Zur Theorie der linearen Formen.

(Von Herrn *K. Hensel.*)

In einer im nächsten Bande dieses Journals erscheinenden Arbeit wird der Nachweis geführt werden, dass die Fundamentalaufgabe der Theorie der algebraischen Functionen einer Variablen, nämlich die Aufgabe, alle *ganzen* algebraischen Functionen aufzustellen, auf ein einfacheres Problem zurückgeführt werden kann, welches sich in seiner allgemeinsten Form folgendermassen aussprechen lässt:

Es seien:

$$(1.)\qquad \begin{cases} A_1 = a_{11}u_1+\cdots+a_{1n}u_n, \\ \vdots \qquad \vdots \qquad\qquad \vdots \\ A_m = a_{m1}u_1+\cdots+a_{mn}u_n \end{cases}$$

m homogene lineare Functionen der Unbestimmten $u_1, \ldots, u_n$, deren Coefficienten a_{ik} entweder rationale Zahlen oder rationale Functionen einer Variablen x sein mögen. Es sollen $u_1, \ldots, u_n$ in der allgemeinsten Weise als *ganze* Zahlen oder als *ganze* Functionen von x so bestimmt werden, dass die m Ausdrücke $A_1, \ldots, A_m$ ebenfalls ganz werden.

Um diese Aufgabe zu lösen, kann unbeschadet der Allgemeinheit $m \geqq n$ angenommen werden, da man ja im entgegengesetzten Falle beliebig viele Linearformen $A_{m+\nu}$ mit den Coefficienten Null hinzunehmen kann. Es sei P der kleinste gemeinsame Nenner aller Coefficienten a_{ik}, und allgemein:

$$A_{ik} = P.a_{ik};$$

dann kann man die in (1.) gestellte Aufgabe auch folgendermassen aussprechen:

Es sollen die Unbestimmten $u_1, \ldots, u_n$ in der allgemeinsten Weise als ganze Zahlen, beziehungsweise als ganze Functionen so bestimmt werden, dass sie den m Congruenzen mit ganzen Coefficienten

$$(1^a.)\qquad A'_i = \sum_k A_{ik} u_k \equiv 0 \pmod{P} \qquad \binom{i=1,2,\ldots,m}{k=1,2,\ldots,n}$$

genügen.

Man kann nun dieses System linearer Congruenzen auf rationalem Wege in ein anderes äquivalentes transformiren, dessen Modul ein Theiler von P ist. Zu diesem Zwecke betrachte man alle Determinanten $n$ter Ordnung, welche aus dem rechteckigen System

$$(2.)\qquad |A_{ik}| \qquad \binom{i=1,\ldots,m}{k=1,\ldots,n}$$

der Coefficienten von $(1^a.)$ gebildet werden können, und suche mit Hülfe des Euklidischen Verfahrens ihren grössten gemeinsamen Theiler P_n mit dem Modul P, so dass also:

$$P_n \backsim (P, D_n)$$

ist, wenn D_n jede dieser Determinanten bezeichnet, und nach einer bekannten Schreibweise allgemein $(f, g, h, \ldots)$ den grössten gemeinsamen Theiler der Functionen $f, g, h, \ldots$ bezeichnet. In derselben Weise bezeichne D_{n-i} jede Unterdeterminante der $(n-i)$ten Ordnung des Systems (2.). Bildet man dann die Reihe der Functionen:

$$(3.)\qquad \begin{cases} P_n \backsim (P, D_n), \\ P_{n-1} \backsim (P, D_n, D_{n-1}), \\ \vdots \qquad\qquad \vdots \\ P_{n-\nu+1} \backsim (P, D_n, \ldots, D_{n-\nu+1}), \end{cases}$$

so muss man zuletzt zu einem Theiler

$$(3^a.)\qquad P_{n-\nu} \backsim (P, D_n, \ldots, D_{n-\nu+1}, D_{n-\nu}) \backsim 1$$

gelangen, es sei denn, dass alle Coefficienten A_{ik} denselben Theiler P_0 mit P gemeinsam haben, der dann durch einfache Division aus $(1^a.)$ oder durch das Heben der Brüche aus (1.) fortgeschafft werden könnte. Es seien ferner:

$$(4.)\qquad D^{(1)}_{n-\nu},\quad D^{(2)}_{n-\nu},\quad \ldots$$

die sämmtlichen Unterdeterminanten $(n-\nu)$ter Ordnung des Systems (2.) in irgend einer Reihenfolge. Bildet man dann die Reihe der grössten gemeinsamen Theiler:

$$(4^a.)\qquad \begin{cases} (P_{n-\nu+1}, D^{(1)}_{n-\nu}), \\ (P_{n-\nu+1}, D^{(1)}_{n-\nu}, D^{(2)}_{n-\nu}), \\ \ldots\ldots\ldots \end{cases}$$

so kommt man wegen (3^a.) zuletzt zu einem Divisor:

$$p \sim (P_{n-\nu+1},\ D^{(1)}_{n-\nu},\ \ldots,\ D^{(i)}_{n-\nu}), \tag{5.}$$

der mit der nächsten Determinante der Reihe (4.) keinen gemeinsamen Theiler mehr hat, der also in P sowie in allen Unterdeterminanten des Systems (2.) bis zu denjenigen der $(n-\nu+1)$ten Ordnung enthalten ist, dagegen mit mindestens einer Unterdeterminante der $(n-\nu)$ten Ordnung gar keinen gemeinsamen Theiler besitzt.

Betrachtet man dann die Congruenzen (1^a.) zunächst nur als solche für den Modul p, so sind bekanntlich alle eine Folge von nur $n-\nu$ unter ihnen, nämlich von denen, welche die zu p theilerfremde Determinante der $(n-\nu)$ten Ordnung enthalten. Es seien dies die $n-\nu$ ersten Formen:

$$\begin{array}{ccl} A_1 & = & A_{11}u_1+\cdots+A_{1\nu}u_\nu+A_{1\nu+1}u_{\nu+1}+\cdots+A_{1n}u_n, \\ \vdots & & \vdots \\ A_{n-\nu} & = & A_{n-\nu,1}u_1+\cdots+A_{n-\nu,\nu}u_\nu+A_{n-\nu,\nu+1}u_{\nu+1}+\cdots+A_{n-\nu,n}u_n, \end{array}$$

und es möge die den Unbestimmten $u_{\nu+1},\ldots,u_n$ entsprechende Determinante diejenige sein, welche mit p keinen gemeinsamen Theiler besitzt. Alsdann kann man bekanntlich $u_{\nu+1},\ldots,u_n$ durch $u_1,\ldots,u_\nu$ so ausdrücken, dass die so sich ergebenden Formen (1^a.) für unbestimmte $u_1,\ldots,u_\nu$ durch p theilbar sind, und dass so die vollständige Auflösung dieses Systems für den Modul p erhalten wird. Seien:

$$u_{\nu+k} = \sum_{l=1}^{\nu} \alpha_{kl}u_l \qquad (k=1,\ldots,n-\nu)$$

diese Auflösungen, deren Coefficienten α_{kl} also *ganze* Zahlen, beziehungsweise *ganze* Functionen von x sind. Setzt man dann an Stelle von $u_1,\ldots,u_n$ die neuen Unbestimmten $v_1,\ldots,v_n$ durch die Substitution:

$$\left\{\begin{array}{ll} u_\lambda = v_\lambda & (\lambda=1,\ldots,\nu), \\ u_{\nu+k} = \sum_{l=1}^{\nu}\alpha_{kl}v_l+pv_{\nu+k} & (k=1,\ldots,n-\nu) \end{array}\right. \tag{6.}$$

mit der Determinante

$$\Delta = p^{n-\nu}, \tag{6^a.}$$

so kann der Bedingung (1^a.) modulo p, also a fortiori modulo P, nur dann genügt werden, wenn $v_1,\ldots,v_n$ ganze Functionen des betrachteten Bereiches sind.

Setzt man aber diese Ausdrücke in die Congruenzen (1^a.) ein, so haben alle Coefficienten mit dem Modul P den gemeinsamen Theiler p, welcher somit fortgehoben werden kann. Sind dann B_{ik} die so sich ergebenden Coefficienten von $v_1, \ldots, v_n$, und setzt man:

$$\frac{P}{p} = P_1,$$

so ergiebt sich, dass alle Lösungen der Congruenzen (1^a.) und nur sie erhalten werden, wenn man $v_1, \ldots, v_n$ als ganze Grössen des Bereiches so bestimmt, dass sie den m Bedingungen

$$(7.) \qquad B'_i = \Sigma B_{ik} v_k \equiv 0 \pmod{P_1}$$

genügen.

Es ist somit das System der Bedingungen (1^a.) durch das ihm äquivalente (7.) ersetzt worden, dessen Modul aber ein kleinerer ist. Die Coefficienten B_{ik} ergeben sich aus den A_{ik} dadurch, dass an Stelle der u die Grössen v durch die Substitution (6.) mit der Determinante $\Delta = p^{n-\nu}$ eingeführt, und die so sich ergebenden Ausdrücke dann durch p dividirt werden. Ist daher D'_n irgend eine Determinante $n$ter Ordnung des Coefficientensystems (7.), D_n die entsprechende des Systems (1^a.), so besteht die Gleichung:

$$D'_n = \frac{D_n . \Delta}{p^n} = \frac{D_n}{p^\nu};$$

es ist daher der Theiler

$$P'_n \sim (P', D'_n) \sim \left(\frac{P}{p}, \frac{D_n}{p^\nu}\right)$$

ein Theiler von P_n.

Durch wiederholte Anwendung dieses Verfahrens erhält man hiernach zuletzt ein System von Congruenzen, dessen Modul gleich Eins ist, welches also durch *alle* ganzen Werthe der alsdann auftretenden Unbestimmten $U_1, \ldots, U_n$ befriedigt wird, und es ergiebt sich so die folgende Lösung der in (1.) gestellten Aufgabe:

> Man kann *auf rationalem Wege* die Unbestimmten $u_1, \ldots, u_n$ durch andere $U_1, \ldots, U_n$ vermittelst der Substitution
>
> $$u_i = \sum_k \gamma_{ik} U_k \qquad (i, k = 1, 2, \ldots, n)$$
>
> mit ganzen rationalen Coefficienten so ausdrücken, dass man alle Lösungen der gestellten Aufgabe (1.) und nur sie erhält, wenn man für $U_1, \ldots, U_n$ beliebige ganze Functionen des Bereiches setzt.

Durch die hier gegebenen Schlüsse kann endlich noch die weitere Frage beantwortet werden, wie der kleinste gemeinsame Nenner P aller Coefficienten a_{ik} beschaffen sein muss, damit die Lösungen $u_1, \ldots, u_n$ der Aufgabe nicht sämmtlich denselben gemeinsamen Theiler mit diesem Nenner haben, der sich ja dann fortheben würde. Aus den Substitutionen (6.), durch welche die u durch die v dargestellt werden, ergiebt sich nämlich, dass dann und nur dann, wenn $\nu > 0$ ist, die sämmtlichen Lösungen nicht den gemeinsamen Factor p haben; der grösste Nenner, für den alle Lösungen von (1.) keinen gemeinsamen Divisor besitzen, ist also der grösste gemeinsame Theiler aller Determinanten D_n des Systems (6.). Es ergiebt sich mithin der Satz:

Das System linearer homogener Functionen:

$$A_i = \Sigma a_{ik} u_k = \Sigma \frac{A_{ik}}{P} u_k$$

wird dann und nur dann durch ganze Grössen $u_1, \ldots, u_n$ ohne gemeinsamen Theiler mit dem Nenner P zu ganzen Functionen des Bereiches gemacht, wenn dieser Nenner in sämmtlichen Determinanten $|A_{ik}|$ der Coefficientenzähler enthalten ist. Der grösste Nenner, der diese Eigenschaft hat, ist somit der grösste gemeinsame Theiler aller dieser Determinanten.

In dieser Arbeit wurden die Coefficienten a_{ik} der zu untersuchenden Linearformen der Einfachheit wegen als Zahlen, oder als Functionen nur einer Variablen vorausgesetzt. Es mag aber erwähnt werden, dass sich dieselben Betrachtungen auch auf den allgemeinsten Fall anwenden lassen, dass diese Coefficienten einem beliebigen „natürlichen Rationalitätsbereiche $(\mathfrak{R}, \mathfrak{R}', \ldots)$" angehören, nur treten alsdann an die Stelle der hier betrachteten einfachen Theiler „Divisorensysteme verschiedener Stufen". Hierauf soll in einer anderen Arbeit noch näher eingegangen werden.