Gedruckt mit Unterstützung aus dem Jerome und Margaret Stonborough-Fonds

Über
Minimalbasen für Körper rationaler Funktionen

Von

Ph. Furtwängler in Wien

(k. M. d. Akad. d. Wiss.)

(Vorgelegt in der Sitzung am 7. Mai 1925)

Bedeutet $\mathfrak{G}$ eine Permutationsgruppe in n Variabeln, so bilden alle rationalen rationalzahligen Funktionen, die bei den Permutationen von $\mathfrak{G}$ ungeändert bleiben, einen (Lagrange'schen) Funktionenkörper. Lagrange hat über diese Körper zuerst bewiesen, daß man ihre Funktionen als rationale rationalzahlige Funktionen von $n+1$ Körperfunktionen darstellen kann, von denen n als die elementarsymmetrischen Funktionen der n Variabeln gewählt werden können. Diese $n+1$ Funktionen sind natürlich algebraisch abhängig. Kommt man bereits mit n (algebraisch unabhängigen) Funktionen aus, so wird das System dieser Funktionen nach E. Nöther als eine Minimalbasis für den betrachteten Funktionenkörper bezeichnet. Die Frage nach der Existenz einer solchen Minimalbasis ist bisher nur in wenigen Fällen beantwortet.

Die folgenden Untersuchungen geben einen Beitrag zur Lösung dieser Frage, aus dem unter anderem hervorgeht, daß für die rationalen rationalzahligen Funktionenkörper, die zu den transitiven auflösbaren Gruppen der Grade 3, 5, 7, 11 gehören, Minimalbasen existieren, die zum Teil explizit angegeben werden.

Die folgenden Untersuchungen sind bereits vor mehr als zwei Jahren ausgeführt, aber bisher nicht publiziert. Inzwischen hat auch Herr S. Breuer mit Unterstützung von Frl E. Nöther sich mit der Frage der Existenz von Minimalbasen für metazyklische Gruppen beschäftigt.[1] Soweit man aus den bisherigen Publikationen entnehmen kann, ist der von den genannten eingeschlagene Weg gerade entgegengesetzt dem hier gewählten. Während dort der Weg von der vollmetazyklischen Gruppe zur zyklischen genommen wird, gehe ich den umgekehrten Weg. Eine allgemeine Lösung des Problems ist bisher noch nicht erreicht.

§ 1.

Es sei p eine ungerade Primzahl und die aus den Potenzen der zyklischen Permutation $(x_0 x_1 \ldots x_{p-1}) = S_p$ gebildete Gruppe sei $\mathfrak{Z}_p$. Der Körper, der aus allen gegenüber $\mathfrak{Z}_p$ invarianten rationalen

[1] Zur Bestimmung der metazyklischen Minimalbasis von Primzahlgrad, Math. Ann., *92* (1924), p. 126.

Funktionen mit Koeffizienten aus R (1) besteht, heiße k_p. Es handelt sich dann um die Frage, ob für diesen Körper eine Minimalbasis existiert. Wir führen die Lagrange'schen Resolventen ein:

$$\xi_i = x_0 + \zeta^i x_1 + \zeta^{2i} x_2 + \ldots + \zeta^{(p-1)i} x_{p-1},$$

indem wir mit ζ eine primitive p^{te} Einheitswurzel bezeichnen, so daß $\xi_i = \xi_{i+mp}$ ist.

Es sei ferner g eine Primitivwurzel für p. Wir verwenden nun ξ_0 als eine Basisfunktion und setzen weiter:

$$\eta_i = \xi_i^{e_0}\, \xi_{gi}^{e_1} \ldots \xi_{g^{p-2}i}^{e_{p-2}} \quad (i = 1, 2, \ldots p-1), \tag{1}$$

wobei die Exponenten die Bedingung

$$\sum_{k=0}^{p-2} g^k e_k \equiv 0\,(p) \tag{2}$$

befriedigen sollen. Wenn (2) erfüllt ist, sind die Funktionen η_i gegenüber $\mathfrak{Z}_p$ invariant, da

$$S\xi_i = \zeta^{-i}\xi_i$$

ist; sie besitzen aber Koeffizienten aus $R(\zeta)$. Gelingt es nun, die Exponenten e_i so zu bestimmen, daß die Funktionen $\xi_0, \eta_1, \eta_2, \ldots \eta_{p-1}$ eine Minimalbasis für den zu $\mathfrak{Z}_p$ gehörigen Funktionenkörper mit $R(\zeta)$ als Koeffizientenbereich bilden, so kann man auch eine Minimalbasis für k_p finden. Denn setzt man

$$\eta_1 = g_1(x)\zeta + g_2(x)\zeta^2 + \ldots + g_{p-1}(x)\zeta^{p-1},$$

wo die $g_i(x)$ rationale, rationalzahlige Funktionen der x bedeuten, so gehören diese zu k_p und bilden zusammen mit ξ_0 eine Minimalbasis für k_p. Denn die Funktionen η_i gehen aus η_1 einfach durch zyklische Vertauschung der $g_i(x)$ hervor; es sind also alle η_i als ganze lineare Funktionen der $g_i(x)$ mit Koeffizienten aus $R(\zeta)$ darstellbar.

Damit die Funktionen $\xi_0, \eta_i\,(i = 1, 2, \ldots p-1)$ eine Minimalbasis bilden, ist notwendig und hinreichend, daß alle Ausdrücke:

$$A = \xi_1^{f_0}\, \xi_g^{f_1} \ldots \xi_{g^{p-2}}^{f_{p-2}} \tag{3}$$

in denen die Exponenten die Kongruenz

$$\sum_{k=0}^{p-2} g^k f_k \equiv 0\,(p) \tag{2'}$$

befriedigen, rational durch sie darstellbar sind. Daß diese Bedingung notwendig ist, ist evident; daß sie auch hinreicht, folgt daraus, daß alle ganzen Funktionen der $\xi_i\,(i=1,2,\ldots p-1)$, die gegenüber $\mathfrak{Z}_p$ invariant sind, aus Termen A mit konstanten Multiplikatoren zusammengesetzt sind.

Um die Darstellbarkeit aller Funktionen (3) festzustellen, genügt es, diese Darstellbarkeit für die folgenden speziellen $p-1$ Funktionen:[1]

$$\xi_1^{-g^i}\xi_{g^i}\quad (i=1,2,\ldots p-2),\ \xi_1^p \tag{4}$$

nachzuweisen, da die Gleichung besteht:

$$\xi_1^{f_0}\xi_g^{f_1}\ldots\xi_{g^{p-2}}^{f_{p-2}}=(\xi_1^{-g}\xi_g)^{f_1}\ldots(\xi_1^{-g^{p-2}}\xi_{g^{p-2}})^{f_{p-2}}\,\xi_1^{f_0+gf_1+\cdots+g^{p-2}f_{p-2}},$$

wobei der Exponent von ξ_1 zufolge (2') durch p teilbar ist.

Es sollen also jetzt Bedingungen für die Exponenten e_i gefunden werden, damit die Funktionen (4) rational durch ξ_0, η_i darstellbar sind. Wir setzen:

$$\begin{vmatrix} e_0 & e_1 & \ldots & e_{p-2} \\ e_{p-2} & e_0 & \ldots & e_{p-3} \\ & & & \\ e_1 & e_2 & \ldots & e_0 \end{vmatrix}=\triangle$$

Es muß dann selbstverständlich $\triangle\neq 0$ sein, weil andernfalls die Funktionen η_i algebraisch abhängig wären. Man kann dann durch Auflösung der Gleichungen (1) nach den ξ_i diese als Potenzprodukte der η_i mit im allgemeinen gebrochenen Exponenten darstellen. Daraus kann man schließen, daß ein Ausdruck A aus (3), der nicht als Potenzprodukt der y_i mit ganzen Exponenten darstellbar ist, überhaupt nicht rational durch die η_i darstellbar ist, weil andernfalls sich eine nicht identische Gleichung zwischen den η_i ergeben würde, was ihrer algebraischen Unabhängigkeit widerspricht. Soll also A rational durch die η_i darstellbar sein, so müssen $p-1$ ganze Zahlen $z_0, z_1,\ldots z_{p-2}$ existieren, so daß

$$\xi_1^{f_0}\xi_g^{f_1}\ldots\xi_{g^{p-2}}^{f_{p-2}}=\eta_1^{z_0}\eta_g^{z_1}\ldots\eta_{g^{p-2}}^{z_{p-2}}\quad(\eta_k=\eta_{k+mp}).$$

Führt man hier für die η_i ihre Werte aus (1) ein, so erkennt man, daß die Exponenten z_i die Gleichungen befriedigen müssen:

$$\left.\begin{array}{l} e_0\ \ z_0+e_{p-2}z_1+\ldots+e_1z_{p-2}=f_0 \\ e_1\ \ z_0+e_0\ \ z_1+\ldots+e_2z_{p-2}=f_1 \\ \\ e_{p-2}z_0+e_{p-3}z_1+\ldots+e_0z_{p-2}=f_{p-2} \end{array}\right\} \tag{5}$$

[1] Diese $p-1$ Funktionen bilden zusammen mit ξ_0 eine Minimalbasis, wenn als Koeffizientenbereich der Körper der p^{ten} Einheitswurzeln genommen wird. Daß in diesem Falle für jedes p eine Minimalbasis existiert, ist ein spezieller Fall eines allgemeinen Satzes von E. Fischer; vgl. Math. Ann., 77 (1916), p. 81.

Gemäß (4) sind die Exponenten e_i so zu wählen, daß die Gleichungen (5) für

$$f_0 = -g^i, f_i = 1, f_j = 0 \quad (i, j, i \neq j) = 1, 2, \ldots p-2 \tag{6}$$

und für

$$f_0 = p, f_1 = f_2 = \ldots = f_{p-2} = 0 \tag{7}$$

ganzzahlige Lösungen z_i haben. Ich bezeichne die Lösungen für die Konstantensysteme (6) mit $z_0^{(i)}, z_1^{(i)}, \ldots z_{p-2}^{(i)}$ $(i = 1, 2, \ldots p-2)$ und für (7) mit $\bar{z}_0, \bar{z}_1, \ldots \bar{z}_{p-2}$.

Bezeichnet man die algebraischen Minoren der Elemente der Determinante $\triangle$ mit E_i, so erhält man

$$z_0^{(i)} = \frac{-g^i E_0 + E_i}{\triangle}, \quad z_1^{(i)} = \frac{-g^i E_{p-2} + E_{i-1}}{\triangle}, \ldots$$

$$z_{p-2}^{(i)} = \frac{-g^i E_1 + E_{i+1}}{\triangle}. \tag{8}$$

$$\bar{z}_0 = \frac{p E_0}{\triangle}, \quad \bar{z}_1 = \frac{p E_{p-2}}{\triangle}, \ldots \quad \bar{z}_{p-2} = \frac{p E_1}{\triangle}. \tag{9}$$

Es ergibt sich zunächst, daß $\triangle$ durch p teilbar sein muß. Denn multipliziert man die Spalten von $\triangle$ der Reihe nach mit $1, g, g^2, \ldots g^{p-2}$ und addiert zur ersten Spalte, so erscheinen in dieser zufolge (2) lauter durch p teilbare Zahlen. Ich behaupte, daß $\triangle = \pm p$ sein muß. Es möge $\triangle$ genau durch q^r teilbar sein, wo q eine von p verschiedene Primzahl ist. Es ist dann die adjungierte Determinante $\overline{\triangle}$ genau durch $q^{r(p-2)}$ teilbar. Andrerseits folgt aus (9), daß $E_i \equiv 0 \, (q^r)$ und daher $\overline{\triangle} \equiv 0 \, (q^{r(p-1)})$ ist, was für $r > 0$ zu einem Widerspruch führt. Es muß also $\triangle$ eine Potenz von p sein. Wäre $\triangle$ durch p^2 teilbar, so würden nach (9) die Kongruenzen $E_i \equiv 0 \, (p)$ folgen. Es hätte daher die durch die Determinante $\triangle$ bestimmte Matrix mod. p höchstens den Rang $p-3$. Es müßten sich also zwei Zeilen, etwa die i^{te} und die k^{te} $(k > i)$, mod. p als lineare Kombination der übrigen darstellen lassen. Wählt man nun in (5): $f_{i-1} = -g^{k-i}$, $f_{k-i} = 1$ und alle übrigen f gleich Null, so ist die Kongruenz $\sum g^i f_i \equiv 0 \, (p)$ erfüllt und das System (5) hätte für diese Werte f keine Lösung.

Die Matrix $(\triangle)$ hat also mod. p den Rang $p-2$, es können nicht alle E_i durch p teilbar sein und es muß $\triangle = \pm p$ sein.

Es soll jetzt nachgewiesen werden, daß die Bedingungen:

$$\triangle = \pm p, \sum_{i=0}^{p=2} e_i g^i \equiv 0 \, (p) \tag{10}$$

für die Exponenten e_i hinreichend sind. Zunächst werden die $\bar{z}_i$ ganze Zahlen, und zwar $\bar{z}_i = \pm E_{p-1-i}$ $(E_{p-1} = E_0)$. Ferner folgt aus bekannten Determinantensätzen:

$$\left.\begin{array}{l} e_0\ \ E_0 + e_1 E_1 + \ldots + e_{p-2} E_{p-2} = \pm p \\ e_1\ \ E_0 + e_2 E_1 + \ldots + e_0\ \ E_{p-2} = 0 \\ \\ e_{p-2} E_0 + e_0 E_1 + \ldots + e_{p-3} E_{p-2} = 0 \end{array}\right\} \tag{11}$$

Dementsprechend müssen auch die Kongruenzen gelten:

$$\left.\begin{array}{l} e_0\ \ E_0 + e_1 E_1 + \ldots + e_{p-2} E_{p-2} \equiv 0\ (p) \\ e_1\ \ E_0 + e_2 E_1 + \quad + e_0 E_{p-2} \equiv 0\ (p) \\ \\ e_{p-2} E_0 + e_0 E_1 + \ldots + e_{p-3} E_{p-2} \equiv 0\ (p) \end{array}\right\} \tag{11'}$$

Faßt man diese als Bestimmungskongruenzen für die Unbekannten E_i auf, so müssen sich die Verhältnisse der E_i aus ihnen eindeutig mod. p bestimmen lassen, da die Matrix $(\triangle)$ mod. p den Rang $p-2$ hat. Setzt man aber

$$E_0 : E_1 \ldots : E_{p-2} \equiv 1 : g : \ldots : g^{p-2}\ (p),$$

so sind zufolge der zweiten Gleichung (10) die Kongruenzen (11′) erfüllt. Es wird daher allgemein:

$$E_i \equiv g^{i-k} E_k\ (p),$$

woraus sich die Ganzzahligkeit der Exponenten $z_i^{(j)}$ gemäß (8) ergibt.

§ 2.

Wir geben einige numerische Resultate.

I. $p = 3$.[1]

$$g = -1;\ e_0 = 2,\ e_1 = -1. \tag{12}$$

$$\triangle = \begin{vmatrix} 2 & -1 \\ -1 & 2 \end{vmatrix} = 3 \quad \sum_{i=0}^{1} e_i g^i = 2 + 1 \equiv 0\ (3)$$

$$\eta_1 = \xi_1^2 \xi_{-1}^{-1},\ \eta_{-1} = \xi_{-1}^2 \xi_1^{-1}. \tag{13}$$

Daß ξ_0, η_1, η_{-1} eine Minimalbasis für den zu $\mathfrak{Z}_3$ gehörigen Funktionenkörper bilden, folgt aus den Formeln:

$$\xi_1^{-2} \xi_{-1} = \eta_1^{-1},\ \xi_1^3 = \eta_1^2 \eta_{-1}.$$

[1] Für diesen Fall ist eine Minimalbasis bereits von F. Seidelmann Dissertation, Erlangen, 1916, angegeben.

Setzt man:

$$\eta_1 = g_1 \zeta_3 + g_{-1} \zeta_3^{-1},$$

so wird:

$$g_1 = \frac{[3\, x_0^2 x_1 - x_0^3] - 6\, x_0 x_1 x_2}{[x_0^2 - x_0 x_1]}, \quad g_{-1} = \frac{[3\, x_0 x_1^2 - x_0^3] - 6\, x_0 x_1 x_2}{[x_0^2 - x_0 x_1]}, \tag{14}$$

wobei [ ] zyklische Summierung bezeichnet, also z. B.:

$$[x_0^2 x_1] = x_0^2 x_1 + x_1^2 x_2 + x_2^2 x_0.$$

Die drei Funktionen $\xi_0 = [x_0]$, g_1, g_{-1} bilden dann eine Minimalbasis für k_3. Zur Bestätigung geben wir die Formeln:

$$\left.\begin{aligned} [x_0 x_1] &= \frac{\xi_0^2 - g_1^2 - g_{-1}^2 + g_1 g_{-1}}{3} \\ x_0 x_1 x_2 &= \frac{\xi_0^3 - g_1^3 - g_{-1}^3 - 3\, \xi_0\, (g_1^2 + g_{-1}^2 - g_1 g_{-1})}{27} \end{aligned}\right\} \tag{15}$$

II. $p = 5$.

$$g = 2,\ e_0 = 1,\ e_1 = 1,\ e_2 = 0,\ e_3 = -1. \tag{16}$$

$$\begin{vmatrix} 1 & 1 & 0 & -1 \\ -1 & 1 & 1 & 0 \\ 0 & -1 & 1 & 1 \\ 1 & 0 & -1 & 1 \end{vmatrix} = 5, \quad \sum_{i=0}^{3} e_i g^i = 1 + 2 - 2^3 \equiv 0\ (5).$$

$$\eta_i = \frac{\xi_i \xi_{2i}}{\xi_{-2i}} \quad (i = \pm 1, \pm 2). \tag{17}$$

Um zu zeigen, daß die Funktionen ξ_0, $\eta_i\ (i = \pm 1, \pm 2)$ eine Minimalbasis für den zu $\mathfrak{Z}_5$ gehörigen Funktionenkörper bilden, seien folgende Formeln angeführt:

$$\begin{aligned} &\xi_1^2 \xi_2^{-1} = \eta_1 \eta_2^{-1} \eta_{-1} \\ &\xi_1^{-2} \xi_{-2}^{-1} = \eta_1^{-1} \eta_{-1}^{-1} \eta_{-2}^{-1}, \quad \xi_1^5 = \eta_1^3 \eta_2^{-1} \eta_{-1}^2 \eta_{-2}. \\ &\xi_1^{-1} \xi_{-1}^{-1} = \eta_1^{-1} \eta_{-1}^{-1} \end{aligned} \tag{18}$$

Um eine Minimalbasis für k_5 zu bestimmen, setze ich:

$$\frac{1}{\eta_1} = \frac{\xi_{-1}}{\xi_1 \xi_2} = \frac{\xi_{-1}^2 \xi_{-2}}{\xi_1 \xi_2 \xi_{-1} \xi_{-2}} = g_1(x) \zeta_5 + g_2(x) \zeta_5^2 + g_3(x) \zeta_5^3 + g_4(x) \zeta_5^4.$$

Setzt man dann:

$$\begin{aligned} \xi_1 \xi_2 \xi_{-1} \xi_{-2} = N = [x_0^4 - x_0 x_1 x_2 x_3 - 5\, x_0^2 x_1 x_4 - 5\, x_0^2 x_2 x_3] \,+& \\ + \sum (x_0^2 x_1^2 - x_0^3 x_1 + 2\, x_0^2 x_1 x_2),& \end{aligned} \tag{19}$$

wo [ ] wie früher zyklische Summierung bedeutet, während Σ zur Abkürzung für symmetrische Funktionen steht, so kommt:

$$g_i = \frac{[x_0^2 x_{4i} + 2\, x_0^2 x_{2i} - 2\, x_0 x_{2i} x_{3i} - x_0^3]}{N}, \; (i = 1, 2, 3, 4) \;\; (x_i = x_{i+5m}), \tag{20}$$

Die Funktionen $\xi_0 = [x_0]$, g_1, g_2, g_3, g_4 bilden dann eine Minimalbasis für k_5.

III. $p = 7$.

$$g = 3,\; e_0 = 1,\; e_1 = 1,\; e_2 = e_3 = e_5 = 0,\; e_4 = -1. \tag{21}$$

$$\begin{vmatrix} 1 & 1 & 0 & 0 & -1 & 0 \\ 0 & 1 & 1 & 0 & 0 & -1 \\ -1 & 0 & 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 1 & 1 & 0 \\ 0 & 0 & -1 & 0 & 1 & 1 \\ 1 & 0 & 0 & -1 & 0 & 1 \end{vmatrix} = -7, \quad \sum_{i=0}^{5} e_i g^i = 1 + 3 - 3^4 \equiv 0\,(7).$$

$$\eta_i = \frac{\xi_i \xi_{3i}}{\xi_{-3i}} \quad (i = \pm 1, \pm 2, \pm 3). \tag{22}$$

Um zu zeigen, daß die Funktionen ξ_0, η_i eine Minimalbasis für den zu $\mathfrak{Z}_7$ gehörigen Funktionenkörper bilden, genügen folgende Formeln:

$$\begin{aligned} \xi_2\, \xi_1^{-2} &= \eta_1^{-1} \eta_{-1}^{-1} \eta_2 & \xi_{-2}\, \xi_1^2 &= \eta_1 \eta_{-1} \eta_{-2} \\ \xi_3\, \xi_1^{-3} &= \eta_1^{-1} \eta_{-1}^{-2} \eta_2 \eta_{-2}^{-1} \eta_{-3} & \xi_{-1}\, \xi_1 &= \eta_1 \eta_{-1} \\ \xi_{-3}\, \xi_1^3 &= \eta_1 \eta_{-1}^2 \eta_{-2} \eta_3 & \xi_1^7 &= \eta_1^3 \eta_{-1}^4 \eta_2^{-2} \eta_{-2}^2 \eta_3 \eta_3^{-1}. \end{aligned} \tag{23}$$

Die Berechnung der Funktionen g_i, die eine Minimalbasis für k_7 bilden, bietet keine Schwierigkeit.

IV. $p = 11$.

$$g = 2,\; e_0 = e_1 = 1,\; e_8 = -1, \text{ alle übrigen } e_i \text{ Null.}$$

$$\sum_{i=0}^{9} e_i g^i = 1 + 2 - 2^8 \equiv 0\,(11).$$

Für die Determinante $\triangle$ ergibt sich der Wert:

$$-N(1 + \zeta_5 + \zeta_5^{-2}) \cdot N(1 - \zeta_5 - \zeta_5^{-2}) = -11,$$

wo ζ_5 eine primitive 5^{te} Einheitswurzel bedeutet.

Die Funktionen η_i haben die Werte:

$$\eta_i = \frac{\xi_i \xi_{2i}}{\xi_{3i}} \quad (i = \pm 1, \pm 2, \ldots \pm 5). \tag{24}$$

§ 3.

Hat man eine Minimalbasis für den zur zyklischen Gruppe $\mathfrak{Z}_p$ gehörigen Funktionenkörper k_p in der hier angegebenen Gestalt gefunden, so gelingt es unter gewissen Voraussetzungen, daraus eine Minimalbasis für die zu den übrigen metazyklischen Gruppen des Grades p gehörigen Funktionenkörper abzuleiten. Es soll dies zunächst für $p = 5$ ausgeführt werden. In diesem Falle treten außer $\mathfrak{Z}_5$, die durch $S = (01234)$ erzeugt wird, noch zwei metazyklische Gruppen $\mathfrak{G}_{10}$ und $\mathfrak{G}_{20}$ auf, bei denen zu S als zweite Erzeugende $t^2 = (14)(23)$, respektive $t = (1243)$ hinzutritt. Die in (20) angegebenen Basisfunktionen g_i erleiden bei Anwendung von t^2, respektive t einfach die durch die Indexvertauschungen angegebenen Vertauschungen. Um daher für die $\mathfrak{G}_{10}$ eine Minimalbasis zu finden, hat man einfach $\begin{Bmatrix} g_1 & g_4 \\ g_2 & g_3 \end{Bmatrix}$ als zwei Variabelnreihen aufzufassen und für die symmetrischen Funktionen der beiden Reihen eine Minimalbasis anzugeben, was bei den symmetrischen Funktionen beliebig vieler Variabelnreihen bekanntlich stets möglich ist. Man erhält in unserem Falle als Minimalbasis für den zur $\mathfrak{G}_{10}$ gehörigen Funktionenkörper mit Koeffizienten aus $R(1)$:

$$[x_0], g_1 + g_4, g_2 + g_3, g_1 g_4, g_1 g_2 + g_3 g_4, \tag{25}$$

wo die g_i aus (20) zu entnehmen sind.

Um das Problem für die $\mathfrak{G}_{20}$ zu lösen, braucht man eine rationalzahlige Minimalbasis für $\mathfrak{Z}_4$. Eine solche ist bekannt,[1] soll aber der Einheitlichkeit wegen nach der hier angewandten Methode kurz hergeleitet werden. Wir setzen:

$$\left.\begin{aligned} x_0 + x_1 + x_2 + x_3 &= \xi_0 \\ x_0 + i x_1 - x_2 - i x_3 &= \xi_1 \\ x_0 - x_1 + x_2 - x_3 &= \xi_2 \\ x_0 - i x_1 - x_2 + i x_3 &= \xi_{-1} \end{aligned}\right\} \tag{26}$$

und nehmen als Erzeugende der $\mathfrak{Z}_4$: (0123).

Setzt man dann:

$$\xi_1^2 \xi_2^{-1} = \eta_1, \; \xi_{-1}^2 \xi_2^{-1} = \eta_{-1}, \; \xi_1 \xi_{-1} = \eta_2, \tag{27}$$

[1] Vgl. die zitierte Dissertation von F. Seidelmann.

so bilden $\xi_0, \eta_1, \eta_{-1}, \eta_2$ eine Minimalbasis mit Koeffizienten aus $R(i)$, wie aus der Formel:

$$\xi_1^4 = \eta_1 \eta_1^{-1} \eta_2^2$$

folgt. Schreibt man noch: $\eta_1 = \vartheta_1 + \vartheta_3 i$, $\eta_{-1} = \vartheta_1 - \vartheta_3 i$, so erhält man als Minimalbasis mit Koeffizienten aus R (1):

$$[x_0], \eta_2 = (x_0 - x_2)^2 + (x_1 - x_3)^2, \vartheta_1 = \frac{(x_0 - x_2)^2 - (x_1 - x_3)^2}{x_0 - x_1 + x_2 - x_3},$$

$$\vartheta_3 = \frac{2\,(x_0 - x_2)\,(x_1 - x_3)}{x_0 - x_1 + x_2 - x_3}. \tag{28}$$

In unserem Falle tritt an Stelle von $x_i | g_{2i}$, wobei die Indizes von g mod. 5 zu nehmen sind, so daß sich als Minimalbasis für den zur $\mathfrak{G}_{20}$ gehörigen Funktionenkörper mit Koeffizienten aus R (1) ergibt:

$$[x_0], g_1 + g_2 + g_3 + g_4, (g_1 - g_4)^2 + (g_2 - g_3)^2, \frac{(g_1 - g_4)^2 - (g_2 - g_3)^2}{g_1 - g_2 + g_4 - g_3},$$

$$\frac{(g_1 - g_4)\,(g_2 - g_3)}{g_1 - g_2 + g_4 - g_3}, \tag{29}$$

wobei die Werte der g_i wieder aus (20) zu entnehmen sind.

Auf Grund der durchgeführten Entwicklungen ist es möglich, das Problem, alle rationalzahligen metazyklischen Gleichungen fünften Grades mit vorgeschriebener Gruppe anzugeben, in abschließender Weise zu behandeln. Ich werde bei anderer Gelegenheit darauf näher eingehen.

§ 4.

Analoge Entwicklungen wie für den Grad 5 lassen sich auch für die Grade 7 und 11 durchführen, so daß man für alle metazyklischen Gruppen dieser Grade rationalzahlige Minimalbasen angeben kann. Um dies einzusehen, sind noch zwei allgemeine Sätze abzuleiten.

Satz. *Kennt man eine rationalzahlige Minimalbasis für die zyklische Gruppe m^{ten} Grades $\mathfrak{Z}_m$, wo m eine beliebige ungerade Zahl bedeutet, so läßt sich auch eine rationalzahlige Minimalbasis für die zyklische Gruppe $2\,m^{ten}$ Grades $\mathfrak{Z}_{2m}$ angeben.*[1]

Beweis: Eine erzeugende Permutation der $\mathfrak{Z}_{2m}$ sei

$$P = (x_0 x_1 \ldots x_{m-1} y_0 y_1 \ldots y_{m-1}).$$

---

[1] Vgl. hierzu S. Breuer, Zyklische Gleichungen sechsten Grades und Minimalbasis, Math. Ann., *86* (1921), p. 108.

Wir setzen dann

$$x_i+y_i = z_i,\ x_i-y_i = (-1)^i u_i,\ (i = 0, 1, \ldots m-1),$$

so daß

$$Pz_i = z_{i+1},\ Pu_i = -u_{i+1}\ (z_{i+m} = z_i,\ u_{i+m} = u_i)$$

$$P^m z_i = z_i,\quad P^m u_i = -u_i$$

gilt. Wir führen ferner ein:

$$z_0^i u_0+z_1^i u_1+\ldots z_{m-1}^i u_{m-1} = v_i\ (i = 0, 1, \ldots m-1).$$

Es gilt dann $Pv_i = -v_i$ und es lassen sich die u_i als rationale rationalzahlige Funktionen der v_i und z_i darstellen. Ist nun $F(x,y)$ eine zur Gruppe $\mathfrak{Z}_{2m}$ gehörige rationale rationalzahlige Funktion der x_i, y_i, so kann man sie zunächst als ebensolche Funktion der z_i, v_i darstellen. Es genügt also, die Darstellbarkeit der zur Gruppe gehörigen rationalzahligen ganzen Funktionen $G(z,v)$ zu prüfen. Die Funktionen müssen natürlich auch bei der Permutation P^m ungeändert bleiben. Ist $c\, v_0^{e_0} v_1^{e_1} \ldots v_{m-1}^{e_{m-1}}$ ein Glied einer solchen Funktion, wobei c eine Funktion der z_i bedeutet, so folgt durch Anwendung von P^m, daß $e_0+e_1+\ldots e_{m-1} \equiv 0\ (2)$ sein muß. Setzt man

$$v_0^2 = w_0,\ v_0 v_1 = w_1, \ldots v_0 v_{m-1} = w_{m-1},$$

so wird:

$$v_0^{e_0} v_1^{e_1} \ldots v_{m-1}^{e_{m-1}} = w_0^{f_0} w_1^{e_1} \ldots w_{m-1}^{e_{m-1}},$$

wo

$$f_0 = \frac{e_0-e_1-e_2 \ldots -e_{m-1}}{2}$$

ist.

Es läßt sich also $G(z, v)$ als rationale rationalzahlige Funktion $R(z, w)$ darstellen. Da $Pw_i = w_i$, $Pz_i = z_{i+1}$, bilden offenbar die Funktionen

$$f_1(z), \ldots f_m(z),\ w_0, w_1, \ldots w_{m-1}$$

eine gesuchte Minimalbasis, wenn die Funktionen $f_i(z)$ eine Minimalbasis für den Körper der rationalen rationalzahligen Funktionen der z_i bilden, die bei der Permutation $(z_0 z_1 \ldots z_{m-1})$ ungeändert bleiben.

Eine zweite Verallgemeinerung unserer Entwicklungen läßt sich in folgender Weise durchführen. Es sei eine Permutationsgruppe $\mathfrak{G}_x = \{P_x^{(i)}\}$ in n Veränderlichen $x_1, x_2, \ldots x_n$ gegeben. Fügt man dann eine beliebige Anzahl von weiteren Reihen von n Veränderlichen $y_i, z_i \ldots$ hinzu (wir nehmen der Einfachheit halber zwei), so bilden auch die Permutationen $\{P_x^{(i)}.P_y^{(i)}.P_z^{(i)}\}$ eine Gruppe $\mathfrak{G}_{xyz}$, wenn $P_y^{(i)}$ und $P_z^{(i)}$ diejenigen Permutationen bedeuten, die aus $P_x^{(i)}$ durch die Vertauschungen (x_i, y_i), respektive (x_i, z_i) hervorgehen. Kennt man dann eine rationalzahlige Minimalbasis für $\mathfrak{G}_x$, so kann man eine solche auch für $\mathfrak{G}_{xyz}$ angeben. Ist nämlich $f_i(x)$ $(i = 0, 1, . . n—1)$ eine rationalzahlige Minimalbasis für $\mathfrak{G}_x$ und setzt man:

$$\left.\begin{aligned} x_1^i y_1 + x_2^i y_2 + . \;\; . + x_n^i y_n &= g_i(x, y) \\ x_1^i z_1 + x_2^i z_i + \ldots + x_n^i z_n &= h_i(x, z), \end{aligned}\right\} (i = 0, 1 \ldots n-1) \qquad (30)$$

so bilden die $3n$ Funktionen f_i, g_i, h_i eine rationalzahlige Minimalbasis für $\mathfrak{G}_{xyz}$. Denn mit Hilfe von (30) kann man jede rationale rationalzahlige Funktion $R(x, y, z)$ in eine ebensolche Funktion $R_1(x, g, h)$ der x_i, g_i, h_i überführen. Da die g_i und h_i bei $\mathfrak{G}_{xyz}$ ungeändert bleiben und die x_i dieselben Vertauschungen wie bei $\mathfrak{G}_x$ erfahren, folgt daraus die Richtigkeit unserer Behauptung.

Auf Grund der ergänzenden Entwicklungen dieses Paragraphen ist es möglich, für alle transitiven auflösbaren Gruppen der Grade 7 und 11 Minimalbasen hinzuschreiben.

Zum Schluß sei noch erwähnt, daß man nicht für alle Primzahlen p die Gleichungen (10) befriedigen kann. Eine notwendige (aber nicht hinreichende) Bedingung dafür ist die Zerlegbarkeit von p in ein Produkt von Hauptidealen im Körper der $(p-1)^{\text{ten}}$ Einbeitswurzeln, wie man erkennt, wenn man in bekannter Weise die Determinante $\triangle$ in der Gestalt:

$$\triangle = \prod_{i=0}^{p-2} (e_0 + e_1 \zeta_{p-1}^i + . \;\; . + e_{p-2} \zeta_{p-1}^{i(p-2)}) = \pm p$$

darstellt, wo ζ_{p-1} eine primitive $(p-1)^{\text{te}}$ Einheitswurzel bedeutet. p zerfällt in $k(\zeta_{p-1})$ in ein Produkt von $\varphi(p-1)$ Primidealen, von denen eines gleich $(p, g-\zeta_{p-1}) = \mathfrak{p}_1$ ist. Wegen der zweiten Bedingung (10) ist dann

$$e_0 + e_1 \zeta_{p-1} + . \;\; . e_{p-2} \zeta_{p-1}^{p-2} \equiv 0 \; (\mathfrak{p}_1)$$

und daher

$$p = \prod_{i=1}^{p-2} (e_0 + e_1 \zeta_{p-1}^i + \ldots + e_{p-2} \zeta_{p-1}^{i(p-2)}), \;\; (i, p-1) = 1.$$

Es muß also p in $k(\zeta_{p-1})$ in ein Produkt von Hauptidealen zerfallen und eins von ihnen muß derart in die Gestalt:

$$e_0 + e_1 \zeta_{p-1} + \ldots e_{p-2} \zeta_{p-1}^{p-2}$$

gesetzt werden können, daß alle Zahlen

$$e_0 + e_1 \zeta_{p-1}^{j} + \ldots e_{p-2} \zeta_{p-1}^{j(p-2)},$$

wo j nicht zu $p-1$ relativ prim ist, algebraische Einheiten sind.

Nach den Tafeln von Reuschle zerfällt 47 im Körper der 23ten Einheitswurzeln nicht in ein Produkt von Hauptidealen und daher ist die Konstruktion einer rationalzahligen Minimalbasis auf dem hier eingeschlagenen Weg für $p = 47$ sicher unmöglich. Da aber die angegebene Zerlegbarkeit von p, die für alle Primzahlen kleiner als 47 vorhanden ist, nicht genügt, kann unsere Konstruktion auch bereits für kleinere Primzahlen als 47 versagen.