

## ÜBER DIE METACYKLISCHEN GLEICHUNGEN VON PRIMZAHLGRAD

VON

A. WIMAN

in UPSALA.

### § 1. *Referat über die Arbeiten von Abel, Kronecker und Herrn Weber.*

Wie lebhaft sich ABEL für das Problem der algebraischen Auflösung der Gleichungen interessiert hat, ist aus wiederholten Äusserungen in seinen Briefen ersichtlich.<sup>1</sup> Zunächst war es ihm gelungen den ersten vollständigen Beweis zu erbringen, dass die allgemeinen Gleichungen von höherem als dem vierten Grade nicht durch Radikale auflösbar oder, wie wir mit Herrn WEBER sagen wollen, nicht metacyklisch sind. Durch eine Vertiefung der hierbei angewandten Methode wollte er alsdann zeigen, wie man alle metacyklischen Gleichungen aufstellen kann.<sup>2</sup> Seine diesbezüglichen Untersuchungen waren leider bei seinem frühzeitigen Tode unvollendet. So hat er die wichtigen Sätze, vermitteltst deren die Aufgabe auf primitive metacyklische Gleichungen von Primzahlpotenzgrad reduziert wird, ohne Beweis hinterlassen (Oeuvres II, p. 222). Bezüglich der metacyklischen Gleichungen vom 5. Grade hat er in einem Briefe an CRELLE (Oeuvres II, p. 266) die allgemeine Gestalt der Wurzeln angegeben. Eine entsprechende Darstellung für die Wurzeln einer metacyklischen Gleichung

---

<sup>1</sup> In einem Briefe an HOLMBOE (Oeuvres II, p. 260) bezeichnet er diese Aufgabe als sein »Thème favori«.

<sup>2</sup> Hier lassen wir unerörtert die wichtigen Klassen von *speciellen* metacyklischen Gleichungen, welche ABEL entdeckt hat, wie die nach ihm benannten ABEL'schen, sowie die damit verwandten Gleichungen der komplexen Multiplikation.

von einem beliebigen Primzahlgrade  $p$  wurde von KRONECKER bei seiner Wiederaufnahme des Problems gegeben.<sup>1</sup> Hierbei treten als Endradikale die  $p^{\text{ten}}$  Wurzeln aus gewissen Grössen  $r$  auf, welche ihrerseits einer cyklischen Gleichung vom Grade  $n$  genügen, wobei  $n$  einen Teiler von  $p - 1$  bedeutet. In seiner späteren Note gab KRONECKER für diese Grössen  $r$  explicite Ausdrücke durch Kreisteilungsgrössen, wobei er den freilich erst in neuerer Zeit von den Herren WEBER und HILBERT bewiesenen Satz benutzte, dass alle im absoluten Rationalitätsbereiche ABEL'schen Körper Kreisteilungskörper sind. Es war aber noch kein Beweis gegeben, dass die Wurzeln einer metacyklischen Gleichung von Primzahlgrad sich wirklich in der angegebenen Weise darstellen lassen. Ein solcher wurde erst von Herrn WEBER erbracht.<sup>2</sup> Die Form der Wurzeln, um welche es sich bei diesem Beweise handelt, ist jedoch in gewissen Fällen nicht als die eigentlich naturgemässe zu betrachten. In der Tat hatte schon KRONECKER, wie oben angedeutet wurde, eine Fallunterscheidung eingeführt. Die verschiedenen Fälle beziehen sich, wie wir hier zeigen wollen, in ziemlich komplizierter Weise einerseits auf die Gruppe der Gleichung, andererseits auf die verschiedenen Möglichkeiten betreffend den gemeinsamen Unterkörper des durch die Wurzeln der Gleichung gebildeten Körpers und des Körpers der  $p^{\text{ten}}$  Einheitswurzeln.

## § 2. Die Gruppe des Körpers $R(x, \varepsilon)$ .

Es sei mit  $R$  der zu Grunde gelegte Rationalitätsbereich bezeichnet. Die Wurzeln  $x_0, x_1, \dots, x_{p-1}$  der Gleichung bestimmen einen Körper  $R(x)$  über  $R$ . Werden hierzu noch die  $p^{\text{ten}}$  Einheitswurzeln adjungiert, so erhält man einen Körper  $R(x, \varepsilon)$ .

Die am Ende des vorigen Paragraphen besprochenen Verhältnisse beruhen nun darauf, dass die einzelnen Radikale, welche in den Ausdrücken für die Wurzeln auftreten, nicht dem Körper  $R(x)$ , sondern erst dem Körper  $R(x, \varepsilon)$  angehören. Da es sich also um Grössen in diesem Körper

<sup>1</sup> Berl. Ber. 1853, p. 365; 1856, p. 203. Doch ist es, nach den unvollständigen Notizen zu urteilen, welche aus dem Nachlasse ABEL's hierüber publiziert worden sind (Oeuvres II, p. 233—243), höchst wahrscheinlich, dass schon ABEL die fragliche Darstellung gekannt hat.

<sup>2</sup> Marb. Ber. 1892, p. 3; Algebra I, Abschn. 18.

handelt, so ist zunächst die zugehörige Gruppe zu bestimmen. Da die Gleichung irreduktibel sein soll, so lassen sich die Wurzeln in solcher Weise ordnen, dass für

$$(S) \quad x'_i = x_{i+1}$$

$$(T) \quad x'_i = x_{ie^g} \quad (i=0, 1, \dots, p-1)$$

die Gruppe  $G$  des Körpers  $R(x)$  durch die Substitutionen  $S$  und  $T$  erzeugt wird,<sup>1</sup> wobei die Indices nach dem Modul  $p$  genommen werden sollen,  $g$  eine Primitivzahl nach  $p$ , und  $e$  einen Teiler von  $p-1$  bedeutet. Die Gruppe  $G$  hat dann die Gradzahl  $\frac{p(p-1)}{e}$ .

Die Grösse  $\varepsilon = e^{\frac{2\pi i}{p}}$  bestimmt bekanntlich über den Körper der rationalen Zahlen einen Körper  $k(\varepsilon)$  vom Grade  $p-1$ , dessen Gruppe durch die Substitution  $U = (\varepsilon : \varepsilon^g)$  erzeugt wird. Der Einfachheit halber machen wir, falls nicht ausdrücklich anderes vorausgesetzt wird, die Annahme, im Rationalitätsbereiche  $R$  sei kein höherer Unterkörper von  $k(\varepsilon)$  als der Körper der rationalen Zahlen enthalten. Der Körper  $R(\varepsilon)$  über  $R$  hat dann ebenfalls den Grad  $p-1$ , und die Gruppe  $T$  dieses Körpers lässt sich durch  $U$  erzeugen.

Den gemeinsamen Unterkörper, welchen die über  $R$  aufgebauten Körper  $R(x)$  und  $R(\varepsilon)$  gemein haben, bezeichnen wir mit  $R(\sigma)$ , wo  $\sigma$  eine den Körper bestimmende Grösse bedeutet. Dieser Körper muss zu ausgezeichneten Untergruppen von sowohl  $G$  als  $T$  gehören, welche je von gleichem Index sein sollen. Die ausgezeichneten Untergruppen von  $G$  sind nun den Teilern von  $\frac{p-1}{e}$  zugeordnet, so dass zu jedem solchen Teiler  $e_1$  eine durch  $S$  und  $T^{e_1}$  erzeugte Gruppe gehört. Den gleichen Index  $e_1$  besitzt die durch  $U^{e_1}$  erzeugte Untergruppe von  $T$ . Sowohl durch  $T$  als durch  $U$  wird offenbar die Reihe der zu  $\sigma$  conjugierten Grössen  $\sigma, \sigma_1, \dots, \sigma_{e_1-1}$  cyklisch verschoben, und es giebt für  $e_1 > 1$  immer eine Operation  $U^l$ , wo  $l$  eine relative Primzahl gegen  $e_1$  sein muss, welche dieselbe Verschiebung wie  $T$  bewirkt.

Die Gruppe  $\Delta$  des Körpers  $R(x, \varepsilon)$  lässt sich durch die Substitutionen ausdrücken, denen bei ihr die den Körper bestimmenden Grössen  $x$  und  $\varepsilon$  unterworfen werden. Wie sofort ersichtlich, dürfen bei  $\Delta$  nur solche Sub-

<sup>1</sup> Vergl. GALOIS, oeuvr., p. 47.

stitutionen in  $R(x)$  und  $R(\varepsilon)$  gleichzeitig ausgeführt werden, bei denen die Grösse  $\sigma$  in dieselbe conjugierte Grösse übergeführt wird. Umgekehrt muss auch  $\Delta$  alle Operationen von dieser Eigenschaft enthalten, denn anderenfalls wäre der Grad von  $\Delta$  nicht  $\frac{p-1}{e_1}$  mal so gross als der Grad von  $G$ . Dies muss aber der Fall sein, weil der Körper  $R(x, \varepsilon)$  in Bezug auf  $R(x)$  den Relativgrad  $\frac{p-1}{e_1}$  besitzt, welche Tatsache aus dem Umstande folgt, dass  $R(x)$  keinen höheren Unterkörper von  $R(\varepsilon)$  als  $R(\sigma)$  vom Grade  $e_1$  enthalten darf. Bezeichnen  $\Sigma$  bez.  $\Sigma_1$  die beiden oben besprochenen ausgezeichneten Untergruppen von  $G$  bez.  $\Gamma$ , so lassen sich die  $\frac{p(p-1)^2}{ee_1}$  Operationen von  $\Delta$  in der folgenden Weise darstellen:

$$(1) \quad (\Sigma, \Sigma_1); (T\Sigma, U^1\Sigma_1); \dots (T^{e_1-1}\Sigma, U^{e_1-1}\Sigma_1),$$

wo die Substitutionen von  $\Sigma$  und  $\Sigma_1$  auf alle möglichen Weisen kombiniert werden.<sup>1</sup>

### § 3. Die Resolventen.

Vermittelst der symmetrischen Funktion

$$x_0 + x_1 + \dots + x_{p-1} = A$$

und der sogenannten LAGRANGE'schen Resolventen

$$(\varepsilon^i, x) = x_0 + \varepsilon^i x_1 + \dots + \varepsilon^{i(p-1)} x_{p-1}$$

gibt man bekanntlich die Wurzeln der Gleichung in der Gestalt:

$$(2) \quad x_x = \frac{1}{p} \left[ A + \sum_{i=1}^{i=p-1} \varepsilon^{-xi} (\varepsilon^i, x) \right].$$

Man hat also in diesen Ausdrücken die  $p^{\text{ten}}$  Wurzeln aus den Grössen

$$\rho_i = (\varepsilon^i, x)^p$$

---

<sup>1</sup> In dem allgemeineren Falle, wo  $R$  einen Unterkörper von  $k(\varepsilon)$  vom Grade  $\delta$  enthält, hat man  $\frac{p-1}{\delta}$  als Grad von  $R(\varepsilon)$ . Es muss dann  $e_1$  auch Teiler von  $\frac{p-1}{\delta}$  sein, und die Gruppe  $\Delta$  besitzt den Grad  $\frac{p(p-1)^2}{ee_1\delta}$ .

zu ziehen. Wir wollen nun zunächst *die Gruppe des durch diese Grössen  $\rho$  bestimmten Körpers  $R(\rho)$  ermitteln* und dann nachweisen, wie die Radikale  $(\varepsilon^i, x)$  durch ein einziges von ihnen und Grössen im Körper  $R(\rho)$  sich rational ausdrücken lassen.

Erstere Aufgabe erledigen wir, indem wir untersuchen, welchen Einfluss die Substitutionen von  $\Delta$  auf diese Grössen  $\rho$  ausüben. Bleiben nämlich alle Grössen  $\rho$  bei einer Untergruppe  $\Delta_1$ , welche innerhalb  $\Delta$  ausgezeichnet sein muss, invariant, so ist die fragliche Gruppe als Faktorgruppe  $\frac{\Delta}{\Delta_1}$  zu charakterisieren. Hierbei haben wir, da  $S$  offenbar keine Vertauschung unter den  $\rho$  bewirkt, nur Substitutionen von der Gestalt  $T^\lambda U^\mu$  in Betracht zu ziehen. Eine solche Operation führt

$$(3) \quad \rho_i = [x_0 + \sum \varepsilon^{ih} x_h]^p$$

in

$$(3') \quad [x_0 + \sum \varepsilon^{ihg^\mu} x_{hg^\lambda}]^p = [x_0 + \sum \varepsilon^{ihg^{\mu-e\lambda}} x_h]^p = \rho_{ig^{\mu-e\lambda}}$$

über. Nehmen wir noch auf den später zu beweisenden Satz Bezug, dass [für  $\mu - e\lambda \not\equiv 0 \pmod{p-1}$ ] wenigstens zwei Grössen  $\rho_i$  und  $\rho_{ig^{\mu-e\lambda}}$  von einander verschieden sind, so können wir jetzt den Satz aussprechen, dass *die Gruppe von  $R(\rho)$  cyclisch ist und den Grad  $\frac{p-1}{e_2}$  besitzt, wo  $e_2$  den grössten Teiler von  $p-1$  bedeutet, welcher bei jeder zulässigen Kombination von  $\mu$  und  $\lambda$  in  $\mu - e\lambda$  aufgeht.* Nach (1) ist  $\mu = kl + k_1 e_1$ ,  $\lambda = k + k_2 e_1$ , also  $\mu - e\lambda = k(l - e) + k_1 e_1 - k_2 e e_1$ , wo die ganzen Zahlen  $k$ ,  $k_1$  und  $k_2$  nach den bezüglichen Moduln  $e_1$ ,  $\frac{p-1}{e_1}$  und  $\frac{p-1}{ee_1}$  beliebig genommen werden können. Hieraus ersieht man, dass  $e_2$  *den grössten gemeinsamen Teiler von  $e_1$  und  $e-l$  darstellen muss.* Die Grössen  $\rho$  zerlegen sich in  $e_2$  Systeme von je  $\frac{p-1}{e_2}$  conjugierten Grössen, so dass die Grössen  $\rho_i, \rho_{ig^{e_2}}, \dots, \rho_{ig^{p-1-e_2}}$  jedesmal zu demselben Systeme gehören, wobei natürlich die Indices  $i, ig^{e_2}, \dots$  nach dem Modul  $p$  zu nehmen sind.

Bei der Auflösung einer metacyklischen Gleichung vom Grade  $p$  sind also von Bedeutung:

1) die Gradzahl  $\frac{p(p-1)}{e}$  der Gruppe der Gleichung; hier giebt es so viele Möglichkeiten, wie  $p-1$  Teiler besitzt;

2) der Grad  $e_1$  des gemeinsamen Unterkörpers von  $R(x)$  und  $R(\varepsilon)$ ; die Anzahl der Möglichkeiten ist hier gleich der Anzahl der verschiedenen Teiler von  $\frac{p-1}{e}$ ;

3) für  $e_1 > 1$  der Exponent  $l$  in der Operation  $TU^l$ , welche in der Gruppe des Körpers  $R(x, \varepsilon)$  auftritt; da  $l$  nach dem Modul  $e_1$ , und zwar als relative Primzahl, zu nehmen ist, so giebt es hier  $\varphi(e_1)$  Möglichkeiten.

Ist eine Grösse  $\rho = 0$ , so verschwinden nach den Grundsätzen der GALOIS'schen Gleichungstheorie auch die übrigen Grössen  $\rho$ , welche demselben conjugierten Systeme angehören. Es muss aber mindestens ein System von Grössen  $\rho$  geben, dessen Glieder nicht identisch verschwinden; anderenfalls wären ja nach (2) die Wurzeln  $x$  gleich gross und rational. Es lässt sich immer durch geeignete Wahl der Indices der Wurzeln erreichen, dass  $\rho_1 = (\varepsilon, x)^p$  nicht verschwindet.

Wir wollen jetzt beweisen, dass die nicht verschwindende Grösse  $\rho_1$  bei keiner Operation von  $\Delta$ , welche in  $\Delta_1$  nicht enthalten ist, ungeändert bleiben kann, also eine primitive Grösse in dem zu  $\Delta_1$  gehörigen Unterkörper von  $R(x, \varepsilon)$  darstellt, so dass alle Grössen des fraglichen Unterkörpers sich rational durch  $\rho_1$  ausdrücken lassen.

Nach (3) und (3') genügt es für unseren Beweis, falls wir nachweisen können, dass  $\rho_1$  von jeder anderen Grösse  $\rho_i$  verschieden sein muss. Nun bleibt der Ausdruck

$$(4) \quad \frac{(\varepsilon^i, x)}{(\varepsilon, x)^i}$$

sowohl bei  $S$  als bei jeder Operation von der Gestalt  $T^\lambda U^{e\lambda}$ , also bei allen in  $\Delta_1$  enthaltenen Operationen, invariant. Es gelten mithin Relationen von der Gestalt

$$(5) \quad (\varepsilon^i, x) = r_i(\varepsilon, x)^i,$$

wo die  $r_i$  solche Grössen des Körpers  $R(x, \varepsilon)$  bedeuten, welche die Operationen von  $\Delta_1$  zulassen. Wäre nun für ein besonderes  $i$

$$(\varepsilon^i, x)^p = (\varepsilon, x)^p,$$

so hätten wir eine Relation

$$(\varepsilon^i, x) = \varepsilon^a(\varepsilon, x),$$

woraus nach (5)

$$(\varepsilon, x)^{i-1} r_i = \varepsilon^a.$$

Da

$$i \not\equiv 1 \pmod{p}$$

so lassen sich die ganzen Zahlen  $k$  und  $k_1$  so bestimmen, dass

$$k(i-1) = 1 + k_1 p.$$

Aus der Relation

$$(\varepsilon, x)^{k(i-1)} \rho_i^k = \varepsilon^{ka}$$

würde man dann erhalten

$$(\varepsilon, x) = \rho_1^{-k_1} \rho_i^{-k} \varepsilon^{ka}.$$

Man hätte also für  $(\varepsilon, x)$  einen Ausdruck, dessen sämtliche Faktoren bei der Operation  $S$  ungeändert bleiben sollten. Dasselbe würde dann auf Grund der Relationen (5) für sämtliche Resolventen  $(\varepsilon^i, x)$  gelten, und mithin nach (2) für die Wurzeln  $x$ . Wir sind also durch unsere Annahme  $\rho_1 = \rho_i$  auf die Ungereimtheit gestossen, dass die Wurzeln  $x$  die Operation  $S$  zulassen sollten.

Nach der jetzt bewiesenen Eigenschaft der Grösse  $\rho_1$ , dass sie eine primitive Grösse des zur Gruppe  $\Delta_1$  gehörigen Unterkörpers von  $R(x, \varepsilon)$  liefert, können wir den Relationen (5) die folgende Form geben:

$$(6) \quad (\varepsilon^i, x) = f_i(\rho_1)(\varepsilon, x)^i,$$

wo die  $f_i$  rationale Funktionen bedeuten. Führt man in einer Relation (6) die Substitutionen von  $\Delta$  aus, so erhält man

$$(7) \quad (\varepsilon^{ig^{ve_2}}, x) = f_i(\rho_{g^{ve_2}})(\varepsilon^{g^{ve_2}}, x)^i \quad \left( \nu = 0, 1, \dots, \frac{p-1}{e_2} - 1 \right),$$

und zwar hat man  $p-2$  solche Systeme von Relationen (7), da man in (6) für  $i$  irgend eine von den Zahlen  $2, 3, \dots, p-2$  setzen kann.



Nachdem wir durch die Relationen:

$$1 - g^{p-1} = p - hp^2; g^\nu = pq_\nu + r_\nu, 0 < r_\nu < p \quad (\nu = 0, 1, \dots, p-1)$$

die ganzen Zahlen  $h$ ,  $q_\nu$  und  $r_\nu$  ermittelt haben, setzen wir

$$(\varepsilon, x)^{hp} k_0^{q_{p-1-e_2}} k_1^{q_{p-1-2e_2}} \dots = K_0(\rho_1).$$

Es geht dann (9) in

$$(10) \quad (\varepsilon, x)^p = [K_0(\rho_1)]^p k_0^{r_{p-1-e_2}} k_1^{r_{p-1-2e_2}} \dots k_{\frac{p-1}{e_2}-1}$$

über.

Es lässt sich beweisen, dass die Grössen  $k_i$  primitive Grössen des Körpers  $R(\rho)$  darstellen, so dass keine zwei unter ihnen einander gleich sein können. Gehörten nämlich diese Grössen schon zu einem Unterkörper von  $R(\rho)$  vom etwaigen Index  $\frac{p-1}{e_2 e_3}$ , so würden sie die Substitution  $(\rho_1 : \rho_{g^{e_2 e_3}})$  zulassen. Man hätte also

$$k_i = k_{i+e_3} = k_{i+2e_3} = \dots = k_{i+\frac{p-1}{e_2}-e_3},$$

wo wir  $i < e_3$  annehmen wollen. In (9) wäre mithin  $k_i$  zu der Potenz

$$g^{p-1-e_2} + g^{p-1-e_2-e_3 e_2} + \dots + g^{e_3 e_2 - i e_2}$$

erhoben. Diese Summe ist aber durch  $p$  teilbar. Es sind ja die betreffenden  $\frac{p-1}{e_2 e_3}$  Glieder Wurzeln der Kongruenz

$$x^{\frac{p-1}{e_2 e_3}} \equiv g^{\frac{(e_3-1)(p-1)}{e_3}} \pmod{p}.$$

Offenbar ist dann auch die Summe der zugehörigen Reste

$$r_{p-1-i e_2} + r_{p-1-i e_2 - e_3 e_2} + \dots + r_{e_3 e_2 - i e_2}$$

durch  $p$  teilbar. Man würde also, falls man in (10) beiderseits die  $p^{\text{ten}}$  Wurzeln auszieht, für  $(\varepsilon, x)$  einen rationalen Ausdruck durch  $\varepsilon$  und Grössen des Körpers  $R(\rho)$  erhalten. Wir hatten aber schon im vorigen Paragraphen Gelegenheit, den Widerspruch bei einer solchen Folgerung hervorzuheben.

Werden in (10) die Substitutionen von  $\Delta$  ausgeführt, so erhält man  $\frac{p-1}{e_2} - 1$  neue Relationen:

$$(11) \quad (\varepsilon^{g^{\nu e_2}}, x)^p = [K_0(\rho_{g^{\nu e_2}})]^p k_\nu^{r_{p-1-e_2}} k_{\nu+1}^{r_{p-1-2e_2}} \dots k_{\nu-1} \quad (\nu = 1, 2, \dots, \frac{p-1}{e_2} - 1),$$

wo die Indices  $\nu + i$  nach dem Modul  $\frac{p-1}{e_2}$  genommen werden.

Schreiben wir zur Abkürzung

$$(12) \quad \tau_\nu = k_\nu^{\frac{1}{p}},$$

so ergibt sich aus (10), indem man rechts und links die  $p^{\text{ten}}$  Wurzeln auszieht,

$$(13) \quad (\varepsilon, x) = K_0(\rho_1) \tau_0^{r_{p-1-e_2}} \tau_1^{r_{p-1-2e_2}} \dots \tau_{\frac{p-1}{e_2}-1}.$$

In entsprechender Weise erhalten wir aus (11)

$$(14) \quad (\varepsilon^{g^{\nu e_2}}, x) = K_0(\rho_{g^{\nu e_2}}) \tau_\nu^{r_{p-1-e_2}} \tau_{\nu+1}^{r_{p-1-2e_2}} \dots \tau_{\nu-1} \quad (\nu = 1, 2, \dots, \frac{p-1}{e_2} - 1),$$

wo die Radikale  $\tau_\nu$  in derselben Weise genommen werden können wie in (13). Nach (8) hat man ja

$$(\varepsilon^{g^{\nu e_2}}, x)(\varepsilon, x)^{-g^{\nu e_2}} = k_{\nu-1} k_{\nu-2}^{g^{e_2}} \dots k_0^{g^{(\nu-1)e_2}}.$$

Man ersieht aber aus den in diesem Paragraphen gegebenen Relationen leicht, dass diese Identität nicht bestehen würde, falls bei der obigen Wahl der  $\tau_\nu$  auf der rechten Seite von (14) noch eine Potenz von  $\varepsilon$  als Faktor hinzukäme.

Einen ähnlichen Ausdruck erhält man für jede Resolvente  $(\varepsilon^i, x)$ . Zunächst lässt sich setzen

$$i \equiv g^{\mu + \nu e_2} \pmod{p} \quad \left[ 0 \leq \mu < e_2, \quad 0 \leq \nu < \frac{p-1}{e_2} \right].$$

Aus den Relationen (6), (7), (13) und (14) erschliesst man dann, dass Identitäten von der Gestalt

$$(15) \quad (\varepsilon^{g^{\mu + \nu e_2}}, x) = K_\mu(\rho_{g^{\nu e_2}}) \tau_\nu^{r_{p-1-e_2+\mu}} \tau_{\nu+1}^{r_{p-1-2e_2+\mu}} \dots \tau_{\nu-1}^{\mu}$$

bestehen müssen, wo eine gegenseitige Abhängigkeit zwischen den  $e_2$  Funktionen  $K_0, K_1, \dots, K_{e_2-1}$  nicht stattfindet. Der Wurzel Ausdruck (2) nimmt jetzt die folgende Gestalt an:

$$(16) \quad \frac{1}{p} \left[ A + \sum_{\mu=0}^{\mu=e_2-1} \sum_{\nu=0}^{\nu=\frac{p-1}{e_2}-1} K_{\mu}(\rho_{g^{\nu e_2}}) \prod_{i=0}^{i=\frac{p-1}{e_2}-1} \tau_{\nu+i}^{r_{p-1-(i+1)e_2+\mu}} \right].$$

Es ist unmittelbar ersichtlich, dass (16) in einen Ausdruck von derselben Schreibweise übergeht, falls man irgend eine Operation der Gruppe  $\Delta$  ausführt. Man findet auch, dass der Ausdruck nur  $p$  Werte annehmen kann, wie man auch die Radikale  $k_{\nu}^{\frac{1}{e_2}} = \tau_{\nu}$  bestimmen mag. In der Tat, multipliziert man das Radikal  $\tau_{\nu}$  mit dem Faktor  $e^{\frac{2k\pi i}{p}}$ , so hat dies dieselbe Wirkung, als ob man dem Radikale  $\tau_0$  den Faktor  $e^{\frac{2k\pi i}{p} r_{p-1-\nu e_2}}$  hinzufügt. Man erhält mithin alle möglichen Werte von (16), indem man unter beliebiger Fixierung der übrigen Radikale dem Radikal  $\tau_0$  seine  $p$  verschiedenen Werte beilegt.

Bei seiner Herleitung der Wurzelform betrachtet Herr WEBER zunächst  $x_0, x_1, \dots, x_{p-1}$  als unabhängige Variable. Erst nachdem die nötigen Sätze über die LAGRANGE'schen Resolventen entwickelt worden sind, macht er die Festsetzung, dass die Variablen  $x$  die Wurzeln einer irreduktibeln metacyklischen Gleichung vom Grade  $p$  sein sollen. In solcher Weise erhält er eine in allen Fällen gültige, von der Rolle, welche die  $p^{\text{ten}}$  Einheitswurzeln gegenüber dem Körper  $R(x)$  spielen, unabhängige Wurzelform, und zwar von der Gestalt (16) für den speciellen Fall  $e_2 = 1$ . Diese Verschiedenheit in den Endresultaten darf natürlich nur scheinbar sein. Bei Herrn WEBER sind die  $p-1$  Grössen  $k_0, k_1, \dots, k_{p-1}$  die Wurzeln einer cyclischen Gleichung. Diese Gleichung braucht aber nicht irreduktibel zu sein, sondern kann in  $e_2$  verschiedene Faktoren zerfallen, wo  $e_2$  einen beliebigen Teiler von  $p-1$  bedeuten kann. Der Körper, welchem die Grössen  $k_i$  angehören, besitzt mithin den Grad  $\frac{p-1}{e_2}$ . Wollte man nun die in der Wurzelform des Herrn WEBER auftretenden Grössen  $k_i$  und  $K_i$  durch ein conjugiertes System von  $\frac{p-1}{e_2}$  Grössen des fraglichen Körpers darstellen, so würde man eben auf unsere Fallunterscheidungen gelangen, so weit sie in (16) ihren Ausdruck finden.

Es drängt sich noch die Frage auf, wie man, wenn die Grössen  $k_i$  oder  $\rho_i$  gegeben sind, also aus der Beschaffenheit einer Wurzelform (16), die Eigenschaften des zugehörigen Körpers  $R(x)$  ablesen kann. In erster Linie handelt es sich dabei um den Grad  $\frac{p(p-1)}{e}$  der Gruppe  $G$ , sowie um den Grad  $e_1$  des gemeinsamen Unterkörpers  $R(\sigma)$  von  $R(x)$  und  $R(\varepsilon)$ .

Die Erledigung dieser Fragen beruht auf zweierlei Erwägungen. Zunächst lässt sich beweisen, dass der gemeinsame Unterkörper  $R(\eta)$  von  $R(\rho)$  und  $R(\varepsilon)$  den Grad  $\frac{ee_1}{e_2}$  besitzt. In der Tat muss jede Operation derjenigen Untergruppe  $\Delta_2$  von  $\Delta$ , zu welcher der Körper  $R(\eta)$  gehört, sich durch Kombination zweier Operationen erzeugen lassen, von denen eine auf die Grössen in  $R(\rho)$ , die andere auf die Grössen in  $R(\varepsilon)$  keinen Einfluss übt. Hieraus erschliesst man, dass  $\Delta_2$  sich durch Kombination von  $\Delta_1$  und  $T^{e_1}$  erzeugen lässt und folglich als Untergruppe von  $\Delta$  den Index  $\frac{ee_1}{e_2}$  besitzen muss. Diesen Umstand können wir benutzen, um das Produkt  $ee_1$  zu ermitteln.

Als Unterkörper von  $R(\rho)$  gehört  $R(\eta)$  zu der durch die Substitution  $(\rho_1 : \rho_{g^{e_1}})$  erzeugten Gruppe. Nun wissen wir aus § 3, dass eine Operation  $T^\lambda U^\mu$ , welche ja  $\varepsilon$  durch  $\varepsilon^{g^\lambda}$  ersetzt,  $\rho_1$  in  $\rho_{g^{\mu-\lambda}}$  überführt. In Bezug auf die Grössen des Körpers  $R(\eta)$  ist also die Operation nur dann mit  $(\rho_1 : \rho_{g^\mu})$  äquivalent, wenn  $\lambda$  durch  $e_1$  teilbar ist. Dann soll aber  $e_1$  ebenfalls Teiler von  $\mu$  sein, und wir haben, um  $e_1$  zu bestimmen, nur darauf Rücksicht zu nehmen, dass die Operationen  $(\rho_1 : \rho_{g^{e_1}})$  und  $(\varepsilon : \varepsilon^{g^{e_1}})$  dieselbe Umordnung unter den Grössen des Körpers  $R(\eta)$  bewirken, und dass es für  $\delta < e_1$  kein Paar in solcher Weise äquivalenter Operationen  $(\rho_1 : \rho_{g^\delta})$  und  $(\varepsilon : \varepsilon^{g^\delta})$  giebt.<sup>1</sup>

### § 5. *Rationale Transformation der Wurzeln.*

Wir können die  $K_\mu$  und  $k_i$  als ganze Funktionen der jedesmal zugehörigen Grösse  $\rho$  annehmen; nach bekannten Methoden kann man ja die Nenner rational machen. Etwaige Faktoren, welche zur  $p^{\text{ten}}$  Potenz in den  $k_i$  auftreten, lassen sich aus dem Wurzelzeichen entfernen und den Funktionen  $K_\mu$  zufügen. Allerdings erreicht man hiermit nicht immer eine ein-

<sup>1</sup> Vergl. KRONECKER, Berl. Ber. (1856), p. 214.

zige bestimmte Normalform für die Funktionen  $k_\nu$ , wie Verhältnisse bei Zahlkörpern lehren, welche ausser Hauptidealen noch Nebenideale besitzen.

Da die Grössen  $\rho$  eine Gleichung von Grade  $\frac{p-1}{e_2}$  befriedigen, so kann

man die Funktionen  $K_\mu$  und  $k_\nu$  als höchstens vom Grade  $\frac{p-1}{e_2} - 1$  betrachten.

Die  $e_2$  Funktionen  $K_\mu$  enthalten also als Koeffizienten der Potenzen der bezüglichen Grössen  $\rho$  insgesamt  $p-1$  rationale Parameter.

Unterwirft man nun die Wurzeln  $x$  einer rationalen Transformation

$$(17) \quad y = a_0 + a_1 x + \dots + a_{p-1} x^{p-1},$$

so ersieht man ohne Schwierigkeit, dass die  $y$  sich in eben derselben Gestalt (16) wie die  $x$  ausdrücken lassen, doch so, dass bei ungeändert gebliebenen  $k_\nu$  die  $K_\mu$  in andere Funktionen übergeführt werden. Da die Transformation (17)  $p$  rationale Parameter enthält, so kann man dem Ausdruck, in welchen (16) übergeht,  $p$  Bedingungen auferlegen, z. B.:

$$(18) \quad A = 0; K_0 = 1; K_1 = K_2 = \dots = K_{e_2-1} = 0.$$

In der Tat hat man, um diese Bedingungen zu erfüllen, nur ein System von  $p$  linearen Gleichungen für  $a_0, a_1, \dots, a_{p-1}$  aufzulösen, und die Determinante dieses Systems darf nicht verschwinden, weil dann eine Wurzel  $x$  einer Relation von niedrigerem als dem  $p^{\text{ten}}$  Grade genügen sollte. *Da also die metacyklischen Körper von Primzahlgrad nur von der Art abhängen, wie das conjugierte System von Funktionen  $k_\nu$  gewählt wird, welche ihrerseits zu cyclischen Körpern niedrigeren Grades gehören, so haben wir hier ein geeignetes Mittel, um alle metacyklischen Zahlkörper von Primzahlgrad aufzustellen und zu klassifizieren, sowie die Kompositionseigenschaften zweier Körper zu studieren, welche in Bezug auf einen gemeinsamen Unterkörper relativ-ABEL'sch sind.* Bei Benutzung dieses Ausgangspunktes wird man ohne Zweifel die schönen Resultate verallgemeinern können, welche zuerst von KRONECKER und dann von den Herren WEBER und HILBERT über die ABEL'schen Zahlkörper gegeben worden sind.