German Exam Fall 2003

#1 START HERE

Die Bedeutung Hilberts für die moderne Mathematik*

"Das ist kein Beweis, das ist Theologie" soll der Mathematiker Gordan ausgerufen haben, als er Hilberts genialen Beweis der Endlichkeit des Systems der Invarianten kennen lernte. Ich möchte versuchen, Ihnen auseinanderzusetzen, worum es sich bei diesem Hilbertschen Theorem handelt, dem Theorem, das seinen Ruhm begründete. Zunächst erinnern wir uns daran, was man unter einem Polynom mehrerer Veränderlicher, etwa x und y, versteht. Es sind Ausdrücke, wie wir sie aus unserer Schulzeit kennen, zum Beispiel $3x^3y - 5xy^2 + 4x^5$, bei deren Bildung nur Addition, Subtraktion und Multiplikation verwendet werden. Naturgemäß treten solche Ausdrücke in den verschiedensten Teilen der Mathematik auf. Beschreibt man etwa die Lage eines Punktes der Ebene durch seine Koordinaten x und y, so berechnet sich das Quadrat des Abstandes dieses Punktes vom Koordinatenursprung durch das Polynom $x^2 + y^2$. Ersetzt man nun das ursprüngliche Koordinatensystem durch ein dagegen verdrehtes, so ändern sich die Koordinaten unseres Punktes. Die neuen Koordinaten werden Werte haben, die sich durch die alten ausdrücken lassen, etwa $\frac{3}{5}x - \frac{4}{5}y$ anstelle von x und $\frac{4}{5}x + \frac{3}{5}y$ anstelle von y. Berechnet man nun im neuen Koordinatensystem das Abstandsquadrat unseres Punktes, so müssen die neuen Koordinaten quadriert und addiert werden. Offenbar kann man sich die Rechnung sparen, man wird eben das alte Abstandsquadrat erhalten. Das Polynom $x^2 + y^2$ ist also, wie man sagt, invariant gegenüber der Ersetzung von x durch $\frac{3}{5}x - \frac{4}{5}y$ und von y durch $\frac{4}{5}x + \frac{3}{5}y$, eine solche Ersetzung wird eine Transformation der Variablen genannt. Nicht jedes Polynom hat diese Eigenschaft, die meisten Polynome sind keine Invarianten gegenüber diesen Transformationen. Es ist naheliegend, nach allen Invarianten zu fragen und man kann ziemlich leicht zeigen, daß $x^2 + y^2$ im Wesentlichen die einzige Invariante für diese Transformationen ist, daß sich nämlich jede andere durch diese eine Invariante ausdrücken läßt wie etwa $4(x^2 + y^2)^4 - 2(x^2 + y^2)$.

In der Geometrie kommen außer Drehungen noch andere Transformationen vor. Jedesmal stellt man dieselbe Frage:

Gegeben sei ein System gewisser Transformationen, man spricht von einer Transformationsgruppe. Gesucht wird das System aller Invarianten,

*) Address given for Hilbert's 100th birthday, 1962.

und es soll gezeigt werden, daß endlich viele von ihnen ausreichen, jede weitere Invariante auszudrücken.

Vor Hilbert bemühte man sich, diese Endlichkeit durch tatsächliche Berechnung der Invarianten zu zeigen. Bei vielen Variablen und einer komplizierten Transformationsgruppe ist dies eine nahezu undurchführbare Aufgabe. Und so findet man denn in der Literatur jener Zeit Arbeiten, die angefüllt sind mit Formeln, die sich über mehrere Seiten erstrecken, und nur noch vergleichbar sind mit den Formeln, die die Bewegung des Mondes wiedergeben.

In dieser mathematischen Atmosphäre ist Hilbert aufgewachsen. Aber schon in seinen frühen Arbeiten verschmähte er es, den angedeuteten dornenvollen Weg zu gehen. Es muß ihm ziemlich bald klar geworden sein, daß ihm nur eine gedankliche Durchdringung des Problems weiterhelfen konnte.

Und so überraschte er denn auch die mathematische Welt im Jahre 1890 mit einem Beweis der Endlichkeit des Invariantensystems für die wichtigsten Transformationsgruppen. Dabei stützt er sich auf einen Satz, den er bereits zwei Jahre vorher gefunden hatte und der Folgendes besagte:

Es sei eine beliebige Menge M von Polynomen gegeben (bei der Anwendung, die Hilbert im Sinne hatte, besteht M aus den Invarianten). Dann gibt es endlich viele Polynome $f_1, f_2, \ldots, f_n$ aus der Menge M so daß sich jedes weitere Polynom f von M in der folgenden Form schreiben läßt:

$$f = g_1 f + g_2 f_2 + \cdots + g_n f_n.$$

Dabei sind die g_i gewisse Polynome.

Man beginnt zu verstehen, warum Gordan diesen Beweis Theologie nannte. Wenn M die Menge der uns noch unbekannten Invarianten ist, so weiß man a priori, daß es unter diesen ebenso unbekannte Invarianten $f_1, f_2, \ldots, f_n$ geben muß, die der eben angeführten Bedingung genügen. Gestützt allein auf diese Tatsache führt Hilbert seinen Beweis zu Ende.

Hilbert selbst war sich über die Tragweite des zum Beweis benötigten Hilfssatzes klar. Sie geht weit über den Rahmen der Invariantentheorie hinaus und führt in das Gebiet der algebraischen Geometrie. Dort ist er der grundlegende Satz, der bis zum heutigen Tage bei jeder Untersuchung in der algebraischen Geometrie benötigt wird. Hilbert stellte auch noch weitere schöne Theoreme dieses Gebietes auf. Er bewies den nach ihm benannten Nullstellensatz und führte die nach ihm benannte Abzählungsfunktion in die algebraische Geometrie ein. Sie spielt auch heute noch bei allen tieferen Untersuchungen eine hervorragende Rolle.

Seit dem Jahre 1893 beschäftigte sich Hilbert mit der algebraischen Zahlentheorie. Wiederum will ich versuchen zu erklären, worum es sich dabei handelt.

Die sogenannte elementare Zahlentheorie (sie ist keineswegs immer elementar) wurde in ihrer heutigen Gestalt von Gauß begründet. Sie beschäftigt sich mit den mathematischen Eigenschaften der gewöhnlichen ganzen Zahlen. Einige dieser Eigenschaften sind uns noch von der Schule her bekannt. Der Satz, daß eine Zahl genau dann durch 3 teilbar ist, wenn ihre Quersumme es ist, der Begriff der Primzahl und anderes mehr. Die Sätze der Zahlentheorie haben von jeher einen großen Reiz auf die Mathematiker ausgeübt. Schon Euklid hatte bewiesen, daß es unendlich viele Primzahlen gibt. Da haben wir den Satz, daß sich jede ganze Zahl auf genau eine Art als Produkt von Primzahlen schreiben läßt, den Satz, daß jede ganze Zahl eine Summe von vier Quadratzahlen ist wie etwa $30 = 16 + 9 + 4 + 1$, daß eine Primzahl, die bei einer Division durch 4 den Rest 1 läßt, bereits Summe von 2 Quadratzahlen ist und vieles mehr.

Euler und Gauß haben bereits die Zahlentheorie auf höhere Bereiche ausgedehnt, Gauß auf alle Zahlen der Form $a + b\sqrt{-1}$, wo a und b gewöhnliche ganze Zahlen sind.

Einer Ausdehnung auf beliebige Zahlbereiche ähnlicher Art steht aber der Umstand im Wege, daß sich dann nicht mehr die Eindeutigkeit der Zerlegung in Primfaktoren zeigen läßt.—So sind z.B. $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ zwei wesentlich verschiedene Zerlegungen der Zahl 6 in Primfaktoren.

Diese Schwierigkeit wurde von Kummer, Kronecker und Dedekind durch die Einführung des Idealbegriffs überwunden. Dabei zerfällt etwa 6 in vier ideale Faktoren, die durch paarweise Zusammenfassung die beiden angeführten "realen" Zerlegungen ergeben.

Dies ist also der Gegenstand der algebraischen Zahlentheorie. Die dabei untersuchten Zahlbereiche heissen die ganzen Zahlen von Zahlkörpern. Nun waren die Untersuchungen Kummers äusserst kompliziert und daher der Mehrzahl der Mathematiker unzugänglich. Die Darstellung Dedekinds ist heute für uns zwar sehr leicht lesbar und elegant, war aber für die damalige Zeit zu modern. So wurde denn der im Jahre 1897 im Jahresbericht der Deutschen Mathematikervereinigung erschienene Zahlbericht Hilberts von allen Mathematikern mit großer Freude begrüßt. Hilbert stellt in ihm alle bis zur damaligen Zeit bekannten Ergebnisse zusammenfassend dar und machte durch große Vereinfachungen die Ergebnisse Kummers einem größeren Leserkreis zugänglich. Auch heute noch zieht jeder Zahlentheoretiker neben den neueren Lehrbüchern dieses grundlegende Werk zu Rate. #1 EN[

~~Wenn wir uns die beiden Beispiele vor Augen haben, die Zahlen $a + b\sqrt{-1}$ von Gauß und die Zahlen der Form $a + b\sqrt{-5}$, so sehen wir, daß sie aus dem Bereich der gewöhnlichen ganzen Zahlen durch Hinzunahme je einer Quadratwurzel entstehen.~~

stop

#2 START HERE

Theorie der Zöpfe.

Von EMIL ARTIN in Hamburg.

§ 1. Einleitung.

Die vorliegenden Untersuchungen sind als ein Ansatz zu einem Wege gedacht, dem Studium der Knoten und Verkettungen näher zu kommen. Es handelt sich um eine Kennzeichnung einfacherer topologischer Gebilde, der Zöpfe. Dabei ist unter einem Zopf im wesentlichen ein Geflecht aus Fäden zu verstehen, wie schon der Name sagt. Die Zöpfe geben Anlaß zu einer Gruppe, da man aus zwei von ihnen durch „Aneinanderhängen" einen dritten komponieren kann. Die Konstitution dieser Gruppe ist einfach genug, um mit einem finiten Verfahren die Entscheidung zu ermöglichen, ob zwei vorgelegte Zöpfe sich ineinander deformieren lassen oder nicht. Schließt man einen Zopf, verknüpft man also Anfang und Ende, so entsteht eine Verkettung. Umgekehrt läßt sich auch jede Verkettung in diese Gestalt bringen. Von hier aus bis zum Knotenproblem ist aber noch ein weiter Weg. Immerhin gestatten bereits die gewonnenen Resultate, Aussagen über die Verkettungen, vor allem über ihre Fundamentalgruppe, zu machen.

Mein besonderer Dank gilt Herrn O. SCHREIER, der mich bei der Abfassung dieser Arbeit tatkräftig unterstützt hat, insbesondere auch bei den langwierigen Rechnungen, mit denen wir zunächst durchzukommen hofften. Seine Hilfe kam mir besonders beim Beweis von Satz 9 zustatten.

§ 2. Komposition und Gruppenerzeugende.

Unter einem Zopf Z von n^{ter} Ordnung verstehen wir folgendes topologisches Gebilde:

Im Raum sei ein Rechteck mit Gegenseiten g_1, g_2 bzw. h_1, h_2 (der „Rahmen" von Z) vorgelegt. Auf jeder der beiden Seiten g_1 und g_2 seien n Punkte $A_1\, A_2 \cdots A_n$ bzw. $B_1\, B_2 \cdots B_n$ gegeben, wobei der Sinn der Numerierung von h_1 nach h_2 laufe. Jedem Punkte A_i sei eindeutig ein Punkt B_{r_i} zugeordnet, mit dem er durch eine doppelpunktfreie Raumkurve μ_i verbunden ist, die keine andere Kurve μ_k schneidet. Die Kurve μ_i erhalte noch die Orientierung von A_i nach B_{r_i}. Zwei solche Zöpfe heißen äquivalent oder kürzer gleich, wenn sie sich ineinander ohne Selbstdurchdringung deformieren lassen. Bei dieser Deformation betrachte man auch die Verlängerungen von g_1 und g_2

4

als undurchdringlich. Man beachte die beiden Orientierungen, die im Zopfe liegen. Die erste betrifft die Numerierung der Punkte A_i, die zweite den Sinn der Kurve μ_i. Bei der Deformation hat man auf diese Orientierungen Rücksicht zu nehmen.

Diese Definition werde nun eingeengt durch die weitere Forderung: Nach passender Deformation von Z sollen die Projektionen der Kurven μ_i auf die Ebene des Rahmens ganz im Innern des Rechtecks laufen, sich nur in endlich vielen Punkten schneiden und mit einer zu g_1 parallelen Geraden nur einen Punkt gemein haben. Da man dreifache Punkte durch leichte Abänderung in Doppelpunkte auflösen kann, wollen wir auch noch annehmen, daß bei der Projektion nur einfache Schnittpunkte auftreten. Schematisch wird sich dann ein Zopf durch eine Zeichnung repräsentieren lassen, wie sie in Fig. 2 zur Darstellung gebracht ist. In Fig. 1 ist als Beispiel ein Geflecht gezeichnet, das wir nicht als Zopf betrachten werden. Im weiteren Verlauf denken wir uns die Zöpfe gleich in einer solchen „Normalgestalt" gegeben.

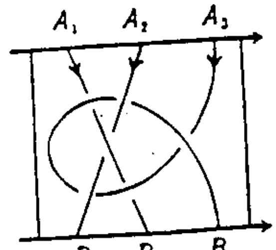

Fig. 1.

Aus zwei Zöpfen Z_1 und Z_2 von n^{ter} Ordnung kann durch Komposition ein dritter gebildet werden, indem man durch Deformation der Normalgestalten die beiden Rechtecke in einer Ebene so aneinanderlegt, daß die Seite g_2 von Z_1 an g_1' von Z_2 anstößt, die Punkte B_i von Z_1 mit den Punkten A_i' von Z_2 zusammenfallen und h_1', h_2' in die Verlängerungen von h_1 und h_2 fallen. Sodann lösche man die Gerade $g_2 = g_1'$. Das Resultat ist ein neuer Zopf, den wir mit $Z_1 Z_2$ bezeichnen. Der Zopf $Z_1 Z_2$ wird also kurz gesagt durch Aneinanderhängen der beiden Zöpfe Z_1 und Z_2 erhalten. In Fig. 2 ist dies andeutungsweise wiedergegeben. Man achte dabei wieder auf die Orientierungen. Wir erwähnen noch ausdrücklich, obwohl dies schon

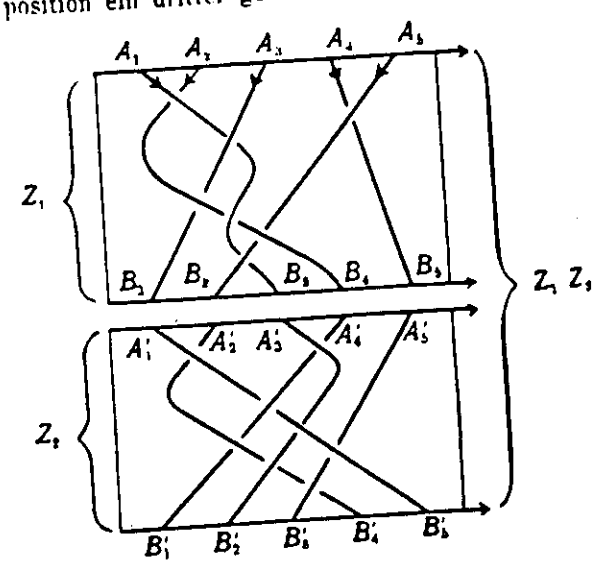

Fig. 2.

Nunmehr kann man leicht einsehen, daß jeder Zopf durch passende Komposition der Elementarzöpfe $\sigma_1^{\pm 1}, \sigma_2^{\pm 1} \dots \sigma_{n-1}^{\pm 1}$ erhalten werden kann, da man ihn nach leichten Deformationen in solche Schichten zerlegen kann, so daß in jeder einzelnen Schicht nur eine Überkreuzung liegt. Die in Fig. 2 vorkommenden Zöpfe gestatten zum Beispiel die Darstellung:

$$Z_1 = \sigma_1 \sigma_4^{-1} \sigma_2^{-1} \sigma_1 \sigma_2^{-1} \sigma_3 \sigma_2^{-1}; \qquad Z_2 = \sigma_1 \sigma_3 \sigma_2^{-1} \sigma_1 \sigma_3 \sigma_2^{-1} \sigma_4 \sigma_3^{-1}.$$

Dies hat aber zur Folge, daß es zu jedem Zopf Z einen inversen Z^{-1} gibt, für den gilt:

$$ZZ^{-1} = Z^{-1} Z = 1. \tag{4}$$

So ist z. B.: $Z_1^{-1} = \sigma_2 \sigma_3^{-1} \sigma_2 \sigma_1^{-1} \sigma_2 \sigma_4 \sigma_1^{-1}$. Die geometrische Bedeutung von Z^{-1} ist auch unmittelbar zu erkennen. Man erhält ihn nämlich, wenn man die Projektion von Z an der Geraden g_2 spiegelt, die Orientierung der Kurven aber im Spiegelbild einfach fortsetzt.

Somit bilden die Zöpfe n^{ter} Ordnung eine Gruppe $\mathfrak{Z}_n$ mit den $(n-1)$ Erzeugenden $\sigma_1, \sigma_2 \cdots \sigma_{n-1}$.

Als Beispiel eines einfachen Zopfes 3. Ordnung führen wir noch den allgemein bekannten Damenzopf an. Er hat die Formel:

$$Z = (\sigma_1 \sigma_2^{-1})^k.$$

#2 END

Auch die Flechtart:

$$Z = (\sigma_1 \sigma_3 \sigma_2^{-1})^k$$

Stop

bei der vier Fäden verwendet werden, findet häufig Anwendung.

§ 3. Definierende Relationen.

Die Darstellung eines Zopfes Z mit Hilfe der σ_i ist natürlich nicht eindeutig, da zwischen den σ_i noch gewisse Relationen bestehen werden, die von den erlaubten Deformationen von Z herrühren. Es wird sich nun zunächst darum handeln, die definierenden Relationen unserer Gruppe zu bestimmen, die Deformationen also zu arithmetisieren. Man überlegt sich nun leicht, daß eine Deformation von Z aus einer Normalgestalt in eine andere stets auch in der Normalgestalt ausgeführt werden kann, so daß es nur auf ein Umordnen der Fäden ankommt.

Dieses Umordnen der Fäden soll nun in einzelne Schritte zerlegt werden. Statt mehrere Fäden zugleich umzuordnen, kann man sukzessiv die einzelnen Fäden über oder unter die anderen wegziehen. Dabei wird man allerdings mehrmals zum gleichen Faden zurückkehren müssen, nachdem man inzwischen die anderen Fäden passend umgelegt hat. Jedenfalls besteht aber ein einzelner Schritt darin, daß ein gewisser Faden allein deformiert wird und die anderen fest bleiben.

6

3 START HERE

20.

Über die analytische Theorie der quadratischen Formen

Annals of Mathematics 36 (1935), 527—606

Zu den bekanntesten Sätzen der Arithmetik gehört die zuerst von Fermat bemerkte Tatsache, dass jede Primzahl der Form $4n + 1$ und keine Primzahl der Form $4n + 3$ Summe von zwei Quadratzahlen ist. Hieraus erhält man leicht die Aussage: Die Gleichung $x^2 + y^2 = p$, in der p eine Primzahl bedeutet, ist dann und nur dann ganzzahlig lösbar, wenn die Congruenz $x^2 + y^2 \equiv p$ (mod q) für jeden natürlichen Modul q eine Lösung hat. Dadurch wird also die Frage nach der Lösbarkeit einer Gleichung in ganzen rationalen Zahlen übergeführt in die Frage nach der Lösbarkeit in ganzen q-adischen Zahlen.

Stellt man sich nun allgemein das Problem, über die Lösbarkeit von

$$ax^2 + bxy + cy^2 = d \tag{1}$$

durch Untersuchung der entsprechenden Congruenzen

$$ax^2 + bxy + cy^2 \equiv d \pmod q \tag{2}$$

zu entscheiden, so lehrt das Beispiel $5x^2 + 11y^2 = 1$, dass aus der Lösbarkeit von (2) für jedes q noch nicht die ganzzahlige Lösbarkeit von (1) zu folgen braucht. Verzichtet man aber auf Lösungen in ganzen Zahlen und lässt auch gebrochene rationale Lösungen zu, so besagt ein wichtiger Satz von Legendre, dass aus der Lösbarkeit von (2) für jedes q die Lösbarkeit von (1) folgt. Dieser Legendresche Satz wurde von Hasse zu einer entsprechenden Aussage für das Problem der linearen Transformation einer quadratischen Form Q von m Variabeln in eine quadratische Form R von n Variabeln verallgemeinert: Damit Q in R durch eine lineare Substitution mit rationalen Coefficienten transformiert werden kann, ist notwendig und hinreichend, dass dies für jedes q mit q-adischen Coefficienten und ausserdem mit reellen Coefficienten möglich ist. Für $m = 2$, $n = 1$ entsteht hieraus der Satz von Legendre, wenn man beachtet, dass in diesem Falle die reelle Lösbarkeit auf grund des quadratischen Reciprocitätsgesetzes eine Folge der q-adischen Lösbarkeit ist. Ein anderer Specialfall des Hasseschen Satzes, nämlich $m = n$, wurde bereits von Minkowski ohne ausführlichen Beweis behandelt.

Um einen Ansatz für eine quantitative Verschärfung der qualitativen Aussage des Legendre-Hasseschen Satzes zu gewinnen, also eine Aussage über Lösungsanzahl statt Lösungsexistenz, stelle man folgende Betrachtung an. Es seien Q und Q_1 zwei quadratische Formen, deren Determinanten $\neq 0$ sind. Wenn sie miteinander äquivalent, d.h. ineinander ganzzahlig transformierbar

14

7

sind, so besteht offenbar eine umkehrbar eindeutige Zuordnung zwischen den ganzzahligen Transformationen von Q in R und von Q_1 in R. Dasselbe gilt, wenn an stelle des Ringes der ganzen rationalen Zahlen der Ring der ganzen q-adischen Zahlen gewählt wird. Es kann nun aber vorkommen, dass zwei Formen Q und Q_1 für jedes q stets q-adisch äquivalent und ausserdem reell äquivalent (d.h. reell ineinander transformierbar) sind, ohne dass sie im Ring der ganzen rationalen Zahlen äquivalent sind; ein Beispiel hierfür liefern $5x^2 + 11y^2$ und $x^2 + 55y^2$. Will man einen Zusammenhang zwischen den Lösungsanzahlen von Gleichungen und Congruenzen finden, so erscheint es ratsam, nicht Q vor Q_1 auszuzeichnen, sondern gleichzeitig die ganzzahligen Transformationen von Q in R und von Q_1 in R zu untersuchen. Man betrachte also die Gesamtheit der quadratischen Formen, die mit Q reell und ausserdem q-adisch für jedes q äquivalent sind; diese bilden das Geschlecht von Q. Aus jeder der endlich vielen Classen äquivalenter Formen des Geschlechts wähle man einen Repräsentanten. Es seien dies $Q, Q_1, \cdots$ mit den Matrizen $\mathfrak{S}, \mathfrak{S}_1, \cdots$, und es sei $\mathfrak{T}$ die Matrix von R.

Es folgt nun zunächst aus dem Legendre-Hasseschen Satz ohne erhebliche Schwierigkeit: Ist Q für jedes q ganzzahlig q-adisch und ausserdem reell in R transformierbar, so ist mindestens eine der Formen $Q, Q_1, \cdots$ ganzzahlig in R transformierbar. Dass darüber hinaus eine quantitative Beziehung zwischen den Anzahlen der ganzen q-adischen und der ganzen rationalen Transformationen besteht, ist das Hauptresultat der vorliegenden Abhandlung. Dieses soll jetzt für den Fall eines positiven definiten Q formuliert werden. Es seien $A(\mathfrak{S}, \mathfrak{T})$, $A(\mathfrak{S}_1, \mathfrak{T}), \cdots$ die Anzahlen der ganzzahligen Transformationen von $Q, Q_1, \cdots$ in R, also die Lösungsanzahlen der Matrizengleichungen $\mathfrak{X}'\mathfrak{S}\mathfrak{X} = \mathfrak{T}$, $\mathfrak{X}_1'\mathfrak{S}_1\mathfrak{X}_1 = \mathfrak{T}, \cdots$. Ferner seien $A(\mathfrak{S}, \mathfrak{S}) = E(\mathfrak{S})$, $A(\mathfrak{S}_1, \mathfrak{S}_1) = E(\mathfrak{S}_1), \cdots$ die Anzahlen der ganzzahligen Transformationen von $Q, Q_1, \cdots$ in sich selbst. Es stellt sich dann heraus, dass die Zahl

$$(3)\qquad \left(\frac{A(\mathfrak{S}, \mathfrak{T})}{E(\mathfrak{S})} + \frac{A(\mathfrak{S}_1, \mathfrak{T})}{E(\mathfrak{S}_1)} + \cdots\right) : \left(\frac{1}{E(\mathfrak{S})} + \frac{1}{E(\mathfrak{S}_1)} + \cdots\right)$$

in überraschend einfachem Zusammenhang steht mit der Anzahl der ganzzahligen Transformationen von Q in R modulo q, also mit der Lösungsanzahl $A_q(\mathfrak{S}, \mathfrak{T})$ der Matrizencongruenz $\mathfrak{X}'\mathfrak{S}\mathfrak{X} \equiv \mathfrak{T} \pmod{q}$. Lässt man nämlich q eine solche Folge von natürlichen Zahlen durchlaufen, dass jede natürliche Zahl in fast allen Gliedern der Folge aufgeht, also z.B. die Folge der Facultäten, so existiert

$$(4)\qquad \lim_{q \to \infty} A_q(\mathfrak{S}, \mathfrak{T})\, q^{\frac{n(n+1)}{2} - mn}$$

im Falle $n < m$ und unterscheidet sich von (3) nur um einen Factor κ, der allein von m, n und den Determinanten $|\mathfrak{S}|$, $|\mathfrak{T}|$ abhängt. Dieser Factor κ lässt sich folgendermassen independent definieren: Man betrachte die $\frac{n(n+1)}{2}$ unabhän-

8

gigen Elemente der Matrix $\mathfrak{T}$ als cartesische Coordinaten eines Punktes im $\frac{n(n+1)}{2}$-dimensionalen Raum. Jedem Gebiete G dieses Raumes entspricht dann vermöge der Gleichung $\mathfrak{X}'\mathfrak{S}\mathfrak{X} = \mathfrak{T}$ bei festem $\mathfrak{S}$ ein Gebiet G' des mn-dimensionalen $\mathfrak{X}$-Raumes. Sind dann $v(G)$ und $v(G')$ die Volumina dieser beiden Gebiete, so lasse man G auf den Punkt zusammenschrumpfen, welcher zur Matrix $\mathfrak{T}$ von R gehört, und bilde dabei

$$\lambda = \lim \frac{v(G')}{v(G)}.$$

Dann ist $\kappa = \frac{1}{2}\lambda$ für $m = n + 1$, $\kappa = \lambda$ für $m > n + 1$.

Die Grösse λ ist gewissermassen als Lösungszahl von $\mathfrak{X}'\mathfrak{S}\mathfrak{X} = \mathfrak{T}$ in reellen Zahlen anzusehen und kann daher als wahrscheinlicher Wert der Anzahlen $A(\mathfrak{S}, \mathfrak{T}), A(\mathfrak{S}_1, \mathfrak{T}), \cdots$ bezeichnet werden. Analog kann man $q^{mn - \frac{n(n+1)}{2}}$ als wahrscheinlichen Wert von $A_q(\mathfrak{S}, \mathfrak{T})$ ansehen, denn es gibt $q^{\frac{n(n+1)}{2}}$ modulo q verschiedene $\mathfrak{T}$ und q^{mn} modulo q verschiedene $\mathfrak{X}$. Der im vorigen Absatz ausgesprochene Satz gestattet also folgende kurze Formulierung: Das Verhältnis der Zahl $\frac{A(\mathfrak{S}, \mathfrak{T})}{E(\mathfrak{S})} + \frac{A(\mathfrak{S}_1, \mathfrak{T})}{E(\mathfrak{S}_1)} + \cdots$ zu ihrem wahrscheinlichen Wert ist gleich dem Grenzwert des Verhältnisses der Zahl $A_q(\mathfrak{S}, \mathfrak{T})$ zu ihrem wahrscheinlichen Wert im Falle $m > n + 1$, und halb so gross im Falle $m = n + 1$.

Der Ausdruck (4) lässt sich auch als ein über alle Primzahlen zu erstreckendes unendliches Produkt schreiben. Bedeutet q speciell eine Potenz p^a einer Primzahl p, so ist die Grösse $A_q(\mathfrak{S}, \mathfrak{T})q^{\frac{n(n+1)}{2} - mn}$ bei festen $\mathfrak{S}$ und $\mathfrak{T}$ für alle hinreichend grossen a constant, also eine rationale Zahl $\alpha_p(\mathfrak{S}, \mathfrak{T})$, die als Lösungsdichte von $\mathfrak{X}'\mathfrak{S}\mathfrak{X} = \mathfrak{T}$ im Körper der p-adischen Zahlen bezeichnet werden kann. Es wird dann (4) gleich dem über alle Primzahlen in natürlicher Reihenfolge zu erstreckenden Produkt $\prod_p \alpha_p(\mathfrak{S}, \mathfrak{T})$ und folglich die "Lösungsdichte im Körper der rationalen Zahlen"

$$\frac{\dfrac{A(\mathfrak{S}, \mathfrak{T})}{E(\mathfrak{S})} + \dfrac{A(\mathfrak{S}_1, \mathfrak{T})}{E(\mathfrak{S}_1)} + \cdots}{\dfrac{\lambda}{E(\mathfrak{S})} + \dfrac{\lambda}{E(\mathfrak{S}_1)} + \cdots} = \prod_p \alpha_p(\mathfrak{S}, \mathfrak{T}), \tag{5}$$

also gleich dem Produkt aller p-adischen Lösungsdichten; dabei ist im Falle $m = n + 1$ rechts noch der Factor $\frac{1}{2}$ hinzuzufügen.

END

Stop

~~[illegible] Lösungsdichten $\alpha_p(\mathfrak{S}, \mathfrak{T})$ haben für alle p, die nicht in $2|\mathfrak{S}||\mathfrak{T}|$ [illegible] einen einfachen expliciten Ausdruck, und auch das Product dieser α_p lässt sich in einfacher Form schreiben. Da jedoch die Bestimmung der übrigen endlich vielen α_p mühsame elementare Rechnungen erfordert und zu unübersichtlichen Werten führt, so erscheint die Gleichung (5) trotz ihrer transcendenten Form als die zweckmässigste Fassung des Zusammenhangs zwischen der~~

15

9