{w}$ prime Zahl in $k(\zeta)$ der Norm einer geeigneten Zahl in $k(M, \zeta)$ nach $\mathfrak{w}$ congruent; hieraus schliesst man weiter, ähnlich wie im vorigen Falle, dass zu jeder zu $\mathfrak{w}$ primen ganzen Zahl ν in $k(\zeta)$ auch in Bezug auf eine beliebig hohe Potenz $\mathfrak{w}^e$ von $\mathfrak{w}$ stets eine ganze Zahl des Körpers $k(M, \zeta)$ gefunden werden kann, deren Relativnorm nach $\mathfrak{w}^e$ der Zahl ν congruent ist.

II Wir wollen nun den ersten Teil des Satzes 150 auch für den Fall $\mathfrak{w} = \mathfrak{l}$ beweisen, dabei können wir μ zu $\mathfrak{l}$ prim annehmen; wir bezeichnen mit λ^m die höchste in $\mu^{l-1}-1$ enthaltene Potenz von λ, wobei jedenfalls $m \geqq 1$ sein wird, und setzen (vergl. Satz 118)

$$\mu^{l-1} \equiv 1 + a\lambda^m, \quad (\mathfrak{l}^{m+1}),$$

wo a eine ganze rationale, zu l prime Zahl bedeuten soll. Ist dann a^* eine ganze rationale Zahl mit der Congruenzeigenschaft $aa^* \equiv -1$ nach l, und setzen wir $\mu^* = \mu^{a^*(l-1)}$, so wird

$$(72.) \qquad \mu^* \equiv 1 - \lambda^m, \quad (\mathfrak{l}^{m+1}).$$

Andererseits gelten die Congruenzen

$$(73.) \qquad \left.\begin{cases} (1-\lambda^{g+1})^l \equiv 1 + \lambda^{l+g} \\ (1-\lambda^{g+1})^{hl} \equiv 1 + h\lambda^{l+g} \end{cases}\right\}, \quad (\mathfrak{l}^{l+g+1}),$$

wo g eine jede positive ganze rationale Zahl und h eine jede positive ganze rationale zu l prime Zahl sein kann. Da die Relativdiscriminante des Körpers $k(M, \zeta)$ in Bezug auf $k(\zeta)$ im gegenwärtig zu untersuchenden Falle den Factor $\mathfrak{l}$ nicht enthalten soll, so ist nach Satz 148 notwendig $m \geqq l$.

IIa Es sei zunächst $m = l$. Man entnimmt dann leicht aus den Congruenzen (72.) und (73.), dass zu jeder beliebigen positiven ganzen rationalen Zahl g stets eine ganze Zahl α_g in $k(\zeta)$ gefunden werden kann derart, dass die Congruenz

$$\mu^* \alpha_g^l \equiv 1 - \lambda^l + \lambda^{l+g}, \quad (\mathfrak{l}^{l+g+1})$$

erfüllt wird. Setzen wir nun $M^* = \sqrt[l]{\mu^*}$ und ferner allgemein für jeden Wert von g:

$$\Omega_g = \frac{1 - \alpha_g M^*}{\lambda},$$

so wird jedesmal Ω_g eine ganze Zahl in $k(M, \zeta)$ und

$$N_k(\Omega_g) \equiv 1 - \lambda^g, \quad (\mathfrak{l}^{g+1}).$$

Hieraus folgt unmittelbar, dass jede ganze Zahl ν in $k(\zeta)$, die der Congruenz $\nu \equiv 1$ nach $\mathfrak{l}$ genügt, Normenrest des Körpers $k(M, \zeta)$ nach $\mathfrak{l}$ ist. Die Beschränkung, die hier in Annahme $\nu \equiv 1$ nach $\mathfrak{l}$ liegt, wird leicht aufgehoben. Ist nämlich ν eine beliebige zu $\mathfrak{l}$ prime Zahl, und wird sie nach $\mathfrak{l}$ der ganzen rationalen Zahl a congruent, so setzen wir $\nu^* = a^{*l} \nu$, wo a^* eine ganze rationale Zahl mit der Congruenzeigenschaft $a a^* \equiv 1$ nach $\mathfrak{l}$ bedeute; dann wird offenbar $\nu^* \equiv 1$ nach $\mathfrak{l}$, und andererseits werden ν und ν^* gleichzeitig Normenrest oder Normennichtrest des Körpers $k(M, \zeta)$ nach $\mathfrak{l}$ sein.

Es sei zweitens in Formel (72.) $m > l$ und mithin $\left\{\frac{\mu}{\mathfrak{l}}\right\} = 1$; dann können wir, wenn g eine beliebige positive ganze rationale Zahl ist, stets zwei ganze Zahlen α_g und α_{g+1} in $k(\zeta)$ construiren derart, dass

$$(74.) \quad \begin{cases} \mu^* \alpha_g^l \equiv 1 + \lambda^{l+1} + \lambda^{l+g+1}, & (\mathfrak{l}^{l+g+2}), \\ \mu^* \alpha_{g+1}^l \equiv 1 + \lambda^{l+1} + \lambda^{l+g+2}, & (\mathfrak{l}^{l+g+3}) \end{cases}$$

wird. Wir setzen gemäss dem Satze 149 $\mathfrak{l} = \mathfrak{L}\mathfrak{L}' \ldots \mathfrak{L}^{(l-1)}$, wo $\mathfrak{L}, \mathfrak{L}', \ldots$ $\ldots, \mathfrak{L}^{(l-1)}$ von einander verschiedene Primideale des Körpers $k(M, \zeta)$ bedeuten. Die beiden Zahlen

$$A_g = \frac{1 - \alpha_g M^*}{\lambda}, \quad A_{g+1} = \frac{1 - \alpha_{g+1} M^*}{\lambda},$$

$M^* = \sqrt[l]{\mu^*}$ gesetzt, sind ganze Zahlen, und da $N_k(A_g) \equiv -\lambda$ nach $\mathfrak{l}^2$ wird, so enthält A_g eines der in $\mathfrak{l}$ aufgehenden Primideale, es sei dies etwa das Primideal $\mathfrak{L}$, zur ersten Potenz und die anderen in $\mathfrak{l}$ aufgehenden Primideale gar nicht. Aus den Formeln (74.) folgt

$$\alpha_g^l \equiv \alpha_{g+1}^l, \quad (\mathfrak{l}^{l+2}),$$

und wir können nun voraussetzen, dass α_{g+1} in der Reihe der Zahlen $\alpha_{g+1}, \zeta\alpha_{g+1}, \ldots, \zeta^{l-1}\alpha_{g+1}$ in solcher Weise gewählt sei, dass $\alpha_g \equiv \alpha_{g+1}$ nach $\mathfrak{l}^2$ und also $A_g \equiv A_{g+1}$ nach $\mathfrak{l}$ ausfällt. Wegen der letzteren Congruenz ist auch die Zahl A_{g+1} durch $\mathfrak{L}$, aber durch keines der Primideale $\mathfrak{L}', \ldots, \mathfrak{L}^{(l-1)}$ teilbar, und da auch $N_k(A_{g+1}) \equiv -\lambda$ nach $\mathfrak{l}^2$ ist, so ist A_{g+1} ebenfalls nur durch die erste Potenz von $\mathfrak{L}$ teilbar. Wir können mit Rücksicht auf das eben Bewiesene die gebrochene Zahl $\frac{A_g}{A_{g+1}}$ in die Form eines Bruches schreiben, dessen Zähler und Nenner zu $\mathfrak{l}$ prim sind. Setzen wir $\frac{A_g}{A_{g+1}} \equiv \Omega_g$ nach $\mathfrak{l}^{g+1}$ in solcher Weise, dass Ω_g eine ganze Zahl in $k(M, \zeta)$ ist, so wird

$$N_k(\Omega_g) \equiv \frac{N_k(A_g)}{N_k(A_{g+1})} \equiv 1 + \lambda^g, \quad (\mathfrak{l}^{g+1}).$$

Da eine solche Formel für jeden positiven Exponenten g möglich ist, so zeigt sich wie vorhin, dass jede zu $\mathfrak{l}$ prime Zahl Normenrest des Körpers $k(M, \zeta)$ ist.

Wir gehen jetzt zum Beweise der zweiten Hälfte von Satz 150 über. Es sei zunächst $\mathfrak{w}$ ein von $\mathfrak{l}$ verschiedenes, in der Relativdiscriminante des Körpers $k(M, \zeta)$ in Bezug auf $k(\zeta)$ aufgehendes Primideal des Körpers $k(\zeta)$; wir haben dann nach Satz 149 $\mathfrak{w} = \mathfrak{W}^l$, wo $\mathfrak{W}$ ein Primideal in $k(M, \zeta)$ ist. Jede ganze Zahl des Körpers $k(M, \zeta)$ muss dann, wie schon mehrfach erwähnt wurde, einer ganzen Zahl in $k(\zeta)$ nach $\mathfrak{W}$ congruent sein. Soll nun eine gegebene, zu $\mathfrak{w}$ prime ganze Zahl ν in $k(\zeta)$ nach $\mathfrak{w}$ congruent der Relativnorm $N_k(A)$ einer ganzen Zahl A in $k(M, \zeta)$ sein, und setzen wir $A \equiv \alpha$ nach $\mathfrak{W}$, so folgt notwendig $\nu \equiv \alpha^l$ nach $\mathfrak{W}$, und daher auch nach $\mathfrak{w}$, d. h. ν ist $l$ter Potenzrest nach $\mathfrak{w}$. Umgekehrt, wenn eine Zahl ν in $k(\zeta)$ ein $l$ter Potenzrest nach $\mathfrak{w}$ ist, so ist ν offenbar auch congruent einer Relativnorm $N_k(A)$ nach $\mathfrak{w}$. Wir entnehmen hieraus, dass die $l$ten Potenzreste nach $\mathfrak{w}$ auch zugleich die sämtlichen Normenreste des Körpers $k(M, \zeta)$ nach $\mathfrak{w}$ liefern.

Es bleibt endlich die Behandlung des Falles übrig, dass $\mathfrak{w} = \mathfrak{l}$ ist und $\mathfrak{l}$ in der Relativdiscriminante des Körpers $k(M, \zeta)$ aufgeht. Wir haben in diesem Falle $\mathfrak{l} = \mathfrak{L}^l$, wo $\mathfrak{L}$ ein Primideal in $k(M, \zeta)$ ist, und können es im Hinblick auf Satz 148 stets einrichten, dass die Zahl μ entweder der Congruenz

$$\mu \equiv \lambda, \qquad (\mathfrak{l}^2)$$

oder einer der folgenden Congruenzen genügt:

$$\mu \equiv 1+\lambda^m, \quad (\mathfrak{l}^{m+1}),$$

wo m einen der Werte $1, 2, \ldots, l-1$ bedeutet. Wir wollen alsdann untersuchen, welche Zahlen in $k(\zeta)$ es in diesen zwei Fällen giebt, die congruent der Relativnorm einer Zahl in $k(M, \zeta)$ nach $\mathfrak{l}^{l+1}$ bez. $\mathfrak{l}^l$ sind, und entnehmen hieraus leicht die Anzahl der nach jeder höheren Potenz von $\mathfrak{l}$ einander incongruenten Normenreste.

Im Falle $\mu \equiv \lambda$ nach $\mathfrak{l}^2$ ist M durch $\mathfrak{L}$, aber nicht durch $\mathfrak{L}^2$ teilbar, und es gelten die Congruenzen

$$(75.)\quad \left\{\begin{array}{rll}
 & N_k(1+M) \equiv 1+\lambda, & (\mathfrak{l}^2),\\
\text{d. i.} & N_k(1+M) \equiv 1+\lambda \quad +\lambda^2\varrho_1, & (\mathfrak{l}^{l+1}),\\
 & N_k(1+M^2) \equiv 1+\lambda^2, & (\mathfrak{l}^3),\\
\text{d. i.} & N_k(1+M^2) \equiv 1+\lambda^2 \quad +\lambda^3\varrho_2, & (\mathfrak{l}^{l+1}),\\
\cdot & \cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot & \cdot\\
 & N_k(1+M^{l-1}) \equiv 1+\lambda^{l-1}, & (\mathfrak{l}^l),\\
\text{d. i.} & N_k(1+M^{l-1}) \equiv 1+\lambda^{l-1}+\lambda^l\varrho_{l-1}, & (\mathfrak{l}^{l+1}),
\end{array}\right.$$

wo $\varrho_1, \varrho_2, \ldots, \varrho_{l-1}$ gewisse ganze Zahlen in $k(\zeta)$ bedeuten. Endlich ist

$$(76.)\qquad N_k(1+\lambda^t M^g) \equiv 1, \quad (\mathfrak{l}^{l+1})$$

für $t = 1, 2, 3, \ldots;\ g = 0, 1, 2, \ldots, l-1$. Nun genügt offenbar jede zu $\mathfrak{L}$ prime ganze Zahl A des Körpers $k(M, \zeta)$ einer Congruenz von der Gestalt

$$\begin{aligned}
A \equiv a(1+M)^{a_1}\ &(1+M^2)^{a_2}\ \ldots(1+M^{l-1})^{a_{l-1}}\\
&(1+\lambda\, M)^{a'_1}\,(1+\lambda\, M^2)^{a'_2}\ldots(1+\lambda\, M^{l-1})^{a'_{l-1}}\\
&\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\;\cdot\\
&(1+\lambda^l M)^{a_1^{(l)}}(1+\lambda^l M^2)^{a_2^{(l)}}\ldots(1+\lambda^l M^{l-1})^{a_{l-1}^{(l)}}, \quad (\mathfrak{l}^{l+1}),
\end{aligned}$$

wo a eine bestimmte der Zahlen $1, 2, \ldots, l-1$ und die $(l+1)(l-1)$ Exponenten $a_1, a_2, \ldots, a_{l-1}^{(l)}$ bestimmte ganze rationale Zahlen aus der Reihe $0, 1, 2, \ldots, l-1$ sind. Wegen der Congruenzen (75.) und (76.) folgt daher:

$$\begin{aligned}
N_k(A) \equiv a^l(1+\lambda+\lambda^2\varrho_1)^{a_1}(1+\lambda^2+\lambda^3\varrho_2)^{a_2}\ldots&\\
\ldots(1+\lambda^{l-1}+\lambda^l\varrho_{l-1})^{a_{l-1}}, \quad (\mathfrak{l}^{l+1}).&
\end{aligned}$$

Der Ausdruck rechter Hand stellt, wenn a die Werte $1, 2, \ldots, l-1$ und die Exponenten $a_1, a_2, \ldots, a_{l-1}$ unabhängig von einander je die Werte $0, 1, 2, \ldots, l-1$ durchlaufen, genau $(l-1)l^{l-1}$ Zahlen dar, und diese sind, wie leicht ersichtlich, alle einander incongruent nach $\mathfrak{l}^{l+1}$. Nun ist jede zu $\mathfrak{l}$ prime Zahl in $k(\zeta)$, welche der Relativnorm $N_k(A)$ einer Zahl A in $k(M, \zeta)$ congruent nach $\mathfrak{l}^{l+1}$ ist, notwendig einem Ausdruck dieser Gestalt nach $\mathfrak{l}^{l+1}$ congruent, und umgekehrt ist auch jeder Ausdruck von dieser Gestalt, wie man aus (75.) entnimmt, der Relativnorm einer Zahl in $k(M, \zeta)$ nach $\mathfrak{l}^{l+1}$ congruent. Mit Hülfe der Congruenzen (73.) erkennt man, dass zwei nach $\mathfrak{l}^{l+1}$ congruente, zu $\mathfrak{l}$ prime Zahlen in $k(\zeta)$ stets gleichzeitig Normenrest oder Normennichtrest nach $\mathfrak{l}$ sind. Die Anzahl der Normenreste nach $\mathfrak{l}$, welche zu $\mathfrak{l}$ prim und untereinander incongruent nach $\mathfrak{l}^{l+1}$ sind, ist also genau gleich $(l-1)l^{l-1}$, d. i. gleich dem $l$ten Teil der nach $\mathfrak{l}^{l+1}$ möglichen incongruenten, zu $\mathfrak{l}$ primen Zahlen in $k(\zeta)$, und dieses Resultat kann sofort auf die Potenzen $\mathfrak{l}^e$ mit Exponenten $e > l+1$ ausgedehnt werden.

Von den übrigen möglichen Annahmen über μ werde hier der Kürze wegen nur die einfachste behandelt; es werde nämlich $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ zu Grunde gelegt. Setzen wir dann $\Omega = M-1$, so ist Ω eine durch $\mathfrak{L}$, aber nicht durch $\mathfrak{L}^2$ teilbare ganze Zahl in $k(M, \zeta)$, und wenn wir berücksichtigen, dass $N_k(\Omega) \equiv \lambda$ nach $\mathfrak{l}^2$ wird, so erkennen wir durch eine leichte Rechnung die Richtigkeit der Congruenzen

$$
(77.)\quad \left\{
\begin{array}{lrcll}
 & N_k(1+\Omega) & \equiv & 1+\lambda, & (\mathfrak{l}^2), \\
\text{d. i.} & N_k(1+\Omega) & \equiv & 1+\lambda+\lambda^2\varrho_1, & (\mathfrak{l}^l), \\
 & N_k(1+\Omega^2) & \equiv & 1+\lambda^2, & (\mathfrak{l}^3), \\
\text{d. i.} & N_k(1+\Omega^2) & \equiv & 1+\lambda^2+\lambda^3\varrho_2, & (\mathfrak{l}^l), \\
\cdot & \cdot\ \cdot\ \cdot\ \cdot & \cdot & \cdot\ \cdot\ \cdot\ \cdot\ \cdot & \cdot \\
 & N_k(1+\Omega^{l-2}) & \equiv & 1+\lambda^{l-2}, & (\mathfrak{l}^{l-1}), \\
\text{d. i.} & N_k(1+\Omega^{l-2}) & \equiv & 1+\lambda^{l-2}+\lambda^{l-1}\varrho_{l-2}, & (\mathfrak{l}^l),
\end{array}
\right.
$$

wo $\varrho_1, \varrho_2, \ldots, \varrho_{l-2}$ gewisse ganze Zahlen in $k(\zeta)$ bedeuten. Wir haben ferner

$$N_k(1+\Omega^{l-1}) = 1+\Sigma_1+\Sigma_2+\Sigma_3+\cdots+\Sigma_{l-1}+N_k(\Omega^{l-1}),$$

wo zur Abkürzung

$$\Sigma_1 = \Omega^{l-1}+(S\Omega)^{l-1}+\cdots+(S^{l-1}\Omega)^{l-1},$$
$$\Sigma_2 = \Omega^{l-1}(S\Omega)^{l-1}+\Omega^{l-1}(S^2\Omega)^{l-1}+\cdots+(S^{l-2}\Omega)^{l-1}(S^{l-1}\Omega)^{l-1},$$
$$\Sigma_3 = \Omega^{l-1}(S\Omega)^{l-1}(S^2\Omega)^{l-1}+\cdots+(S^{l-3}\Omega)^{l-1}(S^{l-2}\Omega)^{l-1}(S^{l-1}\Omega)^{l-1},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

gesetzt ist. Nun ergiebt sich sofort $\Sigma_1 = l$. Die einzelnen Summanden in den Ausdrücken für $\Sigma_2, \Sigma_3, \ldots, \Sigma_{l-1}$ sind sämtlich jedenfalls durch $\mathfrak{L}^l$ teilbar, sie lassen sich ferner in Aggregate von je l Summanden zusammenfassen, die aus einem beliebigen unter ihnen durch die Substitutionen $1, S, S^2, \ldots, S^{l-1}$ hervorgehen; setzen wir nun ein beliebiges Glied in der Gestalt $\lambda\Phi$ an, so bedeutet Φ eine ganze Zahl in $k(M, \zeta)$ und kann daher, wie aus dem Beweise des Hülfssatzes 23 hervorgeht, als ganze rationale Function von Ω und mithin auch von M dargestellt werden, deren Coefficienten ganze oder gebrochene Zahlen in $k(\zeta)$ mit lauter zu $\mathfrak{l}$ primen Nennern sind. Setzen wir dementsprechend $\Phi = F(M)$, so lässt sich das betreffende Aggregat von l Summanden in die Form

$$\lambda\{F(M)+F(\zeta M)+F(\zeta^2 M)+\cdots+F(\zeta^{l-1} M)\}$$

bringen; die hier in der Klammer stehende Summe fällt, wie leicht ersichtlich, stets congruent 0 nach l aus; danach müssen nun die Zahlen $\Sigma_2, \Sigma_3, \ldots, \Sigma_{l-1}$ sämtlich congruent 0 nach $\mathfrak{l}^l$ sein, also wird

$$(78.)\qquad N_k(1+\Omega^{l-1}) \equiv 1+l+\lambda^{l-1} \equiv 1, \quad (\mathfrak{l}^l).$$

Endlich ergeben sich leicht die Congruenzen

$$(79.)\qquad N_k(1+\lambda^t\Omega^g) \equiv 1, \quad (\mathfrak{l}^l)$$

für $t = 1, 2, 3, \ldots; g = 1, 2, 3, \ldots, l-1$.

Nun genügt offenbar jede zu $\mathfrak{L}$ prime ganze Zahl in $k(M, \zeta)$ einer Congruenz von der Gestalt

$$\begin{aligned} A \equiv a(1+\Omega)^{a_1} \quad & (1+\Omega^2)^{a_2} \quad \ldots(1+\Omega^{l-1})^{a_{l-1}}. \\ (1+\lambda\Omega)^{a'_1} \quad & (1+\lambda\Omega^2)^{a'_2} \quad \ldots(1+\lambda\Omega^{l-1})^{a'_{l-1}}. \\ & \cdots\cdots\cdots\cdots \\ (1+\lambda^{l-1}\Omega)^{a_1^{(l-1)}} \quad & (1+\lambda^{l-1}\Omega^2)^{a_2^{(l-1)}} \ldots(1+\lambda^{l-1}\Omega^{l-1})^{a_{l-1}^{(l-1)}}, \quad (\mathfrak{l}^l), \end{aligned}$$

wo a eine der Zahlen $1, 2, \ldots, l-1$, und wo die $l(l-1)$ Exponenten

$a_1, a_2, \ldots, a_{l-1}^{(l-1)}$ bestimmte Zahlen aus der Reihe $0, 1, 2, \ldots, l-1$ sind. Wegen der vorhin aufgestellten Congruenzen (77.), (78.), (79.) folgt hieraus:

$$N_k(A) \equiv a^l(1+\lambda+\lambda^2\varrho_1)^{a_1}(1+\lambda^2+\lambda^3\varrho_2)^{a_2}\ldots$$
$$\ldots(1+\lambda^{l-2}+\lambda^{l-1}\varrho_{l-2})^{a_{l-2}}, \quad (\mathfrak{l}^l).$$

Der hier rechts stehende Ausdruck stellt nun, wenn a die Werte $1, 2, \ldots \ldots, l-1$, und wenn die Exponenten $a_1, a_2, \ldots, a_{l-2}$ unabhängig von einander die Werthe $0, 1, 2, \ldots, l-1$ durchlaufen, $(l-1)l^{l-2}$ Zahlen dar, und diese sind sämtlich zu $\mathfrak{l}$ prim und einander incongruent nach $\mathfrak{l}^l$. Mit Benutzung der Congruenz $N_k(1+\lambda M) \equiv 1+\lambda^l$ nach $\mathfrak{l}^{l+1}$ und weiter der Congruenzen (73.) schliessen wir hieraus, dass genau der $l$te Teil aller zu $\mathfrak{l}$ primen und nach $\mathfrak{l}^l$ einander incongruenten Zahlen Normenreste des Körpers $k(M, \zeta)$ nach $\mathfrak{l}$ liefert, und übertragen dann dieses Resultat sogleich auf den Fall der Potenzen $\mathfrak{l}^e$ mit Exponenten $e = l+1$ bez. $e > l+1$.

Das nämliche Resultat ergiebt sich durch entsprechende Rechnungen auch dann, wenn $\mu \equiv 1$ nach $\mathfrak{l}^2$ genommen wird, und damit ist der Satz 150 in allen Teilen bewiesen. Es sei jedoch bemerkt, dass wir es in unseren späteren Entwickelungen so einrichten können, dass der Satz 150 lediglich für den oben ausführlich bewiesenen Fall $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ zur Verwendung gelangt.

Der Satz 150 bringt eine neue, tief eingreifende Eigenschaft der in der Relativdiscriminante des Körpers $k(M, \zeta)$ in Bezug auf $k(\zeta)$ aufgehenden Primideale $\mathfrak{w}$ zum Ausdruck. Diese Eigenschaft entspricht gewissermassen dem bekannten Satze über die Verzweigungspunkte einer Riemann'schen Fläche, wonach eine algebraische Function in der Umgebung eines Verzweigungspunktes $l$ter Ordnung den Vollwinkel auf den $l$ten Teil desselben conform abbildet. Infolgedessen nenne ich die in der Relativdiscriminante von $k(M, \zeta)$ in Bezug auf $k(\zeta)$ aufgehenden Primideale $\mathfrak{w}$ auch **Verzweigungsideale** für den Körper $k(M, \zeta)$; es bedeuten hier also „Primfactor der Relativdiscriminante", „ambiges Primideal", „Verzweigungsideal" den nämlichen Begriff.

§ 131.

Das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$.

Der Satz 150 weist uns auf die Möglichkeit hin, die nach einer Potenz $\mathfrak{w}^e$ ($e > l$ im Falle $\mathfrak{w} = \mathfrak{l}$) vorhandenen, einander incongruenten Zahlen des Körpers $k(\zeta)$ in l Abteilungen zu sondern, die sämtlich gleich viele Zahlen enthalten, und von denen eine die Normenreste nach $\mathfrak{w}$ umfasst. Um diese Sonderung in übersichtlicher Weise vornehmen zu können, führe ich ein neues Symbol $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ ein, welches zwei beliebigen, von 0 verschiedenen ganzen Zahlen ν, μ des Körpers $k(\zeta)$ in Bezug auf ein beliebiges Primideal $\mathfrak{w}$ in $k(\zeta)$ jedesmal eine bestimmte $l$te Einheitswurzel zuweist, und zwar geschieht dies in folgender Weise:

Es sei zunächst $\mathfrak{w}$ ein von $\mathfrak{l}$ verschiedenes Primideal. Ist dann ν genau durch $\mathfrak{w}^b$ und μ genau durch $\mathfrak{w}^a$ teilbar, so bilde man die Zahl $\varkappa = \frac{\nu^a}{\mu^b}$ und bringe $\varkappa$ in die Gestalt eines Bruches $\frac{\varrho}{\sigma}$, dessen Zähler ϱ und Nenner σ nicht durch $\mathfrak{w}$ teilbar sind. Das **Symbol** $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ werde dann durch die Formel

$$\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = \left\{\frac{\varkappa}{\mathfrak{w}}\right\} = \left\{\frac{\varrho}{\mathfrak{w}}\right\}\left\{\frac{\sigma}{\mathfrak{w}}\right\}^{-1}$$

definirt. Es ergeben sich hieraus unmittelbar für dieses Symbol die einfachen Regeln:

$$(80.)\quad \begin{cases} \left\{\frac{\nu_1\nu_2, \mu}{\mathfrak{w}}\right\} = \left\{\frac{\nu_1, \mu}{\mathfrak{w}}\right\}\left\{\frac{\nu_2, \mu}{\mathfrak{w}}\right\}, \\ \left\{\frac{\nu, \mu_1\mu_2}{\mathfrak{w}}\right\} = \left\{\frac{\nu, \mu_1}{\mathfrak{w}}\right\}\left\{\frac{\nu, \mu_2}{\mathfrak{w}}\right\}, \\ \left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}\left\{\frac{\mu, \nu}{\mathfrak{w}}\right\} = 1, \end{cases}$$

wo ν, ν_1, ν_2, μ, μ_1, μ_2 beliebige von Null verschiedene ganze Zahlen in $k(\zeta)$ bedeuten können.

Um das neue Symbol für den Fall $\mathfrak{w} = \mathfrak{l}$ zu definiren, stellen wir folgende Ueberlegungen an:

Wenn eine beliebige ganze Zahl ω in $k(\zeta)$ vorgelegt ist, welche der Congruenz $\omega\equiv 1$ nach $\mathfrak{l}$ genügt, und wenn wir setzen

$$\omega = c+c_1\zeta+\cdots+c_{l-2}\zeta^{l-2},$$

so dass $c, c_1, \ldots, c_{l-2}$ ganze rationale Zahlen sind, so genügen diese notwendig der Congruenz

$$c+c_1+\cdots+c_{l-2}\equiv 1, \quad (l).$$

Setzen wir dann

$$\omega(x) = c+c_1x+\cdots+c_{l-2}x^{l-2} - \frac{c+c_1+\cdots+c_{l-2}-1}{l}(1+x+\cdots+x^{l-1}),$$

so stellt $\omega(x)$ eine ganzzahlige Function $(l-1)$ten Grades dar, und es wird

$$\omega(1)=1 \quad \text{und} \quad \omega(\zeta)=\omega.$$

Diese Function heisse die **zur ganzen Zahl ω gehörende Function.** Wir schreiben ferner

$$\left[\frac{d^g \log\omega(e^v)}{dv^g}\right]_{v=0} = l^{(g)}(\omega), \tag{81.}$$
$$(g=1, 2, \ldots, l-1)$$

welche Verbindungen von *Kummer* mit Vorteil zur Abkürzung gewisser Rechnungen eingeführt sind. [*Kummer*[12].]

Wird die Zahl ω mit der Congruenzeigenschaft $\omega\equiv 1$ nach $\mathfrak{l}$ auf irgend eine Weise in die Gestalt

$$\omega = a+a_1\zeta+\cdots+a_t\zeta^t$$

gebracht, wo $a, a_1, \ldots, a_t$ ganze rationale Zahlen bedeuten, so stellt

$$\varpi(x) = a+a_1x+\cdots+a_tx^t$$

eine ganzzahlige Function t-ten Grades dar, welche im allgemeinen nicht der Gleichung $\varpi(1)=1$, aber jedenfalls der Congruenz

$$\varpi(1)\equiv 1, \quad (l)$$

Genüge leistet und also für $x=1$ zu l prim ausfällt. Zwischen den Differentialquotienten von $\log\varpi(e^v)$ für $v=0$ und den soeben eingeführten

Differentialquotienten (81.) bestehen folgende Congruenzen:

$$\left[\frac{d^g \log \varpi(e^v)}{d v^g}\right]_{v=0} \equiv l^{(g)}(\omega), \quad (l),$$
$$(g = 1, 2, \ldots, l-2),$$

$$\left[\frac{d^{l-1} \log \varpi(e^v)}{d v^{l-1}}\right]_{v=0} \equiv l^{(l-1)}(\omega) + \frac{1-\varpi(1)}{l}, \quad (l).$$

Die Richtigkeit dieser Congruenzen erkennen wir leicht wegen

$$\omega(x) = \varpi(x) + \frac{1-\varpi(1)}{l}(1+x+\cdots+x^{l-1}) + O(x)(x^l-1),$$

$$\omega(e^v) \equiv \varpi(e^v) + \frac{1-\varpi(1)}{l} v^{l-1}, \quad (l);$$

in der ersten Formel bedeutet $O(x)$ eine bestimmte ganzzahlige Function von x, nnd die zweite Formel soll besagen, dass in den Entwickelungen der beiden Seiten dieser Congruenz nach Potenzen von v die Coefficienten von $1, v, v^2, \ldots, v^{l-1}$ nach l congruent ausfallen.

Sind ν, μ irgend zwei ganze Zahlen in $k(\zeta)$ mit der Congruenzeigenschaft $\nu \equiv 1$, $\mu \equiv 1$ nach $\mathfrak{l}$, so definiren wir das **Symbol** $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ wie folgt:

$$(82.) \quad \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = \zeta^{l^{(1)}(\nu) l^{(l-1)}(\mu) - l^{(2)}(\nu) l^{(l-2)}(\mu) + \cdots - l^{(l-1)}(\nu) l^{(1)}(\mu)}.$$

Aus dieser Definition ergeben sich unmittelbar die folgenden Regeln:

$$(83.) \quad \begin{cases} \left\{\frac{\nu_1 \nu_2, \mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu_1, \mu}{\mathfrak{l}}\right\}\left\{\frac{\nu_2, \mu}{\mathfrak{l}}\right\}, \\ \left\{\frac{\nu, \mu_1 \mu_2}{\mathfrak{l}}\right\} = \left\{\frac{\nu, \mu_1}{\mathfrak{l}}\right\}\left\{\frac{\nu, \mu_2}{\mathfrak{l}}\right\}, \\ \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}\left\{\frac{\mu, \nu}{\mathfrak{l}}\right\} = 1, \end{cases}$$

wo ν, ν_1, ν_2, μ, μ_1, μ_2 beliebige ganze Zahlen $\equiv 1$ nach $\mathfrak{l}$ in $k(\zeta)$ bedeuten können. Bezeichnet r eine Primitivzahl nach l und $s = (\zeta : \zeta^r)$ die entsprechende Substitution der Gruppe des Kreiskörpers $k(\zeta)$, so gilt, wie leicht ersichtlich ist, die weitere Formel

$$(84.) \quad \left\{\frac{s\nu, s\mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}^r.$$

Sind ν, μ beliebige zu $\mathfrak{l}$ prime ganze Zahlen des Körpers $k(\zeta)$, so definire ich das **Symbol** $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}$ durch die Formel

$$\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\} = \left\{\frac{\nu^{l-1},\mu^{l-1}}{\mathfrak{l}}\right\}.$$

Für den Fall, dass eine der Zahlen ν, μ oder beide durch $\mathfrak{l}$ teilbar sind, vergleiche man die Bemerkungen gegen Schluss des § 133.

§ 132.

Einige Hülfssätze über das Symbol $\left\{\frac{\nu,\mu}{\mathfrak{l}}\right\}$ und über Normenreste nach dem Primideal $\mathfrak{l}$.

Hülfssatz 24. Wenn ω eine ganze Zahl in $k(\zeta)$ mit der Congruenzeigenschaft $\omega \equiv 1$ nach $\mathfrak{l}$ ist, so gilt für die Norm $n(\omega)$ von ω in $k(\zeta)$ die Congruenz

$$1^{(l-1)}(\omega) \equiv \frac{1-n(\omega)}{l}, \quad (l).$$

[*Kummer*[20].]

Beweis. Es bedeute $\omega(x)$ die zu ω gehörende Function, und es werde

$$F(x) = \prod_{(g)} \omega(1+x(\zeta^g-1))$$

gesetzt, wo das Product über die Werte $g = 0, 1, 2, \ldots, l-1$ zu erstrecken ist. Der Ausdruck $F(x)$ stellt eine ganzzahlige Function von x dar, und die Coefficienten aller durch x^l teilbaren Glieder dieser Function sind offenbar durch λ^l und folglich wegen der Rationalität der Coefficienten auch durch l^2 teilbar. Durch Entwickelung nach Potenzen von x ergiebt sich nun:

$$(85.)\quad \begin{cases} \log\omega(1+x(\xi-1)) = \dfrac{\xi-1}{1!}\,x\left[\dfrac{\mathrm{d}\log\omega(x)}{\mathrm{d}x}\right]_{x=1} \\[2ex] \qquad +\dfrac{(\xi-1)^2}{2!}\,x^2\left[\dfrac{\mathrm{d}^2\log\omega(x)}{\mathrm{d}x^2}\right]_{x=1}+\cdots \\[2ex] \qquad \cdots+\dfrac{(\xi-1)^{l-1}}{l-1!}\,x^{l-1}\left[\dfrac{\mathrm{d}^{l-1}\log\omega(x)}{\mathrm{d}x^{l-1}}\right]_{x=1}+\cdots. \end{cases}$$

Setzen wir erstens in dieser Entwickelung der Reihe nach

$$\xi = 1,\ \zeta,\ \zeta^2,\ \ldots,\ \zeta^{l-1}$$

ein und addiren die betreffenden Formeln, so entsteht unter Berücksichtigung von

$$(\zeta-1)^g+(\zeta^2-1)^g+\cdots+(\zeta^{l-1}-1)^g = (-1)^g l$$
$$(g=1, 2, \ldots, l-1)$$

die Gleichung:

$$(86.)\quad \begin{cases} \log F(x) = l\Big\{-\dfrac{x}{1!}\left[\dfrac{\mathrm{d}\log\omega(x)}{\mathrm{d}x}\right]_{x=1} \\ \qquad +\dfrac{x^2}{2!}\left[\dfrac{\mathrm{d}^2\log\omega(x)}{\mathrm{d}x^2}\right]_{x=1}-\cdots \\ \qquad \cdots+\dfrac{x^{l-1}}{l-1!}\left[\dfrac{\mathrm{d}^{l-1}\log\omega(x)}{\mathrm{d}x^{l-1}}\right]_{x=1}\Big\}+x^l G, \end{cases}$$

wobei $x^l G$ das Aggregat der durch x^l teilbaren Glieder der Entwickelung andeutet.

Setzen wir zweitens in der Entwickelung (85.) $\xi=\mathrm{e}^v$ ein und bilden den $(l-1)$ten Differentialquotienten nach v, so wird derselbe für $v=0$:

$$(87.)\quad \begin{cases} \left[\dfrac{\mathrm{d}^{l-1}\log\omega(1+x(\mathrm{e}^v_\xi-1))}{\mathrm{d}v^{l-1}}\right]_{v=0} = \dfrac{x}{1!}\left[\dfrac{\mathrm{d}\log\omega(x)}{\mathrm{d}x}\right]_{x=1} \\ \qquad +\dfrac{2^{l-1}-2.1^{l-1}}{2!}x^2\left[\dfrac{\mathrm{d}^2\log\omega(x)}{\mathrm{d}x^2}\right]_{x=1} \\ \qquad +\dfrac{3^{l-1}-3.2^{l-1}+3.1^{l-1}}{3!}x^3\left[\dfrac{\mathrm{d}^3\log\omega(x)}{\mathrm{d}x^3}\right]_{x=1} \\ \qquad +\dfrac{(l-1)^{l-1}-\cdots-(l-1)1^{l-1}}{l-1!}x^{l-1}\left[\dfrac{\mathrm{d}^{l-1}\log\omega(x)}{\mathrm{d}x^{l-1}}\right]_{x=1} \\ \qquad \equiv \dfrac{x}{1!}\left[\dfrac{\mathrm{d}\log\omega(x)}{\mathrm{d}x}\right]_{x=1}-\dfrac{x^2}{2!}\left[\dfrac{\mathrm{d}^2\log\omega(x)}{\mathrm{d}x^2}\right]_{x=1}+\cdots \\ \qquad \cdots-\dfrac{x^{l-1}}{l-1!}\left[\dfrac{\mathrm{d}^{l-1}\log\omega(x)}{\mathrm{d}x^{l-1}}\right]_{x=1}, \quad (l). \end{cases}$$

Durch Vergleichung der beiden Formeln (86.) und (87.) ergiebt sich

$$\log F(x) \equiv -l\left[\frac{\mathrm{d}^{l-1}\log\omega(1+x(\mathrm{e}^v-1))}{\mathrm{d}v^{l-1}}\right]_{v=0}, \quad (l^2),$$

d. h. die Coefficienten von $x, x^2, \ldots, x^{l-1}$ auf der linken Seite sind den entsprechenden Coefficienten rechts nach l^2 congruent, und wenn wir beide Seiten dieser Congruenz in den Exponenten von e setzen, so erhalten wir zunächst in demselben Sinne, dann aber mit Rücksicht auf die zu Beginn dieses Beweises gemachte Bemerkung auch vollständig die Congruenz der zwei ganzzahligen Functionen:

$$F(x) \equiv 1 - l\left[\frac{\mathrm{d}^{l-1}\log\omega(1+x(\mathrm{e}^v-1))}{\mathrm{d}v^{l-1}}\right]_{v=0}, \quad (l^2),$$

und folglich für $x = 1$:

$$n(\omega) \equiv 1 - l.\mathrm{l}^{(l-1)}(\omega), \quad (l^2),$$

womit der Hülfssatz 24 bewiesen ist.

Hülfssatz 25. Wenn die ganzen Zahlen ν, μ in $k(\zeta)$ die Congruenzeigenschaften $\nu \equiv 1$ nach $\mathfrak{l}$ und $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ besitzen, und wenn ausserdem ν congruent der Relativnorm einer ganzen Zahl A des durch $M = \sqrt[l]{\mu}$ bestimmten Kummer'schen Körpers $k(M, \zeta)$ nach $\mathfrak{l}^l$ ist, so existirt eine ganzzahlige Function $f(x)$ vom $(l-1)$ten Grade in x, derart, dass $f(1) > 0$ ist und die Congruenzen

$$n(f(\zeta)) \equiv 1, \quad (l^2)$$

und

$$\nu \equiv f(\mu), \quad (\mathfrak{l}^l)$$

erfüllt sind. [*Kummer*[20].]

Beweis. Nach dem Beweise des Hülfssatzes 23 ist jede ganze Zahl A in $k(M, \zeta)$ in der Gestalt

$$A = \frac{\gamma + \gamma_1(M-1) + \cdots + \gamma_{l-1}(M-1)^{l-1}}{\delta}$$

und folglich auch in der Gestalt

$$A = \frac{\beta + \beta_1 M + \cdots + \beta_{l-1} M^{l-1}}{\delta}$$

darstellbar, so dass $\gamma, \gamma_1, \ldots, \gamma_{l-1}$, δ und $\beta, \beta_1, \ldots, \beta_{l-1}$ ganze Zahlen in $k(\zeta)$ sind und überdies δ zu $\mathfrak{l}$ prim ausfällt. Infolge des letzteren Umstandes können wir

$$A \equiv \alpha + \alpha_1 M + \cdots + \alpha_{l-1} M^{l-1}, \quad (\mathfrak{l}^l)$$

setzen in solcher Weise, dass $\alpha, \alpha_1, \ldots, \alpha_{l-1}$ ganze Zahlen in $k(\zeta)$ sind. Es sei nun

$$\alpha \equiv a^*, \quad \alpha_1 \equiv a_1^*, \quad \ldots, \quad \alpha_{l-1} \equiv a_{l-1}^*, \quad (\mathfrak{l}),$$

wo a^*, a, $\ldots$, a_{l-1}^* ganze rationale positive Zahlen bedeuten sollen; wir setzen

$$f^*(x) = a^* + a_1^* x + \cdots + a_{l-1}^* x^{l-1}.$$

Da in $k(M, \zeta)$ sich $\mathfrak{l} = \mathfrak{L}^l$ und $M \equiv 1$ nach $\mathfrak{L}$ erweist, so folgt

$$A \equiv a + a_1 + \cdots + a_{l-1} \equiv a^* + a_1^* + \cdots + a_{l-1}^*, \quad (\mathfrak{L}).$$

Ist nun A die vorausgesetzte Zahl, für welche $N_k(A) \equiv \nu$ nach $\mathfrak{l}^l$ wird, so erhalten wir weiter

$$\nu \equiv N_k(A) \equiv a^* + a_1^* + \cdots + a_{l-1}^* \equiv 1, \quad (\mathfrak{L})$$

also auch

$$(88.) \qquad a^* + a_1^* + \cdots + a_{l-1}^* \equiv 1, \quad (l).$$

Folglich ist $f^*(\zeta)$ eine Zahl in $k(\zeta)$ mit der Congruenzeigenschaft $f^*(\zeta) \equiv 1$ nach $\mathfrak{l}$. Wir finden nun mit Rücksicht hierauf leicht eine ganze rationale positive Zahl b derart, dass die Norm der Zahl $f(\zeta) = f^*(\zeta) + lb$ im Körper $k(\zeta)$ der Congruenz

$$(89.) \qquad n(f(\zeta)) \equiv 1, \quad (l^2)$$

genügt; dann erfüllt die ganzzahlige Function

$$f(x) = f^*(x) + lb = a + a_1 x + \cdots + a_{l-1} x^{l-1}$$

die Bedingungen des zu beweisenden Hülfssatzes 25. Denn es ist offenbar $A = f(M) + \lambda B$, wo B eine ganze Zahl in $k(M, \zeta)$ bedeutet. Hieraus ergiebt sich leicht durch eine ähnliche Betrachtung wie auf S. 409:

$$(90.) \qquad \nu \equiv N_k(A) \equiv N_k(f(M)), \quad (\mathfrak{l}^l).$$

Andererseits erkennen wir unter Berücksichtigung der Congruenzen

$$a^l \equiv a, \quad a_1^l \equiv a_1, \quad \ldots, \quad a_{l-1}^l \equiv a_{l-1}, \quad (l),$$

dass identisch in x eine Gleichung

$$(91.) \qquad f(x) f(\zeta x) \ldots f(\zeta^{l-1} x) = f(x^l) + l F(x^l)$$

gilt, wo $F(x^l)$ eine ganzzahlige Function von x^l bedeutet. Diese Gleichung liefert für $x = 1$ mit Rücksicht auf (89.) die Congruenz

$$f(1) \equiv f(1) + l F(1), \quad (l^2), \qquad \text{d. h.} \qquad F(1) \equiv 0, \quad (l).$$

Wenn in der Gleichung (91.) $x = M$ genommen wird, so ergiebt sich

$$N_k(f(M)) = f(\mu) + l F(\mu)$$

und hieraus, da $F(\mu) \equiv F(1) \equiv 0$ nach $\mathfrak{l}$ ausfällt,

$$N_k(f(M)) \equiv f(\mu), \quad (\mathfrak{l}^l),$$

d. i. wegen (90.)

$$\nu \equiv f(\mu), \quad (\mathfrak{l}^l).$$

Damit und in Anbetracht von (89.) ist der Hülfssatz 25 vollständig bewiesen.

Hülfssatz 26. Wenn ν, μ ganze Zahlen in $k(\zeta)$ mit den Congruenzeigenschaften $\nu \equiv 1$ nach $\mathfrak{l}$ und $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ bedeuten, und wenn ausserdem ν Normenrest des durch $M = \sqrt[l]{\mu}$ bestimmten Kummer'schen Körpers $k(M, \zeta)$ nach $\mathfrak{l}$ ist, so wird stets

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = 1.$$

[*Kummer*[20].]

Beweis. Aus der bekannten Lagrange'schen Formel für die Umkehrung einer Potenzreihe entnimmt man unmittelbar die folgende Identität:

$$(92.) \quad \left[\frac{\mathrm{d}^{l-1} F(v)}{\mathrm{d} V^{l-1}}\right]_{V=0} = \left[\frac{\mathrm{d}^{l-2} \dfrac{\mathrm{d}F(v)}{\mathrm{d}v} (\varphi(v))^{l-1}}{\mathrm{d}v^{l-2}}\right]_{v=0};$$

dabei stelle man sich unter $F(v)$ eine beliebige Potenzreihe von v, ferner unter $\varphi(v)$ eine Potenzreihe vor, deren constantes Glied von 0 verschieden ist, und denke sich den Zusammenhang der Variabeln v und V durch die Gleichung $V\varphi(v) - v = 0$ vermittelt.

Es seien nun $\nu(x)$ und $\mu(x)$ die zu den Zahlen ν und μ gehörenden Functionen. Da ν Normenrest des Körpers $k(M, \zeta)$ nach $\mathfrak{l}$ sein soll, so giebt es nach Hülfssatz 25 eine ganzzahlige Function $(l-1)$ten Grades $f(x)$ derart, dass

$$(93.) \qquad n(f(\zeta)) \equiv 1, \quad (l^2),$$

$$(94.) \qquad \nu \equiv f(\mu), \quad (\mathfrak{l}^l)$$

und $f(1) > 0$ wird.

Wir setzen nun

$$F(v) = \log f(\mu(e^v)),$$

$$V = \log \mu(e^v),$$

$$\varphi(v) = \frac{v}{\log \mu(e^v)};$$

diese Functionen werden nur an der Stelle $v = 0$ betrachtet werden, und es sollen die Logarithmen so genommen werden, dass sie für $v = 0$ reell sind.

Ersetzen wir die Zeichen ω, $\varpi(x)$, v in der zweiten Formel auf S. 413 oben bez. durch $f(\zeta)$, $f(x)$, V, so wird aus derselben

$$\left[\frac{\mathrm{d}^{l-1}\log f(\mathrm{e}^V)}{\mathrm{d}V^{l-1}}\right]_{V=0} \equiv \mathrm{l}^{(l-1)}(f(\zeta)) + \frac{1-f(1)}{l}, \quad (l).$$

Aus Hülfssatz 24 ergiebt sich unter Berücksichtigung von (93.) die Congruenz

$$\mathrm{l}^{(l-1)}(f(\zeta)) \equiv 0, \quad (l)$$

und folglich wird

$$(95.)\quad \left[\frac{\mathrm{d}^{l-1}F(v)}{\mathrm{d}V^{l-1}}\right]_{V=0} = \left[\frac{\mathrm{d}^{l-1}\log f(\mathrm{e}^V)}{\mathrm{d}V^{l-1}}\right]_{V=0} \equiv \frac{1-f(1)}{l}, \quad (l).$$

Andererseits gilt mit Rücksicht auf (94.) die Congruenz

$$f(\mu(\mathrm{e}^v)) \equiv \nu(\mathrm{e}^v) + \frac{f(1)-1}{l}\, v^{l-1}, \quad (l),$$

welche so aufzufassen ist, dass in den Entwickelungen nach Potenzen von v die Coefficienten von $1, v, \ldots, v^{l-1}$ auf den beiden Seiten einander nach l congruent sind, und hieraus ergiebt sich die Entwickelung

$$(96.)\quad \begin{cases} \dfrac{\mathrm{d}F(v)}{\mathrm{d}v} \equiv \mathrm{l}^{(1)}(\nu) + \mathrm{l}^{(2)}(\nu)\dfrac{v}{1!} + \mathrm{l}^{(3)}(\nu)\dfrac{v^2}{2!} + \cdots \\ \qquad \cdots + \left(\mathrm{l}^{(l-1)}(\nu) + \dfrac{1-f(1)}{l}\right)\dfrac{v^{l-2}}{(l-2)!}, \quad (l), \end{cases}$$

welche so aufzufassen ist, dass die Coefficienten von $1, v, \ldots, v^{l-2}$ auf den beiden Seiten einander nach l congruent sind.

Endlich betrachten wir die Function $\varphi(v)$. Wegen $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ wird $\varphi(v)$ eine Potenzreihe, deren constantes Glied $\equiv -1$ nach l ist. Ferner folgt leicht

$$(\varphi(v))^l \equiv \varphi(v^l) \equiv \varphi(0) \equiv -1, \quad (l)$$

in dem Sinne, dass die Coefficienten von $1, v, \ldots, v^{l-2}$ auf den beiden Seiten einander nach l congruent sind. Es gilt daher weiter in demselben Sinne

$$-(\varphi(v))^{l-1} \equiv \frac{\log\mu(\mathrm{e}^v)}{v}, \quad (l),$$

und es folgt hieraus endlich in eben demselben Sinne die Entwickelung

$$(97.)\quad \begin{cases} -(\varphi(v))^{l-1} \equiv \mathrm{l}^{(1)}(\mu) + \mathrm{l}^{(2)}(\mu)\dfrac{v}{2!} + \mathrm{l}^{(3)}(\mu)\dfrac{v^2}{3!} + \cdots \\ \qquad \cdots + \mathrm{l}^{(l-1)}(\mu)\dfrac{v^{l-2}}{(l-1)!}, \quad (l). \end{cases}$$

Die Zusammenstellung der Congruenz (95.) und der beiden Entwickelungen (96.), (97.) mit (92.) liefert, wegen $\mathfrak{l}^{(1)}(\mu) \equiv -1$ und $(l-g)!(g-1)! \equiv (-1)^g$ nach $\mathfrak{l}$ für $g = 1, 2, \ldots, l-1$, die folgende Congruenz:

$$\mathfrak{l}^{l-1}(\nu)\mathfrak{l}^{(1)}(\mu) - \mathfrak{l}^{(l-2)}(\nu)\mathfrak{l}^{(2)}(\mu) + \cdots - \mathfrak{l}^{(1)}(\nu)\mathfrak{l}^{(l-1)}(\mu) \equiv 0, \quad (\mathfrak{l}),$$

d. i. nach der Definition (82.) des Symbols $\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\}$ in § 131:

$$\left\{\frac{\nu, \mu}{\mathfrak{l}}\right\} = 1,$$

und hiermit ist der Hülfssatz 26 bewiesen.

§ 133.

Das Symbol $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$ zur Unterscheidung zwischen Normenresten und Normennichtresten.

Wir sind jetzt in den Stand gesetzt, soweit die betreffenden Symbole bereits definirt sind, die Richtigkeit der folgenden Behauptung einzusehen:

Satz 151. Wenn ν, μ zwei beliebige ganze Zahlen in $k(\zeta)$ sind, nur dass $\sqrt[l]{\mu}$ nicht in $k(\zeta)$ liegt, und wenn $\mathfrak{w}$ ein beliebiges Primideal des Kreiskörpers $k(\zeta)$ bedeutet, so ist ν Normenrest oder Normennichtrest des durch $M = \sqrt[l]{\mu}$ bestimmten Kummer'schen Körpers $k(M, \zeta)$ nach $\mathfrak{w}$, je nachdem

$$\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = 1 \quad \text{oder} \quad \neq 1$$

ausfällt.

Beweis. Es sei zunächst das Primideal $\mathfrak{w}$ von $\mathfrak{l}$ verschieden und gehe nicht in der Relativdiscriminante des Körpers $k(M, \zeta)$ auf. Ist μ^* eine ganze Zahl in $k(\zeta)$ derart, dass $\frac{\mu^*}{\mu}$ die $l$te Potenz einer Zahl in $k(\zeta)$ ist, so gilt stets $\left\{\frac{\nu, \mu^*}{\mathfrak{w}}\right\} = \left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}$; danach und mit Rücksicht auf Satz 148 können wir hier annehmen, dass μ nicht durch $\mathfrak{w}$ teilbar ist. Wir unterscheiden zwei Fälle, je nachdem $\mathfrak{w}$ im Körper $k(M, \zeta)$ als Product von l Primidealen $\mathfrak{W}_1, \ldots, \mathfrak{W}_l$ darstellbar wird oder in

$k(M, \zeta)$ Primideal bleibt. Nach Satz 149 ist im ersteren Falle $\left\{\frac{\mu}{\mathfrak{w}}\right\} = 1$, im letzteren $\left\{\frac{\mu}{\mathfrak{w}}\right\} \neq 1$ und $\neq 0$.

Im ersteren Falle bestimmen wir eine ganze Zahl A in $k(M, \zeta)$, welche durch $\mathfrak{W}_1$, aber nicht durch $\mathfrak{W}_1^2$ und auch nicht durch eines der Primideale $\mathfrak{W}_2, \ldots, \mathfrak{W}_l$ teilbar ist; dann geht in der Relativnorm $\alpha = N_k(A)$ das Primideal $\mathfrak{w}$ genau zur ersten Potenz auf. Ist nun $\mathfrak{w}^b$ die in ν enthaltene Potenz von $\mathfrak{w}$, so lässt sich $x = \frac{\nu}{\alpha^b}$ als ein Bruch schreiben, dessen Zähler und Nenner zu $\mathfrak{w}$ prim sind, und folglich sind Zähler und Nenner dieses Bruches nach Satz 150 Normenreste des Körpers $k(M, \zeta)$ nach $\mathfrak{w}$. Das Gleiche gilt also auch von ν. Da nach der Definition in § 131

$$\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = \left\{\frac{\mu^b}{\mathfrak{w}}\right\}^{-1} = 1$$

ist, so erweist sich im ersteren Falle der Satz 151 als richtig.

Im zweiten Falle ist die Relativnorm einer ganzen Zahl A in $k(M, \zeta)$ jedesmal genau durch eine solche Potenz von $\mathfrak{w}$ teilbar, deren Exponent ein Vielfaches von l ist. Es sei wiederum $\mathfrak{w}^b$ die in ν enthaltene Potenz von $\mathfrak{w}$; ist dann b kein Vielfaches von l, so kann also ν nicht Normenrest nach $\mathfrak{w}$ sein; in diesem Falle wird andererseits $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = \left\{\frac{\mu^b}{\mathfrak{w}}\right\}^{-1} \neq 1$. Ist dagegen b ein Vielfaches von l, und bedeutet α eine ganze durch $\mathfrak{w}$, aber nicht durch $\mathfrak{w}^2$ teilbare Zahl in $k(\zeta)$, so setzen wir $x = \frac{\nu}{\alpha^b}$ und erkennen, wie im ersteren Falle ν als Normenrest nach $\mathfrak{w}$; andererseits ist jetzt

$$\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\} = \left\{\frac{\mu^b}{\mathfrak{w}}\right\}^{-1} = 1.$$

Damit ist der Satz 151 auch für den zweiten Fall bewiesen.

II Wir nehmen jetzt an, es sei die Relativdiscriminante des Körpers $k(M, \zeta)$ durch das Primideal $\mathfrak{w}$ teilbar; $\mathfrak{w}$ soll dabei von $\mathfrak{l}$ verschieden sein. Es gehe $\mathfrak{w}$ in ν genau zur $b$ten und in μ genau zur $a$ten Potenz auf; dann ist a jedenfalls kein Vielfaches von l. Die Zahl $x = \frac{\nu^a}{\mu^b}$ lässt sich in die Gestalt eines Bruches $\frac{\varrho}{\sigma}$ setzen, dessen Zähler ϱ und dessen Nenner σ zu $\mathfrak{w}$ prim sind. Die Zahl $\varrho\sigma^{l-1}$ ist eine nicht durch $\mathfrak{w}$ teilbare ganze Zahl; nach dem Beweise des Satzes 150 auf S. 406 ist

¹) nach Satz 148, § 393

eine solche ganze Zahl dann und nur dann Normenrest des Körpers $k(M, \zeta)$ nach $\mathfrak{w}$, wenn sie $l$ter Potenzrest nach $\mathfrak{w}$ ist, d. i. hier, wenn $\left\{\frac{\varrho\sigma^{l-1}}{\mathfrak{w}}\right\}=1$ und also $\left\{\frac{\nu, \mu}{\mathfrak{w}}\right\}=1$ ist; damit ist für den gegenwärtigen Fall wiederum der Satz 151 als richtig erkannt.

Es sei endlich $\mathfrak{w}=\mathfrak{l}$. Wir fassen lediglich den Fall ins Auge, dass $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ ist: es ist dies der einzige Fall, für den wir die betreffenden Sätze späterhin brauchen werden; die anderen Fälle gestatten übrigens eine ähnliche Behandlung. Beim Beweise machen wir noch die nicht wesentlich einschränkende Annahme $\nu \equiv 1$ nach $\mathfrak{l}$. Wegen der Annahme $\mu \equiv 1+\lambda$ nach $\mathfrak{l}^2$ kann man laut Satz 150 genau l^{l-1} Normenreste ν^* des Körpers $k(M, \zeta)$ nach $\mathfrak{l}$ bilden, welche congruent 1 nach $\mathfrak{l}$ ausfallen und unter einander nach $\mathfrak{l}^{l+1}$ incongruent sind. Andererseits muss ein jeder Normenrest ν^* von $k(M, \zeta)$ nach $\mathfrak{l}$, für den man $\nu^* \equiv 1$ nach $\mathfrak{l}$ hat, laut Hülfssatz 26 die Bedingung $\left\{\frac{\nu^*, \mu}{\mathfrak{l}}\right\}=1$ erfüllen. Wegen

$$\left.\begin{array}{l}
\mathfrak{l}^{(1)}(\mu) \equiv -1, \\
\mathfrak{l}^{(1)}(1-l) \equiv 0, \quad \mathfrak{l}^{(2)}(1-l) \equiv 0, \quad \ldots, \quad \mathfrak{l}^{(l-2)}(1-l) \equiv 0, \\
\mathfrak{l}^{(l-1)}(1-l) \equiv \dfrac{1-n(1-l)}{l} \equiv -1,
\end{array}\right\} \quad (l)$$

ergiebt sich nach (82.)

$$\left\{\frac{1-l, \mu}{\mathfrak{l}}\right\}=\zeta^{-1}. \tag{98.}$$

Es sei nun α irgend eine erste ganze Zahl in $k(\zeta)$ mit der Congruenzeigenschaft $\alpha \equiv 1$ nach $\mathfrak{l}$, und es werde $\left\{\frac{\alpha, \mu}{\mathfrak{l}}\right\}=\zeta^a$ gesetzt, wo a eine Zahl aus der Reihe $0, 1, 2, \ldots, l-1$ bedeuten soll; dann ist offenbar $\left\{\frac{\alpha(1-l)^a, \mu}{\mathfrak{l}}\right\}=1$; dagegen fällt jedesmal $\left\{\frac{\alpha(1-l)^x, \mu}{\mathfrak{l}}\right\} \neq 1$ aus, wenn x eine von a verschiedene Zahl aus der Reihe $0, 1, 2, \ldots, l-1$ bedeutet. Wählen wir ferner eine ganze Zahl α' in $k(\zeta)$, welche ebenfalls congruent 1 nach $\mathfrak{l}$, aber keiner der l Zahlen $\alpha, \alpha(1-l), \alpha(1-l)^2, \ldots, \alpha(1-l)^{l-1}$ nach $\mathfrak{l}^{l+1}$ congruent ist, so sind auch die l Zahlen $\alpha', \alpha'(1-l), \alpha'(1-l)^2, \ldots, \alpha'(1-l)^{l-1}$ nach $\mathfrak{l}^{l+1}$ sämtlich unter einander incongruent und zugleich keiner der ersteren l Zahlen congruent; unter den letzteren l Zahlen giebt es wegen (98.) offenbar eine und nur eine Zahl — es sei dies etwa $\alpha'(1-l)^{a'}$ — von der Art, dass $\left\{\frac{\alpha'(1-l)^{a'},\ \mu}{\mathfrak{l}}\right\}=1$ ist. Fahren wir in dieser Weise fort, so erkennen wir, dass die Anzahl der vorhandenen nach $\mathfrak{l}^{l+1}$ incongruenten Zahlen ν, die congruent 1 nach $\mathfrak{l}$ sind und der Bedingung $\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\}=1$ genügen, genau gleich l^{l-1} ist, und aus der Uebereinstimmung dieser Anzahl mit der oben gefundenen für die Normenreste ν^* ist ersichtlich, dass umgekehrt auch jede Zahl ν mit diesen zwei Eigenschaften Normenrest des Körpers $k(M,\zeta)$ nach $\mathfrak{l}$ ist.

Durch die bisherigen Ueberlegungen ist der Satz 151 in allen Teilen bewiesen; für den Fall $\mathfrak{w}=\mathfrak{l}$ allerdings nur soweit, als für die Zahlen ν, μ die Congruenzeigenschaften $\nu\equiv 1$ nach $\mathfrak{l}$ und $\mu\equiv 1+\lambda$ nach $\mathfrak{l}^2$ erfüllt sind. Die ν betreffende Einschränkung ist offenbar leicht aufzuheben.

Aus dem Satze 151 folgt, bei Benutzung der ersten Formel in (80.) und (83.), die Formel

$$\left\{\frac{\nu\nu^*,\ \mu}{\mathfrak{w}}\right\}=\left\{\frac{\nu,\ \mu}{\mathfrak{w}}\right\},$$

wo $\mathfrak{w}$ ein beliebiges Primideal in $k(\zeta)$ bedeutet und ν^* ein Normenrest des Körpers $k(M,\zeta)$ nach $\mathfrak{w}$ sein soll.

Um nun das Symbol $\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\}$ auch für den Fall zu definiren, dass eine der beiden Zahlen ν, μ oder beide durch $\mathfrak{l}$ theilbar sind, braucht man nur die allgemeine Gültigkeit der Formeln

$$\left\{\frac{\nu\nu^*,\ \mu}{\mathfrak{l}}\right\}=\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\},\quad \left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\}\left\{\frac{\mu,\ \nu}{\mathfrak{l}}\right\}=1$$

festzusetzen, wobei ν^* ein beliebiger Normenrest des Körpers $k(\sqrt[l]{\mu},\ \zeta)$ nach $\mathfrak{l}$ bedeuten soll. Bei dieser Festsetzung folgt dann insbesondere

$$\left\{\frac{1+a\lambda^l,\ \lambda}{\mathfrak{l}}\right\}=\left\{\frac{1+a\lambda^l}{\mathfrak{l}}\right\}=\zeta^a.$$

Wir können überhaupt die Definition des **Symbols** $\left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\}$ auf die Formeln

$$\left\{\frac{\alpha,\ \zeta}{\mathfrak{l}}\right\}=\zeta^{\frac{n(\alpha)-1}{l}},\quad \left\{\frac{\nu_1\nu_2,\ \mu}{\mathfrak{l}}\right\}=\left\{\frac{\nu_1,\ \mu}{\mathfrak{l}}\right\}\left\{\frac{\nu_2,\ \mu}{\mathfrak{l}}\right\},$$

$$\left\{\frac{\nu^*,\ \mu}{\mathfrak{l}}\right\}=1,\quad \left\{\frac{\nu,\ \mu}{\mathfrak{l}}\right\}\left\{\frac{\mu,\ \nu}{\mathfrak{l}}\right\}=1$$