Ueber Galois' Theorie der algebraischen Gleichungen.

Von

Paul Bachmann in Münster.

Obwohl neuere Bearbeiter, unter ihnen besonders Herr C. Jordan*), die Untersuchungen von Galois**) über die algebraische Auflösbarkeit der Gleichungen dem allgemeinen Verständnisse durch eine weitere Ausführung und systematischere Entwicklung näher gebracht haben, so dürfte doch Mancher vom Studium dieses principiellen Theiles der Lehre von den Gleichungen durch den ausgedehnten Gebrauch der sehr abstracten Substitutionstheorie abgehalten worden sein, welcher von Jenen gemacht wird. Solchen wird vielleicht nachfolgende neue Darstellung des Gegenstandes nicht unwillkommen sein, welche die genannte Theorie, soweit es der Natur der Sache nach möglich scheint, vermeidet, indem sie sich im Wesentlichen nur auf die beiden fundamentalen Begriffe des Zahlenkörpers***) und der Irreductibilität gründet. Bei dieser Behandlung, welche übrigens schon von Herrn Dedekind angegeben worden ist, wird zugleich — meinen wir — von den Phasen des Auflösungsprocesses der Gleichungen eine viel concretere Anschauung, als bei der gebräuchlichen Darstellungsweise, gewonnen.

Nur die einfachsten Sätze über symmetrische und ähnliche Functionen werden vorausgesetzt.

1. Wir beginnen mit der Feststellung einiger fundamentalen Begriffe.

Die aufzulösende Gleichung

$$F(x) = 0 \tag{1}$$

sei eine Gleichung n^{ten} Grades:

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n = 0,$$

*) Vgl. z. B. seinen Commentaire sur Galois in Math. Ann., Bd. I, p. 141.

**) In Liouville's Journal, I. sér. t. XI.

***) Dedekind, sur la théorie des nombres entiers algébriques, § 15., insb. Ende von § 16.; vgl. auch Vorl. über Zahlentheorie von Dirichlet, herausg. von Dedekind, 3. Aufl., Suppl. XI.

deren Coefficienten aus den rationalen Zahlen und irgend welchen gegebenen Grössen $A, B, C, \cdots$ auf rationale Weise d. i. mittels einer endlichen Anzahl von Additionen, Subtractionen, Multiplicationen und Divisionen zusammengesetzt, deren Wurzeln

$$\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{n-1}$$

aber von einander verschieden sind.

Jede Grösse, welche gleichfalls auf rationale Weise aus $A, B, C, \cdots$ und rationalen Zahlen entsteht, wird als rational bekannt bezeichnet.

Wenn im Laufe einer Untersuchung den ursprünglich gegebenen Grössen $A, B, C, \cdots$ andere $y, z, \cdots$ als bekannt hinzugefügt werden, so sagt man, *man adjungire diese der Gleichung*, und nennt sie *adjungirte Grössen.* Durch solche Adjunction wird der Begriff der rational bekannten Grössen verändert, indem nach derselben alle Grössen rational bekannt sind, welche aus $A, B, C, \cdots$ *und* $y, z, \cdots$ rational zusammengesetzt sind.

Eine ganze Function $f(x)$ oder die Gleichung $f(x) = 0$, deren Coefficienten aus irgend welchen Gegebenen rational zusammengesetzt sind, heisst *irreductibel*, wenn es unmöglich ist, $f(x)$ in Factoren geringeren Grades zu zerlegen, deren Coefficienten in demselben Sinne rational sind. Durch Adjunction neuer Grössen kann es sich ereignen, dass eine bis dahin irreductible Gleichung reductibel wird.

Es ist bekannt, dass, wenn eine irreductible Gleichung mit einer anderen in gleichem Sinne rationalen Gleichung *eine* Wurzel gemeinschaftlich hat, *alle* ihre Wurzeln dieser Gleichung genügen. *Zwei in demselben Sinne irreductible Gleichungen, welche eine Wurzel gemeinsam haben, müssen folglich identisch mit einander sein.*

Ein System von Zahlen, die nicht sämmtlich verschwinden und die Eigenschaft haben, dass Summe, Differenz, Product und Quotient irgend zweier, seien sie verschieden oder identisch mit einander, wieder Zahlen des Systems sind, wird nach Herrn Dedekind's Vorgange *ein Zahlenkörper* genannt.

Solchen Körper bilden z. B. in jedem Momente der Untersuchung die rational bekannten Grössen.

Dasselbe gilt, wenn ξ eine Wurzel der irreductibeln Gleichung $f(x) = 0$ und m der Grad dieser Gleichung ist, von den rationalen Functionen von ξ oder auch von den sämmtlichen Grössen

$$A_0 + A_1\xi + A_2\xi^2 + \cdots + A_{m-1}\xi^{m-1}, \tag{2}$$

bei denen $A_0, A_1, \cdots, A_{m-1}$ in demselben Sinne rational sind, wie die Coefficienten der Gleichung. *Ein Körper dieser Art soll kurz ein irreductibler (aus ξ erzeugter) Körper vom Grade m genannt werden.* Da jeder Wurzel der Gleichung ein solcher Körper entspricht, erhält man im Ganzen m der Gleichung entsprechende Körper, welche *zu einander conjugirt* heissen.

Satz I. *Damit die conjugirten Körper* — was die Gesammtheit der in ihnen enthaltenen Zahlen betrifft — *mit einander identisch sind, ist nothwendig und hinreichend, dass jede Wurzel der irreductibeln Gleichung durch jede andere rational ausdrückbar sei.*

Denn, enthalten die den Wurzeln ξ, ξ' entsprechenden Körper dieselben Zahlen, gehören also die Grössen

$$A_0' + A_1'\xi' + A_2'\xi'^2 + \cdots + A_{m-1}' \cdot \xi'^{m-1} \tag{3}$$

für alle rational bekannten Werthe der Coefficienten A' zu den Grössen (2), so findet sich unter diesen auch ξ' selbst; und unter derselben Voraussetzung auch ξ im Körper der Grössen (3). — Umgekehrt, wenn ξ' rational durch ξ ausdrückbar ist, wird jede Zahl (3) zum Körper der Zahlen (2), desgleichen, wenn auch ξ rational ausdrückbar ist durch ξ', jede Zahl dieses Körpers zum Körper der Zahlen (3) gehören, beide Körper also identisch mit einander sein.

Der Körper der Zahlen (2) soll *ein Normalkörper* heissen, wenn er mit den zu ihm conjugirten identisch ist.

2. Die allgemeinste Frage nun, welche man sich bezüglich der Auflösung der Gleichungen stellen kann, ist diese: *durch welche (algebraische) Grössen kann eine gegebene Gleichung gelöst, d. h. können ihre Wurzeln rational ausgedrückt werden?* Zu ihrer Beantwortung wird man versuchen müssen, der Gleichung successive geeignete Grössen $y, z, \cdots$ zu adjungiren der Art, dass schliesslich ihre Wurzeln rational bekannt werden. Um aber diese Operation richtig zu leiten, wird man vor Allem klar zu stellen haben, welche Grössen denn von vornherein zu den rational bekannten gehören.

Die Coefficienten der Gleichung (1) sind bekanntlich bis auf die Vorzeichen gleich den einfachsten symmetrischen Functionen ihrer Wurzeln $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$, und jede rationale *symmetrische* Function der Wurzeln ist rational durch sie ausdrückbar.

Ist nun (1) die *allgemeine* Gleichung n^{ten} Grades, so sind die Coefficienten $a_1, a_2, \cdots, a_n$ Unbestimmte und sie allein die Gegebenen. In diesem Falle sind die genannten Functionen der Wurzeln auch die einzigen Wurzelfunctionen, welche rational bekannt sind; denn eine Gleichung

$$\varphi(\alpha_0, \alpha_1, \cdots, \alpha_{n-1}) = \psi(a_1, a_2, \cdots, a_n),$$

in welcher φ, ψ rationale Functionen der Argumente bezeichnen, kann, ohne identisch zu sein, nicht bestehen, da die Wurzeln, ebenso wie die Coefficienten, Unbestimmte bezeichnen, kann aber nur dann identisch sein, wenn φ sich, ebenso wie ψ, *symmetrisch* aus den Wurzeln zusammensetzt.

Dagegen ist klar, dass eine solche Beziehung zwischen den Wurzeln einer Gleichung und ihren Coefficienten, wenn diese bestimmte

Werthe haben, oder von bestimmt Gegebenen $A, B, C, \ldots$ abhängen, sehr wohl möglich ist, und können dann folglich auch ausser den symmetrischen Functionen der Wurzeln noch andere Gattungen rationaler Wurzelfunctionen existiren, welche als bekannt anzusehen sind. Auch leuchtet ein, dass dieser Gattungen stets neue auftreten können, wenn durch Adjunction geeigneter Grössen der Umfang der Gegebenen erweitert wird.

Hieraus ist ersichtlich, dass wir unsere Untersuchung auf die Betrachtung aller rationalen Functionen von den Wurzeln $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$, deren Coefficienten in den Gegebenen $A, B, C, \cdots$ rational sind, werden zu begründen haben. Diese bilden einen Körper, welcher K heisse.

Nun folgt bekanntlich aus dem Satze von den ähnlichen Functionen, dass jede rationale Wurzelfunction rational ausgedrückt werden kann durch eine solche Function, welche bei den Vertauschungen der n Wurzeln

$$N = 1 \cdot 2 \cdot 3 \cdots n$$

numerisch verschiedene Werthe erlangt. Eine Function dieser Art ist

$$\omega_0 = h_0\alpha_0 + h_1\alpha_1 + \cdots + h_{n-1}\alpha_{n-1}$$

für passende Werthe der h_i; setzt man nämlich z. B.

$$h_0 = 1,\ h_1 = h,\ h_2 = h^2, \cdots, h_{n-1} = h^{n-1},$$

so können zwei bestimmte der N *algebraisch* verschiedenen Werthe von ω_0 höchstens für $n-1$ Werthe von h einander *numerisch* gleich sein, und demnach giebt es nicht mehr als

$$(n-1) \cdot \frac{N(N-1)}{2}$$

verschiedene Werthe von h, für welche *irgend zwei* jener Ausdrücke numerisch gleich sein können. Für jeden anderen Werth von h müssen sie sämmtlich von einander verschieden sein, auch leuchtet ein, dass h sogar rational, ω_0 also im Körper K gewählt werden kann.

3. Diese verschiedenen Werthe von ω_0 sind Wurzeln einer Gleichung $P(x) = 0$, deren Coefficienten als symmetrische Functionen von $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$ rational bekannt sind. Die Function $P(x)$ wird jederzeit, mag man die Gleichung (1) in ihrem ursprünglichen Zustande oder nach Adjunction irgend welcher Grössen betrachten, wie leicht zu sehen, in irreductible Factoren *desselben Grades* zerfallen, weil ihre Wurzeln jede durch eine beliebige von ihnen rational ausdrückbar sind. Wir bezeichnen mit $G(x)$ denjenigen irreductibeln Factor von $P(x)$, welcher rational bekannte Coefficienten und die Wurzel ω_0 hat, seinen Grad mit g, und nennen

(4) $$\omega_0, \omega_1, \omega_2, \cdots, \omega_{g-1}$$

die Wurzeln der irreductibeln, sogenannten *Galois'schen Gleichung*

$$G(x) = 0. \tag{5}$$

Alsdann sind die Functionen des Körpers K, weil sie rational durch ω_0 ausdrückbar sind, offenbar sämmtlich gleich einer Zahl der folgenden Form:

$$C_0 + C_1\omega_0 + C_2\omega_0^2 + \cdots + C_{g-1}\omega_0^{g-1}, \tag{6}$$

in welcher die Coefficienten rational bekannt sind; und umgekehrt repräsentirt jede Zahl dieser Form den Werth einer Function des Körpers K. Diese Zahlen bilden wieder einen Körper G, welcher *der Galois'sche Körper der Gleichung* (1) genannt werden soll. *Die Zahl g heisse sein Grad; sie muss nach der über $P(x)$ gemachten Bemerkung stets ein Theiler von N sein.*

Der Galois'sche Körper ist ein Normalkörper, weil (Satz I.) jede der Functionen $\omega_0, \omega_1, \cdots, \omega_{g-1}$ durch eine beliebige von ihnen rational ausdrückbar ist. Setzt man, dieser Bemerkung entsprechend, indem man mit $\Theta_0, \Theta_1, \cdots, \Theta_{g-1}$ rationale Functionen bezeichnet, die Wurzeln der Gleichung (5) in die Form:

$$\omega_0 = \Theta_0(\omega_0), \quad \omega_1 = \Theta_1(\omega_0), \cdots, \omega_{g-1} = \Theta_{g-1}(\omega_0),$$

so ist, wenn ω *irgend eine* Wurzel von (5) bedeutet, für jeden Werth i aus der Reihe $0, 1, 2, \cdots, g-1$ auch $\Theta_i(\omega)$ eine Wurzel; denn wegen der Irreductibilität der Gleichung (5) wird die rationale Gleichung $G[\Theta_i(x)] = 0$, weil sie die Wurzel ω_0 mit jener gemein hat, durch jede Wurzel ω derselben erfüllt, und demnach

$$G[\Theta_i(\omega)] = 0.$$

Wegen der Irreductibilität der Gleichung (5) wird ferner eine Function

$$u_0 = C_0 + C_1\omega_0 + C_2\omega_0^2 + \cdots + C_{g-1}\cdot\omega_0^{g-1}$$

des Körpers K dann und nur dann von vornherein bekannt sein, wenn $C_1 = C_2 \cdots = C_{g-1} = 0$ ist. Ihr Werth bleibt daher ungeändert, wenn irgend eine der Grössen (4) statt ω_0 gesetzt wird; wie denn auch umgekehrt eine Function u_0, welche bei diesen Substitutionen sich nicht ändert, als symmetrische Function der Grössen (4) dargestellt werden kann, also durch die bekannten Grössen rational ausdrückbar ist. Die Werthe dieser Functionen bilden einen in G enthaltenen Körper C, *den Körper der (ursprünglich) bekannten Functionswerthe*, die Substitutionen aber, welche die Werthe (4) aus ω_0 hervorbringen, *die Gruppe der Gleichung* (1) (Galois).

4. Nunmehr betrachten wir eine Function u_0 des Körpers K, deren Werth dem Körper C nicht angehört. Die g Werthe derselben, welche den Substitutionen der Gruppe entsprechen, werden einer Gleichung $\Pi(x) = 0$ Genüge leisten, deren Coefficienten als unveränderliche Functionen rational bekannt sind. Mit $\Gamma(x)$ bezeichnen wir denjenigen

irreductibeln Factor von $\Pi(x)$, welchem die Wurzel u_0 zukommt, mit γ seinen Grad, und nennen

$$u_0, u_1, u_2, \cdots, u_{\gamma-1}$$

die Wurzeln der irreductibeln Gleichung

$$\Gamma(x) = 0. \tag{7}$$

Die Function u_0 kann rational durch ω_0 dargestellt werden, was in der Gleichung $u_0 = \psi(\omega_0)$ ausgedrückt werde. Aus der rationalen Beziehung

$$\Gamma(u_0) = \Gamma\psi(\omega_0) = 0$$

folgt aber wegen der Irreductibilität der Gleichung (5), dass die sämmtlichen Grössen

$$\psi\Theta_0(\omega_0), \quad \psi\Theta_1(\omega_0), \cdots, \psi\Theta_{g-1}(\omega_0)$$

Wurzeln der Gleichung (7) sind. Angenommen nun, unter diesen seien mehrere, etwa die ersten h, gleich u_0, und folglich

$$\psi\Theta_0(\omega_0) = \psi\Theta_1(\omega_0) = \cdots = \psi\Theta_{h-1}(\omega_0), \tag{8}$$

so bestehen diese Relationen auch für jede andere Wurzel ω der Gleichung (5):

$$\psi\Theta_0(\omega) = \psi\Theta_1(\omega) = \cdots = \psi\Theta_{h-1}(\omega). \tag{9}$$

Die h Wurzeln

$$\Theta_0(\omega), \quad \Theta_1(\omega), \cdots, \Theta_{h-1}(\omega) \tag{10}$$

der Gleichung (5) sind aber erstens untereinander verschieden, weil z. B. aus der Gleichheit $\Theta_1(\omega) = \Theta_2(\omega)$ sich fälschlich $\Theta_1(\omega_0) = \Theta_2(\omega_0)$ ergäbe. Zweitens sind sie auch von den Wurzeln

$$\Theta_0(\omega_0), \quad \Theta_1(\omega_0), \cdots, \Theta_{h-1}(\omega_0) \tag{11}$$

sämmtlich verschieden, sobald es *eine* unter ihnen ist; denn, fände sich auch nur eine von ihnen unter den Wurzeln (11), so würden die sämmtlichen Grössen (9) gleich u_0, und demnach müssten die Wurzeln (10) sämmtlich zu den Wurzeln (11) gehören, welche nach der Voraussetzung *ausschliesslich* den Werth u_0 hervorbringen.

Hieraus ist zu schliessen, dass immer je h von den Wurzeln der Gleichung (5) dieselbe Wurzel der Gleichung (7) hervorbringen und dass folglich g ein Vielfaches von h, nämlich $g = \gamma h$ sein muss. Man gewinnt daher den Satz:

Satz II. *Eine jede Function des Körpers K, welche nicht selbst rational bekannt ist, genügt einer irreductibeln Gleichung mit rational bekannten Coefficienten, deren Grad ein Theiler von g ist.*

Zum Körper K gehören insbesondere die Wurzeln der Gleichung (1) selbst. Ist diese also irreductibel, so muss ihr Grad ein Theiler von g sein. Man findet daher den

Zusatz. *Der Grad des Galois'schen Körpers einer Gleichung vom Grade n ist theilbar durch n, wenn sie irreductibel ist.*

Der Wurzel u_0 der irreductibeln Gleichung (7) entspricht der Körper Γ aller Zahlen von der Form

$$C_0 + C_1 u_0 + C_2 u_0^2 + \cdots + C_{\gamma-1} \cdot u_0^{\gamma-1} \tag{12}$$

mit rational bekannten Coefficienten. Sie enthalten in sich die Zahlen des Körpers C und gehören selbst insgesammt zum Galois'schen Körper G der Gleichung (1).

5. Satz III. *Wird nun die Function u_0 der Gleichung* (1) *adjungirt, so erweitert sich der Körper der rational bekannten Functionswerthe, der ursprünglich C ist, zum Körper* Γ. Gleichzeitig aber wird die bisher irreductible Galois'sche Gleichung reducirt; denn die nach Adjunction von u_0 rationale Gleichung

$$\psi(x) - u_0 = 0 \tag{13}$$

hat, wie gezeigt, nur noch die h Wurzeln

$$\Theta_0(\omega_0), \quad \Theta_1(\omega_0), \quad \cdots, \quad \Theta_{h-1}(\omega_0)$$

mit der Gleichung (5) gemeinschaftlich. Nennt man also

$$\mathfrak{G}(x, u_0)$$

denjenigen in u_0 irreductibeln Factor von $G(x)$, welchem die Wurzel ω_0 zukommt, so ist die Gleichung

$$\mathfrak{G}(x, u_0) = 0 \tag{14}$$

vom Grade $\mathfrak{g} = h$.

Denn zunächst kann ihr Grad $\mathfrak{g}$ nicht grösser sein als h, weil sonst die Gleichung (13) mehr als h Wurzeln mit der Gleichung (5) gemeinsam haben müsste. Andererseits erhält man, wenn u eine Unbestimmte bedeutet, indem man $G(x)$ durch $\mathfrak{G}(x, u)$ theilt, eine Gleichung von der Form:

$$G(x) = \mathfrak{G}(x, u) \cdot Q(x, u) + R(x, u),$$

worin Q und R ganze Functionen von x und u bezeichnen, deren letztere bezüglich x von kleinerem Grade ist als $\mathfrak{G}$. Man findet hieraus die Identität

$$R(x, u_0) = 0,$$

weil diese Beziehung durch jede Wurzel von (14) erfüllt werden muss; d. h. die Coefficienten von $R(x, u)$ verschwinden sämmtlich für $u = u_0$ und folglich wegen der Irreductibilität der Gleichung (7) auch für $u = u_1, u_2, \cdots, u_{\gamma-1}$. Hieraus folgt, dass $G(x)$ durch jede der Functionen

$$\mathfrak{G}(x, u_0), \quad \mathfrak{G}(x, u_1), \quad \cdots, \quad \mathfrak{G}(x, u_{\gamma-1})$$

theilbar ist. Das Product dieser Functionen ist aber eine ganze Function von x vom Grade $\mathfrak{g}\gamma$, deren Coefficienten als symmetrische Functionen der Wurzeln von (7) in den Zahlen des Körpers C rational sind, und welche, weil sie mit der in demselben Sinne rationalen und irreductibeln Function $G(x)$ gemeinsame Wurzeln hat, durch diese

Function vom Grade $h\gamma$ theilbar ist. Da folglich $\mathfrak{g} \gtreqless h$, so findet sich durch Vergleichung mit der bereits erlangten Beziehung $\mathfrak{g} \lesseqgtr h$, wie behauptet, $\mathfrak{g} = h = \frac{g}{\gamma}$.

Satz IV. *Durch Adjunction von u_0 wird demnach die ursprüngliche Galois'sche Gleichung vom Grade g durch die neue Galois'sche Gleichung* (14) *nur noch vom Grade $\frac{g}{\gamma}$, und folglich der ursprüngliche Galois'sche Körper der Gleichung* (1) *vom Grade g durch einen neuen nur noch vom Grade $\frac{g}{\gamma}$ ersetzt, dessen Coefficienten die Zahlen des Körpers Γ sind.*

Werden mehrere Functionen des Körpers K, z. B.

$$u_0', u_0'', \cdots, u_0^{(m)} \tag{15}$$

adjungirt, so kommt dies auf die Adjunction einer einzigen passend gewählten Function dieses Körpers zurück. Denn in dem Ausdrucke

$$u_0 = h_1 u_0' + h_2 u_0'' + \cdots + h_m u_0^{(m)}$$

lassen sich für die h_i (vgl. Nr. 2.) rationale Werthe so wählen, dass bei jeder Vertauschung der Wurzeln, welche wenigstens eine der Functionen verändert, auch u_0 sich ändert; während natürlich u_0 ungeändert bleibt, sobald die Functionen (15) gleichzeitig ihren Werth behalten. Der so bestimmten Function u_0 sind also sämmtliche Functionen (15) ähnlich und können demnach durch u_0 rational ausgedrückt werden. Der Körper, welcher in rationaler Weise aus den Grössen (15) entsteht, muss daher identisch sein mit demjenigen, der in gleicher Weise aus u_0 hervorgebracht wird.

6. Sei jetzt Γ ein beliebiger in G enthaltener Körper (doch wird stillschweigend vorausgesetzt, dass Γ von C und von G selbst verschieden sei), dessen Glieder, wie alle in G enthaltenen, die Werthe von Functionen des Körpers K bezeichnen.

Wir wollen die Grössen (15) *unabhängig von einander nennen, wenn eine Gleichung*

$$k_1 u_0' + k_2 u_0'' + \cdots + k_m \cdot u_0^{(m)} = 0$$

mit rational bekannten Coefficienten nur dann bestehen kann, wenn die letztern gleich Null sind.

Demgemäss wird man im Körper Γ eine gewisse grösste Anzahl, welche g nicht erreicht, von unabhängigen Gliedern $u_0', u_0'', \cdots, u_0^{(m)}$ angeben können der Art, dass jedes andere Glied U von Γ in der Form

$$U = k_1 u_0' + k_2 u_0'' + \cdots + k_m u_0^{(m)} \tag{16}$$

mit rational bekannten Coefficienten darstellbar ist. Denn da die Grössen (15) dem Körper G angehören, erhält man m Gleichungen von der Form:

$$u_0' = C_0' + C_1'\omega_0 + \cdots + C_{g-1}' \cdot \omega_0^{g-1}$$
$$u_0'' = C_0'' + C_1''\omega_0 + \cdots + C_{g-1}'' \cdot \omega_0^{g-1}$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$u_0^{(m)} = C_0^{(m)} + C_1^{(m)}\omega_0 + \cdots C_{g-1}^{(m)} \cdot \omega_0^{g-1},$$

welche gegen die Voraussetzung über die Grössen (15) nicht unabhängig sein könnten, wenn $m > g$ wäre, für $m = g$ aber, da sie unabhängig von einander sein sollen, gestatten würden, ω_0 und damit den gesammten Körper G in der Form (16) auszudrücken d. i. dem Körper Γ einzuverleiben.*)

Ersetzt man nun die Functionen (15) nach dem in voriger Nr. Bemerkten durch eine einzige Function u_0, welche, wie gezeigt worden, einer gewissen irreductibeln Gleichung $\Gamma(x) = 0$ vom Grade γ genügt, deren Coefficienten in den Zahlen des Körpers C rational sind, so wird der Körper Γ identisch mit dem Körper der Zahlen von der Form (12). Demnach ist $m = \gamma$; denn die sämmtlichen Zahlen dieses Körpers sind durch die γ unabhängigen Grössen

$$1, u_0, u_0^2, \cdots, u_0^{\gamma-1}$$

in jener Form mit rational bekannten Coefficienten darstellbar.

Dies Resultat lässt sich folgendermassen aussprechen:

Satz V. *Zu jedem in G enthaltenen Körper Γ gehört eine Function u_0 des Körpers K von der Art, dass Γ als ein aus u_0 gebildeter irreductibler Körper dargestellt werden kann.*

Dies vorausgeschickt, nehmen wir an, Γ sei ein in G enthaltener Normalkörper, welcher selbst keinen Normalkörper weiter umfasst.

Die Wurzeln

$$u_0, u_1, \cdots, u_{\gamma-1}$$

der irreductibeln Gleichung $\Gamma(x) = 0$, deren jede den Körper Γ hervorbringt, sind alsdann (nach Satz I.) rational durch u_0 ausdrückbar; und weil Gleiches von jeder rationalen Function der Wurzeln $u_0, u_1, \cdots u_{\gamma-1}$ der Gleichung $\Gamma(x) = 0$ gilt, ist Γ mit dem Galois'schen Körper dieser Gleichung identisch.

Letzterer kann demnach keinen Normalkörper enthalten. Denn sonst gäbe es eine rationale Function der Grössen $u_0, u_1, \cdots, u_{\gamma-1}$:

$$t = \psi(u_0, u_1, \cdots, u_{\gamma-1}),$$

welche zu ihm gehört und einer irreductibeln Gleichung $\Gamma'(x) = 0$ genügt, deren Wurzeln rational unter einander ausdrückbar sind. Dieselbe Function t ist aber auch eine gewisse in K enthaltene Function von $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$, und wegen der genannten Eigenschaften derselben würde, wenn sie der Gleichung (1) adjungirt wird, der Körper der rational bekannten Functionswerthe sich (nach Satz III.) zu dem aus t gebildeten Normalkörper erweitern, dieser aber gegen die Voraus-

*) Vgl. Vorl. üb. Zahlenth. v. Dirichlet, 3. Aufl., p. 466.

setzung in Γ enthalten sein, da t selbst, als rationale Function von u_0 darstellbar, diesem Körper angehört.

Die Betrachtungen der letzten drei Nummern, welche wir zunächst auf den ursprünglichen Zustand der Gleichung (1) bezogen haben, werden offenbar ihre Gültigkeit auch dann behalten, wenn sie auf einen Augenblick bezogen werden, in welchem derselben bereits eine oder mehrere Functionen des Körpers K adjungirt worden sind.

7. Wir wollen eine irreductible Gleichung, deren Wurzeln rational unter einander abhangen und für welche der Galois'sche Körper keinen Normalkörper enthält, hinfort kurz *eine einfache Gleichung* (C. Jordan) nennen. Bei solcher Ausdrucksweise lehren die vorausgeschickten Betrachtungen den Satz, *dass die Auflösung jeder Gleichung auf die von einfachen Gleichungen zurückführbar ist.*

Denn zuvörderst darf offenbar die gegebene Gleichung (1) als irreductibel vorausgesetzt werden, widrigenfalls man nur jeden ihrer irreductibeln Factoren successive gleich Null zu setzen und in der nachfolgenden Weise zu behandeln hätte.

Enthält nun der Galois'sche Körper G der Gleichung (1) einen Normalkörper, so wird man diesen, wie leicht einzusehen, stets so wählen können, dass er selbst keinen Normalkörper weiter enthält. Eine zu diesem Körper Γ gehörige Function u_0 von den Wurzeln der Gleichung (1) leistet dann einer einfachen Gleichung $\Gamma(x) = 0$ Genüge, und ihre Adjunction d. i. die Auflösung dieser Gleichung erweitert den Körper C der ursprünglich bekannten Functionswerthe zum Körper Γ, indem sie gleichzeitig die ursprüngliche Galois'sche Gleichung $G(x) = 0$ vom Grade g durch eine neue

$$\mathfrak{G}(x, u_0) = 0$$

vom kleineren Grade $\mathfrak{g} = \frac{g}{\gamma}$ ersetzt. Der Galois'sche Körper der Gleichung (1) ist nunmehr identisch mit der Gesammtheit der Zahlen von der Form

$$\Gamma_0' + \Gamma_1'\omega_0 + \Gamma_2'\omega_0^2 + \cdots + \Gamma_{\mathfrak{g}-1}'\cdot\omega_0^{\mathfrak{g}-1},$$

worin die Coefficienten die Zahlen des Körpers Γ bedeuten.

Enthält jener Körper wieder noch einen Normalkörper in sich, so kann man mittels derselben Betrachtung eine neue einfache Gleichung $\Gamma'(x) = 0$ vom Grade γ' einführen, bei deren Auflösung die neue Galois'sche Gleichung durch eine dritte von noch kleinerem Grade $\mathfrak{g}' = \frac{\mathfrak{g}}{\gamma'}$ ersetzt wird; und kann solange in gleicher Weise fortfahren, als der neue Galois'sche Körper noch einen Normalkörper enthält. Da die Grade der Galois'schen Gleichungen aber nicht ohne Ende abnehmen können, muss endlich der Fall eintreten, dass der Galois'sche Körper keinen Normalkörper mehr enthält; dann ist aber die ent-

sprechende Galois'sche Gleichung selbst eine einfache, und durch ihre Auflösung werden alle Functionen, welche der Körper K enthält, bekannt und die Gleichung (1) aufgelöst.

Hieraus entnehmen wir das wichtige Princip, dass es, statt einer gegebenen Gleichung die Wurzeln einer *beliebigen* anderen zu adjungiren, genügen wird, ihr successive die Wurzeln der *einfachen* Gleichungen zu adjungiren, auf deren Auflösung diese letztere zurückkommt. Wenn wir uns demnach jetzt die Frage stellen, welche Wirkung es auf die Gleichung (1) habe, wenn wir ihr die Wurzeln irgend einer anderen Gleichung adjungiren, so dürfen wir diese letztere als einfach voraussetzen.

8. Es sei in irgend einem Momente der Untersuchung C' der Körper der rational bekannten Functionswerthe, G' der Galois'sche Körper der Gleichung (1), und

$$G'(x) = 0$$

die entsprechende Galois'sche Gleichung vom Grade g'. Wir bezeichnen mit

$$\varphi(x) = 0 \tag{17}$$

eine Gleichung vom Grade p mit gegenwärtig rational bekannten Coefficienten, und ihre Wurzeln mit

$$\beta_1, \beta_2, \cdots, \beta_{p-1}.$$

Dieser Gleichung entspricht dann eine gewisse Galois'sche Gleichung

$$H(x) = 0$$

vom Grade q und ein Galois'scher Körper, welcher H heisse.

Die Körper G' und H werden gewisse Glieder gemeinschaftlich haben, welche, nach der Natur der Zahlenkörper, in ihrer Gesammtheit einen besonderen Körper Γ (den grössten gemeinschaftlichen Theiler von G' und H — Dedekind —) bilden. Seine Glieder repräsentiren die Werthe derjenigen Functionen von den Wurzeln der Gleichung (1), welche *auch* als rationale Functionen von den Wurzeln der Gleichung (17) mit rational bekannten Coefficienten dargestellt werden können, und daher nach Auflösung dieser Gleichung rational bekannt werden. Ist demnach der Körper Γ, welcher C' nothwendig in sich enthält, von C' verschieden, so kann er, als in G' enthalten, nach Satz V. durch eine Function u_0 von den Wurzeln der Gleichung (1) hervorgebracht werden, welche einer, in den Zahlen des Körpers C' rationalen und gegenwärtig irreductibeln Gleichung $\Gamma(x) = 0$ vom Grade γ genügt, und folglich sind die Glieder des Körpers Γ identisch mit der Gesammtheit der Zahlen von der Form:

$$C_0' + C_1' u_0 + C_2' u_0^2 + \cdots + C_{\gamma-1}' \cdot u_0^{\gamma-1},$$

in welcher die Coefficienten rational bekannt sind.

Nun sind die Wurzeln der Gleichung $\Gamma(x) = 0$ *einerseits* verschiedene Werthe der Function u_0 von den Wurzeln $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$. *Andererseits* sind die Glieder des Körpers Γ, insbesondere auch u_0 selbst in H enthalten, also mittels $\beta_0, \beta_1, \cdots, \beta_{p-1}$ rational ausdrückbar; und da $\Gamma(x) = 0$ die irreductible Gleichung mit rational bekannten Coefficienten ist, der u_0 genügt, so sind deren Wurzeln auch verschiedene Werthe von u_0 als einer Function von den Wurzeln $\beta_0, \beta_1, \cdots, \beta_{p-1}$, sie sind also selbst rationale Functionen dieser Wurzeln und demnach sämmtlich Glieder des Körpers Γ und können eine jede, so gut wie u_0, benutzt werden, um diesen Körper zu erzeugen.

Das heisst aber nichts Anderes, als dass Γ ein — in G' sowohl, wie in H — enthaltener *Normalkörper* ist.

Indem man nun die Gleichung (17) auflöst, erweitert man nach der Voraussetzung den Körper C' zum Körper Γ d. h. man adjungirt die Function u_0 oder löst die Gleichung $\Gamma(x) = 0$ auf. Hierdurch aber wird nach Satz IV. der Grad des Galois'schen Körpers G' der Gleichung (1) auf $g'' = \frac{g'}{\gamma}$ erniedrigt. Und da der Körper Γ und die Gleichung $\Gamma(x) = 0$ zur Gleichung (17) in demselben Verhältniss stehen, wie zur Gleichung (1), wird die Auflösung der letztern den Grad des Galois'schen Körpers H der Gleichung (17) auf $q' = \frac{q}{\gamma}$ reduciren. Man findet hieraus:

Satz VI. *Wenn die Auflösung der Gleichung* (17) *den Grad g' des Galois'schen Körpers von* (1) *auf g'' erniedrigt, so erniedrigt umgekehrt die Auflösung dieser Gleichung den Grad q des Galois'schen Körpers jener auf q', in der Weise, dass*

$$\frac{g'}{g''} = \frac{q}{q'}$$

ist.

9. Wird nun die bisher beliebige Gleichung (17) als einfach vorausgesetzt, so enthält H als Galois'scher Körper derselben keinen Normalkörper ausser sich selbst, und folglich muss dann Γ mit H identisch sein. Hieraus folgt einerseits, dass jedes Glied von H, insbesondere jede Wurzel der Gleichung (17) eine zu G' gehörige Zahl d. i. eine Function der Wurzeln $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$ ist; andererseits muss $\gamma = q$, und da bei einfachen Gleichungen (vgl. Nr. 6.) der Grad des Galois'schen Körpers gleich dem der Gleichung ist, $\gamma = p$ sein. Man gewinnt folglich den wichtigen

Satz VII. *Der Körper der rational bekannten Functionswerthe einer Gleichung kann durch Auflösung einer einfachen Gleichung nur dann sich erweitern, wenn die Wurzeln der letzteren rationale Functionen von den Wurzeln der ersteren sind. Bei eintretender Erweiterung wird*

der Grad der Galois'schen Gleichung in der Weise reducirt, dass er durch den Grad der einfachen Gleichung getheilt wird.

Versetzen wir uns demgemäss in einen Augenblick, in welchem der Gleichung (1) bereits eine oder mehrere Functionen des Körpers K adjungirt sein können, so werden, bei Beibehaltung der obigen Bezeichnungen, die Functionen des Körpers K sämmtlich durch die Zahlen von der Form

$$C_0' + C_1'\omega_0 + C_2'\omega_0^2 + \cdots + C_{g'-1}'\cdot\omega_0^{g'-1}$$

repräsentirt sein, in welcher die C_i' die Zahlen des Körpers C' sind, und werden es solange auch bleiben, als die Adjunction anderer Grössen den Körper C' der rational bekannten Functionen nicht erweitert, insbesondere also solange nur solche Hilfsgleichungen aufgelöst werden, deren Wurzeln nicht rationale Functionen von den Wurzeln der gegebenen sind. Wird aber durch Auflösung einer einfachen Gleichung (17) vom Grade p, deren Coefficienten von den zuvor Adjungirten abhängig sein können, der Körper C' zu einem in G' enthaltenen Normalkörper Γ erweitert, so wird offenbar dasselbe auch ohne die Hilfsgleichungen durch Adjunction einer Function u_0 des Körpers K geleistet, welche einer *in den Zahlen des Körpers C' rationalen und vor Auflösung der letzten Hilfsgleichung irreductibeln* Gleichung $\Gamma(x) = 0$ vom Grade $\gamma = p$ genügt.

Und diese Bemerkung lässt sich nunmehr auf jeden spätern Moment der Untersuchung übertragen.

10. Da wir für diese Untersuchung uns vorgesetzt haben, die Bedingung für die algebraische Auflösbarkeit einer Gleichung von einem Primzahlgrade zu bestimmen, beschränken wir uns nun auf die Betrachtung derjenigen Gleichungen, welche nach Herrn Kronecker's Vorgange Abel'sche Gleichungen genannt werden und durch den Umstand charakterisirt sind, dass, wenn ihre Wurzeln in bestimmter Weise cyklisch geordnet werden, eine jede von ihnen die gleiche rationale Function von der vorhergehenden ist. Die Theorie derselben*) wird hier als bekannt vorausgesetzt und nur in Erinnerung gebracht, dass eine Abel'sche Gleichung, deren Grad eine zusammengesetzte Zahl ist, auf andere von Primzahlgraden zurückgeführt werden kann. Letztere aber sind einfache Gleichungen; denn, da der Grad ihres Galois'schen Körpers (vgl. Ende von Nr. 6.) ihrem Grade selbst gleich also eine Primzahl ist, kann kein anderer Körper in Letzterem enthalten sein ausser dem der rational bekannten Functionswerthe.

Dies vorausgeschickt, sei p eine Primzahl, ξ eine Wurzel der Gleichung

*) Abel, mémoire sur une classe particulière d'équations résolubles algébriquement, O. compl. I, p. 114, sowie auch Cr. J. Bd 4, p. 26.

$$\frac{x^p-1}{x-1}=0, \tag{18}$$

und $\gamma_0, \gamma_1, \cdots, \gamma_{p-1}$ die Wurzeln der Gleichung

$$x^p = A, \tag{19}$$

in welcher A rational bekannt. Da man jene p Wurzeln in solcher Weise wählen kann, dass

$$\gamma_1 = \xi \cdot \gamma_0,\ \gamma_2 = \xi \cdot \gamma_1, \cdots, \gamma_0 = \xi \cdot \gamma_{p-1}$$

und folglich jede von ihnen dieselbe, nach Adjunction von ξ rationale Function der vorhergehenden ist, wie die erste von der letzten, so ist *die binomische Gleichung* (19) *nach Adjunction von* ξ *eine Abel'sche Gleichung;* dasselbe gilt aber bekanntlich von der Kreistheilungsgleichung (18), und demnach kann man mit Beachtung der vorausgeschickten Bemerkung sagen, dass die Ausziehung einer Wurzel von einem Primzahlgrade, folglich offenbar jede Wurzelausziehung und demnach auch die Lösung jeder durch Wurzelausziehungen auflösbaren Gleichung auf eine Reihe von Abel'schen Gleichungen von Primzahlgraden zurückführbar ist.

Da umgekehrt jede Abel'sche Gleichung algebraisch auflösbar ist, gewinnt man zunächst das Resultat: *Eine Gleichung ist dann und nur dann algebraisch auflösbar, wenn sie durch Abel'sche Gleichungen von Primzahlgraden auflösbar ist.*

Verfolgen wir nun die Phasen der Auflösung bei einer algebraisch lösbaren Gleichung (1), wie sie den successive aufzulösenden Abel'schen Gleichungen von Primzahlgraden entsprechen!

Nachdem möglicherweise die Auflösung einer oder mehrerer solcher Gleichungen den Körper der bekannten Functionswerthe und folglich die Gestalt des Galois'schen Körpers der Gleichung (1) nicht verändert, sei $\varphi(x) = 0$ eine Abel'sche Gleichung vom Primzahlgrade p, deren Auflösung jenen Körper zum Körper Γ erweitert. Nach Nr. 8. ist Γ ein Normalkörper und kann diese Erweiterung (vor. Nr.) auch ohne die Hilfsgleichungen geleistet werden durch Adjunction einer Function u_0 des Körpers K, welche einer irreductibeln Gleichung $\Gamma(x) = 0$ des Grades $\gamma = p$ mit rational bekannten Coefficienten genügt; diese Gleichung ist aber eine Abel'sche Gleichung, da ihre Wurzeln rational von einander abhängig sein müssen und ihr Grad eine Primzahl ist. Da nunmehr und in jedem folgenden Stadium der Untersuchung dieselbe Betrachtung sich wiederholen lässt, so erkennt man, *dass die Wurzeln der sämmtlichen Abel'schen Gleichungen, die zur Lösung der gegebenen dienen, als Functionen des Körpers K vorausgesetzt werden dürfen.*

Sind $\gamma', \gamma'', \gamma''', \cdots$ die Grade dieser successiven Abel'schen Gleichungen, $\Gamma', \Gamma'', \Gamma''', \cdots$ die Normalkörper, zu denen sie allmählich

den Körper C erweitern, so sind jene Zahlen auch die Grade dieser Körper, und *die Auflösung einer jeden Hilfsgleichung erniedrigt jedesmal (Satz VII.) den Grad der augenblicklichen Galois'schen Gleichung in der Weise, dass er durch den Grad der aufgelösten Gleichung getheilt wird.*

11. *Betrachten wir nunmehr eine algebraisch auflösbare irreductible Gleichung*

$$F(x) = 0 \tag{1}$$

vom Primzahlgrade n.

Der Grad g ihres ursprünglichen Galois'schen Körpers wird dann (Satz II., Zusatz) durch n theilbar sein, aber durch keine höhere Potenz von n, weil g in $1 \cdot 2 \cdot 3 \cdots n$ enthalten ist; und wird bei der successiven Auflösung derjenigen Abel'schen Gleichungen von Primzahlgraden, welche zur Auflösung der Gleichung (1) sich eignen, auch solange durch n theilbar bleiben, als keine dieser Gleichungen vom Grade n ist (s. vor. Nr.). Damit aber die Gleichung (1) schliesslich aufgelöst werde, muss der Grad der Galois'schen Gleichung bis auf 1 herabsinken; es muss also ein Augenblick eintreten, in welchem der Grad dieser Gleichung — sie heisse dann $G^{(i)}(x) = 0$, ihr Körper $G^{(i)}$, der gemeinsame Grad beider $g^{(i)}$ — noch durch n theilbar ist, bei Auflösung einer Abel'schen Gleichung $\Gamma(x) = 0$ vom Grade n jedoch durch eine andere $\mathfrak{G}(x) = 0$ mit dem Körper $\mathfrak{G}$ ersetzt wird, deren Grad $\mathfrak{g} = \frac{g^{(i)}}{n}$ nicht mehr durch n theilbar ist.

Vor dieser Auflösung muss die Gleichung (1) noch irreductibel sein; denn würde sie im Gegentheil schon bei Auflösung einer der früheren Abel'schen Gleichungen vom Primzahlgrade p reducirt, und nennten wir

$$u_0, u_1, \cdots, u_{p-1}$$

die Wurzeln derselben und $f(x, u_0)$ einen jetzt irreductibeln Factor von $F(x)$ von möglichst kleinem Grade, so würde $F(x)$, wie man leicht sieht (vgl. Nr. 4.), durch jede der Functionen

$$f(x, u_0), f(x, u_1), \cdots, f(x, u_{p-1})$$

theilbar, welche sämmtlich in gleichem Sinne irreductibel sein müssten, weil sie sämmtlich in u_0 rational wären und keinen in demselben Sinne rationalen Factor von geringerem Grade wie $f(x, u_0)$ enthalten könnten. Da das Product jener Factoren Coefficienten hätte, welche dem Körper der, vor Auflösung der Abel'schen Gleichung bekannten Werthe angehören, müsste es durch die zur selben Zeit irreductible Function $F(x)$ theilbar und offenbar eine Potenz von $F(x)$ sein, weil es keine anderen Wurzeln hat, wie $F(x)$ selbst. Man gewänne also eine Gleichung von der Form:

$$F(x)^\lambda = f(x, u_0) \cdot f(x, u_1) \cdots f(x, u_{p-1}).$$

Nun könnten zwei der irreductibeln Factoren nur entweder ohne gemeinsame Wurzeln oder gänzlich mit einander identisch sein; in der vorstehenden Gleichung müssten daher je λ Factoren einander gleich, folglich p ein Vielfaches von λ also $\lambda = 1$ und

$$F(x) = f(x, u_0) \cdot f(x, u_1) \cdots f(x, u_{p-1})$$

sein, was erfordert, dass die Primzahl n theilbar durch p, also $n = p$ wäre. Dann würde aber durch Auflösung jener Abel'schen Gleichung der vorstehenden Formel gemäss $F(x)$ in Linearfactoren zerlegt, die Gleichung (1) also aufgelöst, und der Grad $g^{(i)}$ könnte nicht mehr durch n theilbar sein.

Nach Auflösung der Gleichung $\Gamma(x) = 0$ aber kann $F(x)$ (nach Satz II., Zusatz) nicht mehr irreductibel sein, und folglich wird durch Wiederholung der eben angestellten Betrachtung, wenn $u_0, u_1, \cdots, u_{n-1}$ jetzt die Wurzeln der Gleichung $\Gamma(x) = 0$ bezeichnen, eine Gleichung von der Form

$$F(x) = f(x, u_0) \cdot f(x, u_1) \cdots f(x, u_{n-1})$$

d. i. eine Zerlegung von $F(x)$ in Factoren *ersten Grades* erhalten. Die Gleichung (1) wird also durch Adjungirung von u_0 aufgelöst. Da hiernach der Grad der Galois'schen Gleichung, welcher vorher $g^{(i)}$ war, durch Adjunction von u_0 auf 1 herabsinken muss, kann $g^{(i)}$ nur gleich n sein; dann ist aber der Körper $G^{(i)}$ vom Grade n identisch mit jedem der irreductibeln Körper, welche durch die Wurzeln $\alpha_0, \alpha_1, \cdots, \alpha_{n-1}$ der gegebenen Gleichung hervorgebracht werden. Mit andern Worten: ein jeder von diesen ist ein Normalkörper, folglich die Wurzeln der Gleichung (1) rational von einander abhängig und die Gleichung (1), weil ihr Grad eine Primzahl, eine Abel'sche Gleichung.

Damit also die Gleichung (1) *algebraisch auflösbar ist, muss sie nach Adjunction der Wurzeln einer gewissen Abel'schen Gleichung selbst eine solche werden.*

12. Hieraus lässt sich das Kriterium für die algebraische Auflösbarkeit der Gleichung (1), welches von Galois gegeben worden ist, folgendermassen herleiten.

Zur einfacheren Darstellung nehmen wir einmal an, es bedürfe, um die Gleichung (1) zu einer Abel'schen zu machen, der Auflösung nur zweier solcher Gleichungen. Die erste von ihnen sei

$$\Gamma'(x) = 0$$

mit den Wurzeln $u_0', u_1', \cdots, u'_{\gamma'-1}$, die andere, deren Coefficienten in u_0' rational sein können,

$$\Gamma''(x) = 0,$$

und ihre Wurzeln $u_0'', u_1'', \cdots, u''_{\gamma''-1}$. Nach Adjunction von u_0' und u_0'' reducirt sich die ursprüngliche Galois'sche Gleichung

$$G(x) = 0$$

vom Grade $n\gamma'\gamma''$ auf eine andere

$$G^{(2)}(x) = 0$$

vom Grade n, deren Wurzeln, wenn Θ eine rationale Function bedeutet, gleich

$$\omega_0, \Theta(\omega_0), \Theta^2(\omega_0), \cdots, \Theta^{n-1}(\omega_0) \tag{20}$$

gesetzt werden können; und die gegebene Gleichung wird dadurch zu einer Abel'schen, d. h. sie wird aufgelöst, wenn noch eine ihrer Wurzeln, etwa α_0, als bekannt angesehen wird.

Die gleichzeitige Adjunction von α_0, u_0', u_0'' ist daher gleichbedeutend mit der Adjunction von ω_0, und folglich ändert jede Substitution der Gruppe, weil sie ω_0 verändert, wenigstens eine der drei Grössen α_0, u_0', u_0''.

Da die Wurzeln (20) der Galois'schen Gleichung dieselben Werthe von u_0' und u_0'' hervorbringen (Nr. 4.), so ändert die Substitution, welche ω_0 in $\Theta(\omega_0)$ verwandelt, die Wurzel α_0, und zwar stellt sie, da sie erst nach n-maliger Wiederholung zu ω_0 zurückführt, und n eine Primzahl ist, offenbar eine cyklische Vertauschung zwischen den n Wurzeln vor, durch welche etwa

$$\alpha_0 \alpha_1 \alpha_2 \cdots \alpha_{n-1}$$

in

$$\alpha_1 \alpha_2 \alpha_3 \cdots \alpha_0$$

übergeht.

Nach Adjunction von α_0 allein würde aber die Gleichung $G(x) = 0$ auf eine andere

$$G_1(x) = 0$$

vom Grade $\gamma'\gamma''$ reducirt werden (Nr. 5.), deren Wurzeln, welche als rationale Functionen von ω_0 mit

$$\omega_0, \varphi'(\omega_0), \varphi''(\omega_0), \cdots, \chi(\omega_0), \cdots$$

bezeichnet werden können, denselben Werth von α_0 hervorbringen, mit andern Worten: die Substitutionen, welche ω_0 in $\varphi'(\omega_0)$, $\varphi''(\omega_0)$ $\cdots \chi(\omega_0), \cdots$ verwandeln, lassen α_0 ungeändert, vertauschen vielmehr nur die anderen Wurzeln und müssen u_0', u_0'' in ihre verschiedenen Werthe verwandeln.

Man kann demnach (Nr. 4.) die $n\gamma'\gamma''$ Wurzeln der Galois'schen Gleichung in der Weise ordnen:

$$\left\{\begin{array}{cccc|c|c} \omega_0, & \varphi'(\omega_0), \cdots & \chi(\omega_0), \cdots & \cdots \\ \Theta(\omega_0), & \Theta\varphi'(\omega_0), \cdots & \Theta\chi(\omega_0), \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \Theta^{n-1}(\omega_0), & \Theta^{n-1}\varphi'(\omega_0), \cdots & \Theta^{n-1}\chi(\omega_0), \cdots & \cdots \end{array}\right. \tag{21}$$

dass jeder Verticalreihe *einer* der Werthe von u_0'', insbesondere den Verticalreihen der ersten Abtheilung die einzelnen Wurzeln der letzten Abel'schen Hilfsgleichung, jeder der unterschiedenen Abtheilungen aber *einer* der Werthe von u_0' entspricht. Die Substitutionen also, welche z. B. die Glieder der zweiten Verticalreihe in einander verwandeln, sind diejenigen Substitutionen der Gruppe, welche u_1'' nicht ändern; sie müssen aber, da u_0'', u_1'' rational durch einander ausdrückbar sind, übereinstimmen mit denjenigen, welche u_0'' nicht verändern; es muss also z. B. $\Theta\varphi'(\omega_0)$ aus $\varphi'(\omega_0)$ entstehen durch die Substitution, welche ω_0 etwa in $\Theta^a(\omega_0)$ verwandelt, also

$$\Theta\varphi'(\omega_0) = \varphi'\Theta^a(\omega_0)$$

sein. Setzt man nun

$$\omega_0 = \omega(\alpha_0, \alpha_1, \cdots, \alpha_{n-1})$$
$$\varphi'(\omega_0) = \omega(\alpha_{y_0}, \alpha_{y_1}, \cdots, \alpha_{y_{n-1}}),$$

so findet sich

$$\Theta(\omega_0) = \omega(\alpha_1, \alpha_2, \cdots, \alpha_0)$$
$$\Theta\varphi'(\omega_0) = \omega(\alpha_{y_1}, \alpha_{y_2}, \cdots, \alpha_{y_0}),$$

desgleichen

$$\varphi'\Theta^a(\omega_0) = \omega(\alpha_{a+y_0}, \alpha_{a+y_1}, \cdots, \alpha_{a+y_{n-1}}),$$

wobei die Indices (mod. n) zu nehmen sind, und folglich die Beziehung

$$y_{z+1} = a + y_z (\text{mod. } n)$$

und allgemeiner

$$y_{z+b} = ab + y_z.$$

Hieraus aber folgt, wenn $z = 0$ gesetzt und dann b mit z bezeichnet und beachtet wird, dass $y_0 = 0$ sein muss,

$$y_z = a \cdot z.$$

Die Substitutionen also, welche ω_0 in $\varphi'(\omega_0)$, $\varphi''(\omega_0)$, ... verwandeln, haben sämmtlich die Form $\binom{z}{az}$ d. h. sie verwandeln den Index z in az, wenn a eine Zahl bedeutet, welche durch n nicht theilbar ist. Dem Schema (21) gemäss entstehen daher die Substitutionen der Gruppe, welche u_0' nicht verändern und der ersten Abtheilung entsprechen, indem Substitutionen von der Form $\binom{z}{az}$ mit den Wiederholungen der cyklischen Substitution $\binom{z}{z+1}$ zusammengesetzt werden, und haben demnach sämmtlich die lineare Form

$$\binom{z}{az+b}. \tag{22}$$

Die Substitutionen ferner, welche die Glieder der zweiten Abtheilung in einander verwandeln, sind diejenigen Substitutionen der Gruppe, welche u_1' nicht ändern, und müssen, da u_0', u_1' rational durch einander ausdrückbar sind, mit denjenigen übereinstimmen, welche der

ersten Abtheilung zugehören. Demnach entsteht z. B. $\Theta\chi(\omega_0)$ aus $\chi(\omega_0)$ durch eine lineare Substitution. Setzt man wieder

$$\chi(\omega_0) = \omega(\alpha_{y_0}, \alpha_{y_1}, \cdots, \alpha_{y_{n-1}})$$

also

$$\Theta\chi(\omega_0) = \omega(\alpha_{y_1}, \alpha_{y_2}, \cdots, \alpha_{y_s}),$$

so ergiebt sich hieraus eine Relation von der Form

$$y_{z+1} \equiv c \cdot y_z + d \pmod{n}$$

also

$$\begin{aligned} y_1 &\equiv d \\ y_2 &\equiv cd + d \\ &\cdots\cdots \\ y_z &\equiv c^{z-1}d + c^{z-2}d + \cdots + d, \end{aligned}$$

insbesondere

$$y_n \equiv d \cdot \frac{c^n - 1}{c - 1}$$

folglich, da $y_n \equiv y_0 \equiv 0$ ist, $c \equiv 1 \pmod{n}$ und

$$y_z \equiv d \cdot z.$$

Es entsteht daher auch jede der Grössen $\chi(\omega_0), \cdots$ mittelst einer Substitution von der Form $\binom{z}{dz}$ aus ω_0, und folglich sind auch die der zweiten, in gleicher Weise aber auch die den folgenden Abtheilungen entsprechenden Substitutionen d. h. die Substitutionen der Gruppe überhaupt sämmtlich von der Form (22).

Da endlich unsere Betrachtung offenbar unabhängig ist von den Voraussetzungen, welche wir, um die Darstellung zu vereinfachen, eingeführt haben, ergiebt sich

Der Galois'sche Satz: Damit eine irreductible Gleichung von einem Primzahlgrade algebraisch auflösbar ist, darf ihre Gruppe nur lineare Substitutionen enthalten.

*Es würde leicht sein, zu beweisen, dass diese Bedingung auch hinreichend ist**). Doch ziehen wir es vor, aus den vorstehenden Betrachtungen diejenige andere Form des Galois'schen Kriteriums herzuleiten, welche von Herrn Kronecker gegeben und als die geeignetere bezeichnet worden ist**).

13. Man kann die successive Adjunction je einer Wurzel der *i* Abel'schen Hilfsgleichungen, deren Grade $\gamma', \gamma'', \cdots, \gamma^{(i)}$ seien, durch die Adjunction einer einzigen Function U_0 ersetzen, welche (Nr. 4.) einer irreductibeln Gleichung

$$H(x) = 0$$

---

*) S. z. B. Serret, Handb. d. höheren Algebra, deutsch von Wertheim, 1868, Bd. 2, pag. 519.

**) Ebendas. pag. 535, oder auch Monatsber. d. B. Ak. 1853.

vom Grade $h = \gamma' \gamma'' \cdots \gamma^{(i)}$ Genüge leistet mit von vornherein bekannten Coefficienten. In dem Schema (21) wird dann jeder Verticalreihe *einer* der verschiedenen Werthe von U_0, welche die Wurzeln der genannten Gleichung sind, zugehören, die Glieder derselben Verticalreihe aber, wie gezeigt worden, durch die Wiederholungen der cyklischen Substitution $\binom{z}{z+1}$ aus einander entstehen; demnach bleiben die Wurzeln der Gleichung $H(x) = 0$ bei denselben Substitutionen der Gruppe ungeändert, können also eine jede durch eine beliebige von ihnen rational ausgedrückt werden.

Andererseits hatten die Substitutionen, welche ω_0 in $\varphi'(\omega_0)$, $\varphi''(\omega_0)$, $\cdots \chi(\omega_0)$, $\cdots$ verwandelten, sämmtlich die Form $\binom{z}{az}$ oder, wenn r eine primitive Wurzel (mod. n) bezeichnet, die folgende: $\binom{z}{r^m z}$. Dasselbe gilt offenbar auch von denjenigen Substitutionen, durch welche eine dieser Grössen in eine beliebige andere von ihnen verwandelt wird. Und wenn nun $\binom{z}{r^k z}$ diejenige dieser Substitutionen bedeutet, bei welcher m den kleinsten Werth k hat, und durch dieselbe geht einer der Werthe von U_0 — er heisse U — in einen anderen $U' = \psi(U)$ über, unter ψ eine rationale Function verstanden, so folgt leicht aus der Irreductibilität der Gleichung $H(x) = 0$, dass die Wiederholung der Substitution $\binom{z}{r^k z}$ die sämmtlichen Wurzeln dieser Gleichung hervorbringt und dass daher diese Gleichung eine Abel'sche ist. Der Satz am Schlusse von Nr. 11. lässt sich darnach präciser folgendermassen fassen:

Damit die Gleichung (1) algebraisch auflösbar ist, muss sie nach Auflösung einer Abel'schen Gleichung mit rational bekannten Coefficienten selbst eine Abel'sche Gleichung werden. Aus der Natur solcher Gleichungen leuchtet nun aber sogleich ein, dass diese nothwendige Bedingung auch ausreichend ist. Und so gewinnen wir schliesslich den

Satz von Kronecker. Eine algebraisch auflösbare irreductibele Gleichung vom Primzahlgrade n ist dadurch charakterisirt, dass ihre Wurzeln so geordnet werden können, dass zwischen ihnen die Beziehungen stattfinden:

$$\alpha_1 = \Theta(\alpha_0, U),\ \alpha_2 = \Theta(\alpha_1, U),\ \cdots,\ \alpha_0 = \Theta(\alpha_{n-1}, U),$$

während Θ *eine rationale Function, U aber die Wurzel einer Abel'schen Gleichung bezeichnet, deren Coefficienten in demselben Sinne, wie die der gegebenen, rational sind.*

Münster i/W. Januar 1881.