15.

Zur Theorie der complexen Zahlen.

(Von dem Herrn Prof. *Kummer* in Breslau.)

(Auszug aus den Berichten der Königl. Akad. der Wiss. zu Berlin vom März 1845.)

Es ist mir gelungen, die Theorie derjenigen complexen Zahlen, welche aus höheren Wurzeln der Einheit gebildet sind und welche bekanntlich in der Kreistheilung, in der Lehre von den Potenzresten und den Formen höherer Grade eine wichtige Rolle spielen, zu vervollständigen und zu vereinfachen; und zwar durch Einführung einer eigenthümlichen Art imaginärer Divisoren, welche ich *ideale complexe Zahlen* nenne; worüber eine kurze Mittheilung zu machen ich mir erlaube.

Wenn α eine imaginäre Wurzel der Gleichung $\alpha^\lambda = 1$, λ eine Primzahl ist und a, a_1, a_2, etc. ganze Zahlen sind, so ist $f(\alpha) = a + a_1\alpha + a_2\alpha^2 + \ldots + a_{\lambda-1}\alpha^{\lambda-1}$ eine complexe ganze Zahl. Eine solche complexe Zahl kann entweder in Factoren derselben Art zerlegt werden; oder auch nicht. Im ersten Fall ist sie eine zusammengesetzte Zahl: im andern Fall ist sie bisher eine complexe Primzahl genannt worden. Ich habe nun aber bemerkt, dafs, wenn auch $f(\alpha)$ auf keine Weise in complexe Factoren zerlegt werden kann, sie deshalb noch nicht die wahre Natur einer complexen Primzahl hat, weil sie schon gewöhnlich der ersten und wichtigsten Eigenschaft der Primzahlen ermangelt: nämlich, dafs das Product zweier Primzahlen durch keine von ihnen verschiedene Primzahl theilbar ist. Es haben vielmehr solche Zahlen $f(\alpha)$, wenn gleich sie nicht in complexe Factoren zerlegbar sind, dennoch die Natur der zusammengesetzten Zahlen; die Factoren aber sind alsdann nicht wirkliche, sondern *ideale complexe Zahlen*. Der Einführung solcher idealen complexen Zahlen liegt derselbe einfache Gedanke zu Grunde, wie der Einführung der imaginären Formeln in die Algebra und Analysis; namentlich bei der Zerfällung der ganzen rationalen Functionen in ihre einfachsten Factoren, die linearen. Ferner ist es auch dasselbe Bedürfnifs, durch welches genöthigt, *Gaufs* bei den Untersuchungen über die biquadratischen Reste (weil hier alle Primfactoren von der Form $4m+1$ die Natur zusammengesetzter Zahlen zeigen) die complexen Zahlen von der Form $a + b\sqrt{-1}$ zuerst einführte.

Um nun zu einer festen Definition der wahren (gewöhnlich idealen) Primfactoren der complexen Zahlen zu gelangen, war es nöthig, die unter allen Umständen bleibenden Eigenschaften der Primfactoren complexer Zahlen zu ermitteln, welche von der Zufälligkeit, ob die wirkliche Zerlegung Statt habe, oder nicht, ganz unabhängig wären: ungefähr eben so, wie man, wenn in der Geometrie von der gemeinschaftlichen Sehne zweier Kreise gesprochen wird, auch dann, wenn die Kreise sich nicht schneiden, eine wirkliche Definition dieser idealen gemeinschaftlichen Sehne sucht, welche für alle Lagen der Kreise pafst. Dergleichen bleibende Eigenschaften der complexen Zahlen, welche geschickt sind, als Definitionen der idealen Primfactoren benutzt zu werden, giebt es mehrere, welche im Grunde immer auf dasselbe Resultat führen und von denen ich eine als die einfachste und allgemeinste gewählt habe.

Ist p eine Primzahl von der Form $m\lambda+1$, so läfst sie sich in vielen Fällen als Product von folgenden $\lambda-1$ complexen Factoren darstellen: $p = f(\alpha).f(\alpha^2).f(\alpha^3)....f(\alpha^{\lambda-1})$; wo aber eine Zerlegung in wirkliche complexe Primfactoren nicht möglich ist: dann sollen die idealen Primfactoren eintreten, um dieselbe zu leisten. Ist $f(\alpha)$ eine wirkliche complexe Zahl und ein Primfactor von p, so hat sie die Eigenschaft, dafs, wenn statt der Wurzel der Gleichung $\alpha^\lambda = 1$ eine bestimmte Congruenzwurzel von $\xi^\lambda \equiv 1$, mod. p, substituirt wird, $f(\xi) \equiv 0$, mod. p, ist. Also auch, wenn in einer complexen Zahl $\Phi(\alpha)$ der Primfactor $f(\alpha)$ enthalten ist, wird $\Phi(\xi) \equiv 0$, mod. p; und umgekehrt: wenn $\Phi(\xi) \equiv 0$, mod. p, und p in $\lambda-1$ complexe Primfactoren zerlegbar ist, enthält $\Phi(\alpha)$ den Primfactor $f(\alpha)$. Die Eigenschaft $\Phi(\xi) \equiv 0$, mod. p ist nun eine solche, welche für sich selbst von der Zerlegbarkeit der Zahl p in $\lambda-1$ Primfactoren gar nicht abhangt; sie kann demnach als Definition benutzt werden, indem bestimmt wird, dafs die complexe Zahl $\Phi(\alpha)$ den idealen Primfactor von p enthält, welcher zu $\alpha = \xi$ gehört, wenn $\Phi(\xi) \equiv 0$, mod. p, ist. Jeder der $\lambda-1$ complexen Primfactoren von p wird so durch eine Congruenzbedingung ersetzt. Dies reicht hin, um zu zeigen, dafs die complexen Primfactoren, sie seien wirklich, oder nur ideal vorhanden, den complexen Zahlen denselben bestimmten Character ertheilen. In der hier gegebenen Weise aber gebrauchen wir die Congruenzbedingungen nicht als Definitionen der idealen Primfactoren, weil diese nicht hinreichend sein würden, mehrere gleiche, in einer complexen Zahl vorkommende ideale Primfactoren vorzustellen, und weil sie, zu beschränkt, nur ideale Primfactoren der realen Primzahlen von der Form $m\lambda+1$ geben würden.

Jeder Primfactor einer complexen Zahl ist immer zugleich auch Primfactor irgend einer realen Primzahl q, und die Beschaffenheit der idealen Primfactoren ist besonders von dem Exponenten abhängig, zu welchem q gehört, für den Modul λ. Derselbe sei f, so dafs $q^f \equiv 1$, mod. λ, und $\lambda - 1 = e \cdot f$. Eine solche Primzahl q läfst sich niemals in mehr als e complexe Primfactoren zerlegen, welche, wenn diese Zerlegung wirklich ausführbar ist, sich als lineare Functionen der e Perioden von je f Gliedern darstellen. Diese Perioden der Wurzeln der Gleichung $\alpha^\lambda = 1$ bezeichne ich durch η, η_1, η_2, ... η_{e-1}; und zwar in der Ordnung, dafs jede in die folgende übergeht, wenn α in α^γ verwandelt wird, wo γ eine primitive Wurzel von λ ist. Bekanntlich sind die Perioden die e Wurzeln einer Gleichung vom $e$ten Grade; und diese, als Congruenz betrachtet, für den Modul q, hat immer e reale Congruenzwurzeln, welche ich durch u, u_1, u_2, ... u_{e-1} bezeichne und in einer entsprechenden Reihenfolge nehme, wie die Perioden, für welche, aufser der Congruenz vom $e$ten Grade, noch andere leicht zu findende Congruenzen gebraucht werden. Wird nun die aus Perioden gebildete complexe Zahl $c'\eta + c'_1\eta_1 + c'_2\eta_2 + ... + c'_{e-1}\eta_{e-1}$ kurz durch $\Phi(\eta)$ bezeichnet, so giebt es unter den Primzahlen q, welche zum Exponenten f gehören, immer solche, die sich auf die Form

$$q = \Phi(\eta)\Phi(\eta_1)\Phi(\eta_2)....\Phi(\eta_{e-1})$$

bringen lassen, in welcher auch die e Factoren niemals eine weitere Zerlegung gestatten. Setzt man statt der Perioden ihre entsprechenden Congruenzwurzeln, wobei sich eine Periode beliebig festsetzen läfst, welche einer bestimmten Congruenzwurzel entsprechen soll, so wird immer einer der e Primfactoren congruent Null, für den Modul q. Enthält nun irgend eine complexe Zahl $f(\alpha)$ den Primfactor $\Phi(\eta)$, so wird sie die Eigenschaft haben, für $\eta = u_k$, $\eta_1 = u_{k+1}$, $\eta_2 = u_{k+2}$, etc. congruent Null zu werden, für den Modul q. Diese Eigenschaft nun (welche eigentlich f besondere Congruenzbedingungen in sich schliefst, deren Entwicklung zu weit führen würde) ist eine bleibende; auch für diejenigen Primzahlen q, welche eine Zerlegung in die e wirklichen complexen Primfactoren nicht gestatten. Sie könnte daher als Definition der complexen Primfactoren benutzt werden, würde aber den Mangel haben, dafs sie die in einer complexen Zahl vorhandenen gleichen idealen Primfactoren nicht ausdrückte.

Die von mir gewählte Definition der idealen complexen Primfactoren, welche im Wesentlichen zwar mit der hier angedeuteten übereinstimmt, aber einfacher und allgemeiner ist, beruht darauf, dafs sich, wie ich besonders beweise, immer eine aus Perioden gebildete complexe Zahl $\psi(\eta)$ finden läfst,

von der Art, dafs $\psi(\eta)\psi(\eta_1)\psi(\eta_2)\ldots\psi(\eta_{e-1})$ (welches eine ganze Zahl ist) durch q theilbar sei, aber nicht durch q^2. Diese complexe Zahl $\psi(\eta)$ hat alsdann immer die obige Eigenschaft, dafs sie congruent Null wird, modulo q, wenn statt der Perioden die entsprechenden Congruenzwurzeln gesetzt werden, also $\psi(\eta)\equiv 0$, mod. q, für $\eta = u$, $\eta_1 = u_1$, $\eta_2 = u_2$, etc. Ich setze nun $\psi(\eta_1)\psi(\eta_2)\ldots\psi(\eta_{e-1}) = \Psi(\eta)$ und definire die idealen Primzahlen folgendermaafsen:

Wenn $f(\alpha)$ die Eigenschaft hat, dafs das Product $f(\alpha).\Psi(\eta_r)$ durch q theilbar ist, so soll dies so ausgedrückt werden: Es enthält $f(\alpha)$ den idealen Primfactor von q, welcher zu $u = \eta_r$ gehört. Ferner, wenn $f(\alpha)$ die Eigenschaft hat, dafs $f(\alpha)(\Psi(\eta_r))^\mu$ durch q^μ theilbar ist, aber $f(\alpha)(\Psi(\eta_r))^{\mu+1}$ nicht theilbar durch $q^{\mu+1}$, so soll dies heifsen: Es enthält $f(\alpha)$ den zu $u = \eta_r$ gehörigen idealen Primfactor von q genau μ mal.

Es würde hier zu weit führen, wenn ich den Zusammenhang und die Übereinstimmung dieser Definition mit den oben angedeuteten, welche durch Congruenzbedingungen gegeben werden, entwickeln wollte; ich bemerke nur, dafs die Bedingung: $f(\alpha)\Psi(\eta_r)$ sei durch q theilbar, f verschiedenen Congruenzbedingungen vollkommen gleichbedeutend ist, und dafs die Bedingung: $f(\alpha)(\Psi(\eta_r))^\mu$ sei durch q^μ theilbar, sich allemal durch $\mu.f$ Congruenzbedingungen vollständig ersetzen läfst. Die ganze von mir bereits fertig ausgearbeitete Theorie der idealen complexen Zahlen, deren Hauptsätze ich hier mittheilen will, ist eine Rechtfertigung sowohl der gegebenen Definition, als auch der gewählten Benennung. Diese Hauptsätze sind folgende:

Das Product zweier oder mehrerer complexen Zahlen hat genau dieselben idealen Primfactoren, wie die Factoren zusammengenommen.

Wenn eine complexe Zahl (welche als Product von Factoren auftritt) alle e Primfactoren von q enthält, so ist sie auch durch q selbst theilbar; enthält sie aber irgend einen dieser idealen Primfactoren nicht, so ist sie nicht durch q theilbar.

Wenn eine complexe Zahl (in Form eines Products) alle e idealen Primfactoren von q enthält, und zwar jeden wenigstens μ mal, so ist sie durch q^μ theilbar.

Wenn $f(\alpha)$ genau m ideale Primfactoren von q enthält, sie mögen verschieden, oder zum Theil, oder sämmtlich gleich sein, so enthält die Norm $Nf(\alpha) = f(\alpha)f(\alpha^2)\ldots f(\alpha^{\lambda-1})$ genau den Factor q^{mf}.

Jede complexe Zahl enthält nur eine endliche, bestimmte Anzahl idealer Primfatoren.

Zwei complexe Zahlen, welche genau dieselben idealen Primfactoren enthalten, unterscheiden sich nur durch eine complexe Einheit, welche als Factor hinzutreten kann.

Eine complexe Zahl ist durch eine andere theilbar, wenn alle idealen Primfactoren des Divisors auch in dem Dividendus enthalten sind; und der Quotient enthält genau den Überschufs der idealen Primfactoren des Dividendus über die des Divisors.

Aus diesen Sätzen geht hervor, dafs die Rechnung mit complexen Zahlen durch Einführung der idealen Primfactoren ganz dieselbe geworden ist, wie die Rechnung mit den ganzen Zahlen und den ganzzahligen realen Primfactoren derselben. Es erledigt sich somit die Klage, welche ich in dem Breslauer Programm zur Jubelfeier der Universität Königsberg S. 18 aussprach: *Maxime dolendum videtur, quod haec numerorum realium virtus, ut in factores primos dissolvi possint, qui pro eodem numero semper iidem sint, non eadem est numerorum complexorum, quae si esset tota haec doctrina, quae magnis adhuc difficultatibus laborat, facile absolvi et ad finem perduci posset. etc.* Auch sieht man, dafs die idealen Primfactoren die innere Natur der complexen Zahlen aufschliefsen, sie gleichsam durchsichtig machen und das innere crystallinische Gefüge derselben zeigen. Ist nämlich eine complexe Zahl nur unter der Form $a+a_1\alpha+a_2\alpha^2+\ldots.+a_{\lambda-1}\alpha^{\lambda-1}$ gegeben, so läfst sich vorläufig wenig über dieselbe aussagen, bis man durch die idealen Primfactoren derselben (welche hier immer durch directe Methoden vollständig gefunden werden können) ihre einfachsten qualitativen Bestimmungen gefunden hat, welche als Grundlagen aller ferneren zahlentheoretischen Untersuchungen dienen.

Die idealen Factoren der complexen Zahlen treten, wie gezeigt, als Factoren von wirklichen complexen Zahlen auf: es müssen deshalb ideale Factoren, mit andern passenden multiplicirt, immer wirkliche complexe Zahlen zu Producten geben. Diese Frage nun, über die Zusammensetzung der idealen Factoren zu wirklichen complexen Zahlen, ist, wie ich an den bereits von mir gefundenen Resultaten zeigen werde, von grofsem Interesse, weil sie mit den wichtigsten Abschnitten der Zahlentheorie in innigem Zusammenhange steht. Die beiden wichtigsten Resultate über diese Frage sind folgende:

Es giebt immer eine endliche, bestimmte Anzahl idealer complexer Multiplicatoren, welche nöthig und hinreichend sind, um alle möglichen idealen complexen Zahlen zu wirklichen zu machen *).

Jede *ideale* complexe Zahl hat die Eigenschaft, dafs eine bestimmte ganze Potenz derselben zu einer *wirklichen* complexen Zahl wird.

Ich gehe in einige nähere Entwickelungen dieser beiden Sätze ein. Zwei ideale complexe Zahlen, welche, mit einer und derselben idealen Zahl multiplicirt, beide zu wirklichen complexen Zahlen machen, nenne ich *äquivalent* oder derselben Classe angehörig, weil diese Untersuchung über die wirklichen und die idealen complexen Zahlen vollständig identisch ist mit der Classification gewisser zusammengehöriger Formen vom $\lambda-1$ten Grade mit $\lambda-1$ Variabeln, über welche *Dirichlet* die Hauptresultate gefunden, aber noch nicht veröffentlicht hat, so dafs ich nicht genau weifs, ob sein Princip der Classification mit diesem, aus der Theorie der complexen Zahlen sich ergebenden genau übereinstimmt. Als besonderer Fall ist die Theorie der Formen vom zweiten Grade mit zwei Variabeln, jedoch nur wenn die Determinante eine Primzahl λ ist, mit in diesen Untersuchungen begriffen, und es stimmt hier unsere Classification mit der *Gaufs*ischen, aber nicht mit der von *Legendre* überein. Auch wirft dieselbe ein helleres Licht auf die *Gaufs*ische Classification der Formen vom zweiten Grade, und auf den wahren Grund der Unterscheidung von *Aequivalentia propria et impropria,* welche, wie nicht zu läugnen, so, wie sie in den *Disquisitiones arithmeticae* auftritt, immer einen Schein des Unpassenden behält. Wenn nämlich dort zwei Formen, wie $ax^2+2bxy+cy^2$ und $ax^2-2bxy+cy^2$, oder $ax^2+2bxy+cy^2$ und $cx^2+2bxy+ay^2$, als verschiedenen Classen angehörend betrachtet werden, während in Wahrheit ein wesentlicher Unterschied derselben nicht aufzufinden ist, und wenn andererseits die *Gaufs*ische Classification dennoch als die der Natur der Sache am meisten entsprechende anerkannt werden mufs: so wird man genöthigt, die sich wirklich nur ganz äufserlich von einander unterscheidenden Formen, wie $ax^2+2bxy+cy^2$ und $ax^2-2bxy+cy^2$, blofs als die Repräsentanten zweier andern, aber wesentlich verschiedenen Begriffe der Zahlentheorie aufzufassen. Diese aber sind in Wahrheit nichts anderes als zwei verschiedene ideale Factoren, welche einer und derselben Zahl angehören. Die ganze Theorie der

*) Ein Beweis dieses wichtigen Satzes, wenn gleich in weit geringerer Allgemeinheit und in ganz anderer Form, findet sich in der Dissertation: *De unitatibus complexis* von *L. Kronecker*, Berlin 1845.

Formen vom zweiten Grade, mit zwei Variabeln, kann nämlich als Theorie der complexen Zahlen von der Form $x+y\sqrt{D}$ aufgefafst werden, und führt dann nothwendig zu idealen complexen Zahlen derselben Art. Diese classificiren sich aber eben so nach den idealen Multiplicatoren, welche nöthig und hinreichend sind, um sie zu wirklichen complexen Zahlen von der Form $x+y\sqrt{D}$ zu machen. Mit der *Gaufs*ischen Classification übereinstimmend, erschliefsen diese so den wahren Grund derselben.

Die allgemeine Untersuchung über die idealen complexen Zahlen hat die gröfste Analogie mit dem bei *Gaufs* sehr schwierig behandelten Abschnitte: *De compositione formarum,* und die Hauptresultate, welche *Gaufs* für die quadratischen Formen pag. 337 sqq. bewiesen hat, finden auch für die Zusammensetzung der allgemeinen idealen complexen Zahlen Statt. Es gehört hier zu jeder Classe idealer Zahlen eine andere Classe, welche, mit dieser multiplicirt, wirkliche complexe Zahlen hervorbringt (die wirklichen complexen Zahlen bilden hier das Analogon der *Classis principalis*). Es sind hier auch Classen, welche, mit sich selbst multiplicirt, wirkliche complexe Zahlen (die *Classis principalis*) geben, also *ancipites;* namentlich ist die *Classis principalis* selbst stets eine *Classis anceps.* Nimmt man eine ideale complexe Zahl $f(\alpha)$ und erhebt sie zu Potenzen, so gelangt man, nach dem zweiten der obigen Sätze, immer zu einer Potenz, welche eine wirkliche complexe Zahl ist; wenn h die kleinste Zahl ist, für welche $(f(\alpha))^h$ eine wirkliche complexe Zahl ist, so gehören $f(\alpha)$, $(f(\alpha))^2$, $(f(\alpha))^3$, ... $f(\alpha)^h$ alle verschiedenen Classen an. Es kann nun geschehen, dafs diese, namentlich bei passender Wahl des $f(\alpha)$, alle vorhandenen Classen erschöpfen: ist es nicht der Fall, so wird leicht bewiesen, dafs die Anzahl aller Classen wenigstens immer ein Vielfaches von h ist. Ich bin vorläufig noch nicht tiefer in dieses Gebiet der Theorie der complexen Zahlen eingedrungen; namentlich habe ich eine Untersuchung der wahren Anzahl der Classen noch nicht unternommen, weil, wie ich durch mündliche Mittheilungen erfahren habe, *Dirichlet,* nach ähnlichen Principien, wie in seinen berühmten Abhandlungen über die quadratischen Formen, diese Anzahl bereits gefunden hat. Ich bemerke nur noch dies Eine über den Character der idealen complexen Zahlen, dafs sie, nach dem zweiten der obigen Sätze, als bestimmte Wurzeln aus wirklichen complexen Zahlen überall angesehen und dargestellt werden können, oder dafs sie immer die Form $\sqrt[h]{(\Phi(\alpha))}$ annehmen, wo $\Phi(\alpha)$ eine wirkliche complexe Zahl ist, und h eine ganze Zahl.

Aus den verschiedenen Anwendungen, welche ich von dieser Theorie der complexen Zahlen schon gemacht habe, hebe ich nur die Anwendung auf die Kreistheilung hervor; als Vervollständigung Dessen, was ich in dem erwähnten Programm bereits mittheilte. Setzt man

$$(\alpha, x) = x + \alpha x^g + \alpha^2 x^{g^2} + \ldots + \alpha^{p-2} x^{g^{p-2}},$$

wo $\alpha^\lambda = 1$, $x^p = 1$, $p = m\lambda + 1$, und g eine primitive Wurzel der Primzahl p ist, so ist bekanntlich $(\alpha, x)^\lambda$ eine von x unabhängige, aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildete complexe Zahl. Für diese habe ich in dem erwähnten Programm, unter der Voraussetzung, dafs p sich in $\lambda - 1$ wirkliche complexe Primfactoren zerlegen läfst, deren einer $f(\alpha)$ sei, folgenden Ausdruck gefunden:

$$(\alpha, x)^\lambda = \pm \alpha^h f(\alpha)^{m_1} . f(\alpha^2)^{m_2} . f(\alpha^3)^{m_3} \ldots . f(\alpha^{\lambda-1})^{m_{\lambda-1}},$$

in welchem die Potenz-Exponenten m_1, m_2, m_3, etc. so bestimmt sind, dafs allgemein m_k positiv kleiner als λ und $k . m_k \equiv 1$, mod. λ ist. Genau derselbe einfache Ausdruck gilt nun, wie sich leicht beweisen läfst, ganz allgemein, auch wenn $f(\alpha)$, der Primfactor von p, nicht ein wirklicher, sondern nur ein idealer ist. Um aber in letzterem Falle den Ausdruck des $(\alpha, x)^\lambda$ in Form einer wirklichen complexen Zahl zu haben, darf man nur das ideale $f(\alpha)$ als Wurzel aus einer wirklichen complexen Zahl darstellen, oder eine der (wenn auch indirecten) Methoden anwenden, welche dazu dienen, eine wirkliche complexe Zahl herzustellen, deren ideale Primfactoren gegeben sind.