Ueber alternirende Formen.

(Von Herrn *P. Muth* in Osthofen, Rheinhessen.)

Bekanntlich hat *Kronecker* in einer „Reduction der Systeme mit n_2 ganzzahligen Elementen“ betitelten Note*) die Reduction einer bilinearen Form mit ganzzahligen Coefficienten in einfachster Weise erledigt. Das principiell Neue der hier entwickelten Methode besteht darin, dass nicht mit der zu reducirenden *Form*, sondern mit dem *Coefficientensysteme* derselben operirt wird. Dieses wird in höchst einfacher Weise umgeformt: Reihen werden mit parallelen Reihen vertauscht, zu parallelen Reihen addirt u. s. w. Diesen Transformationen des Systems entsprechen dann lineare Transformationen der Form. Der Reduction des Systems durch solche *Elementartransformationen* entspricht die Reduction der bilinearen Form durch eben solche Transformationen. Dieses *Kronecker*sche Princip hat mit passender Erweiterung ausgedehnte Verwendung namentlich bei Untersuchungen über Elementartheiler gefunden. Wir werden es im Folgenden benutzen, um bekannte Resultate über alternirende Formen bez. Systeme theils *neu herzuleiten*, theils zu *verallgemeinern*.

I.

Es sei

$$A = \Sigma a_{ik} x_i y_k \qquad (i, k = 1, 2, \ldots, n)$$

eine beliebige bilineare Form von $2n$ Variablen $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_n$ mit dem Coefficientensysteme

$$\mathfrak{A} = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}.$$

*) Dieses Journal (1891) Bd. 107, S. 135—136. Vergl. auch *Kronecker*, Ueber symmetrische Systeme, Sitzungsberichte der Berl. Akademie 1889, S. 349ff. und *Kronecker*, Die Decomposition der Syst. u. s. w. am gl. Orte S. 479ff. u. S. 603ff.

Alsdann bezeichnen wir als *Elementartransformationen* T_1, T_2, T_3 *des Systems* $\mathfrak{A}$ folgende drei Umformungen desselben: 1. die Multiplication einer Reihe mit einer endlichen, von Null verschiedenen Constanten c, 2. die Vertauschung zweier parallelen Reihen, 3. die Multiplication einer Reihe mit einer endlichen, von Null verschiedenen Constanten m mit nachfolgender Addition (Subtraction) zu (von) einer parallelen Reihe.

Geht $\mathfrak{A}$ durch eine Transformation T_1 in $\mathfrak{A}'$ über, ist ferner A' die bilineare Form der x_i, y_i, deren Coefficientensystem — bei derselben Anordnung der Reihen wie oben — mit $\mathfrak{A}'$ identisch ist, so geht A' aus A dadurch hervor, dass eine Variable x_i oder y_k mit c multiplicirt wird, also in A $x_i = cx_i$ bez. $y_k = cy_k$ gesetzt wird. Analog entspricht jeder Transformation T_2 oder T_3 von $\mathfrak{A}$ eine bestimmte lineare Transformation der Form A.*) Diese Transformationen der *Form* A werden wir ebenfalls als *Elementartransformationen* T_1, T_2, T_3 bezeichnen.

Die Determinante einer linearen Transformation T_1 ist gleich c; die Transformationen T_2 und T_3 sind unimodular, d. h. sie haben den Modul -1 bez. 1.

Entsprechende Umformungen T_i, die mit den Zeilen und Spalten von $\mathfrak{A}$ vorgenommen werden, bezeichnen wir als *congruente Transformationen* T_i *von* $\mathfrak{A}$. Zu ihnen gehören *congruente lineare Transformationen* T_i von A. Da bei congruenter Transformation eine alternirende Form wieder in eine eben solche Form übergeht, so geht ein alternirendes System durch congruente Elementartransformationen in ein eben solches System über.

Durch lineare Transformation von A wird der Rang r von $\mathfrak{A}$ nicht geändert; daher bleibt bei den Umformungen T_i von $\mathfrak{A}$ der Rang von $\mathfrak{A}$ ungeändert.

Tritt bei einer Umformung von $\mathfrak{A}$ an Stelle des Elementes a_{ik} ein Element a'_{ik}, welches eine bestimmte Eigenschaft E hat, so sagen wir kurz, $\mathfrak{A}$ sei so umgeformt worden, dass das Element a_{ik} von $\mathfrak{A}$ die Eigenschaft E habe.**) Ferner bezeichnen wir kurz die i-te Zeile (k-te Spalte) eines

*) Vergl. Artikel 27 meines Buches über Elementartheiler (Leipzig 1899). Der Kürze halber erlaube ich mir auch im Folgenden, wenn es nöthig erscheint, auf dasselbe zu verweisen. (Citirt mit ET.)

**) Wir bezeichnen m. a. W. in der Regel das umgeformte System wieder mit $\mathfrak{A}$, seine Elemente wieder mit a_{ik}.

Systems mit $Z_i(S_k)$. Dasjenige System, welches aus $\mathfrak{A}$ dadurch hervorgeht, dass die $Z_1, Z_2, \ldots, Z_k$ und die $S_1, S_2, \ldots, S_k$ gestrichen werden, nennen wir *das k-te innere System* von $\mathfrak{A}$.

II.

Wir nehmen jetzt an, dass die *Form A* (das *System* $\mathfrak{A}$) *alternirend*, also

$$a_{ik} = -a_{ki}, \qquad a_{ii} = 0$$

sei. Da alle Hauptelemente in $\mathfrak{A}$ (ET. S. 14) Null sind, so steht ausserhalb der Hauptdiagonale ein von Null verschiedenes Element $a_{lm} = -a_{ml}$ ($l \gtrless m$). Dieses bringen wir durch Transformationen 2) an Stelle von a_{12}; durch die congruenten Transformationen kommt dann a_{ml} an die Stelle von a_{21}. Jetzt multipliciren wir die S_2 des noch immer alternirenden Systems (I.) mit $\frac{a_{13}}{a_{12}}, \frac{a_{14}}{a_{12}}, \ldots$ und subtrahiren sie dann der Reihe nach von der $S_3, S_4, \ldots$; durch diese und die congruenten T_3 erhalten wir ein alternirendes System, worin *alle* Elemente der Z_1 und S_1, ausser a_{12} und a_{21}, Null sind. Indem wir weiter die S_1 mit $\frac{a_{23}}{a_{21}}, \frac{a_{24}}{a_{21}}, \ldots$ multipliciren und dann der Reihe nach von der $S_3, S_4, \ldots$ subtrahiren, erhalten wir — bei gleichzeitiger Vornahme der zu diesen T_3 congruenten T_3 — ein System von der Gestalt

$$(1.) \qquad \left\{ \begin{array}{cccccc} 0 & a_{12} & 0 & 0 & \ldots & 0 \\ -a_{12} & 0 & 0 & 0 & \ldots & 0 \\ 0 & 0 & 0 & a_{34} & \ldots & a_{3n} \\ 0 & 0 & -a_{34} & 0 & \ldots & a_{4n} \\ \cdot & \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & \cdot & & \cdot \\ 0 & 0 & -a_{3n} & -a_{4n} & \ldots & 0 \end{array} \right\}.$$

Das zweite innere System dieses ebenfalls alternirenden Systems behandeln wir genau, wie eben das ganze System $\mathfrak{A}$. Setzen wir das Verfahren fort, so gelangen wir schliesslich zu einem Systeme $\mathfrak{A}'$, das — abgesehen von einem etwa auftretenden Theilsysteme mit lauter Elementen Null — in lauter Theilsysteme von der Gestalt

$$\begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix},$$

wo $a \gtrless 0$, zerlegbar ist (ET. Art. 22). $\mathfrak{A}'$ hat, wenn $\varkappa$ solcher Theilsysteme auftreten, den Rang $2\varkappa$; nun ist aber $2\varkappa$ auch der Rang von $\mathfrak{A}$. *Der Rang eines alternirenden Systems ist eine gerade Zahl.**) Ferner können wir sagen (I.): Eine alternirende Form A, deren Coefficientensystem vom Range $r = 2\varkappa$ ist, kann durch *congruente Elementartransformationen 2) und 3)* auf die Gestalt

$$(2.)\qquad e_1(x_1y_2-x_2y_1)+e_2(x_3y_4-x_4y_3)+\cdots+e_\varkappa(x_{r-1}y_r-x_ry_{r-1})$$

und durch *congruente Elementartransformationen 1), 2) und 3)* auf die Gestalt

$$(3.)\qquad (x'_1y'_2-x'_2y'_1)+(x'_3y'_4-x'_4y'_3)+\cdots+(x'_{r-1}y'_r-x'_ry'_{r-1})$$

gebracht werden. Die Coefficienten *aller* dieser Substitutionen 1), 2) und 3) sind *rationale* Functionen der Coefficienten von A.

Das zuletzt Bemerkte ergiebt sich daraus, dass (2.) dadurch in (3.) übergeht, dass

$$x_1 = x'_1,\quad x_2 = \frac{1}{e_1}x'_2,\quad x_3 = x'_3,\quad x_4 = \frac{1}{e_2}x'_4 \text{ u. s. w.}$$
$$y_1 = y'_1,\quad y_2 = \frac{1}{e_1}y'_2,\quad y_3 = y'_3,\quad y_4 = \frac{1}{e_2}y'_4 \text{ u. s. w.}$$

gesetzt wird. — Man folgert weiter:

Haben die Coefficientensysteme zweier alternirenden bilinearen Formen von je $2n$ Variablen A und B *gleichen Rang,* so kann man A in B durch *congruente* Substitutionen überführen, deren Coefficienten *rational* von denjenigen von A und B abhängen.**)

III.

In diesem Artikel setzen wir voraus, dass A eine *alternirende Form mit ganzzahligen Coefficienten* sei. Unter Elementartransformationen 1), 2) und 3) verstehen wir die in I beschriebenen Transformationen von A und $\mathfrak{A}$, nur dass jetzt *stets* bei den T_1 $c = -1$ und bei den T_3 für m eine ganze, positive oder negative, endliche Zahl ($\gtrless 0$) zu nehmen ist. Alle T_i sind also hier unimodular (ET. Art. 27). Wir werden jetzt A durch *lauter congruente Elementartransformationen dieser Art* auf die Gestalt (2.) bringen, wobei

---

*) Dies geht schon aus den Untersuchungen *Kroneckers* über die Congruenz der Formen (Monatsb. der Berlin. Acad. 1874, S. 397ff. [Werke Bd. I., S. 423ff.]) hervor. Vergl. ET. S. 151. Ausgesprochen und auf anderem Wege bewiesen wurde der Satz zuerst von Herrn *Frobenius*, d. Journ. (1877), Bd. 82, S. 242 (ET. S. 19).

**) Vergl. zu Obigem ET. S. 151.

$e_1, \dots, e_\varkappa$ *ganze positive Zahlen* vorstellen derart, dass e_2 durch e_1, e_3 durch e_2, u. s. w., $e_\varkappa$ durch $e_{\varkappa-1}$ *theilbar* ist.

Zunächst machen wir durch congruente T_2 und T_1 a_{12} in $\mathfrak{A}$ positiv und kleiner, als der absolute Werth jedes der übrigen Elemente*) von $\mathfrak{A}$ beträgt. Steht dann in der Z_1 ein Element a_{1l} das nicht ganzes Vielfaches von a_{12} ist, so können wir a_{12} nach dem von *Kronecker* an dem zuerst citirten Orte beschriebenen Verfahren noch weiter verkleinern, indem wir durch Transformationen T_3 und T_2, vorgenommen mit der S_2 und S_l, an Stelle von a_{12} den grössten gemeinschaftlichen Theiler von a_{12} und a_{1l} bringen; dann ist a_{1l} durch a_{12} theilbar (ET. Art. 28). Zu diesen Transformationen der Spalten führen wir stets die congruenten der Zeilen aus. Dieses Verfahren setzen wir so lange fort, bis jedes Element der Z_1 durch a_{12} theilbar ist; dann ist auch jedes Element der S_1 durch a_{12} theilbar, da $\mathfrak{A}$ alternirend geblieben ist. Alsdann machen wir durch congruente T_3 alle Elemente der Z_1 und S_1, ausser a_{12} und a_{21}, zu Null. Befindet sich jetzt in der Z_2 ein Element, das nicht durch a_{12} theilbar ist, so addiren wir die Z_2 zur Z_1, dann die S_2 zur S_1 und verkleinern das hierbei *ungeändert* gebliebene a_{12} weiter wie vorhin. Da aber a_{12} nicht kleiner werden kann, als der grösste gemeinschaftliche Theiler aller Elemente des gegebenen Systems (ET. S. 48), so muss nach einer endlichen Anzahl von den vorbeschriebenen Operationen ein Moment eintreten, wo *alle* Elemente der Z_1 und S_1, ausser a_{12} und $a_{21} = -a_{12}$, *Null,* alle Elemente der Z_2 und S_2 aber durch a_{12} *theilbar* sind. Multipliciren wir jetzt die S_1 mit $\frac{a_{23}}{a_{12}}, \frac{a_{24}}{a_{12}}, \dots, \frac{a_{2n}}{a_{12}}$, addiren sie dann zur $S_3, S_4, \dots, S_n$ und nehmen hierauf die congruenten T_3 vor, so erhalten wir ein alternirendes System von der Gestalt (1.). Steht nun in einer $Z_i (i > 2)$ ein Element, welches nicht durch a_{12} theilbar ist, so addiren wir die betreffende Z_i zur Z_1, dann die S_i zur S_1; dabei blieben a_{12} und a_{21} ungeändert, und a_{12} kann jetzt nach dem früheren Verfahren weiter verkleinert werden, da in der Z_1 ein nicht durch a_{12} theilbares Element steht. U. s. w. Nach einer endlichen Anzahl von Operationen müssen wir zu einem Systeme von der Gestalt (1.) gelangen, in welchem a_{12} den grössten gemeinschaftlichen Theiler e_1 *aller* Elemente vorstellt. Das zweite innere System desselben behandeln wir dann, wie eben das gegebene System. U. s. w.

*) Natürlich können mehrere Elemente absolut gleich und kleiner als die übrigen sein. Dann bringen wir irgend eins derselben nach a_{12}.

So kommen wir zu einem Systeme $\mathfrak{A}'$, welches — ausser einem etwa auftretenden Theilsysteme aus lauter Elementen Null — in $\varkappa$ Theilsysteme

$$\begin{pmatrix} 0 & e_1 \\ -e_1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & e_2 \\ -e_2 & 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 & e_\varkappa \\ -e_\varkappa & 0 \end{pmatrix}$$

zerlegbar ist, wenn $r = 2\varkappa$ den Rang des gegebenen System bedeutet. Dabei ist e_2 durch e_1, e_3 durch $e_2, \dots, e_\varkappa$ durch $e_{\varkappa-1}$ theilbar (ET. Art. 28).

Damit ist das zu Anfang dieses Artikels Behauptete bewiesen (I.). Bezeichnen wir den grössten gemeinschaftlichen Theiler aller Subdeterminanten ϱ-ten Grades ($\varrho \leqq r$) von $\mathfrak{A}'$ mit D_ϱ, den ϱ-ten Elementartheiler von $\mathfrak{A}'$ mit E_ϱ, so ist

$$D_1 = e_1, \quad D_2 = e_1^2, \quad D_3 = e_1^2 e_2, \quad D_4 = e_1^2 e_2^2, \quad \dots, \quad D_{r-1} = e_1^2 e_2^2 \dots e_{\varkappa-1}^2 e_\varkappa,$$
$$D_r = e_1^2 e_2^2 \dots e_\varkappa^2;$$

da D_ϱ für das gegebene System gleich D_ϱ für $\mathfrak{A}'$ ist, so gilt *der Satz, dass der grösste gemeinschaftliche Theiler aller Subdeterminanten ϱ-ten Grades eines alternirenden ganzzahligen Systems bei geradem ϱ das Quadrat einer ganzen Zahl ist**).

Ferner ist, da $E_\varrho = \frac{D_\varrho}{D_{\varrho-1}}$ für $\varrho \leqq r$,

$$E_1 = e_1, \quad E_2 = e_1, \quad E_3 = e_2, \quad E_4 = e_2, \quad \dots, \quad E_{r-1} = e_\varkappa, \quad E_r = e_\varkappa.$$

In einem alternirenden Systeme aus ganzen Zahlen ist also der $(2\lambda-1)$*-te Elementartheiler dem* 2λ*-ten gleich,* oder, wie man auch sagen kann (ET. S. 6), *die (einfachen) Elementartheiler eines solchen Systems treten stets paarweise auf.**) Wir können sagen:

Ist A eine alternirende Form mit ganzzahligen Coefficienten, ihr Coefficientensystem vom Range $r = 2\varkappa$, so lässt sich A *durch congruente Elementartransformationen* 1), 2) und 3) auf die Gestalt (2.) bringen, wo

$$e_1, e_1, e_2, e_2, \dots, e_\varkappa, e_\varkappa$$

bez. den *1-ten, 2-ten, ..., r-ten Elementartheiler* von $\mathfrak{A}$ bedeutet.**) Eine einfache, aber sehr bemerkenswerthe Folgerung hieraus ist, dass zwei äquivalente alternirende Formen mit ganzzahligen Coefficienten stets auch *congruent* sind.†)

IV.

Die Entwickelungen des letzten Artikels bleiben mit geringen Modificationen bestehen, wenn die Elemente des alternirenden Systems

---

*) *Frobenius,* d. J. (79), Bd. 86, S. 20ff., § 7.

**) Die Reduction einer alternirenden Form mit ganzen Coefficienten wurde zuerst von Herrn *Frobenius* l. c. mittelst einer anderen Methode ausgeführt.

†) *Frobenius,* l. c.

ganze Functionen einer Veränderlichen sind*) (ET. Art. 34). Der Satz über das paarweise Auftreten der Elementartheiler gilt auch für alternirende Systeme aus ganzen Functionen einer Variablen, woraus seine Giltigkeit für Systeme, deren Elemente binäre Formen gleichen Grades sind, ohne weiteres folgt (ET. Art. 37). Ein Specialfall des letzteren Satzes ist derjenige, dass die Elementartheiler des Coefficientensystems einer *Schar mit alternirenden Grundformen* stets paarweise auftreten.**) Die zuletzt genannten Sätze sind aber als *specielle Fälle* in einem *weit allgemeineren* Theoreme enthalten, bei dessen Beweise wir uns auf die Entwickelungen der § 18 der ET. stützen werden. Dasselbe lautet:

Die Elementartheiler eines alternirenden Systems $\mathfrak{A}$ aus ganzen oder gebrochenen Grössen eines Körpers von Zahlen oder Functionen treten stets paarweise auf.

Beweis. Wir führen den Beweis zunächst für ein alternirendes System $\mathfrak{A}$ aus ganzen oder gebrochenen *rationalen Zahlen.* Der grösste gemeinschaftliche Theiler aller Elemente von $\mathfrak{A}$ (ET. Art. 106) enthalte eine beliebig gewählte Primzahl p zur Potenz α_1 als Factor. Dann giebt es mindestens ein Element in $\mathfrak{A}$, das durch p^{α_1} dividirt, p weder im Zähler noch im Nenner enthält (ein mod. p reguläres Element). Ist a_{lm} ein solches, so bringen wir durch congruente Elementartransformationen 2) a_{lm} an Stelle von a_{12}, $a_{ml} = -a_{lm}$ an Stelle von $a_{21} = -a_{12}$. Multipliciren wir jetzt die S_2 mit den mod. p ganzen Zahlen $\frac{a_{13}}{a_{12}}, \frac{a_{14}}{a_{12}}, \dots, \frac{a_{1n}}{a_{12}}$ und subtrahiren sie dann von der $S_3, S_4, \dots, S_n$, so erhalten wir durch diese Elementartransformationen c) mod. p (ET. S. 226) ein zum gegebenen mod. p äquivalentes System, in welchem alle Elemente der Z_1, ausser a_{12}, Null sind. Durch die zu ihnen congruenten Transformationen wird das System wieder alternirend; wir haben also ein System, in welchem alle Elemente der Z_1 und S_1, ausser a_{12} und a_{21}, Null sind. Bei allen diesen Umformungen c) blieben aber die Z_2 und S_2 unverändert. Daher sind $\frac{a_{23}}{a_{21}}, \frac{a_{24}}{a_{21}}, \dots, \frac{a_{2n}}{a_{21}}$ mod. p ganze Zahlen; multipliciren wir also die S_1 mit diesen Zahlen, subtrahiren sie dann von der $S_3, S_4, \dots, S_n$ und führen die congruenten Transformationen mit den Zeilen aus, so erhalten wir ein zu $\mathfrak{A}$ mod. p äquivalentes System von der

*) *Frobenius*, l. c., § 13.

**) Vergl. ET. S. 142, Anm.

Gestalt (1.). Dieses bringen wir durch zwei weitere congruente Elementartransformationen a) mod. p (ET. S. 226) auf die noch einfachere Form

$$(4.)\qquad \begin{vmatrix} 0 & p^{\alpha_1} & 0 & 0 & \dots & 0 \\ -p^{\alpha_1} & 0 & 0 & 0 & \dots & 0 \\ 0 & 0 & 0 & a_{34} & \dots & a_{3n} \\ 0 & 0 & -a_{34} & 0 & \dots & a_{4n} \\ \cdot & \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & \cdot & & \cdot \\ 0 & 0 & -a_{3n} & -a_{4n} & \dots & 0 \end{vmatrix}.$$

Das zweite innere System von (4.) behandeln wir dann genau, wie eben das ganze System $\mathfrak{A}$. Wir gelangen, dieses Verfahren fortsetzend, schliesslich zu einem Systeme $\mathfrak{A}'$, das — abgesehen von einem etwa auftretenden Theilsysteme aus lauter Nullen — in $\varkappa$ Theilsysteme

$$\begin{pmatrix} 0 & p^{\alpha_1} \\ -p^{\alpha_1} & 0 \end{pmatrix}, \begin{pmatrix} 0 & p^{\alpha_2} \\ -p^{\alpha_2} & 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 & p^{\alpha_\varkappa} \\ -p^{\alpha_\varkappa} & 0 \end{pmatrix}$$

zerlegbar ist, wenn $r = 2\varkappa$ der Rang von $\mathfrak{A}$. Dabei ist

$$\alpha_1 \leqq \alpha_2 \leqq \dots \leqq \alpha_\varkappa.$$

Vergl. ET. Art. 108. Behalten wir die Bezeichnung in III. bei, so ist für $\mathfrak{A}'$

$$D_1 = p^{\alpha_1},\quad D_2 = p^{2\alpha_1},\quad D_3 = p^{2\alpha_1+\alpha_2},\quad D_4 = p^{2(\alpha_1+\alpha_2)}, \dots,$$
$$D_{r-1} = p^{2(\alpha_1+\alpha_2+\dots+\alpha_{\varkappa-1})+\alpha_\varkappa},\quad D_r = p^{2(\alpha_1+\alpha_2+\dots+\alpha_\varkappa)}.$$

Daraus folgt zunächst, da $\mathfrak{A}$ und $\mathfrak{A}'$ mod. p äquivalent sind, p aber eine beliebige Primzahl ist, *dass der grösste gemeinschaftliche Theiler aller Subdeterminanten ϱ-ten Grades von $\mathfrak{A}$ bei geradem ϱ das Quadrat einer rationalen Zahl ist.*

Ferner ist für $\mathfrak{A}'$

$$(5.)\qquad E_1 = p^{\alpha_1},\quad E_2 = p^{\alpha_1},\quad E_3 = p^{\alpha_2},\quad E_4 = p^{\alpha_2},\ \dots,\ E_{r-1} = p^{\alpha_\varkappa},\quad E_r = p^{\alpha_\varkappa};$$

nun ist aber E_ϱ für $\mathfrak{A}$ mod. p gleich E_ϱ für $\mathfrak{A}'$ (ET. S. 226), in Zeichen $E_\varrho(\mathfrak{A}') = E_\varrho(\mathfrak{A})$ mod. p. Da $E_{2\lambda-1}(\mathfrak{A}') = E_{2\lambda}(\mathfrak{A}')$ nach (5.), so ist folglich

$$E_{2\lambda-1}(\mathfrak{A}) = E_{2\lambda}(\mathfrak{A}) \text{ mod. } p;$$

p war aber eine beliebige Primzahl; daher ist

$$E_{2\lambda-1}(\mathfrak{A}) = E_{2\lambda}(\mathfrak{A}),$$

w. z. b. w. — Dieser Beweis bleibt Wort für Wort in den übrigen Fällen unseres Theorems bestehen, nur hat man dann für p eine lineare bezw. irreductibele Function, oder einen wirklichen oder idealen Primtheiler zu nehmen.