Since $6 \equiv -2$, $7 \equiv -1$, $23 \equiv -1 \pmod 8$, by lemma 7, we have a non-decomposable form for $n = 6,7$ [11]), and 23. For $n = 9, 10, 11, 13, 17, 19$, we have that by lemma 3 the forms

$$\begin{pmatrix} 15 & 2_{(i)} \\ & 4 \quad 1_{(i)} \end{pmatrix} \quad (i+1 = 9, 10, 11, 13);$$

$$\begin{pmatrix} 24 & 2_{(i)} \\ & 5 \quad 1_{(i)} \end{pmatrix} \quad (i+1 = 17, 19)$$

are non-decomposable.

In closing, we should like to thank Prof. Mordell for suggesting shorter proofs of lemmas 2, 3 and for his kind help with the manuscript.

(Received 28 March, 1938.)

[11]) These are the same forms given by Prof. Mordell. See footnote [8]).

Zur Verallgemeinerung des Galoisschen Kriteriums der algebraischen Auflösbarkeit.

Von
S. Lubelski (Warszawa).

Das berühmte Galoissche Kriterium [1]) der algebraischen Auflösbarkeit eines Polynoms kann gruppentheoretisch folgendermassen formuliert werden: „Eine Permutationsgruppe $\mathfrak{G}$ vom Primzahlgrad p kann dann und nur dann auflösbar sein, wenn $\mathfrak{G} = \mathfrak{A}\,\mathfrak{P}$ ist, wo $\mathfrak{A}$ und $\mathfrak{P}$ zyklisch sind, dabei ist $\mathfrak{P}$ bzw. $\mathfrak{A}$ von der Ordnung p. bzw. d, $d/p - 1$". Wir wollen in dieser Arbeit vor allem zeigen, dass dieses Kriterium eigentlich die Folgerung eines allgemeinen Permutationssatzes ist:

Ist p prim, so ist der Normalisator einer p-Sylowgruppe $\mathfrak{P}$ der symmetrischen Gruppe $\mathfrak{S}$ von p Elementen, Produkt zweier zyklischer Gruppen $\mathfrak{A}$ und $\mathfrak{P}$, wo $\mathfrak{A}$ die Ordnung $p-1$ und $\mathfrak{P}$ die Ordnung p hat (s. Satz 1).

Das Hauptziel dieser Arbeit ist aber den Galoisschen Satz auch auf solche Polynome, deren Grad nicht prim ist, zu erweitern und zu verallgemeinern. Zu diesem Behufe betrachten wir zunächst verallgemeinerte auflösbare Permutationsgruppen vom Grade p^n, die einen Abelschen Normalteiler von demselben Grade p^n haben. Für derartige Gruppen beweisen wir den nachstehenden Satz.

Voraussetzung: *p ist prim und t eine natürliche Zahl, $\mathfrak{G}$ ist eine Permutationsgruppe vom Grade p^t, die einen transitiven Abelschen Normalteiler $\mathfrak{A}$ enthält*".

Behauptung: *$\mathfrak{G}$ enthält nur solche Permutationen, die höchstens eine Ziffer unverändert lassen, oder es finden sich solche Permutationen $S \neq E$ in $\mathfrak{G}$,*

[1]) E. Galois. Oeuvres, S. 48. (herausgegeben von Liouville im 11. Bande des Journal de mathem. pures et appl. 1846, S. 381 — 444).

E = Einheitspermutation, für die q durch p teilbar ist, wobei q die obere Grenze aller Ziffern ist, die durch eine Permutation S von $\mathfrak{G}$ gleichzeitig unverändert bleiben (s. Satz 2).

In diesem Satze ist hauptsächlich die Voraussetzung von Wichtigkeit, dass $\mathfrak{G}$ einen Abelschen Normalteiler $\mathfrak{A}$ hat. Während Galois [1]), Abel [2]) und Jordan [3]) eine weitgehendere Voraussetzung machten, nämlich dass $\mathfrak{A}$ Abelsch vom Typus $(p, p, \ldots, p)$ ist. Für diese Gruppen gilt sogar der nachstehende, viel schärfere Satz als Satz 2:

Varaussetzung: *$\mathfrak{G}$ ist eine primitive auflösbare Permutationsgruppe vom Grade n. p ist ein Primteiler von n. S und S_1 sind beliebige Permutationen aus $\mathfrak{G}$ und q ist die gemeinsame Anzahl der unveränderten Ziffern von S und S_1.*

Behauptung: *Es ist $q = p^t$, $t \geqslant 0$* (s. Satz 3).

Dieser Satz beleuchtet die Struktur einer primitiven auflösbaren Gruppe, wobei der Einblick in diese Struktur bei kleinen p besonders klar ist.

Unsere Erweiterungen beziehen sich offensichtlich blos auf jene Bedingungen des Galoisschen Kriteriums, die sich als notwendig erweisen. Wir sind aber in der Lage auch eine Verallgemeinerung des Galoisschen Kriteriums anzuführen, bei dem die Bedingungen sowohl notwendig als hinreichend sind. In dieser Richtung kann behauptet werden, dass die Bemühungen von Galois [1]), Abel [4]) und Jordan [3]) keine effektive Ergebnisse gezeitigt haben [5]). Diese, seit mehr als 120 Jahre andauernden, erfolglosen Bemühungen beweisen deutlich, dass man den Ausgangspunkt ändern müsste, um neue Ergebnisse zu erzielen[5]). Es scheint nämlich, dass nicht die Primitivität eines Polynoms, sondern die sogenannte „Regularität" als Ausgangspunkt zur Grundlage der allgemeinen Theorie haranzuziehen wäre, sondern die sogenannte „Regularität", sodass für sogenannte „reguläre" Körper [vgl. die Definition auf S. 130] das Galoissche Kriterium, wie folgt verallgemeinert werden kann:

Voraussetzung: *K ist ein über dem vollkommenen Körper k regulärer Körper vom Grade p^m. K_1 ist ein Unterkörper von K von Grade p^{m-1}. $\mathfrak{G}_i = \mathfrak{A}_i \mathfrak{P}_i (i = 1, 2, \ldots t)$ wo $\mathfrak{P}_i$ bzw. $\mathfrak{A}_i$ eine zyklische Gruppe der Ordnung*

[2]) N. Abel. Oeuvres 2, S. 1—86.

[3]) Dem genannten Problem ist eigentlich sein berühmtes „Traité des substitutions et des équations algebriques, Paris 1870" gewidmet.

[4]) „Tant que le degré de l'équation est un nombre premier, la difficulté n'est pas si grande, mais lors que ce nombre est composé, le diable sy mèle". vgl. S. 265.

[5]) Kronecker hat sogar bemerkt, dass die erhaltenen Ergebnisse nicht nur keinen Fortschritt des genannten Problems gibt, sondern vielmehr dasselbe Problem verdunkelt haben, vgl. L. Kronecker, Werke, B. 5, S. 3—4.

p bzw. $d_i, d_i | p-1$, ist. $\mathfrak{G}$ ist direktes Produkt von $\mathfrak{G}_i, i = 1, 2, 3, \ldots p^{m-1}$, und $\mathfrak{H}$ die Galoissche Gruppe von K. Schliesslich bezeichnet $\overline{\mathfrak{H}}$ die Gruppe, zu der K_1 innerhalb des kleinsten Normalkörpers von K gehört, und $\mathfrak{H}''$ einen Normalteiler von $\mathfrak{H}$, der zu einer gewissen Untergruppe von $\mathfrak{G}$ isomorph ist.

Behauptung: *Damit K algebraisch auflösbar sei, ist es notwendig und hinreichend, dass die Gruppe $\overline{\mathfrak{H}}$ zu einer gewissen Faktorgruppe $\mathfrak{H}/\mathfrak{H}''$ isomorph sei* (s. Satz 4) [6]).

Zunächst wollen wir zeigen, dass der wohlbekannte Galoissche Satz über die algebraische Auflösbarkeit von primzahlgradigen Polynomen seinen Kern in der Theorie der Permutationsgruppen findet. Dazu benötigen wir die folgenden Hilfssätze:

Hilfssatz 1 [7]). *Enthält die endliche Gruppe $\mathfrak{G}$ eine transitive Untergruppe $\mathfrak{G}'$, die ihrerseits sämtliche Permutationen von $\mathfrak{G}$ enthält, welche alle Ziffern verändern, so stimmt $\mathfrak{G}$ mit $\mathfrak{G}'$ auch in denjenigen Permutationen überein, die mindestens zwei Ziffern unverändert lassen.*

Beweis. I. Es bezeichne $\mathfrak{G}_i$ die grösste Untergruppe von $\mathfrak{G}$, deren Permutationen eine Ziffer x_i unverändert lassen. Enthält eine Permutation P genau j unveränderte Ziffern, so befindet sich diese Permutation in genau j Untergruppen $\mathfrak{G}_i$. Um also die Summe $\Sigma\psi(S_i)$ zu berechnen, wo $\psi(X)$ die genaue Anzahl der Ziffern bezeichnet, die in der Permutation X unverändert bleiben, und S_i sämtliche verschiedenen Permutationen einer transitiven Permutationsgruppe $\mathfrak{G}$ durchläuft, genügt es die Ordnungen von $\mathfrak{G}_i$ zu summieren. Da $h = h_i n$ ist, wo h die Ordnung von $\mathfrak{G}$, h_i jene von $\mathfrak{G}_i$ und n den Grad von $\mathfrak{G}$ bezeichnet, so erhält man

$$\Sigma\psi(S_i) = h. \tag{1}$$

II. Demnach ist

$$\Sigma\psi(S_i) - \Sigma\psi(P_j) = h - h',$$

wobei S_i bzw. P_j sämtliche Permutationen von $\mathfrak{G}$ bzw. $\mathfrak{G}'$ durchläuft und h' die Ordnung von $\mathfrak{G}'$ ist. Der Komplex $\mathfrak{M}$, der sämtliche Elemente von $\mathfrak{G}$ enthält, die nicht zu $\mathfrak{G}'$ gehören, ist von der Ordnung $h - h'$, wobei nach Voraussetzung alle seine Permutationen mindestens eine Ziffer unverändert lassen. Enthält $\mathfrak{M}$ mindestens eine Permutation, die zwei Ziffern unverändert lässt, so müsste

[6]) Einige Hauptergebnisse dieser Arbeit sind in der Mitteilung des Verf. enthalten, die dem intern. Math. Kongress in Oslo (1936) vorgelegt wurde. vgl. Bd. 2, S. 17.

[7]) C. Jordan. Journal de math. (2), 17, 1872, S. 351. Unser Beweis verläuft aber viel einfacher.

$$\Sigma\psi(S_i) > \Sigma\psi(P_j) + h - h'$$

sein, was (1) widerspricht.

Hilfssatz 2. *Die Anzahl der verschiedenen Gruppen der Ordnung p, p-prim, in der symmetrischen Gruppe $\mathfrak{S}$ von p Veränderlichen ist gleich $(p-2)!$.*

Beweis. Die Anzahl der Untergruppen p-ter Ordnung in der symmetrischen Gruppe $\mathfrak{S}$ erhält man folgendermassen: Permutieren wir die Elemente eines eingliedrigen Zyklus $Z = (a_1, a_2, \ldots, a_p)$ untereinander, so bekommen wir $p!$ eingliedrige Zyklen, die sich in Mengen von p Elementen verteilen, wobei die Permutationen einer Menge vom Standpunkt der Permutationstheorie gleich sind. Die Anzahl der verschiedenen Zyklen unter diesen ist also $(p-1)!$. Die Potenzen Z^m, $m < p$, bilden ebenfalls eingliedrige Zyklen, und mithin ist die Anzahl der p-Sylowgruppen in $\mathfrak{S}$ gleich $(p-2)!$.

Anmerkung. Aus diesem Satze ergibt sich ohne Schwierigkeit, dass der Wilsonsche Satz eine unmittelbare Folgerung des zweiten Sylowschen Satzes ist.

Jetzt haben wir die Möglichkeit den Beweis der Verallgemeinerung des Galoisschen Satzes zu geben.

Satz 1. *Ist p prim, so ist der Normalisator einer p-Sylowgruppe $\mathfrak{P}$ der symmetrischen Gruppe $\mathfrak{S}$ von p Elementen, Produkt zweier zyklischer Gruppen $\mathfrak{P}$ und $\mathfrak{N}$, wo $\mathfrak{P}$ die Ordnung p, $\mathfrak{N}$ die Ordnung $p-1$ hat.*

Beweis. Ist $\mathfrak{N}$ Normalisator einer p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{S}$, so ist $\mathfrak{P}$ Normalteiler von $\mathfrak{N}$. Nach den Sylowsätzen sind je zwei p-Sylowgruppen konjugiert Mithin kann $\mathfrak{N}$ nicht zwei verschiedene p-Sylowgruppen enthalten. Nach Hilfssatz 1 ist also in $\mathfrak{N}$ die Einheitspermutation die einzige, die mindestens zwei verschiedene Ziffern verändert. Demnach ist $\mathfrak{N} = \mathfrak{E}_1\mathfrak{P}$, wo $\mathfrak{E}_1$ die grösste Untergruppe bezeichnet, die eine bestimmte Ziffer unverändert lässt. Nach den Sylowsätzen (vgl. z. B. A. Speiser [8]) ist die Anzahl der verschiedenen Sylowgruppen dem Index des Normalisators einer beliebigen unter diesen Gruppen gleich. Mithin beträgt nach Hilfssatz 2 die Ordnung von $\mathfrak{N}$ $p(p-1)$. d. h. die Ordnung von $\mathfrak{P}$ bzw. von $\mathfrak{E}_1$ beträgt p bzw. $p-1$. Weisen wir nach, dass es eine Permutationsgruppe von p Veränderlichen gibt, deren Ordnung $p(p-1)$ beträgt und die Produkt zweier

[8]) A. Speiser: Theorie der Gruppen von endlicher Ordnung. Berlin, 1927 (zweite Auflage). S. 67.

zyklischer Gruppen ist, so würde nach den Sylowsätzen unser Satz bewiesen sein. Dazu betrachten wir sämtliche Permutationen

$$\begin{pmatrix} 0, & 1, & 2, & \ldots, & k, & \ldots, & p-1 \\ b, & a+b, & 2a+b, & \ldots & ka+b, & \ldots, & (p-1)a+b \end{pmatrix} = \begin{pmatrix} x \\ ax+b \end{pmatrix},$$

wobei x die Zahlen 1, 2, ..., $p-1$, und b bzw. a ein System von Resten bzw. relativ primen Resten mod p durchläuft. Offenbar bilden diese Permutationen eine endliche Gruppe $\mathfrak{N}_1$ der Ordnung $p(p-1)$, wobei die Permutationen $\begin{pmatrix} x \\ x+b \end{pmatrix}$ einen Normalteiler $\mathfrak{P}_1$ von $\mathfrak{N}_1$ bilden (dies ergibt sich unmittelbar durch Berechnung oder aus den Sylowsätzen). Bezeichnet $\mathfrak{E}_1$ die Untergruppe von $\mathfrak{N}_1$ für die $b = 0$ ist, so ist $\mathfrak{N}_1 = \mathfrak{P}\mathfrak{E}_1$. Es bleibt also zu beweisen, dass $\mathfrak{E}_1$ zyklisch ist. Dazu bemerken wir, dass

$$\begin{pmatrix} x \\ gx \end{pmatrix}^t = \begin{pmatrix} x \\ g^t x \end{pmatrix},$$

wo t eine beliebige natürliche Zahl bezeichnet. Ist also g eine primitive Wurzel von p, so ist $\begin{pmatrix} x \\ gx \end{pmatrix}$ der Ordnung $p-1$, womit der Satz bewiesen ist.

Aus diesem Satze erhält man in unmittelbarer Weise das Galoissche Kriterium.

Folgerung. *Damit ein irreduzibles Polynom vom Primzahlgrad p aus einem vollkommenen Körper K, algebraisch auflösbar sei, ist es notwendig und hinreichend, dass die Permutationen der Galoisschen Gruppe $\mathfrak{G}$ von $f(x)$ höchstens eine Ziffer unverändert lassen.*

Beweis. Die Gruppe $\mathfrak{G}$ ist vom Grade p und mithin ist sie Untergruppe der symmetrischen Gruppe $\mathfrak{S}$ vom p Elementen. Ist $f(x)$ algebraisch auflösbar, so enthält $\mathfrak{G}$ einen Abelschen Normalteiler $\mathfrak{P}$ von Ordnung p (vgl. [4]) Livre 4). $\mathfrak{G}$ muss also zu einem Normalisator $\mathfrak{N}$ von $\mathfrak{P}$ gehören. Mithin sind die Bedingungen des Satzes notwendig. Nun sind sie auch hinreichend. Die p-Sylowgruppe $\mathfrak{P}$ von $\mathfrak{G}$ ist nämlich nach Formel (1) von Ordnung p. $\mathfrak{P}$ ist also Normalteiler von $\mathfrak{G}$ und mithin muss $\mathfrak{G}$ Untergruppe des Normalisators $\mathfrak{N}$ von $\mathfrak{P}$ in Bezug auf die symmetrische Gruppe von p Veränderlichen sein. Nach Satz 1 ist also alles bewiesen.

Wir gehen jetzt zur Frage der Verallgemeinerung des Galoisschen Satzes auf Polynome von zusammengesetztem Grade über. Zunächst werden wir gewisse verallgemeinerte primitive Gruppen betrachten, nämlich solche, deren Abelsche Normalteiler transitiv ist. Im Falle. wenn der Grad Potenz einer Primzahl ist, gilt für solche Gruppen der folgende Satz:

Satz 2. Voraussetzung: *p ist prim und t eine natürliche Zahl. $\mathfrak{G}$ ist*

eine Permutationsgruppe vom Grade p^t, die einen transitiven Abelschen Normalteiler $\mathfrak{A}$ enthält.

Behauptung: *$\mathfrak{G}$ enthält nur solche Permutationen, die höchstens eine Ziffer unverändert lassen, oder es finden sich solche Permutationen $S \neq E$ in $\mathfrak{G}$, E = Einheitspermutation, für die q durch p teilbar ist, wobei q die obere Grenze aller Ziffern ist, die durch eine Permutation S von $\mathfrak{G}$ gleichzeitig unverändert bleiben.*

Beweis. Es bezeichne q die obere Schranke aller Maximalzahlen von unveränderten Ziffern einer Permutation von $\mathfrak{G}$, (vgl. die Behauptung des Satzes). Mit $\mathfrak{I}$ bezeichnen wir eine Untergruppe von $\mathfrak{G}$, deren Permutationen q Ziffern unverändert lassen. Es ist klar, dass wir $q \geq 2$ annehmen können. Nach dem ersten Sylowschen Satze enthält $\mathfrak{I}$ eine Untergruppe $\mathfrak{H}$ vom Primzahlgrad π. Wir wollen zunächst beweisen, dass die mehrgliedrigen Zyklen ohne gemeinsame Ziffern einer Permutation aus $\mathfrak{H}$, dieselbe Gliederzahl haben. Ist nämlich S eine Permutation aus $\mathfrak{H}$ und ist $S = C_1 C_2 \ldots C_g$ die Darstellung von S durch Zyklen ohne gemeinsame Ziffern, und bezeichnet a_i die Ordnung von C_i, $i = 1, 2, \ldots, g$, wobei $a_1 \leqq a_i$ ist, so muss $S^{a_1} = C_1^{a_1} C_2^{a_1} \ldots C_g^{a_1}$ die Einheitspermutation sein, denn andernfalls würde q keine obere Schranke der Maximalzahlen von unveränderten Ziffern der Permutationen aus $\mathfrak{G}$ bezeichnen. Wäre also $\pi = p$, so würde $a_1 = a_2 = \ldots = a_g = p$ sein, und demnach wäre auch q durch p teilbar, d. h. die Behauptung des Satzes ist wahr. Wir können also $\pi \neq p$ annehmen.

Wir betrachten jetzt das Produkt $\mathfrak{A}\mathfrak{H}$. Da eine Abelsche transitive Gruppe bekantlich regulär ist [9]), so ist $\mathfrak{A}$ der Ordnung p^t und es existieren in $\mathfrak{A}$ $p^t - 1$ Permutationen, die alle Ziffern verändern. Nach Hilfssatz 1 existieren also in $\mathfrak{A}\mathfrak{H}$ noch Permutationen, die alle Ziffern verändern. Es sei h die Ordnung einer solchen Permutation P. h ist also Teiler der Ordnung $p^t\pi$ von $\mathfrak{A}\mathfrak{H}$. Ferner sei $P = Z_1 Z_2, \ldots, Z_l$ die Darstellung von P durch Zyklen ohne gemeinsame Ziffern, wobei

$$b_j, \quad j = 1, 2, \ldots, i, \tag{1}$$

die Ordnung von Z_j bezeichnet. Da $\mathfrak{A}\mathfrak{H} = \mathfrak{A}(P^g)$, wo (P^g) sämtliche Potenzen von P enthält, so muss eine der Zahlen (1) gleich π sein. Sonst wäre $\mathfrak{A}(P^g) = \mathfrak{A}$, denn die Ordnung von $\mathfrak{A}(P^g)$ muss Teiler von $p^t\pi$ sein. Die Permutation P enthält also Zyklen der Ordung $p^u\pi^v$, wo $0 \leqq u \leqq t$, $0 \leqq v \leqq 1$. Bezeichnet τ die obere Schranke aller u, so muss $P_1 = P^{p^\tau}$ von der Ordnung π sein, wobei die Anzahl der Ziffern, die P_1 unverändert lässt

[9]) vgl. z. B. H. Weber, Lehrbuch der Algebra I, Braunschweig 1894, S. 537.

durch p teilbar ist. Nach dem zweiten Sylowschen Satze muss die Gruppe $\mathfrak{H}$ mit (P_1^g) konjugiert sein, womit also der Satz bewiesen ist.

Im Beweise des letzten Satzes ist von wesentlicher Bedeutung die Tatsache, dass die Permutationsgruppe $\mathfrak{G}$ einen Abelschen Normalteiler $\mathfrak{A}$ enthält. Über die Gruppe selbst haben wir keine Einschränkungen gemacht. Dagegen machte die Theorie, die durch Galois [1]) Abel [2]) und Jordan [3]) dargestellt wurde, die Voraussetzung, dass $\mathfrak{A}$ Abelsch vom Typus $(p, p, \ldots, p)$ ist, d. h. dass jedes Element von $\mathfrak{A}$ von Ordnung p ist. Nun zeigen wir, dass bei dieser Annahme der letzte Satz in weitgehender Weise verschärft werden kann.

Satz 3. Voraussetzung: *$\mathfrak{E}$ ist eine primitive auflösbare Permutationsgruppe vom Grade $n.p$ ist ein Primteiler von n. S und S_1 sind beliebige Permutationen aus $\mathfrak{E}$. q ist die gemeinsame Anzahl der unveränderten Ziffern von S und S_1.*

Behauptung: *Es ist $q = p^t$, $t > 0$.*

Beweis: Nach einem wohlbekannten Satz (s. z. B [8]). S. 118) ist der Grad einer primitiven auflösbaren Permutationsgruppe Potenz einer Primzahl. Nach Voraussetzung existiert also eine gewisse natürliche Zahl m, sodass $n = p^m$. Ferner kann man nach einem Schmidtschen Satze [10])

$$S = \begin{pmatrix} x_1, \ldots, x_{p^m} \\ f(x_1), \ldots, f(x_{p^m}) \end{pmatrix} = \begin{pmatrix} x \\ f(x) \end{pmatrix}, \quad f(x) = \sum_{j=0}^{m-1} b_j x^{p^j} + b_m,$$

$$S_1 = \begin{pmatrix} x_1, \ldots, x_{p^m} \\ F(x_1), \ldots, F(x_{p^m}) \end{pmatrix} = \begin{pmatrix} x \\ F(x) \end{pmatrix}, \quad F(x) = \sum_{j=0}^{m-1} B_j x^{p^j} + B_m$$

annehmen, wobei x_i, $i = 1, 2, \ldots, p^m$, sämtliche Elemente eines endlichen Körpers k von p^m Elementen durchläuft, und b_j bzw. B_j, $j = 0, 1, \ldots, m$, gewisse konstante Elemente von k bezeichnen. Verändern S und S_1 die Unbestimmte ς nicht und ist $\varsigma \neq 0$, so führt man in sämtlichen Permutationen von $\mathfrak{E}$ die Transformation $(x, x + \varsigma)$ durch. Man kann also $\varsigma = 0$, d. h. $f(0) = F(0) = 0$ annehmen. Wir betrachten jetzt die Polynome $f_1(x) = f(x) - x$ und $F_1(x) = F(x) - x$. Ist η eine andere Unbtstimmte, die $f(x)$ und $F(x)$ zugleich nicht verändern, so folgt aus $f_1(\eta) = F_1(\eta) = 0$, dass zugleich $f_1(l\eta) = F_1(l\eta) = 0$ ist, wenn nur in $l^{p-1} = 1$ ist. Nun hat die letzte Gleichung in k genau $p - 1$ Wurzeln. Also bleiben bei S und S_1 zugleich p Unbestimmte unverändert. Ist ξ eine von 0 und $l\eta$ verschiedene

[10]) O. Schmidt. Auflösbare Gruppen, deren Grad gleich p^2 ist, p-prim. (russisch). Bulletin de l'Uniwersité Kiev, 1913.

Unbestimmte, die auch durch S und S_1 zugleich nicht verändert wird, so erhält man aus den Identitäten

$$f_1(x+y) = f_1(x+y) \quad , \quad F_1(x+y) = F_1(x) + F_1(y)$$

in k, dass S und S_1 zugleich p^2 Unbestimmte nicht verändern. Sind $\eta_1, \eta_2, \ldots, \eta_r$, r Unbestimmte, die durch S und S_1 zugleich nicht verändert werden und für die keine Gleichung der Form

$$\xi = \sum_{l=1}^{r} l_l \eta_l = 0, \quad l_l^p = l_l \ , \ i = 1, 2, \ldots, r,$$

in k besteht, so erhält man, wenn man nur von $l_1 = l_2 = \ldots = l_r = 0$ absieht, dass $f_1(\xi) = F_1(\xi) = 0$, wo $\xi = \Sigma l_l \eta_l$. Ist

$$\xi_1 = \Sigma l_l^{(1)} \eta_l \ , \ \xi_2 = \Sigma \ l_l^{(2)} \eta_l$$

und ist mindestens für ein gewisses i $l_i^{(1)} \neq l_i^{(2)}$, so folgt offenbar $\xi_1 \neq \xi_2$. Mithin bleiben bei S und S_1 zugleich p^r Unbestimmte (Ziffern) zugleich unverändert. So fortfahrend erhalten wir also, dass S und S_1 genau p^t Unbestimmte (Ziffern) zugleich unverändert lassen.

Die Sätze 2 und 3 verschärfen nur die Notwendigkeitsbedingungen. Um die volle Varallgemeinerung des Galoisschen Satzes zu geben, zeigen wir, dass man einen neuen Ausgangspunkt annehmen muss. Diesen Ausgangspunkt wollen wir folgendermassen entwickeln:

Definition. Ein Körper K vom Grade p^m, p-prim, heisse regulär: 1° Im Falle $m = 1$ stets, 2° Für beliebiges m dann, wenn K einen regulären Unterkörper K vom Grade p^{m-1} enthält.

Satz 4. Voraussetzung: *K ist ein über dem vollkommenen Körper k regulärer Körper vom Grade p^m. K_1 ist Unterkörper von K vom Grade p^{m-1}. $\mathfrak{E}_i = \mathfrak{A}_i \mathfrak{P}_i$, wo $\mathfrak{P}_i$, bzw. $\mathfrak{A}_i$ eine zyklische Gruppe von Ordung p bzw. d_i, $d_i | p-1$, ist. $\mathfrak{E}$ ist direktes Produkt von $\mathfrak{E}_i$, $i = 1, 2, \ldots, p^{m-1}$, und $\mathfrak{G}$ die Galoissche Gruppe von K. Schliesslich bezeichet $\bar{\mathfrak{G}}$ die Gruppe zu der K_1 innerhalb des kleinsten Normalkörpers von K gehört, und $\mathfrak{G}''$ ein Normalteiler von $\mathfrak{G}$, der zu einer gewissen Untergruppe von $\mathfrak{E}$ isomorph ist.*

Behauptung: *Damit K algebraisch auflösbar sei, ist es notwendig und hinreichend, dass die gruppe $\bar{\mathfrak{G}}$ einer gewissen Faktorgruppe $\mathfrak{G}/\mathfrak{G}''$ isomorph sei.*

Beweis I. Für $m = 1$ ist der Satz klar. Wir nehmen an, dass der Satz für $m = t$ bewiesen ist und wollen zeigen, dass er auch für $m = t + 1$ wahr ist: Offenbar ist $\mathfrak{G}''$ stets auflösbar. Wäre also $\bar{\mathfrak{G}}$ auflösbar, so würde bekanntlich (vgl. 2. B. [8]) S. 39) auch $\mathfrak{G}$ auflösbar sein. Es genügt also zu zeigen, dass die Bedingungen notwendig sind. Es sei also $F(x)$ bzw. $f(x)$ das algebraisch auflösbare irreduzible Polynom in k, dessen Wurzel x_1 bzw. $\eta(x_1)$ den regulären Körper K bzw. K_1 vom Grade p^m bzw. p^{m-1} bestimmt. Nehmen wir an, dass in K

$$f(x) = f_1(x) f_2(x) \ldots . f_t(x),$$

wo $f_i(x)$ $i = 1, 2, \ldots, t$ in K irreduzibel und vom Grade g_i sind, so ist in K_1, nach dem Bauer-Landsbergschen Satz [11])

$$F(x) = F_1(x) F_2(x) \ldots . F_t(x),$$

wo $F_i(x)$ in K_1 irreduzibel und vom Grade cg_i sind, wo c konstant ist. Da

$$\sum_{i=1}^{t} g_i = p^{m-1}, \quad \sum_{i=1}^{t} c\, g_i = p^m,$$

so muss $c = p$ sein. Ferner erhält man, da für ein gewisses i, $g_i = 1$ ist, dass $F(x)$ in K_1 mindestens einen irreduziblen Faktor vom Grade p enthält.

II. Es sei $\bar{K}$ bzw. K_1 der Wurzelkörper von $F(x)$ bzw. $f(x)$. Ferner sei in K_1

$$F(x) = \Phi_1(x) \Phi_2(x) \ldots . \Phi_h(x),$$

wo $\Phi_j(x)$, $j = 1, 2, \ldots, h$, in $\bar{K}_1$ irreduzibel sind und da $\bar{K}_1$ Galoissch ist, so haben $\Phi_j(x)$, wieder nach dem Bauer-Landsbergschen Satz, denselben Grad g, also ist g/p^m. Da nach 1 $g \leqq p$ sein muss, so ist $g = p$. In $\bar{K}_1$ ist also die Galoissche Gruppe $\mathfrak{G}''$ von $F(x)$ Untergruppe des Systems $\mathfrak{E}$, das durch Verkoppelung besonderer Galoisscher Gruppen von $\Phi_j(x)$, die bekanntlich Produkt zyklischer Gruppen $\mathfrak{P}_i \mathfrak{A}_i$ der Ordnung p und d_i, $d_i/p-1$, sind., entsteht. Nach einem bekannten Satze (vgl. z. B.[9]) § 156, S.511-513) ist die Automorphismengruppe von K_1 der Faktorgruppe $\mathfrak{G}/\mathfrak{G}''$ isomorph. Mithin ist der Satz bewiesen.

(Eingegangen, am 17. Februar 1937.)

[11]) vgl. z. B. M. Bauer. Über einen Takagischen Satz. Journal für Math. B. 163 (1930), S. 249 - 250.