Ueber den gemeinsamen Factor zweier binären Formen.

Von Prof. Dr. M. Noether.

(Vorgetragen in der Sitzung am 12. November 1895.)

Im 13. Hefte (1881) dieser Sitzungsberichte, pag. 41, sowie in der deutschen Bearbeitung von Faà di Bruno's „Binären Formen" (Leipzig, Teubner 1881), pag. 57 ff., finden sich die Bedingungen, dass zwei binäre Formen einen Factor ϱten Grades gemeinsam haben, einfach entwickelt, aber mit einem unvollständigen Schluss, den ich erst 1886 in meinen Vorlesungen bemerkte und verbesserte.

Kurz darauf wurde die einfache und strenge Schlussweise von Herrn Scheibner („Mathem. Bemerkungen", (1), aus einem Briefe an Baltzer, vom 9. Februar 1887; Berichte der Sächs. Ges. d. Wiss. vom 16. Jan. 1888) mitgetheilt; und jetzt wiederum von Herrn Lüroth („Kurze Ableitung der Bedingungen etc.", Ztsch. f. Math. u. Phys., Bd. 40 1895). Ich möchte hier darauf zurückkommen, einmal, um jene Lücke, auf welche nicht hingewiesen worden ist, zu bezeichnen, hauptsächlich aber, um einige weitere Sätze zu folgern.

1. Die beiden Formen seien:

$$(1)\quad \left\{\begin{aligned} \varphi &= a_0 x^m + a_1 x^{m-1} + \ldots\ldots + a_m, \\ \psi &= b_0 x^n + b_1 x^{n-1} + \ldots\ldots + b_n \end{aligned}\right\} \left(\begin{matrix} a_0 \text{ und } b_0 \text{ nicht} \\ \text{zugleich } = 0 \end{matrix}\right).$$

Im Folgenden sollen P_i, Q_i, X_i, F_i, ... ganze Functionen von x, höchstens vom Grad i des Index, bezeichnen. Unmittelbar hat man die Schlüsse:

I. Wenn eine Relation von der Form

$$X_\varrho = P_i \cdot \varphi + Q_i \cdot \psi$$

existiert, wo X_ϱ eine nicht identisch verschwindende ganze Function, höchstens vom ϱten Grade, ist, so haben φ und ψ einen gemeinsamen Factor von höchstens dem Grade ϱ.

II. Wenn eine Relation von der Form

$$o = P_{n-\varrho} \cdot \varphi + Q_{m-\varrho} \cdot \psi,$$

mit nicht identisch verschwindenden $P_{n-\varrho}$ und $Q_{m-\varrho}$, existiert, so haben φ und ψ einen gemeinsamen Factor von mindestens dem Grade ϱ; und umgekehrt.

III. Wenn I. und II. existiert, so haben φ und ψ einen gemeinsamen Factor von genau dem Grade ϱ.

2. Unter D_ϱ ($\varrho = o, 1, \ldots m \leq n$) werde die Determinante

$$D_\varrho = \begin{vmatrix} a_o & a_1 & a_2 & \ldots & a_{m+n-2\varrho-1} \\ & a_o & a_1 & \ldots & a_{m+n-2\varrho-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ & & a_o & a_1 \ldots & a_{m-\varrho} \\ b_o & b_1 & b_2 & \ldots & b_{m+n-2\varrho-1} \\ & b_o & b_1 & \ldots & b_{m+n-2\varrho-2} \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ & & b_o & b_1 \ldots & b_{n-\varrho} \end{vmatrix} \quad \begin{pmatrix} a_i = o, \; b_k = o \\ \text{für } i > m, \; k > n \end{pmatrix}$$

verstanden. Sei zuerst D_ϱ nicht $= o$. Dann kann man die Functionen $P_{n-\varrho-1}$ und $Q_{m-\varrho-1}$ eindeutig so bestimmen, dass eine Identität

$$(2) \quad X_\varrho = P_{n-\varrho-1} \cdot \varphi + Q_{m-\varrho-1} \cdot \psi$$

existiert, in welcher der Coefficient von x^ϱ in X_ϱ zu 1 wird; denn die Vergleichung der Coefficienten, von der $(m + n - \varrho - 1)^{\text{ten}}$ bis zur ϱ^{ten} Potenz von x, giebt ein nicht-homogenes System von $m + n - 2\varrho$ linearen Gleichungen für die $m + n - 2\varrho$ Coefficienten von $P_{n-\varrho-1}$ und $Q_{m-\varrho-1}$, mit der Determinante D_ϱ *). Durch den Coefficienten von x^ϱ sind zugleich die übrigen Coefficienten von X_ϱ eindeutig mitbestimmt; und zwar treten, nach Multiplication von (2) mit D_ϱ, nur noch ganze Functionen der a und b in (2) auf.

In Verbindung mit Satz I folgt:

IV. D_ϱ nicht $= o$ ist hinreichende Bedingung für eine Relation (2), also auch dafür, dass φ und ψ einen Factor von höchstens dem Grade ϱ gemeinsam haben.

---

*) In der citierten Note war auch die Umkehrung dieses Satzes geschlossen, welche aber nicht zutrifft. Die notwendigen und hinreichenden Bedingungen für eine Identität (2) werden unten, Nr. 7, gegeben werden.

3. Sei $D_\varrho = 0$. Dann lässt sich eine Relation befriedigen:

$$(3)\ X_{\varrho-1} = P^1_{n-\varrho-1} \cdot \varphi + Q^1_{m-\varrho-1} \cdot \psi,$$

in welcher $X_{\varrho-1}$ eine Function von höchstens dem Grade $\varrho - 1$, und $P^1_{n-\varrho-1}$, $Q^1_{m-\varrho-1}$ nicht verschwindende Functionen werden. Denn, wie in 2., erhält man hier ein homogenes System von $m + n - 2\varrho$ linearen Gleichungen für die $m + n - 2\varrho$ Coefficienten von $P^1_{n-\varrho-1}$, $Q^1_{m-\varrho-1}$, mit der Determinante $D_\varrho = 0$. Umgekehrt folgt aus der Existenz eine Relation (3), dass $D_\varrho = 0$ ist:

V. $D_\varrho = 0$ ist die notwendige und hinreichende Bedingung für die Existenz einer Relation (3).

4. Sei jetzt angenommen: $D_0 = 0$, $D_1 = 0$, ... $D_{\sigma-1} = 0$ seien notwendig und hinreichend dafür, dass φ und ψ einen Factor von mindestens dem Grade σ gemeinsam haben; was für $\sigma = 0$ zutrifft.

Sollen φ und ψ einen Factor von mindestens dem Grade $\sigma + 1$ gemeinsam haben, so existiert die Relation des Satzes II für $\varrho = \sigma + 1$, also verschwindet, nach V, auch D_σ. Ist umgekehrt noch $D_\sigma = 0$, so existiert nach V die Relation (3) für $\varrho = \sigma$, in welcher aber die linke Seite $X_{\sigma-1}$ durch den angenommenen Factor σ^{ten} Grades teilbar, also identisch 0 wird; daher haben, nach II, φ und ψ einen Factor vom Grade $\sigma + 1$ gemeinsam. In Verbindung mit IV, III hat man somit:

VI. $D_0 = 0$, $D_1 = 0$, ..., $D_{\varrho-1} = 0$ sind die notwendigen und hinreichenden Bedingungen dafür, dass φ und ψ einen grössten gemeinsamen Factor von mindestens dem Grade ϱ besitzen. $D_0 = 0$, $D_1 = 0$, ..., $D_{\varrho-1} = 0$, D_ϱ nicht $= 0$ sind notwendig und hinreichend dafür, dass der grösste gemeinsame Factor von genau dem Grade ϱ ist.

5. Aus V ergibt sich, als unmittelbare Erweiterung dieses Satzes:

VII. Notwendige und hinreichende Bedingungen für das Bestehen einer Relation

$$X_{\varrho-1} = P^1_{n-\sigma-1} \cdot \varphi + Q^1_{m-\sigma-1} \cdot \psi \quad (\sigma \geqq \varrho),$$

in welcher $P^1_{n-\sigma-1}$ und $Q^1_{m-\sigma-1}$ nicht identisch verschwindende Functionen werden und $X_{\varrho-1}$ von höchstens dem Grade $\varrho - 1$ ist, sind:

$$D_\varrho = 0,\ D_{\varrho+1} = 0,\ \ldots,\ D_\sigma = 0.$$

6. Nach Nr. 3 kann für D_ϱ nicht $=0$ keine Relation der Art (2), von Nr. 2, existieren, in welcher die linke Seite unter den Grad ϱ sinkt, sondern nur, eindeutig bestimmt durch den Coefficienten von x^ϱ in X_ϱ, jene Relation (2) selbst. Verbindet man dies mit Satz VII, indem man daselbst $\varrho + 1$ für ϱ einsetzt, so hat man statt No. 2:

VIII. *Für D_ϱ nicht $=0$ sind die notwendigen und hinreichenden Bedingungen für das Bestehen einer Relation*

$$X_\varrho = P_{n-\sigma-1} \cdot \varphi + Q_{m-\sigma-1} \cdot \psi \ (\sigma \geqq \varrho),$$

in welcher der Coefficient von x^ϱ in X_ϱ gleich 1 sein soll, noch:

$$D_{\varrho+1} = 0,\ D_{\varrho+2} = 0,\ \ldots\ D_\sigma = 0.$$

Durch den ersten Coefficienten von X_ϱ ist die Relation eindeutig bestimmt. Für $D_{\sigma+1}$ nicht $=0$ sinken $P_{n-\sigma-1}$ und $Q_{m-\sigma-1}$ nicht zugleich unter die Grade ihrer Indices.

7. Schreibt man in VIII:

$$X_\nu \equiv x^\nu + \ldots = P_{n-\sigma-1} \cdot \varphi + Q_{m-\sigma-1} \cdot \psi,$$
$$D_\nu \text{ nicht} = 0,\ D_{\nu+1} = 0,\ D_{\nu+2} = 0, \ldots,\ D_\sigma = 0,$$

und nimmt

$$\sigma \geqq \varrho > \nu \geqq 0$$

an, so erhält man, indem man diese Relation Glied für Glied mit einer beliebigen Function $(\varrho - \nu)^{\text{ten}}$ Grades, $F_{\varrho-\nu}$, multipliciert, deren höchster Coefficient gleich 1 ist, ebenfalls eine Function ϱ^{ten} Grades in der Form (2), oder der Relation von Satz VIII, obwohl $D_\varrho = 0$ ist:

$$F^1_\varrho \equiv F_{\varrho-\nu} \cdot X_\nu = F_{\varrho-\nu} P_{n-\sigma-1} \cdot \varphi + F_{\varrho-\nu} Q_{m-\sigma-1} \cdot \psi,$$
$$= P''_{n-\varrho-1} \cdot \varphi + Q''_{m-\varrho-1} \cdot \psi,$$

wenn man nur noch weiter annimmt:

$$\sigma \geqq 2\varrho - \nu.$$

Wir wollen aber die Umkehrung beweisen, und damit den Satz:

IX. *Notwendige und hinreichende Bedingung für die Existenz einer Relation*

$$F_\varrho = P_{n-\varrho-1} \cdot \varphi + Q_{m-\varrho-1} \cdot \psi,$$

in welcher der Coefficient von x^ϱ von F_ϱ gleich 1 sein soll, ist: dass entweder D_ϱ nicht $= 0$, was auf VIII. führt; oder dass zu gleicher Zeit

$$D_\nu \text{ nicht} = 0,\ D_{\nu+1} = 0,\ D_{\nu+2} = 0,\ \ldots,\ D_\varrho = 0,\ \ldots,\ D_\sigma = 0,$$

wo

$$\varrho > \nu \geqq 0,\quad \sigma \geqq 2\varrho - \nu$$

ist. Im letzteren Falle ist die Relation für F_ϱ nichts weiter, als die eindeutig bestimmte Relation für X_ν, multipliciert mit einer beliebigen Function $(\varrho - \nu)^{\text{ten}}$ Grades.

Sei also angenommen: $D_\varrho = 0$ und

$$F_\varrho \equiv x^\varrho + \ldots = P_{n-\varrho-1} \cdot \varphi + Q_{m-\varrho-1} \cdot \psi.$$

Dann kann zunächst nicht zugleich $D_{\varrho-1} = 0$, $D_{\varrho-1} = 0, \ldots$, $D_0 = 0$ sein, weil sonst (VI) φ und ψ einen Factor $(\varrho + 1)^{\text{ten}}$ Grades gemeinsam hätten, F_ϱ also $\equiv 0$ wäre. Somit sei

$$D_\nu \text{ nicht} = 0,\ D_{\nu+1} = 0,\ D_{\nu+2} = 0,\ \ldots,\ D_\varrho = 0\ \ (\varrho > \nu \geqq 0).$$

Wegen D_ν nicht $= 0$ lässt sich, genau wie in No. 2, eine Relation

$$F^1_\varrho = P^1_{n-\nu-1} \cdot \varphi + Q^1_{m-\nu-1} \cdot \psi$$

herstellen, in welcher die $\varrho - \nu + 1$ Coefficienten von $x^\varrho, x^{\varrho-1}, \ldots, x^\nu$ in F^1_ϱ willkürlich, nur nicht alle 0, sind, während die übrigen Coefficienten von F^1_ϱ, und die von $P^1_{n-\nu-1}$, $Q^1_{m-\nu-1}$, durch sie eindeutig bestimmt werden. Nimmt man also jene $\varrho - \nu + 1$ willkürlichen Coefficienten von F^1_ϱ übereinstimmend an mit den entsprechenden von F_ϱ, so muss die Relation für F^1_ϱ in die gegebene für F_ϱ, welche der Form nach unter die für F^1_ϱ fällt, übergehen. Eine solche Relation für F^1_ϱ lässt sich aber so erhalten: Wegen D_ν nicht $= 0$, $D_{\nu+1} = 0, \ldots, D_\varrho = 0$ hat man nach VIII:

$$X_\nu \equiv x^\nu + \ldots = P^1_{n-\varrho-1} \cdot \varphi + Q^1_{m-\varrho-1} \cdot \psi,$$

also, nach Annahme einer beliebigen Function $(\varrho - \nu)^{\text{ten}}$ Grades $F_{\varrho-\nu}$:

$$F^1_\varrho = F_{\varrho-\nu} X_\nu = F_{\varrho-\nu} P^1_{\nu-\varrho-1} \cdot \varphi + F_{\varrho-\nu} Q^1_{m-\varrho-1} \cdot \psi;$$

und hier kann man links, wegen der Willkürlichkeit der $\varrho - \nu + 1$ Coefficienten von $F_{\varrho-\nu}$, die $\varrho - \nu + 1$ höchsten Coefficienten von F^1_ϱ mit denen von F_ϱ identisch machen.

Man hat daher:

$$F_\varrho \equiv F_{\varrho-\nu} X_\nu,\ P_{n-\varrho-1} \equiv F_{\varrho-\nu} P^1_{n-\varrho-1},\ Q_{m-\varrho-1} = F_{\varrho-\nu} Q^1_{m-\varrho-1},$$

wie im Satze behauptet wurde. Zugleich ergeben die letzten beiden Gleichungen weiter:

$$P^1_{n-\varrho-1} \equiv P''_{n-(2\varrho-\nu)-1},\quad Q^1_{m-\varrho-1} \equiv Q''_{m-(2\varrho-\nu)-1},$$

$$X_\nu \equiv x^\nu + \ldots = P''_{n-(2\varrho-\nu)-1} \cdot \varphi + Q''_{m-(2\varrho-\nu)-1} \cdot \psi,$$

also nach VIII auch:

$$D_{\varrho+1} = 0, \ D_{\varrho+2} = 0, \ \ldots, \ D_\sigma = 0 \ (\sigma \geqq 2\varrho - \nu),$$

was den Beweis des Satzes vervollständigt. —

Erwähnt sei hierbei nur, dass für D_ϱ nicht $= 0$ die Function $X_\varrho \equiv F_\varrho$ von VIII oder IX nach Multiplication mit D_ϱ der alsdann bei der Operation des Aufsuchens des grössten gemeinsamen Teilers von φ und ψ auftretende Rest ϱ^{ten} Grades ist, während für $D_\varrho = 0$ ein solcher Rest nicht existiert, aber nach IX noch eine analoge Relation für F_ϱ stattfinden kann, wie im allgemeinen Falle für den Rest ϱ^{ten} Grades.

Erlangen, September 1895.