XLV.

Aus Briefen an Frobenius*).

8. Juni 1882**).

... Die Ihnen bekannte Existenz einer Substitution F (bei mir Permutation ψ_0), für welche $\omega^p \equiv F\omega \pmod{\mathfrak{p}}$, bildet auch bei mir die eigentliche Basis; Sie schreiben zwar: „Ich irre wohl nicht, wenn ich annehme, dass der durch diesen Satz angedeutete Weg einer von denen ist, die auch Sie früher einmal eingeschlagen, dann aber wohl schliesslich verlassen und durch einen bessern ersetzt haben.“ Aber ich glaube kaum, dass es einen besseren Weg giebt. Mit Hülfe der Theorie der höheren Congruenzen und mit viel Geduld und Zeit ist es mir nach und nach gelungen, die Schwierigkeiten zu überwinden und die Gesetze möglichst einfach zu gestalten. In diesen ist auch, wie Sie vermuthen, der Satz enthalten, für den Sie einen Beweis wünschen, und den Sie so aussprechen:

Ist eine rationale Primzahl $\mathfrak{o}'p = \mathfrak{p}'_1\mathfrak{p}'_2 \cdots \mathfrak{p}'_{e'}$, wo $\mathfrak{p}'_1, \mathfrak{p}'_2 \cdots \mathfrak{p}'_{e'}$ verschiedene Primideale in $\mathfrak{o}'$ von den Graden $f'_1, f'_2, \cdots f'_{e'}$ sind, so giebt es in der Gruppe Φ des Körpers Ω' eine Substitution ψ_0, die aus e' Cyklen von $f'_1, f'_2, \cdots f'_{e'}$ Elementen besteht.

In der That, wenn alle $a_r = 1$, mithin alle $g_r = g$ sind, so ist X gemeinschaftlicher Theiler aller $\varphi_r \Phi' \varphi_r^{-1}$ und überhaupt aller mit Φ' conjugirten Gruppen $\varphi \Phi' \varphi^{-1}$; da diese aber, wenn wirklich Φ die

*) [Diese Briefe wurden durch Herrn Landau freundlichst zur Verfügung gestellt. Die Briefe von Frobenius an Dedekind waren im Nachlaß nicht zu finden; es fehlten im Nachlaß die Briefe aus den Jahren 1880—1900. E. N.]

**) [Im wesentlichen wiedergegeben bei Frobenius: Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. Sitzungsber. d. Preuß. Akademie d. Wissensch. 1896. E. N.]

Gruppe von $\mathfrak{Q}'$, d. h. $\mathfrak{Q}$ die Norm von $\mathfrak{Q}'$ ist, keinen gemeinsamen Theiler haben, so muß $X = 1$, $g = 1$ sein, d. h. p ist durch kein Primidealquadrat in $\mathfrak{Q}$ theilbar. Dann ist

$$\Psi'_r = 1 + \psi_r^{f'_r} + \psi_r^{2f'_r} + \cdots + \psi_r^{(\sigma_r - 1)f'_r},$$

wo $\psi_r = \varphi_r^{-1} \psi_0 \varphi_r$,

$$\Phi' \varphi_r^{-1} \Psi = \Phi' \varphi_r^{-1} + \Phi' \varphi_r^{-1} \psi_0 + \Phi' \varphi_r^{-1} \psi_0^2 + \cdots + \Phi' \varphi_r^{-1} \psi_0^{f'_r - 1};$$

ersetzt man in der Zerlegung

$$\Phi = \Phi' \varphi_1^{-1} \Psi + \cdots + \Phi' \varphi_{e'}^{-1} \Psi$$

jeden einzelnen Complex $\Phi' \varphi_r^{-1} \Psi$ durch das vorstehende System der f'_r Complexe, so wird Φ überhaupt in

$$n' = f'_1 + f'_2 + \cdots + f'_{e'}$$

Complexe $\Phi' \varphi$ zerlegt, deren jedem bekanntlich eine Permutation von $\mathfrak{Q}'$ (eine Wurzel der irreductibeln Gleichung vom Grade n') entspricht; die Permutation ψ_0 verwandelt dieselben in die Complexe $\Phi' \varphi \psi_0$, bringt also eine Permutation dieser n' Complexe (Elemente) $\Phi' \varphi$ hervor, bei welcher die in $\Phi' \varphi_r^{-1} \Psi$ enthaltenen f'_r Complexe (Elemente, Wurzeln) cyklisch in einander übergehen.

14. Juni 1882*).

... Auf den hiermit wieder zurückerfolgenden Blättern (13—15) haben Sie die Existenz einer Permutation ψ_0 (oder Substitution F) sehr kurz bewiesen. Bei mir ergiebt sich dieselbe z. B. aus der leicht zu beweisenden Existenz einer ganzen Zahl Θ, welche (mod. $\mathfrak{p}$) einer irreductibelen Congruenz f^{ten} Grades mit rationalen Coefficienten genügt, und welche man zugleich (für unseren Zweck) so wählen kann, dass sie nicht durch $\mathfrak{p}$, wohl aber durch jedes andere in p aufgehende Primideal theilbar ist; wenn nun $f(t) = \Pi(t - \Theta|\varphi)$, so ist $f(\Theta) = 0$, mithin $f(\Theta^p) \equiv 0$ (mod. $\mathfrak{p}$), folglich $\Theta^p \equiv \Theta|\psi_0$ (mod. $\mathfrak{p}$); wäre ferner $\mathfrak{p}|\psi_0^{-1}$ verschieden von $\mathfrak{p}$, so wäre $\Theta \equiv 0$ (mod. $\mathfrak{p}|\psi_0^{-1}$), also $\Theta|\psi_0 \equiv 0$ (mod. $\mathfrak{p}$), also $\Theta^p \equiv 0$ (mod. $\mathfrak{p}$), also auch $\Theta \equiv 0$ (mod. $\mathfrak{p}$), contra hyp. Also $\mathfrak{p}|\psi_0^{-1} = \mathfrak{p}$; $\mathfrak{p}|\psi_0 = \mathfrak{p}$. Nun ist (zufolge Def. von Θ)

*) [Im wesentlichen wiedergegeben bei Frobenius: Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe. E. N.]

jede ganze Zahl $\omega \equiv F(\Theta)$ (mod. $\mathfrak{p}$), wo $F(t)$ eine ganze Function mit ganzen rationalen Coefficienten; mithin $\omega \,|\, \psi_0 \equiv F(\Theta) \,|\, \psi_0 = F(\Theta \,|\, \psi_0) \equiv F(\Theta^p) \equiv F(\Theta)^p \equiv \omega^p$ (mod. $\mathfrak{p} \,|\, \psi_0 = \mathfrak{p}$).

5. Februar 1883*).

... Ihr thätiges Interesse an der Zahlentheorie ist mir sehr erfreulich, und die grosse Abkürzung der Untersuchung über die Discriminante, die Sie und Hr. Stickelberger aufgefunden haben, gefällt mir besonders deshalb, weil die mir immer unliebsame Zuziehung der Theorie der höheren Congruenzen (mit Variabeln) wieder aufgehoben wird. Ihr rationales $R(\omega)$ ist mir freilich lange bekannt gewesen, aber ich habe nie daran gedacht, es auf so glückliche Weise zu verwenden. Immerhin lege ich aus besonderen, persönlichen Gründen einigen Werth auf den Satz, dass es immer eine reguläre Ordnung giebt, deren Führer durch ein gegebenes Primideal nicht theilbar ist; hierin besteht für mich der letzte Rest und wirkliche Kern ehemaliger Vermuthungen, die zu klären ich lange Zeit gebraucht habe. Zwar weiss ich nicht mehr, ob ich jemals geglaubt habe, jedes System $\mathfrak{o}$ aller in einem Körper Ω enthaltenen ganzen Zahlen sei eine reguläre Ordnung (welcher Fall für die ersten Kummer'schen Untersuchungen so sehr günstig gewesen ist), aber lange Zeit habe ich es für äusserst wahrscheinlich gehalten und kaum bezweifelt, dass es immer reguläre Ordnungen $\mathfrak{n}$ gebe, für welche $(\mathfrak{o}, \mathfrak{n})$ durch eine gegebene rationale Primzahl nicht theilbar ist; meine alten Papiere enthalten viele Beweisversuche, die natürlich immer im Sande verlaufen, bis endlich die bessere Erkenntniss kam; und dann hat es wieder lange gedauert, bis ich (etwa vor zwei Jahren, wie ich glaube) das oben genannte Residuum sicher stellen konnte.

Ihr Kriterium darüber, ob ein Ideal $\mathfrak{k}$ Führer einer Ordnung sein kann, scheint mir mit dem meinigen auch äusserlich fast identisch zu werden, sobald man die Elementartheiler Ihrer Determinante als invariante Theiler der Classenanzahl $(\mathfrak{b}, \mathfrak{a})$ für beliebige Moduln $\mathfrak{a}$, $\mathfrak{b}$ auffasst, die ganz unabhängig von Determinanten definirt werden können und von denen der erste der kleinste Multiplicator

*) [Einige Einzelheiten aus diesem Briefe sind in § 170 der vierten Auflage der Zahlentheorie übernommen; der in dem Briefe gegebene volle Überblick über die Fragen der Modultheorie ist nirgends publiziert. Für den Schluß des Briefes vgl. XXIX. E. N.]

ist, der $\mathfrak{b}$ in ein Multiplum von $\mathfrak{a}$ verwandelt. Sie haben, wie Sie schreiben, aus Ihrer Form noch keinen Nutzen ziehen können für die Beantwortung der Frage nach den Ordnungen, die ein solches Ideal zum Führer haben; dasselbe gilt auch für meine Form. Diese Aufgabe will besonders angegriffen sein. Es leuchtet ein, dass das kleinste gemeinschaftliche Vielfache beliebig vieler Ordnungen $\mathfrak{n}_1, \mathfrak{n}_2 \cdots$ immer wieder eine Ordnung $\mathfrak{n}$ ist, deren Führer $\mathfrak{k}$ zugleich das kleinste gemeinschaftliche Vielfache von den Führern $\mathfrak{k}_1, \mathfrak{k}_2 \cdots$ jener Ordnungen ist; und dieser Satz lässt sich wenigstens dahin umkehren, dass jede Ordnung $\mathfrak{n}$ das kleinste gemeinschaftliche Vielfache solcher Ordnungen $\mathfrak{n}_1, \mathfrak{n}_2 \cdots$ ist, für welche $(\mathfrak{o}, \mathfrak{n}_1)$, $(\mathfrak{o}, \mathfrak{n}_2) \cdots$ die verschiedenen in $(\mathfrak{o}, \mathfrak{n})$ aufgehenden höchsten Primzahlpotenzen sind; dadurch wird die Untersuchung auf die Betrachtung solcher Ordnungsführer $\mathfrak{k}$ zurückgeführt, deren Normen Primzahlpotenzen sind. Die nähere Untersuchung, die mehr lästig, als principiell schwierig ist, ergiebt eine große Reichhaltigkeit; die Grundlage bildet der einfachste Fall, wo $\mathfrak{k}$ ein Primideal $\mathfrak{p}$ vom Grade f ist: die Anzahl der verschiedenen Ordnungen $\mathfrak{n}$, welche $\mathfrak{p}$ zum Führer haben, ist um eins kleiner, als die Anzahl der Divisoren m von f; jedem echten Divisor m entspricht eine Ordnung $\mathfrak{n}$, welche aus den sämmtlichen Wurzeln ν der Congruenz

$$\nu^{p^m} \equiv \nu \pmod{\mathfrak{p}}$$

besteht; $(\mathfrak{n}, \mathfrak{p}) = p^m$; $N(\mathfrak{p}) = p^f$.

Diese Untersuchung bildet ein Capitel der allgemeinen Theorie der n-gliedrigen Moduln in einem Körper n^{ten} Grades, welche in meiner Gauss-Festschrift (1877), wie ich dort ausdrücklich bemerkt habe, keineswegs vollständig behandelt ist; aber ihre wichtigsten Grundlagen sind doch in dieser Schrift enthalten. Es kommt hierbei auf den Unterschied zwischen umkehrbaren und nicht umkehrbaren Moduln an; ich nenne einen Modul $\mathfrak{a}$ umkehrbar (auch im allgemeinsten Sinn des Worts Modul), wenn ein Modul $\mathfrak{b}$ existirt, für welchen $\mathfrak{a}\mathfrak{b} = \mathfrak{a}^0$, d. h. gleich der Ordnung von $\mathfrak{a}$ wird; alle solche Moduln $\mathfrak{b}$ liefern ein und dasselbe Product $\mathfrak{b}\mathfrak{a}^0$, das ich mit $\mathfrak{a}^{-1}$ bezeichne, und dessen Ordnung immer $= \mathfrak{a}^0$ ist; jedes Product von umkehrbaren Moduln ist wieder ein umkehrbarer Modul, und seine Ordnung ist das Product aus den Ordnungen der Factoren. Unter den n-gliedrigen Moduln eines Körpers Ω vom Grade n sind die einfachsten die Moduln, deren Ordnung $= \mathfrak{o}$; sie sind alle umkehrbar und identisch

mit den Ideal-Quotienten; die Regeln ihrer Multiplication und Division stimmen genau mit denjenigen für rationale Brüche überein; die Definition der Norm ist selbstverständlich. Ähnliches (mit Modification) gilt für die Moduln einer jeden regulären, allgemeiner jeder solchen Ordnung $\mathfrak{n}$, deren Complement $\mathfrak{n}'$ umkehrbar ist (weil für jeden solchen Modul $\mathfrak{a}$ immer $\mathfrak{a}\mathfrak{a}' = \mathfrak{n}'$ ist). Aber sobald $n > 2$ ist, haben durchaus nicht mehr alle Ordnungen diese Eigenschaft. Ist nun $\mathfrak{m}$ ein beliebiger Modul, $\mathfrak{n}$ seine Ordnung, so ist $\mathfrak{m}\mathfrak{o}$ immer ein Modul der Ordnung $\mathfrak{o}$, also ein Ideal-Quotient, und der Führer von $\mathfrak{m}$, d. h. der Quotient $\frac{\mathfrak{m}}{\mathfrak{o}}$ ist $= \mathfrak{f}\mathfrak{m}$, wo $\mathfrak{f}$ der Führer von $\mathfrak{n}$; $N(\mathfrak{m})$ wird definirt als $N(\mathfrak{m}\mathfrak{o})$. Umgekehrt, ist $\mathfrak{a}$ ein Modul der Ordnung $\mathfrak{o}$, so folgt aus der Festschrift (1877) die wichtige Existenz mindestens eines umkehrbaren Moduls $\mathfrak{m}$ jeder Ordnung $\mathfrak{n}$, für welchen $\mathfrak{m}\mathfrak{o} = \mathfrak{a}$ wird; und die sämmtlichen Moduln $\mathfrak{m}_1$ derselben Ordnung $\mathfrak{n}$, welche derselben Forderung $\mathfrak{m}_1\mathfrak{o} = \mathfrak{a}$ genügen, sind die sämmtlichen Producte $\mathfrak{m}\mathfrak{e}$, wo $\mathfrak{e}$ alle diejenigen Moduln der Ordnung $\mathfrak{n}$ durchläuft, für welche $\mathfrak{e}\mathfrak{o} = \mathfrak{o}$ wird. Der Reichthum an solchen Moduln $\mathfrak{e}$ ist sehr gross; sie sind natürlich lauter ganze Moduln, d. h. Vielfache von $\mathfrak{o}$, und zugleich Theiler des Führers $\mathfrak{f}$, da $\frac{\mathfrak{e}}{\mathfrak{o}} = \frac{\mathfrak{n}}{\mathfrak{o}} = \mathfrak{f}$ ist.

Hierin bestehen, wenn ich mich recht erinnere, die hauptsächlichsten Gedanken der genannten Theorie, die ich übrigens noch niemals vollständig ausgearbeitet habe; doch hoffe ich, Ihnen nichts Unrichtiges geschrieben zu haben. Wichtig ist diese Theorie, und namentlich scheint sie unerlässlich für die Aufstellung der allgemeinsten Gesetze, welche die bisher bekannten, sogenannten Reciprocitätssätze in sich schliessen. Bei cubischen Körpern Ω z. B. kommt die Primideal-Zerlegung derjenigen rationalen Primzahlen p, von denen die Grundzahl $D = \Delta(\Omega)$ quadratischer Rest ist (die übrigen p machen keine Schwierigkeit), auf die Betrachtung der ursprünglichen quadratischen Formen $(a, \frac{1}{2}b, c)$ zurück, deren Discriminante $b^2 - 4ac = D$ ist; die Anzahl der Classen dieser Formen oder der entsprechenden Modul-Classen ist immer durch 3 theilbar, und ein gewisses Drittel dieser Classen bildet eine Gruppe; je nachdem p durch eine Form dieser Gruppe darstellbar ist oder nicht, ist $\mathfrak{o}p$ in Ω ein Product von drei Primidealen ersten Grades oder ein Primideal dritten Grades. Für negative D hängt dies mit der complexen Multiplication der

elliptischen Functionen zusammen, was auch Kronecker vollständig erkannt zu haben scheint. Ich habe diesen Satz, der ohne jeden Zweifel ganz allgemein, auch für positive D gilt, vor 11 Jahren durch Induction gefunden (Schlömilch's Zeitschrift, Jahrgang 18; 1873. Literaturzeitung S. 22 und S. 43, wo der durch die Schuld des Herrn Schlömilch ausgelassene Zusatz steht), gestehe aber gern, dass ich ihn noch nicht für alle Fälle bewiesen habe; doch hoffe ich dies noch zu erreichen. Er gilt sogar, wenn D eine positive Quadratzahl, mithin Ω ein Normalkörper ist, der aus der Kreistheilung entspringt. Ich glaube gewiss, man wird dereinst ganz allgemeine Gesetze finden, welche gestatten, die Primideale eines Körpers unmittelbar abzuleiten aus seiner Discriminante und seinen übrigen Invarianten (die auch Ideale verwandter Körper sein können); doch mögen wir wohl noch recht weit von diesem Ziele entfernt sein! In den letzten Jahren habe ich mich sehr wenig mit diesen Fragen beschäftigt, zu denen ich aber grosse Lust habe zurückzukehren, weil sie mir von allen die interessantesten zu sein scheinen. . . .

8. Februar 1895*).

. . . Auf Ihre Arbeit über die Gruppen bin ich sehr gespannt, da die Einfachheit Ihrer Methoden, unter Anderem Ihr Beweis, dass in einer Gruppe, deren Grad durch die Primzahl p theilbar ist, es immer ein Element p^{ter} Ordnung giebt, mich sehr erfreut hat; ich war in den ersten Jahren meiner Gruppen-Studien (1855—1858) auf einem viel umständlicheren Wege dahin gekommen. Auch später habe ich gewisse Gruppen-Fragen immer nur so weit verfolgt, wie es Veranlassungen von anderer Seite her mit sich brachten; sollte es also der Zufall wollen, dass ich mich mit dem Gegenstande Ihrer Arbeit schon jemals beschäftigt hätte, so würde ich doch gewiss weit hinter Ihnen zurückgeblieben sein. Um auf gut Glück zu rathen, frage ich: drängen sich in Ihre Untersuchung auch übercomplexe Grössen ein mit nicht commutativer Multiplication? Doch will ich Sie keineswegs mit der Bitte um eine Antwort bemühen, die

*) [Die jetzt folgenden Briefstellen geben einen wesentlichen Beitrag zur Geschichte der Theorie der hyperkomplexen Größen und der Gruppendeterminante. Auf die Rolle, die Dedekind in dieser Theorie gespielt hat, weist Frobenius an verschiedenen Stellen hin, in den Einleitungen zu den Arbeiten über Gruppencharaktere, über die Primfaktoren der Gruppendeterminante und über die Darstellung der endlichen Gruppen. E. N.]

ich am besten durch Ihre Abhandlung erhalten werde. Ihre äusserst scharfsinnige Untersuchung über die Elementartheiler der Determinanten habe ich mit grossem Interesse studirt; ich leugne nicht, dass ich bei dem Beweise in §. 1 die unbestimmte Empfindung habe, als könnte er auch wohl ohne die Gleichung (6) auf S. 4 gelingen, aber ich bin ganz ausser Stande, etwas Anderes an die Stelle zu setzen. . . .

12. Februar 1895.

. . . Keine Entschuldigung habe ich für meine gewagte Bemerkung bezüglich Ihrer Abhandlung über die Elementartheiler — die unbestimmte Empfindung entspringt aus einer in diesem Falle wohl sehr thörichten Abneigung gegen Potenzen-Folgen — um so mehr muss ich um Nachsicht wegen deren Äusserung bitten. Auch meine Frage wegen der Benutzung übercomplexer Grössen in der Gruppen-Theorie war sehr dreist; sie ging hervor aus einer Beobachtung, die ich im Februar 1886 gemacht, dann aber nicht weiter verfolgt habe, obwohl sie mir merkwürdig genug erschien; vielleicht darf ich mir einmal erlauben, sie Ihnen vorzulegen, auf die Gefahr hin, dass sie vor Ihrer Kritik gänzlich dahin schwindet, möglicherweise auch gar nicht einmal neu ist. . . .

25. März 1896.

. . . Da ich einmal von Gruppen spreche, so möchte ich noch eine andere Betrachtung erwähnen, auf die ich im Februar 1886 gekommen bin. Zu jeder Gruppe n^{ten} Grades G bilde ich eine Form n^{ten} Grades H mit n Variabelen, die ich die Determinante von G nenne: sind $1, 2 \cdots n$ die in irgend einer Ordnung aufgeschriebenen Elemente von G, so lasse ich jedem Elemente r der Gruppe G eine Variabele x_r entsprechen, und bilde die Determinante

$$H = \begin{vmatrix} x_{11'}, & x_{21'} & \cdots & x_{n1'} \\ x_{12'}, & x_{22'} & \cdots & x_{n2'} \\ \cdot & \cdot & \cdot & \cdot \\ x_{1n'}, & x_{2n'} & \cdots & x_{nn'} \end{vmatrix},$$

wo r' das zu r reciproke Element von G bedeutet. Ist G eine Abel'sche Gruppe, und sind $\psi', \psi'' \cdots \psi^{(n)}$ die ihr entsprechenden Charaktere (Einheitswurzeln), so ist die Determinante H eine zerlegbare Form, nämlich das Product der n linearen Factoren

$$\sum_{r} \psi^{(s)}(r)\, x_r = \psi^{(s)}(1)\, x_1 + \cdots + \psi^{(s)}(n)\, x_n,$$

die den n Werthen von s entsprechen (ein Satz, welcher in dieser Allgemeinheit, wie ich glaube, noch nicht ausgesprochen ist). Wenn aber G keine Abel'sche Gruppe ist, so besitzt ihre Determinante H, soweit ich es untersucht habe, ausser linearen Factoren (wie z. B. immer $x_1 + x_2 + \cdots + x_n$) auch Factoren höheren Grades, die im gewöhnlichen Sinne unzerlegbar sind; aber diese werden wieder zerlegbar in lineare Factoren, wenn man ausser den gewöhnlichen Zahlen als Coefficienten auch übercomplexe Zahlen (mit nicht commutativer Multiplication) gestattet, die den Gesetzen der Gruppe G entsprechen. Bei der obigen Quaternion-Gruppe Q z. B. treten auf diese Weise bei der erzwungenen Zerlegung ihrer Determinante in lineare Factoren (deren vier gewöhnliche Coefficienten haben) in der That Hamilton's Quaternion-Zahlen auf. Man darf überhaupt wohl vermuthen, dass die Eigenschaften einer Gruppe G hinsichtlich ihrer Theiler sich in der Zerlegung ihrer Determinante H wiederspiegeln werden; ausser einer Spur, die auf einen Zusammenhang zwischen der Anzahl der gewöhnlichen linearen Factoren von H und denjenigen Normaltheilern A von G hindeutet, welche die Eigenschaft $Ars = Asr$ besitzen, habe ich aber noch gar Nichts gefunden, und es ist überhaupt wohl möglich, dass bei der ganzen Sache vorläufig wenig herauskommen wird. ...

3. April 1896.

... Erwähnen möchte ich noch Folgendes*). Man sieht leicht, dass Q durch 24 Transformationen, bei welchen sich nur die sechs Buchstaben α, α^{-1}, β, β^{-1}, γ, γ^{-1} mit einander vertauschen, isomorph in sich selbst übergeht; die Gruppe T dieser Transformationen ist also eine Untergruppe von der Gruppe V_6 aller 720 Versetzungen von 6 Elementen, und zwar habe ich gefunden, dass diese Gruppe T isomorph ist mit der Gruppe V_4 aller 24 Versetzungen von 4 Elementen a, b, c, d. Bezeichnet man nämlich allgemein mit (a, d) die Vertauschung (Transposition) von nur zwei verschiedenen Elementen a, d, so wird die Gruppe T erzeugt durch die drei Elemente zweiten Grades

$$(\alpha, \alpha^{-1})\,(\beta, \gamma)\,(\beta^{-1}, \gamma^{-1}) \equiv (a, d),$$
$$(\beta, \beta^{-1})\,(\gamma, \alpha)\,(\gamma^{-1}, \alpha^{-1}) \equiv (b, d),$$
$$(\gamma, \gamma^{-1})\,(\alpha, \beta)\,(\alpha^{-1}, \beta^{-1}) \equiv (c, d),$$

*) [Es war hier und im vorangehenden Brief ein Überblick über die Arbeit XXVII über Gruppen, deren sämtliche Teiler normal sind, vorangegangen; Q bedeutet die Quaternionengruppe. E. N.]

wo das Zeichen $\equiv$ das isomorphische Entsprechen bedeuten soll. Dass die Gruppe V_6 eine solche transitive Untergruppe $T \equiv V_4$ (vom Index 30) besitzt, wird wohl schon lange bekannt sein; jedenfalls soll dies von meinem Aufsatz über die Hamilton'schen Gruppen ausgeschlossen werden.

Ebenso wenig werde ich dort von der allgemeinen Bedeutung der Commutatoren $\psi^{-1}\varphi^{-1}\psi\varphi$ sprechen, auf welche ich vor vielen Jahren bei der Aufgabe gekommen bin, aus irgend einem Normal-Körper alle darin enthaltenen Abel'schen Körper auszuscheiden. Man findet leicht (— was, wie ich aus Ihrem Briefe schliesse, auch Ihnen gewiss bekannt ist —) den Satz: „Die erforderliche und hinreichende Bedingung dafür, dass A ein invarianter Theiler der Gruppe G, und zugleich G/A eine Abel'sche Gruppe ist ($Ars = Asr$), besteht darin, dass alle Commutatoren von je zwei Elementen r, s der Gruppe G in der Gruppe A enthalten sind; die kleinste solche Gruppe A (diejenige nämlich, welche durch alle Commutatoren erzeugt wird) ist der gemeinsame Theiler von allen A." Ich erwähne dies auch nur, um nochmals auf die von Ihnen günstig aufgenommene Determinante H irgend einer Gruppe G zurückzukommen, welche ich vor 10 Jahren an einigen sehr speciellen Beispielen (V_3 vom Grade 6, Q vom Grade 8) und einigen allgemeineren (complexe Multiplication) untersucht habe. Auf Ihre Anfrage wegen des einen Punctes gestehe ich, dass ich nichts Bestimmtes weiss, aber ich vermuthe allerdings, dass die Anzahl der linearen Factoren der Determinante H der Index der eben genannten kleinsten Gruppe A, also der Grad der Abel'schen Gruppe G/A ist, und dass diese Factoren in gewisser Weise den Charakteren dieser letzteren Gruppe entsprechen. Es würde mich sehr freuen, wenn Sie sich in diese Dinge versenken wollten, weil ich deutlich fühle, dass ich hier Nichts zu Stande bringen werde. Dass Ihre Determinante der Charakteristiken-Gruppe in den Thetafunctionen wesentlich mit meinem H übereinstimmt (besser umgekehrt), scheint mir nach Einblick in Ihre Abhandlung (Crelle 96, S. 100) ganz unzweifelhaft, und Ihnen gebührt daher auch die volle Priorität für diese Gruppen-Determinanten*). Was den Fall der Abel'schen

*) [Frobenius erwähnt in der Arbeit über die Primfaktoren der Gruppendeterminante, daß er vom Additionstheorem aus, und nicht durch die Gruppe der Relationen, auf die Determinante der Charakteristiken gekommen sei. E. N.]

Gruppen betrifft, so habe ich wohl in den Wiener Sitzungs-Berichten einige darauf bezügliche Aufsätze (von Gegenbauer?) gesehen; doch glaube ich nicht, dass der Satz in seiner Allgemeinheit dort ausgesprochen ist....

6. April 1896.

... Für den Fall, dass Sie sich noch näher mit den Gruppen-Determinanten beschäftigen wollen, erlaube ich mir hiermit, Ihnen wenigstens zwei von den Beispielen zu senden, die ich im Februar 1886 ausgerechnet habe; doch übergehe ich die übercomplexe Zerlegung der nicht linearen Factoren.

Beispiel 1.

Gruppe V_3 der sechs Versetzungen von drei Buchstaben a, b, c.

Bezeichnung und Composition der Substitutionen:

	a	b	c
1	a	b	c
2	b	c	a
3	c	a	b
4	a	c	b
5	c	b	a
6	b	a	c

	1^{-1}	2^{-1}	3^{-1}	4^{-1}	5^{-1}	6^{-1}
1	1	3	2	4	5	6
2	2	1	3	5	6	4
3	3	2	1	6	4	5
4	4	5	6	1	3	2
5	5	6	4	2	1	3
6	6	4	5	3	2	1

Setzt man $1 + \varrho + \varrho^2 = 0$

und
$$u = x_1 + x_2 + x_3, \qquad v = x_4 + x_5 + x_6,$$
$$u_1 = x_1 + \varrho\, x_2 + \varrho^2 x_3, \qquad v_1 = x_4 + \varrho\, x_5 + \varrho^2 x_6,$$
$$u_2 = x_1 + \varrho^2 x_2 + \varrho\, x_3, \qquad v_2 = x_4 + \varrho^2 x_5 + \varrho\, x_6,$$

so wird die Gruppen-Determinante

$$\begin{vmatrix} x_1 & x_3 & x_2 & x_4 & x_5 & x_6 \\ x_2 & x_1 & x_3 & x_5 & x_6 & x_4 \\ x_3 & x_2 & x_1 & x_6 & x_4 & x_5 \\ x_4 & x_5 & x_6 & x_1 & x_3 & x_2 \\ x_5 & x_6 & x_4 & x_2 & x_1 & x_3 \\ x_6 & x_4 & x_5 & x_3 & x_2 & x_1 \end{vmatrix} = (u + v)(u - v)(u_1 u_2 - v_1 v_2)^2$$

am kürzesten wohl durch Multiplication mit der Determinante

$$\left|\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \varrho & \varrho^2 & 1 & \varrho & \varrho^2 \\ 1 & \varrho^2 & \varrho & 1 & \varrho^2 & \varrho \\ \hline 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & \varrho & \varrho^2 & -1 & -\varrho & -\varrho^2 \\ 1 & \varrho^2 & \varrho & -1 & -\varrho^2 & -\varrho \end{array}\right| = 6^3 = 216.$$

Die Gruppe $1 + 2 + 3$ der Commutatoren hat den Index zwei, gleich der Anzahl der linearen Factoren.

Beispiel 2.

Bezeichnet man die Elemente $1, \varepsilon, \alpha, \alpha^{-1}, \beta, \beta^{-1}, \gamma, \gamma^{-1}$ der Quaternion-Gruppe Q mit 1, 2, 3, 4, 5, 6, 7, 8, so ist die entsprechende Gruppen-Determinante

$$\left|\begin{array}{cc|cc|cc|cc} x_1 & x_2 & x_4 & x_3 & x_6 & x_5 & x_8 & x_7 \\ x_2 & x_1 & x_3 & x_4 & x_5 & x_6 & x_7 & x_8 \\ \hline x_3 & x_4 & x_1 & x_2 & x_8 & x_7 & x_5 & x_6 \\ x_4 & x_3 & x_2 & x_1 & x_7 & x_8 & x_6 & x_5 \\ \hline x_5 & x_6 & x_7 & x_8 & x_1 & x_2 & x_4 & x_3 \\ x_6 & x_5 & x_8 & x_7 & x_2 & x_1 & x_3 & x_4 \\ \hline x_7 & x_8 & x_6 & x_5 & x_3 & x_4 & x_1 & x_2 \\ x_8 & x_7 & x_5 & x_6 & x_4 & x_3 & x_2 & x_1 \end{array}\right|$$

$$= \left|\begin{array}{cccc} u_1 & u_2 & u_3 & u_4 \\ u_2 & u_1 & u_4 & u_3 \\ u_3 & u_4 & u_1 & u_2 \\ u_4 & u_3 & u_2 & u_1 \end{array}\right| \times \left|\begin{array}{cccc} v_1 & -v_2 & -v_3 & -v_4 \\ v_2 & v_1 & -v_4 & v_3 \\ v_3 & v_4 & v_1 & -v_2 \\ v_4 & -v_3 & v_2 & v_1 \end{array}\right|$$

$$= \begin{cases} (u_1 + u_2 + u_3 + u_4)\,(u_1 + u_2 - u_3 - u_4)\,(u_1 - u_2 + \\ \quad + u_3 - u_4)(u_1 - u_2 - u_3 + u_4) \\ \quad \times (v_1^2 + v_2^2 + v_3^2 + v_4^2)^2, \end{cases}$$

wo

$$\begin{Bmatrix} u_1 \\ v_1 \end{Bmatrix} = x_1 \pm x_2, \quad \begin{Bmatrix} u_2 \\ v_2 \end{Bmatrix} = x_3 \pm x_4, \quad \begin{Bmatrix} u_3 \\ v_3 \end{Bmatrix} = x_5 \pm x_6, \quad \begin{Bmatrix} u_4 \\ v_4 \end{Bmatrix} = x_7 \pm x_8.$$

Die Anzahl vier der linearen Factoren ist zugleich der Index der Commutator-Gruppe $[2] = 1 + 2$. Die Quadratsumme $v_1^2 + v_2^2$

$+ v_3^2 + v_4^2$ hat mich damals sehr erfreut und dazu veranlasst, auch andere Gruppen-Determinanten in lineare Factoren mit übercomplexen Coefficienten zu zerlegen; dies gelingt zwar, aber herausgekommen ist dabei Nichts!

Mit dem Wunsche, dass diese immerhin merkwürdigen Erscheinungen Sie zu einer tieferen Ergründung reizen mögen, verbleibe ich ...

27. April 1896.

... Aber so viel sehe ich zu meiner unaussprechlichen Freude auch jetzt schon, dass Sie in raschem Siegeslaufe wahrhaft bewunderungswürdige Erfolge errungen haben, und wenn ich heute auch ausser Stande bin, über die Sache selbst zu schreiben, so will ich doch nicht länger zögern, Ihnen meine herzlichsten Glückwünsche zu diesen Erfolgen zu senden, denen ich eine sehr hohe Bedeutung für die Gruppen-Theorie zuschreibe. Meine Bewunderung ist um so grösser, je aufrichtiger ich mir eingestehen muss, dass ich nimmermehr zu solchen Erfolgen hätte gelangen können, weil meiner gar zu einseitigen Bildung das erforderliche Rüstzeug fehlt, das Sie wie kein Anderer beherrschen. Ich würde daher auch Bedenken tragen, die beiliegenden Bogen Ihrer Einsicht zu unterbreiten, aber da Sie mich in einem Ihrer Briefe zur Mittheilung fernerer Beispiele von Gruppen-Determinanten aufgefordert haben, so sende ich Ihnen hierbei ein altes Beispiel 3. und ein daraus durch Verallgemeinerung kürzlich entstandenes Beispiel 4. auf die Gefahr hin, dass Sie über meine ungeübte Handhabung der Technik lächeln werden. Von der schon mehrmals erwähnten Zerlegung in hypercomplexe lineare Factoren, die, wie schwach sie mir augenblicklich auch erscheint, doch vielleicht den Keim von etwas Brauchbarem enthalten kann, werde ich mir ein anderes Mal zu schreiben erlauben, wenn mein Denken sich gebessert hat. ...

Gruppen-Determinanten.

Beispiel 3 (vom 17. Februar 1886).

Verallgemeinerung von Beispiel 1. — Es sei $\mathfrak{A}$ eine Abel'sche Gruppe von m Elementen

und es seien $$\alpha = 1, 2, 3 \cdots m,$$

$$\psi = \psi_1, \psi_2, \psi_3 \cdots \psi_m$$

die Charaktere von $\mathfrak{A}$ (Dirichlet, Aufl. 3, S. 581; Aufl. 4, S. 612); dieselben bilden eine (mit $\mathfrak{A}$ isomorphe) Gruppe in der Weise, dass je zwei solche ψ', ψ'' einen Charakter $\psi'\psi''$ erzeugen, welcher durch $\psi'\psi''(\alpha) = \psi'(\alpha)\psi''(\alpha)$ für alle α definirt ist; $\psi^{-1}(\alpha) = \psi(\alpha^{-1})$; $\psi\psi^{-1} = \psi^0$ ist der Haupt-Charakter, $\psi^0(\alpha) = 1$ für alle α und alle ψ. Die aus den m^2 Einheits-Wurzeln $\psi(\alpha)$ gebildete Determinante

$$\Psi = \begin{vmatrix} \psi_1(1) & \cdots & \psi_1(m) \\ \cdot & \cdots & \cdot \\ \psi_m(1) & \cdots & \psi_m(m) \end{vmatrix} = \pm\Psi' = \pm \begin{vmatrix} \psi_1^{-1}(1) & \cdots & \psi_1^{-1}(m) \\ \cdot & \cdots & \cdot \\ \psi_m^{-1}(1) & \cdots & \psi_m^{-1}(m) \end{vmatrix}$$

ist von Null verschieden; $\Psi\Psi' = m^m$. —

Nun bilde ich aus $\mathfrak{A}$ durch Hinzufügung eines Elementes zweiter Ordnung β, welches sich mit den α nach dem Gesetze

$$\beta\alpha = \alpha^{-1}\beta$$

verbindet, das System

$$\mathfrak{G} = \mathfrak{A} + \mathfrak{A}\beta,$$

welches, wie man leicht sieht (vergl. das folgende Beispiel 4), eine Gruppe ist (im Beispiel 1. war $m = 3$). Es soll die Determinante D dieser Gruppe $\mathfrak{G}$ gebildet werden, also eine Function von $2m$ Variabelen x_α, y_α, die resp. den Elementen α, $\alpha\beta$ entsprechen, nämlich

$$D = \begin{vmatrix} x_{11^{-1}} & \cdots & x_{m1^{-1}} & y_{11} & \cdots & y_{m1} \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ x_{1m^{-1}} & \cdots & x_{mm^{-1}} & y_{1m} & \cdots & y_{mm} \\ y_{11} & \cdots & y_{m1} & x_{11^{-1}} & \cdots & x_{m1^{-1}} \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ y_{1m} & \cdots & y_{mm} & x_{1m^{-1}} & \cdots & x_{mm^{-1}} \end{vmatrix}$$

Um sie umzuformen, multiplicire ich sie zeilenweise mit

$$\Psi\Psi' = \begin{vmatrix} \psi_1(1) & \cdots & \psi_1(m) & 0 & \cdots & 0 \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ \psi_m(1) & \cdots & \psi_m(m) & 0 & \cdots & 0 \\ 0 & \cdots & 0 & \psi_1^{-1}(1) & \cdots & \psi_1^{-1}(m) \\ \cdot & \cdots & \cdot & \cdot & \cdots & \cdot \\ 0 & \cdots & 0 & \psi_m^{-1}(1) & \cdots & \psi_m^{-1}(m) \end{vmatrix}$$

und zwar (wie immer im Folgenden) in der Weise, dass die Spalte des Productes durch die Zeile des Multiplicands D, die Zeile des

Productes durch die Zeile des Multiplicators $\Psi\Psi'$ bestimmt wird; führt man noch die Bezeichnungen

$$u_\mu = \sum^{\alpha} x_\alpha \psi_\mu(\alpha), \qquad v_\mu = \sum^{\alpha} y_\alpha \psi_\mu(\alpha),$$
$$u'_\mu = \sum^{\alpha} x_\alpha \psi_\mu^{-1}(\alpha), \qquad v'_\mu = \sum^{\alpha} y_\alpha \psi_\mu^{-1}(\alpha)$$

ein, so wird das Product

$$D_{\Psi\Psi'} = \left|\begin{array}{c|c} u_1\,\psi_1(1)\cdots u_1\,\psi_1(m) & v_1\,\psi_1^{-1}(1)\cdots v_1\,\psi_1^{-1}(m) \\ \cdots\cdots\cdots & \cdots\cdots\cdots \\ u_m\,\psi_m(1)\cdots u_m\,\psi_m(m) & v_m\,\psi_m^{-1}(1)\cdots v_m\,\psi_m^{-1}(m) \\ \hline v'_1\,\psi_1(1)\cdots v'_1\,\psi_1(m) & u'_1\,\psi_1^{-1}(1)\cdots u'_1\,\psi_1^{-1}(m) \\ \cdots\cdots\cdots & \cdots\cdots\cdots \\ v'_m\,\psi_m(1)\cdots v'_m\,\psi_m(m) & u'_m\,\psi_m^{-1}(1)\cdots u'_m\,\psi_m^{-1}(m) \end{array}\right|.$$

Diese Determinante ist aber zugleich das Product aus Multiplicand

$$\Psi_{\Psi'} = \left|\begin{array}{ccc|ccc} \psi_1(1) & \cdots & \psi_m(1) & 0 & \cdots & 0 \\ \cdots & & \cdots & \cdots & & \cdots \\ \psi_1(m) & \cdots & \psi_m(m) & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & \psi_1^{-1}(1) & \cdots & \psi_m^{-1}(1) \\ \cdots & & \cdots & \cdots & & \cdots \\ 0 & \cdots & 0 & \psi_1^{-1}(m) & \cdots & \psi_m^{-1}(m) \end{array}\right|$$

und Multiplicator

$$\prod^{\mu}(u_\mu u'_\mu - v_\mu v'_\mu) = \left|\begin{array}{ccc|ccc} u_1 & \cdots & 0 & v_1 & \cdots & 0 \\ \cdots & & \cdots & \cdots & & \cdots \\ 0 & \cdots & u_m & 0 & \cdots & v_m \\ \hline v'_1 & \cdots & 0 & u'_1 & \cdots & 0 \\ \cdots & & \cdots & \cdots & & \cdots \\ 0 & \cdots & v'_m & 0 & \cdots & u'_m \end{array}\right|.$$

Mithin ist unsere Gruppen-Determinante

$$D = \prod^{\mu}(u_\mu u'_\mu - v_\mu v'_\mu) = \prod^{\mu}\left|\begin{matrix} u_\mu, & v_\mu \\ v'_\mu, & u'_\mu \end{matrix}\right|$$

zunächst ein Product von m Factoren zweiten Grades. Bedeutet nun a die Anzahl der zweiseitigen (ambigen) Elemente $\alpha = \alpha^{-1}$ der Gruppe $\mathfrak{A}$, so ist $m = aa'$, wo a' die Anzahl aller verschiedenen

Quadrate α^2 bedeutet. Zugleich ist a die Anzahl aller zweiseitigen Charaktere $\psi = \psi^{-1}$; dies folgt unmittelbar aus der oben erwähnten Isomorphie der Gruppe $\mathfrak{A}$ mit der ihrer Charaktere, oder auch aus der Betrachtung der Gruppe $\mathfrak{A}'$ der a' Quadrate α^2, weil ihr Index $(\mathfrak{A}', \mathfrak{A}) = a$ nach einem allgemeinen Satz zugleich die Anzahl derjenigen Charaktere ψ von $\mathfrak{A}$ sein muß, welche den Haupt- (oder jeden anderen bestimmten) Charakter der Untergruppe $\mathfrak{A}'$ in sich schliessen, also die Eigenschaft $\psi(\alpha^2) = 1$, d. h. $\psi = \psi^{-1}$ haben. Für jeden zweiseitigen Charakter ψ_μ wird $u'_\mu = u_\mu$, $v'_\mu = v_\mu$, also $u_\mu u'_\mu - v_\mu v'_\mu = (u_\mu + v_\mu)(u_\mu - v_\mu)$, woraus $2a$ verschiedene lineare Factoren von D entspringen. Die übrigen $m - a$ Charaktere zerfallen in $\frac{1}{2}(m - a)$ Paare ψ_μ und $\psi_{\mu'} = \psi_\mu^{-1}$, und da $u_{\mu'} = u'_\mu$, $v_{\mu'} = v'_\mu$, $u'_{\mu'} = u_\mu$, $v'_{\mu'} = v_\mu$, so entspricht jedem Paar das Quadrat $(u_\mu u'_\mu - v_\mu v'_\mu)^2$ einer quadratischen Function, welche (im gewöhnlichen Sinne) unzerlegbar ist. Die Commutatoren von je zwei Elementen der Gruppe $\mathfrak{G}$ sind, wie man leicht findet, die a' Quadrate α^2; die von ihnen gebildete Gruppe $\mathfrak{A}'$ hat in $\mathfrak{G}$ den Index $(\mathfrak{A}', \mathfrak{G}) = (\mathfrak{A}', \mathfrak{A})(\mathfrak{A}, \mathfrak{G}) = 2a$, welcher mit der Anzahl der linearen Factoren von D übereinstimmt. —

Gruppen-Determinanten.

Beispiel 4 (vom 18. April 1896).

Verallgemeinerung von Beispiel 3. — Zu der Abel'schen Gruppe $\mathfrak{A}$ von m Elementen α (und m Charakteren ψ) lasse ich eine beliebige Gruppe $\mathfrak{B}$ von n Elementen β hinzutreten, welche sich mit jenen nach dem Gesetze

$$\beta\alpha = \alpha^{\beta'}\beta \tag{1}$$

verbinden, unter der Annahme, dass die den n Elementen β entsprechenden n Exponenten β' relative Primzahlen zu m sind und dem Gesetze

$$(\beta_1\beta_2)' \equiv \beta'_1\beta'_2 \pmod{m} \tag{2}$$

genügen. Ich nehme ferner an, dass $\mathfrak{A}$ und $\mathfrak{B}$ nur das Haupt-Element $\alpha^0 = \beta^0$ gemeinsam haben; dann bildet der aus mn verschiedenen Elementen $\alpha\beta$ bestehende Complex

$$\mathfrak{G} = \mathfrak{A}\mathfrak{B} \tag{3}$$

eine Gruppe. Dies ergiebt sich am deutlichsten, wenn man die Gruppen $\mathfrak{A}, \mathfrak{B}$ zunächst ganz getrennt betrachtet und jeder Combination

eines Elementes α von $\mathfrak{A}$ mit einem Elemente β von $\mathfrak{B}$ ein etwa mit (α, β) zu bezeichnendes Element eines neuen Systems $\mathfrak{G}$ entsprechen läßt, mit der Bedingung, daß diese mn Elemente (α, β) alle von einander verschieden sein sollen (der Einfachheit wegen); die Composition dieser Elemente definire man durch

$$(4) \qquad (\alpha_1, \beta_1)(\alpha_2, \beta_2) = (\alpha_1 \alpha_2^{\beta_1'}, \beta_1 \beta_2),$$

so ist $\mathfrak{G}$ wirklich eine Gruppe. Denn erstens gehorcht diese Composition (4) zufolge (2) dem associativen Gesetz; zweitens ist

$$(5) \qquad (\alpha^0, \beta^0)(\alpha, \beta) = (\alpha, \beta)(\alpha^0, \beta^0) = (\alpha, \beta),$$

weil $(\beta^0)' \equiv 1 \pmod{m}$; definirt man ferner die n Zahlen β'' durch

$$(6) \qquad \beta' \beta'' \equiv 1 \pmod{m},$$

woraus auch

$$(7) \qquad (\beta_1 \beta_2)'' \equiv \beta_1'' \beta_2'' \pmod{m}$$

folgt, so ist drittens

$$(8) \qquad (\alpha, \beta)(\alpha^{-\beta''}, \beta^{-1}) = (\alpha^{-\beta''}, \beta^{-1})(\alpha, \beta) = (\alpha^0, \beta^0).$$

Hiermit ist die Gruppen-Eigenschaft von $\mathfrak{G}$ bekanntlich erwiesen, und man kann

$$(9) \qquad (\alpha, \beta)^0 = (\alpha^0, \beta^0), \qquad (\alpha, \beta)^{-1} = (\alpha^{-\beta''}, \beta^{-1})$$

setzen. Zufolge (4) ist nun

$$(10) \qquad (\alpha, \beta) = (\alpha, \beta^0)(\alpha^0, \beta),$$

$$(11) \qquad (\alpha_1, \beta^0)(\alpha_2, \beta^0) = (\alpha_1 \alpha_2, \beta^0),$$

$$(12) \qquad (\alpha^0, \beta_1)(\alpha^0, \beta_2) = (\alpha^0, \beta_1 \beta_2).$$

Es giebt also in $\mathfrak{G}$ eine mit $\mathfrak{A}$ isomorphe Abel'sche Gruppe von m Elementen (α, β^0), und eine mit $\mathfrak{B}$ isomorphe Gruppe von n Elementen (α^0, β), und zufolge (10) ist $\mathfrak{G}$ das Product aus diesen beiden Gruppen, welche nur das Haupt-Element (α^0, β^0) gemeinsam haben; hieraus folgt die Berechtigung, in $\mathfrak{G}$ jedes Element (α, β^0) kurz durch α, jedes Element (α^0, β) kurz durch β zu bezeichnen, woraus dann $\alpha^0 = \beta^0$ und $(\alpha, \beta) = \alpha\beta$, $\mathfrak{G} = \mathfrak{A}\mathfrak{B}$ folgt. Die Composition (4) lautet

$$\alpha_1 \beta_1 \alpha_2 \beta_2 = \alpha_1 \alpha_2^{\beta_1'} \beta_1 \beta_2,$$

worin (1) enthalten ist. (In diesem Winter habe ich mich mit viel allgemeineren Zusammensetzungen von zwei Gruppen $\mathfrak{A}$, $\mathfrak{B}$ zu einer Product-Gruppe $\mathfrak{A}\mathfrak{B}$ beschäftigt). —

Bezeichnet man nun der Einfachheit halber die dem Elemente $\alpha\beta$ entsprechende Variabele der Gruppen-Determinante D selbst mit $\alpha\beta$ (statt mit $x_{\alpha\beta}$), und ordnet die letztere in n^2 Felder von je m^2 Elementen, so wird

$$D = \left|\begin{array}{ccc|c|ccc} \cdots(\alpha\beta_1)(\alpha_1\ \beta_1)^{-1}\cdots & & & \cdots & & \cdots(\alpha\beta_n)(\alpha_1\ \beta_1)^{-1}\cdots \\ \cdots\cdots\cdots & & & \cdots & & \cdots\cdots\cdots \\ \cdots(\alpha\beta_1)(\alpha_m\ \beta_1)^{-1}\cdots & & & \cdots & & \cdots(\alpha\beta_n)(\alpha_m\ \beta_1)^{-1}\cdots \\ \hline \cdots\cdots\cdots & & & \cdots & & \cdots\cdots\cdots \\ \hline \cdots(\alpha\beta_1)(\alpha_1\ \beta_n)^{-1}\cdots & & & \cdots & & \cdots(\alpha\beta_n)(\alpha_1\ \beta_n)^{-1}\cdots \\ \cdots\cdots\cdots & & & \cdots & & \cdots\cdots\cdots \\ \cdots(\alpha\beta_1)(\alpha_m\beta_n)^{-1}\cdots & & & \cdots & & \cdots(\alpha\beta_n)(\alpha_m\beta_n)^{-1}\cdots \end{array}\right|,$$

wo α in jeder Zeile jedes Feldes alle m Elemente $\alpha_1, \alpha_2 \cdots \alpha_m$ von $\mathfrak{A}$ in derselben Ordnung durchläuft. Nun bilde ich aus jedem Charakter ψ von $\mathfrak{A}$ und jedem Element β von $\mathfrak{B}$ die lineare Function von m Variabelen

$$(\beta,\ \psi) = \sum_{\alpha}^{\alpha} (\alpha\beta)\,\psi(\alpha);$$

die Charakter-Potenzen $\psi^{\beta''}$ sind ebenfalls Charaktere ψ, und man erhält

$$\sum_{\alpha}^{\alpha} (\alpha\beta)(\alpha_\mu\beta_\nu)^{-1}\psi^{\beta''}(\alpha) = \sum_{\alpha}^{\alpha} (\alpha\beta\beta_\nu^{-1}\alpha_\mu^{-1})\,\psi^{\beta''}(\alpha)$$

$$= \sum_{\alpha}^{\alpha} (\alpha\alpha_\mu^{-\beta'\beta''}\beta\beta_\nu^{-1})\,\psi^{\beta''}(\alpha) = \sum_{\alpha}^{\alpha} (\alpha\beta\beta_\nu^{-1})\,\psi^{\beta'}(\alpha\alpha_\mu^{\beta'\beta''})$$

$$= (\beta\beta_\nu^{-1},\ \psi^{\beta''})\,\psi^{\beta'\beta''_\nu}(\alpha_\mu).$$

Multiplicirt man daher (wie im Beispiel 3) den Multiplicand D mit dem Multiplicator

$$\pm\mathfrak{P}^n = \left|\begin{array}{ccc|ccc|ccc} \cdots\psi_1^{\beta''_1}(\alpha)\cdots & & & 0 & \cdot & 0 & 0 & \cdots & 0 \\ \cdots\cdots\cdots & & & \cdots & & & \cdots\cdots\cdots & & \\ \cdots\psi_m^{\beta''_1}(\alpha)\cdots & & & 0 & \cdot & 0 & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & & & & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & 0 & \cdot & 0 & \cdots\psi_1^{\beta''_n}(\alpha)\cdots & & \\ \cdots\cdots\cdots & & & \cdots & & & \cdots\cdots\cdots & & \\ 0 & \cdots & 0 & 0 & \cdot & 0 & \cdots\psi_m^{\beta''_n}(\alpha)\cdots & & \end{array}\right|,$$

so erhält man

$$\pm D\Psi^n = \begin{vmatrix} \cdots (\beta_1\beta_1^{-1}, \psi_1^{\beta_1''})\,\psi_1^{\beta_1''}(\alpha)\cdots & \cdots & \cdots (\beta_1\beta_n^{-1}, \psi_1^{\beta_1''})\,\psi_1^{\beta_n''}(\alpha)\cdots \\ \cdots\cdots\cdots\cdots & \cdots & \cdots\cdots\cdots\cdots \\ \cdots (\beta_1\beta_1^{-1}, \psi_m^{\beta_1''})\,\psi_m^{\beta_1''}(\alpha)\cdots & \cdots & \cdots (\beta_1\beta_n^{-1}, \psi_m^{\beta_1''})\,\psi_m^{\beta_n''}(\alpha)\cdots \\ \cdots\cdots\cdots\cdots & \cdots & \cdots\cdots\cdots\cdots \\ \cdots (\beta_n\beta_1^{-1}, \psi_1^{\beta_n''})\,\psi_1^{\beta_1''}(\alpha)\cdots & \cdots & \cdots (\beta_n\beta_n^{-1}, \psi_1^{\beta_n''})\,\psi_1^{\beta_n''}(\alpha)\cdots \\ \cdots\cdots\cdots\cdots & \cdots & \cdots\cdots\cdots\cdots \\ \cdots (\beta_n\beta_1^{-1}, \psi_m^{\beta_n''})\,\psi_m^{\beta_1''}(\alpha)\cdots & \cdots & \cdots (\beta_n\beta_n^{-1}, \psi_m^{\beta_n''})\,\psi_m^{\beta_n''}(\alpha)\cdots \end{vmatrix}.$$

Dies ist wieder das Product aus dem Multiplicand

$$\pm\Psi^n = \begin{vmatrix} \psi_1^{\beta_1''}(\alpha_1)\cdots\psi_m^{\beta_1''}(\alpha_1) & 0\cdots 0 & 0\cdots 0 \\ \cdots\cdots\cdots & \cdots\cdots & \cdots\cdots\cdots \\ \psi_1^{\beta_1''}(\alpha_m)\cdots\psi_m^{\beta_1''}(\alpha_m) & 0\cdots 0 & 0\cdots 0 \\ 0\cdots 0 & \cdots\cdots & 0\cdots 0 \\ 0\cdots 0 & 0\cdots 0 & \psi_1^{\beta_n''}(\alpha_1)\cdots\psi_m^{\beta_n''}(\alpha_1) \\ \cdots\cdots\cdots & \cdots\cdots & \cdots\cdots\cdots \\ 0\cdots 0 & 0\cdots 0 & \psi_1^{\beta_n''}(\alpha_m)\cdots\psi_m^{\beta_n''}(\alpha_m) \end{vmatrix}$$

und dem Multiplicator

$$\begin{vmatrix} (\beta_1\beta_1^{-1}, \psi_1^{\beta_1''})\cdots 0 & \cdots & (\beta_1\beta_n^{-1}, \psi_1^{\beta_1''})\cdots 0 \\ \cdots\cdots\cdots & \cdots & \cdots\cdots\cdots \\ 0\cdots(\beta_1\beta_1^{-1}, \psi_m^{\beta_1''}) & \cdots & 0\cdots(\beta_1\beta_n^{-1}, \psi_m^{\beta_1''}) \\ \cdots\cdots\cdots & \cdots & \cdots\cdots\cdots \\ (\beta_n\beta_1^{-1}, \psi_1^{\beta_n''})\cdots 0 & \cdots & (\beta_n\beta_n^{-1}, \psi_1^{\beta_n''})\cdots 0 \\ \cdots\cdots\cdots & \cdots & \cdots\cdots\cdots \\ 0\cdots(\beta_n\beta_1^{-1}, \psi_m^{\beta_n''}) & \cdots & 0\cdots(\beta_n\beta_n^{-1}, \psi_m^{\beta_n''}) \end{vmatrix},$$

welcher folglich $= D$ ist. Mithin ergiebt sich, wenn

$$D_\psi = \begin{vmatrix} (\beta_1\beta_1^{-1}, \psi^{\beta_1''})\cdots(\beta_1\beta_n^{-1}, \psi^{\beta_1''}) \\ \cdots\cdots\cdots\cdots \\ (\beta_n\beta_1^{-1}, \psi^{\beta_n''})\cdots(\beta_n\beta_n^{-1}, \psi^{\beta_n''}) \end{vmatrix}$$

gesetzt wird, unsere Gruppen-Determinante

$$D = \prod_{\psi} D_{\psi}$$

als Product von m Factoren n^{ten} Grades. —

Jeder Commutator der Gruppe $\mathfrak{B}$, d. h. jedes Element von der Form

$$\gamma = \beta_1^{-1}\beta_2^{-1}\beta_1\beta_2$$

ist permutabel mit jedem Element α von $\mathfrak{A}$, weil

$$\gamma' \equiv \beta_1''\beta_2''\beta_1'\beta_2' \equiv 1 \pmod{m},$$

also $\gamma\alpha = \alpha^{\gamma'}\gamma = \alpha\gamma$. Die von allen diesen Commutatoren γ erzeugte Gruppe sei $\mathfrak{C}$. Unter den Commutatoren der Product-Gruppe $\mathfrak{G} = \mathfrak{A}\mathfrak{B}$ sind zunächst die folgenden

$$\beta^{-1}\alpha^{-1}\beta\alpha = \alpha^{1-\beta''}$$

zu bemerken; bedeutet e den grössten gemeinsamen Theiler aller n Zahlen $1-\beta''$ oder $1-\beta'$ mit m (oder mit dem höchsten Element-Grade in $\mathfrak{A}$), so bilden diese Commutatoren die Gruppe $\mathfrak{A}'$ aller a' verschiedenen Potenzen α^e, und es ist $m = aa'$, wo $a = (\mathfrak{A}', \mathfrak{A})$ die Anzahl aller e-seitigen, d. h. derjenigen Elemente α bedeutet, welche der Bedingung $\alpha^e = \alpha^0$ genügen; da jedem Charakter χ der Gruppe $\mathfrak{A}'$, z. B. ihrem Hauptcharakter genau a Charaktere ψ der Gruppe $\mathfrak{A}$ entsprechen, welche Multipla von χ sind oder χ einschliessen, d. h. für alle Elemente von $\mathfrak{A}'$ mit χ übereinstimmen, so ist a auch die Anzahl aller e-seitigen Charaktere $\psi = \psi^{\beta'} = \psi^{\beta''}$ von $\mathfrak{A}$, was auch aus der Isomorphie von $\mathfrak{A}$ mit der Charakter-Gruppe folgen würde. Da ferner jeder beliebige Commutator der Gruppe $\mathfrak{G}$ von der Form

$$(\alpha_1\beta_1)^{-1}(\alpha_2\beta_2)^{-1}(\alpha_1\beta_1)(\alpha_2\beta_2)$$
$$= \alpha_1^{\beta_1''(\beta_2''-1)}\alpha_2^{\beta_2''(1-\beta_1'')}\cdot\beta_1^{-1}\beta_2^{-1}\beta_1\beta_2 = \alpha^e\gamma$$

ist, so erzeugen alle diese Commutatoren die Gruppe $\mathfrak{A}'\mathfrak{C}$, deren Index $(\mathfrak{A}'\mathfrak{C}, \mathfrak{A}\mathfrak{B}) = (\mathfrak{A}'\mathfrak{C}, \mathfrak{A}\mathfrak{C})(\mathfrak{A}\mathfrak{C}, \mathfrak{A}\mathfrak{B}) = a(\mathfrak{C}, \mathfrak{B})$ ist. Wenn nun ψ ein e-seitiger Charakter ist, so geht der ihm entsprechende Factor

$$D_{\psi} = \begin{vmatrix} (\beta_1\beta_1^{-1}, \psi) & \cdots & (\beta_n\beta_1^{-1}, \psi) \\ \cdot & \cdots & \cdot \\ (\beta_1\beta_n^{-1}, \psi) & \cdots & (\beta_n\beta_n^{-1}, \psi) \end{vmatrix},$$

von D aus der Determinante

$$\begin{vmatrix} y_{\beta_1\beta_1^{-1}} & \cdots & y_{\beta_n\beta_1^{-1}} \\ \cdot & \cdots & \cdot \\ y_{\beta_1\beta_n^{-1}} & \cdots & y_{\beta_n\beta_n^{-1}} \end{vmatrix}$$

der Gruppe $\mathfrak{B}$ offenbar durch die lineare Transformation $y_\beta = (\beta, \psi)$ hervor und enthält folglich dieselbe Anzahl linearer Factoren. Aber mehr kann man auf diese Weise wohl nicht schliessen.

8. Juli 1896*).

. . . Nochmals bitte ich sehr um Entschuldigung für meine Saumseligkeit, für die ich nur wenige gute, aber viele schlechte Gründe angeben könnte; zu den letzteren gehört meine tadelnswerthe Schwäche, mich oft von Nebenfragen, die für die Hauptsache einer Untersuchung ganz werthlos sind, so gefangen nehmen zu lassen, dass ich darüber das eigentliche Ziel aus den Augen verliere. Zu den guten Gründen darf ich wohl den rechnen, dass ich in Folge Ihrer Anregung meine Papiere vom Februar 1886 über Gruppen-Determinanten und deren hypercomplexe lineare Factoren wieder durchstöbert habe.

Auf Ihre Frage, wann ich den allgemeinen Satz über die Zerlegung der Abel'schen Gruppen-Determinanten in lineare Charakter-Factoren gefunden habe, geben diese Papiere (12 Folioseiten vom 2. bis 17. Februar datirt, mit Formeln und nur wenigen Worten)**) nur den Aufschluss, dass dies schon in früherer Zeit geschehen sein muss. Sie behandeln nämlich (mit einer einzigen Ausnahme) nur noch Beispiele von nicht Abel'schen Gruppen, unter denen das vom 17. Februar 1886, welches ich Ihnen im April d. J. mitgetheilt habe, eine Gruppe $\mathfrak{G}$ betrifft, in der die allgemeinste Abel'sche Gruppe $\mathfrak{A}$ als Theiler enthalten ist; hierin steckt natürlich auch der obige Satz A über die Abel'schen Gruppen $\mathfrak{A}$, und die ganze Behandlung der Determinante von $\mathfrak{G}$ ist offenbar derjenigen nachgebildet, welche zur Zerlegung der Determinante von $\mathfrak{A}$, also zu dem Satze A führt; aber dieser Satz A wird nirgends mehr erwähnt. Auf den Begriff der allgemeinen Gruppen-Determinante bin ich zuerst bei dem Studium der Discriminante eines beliebigen Normalkörpers Ω geführt, indem ich solche (sehr nützliche) Basen von Ω betrachtete, die aus den Conjugirten einer einzigen Zahl ω bestehen (bisweilen besitzt auch das System o aller ganzen Zahlen in Ω eine solche Basis, z. B. wenn ω eine m^{te} Einheits-Wurzel, und m durch kein Quadrat theil-

*) [Ein Auszug aus diesem Brief findet sich in der Einleitung der Arbeit über Gruppencharaktere von Frobenius. E. N.]

**) [Dem Inhalt nach vollständig in den hier veröffentlichten Briefen enthalten. E. N.]

bar ist, und dasselbe gilt dann auch von allen Divisoren von Ω, z. B. allen quadratischen Körpern von ungerader Grundzahl); dieses Studium fällt wahrscheinlich in die Zeit um 1880 oder noch früher, und damals werde ich wohl den Satz A gefunden haben; was mich aber veranlasst hat, im Februar 1886 auf die Gruppen-Determinanten zurückzukommen, weiss ich nicht mehr.

Ich füge einige Bemerkungen über die Charaktere der Abel'schen Gruppen $\mathfrak{A}$ hinzu. Das älteste Beispiel ihrer Anwendung ist wohl in den Resolventen von Lagrange (für cyklische $\mathfrak{A}$) zu erkennen. Sodann ist das (von Jacobi verallgemeinerte) Symbol von Legendre zu nennen. Die von Gauss (Art. 131) benutzten Zeichen R, N sind weniger glücklich, als die bestimmte Einführung der Einheits-Wurzeln ± 1 durch Legendre, und so kommt es (Art. 230), dass er auch unter dem Charakter einer Formen-Classe oder eines Geschlechtes eine Relation, nicht eine Zahl versteht; die der Zusammensetzung der Geschlechter entsprechende Zusammensetzung der Charaktere tritt zwar deutlich hervor (Art. 246—248), aber nicht als Multiplication von Zahlen. Die Umwandlung der Gauss'schen Geschlechts-Charaktere in Zahlen hat Dirichlet (Recherches sur diverses applications etc. §. 3) durch Benutzung des Symbols von Legendre bewirkt. Ferner hat Dirichlet in der Abhandlung über die arithmetische Progression alle Charaktere ψ (— ohne diesen Namen zu gebrauchen —) der Abel'schen Gruppe $G^{(m)}$ benutzt, welche von den $\varphi(m)$ Classen relativer Primzahlen zu m gebildet wird, und ebenso alle Charaktere der Gruppe der Formen-Classen (in der Skizze über die Darstellung unendlich vieler Primzahlen durch eine quadratische Form). Nach allem diesen lag es nahe, den Begriff und Namen der Charaktere für jede Abel'sche Gruppe $\mathfrak{A}$ einzuführen, wie ich es in der dritten Auflage von Dirichlet's Zahlentheorie gethan habe. Ich habe dort (in der vierten Auflage S. 612) zur Begründung der Existenz der Charaktere auf §. 149, also auf die Darstellung der Elemente von $\mathfrak{A}$ als Producte von Potenzen von Fundamental-Elementen hingedeutet; doch ziehe ich principiell den folgenden Weg vor, der Nichts von dieser Darstellung voraussetzt. Ist $\mathfrak{A}$ ein Theiler von $\mathfrak{B}$, so ist in jedem Charakter χ von $\mathfrak{B}$ ein Charakter ψ von $\mathfrak{A}$ enthalten (der für alle Elemente von $\mathfrak{A}$ mit χ übereinstimmt); ich nenne ψ den auf $\mathfrak{A}$ bezüglichen Divisor von χ, umgekehrt χ ein Multiplum von ψ. Dann ergiebt sich ganz leicht durch Induction

der Satz: Ist ψ ein Charakter von $\mathfrak{A}$, so ist der Index $(\mathfrak{A}, \mathfrak{B})$ [— mit $(\mathfrak{A}, \mathfrak{B})$ bezeichne ich auch in der allgemeinen Gruppen-Theorie die Anzahl der verschiedenen Complexe $\mathfrak{A}\beta$, aus denen der Complex $\mathfrak{A}\mathfrak{B}$ besteht —] zugleich die genaue Anzahl der verschiedenen Charaktere χ von $\mathfrak{B}$, welche Multipla von ψ sind. Dies leuchtet ein für $(\mathfrak{A}, \mathfrak{B}) = 1$, also $\mathfrak{A} = \mathfrak{B}$, und wenn es für alle Fälle $(\mathfrak{A}, \mathfrak{B}) < m$ bewiesen ist, so gilt es auch für $(\mathfrak{A}, \mathfrak{B}) = m$; denn entweder giebt es eine von $\mathfrak{A}$ und $\mathfrak{B}$ verschiedene Gruppe $\mathfrak{C}$, die Theiler von $\mathfrak{B}$ und Vielfaches von $\mathfrak{A}$ ist, oder nicht; in beiden Fällen ergiebt sich der Schluss leicht, weil im ersten Fall $m = (\mathfrak{A}, \mathfrak{B}) = (\mathfrak{A}, \mathfrak{C})(\mathfrak{C}, \mathfrak{B})$, also $(\mathfrak{A}, \mathfrak{C})$ und $(\mathfrak{C}, \mathfrak{B}) < m$ ist, und weil im zweiten Falle $\mathfrak{B} = \mathfrak{A} + \mathfrak{A}\beta + \mathfrak{A}\beta^2 + \cdots$ ist. Hierin ist aber Alles über Existenz und Anzahl der Charaktere enthalten, und der Satz ist ausserdem sehr nützlich.

Die Art, wie Dirichlet (bei der arithmetischen Progression) darthut, dass seine Reihen L_2 der zweiten Art von Null verschiedene Grenzwerthe haben, weil diese als Factoren der Classen-Anzahl der quadratischen Formen auftreten, führte mich, da ich die quadratischen Körper als Kreiskörper kannte, zu der Bemerkung (Aufl. 3, S. 596 und Aufl. 4, S. 625), dass eine ähnliche Schlussart auch für die Reihen L_3 der dritten Art gilt; denn wenn man den aus den m^{ten} Einheits-Wurzeln gebildeten Kreiskörper K_m betrachtet, und Kummer's Satz über dessen Primideale anwendet, so ist das Product aller $\varphi(m)$ Dirichlet'schen Reihen L identisch mit der Summe $\sum N(\mathfrak{a})^{-s}$, wo $\mathfrak{a}$ alle relativen Primideale zu m durchläuft. Ich weiss nicht, ob Kummer selbst diese Anwendung ausgesprochen hat, glaube es aber kaum.

Da Sie bei Ihrer Frage nach der Auffindungs-Zeit des obigen Satzes A die Classen-Anzahl der Ideale in einem beliebigen Kreiskörper erwähnen, so möchte ich Ihnen (wie neulich auch Weber) noch von einer schönen Sparsamkeit schreiben*), auf die Gefahr hin, dass dieselbe Ihnen, wie mir, schon lange bekannt ist. Die Identität

$$(1) \qquad \sum^{\mathfrak{a}} N(\mathfrak{a})^{-s} = \prod^{\psi} \sum^{n} \psi(n) n^{-s}$$

gilt nämlich auch dann, wenn $\mathfrak{a}$ alle Ideale in K_m, und n alle natürlichen Zahlen durchläuft, falls jeder der $\varphi(m)$ Charaktere ψ der

*) [Vergl. XLI.]

Gruppe $G^{(m)}$ eine erweiterte Bedeutung erhält, so dass ψ für jede ganze rationale Zahl x einen bestimmten Werth $\psi(x)$ annimmt, der mit dem ursprünglichen $\psi(x)$ übereinstimmt, wenn x relative Primzahl zu m ist, und ausserdem die Gesetze $\psi(x+m) = \psi(x)$ und $\psi(xy) = \psi(x)\psi(y)$ erfüllt. Eine solche Erweiterung eines gegebenen Charakters ψ von $G^{(m)}$ lässt sich im Allgemeinen auf mehrere Arten herstellen (deren Anzahl eine Potenz von 2 ist); von diesen genügt aber nur eine einzige der obigen Ideal-Identität (1), und zwar ist sie dadurch vollkommen bestimmt, daß $\psi(x)$ für möglichst wenige Zahlen x verschwinden soll. Einen so erweiterten Charakter ψ nenne ich einen natürlichen Charakter von $G^{(m)}$. Die oben gerühmte Sparsamkeit besteht nun zunächst darin, dass, wenn a ein Divisor von m, alle $\varphi(a)$ natürlichen Charaktere von $G^{(a)}$ auch natürliche Charaktere von $G^{(m)}$ sind; bezeichnet man daher mit $\varphi'(m)$ die Anzahl aller primitiven, nämlich derjenigen natürlichen Charaktere von $G^{(m)}$, welche zu keiner Gruppe $G^{(a)}$ mit kleinerem a gehören, so ist

$$\sum \varphi'(a) = \varphi(m); \tag{2}$$

mithin ist $\varphi'(ab) = \varphi'(a)\varphi'(b)$, wenn a, b relative Primzahlen sind, und für eine Primzahl p ist $\varphi'(p) = p-2$ und $\varphi'(p^n) = (p-1)^2 p^{n-2}$, falls $n > 1$; ferner ist $\varphi'(2m) = 0$, wenn m ungerade (es ist ja auch $K_{2m} = K_m$). Am schönsten offenbart sich aber die Sparsamkeit dadurch, dass die Identität (1) im folgenden Sinne für jeden Kreiskörper Ω gilt. Hat man m so gewählt, dass Ω Divisor von K_m wird, und ist H die Gruppe der Zahlclassen h (mod. m), zu welcher Ω gehört, also H Theiler von $G^{(m)}$, so gilt die Identität (1), wenn $\mathfrak{a}$ alle Ideale in Ω, und ψ alle diejenigen natürlichen Charaktere von $G^{(m)}$ durchläuft, welche der Bedingung $\psi(h) = 1$ genügen (alle Multipla des Haupt-Charakters von H); dies ist gewissermassen der analytische Ausdruck für meinen allgemeinen Satz über die Primideale von Ω (C. R. der Pariser Akademie vom 24. Mai 1880). —

Zu einem gründlichen Studium Ihrer Abhandlung „Über vertauschbare Matrizen“ bin ich aus den oben erwähnten schlechten Gründen noch nicht gekommen; doch glaube ich versichern zu können, dass ich auch bei meinen nach 1887 gelegentlich wieder aufgenommenen Versuchen, die Zerlegung in lineare Factoren auf einfachere Weise abzuleiten, durchaus nicht auf Ihre Wege gekommen bin. Doch

muthet mich Manches darin ähnlich an, wie meine übercomplexen Factoren der Gruppen-Determinanten, auf die ich aber heute nicht mehr eingehen kann. Vielleicht komme ich morgen dazu, die Armada dieser seltsamen Schiffe in See stechen zu lassen; doch wird es wohl heissen: Frobenius afflavit et dissipavit! ...

13. Juli 1896.

... Zuerst erwähne ich, dass mein Beispiel vom 17. Februar 1886 vollständiger und hübscher in der Gestalt $AB = BC$ dargestellt wird, wo A, B, C nicht Determinanten, sondern folgende Systeme, Matrizen, Formen bedeuten:

$$\left\{\begin{array}{c|c} x_{11^{-1}} \cdots x_{m1^{-1}} & y_{11} \cdots y_{m1} \\ \cdots\cdots\cdots & \cdots\cdots\cdots \\ x_{1m^{-1}} \cdots x_{mm^{-1}} & y_{1m} \cdots y_{mm} \\ \hline y_{11} \cdots y_{m1} & x_{11^{-1}} \cdots x_{m1^{-1}} \\ \cdots\cdots\cdots & \cdots\cdots\cdots \\ y_{1m} \cdots y_{mm} & x_{1m^{-1}} \cdots x_{mm^{-1}} \end{array}\right\} = A,$$

$$\left\{\begin{array}{c|c} \psi_1(1), 0 \cdots & \psi_m(1), 0 \\ \cdots\cdots & \cdots\cdots \\ \psi_1(m), 0 \cdots & \psi_m(m), 0 \\ \hline 0, \psi_1^{-1}(1) \cdots & 0, \psi_m^{-1}(1) \\ \cdots\cdots & \cdots\cdots \\ 0, \psi_1^{-1}(m) \cdots & 0, \psi_m^{-1}(m) \end{array}\right\} = B,$$

$$\left\{\begin{array}{cc|ccc|cc} u_1, & v_1' & 0 & \cdots & 0 & 0, & 0 \\ v_1, & u_1' & 0 & \cdots & 0 & 0, & 0 \\ \hline 0, & 0 & \cdot & \cdot & \cdot & 0, & 0 \\ \cdots & & \cdot & \cdot & \cdot & \cdots & \\ 0, & 0 & \cdot & \cdot & \cdot & 0, & 0 \\ \hline 0, & 0 & 0 & \cdots & 0 & u_m, & v_m' \\ 0, & 0 & 0 & \cdots & 0 & v_m, & u_m' \end{array}\right\} = C.$$

Hieraus folgt dann der Satz über die Zerlegung der Gruppen-Determinante D in die Factoren $u_\mu u_\mu' - v_\mu v_\mu'$. Doch das müssen Sie längst durchschaut haben. Im Folgenden beschäftige ich mich ausschliesslich mit dem ersten Beispiel (Fall $m = 3$) vom 2. und 3. Februar 1886; an diesem Beispiel habe ich damals auch zuerst die Zerlegung in hypercomplexe lineare Factoren ausgeführt, und

erst dieser Erfolg hat mich etwas später (jedenfalls vor dem 15. Februar) zu der Beschäftigung mit der Quaternion-Gruppe veranlasst; ich habe Ihnen, wie ich glaube, geschrieben, dass die Reihenfolge die umgekehrte gewesen ist; das war aber ein Irrthum. Nun also! Es war $1 + \varrho + \varrho^2 = 0$ und

$$\begin{vmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_3 & x_1 & x_2 & x_5 & x_6 & x_4 \\ x_2 & x_3 & x_1 & x_6 & x_4 & x_5 \\ x_4 & x_5 & x_6 & x_1 & x_2 & x_3 \\ x_5 & x_6 & x_4 & x_3 & x_1 & x_2 \\ x_6 & x_4 & x_5 & x_2 & x_3 & x_1 \end{vmatrix} = (u+v)(u-v)(u_1u_2 - v_1v_2)^2.$$

$$u = x_1 + x_2 + x_3, \quad u_1 = x_1 + \varrho x_2 + \varrho^2 x_3, \quad u_2 = x_1 + \varrho^2 x_2 + \varrho x_3,$$
$$v = x_4 + x_5 + x_6, \quad v_1 = x_4 + \varrho x_5 + \varrho^2 x_6, \quad v_2 = x_4 + \varrho^2 x_5 + \varrho x_6,$$

also

$$u_1u_2 = x_1^2 + x_2^2 + x_3^2 - x_1x_2 - x_1x_3 - x_2x_3,$$
$$v_1v_2 = x_4^2 + x_5^2 + x_6^2 - x_4x_5 - x_4x_6 - x_5x_6.$$

Nun sei

$$u_1u_2 - v_1v_2 = \alpha\beta,$$
$$\alpha = \alpha_1x_1 + \alpha_2x_2 + \alpha_3x_3 + \alpha_4x_4 + \alpha_5x_5 + \alpha_6x_6,$$
$$\beta = \beta_1x_1 + \beta_2x_2 + \beta_3x_3 + \beta_4x_4 + \beta_5x_5 + \beta_6x_6.$$

Bei der Addition, Subtraction, Multiplication rechne ich mit den 12 Coefficienten α_r, β_r wie mit gewöhnlichen Zahlen und verzichte nur bei ihrer Multiplication mit einander auf das commutative Gesetz, während dasselbe bei ihrer Multiplication mit gewöhnlichen Zahlen und den Variabelen x_r bestehen bleiben soll. Ebenso wird durchweg das associative und distributive Gesetz angenommen. Die Forderung der Identität der Coefficienten (rs) von x_rx_s in $u_1u_2 - v_1v_2$ und in $\alpha\beta$ ergiebt dann 21 Bedingungen; um mit ihnen etwas anfangen zu können, setze ich (wenn dadurch auch die Allgemeinheit beeinträchtigt wird)

(A) $$\alpha_1 = 1, \quad \beta_1 = 1,$$

wodurch die Forderung $(11) = \alpha_1\beta_1 = 1$ erfüllt ist. Dann folgt:

(B)
$$\begin{cases} (12) = \alpha_2 + \beta_2 = -1, & \beta_2 = -1 - \alpha_2, \\ (13) = \alpha_3 + \beta_3 = -1, & \beta_3 = -1 - \alpha_3, \\ (14) = \alpha_4 + \beta_4 = 0, & \beta_4 = -\alpha_4, \\ (15) = \alpha_5 + \beta_5 = 0, & \beta_5 = -\alpha_5, \\ (16) = \alpha_6 + \beta_6 = 0, & \beta_6 = -\alpha_6, \end{cases}$$

sodann

$$(C)\quad \begin{cases} (22) = \alpha_2\beta_2 = 1, & \alpha_2^2 = -1-\alpha_2, \\ (33) = \alpha_3\beta_3 = 1, & \alpha_3^2 = -1-\alpha_3, \\ (23) = \alpha_2\beta_3+\alpha_3\beta_2 = -1, & \alpha_2\alpha_3+\alpha_3\alpha_2 = +1-\alpha_2-\alpha_3, \end{cases}$$

ferner

$$(D)\quad \begin{cases} (44) = \alpha_4\beta_4 = -1, & \alpha_4^2 = 1, \\ (55) = \alpha_5\beta_5 = -1, & \alpha_5^2 = 1, \\ (66) = \alpha_6\beta_6 = -1, & \alpha_6^2 = 1, \\ (45) = \alpha_4\beta_5+\alpha_5\beta_4 = 1, & \alpha_4\alpha_5+\alpha_5\alpha_4 = -1, \\ (46) = \alpha_4\beta_6+\alpha_6\beta_4 = 1, & \alpha_4\alpha_6+\alpha_6\alpha_4 = -1, \\ (56) = \alpha_5\beta_6+\alpha_6\beta_5 = 1, & \alpha_5\alpha_6+\alpha_6\alpha_5 = -1, \end{cases}$$

endlich

$$(E)\quad \begin{cases} (24) = \alpha_2\beta_4+\alpha_4\beta_2 = 0, & \alpha_2\alpha_4+\alpha_4\alpha_2 = -\alpha_4, \\ (34) = \alpha_3\beta_4+\alpha_4\beta_3 = 0, & \alpha_3\alpha_4+\alpha_4\alpha_3 = -\alpha_4, \\ (25) = \alpha_2\beta_5+\alpha_5\beta_2 = 0, & \alpha_2\alpha_5+\alpha_5\alpha_2 = -\alpha_5, \\ (35) = \alpha_3\beta_5+\alpha_5\beta_3 = 0, & \alpha_3\alpha_5+\alpha_5\alpha_3 = -\alpha_5, \\ (26) = \alpha_2\beta_6+\alpha_6\beta_2 = 0, & \alpha_2\alpha_6+\alpha_6\alpha_2 = -\alpha_6, \\ (36) = \alpha_3\beta_6+\alpha_6\beta_3 = 0, & \alpha_3\alpha_6+\alpha_6\alpha_3 = -\alpha_6. \end{cases}$$

Zunächst folgt aus (A) und (B) ein Hoffnungsstrahl! Es wird nämlich

$$(F)\qquad \alpha+\beta = 2x_1-x_2-x_3, \quad \text{mithin} \quad \beta\alpha = \alpha\beta,$$

d. h. die linearen Factoren der Gruppen-Determinante sind alle permutabel mit einander, wodurch ihre Brauchbarkeit erheblich gewinnt.

Bedenkt man nun, dass aus (C) auch

$$\alpha_2^3 = \alpha_3^3 = 1,$$

ferner aus (D) z. B.

$$(\alpha_4\alpha_5)^2 = -1-\alpha_4\alpha_5 = \alpha_5\alpha_4, \quad (\alpha_4\alpha_5)^3 = (\alpha_5\alpha_4)^3 = 1,$$

und aus (C) und (E) z. B.

$$\alpha_2\alpha_4 = \alpha_4\alpha_2^2, \quad \alpha_4\alpha_2 = \alpha_2^2\alpha_4, \quad (\alpha_2\alpha_4)^2 = (\alpha_4\alpha_2)^2 = 1$$

folgt, so wird man fast mit Gewalt zu der Bemerkung getrieben, dass die 15 Bedingungen (C), (D), (E) widerspruchsfrei erfüllt werden,

wenn man zum Beispiel annimmt, dass die sechs Zahlen α_r bei ihrer Multiplication die Gesetze unserer Gruppe

(G)

1	α_2	α_3	α_4	α_5	α_6
α_2	α_3	1	α_5	α_6	α_4
α_3	1	α_2	α_6	α_4	α_5
α_4	α_6	α_5	1	α_3	α_2
α_5	α_4	α_6	α_2	1	α_3
α_6	α_5	α_4	α_3	α_2	1

befriedigen, und dass ausserdem die beiden Summen

(H) $$\eta = 1 + \alpha_2 + \alpha_3, \quad \omega = \alpha_4 + \alpha_5 + \alpha_6$$

verschwinden; zugleich bilden dann die Zahlen β_r^{-1} eine isomorphe Gruppe.

Mit diesem Ergebniss habe ich mich damals (am 3. Februar 1886) durchaus begnügt, und ich bin, weil es mir sehr merkwürdig schien, gleich zu anderen Beispielen übergegangen, erst zu einer Gruppe zehnten Grades, dann aber zu der Quaternion-Gruppe (deren Existenz nahe lag, mir aber bis dahin wahrscheinlich unbekannt geblieben war), und hier wurde ich durch das Auftreten der Summe von vier Quadraten beglückt. Damals habe ich auch zuerst Beispiele von Normalkörpern mit Quaternion-Gruppe construirt, was mir erst nach mehreren vergeblichen Versuchen gelang, als ich erkannte, dass der darin enthaltene biquadratische Abel'sche Körper (Product von drei quadratischen Körpern) durchaus reell sein muss. Dass aber diese Quaternion-Gruppe eine so grosse Rolle in den nicht Abel'schen (Hamilton'schen) Gruppen spielt, die nur Normaltheiler besitzen, habe ich erst im vorigen Jahre gefunden (zu der Vollendung der Abhandlung bin ich aber noch immer nicht gekommen).

Ich kehre zu dem obigen Beispiele der Versetzungen von drei Buchstaben zurück. Offenbar ist die durch (G) in Verbindung mit $\eta = 0$, $\omega = 0$ bestimmte Lösung der Bedingungen (C), (D), (E) nur eine particuläre, wie man schon daraus erkennt, dass die letzteren symmetrisch sowohl in Bezug auf α_2, α_3, als auch in Bezug auf α_4, α_5, α_6 sind. Aber wahrscheinlich giebt es ausser diesen zwei Lösungen

noch unendlich viele andere Arten, die sämmtlichen Producte der Zahlen α_r linear durch die letzteren so darzustellen, dass die Bedingungen (C), (D), (E) erfüllt werden unter Wahrung des associativen und distributiven Gesetzes. Man kann nämlich zwar leicht beweisen, dass

$$\eta^2 = 0, \quad \omega^2 = 0, \quad \eta\omega + \omega\eta = 0$$

sein muss; dass aber η und ω selbst $= 0$ sein müssen, habe ich nicht herstellen können. Freilich dürfte man ja sagen: da u_1, u_2 nur von den Differenzen $x_2 - x_1$, $x_3 - x_1$, und ebenso v_1, v_2 nur von den Differenzen $x_5 - x_4$, $x_6 - x_4$ abhängen, so kann man von vornherein verlangen, dass auch α, β nur von diesen vier Differenzen abhängen, worin ja die Bedeutung der Bedingungen $\eta = 0$, $\omega = 0$ liegt. Da ferner diese Differenzen umgekehrt durch die vier unabhängigen Variabelen u_1, u_2, v_1, v_2 sich ausdrücken lassen, so kommt das Ganze schliesslich auf eine Zerlegung der bilinearen Form oder Determinante

$$u_1 u_2 - v_1 v_2 = \alpha\beta$$

in lineare Factoren

$$\alpha = \varkappa_1 u_1 + \varkappa_2 u_2 + \lambda_1 v_1 + \lambda_2 v_2, \quad \beta = \mu_1 u_1 + \mu_2 u_2 + \nu_1 v_1 + \nu_2 v_2$$

hinaus, wo die Coefficienten $\varkappa$, λ, μ, ν zufolge der obigen Lösung sehr niedliche Theiler der Null werden!

Ich habe mich in der letzten Woche ziemlich viel mit den Bedingungen (C), (D), (E) beschäftigt, und wenn Sie es wünschen, so will ich Ihnen gern noch Alles aufschreiben, was ich dabei gefunden habe. Aber ich halte es für sehr wohl möglich, dass Sie nach der heutigen Probe auf die ganze Zerlegung in hypercomplexe Factoren gar keinen Werth legen; meine eigene Meinung darüber schwankt hin und her. . . .

5. Dezember 1896*).

. . . Die Correctur**) habe ich sogleich mit dem besten Willen angegriffen, die Sache selbst dabei gründlich durchzunehmen, aber ich habe bald eingesehen, dass ich dazu viel mehr Zeit gebrauchen würde, als Ihnen erwünscht wäre; mein Anlauf hat daher nur bis etwa zur zehnten Seite ausgereicht, und dann habe ich mich begnügt, das

*) [In die Zwischenzeit fällt ein Besuch von Frobenius, auf den sich die Bemerkung über Anregung zur Darstellungstheorie (Einleitung zu der Arbeit über Darstellung endlicher Gruppen) zu beziehen scheint, da die Briefe nichts über Darstellung enthalten. E. N.]

**) [Es handelt sich um die Frobeniussche Arbeit über die Primfaktoren der Gruppendeterminante. E. N.]

Übrige nur durchzulesen, um den hauptsächlichen Inhalt in mich aufzunehmen. Derselbe erfüllt mich mit aufrichtiger Bewunderung; so schwierig die grosse Aufgabe war, so belohnend ist auch die Frucht Ihrer gewaltigen Arbeit geworden, die Ihrem Ruhmeskranze ein neues Blatt hinzufügt. Mir gefällt noch ganz besonders, dass nun auch Ihre Vorarbeiten in neuem Lichte erscheinen.

Alles Dies würde ich, wie ich Ihnen schon einmal gesagt habe, niemals zu Stande gebracht haben, aber desto mehr freue ich mich, Ihnen die erste Veranlassung zu dieser schönen Arbeit gegeben zu haben. . . .

13. April 1897.

. . . Ich bin daher auch noch nicht im Stande, Ihre Mittheilungen über die Gruppen mit der erforderlichen vollständigen Klarheit in mich aufzunehmen; aber eine große Freude haben Sie mir doch durch dieselben bereitet; denn soweit ich sie verstehe, bleibt mir kein Zweifel, dass Sie einen neuen grossen Schritt auf Ihrer Siegesbahn gethan haben, und wenn dabei mein Luftschloss der Scheinzahlen vernichtet wird, so bin ich gar nicht betrübt darüber, sondern erfreut, dass Sie den wirklichen Kern der Sache aufdecken; auch zweifle ich gar nicht, dass Sie die letzten Schwierigkeiten ebenso überwinden werden wie im vorigen Jahr*). . . .

*) [Gemeint ist die mehrfach erwähnte Zerlegung in hyperkomplexe Faktoren. Diese spielt eine wesentliche Rolle in der Theorie der nichtkommutativen Körper und deren Zerfällungskörper (vgl. Wedderburn, Transactions of the Am. Math. Soc., Bd. XXII, S. 129—135, 1921; die Wiedergabe bei Dickson: Algebras and their Arithmetics, S. 230 und weitergehende Untersuchungen von E. Noether und R. Brauer; zusammenfassende Darstellung bei v. d. Waerden, Moderne Algebra, Bd. II). Bei dem Dedekindschen Beispiel (Brief vom 13. Juli 1896) handelt es sich um den durch das „allgemeine Element“ α (der entsprechenden zweiseitigen Komponente des Gruppenrings) erzeugten Zerfällungskörper, und um die Zerlegung der Norm von α in diesem (kommutativen) Körper; daher die Vertauschbarkeit $\alpha\beta = \beta\alpha$ (Formel (F)).

Daß die Zerlegung bei Frobenius nicht auftritt, erklärt sich daraus, daß Frobenius von vornherein den Körper aller komplexen Zahlen, also einen algebraisch abgeschlossenen Körper, als Koeffizientenbereich nimmt; hier gibt es keine endlichen nichtkommutativen Erweiterungskörper. Die durch das allgemeine Element erzeugten Zerfällungskörper existieren zwar, aber ihre Heranziehung wird unnötig. Das gilt übrigens auch von dem Dedekindschen Beispiel (nicht von dem Beispiel des Quaternionenkörpers), wo es sich schon um einen vollen Matrizenring über dem Körper der rationalen Zahlen handelt; wie Dedekind bemerkt, treten ja Teiler der Null bei der hyperkomplexen Zerlegung der Gruppendeterminante auf. E. N.]