Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt.

Von **B. L. van der Waerden** in Leipzig.

Das Problem dieser Arbeit könnte man als das einer quantitativen Galoisschen Theorie bezeichnen. Mit einem ähnlichen Problem hat sich schon früher K. Dörge[1]) beschäftigt.

Es sei T die Anzahl aller ganzzahligen Polynome festen Grades

$$f(x)=c_0+c_1x+\ldots+c_n x^n$$

deren Koeffizienten c_ν absolut genommen eine sehr große Schranke N nicht übersteigen. Es sei S die Anzahl derjeniger unter diesen Polynomen $f(x)$, für welche die Gleichung $f(x)=0$ eine bestimmte Galoissche Gruppe $\mathfrak{G}$ besitzt. Den Quotienten $\frac{S}{T}$ nennen wir die Häufigkeit der Polynome oder der Gleichungen mit der Gruppe $\mathfrak{G}$. Es handelt sich nun darum, das Verhalten dieses Quotienten für große Werte von N zu untersuchen.

Es ist schon bekannt[2]), daß $\frac{S}{T}$ gegen Eins strebt, wenn $\mathfrak{G}$ die symmetrische Gruppe ist (Gleichungen ohne Affekt), sonst gegen Null (Gleichungen mit Affekt). Unsere Frage ist nun: Wie stark strebt $\frac{S}{T}$ gegen Null für verschiedene Gruppen $\mathfrak{G}$?

Eine erschöpfende Antwort auf diese Frage würde gleichzeitig das berühmte Hilbertsche Problem der Existenz von Gleichungen mit vorgegebener Gruppe lösen. Die vorliegende Arbeit bietet nur eine Lösung eines Teilproblems, indem zunächst (in § 1) gezeigt wird, daß im Fall einer intransitiven Gruppe (also im Fall zerfallender Polynome) die Häufigkeit wie eine Potenz von $N^{-\lambda}$ gegen Null strebt. Und zwar ist die Häufigkeit der Polynome vom Grade $n=q+r$, welche in Faktoren der Grade q und r zerfallen, im Fall $q<r$ genau von der Größenordnung N^{-q}, im Fall $q=r$ genau von der Größenordnung $N^{-r}\ln N$.

[1]) K. Dörge, Über die Seltenheit der reduziblen Polynome und der Normalgleichungen, Math. Ann. **95** (1925), S. 247—256.

[2]) B. L. van der Waerden, Math. Ann. **109** (1933), S. 13—16.

Auch über die Häufigkeitsverhältnisse der verschiedenen intransitiven Gruppen untereinander läßt sich einiges aussagen.

Für den Fall transitiver Gruppen ist es mir bisher nicht gelungen, ein so scharfes Ergebnis zu erhalten. In § 2 wird die Abschätzung

$$\frac{S}{T} \leqq N^{-\frac{1}{k \ln \ln N}}, \quad k = \frac{1}{6(n-2)}$$

für die gesamte Häufigkeit aller Gleichungen mit Affekt bewiesen. In § 3 wird durch eine teils strenge, teils heuristische Betrachtung über kubische Gleichungen wahrscheinlich gemacht, daß die irreduziblen Gleichungen mit Affekt eine noch kleinere Häufigkeit haben als die reduziblen Gleichungen. Zu diesem Zweck werden zunächst sämtliche zyklische Körper 3. Grades über dem rationalen Zahlkörper gebildet und dann zu jedem dieser Körper sämtliche Gleichungen aufgestellt, deren Wurzeln diesem Körper angehören und deren Koeffizienten die Schranke N nicht überschreiten.

§ 1. Die Häufigkeit der reduziblen Polynome.

Es sei $f(x)$ ein ganzzahliges Polynom vom formalen Grad n, d. h. ein Polynom vom Grade $\leqq n$ der Gestalt

$$f(x) = c_0 + c_1 x + \ldots + c_n x^n$$

mit ganzen rationalen Zahlenkoeffizienten. Wir nehmen an, daß das Polynom nicht identisch verschwindet und daß seine Koeffizienten absolut genommen eine positive Schranke N nicht übersteigen. Es gibt insgesamt

$$T = (2N+1)^n - 1 \geqq (2N)^n$$

solche Polynome $f(x)$. Wir wollen untersuchen, wieviele von diesen Polynomen sich in zwei Faktoren $g(x) \cdot h(x)$ von gegebenen formalen Graden q und r mit $q+r=n$ zerlegen lassen:

$$\begin{aligned} f(x) &= g(x)\, h(x) \\ g(x) &= a_0 + a_1 x + \ldots + a_q x^q \\ h(x) &= b_0 + b_1 x + \ldots + b_r x^r. \end{aligned}$$

Wir haben also zu untersuchen, in wievielen Weisen man die ganzzahligen Koeffizienten a_μ und b_ν der Polynome $g(x)$ und $h(x)$ so bestimmen kann, daß die Koeffizienten c_ν ihres Produktes $f(x) = g(x) \cdot h(x)$ den Ungleichungen

$$|c_\nu| \leqq N \tag{1}$$

genügen. Zu dem Zweck versuchen wir, obere Schranken für die Koeffizienten a_μ und b_ν zu gewinnen.

Nach einem bekannten Satz von Kronecker[3]) ist jedes Produkt $\zeta = a_\mu b_\nu$ Wurzel einer Gleichung

$$\zeta^m + d_1 \zeta^{m-1} + \ldots + d_m = 0, \tag{2}$$

wobei jedes d_j eine Form vom Grade j in $c_0, \ldots, c_n$ ist. Aus (1) folgt jetzt die Abschätzung

$$|d_j| \leqq \delta_j N^j$$

mit festen natürlichen Zahlen δ_j. Nunmehr besagt (2), daß $\frac{\zeta}{N}$ Wurzel einer Gleichung mit unabhängig von N beschränkten Koeffizienten ist. Also ist $\frac{\zeta}{N}$ selbst beschränkt:

$$|\zeta| = |a_\mu b_\nu| \leqq \gamma N, \tag{3}$$

wo die Schranke γ nur von den Gradzahlen q und r abhängt.

Setzt man nun

$$a = \text{Max.}\,(|a_0|, |a_1|, \ldots, |a_q|)$$
$$b = \text{Max.}\,(|b_0|, |b_1|, \ldots, |b_r|)$$

so folgt aus (3)

$$ab \leqq \gamma N. \tag{4}$$

Die Abschätzung (4) ist, von dem genauen Wert des Zahlenfaktors γ abgesehen, die schärfst mögliche. Ersetzt man nämlich in (4) den Zahlenfaktor γ durch den kleineren Zahlenfaktor $\frac{1}{r+1}$, so folgt aus der Bedingung (4) rückwärts die Ungleichung (1), was man sofort sieht, wenn man die Koeffizienten c_λ durch die a_μ und b_ν ausdrückt. Bedingung (4) ist also mit einem größeren Zahlenfaktor notwendig, mit einem kleineren Zahlenfaktor hinreichend für das Erfülltsein von (1).

Bei gegebenen a und b gibt es höchstens $2(q+1)(2a+1)^q$ mögliche Polynome $g(x)$ und $2(r+1)(2b+1)^r$ mögliche Polynome $h(x)$; denn ein Koeffizient a_λ von $g(x)$ muß gleich $\pm a$ sein, wobei $\lambda = 0, 1, \ldots, q$ gewählt werden kann, und die übrigen Koeffizienten a_μ müssen zwischen $-a$ und a liegen. Insgesamt gibt es also bei gegebenen a und b höchstens

$$4(q+1)(r+1)(2a+1)^q(2b+1)^r$$

[3]) L. Kronecker, Sitz.-Ber. preuß. Akad. Wiss., Berlin 1883, S. 957.

Produkte $g(x) \cdot h(x)$. Die Gesamtzahl der zerlegbaren Polynome $f(x) = g(x)\,h(x)$ ist demnach höchstens

$$S_{q,r} = 4\,(q+1)\,(r+1) \sum_{a\,b \leqq M} (2a+1)^q\,(2b+1)^r,$$

wobei $M = \gamma N$ gesetzt wurde und wo a und b alle natürlichen Zahlen durchlaufen.

Wir führen zuerst die Summation über b, die von 1 bis $B = \left[\frac{M}{a}\right]$ läuft, aus. In der für alle positiven x gültigen, aus der Binomialformel folgenden Ungleichung

$$(x+1)^{r+1} - (x-1)^{r+1} \geqq 2\,(r+1)\,x^r$$

setzen wir $x = 2b+1$ und erhalten

$$2\,(r+1)\,(2b+1)^r \leqq (2b+2)^{r+1} - (2b)^{r+1}$$

$$2\,(r+1) \sum_{1}^{B} (2b+1)^r \leqq (2B+2)^{r+1} - 1 \leqq \left(2\,\frac{M}{a} + 2\right)^{r+1}$$

$$S_{q,r} \leqq 2\,(q+1) \sum_{a=1}^{M} (2a+1)^q \left(\frac{4M}{a}\right)^{r+1}$$

$$S_{q,r} \leqq 2\,(q+1)\,(12M)^{r+1} \sum_{1}^{M} (2a+1)^{q-r-1}, \tag{5}$$

Wir können $q \leqq r$ voraussetzen. Im Falle $q < r$ ist die letzte Summe konvergent, d. h. unabhängig von M beschränkt. Das ergibt, wenn man $M = \gamma N$ beachtet:

$$S_{q,r} \leqq \alpha N^{r+1} \quad (q < r). \tag{6}$$

Im Falle $q = r$ dagegen wird

$$S_{q,r} \leqq (r+1)\,(12M)^{r+1} \sum_{1}^{M} \frac{2}{2a+1}$$

$$\leqq (r+1)\,(12M)^{r+1}\, ln\,(M+1),$$

also wegen $M = \gamma N$

$$S_{q,r} \leqq \beta N^{r+1} ln\, N \quad (N \geqq 2). \tag{7}$$

Durch die Formeln (6) und (7) ist das gestellte Problem gelöst. Dividiert man die Anzahlen der reduziblen Polynome durch die Gesamtzahl der Polynome $f(x)$, so erhält man ihre Häufigkeiten. Für diese ergibt sich der Satz:

Die Häufigkeiten der in Faktoren der Grade q und r zerfallenden Polynome $f(x)$ unter allen Polynomen vom for-

malen Grade $n=q+r$, die der Ungleichung (1) genügen, ist $O(N^{-q})$ für $q<r$ und $O(N^{-r} ln N)$ für $q=r$.

Die Abschätzungen (6) und (7) sind, von Zahlenfaktoren abgesehen, absolut scharf. Das ergibt sich aus ihrer Herleitung, denn wenn man auf jeder Stufe der Herleitung die Zahlenfaktoren durch kleinere ersetzt, kann man alle $<$-Zeichen durch $>$-Zeichen ersetzen. Dabei ist nur noch folgendes zu beachten: Wenn man jedes zerlegbare Polynom $f(x)=g(x).h(x)$ nur einmal erhalten will, muß man einen der Faktoren, etwa $g(x)$, so normieren, daß die Koeffizienten a teilerfremd sind und der erste nichtverschwindende unter ihnen positiv ist. Diese Normierung schränkt aber die Anzahl der möglichen $g(x)$ bei gegebenen a höchstens um einen Zahlenfaktor ein.

Im Fall $q<r$ kann man sich noch einfacher durch folgende Überlegung klarmachen, daß die Formel (6) sich nicht mehr verbessern läßt. Unter den zerfallenden Polynomen $f(x)=g(x).h(x)$, die (1) genügen, kommen jedenfalls die Polynome

$$x^q(b_0+b_1x+\ldots+b_rx^r),\ |b_\nu|\leqq N$$

vor, deren Anzahl allein schon mehr als $(2N)^{r+1}$ beträgt.

Es möge hier noch eine Bemerkung über die Galoisschen Gruppen der zerfallenden Gleichungen $g(x).h(x)=0$ Platz finden. Dabei beschränke ich mich auf den Fall $q<r$. Die Reihe rechts in (5) konvergiert in diesem Fall so rasch, daß die Anfangsglieder mit $a=1$ und $a=2$ zusammen schon mehr als die Hälfte der ganzen Summe ausmachen. Das heißt: Der erste Faktor in der Zerlegung $f(x)=g(x)h(x)$ hat in mehr als der Hälfte aller Fälle Koeffizienten $\leqq 2$. Unter den Gleichungen $g(x)=0$ mit Koeffizienten $\leqq 2$ kommen nun selbstverständlich solche mit sehr verschiedenen Galoisschen Gruppen vor. Jedes einzelne solche Polynom $g(x)$ gibt nun zu einer Menge von Produkten $g(x).h(x)$ Anlaß, deren Anzahl von derselben Größenordnung ist wie die Gesamtzahl der zerfallenden Polynome $g(x).h(x)$. Es haben also ganz verschiedene Galoissche Gruppen bis auf Zahlenfaktoren dieselbe Häufigkeit.

Ich habe einmal die Illusion gehabt, die Hilbertsche Vermutung von der Existenz von Gleichungen mit beliebiger Gruppe dahin verschärfen zu können, daß zu jeder Galoisschen Gruppe eine bestimmte Häufigkeit (etwa eine bestimmte Potenz $N^{-\varrho}$) und zu einer größeren Gruppe auch eine wesentlich größere Häufigkeit gehört. In der Tat hat die symmetrische Gruppe die größte Häufigkeit (vgl. § 2). Diese Illusion

erweist sich jetzt als unhaltbar. Zum Beispiel haben unter den Gleichungen 9. Grades die in Faktoren 2. und 7. Grades zerfallenden Gleichungen mit den Galoisschen Gruppen

$$\mathfrak{S}_2 \times \mathfrak{S}_7 \text{ und } \mathfrak{E} \times \mathfrak{S}_7$$

($\mathfrak{S}_\nu$ = symmetrische Gruppe, $\mathfrak{E}$ = Einheitsgruppe) beide die Häufigkeit αN^{-2}, eventuell mit verschiedenen α.

Ein anderes Beispiel: Die in Faktoren 3. und 6. Grades zerfallenden Gleichungen mit der Gruppe $\mathfrak{E} \times \mathfrak{S}_6$ haben die Häufigkeit N^{-3}. Die in Faktoren 4. und 5. Grades zerfallenden Gleichungen mit der Gruppe $\mathfrak{S}_4 \times \mathfrak{S}_5$ aber haben die Häufigkeit N^{-4} (alles von Zahlenfaktoren abgesehen), trotzdem die Gruppe $\mathfrak{S}_4 \times \mathfrak{S}_5$ mehr Elemente hat als die Gruppe $\mathfrak{E} \times \mathfrak{S}_6$.

§ 2. Die Häufigkeit der Gleichungen mit Affekt.

In meiner Arbeit über die Seltenheit der Gleichungen mit Affekt[4]) habe ich bewiesen: Sind $p_1, p_2, \ldots, p_m$ ungerade Primzahlen, ist weiter $P_m = p_1 p_2 \ldots p_m \leqq 2N+1$, und setzt man

$$6(n-2) = k, \quad \left(\frac{k-1}{k}\right)^m = \varepsilon,$$

so haben von den $(2N+1)^{n+1}$ Gleichungen $f(x)=0$, deren Koeffizienten dem Betrage nach $\leqq N$ sind, höchstens

$$S \leqq 2^{n+1}\ 3\varepsilon (2N+1)^{n+1}$$

nicht die symmetrische Gruppe. Die Häufigkeit $\frac{S}{T}$ der Gleichungen mit Affekt ist also höchstens $2^{n+1}\,3\varepsilon$.

Wir wollen nun die Größenordnung von m und ε als Funktionen von N bestimmen. Zu diesem Zweck wählen wir bei gegebenem N die Primzahlen $p_1, p_2, \ldots, p_m$ als die kleinsten m ungeraden Primzahlen und bestimmen m so, daß

$$P_m \leqq 2N+1 < P_{m+1}. \tag{8}$$

Setzt man weiter $x = p_{m+1}$, so ist nach dem Primzahlsatz

$$ln\, 2P_m = ln\, 2 + \sum_1^m ln\, p_\nu = \psi(x-1) \sim x-1 \sim x$$

und ebenso

$$ln\, 2P_{m+1} = ln\, 2 + \sum_1^{m+1} ln\, p_\nu = \psi(x) \sim x$$

[4]) B. L. van der Waerden, Math. Ann. **109** (1931), S. 13—16.

also wegen (6)

$$ln\,(2N+1) \sim ln\,2\,(2N+1) \sim x$$

und wiederum nach dem Primzahlsatz

$$m+2 = \pi(x) \sim \frac{x}{ln\,x} \sim \frac{ln\,(2N+1)}{ln\,ln\,(2N+1)} \sim \frac{ln\,N}{ln\,ln\,N}$$

$$ln\,(2^{n+1}3\,\varepsilon) \sim ln\,\varepsilon \sim m\,ln\,\frac{k-1}{k} \sim \frac{ln\,N}{ln\,ln\,N}\,ln\left(1-\frac{1}{k}\right)$$

Da nun

$$ln\left(1-\frac{1}{k}\right) < -\frac{1}{k}$$

so ist für genügend große N

$$ln\,(2^n 3\,\varepsilon) < -\frac{1}{k}\,\frac{ln\,N}{ln\,ln\,N}$$

$$\frac{S}{T} \leqq 2^n 3\,\varepsilon < N^{-\frac{1}{k\,ln\,ln\,N}}. \tag{9}$$

Damit ist eine Schranke für die Häufigkeit der Gleichungen mit Affekt gefunden. Diese Schranke strebt wohl gegen Null mit wachsendem N, aber nicht wie eine Potenz $N^{-\delta}$ wie die in § 1 gefundenen Schranken, sondern wie eine Potenz von N mit negativem, sehr langsam gegen Null strebendem Exponenten.

Im Fall $n=2$ sind die Gleichungen mit Affekt nichts anderes als die zerfallenden Gleichungen, deren Häufigkeit (nach § 1) $O(N^{-1}\,ln\,N)$ ist. Die Schranke (9) erweist sich somit als unscharf.

Ich vermute, daß die Häufigkeit der Polynome mit Affekt auch für $n>2$ im wesentlichen gleich der Häufigkeit der reduziblen Polynome ist. Es scheint nämlich, daß die irreduziblen Polynome mit Affekt noch erheblich seltener sind als die reduziblen Polynome. Diese Vermutung wird bestätigt durch die heuristische Betrachtung des folgenden Paragraphen, welche es plausibel macht, daß die Häufigkeit der Gleichungen 3. Grades mit alternierender Gruppe $O(N^{-2+\varepsilon})$ ist.

§ 3. Kubische Gleichungen mit alternierender Gruppe.

1. Aufstellung aller zyklischen Zahlkörper dritten Grades.

Jeder zyklische Körper K ist Kreiskörper, etwa Unterkörper des Körpers der m-ten Einheitswurzeln Ω, wobei die Zahl m jeweils möglichst klein gewählt sei. Die Gruppe von Ω ist die multiplikative Gruppe $\mathfrak{G}$ der zu m primen Restklassen mod m. Der Körper K gehört zu einer Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$ mit zyklischer Faktorgruppe. Diese

Untergruppe wird definiert durch einen Charakter $\chi(x)$ mod m, welcher für die Elemente von $\mathfrak{H}$ den Wert Eins annimmt. Der Charakter $\chi(x)$ ist eindeutig als Produkt von Charakteren $\chi_\nu(x)$ modulo den einzelnen in m aufgehenden Primzahlpotenzen darstellbar. Da χ und somit auch alle χ_ν in unserem Fall die Ordnung 3 haben müssen, so kommen in m, außer eventuell der Primzahl 3, nur Primzahlen der Form $p_\nu = 3\nu_\nu + 1$ vor, und zwar kann 3 nur zum Quadrat und die übrigen Primzahlen p_ν nur in der ersten Potenz in m vorkommen. Sonst nämlich würde sich der Charakter $\chi(x)$ schon nach einem kleineren Modul erklären und der Körper K sich schon in einem Kreiskörper mit kleinerem m einbetten lassen. m hat also eine der beiden folgenden Gestalten

$$m = p_1 p_2 \dots p_r \qquad (p_\nu = 3\nu_\nu + 1) \tag{10a}$$

$$m = 9\, p_2 \dots p_r \qquad (p_\nu = 3\nu_\nu + 1). \tag{10b}$$

Ist ζ eine primitive m-te Einheitswurzel, so bilden die Potenzen ζ^λ eine Basis für die ganzen Größen von Ω, wobei im Fall (10a) λ prim zu m, im Fall (10b) λ prim zu $m' = p_2 \dots p_r$ und $\lambda \equiv \pm m'$, $\pm 2m'$, $\pm 3m'$ (mod 9) sein soll[5]). Untersucht man nun, unter welchen Bedingungen eine Linearkombination der Basiselemente ζ^λ die Gruppe $\mathfrak{H}$ gestattet, also zu K gehört, so findet man, daß die Basis für die ganzen Größen von K in beiden Fällen (10) die Gestalt

$$(1, \eta, \eta') \text{ mit } \eta = \sum_{\lambda \text{ in } \mathfrak{H}} \zeta^\lambda$$

hat. Die Konjugierten η' und η'' von η haben ebenfalls die Gestalt $\Sigma \zeta^\lambda$, wo λ eine Nebenklasse $\mathfrak{H}$ in $\mathfrak{G}$ durchläuft. Die Summe $\sigma = \eta + \eta' + \eta''$ ist im Fall (10a) gleich $(-1)^r$, im Fall (10b) gleich 0.

Weiter erhält man nach einiger Rechnung

$$\eta\eta' + \eta'\eta'' + \eta''\eta = \frac{1}{3}(\sigma^2 - m)$$

$$\eta^2 + \eta'^2 + \eta''^2 = \frac{1}{3}(\sigma^2 + 2m).$$

Für die Diskriminante D des Körpers K findet man schließlich

$$D = \begin{vmatrix} 1 & \eta & \eta' \\ 1 & \eta' & \eta'' \\ 1 & \eta'' & \eta \end{vmatrix}^2 = m^2. \tag{11}$$

Mit weniger Rechnung erhält man (11), wenn man einen Satz der Klassenkörpertheorie[6]) heranzieht, nach welchem die Diskriminante

[5]) Vgl. etwa Hilbert, Zahlbericht, Satz 88.

[6]) Vgl. H. Hasse, J. reine u. angew. Math. **162** (1930), S. 169.

eines Abelschen Körpers das Produkt der Führer der verschiedenen Charaktere der Klassengruppe ist. Die Führer dieser Charaktere sind in unserem Falle 1, m, m und ihr Produkt ist m^2.

Zu einem vorgegebenen Wert von m gehören soviele zyklische Körper dritten Grades, als es Untergruppen $\mathfrak{H}$ in $\mathfrak{G}$ gibt. Jede Untergruppe $\mathfrak{H}$ ist nach dem Obigen durch einen Charakter

$$\chi(x)=\chi_1(x)\,\chi_2(x)\ldots\chi_r(x)$$

bestimmt, wo jedes χ_ν ein Charakter der Ordnung 3 modulo p_ν (bzw. mod 9) ist. Nun gibt es zu jedem Faktor p_ν oder 9 genau zwei Charaktere χ_ν und χ_ν^{-1} von der Ordnung 3. Für das Produkt $\chi(x)$ entstehen so 2^r Möglichkeiten. Da aber χ und χ^{-1} stets dieselbe Untergruppe $\mathfrak{H}$ ergeben, so gibt es nur 2^{r-1} verschiedene Untergruppen $\mathfrak{H}$ und daher auch 2^{r-1} verschiedene Körper K bei jedem m der Gestalt (10 a) oder (10 b).

Es sei noch bemerkt, daß alle Körper K total-reell sind.

2. Die Anzahl der Gleichungen $f(x)=0$ bei einem gegebenen Körper K.

Wir wollen nun abzählen, wieviele Polynome

$$f(x)=c_0+c_1x+\ldots+c_nx^n \tag{12}$$

es gibt, deren Wurzeln ξ, ξ', ξ'' konjugierte Zahlen eines festen total-reellen kubischen Zahlkörpers K sind und deren Koeffizienten c_ν die Ungleichungen (1) erfüllen.

Die Zahl ξ läßt sich als Quotient von ganzen Zahlen des Körpers K schreiben:

$$\xi=\frac{\alpha}{\beta}$$

Der größte gemeinsame Idealteiler von α und β sei $\mathfrak{c}$. Dann ist

$$\xi=\frac{\alpha}{\beta}=\frac{\mathfrak{a}\,\mathfrak{c}}{\mathfrak{b}\,\mathfrak{c}},\quad(\mathfrak{a},\mathfrak{b})=1.$$

Die teilerfremden Ideale $\mathfrak{a}$ und $\mathfrak{b}$ sind durch ξ eindeutig bestimmt. Das Ideal $\mathfrak{c}$ aber kann bei gegebenem ξ noch willkürlich in der Idealklasse $\mathfrak{a}^{-1}$ gewählt werden. Um also alle möglichen Körperzahlen ξ zu erhalten, hat man erstens in jeder Idealklasse willkürlich ein Ideal $\mathfrak{c}$ auszuwählen und sodann in allen möglichen Weisen zwei durch $\mathfrak{c}$ teilbare Zahlen α und β mit der Nebenbedingung $(\alpha,\beta)=\mathfrak{c}$ zu nehmen und ihre Quotienten zu bilden. Die Wahl der Ideale $\mathfrak{c}$ aus jeder Idealklasse denken wir uns ein für allemal fest geschehen.

Jede so gebildete Zahl ξ ist Nullstelle des Polynoms[7])

$$\boldsymbol{N}(\alpha-\beta x)=(\alpha-\beta x)(\alpha'-\beta' x)(\alpha''-\beta'' x).$$

Der Inhalt dieses Polynoms, d. h. der G. G. T. seiner Koeffizienten, ist $\boldsymbol{N}(\mathfrak{c})$. Das ganzzahlige Polynom

$$\frac{\boldsymbol{N}(\alpha-\beta x)}{\boldsymbol{N}(\mathfrak{c})} \tag{13}$$

hat also den Inhalt Eins. Da $f(x)$ nach Voraussetzung dieselben Nullstellen ξ, ξ', ξ'' hat wie das Polynom (13), muß $f(x)$ bis auf einen ganzzahligen Faktor d mit (13) übereinstimmen:

$$f(x)=d\cdot\frac{\boldsymbol{N}(\alpha-\beta x)}{\boldsymbol{N}(\mathfrak{c})}. \tag{14}$$

Die Formel (14) stellt, wenn man $d=1, 2, 3, \ldots$ nimmt, alle möglichen Polynome $f(x)$ dar[8]). Bezeichnet man die Anzahl der Polynome (13) mit Inhalt Eins, deren Koeffizienten absolut $\leqq N$ sind, mit $\varphi(N)$, und die Anzahl der Polynome $f(x)$, deren Koeffizienten absolut $\leqq N$ sind, mit $\chi(N)$, so folgt

$$\chi(N)=\varphi(N)+\varphi\left(\frac{N}{2}\right)+\varphi\left(\frac{N}{3}\right)+. \tag{15}$$

Für die folgende Abzählung ist es bequem, die Nebenbedingung $(\alpha, \beta)=\mathfrak{c}$, derzufolge das Polynom (13) das Gewicht Eins hat, fallen zu lassen. Es wird nur daran festgehalten, daß α und β einem der fest ausgewählten Ideale $\mathfrak{c}$ angehören und daß die Koeffizienten des Polynoms (13) dem Betrage nach $\leqq N$ sein sollen. Die so erhaltene Anzahl $\psi(N)$ von Polynomen (13) ist einerseits größer als die Anzahl $\varphi(N)$ mit der obigen Nebenbedingung, andererseits aber höchstens gleich der Gesamtzahl aller Polynome $f(x)$. Somit ist

$$\varphi(N)\leqq\psi(N)\leqq\chi(N). \tag{16}$$

Aus (15) und (16) folgt

$$\psi(N)\leqq\chi(N)\leqq\psi(N)+\psi\left(\frac{N}{2}\right)+\psi\left(\frac{N}{3}\right)+\ldots \tag{17}$$

Die Zahl $\psi(N)$ setzt sich zusammen aus h Summanden $\psi_{\mathfrak{c}}(N)$, die zu den einzelnen aus den Idealklassen ausgewählten Idealen $\mathfrak{c}$ gehören, wo h die Klassenzahl ist.

Zur Bestimmung von $\psi_{\mathfrak{c}}(N)$ haben wir zunächst die Zahlenpaare

[7]) Das fettgedruckte kursive Zeichen $\boldsymbol{N}$ bedeutet: Norm in K.

[8]) Es ist nicht nötig, die negativen Werte $d=-1, -2, \ldots$ in Betracht zu ziehen, da man statt dessen auch α und β beide mit -1 multiplizieren kann.

$(\alpha; \beta)$ des Ideals $\mathfrak{c}$ zu bestimmen, welche den Ungleichungen

$$(18) \qquad |\text{Koeffizienten von } \boldsymbol{N}(\alpha - \beta x)| \leqq \boldsymbol{N}(\mathfrak{c}) \cdot N$$

genügen. Die (unendliche) Anzahl dieser Zahlenpaare stimmt aber aus zwei Gründen noch nicht mit der gesuchten Anzahl der Formen (13) überein:

1. Multipliziert man α und β beide mit einer Einheit ε mit $\boldsymbol{N}(\varepsilon)=1$ so bleibt $\boldsymbol{N}(\alpha - \beta x)$ ungeändert;

2. ersetzt man $(\alpha; \beta)$ durch $(\alpha'; \beta')$ oder $(\alpha''; \beta'')$, so bleibt $\boldsymbol{N}(\alpha - \beta x)$ ungeändert.

Die Vieldeutigkeit 2. kann einfach durch Hinzufügung eines Faktors $1/3$ im Ausdruck für $\psi_{\mathfrak{c}}(N)$ berücksichtigt werden. 1. wird folgendermaßen berücksichtigt:

Es gibt zwei linear-unabhängige Einheiten mit Normen $+1$, welche zusammen mit der Einheitswurzel -1 die ganze Einheitengruppe erzeugen. Im Raum der Logarithmen, d. h. im Raum der Zahlentripel $(l_1 = ln|\beta|,\ l_2 = ln|\beta'|,\ l_3 = ln|\beta''|)$ definiert jede Einheit eine Translation T (Multiplikation von β, β', β'' mit $\varepsilon, \varepsilon' \varepsilon''$):

$$T(l_1, l_2, l_3) = (l_1 + ln\,\varepsilon,\ l_2 + ln\,\varepsilon',\ l_3 + ln\,\varepsilon'').$$

Die Gruppe dieser Translationen hat einen Fundamentalbereich in Gestalt eines unendlich langen Balkens

$$(19) \qquad \begin{cases} 0 \leqq \mu_2 l_2 + \mu_3 l_3 < a \\ 0 \leqq \nu_2 l_2 + \nu_3 l_3 < b \end{cases}$$

dessen Querschnitt die Größe R, der Regulator des Körpers ist. Wir nehmen nun einen sehr viel breiteren Balken

$$(20) \qquad \begin{cases} 0 \leqq l_2 < L \\ 0 \leqq l_3 < M \end{cases}$$

wo L und M groß gegen den größten Durchmesser des Balkens (19) sind. Der Bereich (20) enthält dann annähernd $\frac{LM}{R}$ Fundamentalbereiche (19). Beschränkt man also die Zahl β auf den Bereich (20) oder

$$(21) \qquad 1 \leqq |\beta'| < e^L, \quad 1 \leqq |\beta''| < e^M$$

und dividiert nachträglich die gefundene Anzahl von Zahlenpaaren (α, β) durch $\frac{LM}{R}$, so hat man die Vieldeutigkeit 1. beseitigt.

Es sei $(\gamma_1, \gamma_2, \gamma_3)$ eine Modulbasis des Ideals $\mathfrak{c}$. Dann haben wir also die Anzahl der Zahlenpaare

$$(22) \qquad \alpha = a_1\gamma_1 + a_2\gamma_2 + a_3\gamma_3, \quad \beta = b_1\gamma_1 + b_2\gamma_2 + b_3\gamma_3$$

des Ideals c zu bestimmen, welche die Ungleichungen (18), (21) erfüllen. Außerdem muß natürlich $\beta \neq 0$ sein; das hat aber zur Folge

$$|\beta\beta'\beta''| \geqq 1. \tag{23}$$

Aus den Ungleichungen (18) folgt auf Grund des Kroneckerschen Satzes genau wie in § 1

$$\text{Max}\,(|\alpha|, |\beta|) \cdot \text{Max}\,(|\alpha'|, |\beta'|) \cdot \text{Max}\,(|\alpha''|, |\beta''|) \leqq \gamma c N, \tag{24}$$

wobei γ eine feste natürliche Zahl und $c = N(\mathfrak{c})$ ist. Insbesondere ist

$$|\beta\alpha'\beta''| \leqq \gamma c N, \quad |\beta'\beta\alpha''| \leqq \gamma c N.$$

Dividieren wir diese Ungleichungen durch (23), so folgt

$$|\alpha'| \leqq \gamma c N |\beta'|, \quad |\alpha''| \leqq \gamma c N |\beta''|. \tag{25}$$

Fassen wir die sechs reellen Größen $\alpha, \alpha', \alpha'', \beta, \beta', \beta''$ als Koordinaten in einem 6-dimensionalen Raum auf, so definieren die Formeln (18), (21), (25) einen beschränkten Bereich $\mathfrak{B}$ in diesem Raum, dessen Volum wir mit V bezeichnen. Die Formeln (22) und ihre konjugierten definieren ein Punktgitter im gleichen Raum. Die Gitterkonstante ist gleich $c^2 D$. Es handelt sich nun darum, wieviele Gitterpunkte dem Bereich $\mathfrak{B}$ angehören.

Wenn die Gittermasche klein ist im Vergleich zu der Ausdehnung des Bereichs $\mathfrak{B}$, so ist die Anzahl der Gitterpunkte im Bereich näherungsweise gleich $\frac{V}{c^2 D}$. Das gilt also jedenfalls bei festgehaltenem Körper K für große N oder bei festgehaltenem großem N zumindest für eine beschränkte Anzahl von Körpern K. Eine hinreichende Bedingung für die Gültigkeit der Abschätzung ist, wie eine genauere Überlegung lehrt, daß der Durchmesser der Gittermasche klein ist gegen $(cN)^{\frac{1}{3}}$.

Um das Volum V nach oben abzuschätzen, bemerken wir, daß der Bereich $\mathfrak{B}$ jedenfalls enthalten ist in dem durch (21), (24), (25) definierten größeren Bereich $\mathfrak{B}'$. Entsprechend den 64 möglichen Vorzeichenkombinationen von $\alpha, \alpha', \alpha'', \beta, \beta', \beta''$ zerfällt der Bereich $\mathfrak{B}'$ in 64 gleich große Teilbereiche. Wir untersuchen also einen von diesen Teilbereichen. Er wird durch die Ungleichungen

$$\begin{cases} 1 \leqq \beta' < e^L, & 1 \leqq \beta'' < e^M, & \beta > 0 \\ 0 < \alpha' \leqq (\gamma c N)\beta', & 0 < \alpha'' \leqq (\gamma c N)\beta'', & \alpha > 0 \\ \text{Max}\,(\alpha, \beta) \cdot \text{Max}\,(\alpha', \beta') \cdot \text{Max}\,(\alpha'', \beta'') \leqq \gamma c N & & \end{cases}$$

definiert.

Durch die volumtreue Substitution

$$\begin{cases} \beta' = e^u & \beta'' = e^v & \beta = e^{-u-v}\, y \\ \alpha' = e^u z & \alpha'' = e^v t & \alpha = e^{-u-v}\, x \end{cases}$$

werden neue Integrationsveränderliche x, y, z, t, u, v eingeführt. Das transformierte Gebiet ist

$$\begin{cases} 0 \leqq u < L & 0 \leqq v < M & y > 0 \\ 0 < z \leqq \gamma c N & 0 < t \leqq \gamma c N & x > 0 \\ \text{Max } (x, y) \,.\, \text{Max } (1, z) \,.\, \text{Max } (1, t) \leqq \gamma c N. \end{cases}$$

Die Integration kann nunmehr ohne jede Mühe zuerst nach u und v, sodann nach x und y und schließlich nach z und t ausgeführt werden. Man findet für das Volum V die Abschätzung

$$V \leqq 2^8 \gamma^2 c^2 L M N^2.$$

Die Anzahl der Gitterpunkte im Bereich $\mathfrak{B}$ ist näherungsweise $\frac{V}{c^2 D}$. Um daraus die Anzahl $\chi_c(N)$ der Normen $N(\alpha - \beta x)$ zu erhalten, hat man nach dem obigen noch die Faktoren $\frac{R}{LM}$ und $\frac{1}{3}$ hinzuzufügen. So erhält man gleichmäßig für alle Idealklassen

$$\psi_c(N) \leqq \delta \frac{R}{D} N^2, \quad \delta = \frac{1}{3} \,.\, 2^8 \gamma^2. \tag{26}$$

Dieselbe Abschätzung, nur mit einer anderen Konstante δ, gilt auch nach unten (mit dem Zeichen $\geqq$), wie leicht ersichtlich.

Addiert man die Ungleichungen (26) für alle Idealklassen, so kommt

$$\psi(N) \leqq \delta \frac{h R}{D} N^2. \tag{27}$$

Aus (27) und (17) folgt schließlich

$$\chi(N) \leqq 2\, \delta \frac{h R}{D} N^2. \tag{28}$$

Die Formel (28) gilt um so mehr, wenn die Polynome $f(x)$ mit rationalen Wurzeln $\xi = \xi' = \xi''$ außer Betracht gelassen werden.

3. Die Summation über alle K.

Wir machen nun die Annahme, daß die Formel (28) nicht nur für einen festen Körper K, sondern (eventuell mit einer größeren Konstante δ) für alle Körper K gilt, die bei einem gegebenen großen Wert von N in Frage kommen. Diese Annahme bedeutet, daß auch dann, wenn der Durchmesser der Gittermasche vergleichbar wird mit oder

groß wird gegen die Ausdehnung des Bereiches $\mathfrak{B}$, die Anzahl der Gitterpunkte in $\mathfrak{B}$ doch nicht wesentlich größer wird als das Volum des Bereichs, dividiert durch das Volum der Gittermasche.

Nach Siegel[9]) ist für große D

$$ln\, h\, R \sim ln \sqrt{D}.$$

Somit ist für jedes $\varepsilon > 0$ und genügend große D

$$\begin{aligned} ln\, h\, R &< (1+\varepsilon)\, ln \sqrt{D} \\ h\, R &< \sqrt{D}^{1+\varepsilon}. \end{aligned} \tag{29}$$

Fügen wir in (29) rechts noch einen passenden Faktor δ' hinzu, so gilt die Formel für alle D. Nunmehr ergibt (28)

$$\chi(N) < k N^2 \sqrt{D}^{-1+\varepsilon}, \quad k = 2\delta\delta'. \tag{30}$$

Wir untersuchen nun, welche Werte von D bei gegebenem N in Frage kommen. Die Körperdiskriminante D ist ein Teiler der Diskriminante des Polynoms (12),

$$c_1^2 c_2^2 - 4 c_0 c_2^3 - 4 c_3 c_1^3 - 27 c_0^2 c_3^2 + 18 c_0 c_1 c_2 c_3,$$

welche zufolge der Ungleichungen $|c_\nu| \leqq N$ niemals größer als $27 N^4$ werden kann. Mithin ist

$$D \leqq 27 N^4, \quad m = \sqrt{D} \leqq \sqrt{27}\, N^2.$$

Unsere Annahme, daß die Formel (30) nicht nur für kleine D, sondern für alle D richtig ist, findet eine gewisse Stütze darin, daß sie für sehr große D ebenfalls stimmt. Für die Werte von D nämlich, für welche die rechte Seite der Formel kleiner als Eins wird, ist die linke Seite tatsächlich Null, da dann $D > 27 N^4$ ist. Man könnte sogar glauben, daß die Formel (30) für $\varepsilon = 0$ auch noch richtig wäre.

Um nun die Gesamtzahl aller Polynome $f(x)$ mit zyklischer Gruppe zu erhalten, hat man die Summe $\Sigma \chi(N)$ über alle Körper K zu bilden. Aus (30) folgt

$$S = \sum_K \chi(N) < \sum_K k\, N^2 \sqrt{D}^{-1+\varepsilon}$$

oder wegen (11)

$$S < k N^2 \sum_m 2^{r-1} m^{-1+\varepsilon}$$

summiert über alle m der Gestalt (10) mit $m^2 \leqq 27 N^4$.

[9]) C. L. Siegel, Acta arithmetica **1** (1935), S. 84, Formel (3).

Um diese Summe abzuschätzen, beachten wir, daß alle in Frage kommenden Zahlen m sich durch die Form x^2+xy+y^2 darstellen lassen, und zwar im Fall (10a) in $12 \cdot 2^r$ Weisen, im Fall (10b) in $12 \cdot 2^{r-1}$ Weisen. Mithin ist

$$S < \frac{k}{12} N^2 \sum_{x,y} (x^2+xy+y^2)^{-1+\varepsilon}$$

summiert über alle x und y mit $x^2+xy+y^2 \leqq \sqrt{27}\, N^2$ und $xy \neq 0$. Schätzt man schließlich diese Summe in bekannter Weise durch ein Integral ab, so kommt

$$S < k_1 N^{2+2\varepsilon}.$$

Für die Häufigkeit der Gleichungen 3. Grades mit alternierender Gruppe gilt demnach vermutlich

$$\frac{S}{T} < k_1 N^{-2+2\varepsilon} \qquad (\varepsilon \text{ beliebig positiv}). \tag{31}$$

(Eingegangen: 28. IX. 1935.)