

Über einen algebraischen Satz

F. Mertens,

c. M. k. Akad.

1.

Sind φ, ψ ganze Functionen der Veränderlichen $x, y, .$ mit unbestimmten Coëfficienten und bezeichnet u irgend einen Coëfficienten von φ, v irgend einen von ψ, so lässt sich immer ein Exponent h von der Art angeben, dass das Product $u^h v$ als ganze ganzzahlige Function der Coëfficienten von φ und $\varphi\psi$ darstellbar ist, welche in den Coëfficienten von φ homogen und vom Grade $h-1$ und in denen von $\varphi\psi$ linear-homogen ist. Das Product $\varphi\psi$ ist hiebei in zusammengezogener Gestalt zu denken.

Dieser Satz ist für die Lehre von dem grössten gemeinschaftlichen Theiler von erheblichem Nutzen.

Um denselben zu beweisen, seien φ, ψ zunächst ganze Functionen nur einer Veränderlichen x, ν der Grad von ψ und man bezeichne eine ganze ganzzahlige Function der Coëfficienten von φ und $\varphi\psi$, welche die Coëfficienten von φ homogen und im Grade μ und die von $\varphi\psi$ linear-homogen enthält, allgemein mit (μ).

Ist φ eingliedrig und $= ux^k$, so fallen die Coëfficienten von $u\psi$ mit denen von $\varphi\psi$ zusammen und erscheinen daher unmittelbar in der Gestalt (0).

Ist die Function φ mehrgliedrig und zerlegt man dieselbe in zwei Bestandtheile A und B, deren erster lauter höhere Potenzen von x als der zweite enthält, so sind alle Coëfficienten von $A^{\nu+1}\psi$ und $B^{\nu+1}\psi$ von der Form (ν). Denn einerseits sind alle Coëfficienten des Ausdrucks von der Form (ν), weil derselbe in die Factoren

$$A^{\nu}-A^{\nu-1}B+A^{\nu-2}B^{2}-\ldots\pm B^{\nu}$$

und $(A+B)\psi=\varphi\psi$ zerfällt, deren erster ganze ganzzahlige homogene Functionen ν^{ten} Grades der Coëfficienten von φ zu Coëfficienten hat. Anderseits kann $A^{\nu+1}\psi$ kein Glied enthalten, welches mit einem von $B^{\nu+1}\psi$ zusammenziehbar wäre. Ist nämlich x^{a} die höchste in B vorkommende Potenz von x, so ist A durch x^{a+1}, also $A^{\nu+1}\psi$ durch $x^{(a+1)(\nu+1)}$ theilbar, während $B^{\nu+1}\psi$ den Grad $(\nu+1)(a+1)$ nicht erreicht.

Ist nun G das die höchste oder die niedrigste Potenz von x enthaltende Glied von φ und u der Coëfficient desselben, so nehme man in dem ersten Falle $A=G$ und in dem zweiten $B=G$. Die Coëfficienten von $u^{\nu+1}\psi$ sind dann dieselben wie die von $A^{\nu+1}\psi$, beziehungsweise $B^{\nu+1}\psi$ und besitzen sonach die Gestalt (ν).

Ist aber u der Coëfficient irgend eines mittleren Gliedes G von φ, so sei A die Summe aller Glieder von φ, welche höhere Potenzen von x als G enthalten, und B die Summe der übrigen. Zerlegt man $B^{\nu+1}$ in $G^{\nu+1}$ und die Summe C der übrigen Glieder, so kommt in $G^{(\nu+1)(\nu+1)}\psi$ kein Glied vor, welches mit einem von $C^{\nu+1}\psi$ zusammenziehbar wäre und die Coëfficienten des Ausdrucks

$$(G^{(\nu+1)(\nu+1)}+(-1)^{\nu}C^{\nu+1})\psi=$$
$$=(G^{\nu(\nu+1)}-CG^{(\nu-1)(\nu+1)}+\ldots\pm C^{\nu}).\,B^{\nu+1}\psi$$

sind ganze ganzzahlige Functionen der Coëfficienten von φ und $B^{\nu+1}\psi$, welche in den Coëfficienten von φ homogen und vom Grade $\nu(\nu+1)$ und in denen von $B^{\nu+1}\psi$ linear-homogen sind. Die Coëfficienten von $G^{(\nu+1)(\nu+1)}\psi$ haben also die Gestalt $(\nu^{2}+2\nu)$ und dasselbe gilt somit auch von $u^{(\nu+1)(\nu+1)}\psi$.

In allen Fällen sind also die Coëfficienten von $u^{h}\psi$ in der Gestalt $(h-1)$ darstellbar, wenn $h\geqq(\nu+1)^{2}$ ist.

Aus dem soeben bewiesenen Satze lässt sich eine Folgerung über die Coëfficienten des allgemeineren Products $\varphi^{p}\psi$ ziehen. Bezeichnet m eine Zahl, welche die Gradzahlen von φ und ψ mindestens um eine Einheit übersteigt, und u irgend einen Coëfficienten von φ, so sind alle Coëfficienten von $u^{m^{2}p^{3}}\psi$ als ganze ganzzahlige Functionen der Coëfficienten von φ und $\varphi^p\psi$ darstellbar, welche in den Coëfficienten von φ homogen und vom Grade m^2p^3-p und in denen von $\varphi^p\psi$ linear-homogen sind.

Man fasse $\varphi^p\psi$ als Product der Factoren φ und $\varphi^{p-1}\psi$ auf und bezeichne wieder eine ganze ganzzahlige Function der Coëfficienten von φ und $\varphi^p\psi$, welche die Coëfficienten von φ homogen und im Grade μ, die von $\varphi^p\psi$ aber linear-homogen enthält, allgemein mit (μ). Ist λ der Grad von $\varphi^{p-1}\psi$, so ist $(1+\lambda)^2 \leqq m^2p^2$ und die Coëfficienten von $u^{m^2p^2}\varphi^{p-1}\psi$ haben die Gestalt (m^2p^2-1).

Man fasse weiter $u^{m^2p^2}\varphi^{p-1}\psi$ als Product der Functionen φ und $u^{m^2p^2}\varphi^{p-2}\psi$ auf. Die Function $u^{m^2p^2}u^{m^2p^2}\varphi^{p-2}\psi = u^{2m^2p^2}\varphi^{p-2}\psi$ hat dann wieder Coëfficienten, welche ganz und ganzzahlig aus den Coëfficienten von φ und $u^{m^2p^2}\varphi^{p-1}\psi$ zusammengesetzt sind und, erstere homogen im Grade m^2p^2-1, letztere linear-homogen enthalten. Diese Function hat also auch Coëfficienten von der Form $(2m^2p^2-2)$.

Ist $p>2$, so ergibt sich in derselben Weise, dass $u^{3m^2p^2}\varphi^{p-3}\psi$ lauter Coëfficienten von der Form $(3m^2p^2-3)$ hat.

Fährt man so fort, so gelangt man zur Darstellung der Coëfficienten von $u^{m^2p^3}\psi$ in der Gestalt (m^2p^3-p).

Es lässt sich nun auch der obige Satz für Functionen φ, ψ von mehr als einer Veränderlichen beweisen. Hiebei werde unter m eine Zahl verstanden, welche alle Gradzahlen der Functionen von φ und ψ in Bezug auf die einzelnen in denselben vorkommenden Veränderlichen $x, y, .$ mindestens um eine Einheit übersteigt, und unter (μ) irgend eine ganze ganzzahlige Function der Coëfficienten von φ und $\varphi\psi$, welche in den Coëfficienten von φ homogen und vom Grade μ, in denen von $\varphi\psi$ aber linear-homogen ist.

Man ordne φ nach Potenzen von x und es sei Ux^α der Inbegriff aller Glieder von φ, welche eine bestimmte Potenz x^α von x enthalten. Nach dem Vorhergehenden sind dann die Coëfficienten der verschiedenen Potenzen von x in der Function $U^{m^2}\psi$ ganze und ganzzahlige Ausdrücke der Coëfficienten der einzelnen Potenzen von x in φ und $\varphi\psi$, und zwar enthalten diese Ausdrücke die genannten Coëfficienten von φ homogen und im Grade m^2-1, die von $\varphi\psi$ linear-homogen. $U^{m^2}\psi$ ist daher auch eine ganze Function der Veränderlichen $x, y, \ldots$ welche lauter Coëfficienten von der Form (m^2-1) hat.

Man ordne weiter U nach Potenzen einer zweiten Veränderlichen y und es sei Vy^β der Inbegriff der die Potenz y^β enthaltenden Glieder von U. Setzt man dann in der obigen Folgerung $p = m^2$, so lassen sich die Coëfficienten der verschiedenen Potenzen und Producte von x und y in $V^{m^8}\psi$ als ganze ganzzahlige Ausdrücke der Coëfficienten darstellen, welche in U bei den einzelnen Potenzen von y und in $U^{m^2}\psi$ bei den verschiedenen Potenzen und Producten von x und y stehen, und zwar sind diese Ausdrücke in den genannten Coëfficienten von U homogen und vom Grade m^8-m^2, in denen von $U^{m^2}\psi$ linear-homogen. Es ist daher $V^{m^8}\psi$ auch eine ganze Function von $x, y, \ldots$, deren Coëfficienten alle die Gestalt (m^8-1) haben.

Ist die Anzahl der Variablen >2, so ordne man V nach Potenzen einer dritten Veränderlichen z und greife einen Bestandtheil Wz^γ von V heraus. Man findet dann, wie vorher, dass die Coëfficienten der Function $W^{m^{26}}\psi$ alle die Form $(m^{26}-1)$ haben.

Ist n die Zahl der Veränderlichen, so ergibt sich nach n Schritten, dass $u^h\psi$ lauter Coëfficienten von der Form $(h-1)$ besitzt, wenn $h = m^{3^n}-1$ genommen wird.

2.

Der Satz des Artikels 42 der Disquisitiones arithmeticae von Gauss lautet in seiner wahren zahlentheoretischen Gestalt folgendermassen:

Der grösste gemeinschaftliche Theiler aller Coëfficienten des Products zweier ganzen ganzzahligen Functionen φ, ψ der Veränderlichen $x, y, \ldots$, ist das Product des grössten gemeinschaftlichen Theilers aller Coëfficienten von φ in den grössten gemeinschaftlichen Theiler aller Coëfficienten von ψ.

Der Beweis ergibt sich leicht aus dem Satze des vorhergehenden Abschnitts.

Es seien a irgend ein Coëfficient von φ, b irgend einer von ψ, t, t' die grössten gemeinschaftlichen Theiler aller Coëfficienten von φ, beziehungsweise ψ, und man bezeichne allgemein eine Summe von Vielfachen der Coëfficienten von $\varphi\psi$ mit L. Nach dem Satze des vorhergehenden Abschnitts gibt es einen Exponenten h von der Art, dass das Product $a^h b$ als ganze ganzzahlige Function der Coëfficienten von φ und $\varphi\psi$ darstellbar ist, welche die Coëfficienten von $\varphi\psi$ linear-homogen und die von φ homogen und im Grade $h-1$ enthält. Da ein Product von $h-1$ Coëfficienten der Function φ ein Vielfaches von t^{h-1} ist, so hat demnach jedes der Producte $a^h b$ die Gestalt $t^{h-1}L$. Da ferner t^h der grösste gemeinschaftliche Theiler der h ten Potenzen aller Coëfficienten von φ ist, so muss auch $t^h b$ die Gestalt $t^{h-1}b$ und demzufolge tb die Gestalt L haben. Da dies für alle Coëfficienten b von ψ gilt, so gilt es auch für tt'

Anderseits geht tt' in allen Coëfficienten von $\varphi\psi$ auf.

Wenn aber eine Zahl tt' in jedem Coëfficienten von aufgeht und als Summe L von Vielfachen derselben darstellbar ist, so ist sie der grösste gemeinschaftliche Theiler dieser Coëfficienten.

Der hier gegebene Beweis des Gauss'schen Satzes ist insofern von Interesse, als er ohne den Begriff der Primzahl auskommt. Dies sichert seine Anwendbarkeit in anderen ähnlichen Fragen.

3.

Ich will hier nur noch den Satz des §. 17 der Kronecker'schen Festschrift (Crelle, Bd. 92) darthun, dessen Beweis dort auf den Begriff der irreductibeln Divisoren gestützt ist.

Es seien

$$r_1,\ r_2,\ r_3, \ldots r_\nu$$

ganze algebraische Zahlen eines bestimmten Gattungsbereichs,

$$t_1,\ t_2,\ t_3, \ldots t_\nu$$

Veränderliche,

$$P_1,\ P_2,\ P_3, \ldots P_\nu$$

verschiedene Producte von Potenzen irgend welcher Veränderlichen $x, y, \ldots$ und man setze

$$t = r_1 t_1 + r_2 t_2 + \ldots + r_\nu t_\nu$$
$$\psi = r_1 P_1 + r_2 P_2 + \ldots + r_\nu P_\nu$$

$$N(t) = F$$
$$N(\varphi) = G = \varphi\psi,$$

wo N das Zeichen der Norm ist. Die Normen F, G sind ganze ganzzahlige Functionen der Veränderlichen $t_1, t_2, \ldots t_\nu$, beziehungsweise $x, y, \ldots$ und es handelt sich darum, zu zeigen, dass der grösste gemeinschaftliche Theiler N aller Coëfficienten von G mit dem grössten gemeinschaftlichen Theiler M aller Coëfficienten von F zusammenfällt.

Es genügt darzuthun, dass jede der Zahlen M, N, durch die andere theilbar ist. Dass M in N aufgeht, erhellt unmittelbar. Dass aber auch M durch N theilbar ist, wird bewiesen sein, wenn man darthut, dass die Form $\frac{t\psi}{N}$ algebraisch ganz oder $t\psi$ durch N theilbar ist.

Nach dem Satze des ersten Abschnitts gibt es einen Exponenten h von der Art, dass sich alle Coëfficienten von $r_k^h\psi$ als ganze ganzzahlige Functionen der Coëfficienten von $\varphi\psi = G$ und der Coëfficienten $r_1, r_2, \ldots r_\nu$ von φ darstellen lassen, welche in den Coëfficienten von G linear-homogen und in $r_1, r_2 \ldots r_\nu$ homogen und vom Grade $h-1$ sind. Da alle Coëfficienten von G den Factor N enthalten, so ist demnach $r_k^h\psi$ in der Gestalt Nf_k darstellbar, wo f_k eine ganze ganzzahlige Function von $x, y, \ldots r_1, r_2, \ldots r_\nu$ bezeichnet, welche in $r_1, r_2, \ldots r_\nu$ homogen und vom Grade $h-1$ ist. Denkt man sich daher die Potenz

$$t^{h\nu} = (r_1t_1 + r_2t_2 + \ldots + r_\nu t_\nu)^{h\nu}$$

nach dem polynomischen Satze entwickelt und erwägt, dass jedes Glied dieser Entwickelung wenigstens eine der Grössen $r_1, r_2, \ldots r_\nu$ in der h ten oder einer höheren Potenz enthalten muss, so lässt sich das Product $\psi t^{h\nu}$, wenn man in seinen einzelnen Gliedern $r_1^h\psi, r_2^h\psi, \ldots r_\nu^h\psi$ durch $Nf_1, Nf_2, \ldots Nf_\nu$ ersetzt, in der Gestalt $N\omega$ darstellen, wo ω ganz und ganzzahlig in $x, y, t_1, t_2, \ldots t_\nu, r_1, r_2, \ldots r_\nu$ ist und $r_1, r_2, \ldots r_\nu$ homogen und im Grade $h\nu-1$ enthält.

Nach §. 14 der genannten Festschrift sind nun, wenn

$$F = MP$$

gesetzt wird, die Formen

$$\frac{Pr_1}{t}, \quad \frac{Pr_2}{t}, \ldots \quad \frac{Pr_\nu}{t}$$

algebraisch ganz. Jedes Product von $P^{h\nu-1}$ und $h\nu-1$ Grössen der Reihe $r_1, r_2, \ldots r_\nu$ ist daher durch $t^{h\nu-1}$ theilbar und da die Coëfficienten der einzelnen Potenzen und Producte der Veränderlichen $x, y, \ldots t_1, t_2, \ldots$ in ω ganzzahlig und linear-homogen aus Producten von je $h\nu-1$ Grössen der Reihe $r_1, r_2, \ldots r_\nu$ zusammengesetzt sind, so ist auch $P^{h\nu-1}\omega$ durch $t^{h\nu-1}$ theilbar. Man kann also

$$P^{h\nu-1}\omega = t^{h\nu-1}\omega'$$

setzen, wo ω' eine ganze algebraische Form von $x, y, \ldots t_1, t_2, \ldots t_\nu$ bezeichnet, und es wird

$$P^{h\nu-1}t^{h\nu}\psi = Nt^{h\nu-1}\omega'$$

oder

$$P^{h\nu-1}t\psi = N\omega'.$$

Auf Grund der Primitivität der Form P folgt hieraus die Theilbarkeit von $t\psi$ durch N.