Durch sukzessive Anwendung von Satz 119, (II) unter Berücksichtigung der Minimaleigenschaft des Kompositums (**1**, hinter Def. 5 [21] oder **2**, Satz 116, 2.)) und der Maximaleigenschaft des Durchschnitts (**1**, hinter Def. 5) ergibt sich ferner leicht, daß in jedem Parallelogramm unserer schematischen Figur (mag es eine „Grundmasche" sein oder aus mehreren „Grundmaschen" zusammengesetzt) der Körper links unten der Durchschnitt und der Körper rechts oben das Kompositum der beiden Körper links oben und rechts unten ist. Insbesondere bestehen also neben den rekursiven Darstellungen (3.) auch die alle Zwischenschritte überschlagenden Darstellungen

$$(4.) \qquad \overline{\mathsf{N}}_i = \{\mathsf{N}, \overline{\Lambda}_i\}, \qquad \Lambda_i = [\mathsf{N}, \overline{\Lambda}_i] ,$$

aus denen nach Satz 119, (I) folgt, daß das sukzessive Aufsteigen zu den Grundkörpern der Kette (1.) mit einer sukzessiven Reduktion der Galoisgruppe $\mathfrak{G}$ von N bzgl. K auf die der Kette (2.) nach dem Fundamentalsatz zugeordnete Untergruppenkette

$$(5.) \qquad \mathfrak{G} = \mathfrak{H}_0 \geqq \mathfrak{H}_1 \geqq \mathfrak{H}_2 \geqq \cdots \geqq \mathfrak{H}_r \geqq \mathfrak{E}$$

verbunden ist. Nach (4.) und den Eigenschaften von Kompositum und Durchschnitt ist dann und nur dann, wenn einmal $\Lambda_r = \mathsf{N}$ und damit $\overline{\Lambda}_r = \overline{\mathsf{N}}_r$ ist, d. h. wenn gemäß (5.) die Galoisgruppe $\mathfrak{G}$ auf $\mathfrak{H}_r = \mathfrak{E}$ reduziert ist, $\overline{\Lambda}_r \geqq \mathsf{N}$, d. h. N, wie es als Ziel vorschwebte, durch die Kette (1.) eingefangen.

V. Auflösbarkeit algebraischer Gleichungen durch Wurzelzeichen.

Die in IV entwickelte Theorie verdankt ihre Entstehung und bildet demgemäß die Grundlage für die Behandlung der schon zu Beginn von § 18 erwähnten, berühmten Frage, unter welchen Bedingungen eine algebraische Gleichung durch Wurzelzeichen auflösbar ist. Deren Beantwortung für Grundkörper der Charakteristik 0

ist der vorliegende, letzte Abschnitt gewidmet. Wir präzisieren dazu zunächst die Frage durch die Definition der Auflösbarkeit durch Wurzelzeichen (§ 19), entwickeln sodann als notwendige Hilfsmittel die Theorie der Kreisteilungskörper (§ 20) sowie der reinen und der zyklischen Erweiterungen von Primzahlgrad (§ 21) und leiten darauf durch Anwendung der in IV behandelten Galoisschen Theorie ein gruppentheoretisches Kriterium für die Auflösbarkeit durch Wurzelzeichen her (§ 22). Schließlich skizzieren wir noch den durch die Galoissche Theorie gelieferten Beweis für die auf anderem Wege zuerst von Abel gefundene Nichtauflösbarkeit durch Wurzelzeichen der allgemeinen algebraischen Gleichung höheren als vierten Grades (§ 23).

In § 20 fügen wir einen kurzen Abriß der Theorie der endlichen Körper an und beseitigen dabei insbesondere die in dieser Hinsicht im Beweis von Satz 90 [80] noch gebliebene Unvollständigkeit.

§ 19. Definition der Auflösbarkeit durch Wurzelzeichen.

Wir geben in diesem Paragraphen eine exakte Formulierung dafür, was unter der Ausdrucksweise durch Wurzelzeichen auflösbar zu verstehen ist. Der aus den Elementen geläufige Begriff $\sqrt[n]{a}$, wo a ein Element eines Körpers K und n eine natürliche Zahl ist, wird dort bekanntlich als Lösung der Gleichung $x^n - a = 0$ erklärt. Wegen der hierbei i. a. vorliegenden Mehrdeutigkeit wollen wir die Bezeichnung $\sqrt[n]{a}$ nicht verwenden, operieren vielmehr an Stelle des Wurzelzeichens mit der zugehörigen Gleichung:

Definition 38. Ein **Polynom** der Form $x^n - a$ heißt **rein.**

Damit die zu Eingang dieses Abschnitts gestellte Frage nicht trivial wird, hat man natürlich neben der in ihr genannten Operation

des Wurzelziehens auch die, von diesem Standpunkte aus untergeordneten, vier elementaren Rechenoperationen mit in den Kreis der zulässigen Operationen aufzunehmen[1]). Mit einer Wurzel α eines reinen Polynoms gelten dann also auch alle ihre rationalen Funktionen über dem Grundkörper K, d. h. alle Elemente von $K(\alpha)$ als bekannt. Der Sinn unserer Frage geht aber noch weiter: Es wäre unsystematisch, wenn man der Operation des Wurzelziehens nach einem solchen Schritt Halt gebieten wollte. Vielmehr ist es vernünftig, weiter auch die Wurzeln reiner, dem so erreichten Körper $K(\alpha)$ angehöriger Polynome als bekannt anzusehen usf. Unsere Frage kommt dann also darauf hinaus, unter welchen Bedingungen man die Wurzeln, d. h. den Wurzelkörper eines Polynoms $f(x)$ aus K oder allgemeiner irgendeine Erweiterung Λ von K durch von K ausgehende sukzessive[2]) Adjunktion von Wurzeln reiner Polynome erreichen oder einfangen kann. Hieraus ergibt sich leicht eine Reduktion bezüglich der in Betracht zu ziehenden Wurzelzeichen: Ist nämlich $x^n - a$ ein reines Polynom aus K von zusammengesetztem Grade $n = n_1 n_2$ und α eine seiner Wurzeln, so ist $\alpha^{n_2} = \alpha_1$ eine Wurzel des reinen Polynoms $x^{n_1} - a$ aus K und weiter α eine Wurzel des reinen Polynoms $x^{n_2} - \alpha_1$ aus $K(\alpha_1)$. Somit kann man sich auf die sukzessive Adjunktion von Wurzeln reiner Polynome von Primzahlgrad beschränken. Je nach Geschmack kann nun hierbei noch die Einschränkung hinzugefügt werden, daß diese Polynome in dem jeweils erreichten Körper irreduzibel sein sollen oder nicht. Da die irreduziblen Polynome die einfachsten Bausteine für die Konstruktion algebraischer Erweiterungen sind, erscheint es theoretisch richtiger, diese Beschränkung aufzunehmen[3]). Wir definieren demgemäß:

***Definition 39.** Eine **Erweiterung** Λ von K heißt **rein** über K, wenn sie durch Adjunktion einer Wurzel eines irreduziblen reinen Polynoms aus K herleitbar ist.*

---

[1]) Sonst wären eben nur die reinen Gleichungen durch Wurzelzeichen auflösbar.

[2]) Nicht nur durch simultane. Das besagt hier (anders als bei Satz 62 [52]) mehr, denn α kann sehr wohl Wurzel eines reinen Polynoms aus einer Erweiterung $\bar{K}$ von K sein, ohne doch Wurzel eines reinen Polynoms aus K zu sein.

[3]) Tatsächlich ist die in Satz 127 [144] gegebene Antwort auf unsere Frage (für Grundkörper der Charakteristik 0) von dieser Beschränkung unabhängig, wie sich aus den späteren Sätzen 123, 126 [137. 141] leicht ergibt. Gerade in Hinsicht auf Satz 126 erscheint es mir aber richtiger, die Irreduzibilität zu fordern, da die „gröbere" Fragestellung an der algebraisch interessanten „feineren" Struktur der Kreisteilungskörper ganz vorbeisieht.

***Definition 40.** Eine **Erweiterung** endlichen Grades Λ von K heißt **durch Wurzelzeichen auflösbar** über K, wenn eine Erweiterungskette

$$K = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_r \quad \text{mit} \quad \overline{\Lambda}_r \geqq \Lambda$$

existiert, in der $\overline{\Lambda}_i$ rein und von Primzahlgrad über $\overline{\Lambda}_{i-1}$ ist.

Ein **Polynom** $f(x)$ aus K heißt **durch Wurzelzeichen auflösbar** über K, wenn sein Wurzelkörper über K es ist.

§ 20. Kreisteilungskörper. Endliche Körper.

Um die Frage nach der Auflösbarkeit durch Wurzelzeichen behandeln zu können, haben wir die Theorie des speziellen reinen Polynoms $x^n - e$ vorauszuschicken, dessen Wurzeln im Falle des rationalen Grundkörpers P, wenn man sie gemäß dem sog. Fundamentalsatz der Algebra als komplexe Zahlen darstellt, die Teilung der Peripherie des Einheitskreises in n gleiche Teile leisten. In Hinsicht auf unsere Anwendungen wollen wir uns hier nicht auf diesen Spezialfall P beschränken, sondern allgemeinere Grundkörper K zulassen, nennen aber in Anlehnung an jenen Spezialfall auch allgemein $x^n - e = 0$ die **Kreisteilungsgleichung** und ihren Wurzelkörper T_n den **Kreisteilungskörper** für n über K. Über die Wurzeln der Kreisteilungsgleichung für n über K, die sog. n-ten **Einheitswurzeln** über K, beweisen wir dann zunächst den folgenden Satz:

Satz 120. Es sei K ein Körper, dessen Charakteristik 0 oder eine nicht in n aufgehende Primzahl ist. Dann bilden die n-ten Einheitswurzeln über K bezüglich der Multiplikation eine zyklische Gruppe $\mathfrak{Z}$ der Ordnung n. Es existieren also n verschiedene n-te Einheitswurzeln über K, die sich als die Potenzen

$$\zeta^0 = e, \quad \zeta^1, \ldots, \zeta^{n-1}$$

einer unter ihnen, einer sog. **primitiven n-ten Einheitswurzel** ζ, darstellen lassen.

Beweis: Es seien $\zeta_1, \ldots, \zeta_n$ die Wurzeln von $f_n(x) \equiv x^n - e$. Dann ist die Ableitung

$$f_n'(\zeta_i) = n\,\zeta_i^{n-1} \neq 0 \qquad (i = 1, \ldots, n),$$

weil natürlich $\zeta_i \neq 0$, also nach der Voraussetzung über die Charakteristik von K dann auch $n\zeta_i^{n-1} \neq 0$ ist (Satz 43 [37]). Nach Satz 56 [46] sind also die n Wurzeln ζ_i voneinander verschieden. Da ferner aus $\zeta_i^n = e, \zeta_k^n = e$ folgt $(\zeta_i\zeta_k)^n = e$, bilden die n verschiedenen n-ten Einheitswurzeln eine abelsche Gruppe $\mathfrak{Z}$ der Ordnung n (1, Satz 20 [55] angewandt auf die multiplikative Gruppe der Elemente $\neq 0$ des Kreisteilungskörpers T_n).

Nach Satz 34 [32] hat dann jedes Element ζ_i von $\mathfrak{Z}$ einen bestimmten Teiler m_i von n als Ordnung. Es sei nun ζ ein Element aus $\mathfrak{Z}$ von möglichst hoher Ordnung m. Wir haben zu zeigen, daß $m = n$ ist, woraus ja folgt, daß die n Potenzen $\zeta^0, \zeta^1, \ldots, \zeta^{n-1}$ verschieden sind und somit die Gruppe $\mathfrak{Z}$ erschöpfen. Sei dazu p eine beliebige Primzahl und werde (gemäß Satz 12, 22 [14, 22])

$$m = p^{\mu}\overline{m}, \quad m_i = p^{\mu_i}\overline{m}_i \quad \text{mit} \quad (\overline{m}, p) = 1, \quad (\overline{m}_i, p) = 1$$

gesetzt. Dann haben offenbar $\zeta_i^{\overline{m}_i}, \zeta^{p^{\mu}}$ die Ordnungen $p^{\mu_i}, \overline{m}$, also nach Satz 35 [32] $\zeta_i^{\overline{m}_i}\zeta^{p^{\mu}}$ die Ordnung $p^{\mu_i}\overline{m}$. Wegen der Maximalauswahl von m ist somit $p^{\mu_i}\overline{m} \leqq p^{\mu}m$, d. h. $\mu_i \leqq \mu$. Es enthält also m_i jede Primzahl p höchstens in der Potenz, in der p in m vorkommt, d. h. es ist $m_i \mid m$ (Satz 20 [22]) und somit $\zeta_i^m = e$. Die n verschiedenen n-ten Einheitswurzeln ζ_i sind also sämtlich Wurzeln des Polynoms m-ten Grades $x^m - e$. Daraus folgt $m \geqq n$ (Satz 48 [41]), was mit $m \mid n$ zusammen $m = n$ und damit unsere Behauptung ergibt.

Nach Satz 37 [34] (vgl. auch das zu Satz 31 [30] Ge-

sagte) haben wir noch ohne weiteres:

Zusatz. Ist ζ eine primitive n-te Einheitswurzel über K, so sind alle und nur die Potenzen ζ^m, die den $\varphi(n)$ primen Restklassen m mod. n entsprechen, ebenfalls primitiv.

Hierauf beruht die in folgendem Satz enthaltene Bestimmung der Galoisgruppe des Kreisteilungskörpers T_n:

Satz 121. Ist K ein Körper wie in Satz 120 und ζ eine primitive n-te Einheitswurzel über K, so ist das Polynom

$$g_n(x) \equiv \prod_{\substack{m=0 \\ (m,\,n)=1}}^{n-1} (x - \zeta^m),$$

dessen Wurzeln die $\varphi(n)$ verschiedenen primitiven Einheitswurzeln sind, ein Polynom in K. Ist

$$\bar{g}_n(x) \equiv \prod_{\bar{m}} (x - \zeta^{\bar{m}})$$

der zu ζ gehörige irreduzible (nach Satz 59 [48] separable, nach Satz 99, (III) [88] normale) Faktor von $g_n(x)$, so repräsentieren die $\bar{m}$ eine Untergruppe $\bar{\mathfrak{P}}_n$ der primen Restklassengruppe $\mathfrak{P}_n$ mod. n. Die Galoisgruppe $\mathfrak{G}_n$ des (separablen, normalen) Kreisteilungskörpers T_n ist dann zu dieser Gruppe $\bar{\mathfrak{P}}_n$ isomorph auf Grund der Zuordnung des durch $\zeta \to \zeta^{\bar{m}}$ erzeugten Automorphismus von T_n zu der Restklasse $\bar{m}$ mod. n.

Insbesondere ist also T_n abelsch (Def. 34 [95]) und ferner der Grad von T_n über K ein Teiler von $\varphi(n)$ (Satz 105 [96]).

Beweis: a.) Da nach Satz 107 [98] ein Automorphismus von T_n bzgl. K einerseits die n verschiedenen Wurzeln ζ_i von $x^n - e$ nur untereinander vertauscht, andererseits deren Potenzdarstellungen $\zeta_i = \zeta^{i-1}$ invariant läßt, geht ζ durch ihn wieder in eine primitive n-te Einheitswurzel über, so daß auch

die $\varphi(n)$ verschiedenen primitiven n-ten Einheitswurzeln durch ihn nur untereinander vertauscht werden. Hiernach sind die Koeffizienten von $g_n(x)$ bei allen Automorphismen von T_n bzgl. K invariant und gehören somit zu K (Satz 112, Zusatz [111]).

b.) Da $\mathsf{T}_n = \mathsf{K}(\zeta^0, \ldots, \zeta^{n-1}) = \mathsf{K}(\zeta)$, also eine primitive n-te Einheitswurzel über K gleichzeitig auch primitives Element von T_n bzgl. K ist, können (Satz 105 [96]) die Automorphismen von T_n bzgl. K durch die ihnen entsprechenden Substitutionen von ζ beschriebenw erden. Hat also $\bar{g}_n(x)$ die Bedeutung aus dem Satze, so wird die Galoisgruppe $\mathfrak{G}_n$ von T_n bzgl. K durch die Substitutionen $\zeta \to \zeta^{\overline{m}}$ dargestellt, und ihre Elemente sind hierdurch der Menge $\mathfrak{P}_n$ der durch die $\overline{m}$ repräsentierten primen Restklassen mod. n eineindeutig zugeordnet. Da nun $\zeta \to \zeta^{\overline{m}_1}$ und $\zeta \to \zeta^{\overline{m}_2}$ nacheinander ausgeführt $\zeta \to (\zeta^{\overline{m}_2})^{\overline{m}_1} = \zeta^{\overline{m}_1 \overline{m}_2}$ ergeben, kommt bei dieser Zuordnung die Multiplikation in $\mathfrak{G}_n$ auf die Multiplikation der Restklassen in $\overline{\mathfrak{P}}_n$ hinaus. Daher ist diese Zuordnung isomorph und $\overline{\mathfrak{P}}_n$ eine zu $\mathfrak{G}_n$ isomorphe Untergruppe von $\mathfrak{P}_n$.

Bei der Untersuchung der Auflösbarkeit durch Wurzelzeichen spielen gemäß Def. 40 [129] die Einheitswurzeln von Primzahlordnung $n = p$ eine besondere Rolle. Wir beweisen für diesen Fall in Erweiterung des Satzes 121:

Satz 122. Es sei p eine Primzahl und K ein Körper mit von p verschiedener Charakteristik. Dann ist der Kreisteilungskörper T_p zyklisch über K von einem in $p-1$ aufgehenden Grade.

Beweis: Nach Satz 121 ist der Grad von T_p über K ein Teiler von $\varphi(p)$ und die Galoisgruppe $\mathfrak{G}_p$ von T_p bzgl. K isomorph zu einer Untergruppe $\overline{\mathfrak{P}}_p$ der primen Restklassengruppe $\mathfrak{P}_p$. Nun bilden die Restklassen mod. p nach Satz 28 [27] sogar einen Körper, den Primkörper P_p (Def. 13 [35],

Satz 41 [36]). Die $\varphi(p)$ Elemente von $\mathfrak{P}_p$ sind dann die $p-1$ von Null verschiedenen Elemente von P_p (Satz 17 [20]) und sind als solche Wurzeln der Kreisteilungsgleichung $x^{p-1}-e\doteq 0$ (Satz 29 [29]), also die sämtlichen $(p-1)$-ten Einheitswurzeln über P_p. Nach Satz 120 [129] bilden sie somit bezüglich der Multiplikation eine zyklische Gruppe. Daher ist $\mathfrak{P}_p$, nach Satz 36 [33] also auch die Untergruppe $\overline{\mathfrak{P}}_p$, d. h. $\mathfrak{G}_p$ zyklisch und also T_p zyklisch über K (Def. 34 [95]) von einem in $p-1$ aufgehenden Grade.

Trivialerweise folgt übrigens aus Satz 44 [37]:

Zusatz. Hat K die Charakteristik p, so ist $x^p-e\equiv(x-e)^p$, also e die einzige p-te Einheitswurzel über K, und $\mathsf{T}_p=\mathsf{K}$.

Es ist bemerkenswert, wie die abstrakte Körpertheorie, durch die ohne weitere Schwierigkeiten mögliche Ausdehnung des in der Zahlentheorie gewöhnlich nur für den Grundkörper P bewiesenen Satzes 120 [129] auch auf P_p, auf einfachste Weise zu dem Schluß führt, daß die prime Restklassengruppe $\mathfrak{P}_p$ zyklisch ist, oder, wie man in der Zahlentheorie sagt, daß eine **primitive Wurzel mod. p** existiert, nämlich eine solche ganze Zahl r, daß für jedes zu p prime ganze m eine Potenzdarstellung

$$m\equiv r^{\mu} \bmod. p \quad (\mu=0,\ldots,p-2)$$

besteht.

Wir fügen noch eine Bemerkung über den Spezialfall des Kreisteilungskörpers T_p über dem rationalen Grundkörper P an. Mit zahlentheoretischen Hilfsmitteln (Eisenstein-Schönemannscher Satz, siehe 3, § 20, Aufg. 6) zeigt man, daß das Polynom

$$g_p(x)\equiv\frac{x^p-1}{x-1}\equiv x^{p-1}+x^{p-2}+\cdots+x+1$$

aus Satz 121 in P irreduzibel ist, also T_p den Grad $\varphi(p)=p-1$ über P hat. Ist nun $p-1=2^{\nu}$ $(\nu\geqq 0)$ eine Potenz von 2, so kann nach Satz 109 [101] T_p von P aus durch sukzessive Adjunktion quadratischer Irrationalitäten erreicht werden, weil dann die nach Satz 122 zyklische Galoisgruppe $\mathfrak{G}_p$ von T_p bzgl. P die Ordnung 2^{ν} hat und folglich nach Satz 36 [33] eine Untergruppenkette

$$\mathfrak{G}_p=\mathfrak{H}_0>\mathfrak{H}_1>\cdots>\mathfrak{H}_{\nu}=\mathfrak{E}$$

derart besitzt, daß $\mathfrak{H}_i$ Untergruppe vom Index 2 von $\mathfrak{H}_{i-1}$ ist. Kann umgekehrt T_p von P aus durch sukzessive Adjunktion quadratischer Irrationalitäten erreicht (oder auch nur eingefangen) werden, so enthält die Gruppe $\mathfrak{G}$ nach den Ausführungen in § 17, 2.) [108] und § 18, 3.) [124] eine Untergruppenkette der eben beschriebenen Art[1]), und somit ist dann ihre Ordnung $p-1$ eine Potenz von 2. Daraus ergibt sich das berühmte

Resultat von Gauß. Das reguläre p-Eck für eine Primzahl p ist dann und nur dann mit Zirkel und Lineal konstruierbar, wenn p eine Primzahl von der Form $2^\nu + 1$ ist.

Man weiß bis heute nicht, ob die mit $p = 2, 3, 5, 17, 257, 65537$ beginnende Folge der Primzahlen dieser Form abbricht oder nicht. (Siehe hierzu auch **3**, § 20, Aufg. 14. 15.)

Auf analoge Weise werden wir aus Satz 122 im nächsten Paragraphen als das hauptsächlichste Ziel der Digression dieses Paragraphen die Auflösbarkeit von T_p durch Wurzelzeichen über bestimmten Grundkörpern K folgern.

Auf Grund von Satz 120 [129] kann jetzt mit Leichtigkeit gegeben werden:

Kurzer Abriß der Theorie der endlichen Körper.

A. Wir haben bereits endliche Körper, d. h. solche aus nur endlich vielen Elementen, kennengelernt, nämlich für jede Primzahl p den Primkörper P_p (Restklassenkörper mod. p) aus genau p Elementen (§ 4).

Sei jetzt E ein beliebiger endlicher Körper. Dann ist auch der in E enthaltene Primkörper endlich, also nicht zum rationalen Zahlkörper isomorph. Daher gilt (Satz 41 [36]):

(I) Die Charakteristik von E ist eine Primzahl p.

Nach dem im Anschluß an Satz 41 Gesagten kann dann E als Erweiterung des Primkörpers P_p angesehen werden. Trivialerweise ist dabei E von endlichem Grade über P_p (Def. 25 [57]). Aus der eindeutigen Darstellung $\alpha = a_1\alpha_1 + \cdots + a_m\alpha_m$ der Elemente α aus E durch eine Basis $\alpha_1, \ldots, \alpha_m$ von E bzgl. P_p mit Koeffizienten $a_1, \ldots, a_m$ aus P_p folgt dann:

(II) Ist $[E: P_p] = m$, so hat E genau p^m Elemente.

Wir verallgemeinern jetzt die für den Primkörper P_p selbst im Beweis zu Satz 122 angewandte Schlußweise auf E. Die multiplikative Gruppe der von Null verschiedenen Elemente von E (**1**, § 6, Beisp. 1 [53]) hat nach (II) die Ordnung $p^m - 1$. Diese

[1]) Für den allgemeinen Fall des Einfangens siehe den ausführlichen Beweis zu dem späteren Satz 127, Teil a), Anm. 1 [145].

$p^m - 1$ von Null verschiedenen Elemente genügen daher der Gleichung $x^{p^m-1} - e \doteq 0$ (Satz 34 [32]), sind also die sämtlichen $(p^m - 1)$-ten Einheitswurzeln über P_p, und daher ist die aus ihnen gebildete Gruppe zyklisch (Satz 120):

(III) Ist $[\mathsf{E}:\mathsf{P}_p] = m$, so ist E der Kreisteilungskörper T_{p^m-1} über P_p.

Die von Null verschiedenen Elemente von E sind die Wurzeln der Gleichung $x^{p^m-1} - e \doteq 0$, die sämtlichen Elemente von E also die Wurzeln der Gleichung $x^{p^m} - x \doteq 0$.

In E existiert ein primitives Element ϱ derart, daß die $p^m - 1$ von Null verschiedenen Elemente von E als die Potenzen

$$\varrho^0 = e, \quad \varrho^1, \ldots, \varrho^{p^m-2}$$

darstellbar sind.

Umgekehrt gilt:

(IV) Für beliebiges m ist der Kreisteilungskörper T_{p^m-1} über P_p ein endlicher Körper mit $[\mathsf{T}_{p^m-1}:\mathsf{P}_p] = m$.

Denn T_{p^m-1} ist als Erweiterung endlichen Grades des endlichen Körpers P_p (Satz 83 [70]) selbst ein endlicher Körper (Def. 25, Zusatz [57]). Dieser hat genau p^m Elemente; seine Elemente werden nämlich bereits durch Null und die $p^m - 1$ Wurzeln von $x^{p^m-1} - e$, d. h. durch die p^m Wurzeln von $x^{p^m} - x$ erschöpft; denn diese p^m Wurzeln bilden bereits einen Körper, weil aus $\alpha^{p^m} = \alpha$, $\beta^{p^m} = \beta$ nicht nur (wie im Beweis zu Satz 120) folgt $(\alpha\beta)^{p^m} = \alpha\beta$ und (falls $\beta \neq 0$) $\left(\frac{\alpha}{\beta}\right)^{p^m} = \frac{\alpha}{\beta}$, sondern nach Satz 44 [37] auch $(\alpha \pm \beta)^{p^m} = \alpha \pm \beta$. Nach (II) folgt daher $p^{[\mathsf{T}_{p^m-1}:\mathsf{P}_p]} = p^m$, d. h. in der Tat $[\mathsf{T}_{p^m-1}:\mathsf{P}_p] = m$.

Da durch die Elementanzahl p^m die Charakteristik p und der Grad m eindeutig bestimmt sind, gilt nach (III) und (IV):

(V) Für jede Elementanzahl der Form p^m gibt es genau einen endlichen Körpertypus, nämlich den Kreisteilungskörper T_{p^m-1} über P_p.

Ferner gilt:

(VI) Die Teilkörper von T_{p^m-1} sind alle und nur die Körper $\mathsf{T}_{p^\mu-1}$ mit $\mu \mid m$, und es ist dabei

$$[\mathsf{T}_{p^m-1}:\mathsf{T}_{p^\mu-1}] = \frac{m}{\mu}.$$

Denn einerseits ist, wenn $T_{p^\mu-1} \leqq T_{p^m-1}$ ist, nach Satz 71 [59] $\mu = [T_{p^\mu-1} : P_p] \mid [T_{p^m-1} : P_p] = m$, und $[T_{p^m-1} : T_{p^\mu-1}] = \frac{m}{\mu}$. Andererseits ist, wenn $\mu \mid m$ ist und dementsprechend $m = \mu\mu'$ gesetzt wird,

$$p^m - 1 = p^{\mu\mu'} - 1 = (p^\mu - 1)(p^{\mu(\mu'-1)} + \cdots + p^\mu + 1),$$

also $p^\mu - 1 \mid p^m - 1$, und daher $T_{p^\mu-1} \leqq T_{p^m-1}$, da dann die $(p^\mu - 1)$-ten Einheitswurzeln unter den $(p^m - 1)$-ten vorkommen.

Durch (V) und (VI) ist eine vollständige Übersicht über alle endlichen Körpertypen und ihre gegenseitigen Beziehungen gewonnen.

B. Sei jetzt $E = T_{p^m-1}$ ein endlicher Grundkörper und H eine endliche Erweiterung von E. Trivialerweise ist dann zunächst H von endlichem Grade n über E (Def. 25 [57]) und daher wieder ein endlicher Körper (Def. 25, Zusatz [57]), der nach (VI) die Form $H = T_{p^{mn}-1}$ hat. Ist dann ϱ ein primitives Element von H im Sinne von (III), so ist ϱ erst recht primitives Element im Sinne von Def. 19 [52] von H bzgl. jedes Teilkörpers. Also:

(VII) H ist einfach über E.

Hiermit ist die im Beweis von Satz 90 [80] zurückgebliebene Unvollständigkeit beseitigt.

Da die Charakteristik p von H in der Ordnungszahl $p^m - 1$ der Einheitswurzeln, die H bilden, nicht aufgeht, gilt ferner nach dem in Satz 121 [131] Bemerkten:

(VIII) H ist separabel über E.

Schließlich gilt nach Satz 94 [85]:

(IX) H ist normal über E.

Daher sind die Sätze der Galoisschen Theorie auf die Erweiterung H von E anwendbar. Wenn auch eine Übersicht über die Körper zwischen H und E durch (VI) bereits ohne Verwendung der Galoisschen Theorie gewonnen ist — es sind alle und nur die $T_{p^{m\nu}-1}$ mit $\nu \mid n$ —, so interessiert doch theoretisch die Feststellung:

(X) H ist zyklisch über E.

Die Galoisgruppe von H bzgl. E besteht nämlich aus den Potenzen des Automorphismus

$$A : \alpha \to \alpha^{p^m} \text{ für jedes } \alpha \text{ aus H,}$$

mit $A^n = E$, d. h. aus den n Automorphismen

$$A : \alpha \to \alpha^{p^{m\nu}} \text{ für jedes } \alpha \text{ aus H } (\nu = 0, 1, \ldots, n-1).$$

Nach Satz 44 [37] [siehe auch schon die Schlußweise im Beweis zu (IV)] sind das nämlich in der Tat Automorphismen von H, bei denen jedes Element von E als Wurzel von $x^{p^m} - x$ invariant bleibt, also Automorphismen von H bzgl. E. Diese n Automorphismen von H bzgl. E sind ferner voneinander verschieden, weil für ein primitives Element ϱ von H (im Sinne von (III)) die sämtlichen Potenzen ϱ^i $(i = 1, \ldots, p^{mn} - 1)$, also insbesondere die n Potenzen $\varrho^{p^{m\nu}}$ $(\nu = 0, 1, \ldots, n-1)$ voneinander verschieden sind. Also sind es alle $n = [H : E]$ Automorphismen der Galoisgruppe von H bzgl. E (Satz 105 [96]).

§ 21. Reine und zyklische Erweiterungen von Primzahlgrad.

Zur Behandlung der Frage nach der Auflösbarkeit durch Wurzelzeichen haben wir den speziellen Entwicklungen des vorigen Paragraphen noch die Theorie der irreduziblen reinen Polynome von Primzahlgrad an die Seite zu stellen, auf die sich ja die Def. 40 [129] der Auflösbarkeit durch Wurzelzeichen stützt. Wir beweisen zunächst den folgenden Satz über die Irreduzibilität eines reinen Polynoms von Primzahlgrad:

Satz 123. Es sei p eine Primzahl und $x^p - a$ ein reines Polynom mit $a \neq 0$ aus K. Dann enthält der Wurzelkörper W dieses Polynoms den Kreisteilungskörper T_p über K, und es sind nur die folgenden beiden Fälle möglich:

a.) $x^p - a$ hat eine Wurzel in K, d. h. a ist eine p-te Potenz in K. Dann ist $x^p - a$ reduzibel in K und $W = T_p$.

b.) $x^p - a$ hat keine Wurzel in K, d. h. a ist keine p-te Potenz in K. Dann ist $x^p - a$ irreduzibel in K und sogar in T_p, und überdies normal über T_p, also W rein vom Grade p über T_p.

Beweis: Es seien $\alpha_1, \ldots, \alpha_p$ die Wurzeln von $x^p - a$ und α eine von ihnen. Aus $\alpha^p = a$ folgt dann, weil $a \neq 0$, also auch $\alpha \neq 0$ ist,

$$\left(\frac{x}{\alpha}\right)^p - e \equiv \frac{x^p - \alpha^p}{\alpha^p} \equiv \frac{x-\alpha_1}{\alpha} \cdots \frac{x-\alpha_p}{\alpha}$$
$$\equiv \left(\frac{x}{\alpha} - \frac{\alpha_1}{\alpha}\right) \cdots \left(\frac{x}{\alpha} - \frac{\alpha_p}{\alpha}\right).$$

Nach dem Einsetzungsprinzip (1, Satz 12 [40], angewandt auf $\mathsf{I}[x']$ mit $\mathsf{I} = \mathsf{W}[x]$ und die Einsetzung $x' = \alpha x$) darf hierin αx für x gesetzt werden, so daß

$$x^p - e \equiv \left(x - \frac{\alpha_1}{\alpha}\right) \cdots \left(x - \frac{\alpha_p}{\alpha}\right)$$

resultiert. Die Quotienten $\frac{\alpha_i}{\alpha}$ sind also die p-ten Einheitswurzeln über K, d. h. es ist $\mathsf{W} \geqq \mathsf{T}_p$. Ist ferner ζ eine primitive p-te Einheitswurzel (Satz 120 [129]; — falls K die Charakteristik p hat, $\zeta = e$ [Satz 122, Zusatz]), so gilt bei geeigneter Reihenfolge

$$\alpha_i = \zeta^i \alpha \quad (i = 1, \ldots, p).$$

a.) Liegt nun α in K, so liegen hiernach die α_i in T_p, d. h. es ist $\mathsf{W} \leqq \mathsf{T}_p$ und somit nach obigem $\mathsf{W} = \mathsf{T}_p$.

b.) Liegt aber keins der α in K, und wäre dann

$$h(x) \equiv x^\nu + \cdots + a_0 \quad (1 \leqq \nu \leqq p-1)$$

ein irreduzibler Faktor von $x^p - a$ in K, so hätte $\pm a_0$ als Produkt von gewissen ν Faktoren α_i eine Darstellung

$$\pm a_0 = \zeta^\mu \alpha^\nu.$$

Wird nach Satz 14, 17 [18, 20] $\nu\nu' = 1 + kp$ gesetzt, so folgte wegen $\alpha^p = a$

$$(\pm a_0)^{\nu'} = \zeta^{\mu\nu'} \alpha\, a^k,$$

so daß wegen $a \neq 0$ die Wurzel $\alpha_{\mu\nu'} = \zeta^{\mu\nu'}\alpha = \frac{(\pm a_0)^{\nu'}}{a^k}$ doch in K läge. Also ist dann $x^p - a$ irreduzibel in K und somit $\mathsf{K}(\alpha)$ vom Grade p über K. Wird nun in den gemachten Schlüssen $h(x)$ als irreduzibler Faktor von $x^p - a$ in T_p angenommen, so folgte, daß α und somit $\mathsf{K}(\alpha)$ in T_p enthalten

wäre. T_p hätte also ein Multiplum von p zum Grade über K, während doch nach Satz 121 [131] dieser Grad ein Teiler von $p-1$ ist. Somit ist dann $x^p - a$ auch in T_p irreduzibel und nach Satz 99, (III.) [88]) überdies normal über T_p, also nach Satz 99, (I.) $\mathsf{W} = \mathsf{T}_p(\alpha)$ und daher rein vom Grade p über T_p (Def. 39 [128]).

Für die Frage nach der Auflösbarkeit durch Wurzelzeichen hat uns naturgemäß der Fall b.) des Satzes 123 besonders zu interessieren. Wenn K die Charakteristik p hat, ist dann $x^p - a$ ein inseparables irreduzibles Polynom (Def. 17 [47]). Seine einzige Wurzel α ist p-fach. Im Sinne unserer durchgängigen Beschränkung auf separable Erweiterungen schließen wir diese Möglichkeit im folgenden aus, indem wir bei der Betrachtung reiner Erweiterungen vom Primzahlgrad p die Charakteristik von K als von p verschieden voraussetzen. Dann ist $x^p - a$ (und allgemeiner jedes irreduzible Polynom aus K vom Grade p) a fortiori separabel (Def. 17).

Ferner ist $x^p - a$ im Falle b.) i. a. nicht über K, wohl aber über T_p normal, so daß es für die beabsichtigte Anwendung zweckmäßig erscheint, vor der Adjunktion einer Wurzel eines reinen Polynoms $x^p - a$ vom Primzahlgrad p jeweils erst eine primitive p-te Einheitswurzel ζ zu K zu adjungieren, also zunächst zu dem erweiterten Grundkörper $\overline{\mathsf{K}} = \mathsf{K}(\zeta) = \mathsf{T}_p$ überzugehen, der mit dem Körper $\overline{\mathsf{T}}_p = \{\mathsf{T}_p, \overline{\mathsf{K}}\}$ (Def. 37, Zusatz [118]) der p-ten Einheitswurzeln über $\overline{\mathsf{K}}$ zusammenfällt.

In dieser Hinsicht ist der nachstehende, aus Satz 123 ohne weiteres folgende Satz für uns von Interesse (in dem K sozusagen mit dem eben genannten $\overline{\mathsf{K}}$ zu identifizieren ist):

Satz 124. Ist p eine Primzahl und K ein Körper mit von p verschiedener Charakteristik, der die p-ten Einheitswurzeln über K enthält, so ist jede reine Erweiterung p-ten Grades Λ von K normal (separabel und zyklisch) über K.

Daß Λ als separable normale Erweiterung vom Primzahlgrade p zyklisch über K ist, ist trivial. Denn seine Galoisgruppe bzgl. K hat nach Satz 105 [96] die Primzahlordnung p und muß daher nach Satz 34 [32] mit der Periode jedes ihrer von E verschiedenen Elemente zusammenfallen.

In Umkehrung zu Satz 124 beweisen wir nun den für unsere Anwendung grundlegenden Satz:

Satz 125. Ist p eine Primzahl und K ein Körper mit von p verschiedener Charakteristik, der die p-ten Einheitswurzeln über K enthält, so ist jede normale Erweiterung p-ten Grades Λ von K (a fortiori separabel, zyklisch und) rein über K.

Beweis: Es sei A ein primitives Element der zyklischen Galoisgruppe von Λ bzgl. K, ϑ ein primitives Element von Λ bzgl. K und ζ eine primitive p-te Einheitswurzel über K Dann bilden wir die sog. **Lagrangesche Resolvente** von ϑ:

$$\alpha = \vartheta_E + \zeta^{-1}\vartheta_A + \cdots + \zeta^{-(p-1)}\vartheta_{A^{p-1}}.$$

Wenn dies Element α aus Λ von Null verschieden ist, schließen wir folgendermaßen:

Durch Anwendung von A auf α entsteht wegen $A^p = E$, $\zeta^p = e$ und der Invarianz des Elements ζ aus K bei A

$$\begin{aligned}\alpha_A &= \vartheta_A + \zeta^{-1}\vartheta_{A^2} + \cdots + \zeta^{-(p-1)}\vartheta_{A^p} \\ &= (\vartheta_E + \zeta^{-1}\vartheta_A + \cdots + \zeta^{-(p-1)}\vartheta_{A^{p-1}})\zeta = \alpha\zeta,\end{aligned}$$

also durch wiederholte Anwendung von A

$$\alpha_{A^\nu} = \alpha\zeta^\nu.$$

Hiernach sind die infolge der Annahme $\alpha \neq 0$ voneinander verschiedenen Elemente $\alpha, \alpha\zeta, \ldots, \alpha\zeta^{p-1}$ die konjugierten zu α bzgl. K, d. h. es ist

$$g(x) \equiv (x-\alpha)(x-\alpha\zeta)\cdots(x-\alpha\zeta^{p-1})$$

das zu α gehörige irreduzible Polynom aus K, und α ist ein primitives Element von Λ (Satz 111, 112 [109, 110] nebst Zusatz). Aus

$$x^p - e \equiv (x-e)(x-\zeta)\cdots(x-\zeta^{p-1})$$

folgt nun wie im Beweis zu Satz 123

$$g(x) \equiv x^p - \alpha^p,$$

und somit ist

$$g(x) \equiv x^p - a$$

mit $a = \alpha^p$ in K, also α Wurzel des irreduziblen reinen Polynoms $x^p - a$ aus K. Daher ist dann in der Tat $\Lambda = \mathsf{K}(\alpha)$ rein über K (Def. 39 [128]).

Wir zeigen nun, daß man durch passende Wahl der primitiven p-ten Einheitswurzel ζ erreichen kann, daß $\alpha \neq 0$ ist. Wäre nämlich für jede der $p-1$ primitiven p-ten Einheitswurzeln ζ^ν $(\nu = 1, \ldots, p-1)$ die zugehörige Lagrangesche Resolvente $\alpha_\nu = 0$, so bestände das Gleichungssystem

$$\alpha_\nu = \sum_{\mu=0}^{p-1} (\zeta^\nu)^{-\mu}\, \vartheta_{A^\mu} = 0 \quad (\nu = 1, \ldots, p-1).$$

Multipliziert man dessen ν-te Gleichung mit $\zeta^{\nu\mu'}$ und summiert über ν, so folgte nach Vertauschung der Summationsfolge

$$\sum_{\mu=0}^{p-1} \left(\sum_{\nu=1}^{p-1} \zeta^{\nu(\mu'-\mu)} \right) \vartheta_{A^\mu} = 0.$$

Da nun

$$\sum_{\nu=1}^{p-1} (\zeta^{\mu'-\mu})^\nu = \begin{cases} -e & \text{für } \mu' \not\equiv \mu \bmod p \\ pe - e & \text{für } \mu' \equiv \mu \bmod p \end{cases}$$

ist, weil im ersteren Falle $\zeta^{\mu'-\mu}$ primitive p-te Einheitswurzel, also Wurzel von $\dfrac{x^p - e}{x - e} \equiv x^{p-1} + x^{p-2} + \cdots + x + e$ ist, während im letzteren Falle $(p-1)$-mal der Summand e steht, so resultierten auf diese Weise die Relationen

$$\sum_{\mu=0}^{p-1} \vartheta_{A^\mu} = p\, \vartheta_{A^{\mu'}} \quad (\mu' = 0, 1, \ldots, p-1).$$

Da K nicht die Charakteristik p hat, wären also alle $\vartheta_{A^{\mu'}}$ einander gleich, was für ein primitives Element ϑ von Λ nach Satz 112, Zusatz [111] nicht der Fall ist.

Wir wenden zum Schluß noch die vorstehenden Resultate an, um die Auflösbarkeit durch Wurzelzeichen von T_p über bestimmten Grundkörpern K zu beweisen:

Satz 126. Es sei p eine Primzahl und K ein Körper, dessen Charakteristik 0 oder eine Prim-

zahl $> p$ ist. Dann ist der Kreisteilungskörper T_p durch Wurzelzeichen auflösbar über K, und überdies existiert sogar eine Körperkette

$$K = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_r \quad \text{mit} \quad \overline{\Lambda}_r \geqq T_p,$$

in der $\overline{\Lambda}_i$ nicht nur (gemäß Def. 40 [129]) rein von Primzahlgrad, sondern auch normal über $\overline{\Lambda}_{i-1}$ ist.

Beweis: Wir wenden vollständige Induktion an und setzen dazu die Behauptungen für alle Primzahlen $< p$ (und alle dabei nach der Formulierung des Satzes zulässigen Grundkörper) als bereits bewiesen voraus. Es sei nun d der nach Satz 122 [132] in $p-1$ aufgehende Grad von T_p über K und $d = p_1 \cdots p_\nu$ die Zerlegung von d in (nicht notwendig verschiedene) Primzahlen p_k. Weil nach Voraussetzung die Charakteristik von K, wenn $\neq 0$, auch größer als jede dieser Primzahlen ist, existiert dann nach der Induktionsannahme zunächst eine Körperkette

$$K = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_{r_1} \quad \text{mit} \quad \overline{\Lambda}_{r_1} \geqq T_{p_1},$$

in der $\overline{\Lambda}_i$ rein und normal von Primzahlgrad über $\overline{\Lambda}_{i-1}$ ist, ferner (jetzt von $\overline{\Lambda}_{r_1}$ statt K als Grundkörper ausgehend) eine Körperkette

$$\overline{\Lambda}_{r_1} < \overline{\Lambda}_{r_1+1} < \cdots < \overline{\Lambda}_{r_2} \quad \text{mit} \quad \overline{\Lambda}_{r_2} \geqq T_{p_1}, T_{p_2}\ ^{1}),$$

in der $\overline{\Lambda}_{r_1+i}$ rein und normal von Primzahlgrad über $\overline{\Lambda}_{r_1+i-1}$ ist, usf., zusammengenommen also eine Körperkette

$$K = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_{r_\nu} \quad \text{mit} \quad \overline{\Lambda}_{r_\nu} \geqq T_{p_1}, \ldots, T_{p_\nu},$$

in der durchweg $\overline{\Lambda}_i$ rein und normal von Primzahlgrad über $\overline{\Lambda}_{i-1}$ ist. Es sei nun $\overline{T}_p$ der Kreisteilungskörper für p über $\overline{\Lambda}_{r_\nu}$ und $\overline{d}$ sein nach Satz 119 [120] in d aufgehender Grad über $\overline{\Lambda}_{r_\nu}$. Dann existiert nach ganz entsprechenden Schlüssen wie beim Resultat von Gauss [133/34] (Satz 36, 109, 122 [33,

---

[1]) Der Kreisteilungskörper $\overline{T}_{p_2}$ für p_2 über $\overline{\Lambda}_{r_1}$ enthält natürlich den Kreisteilungskörper T_{p_2} für p_2 über K.

101, 132]) eine Körperkette

$$\overline{\Lambda}_{r_\nu} < \overline{\Lambda}_{r_\nu+1} < \cdots < \overline{\Lambda}_r = \overline{\mathsf{T}}_p,$$

in der $\overline{\Lambda}_{r_\nu+i}$ normal von Primzahlgrad über $\overline{\Lambda}_{r_\nu+i-1}$ ist. Die sukzessiven Grade in dieser letzten Kette sind als Teiler von $\bar{d}$ gewisse der Primzahlen p_k. Da nun in den $\overline{\Lambda}_{r_\nu+i}$ nach Konstruktion die p_k-ten Einheitswurzeln enthalten sind, ist nach dem — wegen der Voraussetzung über die Charakteristik von K — (vgl. auch Satz 42 [37]) anwendbaren Satz 125 $\overline{\Lambda}_{r_\nu+i}$ rein über $\overline{\Lambda}_{r_\nu+i-1}$. Die volle Kette

$$\mathsf{K} = \overline{\Lambda}_0 < \cdots < \overline{\Lambda}_r = \overline{\mathsf{T}}_p$$

hat somit, wenn man noch bedenkt, daß $\mathsf{T}_p \leqq \overline{\mathsf{T}}_p$ ist, alle für die Behauptungen des Satzes erforderlichen Eigenschaften.

Da für die kleinste Primzahl $p = 2$ die Behauptungen wegen $\mathsf{T}_2 = \mathsf{K}$ trivialerweise zutreffen, ist hiermit der Satz durch vollständige Induktion bewiesen.

§ 22. Kriterium für die Auflösbarkeit durch Wurzelzeichen.

Um das in diesem Paragraphen herzuleitende Kriterium für die Auflösbarbeit durch Wurzelzeichen bequem aussprechen zu können, stellen wir die folgende Definition voran:

***Definition 41.** Eine separable normale Erweiterung N von endlichem Grade eines Körpers K heißt **metazyklisch** über K, wenn eine Zwischenkörper-Kette

$$\mathsf{K} = \Lambda_0 < \Lambda_1 < \cdots < \Lambda_r = \mathsf{N}$$

derart existiert, daß Λ_i normal von Primzahlgrad über Λ_{i-1} ist, oder — was nach dem Fundamentalsatz der Galoisschen Theorie dasselbe besagt —, wenn die Galoisgruppe $\mathfrak{G}$ von N bzgl. K eine Untergruppenkette

$$\mathfrak{G} = \mathfrak{H}_0 > \mathfrak{H}_1 > \cdots > \mathfrak{H}_r = \mathfrak{E}$$

derart enthält, daß $\mathfrak{H}_i$ Normalteiler von Primzahlindex von $\mathfrak{H}_{i-1}$ ist.

Ein separables **Polynom** $f(x)$ aus K heißt metazyklisch über K, wenn sein Wurzelkörper **metazyklisch** über K ist.

Der Ausdruck metazyklisch rührt daher, daß dann die einzelnen Schritte Λ_i über Λ_{i-1} bzw. $\mathfrak{H}_{i-1}/\mathfrak{H}_i$ zyklisch sind. Man nennt übrigens **Gruppen** $\mathfrak{G}$ von der in Def. 41 angegebenen Art ebenfalls **metazyklisch.**

Wir beweisen nun das folgende Kriterium für die Auflösbarkeit durch Wurzelzeichen normaler Erweiterungen endlichen Grades, wobei wir uns wegen der im vorigen Paragraphen für Primzahlcharakteristiken zutage getretenen Komplikationen auf Grundkörper der Charakteristik 0 beschränken, so daß also insbesondere die Voraussetzung der Separabilität trivialerweise stets erfüllt ist:

Satz 127. Eine normale Erweiterung N von endlichem Grade über einem Körper K der Charakteristik 0 ist dann und nur dann durch Wurzelzeichen auflösbar, wenn sie metazyklisch ist.

Ein Polynom $f(x)$ aus K ist also dann und nur dann durch Wurzelzeichen auflösbar, wenn es metazyklisch ist.

Beweis: a.) Es sei N durch Wurzelzeichen auflösbar über K. Gemäß Def. 40 [129] existiert dann eine Körperkette

$$K = \overline{\Lambda}_0' < \overline{\Lambda}_1' < \cdots < \overline{\Lambda}_r' \text{ mit } \overline{\Lambda}_r' \geqq N,$$

in der $\overline{\Lambda}_i'$ rein vom Primzahlgrade p_i über $\overline{\Lambda}_{i-1}'$ ist. Nach Satz 126 existiert (ähnlich wie im Beweise jenes Satzes) eine Körperkette

$$K = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_s \text{ mit } \overline{\Lambda}_s \geqq T_{p_1}, \ldots, T_{p_r},$$

in der $\overline{\Lambda}_i$ (rein und) normal von Primzahlgrad über $\overline{\Lambda}_{i-1}$ ist. Es sei nun α_i eine Folge von Elementen aus den $\overline{\Lambda}_i'$ derart, daß α_i Wurzel eines reinen irreduziblen Polynoms $x^{p_i} - a_i$ aus $\overline{\Lambda}_{i-1}'$, also $\overline{\Lambda}_i' = \overline{\Lambda}_{i-1}'(\alpha_i)$ und $\overline{\Lambda}_r' = K(\alpha_1, \ldots, \alpha_r)$ ist. Ent-

weder ist $x^{p_1} - a_1$ auch irreduzibel in $\overline{\Lambda}_s$; dann ist sein Wurzelkörper $\overline{\Lambda}_{s+1}$ über $\overline{\Lambda}_s$ nach Satz 123 [137] und wegen $\mathsf{T}_{p_1} \leqq \overline{\Lambda}_s$ (rein und) normal vom Primzahlgrade p_1 über $\overline{\Lambda}_s$ und zudem $\overline{\Lambda}_{s+1} = \overline{\Lambda}_s(\alpha_1)$. Oder es ist $x^{p_1} - a_1$ reduzibel in $\overline{\Lambda}_s$; dann ist nach demselben Satze $\overline{\Lambda}_{s+1} = \overline{\Lambda}_s$ und zudem $\overline{\Lambda}_{s+1} = \overline{\Lambda}_s(\alpha_1)$. Ebenso schließt man, daß der Wurzelkörper $\overline{\Lambda}_{s+2}$ von $x^{p_2} - a_2$ über $\overline{\Lambda}_{s+1}$ entweder (rein und) normal vom Primzahlgrade p_2 über $\overline{\Lambda}_{s+1}$ oder $= \overline{\Lambda}_{s+1}$ und beidemal zudem $\overline{\Lambda}_{s+2} = \overline{\Lambda}_{s+1}(\alpha_2)$ ist, usf. So ergibt sich bei Fortgehen bis zu $\overline{\Lambda}_{s+r}$ bei nur einmaliger Zählung mehrfach hintereinander auftretender Körper eine Körperkette

$$\mathsf{K} = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_{\bar{r}} \text{ mit } \overline{\Lambda}_{\bar{r}} \geqq \mathsf{N}$$

(letzteres wegen $\overline{\Lambda}_{\bar{r}} = \overline{\Lambda}_s(\alpha_1, \ldots, \alpha_r) \geqq \mathsf{K}(\alpha_1, \ldots, \alpha_r) = \overline{\Lambda}'_r \geqq \mathsf{N}$), in der durchweg $\overline{\Lambda}_i$ (rein und) normal von Primzahlgrad über $\overline{\Lambda}_{i-1}$ ist. Dieser Kette entspricht nach den Ausführungen in § 18, 3.) (vgl. Fig. 5 [125]) eine Zwischenkörperkette

$$\mathsf{K} = \Lambda_0 \leqq \Lambda_1 \leqq \cdots \leqq \Lambda_{\bar{r}} = \mathsf{N},$$

in der Λ_i normal über Λ_{i-1} ist, und zwar von Primzahlgrad, falls nicht $\Lambda_i = \Lambda_{i-1}$ ist (und somit Λ_i ausgelassen werden kann); denn der Grad $[\Lambda_i : \Lambda_{i-1}]$ ist als Teiler des Primzahlgrades $[\overline{\Lambda}_i : \overline{\Lambda}_{i-1}]$ entweder 1 oder eben diese Primzahl [1]) Gemäß Def. 41 ist dann N metazyklisch über K.

b.) Es sei N metazyklisch über K. Gemäß Def. 41 existiert dann eine Zwischenkörperkette

$$\mathsf{K} = \Lambda_0 < \Lambda_1 < \cdots < \Lambda_r = \mathsf{N},$$

in der Λ_i normal vom Primzahlgrad p_i über Λ_{i-1} ist. Wie unter a.) existiert eine Körperkette

$$\mathsf{K} = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_s \text{ mit } \overline{\Lambda}_s \geqq \mathsf{T}_{p_1}, \ldots, \mathsf{T}_{p_r},$$

[1]) Derselbe Schluß wurde übrigens — ohne daß es ausdrücklich hervorgehoben wurde — schon in dem Beweise des Resultats von Gauß in § 20 [134] für die dort auftretenden Primzahlgrade 2 gemacht.

in der $\overline{\Lambda}_i$ rein (und normal) von Primzahlgrad über $\overline{\Lambda}_{i-1}$ ist. Es sei nun ϑ_i eine Folge von Elementen aus den Λ_i derart, daß ϑ_i Wurzel eines normalen Polynoms $g_i(x)$ vom Primzahlgrad p_i aus Λ_{i-1}, also $\Lambda_i = \Lambda_{i-1}(\vartheta_i)$ und $\mathsf{N} = \Lambda_r = \mathsf{K}(\vartheta_1, \ldots, \vartheta_r)$ ist. Entweder ist $g_1(x)$ irreduzibel und somit auch normal in $\overline{\Lambda}_s$; dann ist sein Wurzelkörper $\overline{\Lambda}_{s+1} = \overline{\Lambda}_s(\vartheta_1)$ über $\overline{\Lambda}_s$ wegen $\mathsf{T}_{p_1} \leqq \overline{\Lambda}_s$ nach Satz 125 [140] rein (und normal) vom Primzahlgrad p_1 über Λ_s. Oder es ist $g_1(x)$ reduzibel in $\overline{\Lambda}_s$; dann ist $\overline{\Lambda}_{s+1} = \overline{\Lambda}_s(\vartheta_1) = \Lambda_s$, weil dann $[\overline{\Lambda}_{s+1} : \overline{\Lambda}_s]$ einerseits $< p_1$ ($\leqq$ wegen der Normalität von $g_1(x)$ in Λ_0 und sogar $<$ wegen der Reduzibilität in $\overline{\Lambda}_s$), andererseits ein Teiler von p_1 (nach Satz 119 [120], angewandt auf $\mathsf{K} = \Lambda_0$, $\mathsf{N} = \Lambda_1$, $\overline{\Lambda} = \overline{\Lambda}_s$, $\overline{\mathsf{N}} = \overline{\Lambda}_{s+1}$), also $[\overline{\Lambda}_{s+1} : \overline{\Lambda}_s] = 1$ ist. Ebenso schließt man, daß der Wurzelkörper $\overline{\Lambda}_{s+2} = \overline{\Lambda}_{s+1}(\vartheta_2)$ von $g_2(x)$ über $\overline{\Lambda}_{s+1}$ entweder rein (und normal) vom Primzahlgrad p_2 über $\overline{\Lambda}_{s+1}$ oder $= \overline{\Lambda}_{s+1}$ ist, usf. So ergibt sich durch Fortgehen bis zu $\overline{\Lambda}_{s+\bar{r}}$ bei nur einmaliger Zählung mehrfach hintereinander auftretender Körper eine Körperkette

$$\mathsf{K} = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_{\bar{r}} \quad \text{mit} \quad \overline{\Lambda}_{\bar{r}} \geqq \mathsf{N}$$

(letzteres wegen $\overline{\Lambda}_{\bar{r}} = \overline{\Lambda}_s(\vartheta_1, \ldots, \vartheta_r) \geqq \mathsf{K}(\vartheta_1, \ldots, \vartheta_r) = \mathsf{N}$), in der durchweg $\overline{\Lambda}_i$ rein (und normal) von Primzahlgrad über $\overline{\Lambda}_{i-1}$ ist. Gemäß Def. 40 [129] ist dann N durch Wurzelzeichen auflösbar über K.

Wie aus jedem der beiden Teilbeweise ersichtlich ist, gilt auch allgemein eine entsprechende Verschärfung, wie sie schon in dem speziellen Satz 126 [141] erhalten wurde:

Zusatz. Ist unter den Voraussetzungen von Satz 127 N durch Wurzelzeichen auflösbar über K, so existiert sogar eine Körperkette

$$\mathsf{K} = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_r \quad \text{mit} \quad \overline{\Lambda}_r \geqq \mathsf{N},$$

in der $\overline{\Lambda}_i$ nicht nur (gemäß Def. 40) rein von Primzahlgrad, sondern auch normal über $\overline{\Lambda}_{i-1}$ ist.

Durch Satz 127 in Verbindung mit dem schon in Def. 41 Gesagten wird unsere zu Beginn dieses Abschnitts gestellte Frage entschieden, unter welchen Bedingungen eine algebraische Gleichung $(x) \doteq 0$ in einem Grundkörper K der Charakteristik 0 durch Wurzelzeichen auflösbar ist[1]), wann also ihre Wurzeln durch Rechenausdrücke darstellbar sind, die mittels der vier elementaren Rechenoperationen und der Operation des Wurzelziehens gebildet sind. Stellt man die etwas andere Frage, wann eine Wurzel eines irreduziblen Polynoms $f(x)$ aus K auf diese Weise darstellbar ist, so kommt das auf die Frage nach der Auflösbarkeit durch Wurzelzeichen einer beliebigen Erweiterung Λ endlichen Grades von K hinaus, die umgekehrt auch nicht allgemeiner ist, weil jede solche Erweiterung Λ als Stammkörper eines irreduziblen Polynoms $f(x)$ aufgefaßt werden kann. Wir führen in dieser Hinsicht an, daß die Bedingungen hierfür genau dieselben sind, wie für die oben behandelte Frage, daß nämlich eine beliebige Erweiterung endlichen Grades Λ von K dann und nur dann durch Wurzelzeichen auflösbar ist, wenn dies für die zugehörige normale Erweiterung N (den Wurzelkörper irgendeines irreduziblen Polynoms $f(x)$, für das Λ Stammkörper ist) der Fall ist. Daß mit N auch Λ durch Wurzelzeichen auflösbar ist, ist klar. Umgekehrt zeigt man durch Übergang von einer Körperkette gemäß Def. 41 für Λ zu deren konjugierten, daß mit Λ auch alle konjugierten Erweiterungen durch Wurzelzeichen auflösbar sind, woraus sich dann leicht die Auflösbarkeit durch Wurzelzeichen von N ergibt.

Beispiele durch Wurzelzeichen auflösbarer algebraischer Gleichungen über Grundkörpern der Charakteristik 0.

1.) Alle Gleichungen zweiten, dritten, vierten Grades.

Deren Galoisgruppen sind nämlich isomorph zu Untergruppen der symmetrischen Gruppen $\mathfrak{S}_2$, $\mathfrak{S}_3$, $\mathfrak{S}_4$ (Satz 107 [98]). Die letzteren erweisen sich aber (samt ihren sämtlichen Untergruppen) leicht als metazyklisch.

2.) Alle zyklischen und allgemeiner abelschen Gleichungen, speziell also nach Satz 121 [131] die allgemeine Kreisteilungsgleichung $x^n - 1 \doteq 0$.

Nach Satz 36 [33] ist nämlich jede endliche zyklische Gruppe metazyklisch. Auf die allgemeine Theorie der endlichen abelschen

[1]) Genau genommen liegt übrigens keine Entscheidung der Frage sondern nur eine Zurückführung auf die Aufstellung und Untersuchung der Galoisgruppe vor.

Gruppen, aus der insbesondere leicht folgt, daß diese Gruppen sämtlich metazyklisch sind, können wir hier nicht näher eingehen [1]).

§ 23. Existenz nicht durch Wurzelzeichen auflösbarer algebraischer Gleichungen.

Die Existenz nicht durch Wurzelzeichen auflösbarer Gleichungen wurde durch Abel entdeckt, der zuerst die Unmöglichkeit bewies, die allgemeine Gleichung höheren als vierten Grades durch Wurzelzeichen aufzulösen. Wir wollen in diesem letzten Paragraphen einen modernen Beweis dieses Abelschen Satzes skizzieren.

Zunächst definieren wir:

Definition 42. Ist $K_n = K(x_1, \ldots, x_n)$ der Körper der rationalen Funktionen von n Unbestimmten $x_1, \ldots, x_n$ über K, so heißt das Polynom

$$(1.) \qquad f_n(x) \equiv x^n + x_1 x^{n-1} + \cdots + x_n$$

über K_n das **allgemeine Polynom n-ten Grades** über K.

Dieses allgemeine Polynom n-ten Grades über K ist als eine „unbestimmte" Zusammenfassung aller speziellen Polynome n-ten Grades über K anzusehen, die ja aus ihm durch Einsetzung irgendwelcher Elementsysteme $a_1, \ldots, a_n$ aus K für die Unbestimmten $x_1, \ldots, x_n$ über K gewonnen werden können.

Wir betrachten nun die Zerlegung in Linearfaktoren

$$(2.) \quad f_n(x) \equiv x^n + x_1 x^{n-1} + \cdots + x_n \equiv (x - \xi_1) \cdots (x - \xi_n)$$

des allgemeinen Polynoms n-ten Grades über K in seinem Wurzelkörper $W_n = K_n(\xi_1, \ldots, \xi_n)$. Denkt man sich die n Linearfaktoren rechts ausmultipliziert, so müssen nach **1**, Satz 11 [32] die Koeffizienten gleich hoher Potenzen von x links und rechts übereinstimmen. So erhält man das Formelsystem [2])

---

[1]) Wir verweisen deswegen auf **3**, § 3 Aufg. 9—20 und bezüglich weiterer Sätze über metazyklische Gruppen auf das Buch von Speiser (**1**, Lit.-Verz. 16).

[2]) Wir bezeichnen hier, abweichend von der Festsetzung in **1**, S. 42 die Gleichheit in $K_n = K(x_1, \ldots, x_n)$ und in der algebraischen Erweiterung $W_n = Kn(\xi_1, \ldots, \xi_n)$ nur mit $=$, um $\equiv$ der Gleichheit bei Hinzunahme weiterer

$$(3.)\qquad \begin{cases} x_1 = -(\xi_1 + \cdots + \xi_n) \\ x_2 = \xi_1\xi_2 + \cdots + \xi_{n-1}\xi_n \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x_n = (-1)^n \xi_1 \cdots \xi_n \end{cases}$$

oder zusammengefaßt

$$x_\nu = (-1)^\nu \sum_{\{i_1,\ldots,i_\nu\}} \xi_{i_1} \cdots \xi_{i_\nu} \qquad (\nu = 1, \ldots, n),$$

wo die Summe rechts über alle $\binom{n}{\nu}$ Kombinationen ν-ter Ordnung (**1**, § 16 [108]) der Ziffern $1, \ldots, n$ zu erstrecken ist. Nach diesen Formeln ist speziell

$$(4.)\quad W_n = K_n(\xi_1, \ldots, \xi_n) = K(x_1, \ldots, x_n; \xi_1, \ldots, \xi_n) = K(\xi_1, \ldots, \xi_n).$$

Neben der bisherigen von (1.) über (2.) zu (3.) und (4.) führenden Auffassungsweise kann man auch umgekehrt von (4.), d. h. dem Körper $W_n = K(\xi_1, \ldots, \xi_n)$ der rationalen Funktionen von n jetzt als Unbestimmte vorausgesetzten $\xi_1, \ldots, \xi_n$ über K ausgehen, dann $x_1, \ldots, x_n$ durch die Formeln (3.) als Elemente dieses Körpers W_n und $f_n(x)$ durch die Formel (2.) als Polynom in dem Teilkörper $K_n = K(x_1, \ldots, x_n)$ von $W_n = K(\xi_1, \ldots, \xi_n)$ definieren, wobei dann W_n wieder der Wurzelkörper zu $f_n(x)$ über K_n ist und die Darstellungen (4.) besitzt. Allerdings steht bei dieser letzteren Auffassungsweise die Frage offen, ob das so gebildete Polynom $f_n(x)$ das allgemeine Polynom n-ten Grades über K ist. Da die genannte zweite Auffassungsweise für die beabsichtigte Anwendung handlicher ist, ist es für uns von Bedeutung, diese Frage in bejahendem Sinne zu beantworten:

Satz 128. Ist $W_n = K(\xi_1, \ldots, \xi_n)$ der Körper der rationalen Funktionen von n Unbestimmten $\xi_1, \ldots, \xi_n$ über K, so haben die durch die Formeln (3.) definierten Elemente $x_1, \ldots, x_n$ aus W_n ebenfalls

Unbestimmten (etwa x in (1.) und (2.) sowie $\bar{x}_1, \ldots, x_n$ im Bewelse des folgenden Satzes 128) vorzubehalten.

den Charakter von n Unbestimmten über K[1]), d. h. der Teilkörper $K_n = K(x_1, \ldots, x_n)$ von $W_n = K(\xi_1, \ldots, \xi_n)$ ist ebenfalls vom Erweiterungstypus des Körpers der rationalen Funktionen von n Unbestimmten über K. Insbesondere ist dann also das durch (2.) definierte Polynom $f_n(x)$ über K_n das allgemeine Polynom n-ten Grades über K.

Beweis: Es ist zu zeigen, daß die Normaldarstellungen (**1**, Def. 9 [38]) der Elemente des Integritätsbereiches $K[x_1, \ldots, x_n]$ durch $x_1, \ldots, x_n$ eindeutig sind, und dazu genügt es nachzuweisen, daß aus einer Relation

(5.) $$g(x_1, \ldots, x_n) = 0,$$

wo $g(\bar{x}_1, \ldots, \bar{x}_n)$ eine ganze rationale Funktion von n Unbestimmten $\bar{x}_1, \ldots, \bar{x}_n$ über K ist, die Relation

(6.) $$g(\bar{x}_1, \ldots, \bar{x}_n) \equiv 0$$

folgt. Diesen Nachweis führen wir durch doppelte vollständige Induktion[2]), erstens nach der Anzahl n der Unbestimmten, zweitens nach dem Grade ν_n von g in $\bar{x}_n$.

Für $n = 1$ ist $x_1 = -\xi_1$, also die Behauptung ersichtlich auf Grund des vorausgesetzten Unbestimmtencharakters von ξ_1 richtig. Sei sie schon bis $n-1$ bewiesen. Dann sei

(7.) $$g(\bar{x}_1, \ldots, \bar{x}_n) \equiv \sum_{k=0}^{\nu_n} \bar{x}_n^k \, g_k(\bar{x}_1, \ldots, \bar{x}_{n-1})$$

die (aus der Normaldarstellung durch Zusammenfassung folgende) Darstellung von g als ganze rationale Funktion von $\bar{x}_n$ über $K[\bar{x}_1, \ldots, \bar{x}_{n-1}]$, also speziell

(8.) $$g(\bar{x}_1, \ldots, \bar{x}_{n-1}, 0) \equiv g_0(\bar{x}_1, \ldots, \bar{x}_{n-1}).$$

Setzt man nun in (5.) $\xi_n = 0$, so entsteht nach dem Einsetzungsprinzip (**1**, Satz 12 [40]), das wegen des Unbestimmtencharakters von ξ_n anwendbar ist, die Relation

(9.) $$g(x_1', \ldots, x_{n-1}', 0) = 0,$$

---

[1]) Vgl. **1**, Def. 9 [38] nebst anschließender Erläuterung.

[2]) Den Gedanken, in diesem Beweise doppelte vollständige Induktion anzuwenden, verdanke ich einer brieflichen Mitteilung von Ph. Furtwängler.

wo $x_1', \ldots, x_{n-1}'$ aus $x_1, \ldots, x_{n-1}$ durch die Einsetzung $\xi_n = 0$ in (3.) hervorgehen; setzt man dann in (8.) $(\bar{x}_1, \ldots, \bar{x}_{n-1}) = (x_1', \ldots, x_{n-1}')$, so folgt aus (9.) nach dem Einsetzungsprinzip weiter die Relation

$$(10.) \qquad g_0(x_1', \ldots, x_{n-1}') = 0.$$

Da nun $x_1', \ldots, x_{n-1}'$ nach ihrer Erklärung für $\xi_1, \ldots, \xi_{n-1}$ die entsprechende Bedeutung haben, wie $x_1, \ldots, x_n$ für $\xi_1, \ldots, \xi_n$, so ergibt sich aus (10.) nach der gemachten ersten Induktionsannahme die Relation

$$g_0(\bar{x}_1, \ldots, \bar{x}_{n-1}) \equiv 0,$$

also nach (7.) weiter die Relation

$$(11.) \quad g(\bar{x}_1, \ldots, \bar{x}_n) \equiv \bar{x}_n \sum_{k=0}^{\nu_n - 1} \bar{x}_n^k g_{k+1}(\bar{x}_1, \ldots, \bar{x}_{n-1}) \equiv \bar{x}_n g^{(1)}(\bar{x}_1, \ldots, \bar{x}_n),$$

wo $g^{(1)}(\bar{x}_1, \ldots, \bar{x}_n)$ wieder eine ganze rationale Funktion von $\bar{x}_1, \ldots, \bar{x}_n$ über K ist, die (falls $\nu_n > 0$) in $\bar{x}_n$ den Grad $\nu_n - 1$ hat.

Ist nun der Grad $\nu_n = 0$, so ist $g^{(1)}(\bar{x}_1, \ldots, \bar{x}_n) \equiv 0$ und also die Behauptung (6.) nach (11.) richtig. Sei sie (für das betrachtete feste n) schon bis zum Grade $\nu_n - 1$ bewiesen, so ist, weil aus (11.) durch die Einsetzung $(\bar{x}_1, \ldots, \bar{x}_n) = (x_1, \ldots, x_n)$ die Relation

$$g(x_1, \ldots, x_n) = x_n g^{(1)}(x_1, \ldots, x_n)$$

und aus dieser nach (5.) und wegen $x_n \neq 0$ weiter die Relation

$$g^{(1)}(x_1, \ldots, x_n) = 0$$

folgt, nach dieser zweiten Induktionsannahme

$$g^{(1)}(\bar{x}_1, \ldots, \bar{x}_n) \equiv 0,$$

woraus die Behauptung (6.) nach (11.) folgt. Hiermit ist die Behauptung des Satzes durch doppelte vollständige Induktion bewiesen.

Aus Satz 128 läßt sich übrigens auch leicht die umgekehrte Tatsache folgern, daß die ausgehend von Unbestimmten $x_1, \ldots, x_n$ durch (2.) definierten Elemente $\xi_1, \ldots, \xi_n$ den Charakter von Unbestimmten über K haben. Wir brauchen das jedoch hier nicht.

Wir beweisen nunmehr:

Satz 129. Das allgemeine Polynom n-ten Grades über K ist separabel und seine Galoisgruppe bzgl. K_n ist zur symmetrischen Gruppe $\mathfrak{S}_n$ isomorph.

Beweis: Gemäß Satz 128 denken wir uns das allgemeine Polynom n-ten Grades $f_n(x)$ über K nach der vor Satz 128 besprochenen zweiten Auffassungsweise, d. h. vom Wurzelkörper $W_n = K(\xi_1, \ldots, \xi_n)$ ausgehend durch die Formeln (3.), (2.) gebildet. Daß zunächst $f_n(x)$ separabel ist, folgt dann ohne weiteres aus der Verschiedenheit seiner als n Unbestimmte über K gewählten Wurzeln $\xi_1, \ldots, \xi_n$ (Satz 59, Zusatz [48]). Es sei ferner $\begin{pmatrix} 1 \ldots n \\ i_1 \ldots i_n \end{pmatrix}$ irgendeine Permutation aus $\mathfrak{S}_n$. Nach **1**, Satz 10, 11 [26, 32] ist dann $K(\xi_{i_1}, \ldots, \xi_n)$ zu $K(\xi_1, \ldots, \xi_n)$ auf Grund der Zuordnungen

$$\xi_1 \longleftrightarrow \xi_{i_1}, \ldots, \xi_n \longleftrightarrow \xi_{i_n}$$

isomorph bzgl. K. Da aber die Formeln (3.) symmetrisch in $\xi_1, \ldots, \xi_n$ sind, entsprechen bei dieser Zuordnung die Elemente $x_1, \ldots, x_n$ und somit alle Elemente von $K_n = K(x_1, \ldots, x_n)$ sich selbst, so daß die genannte Isomorphie sogar bzgl. K_n gilt. Da

$$W_n = K(\xi_1, \ldots, \xi_n) = K(\xi_{i_1}, \ldots, \xi_{i_n})$$

ist, erzeugt also jede Permutation aus $\mathfrak{S}_n$ einen Automorphismus von W_n bzgl. K_n und wird daher umgekehrt durch einen solchen Automorphismus im Sinne von Satz 107 [98] geliefert. Aus diesem Satz ergibt sich daher mit Rücksicht auf die bereits hervorgehobene Verschiedenheit der Wurzeln $\xi_1, \ldots, \xi_n$, daß die Galoisgruppe von W_n, d. h. die von $f_n(x)$ bzgl. K_n zur symmetrischen Gruppe $\mathfrak{S}_n$ isomorph ist.

Aus Satz 129 ergibt sich übrigens speziell:

Satz 130. Das allgemeine Polynom n-ten Grades über K ist irreduzibel in K_n.

Beweis: Ist $\bar{f}_n(x)$ das zu einer Wurzel ξ von $f_n(x)$ gehörige

irreduzible Polynom in K_n, so ist einerseits $\bar{f}_n(x) \mid f_n(x)$ (Satz 53 [43]), andererseits $\bar{f}_n(\xi_i) = 0$ für jede Wurzel ξ_i von $f_n(x)$ (Satz 73]61], 129), also wegen der Verschiedenheit der Wurzeln ξ_i auch $f_n(x) \mid \bar{f}_n(x)$ (Satz 47 [40]). Beides zusammen ergibt $\bar{f}_n(x) \equiv f_n(x)$, wie behauptet.

Wir verweilen noch einen Augenblick bei den Formeln (3.), wieder unter der vor Satz 128 [149] besprochenen zweiten Auffassungsweise. Man nennt dann die Elemente $x_1, \ldots, x_n$ aus $K(\xi_1, \ldots, \xi_n)$ die **symmetrischen Grundfunktionen** der Unbestimmten $\xi_1, \ldots, \xi_n$. Allgemein nennt man ferner eine rationale Funktion über K der Unbestimmten $\xi_1, \ldots, \xi_n$ symmetrisch in $\xi_1, \ldots, \xi_n$, wenn sie bei allen Permutationen der n Elemente $\xi_1, \ldots, \xi_n$ in sich übergeht. Durch Anwendung der Sätze 107, 112 [98, 110] nebst Zusatz ergibt sich dann aus Satz 129 unmittelbar:

Satz 131. Eine rationale Funktion über K der Unbestimmten $\xi_1, \ldots, \xi_n$ [d. h. ein Element aus $K(\xi_1, \ldots, \xi_n)$] ist dann und nur dann symmetrisch, wenn sie rationale Funktion über K der symmetrischen Grundfunktionen $x_1, \ldots, x_n$ von $\xi_1, \ldots, \xi_n$ ist [d. h. ein Element aus dem Teilkörper $K(x_1, \ldots, x_n)$ von $K(\xi_1, \ldots, \xi_n)$ ist].

Die tiefer liegende Aussage dieses Satzes, nämlich die durch „nur dann" ausgedrückte, die also aussagt, daß jede symmetrische rationale Funktion über K von $\xi_1, \ldots, \xi_n$ eine rationale Funktion über K von $x_1, \ldots, x_n$ ist, ist eine Teilaussage des unter dem Namen **Satz von den symmetrischen Funktionen** bekannten Theorems, das bisher fast immer der Galoisschen Theorie zugrunde gelegt wurde (vgl. die erste Anm. zum Bew. von Satz 90 [80]). Dieses Theorem geht insofern noch über die Aussage von Satz 131 hinaus, als es weiterhin behauptet:

1.) Jede ganze rationale symmetrische Funktion über K von $\xi_1, \ldots, \xi_n$ ist eine ganze rationale Funktion von $x_1, \ldots, x_n$.

2.) Das letztere gilt auch noch, wenn an Stelle des Körpers K ein Integritätsbereich I steht.

Diese weiteren Aussagen können aber nicht, wie Satz 131, aus der Galoisschen Theorie gefolgert werden[1]).

Wir kehren nunmehr zu der eigentlichen Aufgabe dieses Paragraphen zurück, die wir jetzt auf Grund von Satz 129 in

[1]) Auf einen — mir von Ph. Furtwängler mitgeteilten — Beweis der Aussagen 1), 2.), der ganz analog, wie der Beweis von Satz 128, mit doppelter vollständiger Induktion geführt wird, kann hier nicht eingegangen werden: siehe **3, § 23, Aufg. 3.**

Angriff nehmen können. Da die symmetrische Gruppe $\mathfrak{S}_n$ für $n > 1$ stets den Normalteiler $\mathfrak{A}_n$ vom Index 2 hat (**1**, Satz 63 [113]), ergibt sich eine Reduktion des Wurzelkörpers $W_n = K_n(\xi_1, \ldots, \xi_n)$ vom Grade $n!$ über K_n auf einen Körper vom Grade $\frac{n!}{2}$ über einem aus K_n durch Adjunktion einer Quadratwurzel entstehenden Körper V_n:

Satz 132. Der Wurzelkörper $W_n = K_n(\xi_1, \ldots, \xi_n)$ des allgemeinen Polynoms n-ten Grades $(n > 1)$ über K besitzt einen Teilkörper V_n vom Grade 2 über K_n. Dieser wird, falls K nicht die Charakteristik 2 hat, durch Adjunktion des Elementes

$$\delta = \begin{vmatrix} 1 & \xi_1 & \xi_1^2 & \cdots & \xi_1^{n-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \xi_n & \xi_n^2 & \cdots & \xi_n^{n-1} \end{vmatrix}$$

zu K_n gewonnen, das Wurzel eines reinen Polynoms $x^2 - d$ vom zweiten Grade aus K_n ist[1]).

Beweis: Daß $V_n = K_n(\delta)$ der $\mathfrak{A}_n$ zugeordnete Körper zwischen K_n und W_n ist, folgt gemäß Satz 112, 129 [110, 152] daraus, daß δ bei den geraden Permutationen von $\xi_1, \ldots, \xi_n$ invariant ist, bei den ungeraden dagegen sein Vorzeichen ändert (**1**, Satz 65 [116]), und daß $\delta \neq 0$ (siehe **3**, Teil 1, § 19, Aufg. 4), also nach der Annahme über die Charakteristik $\delta \neq -\delta$ ist. Hiernach ist ferner $\delta^2 = d$ bei allen Permutationen von $\xi_1, \ldots, \xi_n$ invariant, also Element aus K_n (Satz 112, Zusatz [111]).

Das Element $d = \delta^2$, das natürlich sogar zu $K[\xi_1, \ldots, \xi_n]$ gehört, also eine ganze rationale Funktion über K der Wurzeln $\xi_1, \ldots, \xi_n$ ist, heißt die **Diskriminante von $f^n(x)$.**

Nun beweist man in der Gruppentheorie, daß für $n \neq 4$ die alternierende Gruppe $\mathfrak{A}_n$ keinen echten Normalteiler besitzt[2]), und daß $\mathfrak{A}_n$ der einzige Normal-

[1]) Hinsichtlich des Falles, daß K die Charakteristik 2 hat, siehe **3**, § 23, Aufg. 20.

[2]) Speiser, l. c. (**1**, Lit.-Verz. 16), Satz 94. Siehe auch **3**, § 23, Aufg. 13, 14.

teiler von $\mathfrak{S}_n$ ist [1]). Da $\frac{n!}{2}$ für $n \geqq 4$ keine Primzahl ist, kann also für $n > 4$ keine Untergruppenkette von $\mathfrak{S}_n$ der in Def. 41 [143] genannten Art existieren, so daß dann $\mathfrak{S}_n$ nicht metazyklisch ist. Nach Satz 127 [144] ergibt sich so das

Resultat von Abel. Das allgemeine Polynom n-ten Grades über einem Körper K der Charakteristik 0 ist für $n > 4$ nicht durch Wurzelzeichen auflösbar.

Durch diesen Satz ist die Existenz nicht durch Wurzelzeichen auflösbarer Gleichungen zunächst nur für die besonderen Grundkörper K_n von Def. 42 [148] sichergestellt. Eine weitere Frage ist dann, ob es in einem gegebenen Grundkörper K spezielle, d. h. in K selbst gelegene nicht durch Wurzelzeichen auflösbare Gleichungen jeden Grades $n > 4$ gibt. Diese Frage beantwortet sich für den Spezialfall des rationalen Grundkörpers P bejahend durch den

Irreduzibilitätssatz von Hilbert [2]). Ist $g(x; x_1, \ldots, x_n)$ eine ganze rationale Funktion der Unbestimmten $x; x_1, \ldots, x_n$ über P, die ein in $\mathsf{P}_n = \mathsf{P}(x_1, \ldots, x_n)$ irreduzibles Polynom von x ist, so gibt es unendlich viele Elementsysteme $a_1, \ldots, a_n$ aus P, so daß $g(x; a_1, \ldots, a_n)$ in P irreduzibel ist.

Aus diesem Satz ergibt sich die Lösung der zuvor aufgeworfenen Frage für den Grundkörper P folgendermaßen: Sind $\xi_1, \ldots, \xi_n$ die Wurzeln des allgemeinen Polynoms n-ten Grades $f_n(x) = x^n + x_1 x^{n-1} + \cdots + x_n$ über P, so ist nach Satz 112, Zusatz [111] und Satz 129 [152]

$$\vartheta = c_1 \xi_1 + \cdots + c_n \xi_n$$

primitives Element des Wurzelkörpers $\mathsf{W}_n = \mathsf{P}_n(\xi_1, \ldots, \xi_n)$

[1]) Das folgt dann aus dem sog. Jordanschen Satz (Speiser, ebenda Satz 27) in Verbindung mit der evidenten Nichtexistenz von Normalteilern von $\mathfrak{S}_n$ der Ordnung 2. Siehe auch 3, § 23. Aufg. 16.

[2]) D. Hilbert, Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten, Journ. f. d. reine u. angew. Math. 110, 1892.

bzgl. $\mathsf{P}_n = \mathsf{P}(x_1, \ldots, x_n)$, wenn die Koeffizienten c_ν aus P_n so gewählt werden, daß alle Permutationen $\begin{pmatrix} \nu \\ i_\nu \end{pmatrix}$ der ξ_ν verschiedene konjugierte

$$\vartheta_i = c_1 \xi_{i_n} + \cdots + c_n \xi_{i_n}$$

ergeben. Wir denken uns die c_ν in dieser Weise gewählt, und zwar, was nach Satz 49 [41] möglich ist, sogar als Elemente aus dem Integritätsbereich $\Gamma_n = \mathsf{P}[x_1, \ldots, x_n]$. Dann ist

$$g(x; x_1, \ldots, x_n) \equiv \prod_{i=1}^{n!} (x - \vartheta_i)$$

eine Galoissche Resolvente von W_n bzgl. P_n und genügt den Voraussetzungen des Hilbertschen Irreduzibilitätssatzes. Es gibt also unendlich viele Elementsysteme $a_1, \ldots, a_n$ aus P derart, daß $g(x; a_1, \ldots, a_n)$ irreduzibel in P ist. Die Wurzelkörper W über P der diesen Systemen $a_1, \ldots, a_n$ entsprechenden speziellen $f(x)$ haben dann, weil es in ihnen je ein Element ϑ des Grades $n!$ gibt, den höchstmöglichen Grad $n!$ über P (Satz 108 [100]) und somit eine zu $\mathfrak{S}_n$ selbst isomorphe Galoisgruppe (Satz 107 [98]). Nach den Ausführungen dieses Paragraphen sind also diese $f(x)$ für $n > 4$ nicht durch Wurzelzeichen auflösbar. Wir haben daher:

Korollar. Es gibt in P für jeden Grad n unendlich viele algebraische Gleichungen, deren Galoisgruppe zu $\mathfrak{S}_n$ isomorph ist (sog. Gleichungen ohne **Affekt**), insbesondere also für jeden Grad $n > 4$ unendlich viele nicht durch Wurzelzeichen auflösbare algebraische Gleichungen.

Ob dies Resultat auch für allgemeine Grundkörper K, sowie für irgendwelche Untergruppen von $\mathfrak{S}_n$ als vorgeschriebene Galoisgruppen gilt, ist bis heute, abgesehen von einfachen Fällen, unentschieden.