LVI.

Anzeige von P. Bachmann, Die Lehre von der Kreisteilung und ihre Beziehungen zur Zahlentheorie.

[Literaturzeitung der Zeitschrift für Mathematik und Physik, Bd. 18, S. 14—24, 1873.]

Der Aufforderung des Herrn Hofrat Schlömilch, das vorliegende Werk in der „Zeitschrift für Mathematik und Physik“ näher zu besprechen, komme ich um so lieber nach, als ich das Erscheinen desselben mit aufrichtiger Freude begrüßt habe. Denn ein großes und höchst interessantes Gebiet wird hier zum ersten Male in zweckmäßiger Abgrenzung und lichtvoller Darstellung dem lernenden mathematischen Publikum leicht zugänglich gemacht, und zwar unter Voraussetzung von nur sehr mäßigen Vorkenntnissen aus der Algebra und Zahlentheorie.

Die Lehre von der Kreisteilung, d. h. die Theorie der Gleichungen von der Form $x^m = 1$, wo m eine gegebene positive ganze Zahl bedeutet, ist, obwohl eine Menge interessanter Eigenschaften der Einheitswurzeln x schon früher bekannt waren, doch erst durch Gauß auf ihre eigentlichen Prinzipien zurückgeführt und dadurch der Ausgangspunkt für eine ganz neue Wissenschaft von unermeßlicher Ausdehnung geworden. Die siebente Sektion der 1801 erschienenen „Disquisitiones Arithmeticae“, welche den Titel „De aequationibus circuli sectiones definientibus“ führt, enthält eine rein algebraische Methode, die obige Gleichung, deren Auflösung mittels der trigonometrischen Funktionen längst bekannt war, auf andere Gleichungen von niedrigerem und zwar von möglichst niedrigem Grade zu reduzieren. Hierbei tritt zum ersten Male der Begriff der Irreduktibilität auf (Art. 341), welcher entscheidend für die ganze Richtung der späteren Algebra geworden ist; obgleich Gauß nur einen geringen Gebrauch von demselben macht (Art. 346), so zweifle ich doch nicht daran, daß dieses Grundprinzip ihn auch

bei der Entdeckung des Einzelnen geleitet und daß er nur der Kürze halber die synthetische Darstellung vorgezogen hat; namentlich lassen hierauf die gewichtigen Worte schließen (Art. 365): „omnique rigore demonstrare possumus, has aequationes elevatas nullo modo nec evitari nec ad inferiores reduci posse, etsi limites hujus operis hanc demonstrationem hic tradere non patiantur, quod tamen monendum esse duximus, ne quis adhuc alias sectiones praeter eas quas theoria nostra suggerit, e.g. in 7, 11, 13, 19 etc. partes, ad constructiones geometricas perducere speret, tempusque inutiliter terat". Die Wahrheit der in denselben enthaltenen Behauptung ist nach dem gegenwärtigen Stande der Algebra, namentlich seit der Fortbildung und Verallgemeinerung der Gaußschen Gedanken durch Abel und Galois leicht zu beweisen. In der Tat ist aus dem von Gauß gelegten Keime eine Wissenschaft entstanden, welche man, um in einem Nichtkenner wenigstens eine dunkle Vorstellung von ihrem Charakter zu erwecken, vielleicht als die Wissenschaft von der algebraischen Verwandtschaft der Zahlen oder, wenn man sich eines von mir gewählten Ausdruckes bedienen will, als die Wissenschaft von der Verwandtschaft der Körper bezeichnen könnte. Es zeigt sich nämlich, daß die eigentümliche Beschaffenheit einer Gleichung, die Möglichkeit, ihre Auflösung auf die von anderen Gleichungen zurückzuführen, erst dann deutlich erkannt werden kann, wenn man außer ihren Wurzeln noch unendlich viele andere Zahlen betrachtet, welche aus einer oder mehreren von ihnen rational ableitbar sind und deren Inbegriff eben das bildet, was ich einen Körper nenne, nämlich ein System von Zahlen, die sich durch die vier einfachsten, rationalen arithmetischen Operationen immer wieder reproduzieren. Eigenschaften einer Gleichung werden bei dieser Auffassung zu Eigenschaften des entsprechenden Körpers, Beziehungen zwischen Gleichungen stellen sich dar als Verwandtschaft zwischen den Körpern; namentlich entsteht bei gegenseitiger Durchdringung zweier Körper A, B immer wieder ein Körper, ihr kleinstes gemeinschaftliches Multiplum oder kürzer ihr Produkt AB, dessen Natur wesentlich von der Verwandtschaft der beiden Körper abhängt.

Neben dieser Entwicklung der eigentlichen Algebra, welche der Theorie der Kreisteilung den ersten Impuls verdankt, und Hand in Hand mit ihr hat die Zahlentheorie einen großartigen Aufschwung

genommen. Die algebraischen Untersuchungen von Gauß im Gebiete der Kreisteilung bedurften schon einiger, wenn auch sehr elementarer Hilfssätze aus der Zahlentheorie; bald aber zeigte es sich, daß umgekehrt die Kreisteilung zu einer unerschöpflichen Quelle wurde, aus welcher immer neuer und bedeutender Gewinn für die Zahlentheorie ausströmte. Man kann sagen, daß fast alle späteren Fortschritte, welche die Zahlentheorie unter den Händen von Gauß, Jacobi, Dirichlet, Eisenstein, Kummer, Kronecker gemacht hat, entweder der Kreisteilung geradezu ihre Entstehung verdanken oder, was in einigen Fällen noch merkwürdiger war, in einen vorher ungeahnten Zusammenhang mit der Kreisteilung traten. Zu diesen letzteren Fortschritten gehören die Untersuchungen von Gauß und Dirichlet über die Klassenanzahl der quadratischen Formen, zu den ersteren die Erweiterung des Begriffes der ganzen Zahl durch Gauß, deren Verallgemeinerung später zu der Schöpfung der idealen Zahlen durch Kummer geführt hat.

Es ist nun zu verwundern, daß trotz der soeben kurz geschilderten Rolle, welche die Kreisteilung in der Geschichte der neueren Mathematik spielt, und trotz der großen Berühmtheit, deren sie sich vor anderen, mindestens ebenso tiefsinnigen Schöpfungen von Gauß zu erfreuen hat — man denke nur an das Siebenzehneck —, es ist zu verwundern, daß trotzdem kein Lehrbuch erschienen ist, in welchem die Kreisteilung mit voller Berücksichtigung des teils von Gauß, teils von seinen Nachfolgern durchforschten Details als ein abgerundetes Ganzes dargestellt ist. Es ist daher ein höchst dankenswertes Unternehmen des Verfassers, durch das vorliegende Werk diese empfindliche Lücke in unserer mathematischen Literatur auszufüllen, und ich freue mich, hinzufügen zu können, wofür allerdings schon sein Name hinreichende Bürgschaft leistet, daß er dieses Unternehmen in vortrefflicher Weise ausgeführt hat. Für jeden, der ein tieferes Studium der Algebra und ihrer Beziehungen zur Zahlentheorie beabsichtigt, wird dieses Werk den besten Führer abgeben, weil es ihn ohne Voraussetzung großer Vorkenntnisse in die Mitte eines überaus reichen und bisher nicht leicht zugänglichen Stoffes einführt, in welchem man durchaus orientiert sein muß, wenn man zu höheren Untersuchungen fortschreiten will.

Ich erlaube mir nun, im folgenden eine Reihe von Bemerkungen mitzuteilen, zu welchen mich einzelne Stellen oder auch ganze Ab-

schnitte des Werkes veranlaßt haben. Wenn ich dabei einzelne Punkte hervorhebe, bei welchen ich eine andere Anordnung oder Darstellung als die vom Verfasser befolgte erwähne oder empfehle, so geschieht dies keineswegs, um Tadel auszusprechen; jeder, der sich gründlich mit einem bestimmten Gegenstande beschäftigt hat — und seit 18 Jahren habe ich mich diesem Teile der Mathematik mit besonderer Vorliebe zugewandt —, bildet sich gewisse, ihm eigentümliche Gesichtspunkte aus, die er für besonders wertvoll hält, während sie einem andern weniger wichtig erscheinen, und ich gebe zu, daß hierbei vieles reine Geschmackssache ist. Aber ich benutze doch gern diese Gelegenheit, aus meiner langjährigen Beschäftigung mit diesem Gegenstande einige Mitteilungen über meine Ansichten und auch einige Abschweifungen auf verwandte Gegenstände zu machen, in der Hoffnung, daß sie einigen Lesern willkommen sein werden. Ich lasse sie hier ohne innere Verbindung so folgen, wie sie beim Durchlesen des Werkes entstanden sind, indem ich nur auf die betreffende Stelle verweise.

Vorlesung 3, Nr. 2 und 3, Seite 13. Der Nachweis der Existenz primitiver Einheitswurzeln würde, wie ich glaube, durch eine kleine Umstellung an Klarheit und Präzision gewinnen. Da nämlich $\psi(d)$ definiert wird als die Anzahl der n^{ten} Einheitswurzeln, welche zum Exponenten d gehören, so erscheint, ehe nicht das Gegenteil bewiesen ist, $\psi(d)$ als abhängig nicht bloß von d, sondern möglicherweise auch von n, und die Anwendbarkeit des in der vorhergehenden Vorlesung bewiesenen Summensatzes zur Bestimmung von $\psi(d)$ bleibt Zweifeln unterworfen, welche erst nachträglich durch die Bemerkungen in Nr. 3 gehoben werden. Am einfachsten gestaltet sich wohl die Untersuchung, wenn der Begriff der primitiven Einheitswurzeln vorangestellt und $\psi(n)$ als die Anzahl der primitiven n^{ten} Einheitswurzeln definiert wird.

Vorlesung 4, Seite 20. In dieser Vorlesung werden die ersten Begriffe aus der sogenannten Theorie der höheren Kongruenzen mitgeteilt. Eine etwas weiter gehende Darstellung, welche auch die wichtigsten Sätze über Primfunktionen enthielte, würde bei manchen späteren Gelegenheiten sich als sehr nützlich erweisen, namentlich für die 5., 17. und 18. Vorlesung; aber sie würde freilich auch viel mehr Raum erfordern. Der Beweis des Satzes von Schönemann (S. 26) läßt sich unter Voraussetzung des Fermatschen Satzes durch

die Theorie der Transformation der symmetrischen Funktionen abkürzen, welche vom Verfasser doch an manchen Stellen (z. B. in Vorlesung 5, Nr. 4) als bekannt vorausgesetzt wird.

Vorlesung 5, Nr. 6 und 7. Die Mitteilung eines speziellen Falles des allgemeinen Irreduktibilitätssatzes von Kronecker veranlaßt mich, den eigentlichen Nerv seines Beweises (sowie auch desjenigen von Arndt) hier hervorzuheben; dies kann mit verhältnismäßiger Kürze geschehen, wenn man einige allgemeine Begriffe über ganze algebraische Zahlen und einige Sätze aus der Theorie der Ideale als bekannt voraussetzt, welche ich teils in der zweiten Auflage von Dirichlets Vorlesungen über Zahlentheorie bewiesen, teils in den Göttinger „Gelehrten Anzeigen“ (20. September 1871) ohne Beweis mitgeteilt habe. Bedeutet μ eine primitive m^{te} Einheitswurzel, so kommt alles auf den zahlentheoretischen Gehalt der Zahl $(1-\mu)$ an. Ist $m = 1$, so ist $1 - \mu = 0$; ist aber m durch eine einzige Primzahl p teilbar, also eine Potenz derselben, so ist, wie unmittelbar einleuchtet:

$$p = \varepsilon (1-\mu)^{\varphi(m)},$$

wo ε eine Einheit und $\varphi(m)$ die bekannte Funktion der Zahlentheorie bedeutet; ist endlich m durch zwei oder mehrere verschiedene Primzahlen $p, q \ldots$ teilbar, so muß die Zahl $(1-\mu)$, weil sie in allen Zahlen von der Form $(1-\mu^n)$ aufgeht, wo n jede ganze positive Zahl bedeutet, zufolge des vorhergehenden Falles auch in p, in $q \ldots$ aufgehen und folglich eine Einheit sein, was auch unmittelbar aus der Gleichung geschlossen werden kann, welche alle primitiven m^{ten} Einheitswurzeln zu Wurzeln hat. Nun sei a eine Potenz einer Primzahl p, und $m = ab$, wo b durch p nicht teilbar ist; man erhält dann bekanntlich alle primitiven m^{ten} Einheitswurzeln und jede nur einmal, wenn man jede primitive Wurzel der Gleichung $x^a = 1$ mit jeder primitiven Wurzel der Gleichung $x^b = 1$ multipliziert. Ist nun α eine bestimmte der ersteren, β eine bestimmte der letzteren, so lautet der noch etwas verschärfte Satz von Kronecker folgendermaßen:

„Ist die Grundzahl oder Diskriminante $\Delta(\Omega)$ eines Körpers Ω nicht teilbar durch die Primzahl p, so hat die in Ω irreduktible Gleichung $f(x) = 0$, welcher $x = \alpha\beta$ genügt, auch alle $\varphi(a)$ Produkte $\alpha'\beta$ zu Wurzeln, welche den sämtlichen $\varphi(a)$ primitiven Wurzeln α' der Gleichung $x^a = 1$ entsprechen.“

Der Beweis beruht auf folgenden Momenten. Alle Wurzeln μ der Gleichung $f(x) = \Pi(x - \mu) = 0$ sind jedenfalls von der Form $\mu = \alpha'\beta'$, wo α', β' primitive Einheitswurzeln bzw. vom Grade a, b bedeuten. So oft nun β' mit β identisch ist, wird $(\beta - \mu) = \beta(1 - \alpha')$, also materiell, d. h. abgesehen von einem Einheitsfaktor, $= (1 - \alpha)$; ist dagegen β' von β verschieden, so wird $(\beta - \mu) = \beta(1 - \alpha'\beta'')$, wo β'' eine von 1 verschiedene Wurzel der Gleichung $x^b = 1$ bedeutet, also ist zufolge der vorausgeschickten Bemerkungen $(\beta - \mu)$ eine Einheit. Mithin ist

$$f(\beta) = \Pi(\beta - \mu) = \varepsilon'(1 - \alpha)^n,$$

wo ε' eine Einheit, und n die Anzahl der Wurzeln $\mu = \alpha'\beta'$ bedeutet, in welchen $\beta' = \beta$ ist; es wird daher $f(\beta)$ stets und nur dann durch

$$p = \varepsilon(1 - \alpha)^{\varphi(a)}$$

teilbar sein, wenn $n = \varphi(a)$ ist, d. h. wenn wirklich alle $\varphi(a)$ Produkte $\alpha'\beta$ Wurzeln derselben in Ω irreduktiblen Gleichung $f(x) = 0$ sind. Diese Teilbarkeit der Zahl $f(\beta)$ durch p läßt sich aber aus der Voraussetzung, daß die Grundzahl $\Delta(\Omega)$ des Körpers Ω nicht durch p teilbar ist, folgendermaßen beweisen. Zunächst ist diese Voraussetzung identisch mit derjenigen, daß p durch kein Quadrat eines Primideals des Körpers Ω teilbar ist, und diese ist wiederum äquivalent mit der Annahme, daß unendlich viele solche Potenzen

$$s = p^f,\ p^{2f},\ p^{3f} \ldots$$

der Primzahl p existieren, für welche jede ganze Zahl ω des Körpers Ω der Kongruenz

$$\omega^s \equiv \omega \pmod{p}$$

genügt. Da nun die Koeffizienten der Funktion $f(x)$ solche ganze Zahlen ω sind, so folgt

$$f(\beta)^s \equiv f(\beta^s) \pmod{p};$$

wählt man ferner, was immer möglich ist, die Potenz s der Primzahl p so, daß $s \equiv 1 \pmod{b}$, also $\beta^s = \beta$, und zugleich $s \geqq \varphi(a)$ wird, und bedenkt, daß $f(\beta)$ den Faktor $(1 - \alpha)$ wenigstens einmal enthält, also $f(\beta)^s$ durch p teilbar ist, so ergibt sich, daß auch $f(\beta) \equiv 0 \pmod{p}$ ist, wie zu beweisen war.

Durch wiederholte Anwendung dieses Resultates ergibt sich offenbar der folgende Satz, welcher nur noch wenig allgemeiner als der von Kronecker ist:

„Ist m relative Primzahl zu der Grundzahl $\Delta(\Omega)$ des Körpers Ω, so ist die Gleichung, deren Wurzeln die sämtlichen primitiven m^{ten} Einheitswurzeln sind, irreduktibel in Ω."

Vorlesung 6, Seite 43. In dieser Vorlesung beginnt die eigentliche Theorie der Kreisteilung, deren Wesen in der Zurückführung der Gleichung

$$X = \frac{x^p - 1}{x - 1} = 0,$$

wo p eine Primzahl bedeutet, auf Gleichungen niedrigeren Grades besteht. Ich erlaube mir hier einige allgemeine Bemerkungen über die Verteilung des Stoffes und über die Methode der Untersuchung zu machen.

Die Darstellung von Gauß zerfällt in zwei wesentlich verschiedene Teile, deren erster (Art. 342—358) die sukzessive Zerlegung des Systems aller $(p-1)$ Wurzeln r^k der obigen Gleichung in sogenannte Perioden und die Aufstellung der ihnen entsprechenden Gleichungen enthält, während der zweite Teil die Zurückführung derselben auf reine Gleichungen, d. h. ihre Auflösung durch Wurzelzeichen behandelt. Diese scharfe Sonderung halte ich für äußerst zweckmäßig. Der erste Teil hat es nur mit den durch r rational darstellbaren Zahlen zu tun, welche einen Körper R vom Grade $(p-1)$ bilden, und er ist, wenn dies auch in der Darstellung von Gauß nicht hervortritt, wesentlich unabhängig von der Existenz primitiver Kongruenzwurzeln. Der zweite Teil dagegen bedarf der Betrachtung der letzteren und außerdem der Einführung eines Hilfskörpers S vom Grade $\varphi(p-1)$, welcher aus den Wurzeln der Gleichung $x^{p-1} = 1$ gebildet ist; der eigentliche Gegenstand der Untersuchung ist das Produkt RS aus beiden Körpern R und S, welches zugleich der aus den Wurzeln der Gleichung $x^{p(p-1)} = 1$ gebildete Körper vom Grade $(p-1)\varphi(p-1)$ ist. Dieser wesentliche Unterschied zwischen den beiden genannten Teilen würde es mir vorteilhafter erscheinen lassen, wenn der Verfasser den Hauptinhalt der Vorlesungen 9, 15, 16, 17, 18 gleich auf die siebente hätte folgen lassen.

Was ferner die Methode der Entwicklung anbetrifft, so ist nicht zu leugnen, daß in der synthetischen Darstellung von Gauß das Streben nach Kürze den Sieg über die Forderung davongetragen hat, alles aus einem einheitlichen algebraischen Gedanken abzuleiten. Bei meinem ersten gründlichen Studium der Kreisteilung in den Pfingstferien 1855 hatte ich, obgleich ich das Einzelne wohl verstand, doch

lange zu kämpfen, bis ich in der Irreduktibilität das Prinzip erkannte, an welches ich nur einfache, naturgemäße Fragen zu richten brauchte, um zu allen Einzelnheiten mit Notwendigkeit getrieben zu werden. Nachdem diese Gedanken durch eine eingehende Beschäftigung mit den algebraischen Untersuchungen von Abel und namentlich von Galois vervollständigt und durch die im Anfang Dezember desselben Jahres gelungene Auffindung der allgemeinsten Beziehungen zwischen irgend zwei irreduktiblen Gleichungen zu einem gewissen Abschluß gekommen waren, habe ich später in meinen beiden Wintervorlesungen über Kreisteilung und höhere Algebra 1856—1858 die damals gewonnene Methode befolgt, und ich glaube noch heute, daß sie auch für den Lernenden zweckmäßig ist. Statt, wie es der Verfasser mit Gauß tut, unmittelbar von den Perioden auszugehen, stelle man die Frage nach der Anzahl der verschiedenen konjugierten Werte, welche eine in R enthaltene, d. h. durch r rational darstellbare Zahl $\alpha = F(r)$ besitzt, und welche entstehen, wenn r durch alle $(p-1)$ Wurzeln r^k der irreduktiblen Gleichung $X = 0$ ersetzt wird. Bezeichnet man mit h alle diejenigen f inkongruenten Zahlen (mod p), für welche $F(r^h) = F(r)$ ist, so folgt aus der Irreduktibilität sofort, daß diese Zahlen h sich durch Multiplikation reproduzieren, und hieraus weiter, daß sie die sämtlichen Wurzeln der Kongruenz $h^f \equiv 1 \pmod p$ bilden, daß f ein Divisor von $(p-1) = ef$, und daß e die Anzahl der wirklich verschiedenen Werte $F(r^k)$ ist, deren jeder sich f mal wiederholt; die sämtlichen $(p-1)$ Exponenten k zerfallen nämlich in e Komplexe von je f Exponenten hn, denen jedesmal der eine Wert $F(r^n)$ entspricht. Fragt man nach der wirklichen Existenz solcher e-wertigen Zahlen $\alpha = F(r)$, so ergibt sich aus der Bedingung $F(r) = F(r^h)$, daß die rationalen Koeffizienten oder Koordinaten a in der Darstellungsform $\alpha = F(r) = \Sigma a r^k$, auf welche jede in R enthaltene Zahl stets und wegen der Irreduktibilität auch nur auf eine Weise gebracht werden kann, gruppenweise zu je f einander gleich sein müssen, daß nämlich

$$\alpha = a\eta + a_1\eta_1 + \cdots + a_{e-1}\eta_{e-1}$$

sein muß, wo jede der e Größen $\eta, \eta_1, \ldots, \eta_{e-1}$ eine sogenannte Periode, d. h. eine Summe von f Gliedern r^{hn} bedeutet. Soll eine solche Zahl α wirklich e-wertig sein, so brauchen nur fernere gruppenweise Gleichheiten zwischen den e rationalen Zahlen $a, a_1, \ldots, a_{e-1}$

ausgeschlossen zu werden; mithin sind die Perioden selbst solche e-wertige und zwar konjugierte Zahlen. Es ergibt sich dann sofort, daß jede e-wertige Zahl α die Wurzel einer irreduktiblen Gleichung e^{ten} Grades ist und daß jede Zahl $\beta = f(r)$, welche den Bedingungen $f(r) = f(r^h)$ genügt, auch ohne e-wertig zu sein, durch α rational darstellbar ist, daß also alle solche Zahlen β einen Körper R_e vom Grade e bilden, welcher durch e vollständig bestimmt ist. Das allgemeinste Resultat, in welchem der ganze erste Teil der Kreisteilung enthalten und welches auf dieselbe Weise leicht abzuleiten ist, besteht in folgendem. Ist α eine e-wertige, α' eine e'-wertige Zahl, und e'' der größte gemeinschaftliche Teiler von e und $e' = d'e''$, so genügt α' einer in R_e irreduktiblen Gleichung vom Grade d'. Dasselbe kann auch so ausgesprochen werden: Das Produkt der Körper R_e und $R_{e'}$ ist der Körper $R_{e'''}$, wo e''' das kleinste gemeinschaftliche Vielfache von e, e' bedeutet; und $R_{e''}$ ist ihr größter gemeinschaftlicher Divisor. Es bildet nur einen speziellen Fall des oben erwähnten allgemeinen Gesetzes, welches wenigstens teilweise durch die Gleichung

$$(BC, A) = (C, AB)(B, A)$$

ausgedrückt werden kann, wo A, B, C irgend drei Körper sind, und das Symbol (B, A) die Anzahl der in B enthaltenen Zahlen bedeutet, welche in bezug auf A unabhängig sind.

In dem zweiten Teile der Kreisteilung wird die Frage aufgeworfen, ob die im ersten Teile betrachteten irreduktiblen Gleichungen durch Wurzelzeichen lösbar, d. h. auf reine Gleichungen zurückführbar sind. Dieselbe drängt mit Notwendigkeit zur Einführung des Körpers S, und nachdem die Irreduktibilität der Gleichung $X = 0$ in bezug auf S erkannt ist, leuchtet sofort ein, daß die Sätze des ersten Teiles auf das neue Gebiet unmittelbar übertragen werden können. Fragt man nun nach solchen Zahlen, welche reinen Gleichungen genügen, so wird man auf dieselbe Weise zu allen Resolventen und der Benutzung der primitiven Kongruenzwurzeln getrieben, wie im ersten Teile zu den Perioden, und alles Detail ergibt sich mit größter Leichtigkeit.

Der im vorstehenden beschriebene Weg ist vom Verfasser nur teilweise befolgt; aber ich glaube, daß die Klarlegung der algebraischen Prinzipien an dem klassischen und zugleich einfachsten Beispiele der Kreisteilung eine sehr nützliche Vorbereitung für das tiefere Studium der Algebra bildet.

Vorlesung 9, Nr. 4. Die Methode von Kronecker zur Bestimmung des Vorzeichens $\varepsilon = \pm 1$ in der Gleichung

$$\varepsilon \Pi(x^{2h-1} - x^{p-2h+1}) = \sum\left(\frac{k}{p}\right) x^k + (x^p - 1) f(x)$$

läßt sich abkürzen, wenn man durch $(x-1)^{\frac{p-1}{2}}$ dividiert und dann $x = 1$ setzt.

Vorlesung 14. Nachdem die Reziprozitätssätze für kubische und biquadratische Reste in den Theorien der komplexen Zahlen bewiesen sind, ist es von Interesse, zu der Theorie der rationalen Zahlen zurückzukehren. Obgleich dieser Gegenstand seiner Natur nach nicht in das vorliegende Werk gehört, so erlaube ich mir doch, hier aus einer größeren Arbeit über beliebige kubische Körper, an deren Vollendung und Veröffentlichung ich für jetzt durch Amtsgeschäfte gehindert werde, folgendes mitzuteilen. Bedeutet k eine ganze rationale Zahl, deren Kubikwurzel irrational ist, so entspringt aus der Gleichung $x^3 = k$ ein reiner kubischer Körper, dessen Grundzahl die Form $D = -3g^2$ hat, wo g eine aus k leicht abzuleitende ganze Zahl ist. Fragt man nun nach allen in k nicht aufgehenden Primzahlen p von der Form $3n + 1$, von welchen die gegebene Zahl k kubischer Rest ist, so gelangt man mit Hilfe des Reziprozitätssatzes zu folgendem interessanten Resultat, welches im wesentlichen schon Gauß bekannt gewesen ist: die sämtlichen nicht äquivalenten, ursprünglichen positiven quadratischen Formen $ax^2 + bxy + cy^2$, in welchen $b^2 - 4ac = D$, zerfallen in drei Abteilungen von gleich vielen Individuen, deren erste eine Gruppe bildet, durch deren Formen alle und nur solche Primzahlen p dargestellt werden, von welchen k kubischer Rest ist. Mit Hilfe desselben wird die Bestimmung der Anzahl der Idealklassen des kubischen Körpers auf einen bekannten Teil der Theorie der Thetafunktionen zurückgeführt.

Vorlesung 17 und 18. Bei der Begründung der Theorie der idealen Zahlen in der Kreisteilung folgt der Verfasser dem von Kummer eingeschlagenen Wege. Der Versuch, einige Zweifel an der Strenge der ersten, später vervollständigten Darstellung von Kummer zu überwinden, führte mich zuerst im Winter 1855/56 auf die Theorie der höheren Kongruenzen, insbesondere auf die Zerlegung der Funktion $(x^m - 1)$ in Primfunktionen in bezug auf beliebige Primzahlmoduln. Diese Sätze, welche übrigens, wenn ich

nicht irre, zuerst von Schönemann veröffentlicht sind und welche sich auch in dem Nachlasse von Gauß vorgefunden haben, gestatten, wie mir scheint, eine einfachere Begründung von Kummers genialer Theorie. Behält X die frühere Bedeutung und ist q eine von p verschiedene Primzahl, welche (mod p) zum Divisor f von $(p-1) = ef$ gehört, so ist

$$X \equiv Q_0 Q_1 \dots Q_{e-1} (\mathrm{mod}\ q),$$

wo die e Funktionen Q Primfunktionen vom Grade f bedeuten. Bezeichnet man mit h wieder die sämtlichen f in bezug auf p inkongruenten Zahlen $1, q, q^2, \dots, q^{f-1}$, welche die Wurzeln der Kongruenz $h^f \equiv 1 (\mathrm{mod}\, p)$ bilden, und sind Q, Q' irgend zwei der e Primfunktionen, so hat die Kongruenz

$$Q(y) \equiv 0 (\mathrm{modd}\ q, Q')$$

jedesmal f inkongruente Wurzeln $y \equiv x^{h^n}$. Setzt man nun die e Funktionen

$$Q \equiv x^f - u x^{f-1} + \dots (\mathrm{mod}\, q),$$

so ergibt sich hieraus beiläufig

$$\Pi(x - \eta) = F(x) \equiv \Pi(x - u) (\mathrm{mod}\, q),$$

wo $F(x)$ die Funktion vom Grade e bedeutet, welche für die e Perioden η von f Gliedern verschwindet; doch ist dies keineswegs erforderlich für die weitere Begründung. Die e Zahlen, welche der Verfasser mit ψ bezeichnet, können nämlich dem Erfolge nach vollständig ersetzt werden durch die e Zahlen, welche aus dem Produkte

$$Q_0(r) Q_1(r) \dots Q_{e-1}(r) = q f(r)$$

durch Weglassung je eines der e Faktoren $Q(r)$ hervorgehen. Die Beweisführung, namentlich bei den Sätzen über die Potenzen der idealen Primzahlen, wird vereinfacht, wenn man, was stets möglich ist, die e Funktionen Q so wählt, daß $f(r)$ relative Primzahl zu q, d. h. daß $f(x)$ relative Primfunktion zu $X (\mathrm{mod}\, q)$ wird; statt dessen kann man aber auch die Zerlegung der Funktion X in e Faktoren in bezug auf beliebig hohe Potenzen von q benutzen. Hierbei bemerke ich, daß die vom Verfasser (auf S. 262) gegebene Definition der Potenzen der idealen Primzahlen einen kleinen, leicht zu beseitigenden Zweifel übrig läßt, insofern nicht bewiesen wird, daß eine Zahl, welche einen Primfaktor m mal enthält, ihn gewiß auch $(m-1)$ mal enthalten muß; so lange dies nämlich nicht geschehen ist, bleibt es z. B. denkbar, daß eine Zahl einen Primfaktor genau sechsmal und zugleich auch genau achtmal enthält.

Eine ähnliche zweifelhafte Stelle findet sich auch in der allgemeinen Theorie der Ideale, welche ich in der zweiten Auflage von Dirichlets Vorlesungen über Zahlentheorie vorgetragen habe; die Behauptung, daß der Begriff der Potenzen eines Primideals von der zufälligen Definition des letzteren ganz unabhängig ist (§ 163, 4), ist nicht gehörig begründet, aber sie kann leicht durch die unmittelbar darauf folgenden Sätze bewiesen werden. Die ganze Darstellung läßt sich durch einige Umstellungen bedeutend vereinfachen, und eine noch größere Vereinfachung wird vermutlich solchen gelingen, die unbefangen mit frischen Kräften an den Stoff herantreten. Immerhin glaube ich durch diese Theorie, deren Herstellung mich eine mehrjährige unbeschreibliche Anstrengung gekostet hat, etwas Nützliches erreicht zu haben. Ich bin zwar weit davon entfernt, ihren Wert mit demjenigen des ersten schöpferischen Gedankens von Kummer vergleichen zu wollen; aber abgesehen von der ästhetischen Befriedigung, welche die Erkenntnis gewährt, daß dieselben einfachen Gesetze, nach welchen in der rationalen Zahlentheorie die Zahlen aus Primzahlen zusammengesetzt werden, in der Theorie der Ideale jedes Körpers wiederkehren, hat die Gewißheit der allgemeinen Theorie den großen praktischen Vorteil zur Folge, daß man nicht in jedem speziellen Falle immer wieder die ersten Grundlagen aufzusuchen braucht, und daß die Auffindung der speziellen Gesetze ganz außerordentlich erleichtert wird. Wie groß dieser Nutzen ist, erkennt man recht deutlich in dem vorliegenden Falle der Kreisteilung; die Natur aller hier auftretenden Ideale ergibt sich nämlich — wovon man sich leicht überzeugen wird — mit wenigen Federstrichen aus der einzigen Bemerkung, daß die p Zahlen $1, r, r^2, \ldots, r^{p-1}$ in bezug auf jedes in p nicht aufgehende Primideal gewiß inkongruent sind, weil ihre Differenzen sämtlich in der Zahl p aufgehen.

Ich schließe meine schon zu ausführlichen Bemerkungen über das vorliegende Werk, indem ich dasselbe nochmals allen, welche eine gründliche und vielseitige Kenntnis der Kreisteilung und ihrer Beziehungen zur Zahlentheorie erwerben wollen, auf das wärmste zum Studium anempfehle und dem geehrten Verfasser meinen Dank für die Veröffentlichung dieser seiner Vorlesungen ausspreche.

Braunschweig, 1. Februar 1873.

Erläuterungen zur vorstehenden Abhandlung.

Der ursprüngliche Kroneckersche Satz über die Irreduzibilität der Kreisteilungsgleichungen besagt, daß die Gleichung $\varphi_n(x) = 0$ der primitiven n-ten Einheitswurzeln in einem algebraischen Körper $K(\alpha)$ irreduzibel ist, wenn die Gleichungsdiskriminante von α zu n relativ prim ist. In den Bemerkungen zu Vorlesung 5 beweist aber Dedekind etwas schärfer, daß es schon genügen wird, wenn die Körperdiskriminante von $K(\alpha)$ zu n relativ prim ist.

Diejenigen Untersuchungen über die Klassenzahl der kubischen Körper, welche Dedekind in seinen Bemerkungen zu der 14. Vorlesung erwähnt, hat er später in der Abhandlung „Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern“ (XXIX) publiziert (vgl. die Einleitung dieser Arbeit).

Ore.