Werk

Titel: Metazyklische Minimalbasis und komplexe Primzahlen.

Autor: Breuer, Samson

Jahr: 1927

PURL: https://resolver.sub.uni-goettingen.de/purl?243919689_0156|log5

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Metazyklische Minimalbasis und komplexe Primzahlen.[1])

Von *Samson Breuer* in Karlsruhe i. B.

Einleitung.

Die vorliegende Arbeit führt die Frage nach der Existenz von für die Anwendungen besonders geeigneten metazyklischen Minimalbasen von Primzahlgrad auf Fragen von rein *zahlentheoretischer* Natur zurück. Unter einer „*metazyklischen* (zyklischen, halbmetazyklischen, vollmetazyklischen usw.) *Minimalbasis vom oder für den Primzahlgrad p*" versteht man p algebraisch unabhängige rationale Funktionen von p Unbestimmten x_ν, die sämtlich dem Invariantenkörper der betreffenden metazyklischen Permutationsgruppe des Grades p angehören und diesen Körper erzeugen. Man nennt sie überdies rational, wenn ihre Koeffizienten einem vorgelegten, i. a. dem absoluten Rationalitätsbereich $\Re_0$ angehören. Die Bedeutung einer solchen Minimalbasis liegt darin, daß sie *einmal* erlaubt, über einem beliebigen endlichen algebraischen Zahlkörper alle *Galois*schen Körper der entsprechenden Gruppe zu bilden, und daß sie *ferner* die Möglichkeit gibt, die Koeffizienten der auflösbaren Gleichungen p-ten Grades, diese *nach ihren Galoisschen Gruppen getrennt*, durch p unabhängige Parameter darzustellen.

Im § 1 wird nach Erklärung der angewandten Bezeichnungen ein vom Verfasser schon früher[2]) abgeleiteter Satz erweitert bei wesentlicher Vereinfachung der Beweisführung. Durch birationale Transformation der Unbestimmten x_ν wird nämlich der Körper $\Re((x))$ aller rationalen Funktionen der Unbestimmten x_ν in zwei Teile *gespalten*, deren einer von $n+1$ vollmetazyklischen Funktionen der x_ν abhängt und also ein Unterkörper *sämtlicher* metazyklischer Invariantenkörper ist. Daher braucht weiterhin nur noch der zweite, von n „Unbestimmten" abhängende Teilkörper betrachtet, d. h. es brauchen für sämtliche metazyklischen Minimalbasen nur noch je n weitere Basisfunktionen bestimmt zu werden.

Im § 2 wird untersucht, wann diese Aufgabe auf die Bestimmung der Minimalbasen für die *zyklischen* Permutationsgruppen $2n$-ten bzw. n-ten Grades zurückgeführt und so eine „*spezielle Minimalbasis erster Art*" bestimmt werden kann.

---

[1]) Über einen Teil dieser Arbeit hat der Verfasser auf der Naturforscher-Versammlung in Innsbruck 1924 vorgetragen.

[2]) *Breuer, Zur Bestimmung der metazyklischen Minimalbasis von Primzahlgrad*, Mathematische Annalen **92**, 1924; im folgenden zitiert mit *B.*

Dies ist dann und nur dann möglich, wenn *erstens* p als Norm einer „komplexen Primzahl" im Körper der $p-1$-ten Einheitswurzeln dargestellt werden kann, und wenn *zweitens* im gleichen Körper eine komplexe Einheit von bestimmten Eigenschaften existiert. Die letztere Bedingung fällt bei den sogenannten „*Fermat*schen Primzahlen" fort; sie ist *stets* erfüllt, wenn $\frac{p-1}{2}$ gleichfalls eine Primzahl ist.

Im § 3 wird untersucht, wann diese Reduktion auf die zyklischen Minimalbasen $2n$-ten Grades *ohne die Zerspaltung* des § 1 vorgenommen und eine für die Anwendungen, namentlich auf die Theorie der Gleichungen, noch mehr geeignete, weil vollkommen symmetrisch gebaute, „*spezielle Minimalbasis zweiter Art*" bestimmt werden kann. Dies ist dann und nur dann der Fall, wenn nicht nur die Bedingungen für die Existenz einer „speziellen Minimalbasis erster Art" erfüllt sind, sondern weiterhin auch noch im Körper der $\frac{p-1}{2}$-ten Einheitswurzeln eine komplexe Einheit von bestimmten Eigenschaften existiert.

Im § 4 werden die vorhergehenden Untersuchungen an einer Reihe von Beispielen ($p = 3, 5, 7, 11, 13, 17, 19, 23$) erläutert und angewandt.

§ 1. Bezeichnungen; Reduktion auf n Unbestimmte.

Im folgenden bezeichne $p = 2n + 1$ eine Primzahl, ε eine primitive p-te Einheitswurzel, g eine primitive Kongruenzwurzel von p; ε und g seien beliebig, aber fest gewählt. (Im § 4 wählen wir für g stets die kleinste positive primitive Kongruenzwurzel von p.) Die auftretenden Indizes sollen folgende Werte durchlaufen: $j, h = 0, 1, \ldots, n-1$; $t = 1, 2, \ldots, n-1$; $\mu = 0, 1, \ldots, p-2$; $\nu = 0, 1, \ldots, p-1$. Mit α_j bezeichnen wir die n-ten Wurzeln der Einheit, mit α irgendeine unter ihnen; desgleichen mit β_j und β die n-ten Wurzeln der negativen Einheit; ϑ_μ bzw. ϑ sei die gemeinsame Bezeichnung für beide, d. h. für die $2n$-ten Wurzeln der Einheit. Mit x_ν bezeichnen wir p Unbestimmte. Ist dann

$$(1) \qquad \varphi_0((x))^{1}) = \frac{1}{p}(x_0 + x_1 + \cdots + x_{p-1})$$

und

$$(2) \qquad k_\mu = \frac{1}{p}(x_0 + \varepsilon^{g^\mu} x_1 + \varepsilon^{2g^\mu} x_2 + \cdots + \varepsilon^{(p-1)g^\mu} x_{p-1}),$$

so ergibt die Auflösung dieser p Gleichungen nach den x_ν:

$$(3) \quad x_\nu = \varepsilon^{-\nu} k_0 + \varepsilon^{-g\cdot\nu} k_1 + \varepsilon^{-g^2\cdot\nu} k_2 + \cdots + \varepsilon^{-g^{p-2}\cdot\nu} k_{p-2} + \varphi_0((x)).$$

Weiter sei

$$(4) \qquad q_j = \frac{k_{n+j}}{k_j}, \quad r_j = \frac{q_j - 1}{q_j + 1}; \quad \zeta_j = \varepsilon^{g^j} - \varepsilon^{-g^j}\ ^{2})\ ^{3}).$$

---

[1]) Mit (x) kürzen wir in üblicher Weise $(x_0, x_1, \ldots, x_{p-1})$ ab, also $\varphi(x_0, x_1, \ldots, x_{p-1})$ mit $\varphi((x))$.

[2]) Die in *B.* mit r_j bezeichneten Größen $\frac{k_j}{k_0}$ treten hier nicht auf; die Größen $\frac{q_j-1}{q_j+1}$ sind dort, im § 2, nur für spezielle Werte von p eingeführt und anders bezeichnet; für ζ_j ist ebendort η_j gesetzt.

[3]) Die Indizes der (x) sind auf den kleinsten nicht negativen Rest (mod p) zu reduzieren, desgleichen die der (k), (q), (r) und der nachher einzuführenden (v) (mod $2n$); überdies ist für

Wir bezeichnen ferner die erzeugenden Elemente der vollen linearen (oder metazyklischen) Permutationsgruppe mit

$$(5) \qquad S = (x_0, x_1, \ldots, x_{p-1}), \qquad T = (x_1, x_g, x_{g^2}, \ldots, x_{g^{p-2}})\ ^{1}).$$

Ersetzt man in den Koeffizienten einer Funktion der (x) die Einheitswurzel ε durch ε^g — wobei diese beiden Größen also nicht etwa *gegenseitig* vertauscht werden —, so bezeichnen wir diese Operation mit E. Eine Funktion der (k), der (q) oder der (r) ist nach (2) und (4) stets auch eine solche der (x). Wir bezeichnen sie als eine S-Funktion oder $ST^{\varkappa}$-Funktion der (k) usw., wenn sie die Vertauschung S bzw. S und $T^{\varkappa}$ duldet; dabei sei $\varkappa$ irgendein Teiler von $2n$, die Teiler 1 und $2n$ mit eingeschlossen. Wir betrachten im folgenden ausschließlich rationale Funktionen der (x), (k) usw. Wo wir eine Funktion ausdrücklich als rational bezeichnen, wollen wir damit sagen, daß auch ihre Koeffizienten dem zugrundegelegten Rationalitätsbereich $\mathfrak{R}$ bzw., wo nichts anderes gesagt ist, dem absoluten Rationalitätsbereich $\mathfrak{R}_0$ entstammen, wenn man sie, mit Hilfe von (2) und (4), als Funktion der (x) schreibt. Nun geht k_μ bei Anwendung von S in $\varepsilon^{-g^\mu} k_\mu$ über, desgleichen q_j in $\varepsilon^{2g^j} q_j$, da $g^n \equiv -1 \pmod p$ ist. Mithin ist die Funktion

$$(6) \qquad v_0 = k_0^{\lambda_0} k_1^{\lambda_1} \cdots k_{p-2}^{\lambda_{p-2}}$$

dann und nur dann eine S-Funktion, wenn

$$(7) \qquad \lambda_0 + g^1\lambda_1 + g^2\lambda_2 + \cdots + g^{p-2}\lambda_{p-2} \equiv 0 \pmod p \text{ ist,}$$

desgleichen

$$(8) \qquad \psi_0 = q_0^{l_0} q_1^{l_1} \cdots q_{n-1}^{l_{n-1}}$$

dann und nur dann, wenn

$$(9) \qquad l_0 + g^1 l_1 + g^2 l_2 + \cdots + g^{n-1} l_{n-1} \equiv 0 \pmod p \text{ ist.}$$

Mit v_0 und ψ_0 dulden auch die Funktionen v_μ und ψ_j [2]) die Vertauschung S, welche aus ihnen durch die wiederholten zyklischen Vertauschungen

$$(10) \quad (k_0, k_1, \ldots, k_{p-2}) \text{ bzw. } (q_0, q_1, \ldots, q_{n-1}, q_0^{-1}, q_1^{-1}, \ldots, q_{n-1}^{-1})$$

hervorgehen. Eben diese Vertauschungen werden aber unter den (k) und (q) durch E oder durch T^{-1} hervorgerufen. Bei den v_μ und ψ_j bewirken also E oder T^{-1} die Vertauschungen $\binom{v_\mu}{v_{\mu+1}}$ bzw. $\binom{\psi_\mu}{\psi_{\mu+1}}$ oder ausführlich geschrieben

$$(11) \quad (v_0, v_1, \ldots, v_{p-2}) \text{ bzw. } (\psi_0, \psi_1, \ldots, \psi_{n-1}, \psi_0^{-1}, \psi_1^{-1}, \ldots, \psi_{n-1}^{-1}).$$

---

q_{n+j} sinngemäß q_j^{-1} zu setzen und für r_{n+j} entsprechend $-r_j$; ebenso ist $\zeta_{n+j} = -\zeta_j$, da $g^{n+j} \equiv -g^j \pmod p$ ist. Bei dieser Interpretation können wir also auch von den $2n$ Größen η_μ, r_μ, ζ_μ und weiterhin ψ_μ, χ_μ sprechen.

[1]) Siehe Fußnote 3) auf Seite 14.

[2]) Die verschiedene Bezeichnung bei den v_μ und ψ_j rührt davon her, daß zwar aus v_0 durch (10) $2n$ wesentlich verschiedene Funktionen hervorgehen, aus ψ_0 aber nur n, da $\psi_{n+j} = \psi_j^{-1}$ wird; vgl. Fußnote 3) auf Seite 14 und Formel (11). Ähnliches gilt für die χ_j, wegen $\chi_{n+j} = -\chi_j$; vergleiche (13).

Nun ist eine Funktion der (k), (q) usw. dann und nur dann in dem oben definierten Sinne rational, wenn sie E duldet. Die zyklischen, d. h. gegenüber (11) invarianten Funktionen der (v) und (ψ) sind daher, vorausgesetzt, daß ihre einzelnen Glieder die Bedingung (7) bzw. (9) erfüllen, rationale vollmetazyklische Funktionen der (x). Umgekehrt können alle rationalen metazyklischen Funktionen aus φ_0 (1) und Funktionen der Form v_μ (6) bzw. zyklischen Verbindungen der v_μ erzeugt werden[1]). Was wir suchen, sind $p-1$ solche Funktionen, die jeweils zusammen mit φ_0 den gerade betrachteten metazyklischen Körper erzeugen. Ehe wir uns diesem Problem selbst zuwenden, führen wir nun noch die Größen

$$\chi_j = \frac{\psi_j - 1}{\psi_j + 1} \tag{12}$$

ein und bemerken, daß die r_j (4) und χ_j (12) durch E oder T^{-1}, d. h. durch (10) bzw. (11) die gleiche Vertauschung, nämlich $\binom{r_\mu}{r_{\mu+1}}$ bzw. $\binom{\chi_\mu}{\chi_{\mu+1}}$ oder

$$\begin{aligned}&(r_0, r_1, \ldots, r_{n-1}, -r_0, -r_1, \ldots, -r_{n-1}) \quad \text{bzw.}\\ &(\chi_0, \chi_1, \ldots, \chi_{n-1}, -\chi_0, -\chi_1, \ldots, -\chi_{n-1})\end{aligned} \tag{13}$$

erfahren.

Die Aufsuchung der metazyklischen Minimalbasen wird nun, gleichzeitig für alle metazyklischen Körper des Primzahlgrades p, wesentlich vereinfacht durch den folgenden

Satz 1: Der Körper $\Re((x))$[2]) läßt sich durch birationale Transformation der Unbestimmten (x) in zwei Körper $\Re(\varphi_0, \varphi_1, \ldots, \varphi_n)$ und $\Re(Q_0, Q_1, \ldots, Q_{n-1})$ zerlegen, deren einer von $n+1$ vollmetazyklischen Funktionen $\varphi_0, \varphi_1, \ldots, \varphi_n$ der (x) erzeugt wird.

Es möge noch ausdrücklich hervorgehoben werden, daß die Funktionen (φ) und (Q), ebenso wie die beiden Zerlegungskörper, ε nicht enthalten. Der Körper $\Re((\varphi))$ ist also in allen metazyklischen Körpern enthalten. Um von dem Körper $\Re((x))$ zu den *einzelnen* metazyklischen Körpern zu gelangen, brauchen wir *daher nur noch den Körper* $\Re((Q))$ *schrittweise einzuschränken*, d. h. wir müssen seine erzeugenden n Elemente (Q) durch genau n S-Funktionen bzw. $ST^\varkappa$-Funktionen usw. der (Q) ersetzen, die den Körper aller S-Funktionen usw. der (Q) erzeugen und also zusammen mit den ein für allemal bestimmten Funktionen (φ) die gesuchte Minimalbasis bilden.

Die in obigem Satze erwähnte birationale Transformation kann durch folgende Gleichungen vermittelt werden:

$$\varphi_0 = \sum_0^{p-1} x^\nu; \quad \varphi_{j+1} = \sum_0^{n-1} {}_h (q_h^{jp+n+1} + q_h^{-jp-n}) k_h; \quad Q_j = \sum_0^{n-1} {}_h \zeta_h r_{j+h}. \tag{14}$$

Beweis: Zunächst erkennt man bei Beachtung von (4), (13) und Fußnote 3) S. 14 sofort, daß Q_j, wie verlangt, eine „rationale" Funktion der (x) ist, da die

[1]) Vgl. *Weber, Lehrbuch der Algebra*, 2. Aufl. (1898), I. §§ 191, 192.

[2]) Mit $\Re((x))$ bezeichnen wir den Körper aller rationalen Funktionen der (x), deren Koeffizienten einem *beliebig* vorgegebenen Rationalitätsbereich $\Re$ entstammen.

n Glieder dieser Summe durch E nur zyklisch (ohne Vorzeichenänderung!) vertauscht werden. Da ferner $q_h^{-jp-n}k_h = k_{n+h}^{-jp-n}k_h^{jp+n+1} = q_{n+h}^{jp+n+1}k_{n+h}$ ist, so können wir auch schreiben: $\varphi_{j+1} = \sum_0^{p-2\mu} q_\mu^{jp+n+1}k_\mu$. In dieser Form erkennt man, daß φ_{j+1} die Vertauschungen (10), d. h. T und E duldet. Da aber das Leitglied auch die Bedingung (7) erfüllt, so ist φ_{j+1}, wie verlangt, eine rationale vollmetazyklische Funktion der (x); das gleiche gilt selbstverständlich für φ_0. Wir haben nun noch zu zeigen, daß die Gleichungen (14) auch rational nach den (x) aufgelöst werden können. Dazu genügt es im Hinblick auf (3), wenn wir zeigen, daß erstens das Gleichungssystem (14, 3) nach den r_h aufgelöst werden kann, womit nach (4) auch die $q_h = \frac{1+r_h}{1-r_h}$ bekannt sind, und daß weiter das System (14, 2) nach den k_h, d. h. den n Größen $k_0, k_1, \ldots, k_{n-1}$, aufgelöst werden kann: d. h. wir müssen zeigen, daß die Determinanten dieser Systeme nicht *identisch* für alle Werte der Unbestimmten (x) bzw. (q) verschwinden[1]).

Bezeichnen wir für den Augenblick $q_h^{\frac{p}{2}} = s_h$, $(s_h + s_h^{-1})^2 = u_h$, so können wir die Determinante D_1 von (14, 2) folgendermaßen umformen:

$$D_1 = \{q_h^{jp+n+1} + q_h^{-jp-n}\} = (q_0 q_1 \cdots q_{n-1})^{\frac{1}{2}} \{q_h^{jp+n+\frac{1}{2}} + q_h^{-jp-n-\frac{1}{2}}\}$$
$$= (q_0 q_1 \cdots q_{n-1})^{\frac{1}{2}} \{s_h^{2j+1} + s_h^{-2j-1}\}.$$

Nun ist aber

$$(s_h + s_h^{-1})^{2j+1} = (s_h^{2j+1} + s_h^{-2j-1}) + \binom{2j+1}{1}(s_h^{2j-1} + s_h^{-2j+1})$$
$$+ \binom{2j+1}{2}(s_h^{2j-3} + s_h^{-2j+3}) + \cdots + \binom{2j+1}{j}(s_h + s_h^{-1}).$$

Mithin kann man die Determinante $\{s_h^{2j+1} + s_h^{-2j-1}\}$ durch Addition geeigneter Vielfacher darüberstehender Zeilen, von der untersten an angefangen, in die Form bringen:

$$\{s_h^{2j+1} + s_h^{-2j-1}\} = \{(s_h + s_h^{-1})^{2j+1}\} = \{u_h^{j+\frac{1}{2}}\} = (u_0 u_1 \cdots u_{n-1})^{\frac{1}{2}} \{u_h^j\}$$
$$(h, j = 0, 1, \ldots, n-1) \qquad = (u_0 u_1 \cdots u_{n-1})^{\frac{1}{2}} \Delta u_h,$$

wo Δu_h das Differenzenprodukt der u_h bedeutet. Mithin wird

$$D_1 = \Pi q_h^{\frac{1}{2}} \cdot \Pi(q_h^{\frac{p}{2}} + q_h^{-\frac{p}{2}}) \cdot \Delta(q_h^{\frac{p}{2}} + q_h^{-\frac{p}{2}})^2 = \Pi(q_h^{n+1} + q_h^{-n}) \cdot \Delta(q_h^{\frac{p}{2}} + q_h^{-\frac{p}{2}})^2,$$

also *nicht* identisch Null.

Die Determinante D_2 von (14, 3) hängt überhaupt nicht von den (x) ab; ihr Zahlenwert ist leicht zu berechnen. Schreibt man nämlich (14, 3) ausführlich und setzt für r_{n+j} wieder $-r_j$, so wird

---

[1]) Daß die Auflösung von (14) nach den (x), sofern sie überhaupt möglich ist, nur Koeffizienten aus $\mathfrak{R}_0$ enthält, folgt daraus, daß wie vorher gezeigt, für (14) selbst das gleiche gilt.

$$
\begin{aligned}
(15)\quad Q_0 &= \zeta_0 r_0 + \zeta_1 r_1 + \zeta_2 r_2 + \cdots + \zeta_j r_j + \cdots + \zeta_{n-1} r_{n-1}\\
Q_1 &= -\zeta_{n-1} r_0 + \zeta_0 r_1 + \zeta_1 r_2 + \cdots + \zeta_{j-1} r_j + \cdots + \zeta_{n-2} r_{n-1}\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
Q_j &= -\zeta_{n-j} r_0 - \zeta_{n-j+1} r_1 - \zeta_{n-j+2} r_2 - \cdots - \zeta_{n-1} r_{j-1} + \zeta_0 r_j + \zeta_1 r_{j+1}\\
&\qquad + \cdots + \zeta_{n-j-1} r_{n-1}\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
Q_{n-1} &= -\zeta_1 r_0 - \zeta_2 r_1 - \zeta_3 r_3 - \cdots - \zeta_{j+1} r_j - \cdots - \zeta_{n-1} r_{n-2} + \zeta_0 r_{n-1}.
\end{aligned}
$$

Die Determinante D_2 dieses Systems ist also „schiefzyklisch". Bezeichnen wir für den Augenblick

$$\zeta_0 + \beta\zeta_1 + \beta^2\zeta_2 + \cdots + \beta^{n-1}\zeta_{n-1} = F(\beta),$$

so wird

$$D_2 = F(\beta_0) \cdot F(\beta_1) \cdot F(\beta_2) \cdots F(\beta_{n-1})\ ^{1)}.$$

Beachtet man weiter, daß $\zeta_j = \varepsilon^{g^j} - \varepsilon^{g^{n+j}}$ und $\beta^n = -1$ ist, so erhält man

$$
\begin{aligned}
F(\beta) &= \varepsilon^{g^0} + \beta\varepsilon^{g^1} + \beta^2\varepsilon^{g^2} + \cdots + \beta^{n-1}\varepsilon^{g^{n-1}}\\
&\quad + \beta^n\varepsilon^{g^n} + \beta^{n+1}\varepsilon^{g^{n+1}} + \cdots + \beta^{2n-1}\varepsilon^{g^{2n-1}} = (\beta, \varepsilon),
\end{aligned}
$$

d. h. gleich einer *Lagrange*schen Resolvente der Gleichung

$$x^{2n} + x^{2n-1} + \cdots + x + 1 = 0.$$

Mithin wird

$$(16)\qquad D_2 = (\beta_0, \varepsilon)\,(\beta_1, \varepsilon)\,(\beta_2, \varepsilon) \cdots (\beta_{n-1}, \varepsilon).$$

Ist nun $n = 2m$, so sind die (β) paarweise reziproke Zahlen; ist $n = 2m + 1$, so enthalten sie außer den m Paaren reziproker Zahlen noch die negative Einheit. Nun ist aber

$$(17)\qquad (\beta, \varepsilon) \cdot (\beta^{-1}, \varepsilon) = \beta^n p = -p,$$

wie aus der Theorie der Kreisteilung bekannt ist [2]), und diese Formel gilt bei ungeradem n auch speziell für $\beta = -1$; in diesem Falle wird also $(-1, \varepsilon) = \sqrt{-p}$.

---

[1]) Diese Formel ist unabhängig von der Bedeutung der Elemente von D_2. Seien nämlich die ζ_j für den Augenblick Unbestimmte, so multiplizieren wir D_2 mit dem stets von Null verschiedenen Differenzenprodukt

$$D_\beta = \begin{vmatrix} 1 & \beta_0 & \beta_0^2 & \cdots & \beta_0^{n-1} \\ 1 & \beta_1 & \beta_1^2 & \cdots & \beta_1^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \beta_{n-1} & \beta_{n-1}^2 & \cdots & \beta_{n-1}^{n-1} \end{vmatrix}$$

der Wurzeln der Gleichung $u^n + 1 = 0$. Bildet man die inneren Produkte der Zeilen beider Determinanten, so findet man

$$D_\beta \cdot D_2 = \begin{vmatrix} F(\beta_0), & \beta_0 \cdot F(\beta_0), & \beta_0^2 \cdot F(\beta_0) & \cdots \beta_0^{n-1} F(\beta_0) \\ F(\beta_1), & \beta_1 \cdot F(\beta_1), & \beta_1^2 \cdot F(\beta_1) & \cdots \beta_1^{n-1} F(\beta_1) \\ \cdots & \cdots & \cdots & \cdots \\ F(\beta_{n-1}), & \beta_{n-1} F(\beta_{n-1}), & \beta_{n-1}^2 F(\beta_{n-1}) & \cdots \beta_{n-1}^{n-1} F(\beta_{n-1}) \end{vmatrix} \begin{aligned} &= F(\beta_0) \cdot F(\beta_1) \cdots F(\beta_{n-1}) \cdot D_\beta, \\ &D_2 = F(\beta_0) \cdot F(\beta_1) \cdots F(\beta_{n-1}). \end{aligned}$$

Vergleiche *R. F. Scott, Note on a determinant theorem of Mr. Glaisher's.* The Quarterly Journal of pure and applied mathematics XVII, 1881, p. 129—132.

[2]) Vergl. etwa *Weber, Lehrbuch der Algebra*, 2. Aufl. (1898), I. § 177, Formel (3).

Mithin wird für $n = 2m$ durch Einsetzen von (17) in (16) erhalten $D_2 = (-p)^m$; für $n = 2m + 1$ dagegen $D_2 = (-p)^m \cdot \sqrt{-p}$; also allgemein $D_2 = (-p)^{\frac{n}{2}} \neq 0$, w. z. b. w.

§ 2. Spezielle Minimalbasen erster Art; Zusammenhang mit den komplexen Primzahlen.

Wir haben nunmehr die Körper der ST^x-Funktionen der (Q) zu betrachten und für sie Minimalbasen zu suchen. Statt dessen können wir auch — und das trifft den Kern der Aufgabe — die Körper der *„rationalen" ST^x-Funktionen der* (q) betrachten und für *diese* die Minimalbasen suchen, denn der Körper $\mathfrak{R}((q))$ entsteht aus $\mathfrak{R}((Q))$ durch Adjunktion von ε. Alle S-Funktionen der (q) überhaupt lassen sich aus *solchen* Funktionen ψ_j (8) zusammensetzen, welche die Bedingung (9) erfüllen. Eine Minimalbasis für diese Funktionen ψ_j wird nun z. B. durch die n Funktionen

$$q_0^p, \quad q_t q_0^{-g^t} \tag{18}$$

gebildet, denn diese Funktionen erfüllen (9), und nach Adjunktion der einen p-ten Wurzel q_0 sind alle q_j bekannt. Es ist sogar nicht schwer, aus (18) auch eine Minimalbasis für die ST^m-Funktionen der (q) zu gewinnen. Diese wird nämlich durch die Funktionen

$$\left(\frac{q_0^p - 1}{q_0^p + 1}\right)^2, \qquad \frac{q_0^p - 1}{q_0^p + 1} \cdot \frac{q_t q_0^{-g^t} - 1}{q_t q_0^{-g^t} + 1} \tag{19}$$

gebildet [1]). Aber der Lösung unserer eigentlichen Aufgabe kommen wir damit nur wenig näher. Denn die Funktionen (18) und (19) erleiden durch T oder E eine recht verwickelte Substitution, deren Invarianten jedenfalls nicht einfach zu bestimmen sind [2]). Wir können daher aus (18) und (19) unmittelbar weder eine Basis für die *rationalen* S-Funktionen der (q), noch eine solche für deren ST^x-Funktionen gewinnen. Dies wird aber wesentlich erleichtert, wenn es gelingt, die Basisfunktionen (19) durch n *„konjugierte" Basisfunktionen* χ_j (12) zu ersetzen, die bei T^{-1} oder E nur die zyklische Vertauschung (13, 2) erleiden, d. h. wenn es gelingt, eine Funktion ψ_0 (8) zu finden, die zusammen mit den durch T^j aus ihr hervorgehenden Funktionen ψ_j eine Basis für die S-Funktionen der (q) bildet. Eine solche Basis wollen wir im folgenden kurz eine *„spezielle S-Basis erster Art"* nennen. [Sie bildet *im* $\mathfrak{R}(\varepsilon)$ zusammen mit den φ_0, φ_{j+1} (14) eine zyklische Minimalbasis für die (x).] Aus einer speziellen S-Basis $\psi_0, \psi_1, \ldots, \psi_{n-1}$ können wir nun zunächst stets eine *rationale* S-Basis gewinnen, und zwar auf genau demselben Wege, wie wir oben von der Basis (q) der Funktionen der (q) überhaupt zu der Basis (Q) der *rationalen* Funktionen der (q) gelangt sind. Wir führen nämlich nach (12) die $\chi_j = \dfrac{\psi_j - 1}{\psi_j + 1}$ ein, die den r_j entsprechen, und erhalten ganz

[1]) Vergl. *B.* (16) und (18).

[2]) Vergl. *B.* § 1, Ende. Zu der Fußnote 9) daselbst ist zu bemerken, daß Herr *Beck*, nach einer freundlichen Mitteilung an den Verfasser, „glaubt beweisen zu können, daß *jede* Cremona-Transformation durch Wechsel des Raumelementes linear gemacht werden kann".

analog zu (14, 3) die Größen

$$(20)\qquad {}^{\Psi}_{j} = \sum_{0}^{n-1}{}^{h}\zeta_h \chi_{j+h} = -\zeta_{n-j}\chi_0 - \zeta_{n-j+1}\chi_1 - \zeta_{n-j+2}\chi_2 - \cdots - \zeta_{n-1}\chi_{j-1} + \zeta_0\chi_j + \zeta_1\chi_{j+1} + \cdots + \zeta_{n-j-1}\chi_{n-1},$$

die gleich den Q_j (14, 3; 15) gegen E invariant und also rational sind. Sie bilden mithin die gesuchte Minimalbasis für die *rationalen* S-Funktionen der (q) oder, was dasselbe ist, für die S-Funktionen der (Q); sie bilden zusammen mit den $\varphi_0, \varphi_1, \ldots, \varphi_n$ (14) die gesuchte *rationale* zyklische Minimalbasis für die Unbestimmten (x). Diese möge als „*spezielle zyklische Minimalbasis erster Art*" bezeichnet werden.

Die Größen Ψ_j (20) erleiden nun nach (13) durch T^{-1} die Vertauschung

$$(21)\qquad U = (\Psi_0, \Psi_1, \ldots, \Psi_{n-1}, -\Psi_0, -\Psi_1, \ldots, -\Psi_{n-1}).$$

Die fernere Bestimmung der Minimalbasen für die $ST^{\varkappa}$-Funktionen der (Q) verlangt also nur noch das Aufsuchen von Minimalbasen für die Invariantenkörper, die zu den zyklischen, durch die Permutationen $U^{\varkappa}$ jeweils erzeugten Gruppen — den sämtlichen Untergruppen der durch U selbst erzeugten Gruppe — gehören, d. h. also das Aufsuchen von Minimalbasen für zyklische Permutationsgruppen $2n$-ten Grades in dem speziellen Fall, daß die Unbestimmten, von denen der Körper abhängt, paarweise entgegengesetzt gleich sind. Wenn nun n ungrade ist, so kann man diese Aufgabe leicht weiter auf das Aufsuchen der zyklischen Minimalbasen *n-ten* Grades reduzieren. Sei nämlich $n = 2m + 1$, und setzen wir

$$(22)\qquad \Psi_0\Psi_1 = \Omega_0,\ \Psi_1\Psi_2 = \Omega_1,\ \ldots,\ \Psi_j\Psi_{j+1} = \Omega_j,\ \ldots,\ \Psi_{n-2}\Psi_{n-1} = \Omega_{n-2},\ -\Psi_{n-1}\Psi_0 = \Omega_{n-1} = \Omega_{2m},$$

so erleiden die Größen Ω_j durch T^{-1} die Vertauschung

$$(23)\qquad O = (\Omega_0, \Omega_1, \ldots, \Omega_{n-1}).$$

Dann ist aber eine Minimalbasis der zu $O^{\varkappa}$ — $\varkappa$ ein Teiler von n — gehörigen Funktionen der (Ω) zugleich eine Minimalbasis für die zu $U^{\varkappa}$ gehörigen Funktionen der (Ψ). Sie erzeugt nämlich nur solche Funktionen der (Ψ), die $U^{\varkappa}$ dulden, und der Körper der (Ψ) selbst ist vom Grade $\frac{2n}{\varkappa}$ über ihr, weil er vom zweiten Grade über dem der (Ω) ist. Dieses selbst endlich folgt aus der Gleichung

$$\Psi_0^2 = -\Omega_0\Omega_1^{-1}\Omega_2\Omega_3^{-1}\cdots\Omega_{2m-2}\Omega_{2m-1}^{-1}\Omega_{2m},$$

da aus (22) mit Ψ_0 alle Ψ_j rational bekannt sind [1]). Die zu $U^{2\varkappa}$ gehörige Minimalbasis ist gleichfalls leicht zu finden, da die Vertauschungen $U^{2\varkappa}$ und $O^{\varkappa}$ sich nur durch die Elemente unterscheiden, auf die sie sich beziehen. Wir erhalten somit den

Satz 2: Die Kenntnis einer speziellen S-Basis erster Art reduziert das Problem der Aufsuchung von Minimalbasen für

[1]) Vergl. *Breuer, Zyklische Gleichungen 6. Grades und Minimalbasis*, Mathematische Annalen **86**, 1922, S. 108 ff.

die metazyklischen Gruppen p-ten Grades auf das gleiche Problem bei den zyklischen (Permutations-)Gruppen $2n$-ten bzw. n-ten Grades.

Fragen wir daher jetzt, wann eine spezielle S-Basis erster Art existiert, so erkennen wir leicht: Dafür, daß die Funktionen ψ_j eine Basis für die S-Funktionen der (q) bilden, ist *notwendig und hinreichend*, daß die beiden Gleichungen

$$\psi_0^{s_0}\psi_1^{s_1}\cdots\psi_{n-1}^{s_{n-1}} = q_0^p \tag{24}$$

$$\psi_0^{t_0}\psi_1^{t_1}\cdots\psi_{n-1}^{t_{n-1}} = q_0^g q_1^{-1} \tag{25}$$

in ganzen Zahlen s_j, t_j erfüllbar sind. Dies ist *notwendig*, denn q_0^p und $q_0^g q_1^{-1}$ sind S-Funktionen, müssen also durch die ψ_j in dieser Weise darstellbar sein. Und es ist *hinreichend*, weil der Körper der (q) alsdann vom p-ten Grade über dem der (ψ) ist; denn nach Adjunktion von q_0 kennt man aus (25) auch q_1, und ebenso alle anderen q_j aus den Gleichungen, die durch wiederholte Anwendung von T auf (25) aus dieser hervorgehen. Setzt man in die linken Seiten von (24) und (25) für die ψ_j ihre Werte nach (8) ein, also

$$\begin{aligned}
\psi_0 &= q_0^{l_0} q_1^{l_1}\cdots q_{n-2}^{l_{n-2}} q_{n-1}^{l_{n-1}}\\
\psi_1 &= q_0^{-l_{n-1}} q_1^{l_0}\cdots q_{n-2}^{l_{n-3}} q_{n-1}^{l_{n-2}}\\
&\cdots\cdots\cdots\cdots\cdots\\
\psi_{n-1} &= q_0^{-l_1} q_1^{-l_2}\cdots q_{n-2}^{-l_{n-1}} q_{n-1}^{l_0}
\end{aligned} \tag{26}$$

und setzt die Koeffizienten von q_j auf beiden Seiten von (24) und (25) je einander gleich, so liefern die Gleichungen (24) und (25) je n Gleichungen für die Zahlen s_j bzw. t_j, oder genauer gesagt: zwischen diesen Zahlen und den l_j, nämlich:

$$\begin{aligned}
&l_0 s_0 - l_1 s_{n-1} - l_2 s_{n-2} - \cdots - l_{n-1} s_1 = p\\
&l_0 s_1 + l_1 s_0 - l_2 s_{n-1} - \cdots - l_{n-1} s_2 = 0\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&l_0 s_{n-1} + l_1 s_{n-2} + l_2 s_{n-3} + \cdots + l_{n-1} s_0 = 0
\end{aligned} \tag{27}$$

beziehungsweise:

$$\begin{aligned}
&l_0 t_0 - l_1 t_{n-1} - l_2 t_{n-2} - \cdots - l_{n-1} t_1 = g\\
&l_0 t_1 + l_1 t_0 - l_2 t_{n-1} - \cdots - l_{n-1} t_2 = -1\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
&l_0 t_{n-1} + l_1 t_{n-2} + l_2 t_{n-3} + \cdots + l_{n-1} t_0 = 0\,.
\end{aligned} \tag{28}$$

Die Zahlen l_j müssen, wie erinnerlich, noch die Bedingung (9) erfüllen. Unsere Frage lautet daher jetzt einfach so: *Wann existieren drei Systeme von je n ganzen Zahlen* (l), (s), (t), *die die Bedingungen* (9), (27), (28) *erfüllen*?

Hier ergibt sich nun ein enger Zusammenhang mit einer Frage, die am Eingang der Idealtheorie steht[1]), die selbst gerade *Kummer* in den Fällen, wo sie eine

[1]) Vergleiche die „*Festschrift zur Feier des 100. Geburtstages E. Kummers* usw." herausgeg. vom Vorstand der Berliner Math. Ges., Leipzig u. Berlin 1910, S. 53ff. (Briefe *Kummers* an *Kronecker*), sowie *Kummers Gratulationsschrift* zum Jubiläum der Königsberger Universität (1844), wiederabgedruckt unter dem Titel „*Sur les nombres complexes* etc." im Journal de mathématiques pures et appliquées, XII, 1847, p. 185—212.

negative Antwort fand, zur Schöpfung der „idealen Zahlen" geführt hat. [Wir werden es aber im Rahmen dieser Arbeit nur mit „realen Zahlen" zu tun haben, auf Fragen der Idealtheorie selbst überhaupt nicht eingehen und auch von ihrer Terminologie keinen Gebrauch machen.] Betrachten wir nämlich die beiden Kongruenzen

$$(29)\quad (l_0 + l_1 u + l_2 u^2 + \cdots + l_{n-1} u^{n-1})(s_0 + s_1 u + s_2 u^2 + \cdots + s_{n-1} u^{n-1}) \equiv p \pmod{u^n + 1},$$

$$(30)\quad (l_0 + l_1 u + l_2 u^2 + \cdots + l_{n-1} u^{n-1})(t_0 + t_1 u + t_2 u^2 + \cdots + t_{n-1} u^{n-1}) \equiv g - u \pmod{u^n + 1},$$

multiplizieren die linken Seiten aus, schaffen die n-ten und höheren Potenzen der Unbestimmten u weg und vergleichen die *Koeffizienten* gleich hoher Potenzen von u auf beiden Seiten jeder Kongruenz, so erhalten wir offenbar dieselben beiden Gleichungssysteme (27) und (28) wie vorhin beim Vergleich der *Exponenten* gleicher q_j auf beiden Seiten von (24) und (25). Wir führen nun noch zur Abkürzung die Bezeichnung

$$(31)\qquad l_0 + l_1 u + l_2 u^2 + \cdots + l_{n-1} u^{n-1} = l(u)$$

sowie die entsprechend erklärten Bezeichnungen $s(u)$, $t(u)$ ein. Dann sind die Gleichungen

$$(32)\qquad l(\beta) \cdot s(\beta) = p, \qquad l(\beta) \cdot t(\beta) = g - \beta$$

äquivalent mit den Gleichungen (29), (30), sobald wir vorschreiben, daß die Gleichungen (32) für *alle* n Wurzeln β der Gleichung $u^n + 1 = 0$ erfüllt sein sollen. *Die Existenz einer solchen Zerlegung* (32) *der ganzen algebraischen Zahlen* p *und* $g - \beta$, *zusammen mit der hier stets stillschweigend vorausgesetzten Erfüllung der Bedingung* (9), *ist also notwendig und hinreichend für die Existenz einer speziellen S-Basis.* Die Bedingung (9) können wir übrigens nach (31) jetzt auch in der Form schreiben:

$$(33)\qquad l(g) \equiv 0 \pmod{p}.$$

Um nun die Bedingungen (32), (33) eingehender zu untersuchen, denken wir uns die Funktion $u^n + 1$ in ihre irreduzibelen Faktoren zerlegt:

$$(34)\qquad u^n + 1 = f(u) f_1(u) f_2(u) \cdots f_k(u) = f(u) \cdot F(u).$$

Dabei sei $f(u) = 0$ die „irreduzibele Kreisteilungsgleichung für den Grad $2n$", besitze also die primitiven $2n$-ten Einheitswurzeln als Wurzeln. Neben der Bezeichnung β für alle Wurzeln von $u^n + 1 = 0$ führen wir für die Wurzeln von $f(u) = 0$ die Bezeichnung γ, für die von $F(u) = 0$ die Bezeichnung δ ein. Sei nun

$$(35)\qquad 1 = \varrho_1, \varrho_2, \varrho_3, \ldots, \varrho_d = 2n - 1$$

ein vollständiges reduziertes Restsystem für den Modul $2n$, so sind alle Wurzeln von $f(u) = 0$ durch γ, γ^{ϱ_2}, γ^{ϱ_3}, $\ldots$, γ^{ϱ_d} dargestellt, desgleichen alle primitiven Kongruenzwurzeln von p durch g, g^{ϱ_2}, g^{ϱ_3}, $\ldots$, g^{ϱ_d}, wobei γ bzw. g eine beliebige unter ihnen ist. Aus der „vollständigen Zerlegung" der *Fermat*schen Funktion

$$u^{2n} - 1 \equiv (u - 1)(u - 2) \cdots (u - 2n) \pmod{p}$$

erschließt man dann leicht die Kongruenz

$$(36) \qquad f(u) \equiv (u-g)(u-g^{\varrho_2})(u-g^{\varrho_3}) \cdots (u-g^{\varrho_d}) \pmod p.$$

Wir verstehen im folgenden unter m eine ganze positive Zahl von der Eigenschaft, daß $n = m(2k+1)$ ist und bezeichnen mit $N_l l(\beta)$, $N_F l(\beta)$, $N_m l(\beta)$ die Norm der algebraischen Zahl $l(\beta_j)$, je nachdem β_j alle γ[1]), alle δ, oder schließlich alle Wurzeln der Gleichung $u^m + 1 = 0$ durchläuft. Dann beweisen wir zunächst den

Satz 3: Aus den Gleichungen (32) bzw. den Kongruenzen (29, 30) nebst der Kongruenz (33) folgt

$$(37) \qquad N_l l(\beta) = p, \quad N_F l(\beta) = 1, \quad \text{bzw.}$$

$$(38) \qquad l(u) \cdot l(u^{\varrho_2}) \cdot l(u^{\varrho_3}) \cdots l(u^{\varrho_d}) \equiv p \pmod{f(u)} \text{ und } \equiv 1 \pmod{F(u)}.$$

Beweis: Zunächst folgt die Äquivalenz von (37, 1) mit (38, 1) unmittelbar aus dem zu (35) Bemerkten. Das vollständige reduzierte Restsystem (35) für den Modul $2n$ enthält weiter, wie man leicht zeigt, jede reduzierte Restklasse (mod $2m$) gleich oft für ein bestimmtes m von der oben bezeichneten Eigenschaft. Die Kongruenz (38, 2) folgt somit aus (37, 2) — bzw. den hierin enthaltenen Gleichungen $N_m l(\beta) = 1$, wo $m \neq n$ ist — für jeden Modul $u^m + 1$, und also auch für das kleinste gemeinsame Vielfache dieser Moduln, eben für $F(u)$; ebenso folgt (37, 2) aus (38, 2).

Nun folgt aus (32) durch Bildung der Norm

$$N_m l(\beta) \cdot N_m s(\beta) = p^m, \quad N_m l(\beta) \cdot N_m t(\beta) = g^m + 1, \quad \text{folglich}$$

$$(39) \qquad N_m l(\beta) = p^e, \quad \text{wo } 0 \leqq e \leqq m, \quad \text{und } g^m + 1 \equiv 0 \pmod{p^e}.$$

Für $m < n$ muß also $e = 0$ sein, weil sonst (39, 2) der Voraussetzung widerspricht, daß g eine *primitive* Kongruenzwurzel von p ist; damit ist (37, 2) bewiesen. Wäre nun für $m = n$ ebenfalls $e = 0$, also $N_l l(\beta) \cdot N_F l(\beta) = 1$, und also auch $N_l l(\beta) = 1$, d. h.

$$l(u) \cdot l(u^{\varrho_2}) \cdot l(u^{\varrho_3}) \cdots l(u^{\varrho_d}) \equiv 1 \pmod{f(u)},$$

so folgte durch Einsetzen von g für u, unter Beachtung von (36):

$$l(g) \cdot l(g^{\varrho_2}) \cdot l(g^{\varrho_3}) \cdots l(g^{\varrho_d}) \equiv 1 \pmod p$$

im Widerspruch zu (33). Endlich folgt aus (32) noch $l(\beta)[s(\beta) + t(\beta)] = (p+g) - \beta$, also durch Normbildung

$$N_n l(\beta) N_n[s(\beta) + t(\beta)] = (p+g)^n + 1 \quad \text{und} \quad N_n l(\beta) \cdot N_n t(\beta) = g^n + 1,$$

$$(p+g)^n + 1 \equiv g^n + 1 \equiv 0 \pmod{N_n l(\beta)} \text{ und also } \equiv 0 \pmod{p^e},$$

$$(p+g)^n - g^n \equiv 0 \pmod{p^e}, \quad \text{d. h.:}$$

$$p^n + \binom{n}{1} p^{n-1} g + \binom{n}{2} p^{n-2} g^2 + \cdots + \binom{n}{2} p^2 g^{n-2} + p g^{n-1} \equiv 0 \pmod{p^e},$$

folglich $e = 1$, w. z. b. w.

[Man erkennt übrigens auch, daß $l(\gamma)$ eine „komplexe Primzahl" ist — d. h. daß es keine Zerlegung gibt $l(\gamma) = L_1(\gamma) \cdot L_2(\gamma)$, wo L_1 und L_2 beide keine kom-

[1]) Statt $N_l l(\beta)$ schreiben wir daher auch gelegentlich einfach $Nl(\gamma)$, ebenso $Nl(\delta)$ statt $N_F l(\beta)$.

plexen Einheiten sind — und daß es eine *primitive* Größe von $\Re(\gamma)$ sein muß — d. h. daß nicht $l(\gamma_1) = l(\gamma_2)$ sein kann —, weil sonst $N_f l(\beta)$ zwei von 1 verschiedene Teiler haben müßte.]

Wir beweisen weiter als *Umkehrung* den

Satz 4: Gelten für eine ganze rationale Funktion $l(u)$ die Gleichungen (37) [oder die Kongruenzen (38)], so existieren eine primitive Kongruenzwurzel g von p, welche die Kongruenz (33) erfüllt, sowie zwei ganze rationale Funktionen $s(u)$, $t(u)$, die zusammen mit $l(u)$ die Gleichungen (32) [oder die Kongruenzen (29, 30)] erfüllen[1]).

Beweis: Aus (38, 1) folgt unter Beachtung von (36)

$$l(g) \cdot l(g^{\varrho_2}) \cdot l(g^{\varrho_3}) \cdots l(g^{\varrho_d}) \equiv 0 \pmod{p},$$

d. h. die Kongruenz (33) ist erfüllt für mindestens *ein* g, w. z. b. w. Es ist aber dieses g vor den anderen primitiven Kongruenzwurzeln von p keineswegs bevorzugt. Bezeichnen wir nämlich mit $l^{(\varrho_i)}(u)$ die (mod $u^n + 1$) auf den Grad $n - 1$ reduzierte Funktion $l(u^{\varrho_i})$, und wählen wir d Zahlen ν_i so aus, daß $\varrho_i \nu_i \equiv 1 \pmod{2n}$ wird, so sind (37, 38) wie für $l(u)$ so auch für jedes $l^{(\varrho_i)}(u)$ erfüllt, und für ein beliebiges ν_i ist $l^{(\varrho_i)}(g^{\nu_i}) \equiv 0 \pmod{p}$, weil $l(g) \equiv 0 \pmod{p}$ ist. Wir können daher bei der rechnerischen Behandlung für g eine beliebige, z. B. die kleinste positive primitive Kongruenzwurzel von p wählen.

Sei nunmehr $s^*(u)$ so als ganze rationale Funktion [von höchstens $n - 1$-tem Grade] gewählt, daß

$$(40) \qquad s^*(u) \equiv l(u^{\varrho_2}) \cdot l(u^{\varrho_3}) \cdots l(u^{\varrho_d}) \pmod{u^n + 1}$$

ist, so folgt aus (38)

$$(41) \qquad l(u) \cdot s^*(u) = p - G_0(u) \cdot f(u) = 1 - G_4(u) \cdot F(u),$$

wobei $G_0(u)$, $G_4(u)$ gewisse ganze rationale ganzzahlige Funktionen sind, zwischen denen die aus (41) folgende Beziehung besteht

$$(42) \qquad G_0(u) \cdot f(u) - G_4(u) \cdot F(u) = 2n.$$

Wählen wir daher $s(u)$ als ganze rationale Funktion [von höchstens $n - 1$-tem Grade] so, daß

$$(43) \qquad s(u) \equiv s^*(u)\,[p + 1 - l(u)\,s^*(u)] \pmod{u^n + 1}$$

ist, so wird

---

[1]) Ein Teil dieses Satzes ist für einen speziellen Fall bereits bei *Kummer* a. a. O. (s. Fußnote 1) S. 21) bewiesen. Dort wird nämlich mutatis mutandis gezeigt: Ist α eine primitive q-te Einheitswurzel, *wo aber q eine Primzahl ist*; ist ferner die Primzahl $p = 2mq + 1$ in der Form $p = Nl(\alpha)$ darstellbar: so ist $\xi - \alpha$ teilbar durch $l(\alpha)$, und $l(\xi)$ teilbar durch p, wobei ξ der Kongruenz $\xi^{q-1} + \xi^{q-2} + \cdots + \xi^2 + \xi + 1 \equiv 0 \pmod{p}$ genügt. Der Beweis wird jedoch durch eine wesentlich umständlichere Rechnung erbracht als bei uns und läßt sich nicht auf den hier behandelten allgemeineren Fall übertragen. Ganz entsprechendes gilt für den weiter unten zu beweisenden Satz von der eindeutigen Zerlegbarkeit von p.

$l(u) \cdot s(u) \equiv l(u)\, s^*(u)\,[p + 1 - l(u)\, s^*(u)] \pmod{u^n + 1}$, also nach (41)

$\equiv [p - G_0(u) \cdot f(u)]\,[p + G_4(u) \cdot F(u)] \pmod{u^n + 1}$, daher nach (42) und (34)

$\equiv [p^2 - p \cdot 2n - G_0(u) \cdot G_4(u) \cdot (u^n + 1)] \pmod{u^n + 1}$, also wegen $2n = p - 1$

$$l(u) \cdot s(u) \equiv p \pmod{u^n + 1}, \tag{44}$$

d. h. $s(u)$ (43) ist die *eine* Funktion, deren Existenz zu beweisen war.

Setzen wir endlich

$$l^{(\varrho_i)}(u) = l^{(\varrho_i)}(g^{\nu_i}) + (u - g^{\nu_i}) \cdot l_{(1)}^{(\varrho_i)}(u), \tag{45}$$

so sind alle $l_{(1)}^{(\varrho_i)}(u)$ ganze rationale ganzzahlige Funktionen ihres Argumentes, und es wird, unter steter Verwendung nur solcher Funktionen, nach (40), und weil, wie vorhin erwähnt, $l^{(\varrho_i)}(g^{\nu_i}) \equiv 0 \pmod{p}$ ist,

$$s^*(u) \equiv -p\,P_1(u) - (u - g^{\nu_2})(u - g^{\nu_3}) \cdots (u - g^{\nu_d})\,P_2(u) \pmod{u^n + 1},$$

mithin

$$(g - u)\, s^*(u) \equiv p(u - g)\,P_1(u) + (u - g)(u - g^{\nu_2})(u - g^{\nu_3}) \cdots (u - g^{\nu_d})\,P_2(u) \pmod{u^n + 1},$$ also nach (36)

$$\equiv p\,P_3(u) + f(u)\,P_2(u) \pmod{u^n + 1},$$ daher nach (43, 41)

$$(g - u)\, s(u) \equiv [p\,P_3(u) + f(u)\,P_2(u)][p + G_4(u)\,F(u)] \pmod{u^n + 1},$$ also nach (34)

$$(g - u)\, s(u) \equiv p \cdot t(u) \pmod{u^n + 1}, \tag{46}$$

wo $t(u)$ eine (mod $u^n + 1$) wohlbestimmte ganze rationale ganzzahlige Funktion ist. Setzen wir aber hier für p nach (44) $l(u) \cdot s(u)$ ein und kürzen durch $s(u)$ — was erlaubt ist, weil $s(u)$ und $u^n + 1$ teilerfremd sind — so ergibt sich

$$g - u \equiv l(u) \cdot t(u) \pmod{u^n + 1},$$

d. h. $t(u)$ in (46) ist die *andere* Funktion, deren Existenz zu beweisen war.

Wir beweisen endlich noch den

Satz 5: Die Darstellung $p = l(\gamma) \cdot l^{(\varrho_2)}(\gamma) \cdot l^{(\varrho_3)}(\gamma) \cdots l^{(\varrho_d)}(\gamma)$ ist, wenn überhaupt, so im wesentlichen nur auf *eine* Art möglich.

„Im wesentlichen" soll dabei heißen: abgesehen von der Reihenfolge der Faktoren und von Abänderungen einer Funktion $l^*(u)$ in die Form

$$l(u) = G_1(u) \cdot l^*(u) + G_2(u) \cdot f(u), \tag{47}$$

wobei $G_1(u)$, $G_2(u)$ ganze usw. Funktionen sind und $G_1(\gamma)$ *eine komplexe Einheit*, d. h. $NG_1(\gamma) = 1$ ist.

Beweis: Angenommen, es sei

$$p = l(\gamma) \cdot l^{(\varrho_2)}(\gamma) \cdots l^{(\varrho_d)}(\gamma) = k(\gamma) \cdot k^{(\varrho_2)}(\gamma) \cdots k^{(\varrho_d)}(\gamma),$$

so können wir annehmen, daß $k(u)$ die Bedingung (33) $k(g) \equiv 0 \pmod{p}$ für dieselbe Kongruenzwurzel g erfüllt wie $l(u)$. Setzen wir dann wie in (45) $k(u) = k(g) + (u - g)\, k_{(1)}(u)$, so wird ganz wie vorhin erhalten

$$k(u) \cdot s^*(u) \equiv p \cdot P_4(u) \pmod{f(u)},$$ also nach (41)

$$\equiv l(u) \cdot s^*(u) \cdot P_4(u) \pmod{f(u)},$$ also

$$k(\gamma) = l(\gamma) \cdot P_4(\gamma).$$

Bildet man jetzt auf beiden Seiten die Norm über alle γ, so folgt

$$p = p \cdot NP_4(\gamma), \quad \text{folglich} \quad NP_4(\gamma) = 1, \quad \text{w. z. b. w.}$$

In Zusammenfassung der letzten Resultate gewinnen wir den folgenden

Satz 6: Die notwendigen und hinreichenden Bedingungen für die Existenz einer speziellen S-Basis erster Art sind

1. die Existenz einer ganzen rationalen ganzzahligen Funktion $l^*(u)$, die der Gleichung

$$Nl^*(\gamma) = p \tag{48}$$

genügt, sonst aber beliebig ist;

2. die Existenz zweier ebensolcher Funktionen $G_1(u)$ und $G_2(u)$ der Art, daß

$$NG_1(\gamma) = 1, \quad Nl(\delta) = 1 \text{ [1]} \tag{49}$$

wird, wobei $l(u)$ durch (47) erklärt ist.

Die Funktionen $l^*(u)$, $G_1(u)$ können dabei von kleinerem Grade als $f(u)$, die Funktion $G_2(u)$ von kleinerem als $F(u)$ vorausgesetzt werden; $l(u)$ ist höchstens von $n-1$-tem Grade. Die Forderung (49) ist gleichbedeutend damit, daß $G_1(\gamma)$ und — für *jedes* δ — $l(\delta)$ komplexe Einheiten seien.

Der **Beweis** des Satzes ergibt sich unmittelbar aus dem Vorhergehenden. Wir erwähnen nur noch, daß, wenn $G_1(u)$ und $G_2(u)$ die Bedingung (49) für irgendein $l^*(u)$ erfüllen, dann $G_1(u^\varrho)$ und $G_2(u^\varrho)$ das gleiche für $l^*(u^\varrho)$ leisten, daß es also gleichgültig ist, welchen der „konjugierten Teiler von p" man bevorzugen will. Die Beschränkung des Grades für $l(u)$ und $l^*(u)$ ist ohne weiteres verständlich. Setzt man weiter $G_1(u) = g_1(u)f(u) + G_1'(u)$ und $G_2(u) + g_1(u)l^*(u) = g_2(u)F(u) + G_2'(u)$, wo $G_1'(u)$ und $G_2'(u)$ den für $G_1(u)$ und $G_2(u)$ angegebenen Gradbeschränkungen genügen, so wird nach (47):

$$l(u) = G_1'(u)l^*(u) + G_2'(u)f(u) + g_2(u)(u^n + 1),$$

so daß man, was ja vorausgesetzt ist, $l(u)$ nur (mod $u^n + 1$) zu reduzieren braucht, um jener Forderung zu genügen.

Eine allgemeine Untersuchung, für welche Primzahlen die Bedingungen (48) und (49) erfüllt sind, soll im Rahmen dieser Arbeit nicht angeschnitten werden. Für die Untersuchung der Bedingung (48) sei auf die mehrfach erwähnte *Kummer*sche Gratulationsschrift [2] [3] sowie auf das Vorwort der „Tafeln komplexer Prim-

---

[1] Siehe Anm. 1) S. 23. [2] Siehe Anm. 1) S. 21.

[3] Daselbst ist bereits gezeigt, daß die Darstellung (48) nicht immer möglich ist. Für die Darstellung einer Primzahl $p = 2mq + 1$ — wo q eine Primzahl und α eine primitive q-te Einheitswurzel ist — in der Form $p = Nl(\alpha)$ wird nämlich als *notwendig* erkannt, daß $4p$ durch die quadratische Form $x^2 - (-1)^{\frac{p-1}{2}} qy^2$ darstellbar sei, was bekanntlich durchaus nicht immer der Fall ist. (Vgl. auch *Bachmann*, Die Lehre von der Kreisteilung usw. Leipzig 1872, S. 256.) Für eine Reihe von Fällen, in denen diese Darstellung möglich ist, hat *Kummer* sie dortselbst angegeben, darunter auch die Zerlegung von 11 im Körper der 5-ten, von 23 in dem der 11-ten Einheitswurzel. Siehe auch weiter unten § 4.

zahlen" von *Reuschle* [1]) verwiesen. Diesen Tafeln entnehmen wir die Ausdrücke $l^*(\gamma)$ — die also z. T. erst noch gemäß (47) in $l(\gamma)$ umzuformen sein werden — für die weiter unten (§ 4) zu behandelnden Einzelfälle [2]). Wir erwähnen jedoch bereits hier, daß in den genannten Tafeln die Ausdrücke $l^*(\gamma)$ für die Primzahlen bis zu 43 einschließlich sowie für 61, 67, 71 angegeben sind, daß ferner für die meisten übrigen Primzahlen unter 200 dort bereits die Nicht-Existenz von $l^*(\gamma)$ festgestellt wird.

Hinsichtlich der Bedingung (49) begnügen wir uns hier mit dem Beweise des folgenden Satzes:

Satz 7: Bei den Primzahlen $p = 2^{2^b} + 1$ und $p = 2q + 1$, wo q gleichfalls Primzahl, ist die Möglichkeit der Zerlegung (48) allein notwendig und hinreichend für die Existenz einer speziellen S-Basis erster Art.

Beweis: Für $n = 2^{2^b - 1}$ ist $u^n + 1$ irreduzibel, es existieren also überhaupt keine Wurzeln δ, für die (49, 2) erfüllt sein müßte. Für $n = q$ wird

$$f(u) = u^{q-1} - u^{q-2} + u^{q-3} - \cdot + \cdots - u + 1, \quad F(u) = u + 1,$$

daher reduziert sich (49, 2) auf die Bedingung $l(-1) = 1$. Da ferner $f(-1) = q$ wird, so sind nur die Bedingungen

$$(50) \qquad G_1(-1) \cdot l^*(-1) + G_2(-1) \cdot q = 1, \quad NG_1(\gamma) = 1$$

zu erfüllen. Setzt man in der mit (48) äquivalenten Kongruenz (38, 1) $u = -1$ und beachtet, daß das Restsystem (35) hier durch 1, 3, 5, ..., $q - 2$, $q + 2$, ..., $2q - 1$ dargestellt ist, so ergibt sich

$$(51) \quad [l^*(-1)]^{q-1} \equiv p \pmod q \equiv 1 \pmod q, \text{ folglich } l^*(-1) = c \not\equiv 0 \pmod q.$$

Es existieren daher zwei ganze Zahlen $\pi > 0$ und ϱ derart, daß

$$(52) \qquad \pi c + \varrho q = 1$$

wird. Setzt man daher

$$(53) \quad G_1(u) = 1 - u + u^2 - \cdot + \cdots + (-u)^{n-1}, \quad G_2(u) = \varrho,$$

so ist zunächst (50, 1) erfüllt. Das gleiche gilt aber auch für (50, 2), denn es wird

$$(1 + \gamma) G_1(\gamma) = 1 - (-\gamma)^n = 1 + \gamma_1,$$

wo $\gamma_1 = -(-\gamma)^n$, einerlei, ob π gerade oder ungerade ist, ebenfalls eine primitive $2q$-te Einheitswurzel ist, weil nach (52) $\pi \not\equiv 0 \pmod q$. Daher wird wegen

$$N(1 + \gamma) NG_1(\gamma) = N(1 + \gamma_1) \quad \text{und} \quad N(1 + \gamma) = N(1 + \gamma_1)$$

erhalten: $NG_1(\gamma) = 1$, w. z. b. w.

§ 3. Spezielle Minimalbasen zweiter Art.

Die im Vorstehenden behandelten „speziellen zyklischen Minimalbasen erster Art" leiden an einem Übelstand, der sich insbesondere bei der Anwendung

[1]) *Tafeln komplexer Primzahlen ...* von *Dr. C. G. Reuschle.* Berlin 1875.

[2]) Für $p = 11$ und $p = 23$ sind sie bereits bei *Kummer* zu finden. Vgl. Fußnote 3) S. 26.

auf die auflösbaren Gleichungen sehr störend bemerkbar macht. Sie sind nämlich aus zwei völlig heterogenen Bestandteilen zusammengesetzt: sie enthalten einerseits die Funktionen φ_{j+1} (14, 2)[1]), andererseits aber die Funktionen ψ_j (26) bzw. die aus diesen abgeleiteten Ψ_j (20), die zwar untereinander konjugiert sind, mit den φ_{j+1} (14, 2) jedoch in keinem organischen Zusammenhange stehen. Wir stellen daher die Frage: Ist es nicht möglich, *ohne Einführung der* φ_{j+1} (14, 2), unmittelbar, zunächst im $\Re(\varepsilon)$, $2n$ „konjugierte" Funktionen v_μ anzugeben,

$$
\begin{aligned}
v_0 &= k_0^{\lambda_0} k_1^{\lambda_1} \cdots k_{2n-2}^{\lambda_{2n-2}} k_{2n-1}^{\lambda_{2n-1}} \\
v_1 &= k_1^{\lambda_0} k_2^{\lambda_1} \cdots k_{2n-1}^{\lambda_{2n-2}} k_0^{\lambda_{2n-1}} \\
&\cdots\cdots\cdots\cdots\cdots \\
v_n &= k_n^{\lambda_0} k_{n+1}^{\lambda_1} \cdots k_{n-2}^{\lambda_{2n-2}} k_{n-1}^{\lambda_{2n-1}} \\
&\cdots\cdots\cdots\cdots\cdots \\
v_{2n-1} &= k_{2n-1}^{\lambda_0} k_0^{\lambda_1} \cdots k_{2n-3}^{\lambda_{2n-2}} k_{2n-2}^{\lambda_{2n-1}}
\end{aligned}
\tag{54}
$$

[vergleiche (6, 10)], die eine Basis für die S-Funktionen der k_μ bilden? Wenn das nämlich der Fall ist, so können wir in ganz analoger Weise, nur noch etwas kürzer, vorgehen wie im vorhergehenden Abschnitt. Da nämlich die v_μ, wie zu Beginn des § 1 erwähnt, durch E und T^{-1} nur die zyklische Vertauschung (11, 1) erleiden, so dulden die Funktionen

$$
V_\mu = \sum_0^{2n-1} {}_{\mu_1} \varepsilon^{g^{\mu_1 - \mu + 2n}} v_{\mu_1}\ ^2) \qquad (\mu = 0, 1, \ldots, 2n-1)
\tag{55}
$$

oder ausführlicher geschrieben

$$
\begin{aligned}
V_0 &= \varepsilon^{g^0} v_0 + \varepsilon^{g^1} v_1 + \cdots + \varepsilon^{g^{2n-2}} v_{2n-2} + \varepsilon^{g^{2n-1}} v_{2n-1} \\
V_1 &= \varepsilon^{g^{2n-1}} v_0 + \varepsilon^{g^0} v_1 + \cdots + \varepsilon^{g^{2n-3}} v_{2n-2} + \varepsilon^{g^{2n-2}} v_{2n-1} \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
V_{2n-1} &= \varepsilon^{g^1} v_0 + \varepsilon^{g^2} v_1 + \cdots + \varepsilon^{g^{2n-1}} v_{2n-2} + \varepsilon^{g^0} v_{2n-1}
\end{aligned}
\tag{56}
$$

die Vertauschung E, sind also *rational.* Sie bilden aber überdies eine Basis für die rationalen S-Funktionen der k_μ, d. h. eben eine *rationale zyklische Minimalbasis*[1]), weil die Determinante D_3 von (56) nicht verschwindet, wie sich leicht zeigen läßt. Denn es ist nach (55)

$$
D_3 = \left| (\varepsilon^{g^{2n-\mu}})^{g^{\mu_1}} \right|, \qquad (\mu, \mu_1 = 0, 1, \ldots, 2n-1)
$$

wo die Zeilen mit μ, die Spalten mit μ_1 numeriert sind. Da aber $g^{2n-\mu}$ und g^{μ_1} beide (mod p) die Zahlen $1, 2, \ldots, 2n-1, 2n$ durchlaufen, so kann man nach geeigneter Vertauschung der Reihen auch schreiben:

---

[1]) Von der Funktion φ_0 (14, 1) wird hier des kürzeren Ausdruckes wegen abgesehen; sie ist stets zu den anderen Basisfunktionen mit hinzuzunehmen. Ihr besonderer Charakter bildet übrigens bei den Anwendungen kein störendes Moment.

[2]) Der Exponent von g soll auf den kleinsten nicht negativen Rest (mod $2n$) reduziert werden.

$$D_3 = \pm \,|\, (\varepsilon^{\mu'})^{\mu_1'} \,|\, \ldots\ldots\ldots\ldots\ldots\ldots (\mu', \mu_1' = 1, 2, \ldots, 2n-1, 2n)$$
$$= \pm\, \varepsilon \cdot \varepsilon^2 \cdots \varepsilon^{2n} \cdot |\, (\varepsilon^{\mu'})^{\mu_1'-1} \,| = \pm\, |\, (\varepsilon^{\mu'})^{\mu_1'-1} \,|\,,$$

d. h. D_3 ist bis auf das Vorzeichen gleich dem Differenzenprodukt der Gleichung $u^{p-1} + u^{p-2} + \cdots + u + 1 = 0$ und also von Null verschieden, w. z. b. w.

In Analogie zu früheren Bezeichnungen wollen wir die Basis (54) eine *„spezielle S-Basis zweiter Art"*, die Basis (56) eine *„spezielle zyklische Minimalbasis zweiter Art"* nennen.

Nun erleiden die Basisfunktionen V_μ (56) durch T^{-1} nach (11, 1) die Vertauschung

$$\overline{U} = (V_0, V_1, \ldots, V_{2n-1}), \tag{21 a}$$

die sich von U (21) nur dadurch unterscheidet, daß sie sich auf $2n$ *unabhängige* Elemente statt auf deren n bezieht. Was wir im Anschluß an (21) über die Reduktion des Basisproblems gesagt haben, kann daher hier wörtlich wiederholt werden, wenn man nur U durch $\overline{U}$ ersetzt und statt von den $ST^\varkappa$-Funktionen der (Q) von den metazyklischen Funktionen der (x) spricht. Es ist übrigens durchaus nicht schwieriger, Minimalbasen für die durch $\overline{U}^\varkappa$ erzeugten Gruppen zu gewinnen als für die aus $U^\varkappa$ hervorgehenden; vielmehr läßt sich die erste Aufgabe unmittelbar auf die zweite zurückführen. Sehen wir nämlich für den Augenblick von der Bedeutung der V_μ und Ψ_j als Funktionen der k_μ völlig ab und betrachten sie als Unbestimmte, so können wir setzen

$$V_j - V_{n+j} = \Psi_j, \quad V_j + V_{n+j} = \Pi_j. \tag{57}$$

Vermöge (57, 1) entspricht dann die Vertauschung (21) der (21 a). Kennt man jetzt eine aus n Funktionen d_j bestehende Minimalbasis für die durch $U^\varkappa - \varkappa$ ein Teiler von $2n$ — erzeugte Gruppe, so braucht man zu ihr nur die n Koeffizienten c_j der „Tschirnhausen-Transformation"

$$\Pi_j = c_0 + c_1 \Psi_j^2 + c_2 \Psi_j^4 + \cdots + c_{n-1} \Psi_{n-1}^{2(n-1)} \tag{58}$$

hinzuzufügen, um eine Minimalbasis für die durch $\overline{U}^\varkappa$ erzeugte Gruppe zu gewinnen. Denn die Funktionen d_j und c_j dulden $\overline{U}^\varkappa$ — erstere, weil sie $U^\varkappa$ dulden, letztere nach einem bekannten Satze von *Lagrange* bzw. dessen Erweiterung —, und der Körper der (V) ist vom Grade $\frac{2n}{\varkappa}$ über dem der (c, d); denn der Körper der (Ψ) ist vom Grade $\frac{2n}{\varkappa}$ über dem der (d), und mit den (Ψ) sind auch die (Π) nach (58) und die (V) wegen $V_\mu = \frac{1}{2}(\Pi_\mu + \Psi_\mu)$ rational bekannt [1] [2]. Wir gewinnen daher analog zu Satz 2 den

---

[1] Siehe Fußnote 1) S. 20.

[2] Vgl. auch *Breuer, Zur Theorie der metazyklischen Gleichungen von Primzahlgrad,* in *Beiträge zur Algebra,* Sitzungsberichte der Heidelberger Akademie der Wissenschaften, Math.-Naturwiss. Kl. 1925, 5. Abhandlg.

Satz 2a: Die Kenntnis einer speziellen S-Basis zweiter Art reduziert das Problem der Aufsuchung von Minimalbasen für die metazyklischen Gruppen p-ten Grades *ohne Benutzung der Funktionen* φ_{j+1} (14) auf das gleiche Problem bei den zyklischen (Permutations-) Gruppen $2n$-ten bzw. n-ten Grades.

Eine Minimalbasis für die S-Funktionen der (k) wird nun — vergleiche das zu (18) Bemerkte — durch die $2n$ Funktionen

$$k_0^p, \quad k_0^{-g^{\bar{\mu}}} k_{\bar{\mu}} \qquad (\bar{\mu} = 1, 2, \ldots, p-2) \tag{18a}$$

gebildet. Daher ergeben sich, wiederum analog zu dem, was bei (24, 25) ausgeführt wurde, als *notwendig und hinreichend* dafür, daß die v_μ (54) eine Basis für die S-Funktionen der (k) bilden, die beiden Bedingungen:

$$v_0^{\sigma_0} v_1^{\sigma_1} \cdots v_{2n-1}^{\sigma_{2n-1}} = k_0^p, \tag{24a}$$

$$v_0^{\tau_0} v_1^{\tau_1} \cdots v_{2n-1}^{\tau_{2n-1}} = k_0^q k_1^{-1}, \tag{25a}$$

während die Bedingung (7) an Stelle von (9) tritt. Führen wir daher zur Abkürzung die Bezeichnung

$$\lambda_0 + \lambda_1 u + \lambda_2 u^2 + \cdots + \lambda_{2n-1} u^{2n-1} = \lambda(u), \tag{31a}$$

sowie für späteren Gebrauch

$$\bar{l}_0 + \bar{l}_1 u + \cdots + \bar{l}_{n-1} u^{n-1} = \bar{l}(u) \tag{31b}$$

nebst den entsprechend erklärten Bezeichnungen $\sigma(u)$, $\tau(u)$ und $\bar{s}(u)$, $\bar{t}(u)$ ein, so erhalten wir auf dem Wege über Gleichungen (27a, 28a), die wir hier unterdrücken können, die Kongruenzen

$$\lambda(u) \cdot \sigma(u) \equiv p \pmod{u^{2n} - 1} \tag{29a}$$

$$\lambda(u) \cdot \tau(u) \equiv g - u \pmod{u^{2n} - 1} \tag{30a}$$

oder die für *alle* $2n$ Wurzeln ϑ_μ der Gleichung $u^{2n} - 1 = 0$ zu erfüllenden Gleichungen

$$\lambda(\vartheta) \cdot \sigma(\vartheta) = p, \qquad \lambda(\vartheta) \cdot \tau(\vartheta) = g - \vartheta \tag{32a}$$

und die Kongruenz

$$\lambda(g) \equiv 0 \pmod{p} \tag{33a}$$

als notwendige und hinreichende Bedingungen für die Existenz einer speziellen S-Basis zweiter Art.

Setzen wir jetzt

$$\begin{aligned} \lambda_j - \lambda_{n+j} &= l_j, & \lambda_j + \lambda_{n+j} &= \bar{l}_j \\ \sigma_j - \sigma_{n+j} &= s_j, & \sigma_j + \sigma_{n+j} &= \bar{s}_j \\ \tau_j - \tau_{n+j} &= t_j, & \tau_j + \tau_{n+j} &= \bar{t}_j, \end{aligned} \tag{59}$$

so folgt unter Beachtung von (31, 31a, 31b)

(60) $\bar{l}(u) \equiv l(u) \pmod 2$, $\bar{s}(u) \equiv s(u) \pmod 2$, $\bar{t}(u) \equiv t(u) \pmod 2$,

weil sonst die „Gleichungen" (59) keine ganzzahlige Auflösung nach den Größen $\lambda_\mu, \sigma_\mu, \tau_\mu$ hätten. Setzen wir daher

$$\bar{l}(u) - l(u) = 2d(u), \tag{61}$$

so wird

$$\lambda(u) = l(u) + (u^n + 1)\, d(u) = \bar{l}(u) + (u^n - 1)\, d(u). \tag{62}$$

Daher erhalten wir, unter Hinzufügung der entsprechenden Gleichungen für $\sigma(u)$ und $\tau(u)$:

$$\begin{aligned} \lambda(a) &= \bar{l}(a), & \lambda(\beta) &= l(\beta) \\ \sigma(a) &= \bar{s}(a), & \sigma(\beta) &= s(\beta) \\ \tau(a) &= \bar{t}(a), & \tau(\beta) &= t(\beta). \end{aligned} \tag{63}$$

Endlich folgt aus (62, 1)

$$\lambda(g) \equiv l(g) \pmod p. \tag{64}$$

Läßt man daher in (32 a) ϑ zunächst nur die Werte β_j durchlaufen, so gehen diese Gleichungen in (32) über, während (33 a) nach (64) mit (33) äquivalent ist, d. h.: *Für die Existenz einer speziellen S-Basis zweiter Art ist die einer solchen erster Art eine notwendige Voraussetzung.* In der Tat erkennt man, daß die Größen $\frac{v_{n+j}}{v_j}$, die ja in die Basis zweiter Art (54), etwa an Stelle der n letzten Funktionen v_{n+j}, eingeführt werden könnten, mit den Basisfunktionen ψ_j der Basis erster Art (26) übereinstimmen.

Wir lassen nun ϑ in (32 a) alle Werte a_j durchlaufen, und multiplizieren die so erhaltenen Gleichungen je miteinander. Es ergibt sich in leichtverständlicher Bezeichnung:

$$N_{u^n-1}\bar{l}(a) \cdot N_{u^n-1}\bar{s}(a) = p^n, \qquad N_{u^n-1}\bar{l}(a) \cdot N_{u^n-1}\bar{t}(a) = g^n - 1.$$

Ganz ähnlich wie bei (39) ergibt sich hieraus, da g eine primitive Kongruenzwurzel von p ist,

$$N_{u^n-1}\bar{l}(a) = 1, \tag{65}$$

d. h. $\bar{l}(a_j)$ ist für *jedes* a_j eine komplexe Einheit [oder auch: $\lambda(\vartheta)$ ist für jedes imprimitive ϑ eine komplexe Einheit; vergleiche (49, 2)].

Für die Gewinnung einer speziellen S-Basis zweiter Art ist also, neben der Existenz von $l(u)$ gemäß Satz 6, noch die einer ganzen rationalen ganzzahligen Funktion $\bar{l}(u)$ *notwendig*, welche die Bedingungen (60, 1) und (65) erfüllt. Wir beweisen jetzt, daß diese Bedingungen auch *hinreichen*, indem wir zeigen, daß dann auch stets zwei Funktionen $\bar{s}(u)$, $\bar{t}(u)$ existieren, die zusammen mit $\bar{l}(u)$ die Gleichungen

$$\bar{l}(a) \cdot \bar{s}(a) = p, \qquad \bar{l}(a) \cdot \bar{t}(a) = g - a \tag{32 b}$$

für alle a_j erfüllen und den Bedingungen (60, 2 und 3) genügen.

Man bemerkt zunächst, daß das Restsystem (35) die sämtlichen reduzierten Restklassen (mod n) bei ungeradem n je einmal, bei geradem n je zweimal enthält. Wählen wir daher $\bar{s}^*(u)$ als ganze usw. Funktion (von höchstens $n-1$-tem Grade) so, daß

$$\bar{s}^*(u) \equiv \bar{l}(u^{\varrho_2})\,\bar{l}(u^{\varrho_3}) \cdots \bar{l}(u^{\varrho_d}) \pmod{u^n - 1} \tag{40 a}$$

ist, so folgt aus (65) ganz ähnlich wie bei (37, 38):

$$\bar{l}(u)\,\bar{s}^*(u) \equiv 1 \pmod{u^n - 1}.$$

Wählen wir daher weiter $\bar{s}(u)$ (von höchstens $n-1$-tem Grade) so, daß

$$\bar{s}(u) \equiv \bar{s}^*(u)\,[p + 1 - l(u)\,\bar{s}^*(u)] \pmod{u^n - 1}, \text{ d. h. } \bar{s}(u) = p \cdot \bar{s}^*(u) \tag{43 a}$$

ist, so wird

$$\bar{l}(a) \cdot \bar{s}(a) = p$$

für jedes a, entsprechend der Bedingung (32 b, 1). Nun war doch schon früher analog zu (40 a)

$$s^*(u) \equiv l(u^{\varrho_2})\,l(u^{\varrho_3}) \cdots l(u^{\varrho_d}) \pmod{u^n + 1}, \tag{40}$$

es ist aber auch gemäß der aus (60, 1) folgenden Gleichung (61)

$$\bar{l}(u^{\varrho_2})\,\bar{l}(u^{\varrho_3}) \cdots \bar{l}(u^{\varrho_d}) \equiv l(u^{\varrho_2})\,l(u^{\varrho_3}) \cdots l(u^{\varrho_d}) \pmod 2,$$

folglich ist auch

$$\bar{s}^*(u) \equiv s^*(u) \pmod 2. \tag{66}$$

Denn wenn zwei Funktionen beliebigen Grades $H_1(u)$ und $H_2(u)$ nach dem Modul 2 kongruent sind, so behalten sie diese Eigenschaft bei, wenn man sie nach den Moduln $u^n + 1$ bzw. $u^n - 1$ reduziert. Sei nämlich

$$h_1(u) + h_1^*(u) \cdot (u^n + 1) \equiv h_2(u) + h_2^*(u) \cdot (u^n - 1) \pmod 2, \tag{67}$$

wo $h_1(u)$, $h_2(u)$ von höchstens $n-1$-tem Grade seien, so muß auch $h_1^*(u) \equiv h_2^*(u) \pmod 2$ sein, weil sonst die Koeffizienten der höchsten Potenzen von u auf beiden Seiten von (67) nicht kongruent nach dem Modul 2 sein können. Daher ergibt sich wegen

$$h_1(u) \equiv h_2(u) + [h_2^*(u) - h_1^*(u)]\,(u^n - 1) - 2\,h_1^*(u) \pmod 2, \text{ daß}$$
$$h_1(u) \equiv h_2(u) \pmod 2.$$

Damit ist die Kongruenz (66) bewiesen. Multiplizieren wir sie mit der aus ihr selbst und (60, 1) folgenden Kongruenz

$$p + 1 - \bar{l}(u)\,\bar{s}^*(u) \equiv p + 1 - l(u)\,s^*(u) \pmod 2,$$

so folgt nach (43) und (43 a)

$$\bar{s}(u) \equiv s(u) \pmod 2 \tag{68}$$

entsprechend der Bedingung (60, 2).

Nun ist $\bar{s}(u)$ nach (43 a) durch p teilbar. Daher kann man eine Funktion $\bar{t}(u)$ von höchstens $n-1$-tem Grade durch die Kongruenz

(46 a) $$(g-u)\,\bar{s}(u) \equiv p \cdot \bar{t}(u) \pmod{u^n-1}$$

bestimmen. Multipliziert man beide Seiten von (46 a) mit $l(u)$, so erkennt man, daß $\bar{t}(u)$ die Bedingung (32 b, 2) für alle a_j erfüllt. Endlich folgt aus (46), (46 a) und (68) ganz wie vorhin

(69) $$\bar{t}(u) \equiv t(u) \pmod 2$$

entsprechend der Bedingung (60, 3).

Wir können nun den folgenden Satz aussprechen:

Satz 6a: Die notwendigen und hinreichenden Bedingungen für die Existenz einer speziellen S-Basis zweiter Art sind

1. die Existenz einer Funktion $l(u)$ gemäß Satz 6,
2. die Existenz einer ganzen usw. Funktion $\bar{l}(u)$ von höchstens $n-1$-tem Grade der Art, daß

(70) $$\bar{l}(u) \equiv l(u) \pmod 2, \quad N_{u^n-1}\bar{l}(a) = 1$$

wird.

Der **Beweis** des Satzes ergibt sich unmittelbar aus dem Vorhergehenden. Wir erwähnen ganz wie bei Satz 6, daß, wenn $\bar{l}(u)$ die Bedingung (70) für irgendein $l(u)$ erfüllt, dann $\bar{l}(u^\varrho)$ das gleiche für $l(u^\varrho)$ leistet, daß es also auch hier gleichgültig ist, welchen der konjugierten Teiler von p man bevorzugen will. Dies ist besonders wichtig für einen etwaigen Beweis der Nichtexistenz von speziellen S-Basen für einen bestimmten Primzahlgrad. Denn wenn beim Satze 6 die Funktionen $G_1(u)$, $G_2(u)$ für irgend ein $l^*(u)$, oder hier die Funktion $\bar{l}(u)$ für irgend ein $l(u)$ *nicht* existieren, so existieren sie auch für keine der konjugierten Funktionen $l^*(u^\varrho)$ bzw. $l(u^\varrho)$. Für einen Beweis der Nichtexistenz von speziellen S-Basen zweiter Art, d. h. von $\bar{l}(u)$ (70) müßte man aber ganz entsprechend auch zeigen, daß, wenn $\bar{l}^0(u)$ für $l^0(u)$ gemäß (70) existiert, dann auch $\bar{l}(u)$ für $l(u)$ existiert, wenn dabei unter $l^0(u)$ eine Funktion von höchstens $n-1$-tem Grade verstanden wird, welche die Form besitzt

(71) $$l^0(u) = E(u) \cdot l(u) + G(u) \cdot (u^n + 1),$$

wobei $E(\beta)$ für *alle* n Größen β_j eine komplexe Einheit ist. Um dieses zu klären, beachte man zunächst, daß zu jedem $E(u)$ ein $E^{-1}(u)$ existiert — nämlich das (mod u^n+1) reduzierte Produkt $E(u^{\varrho_2})\,E(u^{\varrho_3}) \cdots E(u^{\varrho_d})$ — derart, daß $E(u) \cdot E^{-1}(u) \equiv 1 \pmod{u^n+1}$ ist. Ferner kann aber zu jedem $E(u)$ ein $\overline{E}(u)$ gefunden werden, so daß $E(u) \equiv \overline{E}(u) \pmod 2$ ist, und daß $\overline{E}(a)$ *für alle* a_j eine komplexe Einheit ist, vorausgesetzt freilich, daß n ungerade ist. In diesem Falle nämlich sind die a_j und β_j einander paarweise entgegengesetzt gleich, und wir können daher $\overline{E}(u) = E(-u)$ setzen. Ist aber n gerade, so sind die β_j selbst zu je zweien einander entgegengesetzt gleich, $\overline{E}(u)$ ist also jedenfalls nicht auf so einfache Weise zu bilden. Eine nähere Untersuchung hierüber, wie über ähnliche

in dieser Arbeit noch offen gelassene Fragen, behalten wir uns für eine andere Gelegenheit vor. Im Falle der Existenz von $\overline{E}(u)$, insbesondere also für ungerades n kann aber der erwähnte Beweis leicht geführt werden. Ist nämlich bei (71)

$$l^0(u) \equiv \bar{l}^0(u) \pmod 2,$$

so multiplizieren wir diese Kongruenz mit der folgenden

$$E^{-1}(u) \equiv \overline{E}^{-1}(u) \pmod 2,$$

und erhalten

$$l(u) \equiv \bar{l}^0(u) \cdot \overline{E}^{-1}(u) \pmod 2.$$

Die rechte Seite wird für jedes a_j als Produkt zweier Einheiten selbst eine Einheit. Damit ist unsere Behauptung bewiesen.

Auch hier beschränken wir uns im Rahmen dieser Arbeit auf die Behandlung einiger Beispiele, ohne *allgemein* zu untersuchen, wann die Bedingung (70) erfüllt ist. Es sei nur hervorgehoben, daß die Untersuchungen des § 1 ihre Bedeutung behalten, auch abgesehen davon, daß es Fälle gibt (z. B. $p = 13$), in denen zwar eine spezielle S-Basis erster, nicht aber eine zweiter Art existiert. Denn auch in den Fällen, in denen schon die Basis erster Art nicht existiert, d. h. also in der Mehrzahl der Fälle, wird man doch zur Vereinfachung des Problems (vgl. Satz 1 und den Anfang des § 2) auf die Basisfunktionen φ_{j+1} (14) zurückgreifen.

§ 4. Anwendungen und Beispiele.

Im folgenden werden für einige Primzahlen die Funktion $l(u)$ so, wie sie zur Konstruktion der Funktionen ψ_j (26) nötig ist, und teilweise auch letztere selbst bestimmt. An sich ist hierzu die Berechnung der Funktionen $s(u)$, $t(u)$ nicht erforderlich. Auch diese werden aber überall hinzugefügt, um eine leichte Kontrolle der Richtigkeit an Hand der Formeln (29, 30) sowie überhaupt die *Anwendung* der Basis (26) zu ermöglichen. In einigen Fällen wird auch die Funktion $\bar{l}(u)$ berechnet, die zusammen mit $l(u)$ nach (59) die Bestimmung von $\lambda(u)$ und damit die der speziellen S-Basis zweiter Art (54) erlaubt. Auch hier fügen wir, zur Kontrolle der Richtigkeit an Hand der Formeln (60, 32b) bzw. (29a, 30a) auch die Funktionen $\bar{s}(u)$, $\bar{t}(u)$ bzw. $\sigma(u)$, $\tau(u)$ bei [1]). Auf die verschiedenen erwähnten Kontrollen wird im folgenden in der Regel nicht mehr besonders hingewiesen werden, da der Leser sie leicht durchführen kann, etwa so, wie wir es weiterhin, als Beispiel, im Falle $p = 23$ zeigen.

Die in den vorhergehenden Paragraphen angegebene, *allgemein gültige* Berechnung der Funktionen $s(u)$ und $\bar{s}(u)$ ist übrigens, wie besonders hervorgehoben sei, durchaus nicht immer die *praktisch einfachste.* Wir verzichten jedoch hier

---

[1]) Wo wir im folgenden die Funktionen ψ_j (26) oder v_μ (54) aufgeführt haben, kann deren Eigenschaft, eine Minimalbasis zu bilden, leicht an Hand der entsprechenden Formeln (24, 25) bezw. (24a, 25a) festgestellt werden.

darauf, die leicht erkennbaren Rechenvorteile, insbesondere für die Primzahlen $p = 2q + 1$, aufzuführen.

Wo im folgenden Bezeichnungen $L^*(u)$, $L(u)$, $S(u)$ usw. auftreten, entsprechen sie den gleichen Funktionen mit kleinen Buchstaben, nur erfüllen $L^*(u)$ und $L(u)$, im Gegensatz zu $l^*(u)$ und $l(u)$, die Kongruenz (33) nicht für die *kleinste* positive Kongruenzwurzel von p. Wo Formeln mit Nummern bezeichnet sind, die bereits bei früheren Gleichungen Verwendung fanden, soll damit auf jene als theoretische Grundlage der Rechnung hingewiesen werden.

Im Falle

1. $\boldsymbol{p = 3}$, $n = 1$, $g = 2$

ist zwar eine zyklische Minimalbasis — eine andere kommt hier nicht in Frage — schon lange bekannt[1]), auch werden die Rechnungen beinahe trivial; sie sollen aber doch, einer einfachen Anwendung wegen, angegeben werden. Da hier

(34; 1) $\qquad f(u) = u + 1$ (vgl. auch Satz 7)

ist und $g - \beta$ also nur den Wert 3 annimmt, so ist 3 selbst der gesuchte gemeinsame Teiler $l(\beta)$ von p und $g - \beta$, d. h. es wird

(72) $\qquad l(u) = 3, \quad s(u) = 1, \quad t(u) = 1.$

Wir beschränken uns hier auf Behandlung der speziellen S-Basis zweiter Art und finden leicht

(72 b) $\qquad \bar{l}(u) = 1, \quad \bar{s}(u) = 3, \quad \bar{t}(u) = 1,$

also

(72 a) $\qquad \lambda(u) = 2 - u, \quad \sigma(u) = 2 + u, \quad \tau(u) = 1,$

mithin

(54; 1) $\qquad v_0 = k_0^2 k_1^{-1}, \quad v_1 = k_1^2 k_0^{-1},$

(56; 1) $\qquad V_0 = \varepsilon k_0^2 k_1^{-1} + \varepsilon^2 k_1^2 k_0^{-1}, \quad V_1 = \varepsilon^2 k_0^2 k_1^{-1} + \varepsilon k_1^2 k_0^{-1}.$

Wir machen eine Anwendung dieses Resultates, um die Koeffizienten der *zyklischen* Gleichungen der Form

(73) $\qquad x^3 + a_2 x + a_3 = 0$

durch zwei Parameter, eben die Basisfunktionen V_0 und V_1, auszudrücken. Da nun nach (3)

$$x_\nu = \varepsilon^{-\nu} k_0 + \varepsilon^{-2\nu} k_1 \qquad (\nu = 0, 1, 2),$$

so wird

$$a_2 = x_0 x_1 + x_1 x_2 + x_2 x_0 = -3 k_0 k_1 = -3 v_0 v_1$$
$$a_3 = -x_0 x_1 x_2 \qquad\qquad = -(k_0^3 + k_1^3) = -v_0 v_1 (v_0 + v_1).$$

---

[1]) Vergleiche *F. Hack*, Beiträge zur Anwendung der Gruppentheorie usw., Diss. Tübingen 1895. — *F. Seidelmann*, Die Gesamtheit der kubischen und biquadratischen Gleichungen usw., Diss. Erlangen 1916.

Setzen wir hierein die aus (54; 1 und 56; 1) sich ergebenden Ausdrücke

$$3v_0 = -(V_0 + V_1) + \varepsilon^2 V_0 + \varepsilon V_1, \quad 3v_1 = -(V_0 + V_1) + \varepsilon V_0 + \varepsilon^2 V_1$$

ein, so erhalten wir die gesuchten Ausdrücke

$$(74) \quad a_2 = -(V_0^2 + V_0V_1 + V_1^2), \quad a_3 = \frac{1}{3}(V_0 + V_1)(V_0^2 + V_0V_1 + V_1^2).$$

Setzt man hier noch

$$(75) \qquad V_0 + V_1 = 2r, \quad V_0 - V_1 = 6s,$$

so erhält man die *Hack-Seidelmann*sche [1]) Form der Koeffizienten

$$(74\,a) \qquad a_2 = -3(r^2 + 3s^2), \quad a_3 = 2r(r^2 + 3s^2),$$

vor der die unsere (74) die größere Symmetrie voraus hat, da sie sich nicht ändert, wenn die beiden Parameter V_0, V_1 miteinander vertauscht werden. Dies rührt offenbar davon her, daß V_0, V_1 „konjugierte" Funktionen sind. Bei den Gleichungen fünften Grades fällt dieser Umstand ganz bedeutend ins Gewicht.

2. $\boldsymbol{p = 5}$, $n = 2$, $g = 2$; (34; 2) $f(u) = u^2 + 1$; Satz 7.

Da $5 = (2 + i)(2 - i)$, so findet man unmittelbar

$$(76) \qquad l(u) = 2 - u, \quad s(u) = 2 + u, \quad t(u) = 1,$$

$$(26;\,2) \qquad \psi_0 = q_0^2 q_1^{-1}, \quad \psi_1 = q_1^2 q_0.$$

Die aus (26; 2) mit Hilfe der schon lange bekannten zyklischen Minimalbasis vierten Grades [1]) sich ergebenden metazyklischen Minimalbasen im $\mathfrak{R}(\varepsilon)$ und im $\mathfrak{R}_0$ sind in *B.* § 2 eingehend untersucht, ebenso auch die weiter unten abgeleitete Basis (26; 3) für $p = 7$. Nur sind dort an Stelle der hier eingeführten Funktionen φ_{j+1} (14, 2) andere, aber prinzipiell das Gleiche leistende Funktionen eingeführt. Dort werden auch in der Einleitung und im § 3 die Gründe auseinandergesetzt, aus welchen die so gewonnenen Minimalbasen zur Koeffizienten-Darstellung ungeeignet sind. Diese Gründe gelten aber *nicht* für die nun zu bestimmende spezielle *S*-Basis zweiter Art. Man findet leicht

$$(76\,b) \qquad \bar{l}(u) = u, \quad \bar{s}(u) = 5u, \quad \bar{t}(u) = -1 + 2u,$$

$$(76\,a) \qquad \lambda(u) = 1 - u^2 + u^3, \quad \sigma(u) = 1 + 3u - u^2 + 2u^3, \quad \tau(u) = u - u^2 + u^3,$$

$$(54;\,2) \qquad v_0 = \frac{k_0 k_3}{k_2}, \quad v_1 = \frac{k_1 k_0}{k_3}, \quad v_2 = \frac{k_2 k_1}{k_0}, \quad v_3 = \frac{k_3 k_2}{k_1}.$$

Diese Basis ist infolge ihres symmetrischen Baues zur Darstellung der Koeffizienten der auflösbaren Gleichungen fünften Grades hervorragend geeignet. Der Verfasser hat diese Darstellung an anderem Orte [2]) vollständig durchgeführt,

---

[1]) Siehe Anm. 1) S. 35.

[2]) *Breuer*, Über die irreduzibelen auflösbaren Gleichungen fünften Grades. Festschrift anläßlich des 100-jährigen Bestehens der Technischen Hochschule Karlsruhe 1925, Seite 107—129. — Die dortige Formel (13) entspricht unserer Formel (54; 2) bis auf Numerierung und Bezeichnung.

und zwar unter Trennung der auflösbaren Gleichungen nach ihren *Galois*schen Gruppen.

Wir erwähnen noch, daß im Einklang mit unserer Bemerkung zu Formel (64) hier die Quotienten $\frac{v_2}{v_0}$ und $\frac{v_3}{v^1}$ mit ψ_0, ψ_1 (26; 2) übereinstimmen und betrachten nunmehr den Fall

3. $\boldsymbol{p=7}$, $n=3$, $g=3$; (34; 3) $f(u)=u^2-u+1$, $F(u)=u+1$; Satz 7.

Wir finden bei *Reuschle*[1])

$$L^*(u)=1-3u,$$

also $L^*(5)\equiv 0 \pmod 7$. Da nun[2]) $5^5\equiv 3 \pmod 7$, $5\cdot 5\equiv 1 \pmod 6$, ist folglich $l^*(u)\equiv L^*(u^5) \pmod{u^3+1}$, also $l^*(u)=1+3u^2$, wo $l^*(3)\equiv 0 \pmod 7$; aber $l^*(-1)=4$, mithin (47; 3) $l(u)=l^*(u)-f(u)$, oder bei Division durch den überflüssigen Faktor u, $l(u)=1+2u$.

Das Restsystem (35) wird hier durch 1,5 dargestellt, also ist $s^*(u)=1-2u^2$, woraus sich $s(u)$ nach (43) und $t(u)$ nach (46) sofort bestimmen lassen. Man findet

(77) $l(u)=1+2u$, $s(u)=-1+2u-4u^2$, $t(u)=-1+u-2u^2$,

(26; 3) $\psi_0=q_0q_1^2$, $\psi_1=q_1q_2^2$, $\psi_2=q_2q_0^{-2}$ [3]).

Weiter sieht man unmittelbar, daß

(77 b) $\bar{l}(u)=1$, $\bar{s}(u)=7$, $\bar{t}(u)=3-u$

wird, also

(77 a) $\lambda(u)=1+u-u^4$, $\sigma(u)=3+u-2u^2+4u^3-u^4+2u^5$, $\tau(u)=1-u^2+2u^3-u^4+u^5$

(54; 3)
$$v_0=\frac{k_0k_1}{k_4},\quad v_1=\frac{k_1k_2}{k_5},\quad v_2=\frac{k_2k_3}{k_0},$$
$$v_3=\frac{k_3k_4}{k_1},\quad v_4=\frac{k_4k_5}{k_2},\quad v_5=\frac{k_5k_0}{k_3}.$$

Wie der Fall $p=7$ im Hinblick auf Satz 2 sich unmittelbar an $p=3$ anschließt, so behandeln wir jetzt im Hinblick auf $p=5$ den Fall $p=11$ und weiter $p=23$.

---

[1]) In den „Tafeln" findet man die Form $L^*(u)=1+3u$, weil dort der Körper der Wurzeln von $u^2+u+1=0$ zugrunde gelegt ist, nicht der von $f(u)=0$. Das Vorzeichen von u war also zu ändern. Entsprechendes gilt für die Fälle $p=11$, 23, 19, während wir bei $p=13$, 17 die Funktion $L^*(u)$ unmittelbar von *Reuschle* entnehmen können.

[2]) Vergleiche hierzu die Bemerkung am Anfang des Beweises zu Satz 4.

[3]) Diese Basis (26; 3) ist, ebenso wie die (26; 2) für $p=5$ schon früher von Fräulein *Noether* angegeben worden, wenn auch nur in dieser, ausschließlich für den Bereich $\mathfrak{R}(\epsilon)$ gültigen Form; vgl. hierzu *B.* Einleitung. Dagegen sind die speziellen *S*-Basen zweiter Art (54; 2 und 54; 3), ebenso wie überhaupt die Minimalbasen in allen weiterhin behandelten Fällen, unseres Wissens noch nirgends angegeben worden; selbst die Frage nach der Existenz der Minimalbasis ist für $p>7$ früher noch nicht geklärt worden.

4. $\boldsymbol{p = 11}$, $n = 5$, $g = 2$; (34; 4) $f(u) = u^4 - u^3 + u^2 - u + 1$,
$F(u) = u + 1$; Satz 7.

Wir finden bei *Kummer* und *Reuschle*, nach Multiplikation mit gewissen Potenzen von u

$$L^*(u) = 1 + 2u^2.$$

Wir ordnen hier die Rechnung etwas anders an, als im vorigen Falle. Es ist $L^*(-1) = 3$; (52; 4) $2 \cdot 3 - 1 \cdot 5 = 1$, also $\pi = 2$, $\varrho = -1$; mithin nach (53) und (47) $L(u) = (1 - u)(1 + 2u^2) - f(u)$, oder nach Division durch u^2: $L(u) = 1 - u - u^2$, also $L(7) \equiv 0 \pmod{11}$; folglich wird wegen[1]) $7^3 \equiv 2 \pmod{11}$, $3 \cdot 7 \equiv 1 \pmod{10}$; $l(u) \equiv L(u^7) \pmod{u^5 + 1}$, d. h. $l(u) = 1 + u^2 - u^4$; nun ergibt sich nach (40) sehr einfach

$$\begin{aligned} s^*(u) &= (1 - u - u^2)(1 + u^3 + u^4)(1 + u - u^3) \\ &\equiv 2 + 4u - u^2 - 3u^3 + u^4 \pmod{u^5 + 1}, \end{aligned}$$

und $s(u)$ nach (43), oder auch — wegen $s^*(-1) = 1$ — nach der Formel $s(u) = s^*(u) + 2f(u)$, wodurch ebenfalls $s(-1) = 11$ erreicht wird, sowie schließlich $t(u)$ nach (46). Man findet:

$$\text{(78)} \quad l(u) = 1 + u^2 - u^4, \quad s(u) = 4 + 2u + u^2 - 5u^3 + 3u^4, \quad t(u) = 1 - u^3 + u^4.$$

$$\text{(26; 4)} \quad \psi_0 = \frac{q_0 q_2}{q_4}, \quad \psi_1 = q_0 q_1 q_3, \quad \psi_2 = q_1 q_2 q_4, \quad \psi_3 = \frac{q_2 q_3}{q_0}, \quad \psi_4 = \frac{q_3 q_4}{q_1}.$$

Auch hier gelingt es unschwer, noch eine spezielle S-Basis zweiter Art zu konstruieren. Zunächst genügt nämlich $\bar{l}(u) = 1 - u^2 + u^4$ den Anforderungen des Satzes 6 a; denn $\bar{l}(u) \equiv l(u) \pmod 2$ und $\bar{l}(u)$ ist für alle Wurzeln von $u^5 - 1 = 0$ eine Einheit, weil

$$(1 - u^2 + u^4)(u^2 - u^3 + u^4) = 1 + (1 - u^2 + u^3)(u^5 - 1)$$

ist. Weiter wird nach (40 a)

$$\bar{s}^*(u) \equiv (1 - u + u^2)(1 + u^3 - u^4)(1 + u - u^3) \pmod{u^5 - 1} = u^2 - u^3 + u^4;$$

und hieraus findet man $\bar{s}(u)$ nach (43 a), da $\bar{l}(u) \cdot \bar{s}^*(u) \equiv 1 \pmod{u^5 + 1}$, in der besonders einfachen Gestalt $\bar{s}(u) = 11\,\bar{s}^*(u)$, woraus dann nach (46 a) sich ergibt $\bar{t}(u) \equiv (2 - u) \cdot s^*(u) \pmod{u^5 - 1}$. Mithin wird:

$$\text{(78 b)} \quad \bar{l}(u) = 1 - u^2 + u^4, \quad \bar{s}(u) = 11u^2 - 11u^3 + 11u^4, \quad \bar{t}(u) = -1 + 2u^2 - 3u^3 + 3u^4.$$

---

[1]) Siehe Anm. 2) S. 37.

(78 a) $\lambda(u) = 1 - u^7 + u^9$, $\sigma(u) = 2 + u + 6u^2 - 8u^3 + 7u^4 - 2u^5 - u^6 + 5u^7 - 3u^8 + 4u^9$, $\tau(u) = u^2 - 2u^3 + 2u^4 - u^5 + u^7 - u^8 + u^9$.

(54; 4) $v_0 = \frac{k_0 k_9}{k_7}$, $v_1 = \frac{k_1 k_0}{k_8}$, $v_2 = \frac{k_2 k_1}{k_9}$, $v^3 = \frac{k_3 k_2}{k_0}$, ..., $v_9 = \frac{k_9 k_8}{k_6}$.

5. $\boldsymbol{p = 23}$, $n = 11$, $g = 5$; (34; 5) $f(u) = u^{10} - u^9 + \cdot - \cdot \cdot \cdot - u + 1$, $F(u) = u + 1$; Satz 7.

Wir entnehmen den Tafeln von *Reuschle*, nach Division durch u und Änderung des Vorzeichens [1]) von u die Form

$$L^*(u) = 1 - u^3 - u^5.$$

[Die bei *Kummer* angegebene Form $1 - u - u^9$ ist offenbar nichts anderes als $L^*(u^{15})$, also hiervon nicht wesentlich verschieden.] Durch geeignete Zusammenfassung der konjugierten Faktoren berechnet man ohne große Mühe entsprechend Formel (40)

$$S^*(u) = 14 - 4u - 3u^2 + u^3 + 5u^4 + 8u^6 - 9u^7 + 12u^8 + 2u^9 + 2u^{10}.$$

$L^*(-1) = 3$; (52; 5) $4 \cdot 3 - 1 \cdot 11 = 1$, also $\pi = 2$, $\varrho = -1$; mithin nach (53) und (47) $L(u) = [(1 - u + u^2 - u^3) L^*(u) - f(u)] u^8$, wobei der Faktor u^8 zur Vereinfachung hinzugefügt ist. Wir finden

$$L(u) = 1 + u^2 - u^3 - u^6 + u^7; \quad L(-1) = 1. \tag{79}$$

Statt nun $S(u)$ aus $S^*(u)$ nach (43) zu bestimmen, können wir auch $S^*(u)$ so behandeln, wie das soeben nach (47) mit $L^*(u)$ geschah, also

$$S(u) = G_1'(u) S^*(u) + G_2'(u) f(u) \tag{80}$$

setzen, und dabei $G_1'(u)$, $G_2'(u)$ so wählen, daß *einmal* $S(-1) = 23$ wird, und daß *ferner* das Produkt aus $G_1'(u)$ und dem soeben bei $L^*(u)$ benutzten Multiplikator $G_1(u) = 1 - u + u^2 - u^3$ nach dem Modul $f(u)$ kongruent 1 wird. Nun ist $S^*(-1) = 48$; $3 \cdot 48 - 11 \cdot 11 = 23$. Man erkennt daher leicht, daß $G_1'(u) = 1 + u^4 + u^8$ den gestellten Anforderungen genügt, setzt zur Vereinfachung der Rechnung gemäß (80)

$$S(u) = (1 + u^4 + u^8) [S^*(u) - 4 f(u)] + f(u)$$

und erhält

$$S(u) = 20 + 9u - 4u^2 - 11u^3 + 10u^4 + 16u^5 - 2u^6 - 17u^7 + 5u^8 + 8u^9 - u^{10}. \tag{81}$$

Nun ist $\boldsymbol{L(15)} \equiv 0 \pmod{23}$; da $15^{13} \equiv 5 \pmod{23}$ und $13 \cdot 17 \equiv 1 \pmod{22}$, so wird [2]) $l(u) \equiv L(u^{17})$ und $s(u) \equiv S(u^{17}) \pmod{u^{11} + 1}$, während zuletzt $t(u)$

---

[1]) Siehe Anm. 1) S. 37.

[2]) Siehe Anm. 2) S. 37.

wieder gemäß (46) bestimmt wird. Man erhält

$$(82)\quad \begin{cases} l(u) = 1 - u + u^3 - u^7 + u^9 \\ s(u) = 20 + 4u + 10u^2 + 2u^3 + 5u^4 + u^5 - 9u^6 - 11u^7 - 16u^8 \\ \qquad\qquad - 17u^9 - 8u^{10} \\ t(u) = 4 + 2u^2 + u^4 - 2u^6 - 2u^7 - 3u^8 - 3u^9 - u^{10}. \end{cases}$$

Da die Berechnung dieser Funktionen hier zum größten Teile unterdrückt ist, fügen wir ein einfaches Kontrollschema an Hand der Formeln (29, 30) bei, indem wir nur die Koeffizienten der Potenzen von u hinschreiben, diese selbst aber weglassen und natürlich bei der Multiplikation sofort mod $(u^{11} + 1)$ reduzieren. Dann wird

	0	1	2	3	4	5	6	7	8	9	10
$s(u) \cdot l(u) =$	20,	4,	10,	2,	5,	1,	− 9,	−11,	−16,	−17,	− 8
	− 8,	−20,	− 4,	−10,	− 2,	−5,	− 1,	9,	11,	16,	17
	16,	17,	8,	20,	4,	10,	2,	5,	1,	−9,	−11
	5,	1,	− 9,	−11,	−16,	−17,	− 8,	−20,	− 4,	−10,	− 2
	−10,	− 2,	− 5,	− 1,	9,	11,	16,	17,	8,	20,	4
	23,	0,	0,	0,	0,	0,	0,	0,	0,	0,	0
$t(u) \cdot l(u) =$	4,	0,	2,	0,	1,	0,	− 2,	− 2,	− 3,	− 3,	− 1
	− 1,	− 4,	0,	− 2,	0,	− 1,	0,	2,	2,	3,	3
	3,	3,	1,	4,	0,	2,	0,	1,	0,	− 2,	− 2
	1,	0,	− 2,	− 2,	− 3,	− 3,	− 1,	− 4,	0,	− 2,	0
	− 2,	0,	− 1,	0,	2,	2,	3,	3,	1,	4,	0
	5,	− 1,	0,	0,	0,	0,	0,	0,	0,	0,	0

Aus diesen Kontrollen ergibt sich ohne jede Berücksichtigung der Herleitung von $l(u)$, daß die aus $l(u)$ (82, 1) leicht zu bildenden 11 Funktionen ψ_j (26) eine spezielle S-Basis erster Art bilden.

Mit der Aufstellung dieser Formeln für die Zahlen $p = 11, 23$ sind die metazyklischen Minimalbasen dieser Grade implizite vollständig bekannt und also auch die Darstellbarkeit der Koeffizienten der auflösbaren Gleichungen dieser Grade, getrennt nach *Galois*schen Gruppen, gleich wie in den Fällen $p = 5, 7$ nachgewiesen, da hier nach Satz 2 eine sukzessive Reduktion auf gleichfalls bekannte Minimalbasen stattfindet.

Für die Primzahl $p = 47$, die sich an 5, 11, 23 anschließen würde, ist bereits bei *Kummer* a. a. O. gezeigt, daß sie sich nicht in der Form (48) darstellen läßt. Hier existiert also keine spezielle S-Basis.

An die Zahlen 3, 5 schließt sich nun als nächste *Fermat*sche Primzahl an die Zahl

6. $\boldsymbol{p = 17}$, $n = 8$, $g = 3$; (34; 6) $f(u) = u^8 + 1$; Satz 7.

Wir finden bei *Reuschle*

$$L^*(u) = 1 + u + u^5,$$

also $L^*(\mathbf{10}) \equiv 0 \pmod{17}$; da nun $10^{11} \equiv 3 \pmod{17}$ und $3 \cdot 11 \equiv 1 \pmod{16}$, so wird [1]) $l^*(u) \equiv L^*(u^3) \pmod{u^8 + 1}$, und da hier $l(u) = l^*(u)$, so wird $l(u) = 1 + u^3 - u^7$. Ferner wird hier $s(u) = s^*(u)$ sehr leicht, durch geeignete Zusammenfassung konjugierter Faktoren, nach (40), und schließlich $t(u)$ wie immer nach (46) gefunden. Es wird

$$(83)\quad \begin{cases} l(u) = 1 + u^3 - u^7 \\ s(u) = 1 + 6u + 2u^2 - 5u^3 + 4u^4 - 10u^5 + 8u^6 - 3u^7 \\ t(u) = u - u^3 + u^4 - 2u^5 + 2u^6 - u^7, \end{cases}$$

womit die spezielle S-Basis erster Art (26) auch für diesen Fall bekannt ist.

7. $\boldsymbol{p = 13}$, $n = 6$, $g = 2$; (34; 7) $f(u) = u^4 - u^2 + 1$, $F(u) = u^2 + 1$.

Wir finden bei *Reuschle*

$$L^*(u) = 1 - 2u - u^5.$$

Da hier $L^*(i) = 1 - 3i$, $f(i) = 3$, setzen wir gemäß (47)
$L(u) = 1 \cdot L^*(u) + u \cdot f(u) = 1 - u - u^3$, so daß $L(i) = 1$. Da ferner hier $L(\mathbf{6}) \equiv 0 \pmod{13}$, $6^5 \equiv 2 \pmod{13}$, $5 \cdot 5 \equiv 1 \pmod{12}$, so wird [1]) $l(u) \equiv L(u^5) \pmod{u^6 + 1}$ gefunden und sodann $s^*(u)$, $s(u)$, $t(u)$ wie in den früheren Fällen. Es wird

$$(84)\quad l(u) = 1 - u^3 - u^5, \quad s(u) = 6 + 3u - 5u^2 + 4u^3 + 2u^4 + u^5, \quad t(u) = 1 - u^2 + u^3.$$

Wir erwähnen noch, daß sich hier sehr leicht der Nachweis erbringen läßt, daß eine Funktion $\bar{l}(u)$ gemäß Satz 6a und somit eine spezielle S-Basis zweiter Art *nicht* existiert. Zum Schluß behandeln wir den Fall

8. $\boldsymbol{p = 19}$, $n = 9$, $g = 2$; (34; 8) $f(u) = u^6 - u^3 + 1$,
$F(u) = u^3 + 1 = (u + 1)(u^2 - u + 1)$.

Wir finden bei *Reuschle* nach Änderung des Vorzeichens von u [2])

$$L^*(u) = 1 - u - u^2.$$

Es wird $L^*(-1) = 1$, $L^*(\delta) = -2\delta^2$ für $\delta \neq -1$. Man findet leicht, daß $G_1(u) = -(1 + u^2)$ für die Wurzeln γ von $f(u) = 0$ eine Einheit ist wegen

$$(1 + u^2)(u - u^6 + u^8) = 1 + (u^4 + u - 1)(u^6 - u^3 + 1),$$

und setzt in Anlehnung an (47)

$$L(u) = [-(1 + u)^2 L^*(u) + f(u)]u^{-1} = 1 + u^3 + u^5,$$

was für *alle* Wurzeln von $F(u) = 0$ eine Einheit ist. Nun ist noch $L(\mathbf{14}) \equiv 0 \pmod{19}$, aber $14^{13} \equiv 2 \pmod{19}$ und $13 \cdot 7 \equiv 1 \pmod{18}$, also [1]) wird $l(u) \equiv L(u^7) \pmod{u^9 + 1}$, woraus dann $s^*(u)$, $s(u)$, $t(u)$ in der bis-

[1]) Siehe Anm. 2) S. 37.
[2]) Siehe Anm. 1) S. 37.

herigen Weise leicht bestimmt werden. Man erhält

$$(85)\quad \begin{cases} l(u) = 1 + u^3 - u^8 \\ s(u) = 8 + 4u + 2u^2 + u^3 - 9u^4 + 5u^5 - 7u^6 + 6u^7 + 3u^8 \\ t(u) = 1 - u^4 + u^5 - u^6 + u^7 . \end{cases}$$

In den drei zuletzt behandelten Fällen ist, im Gegensatz zu den vorhergehenden, durch Angabe der Formeln für die $l(u)$, nur eine *Reduktion* des Basisproblems im Sinne des Satzes 2, noch nicht aber dessen vollständige Lösung erreicht, da die zyklischen Minimalbasen 16-ten, 12-ten und 18-ten bzw. 9-ten Grades noch nicht bekannt sind.