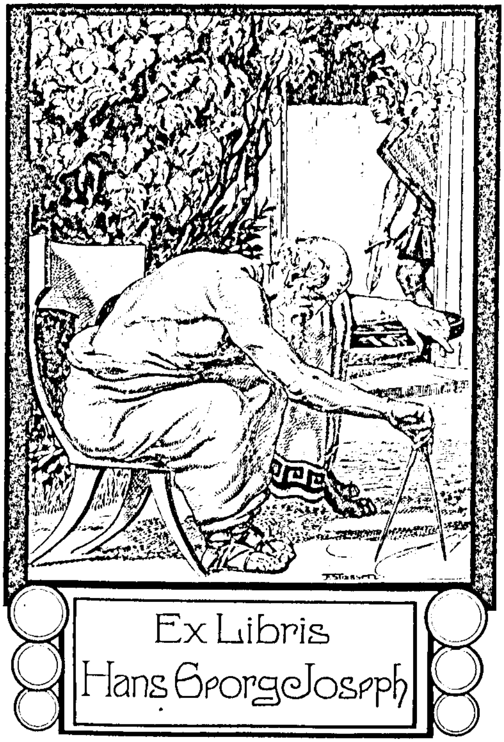

Ex Libris
Hans Georg Joseph

Probleme und Prinzipienfragen
der Mathematik
Vorlesung
gehalten im W. S. 1914/15
von
D. Hilbert.

I. Abschnitt. Die Kreisquadratur.

Meine Herren und Damen!

Unsere Vorlesung, die sich mit den Prinzipien der mathematischen Wissenschaft beschäftigen soll, hat zweierlei Schwierigkeiten. Erstens eine sachliche; obwohl die Fragen, mit denen wir es zu tun haben werden, elementarer Natur sind, so sind die Probleme, die sich dabei ergeben, doch von sehr schwieriger Art, und manche Teile derselben sind noch gar nicht bis zur völligen Klarheit gelöst worden. Dazu kommt noch eine pädagogische Schwierigkeit. Denn so einfach die Fragen an sich auch

sein mögen, so sind doch gewisse mannigfaltige Kenntnisse nötig, und es ist selbstverständlich, daß wir diese nicht alle voraussetzen können. Nun gibt es aber einen Weg, diese Schwierigkeit zu vermeiden, und den will ich auch einschlagen. Ich will nämlich einige spezielle historisch gegebene Probleme behandeln. Wir haben dann den Vorteil, daß wir nicht zu allgemeine Betrachtungen bekommen. Ich will zunächst zwei Probleme behandeln: die Quadratur des Kreises und das euklidische Parallelenaxiom. Das würde dann kein mathematischer Aufbau sein, den wir

nur eventuell für eine spätere Vorlesung vorbehalten müssen.

Wir fangen also mit der Quadratur des Kreises an. Der Kreis ist schon lange Gegenstand der mathematischen Spekulation gewesen. Ich erinnere Sie an die Zahlentheorie, die Kreisteilungszahlen, ferner an die Integralrechnung, die Rektifikation des Kreises. Dann gibt es Teile der Geometrie, die Kreisgeometrie, bei der der Kreis als Element zu Grunde liegt; es gibt eine ganze, sehr interessante und weit durchgeführte Geometrie des Kreises.

Wir wollen nun einmal auf

die Frage aufmerksam werden, auf die das Problem der Quadratur des Kreises uns führt. Da wissen wir, daß Inhalt und Umfang durch die Formeln

$$J = \pi r^2 \qquad U = 2\pi r$$

gegeben sind. Bestimmung des Inhalts und Umfangs kommen also auf die Kenntnis der Zahl π hinaus. Nehmen wir $r = 1$, so ist

$$J = \pi \qquad U = 2\pi$$

Diese Zahl π ist ja nun berechnet worden:

$$\pi = 3,1415926535 89793 \ldots$$

Nun würde also das Problem der Quadratur des Kreises hiernach darin

bestehen, die Zahl π zu konstruieren." Mit diesem Begriff der geometrischen Konstruierens werden wir uns jetzt einige Vorlesungen lang beschäftigen müssen.

§. 1. In der elementaren Geometrie ist dieser Begriff ein wohl leicht aufzufassender und streng zu definierender. Dort ist eine Konstruktion ausführbar, wenn man sie allein mit Hilfe von Lineal und Zirkel ausführen kann, d.h. wenn sie auf folgende Aufgaben zurückführbar ist:

1.) Zwei Punkte durch eine Gerade zu verbinden.

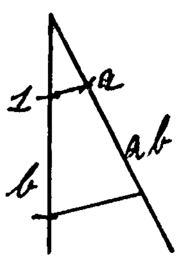
2.) Einen Kreis durch einen gegebenen Punkt um einen gegebenen

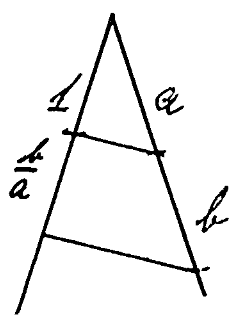
Punkt als Mittelpunkt zu ziehen.

3.) Die Schnittpunkte von gegebenen Geraden und Kreisen zu konstruieren.

Nun fragt es sich aber, welche komplizierteren Aufgaben kann man hierauf zurückführen, und später fragt es sich, fällt unter diese Probleme die Quadratur des Kreises?

Nun würde die Frage entstehen, wodurch ist der Kreis von Aufgaben charakterisiert, die mit Hilfe von Lineal und Zirkel ausführbar sind. Um das zu beantworten, haben wir uns nötig, die Buchstabenrechnung einzuführen.

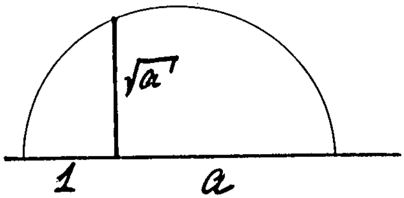

1
a
ab
b


1
a
b/a
b

Wir nehmen eine Strecke, der wir die Zahl 1 erteilen. Allen andern Strecken erteilen wir Buchstaben. Wenn wir dann eine Reihe weiterer Strecken

$a, b, c, \ldots$

haben, was können wir dann für andere Strecken konstruieren? Sind das etwa Strecken, die elementaren Rechnungsoperationen entsprechen? Wir finden leicht, daß wir Summe und Differenz mit Lineal und Zirkel konstruieren können. Auch das Produkt ist konstruierbar, wie die Figur zeigt, ebenso wie der Quotient. Wir sehen also, die vier Rechnungsspecies sind auf



√a
1
a

jeden Fall ausführbar. Nun kann ich aber auch die Quadratwurzel aus irgend einer Strecke ziehen, wie die Figur erkennen läßt. Zu den vier Spezies tritt also noch die Operation des Quadratwurzelziehens. Nun können wir aber auch umgekehrt sagen, daß damit der Bereich der algebraischen Operationen abgeschlossen ist; wir können den Satz aufstellen: Jede durch Lineal und Zirkel konstruierbare Strecke und nur diese kann durch diese fünf Operationen aus der Einheitsstrecke dargestellt werden.

Der Beweis hierfür ist sehr leicht ausführbar; ich will ihn aber

nur skizzieren. Wenn man eine Strecke konstruieren kann, so kommt das darauf hinaus, daß man einen Punkt konstruiert. Ich denke mir ein rechtwinkliges Koordinatensystem zu Grunde legt. Dann heißt unsere Aufgabe, daß wir eine lineare Gleichung, wenn wir es mit einer Geraden, eine quadratische

$$x^2+y^2+Ax+By+C=0,$$

wenn wir es mit einem Kreise zu tun haben, bekommen. Wenn man aber irgend welche Gleichungen dieser Form kombiniert, so ist nur die Auflösung von quadratischen Gleichungen erforderlich, d.h. wir erhalten

nur die fünf Operationen.

Nun würde dann die Frage sein, ob bestimmt vorgelegte Aufgaben diesem Bereiche angehören. Da wollen wir das Problem der Kubusverdoppelung behandeln, ein altes klassisches Problem. Wenn der gegebene Kubus den Inhalt 1 hat, so wird der gesuchte den Inhalt 2 haben. Seine Kante ist also

$$\sqrt[3]{2},$$

und es fragt sich nun, ob wir diese Zahl mit Lineal und Zirkel konstruieren können. Das ist ein algebraisches Problem. Wir nehmen an, die Zahl sei durch Quadratwurzeln darstellbar, und wir werden zeigen, daß wir

dadurch auf einen Widerspruch kommen.

Da müssen wir zunächst zeigen, daß es nicht möglich ist, $\sqrt[3]{2}$ ohne Quadratwurzeln, d.h. durch die vier Species allein darzustellen. Durch diese erhalten wir die rationalen Zahlen; es sei also

$$\sqrt[3]{2} = \frac{a}{b}.$$

Wir können annehmen, daß a und b teilerfremd sind. Dann folgt

$$2 = \frac{a^3}{b^3}$$

$$2b^3 = a^3$$

2 muß in a aufgehen:

$$a = 2a'$$

Dann erhalte ich

$$2b^3 = 2^3 a'^3$$

$$b^3 = 2^2 a'^3$$

und hier kommt der Primteiler 2 auf der rechten Seite vor. Also muß b durch 2 teilbar sein; das widerspricht aber unserer Voraussetzung, da a und b beide den Teiler 2 hätten. $\sqrt[3]{2}$ ist also keine rationale Zahl.

Jetzt nehmen wir an, es sei $\sqrt[3]{2}$ durch einen Ausdruck, der sich aus Quadratwurzeln aufbaut, darstellbar. Dann wird es in diesem sicher vorkommen, daß zum ersten Male aus einer rationalen Zahl eine Quadratwurzel gezogen wird; das sei etwa $\sqrt{13}$. Diese

adjungiere ich dem Bereich der rationalen Zahlen. Bezeichne ich diesen mit

$$(1),$$

so betrachte ich jetzt also den Bereich

$$(1, \sqrt{13}).$$

Jetzt könnte es sein, daß $\sqrt[3]{2}$ schon in diesem Bereich liegt. Dann nenne ich ihn den „kritischen" Bereich und (1) den „vorkritischen". Sonst gehe ich weiter und adjungiere die nächste Quadratwurzel, etwa $\sqrt{2+\sqrt{13}}$; ich betrachte also den Bereich

$$(1, \sqrt{13}, \sqrt{2+\sqrt{13}})$$

Ist $\sqrt[3]{2}$ durch diesen Bereich darstellbar, so nenne ich diesen den kritischen und den vorhergehenden Bereich den vor-

kritischen. Es muß also auf jeden Fall einen kritischen und einen vorkritischen Bereich geben.

Der kritische Bereich ist dadurch charakterisiert, daß in ihm Zahlen der vorkritischen Bereiches

$$\alpha, \beta, \ldots$$

vorkommen, und außerdem noch

$$\Gamma = \sqrt{\gamma},$$

wo γ eine Zahl des vorkritischen Bereiches ist, während Γ ihm nicht angehört. Der kritische Bereich hat also die Form

$$(\alpha, \beta, \ldots, \Gamma)$$

Nun wird es nicht sehr schwer sein, zu zeigen, daß die Annahme

einer solchen kritischen Bereiches auf einen Widerspruch führt. Denn wenn ein kritischer Bereich existiert, so ist

$$\sqrt[3]{2} = \lambda\cdot\Gamma + \mu,$$

wo λ und μ Zahlen des vorkritischen Bereiches sind. Die Funktion ist linear, da

$$\Gamma^2 = j$$

dem vorkritischen Bereiche angehört. Nun folgt

$$2 = \lambda^3\Gamma^3 + 3\lambda^2\Gamma^2\mu + 3\lambda\Gamma\mu^2 + \mu^3$$
$$= 3\lambda^2 j\mu + \mu^3 + \Gamma(\lambda^3 j + 3\lambda\mu^2)$$

Es ist $\lambda \neq 0$, denn sonst wäre

$$\sqrt[3]{2} = \mu$$

im vorkritischen Bereich gelegen.

Γ hat den Faktor

$$\lambda(\lambda^2 f + 3\mu^2)$$

Es ist

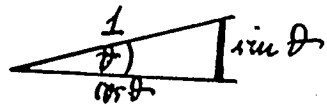
$$f > 0,$$

da Γ reell sein soll. Also ist der Faktor von Γ > 0, und es folgt

$$\Gamma = \frac{2 - (3\lambda^2 f\mu + \mu^3)}{\lambda^3 f + 3\lambda\mu^2},$$

d.h. Γ liegt im vorkritischen Bereich, und das darf nicht sein. Damit ist der Beweis geführt, daß die Kubusverdoppelung nicht zu den mit Lineal und Zirkel lösbaren Problemen gehört.

Nun können wir der Reihe nach noch einige weitere Probleme und Defi-


1
θ
cos θ
sin θ

gaben durchgehen; doch wollen wir das nicht besonders ausführlich machen.

Eine der einfachsten Aufgaben ist die Halbierung eines beliebigen Winkels ϑ. $\cos\vartheta$ und $\sin\vartheta$ sind gegebene Strecken. Um den halben Winkel zu haben, muss ich $\cos\frac{\vartheta}{2}$ resp. $\sin\frac{\vartheta}{2}$ berechnen, und das ist im Augenblick gemacht. Denn es ist

$$\cos\frac{\vartheta}{2} = \sqrt{\frac{\cos\vartheta + 1}{2}},$$

also die Winkelhalbierung möglich; die Konstruktion ist ja bekannt.

Wir wollen aber einmal so sagen: den Winkel halbieren heißt: aus $\cos\vartheta$ und $\sin\vartheta$ $\cos\frac{\vartheta}{2}$ zu finden. Nun bilde ich die komplexe Zahl

$\cos\vartheta + i\sin\vartheta$

Bekanntlich ist

$$\cos\vartheta + i\sin\vartheta = \left(\cos\frac{\vartheta}{2} + i\sin\frac{\vartheta}{2}\right)^2$$

Also heißt das: aus einer gegebenen komplexen Zahl die Quadratwurzel zu ziehen. Wir hatten aber vorhin nur aus einer reellen Zahl die Quadratwurzel zu ziehen brauchen. Man kann also vermuten, daß man aus einer komplexen Zahl die Quadratwurzel ziehen kann nur unter Anwendung unserer fünf Operationen. Das geht in der Tat. Denn wir setzen an:

$$\sqrt{\alpha + i\beta} = \xi + i\eta$$

Daraus folgt

$$\alpha = \xi^2 - \eta^2$$
$$\beta = 2\xi\eta$$

und wir haben

$$\alpha^2+\beta^2=(\xi^2+\eta^2)^2$$

$$\xi^2+\eta^2=\sqrt{\alpha^2+\beta^2}$$

$$\xi^2=\frac{1}{2}\left(\alpha+\sqrt{\alpha^2+\beta^2}\right)$$

$$\xi=\sqrt{\frac{1}{2}\left(\alpha+\sqrt{\alpha^2+\beta^2}\right)}$$

$$\eta=\sqrt{\frac{1}{2}\left(-\alpha+\sqrt{\alpha^2+\beta^2}\right)}.$$

Es ist also wirklich möglich, aus einer komplexen Zahl die Quadratwurzel zu ziehen, aber man braucht zwei übereinandergetürmte Quadratwurzeln. Wir haben nun gesehen, das Problem der Winkelhalbierung kommt darauf hinaus, aus einer komplexen Zahl die Quadratwurzel zu ziehen. Wie kommt es nun, daß dabei nur

eine Quadratwurzel auftritt. Das liegt daran, daß die Zahl, aus der wir die Quadratwurzel zu ziehen hatten, eine ganz spezielle Form hatte; es war nämlich ihr absoluter Betrag gleich 1. Und in der Tat reduzieren sich in dem Fall

$$\alpha^2+\beta^2=1$$

ξ und η auf eine Quadratwurzel, und es ist

$$\frac{\xi}{\eta} = \sqrt{\frac{\alpha+1}{-\alpha+1}} = \sqrt{\frac{(\alpha+1)^2}{\beta^2}} = \frac{\alpha+1}{\beta}$$

$$\eta = \frac{\beta\xi}{\alpha+1}$$

Also braucht man in der Tat nur eine Quadratwurzel zu ziehen, nämlich

$$\xi = \sqrt{\tfrac{1}{2}(\alpha+1)}$$

Wir würden dann zur Dreiteilung eines beliebigen Winkels kommen. Dabei will ich mich aber nicht länger aufhalten. Die Dreiteilung erfordert aus einer komplexen Zahl mit dem absoluten Betrag 1 die dritte Wurzel zu ziehen. Diese Aufgabe ist nicht immer lösbar, nur in ganz speciellen Fällen, z. B. beim Vollwinkel. Der strenge Nachweis wird genau analog dem Nachweis geführt, daß $\sqrt[3]{2}$ nicht konstruierbar ist. So ist also das berühmte Problem der Trisektion des Winkels mit Lineal und Zirkel nicht lösbar.

Nun würden aber einige speciel-

le lösbare Fälle kommen, z. B. läuft die Dreiteilung eines rechten Winkels auf die Konstruktion eines gleichseitigen Dreiecks hinaus. Wir wollen die Teilung des Vollwinkels in p gleiche Teile betrachten, wo p eine Primzahl ist. Mit anderen Worten: wie verhält es sich mit der Konstruktion des regulären p-Ecks?
Der Winkel ist gegeben durch

$$\cos\vartheta + i\sin\vartheta$$

und es ist

$$(\cos\vartheta + i\sin\vartheta)^{\frac{1}{p}} = \cos\frac{\vartheta}{p} + i\sin\frac{\vartheta}{p}$$

Für den Vollwinkel haben wir also

$$\sqrt[p]{1} = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p} = e^{\frac{2i\pi}{p}} = \varrho$$

Wir haben somit die Aufgabe, die Gleichung

$$\varrho^p = 1$$

zu lösen. Das ist die berühmte Kreisteilungsgleichung. Diese ist für $p=3$ sofort lösbar; denn sie hat die Wurzel

$$\rho=1,$$

und nach deren Abspaltung bleibt die quadratische Gleichung

$$\rho^2+\rho+1=0$$

übrig.

Nun käme $p=5$:

$$\rho^5=1.$$

Durch Abspaltung folgt

$$\rho^4+\rho^3+\rho^2+\rho+1=0$$

Hier führen wir ein

$$\rho+\frac{1}{\rho}=\varphi$$

und erhalten

$$\varphi^2+\varphi-1=0$$

Wir haben also lauter quadratische

Gleichungen, d.h. das reguläre Fünfeck ist konstruierbar.

Nun komme

$$\rho^7 = 1,$$

und hier kommen wir auf eine kubische Gleichung. Denn wir erhalten

$$\rho^6+\rho^5+\rho^4+\rho^3+\rho^2+\rho+1=0$$

und wieder durch die Transformation

$$\rho+\frac{1}{\rho}=\varphi$$

$$\varphi^3+\varphi^2-2\varphi-1=0,$$

und das ist eine kubische Gleichung. Nun läßt sich wieder zeigen, diese kubische Gleichung ist nicht auflösbar durch Quadratwurzeln; also ist die Konstruktion des regulären 7-Ecks nicht möglich

Wann ist nun allgemein die Gleichung

$$x^p = 1$$

durch Quadraturseh lösbar? Es ist

$$(x^p - 1) = (x-1)(x^{p-1} + x^{p-2} + \dots + x + 1)$$

Es bleibt also die Gleichung $(p-1)$ten Grades

$$x^{p-1} + x^{p-2} + \dots + x + 1 = 0$$

Diese Gleichung ist irreduzibel im Bereiche (1), wie in der Algebra gezeigt wird. Ferner wird dort bewiesen, daß diese Gleichung nur dann durch Quadraturreihe gelöst werden kann, wenn

$$p - 1 = 2^r$$

ist, und nun kann gezeigt werden, daß diese notwendige Bedingung auch

hinreichend ist.

Aus

$$p = 2^{\nu} + 1$$

liest man sofort ab, daß

$$\nu = 2^{\mu}$$

ist. Denn wäre

$$\nu = u \cdot v,$$

wo u eine ungerade Zahl ist, so hätte ich

$$p = 2^{u \cdot v} + 1$$

Ich setze

$$2^{v} = V,$$

und habe

$$p = V^{u} + 1,$$

und das ist ganz gewiß keine Primzahl, denn es ist teilbar durch $V+1$, weil

n eine ungerade ganze Zahl ist. Ein reguläres p-Eck ist also dann und nur dann durch Lineal und Zirkel konstruierbar, wenn

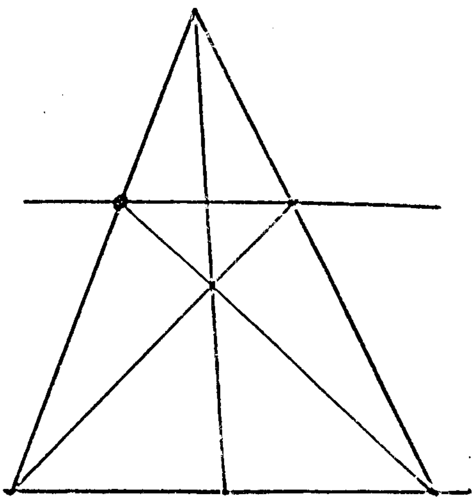
$$p = 2^{2^n} + 1$$

ist. Wir wollen sehen, ob es solche Primzahlen gibt. Dazu machen wir folgende Tabelle

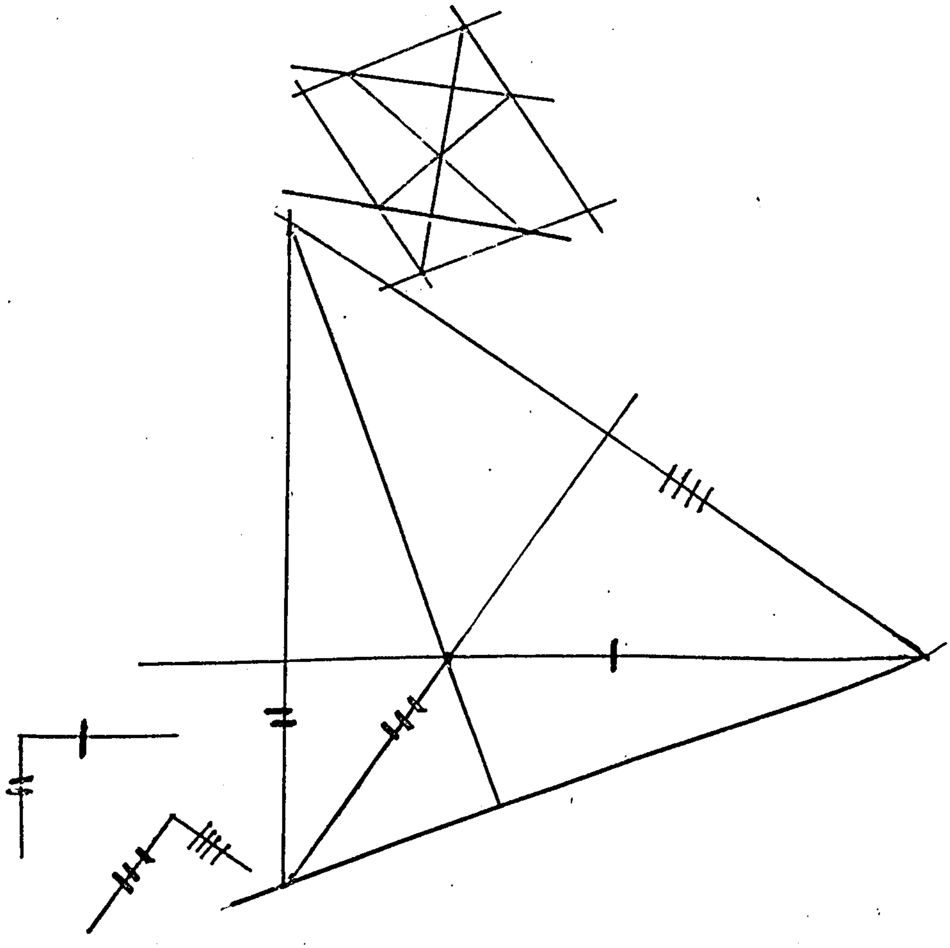
n	p
1	5
2	17
3	257
4	65537
5	4 294 967 297

Die letzte Zahl ist aber keine Primzahl mehr, sondern durch 641 teilbar. Ob es darüber hinaus noch Primzahlen dieser Form gibt, ist nicht bekannt.

Nun wollen wir von Konstruktionen sprechen,



die mit dem Lineal allein zu bewerkstelligen sind. Das Quadraturenproblem zu ziehen fällt dann weg; aber auch Parallelen können wir dann nicht mehr ziehen. Wir können nur Konstruktionen ausführen, die für die projektive Geometrie charakteristisch sind, z. B. die von harmonischen Punkten; aber wir können nicht die eigentlichen Aufgaben der cartesischen Geometrie lösen. Wir müssen also noch ein Hilfsmittel hinzunehmen, indem wir z. B. zwei Parallele oder auch eine halbierte Strecke geben. Dann können wir z. B. zu dieser Strecke durch einen beliebigen Punkt die Parallele ziehen. Natürlich ist das auch umgekehrt so: Kennt man die Parallelen, so kann man aus ihnen den Mittelpunkt der Strecke finden

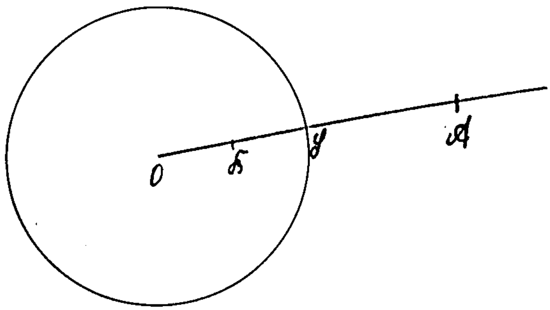


Sind nun zwei Paar Parallele in verschiedenen Richtungen gegeben, so läßt sich leicht zeigen, daß man zu jeder Geraden die Parallele ziehen kann. Wir können auch sagen, es muß noch ein Parallelogramm gegeben sein. Man kann also jetzt die rationalen Operationen alle ausführen. Man kann aber z. B. noch nicht den rechten Winkel konstruieren. Wir wollen daher einen als gezeichnet geben. Man kann sich aber leicht wieder überlegen, daß man mit einem rechten Winkel nicht auskommt, um alle rechten Winkel zu konstruieren. Wenn man aber zwei verschiedene rechte Winkel hat, so kann man alle rechten Winkel konstruieren, d. h. von einem gegebenen Punkte auf eine gegebene Gerade das Lot fällen.

Das wäre über Lineal allein zu sagen. Nun kann man auch fragen, was man mit dem Zirkel allein machen kann. Damit können wir nun alles machen, was man mit Lineal und Zirkel allein machen kann. Das ist natürlich so gemeint, daß man alle Punkte finden kann, deren Konstruktion mit Lineal und Zirkel ausführbar ist. Alle Punkte einer Strecke können nicht gezeichnet werden, aber jeder Punkt der Strecke kann gefunden werden, z. B. der Mittelpunkt.

Um unsere Behauptung zu erweisen, brauchen wir nur folgende zwei Aufgaben mittels des Zirkels allein zu lösen:

1.) Einen gegebenen Kreis, der durch



O
S
y
A

seinen Mittelpunkt und einen Punkt der Peripherie gegeben ist, und eine durch zwei ihrer Punkte gegebene Gerade zu schneiden.

2.) Zwei durch je zwei ihrer Punkte gegebene Strecken zu schneiden.

Die erste Aufgabe ist verhältnismäßig leicht zu lösen; die zweite macht schon mehr Schwierigkeiten. Ich will Ihnen das Prinzip mitteilen, mit dessen Hilfe diese Aufgaben zu lösen sind, das ist das Spiegelungsprinzip.

Wir bestimmen den Punkt B so, daß

$$OA \cdot OB = OS^2$$

ist. Dann heißt B das Spiegelbild von A an dem Kreise. Läßt man A einen Kreis durchlaufen, so durchläuft auch B einen Kreis. Trifft der Kreis durch A den Punkt O,

so wird sein Spiegelbild eine gerade Linie durch O und umgekehrt.

Auf diesem Prinzip ruht nun der Beweis des Satzes, daß jede Konstruktion, die durch Lineal und Zirkel ausgeführt werden kann, auch mit dem Zirkel allein ausführbar ist. Ich kann z. B. mit Hilfe unseres Prinzips durch den Zirkell allein folgende Aufgabe lösen: Den Spiegelpunkt eines gegebenen Punktes zu finden. Wenn man einen Kreis mit gegebenem Mittelpunkt hat, so kann man den Kreis finden, der sein Spiegelbild ist. Daher kann man nun den Schnittpunkt zweier Geraden finden, indem man beide an einem Kreise spiegelt, die Bilder zum Schnitt bringt,

und dann den Schnittpunkt wieder am Kreise spiegelt. Sie können sich nach diesen Andeutungen den vollständigen Beweis zurechtlegen.

Jetzt haben wir gesehen, daß wir wohl das Lineal, nicht aber den Zirkel entbehren können. Nun wollen wir aber doch mal sehen, ob man nicht in gewissem Sinne den Zirkel entbehrlich machen kann, indem man sich nämlich einen einzigen Kreis mit Mittelpunkt gezeichnet gibt. Das ist eine Aufgabe, die Steiner gelöst hat.

Es ist wichtig, daß man sich den Mittelpunkt des Kreises gibt; denn mit dem Lineal allein kann man sich niemals den Mittelpunkt des Kreises verschaffen. Das möchte ich Ihnen folgendermaßen beweisen. Wir führen ein

gewöhnlicher Cartesischer Koordinatensystem ein, dessen Nullpunkt der Mittelpunkt des Kreises ist. Dieser hat die Gleichung

$$x^2+y^2=1$$

Angenommen, es gäbe eine Konstruktion mit Lineal allein, vermöge derer wir den Mittelpunkt konstruieren können. Dann muß es schließlich zwei gerade Linien geben, die durch den Nullpunkt gehen. Dann wende ich auf die ganze x-y-Ebene folgende lineare Transformation an:

$$x=\frac{4x'}{5+3y'}, \quad y=\frac{3+5y'}{5+3y'}$$

Hierbei bleiben alle geraden Linien gerade, da x und y denselben Nenner haben. Unser Kreis geht über in:

$$16x'^2+(3+5y')^2=(5+3y')^2$$

oder

$$x'^2+y'^2=1$$

Er geht also in sich über. Jede Gerade ist verändert, aber wieder in eine Gerade übergegangen. Führt man unsere erste Konstruktion auf den Mittelpunkt, so muß die zweite, die transformierte, es auch tun. Das ist aber sicher nicht der Fall, denn dem Punkt

$$x=0,\ y=0$$

entspricht im neuen Koordinatensystem

$$x'=0,\ y'=\frac{3}{5}$$

Wir bekommen also gar nicht den Mittelpunkt, sondern die neue Konstruktion gibt einen ganz anderen Punkt.

Dies Prinzip kann man noch aus-

darum, wie es Herr Bauer 1912 in den Math. Annalen getan hat. Ich stellte seinerzeit die Vermutung auf, daß man mit mehreren Kreisen ganz gewiß den Mittelpunkt finden kann. Das Resultat ist folgendes: Wenn zwei Kreise gegeben sind, so kann man die Mittelpunkte dann und nur dann finden, wenn die Kreise sich schneiden.

Für drei Kreise, (die sich alle nicht schneiden, denn sonst hätten wir den vorigen Fall,) ist es gelungen, eine Konstruktion zu finden, um den Mittelpunkt zu erhalten. Die Kreise müssen aber die Bedingung erfüllen, nicht demselben Kreisbündel anzugehören, d.h. linear unabhängig zu sein.

Die erste Konstruktion ist von Adler angegeben worden.

Nun kann man noch zwischen Arten von Anwendungen des Zirkels unterscheiden. Man kann sich die Beschränkung auferlegen, den Zirkel nur zum Abtragen von Strecken zu verwenden. Ein Lineal hat man natürlich auch noch zur Verfügung. Dies gibt zu ganz hübschen elementaren Aufgaben Anlaß. Aber man kann fast alle interessanten Aufgaben der elementaren Geometrie ausführen. Es gibt allerdings auch Aufgaben, die durch den Zirkel im allgemeineren, aber nicht im engeren Sinne gelöst werden können. Da fragt es sich nun, welches ist das analytische Kriterium hierfür? Es

stellt sich heraus, daß man bei der beschränkten Anwendung der Zirkels nicht die Quadratwurzel aus einer beliebigen Zahl, sondern nur aus einer Zahl ziehen kann, die selbst Summe von Quadratzahlen konstruierbarer von Quadraten ~~zahlen~~ ist, z.B.

$$\sqrt{1+x^2},$$

mit anderen Worten, man kann die Hypotenuse konstruieren, wenn die Katheten gegeben sind. Quadratwurzeln aus ganzen Zahlen kann ich immer ziehen nach folgendem Schema:

$$\sqrt{2} = \sqrt{1+1}$$
$$\sqrt{3} = \sqrt{1+(\sqrt{2})^2}$$
$$\cdots$$

Ich kann also auch das reguläre Dreieck konstruieren; denn dazu brauche ich nur $\sqrt{3}$ zu konstruieren.

§.2. Nun wollen wir sehen, ob wir nicht Hilfsmittel höherer Art neben Lineal und Zirkel stellen können, und was für Konstruktionen dann ausführbar werden.

Es war die Quadratwurzel aus einer beliebigen Strecke konstruierbar. Es soll jetzt ein Apparat herstellbar sein, mit dem man die dritte Wurzel aus einer reellen Zahl ziehen kann. Dann wäre das Problem der Kubusverdoppelung lösbar. ~~Auch die Konstruktion des regulären 7-Ecks wäre lösbar.~~

Wir wollen nun die Trisektion eines beliebigen Winkels behandeln. Das führt darauf, die dritte Wurzel aus einer komplexen Zahl zu ziehen. Auf diese Aufgabe kommt

man auch folgendermaßen:

Es seien a, b, c, d reelle Größen, so ist die allgemeinste kubische Gleichung

$$ax^3+bx^2+cx+d=0$$

Mit Hilfe der Cardanischen Formel kann man diese Gleichung lösen, und da kommt es vor (nämlich wenn alle Wurzeln reell sind), daß man die Quadratwurzel aus einer komplexen Zahl zu ziehen hat. Das ist der Casus irreducibilis. Wir kommen also auf die Frage, ob dieser Fall seinen Namen wirklich verdient; ist es möglich, ihn zu lösen, indem man Quadrat- und dritte Wurzeln aus reellen Zahlen zieht? Ich werde Ihnen beweisen, daß das nicht der Fall ist; also trägt der Casus irreducibilis seinen Namen mit Recht. Die Konstruktion des regulären 7-Ecks führt auch auf diesen Fall.

Zum Beweise nehmen wir an, es sei möglich, die kubische Gleichung aufzulösen. Wir nehmen sie in der Form

$$x^3+ax\mp b=0$$

an. Es ist

$$x=\sqrt[3]{\frac{b}{2}+\sqrt{v}}+\sqrt[3]{\frac{b}{2}-\sqrt{v}},$$

wo

$$v=\frac{b^2}{4}+\frac{a^3}{27}=-\frac{1}{4\cdot 27}D$$

$$D=(x_1-x_2)^2(x_2-x_3)^2(x_3-x_1)^2=-27b^2-4a^3$$

ist, und wir setzen voraus

$$D>0$$

Wir nehmen den Rationalitätsbereich (1) als Grundbereich an; a und b seien rationale Zahlen. Unsere Gleichung sei in (1) irreduzibel, d.h. sie habe keine rationale Wurzel. Jetzt wollen wir beweisen, daß sie auch dadurch nicht auflös-

bar wird, daß man beliebige Quadrat- und Kubikwurzeln aus reellen Zahlen zieht. Wir nehmen das Gegenteil an; es gebe also einen Ausdruck von folgender Form:

$$x_1 = \frac{\sqrt{\sqrt[3]{\cdots}}}{\sqrt[3]{\sqrt{\cdots}}}$$

Wir überlegen uns nun wieder, daß dann ein kritischer Bereich vorhanden sein muß: Es gibt wieder eine erste Wurzel, die aus einer rationalen Zahl zu ziehen ist, etwa $\sqrt[3]{7}$; dann komme $\sqrt{2+\sqrt[3]{7}}$, u. s. w. Jedenfalls adjungieren wir die betr. Irrationalitäten dem Bereich (1). Dann muß schließlich x_1 in einem Bereich darstellbar sein. In dem Bereich (1) liegt sie noch nicht drin, und zwar muß schon eine Kubikwurzel adjungiert sein, um den

kritischen Bereich zu erhalten. Er muß also einen vorkritischen Bereich

$$(1,\alpha\ldots.)$$

geben, in dem x_1 noch nicht liegen darf. Wohl aber liegt er in dem Bereich

$$(1,\alpha\ldots,\Gamma),$$

und es ist

$$\Gamma = \sqrt[3]{J},$$

wo J dem vorkritischen Bereiche angehört. Dann hat x_1 die Form

$$x_1' = \kappa + \mu\Gamma + \nu\Gamma^2$$

und es sei

$$x_2' = \kappa + \mu\varepsilon\Gamma + \nu\varepsilon^2\Gamma^2 \qquad \varepsilon = e^{\frac{2\pi i}{3}}$$
$$x_3' = \kappa + \mu\varepsilon^2\Gamma + \nu\varepsilon\Gamma^2$$

Ich kann nun eine kubische Gleichung mit Koeffizienten des vorkritischen Bereiches bilden,

dessen Wurzeln x_1', x_2', x_3' sind:

$$x^3+\rho x^2+\sigma x+\tau=0$$

Ferner hat die Gleichung

$$x^3+ax-b=0$$

auch die Wurzel x_1, und ihre Koeffizienten liegen ebenfalls im vorbereiteten Bereich. Also genügt x_1 auch der Differenz beider Gleichungen:

$$\rho x^2+(\sigma-a)x+\tau+b=0$$

Das ist aber nicht möglich, denn dann wäre x_1 durch Quadratwurzelzeichen erhältlich. Also muß

$$\rho=0$$

$$\sigma=a$$

$$\tau=-b$$

sein, d.h. die Gleichungen stimmen überein.

und es ist

$$x_2' = x_2$$
$$x_3' = x_3 .$$

und das sind reelle Zahlen, also muß sein

$$x_2' = \kappa + \mu\varepsilon\Gamma + \underbrace{\nu\varepsilon^2\Gamma^2}_{=\nu(-1-\varepsilon)\Gamma^2} = \text{reell}$$

d.h.

$$\mu\Gamma - \nu\Gamma^2 = 0$$

und da $\Gamma = 0$

$$\mu - \nu\Gamma = 0$$

Es ist $\nu \neq 0$, denn sonst wäre $\mu = 0$, und die kubische Gleichung hätte drei gleiche Wurzeln, d.h. sie wäre reduzibel in (R). Also ist

$$\Gamma = \frac{\mu}{\nu}$$

d.h. Γ läge im vorgeschriebenen Bereich. Damit

haben wir also bewiesen, daß unsere Annahme, es sei die kubische Gleichung lösbar, auf einen Widerspruch führt.

Wir wollen nun weiter sehen, was für andere Hilfsmittel wir noch hinzuziehen können, um den Kreis der lösbaren Aufgaben zu erweitern. Wir wollen uns einen Apparat denken, der es erlaubt, jede kubische Gleichung zu lösen. Ich will hier nur ein Mittel angeben, das analog zu dem ist, das Steiner angegeben hat, um den Zirkel entbehrlich zu machen. Es sei die gleichseitige Hyperbel durch den Punkt (1,1):

$$xy = 1$$

gezeichnet gegeben. Ich behaupte, dann kann man jede kubische Gleichung lösen, also

auch jede biquadratische, da diese durch Kubik- und Quadratwurzeln lösbar ist.

Um meine Behauptung zu beweisen, gehe ich aus von der Gleichung eines beliebigen Kreises

$$x^2+y^2+ax+by+c=0,$$

der durch den Punkt (1,1) geht; es muß also

$$a+b+c+2=0$$

sein. Nun wollen wir von diesem Kreise die Abszissen seiner Schnittpunkte mit der Hyperbel berechnen. Dazu setzen wir

$$y=\frac{1}{x}$$

und erhalten

$$x^2+\frac{1}{x^2}+ax+\frac{b}{x}+c=0$$

Das ist eine Gleichung 4ten Grades. Mit

$$a+b+c+2=0$$

reduciert sie sich aber auf den Grad 3, da wir $x-1$ abspalten können. Diese kubische Gleichung ist

$$x^3+(a+1)x^2+(a+c+1)x-1=0.$$

Ich will nun die Wurzeln einer beliebigen vorgelegten kubischen Gleichung bestimmen. Das kann ich offenbar machen, wenn die vorgelegte Gleichung die Form

$$x^3+\alpha x^2+\beta x-1=0$$

hat; denn ich setze

$$a=\alpha-1$$

$$c=\beta-\alpha$$

$$b=-\alpha+1-\beta+\alpha-2=-\beta-1$$

und zeichne den Kreis

$$x^2+y^2+ax+by+c=0$$

Dieser geht durch den Punkt (1,1), und die Abscissen der anderen Schnittpunkte genügen der gegebenen Gleichung. Also brauche ich nur die Abscissen zu konstruieren. Entweder sind alle drei reell, oder aber es ist eine reell; die andern bestimmen sich aus einer quadratischen Gleichung, lassen sich also mit Zirkel und Lineal konstruieren.

Nun ist aber sehr leicht zu sehen, daß ich die Wurzeln einer allgemeinen kubischen Gleichung auch konstruieren kann. Die Gleichung sei auf

$$y^3 + Ay^2 + b = 0$$

zurückgeführt, was mit Lineal und Zirkel zu machen ist. Ich setze

$$y = \frac{A}{3} \cdot \frac{x+2}{x-1}$$

Dies ist eine mit Lineal und Zirkel ausführbare Transformation. Dann geht unsere Gleichung über in:

$$\left(\frac{A}{3}\right)^3 \left(\frac{x+2}{x-1}\right)^3 + \left(\frac{A}{3}\right)^2 \cdot A \left(\frac{x+2}{x-1}\right)^2 + B = 0$$

Dies ist aber eine Gleichung der verlangten Gestalt; denn der Koeffizient von x^3 ist:

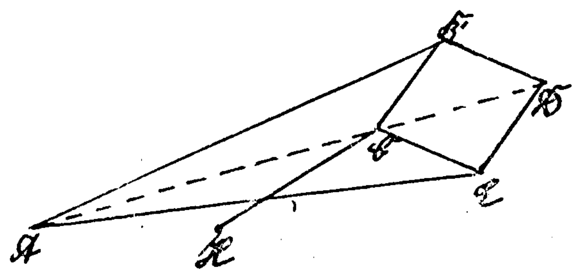
$$\left(\frac{A}{3}\right)^3 + A \cdot \left(\frac{A}{3}\right)^2 + B = B + \left(\frac{A}{3}\right)^2 \cdot \frac{4}{3} A$$

Ferner wird das von x freie Glied:

$$\left(\frac{A}{3}\right)^3 \cdot 2^3 + \left(\frac{A}{3}\right)^2 \cdot A \cdot 2^2 + B = B + \left(\frac{A}{3}\right)^2 \cdot \frac{4}{3} A$$

Die Koeffizienten stimmen aber überein, d. h. wir erhalten unseren alten Typus, wenn wir noch statt x $-x$ würden.

Es ist nun sehr naheliegend, den Mechanismus des Zirkels selbst zu verallgemeinern. Der Zirkel ist ein Gelenkmechanismus mit einem Freiheitsgrad. Da ist er der einfachste Mechanismus in dieser Art. Die Frage ist nun, kann man mit komplizierteren Mechanismen kompliziertere Aufgaben lösen? Es läßt sich zeigen, daß man mit einem geeigneten Gelenkmechanismus jede algebraische Kurve konstruieren kann. Daß man nur algebraische Kurven konstruieren kann, ist selbstverständlich, denn es sind die Gelenke starr miteinander verbunden; es können also nur algebraische Bedingungen vorhanden sein. Den Beweis dieses Satzes will ich nicht durchführen.


A
K

Die einfachste algebraische Kurve ist die gerade Linie. Gibt es einen Gelenkmechanismus, um die gerade Linie zu konstruieren? Ja, das ist die Geradführung. Diese hat zwei Fixpunkte: A und H. Man macht

$$AH = CH$$
$$AE = AB$$
$$CE = CB = ED = BD$$

BCED ist also ein Rhombus. D trägt den Bleistift. Der ganze Apparat hat nur einen Freiheitsgrad; es wird behauptet, daß D eine gerade Linie beschreibt, wenn C einen Kreis um H befährt.

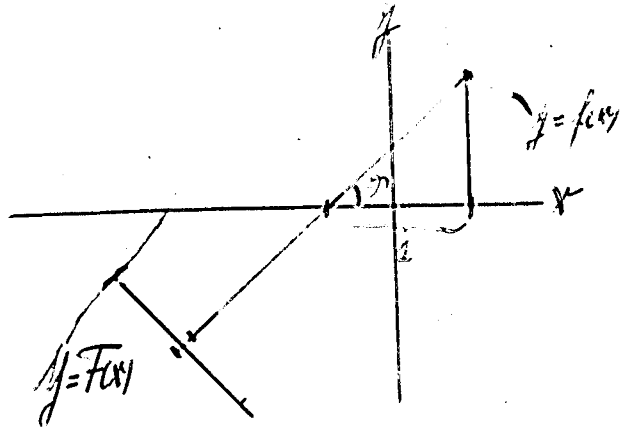
Beweis: A, C und D liegen auf einer geraden Linie, B und E auf einem Kreise um

A. C und D sind so gewählt, daß sie Spiegelbilder in Bezug auf diesen Kreis sind, und

$$AE^2 = AC \cdot AD$$

bleibt während der ganzen Bewegung des Apparates bestehen. Wenn nun C einen Kreis, der wegen $AH = CH$ durch A geht, beschreibt, so beschreibt D eine Gerade, q. e. d.

Zum Schluß möchte ich noch des Integraphen gedenken. Dieser besteht in einem längs der x-Achse verschiebbaren rechtwinkligen Dreieck, dessen eine Kathete von der Länge 1 auf der x-Achse liegt. Die andere trägt den Fahrstift. Dieser ist auf der Kathete verschiebbar. Senkrecht zu der verlängerten Hypotenuse ist eine Stange verschiebbar, welche eine Schnei-


y
y = f(x)
x
y = F(x)

de trägt, die sich nur parallel der Hypotenuse bewegen kann. $y = f(x)$ sei die Kurve, die von dem Fahrstift beschrieben wird. Es ist

$$\operatorname{tg} \vartheta = y = f(x)$$

Die Kurve $Y = F(x)$, die von der Schneide beschrieben wird, hat die Richtung ϑ

$$\frac{dY}{dx} = \operatorname{tg} \vartheta = f(x);$$

das ist

$$Y = \int f(x)\,dx$$

Die Schneide beschreibt also die Integralkurve von $y = f(x)$.

Es sei z. B.

$$y = \sqrt{1-x^2}$$

ein Kreis um den Nullpunkt. Die Integralkurve

$$\int_0^x \sqrt{1-x^2}\,dx = \frac{1}{2}\arcsin x + \frac{x}{2}\sqrt{1-x^2} - \frac{\pi}{4}$$

also

$$\int_0^{+1} \sqrt{1-x^2}\,dx = \frac{\pi}{4}$$

Wir können daher mit den Integralen die Zahl π konstruieren.

Damit sind wir auf unser altes Problem zurückgekommen. Sie sehen, es kommt ganz darauf an, welche Hilfsmittel erlaubt sind, um über die Konstruierbarkeit einer Zahl zu entscheiden.

§. 3. Jetzt wollen wir das Problem der Quadratur des Kreises wesentlich in Angriff nehmen. Wir wollen sehen, wie historisch das Problem entstanden ist, und in welchem Sinne es heute als vollständig gelöst angesehen werden kann.

Die erste Periode in der Geschichte unseres Problems haben wir als die naive

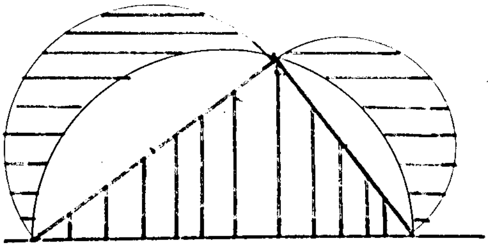
Periode zu beschreiben. Sie reicht von den ersten Anfängen bis zur Erfindung der Differential- und Integralrechnung. Ich sage naive Periode, weil es da vor allen Dingen darauf ankam, mit elementaren Hilfsmitteln näherungsweise Quadraturen der Zahl π herzustellen.

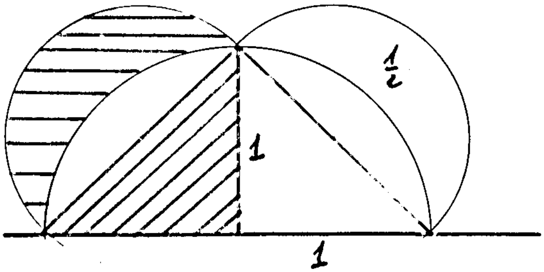
Aus der allerersten Zeit dieser Periode können wir erwähnen, daß in einem alten ägyptischen mathematischen Handbuch (ca. 2000 v. Chr.) sich folgender Wert von π findet:

$$\pi = \left(\frac{4}{3}\right)^4 = 3,16\ldots$$

Dieser Wert ist nicht sehr gut, aber immerhin besser als der, welcher sich in der Bibel findet:

$$\pi = 3$$




1/2
1
1

Dann kommen wir auf Spekulationen, die nicht den Kreis selbst, sondern von Kreisbogen begrenzte Figuren quadrieren wollen. Dazu gehören die Lunulae des Hippokrates; diese lassen sich quadrieren. Man hat dies Problem auch noch verallgemeinert; doch hat diese Aufgabe auf keine schönen Resultate geführt, und ich möchte darüber hinweggehen.

Der erste, der systematisch an die Berechnung von π geht, ist Archimedes. Er fand

$$\pi = \frac{22}{7}$$

Das Mittel, das er anwandte, und das später sehr vervollkommnet wurde, ist das der eingeschriebenen und umgeschriebenen regulären Polygone.

Danach ist ein Rückschlag zu verzeichnen

bis zum 15-ten Jahrhundert. Es beginnt die Zeit der sog. Quadratoren, die das Problem der Quadratur des Kreises zu lösen suchten. Man machte angenäherte Konstruktionen, und behauptete dann, daß sie genau seien. Es ist natürlich keine Rede davon, daß diese Konstruktionen richtig waren. Im Gegenteil, sie waren außerordentlich schlecht; sie lieferten einen viel ungenaueren Wert, als es der Archimedische war.

Ende des 16-ten Jahrhunderts wird uns der andere Wert bekannt, den Archimedes noch nicht hatte:

$$\pi = \frac{355}{113}$$

Dieser Wert ist genau richtig, wenn man π durch kleinste Brüche von gegebener Größenordnung

annähern will.

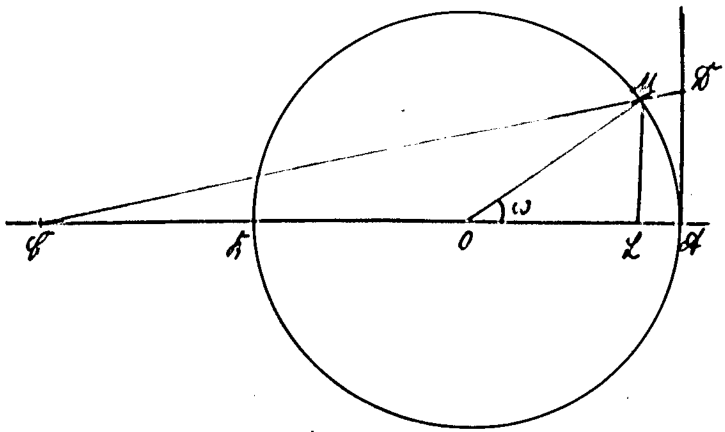
Dann kommen weitere Fortschritte. Es wurde nun die Zahl π als Dezimalbruch berechnet, und zwar sehr genau. Der erste ist hier Vieta; er tat dies mit den theoretischen Hülfsmitteln des Archimedes. Er berechnete π auf 15, endlich Ludolff, nach dem π die Ludolffsche Zahl heisst, auf 35 Stellen.

Nun kam aber Huyghens. Er nahm das Problem in systematischer Weise auf und hat eine sehr einfache Konstruktion angegeben, mit der man eine sehr genaue Annäherung erhält.

Es ist

$$OA = OB = BC \ (=1)$$

Dann ist annäherungsweise



M
D
ω
C
B
O
L
A

$$AM = AD$$

Man kann auch sehen, wie genau die Konstruktion ist. Sie ist desto genauer, je näher M an A liegt. Es ist

$$\frac{\sin\omega}{AD} = \frac{ML}{AD} = \frac{CL}{CA} = \frac{2+\cos\omega}{3}$$

$$AM = \omega$$

also

$$AM - AD = \omega - \frac{3\sin\omega}{2+\cos\omega}$$

Das können wir nach Potenzen von ω entwickeln:

$$\frac{2}{3}\cdot\frac{1}{5!}\,\omega^5 + \ldots\ldots$$

Wenn also ω klein ist, so wird der Fehler sehr unbedeutend.

Das würden die Resultate der ersten Periode sein. Wir kommen nun zu der zweiten Periode, die ich die formale nennen möchte. Sie reicht von der Erfindung der Infinitesi-

malrechnung bis zum Jahr 1761, dem Erscheinungsjahr einer Lambertschen Arbeit. Es ist die formale Periode, weil man von den prinzipiellen Fragen gänzlich absah. Es kommt jetzt nur darauf an, die reichen Hilfsmittel, welche die Differential- und Integralrechnung bietet, für die Aufstellung von Ausdrücken für π zu verwerten. Ich möchte Ihnen drei Arten derselben vorführen: Summen-, Produkt- und Kettenbruchentwicklungen.

$$\left.\begin{aligned}
&1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots\cdots=\frac{\pi^2}{6}\\
&1+\frac{1}{2^4}+\frac{1}{3^4}+\cdots\cdots=\frac{\pi^4}{90}\\
&1+\frac{1}{3^2}+\frac{1}{5^2}+\frac{1}{7^2}+\cdots\cdots=\frac{\pi^2}{8}\\
&1-\frac{1}{3^2}+\frac{1}{5^2}-\frac{1}{7^2}+\cdots\cdots=\frac{\pi^2}{32}\\
&\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}\right\}\ \text{Eulersche Reihen.}$$

Leibnizsche Reihe:

$$1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\dots=\frac{\pi}{4}$$

Diese Reihen lassen sich alle aus einem einheitlichen Prinzip ableiten:

$$\frac{1}{e^{x}-e^{-x}}=\frac{1}{x}-\frac{2x}{\pi^2-x^2}+\frac{2x}{4\pi^2-x^2}-\frac{2x}{9\pi^2-x^2}+\dots,$$

wenn man nach Potenzen von x entwickelt. Die Leibnizsche Reihe erhält man besonders leicht aus

$$\operatorname{arc\,tg} x=\int_0^x\frac{dx}{1+x^2}=\int_0^x dx\left(1-x^2+x^4-x^6+\dots\right)$$

für $x=1$.

Nun kommen wir zu Produktentwicklungen. Wir können nur eine gleich aus unserer ersten Reihe verschaffen:

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\dots=\frac{1}{1-\frac{1}{2^2}}\cdot\frac{1}{1-\frac{1}{3^2}}\cdot\frac{1}{1-\frac{1}{5^2}}\cdots$$

$$=\frac{2^2}{2^2-1}\cdot\frac{3^2}{3^2-1}\cdot\frac{5^2}{5^2-1}\cdots=\frac{\pi^2}{6}$$

Dann können solche Produktdarstellungen, die sich aus der Archimedischen Methode ableiten lassen:

$$\frac{2}{\pi} = \sqrt{\frac{1}{2}} \cdot \sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}}} \cdot \sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}}}} \cdot \ldots\ldots$$

Ferner kann man die Produktentwicklung des sin verwenden:

$$\sin \pi x = \pi x \prod_{n} \left(1 - \frac{x^2}{n^2}\right);$$

für $x = \frac{1}{2}$ ergibt sich

$$\frac{\pi}{2} = \frac{2}{1} \cdot \frac{2}{3} \cdot \frac{4}{3} \cdot \frac{4}{5} \cdot \frac{6}{5} \cdot \frac{6}{7} \cdot \frac{8}{7} \cdot \frac{8}{9} \cdots\cdots \quad \left(\text{Formel von Wallis}\right)$$

Dann können die Kettenbruchentwicklungen; ihre Ableitung ist recht mühsam. Ich will nur zwei Formeln zur Probe angeben.

$$\frac{\pi}{4} = \cfrac{1}{1+\cfrac{1}{2+\cfrac{9}{2+\cfrac{25}{2+\cfrac{49}{2+\cdots}}}}}$$

Die kann aus der Leibnizschen Reihe abgeleitet werden. Eine andere Entwicklung ist

$$\frac{\pi}{4} = \cfrac{1}{1+\cfrac{1}{3+\cfrac{4}{5+\cfrac{9}{7+\cfrac{16}{9+\cdots}}}}}$$

Die Beweise entspringen aus einem einheitlichen Satze von Gauss über die hypergeometrische Reihe; es würde mich aber zu weit führen, das vollständig zu zeigen. Es läßt sich nach dieser Methode auch die Zahl e in einen Kettenbruch entwickeln:

$$e = 2+\cfrac{1}{1+\cfrac{1}{2+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{4+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{6+\cfrac{1}{1+\cdots}}}}}}}}}$$

Die Reihenentwicklungen für π konvergieren meist sehr schlecht, sodaß die Berechnung von π nach ihnen sehr umständlich ist. Es gibt aber Methoden, nach denen man die Zahl π sehr leicht ausrechnen kann. Am einfachsten ist es, wenn man von dem Additionstheorem der tg-funktion ausgeht

$$\operatorname{tg}(\xi+\eta) = \frac{\operatorname{tg}\xi + \operatorname{tg}\eta}{1 - \operatorname{tg}\xi \operatorname{tg}\eta}$$

Daraus folgt für

$$\operatorname{tg}\xi = x \quad \operatorname{tg}\eta = y$$

$$\operatorname{arc\,tg} x + \operatorname{arc\,tg} y = \operatorname{arc\,tg}\frac{x+y}{1-xy}$$

also

$$\operatorname{arc\,tg}\frac{1}{2} + \operatorname{arc\,tg}\frac{1}{3} = \operatorname{arc\,tg} 1 = \frac{\pi}{4}$$

Ferner ist

$$\operatorname{arc\,tg} x = x - \frac{x^3}{3} + \frac{x^5}{5} - \dots$$

und nun läßt sich π sehr gut berechnen.

Man kann sich nun noch die Aufgabe stellen, π möglichst genau zu konstruieren; da hat Borel ein sehr hübsches Resultat herausbekommen:

$$\pi = \frac{10+\sqrt{2^2+15^2}}{8} = 3{,}141593\ldots$$

in Wirklichkeit 26...

Das ist eine außerordentlich einfache Konstruktion, die bis zur 6-ten Decimale genau ist.

Die prinzipielle Frage wird nun in der ~~Ent~~ dritten Periode erledigt, die ich die kritische nennen möchte. Da ist es schon ein Verdienst, mit Bewußtsein die Frage aufgeworfen zu haben, um die es sich handelt. Da würden wohl Sturm und Huyghens in Betracht kommen. Letzterer hat als erster unter den Physikern die Behauptung

aufgestellt, daß die Konstruktion von π mit Lineal und Zirkel nicht möglich sei. Sturm hat auch Versuche gemacht, den Beweis hierfür zu führen.

Wir werden nun eine ganze Reihe solcher Versuche durchzugehen haben; ihr Studium ist sehr instruktiv, wenn sie auch ihr Ziel nicht erreicht haben.

Sturms Versuch ist recht primitiv. Er sagte, der Umstand, daß π durch irrationale Zahlen beliebig scharf angenähert werden kann, lasse auf die Irrationalität von π selbst schließen. Das ist aber ganz verkehrt. In folgenden Beispielen wird eine irrationale Zahl durch rationale, eine rationale durch irrationale, eine rationale durch rationale,

eine irrationale durch irrationale Zahlen angenähert:

$$\sqrt{\frac{3}{2}} = \left(1+\frac{1}{2}\right)^{\frac{1}{2}} = 1 + \left(\frac{1}{2}\right)\cdot\frac{1}{2} + \left(\frac{1}{2}\right)_2\cdot\frac{1}{2^2} + \left(\frac{1}{2}\right)_3\cdot\frac{1}{2^3} + \cdots$$

$$1 = \frac{1}{\sqrt{\frac{3}{2}}} + \frac{(\ldots)}{\sqrt{\frac{3}{2}}} + \cdots$$

$$1 = \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots$$

$$\sqrt{2} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2^2} + \frac{\sqrt{2}}{2^3} + \cdots$$

Ebenso verkehrt ist ein Versuch, aus der Formel

$$\frac{\pi}{2} = \frac{2}{1}\cdot\frac{2}{3}\cdot\frac{4}{3}\cdot\frac{4}{5}\cdots$$

auf die Irrationalität von π zu schließen. Man sagte so: $\frac{\pi}{2}$ ist ein Produkt von unendlich viel Brüchen, und im Zähler stehen die geraden, im Nenner die ungeraden Zahlen. Wenn ich also irgendwo abbreche, so habe ich im Nenner

höhere Primzahlen stehen als im Zähler, die sich also nicht gegen Primzahlen im Zähler fortheben. Es kommen also unendlich viel Primzahlen vor. Daraus folgt dann die Irrationalität von $\frac{\pi}{2}$. Dagegen ist zu bemerken, daß nicht allein die Schlußweise keineswegs bindend ist, sondern auch der behauptete Satz ist nicht richtig. Denn man kann folgende ganzen Zahlen bilden:

$$p_n = \frac{2^{(n+1)!} - 1}{2^{n!} - 1} \qquad q_n = 2^{(n+1)! - n!}$$

Wenn wir nun das Produkt

$$\frac{p_1}{q_1} \cdot \frac{p_2}{q_2} \cdot \frac{p_3}{q_3} \cdot \ldots\ldots = 2$$

bilden, so sehen wir folgendes: die q sind überhaupt nur Potenzen von ~~zw~~ 2. In den Zählern dagegen kommen immer neue Prim-

zahlen vor. Denn ist p eine Primzahl, so ist

$$p \mid 2^{p-1}-1 \mid \left(2^{p-1}\right)^{\frac{(n+1)!}{p-1}}-1,$$

wenn

$$p-1 \mid (n+1)!$$

Ferner sind alle Schlüsse, die man an transzendente Gleichungen knüpft, die π als Wurzel haben, z. B.

$$\sin x = 0$$

$$x = k\pi \qquad k = 0, \pm 1, \pm 2, \dots$$

verfehlt. Man könnte etwa sagen: Dies ist eine transzendente Gleichung mit rationalen Koeffizienten:

$$x - \frac{x^3}{3!} + \frac{x^5}{5!} - \dots\dots = 0.$$

Wäre π eine algebraische Zahl, so müßte es andererseits auch noch Wurzel einer algebraischen Gleichung sein:

$$\varphi^{(\nu)}(x)=0,$$

wo φ ein endlicher ganzer rationaler Ausdruck vom Grade ν in x ist, und man kann auch annehmen, daß φ die im (1) irreducible Gleichung für π ist. Ferner sei schon bewiesen – was nicht schwer ist –, daß $\nu \geq 2$ ist, d.h. π ist nicht rational oder Wurzel einer quadratischen Gleichung. Nun gibt es in der Algebra einen Satz, welcher aussagt: wenn irgend eine Gleichung mit einer irreduciblen eine Wurzel gemeinsam hat, so genügen ihr alle Wurzeln der letzteren. Wenn es jetzt einen Satz geben würde, der diesem Theorem der Algebra entspräche, und für transcendente Gleichungen gälte, so könnte ich

sofort die Transzendenz von π beweisen. Denn dann müßten alle Wurzeln von

$$\varphi(x) = 0$$

auch der Gleichung

$$\sin x = 0$$

genügen, d.h. alle Wurzeln von φ hätten die Form $k\pi$. k ist nicht gleich 0, da sonst $\varphi(x)$ die Wurzel 0 hätte, also reduzibel wäre. Ferner gibt es eine $k \neq \pm 1$, da sonst φ quadratisch wäre. Es ist also

$$\varphi(k\pi) = 0, \text{ wo } k \neq \pm 1$$

und

$$\varphi(\pi) = 0$$

Also hat $\varphi(x) = 0$

mit $\varphi(kx) = 0$

eine Wurzel gemeinsam, folglich haben sie alle Wurzeln gemeinsam; da $\varphi(kx)$ denselben Grad wie $\varphi(x)$ hat, muß identisch in x

$$\varphi(kx) = M\cdot\varphi(x) \qquad M \text{ konstant}$$

sein. Also

$$\varphi(0) = M\cdot\varphi(0)$$
$$M = 1,$$

d. h.

$$\varphi^{(\nu)}(kx) \equiv \varphi^{(\nu)}(x)$$

oder

$$k^\nu x^\nu + \cdots \equiv x^\nu + \cdots$$

d. h.

$$k^\nu = 1,$$

gegen die Voraussetzung.

Nun läßt sich aber der bewußte Analogon zu dem algebraischen Satze nicht be-

weisen, denn es ist gar nicht richtig. Dedekind hat nämlich folgenden Satz aufgestellt und bewiesen:

Wenn α eine beliebige Zahl ist, so gibt es stets eine beständig konvergente Potenzreihe $\mathfrak{P}(x)$ mit rationalen Koeffizienten, derart daß die Gleichung

$$\mathfrak{P}(x)=0$$

die Wurzel $x=\alpha$ und keine andere hat.

Beweis: Wir bilden die Reihe

$$\log\left(1-\frac{x}{\alpha}\right)=-\frac{x}{\alpha}-\frac{x^2}{2\alpha^2}-\frac{x^3}{3\alpha^3}-\cdots\cdots,$$

welche für

$$|x|<|\alpha|$$

konvergiert. Wir setzen nun

$$-\frac{1}{n\alpha^n}=r_n-\varepsilon_n,$$

wo r_n rational und ε_n eine Zahl ist

die der Ungleichung

$$|\varepsilon_n| < \frac{1}{n!}$$

genügt; das ist möglich, da man $\frac{-1}{n a^n}$ durch rationale Zahlen beliebig weit annähern kann. Dann betrachten wir die Reihe

$$g(x) = \varepsilon_1 x + \varepsilon_2 x^2 + \varepsilon_3 x^3 + \cdots .$$

Das ist sicher eine ganze transzendente Funktion von x, da sie wegen

$$|\varepsilon_n| < \frac{1}{n!}$$

für alle x konvergiert. Durch Addition folgt

$$\log\left(1 - \frac{x}{a}\right) + g(x) = \sum (r_n - \varepsilon_n) x^n + \sum \varepsilon_n x^n$$

$$= \sum r_n x^n = r_1 x + r_2 x^2 + \cdots ,$$

also

$$e^{\log(1 - \frac{x}{a}) + g(x)} = e^{r_1 x + r_2 x^2 + \cdots}$$

$$= 1 + (r_1 x + r_2 x^2 + \cdots) + \frac{(r_1 x + r_2 x^2 + \cdots)^2}{2!} + \cdots$$

$$= 1 + r_1 x + \left(\frac{r_1^2}{2!} + r_2\right) x^2 + \cdots\cdots$$

$$= 1 + k_1 x + k_2 x^2 + \cdots\cdots = f(x).$$

Das ist eine Potenzreihe mit rationalen Koeffizienten, die für jedes x konvergiert. Diese stellt

$$\left(1 - \frac{x}{\alpha}\right) e^{g(x)}$$

Also ist $x = \alpha$ eine Wurzel von $f(x) = 0$, und es kann keine andere geben; denn $g(x)$ bleibt als ganze transcendente Funktion überall endlich, also ist $e^{g(x)}$ für jedes endliche $x \neq 0$.

Nun kommt noch ein letzter vergeblicher Versuch, der auf einem ganz richtigen Satze über Funktionen beruht. Es gibt einen Satz von Eisenstein, welcher lautet: Wenn die Potenzreihe

$$y = a + a_1 x + a_2 x^2 + \cdots$$

mit rationalen Koeffizienten eine algebraische Funktion von x darstellt, so kann man stets eine ganze Zahl N so finden, daß die Substitution

$$x = N x'$$

die Potenzreihe vom ersten Gliede abgesehen in eine solche mit ganzen rationalen Koeffizienten überführt.

Aus diesem Satz folgt, daß die Nenner nur endlich viel Primzahlen enthalten dürfen. Wenn also unendlich viel Primzahlen vorkommen, so ist die Funktion sicher nicht algebraisch, sondern transcendent.

Beispiel: $(1-x)^{\frac{1}{2}} = 1 - \frac{1}{2}x + \binom{\frac{1}{2}}{2} x^2 + \dots$

Der Koeffizient des allgemeinen Gliedes ist

abgesehen vom Vorzeichen

$$\frac{\frac{1}{2}\cdot\frac{1}{2}\cdot\frac{3}{2}\cdot\frac{5}{2}\cdots\frac{2n-3}{2}}{1\cdot 2\cdots n}=\frac{1}{2^{2n}}\cdot\frac{1\cdot 3\cdot 5\cdots 2n-3}{1\cdot 2\cdots n}$$

Die Primzahlen heben sich in der Tat weg, bis auf die Primzahl 2.

Die Exponentialfunktion ist transcendent, da der Koeffizient $\frac{1}{n!}$ ist, ebenso ist es mit

$$\operatorname{arc\,tg} x = x-\frac{x^3}{3}+\frac{x^5}{5}-\ldots$$

Daraus kann ich weiter die Transcendenz von $\operatorname{tg} x$ schließen. Ebenso ist $\operatorname{arc\,sin} x$ eine transcendente Funktion. Nun ist

$$\operatorname{arc\,sin} 1=\frac{\pi}{2},$$

und die Transcendenz von π wäre bewiesen, wenn man den Satz hätte, daß

transcendente Funktionen immer transcendente Werte annehmen. Dies ist aber nicht der Fall, z. B.

$$e^0 = 1$$

Nun wäre aber doch die Frage, ob ein Zusammenhang zwischen den transcendenten Funktionen und Zahlen besteht, denn eine algebraische Funktion nimmt für algebraische Argumente stets algebraische Werte an. Es stellt sich aber heraus, daß ein solcher Zusammenhang gar nicht stattfindet. Es gilt nämlich folgender Satz:

Es giebt eine ganze transcendente Funktion, deren Potenzreihe rationale ~~Werte~~ Koeffizienten hat, und deren Werte für jedes rationale Argument selbst rational sind.

Der Beweis beruht auf der Abzählbarkeit der rationalen Zahlen. Es seien

$$\rho_1, \rho_2, \ldots$$

die rationalen Zahlen. Dann bilde ich folgende Funktionen mit rationalen Koeffizienten:

$$g_1 = x - \rho_1$$
$$g_2 = (x-\rho_1)(x-\rho_2)$$
$$\ldots\ldots$$
$$g_n = (x-\rho_1)(x-\rho_2)\cdots(x-\rho_n)$$
$$\ldots\ldots$$

und setze

$$\psi_h = \frac{g_h}{\mathfrak{g}_h},$$

wo $\mathfrak{g}_h$ den absolut größten Koefficienten von g_h bedeutet. ψ_h ist eine Funktion h-ten Grades in x mit ra-

tionalen Koeffizienten, die absolut $\leqq 1$ sind.
Nun setze ich

$$\chi_1 = \psi_1$$
$$\chi_2 = x^{2}\psi_2$$
$$\chi_3 = x^{5}\psi_3$$
$$\cdots\cdots$$
$$\chi_n = x^{m}\psi_n$$
$$\cdots\cdots;$$

dabei ist

$$m = \text{dem Grad von } \chi_{n-1} + 1$$

Nun bilde ich

$$f(x) = \frac{\chi_1}{n_1!} + \frac{\chi_2}{n_2!} + \frac{\chi_3}{n_3!} + \cdots,$$

wo n_ν der Grad von χ_ν ist. Das ist eine beständig konvergente Potenzreihe; jede Potenz von x kommt nur in einem χ vor (so sind die χ gewählt). Wir haben also eine

ganze transzendente Funktion mit rationalen Koeffizienten. x sei eine rationale Zahl

$$x = \beta_\nu ;$$

dann ist

$$g_n = \begin{cases} 0 & \text{für } n \geq \nu \\ \text{rational} & \text{,, } n < \nu \end{cases}$$

also

$$\chi_n \text{ und } \psi_n = \begin{cases} 0 & \text{für } n \geqq \nu \\ \text{rational} & \text{,, } n < \nu \end{cases}$$

also wird $R(\beta_\nu)$ gleich einer Summe von rationalen Zahlen, d.h. rational.

§. 4. Wir gehen nunmehr zu den wirklichen Beweisen über, die uns positiv über die Natur von π und verwandten Zahlen Aufschluß geben. Wir behandeln zunächst die Irrationalität von e.

Es ist sehr schwer, von einer gegebenen Zahl zu sagen, ob sie irrational ist oder nicht; die meisten dieser Fragen sind noch gar nicht gelöst. Zu beweisen, daß $2^{\sqrt{2}}$ irrational ist, ist ein ganz außerordentlich schwieriges Problem, und es ist gar nicht abzusehen, mit welchen Mitteln ~~der~~ er anzugreifen ist; ebenso ist es z.B. mit e^{π}.

Dagegen hat bereits Liouville von der Zahl e den irrationalen Charakter erkannt. Es ist

$$e^x = 1+\frac{x}{1!}+\frac{x^2}{2!}+\dots+\frac{x^{n-1}}{(n-1)!}+e^{\vartheta x}\frac{x^n}{n!}, \quad 0\leqq\vartheta\leqq 1$$

also

$$e = 1+\frac{1}{1!}+\frac{1}{2!}+\dots+\frac{1}{(n-1)!}+e^{\vartheta}\frac{1}{n!}$$

Es sei nun e eine rationale Zahl:

$$e=\frac{A}{B} \qquad (A \text{ u. } B \text{ ganz u. } >0)$$

Dann ist

$$A\cdot(n-1)! = B\cdot(n-1)! + B\cdot\frac{(n-1)!}{1!} + B\cdot\frac{(n-1)!}{2!} + \dots$$
$$\dots + B + B\cdot\frac{1}{n}e^{\vartheta}$$

Also

$$\frac{B\cdot e^{\vartheta}}{n} = \text{ganze Zahl} \qquad 0 \leqq \vartheta \leqq 1$$

Wir wählen n so, daß

$$n > B\cdot e$$

also

$$0 < \frac{Be^{\vartheta}}{n} < 1$$

ist. Wir haben also eine ganze Zahl zwischen 0 und 1; aber so etwas gibt es nicht.

Wenn man diese Methode in geschickter Weise ausdehnt, kann man noch zu weiteren Ergebnissen gelangen, z. B. daß e nicht Wurzel einer quadratischen Gleichung sein kann. Aber viel mehr läßt sich auf diesem Wege nicht erreichen, z. B. gar nichts über die Zahl π. Es fragt sich nun wie man

man weiter zu verfahren hat.

Bei der Zahl π hat Lambert den ersten Schritt getan, und zwar benutzte er Kettenbruchentwicklungen. Ich betrachte

$$\varphi(x,y) = 1 + \frac{1}{1!}\frac{x}{y} + \frac{1}{2!}\frac{x^2}{y(y+1)} + \frac{1}{3!}\frac{x^3}{y(y+1)(y+2)} + \cdots,$$

Dann ist

$$\varphi(x,y) - \varphi(x,y+1) = \frac{x}{y(y+1)} + \frac{1}{1!}\frac{x^2}{y(y+1)(y+2)} + \cdots$$

$$= \frac{x}{y(y+1)}\,\varphi(x,y+2)$$

Wir setzen

$$\psi(x,y) = \frac{x}{y}\,\frac{\varphi(x,y+1)}{\varphi(x,y)}$$

also

$$\psi(x,y) = \frac{x}{y+\psi(x,y+1)} = \cfrac{x}{y+\cfrac{x}{y+1+\cfrac{x}{y+2+\cdots}}}$$

folglich

$$\psi(1,y) = \cfrac{1}{y+\cfrac{1}{y+1+\cfrac{1}{y+2+\cdots}}}$$

Setze ich

$$\chi(y) = 1 + \frac{1}{1!\,y} + \frac{1}{2!}\,\frac{1}{y(y+1)} + \cdots,$$

so wird

$$\psi(1,y) = \frac{1}{y}\,\frac{\varphi(1,y+1)}{\varphi(1,y)} = \frac{1}{y}\,\frac{\chi(y+1)}{\chi(y)}$$

Ist y eine ganze Zahl, so haben wir links einen unendlichen Kettenbruch, also ist der Quotient $\frac{1}{y}\frac{\chi(y+1)}{\chi(y)}$ irrational für ganzzahlige y.

Setzen wir aber

$$x = \frac{1}{4}\xi^2,\ y = \frac{1}{2},$$

so wird

$$\psi\left(\tfrac{1}{4}\xi^2, \tfrac{1}{2}\right) = \frac{\frac{1}{4}\xi^2}{\frac{1}{2}}\,\frac{\varphi\left(\frac{1}{4}\xi^2, \frac{3}{2}\right)}{\varphi\left(\frac{1}{4}\xi^2, \frac{1}{2}\right)} = \frac{1}{2}\xi\,\frac{e^{\xi}-e^{-\xi}}{e^{\xi}+e^{-\xi}}$$

also

$$\frac{1}{2}\xi\,\frac{e^{\xi}-e^{-\xi}}{e^{\xi}+e^{-\xi}} = \cfrac{\frac{1}{4}\xi^2}{\frac{1}{2} + \cfrac{\frac{1}{4}\xi^2}{\frac{3}{2} + \cfrac{\frac{1}{4}\xi^2}{\frac{5}{2} + \cdots}}}$$

oder

$$\frac{e^{\xi}-e^{-\xi}}{e^{\xi}+e^{-\xi}}=\cfrac{\frac{1}{2}\xi}{\frac{1}{2}+\cfrac{\frac{1}{4}\xi^2}{\frac{3}{2}+\cdots}}=\cfrac{\xi}{1+\cfrac{\frac{1}{2}\xi^2}{\frac{3}{2}+\cdots}}=\cfrac{\xi}{1+\cfrac{\xi^2}{3+\cfrac{\frac{\xi^2}{2}}{\frac{5}{2}+\cdots}}}$$

$$=\cfrac{\xi}{1+\cfrac{\xi^2}{3+\cfrac{\xi^2}{5+\cfrac{\frac{\xi^2}{2}}{\frac{7}{2}+\cdots}}}}=\cfrac{\xi}{1+\cfrac{\xi^2}{3+\cfrac{\xi^2}{5+\cfrac{\xi^2}{7+\cfrac{\xi^2}{9+\cdots}}}}}$$

Für $\xi=1$ kommt ein gewöhnlicher Kettenbruch heraus; also ist

$$\frac{e-e^{-1}}{e+e^{-1}}=\frac{e^2-1}{e^2+1}$$

irrational; ~~denn~~ also ist auch e^2 irrational, ~~dass wie e~~ und keine quadratische Irrationalität, denn der Kettenbruch ist nicht periodisch; also ist auch e irrational.

Nun kann man diese Methode noch

verallgemeinern; Lambert hat das so weit getrieben, daß er auch noch die Irrationalität von π beweisen konnte. Wir wollen das aber nicht weiter verfolgen, sondern wir wollen diese Methode nach Hermite umformen. Das Gemeinsame der beiden Methoden besteht darin, daß e resp. e^x durch rationale Funktionen so gut wie möglich angenähert wird, einmal durch die Näherungsbrüche des Kettenbruchs, bei Hermite durch die Hermiteschen Funktionen.

Wir werden e^x durch rationale Funktionen, die Hermiteschen Funktionen, annähern. Diese Funktionen stellt man am leichtesten durch bestimmte Integrale dar. Es soll jetzt bewiesen werden, daß e^x ir-

rational ist, wenn x $(x \neq 0)$ rational ist. Nun brauchen wir das nur zu beweisen für ganzzahliges x, denn

$$e^a = \left(e^{\frac{a}{b}}\right)^b$$

ist mit $e^{\frac{a}{b}}$ rational.

Dazu gehen wir aus von folgendem Integral

$$J = \int_0^1 e^{-xt} t^n (1-t)^n \, dt$$

n ist eine ganze Zahl, über welche wir die Verfügung uns noch vorbehalten. Wir werden später $x = a > 0$ setzen; es ist daher auf jeden Fall

$$0 < J < 1$$

Nun ist

$$J = \left[\frac{\partial^{2n}}{\partial p^n \partial q^n} \int_0^1 e^{-xt+pt+q(1-t)} \, dt \right]_{\substack{p=0 \\ q=0}}$$

$$= \left[\frac{\partial^{2n}}{\partial p^n \partial q^n} e^q \int_0^1 e^{t(-x+p-q)}\, dt\right]_{\substack{p=0\\q=0}}$$

$$= \left[\frac{\partial^{2n}}{\partial p^n \partial q^n} e^q \left[\frac{e^{t(-x+p-q)}}{-x+p-q}\right]_0^1\right]_{\substack{p=0\\q=0}}$$

$$= \left[\frac{\partial^{2n}}{\partial p^n \partial q^n} \frac{e^{p-x} - e^q}{-x+p-q}\right]_{\substack{p=0\\q=0}}$$

$$= e^{-x} \cdot P(x) - Q(x),$$

wo P und Q rationale Funktionen von x sind:

$$P(x) = \left(\frac{\partial^{2n}}{\partial p^n \partial q^n} \frac{e^p}{-x+p-q}\right)_{\substack{p=0\\q=0}}$$

$$Q(x) = \left(\frac{\partial^{2n}}{\partial p^n \partial q^n} \frac{e^q}{-x+p-q}\right)_{\substack{p=0\\q=0}}$$

Das sind die Hermiteschen Funktionen. Uns interessiert ganz allein folgendes: Sehen wir uns $P(x)$ an: q kommt im Zähler gar nicht

vor. Also kommt nach n-maliger Differentiation nach q für q = 0 heraus:

$$R(x) = \left(\frac{\partial^n}{\partial p^n}\, n!\, \frac{e^p}{(-x+p)^{n+1}}\right)_{p=0}$$

Da x = a ganz und rational ist, kommt heraus

$$R(a) = n!\,\frac{A}{a^{2n+1}},$$

wo A eine ganze rationale Zahl ist. Ebenso wird

$$Q(a) = n!\,\frac{B}{a^{2n+1}},$$

wo B ganz und rational ist.

Es sei

$$e^a = \frac{M}{N} > 0 \qquad M, N \text{ ganz u. rational}$$

rational. Dann ist

$$J = \frac{N}{M}\cdot n!\,\frac{A}{a^{2n+1}} - n!\,\frac{B}{a^{2n+1}}$$

$$0 < J\cdot M\cdot\frac{a^{2n+1}}{n!} = NA - MB = \text{ganze Zahl}$$

Nun ist

$$0 < \vartheta < 1;$$

ferner

$$\lim_{n=\infty} \frac{a^{2n+1}}{n!} = 0$$

Wir können also n so groß wählen, daß der Ausdruck links < 1 wird. Das ist aber ein Widerspruch.

Es ist also

$$e^x = \text{irrational}, \text{ wenn } x \text{ rational } \text{u.} \neq 0 \text{ ist.}$$

Daraus folgt, daß

$$\log x = \text{irrat.}, \text{ wenn } x \text{ rat. u.} \neq 1 \text{ ist.}$$

Denn sonst wäre

$$e^{\log x} = x = \text{irrat.}$$

Ich will jetzt beweisen, daß π irrational ist. Ich gehe wieder von einem bestimmten Integral aus:

$$\mathfrak{I} = \int_{-1}^{+1} (1-t^2)^n \cos\frac{\pi}{2} t \, dt$$

da ist

$$0 < \mathfrak{I} < 2$$

Wir können schreiben

$$\mathfrak{I} = \pm \frac{1}{\left(\frac{\pi}{4}\right)^{2n}} \left[\frac{\partial^{2n}}{\partial p^n \partial q^n} \int_{-1}^{+1} \cos\left\{(t-1)\frac{\pi}{4}p + (t+1)\frac{\pi}{4}q\right\} dt \right]_{\substack{p=1\\q=1}}$$

n sei gerade

$$= \pm \frac{1}{\left(\frac{\pi}{4}\right)^{2n}} \left[\frac{\partial^{2n}}{\partial p^n \partial q^n} \frac{\sin\frac{\pi}{2}q + \sin\frac{\pi}{2}p}{\frac{\pi}{4}p + \frac{\pi}{4}q} \right]_{\substack{p=1\\q=1}}$$

$$= \pm \frac{1}{\left(\frac{\pi}{4}\right)^{2n+1}} \left[\frac{\partial^{2n}}{\partial p^n \partial q^n} \frac{\sin\frac{\pi}{2}q + \sin\frac{\pi}{2}p}{p+q} \right]_{\substack{p=1\\q=1}}$$

Dieser Ausdruck ist in p und q symmetrisch; also

$$\mathcal{J} = \pm \frac{2}{\left(\frac{\pi}{4}\right)^{2n+1}} \left[\frac{\partial^{2n}}{\partial p^n \partial q^n} \frac{\sin\frac{\pi}{2}q}{p+q} \right]_{\substack{p=1\\q=1}}$$

$$= \pm \frac{2\,n!}{\left(\frac{\pi}{4}\right)^{2n+1}} \left[\frac{\partial^{n}}{\partial q^n} \frac{\sin\frac{\pi}{2}q}{(1+q)^{n+1}} \right]_{q=1}$$

$$= \pm \frac{2\,n!}{\left(\frac{\pi}{4}\right)^{2n+1}} \cdot \frac{M}{2^{2n+1}}$$, wo M eine ganze Zahl ist.

$$= \pm \frac{2\,n!}{\left(\frac{\pi}{2}\right)^{2n+1}} \cdot M$$

Jetzt nehmen wir an, es wäre π eine rationale Zahl

$$\pi = \frac{a}{b} \qquad a \text{ u. } b \text{ ganz u. rat.}$$

Dann ist

$$\mathcal{J} = \pm 2M \cdot \frac{n!}{\left(\frac{a}{2b}\right)^{2n+1}} = M^* \frac{n!}{a^{2n+1}}$$

Also wird:

$$\vartheta \cdot \frac{a^{2n+1}}{n!} = M^* = \text{ganze Zahl}.$$

Nun läßt sich $\frac{a^{2n+1}}{n!}$ für hinreichend große n kleiner als $\frac{1}{2}$ machen; ferner ist

$$0 < \vartheta < 2,$$

also die linke Seite < 1. Das ist ein Widerspruch.

Wir kommen jetzt auf den Unterschied von algebraischen und transzendenten Zahlen zu sprechen. Ich nenne eine Zahl algebraisch vom n-ten Grade, wenn sie einer irreduziblen Gleichung n-ten Grades mit rationalen Koeffizienten, aber keiner solchen Gleichung niederen Grades genügt.

Es gibt algebraische Zahlen n-ten Grades. Das beweist man am einfachsten,

indem man eine irreducible Gleichung n-ten Grades hinschreibt; eine solche ist

$$x^n - 2 = 0,$$

wie in der Zahlentheorie gezeigt wird.

$$x = \sqrt[n]{2}$$

ist also eine algebraische Zahl genau n-ten Grades.

Beweise für die Existenz transcendenter Zahlen

1) (Liouville.) In der Theorie der Kettenbrüche wird gezeigt, daß jede reelle irrationale Zahl α auf unendlich viel Arten durch Brüche $\frac{p}{q}$ angenähert werden kann, sodaß

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$$

ist. Für rationale Zahlen ist das bekanntlich nicht möglich, sie sind dadurch charakterisiert,

daß sie sich nicht so gut durch Brüche annähern lassen. Eine Zahl α ist rational, wenn

$$\left|\alpha - \frac{p}{q}\right| > \frac{A}{q^2}$$

ist, abgesehen von endlich vielen Ausnahmen q.

Der Liouvillesche Satz ist nun das Analogon hierzu für algebraische Zahlen. Er lautet: Wenn α einer irreduziblen Gleichung vom Grade n genügt, d.h. eine algebraische Zahl n-ten Grades ist, so gibt es stets eine reelle Zahl δ, derart, daß für alle rationalen Brüche $\frac{p}{q}$ die Ungleichung

$$\left|\alpha - \frac{p}{q}\right| > \frac{\delta}{q^n}$$

gilt.

Beweis: Wir nehmen der Einfachheit halber

$$\alpha > 0$$

an. Wir nehmen zunächst die (positiven) Brüche $\frac{p}{q}$, die $< 2\alpha$ sind. α genüge der irreduziblen Gleichung

$$f(x) = ax^n + bx^{n-1} + \dots + k = 0$$
$$= a(x-\alpha)(x-\alpha') \cdots (x-\alpha^{(n-1)}),$$

also

$$f\left(\frac{p}{q}\right) = \frac{C}{q^n}, \qquad C \text{ ganz u. rat.}, \; C \neq 0$$

oder

$$\frac{C}{q^n} = a\left(\frac{p}{q}-\alpha\right)\left(\frac{p}{q}-\alpha'\right) \cdots \left(\frac{p}{q}-\alpha^{(n-1)}\right)$$

$$\left|\frac{p}{q}-\alpha\right| = \left|\frac{C}{q^n}\right| \cdot \frac{1}{\left|a\left(\frac{p}{q}-\alpha'\right) \cdots \left(\frac{p}{q}-\alpha^{(n-1)}\right)\right|}$$

Nun hat der Ausdruck im Nenner

für $0 < \frac{p}{q} < 2$ einen maximalen Wert M; also ist

$$\left|\frac{p}{q} - \alpha\right| \geqq \left|\frac{c}{q^n}\right| \cdot \frac{1}{M}$$

Es ist $1 \leqq c$, also

$$\left|\frac{p}{q} - \alpha\right| \geqq \frac{1}{q^n} \cdot \frac{1}{M}$$

Ich brauche also nur $\delta < \frac{1}{M}$ zu nehmen. Wählen wir aber auch noch $\delta < \alpha$, so gilt die Ungleichung

$$\left|\alpha - \frac{p}{q}\right| > \frac{\delta}{q^n}$$

auch für alle $\frac{p}{q} > 2\alpha$; damit ist der Liouvillesche Satz bewiesen.

Die Existenz von transzendenten Zahlen zeigen wir nun am einfachsten an einem Beispiel. Es sei

$$\alpha = 1 + \frac{1}{2^{1!}} + \frac{1}{2^{2!}} + \frac{1}{2^{3!}} + \cdots$$

Die Reihe konvergiert, sogar stärker als die Reihe für e. Angenommen, α sei eine algebraische Zahl n-ten Grades. Ich setze

$$\frac{p}{q} = 1 + \frac{1}{2^{1!}} + \cdots + \frac{1}{2^{m!}},$$

also

$$q = 2^{m!}$$

Dann ist

$$\alpha - \frac{p}{q} = \frac{1}{2^{(m+1)!}} + \cdots = \frac{1}{2^{(m+1)!}}\left(1 + \frac{1}{2^{(m+2)!-(m+1)!}} + \cdots\right)$$

$$\leqq \frac{1}{2^{(m+1)!}}\left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots\right) = \frac{1}{2^{(m+1)!-1}}$$

$$= \frac{1}{q^n} \cdot \frac{2^{m!\cdot n}}{2^{(m+1)!-1}} = \frac{1}{q^n} \cdot \frac{1}{2^{(m+1)!-m!\cdot n-1}}$$

$$= \frac{1}{q^n} \frac{1}{2^{m!(m+1-n)-1}} = \frac{\varepsilon}{q^n}$$

Wenn ich n genügend groß wähle, so kann ich ε beliebig klein machen. Also kann ich Brüche $\frac{p}{q}$, sodaß

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^n}$$

ist, für jedes δ. Das widerspricht aber dem Liouvilleschen Satz, α ist also transcendent.

2.) Anwendung des Diagonalverfahrens auf die abzählbare Menge der algebraischen Zahlen.

Von einer bestimmten Zahl zu sagen, ob sie transcendent ist oder nicht, ist oft sehr schwer. Für e und π werden wir den Nachweis der Transcendenz erbringen. Dagegen weiß man von vielen Zahlen noch

gen nicht, ob sie überhaupt irrational sind, z.B. $e+\pi$, $e\cdot\pi$, e^π; ferner bei der Γ-Funktion

$$\Gamma(m+1) = \int_0^\infty t^m e^{-t}\,dt$$

Für ganzzahlige m ist dies $= m!$ Dagegen sind die Werte von $\Gamma(x)$ für rationale gebrochene x wahrscheinlich transzendent; man weiß aber nicht einmal, ob sie irrational sind.

Für die Zahl e hat Hermite das Problem erfolgreich gelöst. Die Transzendenz von π konnte er aber nicht beweisen. Erst Lindemann zeigte, daß der Wirkungsbereich der Hermiteschen Untersuchungen sich weiter reichte, als Hermite selbst ahnte, und auch für die Transzendenz von π ausreichte. Über die äußerst mühsamen Untersuchungen Hermite's hat sich dann Weierstraß hergemacht und sie sehr

vereinfacht. Um aber den Beweis hier vortragen zu können, mußten noch weitere Vereinfachungen hinzukommen, die ich seinerzeit in einer Note angegeben habe. Die Schwierigkeit der Hermiteschen Untersuchung liegt darin, von einer gewissen Zahl zu zeigen, daß sie $\neq 0$ ist. Ich habe dies auf zahlentheoretischem Wege getan, während Hermite und Weierstraß Abschätzungen zu Hilfe nahmen. Ich werde zeigen, daß eine Zahl durch eine gewisse Primzahl nicht teilbar ist, woraus dann folgt, daß sie $\neq 0$ ist.

Folgende Hilfsformeln werden wir brauchen:

Für ganzzahliges m ist

$$\Gamma(m+1) = \int_0^\infty z^m e^{-z} dz = m!$$

Ferner ist

$$\lim_{m=\infty} \frac{g^m}{m!} = 0$$

Nun gehen wir an den Transcendenzbeweis für e; wir nehmen an, e sei algebraisch, also

$$a + a_1 e + a_2 e^2 + \cdots + a_n e^n = 0$$

$a, a_1 \cdot \cdot a_n$ sind ganze Zahlen; ohne Einschränkung können wir annehmen $a > 0$. Dann multipliziren wir die Gleichung mit

$$\int_0^\infty = \int_0^\infty z^{p-1}\left[(z-1)(z-2)(z-3)\cdots(z-n)\right]^p e^{-z}\,dz,$$

wo p eine Primzahl ist, deren Wahl wir uns noch vorbehalten. Das Integral existirt offenbar.

Dann erhalten wir

$$a\int_0^\infty + a_1 e\int_0^\infty + a_2 e^2\int_0^\infty + \cdots + a_n e^n\int_0^\infty = 0$$

Die linke Seite zerlege ich in zwei Bestandteile

$$P_1 + P_2 = 0,$$

wo

$$P_1 = a\int_0^\infty + a_1 e\int_1^\infty + a_2 e^2\int_2^\infty + \cdots + a_n e^n\int_n^\infty$$

$$P_2 = a_1 e\int_0^1 + a_2 e^2\int_0^2 + \cdots + a_n e^n\int_0^n$$

ist. P_1 und P_2 will ich nun für sich untersuchen, und zwar P_1 zahlentheoretisch, P_2 analytisch.

a.) Ich betrachte zunächst das erste Glied von P_1:

$$a\int_0^\infty$$

Das ist wesentlich unser Integral $\int_0^\infty$. Was unter dem Integral steht, ist eine ganze rationale Funktion von z, multipliziert mit e^{-z}. Die niedrigste Potenz von z ist

$$\pm(n!)^p z^{p-1}$$

Dann kommt

$$A z^p + A' z^{p+1} + \cdots,$$

wo $A, A' \ldots$ ganze Zahlen sind. Nun wird nach unserer ersten Hilfsformel

$$\int_0^\infty = \pm (n!)^p (p-1)! + A\cdot p! + A'(p+1)! + \ldots$$

Diese ganze Zahl. Alle Glieder bis auf das erste sind durch $p!$ teilbar. Das Ganze ist durch $(p-1)!$ teilbar. Es wird also

$$\int_0^\infty \equiv \pm (n!)^p (p-1)! \pmod{p}$$

Denken wir uns $p > a$ und $p > n$ gewählt, so wird das erste Glied von P_1 durch $(p-1)!$, aber nicht durch $p!$ oder p teilbar.

Nun nehme ich die anderen Glieder von P_1. Da kommt zunächst auf das zweite:

$$e\int_1^\infty z^{p-1}[(z-1)(z-2)\cdots(z-n)]^p e^{-z}dz$$

an. Ich setze

$$z = z'+1$$

Dann wird dies, wenn ich wieder z statt z' schreibe:

$$\int_0^\infty (z+1)^{p-1} z^p (z-1)^p \cdots (z-(n-1))^p e^{-z}dz$$

Die niedrigste Potenz von z ist teilbar durch z^p, also wird das Integral durch $p!$ teilbar.

Und ganz ebenso zeigt man, indem man

$$z = z'+2,\ z'+3, \dots$$

setzt, daß die übrigen Glieder von P_1 durch $p!$ teilbar sind. Also ist P_1 eine ganze Zahl, und

$$(p-1)! \mid P_1 \quad , \quad p \nmid P_1;$$

also muß

$$P_1 \neq 0$$

und auch

$$\frac{P_1}{(p-1)!} = \text{ganze rationale Zahl} \neq 0 \text{ sein}$$

b.) P_2 wird nun numerisch abgeschätzt. Ich nehme zunächst das erste Integral. M sei das Maximum der Ausdrucks

$$z(z-1)(z-2) \cdots (z-n)$$

im Intervall 0 bis n. Dann ist

$$\left|\int_0^1\right| \leqq \int_0^1 M^{p-1}(z-1)\cdots\cdots(z-n)\,e^{-z}\,dz$$
$$= M^{p-1}\int_0^1 (z-1)\cdots(z-n)\,e^{-z}\,dz$$

Das Integral hat einen endlichen Wert. Ebenso

$$\left|\int_0^2\right| \leqq M^{p-1}\cdot \ast \quad , \text{ wo } \ast \text{ eine endliche Zahl ist.}$$

u. s. f.

Also

$$\left|P_2\right| \leqq M^{p-1}\cdot Q,$$

unter Q eine endliche Zahl verstanden, und

$$\left|\frac{P_2}{(p-1)!}\right| \leqq \frac{M^{p-1}}{(p-1)!}Q$$

Für große Werte p läßt sich dies nach unserer Hilfsformel <1 machen.

Dann habe ich

$$P_1 + P_2 = 0$$

oder

$$\frac{P_1}{(p-1)!} + \frac{P_2}{(p-1)!} = 0$$

Damit gibt es eine ganze Zahl, die nicht absolut < 1, und die ist [illegible]. Damit ist der Beweis für die Transcendenz von e erbracht.

Nun wollen wir noch [illegible] Beweis für die Zahl π [illegible]. Wir [illegible].

Zunächst betrachten wir die Gleichung

$$e^{i\pi}+1=0$$

Angenommen, π sei eine algebraische Zahl, dann ist auch $i\pi$ eine solche. Dann genügt $x=\pi$ der Gleichung

$$f(x)=0,$$

so genügt $iy=i\pi$

$$f(-iy)=0$$

und

$$f(iy)\cdot f(-iy)=0.$$

und dies ist eine algebraische Gleichung für $i\pi$.

Wir setzen

$$i\pi = \alpha_1$$

Dann sei die algebraische Gleichung für α_1:

$$f(\alpha_1) = 0$$

vom Grade n; die anderen Wurzeln seien

$$\alpha_2, \alpha_3 \dots \alpha_n$$

Ferner ist

$$e^{\alpha_1} + 1 = 0$$

Nun kommt der Gedanke von Lindemann.

Wir haben jetzt die Gleichung

$$e^{\alpha_1} + 1 = 0,$$

welche von der Form der früher betrachteten Gleichung

$$a + a_1 e + \dots + a_n e^n$$

ist, und zwar von der denkbar einfachsten Form

Sie ist allerdings insofern kompliziert, als α_1 keine ganze, sondern eine algebraische Zahl ist. Kann man nun diesen Umstand nicht unschädlich machen durch Aufgabe der Einfachheit der Bildung? Vielleicht läßt es sich erreichen, daß sie symmetrisch wird in $\alpha_1 \dots \alpha_n$; dann läßt sich hoffen, den Hermiteschen Beweis umbilden zu können.

Und das gelingt nun in der That. Wir bilden

$$
\begin{aligned}
0 &= (1+e^{\alpha_1})(1+e^{\alpha_2})\cdots\cdots(1+e^{\alpha_n}) \\
&= 1+e^{\alpha_1}+e^{\alpha_2}+\dots+e^{\alpha_n}+e^{\alpha_1+\alpha_2}+e^{\alpha_1+\alpha_3}+\dots \\
&\quad \dots+e^{\alpha_1+\alpha_2+\alpha_3}+\dots\dots+e^{\alpha_1+\alpha_2+\dots+\alpha_n}
\end{aligned}
$$

Die Exponenten genügen folgenden algebraischen Gleichungen:

$$
\begin{array}{lll}
f(x)=0 & x=\alpha_i & \\
f_2(y)=0 & y=\alpha_i+\alpha_k & i\neq k \\
f_3(z)=0 & z=\alpha_i+\alpha_k+\alpha_l & i\neq k\neq l \\
\text{– – – –} & &
\end{array}
$$

Also ist

$$g(x) = f(x) \cdot f_2(x) \cdot f_3(x) \cdot \ldots \ldots = 0$$

eine Gleichung, die jeden Exponenten zur Wurzel hat. Ich bezeichne die Exponenten jetzt mit

$$\beta_1, \beta_2 \ldots\ldots \beta_N$$

Es ist also

$$1 + e^{\beta_1} + e^{\beta_2} + \ldots + e^{\beta_N} = 0,$$

und die β genügen der Gleichung

$$g(x) = 0$$

mit rationalen Koeffizienten. Nun können aber einige Wurzeln von $g(x)$ Null sein, deren Anzahl sei $a-1$. Dann haben wir

$$a + e^{\beta_1} + e^{\beta_2} + \ldots + e^{\beta_M} = 0 \qquad M = N-(a-1)$$

$\beta_1 \ldots \beta_M$ genügen der Gleichung

$$\frac{g(x)}{x^{a-1}} = 0$$

vom Grade M.

$$\frac{g(x)}{x^{a-1}} = bx^{M} + b_1 x^{M-1} + \dots + b_M = 0,$$

wo die b ganze Zahlen, $b_M \neq 0$, $b \neq 0$ ist.

Die Gleichung, welche zu

$$a + a_1 e + \dots + a_n e^n = 0$$

analog ist, ist nun

$$a + e^{k_1} + e^{k_2} + \dots + e^{k_M} = 0.$$

Früher genügten die Exponenten der Gleichung

$$(x-1)(x-2)\cdots(x-n) = 0$$

An deren Stelle ~~tritt~~ jetzt

$$bx^{M} + b_1 x^{M-1} + \dots + b_M = 0.$$

Nunmehr werden wir das Hermitesche Verfahren verallgemeinern. Wir multiplizieren unsere Gleichung mit dem Integral

$$\int_0^\infty = \int_0^\infty z^{p-1}\left[b^{M}(bz^{M} + b_1 z^{M-1} + \dots + b_M)\right]^{p} e^{-z}\,dz,$$

und zerlegen die so entstehende Gleichung

in die Teile

$$P_1 + P_2 = 0,$$

wo

$$P_1 = a\int_0^{\infty} + e^{p_1}\int_{p_1}^{\infty} + e^{p_2}\int_{p_2}^{\infty} + \cdots\cdots + e^{p_\mu}\int_{p_\mu}^{\infty}$$

$$P_2 = e^{p_1}\int_0^{p_1} + e^{p_2}\int_0^{p_2} + \cdots + e^{p_\mu}\int_0^{p_\mu}$$

ist. P_1 wird wieder arithmetisch, P_2 numerisch behandelt.

1.) Das erste Glied von P_1 ist

$$a(p-1)!\,(b^{\mu}\cdot b_{\mu})^{p}$$

Wählen wir

$$p > \begin{cases} a \\ b \\ b_\mu \end{cases},$$

so wird das eine ganze Zahl, welche durch $(p-1)!$, aber nicht durch $p!$ teilbar ist.

Ferner ist, wenn wir z_1+p_1 statt z schreiben:

$$e^{p_1}\int_{p_1}^{\infty} = \int_0^{\infty}(z+p_1)^{r-1}\left[b^{\mu}(b(z+p_1)^{\mu}+\dots+b_{\mu})\right]^{p}e^{-z}dz$$

Die Klammer wird eine ganze rationale Funktion mit ganzen Koeffizienten in z und p_1:

$$G(z, p_1);$$

also

$$e^{p_1}\int_{p_1}^{\infty} = \int_0^{\infty}(z+p_1)^{r-1}\left[b^{\mu}\cdot G(z,p_1)\right]^{p}e^{-z}dz$$

Ferner hat, da

$$b p_1^{\mu} + \dots + b_{\mu} = 0$$

ist, G den Faktor z; der Rest ist in z und p_1 vom $(\mu-1)$ten Grade. Multiplizieren wir ihn mit $b^{\mu-1}$, so ist er eine gleiche Funktion von z und $B_1 = b\cdot p_1$; also habe ich

$$b^{\mu-1}\cdot G(z,p_1) = z\cdot H(z, bp_1) = z\cdot H(z, B_1)$$

Folglich wird

$$e^{p_1}\int_{p_1}^{\infty} = \int_0^{\infty}(bz+B_1)^{r-1}\cdot b\left[z\cdot H(z,B_1)\right]^{p}e^{-z}dz$$

$$= \int_0^\infty z^\rho K(z, B_1)\, e^{-z}\, dz$$

Ebenso machen wir es mit den andern Gliedern; also wird

$$e^{\beta_1}\int_{\beta_1}^{\infty} + \cdots + e^{\beta_\mu}\int_{\beta_\mu}^{\infty} = \int_0^\infty z^\rho \big(K(z,B_1)+\cdots+K(z,B_\mu)\big)\, e^{-z}\, dz$$

und das ist eine ganze Zahl, die durch $p!$ teilbar ist. Denn schreibe ich

$$z = \frac{Z}{b},$$

so ist

$$b\cdot\left(\frac{Z}{b}\right)^{\mu} + \cdots + b_\mu = 0$$

oder

$$Z^{\mu} + B_1 Z^{\mu-1} + \cdots + B_\mu = 0,$$

wo die B ganze Zahlen sind, und diese Gleichung hat die Wurzeln $B_1 \dots B_\mu$.
Unter dem Integral steht eine [illegible] Funktion von

z, die symmetrisch in $B_1 \dots B_n$ ist. Also hat sie ganzzahlige Koeffizienten. Das Integral ist also reell und hat nach unserer Hilfsformel den Faktor $p!$.

2.) $|P_2|$ wird genau wie früher abgeschätzt:

$$|P_2| < M^{p-1} \cdot \varepsilon$$

Nun können wir wieder wie früher schließen:

$$\frac{P_1}{(p-1)!} + \frac{P_2}{(p-1)!} = 0$$

Das erste Glied ist eine ganze Zahl $\neq 0$, das zweite absolut < 1, und das ist ein Widerspruch.

Ich will jetzt noch den allgemeinsten Lindemannschen Satz nennen, der sich genau ebenso beweisen läßt, wie der vorige, er bedarf nur komplizierterer Rechnungen. Dieser Satz heißt folgendermaßen:

Es seien $X_1, X_2 \dots X_n$ n algebraische

Zahlen, von denen keine Null ist, und $x_1, x_2 \dots x_n$ n algebraische Zahlen, von denen keine zwei einander gleich sind. Dann ist die Gleichung

$$X_1 e^{x_1} + X_2 e^{x_2} + \dots + X_n e^{x_n} = 0$$

unmöglich.

Dieser Satz enthält die Transcendenz von e durch die Ungleichung

$$e - \alpha \cdot e^0 \neq 0,$$

die von π durch

$$e^{i\pi} + e^0 \neq 0$$

Wir können aber noch andere sehr interessante Resultate aus ihm ableiten. Wir setzen

$$n = 2,$$

$$\left.\begin{array}{l} X_1 = -1,\ X_2 = X \neq 0 \\ x_1 = x \neq 0,\ x_2 = 0 \end{array}\right\} X \text{ und } x \text{ algebraisch.}$$

Dann ist

$$-e^x + X \neq 0$$

$$e^x \neq X,$$

d.h. e^x ist für algebraisches $x \neq 0$ transcendent. Daraus folgt sofort, daß $\log x$ für $x \neq 1$ dieselbe Eigenschaft besitzt.

Wir setzen ferner

$$n = 3$$

$$X_1 = i,\ X_2 = -i,\ X_3 = 2X \neq 0$$

$$x_1 = ix \neq 0,\ x_2 = -ix,\ x_3 = 0$$

Dann ist

$$ie^{ix} - ie^{-ix} + 2X \neq 0$$

d.h. $$\sin x = \frac{e^{ix} - e^{-ix}}{2i} \neq X$$

d.h. für algebraisches $x \neq 0$ ist $\sin x$ transcendent.

Endlich setzen wir

$$n = 3$$

$$X_1 = i,\ X_2 = -i,\ X_3 = 2$$

$$x_1 = ix \neq 0,\ x_2 = -ix,\ x_3 = y \text{ (reell)}$$

Dann ist

$$ie^{ix} - ie^{-ix} + 2e^{y} \neq 0$$

$$\sin x \neq e^{y}$$

Die Gleichung

$$e^{y} = \sin x$$

ist für algebraische x und y (reell) unmöglich, d.h.

$$y = \log \sin x$$

ist für algebraische x transcendent.

Damit verlassen wir diesen ganzen Abschnitt. Wir haben an der Hand des alten Problems der Quadratur des Kreises eine Fülle der mannigfaltigsten Beziehungen zu den verschiedensten mathematischen Disziplinen und veral-

un zu den Grundlagen geworden. Nun wollen wir es mit einem andern berühmten Problem ebenso machen, nämlich mit dem Parallelenproblem.

II. Abschnitt.
Das Parallelenproblem.

§. 5. Wir müssen zunächst über die Grundlagen der Geometrie sprechen, wir begnügen uns dabei mit der ebenen Geometrie. Ich unterscheide fünf Gruppen von Axiomen. Die Axiome sind Aussagen über zwei Systeme von Dingen; die Dinge des ersten Systems nennen wir Punkte und bezeichnen sie durch große lateinische Buchstaben; die Dinge des zweiten Systems heißen Gerade und werden durch kleine lateinische Buchstaben bezeichnet.

Gruppe I. Axiome der Verknüpfung.

I_1. Zwei voneinander verschiedene Punkte A, B bestimmen stets eine Gerade a.

I_2. Irgend zwei voneinander verschiedene Punkte einer Geraden bestimmen diese Gerade.

I_3. Auf jeder Geraden a gibt es wenigstens zwei Punkte A, B; und es gibt mindestens einen Punkt C, der nicht auf der Geraden a liegt.

Gruppe II. Axiome der Anordnung.

II_1. Wenn A, B, C Punkte einer Geraden sind, und B zwischen A und C liegt, so liegt B auch zwischen C und A.

II_2. Wenn A und C zwei Punkte einer Geraden sind, so gibt es wenigstens einen Punkt B, der zwischen A und C liegt, und wenigstens einen Punkt D, so daß C zwischen A und D liegt.

II_3. Unter irgend drei Punkten einer Geraden gibt es stets einen und nur einen, der zwischen den beiden andern liegt.

Erklärung: Wir betrachten auf einer Geraden a zwei Punkte A und B; wir nennen das System der beiden Punkte eine Strecke und bezeichnen dieselbe mit AB oder BA. Die Punkte zwischen A und B heißen Punkte der Strecke AB oder auch innerhalb der Strecke AB gelegen; die Punkte A, B heißen Endpunkte der Strecke AB. Alle übrigen Punkte der Geraden a heißen außerhalb der Strecke AB gelegen.

II_4. Es seien A, B, C drei nicht auf einer Geraden liegende Punkte. Dann geht jede Gerade, die durch einen Punkt der Strecke AB geht, durch einen Punkt der Strecke BC oder

oder durch einen der Strecke AB, d.h. eine Gerade, die in ein Dreieck hineingeht, tritt auch wieder heraus.

Erklärung: Es seien A, A', O, B vier Punkte einer Geraden a, sodass O zwischen A und B, aber nicht zwischen A und A' liegt; dann sagen wir, die Punkte A, A' liegen in der Geraden a auf ein und derselben Seite vom Punkte O, und die Punkte A, B liegen in a auf verschiedenen Seiten von O. Die sämtlichen auf ein und derselben Seite von O gelegenen Punkte der Geraden a heißen auch ein von O ausgehender Halbstrahl; somit teilt jeder Punkt einer Geraden diese in zwei Halbstrahlen. h, k seien irgend zwei ver-

schiedene von O ausgehende Halbstrahlen, die verschiedenen Geraden angehören. Das System dieser beiden Halbstrahlen nennen wir einen Winkel und bezeichnen ihn mit $\sphericalangle(h,k)$ oder $\sphericalangle(k,h)$.

Gruppe III. Axiome der Kongruenz.

III_1. Wenn A, B zwei Punkte auf einer Geraden a und ferner A' ein Punkt auf derselben oder einer anderen Geraden a' ist, so kann man auf einer gegebenen Seite der Geraden a' ~~stets~~ einen und nur einen Punkt B' finden, sodaß die Strecke AB der Strecke A'B' kongruent oder gleich ist, in Zeichen:

$$AB \equiv A'B'$$

Jede Strecke ist sich selbst kongruent, d.h.

$$AB \equiv AB, \quad AB \equiv BA$$

III_2. Ist $AB \equiv A'B'$ und $AB \equiv A''B''$, so ist auch $A'B' \equiv A''B''$.

III_3. Es seien AB und BC Strecken ohne gemeinsame Punkte auf der Geraden a und ferner $A'B'$ und $B'C'$ Strecken auf derselben oder einer anderen Geraden a' ebenfalls ohne gemeinsame Punkte; wenn dann

$$AB \equiv A'B', \quad BC \equiv B'C'$$

ist, so ist auch stets

$$AC \equiv A'C'$$

III_4. Gegeben sei ein Winkel $\sphericalangle(h,k)$, ferner ein von O' ausgehender Halbstrahl h'. Dann läßt sich auf jeder der beiden Seiten von h' ein und nur ein von O' ausgehender Halbstrahl k' finden, sodaß

$$\sphericalangle(h,k) \equiv \sphericalangle(h',k')$$

Es ist

$$\sphericalangle(h,k) \equiv \sphericalangle(h,k),\ \sphericalangle(h,k) \equiv \sphericalangle(k,h)$$

$\overline{\underline{III}}_5$. Ist $\sphericalangle(h,k) \equiv \sphericalangle(h',k')$ und $\sphericalangle(h,k) \equiv \sphericalangle(h'',k'')$, so ist $\sphericalangle(h',k') \equiv \sphericalangle(h'',k'')$

Das $\overline{\underline{III}}_3$ entsprechende Axiom über Winkel läßt sich jetzt schon beweisen.

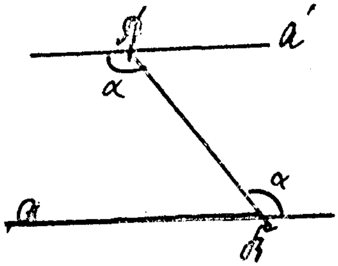
$\overline{\underline{III}}_6$. (Erster Kongruenzsatz.) Wenn für zwei Dreiecke ABC und $A'B'C'$ die Kongruenzen

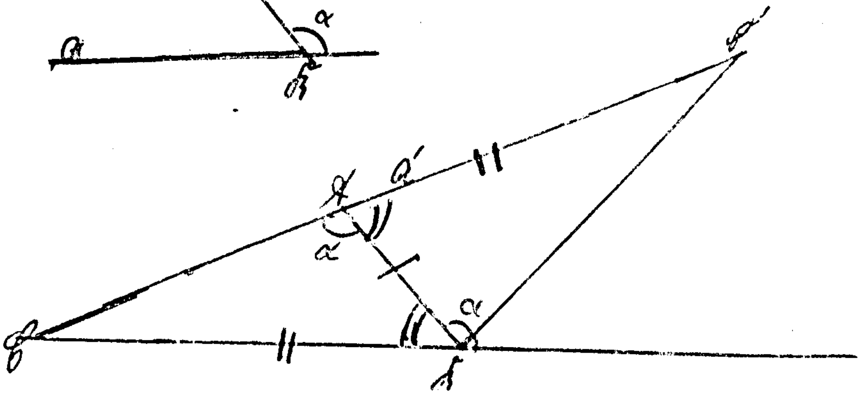
$$AB \equiv A'B',\ AC \equiv A'C',\ \sphericalangle BAC \equiv \sphericalangle B'A'C'$$

gelten, so ist auch

$$\sphericalangle ABC \equiv \sphericalangle A'B'C' \text{ und } \sphericalangle ACB \equiv \sphericalangle A'C'B'.$$

Gruppe $\overline{\underline{IV}}$. Das Parallelenaxiom. Es sei a eine beliebige Gerade und A ein Punkt außerhalb a: dann gibt es höchstens eine Gerade, die durch A läuft und a nicht schneidet.


a′
α
α


a′
α
α

Die erste Frage ist, gibt es durch A überhaupt eine Gerade, welche a nicht trifft? Auf diese Frage gibt das Parallelenaxiom keine Antwort; es hat mit dem Axiom gar nichts zu schaffen. Wir wollen eine Gerade, die a nicht trifft, eine Parallele zu a nennen. Es ist ein Satz, daß es zu a durch A eine Parallele gibt. Um das zu beweisen, verbinde ich A mit irgend einem Punkte B der Geraden ~~A~~ a und trage den Winkel α an AB im Punkte A nach der entgegengesetzten Seite hin an. Die so entstehende Gerade a' trifft a nicht. Denn angenommen, a' treffe a im Punkte C; ich trage BC auf a' nach der entgegengesetzten Seite von A bis C' ab. Dann ist

$$\Delta CAB \equiv \Delta C'BA, \quad \text{(1. Kongruenzsatz)}$$

Also wäre auch $\sphericalangle ABC'' = \alpha$, d. h. C'' läge auf a und a' hätte mit a zwei Punkte gemeinsam.

Nun kann man alle Sätze über Parallele leicht beweisen.

Gruppe V. Stetigkeitsaxiome.

V_1. (Archimedischer Axiom oder Axiom des Messens.) Es sei A_1 ein beliebiger Punkt auf einer Geraden zwischen den beliebig gegebenen Punkten A und B; man konstruiere dann die Punkte $A_2, A_3, A_4 \ldots$, sodaß A_1 zwischen A und A_2, ferner A_2 zwischen A_1 und A_3, ferner A_3 zwischen A_2 und A_4 liegt u. s. w. und überdies die Strecken

$$AA_1,\ A_1A_2,\ A_2A_3,\ A_3A_4 \ldots$$

einander gleich sind: dann gibt es in der

Reihe der Punkte $A_2, A_3, A_4 \dots$ stets einen solchen Punkt A_n, daß B zwischen A und A_n liegt.

V_2 (Axiom der Vollständigkeit.) Die Elemente (Punkte, Gerade) der Geometrie bilden ein System von Dingen, welches bei Aufrechterhaltung sämtlicher genannten Axiome keiner Erweiterung mehr fähig ist, d. h. zu dem System der Punkte, Geraden ist es nicht möglich, ein anderes System von Dingen hinzuzufügen, sodaß in dem durch Zusammensetzung entstehenden System sämtliche aufgeführten Axiome I – IV, V_1 erfüllt sind.

Mit Hilfe dieser Axiome kann man nun die ganze euklidische Geometrie auf-

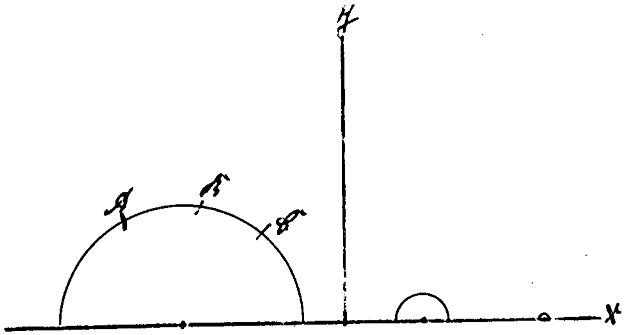
bauen. Davon werden wir aber nicht weiter reden; Sie finden das in meinem Buche über die Grundlagen der Geometrie. Eine zweite Frage ist die nach der Widerspruchslosigkeit; das ist i. A. bei allen axiomatischen Untersuchungen der schwierigste Punkt. Drittens ist aber der Punkt zu erwähnen, der am besten die Fruchtbarkeit axiomatischer Untersuchungen ins Licht stellt, und auf den ich vor allem eingehen will; das ist die Frage nach der Unabhängigkeit der Axiome. Die berühmte Frage ist hier die, ob Euklid darin Recht hatte, das Parallelenaxiom in sein System aufzunehmen. Man kann dieselbe Frage aber auch bei den anderen Axiomen erheben.

Wir wollen nun beweisen, dass das Parallelenaxiom nicht überflüssig ist. Die Methode der Beweisgänger ist die, dass wir ein vollständiges System von Dingen angeben, bei welchem alle Axiome ausser dem Parallelenaxiom gültig sind, und das in sich widerspruchslos ist. Dieses System nennt man „Nichteuklidische Geometrie".

Wir wollen nun dieses System definieren. Ich errichte in der euklidischen Ebene ein rechtwinkliges Koordinatenkreuz. In meinem neuen System verstehe ich unter „Punkten" die sämtlichen Punkte der positiven Halbebene, d.h. alle Punkte der euklidischen Ebene, für die

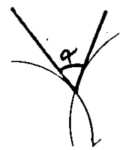
$$y > 0$$

ist. Ferner zeichne ich irgend einen Halbkreis,



dessen Mittelpunkt auf der x-Achse liegt. Alle derartigen Halbkreise in der oberen Halbebene – die Endpunkte werden dabei nicht mitgerechnet! –, ebenso alle Geraden der oberen Halbebene, welche senkrecht auf der x-Achse stehen – wieder mit Ausnahme des Endpunktes – bilden ~~nun~~ die Geraden meines neuen Systems.

Ich habe nun zu sehen, ob unsere Axiome erfüllt sind. Für die Gruppe I ist das selbstverständlich, ebenso für die Gruppe II, sobald man festsetzt, daß B „zwischen" A und C liegt. Bei der Gruppe III ist die Sache schwieriger. Ich muß zunächst, um Strecken abtragen zu können, etwas der Länge entsprechendes definieren. Unter der Länge der Strecke AB verstehe ich



α

$$L(AB) = \int_A^B \frac{ds}{y} = \int_A^B \frac{\sqrt{dx^2+dy^2}}{y}$$

Der Winkel wird wie üblich durch die Tangenten definiert. Daß man jede endliche Länge von einem beliebigen Punkte einer Geraden auf dieser abtragen kann, liegt daran, daß

$$\int_A^B \frac{ds}{y}$$

unendlich wird, wenn A oder B sich der x-Achse nähern. III_1 bis III_5 sind jetzt trivial. Das einzige, was wir beweisen müssen, ist III_6.

Dazu müssen wir erst die Bewegung analytisch definieren:

$$z' = \frac{\alpha z+\beta}{\gamma z+\delta}, \qquad \alpha\delta-\beta\gamma=1$$

wo

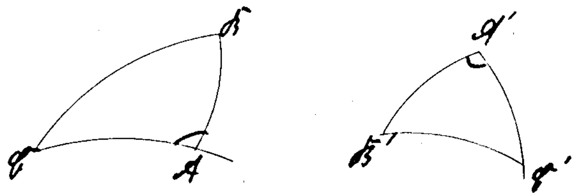
$$z = x+iy, \quad z' = x'+iy'$$

Das ist eine Transformation der euklidischen Ebene in sich. Mit Hilfe dieser Definition der Bewegung will ich nun III_6 beweisen. Ich muß zeigen:

1.) Daß die Winkel bei dieser Transformation erhalten bleiben.

2.) Daß Gerade in Geraden übergehen und die Längen sich nicht ändern.

Schließlich muß ich noch zeigen, daß ich eine Bewegung angeben kann, d.h. $\alpha, \beta, \gamma, \delta$ so wählen kann, daß A in A' und die Richtung AB in die Richtung $A'B'$ übergeht. Dazu genügt es zu zeigen, daß AB in die y-Achse transformiert werden kann, und daß ich jeden Punkt der y-Achse in jeden anderen Punkt der y-Achse überführen kann, denn durch ku-


B
C
A
A'
B'
C'

sammensetzung von Bewegungen erhalte ich wieder eine Bewegung.

Wenn ich das gemacht habe, so kann ich III_6 beweisen, indem ich die Dreiecke zur Deckung bringe. Ich bestimme $\alpha, \beta, \gamma, \delta$ so, daß A in A' und die Richtung AB in $A'B'$ übergeht. Daraus, daß die Längen invariant sind, folgt von selbst, daß B in B' übergeht. Da aber bei jeder solchen Transformation die Winkel erhalten bleiben, und die Winkel bei A und A' n. V. gleich sind, so muß die Gerade AC in die Gerade $A'C'$ übergehen. Ferner muß wegen $\overline{CA} = \overline{C'A'}$ C in C' übergehen. Also ist $\overline{BC} = \overline{B'C'}$, und auch die Winkel bleiben nach unseren Axiomen erhalten.

Nun müssen wir die oben bezeichneten

Tatsachen beweisen. Es ist

$$2iy' = \frac{\alpha z+\beta}{\gamma z+\delta} - \frac{\alpha\bar{z}+\beta}{\gamma\bar{z}+\delta} = \frac{z-\bar{z}}{(\gamma z+\delta)(\gamma\bar{z}+\delta)} = \frac{2iy}{(\gamma z+\delta)(\gamma\bar{z}+\delta)}$$

$$y' = \frac{y}{|\gamma z+\delta|^2}$$

Also gehen Punkte in Punkte über; denn aus $y>0$ folgt $y'>0$. Ferner ist

$$\frac{dz'}{dz} = \frac{(\gamma z+\delta)\alpha - (\alpha z+\beta)\gamma}{(\gamma z+\delta)^2} = \frac{1}{(\gamma z+\delta)^2}$$

also

$$\left|\frac{dz'}{dz}\right| = \frac{1}{|\gamma z+\delta|^2}$$

Ferner ist

$$|z| = \sqrt{z\cdot\bar{z}} = \sqrt{x^2+y^2}$$

also

$$|dz| = \sqrt{dz\cdot d\bar{z}} = \sqrt{dx^2+dy^2} = ds$$

Nun können wir sofort sehen, daß die Länge bei der Bewegung invariant ist; denn es ist:

$$L(A'B') = \int_{A'}^{B'} \frac{ds'}{y'} = \int_{A'}^{B'} \frac{|dz'|}{y'} = \int_{A}^{B} \frac{|dz|}{|\gamma z+\delta|^2} \cdot \frac{|\gamma z+\delta|^2}{y}$$

$$= \int_{A}^{B} \frac{|dz|}{y} = \int_{A}^{B} \frac{ds}{y} = L(AB)$$

Die anderen Sätze beweisen wir ohne Rechnung folgendermaßen: Eine spezielle Bewegung ist folgende:

$$z' = z + \mu,$$

wo μ eine reelle Konstante ist, und auch diese:

$$z' = -\frac{1}{z},$$

die Transformation durch reziproke Radien am Einheitskreise. Aus diesen beiden Bewegungen läßt sich jede andere zusammensetzen nach folgendem Schema:

$$z : z+\mu : -\frac{1}{z}+\mu : -\frac{1}{z+\nu}+\mu : -\frac{1}{-\frac{1}{z}+\nu}+\mu = \frac{z}{1-\nu z}+\mu :$$

$$\frac{z+\varrho}{1-\nu z-\nu\varrho}+\mu=\frac{z+\varrho+\mu-\mu\nu z-\mu\nu\varrho}{1-\nu z-\nu\varrho}$$

Dann muß sein

$$\alpha = 1-\mu\nu \qquad \beta=\varrho+\mu-\mu\nu\varrho$$
$$\gamma = -\nu \qquad \delta = 1-\nu\varrho$$

In der Tat ist

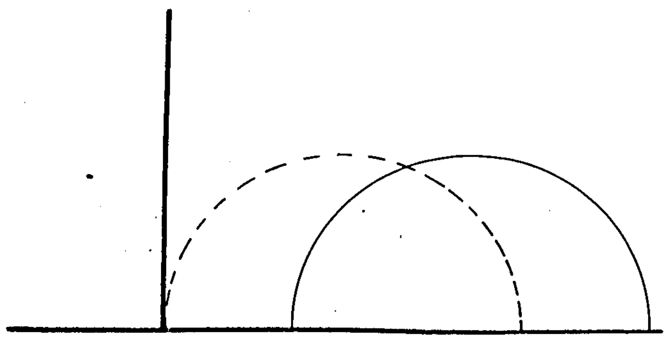
$$\alpha\delta-\beta\gamma=1$$

Durch geeignete Wahl von μ, ν, ϱ kann man jede Bewegung erhalten; denn sind $\alpha, \beta, \gamma, \delta$ gegeben, so folgt

$$\nu=-\gamma$$
$$\mu=\frac{\alpha-1}{\gamma} \qquad (\gamma\neq 0)$$

u.s.f.

Wir brauchen also alles nur für unsere speziellen Bewegungen zu beweisen. Daß bei den beiden Transformationen Kreise in Kreise



übergehen und Winkel erhalten bleiben, ist bekannt. Daher gehen auch die zur x-Achse orthogonalen Kreise in ebensolche über. Ferner ist es möglich eine Bewegung herzustellen, welche den Punkt A in einen Punkt der y-Achse und die Richtung AB in die y-Achse transformiert. Wir wenden zunächst die Verschiebung

$$z' = z + \mu$$

an, durch welche die Gerade AB an die y-Achse herangerückt wird. Dann wenden wir die Transformation

$$z' = -\frac{1}{z}$$

an, durch welche die Gerade in die y-Achse übergeht. Schließlich brauchen wir noch eine Bewegung, bei welcher die y-Achse unverändert bleibt, aber irgend ein vor-

gegebener Punkt P auf ihr in irgend einen anderen Punkt P' übergeht. Das geschieht durch die Transformation

$$z' = pz \qquad p > 0$$

$$\alpha = \sqrt{p} \qquad \beta = 0$$

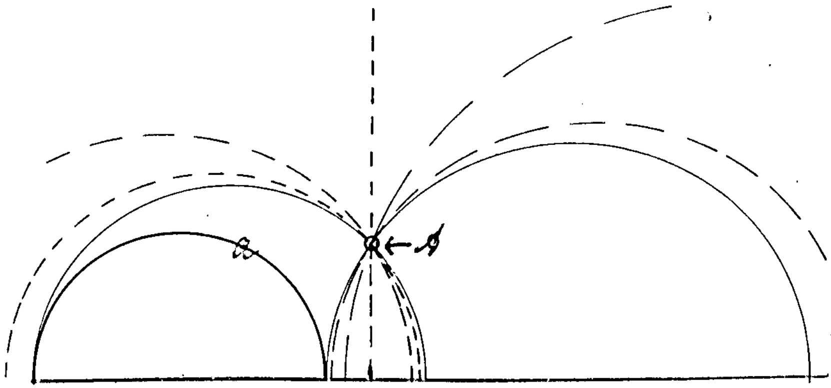
$$\gamma = 0 \qquad \delta = \frac{1}{\sqrt{p}}$$

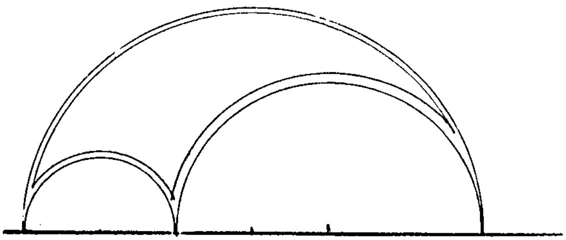
Es ist

$$x' = p \cdot x \qquad y' = p \cdot y$$

Also bleibt die y-Achse unverändert; ich kann aber p so wählen, daß P in P' übergeht.

Auch die Stetigkeitsaxiome sind erfüllt. Denn da ich Längen addieren kann, kann ich über jede gegebene Länge hinauskommen. Das Vollständigkeitsaxiom wäre etwas schwieriger zu beweisen; wir wollen uns nicht dabei aufhalten



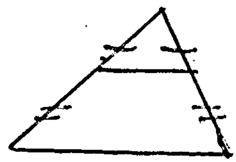


Wie ist es nun mit dem Parallelenaxiom? Offenbar gibt es zu a durch A ein ganzes Bündel von Parallelen, dessen Grenzgeraden rot ausgezogen sind.

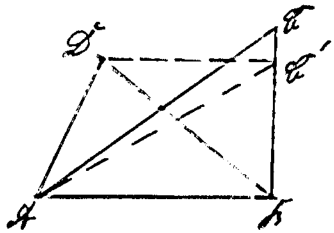
Natürlich gelten jetzt alle Sätze nicht mehr, zu deren Beweis man das Parallelenaxiom braucht, z. B. der von der Winkelsumme im Dreieck, welche man beliebig klein machen kann. Daß sie nicht größer als 2 R sein kann, hat Legendre bewiesen.

Ich will nun noch zwei Punkte erwähnen, die Lehre von den Proportionen und die von den Flächeninhalten.

Was die erstere anbetrifft, möchte ich folgendes bemerken: In den üblichen Lehrbüchern wird ein Dreieck genommen, eine Parallele zur Grund-



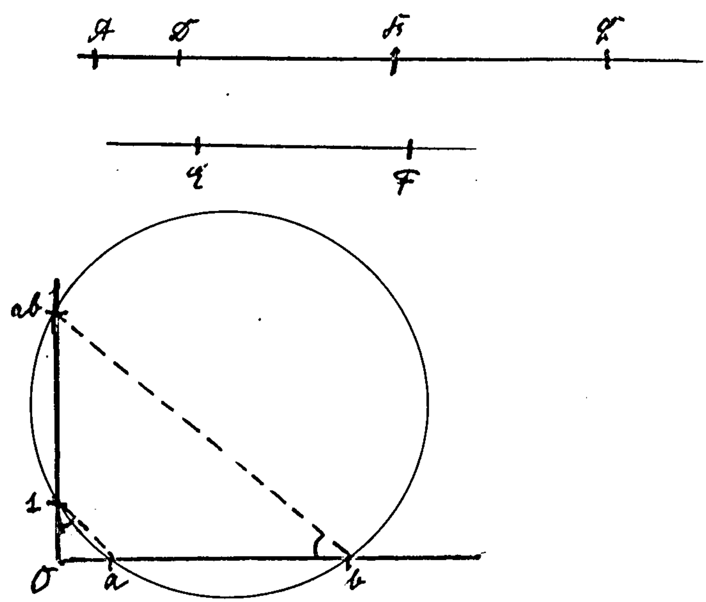
Linie gezogen, und dann mit mehr oder weniger geschickten Redensarten behauptet, daß die Abschnitte auf den Seiten sich gleich verhalten. Wenn die Strecken kommensurabel sind, läßt sich das mit den Kongruenzsätzen beweisen. Man würde mit Hilfe der Stetigkeitsaxiome diesen Satz streng beweisen können. Es fragt sich aber, ob man nicht ohne diese Axiome auskommen kann. Kann man nicht vielleicht die Proportionenlehre ebenso wie die Dreiecksätze mit Hilfe der Axiomgruppen I bis IV begründen? Euklid begründet die Proportionenlehre auf die von den Flächeninhalten. Nachdem er in üblicher Weise gezeigt hat, daß Dreiecke mit gleicher Grundlinie und Höhe inhaltsgleich sind, lehrt er den


D
C
C'
A
B

Satz nun: Dreiecke mit gleicher Grundlinie und gleichem Flächeninhalt haben gleiche Höhen, und gibt dafür folgenden Beweis: Er zieht $DC' \parallel AB$. Dann müßten $\triangle ABC$ und $\triangle ABC'$ gleichen Inhalt haben. Nun schließt er: weil ABC' in ABC liegt, kann es mit ABC nicht gleichen Inhalt haben. Das muß aber erst bewiesen werden, und es fragt sich, ob man das ohne die Stetigkeitsaxiome beweisen kann. Das ist in der Tat der Fall, aber es ist äußerst mühsam.

Ich will daher den Beweis nur skizzieren; die genaue Ausführung finden Sie in meinen Grundlagen der Geometrie.

Zwei Polygone heißen zerlegungsgleich, wenn sie in eine endliche Anzahl von Dreiecken zerlegt


ab
1
O
a
b

werden können, die paarweise einander kongruent sind. Zwei Polygone heißen inhaltsgleich, wenn es möglich ist, zu denselben zerlegungsgleiche Polygone hinzuzufügen, sodaß die beiden zusammengesetzten Polygone einander zerlegungsgleich sind.

Nun führen wir eine sog. Streckenrechnung ein. Gegeben seien die Strecken

$$AB = a \qquad CF = b$$

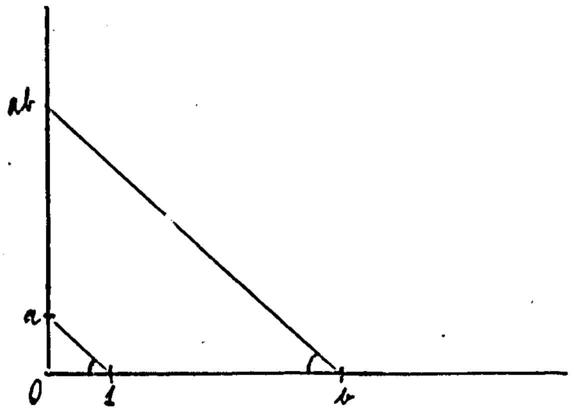
Wir definieren

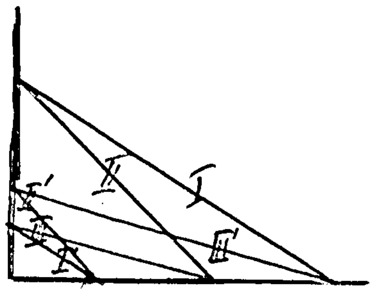
$$AC = a+b$$

$$AD = a-b$$

Das Produkt definieren wir so: wir legen durch 1, a, b einen Kreis; den zweiten Schnittpunkt mit der senkrechten Achse nennen wir ab. Aus dieser Definition folgt sofort

$$ab = ba$$


ab
a
0
1
b


II
I
I'
II'
I

Eine zweite Art der Konstruktion ist die nebenstehende. Denn

$$\underset{\text{f. 146}}{\Delta\, O 1 a} \sim \underset{\text{f. 147}}{\Delta\, O 1 a}$$

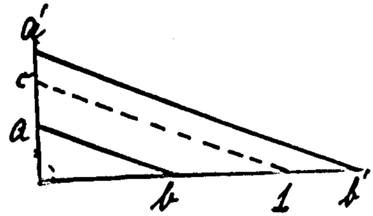
$$\Delta\, O b\, ab \sim \Delta\, O b\, ab$$

Auch hier gilt das kommutative Gesetz, da es bei der ersten Konstruktion gilt. Dadurch erhalten wir den speziellen Pascalschen Satz: Man nehme drei Streckenzüge I, II, III, von denen II mit den Schenkeln des rechten Winkels einen Winkel von 45° einschließe. Führt man den Streckenzug durch Parallele zu I, II, III weiter, so gelangt man zum Ausgangspunkt zurück.

Mit Hilfe dieser Sätze läßt sich dann leicht das assoziative Gesetz beweisen:

$$a(bc) = (ab)c$$

Ferner gilt das distributive Gesetz:


a'
c
a
b
1
b'

$$a(b+c) = ab+ac$$

Auch die Division kann man jetzt einführen, wenn man unter $\frac{1}{a}$ die Strecke b versteht, für die

$$ab = 1$$

ist.

Wir schreiben

$$a : b = a' : b',$$

wenn

$$ab' = a'b$$

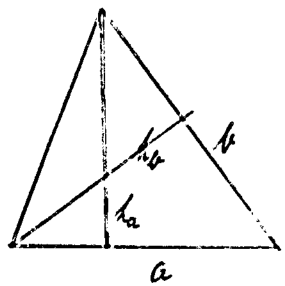
ist.

Dreiecke mit gleichen Winkeln heißen ähnlich. Bei ähnlichen Dreiecken ist

$$a : b : c = a' : b' : c'$$

Wir wollen diesen Satz nur für rechtwinklige Dreiecke beweisen. Es ist

$$a = cb$$
$$a' = cb'$$



h_b
b
h_a
a

Also

$$ab' = ba'$$

Das Genauere möge man in meinem Buche nachlesen. Damit ist die Proportionenlehre begründet. Wir haben dabei weder von Stetigkeit noch von Zahlen gesprochen.

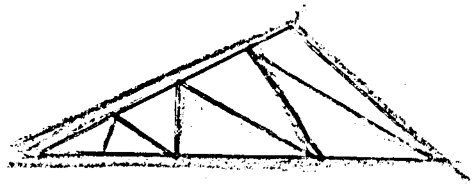
Nun kommt der Begriff des Inhaltsmaßes, zunächst für ein Dreieck. Es ist

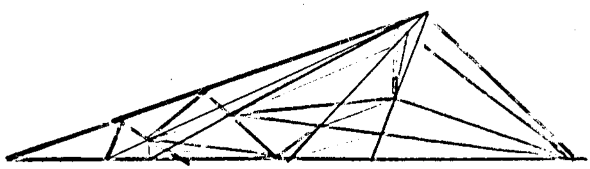
$$a : b = h_b : h_a$$

oder

$$\frac{1}{2} a \cdot h_a = \frac{1}{2} b \cdot h_b = \frac{1}{2} c\, h_c = J$$

J heißt das Inhaltsmaß des Dreiecks. Zerlegt man ein Dreieck in Teildreiecke und nimmt von jedem das Inhaltsmaß, so ist die Summe der Inhaltsmaße gleich dem Inhaltsmaß des ganzen Dreiecks.





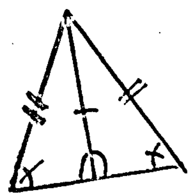
Bew.: Wird das Dreieck nur durch Transversalen von einer Ecke aus zerschnitten, so ist der Satz selbstverständlich.

Wenn keine inneren Schnittpunkte da sind, so betrachten wir successive die farbigen Dreiecke, für die der vorige Fall eintritt.

Im allgemeinen Fall wird eine Seite ausgezeichnet, indem man von der gegenüberliegenden Ecke aus Transversalen zieht (rot). Die Teildreiecke gehören zum vorigen Fall, wenn man ~~bunt~~ Vierecke durch (grüne) Linien in Dreiecke zerlegt.

Inhaltsgleiche Dreiecke haben das gleiche Inhaltsmaß; denn sie sind Summe resp. Differenz von zerlegungsgleichen Polygonen, welche natürlich gleiches Inhaltsmaß haben.

Nun kommen wir endlich zu unserem



Satz: Inhaltsgleiche Dreiecke mit gleicher Grundlinie haben gleiche Höhen.

Denn es ist

$$\frac{1}{2} ha = \frac{1}{2} h'a$$

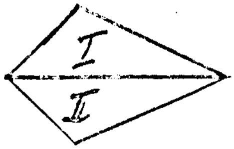
Das multiplizieren wir mit c, welches durch die Gleichung

$$c \cdot \frac{1}{2} a = 1$$

definiert wird, und erhalten

$$h = h', \text{ q.e.d.}$$

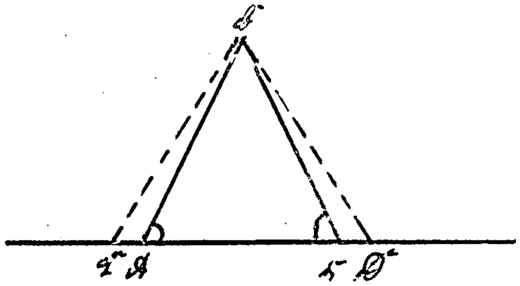
Nun möchte ich noch einige Bemerkungen über die Axiome selbst machen. Man kann unter Umständen einige Axiome abändern oder einengen. Eine Frage liegt hier nahe: Wir haben uns bei dem Kongruenzaxiom III_6 nicht darum gekümmert, wie das Dreieck liegt. Wir können dann den Satz von den Basiswinkeln im gleichschenkligen Dreieck nicht beweisen.


I
II

Nun fragt es sich, läßt sich dieser Satz beweisen, wenn man III_6 nur im engeren Sinne zuläßt; also die Dreiecke I u. II nicht als kongruent ansieht. Es stellt sich heraus, daß man sich darüber schlüssig werden muß, ob man die Axiomgruppe V zuläßt oder nicht. Nimmt man die Stetigkeitsaxiome hinzu, so kann man mit dem engeren Kongruenzsatz den Basiswinkelsatz beweisen, und erhält daraus dann den Kongruenzsatz im weiteren Sinne. Aber wenn man die Stetigkeitsaxiome ausschließt, wie wir es bei der Proportionenlehre gemacht haben, dann habe ich in meinem Buche gezeigt, daß es nicht möglich ist, den Satz vom gleichschenkligen Dreieck zu beweisen. Ebensowenig kann man den Satz beweisen, daß ein Polygon nicht inhaltsgleich

einem Polygon ist, in dessen Innern er liegt.

Ich möchte nun auf einige Punkte zu sprechen kommen, welche noch einer genaueren Untersuchung bedürfen. Mit Hilfe von $\underline{III}_6$ im weiteren Sinne kann man beweisen, daß das kommutative Gesetz bei der Winkeladdition gilt. Wenn wir aber $\underline{III}_6$ nur im engeren Sinne zulassen, so müssen diese Dinge näher diskutiert werden. Das wäre der eine Punkt. Nun könnte man aber dies Gesetz als Axiom formulieren, und $\underline{III}_6$ nur im engeren Sinne zulassen. Dann läßt der Satz von den Basiswinkeln ohne Stetigkeitsaxiome nicht beweisen. Die Frage ist nun, was kann man noch hinzufügen,



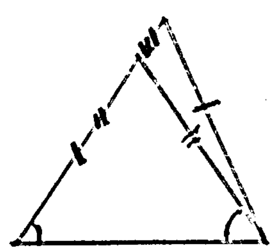
um diesen Satz beweisbar zu machen? Man könnte den Satz selbst ja als Axiom nehmen; es besteht aber die Frage, ob man nicht besonders anschauliche Axiome finden kann, welche nur das leisten. Ein solches Axiom wäre dies, daß ein Polygon einem anderen Polygon, in dessen Innern es liegt, nicht inhaltsgleich sein kann. Damit kann man den Satz vom gleichschenkligen Dreieck beweisen. (Dieser Satz enthält zwei Sätze: 1.) aus der Gleichheit der Schenkel folgt die der Winkel; 2.) die Umkehrung hiervon.) Wir können mit unserem Axiom 2.) beweisen: Ich mache

$$AD = BE, \quad BC = AE$$

Dann ist

$$\triangle CAD \cong \triangle ABE$$ (im engeren Sinne)

also sind die Dreiecke inhaltsgleich; sie haben dieselbe



Stücke; daher müssen sie auch dieselbe Basis haben:

$$EB = AD$$

d.h. $BC = AC$, q.e.d.

Ob man auch 1.) beweisen kann, will ich dahingestellt sein lassen.

Ein directer Beweis wäre folgender: In jedem Dreieck ist die Summe zweier Seiten größer als die dritte. Es wäre z.B. zu untersuchen, ob man dies aus dem Kongruenzsatze beweisen kann. Mit unserem neuen Beweis können wir 1.) beweisen. Angenommen, die Basiswinkel wären nicht gleich; wir tragen dann den linken Winkel rechts an. nach 2) sind die Schenkel des so entstehenden Dreiecks gleich. Also haben wir ein Dreieck, wo die Summe zweier Seiten gleich der dritten ist.

Nun möchte ich noch folgende Bemerkung machen: Man spricht für gewöhnlich von zwei nichteuklidischen Geometrien, von der Bolyai-Lobatschefskischen und der Riemann-Helmholtzschen. Ich habe aber nur von einer nichteuklidischen Geometrie gesprochen. Das liegt daran, daß ich die Axiome der Gruppe II so formuliert habe, daß die zweite nichteuklidische Geometrie von vornherein ausgeschlossen wurde. Unter drei beliebigen Punkten einer Geraden hatte nämlich einer eine bevorzugte Lage, denn er lag „zwischen" den beiden andern. Man kann aber die Axiome II auch so formulieren, daß die Anordnung der Punkte auf der Geraden möglich ist ohne eine solche

Bewegung. Das ist für die Riemann-Helmholtzsche Geometrie nötig; ich will von ihr kurz etwas sagen. Man betrachte alle geraden Linien und Ebenen im Raume, welche durch einen festen Punkt gehen. Wir fassen jede solche Gerade als Punkt und jede solche Ebene als gerade Linie auf. Dann sind alle Axiome I bis III und V erfüllt, nur IV nicht. Freilich die Anordnungsaxiome sind ein wenig modifiziert. Wir streichen das Axiom: Unter drei Punkten auf einer Geraden liegt einer und nur einer zwischen den beiden andern. Auch die anderen Axiome muss man so umändern, dass sie einen vernünftigen Sinn erhalten. Man spricht statt von drei immer von vier Punkten

An Stelle der gestrichenen Axiome tritt folgendes: Wenn ich vier Punkte auf einer Geraden habe, so können sie so angeordnet werden, daß die Punkte des einen Paares die des anderen trennen. Als Länge einer Strecke definieren wir den Winkel, den die die Endpunkte vorstellenden Geraden bilden. Die Kongruenzaxiome gelten natürlich; sie sind nichts anderes als die Kongruenzsätze der sphärischen Geometrie. Dann ist es ohne weiteres klar, daß alle Geraden einen Punkt gemeinsam haben; also gibt es überhaupt keine parallelen Geraden. Infolgedessen ist der Satz von der Winkelsumme im Dreieck falsch; sie ist stets $> 2R$.

Das ist das Wesentliche über die sog. elliptische

Geometrie; die Bolyai-Lobatschefskische heißt auch hyperbolische, die gewöhnliche euklidische parabolische Geometrie.

Ich will zum Schluß noch einige axiomatische Betrachtungen über andere Gebiete anfügen. Da wäre z.B. die Frage, ob man den Satz vom Parallelogramm der Kräfte beweisen kann. Natürlich kann man, ohne etwas vorauszusetzen, nichts beweisen. Man kann aber sehen, ob man den Satz nicht aus geeigneten Grundlagen ableiten kann. Ich will Ihnen über ziemlich abgeschlossene Untersuchungen von Darboux über diesen Gegenstand referieren.

Wir betrachten die Kräfte

$$\mathfrak{A} = (\mathfrak{A}_x, \mathfrak{A}_y, \mathfrak{A}_z)$$
$$\mathfrak{B} = (\mathfrak{B}_x, \mathfrak{B}_y, \mathfrak{B}_z)$$
$$\mathfrak{C} = (\mathfrak{C}_x, \mathfrak{C}_y, \mathfrak{C}_z)$$

und es sei

$$\mathfrak{C}_x = \mathfrak{A}_x + \mathfrak{B}_x$$
$$\mathfrak{C}_y = \mathfrak{A}_y + \mathfrak{B}_y$$
$$\mathfrak{C}_z = \mathfrak{A}_z + \mathfrak{B}_z$$

Der Inhalt des Satzes vom Kräfteparallelogramm ist die Ersetzbarkeit der Kräfte $\mathfrak{A}$ und $\mathfrak{B}$ durch die Kraft $\mathfrak{C}$. Man schreibt

$$\mathfrak{C} = \mathfrak{A} + \mathfrak{B}.$$

Um dies zu beweisen, muß man ein System von Axiomen aufstellen; ich will Ihnen das einfachste bisher bekannte System angeben. Wir können die Frage auch so formulieren: Was für Axiome über Vektoren müssen wir voraussetzen, wenn wir den Satz von der Vektoraddition beweisen wollen? Dazu brauchen wir folgende sechs Axiome:

1.) Zu je zwei Vektoren $\mathfrak{A}$, $\mathfrak{B}$ gehört eindeutig bestimmt ein dritter, ihre Summe $\mathfrak{C}$:

$$\mathfrak{A} + \mathfrak{B} = \mathfrak{C}$$

2.) Es gilt das kommutative Gesetz

$$\mathfrak{A} + \mathfrak{B} = \mathfrak{B} + \mathfrak{A}$$

3.) Es gilt das associative Gesetz

$$\mathfrak{A} + (\mathfrak{B} + \mathfrak{C}) = (\mathfrak{A} + \mathfrak{B}) + \mathfrak{C}$$

4.) Wenn α eine reelle Zahl ist, so ist

$$\mathfrak{A} + \alpha\mathfrak{A} = (1 + \alpha)\,\mathfrak{A}$$

5.) Wenn ich eine Drehung $\mathfrak{D}$ auf den Vektor $\mathfrak{A} + \mathfrak{B}$ ausführe, so ist das dasselbe, als wenn ich $\mathfrak{D}$ auf $\mathfrak{A}$ und $\mathfrak{B}$ einzeln anwende und dann addiere:

$$\mathfrak{D}(\mathfrak{A} + \mathfrak{B}) = \mathfrak{D}\mathfrak{A} + \mathfrak{D}\mathfrak{B}$$

6.) Stetigkeitsaxiom: Die Komponenten von $\mathfrak{C}$ sind stetige Funktionen der Komponenten von $\mathfrak{A}$ und $\mathfrak{B}$.

Mit Hilfe dieser Axiome läßt sich der Satz vom Kräfteparallelogramm beweisen. Dies ist aber sehr mühsam, und wir wollen nicht darauf eingehen.

III. Abschnitt.

Die logischen und mathematischen Paradoxien.

Mit Paradoxien hat man sich von alters her beschäftigt; besonders wurden solche von den Sophisten aufgestellt. Ich erinnere an das Paradoxon vom fliegenden Pfeil und an das von Achilles und der Schildkröte. Sie beide zeigen, daß es sich dabei nur um eine schiefe und von uns abzulehnende Anwendung der Stetigkeitsbegriffe handelt; es wird so getan, als hätte jede unendliche Reihe auch einen unendlichen Wert.

Dann kommen wir zu den Paradoxien von Kant, über die ich nicht viel mehr sagen will. Er nennt sie Antinomien; das sind wesentlich Anwendungen der Begriffe der mathematischen Unendlichkeit in Raum und Zeit auf die Wirklichkeit.

Wir werden uns wesentlich mit den logischen Paradoxien beschäftigen. Ich will Ihnen gleich zwei typische Beispiele nennen, die allerdings nicht die besten sind.

1) Dieser Satz, den ich hier aufschreibe, ist unwahr.

Dieses Paradoxon ist aus dem Altertum bekannt unter dem Namen des Paradoxons vom lügenden Kreter.

2.) Die kleinste ganze Zahl, die nicht mit

weniger als sechsundzwanzig Silben definiert werden kann.

Dieser Satz hat 25 Silben; die Zahl kann also doch mit 25 Silben definiert werden.

Aus dem, was ich hier gesagt habe, können wir schon einige Gesichtspunkte gewinnen. Die Art und Weise, wie Ihnen gewöhnlich eine Wissenschaft vorgeführt wird und auch mit Recht vorgeführt werden muß, ist die, wie man bei einem Gebäude erst das Fundament errichtet und dann darauf weiter baut. Die historische Entwickelung ist aber gar nicht so, daß man erst das Fundament legt und dann den Bau errichtet, sondern man greift zunächst irgend was heraus und kümmert sich wenig darum, ob das begründet ist. Man

baut hinein aufs Geratewohl, um vorwärts zu kommen, und erst wenn es ganz schlimm wird und gar nicht mehr auszuhalten ist in diesem Raum, dann erst kümmert man sich um die Fundamente. So ist das immer geschehen: zuerst werden die Fragen, welche für die Anwendungen der Theorie nötig sind, beantwortet, und erst später werden die Fundamente ausgebaut. Ich glaube, daß dies auch der richtige Weg ist; würde man mit den Fundamenten anfangen, so würden viele unnütze Fundamente errichtet werden.

So ist z. B. die Zahlentheorie ausgebaut worden ohne sich über den Begriff der ganzen Zahl selbst Kopfschmerzen zu machen, weil sich nicht das Bedürfnis dazu einstellte. Dann

kam die Differentialrechnung, bei der man sich auch nicht im geringsten um die Fundamente kümmerte. Man stellte die tollsten Sätze nebeneinander, die sich direkt widersprechen, ohne es zu merken, aber der große Erfolg der Disziplin täuschte darüber hinweg. Wie nun aber die funktionentheoretischen Begriffe dazu kamen, wurde es notwendig, auch die Fundamente zu begründen; das geschah durch Cauchy, Riemann und Weierstrass, dessen Darstellungen heute maßgebend sind.

Ähnlich ging es mit dem Gebiete der Mengenlehre: da wurden Überschätzungen gemacht und die schönsten Sätze aufgestellt, bis man auf Schwierigkeiten kam, die eigentlich in letzter Instanz noch heute nicht gelöst sind.

Da möchte ich am liebsten an unsere

Paradoxieen anknüpfen. Sie werden sofort erkennen, daß in dem Begriff „Definieren" eine Schwierigkeit liegt. Was heißt das „definieren"? Ich werde Ihnen Beispiele geben, bei denen Sie zweifelhaft sein werden, ob man das als Definition ansehen soll oder nicht.

Ich definiere die Zahl a folgendermaßen:

Es sei

$$a = \begin{cases} 1, \text{ wenn } 2^{\sqrt{2}} \text{ eine irrationale Zahl ist,} \\ 0, \text{ " " " rationale " ".} \end{cases}$$

Wird man diese Definition anerkennen oder nicht? Man kann sagen, ja! Denn $2^{\sqrt{2}}$ ist eine ganz bestimmte Zahl; diese ist entweder rational oder irrational, also ist a ganz genau definiert. Andrerseits kann ich fragen, ist a nun 0 oder 1? Es ist gar keine Möglichkeit sichtbar, dies zu entscheiden. Es ist ja nicht undenkbar, daß man

einmal den Beweis führen kann, daß 2^{π} irrational ist; aber vielleicht wird sich das niemals entscheiden lassen, und unsere Definition versagt praktisch für alle Zeiten. Das ist jedenfalls ein Fall, der auf der Schwelle liegt. Wir werden uns entscheiden müssen, ob wir die Zahl a als definiert ansehen wollen oder nicht. Nach der Weierstrass'schen Auffassung wäre die Definition zuzulassen: der Wert der Zahl a ist mir zwar nicht bekannt, aber sie hat einen ganz bestimmten Wert; ich brauche diesen aber auch nicht zu wissen.

Ein anderes Beispiel wäre folgendes: Es sei

$$\alpha = 0, z_1 z_2 z_3 z_4 \ldots$$

ein Decimal- oder Dualbruch. α ist definiert, wenn man die Ziffern z alle angeben kann,

nun sind das aber unendlich viele, also ist von einem wirklichen Angeben nicht die Rede. Nach der Weierstrass'schen Auffassung muss ein Gesetz vorhanden sein, nach dem diese Ziffern fortschreiten; ich muss also die n-te angeben können. Ich stelle folgendes Gesetz auf: Ich habe einen Würfelbecher mit 6 Würfeln; z_n sei die Anzahl der Würfel, welche beim n-ten Wurf vom Tische herunterrollen. Werde ich α jetzt als definiert ansehen? Nein; es muss ein mathematisches Gesetz vorhanden sein. Wenn aber kein mathematisches Gesetz da ist, so lehne ich die Definition ab.

Das sollen Beispiele dafür sein, wie in der Tat in dem Begriffe des Definiertseins Schwierigkeiten liegen können.

Ein anderes Beispiel ist folgendes

$a = 1$, wenn die $10^{(10^{10})}$-te Dezimale von π gerade ist

$a = 0$, " " " " " " " ungerade.

Die Definition ist vollständig, denn man kennt die Gesetze der Dezimalbruchentwicklung von π und weiß, wie man zur Entscheidung gelangen kann, wenn sie auch praktisch unmöglich ist.

Schließlich betrachten wir die Definition

$a = 1$, wenn $2^{\sqrt{2}}$ irrational ist,

a ist sinnlos, " " rational ".

Man kann hier noch nicht einmal entscheiden, ob die Definition einen Sinn hat. Trotzdem ist die Wahrscheinlichkeit nicht groß, daß a einen Sinn hat und gleich 1 ist.

Die beste bisherige Theorie dieser Dinge stammt von Russel und heißt Stufentheorie. Man

kann Vollständigkeit nur behaupten in der Stufe der mathematischen Erkenntnis, in der man sich gerade augenblicklich befindet. Treten wir auf eine andere Stufe, finden wir neue Gesetze und Tatsachen. So kann eine Definition Sinn erhalten, die früher keinen hatte.

Um den Dingen näher zu kommen, erinnere wir nochmals an den Satz von der Nichtabzählbarkeit des Kontinuums der reellen Zahlen; der Beweis wurde durch das Diagonalverfahren geführt. Nun kann man ein Paradoxon konstruieren und einen Beweis für die Abzählbarkeit geben. Man kann jede Zahl des Kontinuums in einen Dualbruch entwickeln nach einem bestimmten Gesetz.

Es ist jedenfalls nur eine endliche Anzahl von Silben nötig, die Zahl zu definieren. Man schreibe nun alle Silben auf eine Tafel, auf eine zweite die Kombinationen von je 2 Silben, auf eine dritte die von drei etc. Das sind abzählbar viele Tafeln; die keinen Sinn ergeben, lasse ich weg. Es bleiben die Tafeln übrig, die ~~Zal~~ Zahlen definieren. Diese sind also abzählbar. Man könnte so überhaupt beweisen, daß alle Dinge abzählbar sind, daß es überhaupt keine höheren Mächtigkeiten gibt.

Nach dem Cantorschen Diagonalverfahren muß man aber sicher eine Zahl finden können, die auf keiner Tafel steht. Auf jeder Tafel steht das Gesetz der Dualbruchentwicklung. Ist z_n die n-te Stelle

der n-ten Zahl, so setze man

$$\bar{z}_n = 0, \text{ wenn } z_n = 1 \text{ ist}$$
$$\bar{z}_n = 1, \quad " \quad z_n = 0 \quad "$$

und bilde

$$0, \bar{z}_1 \bar{z}_2 \bar{z}_3 \ldots$$

Dieses Gesetz ist aber auch mit einer endlichen Anzahl von Silben auszudrücken, steht also auf irgend einer Tafel, etwa der m-ten. Unsere Vorschrift heißt aber: man nehme an der m-ten Stelle die Ziffer, die nicht an der m-ten Stelle steht; und das ist nicht ausführbar, die Tafel enthält einen Widerspruch.

Poincaré meint, man müsse die Tafeln vorher mustern und nur diejenigen behalten, die einen vernünftigen Sinn haben. Dann sei kein Widerspruch mehr möglich.

Man müßte z. B. den Begriff der Definierbarkeit durch Silben ausschalten. Es fragt sich nun, ob dann die Paradoxien verschwinden. Die bisher angeführten wären dann natürlich von vornherein sinnlos.

Man kann aber noch andere Paradoxien konstruieren, welche rein logischer oder mathematischer Natur sind, die alsdann also auch nicht behoben sind.

1) Betrachtet man Mengen, so gibt es ganz sicher Mengen, die sich selbst nicht als Element enthalten. Nun betrachten wir alle Mengen, die sich selbst nicht als Element enthalten; sie seien

$N_1, N_2 \ldots$

Die Menge aller dieser Mengen sei N. Nun sind zwei Fälle möglich:

a.) N kommt unter den N_i bereits vor, es sei z.B.

$$N = N_1$$

N_1 enthält sich nicht selbst als Element; N enthält sich aber als Element. Das ist ein Widerspruch, also kann nicht $N = N_i$ sein.

b.) Es tritt also der zweite Fall ein; N enthält sich nicht als Element. Dann muß also N unter den N_i bereits vorhanden sein. Also enthält sich N als Element; wir haben auch hier einen Widerspruch (Russell u. Zermelo)

Nun hat Dedekind, der sich neben Frege und Cantor vor allen Dingen mit diesen Sachen beschäftigt hat, sich gerade auf solche Betrachtungen gestützt. Erst durch Aufdeckung dieser Paradoxieen zeigte sich, daß man hier

vorsichtig sein muss:

Man kann nun nach der Stufentheorie auch philosophische Begriffe, wie Menge, Element etc. ausschalten. Man kann aber auch rein mathematische Paradoxien aufstellen:

2.) Wenn man eine wohldefinierte Menge von Zahlen hat: M_1, und eine zweite Menge M_2, so kann man sie addieren:

$$M_1 + M_2 = M$$

Dies kann man mit beliebig vielen Mengen tun; die Summe bildet wieder eine Menge. Ebenso erlaubt ist das sog. Selbstbelegungsprincip. Jeder Zahl der Menge

$$a_1, a_2, a_3 \ldots \qquad (M)$$

ordne ich eine Zahl von M zu; bez.:

$$b_1, b_2, b_3 \ldots \qquad (b_i = a_k)$$

Habe ich eine andere Zuordnung

$$z_1', z_2', z_3' \dots,$$

so kann ich natürlich die Menge aller Zuordnungen bilden. Sie heißt M^M und man nennt sie die Selbstbelegungsmenge. (Ist M die Menge aller reellen Zahlen, so ist M^M die Menge aller reellen Funktionen)

Nun nehme ich die Menge der natürlichen Zahlen

$$1, 2, 3 \dots \quad (M)$$

und bilde durch Addition und Selbstbelegung neue Mengen, und zwar alle, die es gibt, z.B.

$$M + M^M + (M^M)^{(M^M)} + \dots$$

Alle diese Mengen addiere ich und nenne ihre Summe U. Diese Menge U

ist nun ein Paradoxon. Es sei $U^U = V$. Dann ist gewiß $V < U$; denn V geht allein durch zugelassene Prozesse aus U hervor. Nun kann man beweisen, daß die Relation

$$U^U < U$$

unmöglich ist. Damit haben wir ein Paradoxon, daß sich nicht durch Ausschaltung irgendwelcher Begriffsbestimmungen aufheben läßt.

Nun ist noch der Beweis nachzutragen, daß

$$U^U < U$$

unmöglich ist. Wäre nämlich $U^U < U$, so könnte man die Elemente von U^U ganz in U unterbringen. Man kann aber nicht eine Belegung von U bilden, die nicht

Andere Form des Beweises.

ω, σ, τ seien Elemente in U

Ω, Σ, T " " " U^U

Wäre $U^U < U$, so entsprächen sich die Elemente von U u. U^U eineindeutig.

$$\left.\begin{matrix} & \omega, & \sigma, & \tau \\ \Omega & \Omega_\omega & \Omega_\sigma & \Omega_\tau \\ \Sigma & \Sigma_\omega & \Sigma_\sigma & \Sigma_\tau \\ T & T_\omega & T_\sigma & T_\tau \end{matrix}\right\} \text{ seien die Belegungen.}$$

Ich bilde die Belegung

$$\begin{matrix} \omega & \sigma & \tau \\ \overline{\Omega_\omega} & \overline{\Sigma_\sigma} & \overline{T_\tau} \end{matrix}$$

$\neq \Omega_\omega$ " "

Diese ist nicht in U^U enthalten; das ist ein Widerspruch.

also ist $U < U^U$

in U enthalten sein kann. Seien

$$u_1, u_2, u_3 \ldots\ldots$$

die Elemente von U. $f_i(u)$ sei eine Belegung;
~~Dann mögl. sind.~~ $\cancel{U^U = (f_1, f_2, f_3 \ldots\ldots)}$ ~~sein~~

Sei z. B. $\quad f_1(u_1) = u_{f_1}$

Nun wähle ich ein von u_{f_1} verschiedenes Element von U, u_{g_1}, und bilde

$$g(u_1) = u_{g_1}$$

Sei nun

$$f_2(u_2) = u_{f_2}\;;$$

ich nehme $u_{g_2} \neq u_{f_2}$ und bilde

$$g(u_2) = u_{g_2}$$

u.s.f. (Diagonalverfahren.)

Dann erhalte ich eine neue Funktion g, die in der Menge aller f_i nicht enthalten ist, und nicht in U untergebracht werden kann.

Die Schwierigkeit bei unseren Paradoxen liegt in dem Begriff „alle". Wir können uns nicht auf den Standpunkt stellen, die rein logischen Prinzipien auf die Mathematik ohne weiteres zu übertragen.

Wie verhalten wir uns nun gegen den Widerspruch der „Menge aller Mengen"? Ganz ist dieser Widerspruch noch nicht gelöst.

Ich erinnere Sie an unsere axiomatische Methode in der Geometrie. Das ist auch eine Art von Stufentheorie. Früher hatten wir die Arithmetik und Analysis hingenommen, das geht jetzt nicht mehr. Wir verfahren so, daß wir zunächst das System der reellen Zahlen behandeln u. die ganzen Zahlen beiseite lassen. Bei den reellen Zahlen kommt schon der Begriff der Allheit vor. Unser erster Teil ist also der axiomatische Aufbau der Theorie

der reellen Zahlen. Ich will dies Problem nicht systematisch, sondern mehr andeutungsweise unter Hervorhebung einzelner Punkte behandeln.

~~I. Gruppe: Axiome der Verknüpfung.~~

Ich habe ein System von Dingen, die ich Zahlen nenne, welche folgenden Axiomen genügen.

I. Gruppe, ~~der~~ Axiome Verknüpfung.

I1) Aus der Zahl a und der Zahl b entsteht durch „Addition" eine bestimmte Zahl c

$$c = a + b, \quad a + b = c$$

I$_2$.) Zu ~~einer~~ zwei gegebenen Zahlen a, b existiert stets eine und nur eine Zahl x, und außerdem eine und nur eine Zahl y, sodass

$$a + x = b, \quad y + a = b$$

ist.

I$_3$.) Es gibt eine bestimmte Zahl – sie heiße 0 –,

sodaß für jede Zahl a

$$a+0=a, \quad 0+a=a$$

ist.

$I_4.)$ Aus a und b entsteht auf eine eindeutige Art durch „Multiplikation" eine Zahl c:

$$a \cdot b = c$$

$I_5.)$ Zu zwei gegebenen Zahlen a, b existiert, sofern a nicht 0 ist, stets eine und nur eine Zahl x, und außerdem eine und nur eine Zahl y, sodaß

$$ax=b, \quad ya=b$$

ist.

$I_6.)$ Es gibt eine bestimmte Zahl, – sie heiße 1 –, sodaß

$$a \cdot 1 = a, \quad 1 \cdot a = a$$

ist.

II. Gruppe; Axiome der Rechnung.

II_7.) Assoziatives Gesetz der Addition:

$$a+(b+c)=(a+b)+c$$

II_8.) Kommutatives G. d. A.

$$a+b=b+a$$

II_9.) a.s. G. d. Mult.

$$a(bc)=(ab)\cdot c$$

II_{10}.) Erstes distributives Gesetz

$$a(b+c)=ab+ac$$

II_{11}.) Zweites " "

$$(a+b)c=ac+bc$$

II_{12}.) Kommut. G. d. M.

$$ab=ba$$

III. Gruppe; Axiome der Anordnung.

III_{13}.) Von zwei beliebigen verschiedenen Zahlen a, b ist stets eine größer als die andere; diese heißt dann die kleinere: $a>b$, $b<a$

III.14.) Ist $a>b$, $b>c$, so ist $a>c$.

III.15.) Ist $a>b$, so ist $a+c>b+c$ und $c+a>c+b$

III.16.) Ist $a>b$ und $c>0$, so ist $ac>bc$ und $ca>cb$

IV. Gruppe. Axiome der Stetigkeit.

IV.17.) Archimedischer Axiom. Sind $a>0$ und $b>0$ zwei beliebige Zahlen, so ist es möglich, a zu sich selbst so oft zu addieren, daß

$$a+a+\cdots+a>b$$

ist.

IV.18.) Vollständigkeitsaxiom. Es ist nicht möglich dem System der Zahlen weitere Dinge hinzuzufügen, sodaß auch in dem durch Zusammensetzung entstehenden ~~Axiome~~ System die Axiome 1/17 erfüllt sind; oder: die Zahlen bilden ein System von Dingen, das bei Aufrechterhaltung der bisherigen Axiome keiner Erweiterung mehr fähig ist

Aus diesen Axiomen läßt sich die ganze Theorie der reellen Zahlen aufbauen. Das geschieht so: Aus der 1 erhält man nach I_1

$$1+1=2,\quad 2+1=3, \ldots$$

aus I_2 folgen die negativen ganzen, aus I_5 die rationalen Zahlen. Die irrationalen Zahlen erhalte ich aus der Gruppe III. Wenn ich z.B. beweisen will, daß $\sqrt{2}$ eine Zahl ist, so füge ich sie dem System zu; dann muß nach dem Vollständigkeitsaxiom $\sqrt{2}$ eine Zahl sein. Umgekehrt: habe ich ein Ding x des Systems, so ist entweder $x=0$, dann ist es eine rat. Zahl, sonst ist $x \geq 0$, etwa >0. Ich behaupte nun, $1>0$; – wir wollen das später beweisen. Dann ist

$$x>0,\quad 1>0,$$

also nach dem Stetigkeitsaxiom

$$1+1+\cdots+1 < x < 1+1+\cdots+1+1$$

Auf solche Art läßt sich x in einen Dezimalbruch entwickeln, d.h. es ist eine Zahl.

Wir müssen noch beweisen

$$1 > 0$$

oder einfacher

$$1 \neq 0$$

[Wäre $1 = 0$, so wäre

$$1 + 1 = 1 \;]$$

Es gibt eine Zahl $a \neq 0$; denn es soll Dinge geben; die können also nicht alle gleich 0 sein. Nun ist

$$0 + 0 = 0$$

also

$$a(0+0) = a \cdot 0$$

$$a \cdot 0 + a \cdot 0 = a0$$

. ferner ist nach I_3.

$$a \cdot 0 + 0 = a \cdot 0$$

; also nach $I_2.1$

$$a \cdot 0 = 0$$

Also ist

$$a = a \cdot 1 = a \cdot 0 = 0$$

und das ist ein Widerspruch; also ist $1 \neq 0$.

Es fragt sich, welche Axiome von einander unabhängig sind, und welche nicht. Da wollen wir einige Beispiele herausgreifen, z. B. die Existenz der Zahl 0. Läßt sich diese folgern aus den Axiomen 1, 2, 4/18? Ja! und zwar folgendermaßen aus 1, 2 und 7, 8: Es gibt eine Zahl x, sodaß

$$x + a = a$$

ist, zu jeder Zahl b ein y, sodaß

$$y + b = b$$

Zur Existenz der Zahl 0 ist zu zeigen:

$$x = y$$

Bew.: Es ist

$$b + (x + a) = b + a +$$
$$(y + b) + a = b + a$$

also

$$b+(x+a)=(y+b)+a$$

also $$(b+x)+a=(y+b)+a$$

$$b+x=y+b=b$$

~~d.h. x=y, q.e.d.~~

also $$y+b=b$$

$$b+x=b$$

x ist also unabhängig von a, also ist sie die links- u. rechtsseitige Invariante der Addition, d.h. die Null. Ähnlich läßt sich die Existenz der Zahl 1 nachweisen aus Axiom 4, 5, 9. Wir setzen

$$xa=a \quad (5) \qquad a\neq 0$$

und $$yb=b \quad (5)$$

also

$$bxa=yba \quad (9)(4)$$

$$bx=yb=b \quad (5)$$

$$bx=b,\ q.e.d.$$

$x \cdot a = a$ gilt aber auch für $a = 0$; denn

ist etwa $\quad b + y = 0 \qquad b \neq 0,\ y \neq 0,$

also

$$xy = y$$

$$xa + xy = a + y$$

$$x(a+y) = 0$$

$$x \cdot 0 = 0$$

Für jede Zahl a ist

$$a \cdot 0 = 0$$

Bew.: $\quad b + 0 = b$

$$ab + a \cdot 0 = a \cdot b$$

$$a \cdot 0 = 0$$

Das kommutative Gesetz der Addition läßt sich aus den distributiven Gesetzen u. der Gruppe I beweisen u. dem assoziativen der Addition.

Bew.: Es ist

$$(a+b)(1+1) = (a+b) \cdot 1 + (a+b)1$$

$$(a+b)(1+1) = a\cdot 1 + b\cdot 1 + a\cdot 1 + b\cdot 1$$
$$= a+b+a+b$$

Andrerseits ist

$$(a+b)(1+1) = a(1+1) + b(1+1) = a1 + a1 + b\cdot 1 + b1$$
$$= a+a+b+b$$

d. h.

$$a+b+a+b = a+a+b+b$$
$$a+b+a \quad = a+a+b$$
$$b+a \quad = \quad a+b, \text{ q. e. d.}$$

Gehen wir zu den Stetigkeitsaxiomen über, so gibt es auch da interessante Abhängigkeiten u. Unabhängigkeiten. Wir wollen das kommutative Gesetz der Multiplikation betrachten (12.). Aus den Axiomen der ersten Gruppen läßt es sich nicht beweisen, wohl aber mit Hilfe der Stetigkeitsaxiome.

Wäre $ab \neq ba$, so setzen wir

$$d = ab - ba$$

$$(a+b)(1+1) = a\cdot 1 + b\cdot 1 + a\cdot 1 + b\cdot 1$$
$$= a+b+a+b$$

Andrerseits ist

$$(a+b)(1+1) = a(1+1) + b(1+1) = a1 + a1 + b\cdot 1 + b1$$
$$= a+a+b+b$$

d.h.

$$a+b+a+b = a+a+b+b$$
$$a+b+a = a+a+b$$
$$b+a = a+b, \text{ q.e.d.}$$

Gehen wir zu den Stetigkeitsaxiomen über, so gibt es auch da interessante Abhängigkeiten u. Unabhängigkeiten. Wir wollen das kommutative Gesetz der Multiplikation betrachten (12.). Aus den Axiomen der ersten Gruppen läßt es sich nicht beweisen, wohl aber mit Hilfe der Stetigkeitsaxiome.

Wäre $ab \neq ba$, so setzen wir

$$d = ab - ba$$

Mit Hilfe von (17) läßt sich hieraus ein Widerspruch konstruieren.

Schwieriger ist es, zu zeigen, daß $ab = ba$ nicht aus den Gruppen I/III folgt.

Ein anderer Punkt von prinzipiellem Interesse ist die Nichtbeweisbarkeit der Axiome der Stetigkeit aus den Gruppen I/III. Ich will Ihnen beweisen, daß das Axiom (17) unabhängig ist von den Axiomen 1/16. Dazu muß ich ein System von Dingen angeben, welche 1/16 erfüllen, aber nicht 17.

Dazu nehme ich einen Parameter t; mein System von Dingen sind die rationalen Funktionen von t mit rationalen Koeffizienten; das allgemeine Ding meines Systems ist also

$$\frac{A_1 t^{n_1} + A_2 t^{n_2} + \ldots + A_\nu t^{n_\nu}}{B_1 t^{m_1} + B_2 t^{m_2} + \ldots + B_\mu t^{m_\mu}}$$

die A u. B sind rationale Zahlen $\neq 0$, die n u. m ganze Zahlen > 0.

Die 0 soll auch zum System gehören. Addiert und multipliziert wird im gewöhnlichen Sinne. Dann sind die Gruppen I u. II erfüllt. Ferner soll

$$a > b$$

sein, wenn

$$a - b = R(t),$$

das an gewissen Stellen sein Vorzeichen ändern kann, nämlich an den Nullstellen des Zählers und des Nenners, für die t, welche größer als diese Nullstellen sind – für diese wechselt $R(t)$ sein Zeichen nicht mehr –, positiv ist. Bei dieser Festsetzung ist Gruppe III erfüllt. Jedoch das Archimedische Axiom ist nicht richtig. Um das zu zeigen, setze ich

$$a = 1, \quad b = t$$

Es ist also zu zeigen

$$n < t,$$

wo n eine feste ganze Zahl ist. Die rationale Funktion $n - t$ ist für wachsende t negativ, also in der Tat stets $n < t$.

Das ist das einfachste Beispiel eines nichtarchimedischen Zahlensystems. In ihm sind Zahlen[70] enthalten, die kleiner sind als jede rationale Zahl, z.B. $\frac{1}{t}$; denn

$$\frac{1}{t} - r$$

ist für große t negativ, wie klein auch r sei. Man kann also die Zahl $\frac{1}{t}$ als aktual unendlich klein ~~sein~~ ansehen, ebenso wie die Zahl t als aktual unendlich groß.

Es läßt sich ein nichtarchimedisches System angeben, wo $ab \neq ba$ ist; damit ist die Unabhängigkeit des

Axiomes (12) von den Gruppen I/III beweisen; wir können jedoch hier nicht darauf eingehen.

Die reellen Zahlen geben uns wieder ein sehr schönes Beispiel für die Anwendung der axiomatischen Methode. Unseren eigentlichen Untersuchungsgegenstand haben wir aber in dem Paradoxon der Menge U^u zu sehen, zu deren Aufklärung wir alle diese Dinge besprechen. Wir müssen nun weiter an die Untersuchung des Begriffes „alle" gehen.

Die reellen Zahlen sind ein System von Dingen, bei dem wir keinen Widerspruch gefunden haben; jedoch können wir auch nicht die Widerspruchslosigkeit des Systems beweisen. Bei den geometrischen Axiomen konnten wir die Frage auf die Widerspruchslosigkeit der reellen Zahlen reduzieren, etwas analoges haben wir jetzt nicht.

Dagegen haben wir das Paradoxon der Menge M^u, welches doch indirekt mit dem System der reellen Zahlen zusammenhängt. Wir können aber noch einen guten Schritt weiter gehen: der Begriff „alle" steckt schon im Begriff der Anzahl, und unser Paradoxon können wir ebenso gut aus den ganzen Zahlen, wie aus den reellen aufbauen. Wir müssen uns daher mit dem Begriff der ganzen Zahlen oder der Anzahl beschäftigen. Wir haben ja auch im Axiom 17 den Begriff der Anzahl schon benutzt; es ist also eine besondere Untersuchung desselben sehr erwünscht.

Die ganzen Zahlen wurden zuerst behandelt von Dedekind, Frege und Cantor.

Wie ich schon sagte, haben die ersten beiden Forscher die Unzulänglichkeit ihrer Untersuchungen selbst anerkannt, trotzdem war z. B. die Schrift von Dedekind: Was sind und was sollen die Zahlen? epochemachend.

Von Cantor stammt der Ausdruck der konsistenten und nicht konsistenten Mengen; erstere sind die Mengen, welche keinen Widerspruch in sich schließen.

Wir werden die ganzen, positiven Zahlen wieder nach der axiomatischen Methode behandeln, als Grundlage lassen wir die Gesetze der Logik zu. Wir stellen folgende Axiome auf:

I. 1 ist eine Zahl; durch den Prozess der Zählen entsteht wieder eine Zahl, oder: Wenn n eine Zahl ist, so ist auch $n+1$ eine Zahl. (Axiom vom Prozess der Zählens.)

$n+1$ braucht hiernach nicht $\neq n$ zu sein!

II. Es ist $n+1>n$

III. Wenn $b>a$, $c>b$ ist, so ist auch $c>a$.

IV. Wenn $b>a$ ist, so ist $b\neq a$.

Hieraus folgt, daß durch Zählung immer neue Zahlen entstehen.

V. Wenn eine Aussage X_n richtig ist für $n=1$ und für $n+1$ im Falle ihrer Richtigkeit für n, so ist sie für jedes n richtig. (Induktionsaxiom).

Wir zeigen in Kürze die Unabhängigkeit der Axiome. II ist von den anderen unabhängig. Dazu nehme ich folgendes System

$$1,\ 1+1=1;$$

das System besteht also nur aus dem Ding 1. Die Unabhängigkeit von III folgt aus dem System

$$1,\ 1+1=2,\ 2+1=1, \text{ wo } 1>2,\ 2>1 \text{ sei.}$$

Daß IV nicht aus den anderen Axiomen beweisbar

ist, zeigt das System

$$1,\ 1+1=1 \text{ mit der Festsetzung } 1>1$$

Nun kommt die Unabhängigkeit von V. Dazu nehmen wir das System

$$\begin{cases} 1, 2, 3, 4 \dots\dots \\ 1', 2', 3', 4' \dots\dots \end{cases}$$

und es sei

$$1+1=2,\ 2+1=3, \text{ u. s. w.}$$

$$1'+1=2',\ 2'+1=3', \text{ u. s. w.}$$

Jede gestrichene Zahl sei größer als jede ungestrichene; sonst mögen die gewöhnlichen Regeln gelten. Dann sind I/IV erfüllt, aber nicht V. Denn es seien die Aussagen

$$X_1, X_2, X_3, \dots\dots$$

richtig; es sei etwa

$$X_n:\ 1=1$$

$X_{1'}, X_{2'}, X_{3'}, \ldots$ seien aber falsche Aussagen, etwa

$X_{u'}: 1 \neq 1$.

Dann ist V nicht erfüllt; denn X_1 ist richtig, und wenn X_n richtig ist, so ist es auch X_{n+1}. Nach V müßten also alle Aussagen X_u richtig sein; $X_{u'}$ ist aber falsch. Das Induktionsaxiom verhindert also, daß sich hinter einer Zahlenreihe eine andere anreiht.

Nun kommt es darauf an, zu zeigen, wie man aus diesen Axiomen alle Sätze über ganze Zahlen beweist. Es werden im Ganzen 12 Sätze sein, aus denen die anderen leicht folgenden.

Satz 1.) Ist $a \neq 1$, so gibt es eine Zahl b, sodaß $a = b+1$ ist.

Bew.: Für $a = 1$ ist der Satz richtig, denn dann ist

keine Behauptung da. Ist er für a richtig, so ist er für $a+1$ richtig; das ist auch ohne die Voraussetzung wahr, denn es ist

$$a+1 = (a)+1;$$

also ist der Satz für alle a nach V. richtig.

Definition: Es ist $a<b$, wenn $a \neq b$ und nicht $a>b$.

Satz 2) Wenn $b>a$, so ist $a<b$.

Bew.: α.) $a \neq b$, denn $b>a$ (IV.)

β.) Es ist nicht $a>b$; denn sonst wäre nach III $a>a$ im Widerspruch zu IV.

~~Satz 3)~~

Definition: $a+(b+1)$ ist gleich $(a+b)+1$ (Definition der Addition) Ist $b=1$, so ist $a+b=a+1$. Nach V. ist die Summe $a+b$ definiert, wenn $a+(b+1)$ definiert ist unter der Voraussetzung, daß ich $a+b$ kenne; daß gewährleistet durch unsere Definition

Satz 3.) $(a+b)+c = a+(b+c)$

Bew. Für $c=1$ ist der Satz nach Definition der Addition richtig. Er sei richtig für c; dann ist er auch für $c+1$ richtig, denn

$$(a+b)+(c+1) = ((a+b)+c)+1 = (a+(b+c))+1 = a+((b+c)+1)$$
$$= a+(b+(c+1))\text{, q. e. d.}$$

Also ist nach V. der Satz richtig.

Satz 4.) $a+b=b+a$

Bew. Der Satz ist richtig für $b+1$; denn

$$a+1=1+a$$

ist richtig für $a=1$; ist es für a richtig, so ist

$$(a+1)+1=(1+a)+1= 1+(a+1),$$

also ist allgemein $a+1=1+a$. Ferner folgt aus
$a+b=b+a$

$$a+(b+1) = (a+b)+1 = (b+a)+1 = b+(a+1)$$
$$= b+(1+a) = (b+1)+a.$$

Also ist der Satz nach V. richtig.

Satz 5.) Ist $a<b$, so ist $b=a+c$

Bew.: Der Satz ist richtig für $a=1$ nach Satz 1.) u. 4)

Ist er für a richtig, so ist er es auch für $a+1$; denn ist $a+1<b$, so ist $a<b$; ~~also $b=a+c$~~ denn wäre nicht $a<b$, so wäre

$$\left.\begin{array}{ll} \text{entweder } a=b, & \text{also } a+1>b \text{ (II)} \\ \text{oder } a>b, & \text{also } a+1>b \text{ (VIII)} \end{array}\right\} \text{Widerspruch gegen } a+1<b$$

Folglich ist

$$b=a+c;$$

c ist >1; denn sonst wäre

$$a+1<b=a+1.$$

Also (Satz. 1, 2. 5.)

$$b=(a+1)+c', \text{ q.e.d.}$$

Satz 6.) Wenn $b>a$ ist, so ist $b=a+c$.

Bew.: Aus 2.) folgt $a<b$, also nach 5.) $b=a+c$.

Satz 7.) Ist $b=a+c$, so ist $b>a$.

Bew.: Der Satz ist richtig für $c = 1$ nach (II)
Ist er für c richtig, so ist er auch für $c+1$ richtig; denn

$$b = a+(c+1) = a+(c+1) > a+c > a$$

Zusatz: Es gibt keine der 1 vorangehende Zahl; denn nach 1.) ist für jede Zahl $\neq 1$:

$$b = a+1 = 1+a,$$

also $\qquad b > 1$

Satz 8.) Ist $b < a$, so ist $a > b$

Bew.: Nach 5.) ist

$$a = b+c,$$

nach 1.) $a > b$, q.e.d.

Satz 9.) α.) Wenn $a > b$ ist, so ist $a+c > b+c$

β.) " $a < b$ " , " " $a+c < b+c$

Bew.: α.) Nach 6.) ist

$$a = b+d$$

$$a+c = b+d+c = (b+c)+d$$

also nach 7.)

$$a+c > b+c, \text{ q.e.d.}$$

β.) Nach 8.) ist

$$b > a+c$$

nach α.)

$$b+c > a+c$$

nach 7.)

$$a+c < b+c, \text{ q.e.d.}$$

Satz 10.) Ist $a+c = b+c$, so ist $a = b$.

Bew.: Wäre $a \neq b$, so wäre $a \gtrless b$.

α.) Ist $a > b$, so ist

$$a+c > b+c \text{ gegen die Vor.}$$

β.) Ist $a < b$, so ist

$$a+c < b+c \quad \text{"} \quad \text{"} \quad \text{"}$$

Satz 11.) Ist $a \neq 1$, so ist $a > 1$.

Bew.: $a = b+1$ (Satz 1.)), also nach 1.)

$$a > 1$$

d.h. es gibt eine kleinste Zahl; diese ist 1. Daß es keine letzte Zahl gibt, folgt aus Axiom I, daß es keine größte gibt, aus Axiom II.

Satz 12.) Ist $a > b$ und $a \neq b+1$, so ist

$$a > b+1$$

oder: Zwischen zwei aufeinanderfolgenden Zahlen gibt es keine Zahl.

Bew.: Nach 6.) ist

$$a = b+c$$

und $c \neq 1$ n. V., also nach 11.) $c > 1$

$$c = 1+c',$$

also

$$a = (b+1)+c' > b+1, \text{ q. e. d.}$$

Der Beweis von weiteren Sätzen sowie die Einführung der Multiplikation bieten keine Schwierigkeiten mehr; letztere geschieht durch folgende

Gleichungen:

$$a \cdot 1 = a$$

$$a(b+1) = a \cdot b + a$$

Wir hätten auch ein anderes Axiomensystem an die Spitze stellen können, etwa:

$\underline{I}_a$.) wie $\underline{I}$

$\underline{II}_a$.) Aus $a+1=b+1$ folgt $a=b$, oder: jeder Zahl geht nur eine einzige voran.

$\underline{III}_a$.) $a+1 \neq 1$; 1 ist ~~die~~ eine erste Zahl, der 1 geht gar keine Zahl voran.

$\underline{IV}_a$.) wie $\underline{V}$.

Diese vier Axiome sind wieder alle nötig und von einander unabhängig; denn

ad. $\underline{II}_a$.) $1+1=2$, $2+1=2$

$\underline{I}_a, \underline{III}_a, \underline{IV}_a$ sind erfüllt.

ad. $\underline{III}_a$.) $1+1=1$; $\underline{I}_a, \underline{II}_a, \underline{IV}_a$ sind erfüllt

ad. $\underline{IV}_a$.) wie früher bei $\underline{V}$.

Auch unsere Sätze lassen sich wieder beweisen, z.B. 1), 3) 4) wie früher. Satz 10.) wird folgendermaßen bewiesen: für $c = 1$ ist er nach $\underline{II}_a$ richtig; ist er für c richtig, so folgt aus

$$a + (c+1) = b + (c+1)$$

nach $\underline{II}_a$ $\quad a + c = b + c$

also $\quad a = b$, q.e.d.

Definition: Ist $a = b + c$, so heißt $a > b$.

Wir beweisen $\underline{II}$, $\underline{III}$, $\underline{IV}$; daraus folgt dann alles übrige.

ad $\underline{II}$.: $b + c > b$, also $b + 1 > b$

ad. $\underline{III}$.: Wird $b = a + d$, $c = b + e$, also $c = a + (d + e)$, d.h. $c > a$

ad. $\underline{IV}$.: Es ist $b > a$, d.h. $b = a + c$. Wäre nun $b = a$, so wäre $a = a + c$. Dies ist für $a = 1$ nicht richtig ($\underline{III}_a$.)

also $\quad a \neq 1$, d.h. nach Satz 1.) $a = 1+d$, also

$$1+d = (1+c)+d \quad \text{(S. 3.))}$$

also (S. 10.)) $\quad 1 = 1+c$

das ist ein Widerspruch gegen IIIa.

Es würde jetzt sehr am Platz sein, die wichtigsten Begriffe der Mengentheorie Ihnen vorzuführen; dazu würde aber die Zeit nicht reichen. Dagegen will ich noch einen anderen Punkt behandeln, der einen sehr geeigneten Abschluß dieser Vorlesung bildet; das ~~ist~~ sind die Gesetze der Logik. Ich will Ihnen noch die Grundgesetze des Logikcalculs vorführen. Auch hier suchen wir die axiomatische Methode zur Geltung zu bringen.

Wir haben ein System von Dingen; das sind jetzt die Urteile $X, Y, Z, U \ldots$. Wir haben also jetzt die Fähigkeit, Urteile zu bilden. Die Urteile werden in zwei Kategorien

geteilt, in richtige und falsche Urteile. Diese Einteilung nun ist nicht willkürlich, sondern erfolgt nach bestimmten Gesetzen, den Axiomen.

Definitionen: $\bar{X}$ heißt „nicht X", die Negation. „X und Y gehören zur selben Klasse" wird angedeutet durch $X = Y$; analog $X \neq Y$ heißt: X und Y gehören zu verschiedenen Klassen. „und" wird durch +, „oder" durch • angedeutet. Wenn eine Aussage X ~~richtig ist~~, so schreiben wir dafür $X=0$, d.h. X gehört in die Klasse, der die Aussage angehört, welche nichts aussagt. Daß die Aussage X falsch ist, deuten wir an durch $X=1$. Wir können schreiben $\bar{1}=0$, $\bar{0}=1$; man könnte daher das Zeichen 1 vermeiden.

Nun stellen wir die Axiome der Logik auf.

I. Ist $X=Y$, so kann X durch Y ersetzt werden (Definition des Zeichens $=$).

II. Aus zwei Aussagen X, Y entsteht eine neue $X+Y$ (Definition des Zeichens $+$)

III. Aus zwei Aussagen X, Y entsteht noch auf eine andere Weise eine neue $X \cdot Y$ (Definition des Zeichens $\cdot$)

IV. $X+Y=Y+X$

V. $(X+Y)+Z=X+(Y+Z)$

VI. $X \cdot Y = Y \cdot X$

VII. $(X \cdot Y) \cdot Z = X \cdot (Y \cdot Z)$

VIII. $X \cdot (Y+Z) = X \cdot Y + X \cdot Z$ (Wegen IV u. VI gilt auch das andere distributive Gesetz)

IX. $X+\overline{X}=1$ (Definition des Widerspruchs)

X. $X \cdot \overline{X} = 0$

XI. $1+1=1$

XII. $1 \cdot X = X$

Nun müssen wir aus diesen Axiomen eine Reihe weiterer Sätze ableiten.

1) Beh.: $X+X=X$ oder: wenn der Kandidat die falsche Antwort wiederholt, so bleibt sie doch falsch.

Bew.: $X+X = 1\cdot X + 1\cdot X = (1+1)X = 1\cdot X = X$

2.) Beh.: $1+X=1$

Bew.: $1+X = X+\overline{X}+X = X+X+\overline{X} = X+\overline{X} = 1$

3.) Beh.: $X+0=X$

Bew.: $X+0 = X+X\cdot\overline{X} = X(1+\overline{X}) = X\cdot 1 = X$

4.) Beh.: $X\cdot X=X$

Bew.: $X\cdot X = X(X+0) = X\cdot X+X\cdot\overline{X} = X(X+\overline{X}) = X\cdot 1 = X$

5.) Beh.: $X\cdot 0=0$

Bew.: $X\cdot 0 = X\cdot X\cdot\overline{X} = X\cdot\overline{X} = 0$

Nun kann man sich auch mit Unabhängigkeitsbeweisen beschäftigen. Man kann z. B. die letzten

0 und 1 sind die gewöhnlichen Zahlen 0 u. 1.

aufgestellten ~~Sätze~~ Axiome XI u. XII nicht aus I/X beweisen. Ich will den Beweis andeuten. Man verstehe unter X.. die reellen Zahlen und unter = die gewöhnliche Gleichheit. $\bar{X}$ sei $1-X$, $X+Y$ die gewöhnliche Summe, $X\cdot Y$ stets 0. Dann sind alle Axiome I/X erfüllt; dagegen sind XI und XII nicht erfüllt.

Nun will ich Ihnen noch zeigen, wie man die gewöhnlichen Gesetze des logischen Schließens aus unseren zwölf Axiomen ableiten kann. Wir beweisen zunächst noch drei Sätze.

6.) Die Aussage $\bar{X}$, das Gegenteil, ist durch die Axiome IX u. X eindeutig festgelegt.

Beweis: Es sei
$$X+Y=1$$
$$X\cdot Y=0$$

Dann ist
$$Y=Y+0=Y\cdot 1+X\cdot\bar{X}=Y\cdot(X+\bar{X})+X\cdot\bar{X}$$

$$\cancel{y + z + \bar{y}\cdot\bar{z} = (y+z)(1+\bar{y}\cdot z) + \overline{\bar{y}\cdot\bar{z}} =}$$

$$= \overline{X}(Y+X)+X\cdot Y = \overline{X}\cdot 1 + X\cdot Y = \overline{X}+0 = \overline{X}, \text{ q.e.d.}$$

7.) Wenn $Y=\overline{X}$ ist, so ist $\overline{Y}=X$.

Bew.: Es ist

$$X+\overline{X}=1, \quad X\cdot\overline{X}=0$$

also

$$X+Y=1, \quad X\cdot Y=0,$$

also nach 6.) $\overline{Y}=X$

8.) Es ist

$$\overline{Y+Z} = \overline{Y}\cdot\overline{Z}$$

$$\overline{Y\cdot Z} = \overline{Y}+\overline{Z}$$

Bew.: Es ist zu zeigen

$$Y+Z+\overline{Y}\cdot\overline{Z}=1$$

$$(Y+Z)\overline{Y}\cdot\overline{Z}=0$$

Die zweite Gl. ist klar, denn

$$(Y+Z)\overline{Y}\cdot\overline{Z} = Y\cdot\overline{Y}\cdot\overline{Z}+\overline{Y}\cdot Z\cdot\overline{Z}=0$$

Ferner ist

$$Y+Z+\overline{Y}\cdot\overline{Z} = Y1+Z\cdot 1+\overline{Y}\cdot\overline{Z}+\overline{Y}\cdot\overline{Z} = Y(1+\overline{Z})+Z(1+\overline{Y})+\overline{Y}\cdot\overline{Z} = Y+(Y+\overline{Y})\overline{Z}+Z+(Z+\overline{Z})\overline{Y} = 1+1=1$$

Ähnlich beweist man die zweite Behauptung.

Nun kommen wir zu den Gesetzen der Logik.

$$\overline{X}\cdot Y = 0$$

heißt: aus X folgt Y.

Ist $X+Y$ richtig, so ist auch X richtig; denn

$$\overline{X+Y}\cdot X = \overline{X}\cdot\overline{Y}\cdot X = 0$$

Ist X richtig, und folgt Y aus X, so ist auch Y richtig; denn

$$\overline{X}\cdot Y = 0$$

$$X = 0$$

$$X\cdot Y = 0$$

$$(X+\overline{X})Y = Y = 0$$

Wenn Y aus X, Z aus Y folgt, so folgt auch Z aus X; denn

$$\overline{X}\cdot Y = 0,\quad \overline{Y}\cdot Z = 0$$

also

$$\cancel{\overline{X}(Y\overline{Y})Z = \overline{X}Z = 0}$$

$\bar{X} y Z + \bar{X} \bar{y} Z = \bar{X} \cdot Z = 0$

Jede Aussage haben wir als eine Gleichung dargestellt; es fragt sich nun, ob sich jede Aussage auf eine einfachste Form, eine „Normalform" bringen läßt. Das geht in der Tat, und zwar auf zwei Arten.

Einmal löst man alle Klammern auf und läßt alle Glieder, welche Faktoren der Form $X \cdot \bar{X}$ haben, fort. Dann ordnet man nach homogenen Gliedern, indem man stets $X + \bar{X}$ durch 1 ersetzt. So erhält man eine Additiv-normalform. Z. B. ist

$X + X \cdot Z = X(1+Z) = X$, also ist

X die Normalform von $X + X \cdot Z$. Eine andere

Normalform ist

$$X+\bar{Y}Z+X\bar{Y}U+\bar{X}\bar{Y}UV=0$$

Nun gibt es aber noch eine Normalform: bei der ersten haben wir das Zeichen + bevorzugt; jetzt wollen wir das Zeichen · bevorzugen, z. B.

$$\bar{X}\cdot\overline{\bar{Y}Z}\cdot\overline{X\bar{Y}U}\cdot\overline{\bar{X}\bar{Y}UV}=1$$

das Gegenteil der obigen Aussage; dies ist

$$=\bar{X}(Y+\bar{Z})(\bar{X}+Y+\bar{U})(X+Y+\bar{U}+\bar{V})=1$$

und das wäre die gewünschte Normalform. Ich will aber diese Aussage $=0$ gesetzt haben; dazu löse ich die Klammern auf und bringe den Ausdruck auf die erste Normalform:

$$Y\cdot\bar{X}+\bar{Z}\cdot\bar{X}=1$$

also wird die gesuchte Multiplikativnormalform:

$$(\bar{Y}+X)(X+Z)=0$$

Bei der ersten Normalform kann man sofort Teilurteile herauslesen; daher wird sie in der Regel bevorzugt; allerdings hat das nur einen Sinn, wenn etwas positives gesagt wird. Bei einer Kritik wäre die zweite Normalform zu bevorzugen.

Auch die allgemeine Art des Schließens läßt sich mit Hilfe des Logikkalkuls darstellen. Aus X folgt Y, hieß

$$\bar{X} \cdot Y = 0$$

Ferner war Y mit X richtig, wie wir sahen. Denn es war

$$Y = Y(X+\bar{X}) = YX + Y\bar{X} = 0$$

Dies will ich noch etwas generalisieren. Es ist

$$\bar{X} \cdot Y + X = 0,$$

indem wir beide Voraussetzungen zusammen-

mennehmen. Es muss also eine Kombination A geben, sodass

$$A(\bar{X}Y+X)=Y$$

ist. Mathematisch schliessen heisst also nichts anderes, als einen geeigneten Faktor zu finden, der mit der Voraussetzung multipliziert die Behauptung ergibt. Näheres darüber mögen Sie in Schröders Handbuch des Logikkalkuls nachlesen.